2021–2023

MP2I
MPI⋆

Hugo Salou

Table des matières

I MP2I – Informatique **25**

0 Structures de données : arbres **27**
.0 I. Introduction - définition . . . 27
.0.0 Utilisation des arbres . . . 27
.0.0 Classification . . . 28
.0.0 Définitions . . . 28
.0.0 Définition inductive . . . 30
.0.0 Remarques : . . . 30
.0 II. Arbres particuliers . . . 31
.0.0 Définitions . . . 31
.0.0 Propriétés . . . 32
.0.0 Transformation d'un arbre en arbre binaire . . . 33
.0.0 Arbres binaires : implémentation sous forme de tableau en C (sérialisation) . . . 40
.0.0 Arbres binaires de recherche . . . 43
.0.0 Arbres binaires bicolores (rouge - noir) . . . 46
.0 III. Parcours d'arbres . . . 51
.0.0 Définition . . . 51
.0.0 Utilisation des arbres . . . 51
.0.0 Parcours en profondeur . . . 51
.0.0 Parcours en profondeur : arbre d'expression . . . 53
.0.0 Parcours en largeur . . . 57
.0 IV. Implémentation . . . 58
.0.0 Arbres binaires de recherche . . . 58
.0.0 Arbre bicolore . . . 60
.0.0 Équilibrage des arbres (arbres binaires de recherche) . . . 60
.0 V. Tas et files de priorité . . . 63
.0.0 Tas : définition . . . 63
.0.0 Implémentation des tas . . . 65
.0.0 Opérations sur les tas . . . 67
.0.0 Tri par tas (*heap sort*) . . . 68
.0.0 Files de priorité . . . 69

0 Structures de données : graphes **71**
.0 I. Introduction . . . 71
.0 II. Définitions . . . 72
.0.0 Graphes non orientés . . . 72

.0.0 Graphes orientés . . . 73
.0.0 Graphes pondérés . . . 74
.0.0 Graphes bipartis . . . 75
.0 III. Implémentation . . . 76
.0.0 Listes d'adjacences . . . 76
.0.0 Matrices d'adjacence . . . 80
.0 III. Parcours de graphe . . . 81
.0.0 Définitions . . . 81
.0.0 Parcours en largeur . . . 82
.0 IV. Algorithmes des graphes . . . 84
.0.0 Algorithmes du plus court chemin . . . 84

0 Bases de données 93
.0 I. Introduction . . . 93
.0.0 Besoin . . . 93
.0.0 Définition d'une relation . . . 93
.0.0 Vocabulaire . . . 94
.0.0 Opérations sur les données . . . 94

0 Méthodes de programmation : diviser pour régner 99
.0 Introduction . . . 99
.0 I. Principe . . . 99
.0.0 a. Diviser . . . 99
.0.0 b. Régner . . . 100
.0.0 c. Combiner . . . 100
.0.0 Coût temporel : . . . 101
.0 II. Exemples déjà vus en cours . . . 101
.0 III. Autres exemples . . . 101
.0.0 Algorithmes de tri . . . 101
.0.0 Tri fusion : . . . 101
.0.0 Tri rapide . . . 103

0 Méthodes de programmation : programmation dynamique 105
.0 I. Introduction - Cadre pour l'algorithmique . . . 105
.0.0 Problème de décision (ou reconnaissance) . . . 106
.0.0 Problème de recherche . . . 106
.0.0 Problème de dénombrement . . . 107
.0.0 Problème d'optimisation . . . 107
.0.0 Problème de fonction . . . 107
.0 II. Programmation dynamique : exemple . . . 108
.0.0 Découpe de barres d'acier . . . 108
.0 III. Principe de la programmation dynamique . . . 111
.0.0 Historique . . . 111
.0.0 Cadre d'utilisation . . . 111
.0.0 Conception . . . 111
.0.0 Bilan . . . 113

0 Méthodes de programmation : algorithmes gloutons 115
.0 II. Exemple : choix d'activités . . . 115
.0.0 Bilan . . . 118

.0 III. Codage Huffman 118
.0.0 Exemple : 119
.0.0 Construction du codage de Huffman 121
.0.0 Démonstration du lemme 1 122
.0.0 Démonstration du lemme 2 124

0 Projets **125**
.0 I. n reines – backtracking 125
.0.0 Groupe A. Iba, Antoine R., Bastien D., Arthur 125
.0.0 Groupe B. Narada, Nicolas, Charlotte, Alan 126
.0 II. Boyer-Moore – Recherche d'un motif 126
.0.0 Groupe A. Ruben, Noémie, Alex, Juliette, Antoine V. . . 126
.0.0 Groupe B. Khadim, Iwan, Émile, Tibério 127
.0 III. Résolution de Sudoku – Backtracking 127
.0.0 Groupe A. Bastien F., Thomas, Timothée S., Hugo 127
.0.0 Groupe B. Aubin, Samy, Kyriann 127
.0 IV. Compression Lempel-Ziv-Welch 128
.0.0 Groupe A. Dorian, Lucine, Benoît, Kilian, Nathan R. . . 128
.0.0 Groupe B. Timothée N-L., Nathan S., Lilian, Loïc 128
.0 II. Rabin-Karp – Recherche d'un motif 129
.0.0 Groupe A. Nathan F., Ywan, Damien, Corentin, Germain 129
II.5.2 Groupe B. Martin, Louis, Ilan, Valentin 130

II MP2I – Mathématiques – Cours **131**

0 Logique (rudiments) **133**
1 Algèbre de Boole 133
2 Déduction naturelle 136
3 Raisonement par l'absurde 137
4 Prédicat 137

1 Calculs algébriques **139**
1 Sommes 139
2 Formules à connaître 145
3 Sommes doubles 149
4 Sommes sur un ensemble fini 150
5 Produits 151
6 Rappels sur ln et exp 152

2 Nombres complexes **155**
1 Trigonométrie 155
2 Nombres complexes de module 1 159
3 Géométrie des nombres complexes 162
4 Exponentielle complexe 171
5 Fonctions de $\mathbb{R}$ dans $\mathbb{C}$ 172

3 Étude de fonctions **179**
1 Calculs de limites 180
2 Asymptotes, branches paraboliques et prolongement par continuité 182

4 Fonctions usuelles **185**
1 Logarithme népérien . . . 185
2 Exponentielle . . . 190
3 Fonctions puissances . . . 191
4 Exponentielle et logarithme de base a . . . 195
5 Fonctions trigonométriques . . . 197
6 Fonctions trigonométriques réciproques . . . 200
7 Trigonométrie hyperbolique . . . 208

5 Calcul intégral **213**
1 Généralités . . . 213

6 Équations différentielles linéaires **217**
1 . . . 219
2 Annexe . . . 220

7 Développements limités **223**

8 Ensembles, applications, relations et lois de composition **229**
1 Théorie naïve des ensembles . . . 229
2 Applications . . . 234
3 Relations binaires . . . 241
4 Lois de composition . . . 251
5 Divers . . . 255

9 Inégalités dans $\mathbb{R}$ **261**
1 . . . 261
2 . . . 261
3 . . . 261
4 Bornes supérieures . . . 261
5 Partie entière . . . 264
6 Densité . . . 265
7 . . . 266
8 . . . 266
9 Propriétés de $(\mathbb{R}, \leq)$ . . . 269
10 Inégalités Classiques . . . 272
11 Valeur Absolue . . . 276
12 Bornes Inférieure / Supérieure . . . 276
13 Partie Entière . . . 280
14 Densité . . . 281
15 Intervalles . . . 283
16 Fonction Convexes . . . 286

10 Nombres entiers - $\mathbb{N}$ **295**
1 Axiomatique de $\mathbb{N}$ . . . 295
2 Récurrence . . . 296
3 Divisibilité . . . 299
4 Arithmétique modulaire . . . 303
5 Axiomatique de $\mathbb{N}$ . . . 306
6 Récurrences . . . 308
7 Divisibilité . . . 309

8 Division Euclidienne . . . 310
9 Arithmétique Modulaire . . . 312
10 PCGD et PPCM . . . 315
11 Décomposition en Facteurs Premiers . . . 322

11 Suites numériques 327
1 Modes de définition . . . 327
2 Limites . . . 327
3 Limites et inégalités . . . 336
4 Suites extraites . . . 343
5 Suites récurrentes . . . 348
6 Comparaison de suites . . . 350
7 Suites complexes . . . 355
8 Annexe . . . 358

12 Structures algébriques usuelles 361
1 Groupes . . . 361
2 Anneaux . . . 374
3 Corps . . . 382
4 Actions de groupes . . . 384
5 Bilan . . . 385

13 Systèmes linéaires et calculs matriciels 387

14 Continuité 399
1 Définition d'une limite de fonctions . . . 399
2 Continuité uniforme . . . 411
3 Fonctions à valeurs dans $\mathbb{C}$ . . . 415
4 Annexe . . . 416

15 Espaces vectoriels 419
1 Définition et premières propriétés . . . 419
2 Sous-espaces vectoriels . . . 421
3 Familles de vecteurs . . . 432

16 Dérivation 443
1 Définition et premières propriétés . . . 443
2 Théorème de Rolle et accroissements finis . . . 446
3 Dérivées n-ièmes . . . 450
4 Fonctions à valeurs complexes . . . 455

17 Dimension finie 457

18 Polynômes formels 467
1 Définition . . . 467
2 Évaluation . . . 474
3 Arithmétique dans $\mathbb{K}[X]$ . . . 479
4 L'espace vectoriel $\mathbb{K}[X]$ . . . 494

19 Applications linéaires 503
1 Premières propriétés . . . 503

2 Noyau et image . . . 507
3 Théorème du rang . . . 509
4 Formes linéaires . . . 513
5 Projections et symétries . . . 519

20 Fractions rationnelles **527**
1 Construction de $\mathbb{K}(X)$ . . . 527
2 Décomposition en éléments simples . . . 533

21 Matrices et applications linéaires **547**
1 Matrices d'un vecteur . . . 547
2 Matrice d'une famille de vecteurs . . . 548
3 Matrices d'une application linéaire . . . 552
4 Formules de changement de bases . . . 559
5 Conséquences . . . 567
6 Matrices par blocs . . . 573

22 Fonctions de deux variables **577**
1 Quelques généralités . . . 577
2 Topologie de $\mathbb{R}^2$ . . . 578
3 Dérivation . . . 586

23 Dénombrement **599**
1 Cardinal d'un ensemble . . . 599
2 Dénombrement . . . 607
3 Preuves combinatoires . . . 614
4 Bilan . . . 616

24 Groupe symétrique **619**
1 Mise en situation . . . 619
2 Cycles . . . 621
3 Transpositions . . . 627
4 Signature d'une permutation . . . 628
5 Bilan . . . 631

25 Séries numériques **633**
1 Défintions et premières propriétés . . . 633
2 Séries à termes positifs . . . 635
3 Comparaison avec une intégrale . . . 637
4 Opérations sur les séries . . . 640
5 Séries absolument convergente . . . 641
6 Séries alternées . . . 643
7 Résumé et exemples . . . 644
8 Applications . . . 647
8.1 Formule de Stirling . . . 647
8.2 Développement décimal . . . 651
8.3 Exponentielle . . . 655

26 Déterminant **657**
1 Motivation . . . 657
2 Définitions . . . 658

3 Déterminant d'un endomorphisme 663
4 Déterminant d'une matrice carrée 665
5 Développement suivant une ligne ou une colonne 670

27 Espace probabilisé fini 677
1 Définitions 677
2 Probabilité conditionnelle 680
3 Événements indépendants 687
4 Bilan 690

28 Sous-espaces affines d'un espace vectoriel 693
1 Espace affine (Hors Programme) 693
2 Sous-espaces affines 697
3 Parallèlisme et hyperplans 698
4 Repère affine 699

29 Produit scalaire 701
1 Définitions 701
2 Quelques formules 703
3 Familles orthogonales 706
4 Projection orthogonale 712
5 Annexe 718
5.1 Produit vectoriel 718
5.2 Calcul différentiel 721
5.3 Séries de Fourier 721
5.4 Espace-temps de Minkowsky 723

30 Intégrale de Riemann 725
1 Intégrale d'une fonction en escaliers 725
2 Sommes de Darboux 727
3 Propriétés de l'intégrale 730
4 Théorème fondamental de l'Analyse 736
5 Fonctions continues par morceaux 738
6 Sommes de Riemann 739
7 Retour sur les formules de Taylor 741
8 Fonctions réglées 743

31 Variables aléatoires 745
1 Définitions 745
2 Exemples de lois 746
3 Couples de variables aléatoires 747
4 Familles de variables aléatoires 749
5 Espérance d'une variable aléatoire 750
6 Variance 754
7 Covariance (Hors-Programme) 759
8 Loi des grands nombres 760

32 Familles sommables 765
1 Motivation 765
2 Familles sommables positives 765
3 Familles sommables réelles 770

4 Familles sommables de nombres complexes . . . 775
5 Produit de Cauchy de deux séries . . . 776

33 Annexe **779**
1 Algorithme de Metropolis-Hastings . . . 779
2 Gradient automatique . . . 780

III MP2I – Mathématiques – TDs **783**

11 TD 11 **785**
.0 Exercice 3 . . . 785
.0 Exercice 6 . . . 786
.0 Exercice 7 . . . 787
.0 Exercice 9 . . . 788
.0 Exercice 10 . . . 789
.0.1 Méthode 1 . . . 789
.0.2 Méthode 2 . . . 790
.0 Exercice 11 . . . 790
.0 Exercice 12 . . . 792
.0 Exercice 3 . . . 792
.0 Exercice 14 . . . 792
.0 Exercice 19 . . . 793
.0 Exercice 21 . . . 795
.0 Exercice 23 . . . 796
.0 Exercice 23 . . . 799
.0 Exercice . . . 801
.0 Exercice . . . 803

12 TD 12 **805**
.0 Exercice 2 . . . 805
.0 Exercice 3 . . . 806
.0 Exercice 6 . . . 806
.0 Exercice 7 . . . 806
.0 Exercice 10 . . . 806
.0 Exercice 12 . . . 807
.0 Exercice 15 . . . 808
.0 Exercice 19 . . . 808
.0 Exercice 20 . . . 809

13 TD 13 **811**
.0 Exercice 5 . . . 811
.0 Exercice 9 . . . 812
.0 Exercice 10 . . . 812

14 TD 14 **815**
.0 Exercice 1 . . . 815
.0 Exercice 2 . . . 816
.0 Exercice 3 . . . 816
.0 Exercice 4 . . . 816

.0 Exercice 5 . . . 817
.0 Exercice 6 . . . 817
.0 Exercice 7 . . . 818
.0 Exercice 8 . . . 818
.0 Exercice 9 . . . 819
.0 Exercice 10 . . . 819
.0 Exercice 11 . . . 820
.0 Exercice 12 . . . 820
.0 Exercice 13 . . . 821

15 TD 15 **823**
.0 Exercice 3 . . . 823
.0 Exercise 7 . . . 824
.0 Exercice 8 . . . 824
.0 Exercice 9 . . . 825
.0 Exercise 10 . . . 825
.0 Exercice 11 . . . 827
.0 Exercice 12 . . . 830

16 TD 16 **831**
.0 Exercice 1 . . . 831
.0 Exercice 2 . . . 831
.0 Exercice 3 . . . 831
.0 Exercice 4 . . . 832
.0 Exercice 5 . . . 832
.0 Exercice 7 . . . 833

17 TD 17 **837**
.0 Exercice 4 . . . 837
.0 Exercice 5 . . . 842
.0 Exercice 6 . . . 844
.0 Exercice 7 . . . 844
.0 Exercice 8 . . . 845
.0 Exercice 9 . . . 846

18 TD 18 **849**
.0 Exercice 1 . . . 849
.0 Exercice 2 . . . 849
.0 Exercice 4 . . . 850
.0 Exercice 5 . . . 851
.0 Exercice 7 . . . 851
.0 Exercice 8 . . . 852
.0 Exercice 10 . . . 853
.0 Exercice 11 . . . 854
.0 Exercice 12 . . . 854
.0 Exercice 13 . . . 855
.0 Exercice 15 . . . 855
.0 Exercice 17 . . . 856
.0 Exercice 18 . . . 857
.0 Exercice 19 (supplémentaire) . . . 861

19 TD 19 **863**
.0 Exercice 1 . . . 863
.0 Exercice 3 . . . 864
.0 Exercice 6 . . . 866
.0 Exercise 7 . . . 867
.0 Exercice 9 . . . 869
.0 Exercise 10 . . . 871
.0 Exercice 11 . . . 871
.0 Exercice 12 . . . 873

20 TD 20 **877**
.0 Exercice 2 . . . 877
.0 Exercice 5 . . . 881
.0 Exercice 6 . . . 881
.0 Exercice 7 . . . 882

21 TD 21 **885**
.0 Exercice 1 . . . 885
.0 Exercice 2 . . . 886
.0 Exercice 4 . . . 887
.0 Exercice 5 . . . 888
.0 Exercice 7 . . . 890
.0 Exercice 8 . . . 891

22 TD 22 **899**
.0 Exercice 2 . . . 899
.0 Exercice 3 . . . 900
.0 Exercice 4 . . . 900
.0 Exercice 6 . . . 901
.0 Exercice 7 . . . 902
.0 Exercice 8 . . . 903
.0 Exercice 9 . . . 904
.0 Exercice 10 . . . 905
.0 Exercice 11 . . . 906
.0 Exercice 12 . . . 907

23 TD 23 **909**
.0 Exercice 1 . . . 909
.0 Exercice 2 . . . 909
.0 Exercice 3 . . . 911
.0 Exercice 4 . . . 911
.0 Exercice 5 . . . 911
.0 Exercice 6 . . . 912
.0 Exercice 7 . . . 912
.0 Exercice 8 . . . 913
.0 Exercice 10 . . . 915
.0 Exercice 11 . . . 916
.0 Exercice 12 . . . 917
.0 Exercice 13 . . . 918
.0 Exercice 14 . . . 919

24 TD 24 **921**
.0 Exercice 2 . . . 921
.0 Exercice 3 . . . 922
.0 Exercice 4 . . . 923
.0 Exercice 5 . . . 923
.0 Exercice 6 . . . 923
.0 Exercice 7 . . . 923
.0 Exercice 8 . . . 924

25 TD 25 **925**
.0 Exercice 1 . . . 925
.0 Exercice 2 . . . 926
.0 Exercice 3 . . . 926
.0 Exercice 4 . . . 927
.0 Exercice 5 . . . 927
.0 Exercice 6 . . . 929
.0 Exercice 7 . . . 930
.0 Exercice 8 . . . 931
.0 Exercice 9 . . . 932
.0 Exercice 10 . . . 932
.0 Exercice 11 . . . 934
.0 Exercice 12 . . . 934
.0 Exercice . . . 937

26 TD 26 **939**
.0 Exercice 2 . . . 939
.0 Exercice 3 . . . 939
.0 Exercice 4 . . . 940
.0 Exercice 6 . . . 941
.0 Exercice 7 . . . 941
.0 Exercice 8 . . . 945
.0 Exercice 9 . . . 945
.0 Exercice 10 . . . 945
.0 Exercice . . . 945

27 TD 27 **947**
.0 Exercice 1 . . . 947
.0 Exercice 2 . . . 948
.0 Exercice 3 . . . 948
.0 Exercice 4 . . . 948
.0 Exercice 5 . . . 949
.0 Exercice 6 . . . 950
.0 Exercice 7 . . . 950
.0 Exercice 8 . . . 951
.0 Exercice 9 . . . 953
.0 Exercice 10 . . . 954
.0 Exercice 11 . . . 954
.0 Exercice 12 . . . 955
.0 Exercice 13 . . . 956
.0 Exercice 14 . . . 957

28 TD 28 **959**
.0 Exercice 1 . . . 959
.0 Exercice 2 . . . 959
.0 Exercice 3 . . . 960
.0 Exercice 4 . . . 961
.0 Exercice 5 . . . 962

29 TD 29 **963**
.0 Exercice 1 . . . 963
.0 Exercice 2 . . . 964
.0 Exercice 3 . . . 964
.0 Exercice 4 . . . 965
.0 Exercice 5 . . . 966
.0 Exercice 6 . . . 967
.0 Exercice 7 . . . 968
.0 Exercice 8 . . . 969
.0 Exercice 9 . . . 970
.0 Exercice 10 . . . 971
.0 Exercice 11 . . . 971
.0 Exercice 12 . . . 972
.0 Exercice 13 . . . 973
.0 Exercice 14 . . . 973
.0 Exercice 15 . . . 974

30 TD 30 **975**
.0 Exercice 1 . . . 975
.0 Exercice 2 . . . 975
.0 Exercice 3 . . . 976
.0 Exercice 4 . . . 977
.0 Exercice 5 . . . 977
.0 Exercice 6 . . . 978
.0 Exercice 7 . . . 979
.0 Exercice 8 . . . 980
.0 Exercice 9 . . . 980
.0 Exercice 10 . . . 981

31 TD 31 **983**
.0 Exercice 1 . . . 983
.0 Exercice 2 . . . 983
.0 Exercice 3 . . . 984
.0 Exercice 4 . . . 984
.0 Exercice 5 . . . 985
.0 Exercice 6 . . . 986
.0 Exercice 7 . . . 986
.0 Exercice 8 . . . 987
.0 Exercice 9 . . . 988
.0 Exercice 10 . . . 989

32 TD 32 **991**
.0 Exercice 1 . . . 991

.0 Exercice 2 992
IV.3 Exercice 4 993

IV MPI – Informatique – Cours 995

-1 Ordres et induction 997
IV.1 Motivation 997
IV.2 Ordre 999
IV.2.1 Ordre produit 1000
IV.2.2 Ordre lexicographique 1003
IV.3 Induction nommée 1006
IV.4 Synthèse du chapitre 1012

0 Logique 1015
IV.1 Motivation 1015
IV.2 Syntaxe 1016
IV.3 Sémantique 1019
IV.3.1 Algèbre de Boole 1019
IV.3.2 Fonctions booléennes 1020
IV.3.3 Interprétation d'une formule comme une fonction booléenne 1021
IV.3.4 Liens sémantiques 1022
IV.4 Le problème Sat – Le problème Validité 1023
IV.4.1 Résolution par tables de vérité 1024
IV.5 Représentation des fonction booléennes 1024
IV.5.1 Par des formules ? 1024
IV.5.2 Par des formules sous formes normales ? 1027
IV.6 Algorithme de Quine 1030
IV.7 Synthèse du chapitre 1035

1 Langages réguliers et Automates 1037
IV.1 Motivation 1037
IV.1.1 $1^{\underline{\text{ère}}}$ motivation 1037
IV.1.2 $2^{\underline{\text{nde}}}$ motivation 1037
IV.2 Mots et langages, rappels 1038
IV.3 Langage régulier 1040
IV.3.1 Opérations sur les langages 1040
IV.3.2 Expressions régulières 1041
IV.4 Automates finis (sans ε-transitions) 1044
IV.4.1 Définitions 1044
IV.4.2 Transformations en automates équivalents 1047
IV.5 Automates finis avec ε-transitions 1051
IV.5.1 Cloture par concaténation 1052
IV.5.2 Cloture par étoile 1054
IV.5.3 Cloture par union 1054
IV.6 Théorème de Kleene 1057
IV.6.1 Langages locaux 1057
IV.6.2 Expressions régulières linéaires 1062
IV.6.3 Automates locaux 1065

IV.6.4 Algorithme de Berry-Sethi : les langages réguliers sont reconnaissables 1069
IV.6.5 Les langages reconnaissables sont réguliers 1070
IV.7 La classe des langages réguliers 1074
IV.7.1 Limite de la classe/Lemme de l'étoile 1075
Annexe 1.A Comment prouver la correction d'un programme ? 1078
Annexe 1.B Hors-programme 1079

2 Algorithmes probabilistes 1081
IV.1 Introduction 1081
IV.2 Algorithme de Monte-Carlo 1084
IV.3 Algorithme de type Las-Vegas 1086
Annexe 2.A Hors-programme 1093

3 Apprentissage 1095
IV.1 Motivation 1095
IV.2 Vocabulaire 1095
IV.3 Apprentissage supervisé 1096
IV.3.1 k plus proches voisins 1097
IV.3.2 Arbres k-dimensionnels 1099
IV.3.3 Algorithme id3 1100
IV.4 Apprentissage non supervisé 1106
IV.4.1 Algorithme hac, classification hiérarchique ascendant . . .1106
IV.4.2 k-moyenne 1106

4 Calculabilité, Décidabilité, Complexité 1109
IV.1 Remarques mathématiques 1109
IV.2 Problèmes 1110
IV.3 Décidabilité 1111
IV.3.1 Modèles de calcul 1111
IV.3.2 Décidabilité 1112
IV.3.3 Langages et problèmes de décision 1114
IV.3.4 Sérialisation 1115
IV.3.5 Machine universelle 1116
IV.3.6 Théorème de l'Arrêt 1117
IV.3.7 Réduction 1118
IV.4 Classe **P** et **NP** 1120
IV.4.1 Complexité d'une machine 1120
IV.4.2 Classe **P** 1120
IV.4.3 Classe **NP** 1122
IV.4.4 **NP**-difficile 1123

5 Trois exemples d'algorithmes de graphes 1129
IV.1 Composantes fortement connexes (cfc) 1129
IV.1.1 Rappels 1131
IV.1.2 Rangement particulier de graphe 1133
IV.1.3 Graphe transposé et cfc 1135
IV.1.4 Calcul de tri préfixe 1137
IV.1.5 Algorithme de Kosaraju 1138
IV.1.6 Applications 1138

IV.2 Arbres couvrants de poids minimum 1141
IV.3 Couplage dans un graphe biparti 1146
Annexe 5.A Remarques supplémentaires 1150

6 Preuves **1151**
IV.0 Motivation 1151
IV.0.1 Tables de vérité 1151
IV.0.2 Équations 1152
IV.0.3 Raisonnement mathématiques 1152
IV.1 La déduction naturelle en logique propositionnelle 1152
IV.1.1 Séquents 1152
IV.1.2 Preuves 1153
IV.1.3 Déduction naturelle 1155
IV.2 La logique du premier ordre 1158
IV.2.1 Syntaxe de la logique du premier ordre 1159
IV.2.2 Substitution 1162
IV.2.3 Extension au premier ordre de la déduction naturelle . . . 1164
IV.2.4 Règles dérivées 1167
IV.2.5 Sémantique 1167
IV.3 Synthèse du chapitre 1171

7 Tentative de réponse à la NP-complétude **1173**
IV.0 Motivation 1173
IV.1 Problèmes d'optimisation 1173
IV.2 Algorithmes d'approximations 1175
IV.3 *Branch and Bound* — Séparation et évaluation 1179
Annexe 7.A Programmation dynamique 1182

8 Jeux **1185**
IV.1 Jeux sur un graphe 1185
IV.2 Résolution par heuristique 1192

9 Grammaires non contextuelles **1195**
IV.1 Définition, vocabulaire, propriétés 1196
IV.1.1 Grammaires non contextuelles 1196
IV.1.2 Dérivation 1197
IV.1.3 Preuves par induction 1199
IV.1.4 Définitions équivalentes 1200
IV.2 La hiérarchie de Chomsky 1203
IV.2.1 Avec les langages réguliers 1203
IV.2.2 Lien avec les langages décidables 1206

10 Concurrence **1207**
IV.1 Motivation 1207
IV.2 *Mutex* 1210
IV.2.1 À deux fils d'exécutions 1210
IV.2.2 À N fils d'exécutions 1212
IV.3 Sémaphore 1213

V MPI – Informatique – TDs 1215

1 Ordre & Induction 1217
V.1 Listes, listes, listes ! . . . 1217
V.2 Ensembles définis inductivement . . . 1218
V.3 Arbres, Arbres, Arbres ! . . . 1218
V.4 Ordre sur *powerset* . . . 1219
V.5 Ordres bien fondés en vrac . . . 1220
V.6 Définition inductive des mots et ordre préfixe . . . 1220
V.7 $\mathcal{N}$ . . . 1221
V.8 Résultats manquants du cours . . . 1222

2 Logique propositionnelle 1223
V.1 Logique avec `If` . . . 1223
V.1.1 Représentatibilité des fonctions booléennes par formules de $\mathcal{F}_{\texttt{if}}$ . . . 1223
V.2 Définitions de cours : syntaxe . . . 1224
V.3 Formules duales . . . 1226
V.4 Conséquence sémantique . . . 1227
V.5 Axiomatisation algèbre de Boole . . . 1227
V.6 Exercice 6 : Barre de Scheffer . . . 1227
V.7 Énigmes en logique propositionnelle . . . 1228
V.7.1 Fraternité . . . 1228
V.7.2 Alice au pays des merveilles . . . 1228
V.7.3 Socrate et Cerbère . . . 1229
V.8 Compléments de cours, en vrac . . . 1229

3 Langages et expressions régulières 1231
V.1 Propriétés sur les mots . . . 1231
V.2 Construction d'automates . . . 1232
V.3 Déterminisation 1 . . . 1233
V.4 Déterminisation 2 . . . 1233
V.5 Une équivalence sur les mots . . . 1234
V.6 Langages . . . 1234
V.7 Propriétés sur les opérations régulières . . . 1234
V.8 Habitants d'expressions régulières . . . 1236
V.9 Regexp Crossword . . . 1236
V.10 Description d'automates au moyen d'expression régulières . . . 1236
V.11 Vocabulaire des automates . . . 1236
V.12 Complétion d'automate . . . 1237
V.13 Exercice supplémentaire 1 . . . 1237

4 Langages et expressions régulières (2) 1239
V.1 Déterminisation de taille exponentielle . . . 1239
V.2 Suppression des ε-transitions . . . 1240
V.3 Déterminisation d'automates avec ε-transitions . . . 1240
V.4 Automates pour le calcul de modulo . . . 1242
V.5 Automates pour le calcul de l'addition en binaire . . . 1242
V.5.1 Nombres de même tailles . . . 1242

5 Langages et expressions régulières (3) 1243
V.1 Exercice 4 1243
V.2 Exercice 5 1244
V.3 Exercice 6 : Langages reconnaissables ou non 1244

6 Algorithmes probabilistes 1245
V.1 Exercice 1 : Vérification d'égalité polynomiale 1245
V.2 Test de primalité probabiliste 1246
V.2.1 Résultats mathématiques 1246
V.2.2 Algorithme 1246
V.2.3 Implémentation 1247
V.3 Exercice 3 : Échantillonnage 1247

7 Décidabilité, Calculabilité 1249
V.1 Quelques problèmes décidables 1249
V.2 Sérialisation de types énumérés 1249
V.3 Stabilité de la classe des langages décidables 1250
V.4 Non monotonie du caractère décidable des langages 1251
V.5 Réduction 1252
V.6 Amélioration de code 1254
V.7 Théorème de Rice 1255
V.8 Un changement de modèle de calcul 1255

8 Classe P, classe NP 1257
V.1 Problèmes de partitions 1257
V.2 Optimisation linéaire en nombres entiers 1258
V.3 Clique, Stable et Couv.Sommets 1258
V.4 1260

9 Algorithmique des graphes 1261
V.1 Arbres et forêts 1261
V.2 Tri topologique 1261
V.3 Détection de graphe biparti 1262
V.4 Exploration du graphe $\mathfrak{S}_n$ 1262
V.5 Parcours selon le miroir d'un tri préfixe 1262

10 Preuves en logique propositionnelle 1263
V.1 Premiers arbres de preuves 1264
V.2 Divers arbres de preuves 1264
V.3 Lois de de Morgan 1265
V.4 Distributivités entre $\wedge$ et $\vee$ 1265
V.5 Implications 1266
V.6 Implications (partie 1 : simplifications) 1267
V.7 Implications (partie 2 : transformations) 1269

11 Preuves 1273
V.1 Formalisation 1273
V.2 Variables libres et liées, clôture universelle 1273
V.3 Substitution 1274
V.4 Quelques arbres de preuves 1276
V.5 Distributivité des quantificateurs 1276

V.6 Semi-distributivité des quantificateurs 1277
V.7 Logique classique du premier ordre 1277

12 Algorithmes d'approximation 1279
V.1 Un problème proche de Knapsack 1279
V.2 Le problème BinPacking 1281
V.3 Le problème VoyageurCommerce 1281

13 Jeux 1283
V.1 Attracteurs pour le jeu de la soustraction généralisé 1283
V.2 Chomp 1284
V.3 Hex 1284
V.4 Calcul de MinMax 1284
V.5 Calcul de MinMax avec mémoïsation 1284

14 Grammaires non contextuelles (1) 1285
V.1 Exemples de dérivations 1285
V.2 Arbres de dérivations 1285
V.3 Construction de grammaires 1286
V.4 Raisonner par induction sur une grammaire 1287
V.5 Ambigüité 1287
V.6 Langage de Dyck 1287
V.7 Listes OCaml 1288
V.8 Mots de Łukasiewicz 1288

15 Grammaires non contextuelles (2) 1291
V.1 Forme normale conjonctive 1291
V.2 Réduction de grammaire et systèmes de conséquences 1292
V.2.1 Digression OCaml 1292
V.3 Grammaires propres 1292
V.4 Un lemme d'itération 1292
V.5 Les langages réguliers sont non contextuels 1292
V.5.1 Avec des automates 1292
V.5.2 Avec des expressions régulières 1293

16 Concurrence 1295
V.1 Entrelacements 1295
V.2 Généralisation de l'algorithme de Peterson à N fils 1295
V.3 Parallélisation pour le produit de deux matrices 1296
V.4 Calcul du maximum par "diviser pour régner" 1296
V.5 Un très mauvais algorithme de tri 1296

17 Concurrence 1297
V.1 Addition binaire en parallèle 1297
V.2 Producteurs–consommateurs en mémoire non bornée 1297
V.2.1 Version allégée de la solution vue en cours 1297
V.3 Rendez-vous à l'aide de sémaphores 1297
V.3.1 Deux fils d'exécutions se rencontrent une fois 1297
V.3.2 Plusieurs fils se rencontrent une fois 1298
V.3.3 Plusieurs fils d'exécution se rencontrent plusieurs fois . .1299

18 Complexité amortie **1301**
V.1 Complexité amortie 1301
V.2 Incrementation compteur binaire 1302
V.3 Tableaux dynamiques 1302
V.4 Tableaux dynamiques, 2 1302

19 Diviser pour régner **1303**
V.1 Suites récurrentes de complexité 1303
V.2 Multiplication d'entiers par algorithme de Karatsuba 1304

VI MPI – Informatique – Annexes **1305**

1 Complexité amortie **1307**

2 Algorithmes Dijkstra et $A^\star$ **1313**

3 Diviser pour régner **1317**

4 Lemme d'Arden et retour sur le théorème de Kleene **1319**

5 Tas et files de priorités **1321**

6 Arithmétique **1323**

7 Arbres rouges-noirs **1325**

8 Complexité moyenne **1327**

9 Preuves de correction pour les fonctions récursives **1329**

VII MPI – Mathématiques – Cours **1331**

1 1 **1333**
VII.1La nature d'une suite ou d'une série 1333
VII.2Comparer série et intégrale 1335

2 Algèbre linéaire **1351**

3 Intégrer sur un intervalle **1369**
VII.1Intégrer une fonction continue par morceaux sur un segment . . . 1369
VII.2Qu'est ce qu'une intégrale généralisée ? 1369
VII.3Intégrer les $\sim$, $\wr$, et O 1372
VII.4La convergence absolue 1374
VII.5Intégrer par parties et changer de variables 1375

4 Diagonalisation & trigonalisation **1379**
VII.1(Ne pas) être diagonalisable 1379
VII.2Valeurs & vecteurs propres 1382
VII.3Le polynôme caractéristique 1383
VII.4Les sous-espaces propres 1389

VII.5Critères de diagonalisabilité 1393
VII.6Trigonalisation 1396
VII.7Le théorème de Cayley & Hamilton et les sous-espaces caractéristiques 1398
VII.8Polynômes annulateurs 1400
VII.9Stabilité 1402

5 Suites de fonctions **1407**
VII.1Deux manières de converger 1407
VII.2Continuité 1409
VII.3Intégrer 1411
VII.4Dériver 1415
VII.5Approximation uniforme par des polynômes 1417

6 Séries de fonctions **1421**
VII.1Trois manières de converger 1421
VII.1.1 Convergence simple et convergence uniforme 1421
VII.1.2 Convergence normale 1424
VII.2Continuité 1425
VII.3Intégrer 1427
VII.4Dériver 1429

7 Probabilités **1431**
VII.0Dénombrabilité 1431
VII.1Résultats et événements 1432
VII.2Probabilité 1433
VII.3La continuité (dé)croissante 1434
VII.4L'indépendance 1436
VII.5Probabilité conditionnelle 1438
VII.6La formule des probabilités totales 1439
VII.7La formule des probabilités composées 1441
VII.8Formule de Bayes 1442

8 Intégrales à paramètre **1445**
VII.1Continuité 1445
VII.2Dérivabilité 1448

9 Produits scalaires **1453**
VII.1Qu'est-ce qu'un produit scalaire ? 1453
VII.2(In)égalités 1457
VII.3Orthogonalité 1459
VII.4Bases orthonormées 1463
VII.5Lalgorithme de Gram-Schmidt 1463
VII.6Projection orthogonale (sur un *sev* de dimension finie) 1464
VII.7Hyperplans 1468

10 Séries entières **1471**
VII.1Rayon de convergence 1473
VII.2Convergence normale et continuité 1476
VII.3Intégrer 1476
VII.4Dériver 1477

VII.5(Ne pas) être développable en série entière 1480
VII.6Produit de Cauchy et somme de deux séries entières 1482
VII.7Séries entières complexes 1484

11 Variables aléatoires **1485**
VII.1Variables aléatoires discrètes 1485
VII.2La loi binomiale 1487
VII.3La loi géométrique 1488
VII.4La loi de Poisson 1490
VII.5Espérance 1492
VII.6Variance et écart-type 1495
VII.7Les inégalités de Markov et de Bienaymé–Tchebychev, inégalités de concentration 1498
VII.8Série génératrice 1500

12 Endomorphismes remarquables d'un espace euclidien **1503**
VII.1Qu'est ce qu'une matrice orthogonale ? 1503
VII.2Isométries vectorielles 1506
VII.3Endomorphismes adjoints 1509
VII.4Stabilité de l'orthogonal 1513
VII.5Le théorème spectral 1514
VII.6Rotations et réflexions 1518

13 Espaces vectoriels normés **1523**
VII.1Normes et distances 1523
VII.2Boules 1525
VII.3Limite d'une suite 1527
VII.4Comparer des normes 1529
VII.5Adhérence 1532
VII.6Limite d'une fonction 1534
VII.7Continuité d'une fonction 1536
VII.8Linéarité & continuité 1537
VII.9Norme subordonnée 1540
VII.10Ouverts et fermés 1543

14 Couples de variables aléatoires discrètes **1547**
VII.1Lois conjointe et marginales 1547
VII.2La somme de deux variables aléatoires 1549
VII.3Espérance et variance d'une somme 1551
VII.4La loi faible des grands nombres 1555

15 Calcul différentiel **1557**
VII.1Dérivées partielles 1559
VII.2Dérivées partielles 1559
VII.3La différentielle d'une fonction 1563
VII.4Le gradient 1569
VII.5La différentielle d'une composée 1575
VII.6Dérivées secondes 1578
VII.7Optimisation 1579

VIII MPI – Mathématiques – Annexes 1585

1 Structures algébriques et division euclidienne 1587
VIII.1 Division euclidienne 1587
VIII.2 Structures algébriques 1588
VIII.3 Idéaux 1590
VIII.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$ 1592
VIII.5 L'ordre d'un élément 1594

2 La compacité 1597

3 Séries de vecteurs et exponentielle de matrices 1601

4 Cadeaux 1607

Partie I

MP2I – Informatique

Chapitre

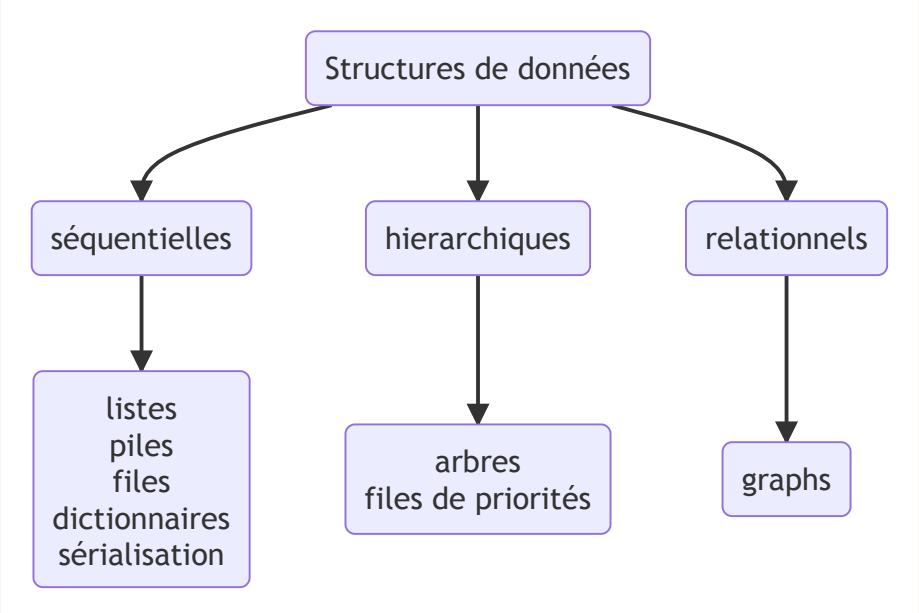
Structures de données : arbres

I. Introduction - définition

Utilisation des arbres

— Arbres syntaxiques
— Arbre lexicographique
— Arbre de décision / classification (ML)
— Compression de données
— Expressions mathématiques

Classification



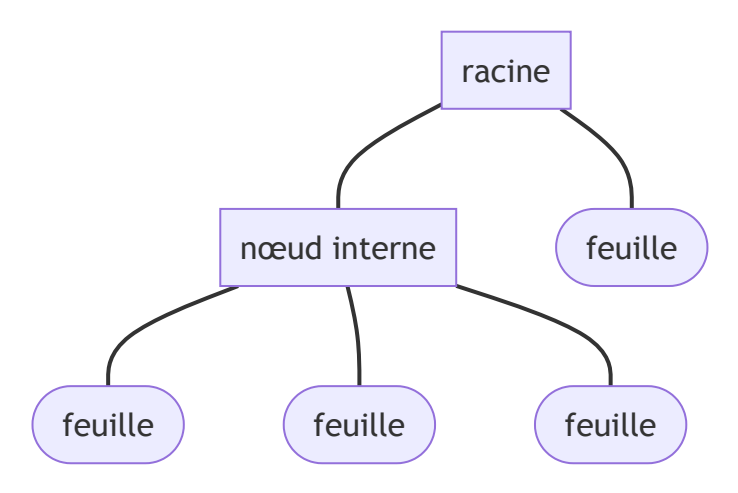
Définitions

Un arbre (enraciné) est

- soit un ensemble vide
- soit un ensemble fini non vide A muni d'une relation binaire $<$ (est le fils de ...) telle que
- il existe $r \in A$ tel que $\forall x \in A, r < x$ (il existe un ancêtre)
- $\forall x \in A \setminus \{r\}, \exists! y \in A, x < y$ (il y a un père unique)
- $\forall x \in A \setminus \{r\}, \exists n \in \mathbb{N}$ et $(x_1, x_2, \ldots, x_n) \in A^n, x < x_1 < x_2 < \cdots < x_n < r$ (chaque élément descend de l'ancêtre)

On parle aussi de frères, de descendance et d'ancêtres.

L'*arité* d'un père correspond au nombre de ses fils

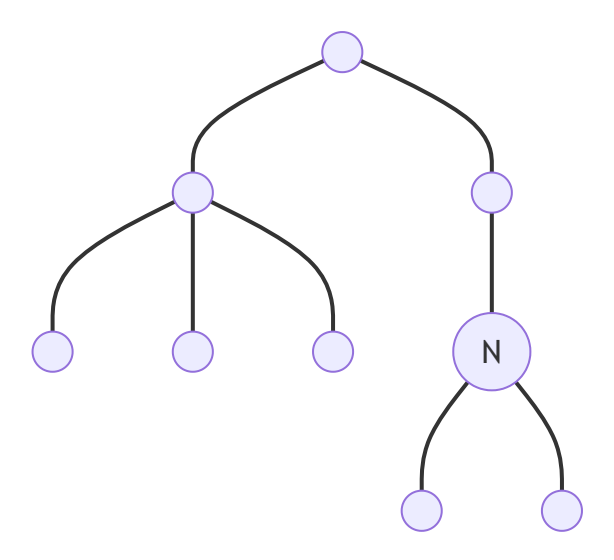


Un *arbre n-aire* est un arbre dont les nœuds sont d'arité maximale n Dans l'exemple, chaque nœud a au maximum une arité de 3 donc l'arbre est un arbre ternaire.

La *taille* de l'arbre est le nombre de nœuds qui le compose. Dans l'exemple, la taille est 6.

La *profondeur* d'un nœud est :

— -1 si l'arbre est vide
— 0 pour la racine
— le nombre de nœuds depuis la racine avant d'atteindre le nœud



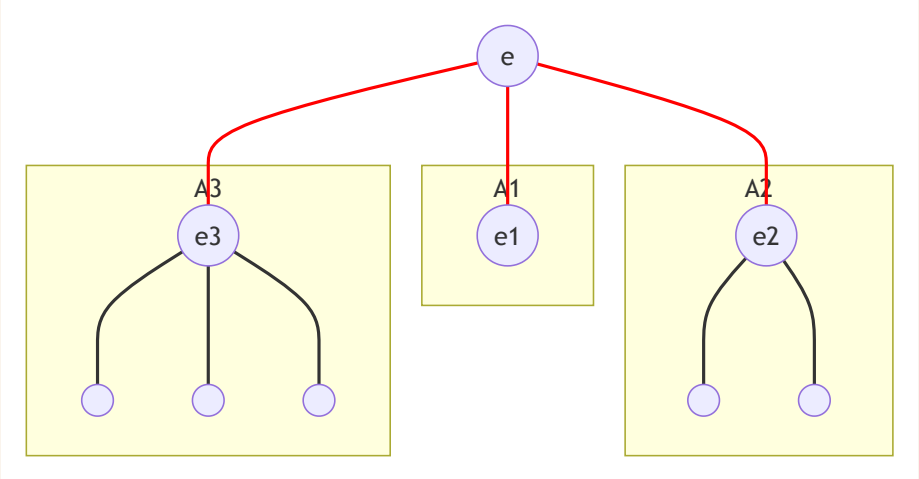
Par exemple, le nœud N a une profondeur de 2.

La *hauteur* de l'arbre est la profondeur maximale de ses feuilles. Dans l'exemple, la hauteur est de 3.

Définition inductive

Soit A un ensemble fini appelé nœuds.

- les arbres de hauteur 0 sont les éléments de A noté $(e, 0)$ où e est la racine de l'arbre
- Si $e \in A$ et Si $A_1, A_2, \ldots, A_n$ sont des arbres de hauteur respectives $h_1, h_2, \ldots, h_n$ et dont les racines respectives sont $e_1, e_2, \ldots, e_n$, alors en connectant e à $e_1, e_2, \ldots e_n$, on définit $\big(e, (A_1, A_2, \ldots, A_n)\big)$ l'arbre de racine e, de hauteur $1 + \max\limits_{k \in [\![1,n]\!]}(h_k)$ de sous arbres $A_1, A_2, \ldots, A_n$



Remarques :

Arbre marqué : Chaque nœud associé à une étiquette / valeur

Arbre non marqué : Les nœuds n'ont pas de valeurs associés

Un arbre est un graph :

- Simple : pas de boucles ou d'arêtes multiples
- Non orienté : les parcours $a \to b$ et $b \to a$ sont toujours possible
- Acyclique : pas de "boucles"
- Connexe : tous les nœuds sont accessibles

Propriété :

Pour un arbre de hauteur h d'arité $a > 1$, le nombre n de nœuds vérifie

$$h + 1 \geqslant n \geqslant \frac{a^{h+1} - 1}{a - 1}$$

Preuve :

Le nombre minimal de nœuds pour une hauteur donnée est un arbre contenant 1 nœud par hauteur. Le nombre maximal de nœuds pour une hauteur donnée est un arbre contenant i nœud par niveau i.

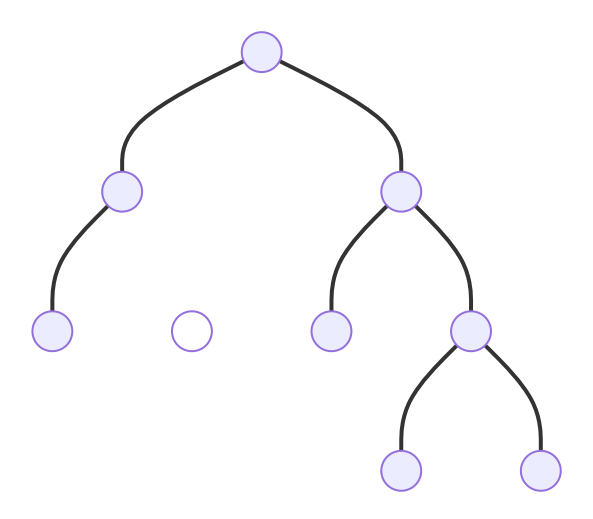
$$\sum_{i=0}^{h} 1 \geqslant n \geqslant \sum_{i=0}^{h} a^i$$
$$\iff h+1 \geqslant n \geqslant \frac{a^{h+1}-1}{a-1}$$

II. Arbres particuliers

Définitions

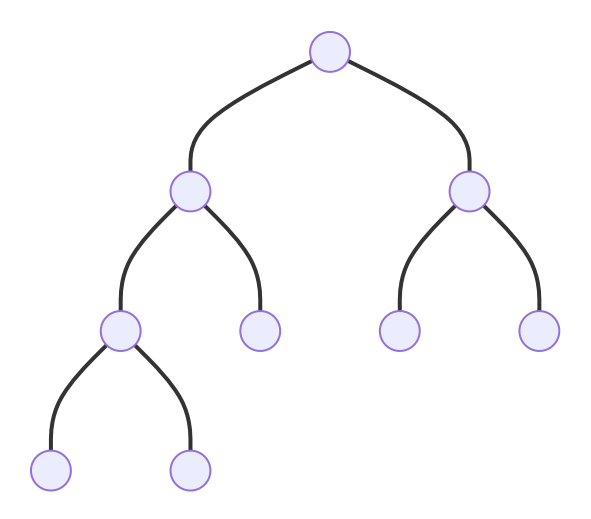
Arbres binaires :

Tous les nœuds sont d'arité au maximum 2.



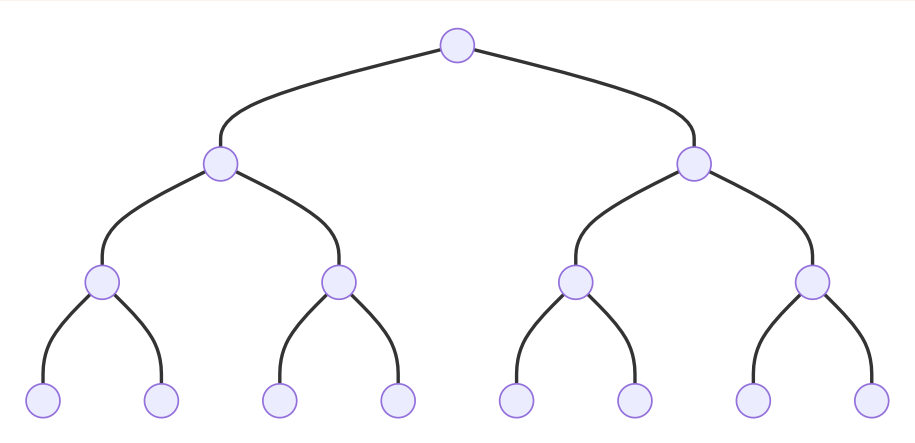
Arbre binaire entier :

Tous les nœuds sont d'arité 2



Arbre binaire complet

Arbre binaire dont les feuilles ont toutes la même profondeur. Il possède le nombre maximal de feuilles pour une hauteur donnée. On parle donc de fils gauche et de fils droit.



Propriétés

Nombre de nœuds $n \leqslant 2^p$ (pour un niveau p)

Hauteur h : $\lfloor \log_2(n) \rfloor < h \leqslant n - 1$

Arbre binaire à i nœuds interne (et la racine) d'arité 2 et f feuilles : $f = i + 1$

Nombre de feuilles $f \leqslant 2^h$

Profondeur maximale d'un arbre d'arité a composée de n nœuds :

$$\log_a \big((a-1) \times n + 1\big) - 1 \leqslant h \leqslant n - 1$$

Remarque :

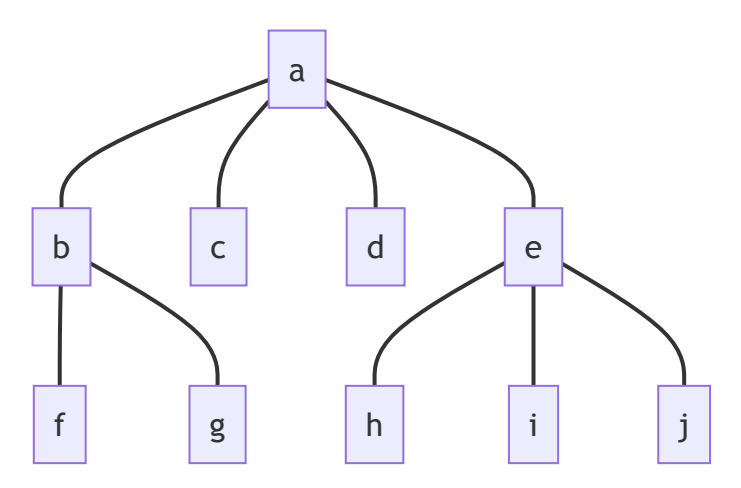
$$\begin{aligned} & \log_a((a-1)\times n+1)-1 \leqslant h \\ \Longrightarrow\ & \log_a((a-1)\times n) < \log_a((a-1)\times n+1) \leqslant h+1 \\ \Longrightarrow\ & \lfloor \log_a((a-1)\times n) \rfloor < h+1 \\ \Longrightarrow\ & \lfloor \log_a((a-1)\times n) \rfloor \leqslant h \end{aligned}$$

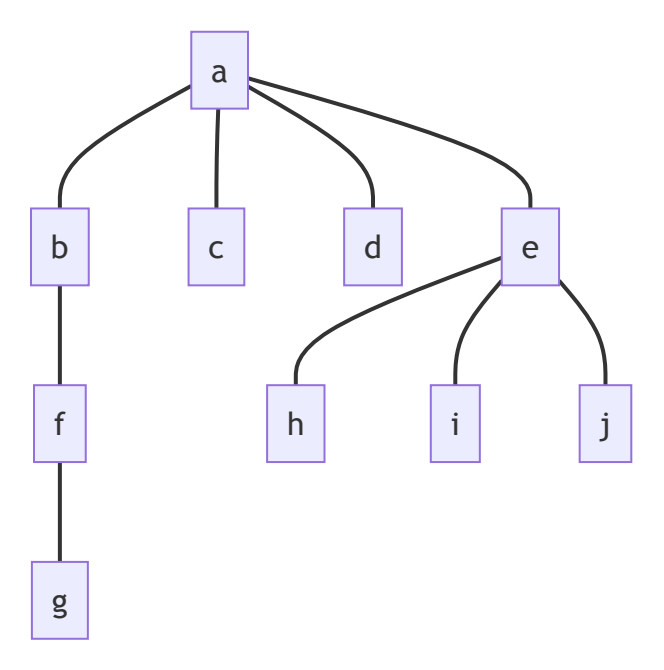
soit $\lfloor \log_a((a-1)\times n) \rfloor \leqslant h \leqslant n-1$

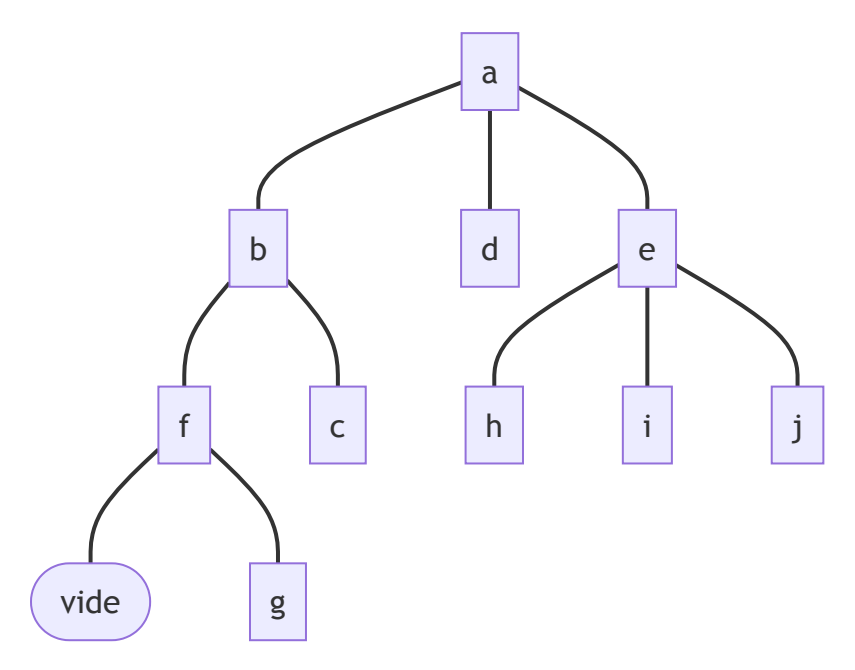
Transformation d'un arbre en arbre binaire

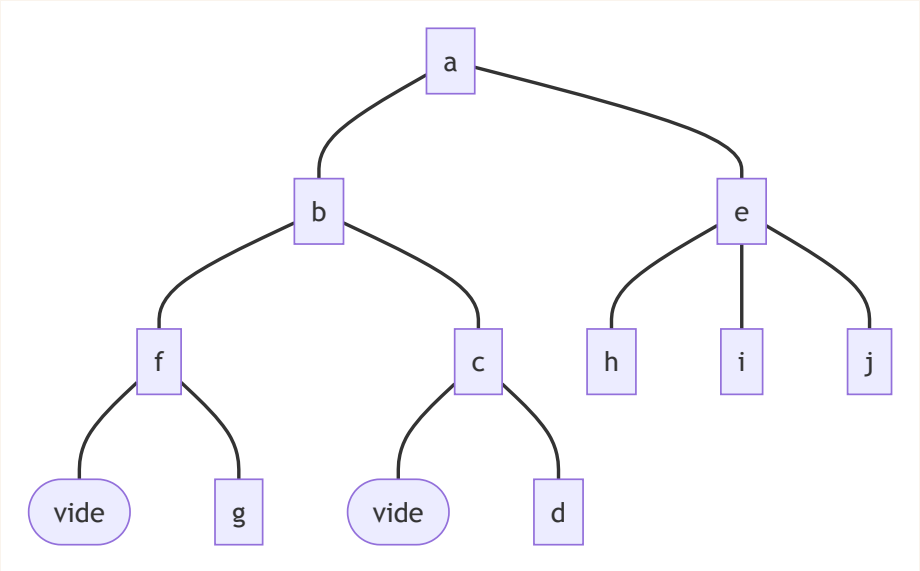
Algorithme de transformation d'un arbre n-aire A en arbre binaire :

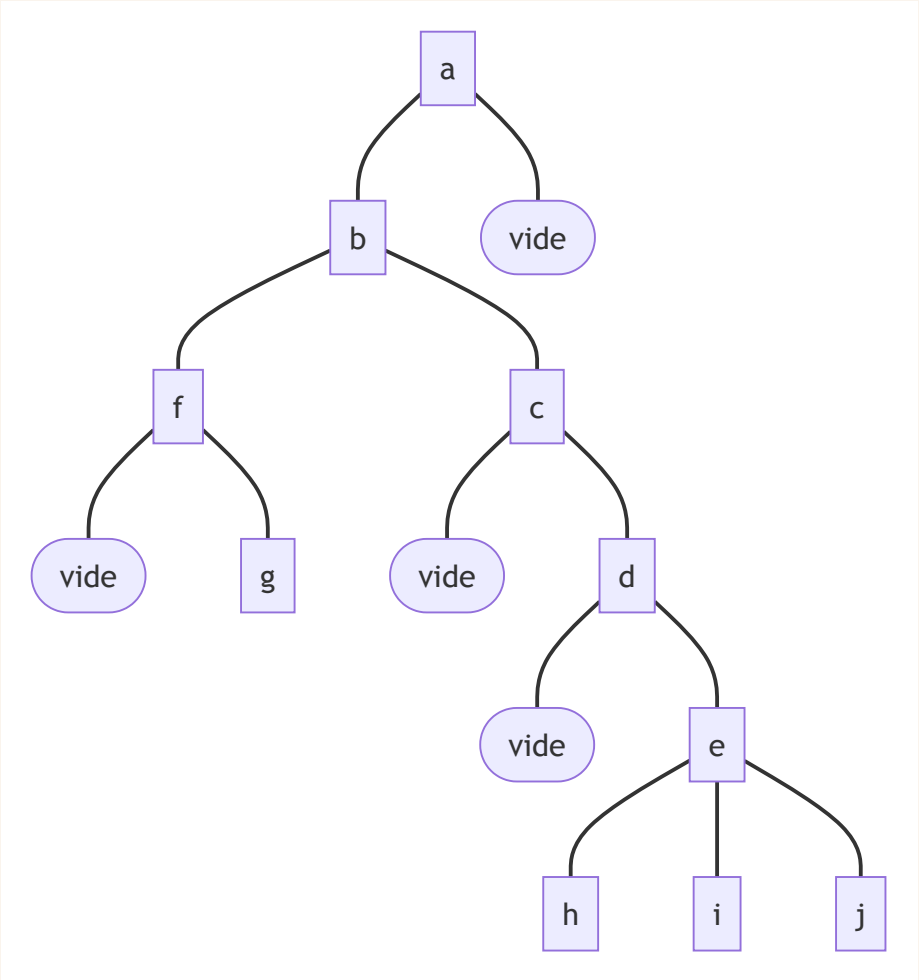
```
Pour chaque e ∈ A
Laisser e_g (fils le plus à gauche) en place
Supprimer les autres fils de e et les chainer à e_g
Le nœud e_d est le prochain frère de e
Fin pour
```

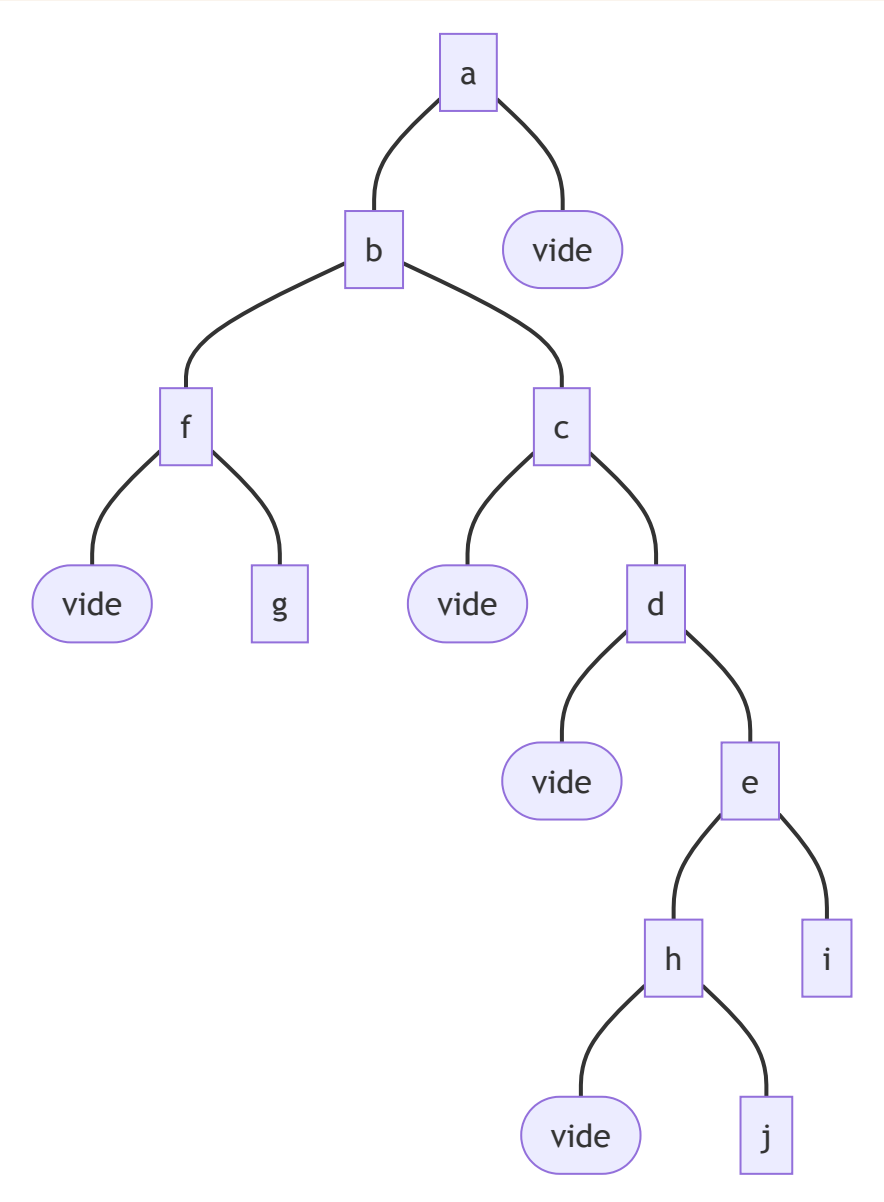


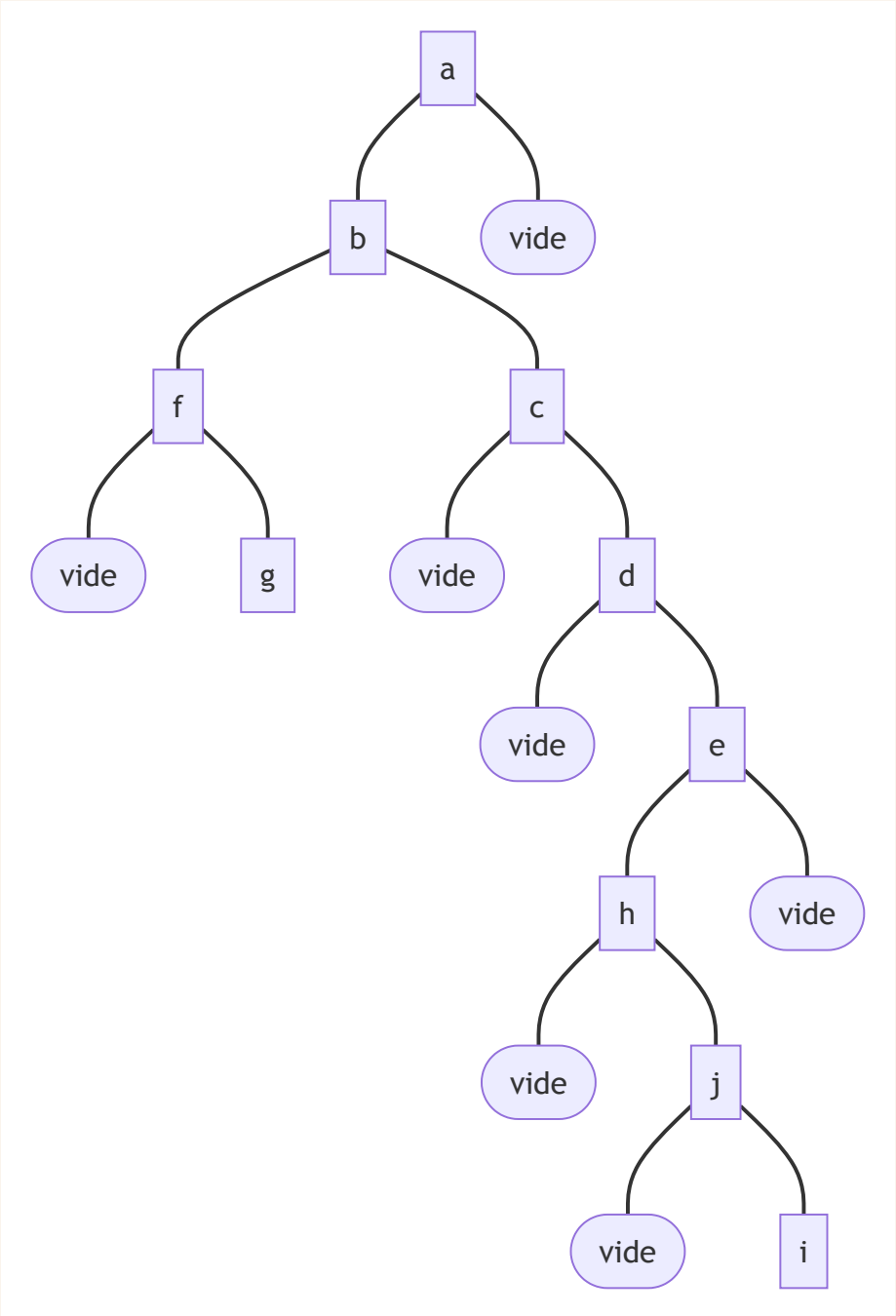

a
b
c
d
e
f
h
i
j
g


a
b
d
e
f
c
h
i
j
vide
g

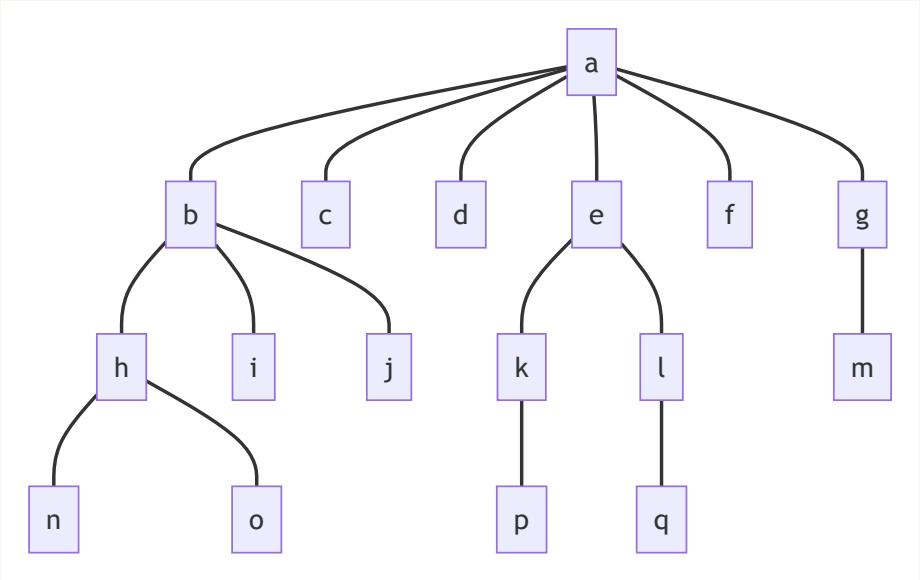

a
b
e
f
c
h
i
j
vide
g
vide
d

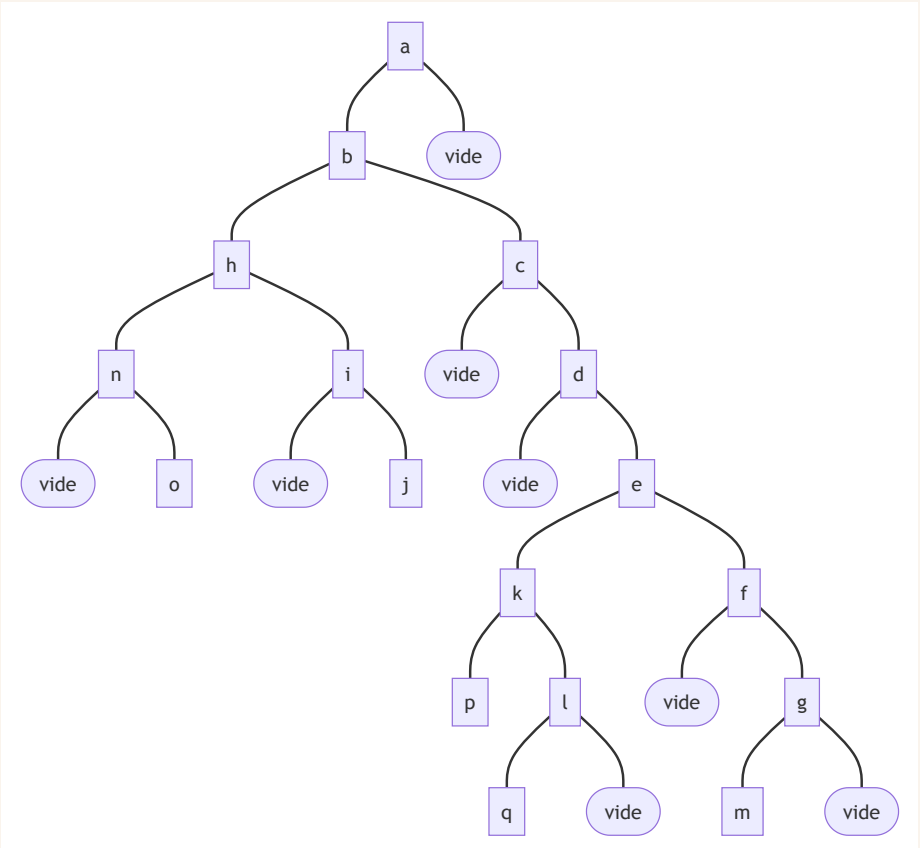

a
b
vide
f
c
vide
g
vide
d
vide
e
h
i
j


a
b
vide
f
c
vide
g
vide
d
vide
e
h
i
vide
j



Exercice :


a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q


a
b
vide
h
c
n
i
vide
d
vide
o
vide
j
vide
e
k
f
p
l
vide
g
q
vide
m
vide

Arbres binaires : implémentation sous forme de tableau en C (sérialisation)

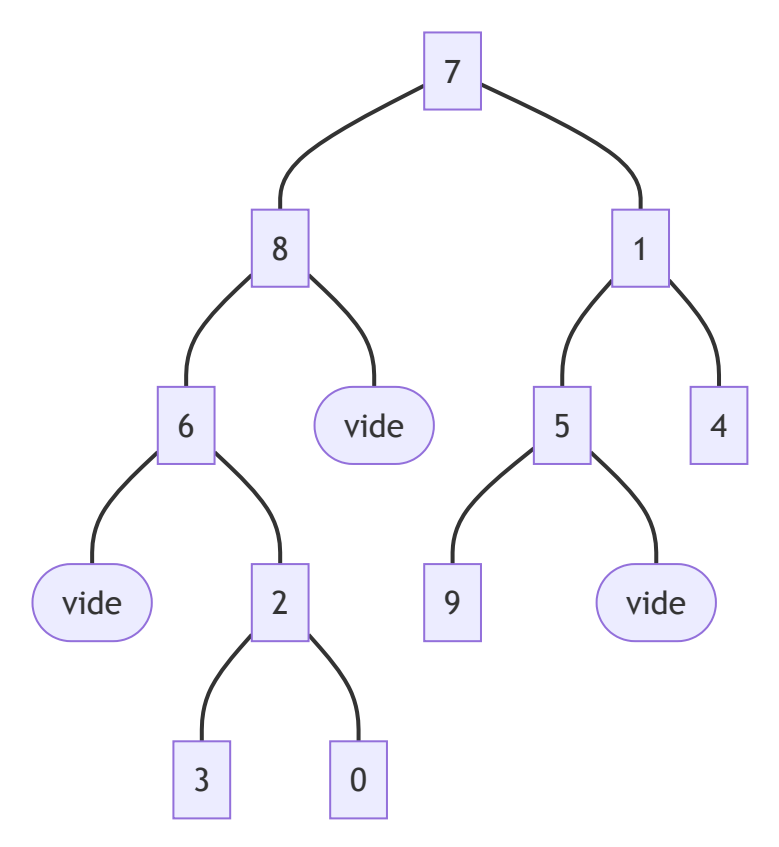
On stocke un arbre binaire dans un tableau d'enregistrements Chaque enregistrement E est défini par :

- E.clé : valeur du nœud
- E.gauche : indice du fils gauche dans le tableau
- E.droit : indice du fils droit dans le tableau

Une valeur de E.gauche ou E.droit égale à -1 indique qu'il n'existe pas de fils.

Indice dans le tableau	0	1	2	3	4	5	6	7	8	9
Clé	23	2	3	5	7	11	13	37	41	19
Gauche	-1	5	3	-1	-1	9	-1	8	6	-1
Droit	-1	4	0	-1	-1	-1	2	1	-1	-1

1. Représenter cet arbre. Est-il binaire ? Entier ? Complet ?



C'est un arbre binaire mais il n'est pas complet ni entier.

2. Définir le code en C permettant de définir ce tableau (statique)

```c
typedef struct item {
    int val;
    int left;
    int right;
};

item table[10];
```

3. Écrire une fonction en C qui renvoie l'enregistrement de la racine

```c
int getRoot(item* table, int len, item* root) {
    for(int i = 0; i < len; i++) {
        for(int j = 0; j < len; j++) {
            // on vérifie si i est un fils de j
            if(table[j].left == i || table[j].right == i) {
                break; // nouvelle itération de la boucle exterieure
            }
        }

        return i;
    }

    // pas de racine, il y a une boucle
    return -1;
}
```

Solution :

```c
item getRoot(item* table) {
    int search[10] = {0};

    for(int i = 0; i < 10; i++) {
        if(table[i].left != -1) {
            search[table[i].left] = 1;
        }

        if(table[i].right != -1) {
            search[table[i].right] = 1;
        }
    }

    for(int i = 0; i < 10; i++) {
        if(search[i] == 0)
            return table[i];
    }
}
```

Solution 2 :

```c
item getRoot(item* table, int len) {
    int root = 0;
```

```
        for(int i = 0; i < len; i++) {
            root += i;

            if(table[i].left != -1) {
                root -= table[i].left;
            }

            if(table[i].right != -1) {
                root -= table[i].right;
            }
        }

        return table[root];
    }
```

4. Écrire une fonction en C qui affiche la valeur de toutes les feuilles de T

```
    void showValues(item* table, int len) {
        item root;
        int rootIndex = getRoot(table, len, &root);

        showChildValues(rootIndex, table);
    }

    void showChildValues(int index, item* table) {
        item val = table[index];

        if(val.left == -1 && val.right == -1) {
            printf("%d\n", val.val);
        }

        if(val.left != -1)
            showChildValues(val.left, table);

        if(val.right != -1)
            showChildValues(val.right, table);
    }
```

Solution :

```
void showValues(item* table, int len) {
    for(int i = 0; i < len; i++) {

        // uniquement vrai si gauche = droite = -1
        if(table[i].left == table[i].right) {
            printf("%d", table[i].val);
        }
    }
}
```

Arbres binaires de recherche

Arbre binaire marqué :

— Présence d'une étiquette pour chaque nœud x de A

— Étiquettes

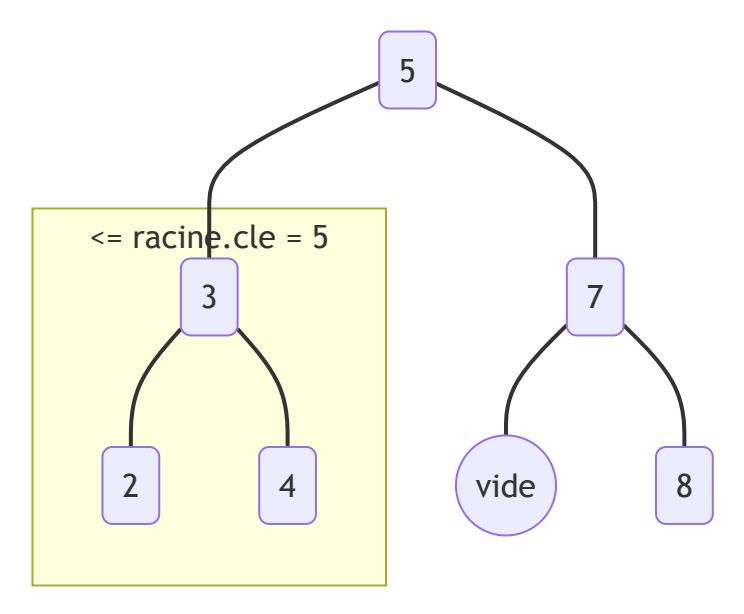
- — Même type
- — Présence d'une clé appartenant à un ensemble E
- — Relation d'ordre total sur E
- — Notation x.clé

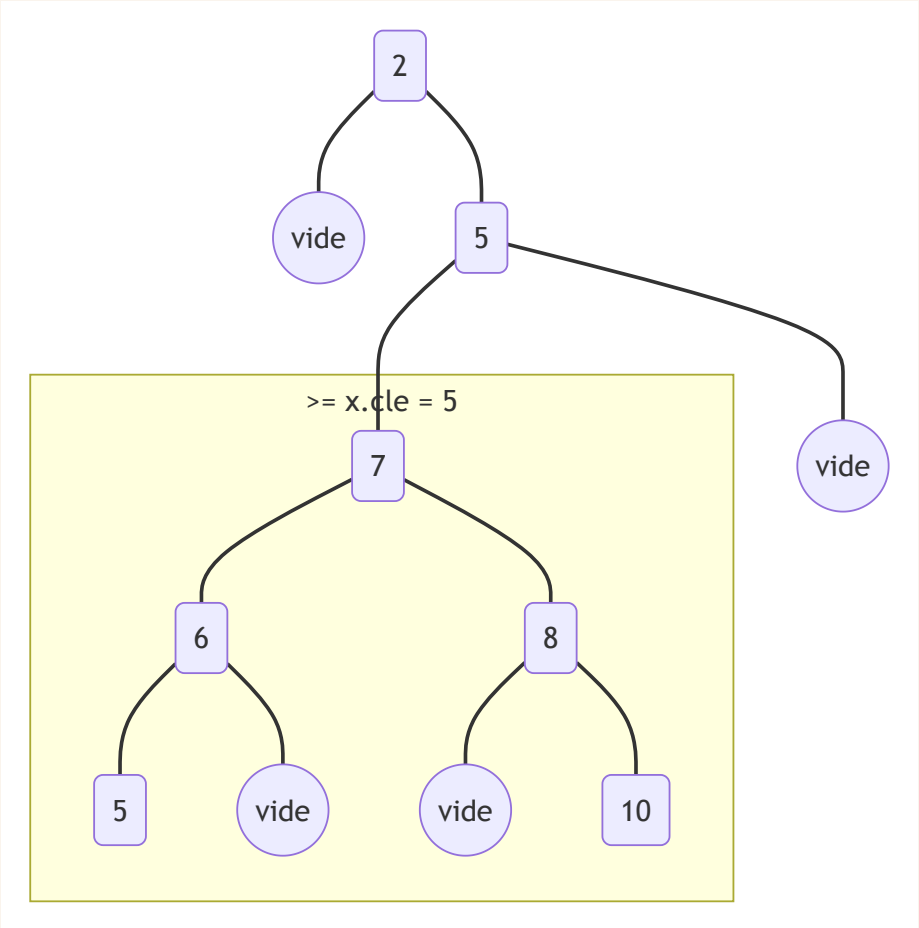
Organisation de l'arbre binaire de recherche : soit un nœud x de A.

— Alors toutes les étiquettes des nœuds y des sous arbres gauches de x sont telles que y.clé $\leqslant x$.clé

— Et toutes les étiquettes des nœuds y des sous arbres droits de x sont telles que y.clé $\geqslant x$.clé

Exemples :





Nœud :

- Étiquette
  - clé
  - information
- Fils gauche
- Fils droit

Opérations fondamentales des ABR :

- Constructeur
- Accesseurs
  - Recherche d'une clé
  - Rechercher le minimum
  - Rechercher le maximum
  - Rechercher un successeur
  - Rechercher un prédécesseur
- Transformateurs

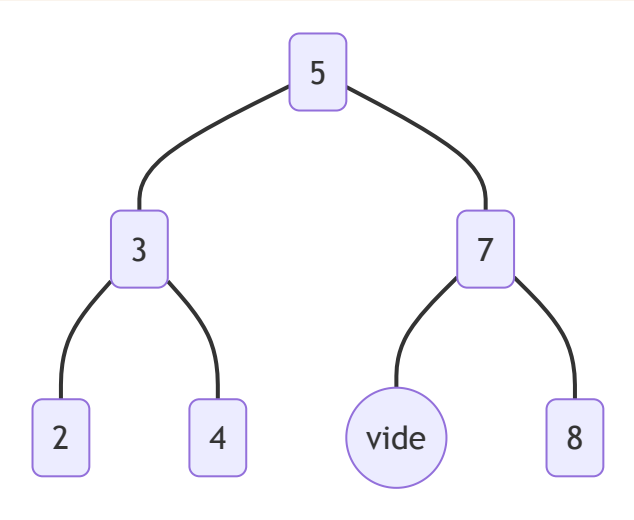
— Insérer un nœud
— Supprimer un nœud

Utilité : faciliter une recherche avec une recherche par clé dans l'ABR

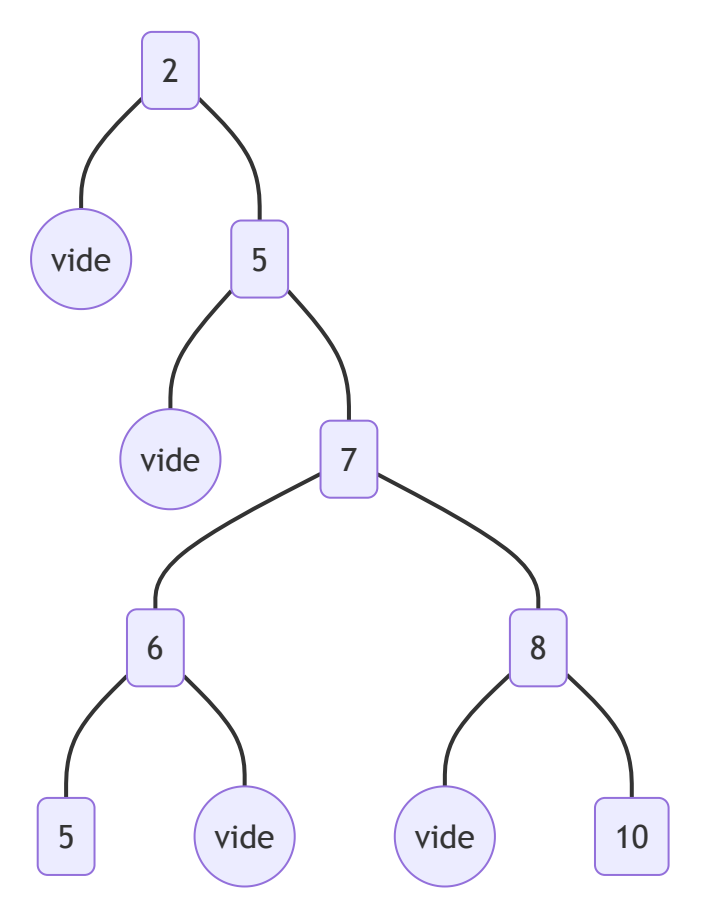
— temps de recherche proportionnel à la hauteur h de l'arbre

— $T(n) = \mathcal{O}(n)$ recherche linéaire dans le pire des cas (liste chainée)
— $T(n) = \mathcal{O}\big(\log_2(n)\big)$ recherche en temps logarithmique en moyenne pour un ABR complet.

— Dépend de la construction de l'arbre :



6 nœuds, hauteur 2 : Efficace



6 nœuds, hauteur 4 : Peu efficace

L'efficacité augment quand la hauteur diminue.

Arbre dégénéré (filiforme) : chaque nœud n'a qu'un enfant.

Arbres binaires bicolores (rouge - noir)

Arbre de recherche : possibilité d'arbre déséquilibré (filiforme, dégénéré)

- Recherche en $\mathcal{O}(n)$ où n est le nombre de nœuds
- aucun apport par rapport à une liste chainée

Arbre bicolore : arbre de recherche particulier, approximativement équilibré

- Recherche en $\Theta\big(\log_2(n)\big)$

Arbre binaire bicolore $\rightarrow$ marqué

- présence d'une étiquette pour chaque nœud x de A
- Fils gauche, fils droit
- Étiquettes
  - même type

— clé
— information
— information supplémentaire : *couleur* (1 bit)

Propriétés rouge noir :

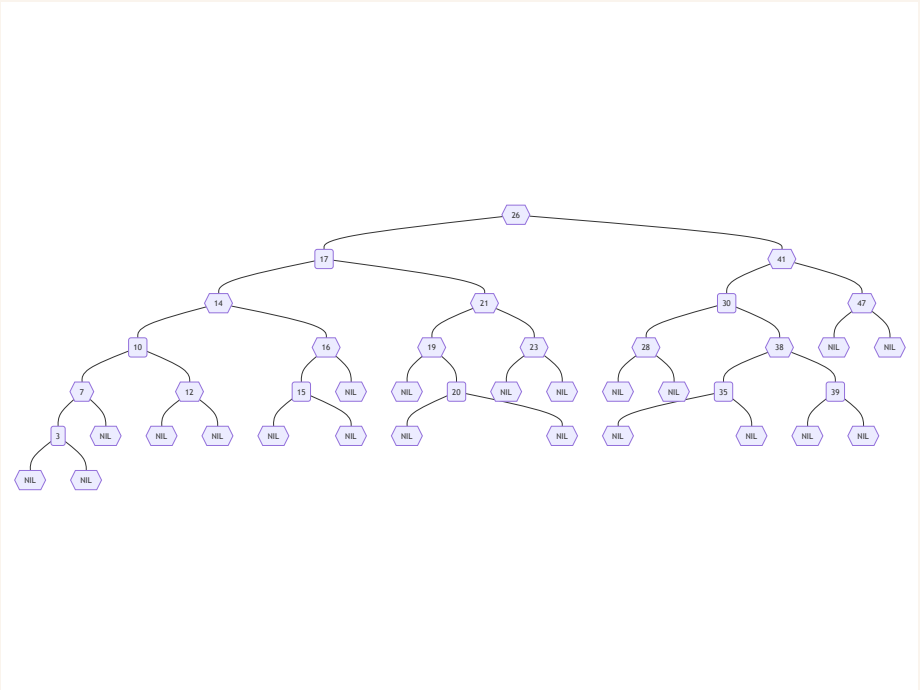
— chaque nœud est soit rouge, soit noir
— chaque feuille est noire
— la racine est noire
— si un nœud est rouge, ses deux enfants sont noirs
— pour chaque nœud, tous les chemins simples reliant le nœud à des feuilles situées plus bas dans l'arbre contiennent le même nombre de nœuds noirs

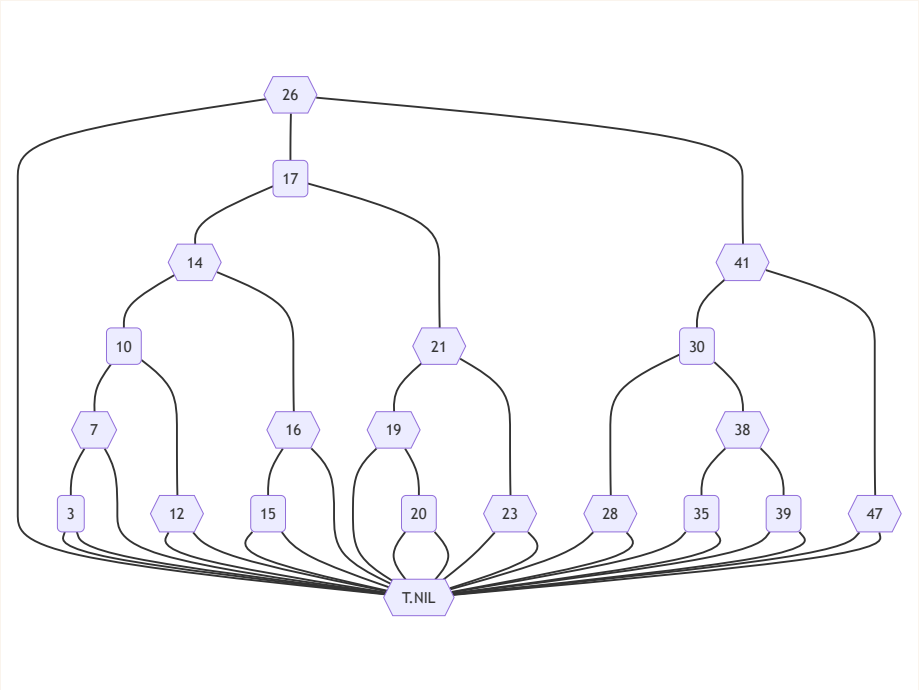
Remarque :

— Ajout de nœuds noirs vide (pointeur sur NIL) pour générer les feuilles
— Informations contenues dans les nœuds internes

Exemple :

Les nœuds rouges sont entre [] et les nœuds noirs entre ⟨⟩





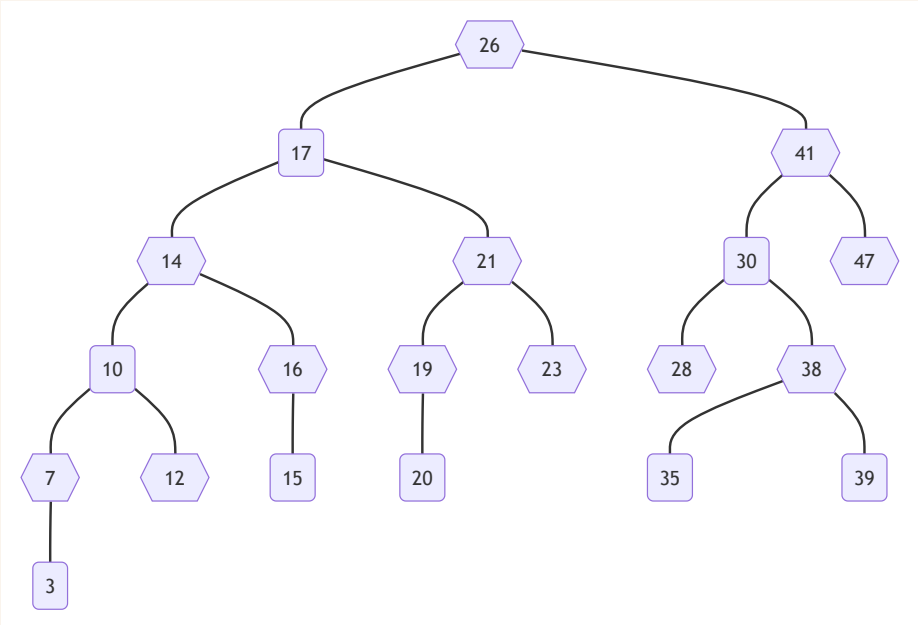
T.NIL : sentinelle

— Simplification des conditions aux limites
— Même attributs qu'un nœud ordinaire :

— Valeur : noir
— Autres attributs : valeurs quelconques

— Aussi parent de la racine

Hauteur noire omise



Propriété rouge - noire : la longueur L d'un chemin allant de la racine à une feuille est comprise entre h_n et $2h_n$.

Chemin : suite de nœuds dont chacun est le prédécesseur ou le successeur du suivant.

h_n étant la profondeur noire de l'arbre.

Justification :

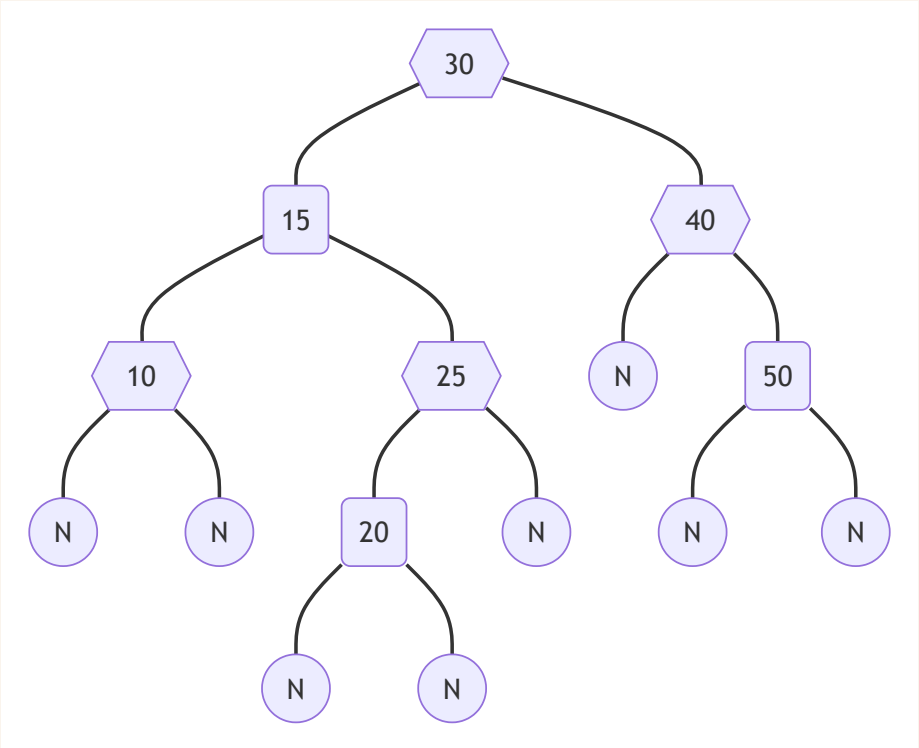
Si tous les nœuds sont noirs, alors h_n est égale à la profondeur de l'arbre.

S'il y a systématiquement une alternance entre nœuds rouges et noirs, alors la hauteur totale h de l'arbre vaut $2h_n$

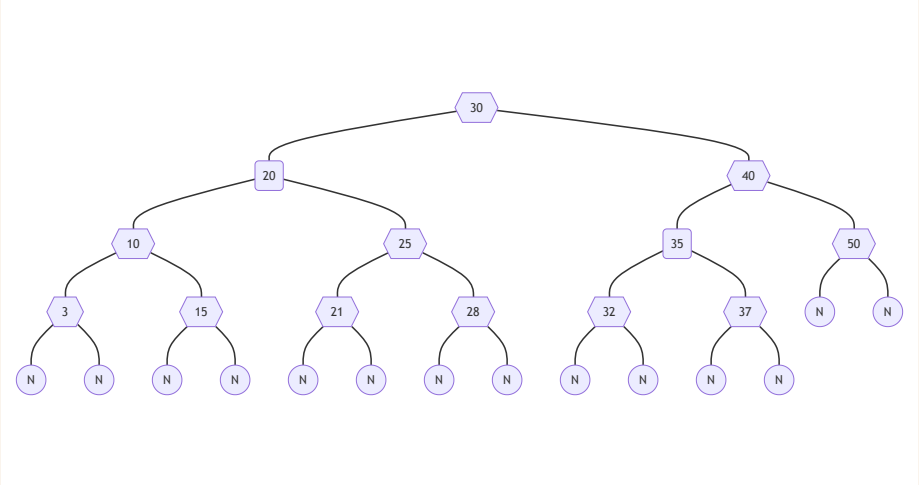
Exercice 1 :

— Arbre 1 : non (rouge → rouge)
— Arbre 2 : non (racine rouge)
— Arbre 3 : non (nombre de nœuds noirs $\neq$)
— Arbre 4 : non (n'est pas un ABR car $10 < 22$)

Exercice 2 :



Exercice 3 :



1. hauteurs $h_n(30) = 3$, $h_n(20) = 3$, $h_n(35) = 2$ et $h_n(50) = 1$
2. Dans le meilleur des cas, il n'y a pas de nœuds rouges, donc $h = h_n$ et donc le nombre de feuille f vaut 2^h donc $2^{h_n(x)}$. Or, le nombre de nœuds internes i valide $f = i + 1$ donc $i = f - 1$ et donc $i \geqslant 2^{h_n(x)} - 1$

3. Dans le meilleur des cas, on a $h = h_n$.

$$\begin{aligned} i \geqslant 2^{h_n(x)} - 1 &\iff i + 1 \geqslant 2^{h_n(x)} \\ &\iff \log_2(i+1) \geqslant h_n(x) = h \end{aligned}$$

III. Parcours d'arbres

Définition

Soit un arbre A de taille n.

Objectif :

- visiter les nœuds pour traitement
- contrainte : chaque nœud doit être traité une seule fois

Définition :

Un parcours d'arbre est une succession de nœuds $(n_1, n_2, \ldots, n_n)$, indiquant l'ordre dans lequel ils ont été visités

Pricipe général des parcours d'arbre :

- marquage du nœud après sont traitement pour ne plus le traiter
- maintien d'un ensemble de nœuds en attente de traitement

Existence de plusieurs manières de parcourir un arbre

Utilisation des arbres

Arbres d'expression → représentation d'expressions

- Arbre syntaxique
- Expressions mathématiques

Arbres préfixes (ou trie) → représentation d'un ensemble de mots

Parcours en profondeur

Définitions

Principe de parcours en profondeur :

- Utilisation de la définition inductive des arbres
- Proposition d'algorithmes récursifs

$\implies$ Exploration d'un des sous-arbres avant d'explorer le sous-arbre suivant

Plusieurs posibilités :

- Exploration en partant de la racine
- Exploration en partant des feuilles

— Exploration symétrique

Remarque : Le choix de traiter de gauche à doite est arbitraire.

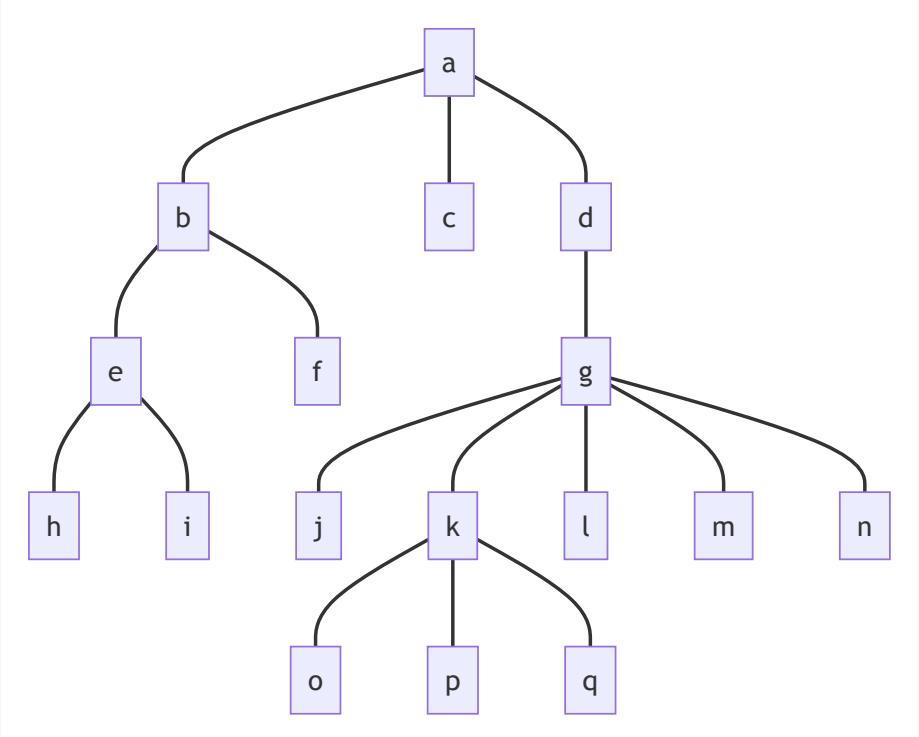
Ordre préfixé :

— Départ à la racine
— Exploration préfixe du sous-arbre gauche
— Exploration préfixe du sous-arbre droit
— ⋮
— Exploration du sous-arbre A_n

Pour un arbre binaire, ordre = père, fils gauche, fils droit.

Pour l'arbre ci-dessous, l'ordre préfixé est

$$a \to b \to e \to h \to i \to f \to c \to d \to g \to j \to k \to o \to p \to q \to l \to m \to n$$



Ordre infixé ou parcours symétrique :

— Exploration infixé du sous-arbre gauche
— Puis racine
— Exploration infixé du sous-arbre droit
— ⋮
— Exploration des nœuds de A_n en ordre infixé

Pour un arbre binaire, ordre : fils gauche, père, fils droit.

Pour un ABR : ordre infixé

— Obtention de la suite ordonnée des étiquettes

Pour l'arbre précédent, l'ordre infixé est

$$h \to e \to i \to b \to f \to a \to c \to j \to g \to o \to k \to p \to q \to l \to m \to n \to d$$

Ordre postfixé :

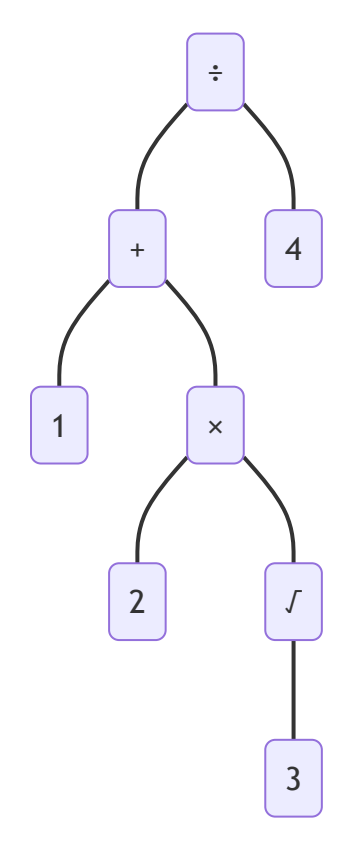
— Exploration postfixé du sous-arbre gauche
— Exploration postfixé du sous-arbre droit
— $\vdots$
— Exploration du sous-arbre A_n
— Traitement de la racine

Pour une arbre binaire, l'ordre est fils gauche, fils droit, père
Parcours en profondeur de l'arbre précédent :

$$h \to i \to e \to f \to b \to c \to j \to o \to p \to q \to k \to l \to m \to n \to g \to d \to a$$

Parcours en profondeur : arbre d'expression

Problème lié aux expressions infixes : gestion des parenthèses
$\left(1 + 2 \times \sqrt{3}\right) / 4$ pour $\frac{1+2\sqrt{3}}{4}$
Représentation d'une expression sous forme d'arbre :



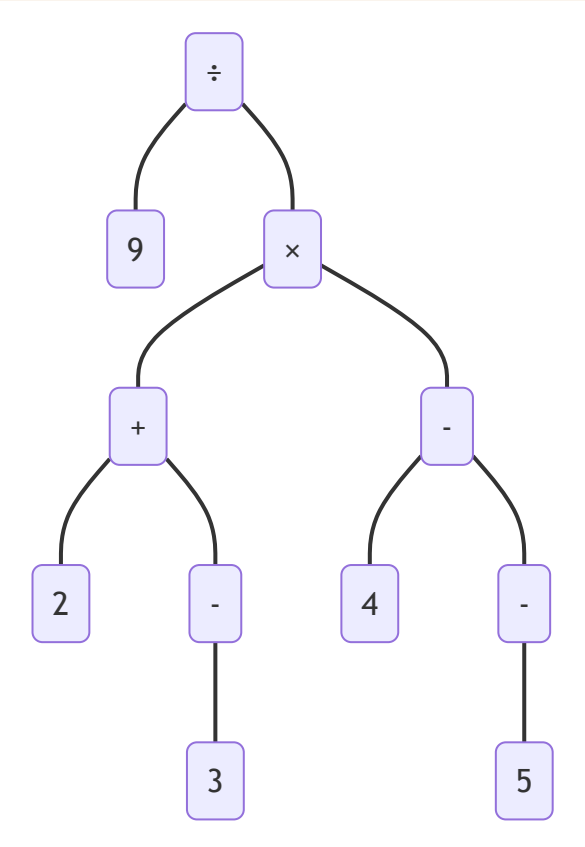
Parcours de l'arbre :

- Infixe : $(1 + (2 \times \sqrt{3})) / 4$
- Préfixe : $/ (+ 1 (\times 2 \sqrt{3})) 4$
- Postfixe : $(1 (2 (3 \sqrt{}) \times) +) 4 /$

Notation polonaise inversée (NPI) :

- Notation postfixé
- Nécessité de deux piles :
  - pile d'expression
  - pile de calcul

$$\frac{9}{(2+(-3))\times(4-(-5))}$$



Infixe : $9 \div ((2 + (-3)) \times (4 - (-5)))$

Préfixe : $\div 9 (\times (+ 2 (- 3)) (- 4 (- 5)))$

Postfixe : $9 ((2 (3 -) +) (4 (5 -) -) \times) \div$

Etape	1	2	3	4	5	6	7	8	9	10	11	12
Mot lu	9	2	3	neg	+	4	5	neg	−	×	÷	
Pile	9	2	3	−3	−1	−1	5	−5	9	−9	−9	−1
		9	2	2	9	9	4	4	−1	9	9	
			9	9			−1	−1	9			
			9	9				9				

Parcours de l'arbre → utilisation d'une pile

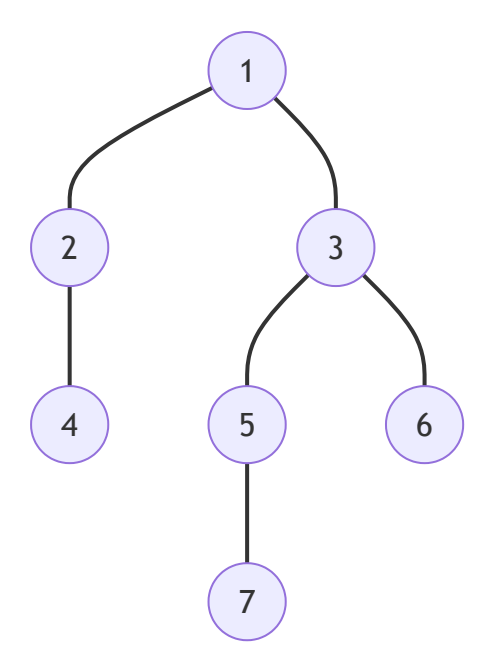
Visite des fils droits avant les fils gauches pour retrouver l'ordre préfixe (fils gauche en somme de pile)

Pile :

1	
3	2
3	4

3	
6	5
6	7
6	

Clés traité : $1 \rightarrow 2 \rightarrow 4 \rightarrow 3 \rightarrow 5 \rightarrow 7 \rightarrow 6$



Bilan

Parcours d'un arbre → fonction récursive

Comportement d'une pile

Depth First Search (DFS)

```
Fonction ParcoursArbre(Élément)
  Entrée: pointeur sur un nœud de l'arbre
  Sortie: traitement sur chacun des nœuds du sous-arbre enraciné en un élément
  Début
    Si Élément != NIL Alors
      Traitement Élément     != parcours préfixé
      Parcours arbre.gauche
      Traitement Élément     != parcours infixé
      Parcours arbre.droit
      Traitement Élément     != parcours postfixé
    Fin Si
  Fin
```

Parcours en largeur

Principe du parcours en largeur :

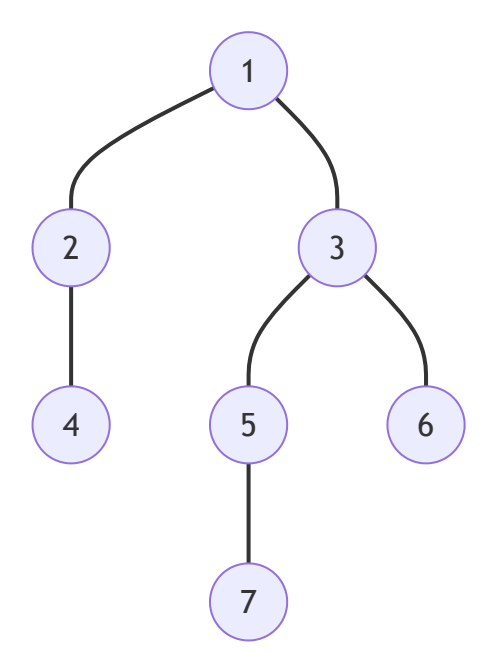
- Départ de la racine
- Exploration des nœuds par niveaux de l'arbre
- Pour un même niveau, parcours de gauche à droite

$\Longrightarrow$ Parcours réalisé à l'aide d'une file

Visite des fils gauches avant les fils droits

Parcours intéressant pour

- une recherche avec la plus petite profondeur possible
- pour une énumération



File :

1		
3	2	
4	3	
6	5	4
6	5	
7	6	
7		

Clés traitées : $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7$

IV. Implémentation

Arbres binaires de recherche

Type arbre n'existe pas → sérialisation (stockage sous un autre format)

Deux implémentations possibles :

1. Par tableaux (voir exercice)
2. Par enregistrement et pointeurs

Solution par enregistrement :

- Création du type nœud
- Creation du type arbre pointant sur la racine de l'arbre (en C)
- Arbre complet contenu dans un enregistrement d'enregistrements (en OCAML)

  $\Longrightarrow$ structure récursive

Quels champs pour un nœud ?

- entier `clé`
- pointeur `fils_gauche`
- pointeur `fils_droit`
- pointeur `parent`
- enregistrement `informations`

En C, nécessité d'écrire une fonction créant un nœud :

- Entrée :
  - valeur (`int`)
  - info (enregistrement contenu dans le nœud)
- Sortie :
  - pointeur sur le nœud créé (les champs `fils_gauche`, `fils_droit` et `parent` sont initialisé à `NULL`)

Constructeur : créer un arbre

- Entrée : aucun
- Sortie : pointeur sur la racine, qui peut être `NULL`/`NIL`
- Sémantique :
  - Fonction créant un pointeur sur la racine
  - Pointeur sur la racine initialisé à `NULL`/`NIL`

Transformateur : insérer un nouveau nœud → nouvelle feuille. Plusieurs cas à envisager :

- Arbre vide → insérer au niveau de la racine
- Arbre non vide
  - Début de la racine

- Parcours de l'arbre par chemin descendant à la recherche d'un `NULL`/`NIL`
- Pointeur sur nœud, descendant l'arbre jusqu'à `NIL` (pointeur de traine)
- Mise à jour du parent de nouveau
- Mise à jour du fils gauche / droit du futur parent
- Nécessité d'un pointeur temporaire conservant l'adresse du futur parent
- Mise à jour dans la boucle du pointeur sur parent

$\Longrightarrow$ Deux phases :

1. Recherche de la feuille
2. Modification de l'arbre / mise à jours des nœuds

Cette fonction est linéaire en temps : $\mathcal{O}(h)$ où h est la hauteur de l'arbre.

Transformateur : Supprimer un nœud

- Argument : pointeur sur l'arbre, valeur de la clé
- Retourne : arbre modifié
- Sémantique : ?

Quel cas envisager ?

Il faut vérifier que la clé est présent dans l'arbre

Suppression d'une feuille

Suppression d'un nœud interne / racine ayant un seul enfant

Suppression d'un nœud interne / racine ayant deux enfants

- Suppression d'une feuille : modification du parent et suppression de la feuille
- Suppression d'un nœud interne / racine ayant un seul enfant
  - modification du parent (Parent.gauche ou Parent.doit pointe sur l'enfant non nul du nœud supprimé)
  - modification de l'enfant (Enfant.parent pointe sur le parent du nœud supprimé)
- Suppression d'un nœud interne / racine ayant deux enfants
  - Enfant droit est le *successeur* (la définition est après) du nœud à supprimer
  - Enfant droit devient le fils de Parent à la place du nœud à supprimer : mise à jour de Parent.gauche et de Enfant droit.parent
  - Enfant gauche devient le fils gauche de Enfant droit : mise à jours de Enfant droit.gauche et Enfant gauche.parent

Prédécesseurs et successeurs : Si toutes les clés sont distinctes, le successeur d'un nœud x est le nœud y possédant la plus petite clé supérieure à x.clé

Les algorithmes sont sur la feuille "Structures hiérarchiques — Arbres" mais uniquement pour information : on n'a pas à savoir les écrire.

Arbre bicolore

Modification du type : ajout d'un champ pour désigner la couleur

Opérations d'insertion et de suppression :

→ visite des nœuds pour préserver les propriétés des arbres bicolores

NON TRAITÉ (aucune indication dans le programme)

Équilibrage des arbres (arbres binaires de recherche)

Préservation des propriétés de l'arbre binaire de recherche

Utile pour équilibrage des arbres

→ se rapprocher d'un arbre entier

→ éviter les arbres filiformes (car la recherche est en $\mathcal{O}(n)$)

Arbre H-équilibré :

Déséquilibre d'un arbre en a :

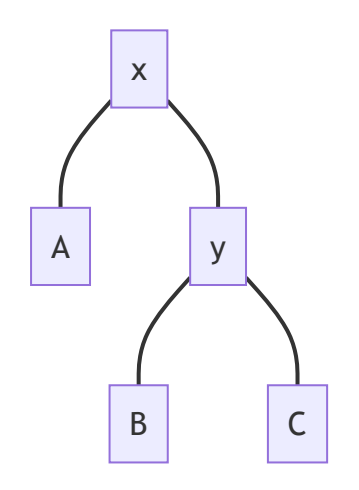
$$\text{déséquilibre}(a) = h\big(\text{gauche}(a)\big) - h\big(\text{droit}(a)\big)$$

Un arbre a est H-équilibré si, pour tous ses sous–arbres b on a :

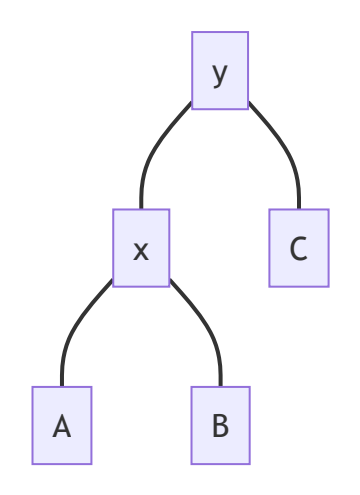
$$\text{déséquilibre}(b) \in \{-1, 0, 1\}$$

Un arbre AVL (Adelson – Velskii – Landis en 1962) est un arbre H-équilibré.

Arbre initial :



Après une rotation gauche, on a



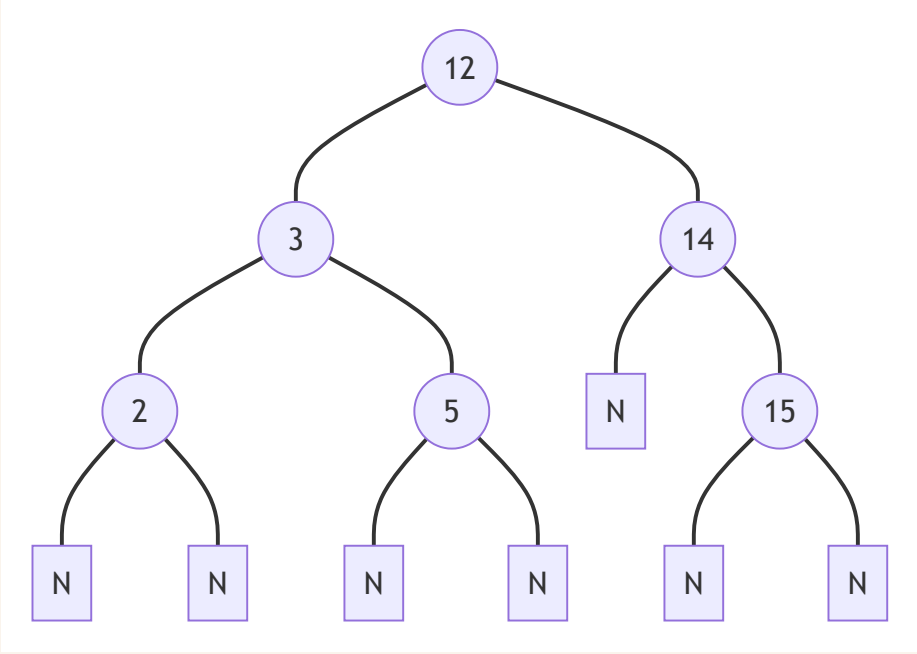
Après une rotation droite, on retrouve l'arbre initial.

Rotation gauche : x va à droite

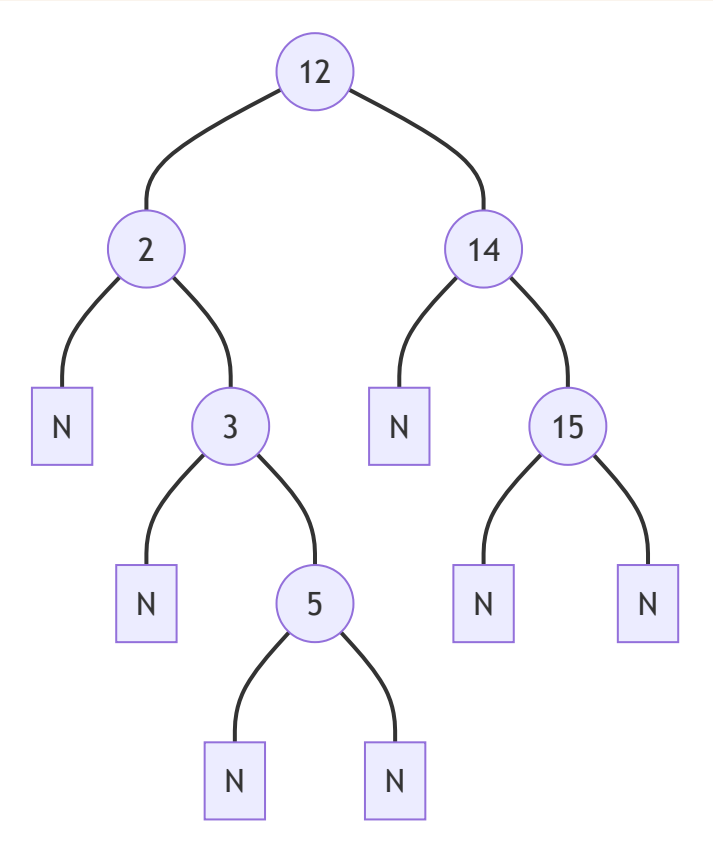
Rotation droite : y va à gauche

Exercice 1 :

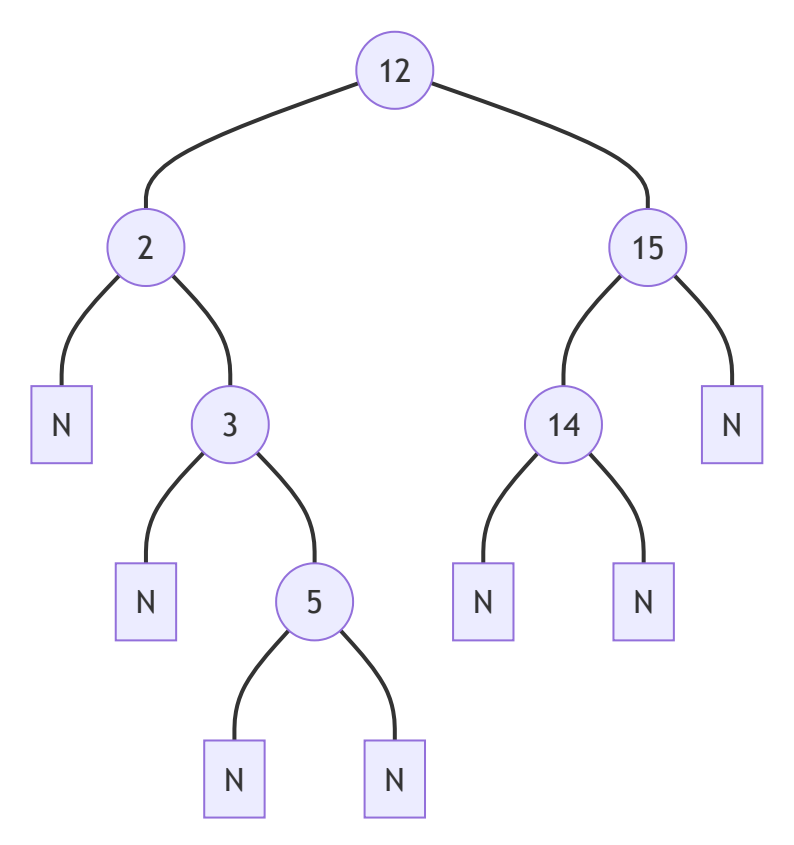
1. Arbre A_1
   a. déséquilibre$(A_1) = 3 - 3 = 0$, il est donc H-équilibré
   b.



   Après une rotation à droite de centre le nœud 3 :



Après la rotation à gauche de centre le nœud 14 :



2. Arbre A_2

   a. déséquilibre$(A_2) = 0$
   b. Rotation à gauche de centre 5 puis à droite de centre 14

V. Tas et files de priorité

Tas : définition

Un tas est un arbre binaire :

— tel que (condition sur le squelette) : toutes les feuilles sont de profondeur h ou $h-1$. Pour toute profondeur $p < h$, il y a exactement 2^p nœuds. Toutes les feuilles (de profondeur h) sont le plus à gauche de l'arbre
— tournoi (condition sur les étiquettes) : l'étiquette d'un nœud est supérieure (inférieure) ou égale à celles de ses fils

Tas max : l'étiquette d'un nœud est supérieure ou égale à celles de ses fils.

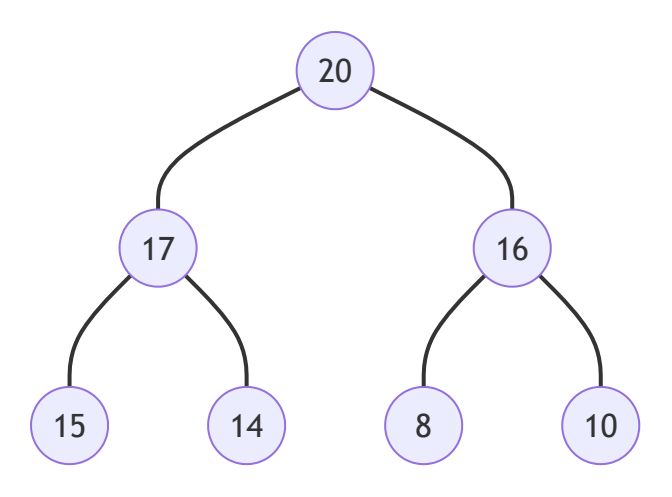
Tas min : l'étiquette d'un nœud est inférieure ou égale à celles de ses fils.

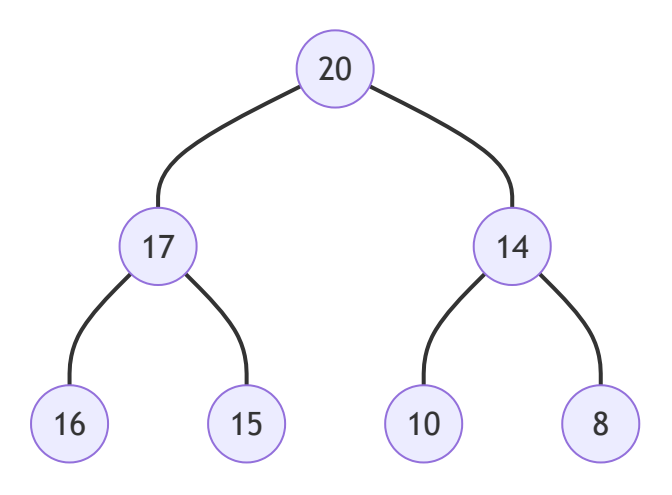
Structure bin adaptée pour gérer les files de priorité :

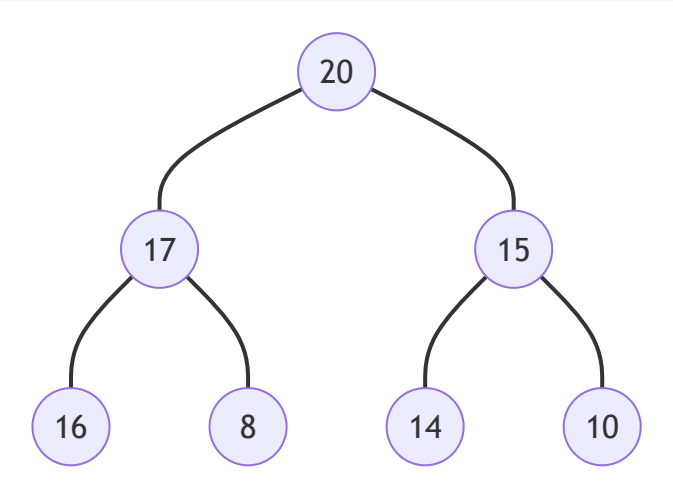
implémentation : (priorité, élément)

la priorité sert de clé

Exercice : construire 3 tas max contenant les nœuds de clés $\{8, 10, 14, 15, 16, 17, 20\}$







Implémentation des tas

Implémentation dans un tableau :

— Chaque nœud correspond à un élément du tableau
— Fils gauche d'un nœud i stocké à l'indice $2i$
— Fils droit d'un nœud i stocké à l'indice $2i + 1$
— Parent d'un nœud i stocké à l'indice $\lfloor \frac{i}{2} \rfloor$

Tableau A représentant un tas : deux attributs (algorithmique) :

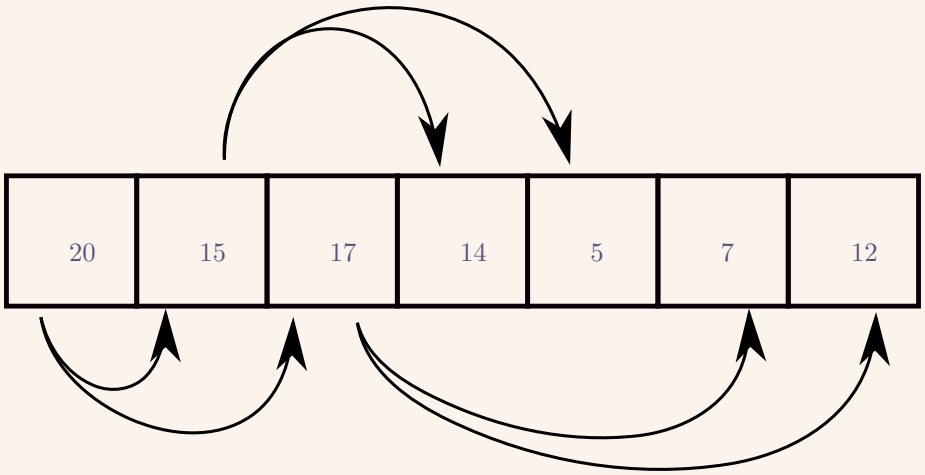
— A.longueur : nombre d'éléments dans un tableau,
— A.taille : nombre d'éléments dans le tas,
— Le premier élément du tableau A est la racine du tas,
— On a A.longueur $\leqslant$ A.taille.

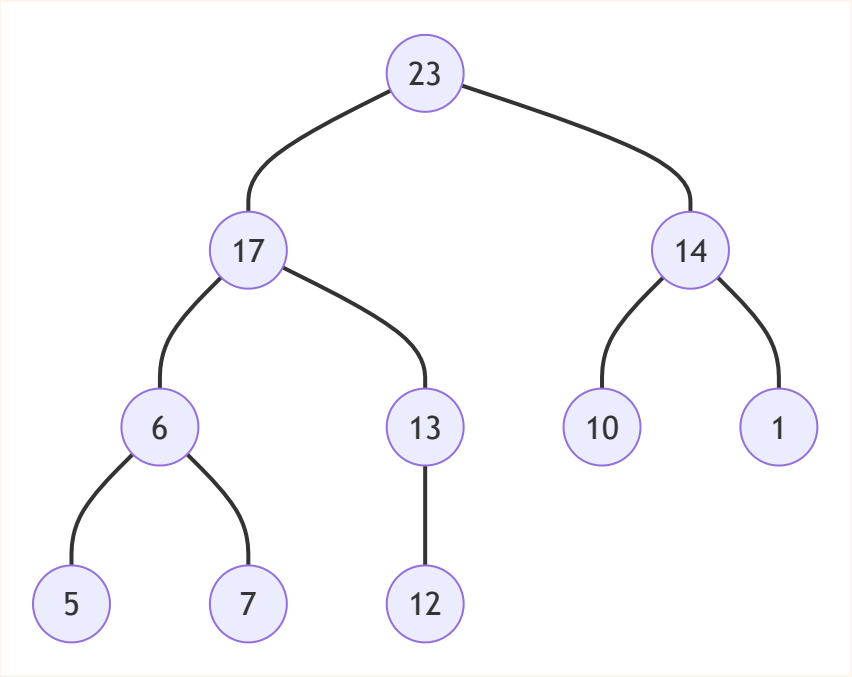
Possibilités :

— Stocker la taille du tas à l'indice 0 du tableau lors de la programmation,
— Définir un enregistrement contenant la taille du tas et le tableau.

Exercice 2 :

1. Au maximum, on a un arbre complet de hauteur h donc $2^{h+1} - 1$ nœuds. Au minimum, on a un arbre complet de hauteur $h - 1$ et le nœud le plus à gauche à un fils gauche. On a donc au minimum 2^h nœuds.
2.





Cet arbre n'est pas un tas max car $7 > 6$. Il faut donc enlever 7 et 12 :

$$[\,23, 17, 14, 6, 13, 10, 1, 5\,]$$

La taille de ce tas est 8.

3. On suppose que le nœud stocké en $\lfloor \frac{n}{2} \rfloor + 1$ est un parent. Alors, son fils gauche est stocké en $2\left(\lfloor \frac{n}{2} \rfloor + 1\right)$. Or

$$\left\lfloor \frac{n}{2} \right\rfloor + 1 > \frac{n}{2} \iff 2\left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right) > n.$$

Donc, l'indice étant en dehors du tableau, il n'a pas de fils. C'est donc une feuille.

Soit $k \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$. $k \times 2 \leqslant 2$ donc k a un fils donc ce n'est pas une feuille.

Opérations sur les tas

Trois opérations

1. Préservation de la propriété des tas max

   Reçoit un tableau et un indice du tableau

   Modifie le tableau pour qu'il contienne un tas max

2. Construction d'un tas max

   Reçoit un tableau

   Retourne un tas max

3. Tri par tas

   Tri d'un tableau par ordre croissant (décroissant) en utilisant les propriétés d'un tas max (min).

Conservation de la propriété des tas max

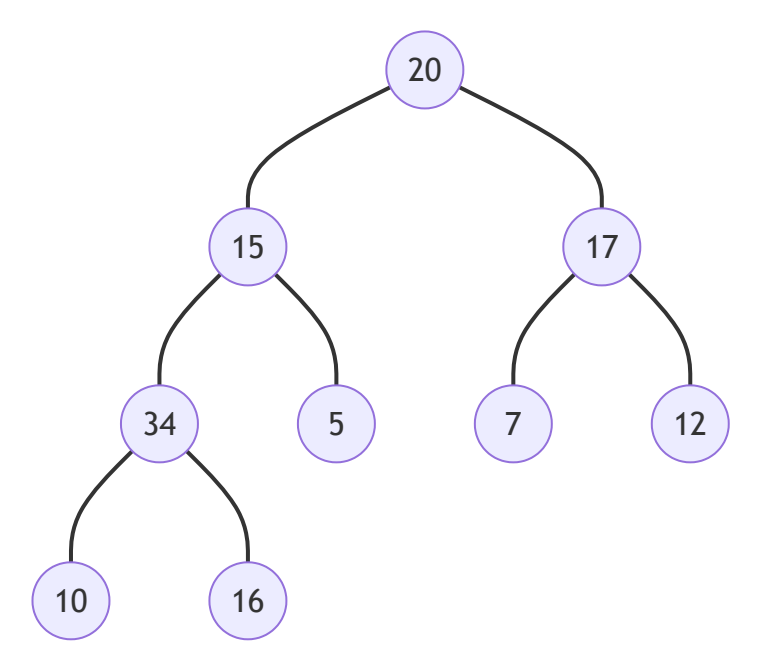
(code sur la feuille)

État de l'arbre et du tableau pour l'appel de `entasserMax(A, 2)` *avec*

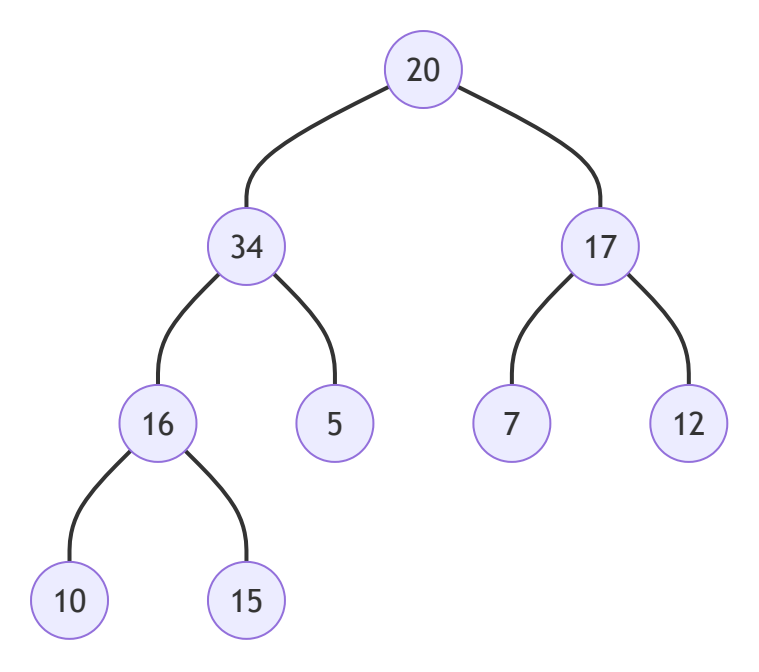
$$A = [\ 20, 15, 17, 34, 5, 7, 12, 10, 16\ ] \quad ?$$

Après une itération, on a $A = [\ 20, 34, 17, 15, 5, 7, 12, 10, 16\ ]$.

Après deux itération, on a $A = [\ 20, 34, 17, 16, 5, 7, 12, 10, 15\ ]$.



devient



Que représente i pour l'arbre résultant ?

Le i représente l'indice dans le tableau de l'arbre de la racine du tas max que l'on veut former.

Fonction `entasserMax` :

- Reçoit un tableau A représentant un tas,
- Reçoit un i,
- Retourne A modifié.

- `entasserMax` fait l'hypothèse que les sous arbres gauche et droit du nœud i sont des tais mais que le nœud i est peut être plus petit que ses enfant.

- `entasserMax` fait alors descendre le nœud i jusqu'à ce que la propriété de tas max soit rétablie localement.

- Complexité en $\mathcal{O}(\ln n) = \mathcal{O}(h)$

Fonction `construireTasMax` :

- Construction d'un tas,
- Conversion en tas max,
- Invariant : au début de chaque itération de la boucle pour, chaque nœud $i+1, i+2, \ldots, n$ est la racine d'un tas max,
- Complexité en $T(n) = \mathcal{O}(n \ln n)$.

Tri par tas (*heap sort*)

On fait remonter la dernière valeur du tableau en l'interchangeant avec la racine du tas (la plus grande valeur). Pour éviter de faire remonter la plus grande valeur

à la racine, on diminue la taille du tas. On recrée un tas local en replaçant la valeur maximale à la racine.

Première étape :

> Construction du tas max
>
> La première valeur est la racine donc l'élément de clé la plus grande.
>
> On place cet élément en dernier.

Seconde étape :

> On rétablit la propriété de tas max sur le tableau privé du dernier élément.

Répétition du processus jusqu'à arriver à un tas de taille 2.

Complexité en $\mathcal{O}(n \ln n)$.

Files de priorité

Exemple d'utilisation très répandue des tas → gestion de files de priorités

Objectifs : classer des événements par ordre de priorité

Nœuds → association (priorité, élément)

Existence de files de priorités min et de files de priorités max

Exemple d'utilisation de files de priorités

- Ordonnancement des tâches
- Ordinateurs multi threads (programme de spé.)
- Parcours en largeur de graphs (Dijkstra, $A^\star$, Prim, ...)

Opérations sur les files de priorités

Opérations sur les tas max → restent accessibles :

- `entasserMax(A, i)`
- `construireTasMax(A)`

Opérations propres aux files max :

- `maximumTas(A)`
- `extraireMaxTas(A)`
- `augmenterCle(A, i, cle)`
- `insererTasMax(A, cle)`

Opération propres aux files min :

- `minimumTas(A)`
- `extraireMinTas(A)`
- `diminuerCle(A, i, cle)`
- `insererTasMin(cle)`

Opérations propres aux files de priorité max

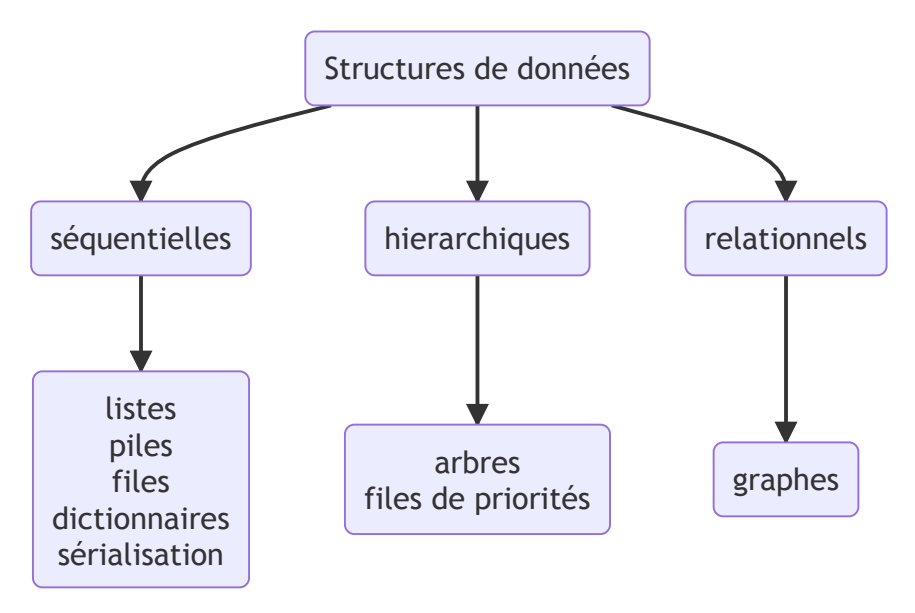
- Opération `maximumTax(A)` :
  - Entrée : tableau `A`
  - Sortie : élément de priorité maximale
  - Sémantique :
    - Retourne -1 si le tas est vide
    - Retourne la racine sinon
    - Ne supprime pas les éléments du tas
- Opération `extraireMaxTas(A)` :
  - Entrée : tableau `A`
  - Sortie : élément de priorité maximale, tableau modifié
  - Sémantique :
    - Retourne -1 si le tas est vide
    - Retourne la racine et le tableau modifié sinon
    - Supprime l'élément du tas
    - Reconstitue la propriété de tas max
- Opération `augmenterCle(A, i, cle)` (c.f. feuille)
- Opération `insérerTasMax(A, cle)` (c.f. feuille)

Chapitre

Structures de données : graphes

I. Introduction

Rappel : classification des structures de données



Exemples de domaines d'utilisation des graphes :

— Réseaux sociaux (liens "d'amitiés" entre deux membres)
— Réseau routier, internet, lignes aériennes, routes maritimes
— Interaction entre deux espèces (réseau trophique)
— Réseaux neuronaux
— Réseaux abstraits (modélisation de prédicats)

II. Définitions

Graphes non orientés

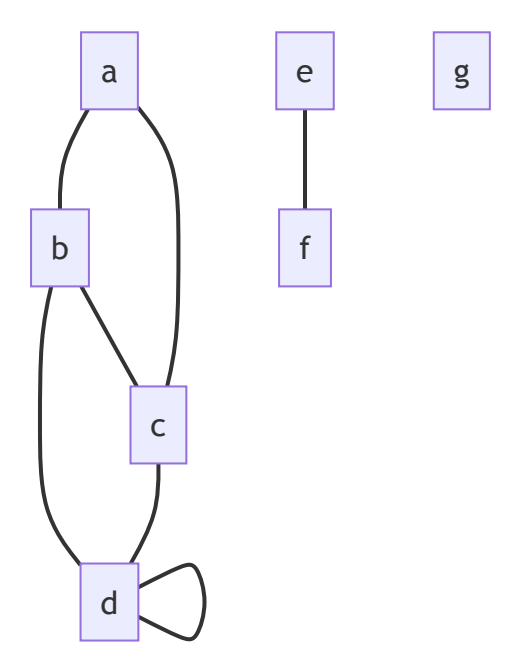
$G = (S, A)$ est un graphe non orienté si

- S est un ensemble fini
- A est une partie de S ayant 1 ou 2 éléments.

Les éléments de S sont appelés nœuds ou sommets de G (*vertices*). Les éléments de A sont appelés arêtes (*edges*).

Exemple :

$$G_2 = \Big(\{a, b, c, d, e, f, g\}, \big\{\{a, b\}, \{b, c\}, \{b, d\}, \{c, d\}, \{d\}, \{e, f\}\big\}\Big)$$



L'arête $\{s\}$ est une boucle.

Un graphe est dit simple s'il ne contient pas de boucles.

L'ordre du graphe est $|S|$ et la taille du graphe est $|S| + |A|$.

Un graphe discret est un graphe sans arêtes. Un graphe vide est un graphe ne contenant aucun sommet et aucune arête.

Le degré d'un sommet $d(s)$ est le nombre d'arêtes ayant s pour extrémité.

Exemple : $d(a) = 2$; $d(g) = 0$; $d(d) = 4$ (on compte les boucles deux fois).

Lemme : *c.f. poly*

Soit $G = (S, A)$ un graphe orienté ou non. Le chemin d'un sommet s à un sommet t de G est la suite finie $c = (s_0, s_1, \ldots, s_n)$ non vide de sommets tels que

— $s_0 = s$
— $s_n = t$
— $\forall i \in [\![0, n-1]\!], \exists a \in A, a = \{s_i, s_{i+1}\}$

— t est accessible depuis s s'il existe un chemin joignant s à t.
— L'entier n est la longueur du chemin.
— La distance de s à t, noté $d(s,t)$ est la longueur minimale d'un chemin joignant s à t.
— Si t est inaccessible depuis s, alors $d(s,t) = \infty$.

Un cycle, ou chemin fermé est un chemin joignant un sommet s à lui-même. Dans un graphe non orienté, la longueur d'un chemin fermée est au moins égale à 1. Toutes les arêtes du chemin sont distinctes. Un chemin de longueur 1, $\{s\} \in A$ est une boucle. Un graphe acyclique est un graphe n'ayant pas de cycles.

Un graphe non orienté est dit connexe lorsque tous les sommets sont à une distance finie les uns des autres. Un graphe non connexe peut être décomposé en plusieurs composantes connexes, les sous graphes connexes maximaux.

Théorème : Un graphe connexe d'ordre n possède $n-1$ arêtes.

Démonstration :

— Avec $n = 1$, on a un graphe contenant 1 nœud, il a donc aucune ou une arête, donc au moins 0.
— On a un graphe connexe ayant n nœuds et au moins $n-1$ arêtes. On ajoute un nœud. Pour avoir un graphe connexe d'ordre n, il faut relier ce nouveau nœud à au moins 1 sommet préexistant. On a donc au moins n arêtes.

Théorème : Si, dans un graphe G simple, tout sommet est de degré supérieur ou égal à 2, alors G possède au moins un cycle.

Démonstration : Partons d'un sommet arbitraire noté V_1. On peut construire une suite finie de sommets $v_1, v_2, \ldots, v_k$ telle que $v_i \notin \{v_1, v_2, \ldots, v_{i-1}\}$ et v_i est un voisin de v_{i-1}. Puisque les sommets de G sont un nombre fini, cette construction se termine. Or, v_k est au moins de degré 2. Donc, il possède, outre v_{k-1}, un voisin v_j dans la séquence. Alors $(v_j, v_{j+1}, \ldots, v_k, v_j)$ est un cycle de G.

Graphes orientés

Un graphe $G = (S, A)$ est orienté si

— S est un ensemble fini
— A est une partie de $S \times S$

Les éléments de S sont appelés nœuds ou sommets de G, et un élément $(s, s') \in A$ est un arc, représenté par une flèche de s à s'.

Un arc (s, s) est une boucle. Un graphe est dit simple s'il ne contient pas de boucles.

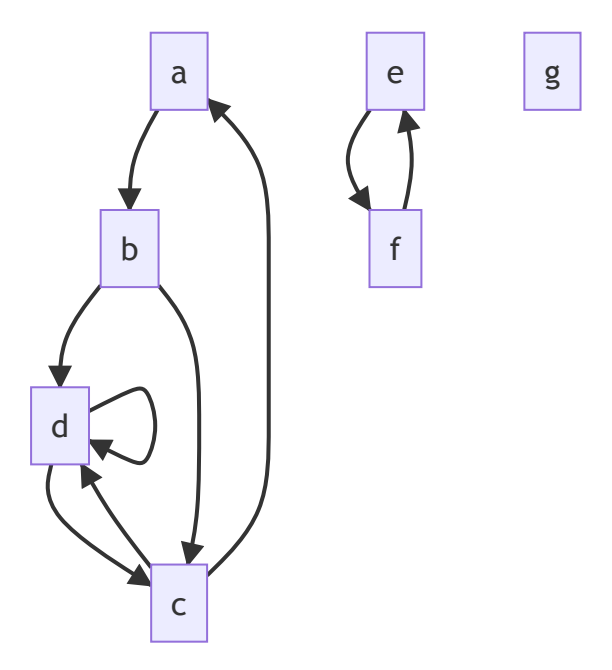
Avec $z = (s, s')$, on dit que s et s' sont les extrémités de z, ou qu'il sont reliés par z. On dit que s est l'extrémité initiale (de départ) de z, ou un prédécesseur

s (voisin entrant). On dit que s' est l'extrémité finale (d'arrivée) de z. L'ordre du graphe est le nombre de sommets, $|S|$. La taille du graphe est $|S| + |A|$.

Un graphe discret est un graphe sans arc (ou arête). Un graphe vide $G = (\varnothing, \varnothing)$ est un graphe sans sommet ni arc.

Le degré sortant d'un sommet s, $d_+(s)$, est le nombre d'arcs partant de s. Le degré entrant d'un sommet s, $d_-(s)$, est le nombre d'arcs arrivant en s. Le degré d'un sommet s, $d(s)$ est la somme du degré sortant et du degré entrant.

$$\begin{cases} d_+(s) = \#\{s' \in E \mid (s, s') \in A\} \\ d_-(s) = \#\{s' \in E \mid (s', s) \in A\} \\ d(s) = d_+(s) + d_-(s). \end{cases}$$



Par exemple, le degré de a est 2, le degré de g est 0 et le degré de d est 5.

Un cycle est un chemin joignant un sommet s à lui-même.

Graphes pondérés

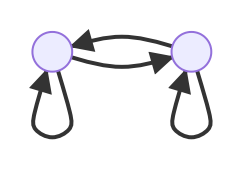
On dit que $G = (S, A, f)$ est un graphe pondéré ou étiqueté si (S, A) est un graphe orienté ou non, et f est une application de A dans un ensemble E.

Si $z \in A$, alors $f(z)$ est l'étiquette de z. On indique $f(z)$ à proximité de l'arête ou de l'arc sur le diagramme sagittal (cf ci-dessous).

Si $E = \mathbb{R}$, $f(z)$ est le coût ou poids de l'arête ou de l'arc.

Le poids ou le coût d'un chemin dans un graphe pondéré est la somme des poids des arêtes parcourus. On l'appelle parfois longueur du chemin (mais c'est en contradiction avec la définition de longueur dans un graphe non pondéré).

E peut être autre chose qu'un nombre. Dans ce cas, on parle de graphe étiqueté (par exemple, les automates).



Graphes bipartis

Soit $G = (S, A)$ un graphe orienté ou non. On dit que G est biparti si l'on peut partitionner S en deux parties S_1 et S_2 telles que deux sommets appartenant à la même partie ne sont pas adjacents (voisins).

Un problème complexe (par exemple un problème NP difficile) sur les graphes peut être simplifié si on a un graphe biparti (cf programme de spé).

Théorème : Un graphe est biparti si et seulement s'il ne contient pas de cycle de longueur impaire.

Démonstration :

— Soit G un graphe biparti non pondéré de classe S_1 et S_2.

  Tout cycle de ce graphe peut se parcourir en partant d'un sommet v de S_1 et doit revenir au sommet de départ en alternant des sommets de S_2 et de S_1.

  Pour revenir à un sommet de S_1, on est obligé de faire des allers retours, qui, par définition, sont de longueur 2.

  Chacun des cycles est de longueur paire.

— On suppose, pour simplifier, que G est connexe (sinon, appliquer le raisonnement à chacune des composantes connexes), non biparti et simple.

  Soit I l'ensemble des sommets à une distance impaire de v. Soit P l'ensemble des sommets à une distance paire de v. On a $S = P \cup I$ et $P \cap I = \varnothing$. Soit $v \in P$.

  Comme G n'est pas biparti, il existe deux sommets adjacents x_1 et x_2 appartenant à P (où à I).

  Comme G est connexe, il existe un chemin c_1 allant de x_1 à v et un chemin c_2 allant de v à x_2 de même parité que c_1.

  La somme des longueurs de c_1 et c_2 est donc paire. Pour former un cycle, il faut alors constituer le chemin $c_2 \cup \{x_1, x_2\} \cup c_1$ de longueur impaire.

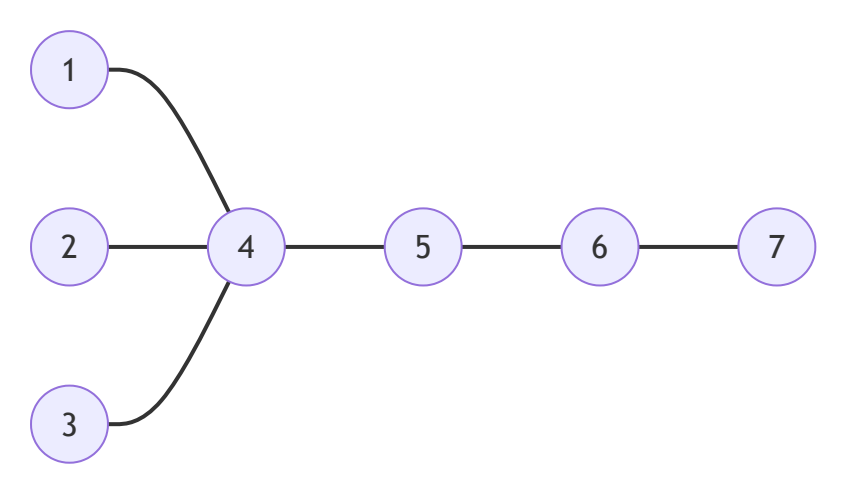
Rappel : Un arbre est un graphe connexe acyclique non orienté.

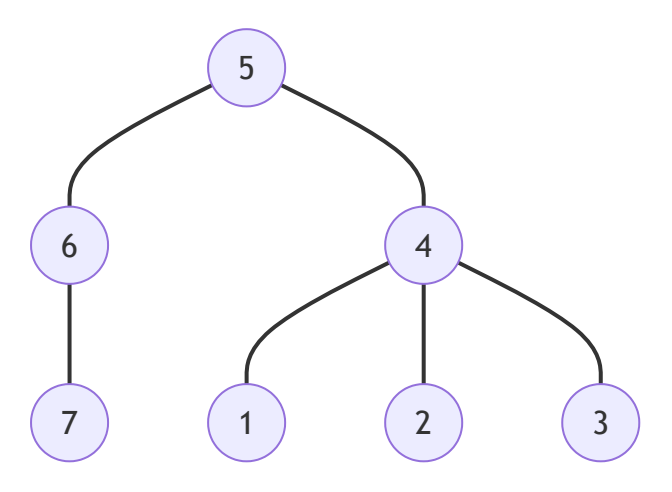
Théorème : Si a et b sont deux sommets distincts d'un arbre G, il existe un unique chemin reliant a et b.

Démonstration : G est connexe, ce qui assure l'existence d'un chemin reliant a et b. S'il existe un autre chemin, un cycle pourrait être construit en utilisant les deux chemins reliant a et b. Or, G est acyclique. On en déduit que le chemin

reliant a et b est unique.

Conséquence : Soit un arbre représenté par un graphe G connexe acyclique non orienté. On a la possibilité de choisir arbitrairement un sommet r de G et d'orienter les arêtes de G pour créer les chemins reliant r à chacun des sommets. On obtient un arbre enraciné en r.





III. Implémentation

Listes d'adjacences

Une liste d'adjacence est la liste des sommets adjacents à un sommet donné. Dans le cas d'un graphe orienté, c'est la liste des successeurs (ou des prédécesseurs).

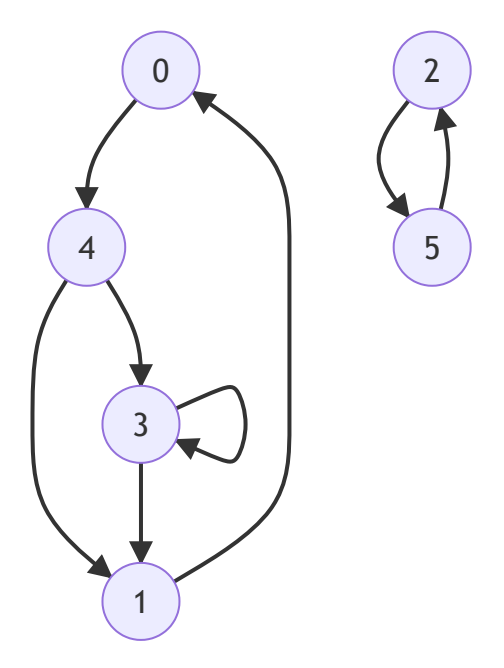
Attention : coïncidence entre le numéro de sommet et l'indice dans la liste.

Par exemple, la matrice d'adjacence du graphe suivant est

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

et la liste d'adjacence est

$$[[4],\ [0,\ 3],\ [5],\ [1,\ 3],\ [1,\ 3],\ [2]].$$

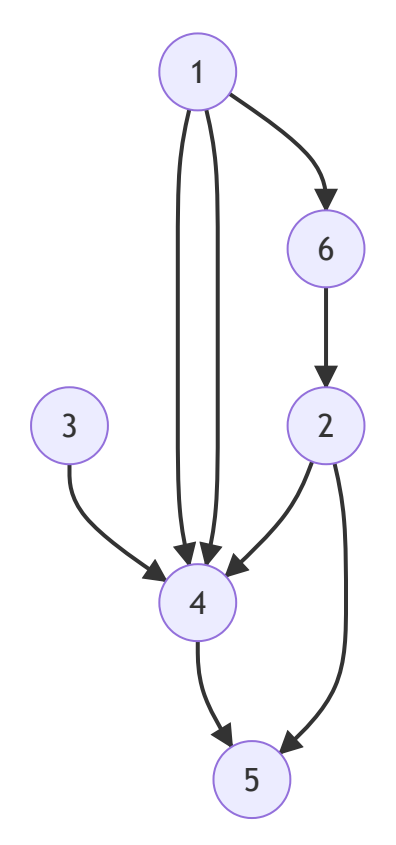


Enregistrements utilisés :

— `Sommet` : liste des sommets adjacents.

1. identifiant nommé `id` de type `'a`
2. liste des sommets adjacents, nommé `voisin` de type `'a list`

— `Graphe` : liste des sommets adjacents.



1. Écrire les instructions définissant les deux types et créant le graphe ci dessus :

```
(* Sommet : identifiant et liste de voisins *)
type 'a sommet = { id : 'a; voisins : 'a list};;

(* Graphe : liste de sommets *)
type 'a graphe = 'a sommet list;;

let g = [
    { id = 1; voisins = [2; 4; 6] };
    { id = 2; voisins = [4; 5] };
    { id = 3; voisins = [4] };
    { id = 4; voisins = [5] };
    { id = 5; voisins = [] };
    { id = 6; voisins = [2] }
];;
```

2. Écrire un fonction récursive `ajoute_arete g a b` de type : `ajoute_arete : 'a sommet list -> 'a -> 'a -> 'a sommet list = <fun>`. Aide : `List.mem` indique si le premier argument est un élément de la liste passée (2nd argument).

   Pré-condition : les sommets passés en arguments sont des sommets du

graphe.

```
(* pré-condition : a et b sont des sommets du graphe *)
let rec ajoute_arete g a b = match g with
  | [] -> failwith "Graphe vide"
    (* impossible d'ajouter une arête *)
  | s :: q when s.id = a && List.mem b s.voisins -> g
    (* teste si a est en tête de liste : si oui (s.id = a) et que b est déjà
       présent parmi les voisins de a (List.mem b s.voisins).
       Dans ce cas, on retourne le graphe inchangé *)
  | s :: q when s.id = a -> { id = a; voisins = b :: (s.voisins) } :: q
  | s :: q -> s :: (ajoute_arete q a b);;
```

3. Écrire une fonction recursive `supprime_arete g a b` de signature `supprime_arete : 'a sommet list -> 'a -> 'a -> 'a sommet list = <fun>` supprimant l'arête entre le sommet a et le sommet b contenu dans le graphe g.

```
let rec supprime_arete g a b = match g with
  | [] -> []
  | s :: q when s.id = a ->
    let rec aux l = match l with
      | [] -> []
      | u :: q when u = b -> q
      | u :: q -> u :: (aux q)
    in { id = a; voisins = (aux s.voisins) } :: q
  | s :: q -> s :: (supprime_arete q a b);;
```

ou

```
let rec supprime_arete g a b =
  let rec aux = function
    (* parcours de la liste des voisins de a *)
    | [] -> failwith "sommet b absent des voisins de a"
      (* pas de voisins *)
    | t :: q when t = b -> q
      (* b : premier voisin dans la liste *)
    | t :: q -> t :: (aux q)
      (* recherche de b parmi les voisins suivants *)
  in match g with
    | [] -> failwith "sommet a absent"
    | s :: q when s.id = a -> { id = a; voisins = aux s.voisins } :: q
      (* sommet a trouvé : appel de aux pour rechercher b parmi les voisins *)
    | s :: q -> s :: (supprime_arete q a b);;
      (* recherche de a parmi les sommets suivants dans le graphe *)
```

4. Écrire une fonction récursive `ajoute_sommet` de signature `ajoute_sommet : 'a sommet list -> 'a -> 'a sommet list = <fun>` ajoutant un sommet.

```
let rec ajoute_sommet g a =
  match g with
```

```
    | [] -> [{ id = a; voisins = {} }]
      (* graphe vide -> ajout du sommet *)
    | x :: q when x.id = a -> g
      (* a dans le graphe -> pas de modification de g *)
    | x :: q -> x :: (ajoute_sommet q a);;
      (* poursuite de la recherche de a dans le reste du graphe *)
```

5. Écrire un fonction récursive `supprime_sommet g a` permettant de supprimer un sommet a du graphe g avec la signature `supprime_sommet : 'a sommet list -> 'a -> 'a sommet list = <fun>`.

```
let rec supprime_sommet g a =
  (* exploration de la liste des voisins pour éliminer a *)
  let rec aux = function
    | [] -> []
    | t :: q when t = a -> q
    | t :: q -> t :: (aux q)
  in match g with
    | [] -> []
    | s :: q when s.id = a -> supprime_sommet q a
    | s :: q ->
      let ns = { id = s.id; voisins = aux s.voisins }
        in ns :: (supprime_sommet q a);;
```

Bilan :

En C : tableau de pointeurs sur liste chaînée d'enregistrements (voir chaînage externe)

Ordre des sommets arbitraire dans la liste des voisins

Remplacement du numéro du sommet par un doublet (sommet, poids) pour un graphe pondéré.

Avantages :

- représentation assez souple : facilité pour ajouter ou supprimer des sommets ou des arêtes,
- occupation mémoire en $n + p$ (n sommets et p arcs)

Inconvénient : pas d'accès rapide à un sommet ou à une arête particulière

Matrices d'adjacence

```
let liste_to_matrice liste =
  let n = List.length liste in
  let matrice = Array.make_matrix n n 0 in

  for a = 0 to (n - 1) do
    let voisins = (List.nth liste a).voisins in

    for b = 0 to (List.length voisins - 1) do
      matrice.(a).(List.nth voisins b) <- 1;
```

```
    done;
  done;

  matrice;;

let matrice_to_liste matrice =
  let liste = ref [] in
  let n = Array.length matrice in
  for a = 0 to (n - 1) do
    let voisins = ref [] in
    for b = (n-1) downto 0 do
      if matice.(a).(b) <> 0 then
        voisins := b :: !voisins;
    done;

    let enr = { id = a; voisins = !voisins } in
    liste := enr :: !liste;
  done;
  liste;;
```

Bilan

Remplacement du 1 par le poids de l'arc pour un graphe pondéré

Avantages :

- Facilité en coût constant aux informations (coût d'un accès tableau)
- Facilité pour ajouter ou supprimer des sommets ou des arêtes

Inconvénients :

- Ajout / Suppression de sommets
- Coût en mémoire : n^2 variables où n est le nombre de sommets

III. Parcours de graphe

Définitions

Parcours de graphe : Énumération de l'ensemble des sommets accessibles par un chemin pour le appliquer un traitement

Objectif : Étude d'une propriété du graphe (biparti, connexité, ...)

Différentes possibilités mais nécessité de maintenir à jour deux listes :

- Liste des sommets déjà traités → déjà vus
- Liste des sommets en cours de traitement → à traiter

Différence entre parcours :

- Manière dont sont ajoutés et extraits les sommets
- Dépend de la structure de données utilisée

Principe :

```
à_traiter <-- [ s0 ]
déjà_vus <-- [ s0 ]

tant que à_traiter != [] faire
  extraire s de à_traiter
  appliquer le traitement à s
  ajouter s à déjà_vus

  pour tout les voisins t de s faire
    si t n'est pas déjà dans déjà_vus alors
      ajouter t à à_traiter
    fin si
  fin pour
fin tant que
```

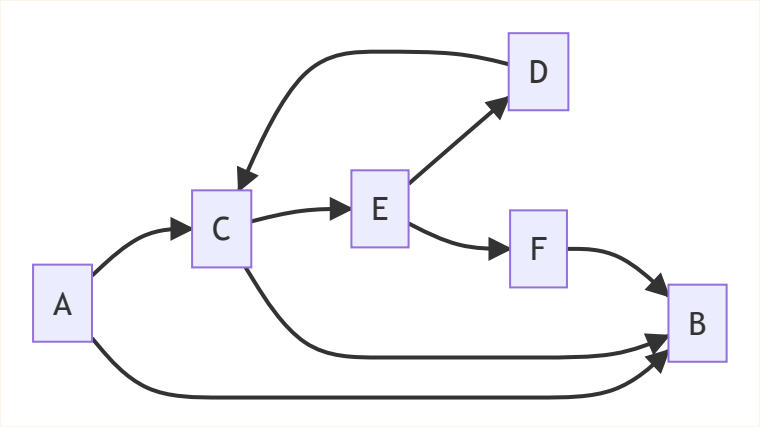
Parcours en largeur

Breadth First Search (BFS)

Structure utilisée : file d'attente (FIFO) pour stocker les sommets

Utilisé notamment pour les recherches de plus court chemin

Exemple : pour le graphe



→ à traiter	déjà vus
A	∅
BC	A
C	AB
E	ABC
DF	ABCE
F	ABCED
∅	ABCEDF

Pour gérer une file en OCamL, on utilise le module `Queue` et éventuellement la fonction `List.iter`. (les fonctions ne sont pas à connaître ; si on en a besoin,

elle seront rappelées)

```
let bfs_queue traitement g initial =
  (* Création d'un array de false : mémoire des sommets traités *)
  let deja_vus = Array.make (Array.length g) false in
  (* Creation d'une file pour ordre de traitement *)
  let a_traiter = Queue.create() in

  (* Fonction traitement d'un sommet et mise à jour des structures *)
  let ajoute x =
    if not deja_vus.(x) then
      begin
        (* Consultation de deja_traite : si le sommet n'a pas été traité *)
        traitement x;
        deja_vus.(x) <- true (* Mise à jours de la liste des sommets traités : true *)
        Queue.push x a_traiter (* Ajout du sommet de la file *)
      end
  in
    ajoute initial; (* Appel de ajout avec le sommet initial *)

  (* Tant que la file n'est pas vide *)
  while not (Queue.is_empty a_traiter) do
    let x = Queue.pop a_traiter in (* Extraction du sommet de la file *)

    (* Pour appeler ajoute à chacun des éléments de g.(x), donc les successeurs de x *)
    List.iter ajoute g.(x);
  done;;

let bfs_artisanal traitement g initial =
  let deja_vus = Array.make (Array.length g) false in
  deja_vus.(initial) <- true;

  let rec traite_sommet liste = match liste with
    | []     -> ()
    | x :: q -> traitement x;
                traite_sommet (q @ voisins g.(x))
  and voisins liste = match liste with
    | []                        -> []
    | y :: q when deja_vus.(y)  -> voisins q
    | y :: q                    -> deja_vus.(y) <- true;
                                   y :: voisins q
  in traite_sommet [ initial ];;
```

Complexité majorée par la taille de graphe donc $\mathcal{O}\big(|S| + |A|\big)$.

Départ du sommet O.

Quand la file `a_traiter` est vide, on identifie les composantes connexes.

IV. Algorithmes des graphes

Algorithmes du plus court chemin

A. Dijkstra

1. Définition et théorème Plus court chemin dans un graphe pondéré : longueur / coût d'un chemin : somme des poids des arêtes

Objectif : déterminer le chemin de longueur minimale entre deux sommets s et s'

Théorème : Soit $G = (S, A)$ un graphe orienté pondérés à poids positifs ou nuls. Soient s et s' deux sommets de G. Si s et s' sont reliés par un chemin, alors il existe un plus court chemin de s à s'.

Démonstration : Soit c un chemin joignant s à s'. Si c passe à deux reprises par le même sommet, un cycle est présent sur le chemin c. Ce cycle peut être supprimé du chemin c. Le processus peut être itéré jusqu'à la disparition des cycles du chemin. Le plus court chemin de s à s' est donc un chemin pour lequel tous les sommets $(s, s_1, \ldots, s')$ sont distincts. Le nombre de sommets étant fini, le nombre de chemins passant par des sommets distincts l'est aussi. Il existe donc un chemin de longueur minimale parmi ces chemins.

Algorithme de Dijkstra : plus court chemin depuis un sommet vers tous les autres sommets du graphe.

Soit $G = (S, A)$ un graphe pondéré et soit M un ensemble de sommets. Un M-chemin est un chemin dont tous les sommets jusqu'à l'avant denier sont dans M et le dernier sommet n'est pas dans M.

Théorème : Soit c un M-chemin, de longueur minimale et x sont dernier sommet (on fixe c PUIS on fixe x). Alors c est le plus court chemin de s à x.

Démonstration (par l'absurde) :

> Supposons qu'il existe c' un chemin de s à x, de longueur strictement inférieure à la longueur de c :
>
> $$\ell(c') < \ell(c)$$
>
> où $\ell(c)$ est la longueur du chemin c.
>
> Soit x', le premier sommet de c' n'étant pas dans M.
>
> Le sous chemin c'' de s à x' est un M-chemin. Donc $\ell(c'') \leqslant \ell(c')$ car les poids sont positifs ou nuls.
>
> Et, $\ell(c'') < \ell(c)$, ce qui contredit l'hypothèse selon laquelle c est un chemin de longueur minimale allant de s à x.

2. Principe de l'algorithme de Dijkstra On définit :

— distance : ensemble des distances depuis s ; distance[i] est la longueur du plus court chemin de s à i. À l'initialisation, toutes les distances sont infinies. L'algorithme affine progressivement l'estimation du plus court chemin.

— prédécesseur : ensemble des prédécesseurs pour un chemin depuis s où prédécesseur$[i]$ est le prédécesseur du sommet i sur le le plus court chemin provisoire depuis s.
— M est l'ensemble des sommets déjà traités ; on utilise le théorème des M-chemins pour bâtir progressivement les plus courts chemins depuis s.
— E est l'ensemble des sommets en attente d'être traités. On a constamment $S = M \cup E$: invariant de l'algorithme de Dijkstra.

Propriétés : cf poly

3. Exemple

1. Indiquer l'état de `Distances`, `Prédécesseurs`, M et E après chaque itération.

   Pour l'initialisation,

   $$\begin{cases} M = \varnothing, \\ E = \{0, 1, 2, 3, 4\}, \\ \text{Distance} : [0, +\infty, +\infty, +\infty, +\infty], \\ \text{Prédécesseur} : [\text{nil}, \text{nil}, \text{nil}, \text{nil}, \text{nil}]. \end{cases}$$

   Après une itération, on a

   $$\begin{cases} M = \{0\}, \\ E = \{1, 2, 3, 4\}, \\ \text{Distance} : [0, 10, +\infty, 5, +\infty], \\ \text{Prédécesseur} : [\text{nil}, 0, \text{nil}, 0, \text{nil}]. \end{cases}$$

   Après deux itérations, on a

   $$\begin{cases} M = \{0, 3\}, \\ E = \{1, 2, 4\}, \\ \text{Distance} : [0, 8, 14, 5, 7], \\ \text{Prédécesseur} : [\text{nil}, 3, 3, 0, 3]. \end{cases}$$

   Après trois itérations, on a

   $$\begin{cases} M = \{0, 3, 4\}, \\ E = \{1, 2\}, \\ \text{Distance} : [0, 8, 13, 5, 7], \\ \text{Prédécesseur} : [\text{nil}, 3, 4, 0, 3]. \end{cases}$$

   Après quatre itérations, on a

   $$\begin{cases} M = \{0, 3, 4, 1\}, \\ E = \{2\}, \\ \text{Distance} : [0, 8, 9, 5, 7], \\ \text{Prédécesseur} : [\text{nil}, 3, 1, 0, 3]. \end{cases}$$

Après cinq itérations, on a

$$\begin{cases} M = \{0, 3, 4, 1, 2\}, \\ E = \varnothing, \\ \text{Distance} : [0, 8, 9, 5, 7], \\ \text{Prédécesseur} : [\text{nil}, 3, 1, 0, 3]. \end{cases}$$

Autre présentation :

0	1	2	3	4	sommet séléctionné
0	∞	∞	∞	∞	0
$\varnothing$	10_0	∞	5_0	∞	3
$\varnothing$	8_3	14_3	$\varnothing$	7_3	4
$\varnothing$	8_3	13_4	$\varnothing$	$\varnothing$	1
$\varnothing$	$\varnothing$	9_1	$\varnothing$	$\varnothing$	2

2. Pour `distance`, `prédécesseur`, M et E, on utilise des tableaux. Pour le graphe G, on utilise une matrice d'adjacence.
3. Pour le graphe, on utilise une liste d'adjacence car ça économise de la mémoire et l'accès aux voisins est plus simple. Pour `distance` et `prédécesseur`, on utilise deux tableaux d'entiers de dimension $\#S$. Pour M et E, on utilise un tableau de bouléens de taille $\#S$ où $x \to$ `true` représente $x \in E$ et $x \notin M$ et $x \to$ `false` représente $x \in M$ et $x \notin E$.
4. On utilise la stratégie gloutonne.

```
Alorgithme Dijkstra(G, s):
    distances = créer_tableau(nb_sommets, +infini)
    prédécesseurs = créer_tableau(nv_sommets, nil)
    distances[s] = 0
    dist = créer_file(nb_sommets)
    E = créer_tableau(nb_sommets, true)

    Tant que dist n'est pas vide faire
        u <- extraire_min(dist)
        rétablire_propriété_file(dist) # O(|S| ln(|S|))
        E[u] = false

        Pour chaque voisin v de u présent tel que E[v] = true faire # O(|A|)
            Si distances[v] >= distances[u] + pondération(u,v) alors
                distances[v] = distances[u] + pondération(u,v) alors
                diminuer_clé(dist, v) # O(ln(|S|))
                prédécesseurs[v] = u
            Fin Si
        Fin Pour
    Fin Tant Que
```

La complexité de cet algorithme est donc

$$\mathcal{O}\Big(\big(|A| + |S|\big) \times \ln\big(|S|\big)\Big).$$

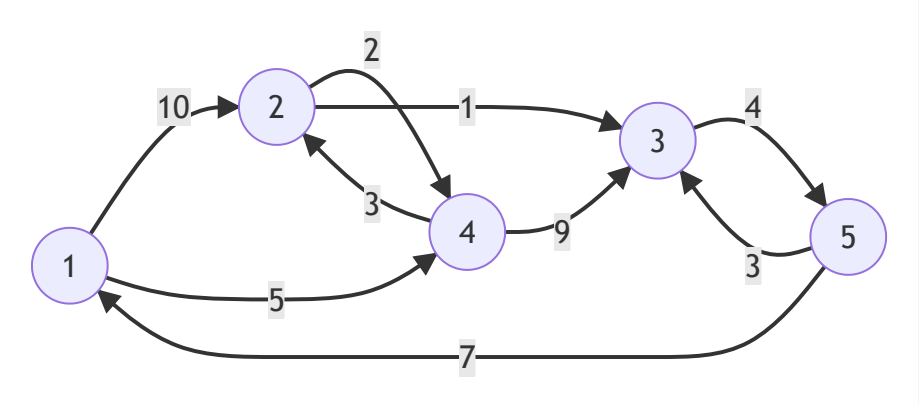
La terminaison et l'invariant sont sur le polycopié.

B. Floyd-Warshall

Plus court chemin dans un graphe pondéré avec des pondérations positives ou négatives mais pas de cycle de poids strictement négatifs.

Plus courts chemins entre toutes les paires de sommets.

Utilisation de la programmation dynamique : sous structure optimale, chevauchement de sous-problèmes et mémorisation des résultats.



Dans le graphe, quel est le plus court chemin de 5 à 2 ?

$$5 \to 1 \to 4 \to 2 \qquad \text{coût : } 15$$

Mise en place de deux matrices :

- une matrice contenant les chemins (prédécesseurs) $\to P$
- une matrice contenant les distances $\to D$

$$D = \begin{array}{c} \\ \text{sommet de départ} \end{array} \overset{\text{sommet d'arrivée}}{\begin{bmatrix} 0 & 8 & 9 & 5 & 7 \\ 11 & 0 & 1 & 2 & 4 \\ 11 & 19 & 0 & 16 & 4 \\ 9 & 3 & 4 & 0 & 2 \\ 7 & 15 & 6 & 12 & 0 \end{bmatrix}} \qquad P = \begin{bmatrix} 1 & 4 & 2 & 1 & 4 \\ 5 & 2 & 2 & 2 & 4 \\ 5 & 4 & 3 & 1 & 3 \\ 5 & 4 & 2 & 4 & 4 \\ 5 & 4 & 5 & 1 & 5 \end{bmatrix}$$

Structure d'un plus court chemin Sur un chemin $c = (v_1, v_2, \ldots, v_m)$, on définit les sommets intermédiaires de c comme étant l'ensemble des sommets $\{v2, \ldots, v_{m-1}\}$.

On considère :

- $S = \{1, 2, \ldots, n\}$, les sommets de $G = (S, A, f)$, graphe pondéré sans cycle de longueur strictement négative.
- Sous-ensemble de G : $\{1, 2, \ldots, k\}$ les sommets pour un k donné
- Un couple (i, j) de sommets quelconques de G
- Tous les chemins allant de i à j dont les sommets intermédiaires sont tous dans $\{1, 2, \ldots k\}$.
- Parmi ces chemins, p est le chemin de longueur minimale

k est-il visité par p ?

> **Non** $\rightarrow$ un plus court chemin de i à j ayant tous ses sommets intermédiaires dans $\{1, 2, \ldots, k-1\}$ est aussi un plus court chemin ayant tous ses sommets intermédiaires dans $\{1, 2, \ldots, k\}$.
>
> **Oui** $\rightarrow$ le chemin p se divise en $i \overset{p_1}{\rightsquigarrow} k \overset{p_2}{\rightsquigarrow} j$ avec p_1 le plus court chemin de i à k ayant tous ses sommets intermédiaires dans $\{1, 2, \ldots, k-1\}$ et p_2, plus court chemin de k à j ayant tous ses sommets intermédiaires dans $\{1, 2, \ldots, k-1\}$.

Exemple : pour aller de $i = 5$ à $j = 2$, le chemin le plus court $(5, 1, 4, 2)$. Les sommets intermédiaires sont 1 et 4 ; 4 dernier sommet intermédiaire de p. Les sommets intermédiaires sont dans le sous-ensemble de sommets $\{1, 3, 4\}$.

> Pour $k = 4$, 4 est sur le chemin p ; il se décompose donc en un chemin p_1 de 5 à 4 dont les sommets intermédiaires sont dans $\{1, 3\}$, et en un chemin p_2 de 4 à 2 dont tous les chemins intermédiaires sont dans $\{1, 3\}$.

p_1 et p_2 sont les chemins de longueur minimale entre 5 et 4, d'une part, et entre 4 et 2 d'autre part.

Mise en place d'une relation de récurrence en considérant ensuite p_1 et p_2 avec $k = 3$.

On a donc $D = (d_{i,j})$ avec

$$d_{i,j}^{(k)} = \begin{cases} f_{i,j} & \text{si } k = 0 \\ \min\left(d_{i,j}^{(k-1)}, d_{i,k}^{(k-1)} + d_{k,j}^{(k-1)}\right) & \text{si } k > 0. \end{cases}$$

Le cas où $k = 0$ correspond à l'initialisation (chemin sans sommet intermédiaire). La matrice D correspond alors à la matrice d'adjacence

$$d_{i,j} = \begin{cases} 0 & \text{si } i = j \\ f_{i,j} & \text{si } i \neq j \text{ et } (i,j) \in A \\ +\infty & \text{si } i \neq j \text{ et } (i,j) \notin A. \end{cases}$$

Idée de l'algorithme :

- On fixe un sommet k.
- Pour chaque couple de sommets (i, j), on regarde si inclure k dans le chemin permet d'obtenir un chemin plus court.
- On itère pour chaque sommet k de S.

Mise à jour des prédécesseurs : matrice P

En pratique, deux manière de procéder

1. Détermination de D puis recherche de P à partir de D
2. Détermination simultanée de D et de $P \rightarrow$ formulation d'une relation de récurrence entre $P^{(k)}$ et $P^{(k-1)}$.

Initialisation de $P \to P^{(0)}$:

$$p_{i,j} = \begin{cases} \text{nil ou } -1 & \text{si } i = j \text{ ou } f_{i,j} = \infty \\ i & \text{si } i \neq j \text{ et } f_{i,j} < \infty \end{cases}$$

Relation de récurrence pour la matrice P :

$$p_{i,j}^{(k)} = \begin{cases} p_{i,j}^{(k-1)} & \text{si } d_{i,j}^{(k-1)} \leqslant d_{i,k}^{(k-1)} d_{k,j}^{(k-1)} \\ p_{k,j}^{(k-1)} & \text{si } d_{i,j}^{(k-1)} > d_{i,k}^{(k-1)} d_{k,j}^{(k-1)} \end{cases}$$

Pour $k = 4$, on a

$$D = \begin{pmatrix} 0 & 8 & 9 & 5 & 7 \\ \infty & 0 & 1 & 2 & 4 \\ \infty & \infty & 0 & \infty & 4 \\ \infty & 3 & 4 & 0 & 2 \\ 7 & 15 & 6 & 12 & 0 \end{pmatrix} \qquad P = \begin{pmatrix} & 4 & 2 & 1 & 4 \\ ? & & 2 & 2 & 4 \\ ? & ? & & ? & 3 \\ ? & 4 & 2 & & 4 \\ 5 & 4 & 5 & 1 & \end{pmatrix}.$$

Avec $k = 5$, les matrices deviennent

$$D = \begin{pmatrix} 0 & 8 & 9 & 5 & 7 \\ 11 & 0 & 1 & 2 & 4 \\ 11 & 19 & 0 & \infty & 4 \\ \infty & 3 & 4 & 0 & 2 \\ 7 & 15 & 6 & 12 & 0 \end{pmatrix} \qquad P = \begin{pmatrix} & 4 & 2 & 1 & 4 \\ 5 & & 2 & 2 & 4 \\ 5 & 4 & & ? & 3 \\ ? & 4 & 2 & & 4 \\ 5 & 4 & 5 & 1 & \end{pmatrix}$$

En effet, $d_{3,2} = \infty$ et $d_{3,5} + d_{5,2} = 4 + 15 = 19 \to$ remplacement dans D.

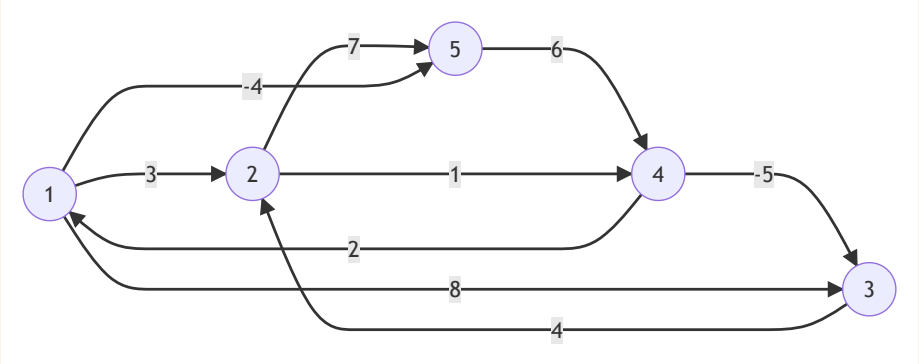
Pour le chemin : décomposition de $(3, \ldots, 2)$ en $(3, \ldots, 5)$ et $(5, \ldots, 2)$; et on exclut 5 du sous-ensemble des sommets intermédiaires, on ne considère plus que le chemin 5 à 2.

> $\to$ prédécesseur de 2 dans le chemin de 3 à 2 devient prédécesseur de 2 dans le chemin de 5 à 2 donc 4.

```
Algorithme FloydWarsallAscendant(G)
    Début
        n = |S|
        D = G
        P = créer_tableau(n * n, prédécesseur dans G)

        Pour k = 1 à n faire
            Pour i = 1 à n faire
                Pour j = 1 à n faire
                    Si i != j et D(i,j) > D(i,k) + D(k,j) alors
                        D(i,j) = D(i,k) + D(k,j)
                        P(i,j) = P(k,j)
                    Fin Si
                Fin Pour
            Fin Pour
        Fin Pour
    Fin
```

Évolution des matrices D et P pour le graphe suivant ?



Pour $k = 0$, on a

$$D = \begin{pmatrix} / & 3 & 8 & \infty & -4 \\ \infty & / & \infty & 1 & 7 \\ \infty & 4 & / & \infty & \infty \\ 2 & \infty & -5 & / & \infty \\ \infty & \infty & \infty & 6 & / \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} / & 1 & 1 & ? & 1 \\ ? & / & ? & 2 & 2 \\ ? & 3 & / & ? & ? \\ 4 & ? & 4 & / & ? \\ ? & ? & ? & 5 & / \end{pmatrix}$$

Pour $k = 1$, on a

$$D = \begin{pmatrix} / & 3 & 8 & \infty & -4 \\ \infty & / & \infty & 1 & 7 \\ \infty & 4 & / & \infty & \infty \\ 2 & 5 & -5 & / & -2 \\ \infty & \infty & \infty & 6 & / \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} / & 1 & 1 & ? & 1 \\ ? & / & ? & 2 & 2 \\ ? & 3 & / & ? & ? \\ 4 & 1 & 4 & / & 1 \\ ? & ? & ? & 5 & / \end{pmatrix}$$

Pour $k = 2$, on a

$$D = \begin{pmatrix} / & 3 & 8 & 4 & -4 \\ \infty & / & \infty & 1 & 7 \\ \infty & 4 & / & 5 & 11 \\ 2 & 5 & -5 & / & -2 \\ \infty & \infty & \infty & 6 & / \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} / & 1 & 1 & 2 & 1 \\ ? & / & ? & 2 & 2 \\ ? & 3 & / & 2 & 2 \\ 4 & 1 & 4 & / & 1 \\ ? & ? & ? & 5 & / \end{pmatrix}$$

Pour $k = 3$, on a

$$D = \begin{pmatrix} / & 3 & 8 & 4 & -4 \\ \infty & / & \infty & 1 & 7 \\ \infty & 4 & / & 5 & 11 \\ 2 & -1 & -5 & / & -2 \\ \infty & \infty & \infty & 6 & / \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} / & 1 & 1 & 2 & 1 \\ ? & / & ? & 2 & 2 \\ ? & 3 & / & 2 & 2 \\ 4 & 3 & 4 & / & 1 \\ ? & ? & ? & 5 & / \end{pmatrix}$$

Pour $k = 4$, on a

$$D = \begin{pmatrix} / & 3 & -1 & 4 & -4 \\ 3 & / & -4 & 1 & -1 \\ 7 & 4 & / & 5 & 3 \\ 2 & -1 & -5 & / & -2 \\ 8 & 5 & 1 & 6 & / \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} / & 1 & 4 & 2 & 1 \\ 4 & / & 4 & 2 & 1 \\ 4 & 3 & / & 2 & 1 \\ 4 & 3 & 4 & / & 1 \\ 4 & 3 & 4 & 5 & / \end{pmatrix}$$

Pour $k = 5$, on a

$$D = \begin{pmatrix} / & 1 & -3 & 2 & -4 \\ 3 & / & -4 & 1 & -1 \\ 7 & 4 & / & 5 & 3 \\ 2 & -1 & -5 & / & -2 \\ 8 & 5 & 1 & 6 & / \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} / & 3 & 4 & 5 & 1 \\ 4 & / & 4 & 2 & 1 \\ 4 & 3 & / & 2 & 1 \\ 4 & 3 & 4 & / & 1 \\ 4 & 3 & 4 & 5 & / \end{pmatrix}$$

On implémente G à l'aide d'une matrice d'adjacence. La complexité de cet algorithme est en $\mathcal{O}\big(|S|^3\big)$; c'est intéressant pour les graphes de petite taille ou de taille modérée.

Chapitre

Bases de données

Objectifs :

- structure d'une base de données
- interrogation d'une base de donnée

I. Introduction

Besoin

Stockage d'un grand nombre de données :

optimisation du volume de stockage

intégrité des données

Redondance ces stockages
Redondance des alimentations électriques / systèmes de refroidissements

Rapidité d'accès à l'information

Délocalisation du stockage dans le Cloud

Définition d'une relation

Relation :

- modèle abstrait → structure mais pas d'opérations
- pas associé à un langage
- pratique pour l'analyse du monde réel

Relation / table : $R = (A_0 : D_0, A_1 : D_1, \ldots)$ où A_i est le nom de l'attribut et D_i est le domaine de l'attribut A_i :

→ ensemble des valeurs possibles (fini ou non)

→ type asocié

Base de données → ensemble de relations

Nécessité de représenter les relations : tableau, enregistrements,...

Vocabulaire

— Relation et tables sont synonymes.
— Attributs, champs et traits sont synonymes
— Instance, enregistrement, observation (≃ ligne de données)

Clé primaire : ensemble d'attributs permettant l'identification d'un enregistrement sans ambigüité.

L'implémentation de SQL n'est pas au programme, uniquement la syntaxe l'est.

Opérations sur les données

Type d'opération sur les données → requêtes

— Créer / insérer
— Mettre à jour / modifier
— Détruire
— Rechercher → la seule au programme

Traitement de la requête :

1. Analyse syntaxique
2. Optimisation par le SGBD (système de gestion de base de données) → Hors programme
3. Exécution pour obtenir le résultat

Interrogation de la base de données :

calcul relationnel → hors programme

algèbre relationnelle → hors programme

langage de requête : SQL → au programme

Sélection : renvoie une table contenant une partie des enregistrements.

Projection : Renvoie une table contenant une partie des attributs.

Le résultat de la requête ci-dessous est une table.

```
SELECT att_1, att_1, ... FROM nom_table WHERE condition;
```

Pour récupérer tous les attributs, on utilise `*`.

Pour les conditions, on peut utiliser `+`, `-`, `*`, `/`, `=`, `<>`, `<=`, `>=`, `<`, `>`, `and`, `or`, `not`, `is null`, `is not null`.

Exemples :

```
SELECT Id, Nom FROM villes WHERE Region = "Pays de la Loire";
SELECT Id, Nom, Nb_hab FROM villes WHERE Id = 5;
SELECT Id, Nom, Nb_hab FROM villes WHERE Nom = "Nantes";
SELECT Id, Nom, Nb_hab FROM villes WHERE Nb_hab = 934000;
SELECT * FROM villes WHERE Region = "Pays de la Loire";
SELECT Id, Nom FROM villes WHERE Id >= 5;
SELECT Id, Nom, Nb_hab FROM villes WHERE Region = "Pays de la Loire" ORDER BY Id DESC
SELECT DISTINCT Region FROM villes ORDER BY Region ASC;
```

L'utilisation de `ORDER BY` permet d'ordonner les éléments d'une table lors d'une requête.

ordre lexicographique, comparaison de nombres

possibilités de combiner l'ordre : `ORDER BY Region ASC, Nom DESC`.

L'utilisation de `DISTINCT` permet de supprimer les redondances de la table de retour de requête.

Au lieu de faire `X = "Possibilité 1" OR X = "Possibilité 2"`, on peut écrire `X IN ("Possibilité 1", "Possibilité 2")`.

Attention, si on a une valeur à `NULL`, on ne peut pas utiliser l'égalité (`X = NULL`) mais on doit utiliser le mot clé `IS` (`X IS NULL`).

Autre possibilité pour le 5. : utiliser `GROUP BY` en fin de requête pour regrouper les attributs identiques (normalement prévu pour une utilisation plus complexe).

Le mot clé `LIMIT` permet de limiter le nombre de lignes retournées. Si on veut omettre des lignes au début, on utilise l'instruction `OFFSET`.

Exemples :

```
SELECT Id, Nom, Region FROM Villes
ORDER BY Region ASC, Nom DESC;

SELECT Id, Nom, Region FROM Villes
ORDER BY Region ASC, Nom DESC LIMIT 3;

SELECT Id, Nom, Region FROM Villes
ORDER BY Region ASC, Nom DESC LIMIT 3 OFFSET 5;
```

Aggrégations : opérations sur les valeurs d'un attribut `MIN`, `MAX`, `AVG`, `COUNT`, `SUM`.

`GROUP BY` : regroupement (en fin de requête).

`NULL` : ignorés.

Attention : pas d'agrégation dans le `WHERE`.

`AS` : alias

Filtrage des agrégats avec `HAVING` (en fin de requête) → après un `GROUP BY` (mais cela dépend des environnements)

`WHERE` → attribut unique

`HAVING` →

Exemple de syntaxe :

```
SELECT MIN(att_2) FROM nom_table WHERE condition_1
GROUP_BY att_1 HAVING condition_2
```

Exemples :

```
SELECT MIN(Nb_hab) FROM Villes;

SELECT AVG(Nb_hab) AS A_TROUVER FROM Villes;

SELECT Region, AVG(Nb_hab_region) as moyenne FROM Villes
GROUP BY Region ORDER BY moyenne DESC;
```

```
# 3 solutions :

SELECT Nom FROM Villes GROUP BY Id
HAVING Nb_hab_region = MIN(Nb_hab_region); # je ne sais pas si ça marche...

SELECT Nom FROM Villes WHERE Nb_hab = (SELECT MIN(Nb_hab FROM Villes);

SELECT Nom FROM Villes ORDER BY Nb_hab ASC LIMIT 1;

SELECT COUNT(Nb_hab) AS PAS_UN_PIEGE FROM Villes;

SELECT COUNT(DISTINCT Nb_hab_region) as Plus_compliquee FROM Villes;

SELECT Region, AVG(Nb_hab) AS moyenne FROM Villes
GROUP BY Region HAVING moyenne > 200 000;
```

Stockage redondant de `Nb_hab_region` : utilisation de deux tables `Villes` et `Region`.

Le lien entre les tables est fait avec un identifiant primaire au lieu de chaînes de caractères (car les accents sont difficiles à prévoir) :

- dans la table `Villes`, on stocke `ID_Region`
- dans la table `Region`, on a un attribut `ID`

Type `IPK` → *Integer Primary Key*.

Attention aux ambigüité sur les noms d'attributs.

Opérations sur les tables ↔ opérations sur les ensembles

- Intersection avec `INTERSECT` :

```
SELECT * FROM Villes_1 INTERSECT SELECT * FROM Villes_2
```

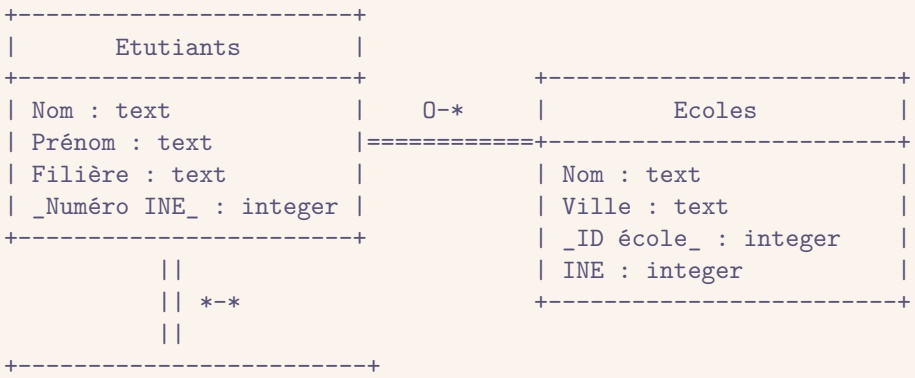
- Union avec `UNION` :

```
SELECT * FROM Villes_1 UNION SELECT * FROM Villes_2
```

- Soustraction avec `EXCEPT` :

```
SELECT * FROM Villes_1 EXCEPT SELECT * FROM Villes_2
```

Représentation des modèles entité-relation :



```
|        Concours          |
+--------------------------+
| Nom : text               |
| _ID Concours_ : integer  |
| INE : integer            |
+--------------------------+
```

Produit cartésien :

```
SELECT att FROM table1 JOIN table2
```

On associe chaque ville à chaque région (même Bordeaux – Pays de la Loire ou Bordeaux – Bretagne).

Utilisation de `ON` à la place de `WHERE` pour vérifier une condition sur un `JOIN` :

```
SELECT Villes.Nom, Regions.Nom FROM Villes JOIN Regions
ON Villes.ID_Region = Regions.ID_Regions
```

retourne

Nom_ville	Nom_region
Bordeaux	Nouvelle-Aquitaine
Angoulème	Nouvelle-Aquitaine
Lyon	Auvergne-Rhône-Alpes
...	...

On peut utiliser plusieurs `JOIN ... ON ...` :

```
SELECT * FROM T1 JOIN T2 ON ... JOIN T3 ON ...;
```

Jointure gauche `LEFT JOIN` : retourne une table contenant toutes les occurrences de la table *gauche* (1ère citée) même si elles ne vérifient pas la condition du `ON`.

```
SELECT Villes.Nom AS Nom_villes, Region.Nom AS Nom_region
FROM Regions LEFT JOIN Villes ON Villes.ID_Regions = Regions.ID;

SELECT Villes.Nom AS Nom_villes, Region.Nom AS Nom_region
FROM Villes LEFT JOIN Regions ON Villes.ID_Regions = Regions.ID;
```

Exercice :

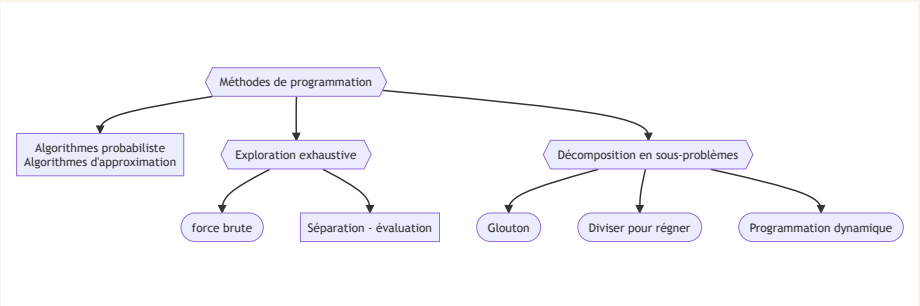
```
SELECT Villes.Nom, Regions.Nom, Regions.Nb_hab FROM Villes
WHERE Villes.Nom = "Nantes" JOIN Regions
ON Villes.ID_Region = Regions.ID;

SELECT Villes.Nom, Regions.Nom, Villes.Nb_hab FROM Villes
JOIN Regions ON Villes.ID_Region = Regions.ID
ORDER BY Villes.Nb_hab DESC LIMIT 1;
```

Chapitre

Méthodes de programmation : diviser pour régner

Introduction



I. Principe

Résolution d'un problème en 3 étapes

1. *Diviser* le problème P en sous problèmes $\rightarrow$ apparition d'un certain nombre de sous-problèmes de même instance que P
2. *Régner* : résoudre les sous problèmes de manière récursive ou non
3. *Combiner* les solutions au sous problèmes en une solution à P

a. Diviser

Division d'un problème P en sous problèmes de taille environ $\frac{n}{b}$.

Par exemple,

— On divise en 2 sous problèmes de taille identique $b = 2$
— On divise en 2 sous problèmes de taille inégale
— Autres combinaisons de sous problèmes

On divise les problème jusqu'à ce que les sous problèmes aient une résolution triviale.

Lien avec les algorithmes récursifs :

— un problème non trivial : appel récursif
— un problème trivial : cas de base

Problème lié avec la récursivité : taille de la pile. Solution : arrêt des appels récursifs quand un seuil s est atteint. Ce seuil s peut dépendre de :

— des ressources machines
— type de données
— ⋮

Il est possible de combiner les méthodes de programmation pour gagner en efficacité. Par exemple, pour trouver des racines à une fonction.

Il est possible d'avoir plusieurs cas de base :

— moins efficace du point de vue temporel
— plus efficace du point de vue gestion de la mémoire

Le coût engendré par l'étape de division est noté $D(n)$

b. Régner

Obtention d'un ou de plusieurs sous problème(s) trivial(aux) : résolution directe (cas de base)

Possibilité d'obtenir des sous problèmes un peu différents du problème : intégration de ces cas dans l'étape combiner

On note le coût engendré par l'étape régner $aT\left(\frac{n}{b}\right)$

Par exemple,

— pour une division en 2 sous problèmes de taille égale dont les 2 doivent être résolus, $a = 2, \quad b = 2$. On a donc $2T\left(\frac{n}{2}\right)$
— pour une division en 2 sous problèmes de taille égale dont un seul doit être résolu, $a = 1, \quad b = 2$. On a donc $T\left(\frac{n}{2}\right)$

c. Combiner

Combinaison des solutions au sous problèmes (même ou différente instance)

Production de la solution au problème P

Coût : $C(n)$

Coût temporel :

Forme général :

$$T(n) = aT\left(\frac{n}{b}\right) + D(n) + C(n)$$

Remarque : les parties entières $\lfloor \quad \rfloor$ sont généralement omises. Par exemple, $\frac{n}{2}$ si n est impaire

Conditions souvent ignorés : $n = 1$ ou $n = s$ avec un coût supposé en $\Theta(n)$. Ce n'est pas forcément le cas (non traité)

II. Exemples déjà vus en cours

— Recherche de valeur dans un tableau trié

$\Theta(n)$ pour la version itérative

$\Theta(\ln n)$ pour la version diviser pour régner (dichotomie) On a $a = 1$ et $b = 2$ car le tableau est divisé en 2.

— Exponentiation a^n

$\Theta(n)$: coût linéaire pour la version itérative

$O(\ln n)$ pour la version récursive car le problème est divisé par 2 à chaque appel récursif

III. Autres exemples

Algorithmes de tri

Stratégie :

— exploration exhaustive (toutes les possibilités) : bogosort
— glouton : tri par insertion
— diviser pour régner : diviser en sous tableaux dont le tri est trivial (tri fusion)

Déjà vus :

— tri par insertion (glouton exact) meilleur : $O(n)$, pire : $O(n^2)$
— tri par sélection (glouton) $O(n^2)$

Tri fusion :

Complexité : $O\big(n\ln(n)\big)$ car

— Division : pour une profondeur de k, on a $2^k \geqslant n \geqslant 2^{k+1}$ donc $n = e^{k\ln 2}$ et donc $k = \log_2(n)$
— Combinaison : On a n comparaisons car il y a n éléments dans le tableau

Mise en place :

```
Fonction TriFusion(T, inf, sup)
    Si inf = sup
        Retourner T
    Sinon
        m <- floor((inf + sup) / 2)

        TriFusion(T, inf, m)
        TriFusion(T, m+1, sup)

        Fusion(T, inf, m, sup)
    Fin Si
Fin

Fonction Fusion(T, inf, m, sup)
    taille1 <- floor(m - inf) + 1
    taille2 <- floor(sup - m)

    gauche <- []
    droite <- []

    Pour i = inf à sup
        Si i <= m
            gauche[i] <- T[i]
        Sinon
            droite[i - m] <- T[i]
        Fin Si
    Fin Pour

    i <- 0
    j <- 0
    k <- 0

    Tant que i < taille1 && j < taille 2
        Si gauche[i] < droite[j]
            T[k] = gauche[i]
            i <- i + 1
        Sinon
            T[k] = droite[j]
            j <- j + 1
        Fin Si

        k <- k + 1
    Fin tant que

    Si i > taille1
        Tant que j > taille2
            T[k] <- droite[j]
            k <- k + 1
            j <- j + 1
        Fin tant que
```

```
    Sinon
        Tant que i > taille1
            T[k] <- gauche[i]
            k <- k + 1
            i <- i + 1
        Fin tant que
    Fin Si
Fin
```

Tri rapide

Principe :

- positionner une valeur directement à sa place définitive
- placer les plus petits à gauche et les plus grands à droite

Avantage : économe en place (pas de nouveau tableau, pas de variable auxiliaire)

La fonction `TriRapide` sépare le tableau en fonction de la position de la clé

```
Fonction TriRapide(T, inf, sup)
    Si sup <= inf
        Retourner T
    Fin Si

    clé <- Position(T, inf, sup)

    TriRapide(T, inf, clé)
    TriRapide(T, clé + 1, sup)
Fin

Fonction Position(T, inf, sup)
    clé <- T[inf]
    i <- inf // gauche
    j <- sup // droite

    Tant que j >= i
        Tant que i < j et T[i] < cle
            i <- i + 1
        Fin Tant que

        Tant que i < j et T[j] > cle
            j <- j - 1
        Fin Tant que

        Si j > i et T[i] > T[j]
            Échanger(T, i, j)
        Fin Si
    Fin Tant que

    Échanger(T, 0, j)
```

```
    Retourner j
Fin

Fonction Échanger(T, i, j)
    temp <- T[j]
    T[j] <- T[i]
    T[i] <- temp
Fin
```

Étude des boucles

- boucle sur i

  terminaison : $j - i + 1$

  invariant : $\forall k \in [\![\inf +1, i]\!], T[k-1] \leqslant cle$
- boucle sur j

  terminaison : j

  invariant : $\forall k \in [\![j, \sup]\!], T[k+1] \geqslant cle$
- boucle extérieur :

  terminaison : $j - i + 1$

  invariant : combinaison des invariants des deux boucles

Complexité :

- meilleur des cas : $O\big(n \ln(n)\big)$
- pire des cas : $O\big(n^2\big)$

Autre algorithme :

```
Fonction Position(T, inf, sup)
    cle <- T[inf]
    j <- sup + 1

    Pour i = sup à inf + 1 (décroissant)
        Si T[i] >= cle
            j <- j - 1
            Échanger(T, i, j)
        Fin Si
    Fin Pour

    Échanger(T, inf, j-1)

    Retourner j-1
Fin
```

Chapitre

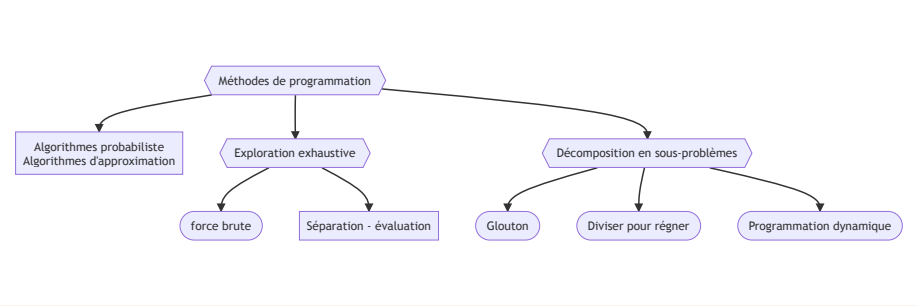
Méthodes de programmation : programmation dynamique

Programmation dynamique

Objectifs du cours :

— Cadre pour les techniques de programmation
— Programmation dynamique

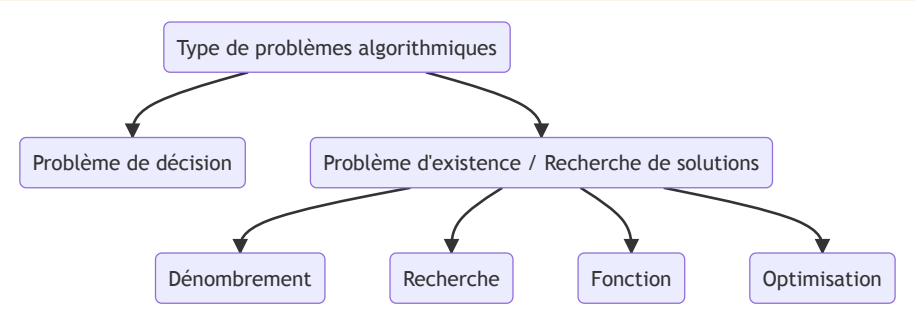
I. Introduction - Cadre pour l'algorithmique



Formulation d'un problème en algorithmique :

— Soit P un problème quelconque
— Soit I une instance de P
— Soit A un algorithme résolvant le problème P

Quelles sont les familles de problèmes P ?

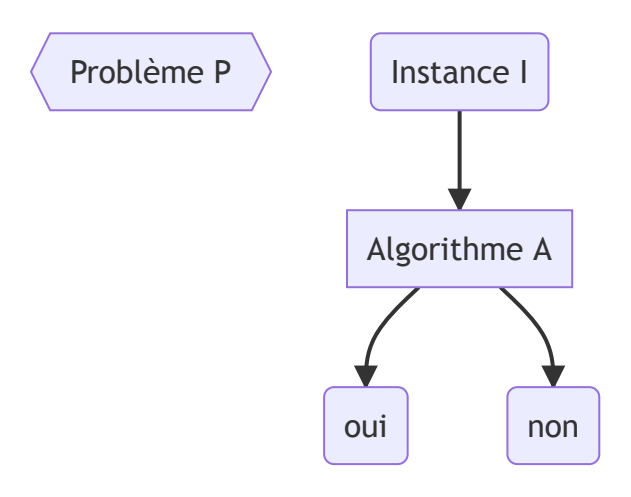


Problème de décision (ou reconnaissance)

Objectif : validation de l'existence d'une solution

A chaque instance du problème P, la réponse apportée par l'algorithme est oui ou non (résultat binaire)

Problème de classification



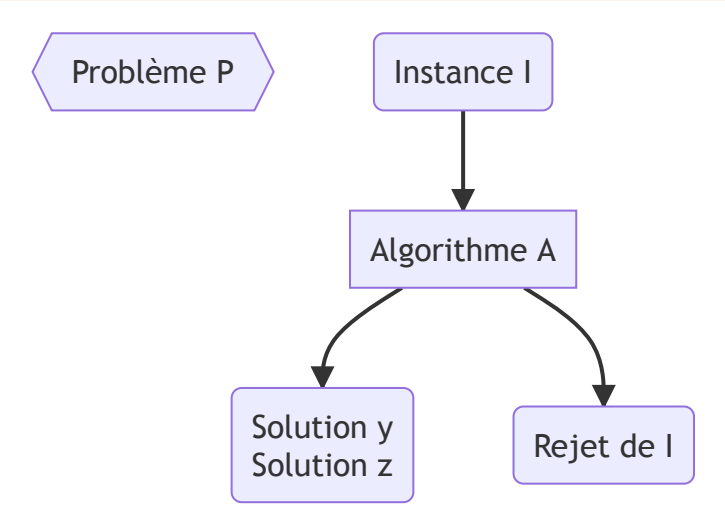
Exemple : soit n un entier naturel, déterminer si n est un nombre premier

Problème de recherche

Objectif : trouver une solution lorsqu'un algorithme n'est pas écrit mais que la spécification de la solution est connue.

Trouver, si elle existe, une solution associée à une instance d'entrée grace à une relation figurant dans l'énoncé de la recherche.

Problème de décision : restriction d'un problème de recherche



Exemple : trouver les facteurs premiers d'un entier naturel n

Problème de dénombrement

Objectif : dénombrer les solutions

Déterminer le nombre de solutions à un problème de recherche

Sous problème du problème de dénombrement et de décision :

— unicité d'une solution optimale
— énumération des solutions

Exemple : soit n un entier naturel, déterminer le nombre de facteurs premiers non triviaux de n

Problème d'optimisation

Objectif : recherche de la meilleure solution parmi toutes les solutions possibles d'un problème P sur une instance I

Détermination d'un jeu de paramètres en entrée d'une fonction donnant à cette fonction la valeur maximale ou minimale

Optimisation sous contrainte ou sans contrainte (méthode de descente, programmation linéaire, ...)

Exemple : recherche du plus grand facteur premier non trivial d'un entier naturel n

Problème de fonction

Objectif : engendrer les solution

Un seul résultat attendu pour chaque entrée

Plus complexe que le problème de décision car le résultat est une valeur plutôt qu'un résultat binaire

Exemple : problème de régression → prévision de valeur

II. Programmation dynamique : exemple

Découpe de barres d'acier

Entreprise → achat et revente de barres d'acier

Coupe de barres d'acier pour optimiser les profits

Hypothèses :

- Découpe d'une barre en barres de $i = 1,\ 2,\ \ldots$ cm
- Prix des tronçons de i cm à la revente connus :

Longueur i (cm)	1	2	3	4	5	6	7	8	9	10
Prix	1	5	8	9	10	17	17	20	24	30

Bilan des présentations :

- Pas facile de présenter un code $\Longrightarrow$ algorithme ?
- Attention à la lisibilité (couleur et taille)
- Trop de code → difficile à appréhender
- Position / pertinence des commentaires
- Pertinence des éléments sur les diapos
  - Utilité
  - Aide / illustration du discours
- Définir un plan
- Exemples
- Éviter trop de textes / phrases trop longues
- Travail en équipe → répartition des rôles
  - oral
  - élaboration du diapo
  - relecture des diapos

Présentation orale :

1. Contexte / Présentation du problème
2. Plan
3. Méthodes utilisées
   - Formulation mathématique du problème (éventuellement)
   - Choix / justification du choix d'une méthode de programmation
4. Détail / Mise en œuvre des méthodes
   - Architecture global ? (liste des fonctions, et rôles de ces fonctions)
   - Algorithmes pour les principes (à dérouler ?)

- Code pour les particularités de traduction → exploitation des langages
- Correction / terminaison des algorithmes

5. Bilan / Comparaison des performances ? → complexité

Le revenu maximum est donc $r_n = \max(p_n, p_1 + r_{n-1}, \ldots, p_{n-1} + r_1)$.

Revenu maximum : $r_n = \max_{i \in \mathbb{N}}(p_i + r_{n-i})$

La valeur de i qui maximise r_n est inconnue : il faut tester toutes les valeurs

Décomposition du problème initial en 2 sous problèmes du même type de taille plus petite, indépendants → instances plus petites du problème initial

Solution optimale global : celle qui maximise chacun des 2 sous problèmes

Autres manière d'organiser la structure :

- Structure récursive : découpe = tronçon de gauche de longueur i ne pouvant être découpé + tronçon pouvant être découpé de longueur $n - i$
- Solution sans coupe
  - Le tronçon de coupe est de taille $i = n$, de revenu p_n
  - le revenu du tronçon de droite restant de taille 0 est $r_0 = 0$

Nouvelle expression de l'optimisation de la coupe :

$$r_n = \max_{0 \leqslant i \leqslant n} (p_i + r_{n-i})$$

Implémentation utilisant la récursivité (cf. présentations) → complexité temporelle : $O(2^n)$

Optimisation de la récursivité par la programmation dynamique

Fonction récursive inefficace : plusieurs évaluations identiques → chevauchements des sous problèmes

Idée : mémoriser les résultats pour ne les évaluer qu'une seule fois

- consulter les résultats mémorisés
- Si évaluation déjà produite, la renvoyer
- Sinon, procéder à l'évaluation

Compromis temps/mémoire

- Programmation dynamique plus coûteuse en mémoire mais gain temporel
- Recherche d'une complexité polynomiale plutôt qu'exponentielle
  - Coût polynomial si chacun des sous problèmes distincts se résout en temps polynomial par rapport à la taille des données d'entrée : $O(n^\alpha)$.

Idée : mémoriser les résultats pour ne les évaluer qu'une seule fois

- approche descendante : mémoïsation

— approche ascendante

Approche descendante

— Écriture de la fonction récursive
— Modification
  — Introduction d'une structure permettant de sauvegarder les évaluations
  — structure utilisée : tableau ou table de hachage
  — Vérification si le sous problème est déjà évaluée avant les appels récursifs

Approche ascendante :

— Associée à une notion de taille dans les sous problèmes
— Tri des sous problèmes par taille
— Résolution des sous problèmes en commençant par les plus petits

```
Fonction CoupeBarreMemo(p,n):
    Entrée: p, le tableau des revenus et n taille de la barre (entier)
    Sortie: q, revenu maximum (entier)

    Début
        memo = CreerTableau(dimension: n, valeurs: -1)

        Fonction Aux(p, n, memo):
            Début
                Si memo[n] >= 0 alors
                    Retourner memo[n]
                Fin Si

                Si n = 0 alors
                    q = 0
                Sinon
                    q = -1

                    Pour i allant de 1 à n faire
                        q = max(q, p[i] + Aux(p, n-i, memo))
                    Fin Pour
                Fin Si

                memo[n] = q

                Retourner q
            Fin
        Retourner Aux(p, n, memo)
    Fin
```

Ordre des appels récursifs pour $n = 4$:

$$4 \to 3 \to 2 \to 1$$

donc programmation dynamique *descendante*

```
Fonction CoupeBarreAsc(p, n)
    Entrée: p, tableau des revenus et n, taille de la barre (entier)
    Sortie: q, revenu maximum (entier)

    Début
        asc = CreerTableau(dimension : n + 1, valeurs : -1)
        asc[1] = 0

        Pour j allant de 2 à n + 1 faire
            q = -1

            Pour i allant de 1 à j - 1 faire
                q = max(q, p[i] + asc[j-i])
            Fin Pour

            asc[j] = q
        Fin Pour

        Retourner asc[n]
    Fin
```

III. Principe de la programmation dynamique

Historique

Programmation dynamique → planification de tâches (Richard Bellman 1953)

Résolution de problèmes d'optimisation

Cadre d'utilisation

Chevauchement de sous problèmes : évaluation redondante (plusieurs appels d'une fonction avec les mêmes arguments)

Ordre total → possibilité d'ordonner les sous problèmes

La solution d'un problème se calcule à partir des solutions des sous problèmes

→ Optimisation d'une programmation récursive

Conception

Définition des sous problèmes

Identifier la relation de récurrence entre les sous problèmes

> Nécessité de comprendre les interdépendances entre les sous problèmes

En déduire un algorithme récursif avec approche ascendante et descendante

> Méthode ascendante et descendante

Résoudre le sous problème original à partir des solutions des sous problèmes

Nécessité de comprendre les interdépendances entre les sous problèmes

Arbre des appels récursifs → identification des chevauchements

Mise en place du graphe des sous problèmes :

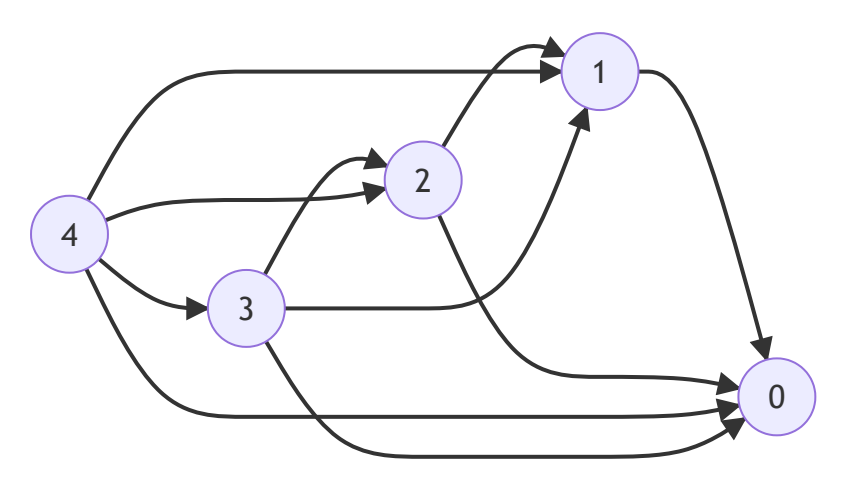
Graph orienté

— sommet pour chaque sous problème
  — arc orienté allant du sous problème x au sous problème y
  — solution optimale de x dépend de la solution optimale de y

Taille du graph donne une indication sur le temps d'exécution

Chaque sous problème n'est résolu qu'une fois → somme des temps

Exemple : découpe de barre avec $n = 4$



Méthode ascendante :

Résolution des sous problèmes les plus petits en premier

Nécessité d'un ordre total sur l'ensemble des sous problèmes → sous problème traité lorsque les sous problèmes dont il dépend ont été résolus

Méthode descendante (mémoïsation) :

Mémoïser : Conserver les résultats à la fin de l'exécution d'une fonction le résultat associé aux arguments d'appels pour éviter d'avoir à recalculer

Parcours en profondeur du graph de sous problèmes

Complexité

Temporelle → polynomiale n^{α}

Nombre de sous problèmes à évaluer

Temps nécessaire pour évaluer chaque sous problème

nombre de sous problèmes × complexité par sous problèmes (sans compter les appels récursifs)

Spatiale

Nombre de sous problèmes dont il faut garder la trace à chaque étape

Bilan

Exploration exhaustive → Force brute

Détermination de toutes les solutions

Choix d'une des solutions

Décomposition en sous problèmes

— Diviser pour régner

Décomposer en sous problèmes

Instances plus petites du problème initial

Obtention de sous problèmes triviaux

Combinaison des solutions triviales

— Gloutons

Choix d'une solution optimale à un problème élémentaire

Incorporation progressive des solutions

— Programmation dynamique

Décomposer en sous problèmes

Instances plus petites du problème initial

Chevauchement des sous problèmes

Ordre total parmi les sous problèmes

Mémorisation des résolutions

Chapitre

Méthodes de programmation : algorithmes gloutons

c.f. polycopié

II. Exemple : choix d'activités

Sous-structure optimale :

> Ajout de a_k dans $A_{ij} \rightarrow$ définition de deux sous-problèmes dans S_{ij}.
>
> On peut définir
>
> $$A_{jk} = A_{ij} \cap S_{ik}$$
> $$A_{kj} = A_{ij} \cap S_{kj}$$
>
> On a donc $A_{ij} = A_{ik} \cup \{a_k\} \cup A_{kj}$ avec A_{ik} avec $|A_{ij}| = |A_{ik}| + |A_{kj}| + 1$.

À démontrer : la solution optimale A_{ij} doit-elle nécessairement inclure les solution optimales de S_{ik} et S_{ki} ?

> Hypothèse : On peut bâtir A'_{ik}, sous ensemble d'activités mutuellement compatibles dans S_{ik} tel que $|A'_{ik}| > |A_{ik}|$.
>
> Alors, on peut trouver un sous-ensemble A'_{ij} tel que $A'_{ij} = A'_{ik} \cup \{a_k\} \cup A_{kj}$. On a alors $|A'_{ij}| = |A'_{ik}| + |A_{kj}| + 1 > |A_{ij}| = |A_{ik}| + |A_{kj}| + 1$.
>
> Ce qui contredit l'hypothèse initiale affirmant que A_{ij} est un sous-ensemble de plus grande taille d'activités mutuellement compatible de S_{ij}.

Raisonnement similaire pour A_{kj}.

Conclusion : La solution optimale de S_{ij} inclut les solutions optimales de S_{ik} et S_{kj}.

Chevauchements de sous-problèmes :

Taille d'une solution optimale pour S_{ij} contenue dans le tableau à 2 dimensions : $|A_{ij}| = c[i,\, j]$.

Soit $c[i,\, j] = c[i,\, k] + c[k,\, j] + 1$.

En pratique, on ignore si la solution optimale du sous-problème S_{ij} contient la solution a_k.

Nouvelle formulation : examen de toute les activités de S_{ij} pour déterminer k :

$$c[i,\, j] = \begin{cases} 0 & \text{si } S_{ij} = \varnothing, \\ \max\limits_{a_k \in S_{ij}} \Big\{ c[i,\, k] + c[k,\, j] + 1 \Big\} & \text{si } S_{ij} \neq \varnothing. \end{cases}$$

D'où les chevauchements de sous-problèmes (résoudre $S_{i,m+1}$ nécessite de résoudre S_{im}).

Programmation dynamique envisageable mais lourde à mettre en œuvre.

c.f. polycopié

Est-ce que le choix glouton fait toujours partie de la solution optimale ?

Théorème :

Soit un sous-problème S_k non vide. Soit a_m l'activité de S_k ayant l'heure d'achèvement la plus précoce.

Alors, a_m est incluse dans un certain sous-ensemble de taille maximale d'activités mutuellement compatibles de S_k.

Démonstration :

Soit A_k un sous-ensemble de taille maximale d'activités mutuellement compatibles de S_k. Soit a_j la première activité de A_k.

Si $a_j = a_m$, alors le théorème est démontré.

Si $a_j \neq a_m$, soit $A'_k = \big(A_k \setminus \{a_j\}\big) \cup \{a_m\}$, a_m ayant l'heure d'achèvement la plus précoce dans S_k : $f_m \leqslant f_j$. A'_k est aussi un sous-ensemble d'activités mutuellement compatibles de S_k. Par ailleurs, $|A'_k| = |A_k|$, donc A'_k est un sous-ensemble de taille maximale d'activités mutuellement compatibles de S_k, contenant a_m.

Le théorème est donc démontré.

Mise en œuvre des algorithmes :

— Récursif :

```
Fonction ChoixActivitesRecursif(d, f, k, n)
  Entrée: d, tableau des dates de début des activités;
          f, tableau des dates de fin des activités;
          k, indice de l'activité courante (entier);
          n, longeur du tableau d et f (entier).
  Sortie: A, combinaison d'activités.
  Précondition: f et d sont triés par date de fin croissantes.
  Post-condition: A est un sous-ensemble de taille maximale
                  d'activités mutuellement compatibles.
  Début
    m := k + 1

    Tant que m <= n et d[m] <= f[k] faire
      m := m + 1
    Fin Tant que

    Si m <= n alors
      Retourner Combiner({ m }, ChoixActivitesRecursif(d, f, m, n))
    Sinon
      Retourner ∅
    Fin Si
  Fin
```

Complexité en $\Theta(n)$

— Itératif :

```
Fonction ChoixActivitesIteratif(d, f, k, n)
  Entrée: d, tableau des dates de début des activités;
          f, tableau des dates de fin des activités.
  Sortie: A, combinaison d'activités.
  Précondition: f et d sont triés par date de fin croissantes.
  Post-condition: A est un sous-ensemble de taille maximale
                  d'activités mutuellement compatibles.
  Début
    n := d.longueur
    A := { 1 }
    k := 1

    Pour m allant de 2 à n faire
      Si d[m] >= f[k] alors
        A := Combiner(A, { m })
        k := m
      Fin Si
    Fin Pour

    Retourner A
  Fin
```

Complexité en $\Theta(n)$

Bilan

c.f. polycopié

1. Détermination de la sous-structure optimale :

$$A_{ij} = A_{ik} + \{a_k\} + A_{kj}$$

2. Formulation de la récurrence (mais non exploité pour un algo. récursif)

$$c[i,\, j] = \begin{cases} 0 & \text{si } S_{ij} = \varnothing, \\ \max\limits_{a_k \in S_{ij}} \left\{ c[i,\, k] + c[k,\, j] + 1 \right\} & \text{si } S_{ij} \neq \varnothing. \end{cases}$$

3. Le choix glouton conduit à un unique sous-problème :

$$A_k = \{a_k\} + \text{solution optimale au sous-problème } S_k$$

4. Le choix glouton + théorème
5. Algorithme récursif
6. Algorithme itératif

III. Codage Huffman

Objectif : Économiser l'espace mémoire ; limité aux suites de caractères pour le cours MP2I.

Compression de données : RLE

> Code RLE déjà vu au premier semestre, en devoir : codage sans perte de données mais peu efficace sur les textes

Encodages au programme (sans perte de données) :

— Lempel-Zil-Welch (LZW) → project de fin d'année
— Huffman

> → algorithme glouton
>
> → très efficace pour les textes (entre 20% et 90% d'économie)
>
> → utilisation d'une table de fréquences d'apparition pour l'encodage
>
> → encodage de chaque caractère par une chaîne binaire
>
> → utilisé pour les fichiers `zip`, pour la compression `JPEG` et `PNG`.

Exemple :

Texte de 100 000 caractères utilisant uniquement 6 caractères distincts : ‘a’, ‘b’, ‘c’, ‘d’, ‘e’, et ‘f’.

Fréquence d’apparition des différents caractères connus

Encodage de longueur fixe *v.s.* encodage de longueur variable.

Caractère	a	b	c	d	e	f
Fréquence ($\times 10^3$)	45	13	12	16	9	5
Encodage (longueur fixe)	000	001	010	011	100	101
Encodage (longueur variable)	0	101	100	111	1101	1100

Tailles des fichiers ?

— Encodage de longueur fixe : 300 000 bits
— Encodage de longueur variable : 224 000 bits

On a donc 25% d’économie avec l’encodage de longueur variable.

Exemple : `0 111 101 101` → `a d b b`

Pourquoi n’y a-t-il pas d’ambigüité pour le décodage ?

Codage préfixe : aucun mot code n’est le préfixe d’un autre mot code.

Un codage préfixe peut toujours donner la compression maximale entre tous les codages de caractère.

Utilisation d’un arbre binaire :

Feuilles → caractères et fréquences d’apparition des caractères

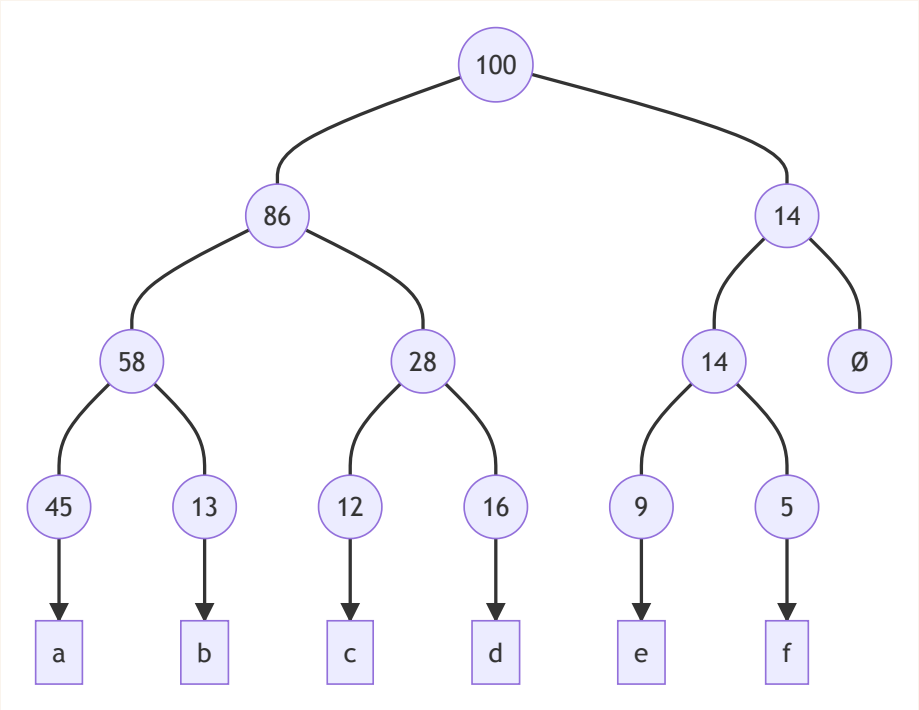
Étiquettes des nœuds internes et racines → fréquences d’apparition

Vers le fils gauche → 0

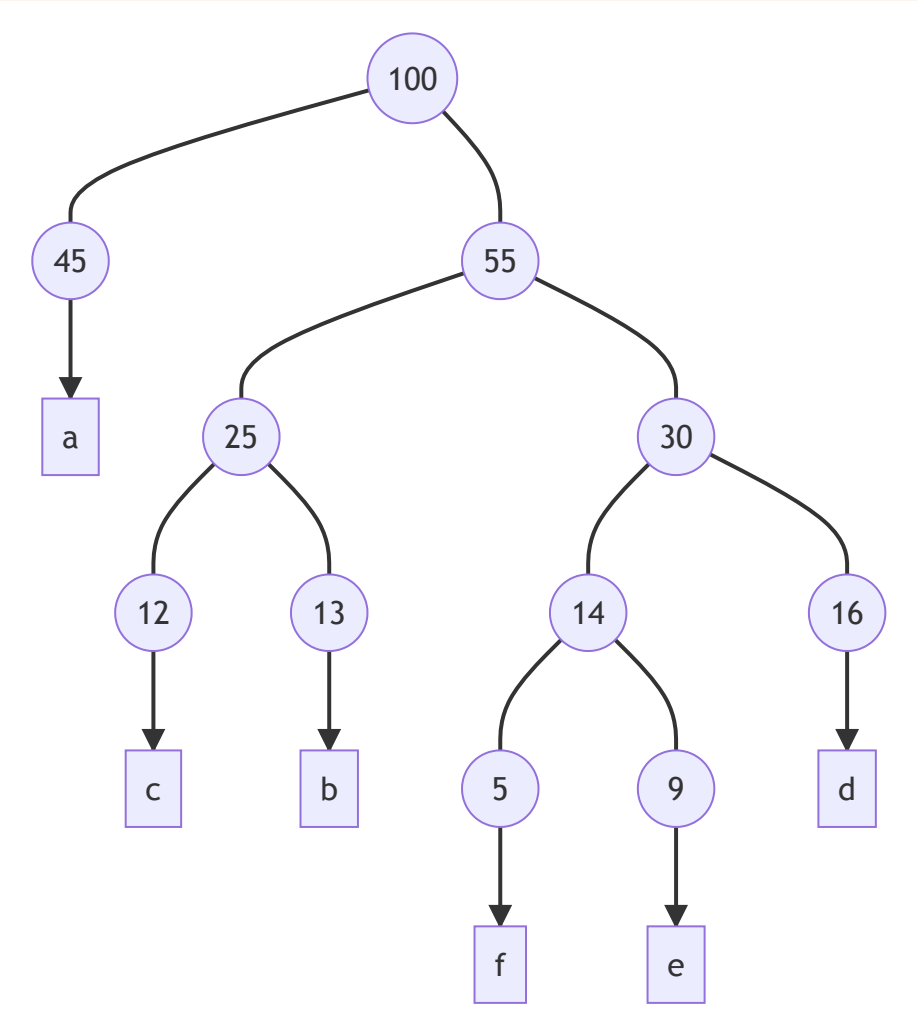
Vers le fils droit → 1

Codage optimal → arbre binaire dont les nœuds sont d’arité 2.

Encodage de longueur fixe :



Encodage de longueur variable :



Construction du codage de Huffman

Coût de l'arbre : $\sum_{i=1}^{n} f_i \times p_i$ où p_i est la profondeur du caractère i, f_i la fréquence du caractère i.

Utilisation d'une file de priorité min F contenant les arbres $\rightarrow$ forêt

Pour chaque arbre de la forêt :

Chaque nœud interne contient une fréquence

Chaque feuille contient un caractère et sa fréquence d'apparition

La forêt est ordonnée par ordre de fréquences croissantes.

État initial de la forêt F_0 :

Chaque arbre ne contient qu'un seul nœud : un caractère et sa fréquence.

Donc, Card$(F_0) = n =$ nombre de caractères différents dans le texte à encoder.

Construction de l'arbre :

— Extraire le minimum de la file
— Extraire le minimum de la file
— Fusionner les deux arbres extraits dans un nouvel arbre

→ structure de file min

— Insérer le nouvel arbre dans la file
— Rétablir la structure du file min

```
Fonction construitHuffman(F)
    Entrée : F, file de priorité min, forêt d'arbres (files min)
    Sortie : F, contenant un seul élément, l'abre d'encodage Huffman
    Pré-condition : F contient les caractères et leurs fréquences (ordre croissant)
    Post-condition : F, contenant un seul élément, l'abre d'encodage Huffman

    Début
        Si #F = 1 alors
            Returner F
        Sinon
            A1 = F.définer // Extraire_min(F)
            A2 = F.définer // Extraire_min(F)
            A = A1 + A2 // construction de l'arbre tournoi
            freq[A] = freq[A1] + freq[A2] // Calcul de la fréquence de A
            Insérer(A, F) // Insertion à la bonne place de A dans F
            Retourner construitHuffman(F) // Appel récursif
        Fin Si
    Fin
```

Démonstration du lemme 1

a et b deux feuilles sœurs de profondeur maximale pour l'arbre T.

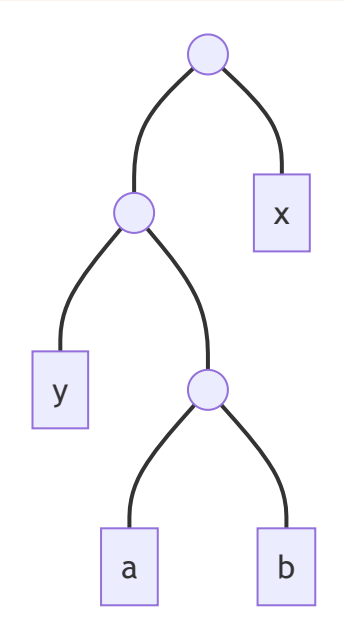
$$a.\text{freq} \leqslant b.\text{freq} \quad \text{et} \quad x.\text{freq} \leqslant y.\text{freq}$$

Comme x et y sont de fréquences les plus basses :

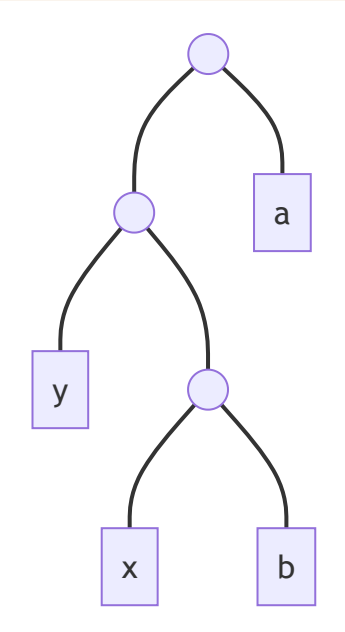
$$x.\text{freq} \leqslant a.\text{freq} \quad \text{et} \quad y.\text{freq} \leqslant b.\text{freq}$$

Si x.freq alors $x.\text{freq} = a.\text{freq} = y.\text{freq} = b.\text{freq}$ donc le lemme est démontré.

Si $x.\text{freq} \neq b.\text{freq}$, on a :



En permutant les feuilles a et x, on obtient T' :



On cherche le signe de $c(T) - c(T')$.

$$\begin{aligned} c(T) - c(T') &= x.\text{freq} \times p_x + a.\text{freq} \times p_a - x.\text{freq} \times p'_x - a.\text{freq} + p'_a \\ &= x.\text{freq} \times p_x + a.\text{freq} \times p_a - x.\text{freq} \times p_a - a.\text{freq} \times p_x \\ &= \underbrace{(a.\text{freq} - x.\text{freq})}_{\geqslant 0} \times \underbrace{(p_a - p_x)}_{\geqslant 0} \end{aligned}$$

$$\begin{aligned} c(T') - c(T'') &= y.\text{freq} \times p'_y + b.\text{freq} \times p'_b - y.\text{freq} \times p''_y - b.\text{freq} + p''_y \\ &= x.\text{freq} \times p'_y + b.\text{freq} \times p'_b - y.\text{freq} \times p'_b - b.\text{freq} \times p'_b \\ &= \underbrace{(b.\text{freq} - y.\text{freq})}_{\geqslant 0} \times \underbrace{(p'_b - p'_y)}_{\geqslant 0} \end{aligned}$$

Démonstration du lemme 2

Pour chaque caractère $c \in A \setminus \{x, y\}$ on a :

$$c.\text{freq} \times p_c = c.\text{freq} \times p'_c$$

car T est bâti à partir de T'.

Pour les caractères x, y et z :

z est le parent de x et de y donc $p_x = p_y = p'_z + 1$.

D'où

$$\begin{aligned} x.\text{freq} \times p_x + y.\text{freq} \times p_y &= (x.\text{freq} + y.\text{freq}) \times (p'_z + 1) \\ &= z.\text{freq} \times p'_z + (x.\text{freq} + y.\text{freq}) \end{aligned}$$

D'où

$$C(T) = C(T') \times (x.\text{freq} + y.\text{freq})$$
$$C(T') = C(T) - x.\text{freq} - y.\text{freq}$$

Raisonnement par l'absurde : T ne représente pas un codage préfixe optimal de A de coût minimal. Il existe T'' tel que $C(T'') < C(T)$

Dans T'', x et y sont frères

Soit T'', l'arbre T'' pour lequel le parent commun à x et y a été remplacé par z, de fréquence $z.\text{freq} = x.\text{freq} + y.\text{freq}$.

Donc $C(T'') - x.\text{freq} - y.\text{freq} < C(T) - x.\text{freq} - y.\text{freq}$.

Soit $C(T''') < C(T')$, ce qui contredit l'hypothèse affirmant que T' représente un codage préfixe optimal de coût minimal pour A'.

Donc T représente bien un codage préfixe optimal de coût minimal pour A.

Chapitre

Projets

→ 5 sujets

- Backtracking
  - 8 reines
  - Sudoku
- Recherche de motifs
  - Boyer-Moore
  - Rabin-Karp
- Compression LZW

Triés par ordre croissant en difficulté.

Normalement, 2 groupes par sujet

On y consacre les TPs, TDs, Khôlles (et éventuellement un cours).

Soutenances : 14 juin $10^h \rightarrow 12^h$ et $15^h \rightarrow 17^h$ (sur les heures de TIPE)

À rendre : présentation (au format PDF) et codes (C et/ou oCamL) ; au plus tard pour le 20 Juin.

Contenu de la présentation :

- Description des méthodes
- Exemple
- Implementations (et les choix qui ont été fait)
- Analyse de algorithme
- Résultats
- Conclusion et perspectives

L'oral durera au maximum 20-25 min (on aura la durée exacte plus tard).

I. n reines – backtracking

Groupe A. Iba, Antoine R., Bastien D., Arthur

Problème : placer le nombre maximal de reines sur un échiquier de $n \times n$.

Rappel : la reine attaque la ligne, la colonne et les deux diagonales.

Backtracking : expiration exhaustive ; on part de la racine, et on descend dans l'arbre. Si on ne trouve pas de solution, on remonte.

Algorithme : On procède ligne par ligne. Une structure est créée contenant la position des reines déjà posées et le nombre de reines à poser. On tente de poser un maximum de reines. Quand on ne peut plus poser de reines, on remonte dans l'arbre des possibilités et on essaie une nouvelle position pour la reine. La solution partielle est une liste $(r_1, \ldots, r_n)$ où r_i est la position de la i-ème reine.

Complexité : l'algorithme a une complexité en $\mathcal{O}(n!)$.

Exemples :

N	# Solutions
3	0
4	2
5	10
6	4
7	40
8	92
9	352
10	724

Groupe B. Narada, Nicolas, Charlotte, Alan

Même sujet que le groupe précédent.

Conjecture : On peut placer une reine sur chaque ligne.

On n'essaie pas toutes les configurations car certaines sont impossibles ; on fixe les contraintes.

Différence avec le groupe A. : la structure contient tous les tableaux solutions. Le problème est que la complexité en mémoire est très importante et à partir de $n = 11$, il est impossible que le programme se termine sur `repl.it`.

Complexité temporelle : $\mathcal{O}(n!)$.

Complexité mémorielle : $\mathcal{O}$(beaucoup).

II. Boyer-Moore – Recherche d'un motif

Groupe A. Ruben, Noémie, Alex, Juliette, Antoine V.

Algorithme de recherche de motif dans un texte → un des algorithme les plus populaire et efficace pour la recherche de motif.

Approche naïve : on tente de placer le motif sur chaque lettre $\implies$ complexité importante

On commence par la fin du motif et s'il n'y a pas une lettre du motif, on fait un "saut" de la taille du motif moins la position dans la table de saut du caractère qui a bloqué le motif.

Il est possible que l'on rate la solution si l'on ne fait pas attention (exemple : rechercher "AAA" dans "BBAAAZZ").

Implémentation en OCaml plus adaptée que celle en C car utilisation de listes.

Groupe B. Khadim, Iwan, Émile, Tibério

Complexité de la méthode exhaustive : $\mathcal{O}(\ell \times k)$ où ℓ est la longueur de la chaîne, k est celle du motif.

Méthode avec décalage (Boyer-Moore) : meilleur des cas $\mathcal{O}\left(\frac{\ell}{k}\right)$ (approximatif).

Méthode optimisée : utilisation de liste chaînées et de plusieurs "curseurs" pour analyser le texte.

$\longrightarrow$ Pas de problème pour la recherche de "AAA" dans "BBAAAZZ"

Boyer-Moore II (hors programme) : utilisation de deux tables de saut ; si on trouve une lettre mais pas la suivante, on regarde dans le motif si l'on ne peut pas avoir trouvé une autre partie du motif et on fait le "saut" nécessaire.

III. Résolution de Sudoku – Backtracking

Groupe A. Bastien F., Thomas, Timothée S., Hugo

Bah, non. $\Longrightarrow$ Complexité en $\mathcal{O}$(beaucoup).

Groupe B. Aubin, Samy, Kyriann

On choisit *arbitrairement* une solution.

Attention, ici n est la taille de la grille entière.

Utilisation du backtracking mais avec des contraintes au lieu de possibilités.

Choix à faire à chaque cases réduisant les possibilités des autres, si aucune possibilité pour une case, on change la case précédente.

Utilisation du récursif d'où l'utilisation du OCaml. Deux structures utilisées : `case_contrainte` et `case_grille`.

Utilisation d'une seule boucle pour faire à la fois la vérification ligne et colonne $\Longrightarrow$ $\mathcal{O}(n)$ où n est la taille *totale* de la grille.

Construction de la file de priorité en $\mathcal{O}(n^3)$.

Résolution du Sudoku en $\mathcal{O}\left(n^{n^2}\right)$.

Mettre à jour la liste des cases à traiter permettrais de remplir la 20 % de la grille.

IV. Compression Lempel-Ziv-Welch

Groupe A. Dorian, Lucine, Benoît, Kilian, Nathan R.

Des variantes de l'algorithme sont utilisées pour le format `GIF` et `TIFF`.

Utilisation des redondances dans le texte pour diminuer la taille → dictionnaire.

Au lieu d'utiliser 8 bits pour stocker un caractère, diminuer cette taille en fonction de la fréquence dans le texte.

Présence d'un caractère pour indiquer la fin du texte (`EOF`) → `\Z`.

Formation de séquences à partir des séquences déjà créées : "TON" utilise la séquence "TO".

Peut aller de 10 % à 50 % de compression. Pour 10 000 caractères de Harry Potter, on a 40 % de compression.

Spécificité du C : "méthode `append`"

avec des tableaux → trop coûteux

avec les liste chaînées

D'où l'utilisation de deux liste chaînées : pour le code et pour le dictionnaire.

Puis, transformation de la liste chaînée à un tableau pour la fin de la fonction principale.

Différence : ajout d'un champ `queue` à la liste chainée pour avoir une complexité d'ajout d'un élément en $\mathcal{O}(1)$.

(ajout de Khadim : on peut utiliser une fonction Hors-programme qui permettrai l'utilisation des tableaux au lieu des listes chaînées).

Utilisation du code `ASCII` pour représenter la séquence.

Autre possibilité : utilisation d'une fonction récursive ? $\implies$ OCaml

Pour le code en OCaml, utilisation d'un tableau pour représenter le dictionnaire.

Améliorations : deuxième passage pour détecter des motifs de motifs ($\rightsquigarrow$ mots communs) uniquement possible car on stocke le dictionnaire pour la décompression. Possibilité d'un troisième passage, etc...

Décompression en $\mathcal{O}(n)$.

Groupe B. Timothée N-L., Nathan S., Lilian, Loïc

Utilisation également dans le format `ZIP`.

Surtout efficace sur des textes longs car répétition de motifs.

Utilisation d'indices supérieurs à 255 $\implies$ plusieurs octets (contrairement au code `ASCII`).

Utilisation de tableaux pour représenter le dictionnaire (contrairement au groupe précédent).

$\rightsquigarrow$ retrouver le dictionnaire à partir du texte décodé.

Complexités : - compression en $\mathcal{O}(n \times p)$ où la taille du code est q et celle du dictionnaire est n ; - décompression en $\mathcal{O}(n^2 \times p)$.

Économie en mémoire allant jusqu'à 50 %. Bien plus efficace sur les textes longs ou sur les images.

Sans avoir accès au dictionnaire, on ne peut pas compresser deux fois (ou plus).

II. Rabin-Karp – Recherche d'un motif

Groupe A. Nathan F., Ywan, Damien, Corentin, Germain

Recherche de motifs : simple ($\rightarrow$ Boyer-Moore) et multiple ($\rightarrow$ Rabin-Karp)

Force brute : comparer les caractères uns à uns $\Longrightarrow$ complexité très importante. Complexité en $\mathcal{O}(n\,m)$ où n est la taille du texte et m est celle du motif.

Utilisation d'une structure `tableau` et de `realloc` (H.P.) pour diminuer l'empreinte mémoire.

Principe de l'algorithme de Rabin-Karp : Utilisation d'une fonction de *hashage* ($\rightarrow$ prétraitement ; par exemple calcul décimal de Hörner). Attention aux potentiels faux positifs dûs à l'utilisation du modulo (notamment).

Équilibre à trouver pour la taille du *modulo* entre espace mémoire et taux de faux positifs.

Prétraitement (réalisé, dans ce cas, avec la méthode de calcul décimal de Hörner) : Calcul du hash initial en $\mathcal{O}(n)$ où n est la taille du motif puis utilisation de la relation de récurrence pour un calcul en $\mathcal{O}(\ln n)$. Au final, le prétraitement est en $\mathcal{O}(n \ln n)$.

Traitement : calcul du hash, comparaison entre le hash du texte et celui du motif. Complexité entre $\mathcal{O}(n)$ et $\mathcal{O}(n\,m)$ en fonction du nombre de "faux positifs".

Complexité globale entre $\mathcal{O}(n \ln n)$ et $\mathcal{O}(n\,m)$.

Extensions :

- Filtre de Bloom : tableau de plusieurs fonctions de hashage. Représenté en C avec deux structures : `hashFunctions` et `bloomFilter`. Permet de réduire le nombre de "faux positifs" mais ils restent possible.
- Tableau à deux dimensions : utilisable dans une image (recherche multiple de Smiley dans une image).

Améliorations possibles : utiliser une meilleur fonction de hashage, utiliser un meilleur "modulo".

Exemple : utiliser Boyer-Moore pour trouver des patterns dans l'ADN est peu efficace car l'alphabet est petit (4 caractères) et donc les sauts ne sont pas de longueur importantes. L'utilisation, dans cet exemple, de Rabin-Karp est donc beaucoup plus efficace.

Attention : la complexité des fonctions dans C n'est pas forcément en $\mathcal{O}(1)$; par exemple, l'utilisation d'un `malloc` pour un grand espace peut prendre bien plus longtemps qu'un simple `malloc` pour peu de mémoire.

Groupe B. Martin, Louis, Ilan, Valentin

Différences avec le groupe précédent :

— Prétraitement en $\mathcal{O}(n)$.
— Recherche en $\mathcal{O}(n\,m - m^2)$.

Implémentation en C car pas de récurrence, uniquement de l'itératif et utilisation de tableaux.

Importance de la fonction de hashage $\rightarrow$ équilibre.

Pour des textes courts, l'algorithme de Rabin-Karp n'avantage pas plus que la force brute.

Utilisation d'autres bases que la base *10* : pour le code `ASCII`, on utilise la base *256*.

Attention à la lisibilité des diapositives.

Partie II

MP2I – Mathématiques – Cours

Chapitre 0

Logique (rudiments)

Définition : Un proposition est un énoncé qui est soit vrai, soit faux.

Exemple :

$$\left.\begin{array}{l} A : \text{“}B \text{ est vraie ”} \\ B : \text{“}A \text{ est fausse ”} \end{array}\right\} \text{Le système } \{A, B\} \text{ est une auto-contradiction}$$

Définition : Démontrer une proposition revient à prouver qu'elle est vraie.

1 Algèbre de Boole

Définition : Soient A et B deux propositions. La proposition A et B est définie par la table de vérité suivante :

A	B	A et B
V	V	V
V	F	F
F	V	F
F	F	F

Définition : Soient A et B deux propositions. La proposition A ou B est définie par la table de vérité suivante :

A	B	A ou B
V	V	V
V	F	V
F	V	V
F	F	F

Définition : Soit A une proposition. La négation de A, notée non(A) est définie par :

A	non(A)
V	F
F	V

Définition : Deux propositions A et B sont équivalentes si elles ont la même table de vérité. Dans ce cas, on note $A \iff B$.

Proposition : Soient A, B et C trois propositions.

1. $(A \text{ et } B) \text{ et } C \iff A \text{ et } (B \text{ et } C)$
2. $A \text{ et } A \iff A$
3. $A \text{ et } B \iff B \text{ et } A$
4. $(A \text{ ou } B) \text{ ou } C \iff A \text{ ou } (B \text{ ou } C)$
5. $A \text{ ou } A \iff A$
6. $A \text{ ou } B \iff B \text{ ou } A$
7. $\text{non } (\text{ non } (A)) \iff A$
8. $A \text{ et } (B \text{ ou } C) \iff A \text{ et } B \text{ ou } A \text{ et } C$
9. $A \text{ ou } (B \text{ et } C) \iff (A \text{ ou } B) \text{ et } (A \text{ et } C)$
10. $\text{non } (A \text{ et } B) \iff \text{non } (A) \text{ ou non } (B)$
11. $\text{non } (A \text{ ou } B) \iff \text{non } (A) \text{ et non } (B)$

Preuve :
8.

A	B	C	B ou C	A et (B ou C)	A et B	A et C	(A et B) ou (A et C)
V	V	V	V	V	V	V	V
V	V	F	V	V	F	F	V
V	F	V	V	V	F	V	V
V	F	F	F	F	F	F	F
F	V	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F

10.

A	B	A et B	non (A et B)	non (A)	non (B)	non (A) ou non (B)
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

□

Définition : Soient A et B deux propositions. La proposition $A \implies B$ (A implique B) est définie par :

A	B	$A \implies B$
V	V	V
V	F	F
F	V	V
F	F	V

Définition : Soient A et B deux propositions telles que $A \implies B$ est vraie. On dit que A est une condition suffisante pour que B soit vraie. On dit que B est une condition nécessaire pour que A soit vraie.

Proposition (Contraposée) **:** Soient A et B deux propositions.

$$(A \implies B) \iff (\text{ non } B \implies \text{ non } A)$$

Preuve :

A	B	non A	non B	non $B \implies$ non A	$A \implies B$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

□

Proposition : Soient A et B deux propositions.

$$(A \implies B) \iff \big((A \implies B) \text{ et } (B \implies A)\big)$$

Preuve :

A	B	$A \iff B$	$A \implies B$	$B \implies A$	$(A \implies B)$ et $(B \implies A)$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

□

Proposition : Soient A et B deux propositions.

$$(A \implies B) \iff (B \text{ ou } \text{non } (A))$$

Preuve :
On obtient par contraposée

$$\text{non } (A \implies B) \iff (A \text{ et } \text{non } (B))$$

donc

$$\begin{aligned}(A \implies B) &\iff \text{non } (A \text{ et } \text{non } (B)) \\ &\iff \text{non } (A) \text{ ou } \text{non } (\text{ non } (B)) \\ &\iff \text{non } (A) \text{ ou } B \\ &\iff B \text{ ou } \text{non } (A)\end{aligned}$$

□

2 Déduction naturelle

Dans ce paragraphe, A et B sont deux propositions.

Comment démontrer A et B ? $\boxed{A \text{ et } B}$

— On démontre A
— On démontre B

Comment utiliser l'hypothèse A et B ?
On utilise A ou on utilise B.

u B

Comment démontrer A ou B ?
On essaie de démontrer A. Si on y arrive, alors on a prouvé A ou B sinon on démontre B.

Variante
On suppose A faux. On démontre B.

Comment utiliser l'hypothèse A ou B ?
On fait une disjonction des cas :

— Cas 1 : On suppose A

— Cas 2 : On suppose B

$\Longrightarrow B$

Comment démontrer $A \Longrightarrow B$?
On suppose A. On démontre B.

Comment utiliser l'hypothèse $A \Longrightarrow B$?
On démontre A. On utilise B.

3 Raisonement par l'absurde

Situation :

Soient A et B deux propositions.
On veut montrer $A \Longrightarrow B$.
On suppose A. On suppose aussi B faux.
On cherche à faire apparaître une contradiction ($\lightning$)

4 Prédicat

Définition : Un prédicat $P(x)$ est un énoncé dont la valeur de vérité dépend de l'objet x, élément d'un ensemble E.
Le domaine de validité de P est l'ensemble des valeurs x de E pour lequelles $P(x)$ est vraie :

$$\{x \in E \mid P(x)\}$$

Remarque (Notation) :
On écrit

$$\forall x \in E, P(x)$$

pour dire que $P(x)$ est vraie pour tous les x de E.

On écrit

$$\exists x \in E, P(x)$$

pour dire qu'il existe (au moints) un élément $x \in E$ pour lequels $P(x)$ est vraie.

On écrit

$$\exists! x \in E, P(x)$$

pour dire qu'il existe un unique élément $x \in E$ tel que $P(x)$ est vraie.

$\boxed{\forall x \in E, P(x)}$

Comment démontrer $\forall x \in E, P(x)$?
Soit $x \in E$ (fixé quelconque). Montrons $P(x)$.

Comment utiliser $\forall x \in E, P(x)$?
On choisit (spécialise) une ou plusieurs (voir toutes) valeurs de x et on exploite $P(x)$.

Exemple :
Soient $a, b, c \in \mathbb{R}$. On suppose que

$$\forall n \in \mathbb{N}, a + b \times 2^n + c \times 3^n$$

Montrons que $a = b = c = 0$.

On sait que $(S) : \begin{cases} a+b+c=0 & (n=0) \\ a+2b+3c=0 & (n=1) \\ a+4b+9c=0 & (n=2) \end{cases}$

$$(S) \iff \begin{cases} a+b+c=0 \\ b+2c=0 \\ 3b+8c=0 \end{cases} \iff \begin{cases} a+b+c=0 \\ b+2c=0 \\ 2c=0 \end{cases} \iff \begin{cases} c=0 \\ b=0 \\ a=0 \end{cases}$$

Chapitre 1

Calculs algébriques

1 Sommes

Remarque (Notation) :
Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres complexes. Pour $p \leqslant q \in \mathbb{N}$, on note

$$\sum_{k=p}^{q} u_k$$

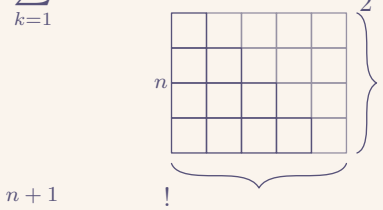
le nombre $u_p + u_{p+1} + \cdots + u_q$.

Par convention,

$$\sum_{k=p}^{q} u_k = 0 \qquad \text{si } q < p.$$

Exemple :

$$\forall n \in \mathbb{N}^\star, \sum_{k=1}^{n} k = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$



Proposition : Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres complexes.

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} u_k = \sum_{k=0}^{n} u_{n-k}$$

Preuve :
Soit $n \in \mathbb{N}$.

$$\begin{aligned}\sum_{k=0}^{n} u_{n-k} &= u_n + u_{n-1} + u_{n-2} + \cdots + u_0 \\ &= u_0 + u_1 + u_2 + \cdots + u_n \\ &= \sum_{k=0}^{n} u_k\end{aligned}$$

□

Proposition : Soient $(u_n)_{n\in\mathbb{N}}$ une suite de nombres complexes, $(p, q, r, s) \in \mathbb{N}^4$ et $\varphi : [\![p, q]\!] \to [\![r, s]\!]$ une bijection (i.e. $\forall y \in [\![r, s]\!], \exists! x \in [\![p, q]\!], \varphi(x) = y$).

Alors,

$$\sum_{k=r}^{s} u_k = \sum_{k=p}^{q} u_{\varphi(k)}.$$

Preuve :

$$\sum_{k=p}^{q} u_{\varphi(k)} = u_{\varphi(p)} + u_{\varphi(p+1)} + \cdots + u_{\varphi(q)}$$

$$\sum_{k=r}^{s} u_k = u_r + u_{r+1} + \cdots + u_s$$

Comme φ est bijective, chaque terme u_k avec $k \in [\![r, s]\!]$ apparaît une fois et une seule fois dans la somme

$$u_{\varphi(p)} + u_{\varphi(p+1)} + \cdots + u_{\varphi(q)}.$$

Ainsi, les deux sommes sont identiques. □

Exemple :
On pose

$$\forall k \in \mathbb{N}, u_k = \frac{1}{k-4}.$$

On pose également $\varphi : [\![1, 5]\!] \to [\![-1, 3]\!]$: une bijection.

Alors,

$$\sum_{k=-1}^{3} \frac{1}{k-4} = -\frac{1}{5} - \frac{1}{4} - \frac{1}{3} - \frac{1}{2} - 1$$

et

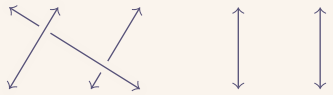
$$\begin{aligned}\sum_{k=1}^{5} u_{\varphi(k)} &= \frac{1}{\varphi(1)-4} + \frac{1}{\varphi(2)-4} + \frac{1}{\varphi(3)-4} + \frac{1}{\varphi(4)-4} + \frac{1}{\varphi(5)-4} \\ &= -\frac{1}{5} - \frac{1}{3} - \frac{1}{3} - \frac{1}{2} - 1.\end{aligned}$$

Exemple :
Soit φ la bijection définie par

$$\varphi : [\![1,5]\!] \longrightarrow [\![1,5]\!]$$
$$k \longmapsto \begin{cases} 2 & \text{si } k = 1 \\ 3 & \text{si } k = 2 \\ 1 & \text{si } k = 3 \\ 4 & \text{si } k = 4 \\ 5 & \text{si } k = 5 \end{cases}$$

$$\sum_{k=1}^{5} u_k = u_1 + u_2 + u_3 + u_4 + u_5$$

$$\sum_{k=1}^{5} u_{\varphi(k)} = u_2 + u_3 + u_1 + u_4 + u_5 !$$



Proposition (téléscopage) **:** Soit $(u_k)_{k\in\mathbb{N}}$ une suite de nombres complexes.

$$\forall p \leqslant q \in \mathbb{N}, \sum_{k=p}^{q} (u_{k+1} - u_k) = u_{q+1} - u_p.$$

Méthode 1 Soient $p \leqslant q$.

$$\begin{aligned}\sum_{k=p}^{q} (u_{k+1} - u_k) &= \cancel{u_{p+1}} - u_p + \cancel{u_{p+2}} - \cancel{u_{p+1}} \cdots + u_{q+1} - \cancel{u_q} \\ &= u_{q+1} - u_p\end{aligned}$$

MÉTHODE 2 Soient $p \leqslant q$.

$$\sum_{k=p}^{q}(u_{k+1}-u_k)=\sum_{k=p}^{q}u_{k+1}-\sum_{k=p}^{q}u_k$$

Soit $\varphi : \begin{array}{ccc} [\![p,q]\!] & \longrightarrow & [\![p+1,q+1]\!] \\ k & \longmapsto & k+1 \end{array}$. φ est bijective donc

$$\sum_{k=p}^{q}u_{k+1}=\sum_{k=p}^{q}u_{\varphi(k)}=\sum_{k=p+1}^{q+1}u_k.$$

D'où,

$$\begin{aligned}\sum_{k=p}^{q}(u_{k+1}-u_k) &= \sum_{k=p+1}^{q+1}u_k-\sum_{k=p}^{q}u_k \\ &= \left(u_{q+1}+\sum_{k=p+1}^{q}u_k\right)-\left(u_p+\sum_{k=p+1}^{q}u_k\right) \\ &= u_{q+1}-u_p\end{aligned}$$

□

REMARQUE (Analogie avec le calcul intégral) :

$$\int_a^b f'(x)\,\mathrm{d}x=f(b)-f(a).$$

EXEMPLE :
Calculer $\displaystyle\sum_{k=1}^{n}\frac{1}{k(k+1)}$ pour $n\in\mathbb{N}^\star$.

Soit $n\in\mathbb{N}^\star$.

$$\begin{aligned}\forall k\in[\![1,n]\!],\ \frac{1}{k(k+1)} &= \frac{(1+k)-k}{k(k+1)} \\ &= \frac{k+1}{k(k+1)}-\frac{k}{k(k+1)} \\ &= \frac{1}{k}-\frac{1}{k+1}\end{aligned}$$

et, par téléscopage, on obtient donc

$$\begin{aligned}\sum_{k=1}^{n}\frac{1}{k(k+1)} &= \sum_{k=1}^{n}\left(\frac{1}{k}-\frac{1}{k+1}\right)\\ &= \frac{1}{1}-\frac{1}{n+1}\\ &= 1-\frac{1}{n+1}.\end{aligned}$$

Par contre, on n'a pas de formule simple pour $\sum_{k=1}^{n}\frac{1}{k^2}$ (mais on sait que $\sum_{k=1}^{n}\xrightarrow[n\to+\infty]{}\frac{\pi^2}{6}$).

Exemple (à connaître) :

Calculer $\sum_{k=1}^{n}k^2$ et $\sum_{k=1}^{n}k^3$ pour $n\in\mathbb{N}^\star$.

On cherche $(u_n)_{n\in\mathbb{N}}$ telle que

$$\forall k\in\mathbb{N}^\star, u_{k+1}-u_k=k^2.$$

On cherche donc (u_k) sous la forme

$$\forall k\in N^\star, u_k=ak^3+bk^2+ck+d$$

avec $(a,b,c,d)\in\mathbb{R}^4$.

Soit $k\in\mathbb{N}^\star$.

$$\begin{aligned}u_{k+1}-u_k &= a(k+1)^3+b(k+1)^2+c(k+1)+\cancel{d}-ak^3-bk^2+ck+\cancel{d}\\ &= a(\cancel{k^3}+3k^2+3k+1)+b(\cancel{k^2}+2k+1)+c(\cancel{k}+1)-\cancel{ak^3}-\cancel{bk^2}-\cancel{ck}\\ &= k^2\times a+k(3a+2b)+(a+b+c)\end{aligned}$$

On résout le système

$$(S):\quad\begin{cases}3a=1,\\ 3a+2b=0,\\ a+b+c.\end{cases}\quad\Longleftrightarrow\quad\begin{cases}a=\frac{1}{3},\\ b=-\frac{1}{2},\\ c=\frac{1}{2}-\frac{1}{3}=\frac{1}{6}.\end{cases}$$

On vient de montrer que,

$$\forall k\in N^\star, k^2=u_{k+1}-u_k\qquad\text{avec } u_k=\frac{1}{3}k^3-\frac{1}{2}k^2+\frac{1}{6}k.$$

Donc, par téléscopage,

$$\begin{aligned}\forall n \in \mathbb{N}^\star, \sum_{k=1}^{n} k^2 &= u_{n+1} - u_1 \\ &= \frac{1}{3}(n+1)^3 - \frac{1}{2}(n+1)^2 + \frac{1}{6}(n+1) - \cancel{\frac{1}{3}} + \cancel{\frac{1}{2}} - \cancel{\frac{1}{6}} \\ &= \frac{n+1}{6}\big(2(n+1)^2 - 3(n+1) + 1\big) \\ &= \frac{n+1}{6}(2n^2 + 4n + 2 - 3n - 3 + 1) \\ &= \frac{n(n-1)(2n+1)}{6}\end{aligned}$$

Proposition : Soit $n \in \mathbb{N}$ et $q \in \mathbb{C}$,

$$\sum_{k=0}^{q} q^k = \begin{cases} n+1 & \text{si } q = 1 \\ \dfrac{1-q^{n+1}}{1-q} & \text{sinon.} \end{cases}$$

Preuve :
Soit $n \in \mathbb{N}$.

1.

$$\begin{aligned}(1-q)\sum_{k=0}^{n} q^k &= \sum_{k=0}^{n} q^k - q\sum_{k=0}^{n} q^k \\ &= \sum_{k=0}^{n} q^k - \sum_{k=0}^{n} q^{k+1} \\ &= \sum_{k=0}^{n} (q^k - q^{k+1}) \\ &= 1 - q^{n+1}\end{aligned}$$

Si $q \neq 1$,

$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}.$$

Si $q = 1$,

$$\sum_{k=0}^{n} q^k = \sum_{k=0}^{n} 1 = n+1.$$

2. On pose, pour $n \in \mathbb{N}$, $S_n = \sum_{k=0}^{n} q^k$.

   On a, d'une part :

$$\forall n \in \mathbb{N}, S_{n+1} = \sum_{k=0}^{n+1} q^k = S_n + q^{n+1}$$

   et d'autre part

$$\forall n \in \mathbb{N}, S_{n+1} = 1 + \sum_{k=1}^{n+1} q^k = 1 + qS_n.$$

   Et donc,

$$\begin{aligned} \forall n \in \mathbb{N}, 1 + qS_n = S_n + q^{n+1} &\iff 1 + (q-1)S_n = q^{n+1} \\ &\iff S_n(q-1) = q^{n+1} - 1 \\ &\iff S_n = \frac{q^{n+1}-1}{q-1} \text{ pour } q \neq 1. \end{aligned}$$

□

2 Formules à connaître

Définition : Soient $k, n \in \mathbb{N}$. On définit "k parmi n" par

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!\,(n-k)!} & \text{si } k \leqslant n, \\ 0 & \text{sinon.} \end{cases}$$

Proposition : Avec les notations précédentes,

1. $\binom{n}{k} = \binom{n}{n-k}$
2. $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$

Preuve : 1. $\binom{n}{n-k} = \dfrac{n!}{(n-k)!(n-(n-k))!} = \dfrac{n!}{(n-k)!\,k!} = \binom{n}{k}$

2.

$$\begin{aligned}\binom{n}{k+1}+\binom{n}{k} &= \frac{n!(n-k)}{(k+1)!(n-k-1)!(n-k)}+\frac{n!(k+1)}{k!(n-k)!(k+1)}\\ &= \frac{n!(n-\not{k}+\not{k}+1)}{(k+1)!(n-k)!}\\ &= \frac{(n+1)!}{(k+1)!(n-k)!}\\ &= \binom{n+1}{k+1}\end{aligned}$$

□

Proposition (binôme de Newton) **:** Soient $(a,b)\in\mathbb{C}^2$ et $n\in\mathbb{N}$. Alors

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

sauf si $\begin{cases}a+b=0,\\ n=0.\end{cases}$

Remarque (triangle de Pascal) :

$n=0$						1						
$n=1$					1		1					
$n=2$				1		2		1				
$n=3$			1		3		3		1			
$n=4$		1		4		6		4		1		
$n=5$	1		5		10		10		5		1	
$n=6$	1		6		15		20		15		6	1

Exemple :

$$\forall n\in\mathbb{N},\sum_{k=0}^{n}\binom{n}{k}=\sum_{k=0}^{n}\binom{n}{k}1^k1^{n-k}=(1+1)^n=2^n.$$

Preuve :
Soient $(a,b)\in\mathbb{C}^2$.

Pour tout $n\in\mathbb{N}$, on pose

$$P(n):\text{“}(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\text{”}$$

avec la convention $\forall z \in \mathbb{C}, z^0 = 1$.

— Soit $n \in \mathbb{N}$. On suppose $P(n)$ vraie. Montrons $P(n+1)$.

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\ &= a\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} + b\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{k+1} b^{n-k} + \sum_{k=0}^{n} a^k b^{n+1-k}\end{aligned}$$

On pose $\varphi : \begin{array}{ccc}[\![0,n]\!] & \longrightarrow & [\![1,n+1]\!] \\ k & \longmapsto & k+1\end{array}$ bijective.

Donc,

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} &= \sum_{k=0}^{n} u_{\varphi(k)} \\ &= \sum_{k=1}^{n+1} u_k \text{ où } \forall n \in [\![1,n+1]\!], u_k = \binom{n}{k-1}a^k b^{n-k+1}.\end{aligned}$$

D'où

$$\begin{aligned}(a+b)^{n+1} &= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k + b^{n+1-k} + \sum_{k=0}^{n} a^k b^{n+1-k} \\ &= \binom{n}{n}a^{n+1}b + \sum_{k=1}^{n}\binom{n}{k-1}a^k b^{n+1-k} \\ &+ \binom{n}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} \\ &= \sum_{k=1}^{n}\left(\binom{n}{k} + \binom{n}{k-1}\right)a^k b^{n+1-k} + a^{n+1} + b^{n+1} \\ &= \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k}.\end{aligned}$$

— Montrons $P(0)$ $(a+b)^0 = 1$.

$$\sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1 \times 1 \times 1$$

Donc,

$$(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$$

□

Exemple :
Calculer, pour tout $n \in \mathbb{N}$, $\sum_{k=0}^{n} (-1)^k \binom{n}{k}$. On applique la formule du binôme de Newton avec $a = -1$ et $b = 1$:

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} (-1)^k \binom{n}{k} = (-1+1)^n = \begin{cases} 0 \text{ si } n > 0, \\ 1 \text{ si } n = 0. \end{cases}$$

Proposition : Soient $(a, b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$. Alors,

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

Preuve :

$$\begin{aligned} (a-b) \sum_{k=0}^{n-1} a^k &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} + \sum_{k=0}^{n-1} a^k b^{n-k} \\ &= \sum_{k=0}^{n-1} \big(\underbrace{a^{k+1} b^{n-(k+1)}}_{u_{k+1}} - \underbrace{a^k b^{n-k}}_{u_k} \big) \\ &= u_n - u_0 \\ &= a^n - b^n \end{aligned}$$

□

3 Sommes doubles

Exemple :

$$S = \sum_{i=1}^{n} \sum_{j=1}^{i} a_{i,j}$$

$$\begin{aligned} S = \sum_{j=1}^{1} a_{1,j} + \sum_{j=1}^{2} a_{2,j} + \sum_{j=3}^{3} a_{3,j} + \cdots + \sum_{j=1}^{n} a_{n,j} \\ = a_{11} \\ + a_{21} + a_{22} \\ + a_{31} + a_{32} + a_{33} \\ \vdots \\ + a_{n,1} + \cdots + a_{n,n} \end{aligned}$$

Exemple :

$$\begin{aligned} \sum_{i=1}^{n} \sum_{j=1}^{i} &= \sum_{i=1}^{n} (2^i - 1) \\ &= \sum_{i=1}^{n} 2^i - n \\ &= 2 \times \frac{1 - 2^n}{1 - 2} - n \\ &= 2(2^n - 1) - n \end{aligned}$$

Exemple :
Soit $n \in \mathbb{N}^\star$.

$$S = \sum_{j=1}^{i} \sum_{i=1}^{n} \binom{i}{j} \Bigg] \text{Aucun sens !}$$

Exemple :
Soit $n \in \mathbb{N}^\star$.

$$S = \sum_{i=1}^{n} \sum_{j=i}^{n} \binom{i}{j}$$

On pose

$$a_{j,i} = \binom{i}{j}.$$

Alors,

$$\begin{array}{rcccccccc} S & = & a_{11} & + & a_{12} & + & \cdots & + & \boxed{a_{1n}} \\ & & & + & a_{22} & + & \cdots & + & \boxed{a_{2n}} \\ & & & & & & \ddots & \vdots & \boxed{\vdots} \\ & & & & & & & + & \boxed{a_{nn}} \end{array}$$

$$\sum_{j=1}^{i} a_{j,i} = \sum_{j=1}^{i} \binom{i}{j} \qquad \boxed{\cdot} = \sum_{j=1}^{n} a_{j,n} = \sum_{j=1}^{n} \binom{n}{j}$$
$$= 2^i - 1 \qquad\qquad = 2^n - 1$$

Donc,

$$\sum_{i=1}^{n} \sum_{j=1}^{i} \binom{i}{j} = 2(2^n - 1) - n.$$

4 Sommes sur un ensemble fini

Définition : Soit I un ensemble fini. Soit $(a_i)_{i \in I}$ une famille de nombres complexes.

On note $\sum_{i \in I} a_i$ la somme des éléments de cette famille.

Exemple :
Soit $I = \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$. On pose

$$\begin{cases} a_\heartsuit = 0 \\ a_\clubsuit = -1 \\ a_\spadesuit = i \\ a_\diamondsuit = 1 + i. \end{cases}$$

Alors

$$\sum_{j \in I} a_j = 0 - 1 + i + 1 + i = 2i.$$

Exemple :
Avec $I = \{x \mapsto x^2, x \mapsto x^3, x \mapsto x^4\}$, on pose $\forall i \in I, a_i = i(2)$.

Alors,

$$\sum_{i \in I} a_i = 2^2 + 2^3 + 2^4.$$

Exemple :

— $\sum_{k \in [\![1,n]\!]} 2^k = \sum_{k=1}^{n} 2^k = 2(2^n - 1)$.

— $\displaystyle\sum_{\substack{k\in[\![1,n]\!]\\ k \text{ pair}}} 2^k = \sum_{\substack{1\leqslant j\leqslant \frac{n}{2}\\ j \text{ entier}}} 2^{2j}$.

Proposition : Soit $\varphi : I \to J$ une bijection et $(a_j)_{j\in J}$ une famille de nombres complexes. Alors

$$\sum_{j\in J} a_j = \sum_{i\in I} a_{\varphi(i)}.$$

□

Exemple :

$$\sum_{i\in\{2,4,6,8\}} a_i = \sum_{j=1}^{4} a_{2j}.$$

Exemple :

$$\begin{aligned} S = \sum_{i=1}^{n}\sum_{j=i}^{n} a_{ij} &= \sum_{(i,j)\in\left\{(1,1),\ldots,(1,n),(2,2),\ldots,(2,n),\ldots,(n,n)\right\}} a_{i,j} \\ &= \sum_{1\leqslant i\leqslant j\leqslant n} a_{ij} \\ &= \sum_{j=1}^{n}\sum_{i=1}^{j} a_{ij}. \end{aligned}$$

5 Produits

Définition : Soit $(a_i)_{i\in I}$ une famille de nombres complexes.

On note $\displaystyle\prod_{i\in I} a_i$ le produit de ces éléments.

Proposition : Soit $(u_n)_{n\in\mathbb{N}}$ une suit de nombres complexes non nuls. Alors

$$\forall n \in \mathbb{N}, \prod_{k=0}^{n} \frac{u_{k+1}}{u_k} = \frac{u_{n+1}}{u_0}.$$

□

Remarque (B Attention) :

$$\prod_{i\in I}(\lambda a_i) = \lambda^{\#I} \times \prod_{i\in I} a_i$$

où $\#I$ est le nombre d'éléments de I.

6 Rappels sur ln et exp

Proposition :

— Soit $(a_i)_{i\in I}$ une famille finie de réels strictement positifs. Alors,

$$\ln\left(\prod_{i\in I} a_i\right) = \sum_{i\in I} \ln a_i.$$

— Soit $(b_i)_{i\in I}$ une famille de réels. Alors

$$\exp\left(\sum_{i\in I} b_i\right) = \prod_{i\in I} \exp(b_i).$$

Remarque :
Soit $f : I \to \mathbb{R}^\star$ dérivable. On pose $g : x \mapsto \ln|f(x)|$.

Alors g est dérivable sur I et

$$\forall x \in I, g'(x) = \frac{f'(x)}{f(x)}$$

On dit que $\dfrac{f'}{f}$ est la dérivée logarithmique de f.

Soient $f_1, f_2 : I \to \mathbb{R}^\star$ dérivables. Alors

$$\frac{(f_1\, f_2)'}{f_1\, f_2} = \frac{f_1'}{f_1} + \frac{f_2'}{f_2}.$$

Remarque :
Soit $a \in \mathbb{R}$.

— Soit $n \in \mathbb{N}^\star$. Alors, $a^n = \overbrace{a \times a \times a \times \cdots \times a}^{n \text{ fois}}$.

— Soit $n \in \mathbb{Z}_\star^-$. Si $a \neq 0$, alors $a^n = \dfrac{1}{a^{-n}}$.

— Si $a \neq 0$, $a^0 = 1$ et

$$\forall p, q \in \mathbb{Z}, a^p \times a^q = a^{p+q}.$$

— Soit $p \in \mathbb{Z}$ et $a > 0$.

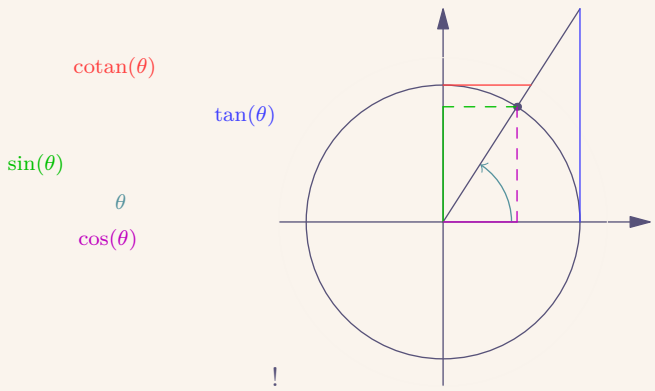
$$a^p = \exp(\ln a^p) = \exp(p \ln a) = e^{p \ln a}.$$

Définition : Soit $a \in \mathbb{R}_\star^+$ et $p \in \mathbb{R}$. On pose $a^p = e^{p \ln a}$.

Chapitre 2

Nombres complexes

1 Trigonométrie



!

Définition : On définit, pour

$$\theta \in \bigcup_{k\in\mathbb{Z}} \left]-\frac{\pi}{2}+k\pi, \frac{\pi}{2}+k\pi\right[$$
$$\iff \theta \in \mathbb{R} \setminus \left\{\frac{\pi}{2}+2\pi k \mid k \in \mathbb{Z}\right\}$$

la tangente de θ par

$$\tan\theta = \frac{\sin\theta}{\cos\theta}$$

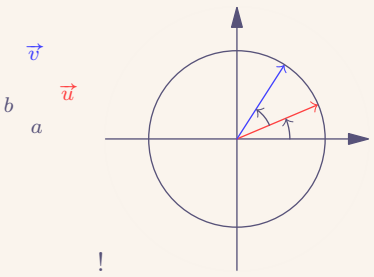
Définition : Pour $\theta \in \bigcup_{k\in\mathbb{Z}}]-k\pi,(k+1)\pi[$, on définit la contangente de θ par

$$\operatorname{cotan}\theta = \frac{\cos\theta}{\sin\theta}$$

Proposition : Soient $(a,b) \in \mathbb{R}^2$.

1. $\cos(-a) = \cos(a)$
2. $\cos(a+2\pi) = \cos(a)$
3. $\cos(a+\pi) = -\cos(a)$
4. $\cos(\pi-a) = -\cos(a)$
5. $\sin(-a) = -\sin(a)$
6. $\sin(a+2\pi) = \sin(a)$
7. $\sin(a+\pi) = -\sin(a)$
8. $\sin(\pi-a) = \sin(a)$
9. $\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$
10. $\sin(a+b) = \cos(a)\sin(b) + \sin(a)\cos(b)$
11. $\cos\left(\frac{\pi}{2}-a\right) = \sin(a)$
12. $\sin\left(\frac{\pi}{2}-a\right) = \cos(a)$

Preuve : 8. Soient $\vec{u} = (\cos(a),\sin(a))$ et $\vec{v} = (\cos(b),\sin(b))$



!

D'une part, $\vec{u}\cdot\vec{v} = \cos(a)\cos(b) + \sin(a)\sin(b)$
D'autre part, $\vec{u}\cdot\vec{v} = \|\vec{u}\| \times \|\vec{v}\| \times \cos(\widehat{\vec{u},\vec{v}}) = \cos(a-b)$
On a montré que

$$\forall (a,b) \in \mathbb{R}^2, \cos(a-b) = \cos(a)\cos(b) + \sin(a)\sin(b)$$
$$\text{d'où } \forall (a,b) \in \mathbb{R}^2, \cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$$

11. $\forall a \in \mathbb{R}, \cos\left(\frac{\pi}{2} - a\right) = \overbrace{\cos\left(\frac{\pi}{2}\right)}^{=0}\cos(a) + \overbrace{\sin\left(\frac{\pi}{2}\right)}^{=1}\sin(a) = \sin(a)$
12. $\forall a \in \mathbb{R}, \cos(a) = \cos\left(-a + \frac{\pi}{2} + \frac{\pi}{2}\right) = \sin\left(\frac{\pi}{2} - a\right)$
10.

$$\begin{aligned}\forall (a,b) \in \mathbb{R}^2, \sin(a+b) &= \cos\left(\left(\frac{\pi}{2} - a\right) - b\right)\\ &= \cos\left(\frac{\pi}{2} - a\right)\cos(b) + \sin\left(\frac{\pi}{2} - a\right)\sin(b)\\ &= \sin(a)\cos(b) + \cos(a)\sin(b)\end{aligned}$$

□

Proposition : Soient a et b deux réels tels que $a \not\equiv \frac{\pi}{2}\ [\pi]$ et $b \not\equiv \frac{\pi}{2}\ [\pi]$.

1. $\tan(a+\pi) = \tan(a)$
2. $\tan(-a) = -\tan(a)$
3. Si $a + b \not\equiv \frac{\pi}{2}\ [\pi]$, alors, $\tan(a+b) = \dfrac{\tan(a) + \tan(b)}{1 - \tan(a)\tan(b)}$

Preuve : 3. On suppose $a + b \not\equiv \frac{\pi}{2}\ [\pi]$

$$\begin{aligned}\tan(a+b) &= \frac{\sin(a+b)}{\cos(a+b)} \\ &= \frac{\sin(a)\cos(b)+\sin(b)\cos(a)}{\cos(a)\cos(b)-\sin(a)\sin(b)} \\ &= \frac{\frac{\sin(a)\cos(b)}{\cos(a)\cos(b)}+\frac{\sin(b)\cos(a)}{\cos(a)\cos(b)}}{\frac{\cos(a)\cos(b)-\sin(a)\sin(b)}{\cos(a)\cos(b)}} \\ &= \frac{\tan(a)+\tan(b)}{1-\tan(a)\tan(b)}\end{aligned}$$

□

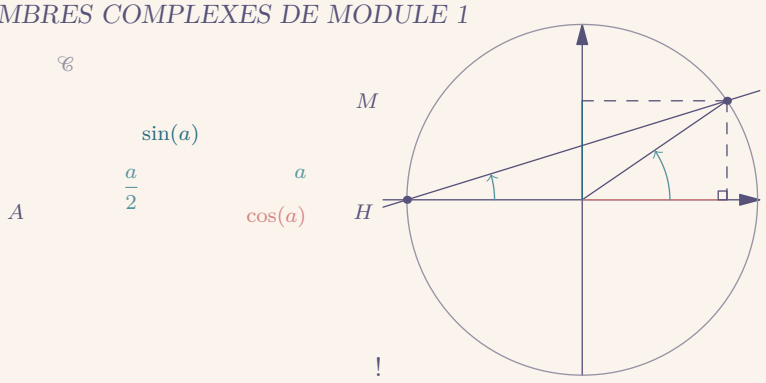
Proposition : Soit $a \in \mathbb{R}$.

1. Si $a \not\equiv \frac{\pi}{2}\ [\pi]$, alors, $1+\tan^2(a) = \frac{1}{\cos^2(a)}$
2. Si $a \not\equiv \pi\ [2\pi]$
   - $\cos(a) = \frac{1-\tan^2\left(\frac{a}{2}\right)}{1+\tan\left(\frac{a}{2}\right)}$
   - $\sin(a) = \frac{2\tan\left(\frac{a}{2}\right)}{1+\tan^2\left(\frac{a}{2}\right)}$
   - Si $a \not\equiv \frac{\pi}{2}\ [\pi]$, $\tan(a) = \frac{2\tan\left(\frac{a}{2}\right)}{1+\tan^2\left(\frac{a}{2}\right)}$

Preuve : 1. On suppose que $a \not\equiv \frac{\pi}{2}\ [\pi]$

$$1+\tan^2(a) = 1+\frac{\sin^2(a)}{\cos^2(a)} = \frac{\cos^2(a)+\sin^2(a)}{\cos^2(a)} = \frac{1}{\cos^2(a)}$$

2. On peut le prouver par le calcul avec les formules de la tangeante mais on peut également le prouver géométriquement.



Soit $M(x_0, y_0) \neq A$ sur le cercle trigonométrique $\mathscr{C}$. On note t la pente de la demi-droite $[AM)$.
On en déduit que l'équation de la droite (AM) est

$$y = tx + t = t(x + 1)$$

On sait que $M \in (AM)$ donc

$$y_0 = t(x_0 + 1)$$

On sait aussi que ${x_0}^2 + {y_0}^2 = 1$
Donc,

$$x_0 + t^2(x_0 + 1)^2 = 1$$

et donc

$${x_0}^2 \underbrace{(1 + t^2)}_{\neq 0} + 2t^2 x_0 + t^2 - 1 = 0$$

On résout cette équation du second degré et on trouve deux racines :
$x_0 = -1$ et $x_0 = \dfrac{1 - t^2}{1 + t^2}$.
Comme $M \neq A$, $x_0 = \dfrac{1 - t^2}{1 + t^2}$ et $y_0 = t\left(\dfrac{1 - t^2}{1 + t^2} + 1\right) = \dfrac{2t}{1 + t^2}$
Enfin,

$$t = \frac{|HM|}{|AH|} = \tan\left(\frac{a}{2}\right)$$

car AHM est rectangle en H (d'après le théorème de Thalès)
Donc,

$$\begin{cases} \cos(a) = \dfrac{1 - \tan^2\left(\frac{a}{2}\right)}{1 + \tan^2\left(\frac{a}{2}\right)} \\ \sin(a) = \dfrac{2\tan\left(\frac{a}{2}\right)}{1 + \tan^2\left(\frac{a}{2}\right)} \end{cases}$$

□

2 Nombres complexes de module 1

Proposition : Soient $(a, b) \in \mathbb{R}^2$.

$$(\cos(a) + i\sin(a)) \times (\cos(b) + i\sin(b)) = \cos(a+b) + i\sin(a+b)$$

Preuve :

$$\begin{aligned}(\cos(a) + i\sin(a)) \times (\cos(b) + i\sin(b)) &= \cos(a)\cos(b) - \sin(a)\sin(b) \\ &\quad + i(\cos(a)\sin(b) + \cos(b)\sin(a)) \\ &= \cos(a+b) + i\sin(a+b)\end{aligned}$$

□

Définition : Pour $a \in \mathbb{R}$, on pose $e^{ia} = \cos(a) + i\sin(a)$
Ainsi, $\forall (a, b) \in \mathbb{R}^2, e^{ia} \times e^{ib} = e^{i(a+b)}$

Proposition : Soient a, b, c trois nombres complexes avec $a \neq 0$ et z_1, z_2 les racines de $P : z \mapsto az^2 + bz + c$
Alors, $z_1 \times z_2 = \dfrac{c}{a}$ et $z_1 + z_2 = -\dfrac{b}{a}$

Exemple :
$(E) : z^2 - 3z + 2 = 0$
On remarque que $2 \times 1 = 2$ et $2 + 1 = 3$ donc 2 et 1 sont deux solutions de (E).

Méthode 1 Soit $\Delta = b^2 - 4ac$ et δ une racine carrée de Δ

$$z_1 = \frac{-b - \delta}{2a} \text{ et } z_2 = \frac{-b + \delta}{2a}$$

Donc,

$$z_1 \times z_2 = \frac{b^2 - \delta^2}{4a^2} = \frac{b^2 - \Delta}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a} \quad z_1 + z_2 = \frac{-b - b - \delta + \delta}{2a} = -\frac{2b}{2a} = -\frac{b}{a}$$

Méthode 2

$$\forall z \in \mathbb{C}, az^2 + bz + c = a(z - z_1)(z - z_2) = a(z^2 - (z_1 + z_2)z + z_1 z_2)$$

En particulier,

$$\begin{cases} \text{avec } z=0, & c = az_1z_2 \\ \text{avec } z=0, & \cancel{d} + b + \cancel{c} = a(\cancel{1} - (z_1+z_2) + \cancel{z_1z_2}) \end{cases}$$

donc

$$b = -a(z_1+z_2)$$

et donc

$$\begin{cases} z_1z_2 = \dfrac{c}{a} \\ z_1+z_2 = -\dfrac{b}{a} \end{cases}$$

□

Proposition : Soient $(a,b,c) \in \mathbb{C}^3$ et z_1, z_2, z_3 les solutions de

$$z^3 + az^2 + bz + c = 0$$

Alors,

$$\begin{cases} z_1z_2z_3 = -c \\ z_1z_2 + z_2z_3 + z_1z_3 = b \\ z_1+z_2+z_3 = -a \end{cases}$$

□

Proposition : Soient $a_1, a_2, \ldots, a_n$ des nombres complexes et $z_1, z_2, \ldots, z_n$ les solutions de

$$z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 1$$

Alors,

$$\forall k \in [\![1,n]\!], \quad \sum_{1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_k \leqslant n} z_{i_1} \times z_{i_2} \times \cdots \times z_{i_k} = (-1)^k a_{n-k}$$

$$\sum_{k=1}^{n} z_k = -a_{n-1}$$

$$\prod_{k=1}^{n} z_k = (-1)^k a_0$$

Preuve (incomplète pour $n=3$) *:*

$$\forall z \in \mathbb{C}, z^3 + az^2 + bz + c = (z - z_1)(z - z_2)(z - z_3) = z^3 + z^2(-z_1 - z_2 - z_3) + z(z_2z_3 + z_1z_2 + z_1z_3) - z_1z_2z_3$$

$$\text{On identifie } \begin{cases} a = -z_1 - z_2 - z_3 \\ b = z_1z_2 + z_2z_3 + z_1z_3 \\ c = -z_1z_2z_3 \end{cases}$$ □

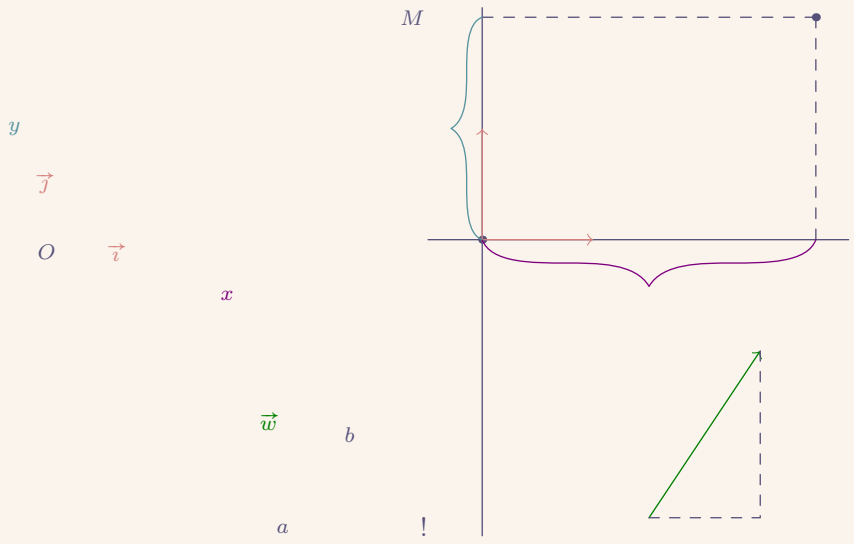
Exemple :
On pose

$$\begin{cases} s = z_1 + z_2 + z_3 \\ q = z_1z_2 + z_2z_3 + z_1z_3 \\ p = z_1z_2z_3 \end{cases}$$

et $P = z_1^3 + z_2^3 + z_3^3$

3 Géométrie des nombres complexes

Dans ce paragraphe, $\mathcal{P}$ dérisgne un plan euclidien muni d'un repère orthonormé $(O, \vec{\imath}, \vec{\jmath})$



Définition : Soit $M \in \mathcal{P}$. On note (x, y) les coordonnées du point M par rapport au repère $(O, \vec{\imath}, \vec{\jmath})$

L'affixe de M est le nombre

$$z_M = x + iy \in \mathbb{C}$$

Soit $\vec{w} \in \vec{\mathcal{P}}$ (le plan des vecteurs) et (a, b) les coordonées de $\vec{w}$.
L'affixe de $\vec{w}$ est

$$z_{\vec{w}} = a + ib \in \mathbb{C}$$

Proposition : Soit $(A, B) \in \mathcal{P}^2$ et $(\overrightarrow{w_1}, \overrightarrow{w_2}) \in \vec{\mathcal{P}}^2$

1. $z_{\overrightarrow{AB}} = z_B - z_A$
2. $z_{\overrightarrow{w_1}+\overrightarrow{w_2}} = z_{\overrightarrow{w_1}} + z_{\overrightarrow{w_2}}$

□

Proposition : Soit $(\overrightarrow{w_1}, \overrightarrow{w_2}) \in \vec{\mathcal{P}}^2$ avec $\overrightarrow{w_1} \neq \vec{0}$ et $\overrightarrow{w_2} \neq \vec{0}$
Alors, $\left|\dfrac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}}\right| = \dfrac{\|\overrightarrow{w_1}\|}{\|\overrightarrow{w_2}\|}$ et $\arg\left(\dfrac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}}\right) = \underbrace{\widehat{(\overrightarrow{w_1}, \overrightarrow{w_2})}}_{\text{l'angle entre } \overrightarrow{w_1} \text{ et } \overrightarrow{w_2}}$

Preuve :
Soient $(r_1, r_2) \in \left(\mathbb{R}^+\right)^2$ et $(\theta_1, \theta_2) \in ([0, 2\pi[)^2$ tels que

$$z_{\overrightarrow{w_1}} = r_1 e^{i\theta_1} \text{ et } z_{\overrightarrow{w_2}} = r_2 e^{i\theta_2}$$

Alors,

$$\frac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$$

donc

$$\begin{cases} \left|\dfrac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}}\right| = \dfrac{r_1}{r_2} = \dfrac{\|\overrightarrow{w_1}\|}{\|\overrightarrow{w_2}\|} \\ \arg\left(\dfrac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}}\right) \equiv \theta_1 - \theta_2 \ [2\pi] \end{cases}$$

car $\theta_1 - \theta_2$ est l'angle entre $\overrightarrow{w_1}$ et $\overrightarrow{w_2}$ □

Corollaire : Avec les hypothèses et notations précédentes,

1. $\overrightarrow{w_1}$ et $\overrightarrow{w_2}$ sont collinéaires $\iff \dfrac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}} \in \mathbb{R}$
2. $\overrightarrow{w_1}$ et $\overrightarrow{w_2}$ sont orthogonaux $\iff \dfrac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}} \in i\mathbb{R}$

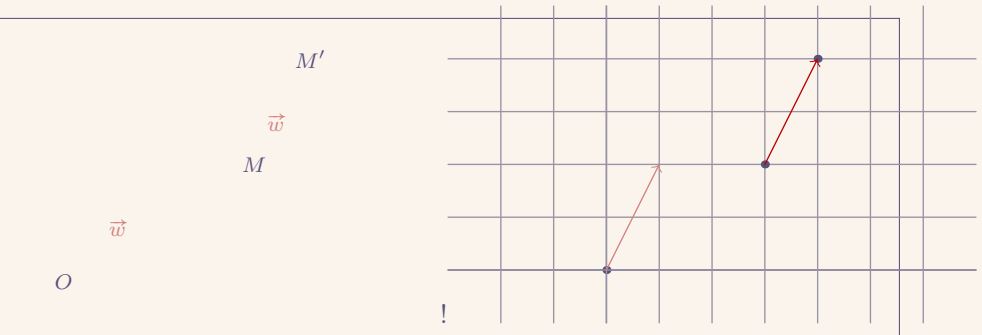
Preuve : 1.

$$\begin{aligned}\overrightarrow{w_1} \text{ et } \overrightarrow{w_2} \text{ sont colinéaires} &\iff \widehat{(\overrightarrow{w_1}, \overrightarrow{w_2})} \equiv 0 \ [\pi] \\ &\iff \arg\left(\frac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}}\right) \equiv 0 \ [\pi] \\ &\iff \frac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}} \in \mathbb{R}\end{aligned}$$

2.

$$\begin{aligned}\overrightarrow{w_1} \text{ et } \overrightarrow{w_2} \text{ sont orthogonaux} &\iff \widehat{(\overrightarrow{w_1}, \overrightarrow{w_2})} \equiv \frac{\pi}{2} \ [\pi] \\ &\iff \arg\left(\frac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}}\right) \equiv \frac{\pi}{2} \ [\pi] \\ &\iff \frac{z_{\overrightarrow{w_1}}}{z_{\overrightarrow{w_2}}} \in i\mathbb{R}\end{aligned}$$

□



Définition : Soit $\vec{w} \in \vec{\mathcal{P}}$. La translation de vecteur $\vec{w}$ est l'application

$$\begin{aligned} t_{\vec{w}} : \mathcal{P} &\longrightarrow \mathcal{P} \\ M &\longmapsto M' \end{aligned}$$

où M' vérifie $\overrightarrow{MM'} = \vec{w}$

Proposition : Soit $\vec{w} \in \vec{\mathcal{P}}$ et $(M, M') \in \mathcal{P}^2$

$$M' = t_{\vec{w}}(M) \iff z_{M'} = z_M + z_{\vec{w}}$$

Preuve :

$$\begin{aligned} M' = t_{\vec{w}}(M) &\iff \overrightarrow{MM'} = \vec{w} \\ &\iff z_M - z_{M'} = z_{\vec{w}} \\ &\iff z_{M'} = z_M + z_{\vec{w}} \end{aligned}$$

□

Exemple (Décrire l'ensemble $E = \left\{M \in \mathcal{P} \mid \exists t \in \mathbb{R}, z_M = 1 + e^{it}\right\}$) :
L'ensemble $\mathscr{C} = \left\{M \in \mathcal{P} \mid \exists t \in \mathbb{R}, z_M = e^{it}\right\}$ est le cercle trigonométrique. La translation $t_{\vec{u}}$ a pour expression complexe $z \mapsto z + 1$ Donc, $E = t_{\vec{u}}(\mathscr{C})$ est le cercle de rayon 1 et de centre le point d'affixe 1.

Proposition : Soient $\overrightarrow{w_1}, \overrightarrow{w_2} \in \vec{\mathcal{P}}$.

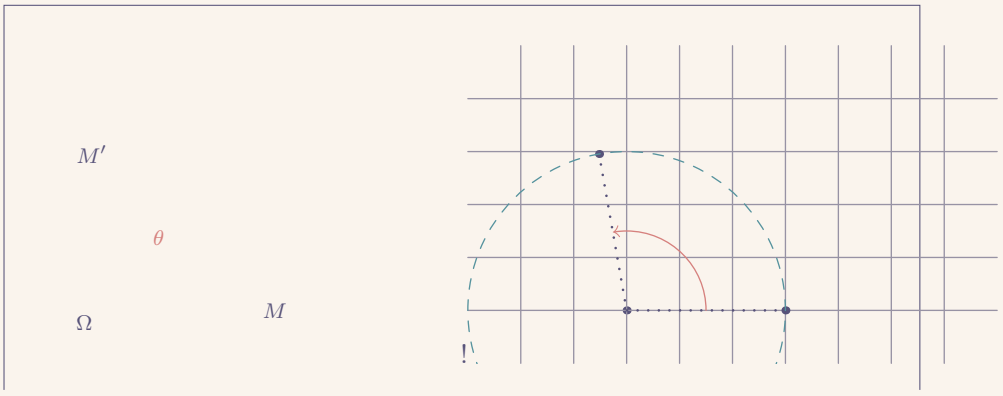
$$t_{\overrightarrow{w_2}} \circ t_{\overrightarrow{w_1}} = t_{\overrightarrow{w_1}+\overrightarrow{w_2}}$$

Preuve :
Soit $M \in \mathcal{P}$ d'affixe z. On pose $M_1 = t_{\overrightarrow{w_1}}(M)$ et $M' = t_{\overrightarrow{w_1}}(M_1)$ et on note également $M'' = t_{\overrightarrow{w_1}+\overrightarrow{w_2}}(M)$

$$\begin{aligned} z_{M'} &= z_{M_1} + z_{\overrightarrow{w_2}} \\ &= (z + z_{\overrightarrow{w_1}}) + z_{\overrightarrow{w_2}} \\ &= z + z_{\overrightarrow{w_1}+\overrightarrow{w_2}} \end{aligned}$$

Donc, $M' = M''$

□



Définition : Soit $\Omega \in \mathcal{P}$ et $\theta \in \mathbb{R}$.
La rotation de centre Ω et d'angle θ est l'application

$$\begin{aligned} \rho_{\Omega,\theta} : \mathcal{P} &\longrightarrow \mathcal{P} \\ M &\longmapsto M' \end{aligned}$$

où M' vérifie

$$\begin{cases} \|\overrightarrow{\Omega M}\| = \|\overrightarrow{\Omega M'}\| \\ \widehat{(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'})} = \theta \end{cases}$$

Proposition : Soit $\Omega \in \mathcal{P}$ d'affixe ω, $\theta \in \mathbb{R}$ et $(M, M') \in \mathcal{P}^2$

$$(\star) : \qquad M' = \rho_{\Omega,\theta}(M) \iff z_{M'} = \omega + e^{i\theta}(z_M - \omega)$$

*Preuve*Cas 1 On suppose $M \neq \Omega$.

$$\begin{aligned} M' = \rho_{\Omega,\theta}(M) &\iff \begin{cases} \|\overrightarrow{\Omega M}\| = \|\overrightarrow{\Omega M'}\| \\ \widehat{(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'})} = \theta \end{cases} \\ &\iff \begin{cases} \left|z_{\overrightarrow{\Omega M}}\right| = \left|z_{\overrightarrow{\Omega M'}}\right| \\ \arg\left(\dfrac{z_{\overrightarrow{\Omega M}}}{z_{\overrightarrow{\Omega M'}}}\right) = \theta \end{cases} \\ &\iff e^{i\theta} = \frac{z_{\overrightarrow{\Omega M}}}{z_{\overrightarrow{\Omega M'}}} \\ &\iff z_{\overrightarrow{\Omega M'}} = e^{i\theta} z_{\overrightarrow{\Omega M}} \\ &\iff z_{M'} - \omega = e^{i\theta}(z_M - \omega) \\ &\iff z_{M'} = \omega + e^{i\theta}(z_M - \omega) \end{aligned}$$

Cas 2 On suppose $M = \Omega$.
Alors,

$$\begin{aligned} M' = \rho_{\Omega,\theta}(M) &\iff M' = M \\ &\iff z_{M'} = z_M \\ &\iff z_{M'} = z_M + e^{i\theta}(z_M - z_M) \\ &\iff z_{M'} = \omega + e^{i\theta}(z_M - \omega) \end{aligned}$$

□

Remarque (Cas particulier) :

Si $\Omega = O$ alors

$$(\star) \iff z_{M'} = e^{i\theta} z_M$$

Corollaire : Soit $\Omega \in \mathscr{P}$ d'affixe ω et $\theta \in \mathbb{R}$.

$$\begin{aligned}\rho_{\Omega,\theta} &= t_{\overrightarrow{O\Omega}} \circ \rho_{O,\theta} \circ t_{\overrightarrow{\Omega O}} \\ &= t_{\overrightarrow{O\Omega}} \circ \rho_{O,\theta} \circ (t_{\overrightarrow{O\Omega}})^{-1}\end{aligned}$$

Proposition : Soient $(\Omega_1, \Omega_2) \in \mathscr{P}^2$ et $(\theta_1, \theta_2) \in \mathbb{R}^2$

$$\rho_{\Omega_1,\theta_1} \circ \rho_{\Omega_1,\theta_2} = \rho_{\Omega_1,\theta_1+\theta_2} = \rho_{\Omega_1,\theta_2} \circ \rho_{\Omega_1,\theta_1}$$

Si $\begin{cases}\Omega_1 \neq \Omega_2 \\ \theta_1 + \theta_2 \not\equiv 0 \ [2\pi]\end{cases}$ alors $\rho_{\Omega_1,\theta_1} \circ \rho_{\Omega_2,\theta_2}$ est une rotation d'angle $\theta_1 + \theta_2$

Si $\begin{cases}\Omega_1 \neq \Omega_2 \\ \theta_1 + \theta_2 \equiv 0 \ [2\pi]\end{cases}$ alors $\rho_{\Omega_1,\theta_1} \circ \rho_{\Omega_2,\theta_2}$ est une translation

Preuve :
On note ω_1 l'affixe de Ω_1 et ω_2 l'affixe de Ω_2. On pose $\rho_1 = \rho_{\Omega_1,\theta_1}$ et $\rho_2 = \rho_{\Omega_2,\theta_2}$
Soit $M \in \mathscr{P}$ d'affixe z. On pose

$$\begin{aligned}M_2 &= \rho_2(M) \\ M' &= \rho_1 \circ \rho_2(M) = \rho_1(M_2)\end{aligned}$$

et on note z_2 et z' les affixes de M_2 et M'
On a

$$\begin{aligned}z' &= \omega_1 + e^{i\theta_1}(z_2 - \omega_1) \\ &= \omega_1 + e^{i\theta_1}(\omega_2 + e^{i\theta_2}(z - \omega_2) - \omega_1) \\ &= \omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} + e^{i(\theta_1+\theta_2)}(z - \omega_2)\end{aligned}$$

1. On suppose $\Omega_1 = \Omega_2$ donc $\omega_1 = \omega_2$. On a donc

$$z' = \omega_1 + e^{i(\theta_1+\theta_2)}(z - \omega_1)$$

On reconnaît l'expression d'une rotation de centre Ω_1 et d'angle $\theta_1 + \theta_2$

2. On suppose $\Omega_1 \neq \Omega_2$ et $\theta_1 + \theta_2 \equiv 0\ [2\pi]$. On a donc

$$\begin{aligned} z' &= \underbrace{\omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} - \omega_2}_{} + z \\ &= z + \omega \end{aligned}$$

On reconnaît l'expression d'une translation de vecteur ω.

3. On suppose $\Omega_1 \neq \Omega_2$ et $\theta_1 + \theta_2 \not\equiv 0\ [2\pi]$
On cherche $\omega \in \mathbb{C}$ tel que

$$\begin{aligned} &\forall z \in \mathbb{C}, \omega + e^{i(\theta_1+\theta_2)}(z-\omega) = \omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} + e^{i(\theta_1+\theta_2)}(z-\omega_2) \\ \iff &\omega - e^{i(\theta_1+\theta_2)}\omega = \omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} - \omega_2 e^{i(\theta_1+\theta_2)} \\ \iff &\omega = \frac{\omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} - \omega_2 e^{i(\theta_1+\theta_2)}}{1 - e^{i(\theta_1+\theta_2)}} \end{aligned}$$

On reconnait l'expression complexe d'une rotation d'angle $\theta_1 + \theta_2$ de centre Ω d'affixe ω

□

Proposition : Soit $\Omega \in \mathcal{P}$ d'affixe ω, $\vec{w} \in \vec{\mathcal{P}}$ d'affixe u. Soit $\theta \in \mathbb{R}$ avec $\theta \not\equiv 0\ [2\pi]$.

— $t_{\vec{w}} \circ \rho_{\Omega,\theta}$ est une rotation d'angle θ
— $\rho_{\Omega,\theta} \circ t_{\vec{w}}$ est aussi une rotation d'angle θ

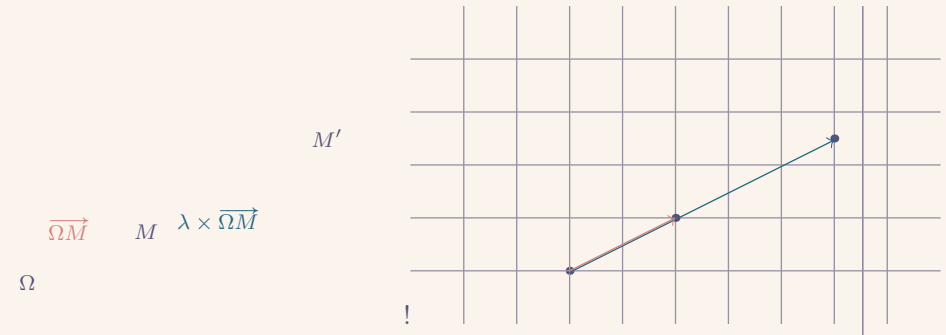
Preuve :
Soit $M \in \mathcal{P}$ d'affixe z et $M' = t_{\vec{w}} \circ \rho_{\Omega,\theta}(M)$ d'affixe z'
On a alors :

$$z' = (\omega + e^{i\theta}(z-\omega)) + u$$

On cherche $\omega' \in \mathbb{C}$ tel que

$$\begin{aligned} &\forall z \in \mathbb{C}, \omega + u + e^{i\theta}(z-\omega) = \omega' + e^{i\theta}(z-\omega') \\ \iff &\omega + u - e^{i\theta}\omega = \omega' - e^{i\theta}\omega' \\ \iff &\omega' = \frac{\omega + u - e^{i\theta}\omega}{1 - e^{i\theta}} \end{aligned}$$

On reconnaît l'expression complexe d'une rotation d'angle θ □



Définition : Soit $\Omega \in \mathcal{P}$ et $\lambda \in \mathbb{R}$.
L'homothétie de centre Ω et de rapport λ est l'application

$$\begin{aligned} h_{\Omega,\lambda} : \mathcal{P} &\longrightarrow \mathcal{P} \\ M &\longmapsto M' \end{aligned}$$

où M' vérifie $\overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M}$

Proposition : Soit $\Omega \in \mathcal{P}$ d'affixe ω, $\lambda \in \mathbb{R}$. Soient $M \in \mathcal{P}$ d'affixe z et $M' \in \mathcal{P}$ d'affixe z'.

$$M' = h_{\Omega,\lambda}(M) \iff z' = \omega + \lambda(z - \omega)$$

Preuve :

$$\begin{aligned} M' = h_{\Omega,\lambda}(M) &\iff \overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M} \\ &\iff z_{\overrightarrow{\Omega M'}} = z_{\lambda \overrightarrow{\Omega M}} \\ &\iff z' - \omega = \lambda(z - \omega) \\ &\iff z' = \omega + \lambda(z - \omega) \end{aligned}$$

□

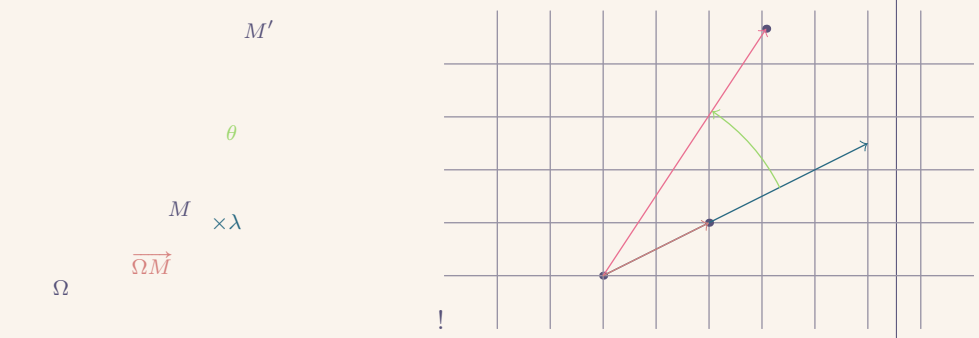
Proposition : Soient $(\Omega_1, \Omega_2) \in \mathcal{P}^2$ et $(\lambda_1, \lambda_2) \in \mathcal{P}^2$

1. Si $\Omega_1 = \Omega_2$ alors, $h_{\Omega_1,\lambda_1} \circ h_{\Omega_2,\lambda_2} = h_{\Omega_1,\lambda_1\lambda_2}$
2. Si $\Omega_1 \neq \Omega_2$ et $\lambda_1\lambda_2 \neq 1$, alors, $h_{\Omega_1,\lambda_1} \circ h_{\Omega_2,\lambda_2}$ est une homothétie de rapport $\lambda_1\lambda_2$
3. Si $\Omega_1 \neq \Omega_2$ et $\lambda_1\lambda_2 = 1$, alors, $h_{\Omega_1,\lambda_1} \circ h_{\Omega_2,\lambda_2}$ est une translation.

□

Proposition : Soit $\Omega \in \mathcal{P}$, $\lambda \in \mathbb{R} \setminus \{1\}$, $\vec{w} \in \vec{\mathcal{P}}$.
Alors, $t_{\vec{w}} \circ h_{\Omega,\lambda}$ et $h_{\Omega,\lambda} \circ t_{\vec{w}}$ sont homothéties de rapport λ. □

Remarque (Cas particulier) :
Soit $M \in \mathcal{P}$ d'affixe z, $\lambda \in \mathbb{R}$ et $M' = h_{O,\lambda}(M)$ d'affixe z'
On a $z' = \lambda z$



Définition : Soient $\Omega \in \mathcal{P}$, $(\theta, \lambda) \in \mathbb{R}^2$. La similitude (directe) de centre Ω, d'angle θ et de rapport λ est

$$S_{\Omega,\theta,\lambda} = h_{\Omega,\lambda} \circ \rho_{\Omega,\theta}$$

Proposition : Avec les notations précédentes,

$$S_{\Omega,\theta,\lambda} = \rho_{\Omega,\theta} \circ h_{\Omega,\lambda}$$

Preuve :
On note ω l'affixe de Ω. L'expression complexe de $S_{\Omega,\theta,\lambda}$ est

$$\begin{aligned} z' &= \omega + \lambda(\omega + e^{i\theta}(z - \omega) - \omega) \\ &= \omega + \lambda e^{i\theta}(z - \omega) \end{aligned}$$

L'expression complexe de $\rho_{\Omega,\theta} \circ h_{\Omega,\lambda}$ est

$$\begin{aligned} z' &= \omega + e^{i\theta}(\omega + \lambda(z - \omega) - \omega) \\ &= \omega + \lambda e^{i\theta}(z - \omega) \end{aligned}$$

Les deux expressions sont identiques. □

Proposition : L'expression complexe de $S_{\Omega,\theta,\lambda}$ est

$$z' = \omega + \lambda e^{i\theta}(z - \omega)$$

Définition : Pour $z \in \mathbb{C}$, on pose

$$\exp(z) = e^{\mathfrak{Re}(z)} \times (\cos(\mathfrak{Im}(z)) + i\sin(\mathfrak{Im}(z))$$

Ainsi, si $z = a + ib$ avec $(a, b) \in \mathbb{R}^2$,

$$\exp(z) = \exp(a + ib) = e^a \times (\cos(b) + i(\sin(b)) = e^a e^{ib}$$

Proposition : Soient $z_1, z_2 \in \mathbb{C}$.

$$\exp(z_1 + z_2) = \exp(z_1) \times \exp(z_2)$$

Preuve :
On pose $\begin{cases} z_1 = a + ib \\ z_2 = c + id \end{cases}$ avec $(a, b, c, d) \in \mathbb{R}^4$

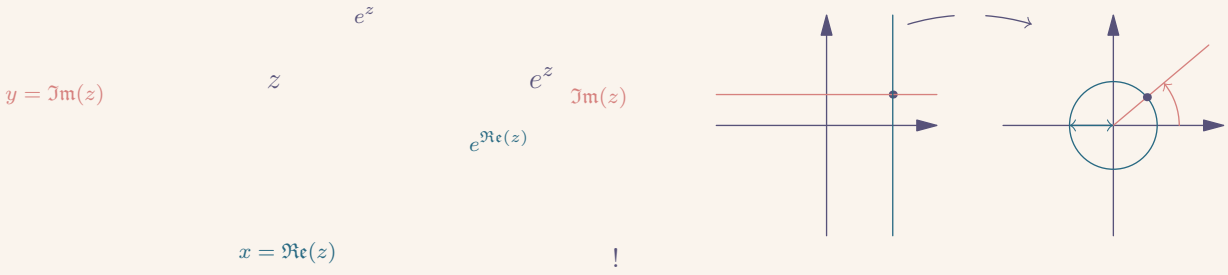
$$\begin{aligned} \exp(z_1) \times \exp(z_2) &= e^a \times e^{ib} \times e^c \times e^{id} \\ &= e^{a+c} e^{i(b+d)} \\ &= \exp(z_1 + z_2) \end{aligned}$$

□

Remarque (Notation) :
On écrit e^z à la place de $\exp(z)$ pour $z \in \mathbb{C}$.

Proposition :

$$\forall z \in \mathbb{C}, \begin{cases} |e^z| = e^{\mathfrak{Re}(z)} \\ \arg(e^z) \equiv \mathfrak{Im}(z) \ \ [2\pi] \end{cases}$$



Remarque :
$\exp : \mathbb{C} \to \mathbb{C}$ n'est pas bijective :

— $\begin{cases} \exp(0) = \exp(2i\pi) = 1 \\ 0 \neq 2i\pi \end{cases}$

— 0 n'a pas d'antécédant

Il n'y a donc pas de logarithme complexe.

5 Fonctions de $\mathbb{R}$ dans $\mathbb{C}$

Définition : Soit f définie sur $D \subset \mathbb{R}$ à valeurs dans $\mathbb{C}$ ($\forall x \in D, f(x) \in \mathbb{C}$)
On pose :

$$\begin{aligned} \mathfrak{Re}(f) : D &\longrightarrow \mathbb{R} \\ x &\longmapsto \mathfrak{Re}(f(x)) \end{aligned}$$

et

$$\begin{aligned} \mathfrak{Im}(f) : D &\longrightarrow \mathbb{R} \\ x &\longmapsto \mathfrak{Im}(f(x)) \end{aligned}$$

Exemple :

$$\begin{aligned} f : [0, 2\pi[&\longrightarrow \mathbb{C} \\ x &\longmapsto e^{(1+i)x} \end{aligned}$$

On a :

$$\begin{aligned} \mathfrak{Re}(f) : [0, 2\pi[&\longrightarrow \mathbb{R} \\ x &\longmapsto e^x \cos(x) \end{aligned}$$

et

$$\begin{aligned} \mathfrak{Im}(f) : [0, 2\pi[&\longrightarrow \mathbb{R} \\ x &\longmapsto e^x \sin(s) \end{aligned}$$

Définition : Soit $f : D \to \mathbb{C}$. On dit que
- f est continue si $\mathfrak{Re}(f)$ et $\mathfrak{Im}(f)$ sont continues
- f est dérivable si $\mathfrak{Re}(f)$ et $\mathfrak{Im}(f)$ sont dérivables.
  Dans ce cas, la dérivée de f est

$$\begin{aligned} f' : D &\longrightarrow \mathbb{C} \\ x &\longmapsto \mathfrak{Re}(f)'(x) + i\mathfrak{Im}(f)'(x) \end{aligned}$$

Exemple :

$$\begin{aligned} f : [0, 2\pi[&\longrightarrow \mathbb{C} \\ x &\longmapsto e^{(1+i)x} \end{aligned}$$

$x \mapsto e^x$ et $x \mapsto \cos(x)$ sont dérivables sur $[0, 2\pi[$ donc $\mathfrak{Re}(f)$ est dérivable.
$x \mapsto e^x$ et $x \mapsto \sin(x)$ sont dérivables sur $[0, 2\pi[$ donc $\mathfrak{Im}(f)$ est dérivable.
Donc f est dérivable.

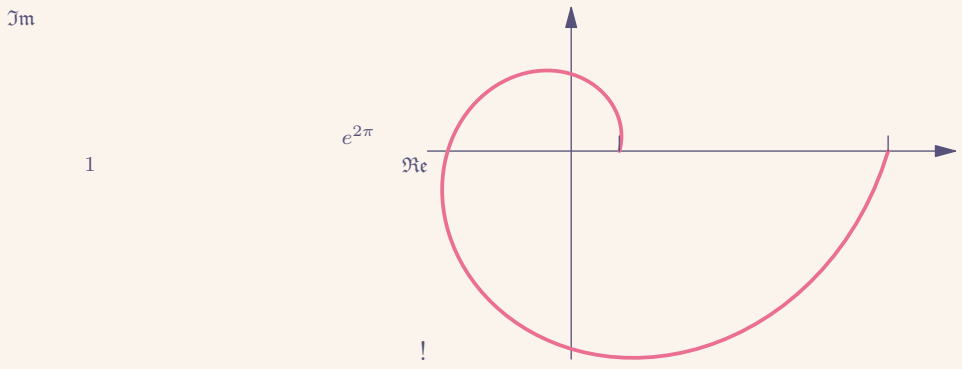
$$\forall x \in [0, 2\pi[, \begin{cases} \mathfrak{Re}(f)'(x) = e^x \cos(x) - e^x \sin(x) \\ \mathfrak{Im}(f)'(x) = e^x \cos(x) + e^x \sin(x) \end{cases}$$

Donc,

$$\forall x \in [0, 2\pi[, f'(x) = e^x(\cos(x) - \sin(x)) + ie^x(\sin(x) + \cos(x))$$

Remarque :
On peut représenter f de la façon suivante.

$$\begin{aligned} f : [0, 2\pi[&\longrightarrow \mathbb{C} \\ t &\longmapsto e^{(1+i)t} \end{aligned}$$



Proposition : Soient u et v deux fonctions dérivables sur $D \subset \mathbb{R}$ à valeurs dans $\mathbb{C}$

1. $u+v$ dérivable et $(u+v)' = u' + v'$
2. uv dérivable et $(uv)' = u'v + v'u$
3. Si $v \neq 0$, $\dfrac{u}{v}$ dérivable et $\left(\dfrac{u}{v}\right) = \dfrac{u'v - v'u}{v^2}$

Preuve :

On pose $\begin{cases} a = \mathfrak{Re}(u) \\ b = \mathfrak{Im}(u) \end{cases}$ et $\begin{cases} c = \mathfrak{Re}(v) \\ d = \mathfrak{Im}(v) \end{cases}$

1. $\begin{cases} \mathfrak{Re}(u+v) = a + c \\ \mathfrak{Im}(u+v) = b + d \end{cases}$ donc $\begin{cases} \mathfrak{Re}(u+v)' = a' + c' \\ \mathfrak{Im}(u+v)' = b' + d' \end{cases}$ Donc,

$$\begin{aligned} (u+v)' &= a' + c' + i(b' + d') \\ &= (a' + ib') + (c' + id') \\ &= u' + v' \end{aligned}$$

2. $\begin{cases} \mathfrak{Re}(uv) = ac - bd \\ \mathfrak{Im}(uv) = ad + bc \end{cases}$ donc $\mathfrak{Re}(uv)$ et $\mathfrak{Im}(uv)$ sont dérivables et

$$\begin{cases} \mathfrak{Re}(uv)' = a'c + c'a - b'd - d'b \\ \mathfrak{Im}(uv)' = a'd + d'a + b'c + c'b \end{cases}$$

Donc,

$$(uv)' = a'c + c'a - b'd - d'b + i(a'd + d'a + b'c + c'b)$$

Or,

$$\begin{cases} u'v = (a' + ib')(c + id) = a'c - b'd + i(b'c + a'd) \\ v'u = (a + ib)(c' + id') = ac' - bd' + i(bc' + ad') \end{cases}$$

Donc,

$$(uv)' = u'v + v'u$$

3. On suppose que

$$\forall x \in D, v(x) \neq 0$$

On a donc

$$\forall x \in D, \frac{u}{v} = \frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}$$

C'est plus simple de voir $\dfrac{u}{v}$ comme le produit de u et de $\dfrac{1}{v}$

$$\frac{1}{v} = \frac{1}{c+id} = \frac{c-id}{c^2+d^2}$$

$\underbrace{\dfrac{c}{c^2+d^2}}_{=\mathfrak{Re}\left(\frac{1}{v}\right)}$ et $\underbrace{-\dfrac{d}{c^2+d^2}}_{=\mathfrak{Im}\left(\frac{1}{v}\right)}$ sont dérivables donc $\dfrac{1}{v}$ aussi

$$\begin{cases} \mathfrak{Re}\left(\dfrac{1}{v}\right)' = \left(\dfrac{c}{c^2+d^2}\right)' = \dfrac{c'(c^2+d^2) - c(2cc'+2dd')}{(c^2+d^2)^2} \\ \mathfrak{Im}\left(\dfrac{1}{v}\right)' = \left(-\dfrac{d}{c^2+d^2}\right)' = \dfrac{-d'(c^2+d^2) + d(2cc'+2dd')}{(c^2+d^2)^2} \end{cases}$$

Donc, d'une part,

$$\begin{aligned} \left(\frac{1}{v}\right)' &= \frac{c'(c^2+d^2) - c(2cc'-2dd') - id'(c^2+d^2) + d(2cc'+2dd')}{(c^2+d^2)^2} \\ &= \frac{(c^2+d^2)(c'-id') + (2cc'+2dd')(-c+id)}{(c^2+d^2)^2} \\ &= \frac{-c'c^2 + c'd^2 - 2cdd' + i(2cc'd - d'c^2 + d^2d')}{(c^2+d^2)^2} \end{aligned}$$

D'autre part,

$$\begin{aligned} \frac{-v'}{v^2} &= \frac{-c'-d'i}{(c+di)^2} \\ &= \frac{-(c'+id')(c-id)^2}{(c^2+d^2)^2} \\ &= -\frac{(c'+id')(c^2-2icd-d^2)}{(c^2+d^2)^2} \\ &= \frac{-c'c^2 + c'd^2 - 2cdd' + i(2cc'd - d'c^2 + d'd^2)}{(c^2+d^2)^2} \\ &= \left(\frac{1}{v}\right)' \end{aligned}$$

Donc, $\dfrac{u}{v}$ dérivable et

$$\left(\frac{u}{v}\right)' = u'\left(\frac{1}{v}\right) + u\left(\frac{1}{v}\right)' = \frac{u'}{v} - \frac{uv'}{v^2} = \frac{u'v - uv'}{v^2}$$

□

Proposition : Soit $v : D \to \mathbb{R}$ et $u : \mathbb{R} \to \mathbb{C}$ deux fonctions dérivables (avec $D \subset \mathbb{R}$).
Alors, $u \circ v$ est dérivable et

$$(u \circ v)' = (u' \circ v) \times v'$$

Preuve :
On pose $u = a + ib$ avec $\begin{cases} a = \mathfrak{Re}(u) \\ b = \mathfrak{Im}(u) \end{cases}$ donc,

$$\forall x \in \mathbb{R}, u(x) = a(x) + ib(x)$$

Donc,

$$\forall x \in D, (u \circ v)(x) = a(v(x)) + ib(v(x))$$

Donc,

$$\begin{aligned} \mathfrak{Re}(u \circ v) &= a \circ v \\ \mathfrak{Im}(u \circ v) &= b \circ v \end{aligned}$$

Or,

$$\begin{aligned} \mathfrak{Re}(u \circ v)' &= (a \circ v)' = (a' \circ v) \times v' \\ \mathfrak{Im}(u \circ v)' &= (b \circ v)' = (b' \circ v) \times v' \end{aligned}$$

D'où

$$\begin{aligned} (u \circ v)' &= (a' \circ v) \times v' + i(b' \circ v) \times v' \\ &= (a' \circ v + ib' \circ v) \times v' \\ &= ((a' + ib') \circ v) \times v' \\ &= (u' \circ v) \times v' \end{aligned}$$

□

Proposition : Soit $u : D \to \mathbb{C}$ et $f : \begin{array}{ccc} D & \longrightarrow & \mathbb{C} \\ x & \longmapsto & e^{u(x)} \end{array}$
Alors, f est dérivable sur D et

$$\forall x \in D, f'(x) = u'(x)e^{u(x)}$$

Preuve :
On pose $\begin{cases} a = \mathfrak{Re}(u) \\ b = \mathfrak{Im}(u) \end{cases}$ donc

$$\begin{aligned} \forall x \in D, f(x) &= e^{u(x)} \\ &= e^{a(x)+ib(x)} \\ &= e^{a(x)}(\cos(b(x)) + i\sin(b(x))) \end{aligned}$$

Donc, $\begin{cases} \mathfrak{Re}(f) : x \mapsto e^{a(x)}\cos(b(x)) \\ \mathfrak{Im}(f) : x \mapsto e^{a(x)}\sin(b(x)) \end{cases}$
a, b, cos, sin, exp sont dérivables donc $\mathfrak{Re}(f)$ et $\mathfrak{Im}(f)$ aussi donc f est dérivable.

□

Chapitre 3

Étude de fonctions

Étudier une fonction c'est déterminer tous les éléments (tangentes, asymptotes) qui permettent d'obtenir l'allure de la courbe représentative de la fonction.

Exemple :

$$f : x \mapsto \frac{x^2 - 2x + 3}{x^2 + 2x - 3}$$

1. On détemine le domaine de définition de la fonction f.
   Soit $x \in \mathbb{R}$.

   $$x^2 + 2x - 3 = 0 \iff x \in \{-3, 1\} \quad \text{car} \begin{cases} -3 + 1 = -2 = -\dfrac{b}{a} \\ -3 \times 1 = -3 = \dfrac{c}{a} \end{cases}$$

   Donc f est définie sur $\mathcal{D}$ avec $\mathcal{D} =]-\infty, -3[\cup]-3, -1[\cup]-1, +\infty[$
2. Asymptotes et limites
   Soit $x \in \mathcal{D}$

   $$f(x) = \frac{\cancel{x^2}\left(1 - \frac{2}{x} + \frac{3}{x^2}\right)}{\cancel{x^2}\left(1 + \frac{2}{x} - \frac{3}{x^2}\right)} \xrightarrow[x \to \pm\infty]{} 1$$

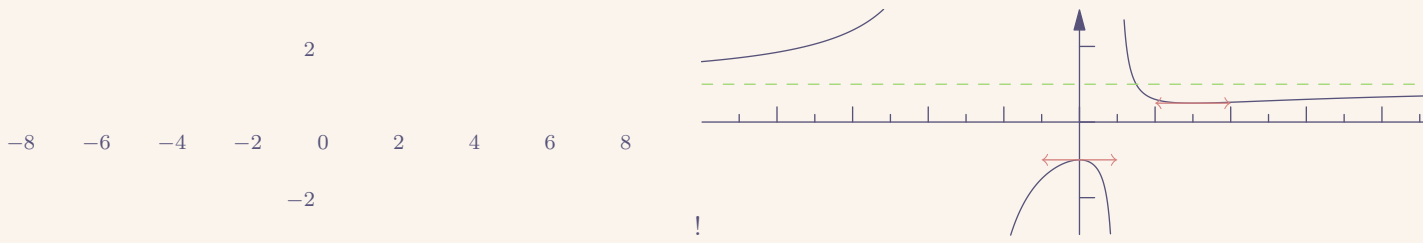
   $$\left.\begin{array}{l} x^2 - 2x + 3 \xrightarrow[x \to -3]{} 9 + 6 + 3 = 18 \\ x^2 + 2x - 3 \xrightarrow[x \to -3]{} 0 \end{array}\right\} \text{ donc } \begin{cases} f(x) \xrightarrow[\substack{x \to -3 \\ <}]{} +\infty \\ f(x) \xrightarrow[\substack{x \to -3 \\ >}]{} -\infty \end{cases}$$

   $$\left.\begin{array}{l} x^2 - 2x + 3 \xrightarrow[x \to 1]{} 2 \\ x^2 + 2x - 3 \xrightarrow[x \to 1]{} 0 \end{array}\right\} \text{ donc } \begin{cases} f(x) \xrightarrow[\substack{x \to 1 \\ <}]{} -\infty \\ f(x) \xrightarrow[\substack{x \to 1 \\ >}]{} +\infty \end{cases}$$

3. f est dérivable sur $\mathscr{D}$ et

$$\begin{aligned}\forall x \in \mathscr{D}, f'(x) &= \frac{2(x-1)(x^2+2x-3) - 2(x^2-2x+3)(x+1)}{(x^2+2x-3)^2} \\ &= \frac{2(2x^2-6x)}{(x^2-2x+3)^2} \\ &= \frac{4x(x-4)}{(x^2-2x+3)^2}\end{aligned}$$

x	$+\infty$		-3		0		1		3		$+\infty$
$f'(x)$		$+$	‖	$+$	0	$-$	‖	$-$	0	$+$	
f	1	↗	$+\infty$ ‖ $-\infty$	↗	-1	↘	$-\infty$ ‖ $+\infty$	↘	$\frac{1}{2}$	↗	1



!

1 Calculs de limites

Rappel :
Soient f et g deux fonctions et $a \in \mathbb{R} \cup \{-\infty, +\infty\}$.

On ne connaît pas, à l'avance, les limites de

— $f(x) - g(x)$ si $\begin{cases} f(x) \xrightarrow[x \to a]{} +\infty \\ g(x) \xrightarrow[x \to a]{} +\infty \end{cases}$ (“$\infty - \infty$”)

— $\dfrac{f(x)}{g(x)}$ si $\begin{cases} f(x) \xrightarrow[x \to a]{} 0 \\ g(x) \xrightarrow[x \to a]{} 0 \end{cases}$ (“$\frac{0}{0}$”)

— $\dfrac{f(x)}{g(x)}$ si $\begin{cases} f(x) \xrightarrow[x \to a]{} \pm\infty \\ g(x) \xrightarrow[x \to a]{} \pm\infty \end{cases}$ (“$\frac{\infty}{\infty}$”)

— $f(x) \times g(x)$ si $\begin{cases} f(x) \xrightarrow[x \to a]{} 0 \\ g(x) \xrightarrow[x \to a]{} \pm\infty \end{cases}$ (“$0 \times \infty$”)

Exemple :
$\lim\limits_{n\to+\infty}\left(1+\dfrac{1}{n}\right)^n$?

$$\forall n\in\mathbb{N},\left(1+\frac{1}{n}\right)^n=e^{n\ln\left(1+\frac{1}{n}\right)}$$

et

$$\begin{cases}\ln\left(1+\dfrac{1}{n}\right)\xrightarrow[n\to+\infty]{}0\\ n\xrightarrow[n\to+\infty]{}+\infty\end{cases}$$

donc c'est une forme indéterminée.

Proposition :
Si $\begin{cases}f(x)\xrightarrow[x\to a]{}1\\ g(x)\xrightarrow[x\to a]{}\pm\infty\end{cases}$ alors, on ne sait pas à l'avance calculer $\lim\limits_{x\to a}\big(f(x)\big)^{g(x)}$. □

Définition : Soient f et g deux fonctions et $a\in\overline{\mathbb{R}}$ où $\overline{\mathbb{R}}=\mathbb{R}\cup\{+\infty,-\infty\}$.

On dit que f et g sont <u>équivalentes au voisinage de a</u> (ou éqivalentes en a) s'il existe une fonction u telle que

$$\begin{cases}f=g\times u\\ u(x)\xrightarrow[x\to a]{}1\end{cases}$$

On note alors $f\underset{a}{\sim}g$ ou $f(x)\underset{x\to a}{\sim}g(x)$.

Proposition : Un polynôme est équivalent en $\pm\infty$ à son terme de plus haut degré.

Preuve :
Soit $P:x\mapsto\sum\limits_{k=0}^{n}a_kx^k$ avec $a_n\neq0$. On pose $Q:x\mapsto a_nx^n$.

$$\begin{aligned}\forall x \in \mathbb{R}, P(x) &= a_n x^n \left(\sum_{k=0}^{n} \frac{a_k x^k}{a_n x^n} \right) \\ &= Q(x) \left(1 + \sum_{k=0}^{n-1} \frac{a_k}{a_n} \times \underbrace{\left(\frac{1}{x^{n-k}} \right)}_{u(x)} \right) \\ &= Q(x)\, u(x)\end{aligned}$$

On a $u(x) \xrightarrow[x \to \pm\infty]{} 1$ donc $P(x) \underset{x \to +\infty}{\sim} Q(x)$. □

Proposition : Un polynôme est équivalent en 0 à sont terme de plus bas degré.

Preuve :
À faire □

Remarque :
Soient f et g deux fonctions définies au voisinage de a tel que

$$\forall x \in I, g(x) \neq 0$$

où I est un intervalle
- qui contient a si $a \in \mathbb{R}$,
- dont une borne est a si $a = \pm\infty$.

Alors,

$$f \underset{a}{\sim} g \iff \frac{f(x)}{g(x)} \xrightarrow[\substack{x \to a \\ \neq}]{} 1.$$

Exemple :
$x^2 + x^3 \underset{x \to 0}{\sim} x^2$ car $\dfrac{x^2 + x^3}{x^2} = 1 + x \xrightarrow[x \to 0]{} 1$.

Exemple :
Soit f une fonction.

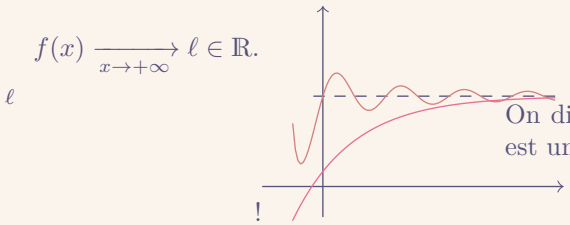
$$f \underset{0}{\sim} 0 \iff \exists I \text{ voisinage de } a, \forall x \in I, f(x) = 0.$$

2 Asymptotes, branches paraboliques et prolongement par continuité

Limite en $+\infty$:

Cas 1

$f(x) \xrightarrow[x\to+\infty]{} \ell \in \mathbb{R}$.



On dit que la droite d'équation $y = \ell$ est une asymptote horizontale.

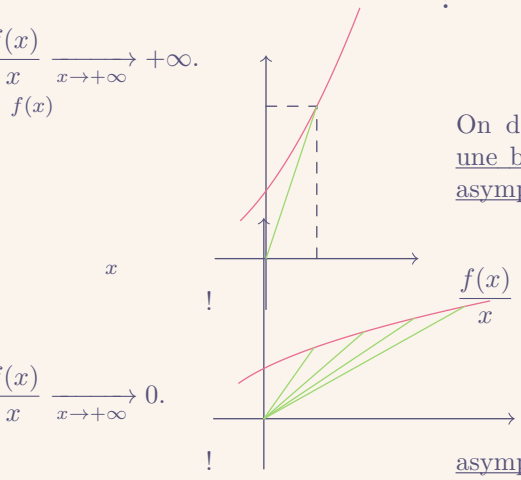
2

$f(x) \xrightarrow[x\to+\infty]{} \pm\infty$ dans ce cas, on cherche $\lim\limits_{x\to+\infty} \dfrac{f(x)}{x}$.

cas 1 $\dfrac{f(x)}{x}$ n'a pas de limite en $+\infty$.

?

cas 2 $\dfrac{f(x)}{x} \xrightarrow[x\to+\infty]{} +\infty$.

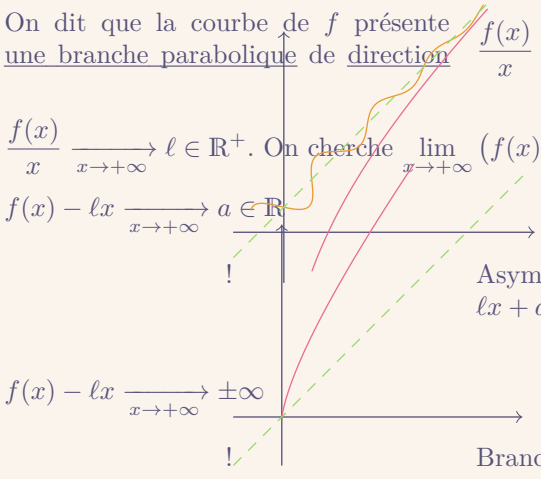


On dit que la courbe de f présente une branche parabolique de direction asymptotique l'axee des ordonées.

$\dfrac{f(x)}{x}$ est la pente de la droite verte.

cas 3 $\dfrac{f(x)}{x} \xrightarrow[x\to+\infty]{} 0$.

On dit que la courbe de f présente une branche parabolique de direction asymptotique l'axe des ordonées.



$\dfrac{f(x)}{x}$ est la pente de la droite verte.

cas 4 $\dfrac{f(x)}{x} \xrightarrow[x\to+\infty]{} \ell \in \mathbb{R}^+$. On cherche $\lim\limits_{x\to+\infty} \big(f(x) - \ell x\big)$.

us cas 1 $f(x) - \ell x \xrightarrow[x\to+\infty]{} a \in \mathbb{R}$

Asymptote oblique d'équation $y = \ell x + a$.

us cas 2 $f(x) - \ell x \xrightarrow[x\to+\infty]{} \pm\infty$

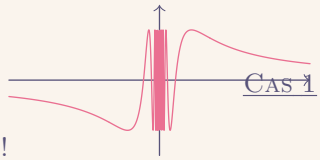
Branche parabolique de direction asymptotique la droite d'équation $y = \ell x$.

us cas 2 $f(x) - \ell x$ n'a pas de limite

?

Limite en $a \in \mathbb{R}$:

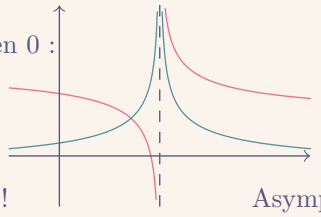
On cherche $\lim\limits_{x \to a} f(x)$.



Cas 1

Pas de limite

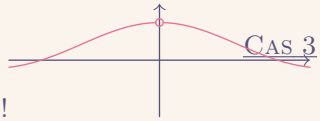
ex $x \mapsto \sin\left(\dfrac{1}{x}\right)$ en 0 :



$f(x) \xrightarrow[x \to a]{} \pm\infty$

Cas 2

Asymptote verticale d'équation $x = a$.

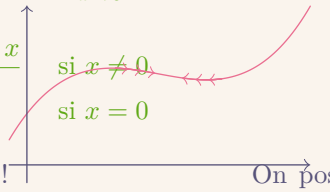


Cas 3

$f(x) \xrightarrow[x \to a]{} \ell \in \mathbb{R}$.

ex $f : x \mapsto \dfrac{\sin x}{x}$ $f(x) \xrightarrow[x \to 0]{} 1$, dans ce cas, on pose

$$f(x) = \begin{cases} \dfrac{\sin x}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases}$$



On pose $f(a) = \ell$. On dit que l'on a prolongé par continuité la fonction f.

Chapitre 4

Fonctions usuelles

1 Logarithme népérien

Théorème (théorème fondamental de l'analyse) **:** Soit f une fonction continue sur un intervalle I. Alors il existe F dérivable sur I telle que

$$\forall x \in I, F'(x) = f(x).$$

Preuve (c.f. chapitre 5 : calcul intégral) *:*

□

Définition : La fonction $\underline{\ln}$ est l'unique primitive sur $\mathbb{R}_\star^+$ de $x \mapsto \dfrac{1}{x}$ qui s'annule en 1.

Proposition :
1. $\ln 1 = 0$;
2. ln est dérivable sur $\mathbb{R}_+^\star$ et

$$\forall x > 0, \ln' x = \frac{1}{x}.$$

□

Corollaire :

$$\forall x > 0, \ln x = \int_1^x \frac{\mathrm{d}t}{t}.$$

Preuve :
Soit

$$\begin{aligned}\varphi : \mathbb{R}_\star^+ &\longrightarrow \mathbb{R}\\ x &\longmapsto \int_1^x \frac{\mathrm{d}t}{t}.\end{aligned}$$

On a

$$\begin{aligned}\forall x > 0, \varphi(x) &= [\ln t]_1^x\\ &= \ln x - \ln 1\\ &= \ln x\end{aligned}$$

□

Remarque :

$$\begin{aligned}u : \mathbb{R}_\star^- &\longrightarrow \mathbb{R}\\ x &\longmapsto \ln(-x)\end{aligned}$$

u est dérivable sur $\mathbb{R}_\star^-$ et

$$\forall x < 0, u'(x) = \ln'(-x) \times (-1) = \frac{-1}{-x} = \frac{1}{x}.$$

Donc u est une primite de $x \mapsto \dfrac{1}{x}$ sur $\mathbb{R}_\star^-$.

Soit $v : \begin{array}{ccc}\mathbb{R}^\star & \longrightarrow & \mathbb{R}\\ x & \longmapsto & \ln\big(|x|\big).\end{array}$ $|x|$ est dérivable sur $\mathbb{R}^\star$ donc v aussi.

$$\begin{aligned}\forall x > 0, v(x) &= \ln x\\ \text{donc } \forall x > 0, v'(x) &= \frac{1}{x}.\end{aligned}$$

$$\begin{aligned}\forall x < 0, v(x) &= \ln(-x) = u(x)\\ \text{donc } \forall x < 0, v'(x) &= \frac{1}{x}.\end{aligned}$$

Donc, $\forall x \in \mathbb{R}^\star, v'(x) = \dfrac{1}{x}$. Ainsi, v est <u>une</u> primitive de $x \mapsto \dfrac{1}{x}$ sur $\mathbb{R}^\star$ mais cette primitive n'est pas unique :

$$\begin{aligned}w : \mathbb{R}^\star &\longrightarrow \mathbb{R}\\ x &\longmapsto \begin{cases}1 + \ln x & \text{si } x > 0\\ \ln(-x) - 3 & \text{si } x < 0\end{cases}\end{aligned}$$

est une autre primitive de $x \mapsto \dfrac{1}{x}$ sur $\mathbb{R}^\star$.

Corollaire : ln est strictement croissante sur $\mathbb{R}_\star^+$.

Preuve :

$$\forall x > 0, \ln' x = \frac{1}{x} > 0.$$

□

Proposition : Soit f une fonction croissante sur $]a, b[$ avec $\begin{cases} a \in \mathbb{R} \cup \{-\infty\} \\ b \in \mathbb{R} \cup \{+\infty\}. \end{cases}$ et $a < b$.

1. Si f est majorée, $\lim\limits_{\substack{x \to b \\ <}} f(x) \in \mathbb{R}$.
2. Si f n'est pas majorée, $\lim\limits_{\substack{x \to b \\ <}} f(x) = +\infty$.
3. Si f est minorée, $\lim\limits_{\substack{x \to a \\ >}} f(x) \in \mathbb{R}$.
4. Si f n'est pas minorée, $\lim\limits_{\substack{x \to a \\ >}} f(x) = -\infty$.

□

Proposition :

$$\forall a, b \in \mathbb{R}_\star^+, \ln(ab) = \ln a + \ln b.$$

Preuve :
Soit $a > 0$ et u : $\begin{array}{ccc} \mathbb{R}_\star^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln(ax). \end{array}$

u est dérivable sur $\mathbb{R}_\star^+$ et

$$\forall x > 0, u'(x) = \ln'(ax) \times a = \frac{a}{ax} = \frac{1}{x}$$

Donc u est une primitive de $x \mapsto \dfrac{1}{x}$ sur $\mathbb{R}_\star^+$. Comme $\mathbb{R}_\star^+$ est un intervalle, il existe $C \in \mathbb{R}$ telle que

$$\forall x \in \mathbb{R}_\star^+, u(x) = \ln x + C.$$

En particulier,

$$\begin{array}{ccc} u(1) & = & \ln 1 + C \\ \| & & \| \\ \ln a & = & C \end{array}$$

Donc

$$\forall x > 0, \ln(ax) = \ln x + \ln a.$$

□

Corollaire : Soit $a > 0$ et $n \in \mathbb{Z}$. Alors $\ln(a^n) = n \ln(a)$.

Preuve (par récurrence sur n) *:*
Pour $n \in \mathbb{N}$, on pose

$$\mathcal{P}(n) : \text{“ } \ln(a^n) = n \ln a \text{”}.$$

— Avec $n = 0$, $\ln(a^n) = \ln 1 = 0 = 0 \times \ln a$
— Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}(n)$ vraie.

$$\begin{aligned} \ln(a^{n+1}) &= \ln(a \times a^n) \\ &= \ln a + \ln(a^n) \\ &= \ln a + n \ln a \\ &= (n+1) \ln a \end{aligned}$$

Donc

$$\forall n \in \mathbb{N}, \ln(a^n) = n \ln a.$$

—

$$\ln\left(\frac{1}{a}\right) + \ln a = \ln\left(\frac{1}{a} \times a\right) = \ln 1 = 0$$

donc $\ln \dfrac{1}{a} = -\ln a$
— Soit $n \in \mathbb{Z}^-$. Alors,

$$\ln(a^n) = \ln\left(\left(\frac{1}{a}\right)^{-n}\right) = -n \ln \frac{1}{a} = n \ln a.$$

□

Corollaire :

$$\begin{cases} \lim\limits_{x\to+\infty} \ln x = +\infty \\ \lim\limits_{x\to 0} \ln x = -\infty \end{cases}$$

Preuve :
Comme ln est croissante sur $]0,+\infty[$, on sait que $\lim\limits_{x\to+\infty} \ln x$ existe. C'est un réle ou $+\infty$.

Supposons cette limite réelle : on pose $\lim\limits_{x\to+\infty} \ln x = \ell \in \mathbb{R}$. Alors $\lim\limits_{n\to+\infty} \ln(2^n) = \ell$ car $2^n \xrightarrow[n\to+\infty]{} +\infty$.

Or,

$$\forall x \in \mathbb{N}, \ln(2^n) = n \ln 2$$

et $2 > 1$ donc $\ln 2 > \ln 1 = 0$ donc $n \ln 2 \xrightarrow[n\to+\infty]{} +\infty$: une contradiction.

Donc $\ln x \xrightarrow[x\to+\infty]{} +\infty$.

$$\forall x > 0, \ln x = -\ln \frac{1}{x} \xrightarrow[\substack{x\to 0\\ >}]{} -\infty$$

car $\dfrac{1}{x} \xrightarrow[\substack{x\to 0\\ >}]{} +\infty$. □

Proposition :

$$\lim_{x\to+\infty} \frac{\ln x}{x} = 0.$$

Preuve :
Soit $x \geqslant 1$. On a

$$0 = \ln 1 \leqslant \ln x = \int_1^x \frac{1}{t}\,\mathrm{d}t.$$

et

$$\forall t \in [1,x], t \geqslant \sqrt{t}$$

donc

$$\forall t \in [1,x], \frac{1}{t} \leqslant \frac{1}{\sqrt{t}}.$$

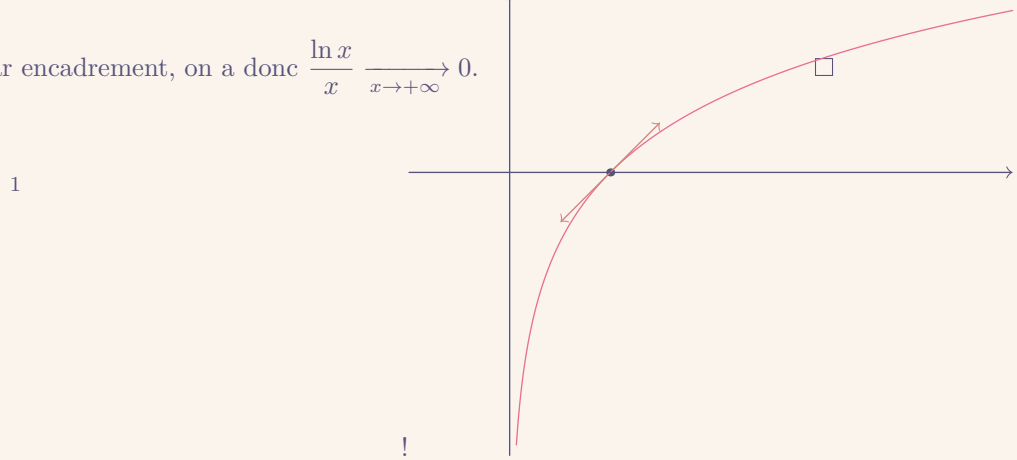
Par croissance de l'intégrale, on en déduit que

$$\ln x = \int_0^1 \frac{1}{t}\,\mathrm{d}t \leqslant \int_1^x \frac{1}{\sqrt{t}}\,\mathrm{d}t = \left[2\sqrt{t}\right]_1^x = 2\sqrt{x} - 2.$$

Ainsi,

$$\forall x \geqslant 1, 0 \leqslant \frac{\ln x}{x} \leqslant \underbrace{2\left(\frac{1}{\sqrt{x}} - \frac{1}{x}\right)}_{\substack{\longrightarrow 0 \\ x\to+\infty}}.$$

Par encadrement, on a donc $\dfrac{\ln x}{x} \xrightarrow[x\to+\infty]{} 0$. □



2 Exponentielle

Proposition : $\ln : \mathbb{R}_+^\star \to \mathbb{R}$ est bijective.

Preuve :
ln est continue sur $\mathbb{R}_\star^+$ (car elle est dérivable) et strictement croissante, donc elle établit une bijection de $]0, +\infty[$ dans $\left]\lim\limits_{\substack{x\to 0 \\ >}} \ln x, \lim\limits_{x\to+\infty} \ln x\right[=]-\infty, +\infty[= \mathbb{R}$. □

Définition : La fonction exponentielle est la réciproque du logarithme népérien. On la note exp.

Proposition :
1. $\exp : \mathbb{R} \to \mathbb{R}_+^\star$ est dérivable et $\forall x \in \mathbb{R}, \exp'(x) = \exp(x)$;
2. $\begin{cases} \lim\limits_{x\to+\infty} \exp(x) = +\infty; \\ \lim\limits_{x\to-\infty} \exp(x) = 0; \end{cases}$
3. $\lim\limits_{x\to+\infty} \dfrac{\exp(x)}{x} = +\infty$;
4. $\forall a, b \in \mathbb{R}, \exp(a+b) = \exp(a) \times \exp(b)$.

Preuve : 1. Soit $x \in \mathbb{R}$.

$$\ln'\big(\exp(x)\big) = \frac{1}{\exp(x)} \neq 0$$

donc exp est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, \exp'(x) = \frac{1}{\ln'\big(\exp(x)\big)} = \exp(x).$$

2. — $\ln u \xrightarrow[u\to 0]{} -\infty$ donc $\exp(x) \xrightarrow[x\to-\infty]{} 0$
   — $\ln u \xrightarrow[u\to+\infty]{} +\infty$ donc $\exp(x) \xrightarrow[x\to+\infty]{} +\infty$.
3. Pour $x \in \mathbb{R}$, on pose $x = \ln u \ \Big(\iff u = \exp(x)\Big)$. Donc

$$\frac{\exp(x)}{x} = \frac{u}{\ln u} = \frac{1}{\frac{\ln u}{u}} \xrightarrow[u\to+\infty]{} +\infty.$$

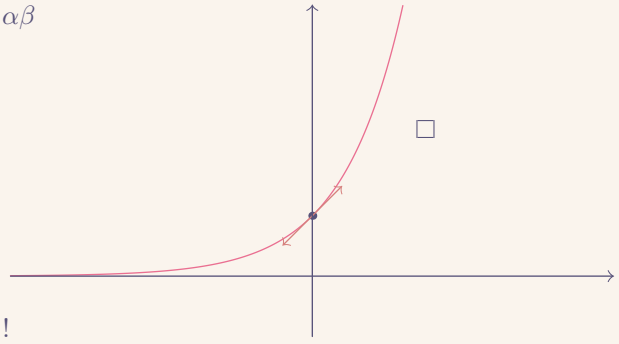
4. Soient $a, b \in \mathbb{R}$. On pose $\begin{cases} a = \ln \alpha, \\ b = \ln \beta. \end{cases}$

   On a $\exp(a) \times \exp(b) = \alpha\beta$ et

$$\begin{aligned} \exp(a+b) &= \exp\big(\ln(\alpha) + \ln(\beta)\big) \\ &= \exp\big(\ln(\alpha\beta)\big) \\ &= \alpha\beta \end{aligned}$$

□

1



!

3 Fonctions puissances

Remarque (Rappel) :

$$\forall a \in \mathbb{R}, \forall x > 0, x^a = \exp(a \ln x).$$

En particulier, en posant $x = e = \exp(1)$, on a donc

$$\forall a \in \mathbb{R}, e^a = \exp(a).$$

Remarque (Notation) :

Soit $a \in \mathbb{R}$. Pour ce chapitre, on note p_a : $\begin{array}{ccc} \mathbb{R}_+^\star & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^a. \end{array}$

Proposition : Soit $a \in \mathbb{R}$. p_a est dérivable sur $\mathbb{R}_\star^+$ et

$$\forall x > 0, p_a'(x) = ax^{a-1}.$$

Preuve :

$$\forall x \in \mathbb{R}_\star^+, p_a(x) = e^{a \ln x}.$$

Or, ln, exp, $x \mapsto ax$ sont dérivables sur leur domaine de définition donc p_a aussi et

$$\forall x > 0, p_a'(x) = \frac{a}{x} e^{a \ln x} = \frac{a}{x} x^a = ax^{a-1}.$$

□

Corollaire :
1. $\forall a \in \mathbb{R}_-^\star$, p_a est strictement décroissante.
2. $\forall a \in \mathbb{R}_+^\star$, p_a est strictement croissante.
3. p_0 est la fonction constante égale à 1.

Preuve :
Pour tout $x > 0$, $p_a'(x)$ est du signe de a puisque

$$x^{a-1} = e^{(a-1)\ln x} > 0.$$

□

Proposition :
1. Si $a > 0$, $\begin{cases} p_a(x) \xrightarrow[x \to +\infty]{} +\infty, \\ p_a(x) \xrightarrow[\substack{x \to 0 \\ >}]{} 0; \end{cases}$
2. Si $a < 0$, $\begin{cases} p_a(x) \xrightarrow[x \to +\infty]{} 0, \\ p_a(x) \xrightarrow[\substack{x \to 0 \\ >}]{} +\infty; \end{cases}$
3. Si $a = 0$, $\begin{cases} p_a(x) \xrightarrow[x \to +\infty]{} 1, \\ p_a(x) \xrightarrow[\substack{x \to 0 \\ >}]{} 1. \end{cases}$

Preuve :
À faire □

Proposition : On suppose $a > 0$.

1. Si $a > 1$, alors $\dfrac{p_a(x)}{x} \xrightarrow[x\to+\infty]{} +\infty$;
2. Si $a < 1$, alors $\dfrac{p_a(x)}{x} \xrightarrow[x\to+\infty]{} 0$;
3. Si $a = 1$, alors $\forall x > 0, p_a(x) = x$.

Preuve :

$$\forall x > 0, \frac{p_a(x)}{x} = \frac{x^a}{x} = x^{a-1}.$$

□

Proposition : On suppose $a > 0$. On peut prolonger p_a par continuité en 0 en posant $p_a(0) = 0$.

1. Si $a > 1$, alors $p'_a(x) \xrightarrow[\substack{x\to 0\\ >}]{} 0$;
2. Si $a < 1$, alors $p'_a(x) \xrightarrow[\substack{x\to 0\\ >}]{} +\infty$;

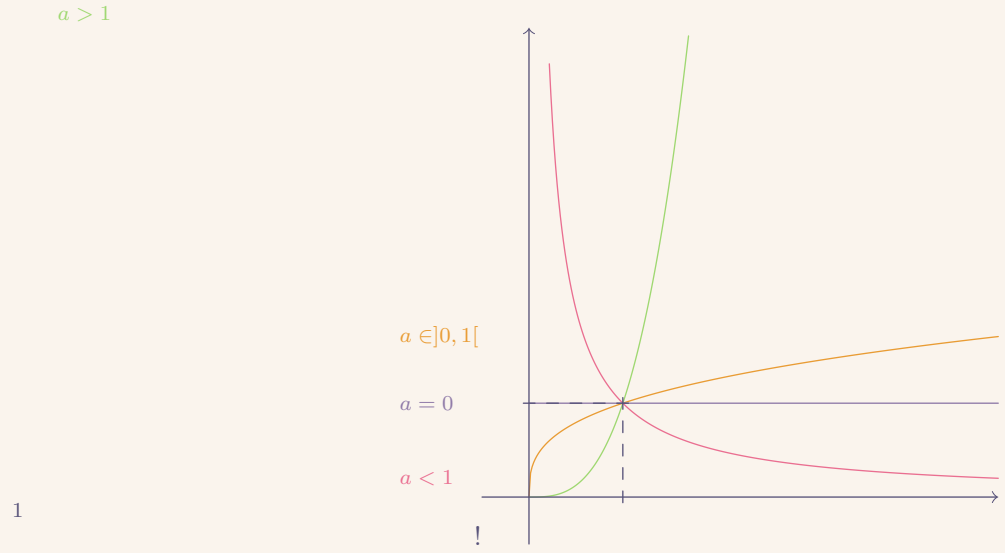
Preuve : 1. On suppose $a > 1$. Alors,

$$\forall x > 0, p'_a(x) = ax^{a-1} \xrightarrow[\substack{x\to 0\\ >}]{} 0.$$

2. On suppose $a < 1$.

$$\forall x > 0, p'_a(x) = ax^{a-1} \xrightarrow[\substack{x\to 0\\ >}]{} +\infty.$$

□



Proposition (croissances comparées) **:** Soient $a, b \in \mathbb{R}_\star^+$. Alors,

$$\lim_{x\to+\infty} \frac{\ln^a(x)}{x^b} = 0.$$

Exemple :
Si on ne dispose pas de la formule :

$$\lim_{x\to+\infty} \frac{\ln x}{\sqrt{x}} = \ ?$$

On a

$$\frac{\ln x}{\sqrt{x}} = \frac{2\ln(\sqrt{x})}{\sqrt{x}} = \underbrace{2\,\frac{\ln u}{u}}_{\xrightarrow[u\to+\infty]{}0} \quad \text{avec } u = \sqrt{x} \xrightarrow[x\to+\infty]{} +\infty.$$

Preuve :

$$\forall x > 1,\ \frac{\ln^a(x)}{x^b} = \frac{e^{a\ln(\ln x)}}{e^{b\ln x}} = e^{a\ln(\ln x) - b\ln x}.$$

Or $\ln(\ln x) = \underset{x\to+\infty}{o}(\ln x)$ car $\dfrac{\ln(\ln x)}{\ln x} = \underbrace{\dfrac{\ln u}{u}}_{\xrightarrow[u\to+\infty]{}0}$ avec $u = \ln x \xrightarrow[x\to+\infty]{} +\infty$.

Donc,

$$\frac{\ln^a(x)}{x^b} = e^{o(\ln x) - b\ln x} = e^{\ln(x)\left(-b+o(1)\right)} \xrightarrow[x\to+\infty]{} 0.$$

car $\begin{cases} -b + o(1) \xrightarrow[x\to+\infty]{} -b < 0 \\ \ln x \xrightarrow[x\to+\infty]{} +\infty. \end{cases}$ □

Corollaire :

$$x \ln x \xrightarrow[\substack{x\to 0 \\ >}]{} 0.$$

Preuve :
Pour $x \in]0,1[$, on pose $u = \dfrac{1}{x} \xrightarrow[\substack{x\to 0 \\ >}]{} +\infty$.

Donc,

$$\begin{aligned} \forall x \in]0,1[, x \ln x &= \frac{\ln\left(\frac{1}{u}\right)}{u} \\ &= -\frac{\ln u}{u} \xrightarrow[u\to+\infty]{} 0. \end{aligned}$$

□

Corollaire : Soit $a > 0$. Alors

$$\lim_{x\to+\infty} \frac{x^a}{e^x} = 0.$$

Preuve :
On fait le changement de variables $u = e^x \xrightarrow[x\to+\infty]{} +\infty$.

$$\forall x > 0, \frac{x^a}{e^x} = \frac{\ln^a u}{u} \xrightarrow[u\to+\infty]{} 0.$$

□

4 Exponentielle et logarithme de base a

Définition : Soit $a > 0$. L'application $\exp_a : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}_\star^+ \\ x & \longmapsto & a^x = e^{x \ln a} \end{array}$ est appelée exponentielle de base a.

Remarque :

L'exponentielle de base e est l'exponentielle classique.

Proposition : $\exp_a$ est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, \exp_a'(x) = \ln(a)\exp_a(x) = a^x \ln a.$$

□

Corollaire :
1. Si $a \in]0,1[$, alors $\exp_a$ est strictement décroissante.
2. Si $a > 1$, alors $\exp_a$ est strictement croissante.
3. Si $a = 1$, alors $\exp_a(x) = 1$ pour tout $x \in \mathbb{R}$.

□

Proposition :
1. Si $a \in]0,1[$,
   - $\exp_a(x) \xrightarrow[x\to+\infty]{} 0$,
   - $\exp_a(x) \xrightarrow[x\to-\infty]{} +\infty$,
   - $\dfrac{\exp_a(x)}{x} \xrightarrow[x\to-\infty]{} -\infty$;
2. Si $a > 1$,
   - $\exp_a(x) \xrightarrow[x\to+\infty]{} +\infty$,
   - $\dfrac{\exp_a(x)}{x} \xrightarrow[x\to+\infty]{} +\infty$,
   - $\exp_a(x) \xrightarrow[x\to-\infty]{} 0$;

$a > 1$

1

Proposition : Si $a \in \mathbb{R}_\star^+ \setminus \{1\}$, alors $\exp_a$ est bijective.

Définition : Soit $a > 0$ et $a \neq 1$.

La réciproque de $\exp_a$ est appelé logarithme de base a et est noté $\log_a$.

Proposition : Si $a \in \mathbb{R}_\star^+ \setminus \{1\}$, alors

$$\forall x > 0, \log_a(x) = \frac{\ln x}{\ln a}.$$

Preuve :
Soit $a \in \mathbb{R}_\star^+ \setminus \{1\}$.

— Soit $x > 0$,

$$\exp_a\left(\frac{\ln x}{\ln a}\right) = e^{\frac{\ln x}{\ln a} \times \ln a} = e^{\ln x} = x$$

— Soit $x \in \mathbb{R}$,

$$\frac{\ln\left(\exp_a(x)\right)}{\ln a} = \frac{\ln\left(e^{x \ln a}\right)}{\ln a} = \frac{x \ln a}{\ln a} = x.$$

Donc, $\log_a : x \mapsto \dfrac{\ln x}{\ln a}$ est bien la réciproque de $\exp_a$. □

Exemple :

Combien y a-t-il de chiffres dans la représentation décimale de 2^{2021} ?

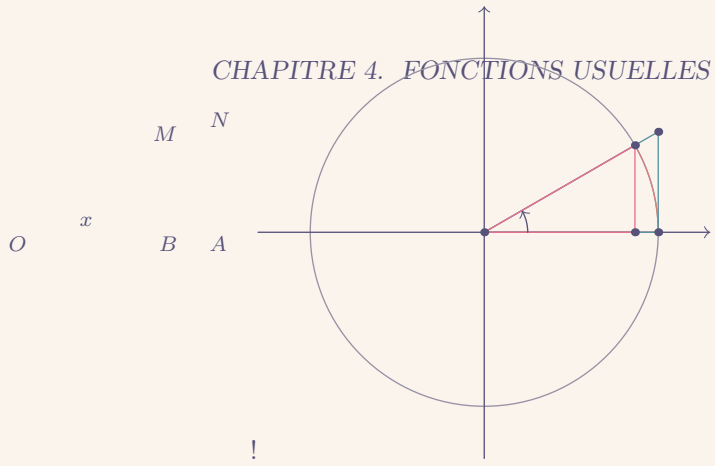
Soit $N \in \mathbb{N}$. La représentation décimale de 2^{2021} a N chiffres si et seulement si

$$\begin{aligned}
&10^{N-1} \leqslant 2^{2021} < 10^N \\
\iff &N - 1 \leqslant \log_{10}\left(2^{2021}\right) < N \\
\iff &N - 1 \leqslant 2021 \log_{10} 2 < N \\
\iff &N > 2021 \log_{10} 2 \text{ et } N \leqslant 2021 \log_{10}(2) + 1 \\
\iff &\underbrace{2021 \log_{10} 2}_{\simeq 608{,}3} < N \leqslant 2021 \log_{10}(2) + 1 \implies N = 609.
\end{aligned}$$

5 Fonctions trigonométriques

Proposition :

$$\lim_{x \to 0} \frac{\sin x}{x} = 1$$



Preuve :
Soit $x \in \left]0, \frac{\pi}{2}\right[$. On pose $M(\cos x, \sin x)$ et $N(1, \tan x)$.

Le triangle OBM est contenu dans le secteur OAM donc

$$\frac{\cos(x)\sin(x)}{2} \leqslant \frac{x}{2}.$$

Le secteur OAM est contenu dans le triangle OAN donc

$$\frac{x}{2} \leqslant \frac{\tan x}{2} = \frac{\sin x}{2\cos x}.$$

D'où,

$$\cos x \leqslant \frac{\sin x}{x} \leqslant \frac{1}{\cos x}$$

Or, $\cos x \xrightarrow[\substack{x\to 0\\ >}]{} 1$ et $\dfrac{1}{\cos x} \xrightarrow[\substack{x\to 0\\ >}]{} 1$.

Par encadrement, on en déduit que

$$\frac{\sin x}{x} \xrightarrow[\substack{x\to 0\\ >}]{} 1$$

et

$$\forall x \in \left]-\frac{\pi}{2}, 0\right[, \frac{\sin x}{x} = \frac{\sin(-x)}{-x} \xrightarrow[\substack{x\to O\\ >}]{} 1 \text{ d'après le calcul précédent.}$$

□

Corollaire : sin et cos sont dérivables sur $\mathbb{R}$ et $\begin{cases}\sin' = \cos,\\ \cos' = -\sin.\end{cases}$

Preuve :
Soit $x \in \mathbb{R}$ et $h \in \mathbb{R}^\star$.

$$\begin{aligned}\frac{\sin(x+h)-\sin x}{h} &= \frac{\sin(x)\cos(h)+\cos(x)\sin(h)-\sin(x)}{h}\\ &= \frac{-1+\cos h}{h}\sin x + \frac{\sin h}{h}\cos x\\ &= \sin x \times \frac{-2\sin^2\frac{h}{2}}{h} + \cos x \frac{\sin h}{h}\end{aligned}$$

Or, $\sin^2\dfrac{h}{2} \underset{h\to 0}{\sim} \left(\dfrac{h}{2}\right)^2 = \dfrac{h^2}{4}$. Alors

$$\frac{\sin^2\frac{h}{2}}{h} \underset{h\to 0}{\sim} \frac{h}{4} \xrightarrow[h\to 0]{} 0.$$

Donc,

$$\frac{\sin(x+h)-\sin x}{h} \xrightarrow[h\to 0]{} \cos x.$$

Également, $\forall x \in \mathbb{R}, \cos x = \sin\left(\dfrac{\pi}{2}-x\right)$ donc

$$\forall x \in \mathbb{R}, \cos'(x) = \cos\left(\frac{\pi}{2}-x\right)\times(-1) = -\sin x.$$

□

Proposition : La fonction tan est dérivable sur $\left\{x \in \mathbb{R} \mid x \not\equiv \dfrac{\pi}{2} \ [\pi]\right\} = D$ et

$$\forall x \in D, \tan' x = 1+\tan^2 x = \frac{1}{\cos^2 x}.$$

Preuve :
$\forall x \in D, \tan x = \dfrac{\sin x}{\cos x}$; sin et cos sont dérivables sur $\mathbb{R}$ donc tan est dérivable sur D.

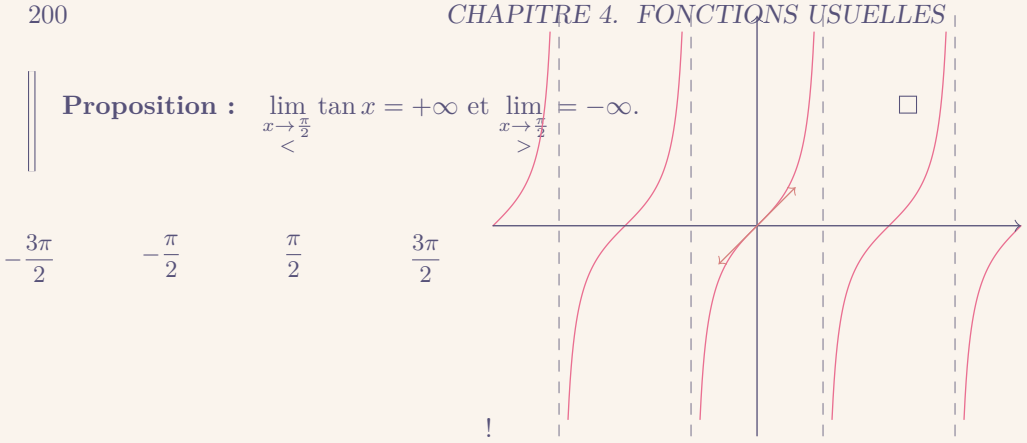
$$\forall x \in D, \tan' x = \frac{\cos^2 x+\sin^2 x}{\cos^2 x} = \frac{1}{\cos^2 x}$$

$$\| $$

$$1+\tan^2 x$$

□

Proposition : $\lim\limits_{\substack{x\to\frac{\pi}{2}\\<}} \tan x = +\infty$ et $\lim\limits_{\substack{x\to\frac{\pi}{2}\\>}} = -\infty$. □



Proposition : cotan est dérivable sur $D = \{x \in \mathbb{R} \mid x \equiv 0 \ [\pi]\}$ et

$$\forall x \in D, \operatorname{cotan}' x = -\frac{1}{\sin^2 x} = -1 - \operatorname{cotan}^2 x.$$

Preuve :
On a

$$\forall x \in D, \operatorname{cotan} x = \frac{\cos x}{\sin x}.$$

Donc,

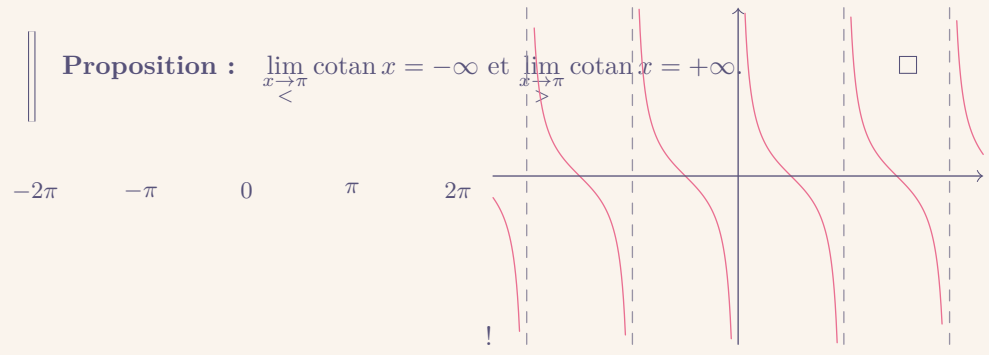
$$\forall x \in D, \operatorname{cotan}' x = \frac{-\sin^2 x - \cos^2 x}{\sin^2 x} = -\frac{1}{\sin^2 x}$$

$$\| $$

$$-1 - \operatorname{cotan}^2 x.$$

□

Proposition : $\lim\limits_{\substack{x\to\pi\\<}} \operatorname{cotan} x = -\infty$ et $\lim\limits_{\substack{x\to\pi\\>}} \operatorname{cotan} x = +\infty$. □



6 Fonctions trigonométriques réciproques

Proposition–Définition : L'application $\begin{array}{ccc}\left[-\frac{\pi}{2},\frac{\pi}{2}\right] & \longrightarrow & [-1,1] \\ x & \longmapsto & \sin x\end{array}$ est bijective. On appelle arcsinus la réciproque de cette bijection et on la note Arcsin.

Pour tout $x \in [-1,1]$, $\operatorname{Arcsin} x$ est le seul angle compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ donc le sinus vaut x. □

EXEMPLE : — $\operatorname{Arcsin} 0 = 0$,
- $\operatorname{Arcsin} 1 = \frac{\pi}{2}$,
- $\operatorname{Arcsin}\left(\sin\frac{3\pi}{2}\right) \neq \frac{3\pi}{2}$ car $\operatorname{Arcsin}(-1) = -\frac{\pi}{2}$.
- $\operatorname{Arcsin}\left(\sin\frac{7\pi}{5}\right) = \frac{-2\pi}{5}$ car $\sin\frac{7\pi}{5} = \sin\left(\pi - \frac{7\pi}{5}\right) = \sin\left(-\frac{2\pi}{5}\right)$ et $-\frac{2\pi}{5} \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right]$.

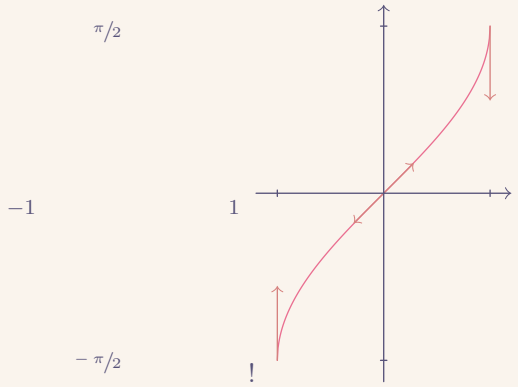
Proposition :
1. $\forall x \in [-1,1], \operatorname{Arcsin} x \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right]$
2. $\forall \theta \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right], \operatorname{Arcsin}(\sin\theta) = \theta$
3. $\forall x \in [-1,1], \sin(\operatorname{Arcsin} x) = x$
4. $\forall x \in [-1,1], \cos(\operatorname{Arcsin} x) = \sqrt{1-x^2}$

Preuve : 1., 2. et 3. correspondent à la définition de Arcsin.

4. Soit $x \in [-1,1]$. On pose $\theta = \operatorname{Arcsin} x \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right]$. On sait que $\cos^2\theta + \sin^2\theta = 1$ donc $\cos^2\theta = 1 - \sin^2\theta = 1 - \sin^2(\operatorname{Arcsin} x) = 1 - x^2$. On en déduit que $|\cos\theta| = \sqrt{1-x^2}$. Comme $\theta \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right]$, $\cos\theta \geqslant 0$ et donc
$$\cos(\operatorname{Arcsin} x) = \sqrt{1-x^2}.$$

□

Proposition :
1. Arcsin est impaire
2. Arcsin est continue sur $[-1,1]$
3. Arcsin est dérivable sur $]-1,1[$ et
$$\forall x \in]-1,1[, \operatorname{Arcsin}' x = \frac{1}{\sqrt{1-x^2}} > 0$$
4. Arcsin n'est pas dérivable en 1 et en -1.



Preuve : 1. Soit $x \in [-1,1]$. Alors $-x \in [-1,1]$. On pose $\theta = \operatorname{Arcsin}(-x)$. θ est le seul nombre compris entre $-\dfrac{\pi}{2}$ et $\dfrac{\pi}{2}$ vérifiant $\sin\theta = -x$.

$\operatorname{Arcsin} x \in \left[-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right]$ donc $-\operatorname{Arcsin} x \in \left[-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right]$. On a

$$\sin(-\operatorname{Arcsin} x) = -\sin(\operatorname{Arcsin} x) = -x$$

donc

$$\theta = \operatorname{Arcsin}(-x) = -\operatorname{Arcsin} x.$$

2. sin est continue et strictement croissante sur $[-\pi/2, \pi/2]$ à valeurs dans $[-1,1]$ donc Arcsin est continue sur $[-1,1]$.
3. Soit $x \in [-1,1]$. $\sin'(\operatorname{Arcsin} x) = \cos(\operatorname{Arcsin} x) = \sqrt{1-x^2}$ donc

$$\forall x \in]-1,1[, \sin'(\operatorname{Arcsin} x) \neq 0.$$

Donc Arcsin est dérivable sur $]-1,1[$ et

$$\forall x \in]-1,1[, \operatorname{Arcsin}' x = \frac{1}{\sqrt{1-x^2}}$$

4. Arcsin est continue sur $[-1,1]$, dérivable sur $]-1,1[$, et

$$\forall x \in]-1,1[, \operatorname{Arcsin}' x = \frac{1}{\sqrt{1-x^2}} \xrightarrow[x\to\pm1]{} +\infty.$$

D'après le théorème de la limite de la dérivée, Arcsin n'est pas dérivable en ± 1.

□

Remarque :
Une primitive de $x \mapsto \dfrac{1}{\sqrt{1-x}}$ est Arcsin.

Proposition–Définition : L'application $\begin{array}{ccc}[0,\pi] & \longrightarrow & [-1,1] \\ x & \longmapsto & \cos x\end{array}$ est bijective. On note sa réciproque Arccos.

En d'autres termes, pour $x \in [-1,1]$, $\operatorname{Arccos} x$ est le seul angle compris entre 0 et π dont le cosinus vaut x.

Preuve :
Théorème de la bijection continue. □

Exemple :
$\operatorname{Arccos} 0 = \dfrac{\pi}{2}$, $\operatorname{Arccos} \dfrac{1}{2} = \dfrac{\pi}{3}$, $\operatorname{Arccos}\left(-\dfrac{1}{2}\right) = \dfrac{2\pi}{3}$,
$\operatorname{Arccos}\left(\cos \dfrac{75\pi}{67}\right) = \dfrac{59\pi}{67} \in [0,\pi]$ car $\cos \dfrac{75\pi}{67} = \cos\left(\dfrac{75\pi}{67} - 2\pi\right) = \cos\left(-\dfrac{59\pi}{67}\right) = \cos \dfrac{59\pi}{67}$.

Proposition :
1. $\forall x \in [-1,1]$, $\operatorname{Arccos} x \in [0,\pi]$,
2. $\forall \theta \in [0,\pi]$, $\operatorname{Arccos}(\cos\theta) = \theta$,
3. $\forall x \in [-1,1]$, $\cos(\operatorname{Arccos} x) = x$,
4. $\forall x \in [-1,1]$, $\sin(\operatorname{Arccos} x) = \sqrt{1-x^2}$.

Preuve : 1., 2. et 3. correspondent à la définition de Arccos.
4. Soit $x \in [-1,1]$.

$$\sin^2(\operatorname{Arccos} x) = 1 - \cos^2(\operatorname{Arccos} x) = 1 - x^2$$
$$\text{donc } \big|\sin(\operatorname{Arccos} x)\big| = \sqrt{1-x^2}.$$

Or, $\operatorname{Arccos} x \in [0,\pi]$ donc $\sin(\operatorname{Arccos} x) \geqslant 0$ et donc

$$\sin(\operatorname{Arccos} x) = \sqrt{1-x^2}.$$

□

Proposition :
1. Arccos est continue sur $[-1,1]$,
2. Arccos est dérivable sur $]-1,1[$ et

$$\forall x \in]-1,1[, \operatorname{Arccos}' x = -\frac{1}{\sqrt{1-x^2}}.$$

Preuve : 1. cos est coninue et strictement décroissante sur $[0, \pi]$ à valeurs dans $[-1, 1]$ donc Arccos continue dans $[-1, 1]$.

2.

$$\begin{aligned}\forall x \in]-1, 1[,\ \cos'(\operatorname{Arccos} x) &= -\sin(\operatorname{Arccos} x) \\ &= -\sqrt{1-x^2} \neq 0\end{aligned}$$

donc Arccos est dérivable sur $]-1, 1[$ et

$$\operatorname{Arccos}' x = -\frac{1}{\sqrt{1-x^2}} < 0.$$

□

Corollaire :

$$\forall x \in [-1, 1],\ \operatorname{Arccos} x + \operatorname{Arcsin} x = \frac{\pi}{2}$$

Preuve :

Méthode 1 Soit $f : \begin{array}{ccc}[-1,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \operatorname{Arcsin} x + \operatorname{Arccos} x\end{array}$ continue sur $[-1, 1]$ et dérivable sur $]-1, 1[$. On a

$$\forall x \in]-1, 1[,\ f'(x) = \frac{1}{\sqrt{1-x^2}} - \frac{1}{\sqrt{1-x^2}} = 0.$$

donc f est constante sur $]-1, 1[$:

$$\exists C \in \mathbb{R},\ \forall x \in]-1, 1[,\ f(x) = C.$$

En particulier,

$$f(0) = \operatorname{Arccos} 0 + \operatorname{Arcsin} 0 = \frac{\pi}{2} + 0 = \frac{\pi}{2}.$$

Méthode 2 Soit $x \in [0, 1]$.

$$\begin{aligned}\sin(\operatorname{Arccos} x) = \sqrt{1-x^2} &= \cos(\operatorname{Arcsin} x) \\ &= \sin\left(\frac{\pi}{2} - \operatorname{Arcsin} x\right)\end{aligned}$$

donc

$$\operatorname{Arccos} x \equiv \frac{\pi}{2} - \operatorname{Arcsin} x\ \ [2\pi]\ \text{ ou }\ \pi - \operatorname{Arccos} x \equiv \frac{\pi}{2} - \operatorname{Arcsin} x\ \ [2\pi]$$

donc

$$\exists k \in \mathbb{Z},\ \operatorname{Arccos} x + \operatorname{Arcsin} x = \frac{\pi}{2} + 2k\pi$$
$$\text{ou } \exists k \in \mathbb{Z},\ -\operatorname{Arccos} x + \operatorname{Arcsin} x = -\frac{\pi}{2} + 2k\pi.$$

Or, $\begin{cases} 0 \leqslant \operatorname{Arccos} x \leqslant \pi \\ 0 \leqslant \operatorname{Arcsin} x \leqslant \dfrac{\pi}{2} \end{cases}$ donc $0 \leqslant \operatorname{Arccos} x + \operatorname{Arcsin} x \leqslant \pi$

$\iff \begin{cases} -\dfrac{\pi}{2} \leqslant -\operatorname{Arccos} x \leqslant 0 \\ 0 \leqslant \operatorname{Arcsin} x \leqslant \dfrac{\pi}{2} \end{cases}$ donc $-\dfrac{\pi}{2} \leqslant -\operatorname{Arccos} x + \operatorname{Arcsin} x \leqslant \dfrac{\pi}{2}$

D'où

$$\operatorname{Arccos} x + \operatorname{Arcsin} x = \frac{\pi}{2} \text{ ou } -\operatorname{Arccos} x + \operatorname{Arcsin} x = -\frac{\pi}{2}$$

— Si $-\operatorname{Arccos} x > -\dfrac{\pi}{2}$ ou $\operatorname{Arcsin} x > 0$, alors $-\operatorname{Arccos} x + \operatorname{Arcsin} x > -\dfrac{\pi}{2}$ et donc

$$\operatorname{Arccos} x + \operatorname{Arcsin} x = \frac{\pi}{2}.$$

— Si $-\operatorname{Arccos} x = \dfrac{\pi}{2}$ et $\operatorname{Arcsin} x = 0$, alors $x = 0$ et donc

$$\operatorname{Arccos} x + \operatorname{Arcsin} x = \frac{\pi}{2} + 0 = \frac{\pi}{2}.$$

Soit $x \in [-1, 0[$. On pose $y = -x \in [0, 1]$

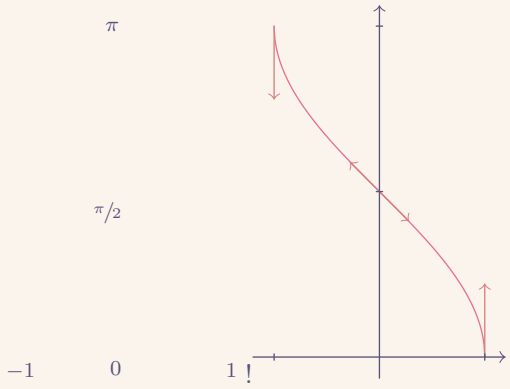
— $\operatorname{Arcsin} x = -\operatorname{Arcsin} y$,

— $\operatorname{Arccos} x = \pi - \operatorname{Arccos} y$: en effet, $\cos(\pi - \operatorname{Arccos} y) = -\cos(\operatorname{Arccos} y) = -y = x$ et $0 \leqslant \operatorname{Arccos} y \leqslant \pi$ donc $-\pi \leqslant \operatorname{Arccos} y \leqslant 0$ et donc $0 \leqslant \pi - \operatorname{Arccos} y \leqslant \pi$

D'où,

$$\begin{aligned} \operatorname{Arccos} x + \operatorname{Arcsin} x &= \pi - \operatorname{Arccos} y - \operatorname{Arcsin} y \\ &= \pi - (\operatorname{Arccos} y + \operatorname{Arcsin} y) \\ &= \pi - \frac{\pi}{2} \\ &= \frac{\pi}{2}. \end{aligned}$$

□



Proposition–Définition : L'application $\left]-\frac{\pi}{2},\frac{\pi}{2}\right[\longrightarrow \mathbb{R}$, $x \longmapsto \tan x$ est bijective. On note Arctan la réciproque de cette bijection.

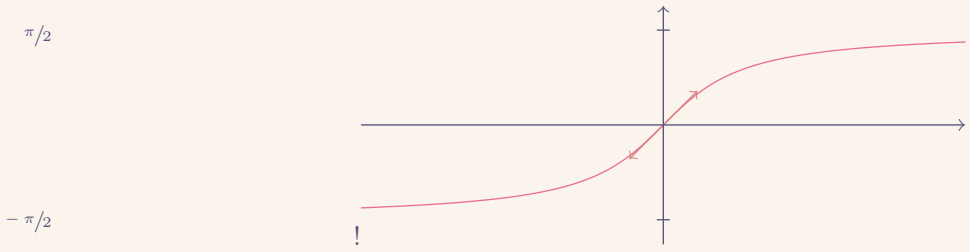
C'est à dire, pour tout $x \in \mathbb{R}$, $\operatorname{Arctan} x$ est le seul angle compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ (exclus) dont la tangente vaut x.

Preuve :
Théorème de la bijection continue. □

Exemple :
$\operatorname{Arctan} 0 = 0$, $\operatorname{Arctan} 1 = \frac{\pi}{4}$, $\operatorname{Arctan} \sqrt{3} = \frac{\pi}{3}$,
$\operatorname{Arctan}(\tan \frac{9\pi}{7}) = \frac{2\pi}{7} \in \left]-\frac{\pi}{2},\frac{\pi}{2}\right[$ car $\tan \frac{9\pi}{7} = \tan\left(\frac{9\pi}{7} - \pi\right) = \tan \frac{2\pi}{7}$.

Proposition :

1. Arctan est dérivable sur $\mathbb{R}$ et
$$\forall x \in \mathbb{R},\ \operatorname{Arctan}' x = \frac{1}{1+x^2},$$
2. $\begin{cases} \lim\limits_{x\to+\infty} \operatorname{Arctan} x = \frac{\pi}{2}, \\ \lim\limits_{x\to-\infty} \operatorname{Arctan} x = -\frac{\pi}{2}, \end{cases}$
3. Arctan est impaire.



Preuve : 1. $\forall x \in \mathbb{R}$, $\tan'(\operatorname{Arctan} x) = 1 + \tan^2(\operatorname{Arctan} x) = 1 + x^2 \neq 0$
donc Arctan est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, \operatorname{Arctan}'(x) = \frac{1}{1+x^2}.$$

2. On déduit des limites de tan les limites de Arctan.
3. Comme pour Arcsin.

□

Proposition :

$$\forall x \in \mathbb{R}^\star, \operatorname{Arctan} x + \operatorname{Arctan} \frac{1}{x} = \begin{cases} \dfrac{\pi}{2} & \text{si } x > 0 \\ -\dfrac{\pi}{2} & \text{si } x < 0 \end{cases}$$

Preuve :
On pose $f : \begin{array}{ccc} \mathbb{R}^\star & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \operatorname{Arctan} x + \operatorname{Arctan} \dfrac{1}{x} \end{array}$ dérivable sur $\mathbb{R}^\star$ par

$$\begin{aligned} f'(x) &= \frac{1}{1+x^2} - \frac{1}{1+\left(\frac{1}{x}\right)^2} \times \frac{1}{x^2} \\ &= \frac{1}{1+x^2} - \frac{1}{1+x^2} \\ &= 0 \end{aligned}$$

B $\mathbb{R}^\star$ n'est pas un intervalle !
— $\mathbb{R}_\star^+$ est un intervalle donc $\exists C^+ \in \mathbb{R}, \forall x \in \mathbb{R}_\star^+, f(x) = C^+$
— $\mathbb{R}_\star^-$ est un intervalle donc $\exists C^- \in \mathbb{R}, \forall x \in \mathbb{R}_\star^-, f(x) = C^-$
$f(1) = \dfrac{\pi}{4} + \dfrac{\pi}{4} = \dfrac{\pi}{2}$ donc $C^+ = \dfrac{\pi}{2}$,
$f(-1) = -\dfrac{\pi}{4} - \dfrac{\pi}{4} = -\dfrac{\pi}{2}$ donc $C^- = -\dfrac{\pi}{2}$. □

7 Trigonométrie hyperbolique

Définition : Pour tout $x \in \mathbb{R}$, on pose

$$\begin{cases} \operatorname{ch} x = \dfrac{e^x + e^{-x}}{2}, \\ \operatorname{sh} x = \dfrac{e^x - e^{-x}}{2}, \\ x = \dfrac{\operatorname{sh} x}{\operatorname{ch} x}. \end{cases}$$

ch est appelé cosinus hyperbolique, sh est appelé sinus hyperbolique et est appelé tangeante hyperbolique.

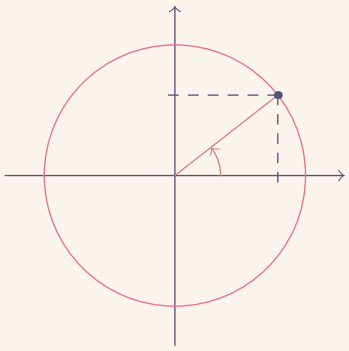
Remarque :
Ces formules rappèlent les formules d'Euler : pour tout $x \in \mathbb{R}$,

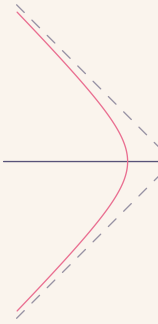
$$\cos x = \frac{e^{ix} + e^{-ix}}{2} \quad \longleftrightarrow \quad \operatorname{ch} x = \frac{e^x + e^{-x}}{2}$$
$$\sin x = \frac{e^{ix} - e^{-ix}}{2i} \quad \longleftrightarrow \quad \operatorname{sh} x = \frac{e^x - e^{-x}}{2}$$

$\sin\theta$ M $\operatorname{sh} x$ M

θ

$\cos\theta$ $\operatorname{ch} x$





$+ y^2 = 1$ $x^2 - y^2 = 1$!

Proposition :

$$\forall t \in \mathbb{R}, \operatorname{ch}^2 t - \operatorname{sh}^2 t = 1.$$

Preuve :

Soit $t \in \mathbb{R}$.

$$\begin{aligned}
\operatorname{ch}^2 t - \operatorname{sh}^2 t &= \left(\frac{e^t + e^{-t}}{2}\right)^2 - \left(\frac{e^t - e^{-t}}{2}\right)^2 \\
&= \frac{\cancel{e^t} + e^{-t} - \cancel{e^t} + e^{-t}}{2} \times \frac{e^t + \cancel{e^{-t}} + e^t - \cancel{e^{-t}}}{2} \\
&= \frac{2e^{-t}}{2} \times \frac{2e^t}{2} \\
&= e^{-t} \times e^t \\
&= 1
\end{aligned}$$

□

Exercice :
Expliciter $\operatorname{ch}(a+b)$ *avec* $(a,b) \in \mathbb{R}^2$.

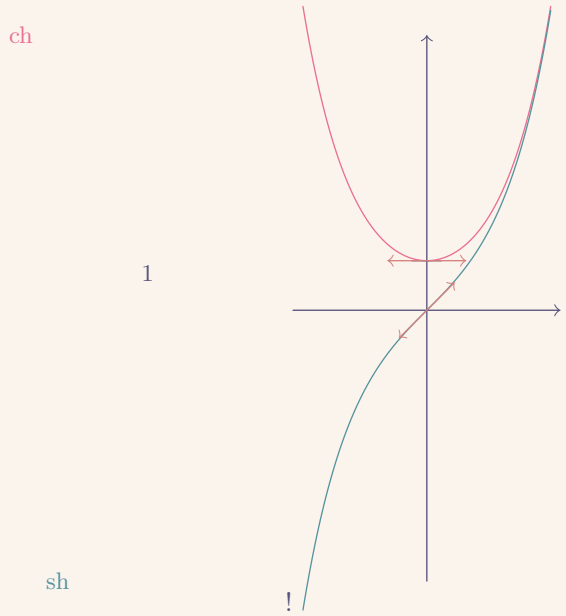
$$\begin{aligned}
\operatorname{ch}(a)\operatorname{ch}(b) + \operatorname{sh}(a)\operatorname{sh}(b) &= \frac{2e^{a+b} + e^{b-a} + e^{a-b}}{4} + \frac{2e^{-(a+b)} - e^{a-b} - e^{b-a}}{4} \\
&= \frac{1}{4}\left(2e^{a+b} + 2e^{-(a+b)}\right) \\
&= \frac{e^{a+b} + e^{-(a+b)}}{2} \\
&= \operatorname{ch}(a+b).
\end{aligned}$$

Expliciter $\operatorname{sh}(a+b)$ *avec* $(a,b) \in \mathbb{R}^2$.

$$\begin{aligned}
\operatorname{sh}(a)\operatorname{ch}(b) + \operatorname{sh}(b)\operatorname{ch}(a) &= \frac{1}{4}\left(2e^{a+b} + \cancel{e^{a-b}} - \cancel{e^{b-a}} + \cancel{e^{b-a}} - \cancel{e^{a-b}} - 2e^{-(a+b)}\right) \\
&= \frac{e^{a+b} - e^{-(a+b)}}{2} \\
&= \operatorname{sh}(a+b)
\end{aligned}$$

Proposition :
1. ch est paire, sh est impaire ;
2. ch et sh sont dérivables sur $\mathbb{R}$ et $\begin{cases} \operatorname{ch}' = \operatorname{sh}, \\ \operatorname{sh}' = \operatorname{ch}; \end{cases}$
3. sh est strictement croissante sur $\mathbb{R}$, ch est strictement croissante sur $\mathbb{R}^+$;
4. $\lim\limits_{x \to +\infty} \operatorname{ch} x = +\infty$, $\lim\limits_{x \to +\infty} \operatorname{sh} x = +\infty$ et $\lim\limits_{x \to -\infty} \operatorname{sh} x = -\infty$;

5. $\operatorname{ch} x \underset{x\to+\infty}{\sim} \frac{1}{2}e^x$ et $\operatorname{sh} \underset{x\to+\infty}{\sim} \frac{1}{2}e^x$.



Preuve : 1.

$$\begin{cases} \operatorname{ch}(-x) = \dfrac{e^{-x}+e^{-(-x)}}{2} = \dfrac{e^x+e^{-x}}{2} = \operatorname{ch} x; \\ \operatorname{sh}(-x) = \dfrac{e^{-x}-e^{-(-x)}}{2} = \dfrac{e^{-x}-e^x}{2} = -\dfrac{e^x-e^{-x}}{2} = -\operatorname{sh} x. \end{cases}$$

2. $x \mapsto e^x$ et $x \mapsto e^{-x}$ sont dérivables sur $\mathbb{R}$ donc ch et sh aussi. On a donc
$$\forall x \in \mathbb{R}, \begin{cases} \operatorname{ch}'(x) = \dfrac{e^x-e^{-x}}{2} = \operatorname{sh}(x); \\ \operatorname{sh}'(x) = \dfrac{e^x+e^{-x}}{2} = \operatorname{ch}(x). \end{cases}$$

3. $\forall x \in \mathbb{R}, \operatorname{sh}' x = \operatorname{ch} x = \dfrac{e^x+e^{-x}}{2} > 0$ donc sh strictement croissante sur $\mathbb{R}$.
$\forall x \in \mathbb{R}_\star^+, \operatorname{ch}' x = \operatorname{sh} x > \operatorname{sh} 0 = 0$ (car sh strictement croissante) et $\operatorname{ch}' 0 = \operatorname{sh} 0 = 0$. Donc, ch est strictement croissante sur $\mathbb{R}^+$.

4. et 5.
$$\forall x \in \mathbb{R}, \begin{cases} \operatorname{ch} x = \dfrac{1}{2}\left(e^x+e^{-x}\right) = \dfrac{e^x}{2}\left(1+e^{-2x}\right) \underset{x\to+\infty}{\sim} \dfrac{e^x}{2} \longrightarrow +\infty; \\ \operatorname{sh} x = \dfrac{1}{2}\left(e^x-e^{-x}\right) = \dfrac{e^x}{2}\left(1-e^{-2x}\right) \underset{x\to+\infty}{\sim} \dfrac{e^x}{2} \longrightarrow +\infty; \end{cases}$$

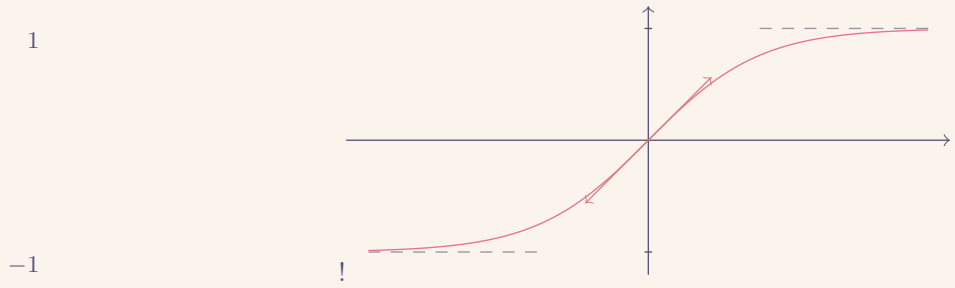
□

Remarque :
La courbe représentative de ch est appelée “chaînette”.

Proposition : 1. est imapire ;
2. est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, {}'x = \frac{1}{\mathrm{ch}^2 x} = 1 - {}^2x;$$

3. est strictement croissante sur $\mathbb{R}$;
4. $\lim\limits_{x\to+\infty} x = 1$ et $\lim\limits_{x\to-\infty} x = -1$.



Preuve : 1. Soit $x \in \mathbb{R}$.

$$(-x) = \frac{\mathrm{sh}(-x)}{\mathrm{ch}(-x)} = -\frac{\mathrm{sh}\, x}{\mathrm{ch}\, x} = -x.$$

2. sh et ch sont dérivables sur $\mathbb{R}$ et $\forall x \in \mathbb{R}$, $\mathrm{ch}\, x \neq 0$ donc est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, {}'x = \frac{\mathrm{ch}^2 x - \mathrm{sh}^2 x}{2} = \frac{1}{\mathrm{ch}^2 x}$$
$$= 1 - \frac{\mathrm{sh}^2 x}{\mathrm{ch}^2 x} = 1 - {}^2x.$$

3. $\forall x \in \mathbb{R}, {}'x = \dfrac{1}{\mathrm{ch}^2 x} > 0$ donc est strictement croissante sur $\mathbb{R}$.
4. On a

$$\forall x \in \mathbb{R}, x = \frac{\mathrm{sh}\, x}{\mathrm{ch}\, x} \sim \frac{e^x/2}{e^x/2} = 1 \xrightarrow[x\to+\infty]{} 1$$

et, comme est impaire,

$$\lim_{x\to-\infty} x = -\lim_{x\to+\infty} x = -1.$$

□

Exercice :
Résoudre $\operatorname{sh} x = y$ *d'inconnue* x *et* y *étant un paramètre réel.*

Soit $x \in \mathbb{R}$.

$$\begin{aligned}
\operatorname{sh} x = y &\iff \frac{e^x - e^{-x}}{2} = y \\
&\iff (e^x)^2 - 1 = 2ye^x \\
&\iff (e^x - y)^2 - \overbrace{(y^2+1)}^{>0} = 0 \\
&\iff \left(e^x - y - \sqrt{y^2+1}\right)\left(e^x - y + \sqrt{y^2+1}\right) \\
&\iff e^x = y + \sqrt{y^2+1} \text{ ou } e^x = y - \sqrt{y^2+1}
\end{aligned}$$

Or, $\left(y + \sqrt{1+y^2}\right)\left(y - \sqrt{1+y^2}\right) = -1 < 0$ donc $y + \sqrt{1+y^2}$ et $y - \sqrt{1+y^2}$ sont de signes opposés.

Comme $y + \sqrt{1+y^2} > y - \sqrt{1+y^2}$, on a $\begin{cases} y + \sqrt{1+y^2} > 0 \\ y - \sqrt{1+y^2} < 0 \end{cases}$ d'où

$$\operatorname{sh} x = y \iff e^x = y + \sqrt{1+y^2} \iff x = \ln\left(y + \sqrt{1+y^2}\right).$$

On a trouvé la réciproque de sh :

$$\begin{aligned}
\operatorname{Argsh} : \mathbb{R} &\longrightarrow \mathbb{R} \\
x &\longmapsto \ln\left(x + \sqrt{1+x^2}\right)
\end{aligned}$$

Chapitre 5

Calcul intégral

1 Généralités

Définition : Soient I un intervalle de $\mathbb{R}$, f une fonction continue et $a, b \in I$.

On définit l'intégrale de f de a à b par

$$\int_a^b f(x)\,\mathrm{d}x = \big[F(x)\big]_a^b = F(b) - F(a)$$

où F est une primitive quelconque de f.

La variable x est muette :

$$\int_a^b f(x)\,\mathrm{d}x = \int_a^b f(u)\,\mathrm{d}u = \int_a^b f(t)\,\mathrm{d}t = \int_a^b f(❀)\,\mathrm{d}❀ \neq \int_a^b f(x)\,\mathrm{d}t$$

Proposition (Croissance) **:** Soient f et g continues sur I, $a, b \in I^2$ tels que $\begin{cases} \forall x \in I, f(x) \leqslant g(x), \\ a \leqslant b. \end{cases}$

Alors

$$\int_a^b f(x)\,\mathrm{d}x \leqslant \int_a^b g(x)\,\mathrm{d}x.$$

Preuve :
On pose, pour tout $x \in I$, $h(x) = g(x) - f(x) \geqslant 0$. h est continue sur I.

Soit H une primitive de h sur I. Donc

$$\begin{aligned}\int_a^b f(x)\,\mathrm{d}x - \int_a^b f(x)\,\mathrm{d}x &= \int_a^b \big(f(x)-g(x)\big)\,\mathrm{d}x \\ &= -\int_a^b h(x)\,\mathrm{d}x \\ &= H(a)-H(b)\end{aligned}$$

Or, $h = H' \geqslant 0$ donc H est croissante sur I. Comme $b \geqslant a$, $H(b) \geqslant H(a)$ et donc $\displaystyle\int_a^b f(x)\,\mathrm{d}x - \int_a^b g(x)\,\mathrm{d}x \leqslant 0$. □

Proposition (Linéarité) **:** Soient f et g continues sur I, $\alpha, \beta \in \mathbb{R}$ et $a, b \in \mathbb{R}$. Alors,

$$\int_a^b \big(\alpha\, f(x) + \beta\, g(x)\big)\,\mathrm{d}x = \alpha \int_a^b f(x)\,\mathrm{d}x + \beta \int_a^b g(x)\,\mathrm{d}x.$$

Preuve :
Soient F et G deux primitives sur I de f et g respectivement.

$\alpha F + \beta G$ est un primitive de $\alpha f + \beta g$ sur I car

$$(\alpha F + \beta G)' = \alpha F' + \beta G' = \alpha f + \beta g.$$

D'où

$$\begin{aligned}\int_a^b \big(\alpha f(x) + \beta(g)\big)\,\mathrm{d}x &= (\alpha F + \beta G)(b) - (\alpha F + \beta G)(a) \\ &= \alpha F(b) + \beta G(b) - \alpha F(b) - \beta G(a) \\ &= \alpha\big(F(b) - F(a)\big) + \beta\big(G(b) - G(a)\big) \\ &= \alpha \int_a^b f(x)\,\mathrm{d}x + \beta \int_a^b g(x)\,\mathrm{d}x.\end{aligned}$$

□

Proposition (Chasles) **:** Soit f continue sur un interval I, $a, b, c \in I$. Alors

$$\int_a^b f(x)\,\mathrm{d}x = \int_a^c f(x)\,\mathrm{d}x + \int_c^b f(x)\,\mathrm{d}x.$$

Preuve :
Soit F une primitive de f sur I. Alors,

$$\begin{aligned}\int_a^c f(x)\,\mathrm{d}x + \int_b^c \mathrm{d}x &= F(c) - F(a) + F(b) - F(c)\\ &= F(b) - F(a)\\ &= \int_a^b f(x)\,\mathrm{d}x.\end{aligned}$$

□

Proposition : Soit f positive et continue sur un interval I, $(a,b) \in I^2$ avec $a \leqslant b$. Alors

$$\int_a^b f(x)\,\mathrm{d}x = 0 \iff \forall x \in [a,b], f(x) = 0.$$

Preuve :
Soit F une primitive de f.

" $\Longrightarrow$ " On suppose que $\displaystyle\int_a^b f(x)\,\mathrm{d}x = 0$. Donc $F(b) = F(a)$.

Comme $F' = f \geqslant 0$, F est croissante.

□

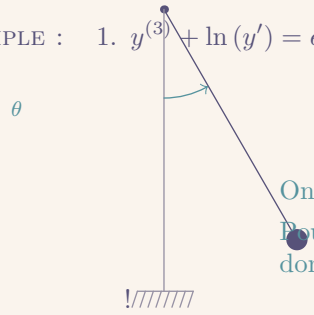
Chapitre 6

Équations différentielles linéaires

Définition : Une équation différentielle est une égalité faisant intervenir une fonction inconnue y ainsi que ses dérivées successives $y', y'', y^{(3)}, \dots, y^{(n)}$.

Exemple : 1. $y^{(3)} + \ln(y') = e^y$

2.

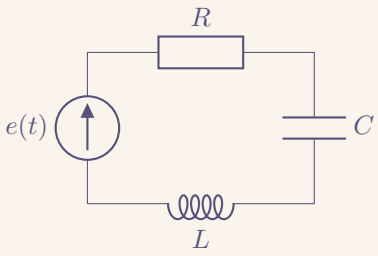


On a $\ddot{\theta} + \sin(\theta) = 0$ i.e. $\dfrac{d^2\theta}{dt^2} + \sin(\theta) = 0$

Pour les "petits angles", $\sin(\theta) \simeq 0$. On résout donc

$$\ddot{\theta} = -\theta$$

3. $$L\frac{d^2q}{dt^2} + R\frac{dq}{dt} + \frac{1}{C}q = e(t)$$
$$L\ddot{q} + R\dot{q} + \frac{1}{C}q = e(t)$$



4. Modèle de population : $\dfrac{dN}{dt} = \lambda N(1 - N)$

Définition : Une équation différentielle linéaire d'ordre n est de la forme

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_0 y = b(t)$$

où $b, a_0, a_1, \ldots, a_n$ sont des fonctions connues et continues sur un intervalle I. On dit que b est le second membre de l'équation.

EXEMPLE $(\cos(t)y'' + \sin(t)y' = \tan(t))$:

Proposition (Principe de superposition) **:** Soient b_1 et b_2 continues sur I. Soient $a_0, a_1, \ldots, a_n$ également continues sur I.

$$(E_1): \quad \sum_{k=0}^{n} a_k y^{(k)} = b_1$$
$$(E_2): \quad \sum_{k=0}^{n} a_k y^{(k)} = b_2$$

Soient $(\lambda_1, \lambda_2) \in \mathbb{C}^2$.

$$(E): \quad \sum_{k=1}^{n} a_k y^{(k)} = \lambda_1 b_1 + \lambda_2 b_2$$

$$\left.\begin{array}{l} y_1 \text{ solution de } (E_1) \\ y_2 \text{ solution de } (E_2) \end{array}\right\} \implies \lambda_1 y_1 + \lambda_2 y_2 \text{ solution de } (E)$$

Preuve :
On pose $y = \lambda_1 y_1 + \lambda_2 y_2$ dérivable n fois car c'est le cas de y_1 et y_2 Donc,

$$\forall k \in [\![0, n]\!], y^{(k)} = \lambda_1 y_1^{(k)} + \lambda_2 y_2^{(k)}$$

D'où,

$$\begin{aligned} \sum_{k=0}^{n} a_k y^{(k)} &= \sum_{k=0}^{n} a_k \left(\lambda_1 y_1^{(k)} + \lambda_2 y_2^{(k)}\right) \\ &= \lambda_1 \sum_{k=1}^{n} a_k y_1^{(k)} + \lambda_2 \sum_{k=1}^{n} a_k y_2^{(k)} \\ &= \lambda_1 b_1 + \lambda_2 b_2 \end{aligned}$$

□

Proposition : Soit (E) l'équation différentielle $\sum_{k=0}^{n} a_k y^{(k)} = b$ où $a_0, a_1, \ldots, a_n$ sont des fonctions homogènes. L'équation homogène associée à (E) est

$$(H) : \sum_{k=0}^{n} a_k y^{(k)} = 0$$

Les solutions de (E) sont toutes de la forme $h + y_0$ où h est solution de (H) et y_0 solution de (E).

Preuve :
Soit y une solution de (E) et y_0 une solution particulière de (E). On pose $h = y - y_0$.
D'après le principe de superposition, h est une solution de (H).
Réciproquement, si h est une solution de (H) et y_0 une solution de (E) alors $h + y_0$ est aussi solution de (E). □

Théorème (Théorème de Cauchy) **:** Soit (E) une équation linéaire différentielle.

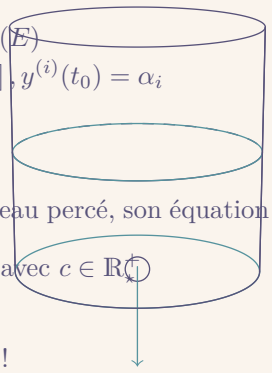
$$(E) : \quad y^{(n)} + \sum_{k=0}^{n-1} a_k y^{(k)} = b$$

où $a_0, a_1, \ldots, a_n$ sont continues sur un intervalle I.
Soit $t_0 \in I$ et $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$.
Il existe **une et une seule** fonction y telle que

$$\begin{cases} y \text{ solution de } (E) \\ \forall i \in [\![0, n-1]\!], y^{(i)}(t_0) = \alpha_i \end{cases}$$

Exemple :
On ne peut pas déduire le passé d'un sceau percé, son équation est non-linéaire.

$$h' = -c\sqrt{h} \text{ avec } c \in \mathbb{R}_+^*$$



!

1

Soit (E) l'équation $y' + ay = b$ où a et b sont continues sur un intervalle I.

Proposition : Soit A une primitive de a sur un intervalle I.

$$(H): \quad y' + ay = 0$$

Les solutions de (H) sont $t \mapsto \lambda e^{-A(t)}$ avec $\lambda \in \mathbb{C}$

Preuve :
Soit y une fonction dérivable sur I. On pose

$$z : t \mapsto y(t)e^{A(t)}$$

dérivable sur I et

$$\begin{aligned} \forall t \in I, z'(t) &= y'(t)e^{A(t)} + y(t)A'(t)e^{A(t)} \\ &= \left(y'(t) + a(t)y(t)\right) e^{A(t)} \end{aligned}$$

$$\begin{aligned} y \text{ solution de } (H) &\iff \forall t \in I, y'(t) + a(t)y(t) = 0 \\ &\iff \forall t \in I, z'(t) = 0 \\ &\iff \exists \lambda \in \mathbb{C}, \forall t \in I, z(t) = \lambda \\ &\iff \exists \lambda \in \mathbb{C}, \forall t \in I, y(t) = \lambda e^{-A(t)} \end{aligned}$$

□

Remarque (pseudo preuve) :

$$\begin{aligned} \frac{dy}{dt} + a(t)y = 0 &\iff \frac{dy}{y} = -a(t)dt \\ &\iff \int \frac{dy}{y} = \int -a(t)dt \\ &\iff \ln(y) = -A(t) + K \\ &\iff y = e^{-A(t)+K} \\ &\iff y = \lambda e^{-A(t)} \text{ avec } \lambda = e^K \end{aligned}$$

2 Annexe

$y : I \to E$ où E est un $\mathbb{K}$-espace vectoriel.

$$\begin{aligned} (\star): \quad & y' + a(x)y = 0 \text{ et } y(x_0) = 0 \\ \iff & \forall x \in I, y(x) = -\int_{x_0}^{x} a(u)y(u)\, du \end{aligned}$$

$$\begin{aligned} T : E^I &\longrightarrow E^I \\ y &\longmapsto \left(x \mapsto -\int_{x_0}^{x} a(u)y(u)\ du \right) \end{aligned}$$

donc $(\star) \iff T(y) = y$

Chapitre 7

Développements limités

Définition : Soit f une fonction définie au voisinage d'un point $a \in \mathbb{R}$.

On dit que f possède un développment limité d'ordre n au voisinage de a s'il existe des réels $(c_0, \dots, c_n) \in \mathbb{R}^{n+1}$ tels que

$$f(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \cdots + c_n(x-a)^n + \underset{x\to a}{o}\big((x-a)^n\big).$$

En particulier, avec $a = 0$, on a

$$f(x) = \underbrace{c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n}_{\text{développement de Taylor}} + \underbrace{\underset{x\to 0}{o}(x^n)}_{\text{reste}}.$$

Théorème (Taylor-Young) **:** Si f est de classe $\mathscr{C}^n$ (i.e. f définie et dérivable n fois et $f^{(n)}$ est continue) au voisinage de a, alors f admet un développement limité d'ordre n au voisinage de a est

$$f(x) = f(a)+(x-a)f'(a)+(x-a)^2\frac{f''(a)}{2!}+\cdots+(x-a)^n\frac{f^{(n)}(a)}{n!}+\underset{x\to a}{o}\big((x-a)^n\big).$$

□

Remarque :
Cette formule est à éviter en pratique : il est bien trop difficile de calculer $f^{(n)}$ pour tout n.

Cependant, on peut quand même en déduire le développement limité de exp, cos, sin et $x \mapsto (1+x)^\alpha$ en 0.

Corollaire :

$$e^x = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!} + \underset{x\to 0}{o}(x^n),$$
$$\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots + (-1)^n \frac{x^{2n}}{(2n)!} + \underset{x\to 0}{o}(x^{2n}),$$
$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + \underset{x\to 0}{o}(x^{2n+1}),$$
$$\forall \alpha \in \mathbb{R}, (1+x)^\alpha = 1 + \alpha x + \alpha(\alpha-1)\frac{x^2}{2!} + \alpha(\alpha-1)(\alpha-2)\frac{x^3}{3!} + \cdots$$
$$+ \alpha(\alpha-1)\cdots\big(\alpha-(\alpha-1)\big)\frac{x^n}{n!} + \underset{x\to 0}{o}(x^n).$$

Remarque :
Avec $\alpha = -1$, on obtient le développement limité de $\dfrac{1}{1+x}$ en 0 :

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + \underset{x\to 0}{o}(x^n).$$

On en déduit donc le développement limité en 0 de $\dfrac{1}{1-x}$:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots + x^n + \underset{x\to 0}{o}(x^n)$$

Avec $\alpha = \dfrac{1}{2}$, on obtient le développement limité à l'ordre 2 de $\sqrt{1+x}$:

$$\sqrt{1+x} = 1 + \frac{x}{2} - \frac{x^2}{8} + \underset{x\to 0}{o}(x^2).$$

Théorème (primitivation) **:** Soit f une fonction continue en a ayant un développement limité d'ordre n au voisinage de a. Soient $(c_0, c_1, \ldots, c_n) \in \mathbb{R}^{n+1}$ tels que

$$f(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \cdots + c_n(x-a)^n + \underset{x\to a}{o}\big((x-a)^n\big).$$

Soit F une primitive de f. Alors F a un développement limité d'ordre $n+1$ au voisinage de a et

$$F(x) = F(a) = c_0(x-a) + c_1\frac{(x-a)^2}{2} + \cdots + c_n\frac{(x-a)^{n+1}}{n+1} + \underset{x\to a}{o}\big((x-a)^{n+1}\big).$$

□

Corollaire : En primitivant le développement limité de $\dfrac{1}{x+1}$, on obtient le développement limité de $\ln(1+x)$:

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots + (-1)^n \frac{x^{n+1}}{n+1} + \underset{x\to 0}{\wp}(x^{n+1}).$$

On en déduit aussi le développement limité de Arctan :

$$\operatorname{Arctan} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots + (-1)^n \frac{x^{2n+1}}{2n+1} + \underset{x\to 0}{\wp}(x^{2n+1}).$$

□

Exercice (*Calculer $DL_5(0)$ de* tan) :

Méthode 1 (quotient) : $\tan x = \dfrac{\sin x}{\cos x}$.

On a

$$\begin{cases} \sin x = x - \dfrac{x^3}{6} + \dfrac{x^5}{120} + \wp(x^5), \\ \cos x = 1 - \dfrac{x^2}{2} + \dfrac{x^4}{24} + \wp(x^5). \end{cases}$$

On calcule d'abord le développement limité de $\dfrac{1}{\cos x}$:

$$\begin{aligned} \frac{1}{\cos x} &= \frac{1}{1 - \frac{x^2}{2} + \frac{x^4}{24} + \wp(x^5)} \\ &= \frac{1}{1+u} \text{ avec } u = -\frac{x^2}{2} + \frac{x^4}{24} + \wp(x^5) \xrightarrow[x\to 0]{} 0 \\ &= 1 - u + u^2 + \wp(u^2) \\ &= 1 - \left(-\frac{x^2}{2} + \frac{x^4}{24} + \wp(x^5)\right) \\ &\quad + \left(-\frac{x^2}{2} + \frac{x^4}{24} + \wp(x^5)\right) \\ &\quad + \wp\left(\left(-\frac{x^2}{2} + \frac{x^4}{24} + \wp(x^5)\right)^2\right) \\ &= 1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + \wp(x^5) \\ &= 1 + \frac{x^2}{2} + \frac{5x^4}{24} + \wp(x^5). \end{aligned}$$

On en déduit le développement limité de $\tan x$:

$$\begin{aligned}\tan x &= \left(x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5)\right)\left(1 + \frac{x^2}{2} + \frac{5x^4}{24} + o(x^5)\right)\\ &= x + \frac{x^3}{2} + \frac{5x^5}{24} - \frac{x^3}{6} - \frac{x^5}{12} + \frac{x^5}{120} + o(x^5)\\ &= x + \frac{x^3}{3} + \frac{2x^5}{15} + o(x^5).\end{aligned}$$

À connaître :

$$\boxed{\tan x = x + \frac{x^3}{3} + \underset{x\to 0}{o}(x^3).}$$

Méthode 2 (déterminer les coefficiants)

On identifie les coefficants :

$$\begin{aligned}\sin x &= (\tan x)(\cos x)\\ &= \left(c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + o(x^5)\right)\\ &\times \left(1 - \frac{x^2}{2} + \frac{x^4}{24} + o(x^5)\right)\\ &= c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + o(x^5)\\ &- c_0\frac{x^2}{2} - c_1\frac{x^3}{2} - c_2\frac{x^4}{2} - c_3\frac{x^5}{2} + c_0\frac{x^4}{24} + c_1\frac{x^5}{24}\end{aligned}$$

Par unicité du développement limité,

$$\begin{cases} c_0 = 0\\ c_1 = 1\\ c_2 - \dfrac{c_0}{2} = 0\\ c_3 - \dfrac{c_1}{2} = -\dfrac{1}{6}\\ c_4 - \dfrac{c_2}{2} + \dfrac{c_0}{24} = 0\\ c_5 - \dfrac{c_3}{2} + \dfrac{c_1}{24} = \dfrac{1}{120}\end{cases}$$

et donc

$$\begin{cases} c_0 = c_2 = c_4 = 0\\ c_1 = 1\\ c_3 = \dfrac{1}{3}\\ c_5 = \dfrac{2}{15}\end{cases}$$

Méthode 3 (primitivation)

On sait que

$$\frac{\tan x - \tan 0}{x - 0} \xrightarrow[x\to 0]{} \tan'(0) = 1$$

donc $\tan x \sim x$ et donc $\tan x = x + o(x)$.

D'où

$$\begin{aligned}\tan'(x) = 1 + \tan^2(x) &= 1 + \big(x + o(x)\big)^2 \\ &= 1 + x^2 + o(x^2).\end{aligned}$$

En intégrant, on en déduit que

$$\tan x = \tan 0 + x + \frac{x^3}{3} + o(x^3)$$

Donc,

$$\begin{aligned}\tan'(x) &= 1 + \tan^2 x \\ &= 1 + \left(x + \frac{x^3}{3} + o(x^3)\right)^2 \\ &= 1 + x^2 + \frac{x^6}{9} + o(x^6) + 2\frac{x^4}{3} + o(x^4) + o(x^6) \\ &= 1 + x^2 + \frac{2}{3}x^4 + o(x^4)\end{aligned}$$

On en déduit donc le développement limité à l'ordre 5 de tan :

$$\tan x = \underbrace{\tan 0}_{\substack{\| \\ 0}} + \frac{x^3}{3} + \frac{2}{15}x^5 + o(x^5)$$

Chapitre 8

Ensembles, applications, relations et lois de composition

1 Théorie naïve des ensembles

Définition : Un ensemble est une collection finie ou infinie d'objets de même nature ou non. L'ordre de ces objets n'a pas d'importance.

Exemple : 1. $\{1, x \mapsto x^2, \{1\}\}$ est un ensemble : ses éléments dont l'entier 1, la fonction $x \mapsto x^2$ et un ensemble contenant uniquement 1 (un singleton).
2. $\mathbb{N}$ est un ensemble infini

Remarque (Notation) :
Soit E un ensemble et x un objet de E.
On écrit $x \in E$ ou bien $x \ni E$.

Remarque (B Paradoxe) :
On note Ω l'ensemble de tous les ensembles. Alors, $\Omega \in \Omega$.
Ce n'est pas le cas de tous les ensembles :

$$\mathbb{N} \notin \mathbb{N} \text{ car } \mathbb{N} \text{ n'est pas un entier}$$

On distingue donc 2 types d'ensembles :

— ceux qui vérifient $E \notin E$, on dit qu'ils sont ordinaires
— ceux qui vérifient $E \in E$, on dit qu'ils sont extra-ordinaires

On note O l'ensemble de tous les ensembles ordinaires.

— Supposons O ordinaire. Alors, $O \notin O$
Or, O est ordinaire et donc $O \in O$ ↯
— Supposons O extra-ordinaire.
Alors $O \in O$ et donc O ordinaire ↯

C'est un paradoxe

Pour éviter ce type de paradoxe, on a donné une définition axiomatique qui explique quelles sont les opérations permettant de combiner des ensembles pour en faire un autre.

Définition : Soit E un ensemble et F un autre ensemble. On dit que E et F sont égaux (noté $E = F$) si E et F contiennent les mêmes objets.

Exemple : 1. $E = \{1, 2, 3\}$ et $F = \{3, 2, 1, 2\}$
On a bien $E = F$.

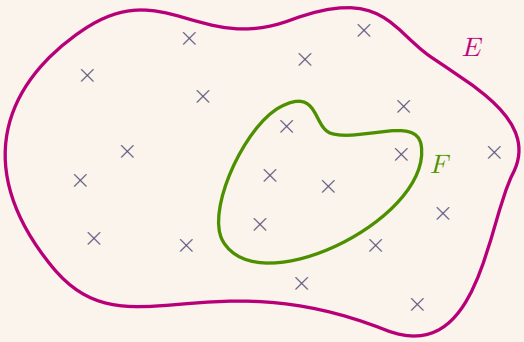
2. $\mathbb{N} \neq \mathbb{Z}$ car $\begin{cases} -1 \in \mathbb{Z} \\ -1 \notin \mathbb{N} \end{cases}$

3. $E = \{0, \{0\}\} \neq \{0\} = F$
car $\begin{cases} \{0\} \in E \\ \{0\} \notin F \end{cases}$
mais, $F \in E$

Définition : L'ensemble vide, noté $\emptyset$ est le seul ensemble à n'avoir aucun élément.

Définition : Soient E et F deux ensembles. On dit que F est inclus dans E, noté $F \subset E$ ou $E \supset F$ si tous les éléments de F sont aussi des éléments de E.

$$\forall x \in F, x \in E$$



Proposition : Pour tout ensemble E, $\subset E$

Preuve (par l'absurde) *:*
Si $\not\subset E$ alors $\exists x \in , x \notin E$: une contradiction $\lightning$

□

Exemple : 1. $E = \{1, 2, 3\}$ et $F = \{1, 3\}$

On a $F \subset E$ mais pas $E \subset F$ car $\begin{cases} 2 \in E \\ 2 \notin F \end{cases}$

2. $F = \{0\}$ et $E = \{0, \{0\}\}$

   — $F \in E$ car $\{0\} \in E$
   — $F \subset E$ car $0 \in E$

3. $E = \{\{0\}\}; F = \{0\}$
   — $F \not\subset E$ car $0 \notin E$
   — $F \in E$

4. $E = \{\{\{0\}\}\}; F = \{0\}$
   — $F \notin E$
   — $F \not\subset E$
   — $\subset F$
   — $\subset E$

Définition : Soit E un ensemble. On peut former l'ensemble de toutes les parties de E (une partie de E est un ensemble F avec $F \subset E$). On le note $\mathcal{P}(E)$

$$A \in \mathcal{P}(E) \iff A \subset E$$

EXEMPLE : 1. $E = \{42\}$
Les sous-ensembles de E sont et $\{42\} = E$ donc

$$\mathcal{P}(E) = \{, \{42\}\}$$

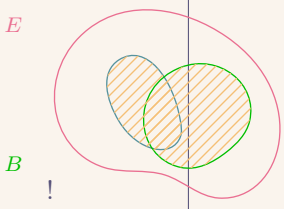
2. $\mathcal{P}() = \{\}$
3. $E = \{0, 1\}$ donc $\mathcal{P}(E) = \{, \{0\}, \{1\}, \{0, 1\}\}$
4. $E = \{, \{\}\}$ donc $\mathcal{P}(E) = \{, \{\}, \{\{\}\}, \{, \{\}\}\}$
5. $E = \{, \{\}\}$

$$\begin{aligned}\mathcal{P}(\mathcal{P}(E)) &= \mathcal{P}(\{, \{\}, \{\{\}\}, E) \\ &= \{, \{\}, \{\{\}\}, \{\{\{\}\}\}, \{E\}, \{, \{\}\}, \{, \{\{\}\}\}, \{, E\}, \{\{\}, \\ &\quad \{\{\}\}\}, \{\{\}, E\}, \{\{\{\}\}, E\}, \{, \{\}, \{\{\}\}\}, \{, \{\}, E\}, \\ &\quad \{, \{\{\}\}, E\}, \{\{\}, \{\{\}\}, E\}, \{, \{\}, \{\{\}\}, E\}\}\end{aligned}$$

Définition : Soit E un ensemble et $A, B \in \mathcal{P}(E)$

1. La réunion de A et B est

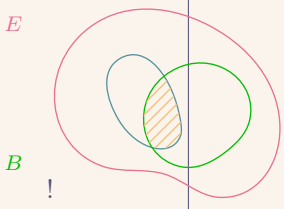
$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$



!

2. L'intersection de A et B est

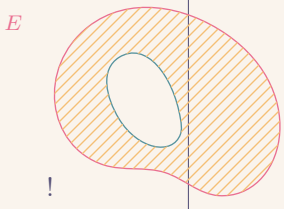
$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$



!

3. Le complémentaire de A dans E est

$$E \setminus A = \{x \in E \mid x \notin A\} = C_E A$$

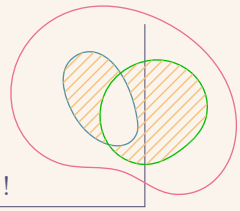


!

4.

La différence symétrique de A et B est

$$A\Delta B = \{x \in E \mid (x \in A \text{ et } x \notin B) \text{ ou } (x \notin A \text{ et } x \in B)\}$$
$$= (A \cup B) \setminus (A \cap B)$$



!

Proposition : Soit E un ensemble et $A, B, C \in \mathcal{P}(E)$

1. $A \cap A = A$
2. $B \cap A = A \cap B$
3. $A \cap (B \cap C) = (A \cap B) \cap C$
4. $A \cap \ = $
5. $A \cap E = A$
6. $A \cup A = A$
7. $B \cup A = A \cup B$
8. $A \cup (B \cup C) = (A \cup B) \cup C$
9. $A \cup \ = A$
10. $A \cup E = E$
11. $(E \setminus A) \setminus A = E \setminus A$
12. $E \setminus (E \setminus A) = A$
13. $E \setminus \ = E$
14. $E \setminus E = $
15. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
16. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
17. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$
18. $E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B)$

Preuve : 16. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

— Soit $x \in A \cap (B \cup C)$ donc $x \in A$ et $x \in B \cup C$

Cas 1 $x \in B$, alors $x \in A \cap B$ et donc $x \in (A \cap B) \cup (A \cap C)$
Cas 2 $x \in C$, alors $x \in A \cap C$ et donc $x \in (A \cap B) \cup (A \cap C)$

On a prouvé

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$$

— Soit $x \in (A \cap B) \cup (A \cap C)$

Cas 1 $x \in A \cap B$ donc $x \in A$ et $x \in B$ donc $x \in B \cup C$ et donc $x \in A \cap (B \cup C)$
Cas 2 $x \in A \cap C$ donc $x \in A$ et $x \in C$ donc $x \in B \cup C$ et donc $x \in A \cap (B \cup C)$

On a prouvé

$$A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C)$$

17. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$

— Montrons que $x \in E \setminus (A \cup B) \implies x \in (E \setminus A) \cap (E \setminus B)$
Soit $x \in E \setminus (A \cup B)$ donc $x \notin A \cup B$

— Si $x \in A$, alors $x \in A \cup B$ ↯
donc $x \notin A$ i.e. $x \in E \setminus A$

— Si $x \in B$ alors, $x \in A \cup B$ ↯
Donc $x \notin B$ i.e. $x \in E \setminus B$

On en déduit que $x \in (E \setminus A) \cap (E \setminus B)$

— $x \in (E \setminus A) \cap (E \setminus B)$. Montrons que $x \in E \setminus (A \cup B)$
On suppose que $x \notin E \setminus (A \cup B)$ donc $x \in A \cup B$

— Si $x \in A$, on a une contradiction car $x \in E \setminus A$

— Si $x \in B$, on a une contradiction car $x \in E \setminus B$

donc $x \in E \setminus (A \cup B)$

□

2 Applications

Définition : Une application f est la donnée de

— un ensemble E appelé ensemble de départ

— un ensemble F appelé ensemble d'arrivée

— une fonction qui associe à tout élément x de E un unique élément de F noté $f(x)$

L'application est notée

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

Exemple : 1. Soit $\mathcal{P}$ le plan (affine) et $A \in \mathcal{P}$. Soit $\mathcal{D}$ l'ensemble des droites.

$$\begin{aligned} f : \mathcal{P} \setminus \{A\} &\longrightarrow \mathcal{D} \\ B &\longmapsto (AB) \end{aligned}$$

2. $E = \mathscr{C}^1([0,1], \mathbb{R})$ l'ensemble des fonctions à valeurs réelles de classe $\mathscr{C}^1$ sur $[0,1]$
$F = \mathscr{C}^0([0,1], \mathbb{R})$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \end{aligned}$$

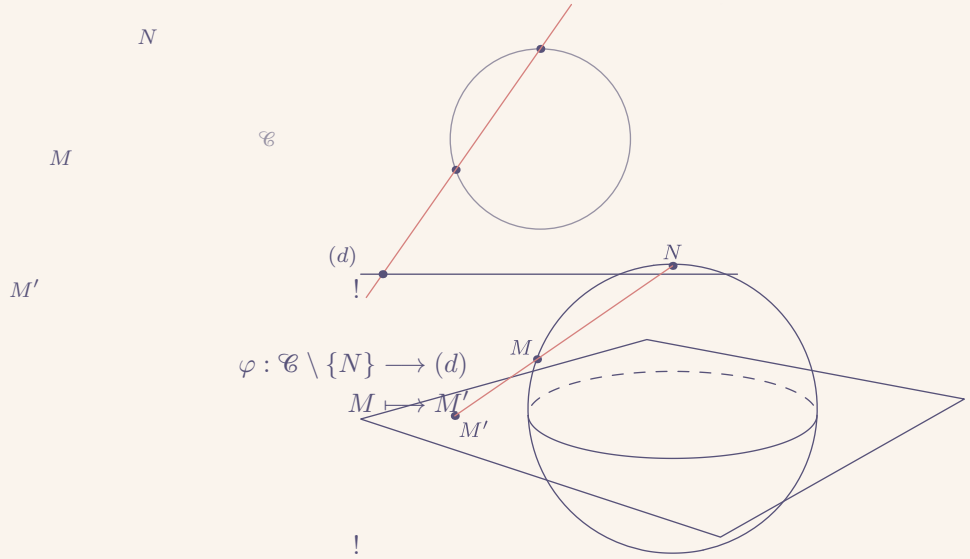
3. $E = \mathscr{C}^1([0,1], \mathbb{R})$ et $F = \mathbb{R}$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f'\left(\frac{1}{2}\right) \end{aligned}$$

4. $E = [0,1]$ et $F = \mathscr{C}^0([0,1], \mathbb{R})$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ x &\longmapsto \int_a^x t^2 \ln(t)\, dt \end{aligned}$$

5.

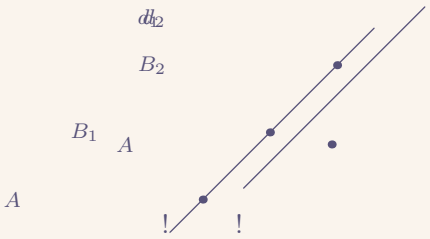


6.

Définition : Soit $f : E \to F$ une application. On dit que f est

- injective si tout élément de F a au plus un antécédent par f
- bijective si tout élément de F a un unique antécédent par f
- surjective si tout élément de F a au moins un antécédent par f

Exemple (suite des exemples précédents) : 1. L'application n'est ni injective ni surjective



B_1 et B_2 sont deux antécédants de d_1
d_2 n'a pas d'antécédant par f

2. L'application n'est pas injective :
   - $f : x \mapsto x$ est continue
   - $x \mapsto \dfrac{x^2}{2}$ et $x \mapsto \dfrac{x^2}{2} + 42$ sont deux antécédants de f.

   Mais, l'application est surjective d'après le théorème fondamental de l'analyse
3. L'application n'est pas injective ($x \mapsto 0$ et $x \mapsto 42$ sont deux antécédants de 0) mais elle est surjective ($\forall x \in \mathbb{R}, x \mapsto ax$ est un antécédant de a).
4. L'application est injective mais pas surjective (les images sont des primitives de $x \mapsto x^2 \ln(x)$)

5. et 6. sont bijectives

Définition : Soit $f : E \to F$ et $g : F \to G$. L'application notée $g \circ f$ est définie par

$$\begin{aligned} g \circ f : E &\longrightarrow G \\ x &\longmapsto g(f(x)) \end{aligned}$$

On dit que c'est la composée de f et g.

Proposition : Soient $f : E \to F, g : F \to G, h : G \to G$. Alors, $h \circ (g \circ f) = (h \circ g) \circ f$

Preuve :
Par définition, $g \circ f : E \to F$ donc $h \circ (g \circ f) : E \to H$
et $h \circ g : F \to H$ donc $(h \circ g) \circ f : E \to H$ Soit $x \in E$.

$$\begin{aligned} h \circ (g \circ f)(x) &= h(g \circ f(x)) \\ &= h(g(f(x))) \end{aligned}$$

$$\begin{aligned} (h \circ g) \circ f(x) &= h \circ g(f(x)) \\ &= h(g(f(x))) \end{aligned}$$

Donc, $h \circ (g \circ f)(x) = (h \circ g) \circ f(x)$ □

Remarque (B Attention) :
En général, $g \circ f \neq f \circ g$

Par exemple, $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array}$ et $g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{x} \end{array}$

Alors, $f \circ g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x \end{array}$ et $g \circ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & |x| \end{array}$

donc $f \circ g \neq g \circ f$

Proposition : Soient $f : E \to F$ et $g : F \to G$

1. Si $g \circ f$ est injective, alors f est injective
2. Si $g \circ f$ est surjective, alors g est surjective

3. Si f et g sont surjectives, alors $g \circ f$ est surjective
4. Si f et g sont injectives, alors $g \circ f$ est injective

Preuve : 1. On suppose $g \circ f$ injective. On veut montrer que f est injective. Soient $(x, y) \in E^2$. On suppose $f(x) = f(y)$. Montrons que $x = y$.
Comme $f(x) = f(y)$, $g(f(x)) = g(f(y))$ i.e. $g \circ f(x) = g \circ f(y)$
Or, $g \circ f$ injective donc $x = y$

2. On suppose $g \circ f$ surjective. On veut montrer que g est surjective. Soit $y \in G$. On cherche $x \in F$ tel que $g(x) = y$.
Comme $g \circ f : E \to G$ surjective, y a un antécédant $z \in E$ par $g \circ f$.
On pose $x = f(z) \in F$ et on a bien $g(x) = y$
3. On suppose f et g injectives. Montrons que $g \circ f$ injective. Soient $x, y \in E$. On suppose $g \circ f(x) = g \circ f(y)$. Montrons $x = y$
On sait que $g(f(x)) = g(f(y))$. Comme g est injective, $f(x) = f(y)$ et comme f est injective, $x = y$
4. On suppose f et g surjectives. Soit $y \in G$. On cherche $x \in E$ tel que $g \circ f(x) = y$
Comme g est surjective, y a un antécédant $z \in F$ par g
Comme f est surjectives, z a un antécédant $x \in E$ par f
On en déduit $g \circ f(x) = g(f(x)) = g(z) = y$

□

Remarque :
$f : E \longrightarrow F$

$$f \text{ injective} \iff \Big(\forall (x, y) \in E^2, f(x) = f(y) \implies x = y\Big)$$

Définition : Soit $f : E \to F$ une bijection. L'application $\begin{cases} F & \longrightarrow & E \\ y & \longmapsto & \text{l'unique antécédent de } y \text{ par } f \end{cases}$ est la réciproque de f notée f^{-1}

Définition : L'identité de E est id_E : $\begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x \end{array}$

Proposition : Soient $f : E \to F$ et $g : F \to E$

$$\left.\begin{array}{l} f \circ g = \mathrm{id}_F \\ g \circ f = \mathrm{id}_E \end{array}\right\} \iff \begin{cases} f \text{ bijective} \\ f^{-1} = g \end{cases}$$

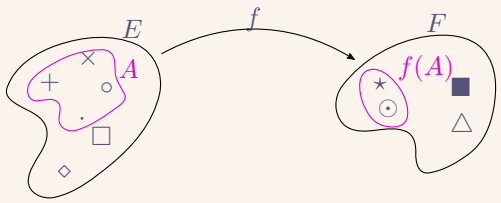
Preuve (déjà faite) *:*

□

Définition : Soit $f : E \to F$

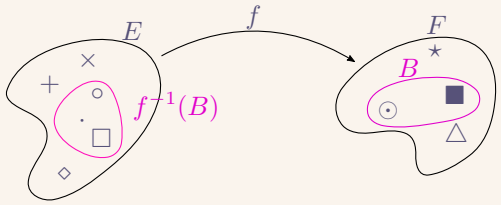
1. Soit $A \in \mathcal{P}(E)$. L'image directe de A par f est

$$f(A) = \{f(x) \mid x \in A\}$$



2. Soit $B \in \mathcal{P}(F)$. L'image réciproque de B par f est

$$f^{-1}(B) = \{x \in E | f(x) \in B\}$$



Remarque :

— $y \in f(A) \iff \exists x \in A, y = f(x)$,
— $x \in f^{-1}(B) \iff f(x) \in B$.

Proposition : Soient $f : E \to F$, $A \in \mathcal{P}(E)$ et $F \in \mathcal{P}(F)$.

1. $f^{-1}\big(f(A)\big) \supset A$,
2. Si f est injective alors $f^{-1}\big(f(A)\big) = A$,
3. $f\big(f^{-1}(B)\big) \subset B$,
4. Si f est surjective, alors $f\big(f^{-1}(B)\big) = B$.

Preuve : 1. Soit $x \in A$. Montrons que $x \in f^{-1}\big(f(A)\big)$ i.e. montrons que $f(x) \in f(A)$. Comme $x \in A$, $f(x) \in f(A)$.

2. On suppose f injective. Montrons que $f^{-1}\big(f(A)\big) = A$. Soit $x \in f^{-1}\big(f(A)\big)$, montrons que $x \in A$. On sait que $f(x) \in f(A)$. Donc, il existe $a \in A$ tel que $f(x) = f(a)$. Or, f est injective et donc $x = a$. On en déduit que $x \in A$.

   D'après 1., on sait que $f^{-1}\big(f(A)\big) \supset A$. On a montré $f^{-1}\big(f(A)\big) \subset A$. Donc
   $$f^{-1}\big(f(A)\big) = A.$$
3. Soit $y \in f\big(f^{-1}(B)\big)$. Montrons $y \in B$. On sait qu'il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. On a donc $f(x) \in B$ et donc $y \in B$.
4. On suppose f surjective, montrons $B \subset f\big(f^{-1}(B)\big)$. Soit $y \in B$, montrons $y \in f\big(f^{-1}(B)\big)$. On cherche $x \in f^{-1}(B)$ tel que $y = f(x)$. C'est à dire, on cherche $x \in E$ tel que $f(x) \in B$ et $y = f(x)$. On sait que f est surjective donc y a un antécédant $x \in E$ tel que $B \ni y = f(x)$.

   On vient de montrer $B \subset f\big(f^{-1}(B)\big)$ et on a montré dans 3. que $B \supset f\big(f^{-1}(B)\big)$. On en déduit que
   $$f\big(f^{-1}(B)\big) = B.$$

□

Proposition : Soit $f : E \to F$ et $(A, B) \in \mathcal{P}(F)^2$. Alors

$$\begin{cases} f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), & (1) \\ f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B). & (2) \end{cases}$$

Preuve :
Soit $x \in E$.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\iff f(x) \in A \cup B \\ &\iff f(x) \in A \text{ ou } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ ou } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

$$\begin{aligned} x \in f^{-1}(A \cap B) &\iff f(x) \in A \cap B \\ &\iff f(x) \in A \text{ et } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ et } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

□

Proposition : Soient $f : E \to F$ et $(A, B) \in \mathcal{P}(E)^2$.

1. $f(A \cap B) \subset f(A) \cap f(B)$
2. Si f est injective, $f(A \cap B) = f(A) \cap f(B)$
3. $f(A \cup B) = f(A) \cup f(B)$.

Preuve :

1. Soit $y \in f(A \cap B)$. Soit $x \in A \cap B$ tel que $y = f(x)$. Comme $x \in A$, $f(x) \in f(A)$ et comme $x \in B$, $f(x) \in f(B)$ et donc $y \in f(A) \cap f(B)$
2. On suppose f injective. Soit $y \in f(A) \cap f(B)$.
   Comme $y \in f(A)$, il existe $a \in A$ tel que $y = f(a)$.
   Comme $y \in f(B)$, il existe $b \in B$ tel que $y = f(b)$.

   Comme f est injective, $a = b$ et donc $a \in A \cap B$. On en déduit que

   $$y = f(a) \in f(A \cap B).$$

3. Soit $y \in F$. Alors

$$\begin{aligned} y \in f(A \cup B) &\iff \exists x \in A \cup B; y = f(x) \\ &\iff (\exists x \in A \text{ ou } \exists x \in B), y = f(x) \\ &\iff y \in f(A) \text{ ou } y \in f(B) \\ &\iff y \in f(A) \cup f(B). \end{aligned}$$

□

Remarque (Contre-exemple pour 2.) :
Cas d'une application qui n'est pas injective

On pose $A = \mathbb{R}_\star^+$, $B = \mathbb{R}_\star^-$ et

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto x^2 \end{aligned}$$

On a $A \cap B =$ donc $f(A \cap B) =$.

Or, $\left.\begin{array}{l} f(A) = \mathbb{R}_\star^+ \\ f(B) = \mathbb{R}_\star^+ \end{array}\right\}$ donc $f(A) \cap f(B) = \mathbb{R}_\star^+$.

On a

$$f(A \cap B) \neq f(A) \cap f(B).$$

Définition : Soit $f : E \to F$ et $A \in \mathcal{P}(E)$.

La restriction de f à A est

$$\begin{aligned} f_{|A} : A &\longrightarrow F \\ x &\longmapsto f(x)a \end{aligned}$$

On dit aussi que f est **un** prolongement de $f_{|A}$.

Remarque (Notation) :
L'ensemble des applications de E dans F est noté F^E.

Exemple :

On pose $f : \begin{array}{ccc} \mathbb{R}^\star & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{1}{x} \end{array}$ et $g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \dfrac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{array}$ un prolongement de f car $g_{|\mathbb{R}^\star} = f$.

L'applications $h : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \dfrac{1}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases} \end{array}$ est un autre prolongement de f.

3 Relations binaires

Définition : Soit E un ensemble. Un relation (binaire) sur E est un prédicat définit sur E^2.

Exemple : 1. Avec $E = \mathbb{C}$, $=$ est une relation binaire,
2. Avec $E = \mathbb{R}$, $\leqslant$ est une relation binaire,
3. Avec E l'humanité et la relation binaire $\wedge$:

$$x \wedge y \iff x \text{ et } y \text{ ont la même mère.}$$

Définition : Soit E un ensemble, $\diamond$ une relation sur E. On dit que $\diamond$ est un relation d'équivalence si

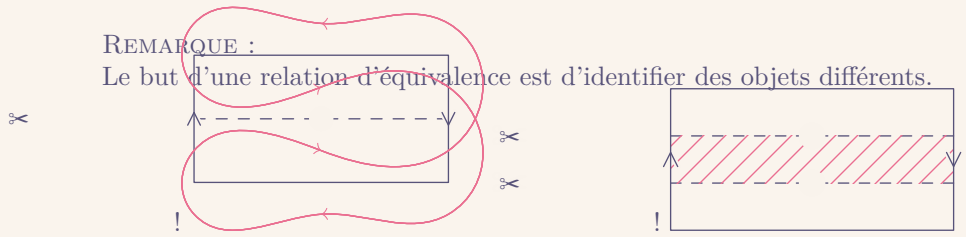
1. $\forall x \in E, x \diamond x$, (réflectivité)
2. $\forall x, y, \in E, x \diamond y \implies y \diamond x$, (symétrie)
3. $\forall x, y, z \in E, \left.\begin{array}{l} x \diamond y \\ y \diamond z \end{array}\right\} \implies x \diamond z$ (transitivité)

Exemple :
Avec $E = \mathbb{Z}$ et

$$x \diamond y \iff x \equiv y \ [3]$$

" $\diamond$ " est une relation d'équivalence.

Remarque :
Le but d'une relation d'équivalence est d'identifier des objets différents.



Définition : Soit E un ensemble et $\diamond$ une relation d'équivalence sur E. Soit $x \in E$. La classe de x (modulo $\diamond$) est

$$\mathscr{Cl}_{\diamond}(x) = \mathscr{Cl}(x) = \overline{x} = \{y \in E \mid y \diamond x\}.$$

Exemple : 1. Avec $E = \mathbb{C}$ et $\diamond =$ " $=$ ",

$$\forall z \in \mathbb{C}, \overline{z} = \mathscr{Cl}(z) = \{z\}.$$

2. Avec $E = \mathbb{Z}$ et $\diamond =$ congruence modulo 5, on a

$$\overline{0} = \{5k \mid k \in \mathbb{Z}\} \qquad \overline{1} = \{5k+1 \mid k \in \mathbb{Z}\}$$
$$\overline{2} = \{5k+2 \mid k \in \mathbb{Z}\} \qquad \overline{3} = \{5k+3 \mid k \in \mathbb{Z}\}$$
$$\overline{4} = \{5k+4 \mid k \in \mathbb{Z}\} \qquad \overline{5} = \overline{0}$$

On constate que

$$x \equiv y \ [5] \iff \overline{x} = \overline{y}.$$

Proposition : Soit E un ensemble muni d'une relation d'équivalence $\diamond$. Alors

$$\forall x, y \in E, x \diamond y \iff \overline{x} = \overline{y}.$$

Preuve :
Soient $x, y \in E$.

- On suppose $x \diamond y$. Soit $z \in \overline{x}$. On sait que $z \diamond x$ et $y \diamond x$. Par transitivité, on en déduit que $z \diamond y$ et donc $z \in \overline{y}$.
- Soit $z \in \overline{y}$, donc $y \diamond z$. Or $x \diamond y$. Comme $\diamond$ est symétrique, on a $y \diamond x$ et par transitivité, on a donc $z \diamond x$. Donc $z \in \overline{x}$.
- On suppose $\overline{x} = \overline{y}$. $\diamond$ réfléctive donc $x \diamond x$ et donc $x \in \overline{x} = \overline{y}$ donc $x \in \overline{y}$ et donc $x \diamond y$.

□

Hors-Programme

Définition : Soit E un ensemble et $\diamond$ une relation d'équivalence.

L'ensemble

$$\{\overline{x} \mid x \in E\} = {}^{E}/_{\diamond}$$

est appelé quotient de E modulo $\diamond$.

Exemple : 1. $E = \mathbb{Z}$ et $\diamond$ = congruence modulo 5 :

$${}^{E}/_{\diamond} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = {}^{\mathbb{Z}}/_{5\mathbb{Z}}$$

2. *Construction de* $\mathbb{Q}$

On suppose avoir déjà construit $\mathbb{Z}$ mais pas $\mathbb{Q}$: on veut donc donner un définition de ${}^{p}/_{q}$ sans parler de division.

On pose

$$E = \mathbb{Z} \times \mathbb{N}^{\star} = \{(p, q) \mid p \in \mathbb{Z}, q \in \mathbb{N}^{\star}\}.$$

Soit $\sim$ la relation définie par

$$(p, q) \sim (p', q') \iff pq' = p'q$$

Montrons que $\sim$ est une relation d'équivalence.

— Soient $(p, q) \in E$. $\sim$ est réfléctive car $(p, q) \sim (p, q) \iff pq = pq$.

— Soient $(p, q), (p', q') \in E$. On suppose $(p, q) \sim (p', q')$.

$$\begin{aligned}(p, q) \sim (p', q') &\iff pq' = p'q \\ &\iff p'q = pq' \\ &\iff (p', q') \sim (p, q)\end{aligned}$$

Donc $\sim$ est symétrique.

— Soient $(p, q), (p', q'), (p'', q'') \in E$. On suppose

$$\begin{cases}(p, q) \sim (p', q') \\ (p', q') \sim (p'', q'')\end{cases}$$

On sait que

$$(p, q) \sim (p'', q'') \iff pq'' = p''q$$

Or,

$$\begin{cases}pq' = qp' \\ p'q'' = p''q'\end{cases} \quad \text{donc } pq'p'q'' = p'q'p''q'$$

Donc

$$p'q'(pq'' - p''q) = 0$$

et donc

$$p' = 0 \text{ ou } pq'' - p''q = 0$$

Si $p' = 0$, alors $\begin{cases} pq' = 0 \\ p''q' = 0 \end{cases}$ et donc $\begin{cases} p = 0 \\ p'' = 0 \end{cases}$. On a donc

$$pq'' = 0 = p''q$$

Si $p' \neq 0$, on a $pq'' - p''q = 0$ et donc

$$pq'' = p''q$$

On a donc $(p, q) \sim (p'', q'')$.

On pose $\mathbb{Q} = {}^{E}/_{\sim}$ et

$$\forall (p, q) \in E,\ \frac{p}{q} = \mathscr{C}\ell\big((p, q)\big).$$

Ainsi,

$$\begin{aligned} \frac{p}{q} = \frac{p'}{q'} &\iff \mathscr{C}\ell\big((p, q)\big) = \mathscr{C}\ell\big((p', q')\big) \\ &\iff (p, q) \sim (p', q') \\ &\iff pq' = p'q \end{aligned}$$

3. *Construction de $\mathbb{Z}$ à partir de $\mathbb{N}$*

   On pose $E = \mathbb{N} \times \mathbb{N}^\star$ et $\sim$ la relation $(p, q) \sim (p', q') \iff p + q' = p' + q$.

   $\sim$ est une relation d'équivalence. On pose donc $\mathbb{Z} = {}^{\mathbb{N}}/_{\sim}$ et pour $n \in \mathbb{N}$, on définit n par $\mathscr{C}\ell\big((n, 0)\big)$ et $-n$ par $\mathscr{C}\ell\big((0, n)\big)$.

4. *Constrcution de $\mathbb{C}$ à partir de $\mathbb{R}$*

   On pose E l'ensemble des polynômes à coefficients réels ($E = \mathbb{R}[X]$) et $\diamond$ la relation d'équivalence

   $$P \diamond Q \iff P \equiv Q \ \left[x^2 + 1\right]$$

   On pose $\mathbb{C} = {}^{E}/_{\diamond}$.

Il manque une partie du cours ici

Définition : Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E.

On dit que $(A_i)_{i\in I}$ est une partition de E si

$$\begin{cases} E = \bigcup_{i\in I} A_i \\ \forall i \neq j, A_i \cap A_j = \end{cases}$$

On a donc

$$\forall x \in E, \exists! i \in I, x \in A_i.$$

Proposition : Soit E un ensemble muni d'une relation d'équivalence $\diamond$. Les classes d'équivalences de E modulo $\diamond$ forment une partition de E.

Preuve : — Soit $x \in E$. On sait que $x \diamond x$ donc $\overline{x} \ni x$. On a montré $E \subset \bigcup_{y\in E} \overline{y}$.

— $\forall y \in E, \overline{y} \subset E$ donc $E \supset \left(\bigcup_{y\in E} \overline{y} \right)$.

— Soit $x, y \in E$ tel que $\overline{x} \neq \overline{y}$. Montrons que $\overline{x} \cap \overline{y} = $. Soit $z \in \overline{x} \cap \overline{y}$. $z \in \overline{x}$ donc $z \diamond x$. De même, $z \in \overline{y}$ donc $z \diamond y$. Par transitivité, $x \diamond y$ et donc $\overline{x} = \overline{y}$: une contradiction.

□

Proposition : Soit E un ensemble et $(A_i)_{i\in I}$ une partition de E telle que

$$\forall i \in I, A_i \neq .$$

Alors il existe une relation d'équivalence $\diamond$ telle que pour tout $i \in I$, A_i est une classe d'équivalence modulo $\diamond$.

Preuve :
Soit $\diamond$ la relation définie par

$$x \diamond y \iff \exists i \in I, \begin{cases} x \in A_i \\ y \in A_i \end{cases}$$

— Soit $x \in E$. Comme $E = \bigcup_{i\in I} A_i$, il existe $i \in I$ tel que $x \in A_i$ donc $x \diamond x$.

— Soient $x, y \in E$. On suppose $x \diamond y$. Soit $i \in I$ tel que $\begin{cases} x \in A_i \\ y \in A_i \end{cases}$ donc

$\begin{cases} y \in A_i \\ x \in A_i \end{cases}$ et donc $y \diamond x$.

— Soit $x, y, z \in E$. On suppose $x \diamond y$ et $y \diamond z$.

Soit $i \in I$ tel que $\begin{cases} x \in A_i \\ y \in A_i. \end{cases}$

Soit $j \in I$ tel que $\begin{cases} y \in A_j \\ z \in A_j. \end{cases}$

On a donc $y \in A_i \cap A_j$. Si $i \neq j$, alors $y \in$: une contradiction. Donc $i = j$ et donc $\begin{cases} x \in A_i \\ z \in A_i \end{cases}$. On en déduit que $x \diamond z$.

Ainsi $\diamond$ est une relation d'équivalence.

— Soit $i \in I$ et soit $x \in A_i \neq$.

$$\overline{x} = \{y \in E \mid y \diamond x\} = \{y \in E \mid y \in A_i\} = A_i.$$

□

Définition : Soit E un ensemble et $\diamond$. On dit que $\diamond$ est une relation d'ordre sur E si

1. $\diamond$ est réfléctive ($\forall x \in E, x \diamond x$),
2. $\diamond$ est anti-symétrique :

$$\forall x, y \in E, \quad \left.\begin{matrix} x \diamond y \\ y \diamond x \end{matrix}\right\} \implies x = y,$$

3. $\diamond$ est transitive $\Big(\forall x, y, z \in E, (x \diamond y \text{ et } y \diamond z) \implies x \diamond z\Big)$.

En général, la relation $\diamond$ est notée $\leqslant$ ou $\preccurlyeq$. On dit aussi que $(E, \diamond)$ est un ensemble ordonné.

Exemple : 1. $(\mathbb{R}, \leqslant)$ est un ensemble ordonné.

2. $\big(\mathcal{P}(E), \subset\big)$ est un ensemble ordonné.
3. $(\mathbb{N}, |)$ est un ensemble ordonné.
4. $(MP2I, \preccurlyeq)$ avec

$$x \preccurlyeq y \iff \text{note de } x \leqslant \text{note de } y$$

n'est un ensemble ordonné car $\preccurlyeq$ n'est pas anti symétrique.

5. $E = \mathbb{N}^2$ et $\preccurlyeq$ définie par

$$(x, y) \preccurlyeq (x', y') \iff x < x' \text{ ou } \begin{cases} x = x' \\ y \leqslant y' \end{cases}$$

$(E, \preccurlyeq)$ est un ensemble ordonné.

Définition : Soit $(E, \leqslant)$ un ensemble ordonné. Soient $x, y \in E$. On dit que x et y sont comparables si

$$x \leqslant y \text{ ou } y \leqslant x.$$

On dit que $\leqslant$ est un ordre total si tous les éléments de E sont comparables 2 à 2.

Exemple : — $(\mathbb{R}, \leqslant)$ est totalement ordonné
— $\big(\mathcal{P}(E), \subset\big)$ n'est pas totalement ordonné en général :

Soient $a, b \in E$ avec $a \neq b$. $\{a\}$ et $\{b\}$ ne sont pas comparables.
— $(\mathbb{N}, |)$ n'est pas totalement ordonné :

$2 \nmid 5$ et $5 \nmid 2$ donc 2 et 5 ne sont pas comparables.

Définition : Soit $(E, \leqslant)$ un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$. On dit que A est majorée par M, que M majore A ou que M est un majorant de A si

$$\forall a \in A, a \leqslant M.$$

Soit $m \in E$. On dit que A est minorée par m, que m minore A ou que m est un minorant de A si

$$\forall a \in A, m \leqslant a.$$

Il manque une partie du cours ici

Exemple : 1. $E = \mathbb{R}$ muni de $\leqslant$ et $A = [2, 5]$.

On sait que $\sup A = 5$ car

$$\forall x \in A, x \leqslant 5$$

et

$$\forall y \leqslant 5, \quad 5 > \frac{y+5}{2} > y$$

donc y ne majore pas A.

2. $E = \mathbb{R}$ avec $\leqslant$ et $A =]2, 5[$. $A \not\ni \sup A = 5$ par le même raisonnement.
3. $E = \mathbb{N}^\star$ avec $|$ et $A = \{p, q\}$ avec $p \neq q \in E$. $\sup A = \text{PPCM}(p, q) = p \vee q$ (c.f. chapitre 10 arithmétique)
4. $\mathcal{P}(E)$ avec $\subset$ et $A = \{P, Q\}$ avec $P, Q \in \mathcal{P}(E)$ et $P \neq Q$. $\sup A = P \cup Q$.
5. $E = \{0, 1\} \times \mathbb{Z}$ muni de $\leqslant$ défini par

$$(x_1, y_1) \leqslant (x_2, y_2) \iff x_1 < x_2 \text{ ou } \begin{cases} x_1 = x_2 \\ y_1 \leqslant y_2 \end{cases}$$

et $A = \{0\} \times \mathbb{Z}$. (x, y) majore $A \iff x = 1$ donc A est majorée mais n'a pas de borne supérieure.

Proposition : Soit $(E, \leqslant)$ un ensemble ordonné et $A \in \mathcal{P}(E)$. Si A a une borne supérieure, alors celle-ci est unique. On la note $\sup A$.

Preuve :
Soit M_1 et M_2 deux bornes supérieures de A.

Donc M_2 majore A. Comme M_1 est une borne supérieure de A, on a $M_1 \leqslant M_2$.

De même, on en déduit que $M_2 \leqslant M_1$.

Comme $\leqslant$ est antisymétrique, $M_1 = M_2$. □

Proposition–Définition : Soit $(E, \leqslant)$ un ensemble ordonné et $A \in \mathcal{P}(E)$ minorée par $m \in E$. On dit que m est une borne inférieur de A si

$$\begin{cases} \forall a \in A,\ m \leqslant a, \\ \forall x \in E,\ (\forall a \in A,\ x \leqslant a) \implies x \leqslant m. \end{cases}$$

Dans ce cas, m est unique et on la note $\inf(A)$. □

Définition : Soit $(E, \leqslant)$ un ensemble ordonné et $A \in \mathcal{P}(E)$.

1. Soit $M \in E$. On dit qye M est le plus grand élément de A ou que M est le maximum de A si

$$\begin{cases} \forall a \in A,\ a \leqslant M, \\ M \in A. \end{cases}$$

   Dans ce cas, on le note $M = \max(A)$.
2. Soit $m \in E$. On dit que m est le plus petit élément de A ou que m est le minimum de A si

$$\forall a \in A,\ a \geqslant mm \in A$$

   Dans ce cas, on le note $m = \min(A)$.

Proposition : En cas d'éxistence, il y a unicité du minimum et du maximum.

Preuve :
Soient M_1 et M_2 deux maxima. On a $M_1 \in A$ donc $M_1 \leqslant M_2$. Or, $M_2 \in A$

donc $M_2 \leqslant M_1$. On en déduit que $M_1 = M_2$. □

Proposition : Soit $(E, \leqslant)$ un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$.

$$M = \max(A) \iff \begin{cases} M = \sup(A), \\ M \in A; \end{cases}$$

$$M = \min(A) \iff \begin{cases} M = \inf(A), \\ M \in A. \end{cases}$$

Preuvë “ $\Longrightarrow$ ” On suppose $M = \max(A)$. On sait déjà que $M \in A$ et que M est un majorant de A.

Soit M' un majorant de A. $M \in A$ donc $M' \geqslant M$. On en déduit que $M = \sup(A)$.

“ $\Longleftarrow$ ” On suppose $M = \sup(A) \in A$. Alors M majore A et $M \in A$ donc $M = \max(A)$.

□

Exemple :
$E = \mathbb{N}^\star$ muni de $|$ et $A = \{3, 5\}$. $\sup(A) = 3 \vee 5 = 15 \notin A$ donc A n'a pas de maximum.

Définition : Soit $(E, \leqslant)$ un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in A$.

On dit que M est un élément maximal de A si aucun élément de A n'est strictement supérieur à M :

$$\nexists\, a \in A, \begin{cases} M \leqslant a, \\ M \neq a. \end{cases}$$

On dit que M est un élément minimal de A si aucun élément de A n'est strictement inférieur à M :

$$\nexists\, a \in A, \begin{cases} M \geqslant a, \\ M \neq a. \end{cases}$$

Exemple :
$E = \{n \in \mathbb{N} \mid n \geqslant 2\} = \mathbb{N} \setminus \{0, 1\}$ muni de $|$ et $A = E$. Les éléments minimaux de E sont les nombres premiers, il y en a une infinité. Il n'y a donc pas d'élément maximal.

Proposition : Avec les notations précédentes, si A a un maximum M alors M est le seul élément maximal de A.

Preuve :
Soit $M = \max(A)$. Soit $a \in A$ tel que $M \leqslant a$ et $M \neq a$. Comme $a \in A$ et $M = \max(A)$, on sait que $a \leqslant M$. Par antisymétrie, on en déduit que $a = M$: une contradiction.

Donc M est un élément maximal de A.

Soit M' un élément maximal de A. $M' \in A$ donc $M' \leqslant M$ et donc $M = M'$. □

Définition : Soient $(E, \leqslant)$ et $(F, \preccurlyeq)$ deux ensembles ordonnés et $f : E \to F$. On dit que

1. f est croissante si
$$\forall (x, y) \in E^2, x \leqslant y \implies f(x) \preccurlyeq f(y);$$
2. f est décroissante si
$$\forall (x, y) \in E^2, x \leqslant y \implies f(x) \succcurlyeq f(y).$$

Exemple :
$E = \mathbb{N}^\star$ muni de $|$, $F = \mathbb{N}^\star$ muni de $\leqslant$ et $f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & x. \end{array}$

Soit $(x, y) \in E^2$ tels que $x \mid y$. Alors $x \leqslant y$ donc f est croissante.

On pose
$$\begin{array}{rcl} g : F & \longrightarrow & E \\ n & \longmapsto & n. \end{array}$$

$2 \leqslant 3$ mais $2 \nmid 3$ donc g n'est pas croissante et $2 \leqslant 5$ mais $5 \nmid 2$ donc g n'est pas décroissante.

Définition : Soit $(E, \leqslant)$ un ensemble ordonné et $A \in \mathcal{P}(E)$. On dit que A est bornée si A est à la fois majorée et minorée.

Définition : Avec les notations précédentes, un extremum de A (sous reserve d'existence) est un maximum ou un minimum de A.

4 Lois de composition

Définition : Une loi de composition interne est une application f de $E \times E$ dans E.

On la note $x \star y$ au lieu de $f(x, y)$ (on est libre de choisir le symbôle).

Définition : Soit E un ensemble muni d'une loi de composition interne $\boxtimes$.

On dit que $\boxtimes$ est associative si

$$\forall (x, y, z) \in E^3,\ (x \boxtimes y) \boxtimes z = x \boxtimes (y \boxtimes z).$$

Dans ce cas, on écrit plutôt $x \boxtimes y \boxtimes z$.

Exemple : — $+$ et $\times$ dans $\mathbb{C}$ sont associatives ;
— $\circ$ est associative ;
— la multiplication matricielle est aussi associative.

Définition : On dit que $\boxtimes$ est commutative si

$$\forall (x, y) \in E^2, x \boxtimes y = y \boxtimes x.$$

Exemple : — $+$ et $\times$ dans $\mathbb{C}$ sont commuatives ;
— $\circ$ n'est pas commutative ;
— la multiplication matricielle n'est pas commutative.

Définition : Soit $e \in E$. On dit que e est un
— élément neutre à gauche si

$$\forall x \in E,\ e \boxtimes x = x;$$

— élément neutre à droite si

$$\forall x \in E,\ x \boxtimes e = x;$$

— élément neutre si

$$\forall x \in E,\ e \boxtimes x = x \boxtimes e = x.$$

Proposition : Sous reserve d'existence, il y a unicité de l'élément neutre.

Preuve :
Soient e et e' deux éléments neutre.
- $e \boxtimes e' = e'$ car e est neutre,
- $e \boxtimes e' = e$ car e' est neutre.

On a donc $e = e'$. □

Axiome (axiome du choix) **:** Soit E un ensemble non vide. Il existe $f : \mathcal{P}(E) \setminus \{\} \to E$ telle que

$$\forall A \in \mathcal{P}(E) \setminus \{\},\ f(A) \in A.$$

Définition : Soit $f : E \to F$. Le graphe de f est

$$\Big\{ \big(x, f(x)\big) \mid x \in E \Big\} \subset E \times F.$$

Proposition : Soit $G \subset E \times F$. G est le graphe d'une application si et seulement si

$$\forall x \in E,\ \exists! y \in F,\ (x, y) \in G.$$

Preuve " $\Longrightarrow$ " par définition d'une application
" $\Longleftarrow$ " On pose $f(x)$ le seul élément y de F qui vérifie $(x, y) \in G$. Alors $f \in F^E$ et son graphe vaut G.

□

Définition : Soit $A \in \mathcal{P}(E)$. L'indicatrice de A est

$$\mathbb{1}_A : E \longrightarrow \{0, 1\}$$
$$x \longmapsto \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{cases}$$

Exemple : 1. Dans $\mathbb{C}$, le neutre de $+$ est 0 et le neutre de $\times$ est 1.
2. Dans E^E, le neutre de $\circ$ est id_E.
3. Dans $\mathcal{M}_n(\mathbb{C})$ (l'ensemble des matrices carrées $n \times n$ à valeurs dans $\mathbb{C}$), le neutre de $\times$ est I_n :

$$I_n = \begin{pmatrix} 1 & \ddots & (0) \\ & \ddots & \\ (0) & \ddots & 1 \end{pmatrix}$$

Définition : Soit E un ensemble muni d'une loi de composition interne $\boxtimes$ et $x \in E$.

1. On dit que x est simplifiable à gauche si

$$\forall (y,z) \in E^2,\ (x \boxtimes y = x \boxtimes z) \implies x = z.$$

et que x est simplifiable à droite si

$$\forall (y,z) \in E^2,\ (y \boxtimes x = z \boxtimes y) \implies x = z.$$

2. On dit que x est symétrisable à gauche s'il exiiste $y \in E$ tel que $y \boxtimes x = e$ où e est l'élément neutre de $\boxtimes$.

   De même, on dit que x est symétrisable à droite s'il existe $y \in E$ tel que $x \boxtimes y = e$.

   On dit que x est symétrisable s'il est symétrisable à gauche et à droite, donc s'il existe $y \in E$ tel que $x \boxtimes y = y \boxtimes x = e$.

Exemple :
$E = \mathbb{N}$ muni de la loi $+$, tous les éléments de E sont simplifiables. 0 est le seuele élément de E symétrisable.

Proposition : Avec les notations précédentes, si $\boxtimes$ est associative, et x est symétrisable, alors x est simplifiable.

Preuve :
Soient $y, z \in E$.

— On suppose $x \boxtimes y = x \boxtimes z$. Soit $a \in E$ tel que $a \in E$ tel que $a \boxtimes x = e$. Alors

$$a \boxtimes (x \boxtimes y) = a \boxtimes (x \boxtimes z).$$

Or,

$$\begin{aligned} a \boxtimes (x \boxtimes y) &= (a \boxtimes x) \boxtimes y \\ &= e \boxtimes y \\ &= y. \end{aligned}$$

De même, $a \boxtimes (x \boxtimes z) = z$.

Donc $y = z$.

— De même, si $y \boxtimes x = z \boxtimes x$, on "multiplie" x à droite par a et on obtient $y = z$.

□

Proposition–Définition : On suppose $\boxtimes$ associative. Soit $x \in E$ symétrisable. Alors

$$\exists! y \in E,\ x \boxtimes y = y \boxtimes x = e.$$

On dit que y est le symétrique de x et on le note $y = x^\star$.

Preuve :
Soeint $x, y, z \in E$ tels que

$$\begin{cases} x \boxtimes y = y \boxtimes x = e \\ x \boxtimes z = z \boxtimes x = e \end{cases}$$

Alors, $x \boxtimes y = x \boxtimes z$ et, en simplifiant par x, on a $y = z$. □

Exemple :
Les fonctions symétrisables de $(E^E, \circ)$ sont les bijections et le symétrique d'une bijection est sa réciproque.

Remarque : 1. Si la loi est notée $+$, on parle d'opposé plutôt que de symétrique et on le note $-x$ au lieu de $x^\star$. L'élément neutre est noté 0_E.

2. Si la loi est notée $\times$, on parle d'élément inversible au lieu de symétrisable, d'inverse au lieu de symétrique et on note x^{-1} au lieu de $x^\star$. On note le neutre 1_E.

Exercice :
Soient $x, y \in E = \mathbb{R}_\star^+$. On définit la loi de composition interne $\oplus$:

$$x \oplus y = \frac{1}{\frac{1}{x} \oplus \frac{1}{y}}.$$

Cette loi peut-être utile en physique pour le calcul de résistances équivalentes en parallèles.

— Associativité : soient $x, y, z \in E$.

D'une part, on a

$$x \oplus (y \oplus z) = \frac{1}{\frac{1}{x} + \frac{1}{\frac{1}{\frac{1}{y}+\frac{1}{z}}}} = \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

D'autre part, on a

$$(x \oplus y) \oplus z = \frac{1}{\frac{1}{\frac{1}{\frac{1}{x}+\frac{1}{y}}} + \frac{1}{z}} = \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

La loi $\oplus$ est associative.

— Commutativité : soient $x, y \in E$.

$$x \oplus y = \frac{1}{\frac{1}{x}+\frac{1}{y}} = \frac{1}{\frac{1}{y}+\frac{1}{x}} = y \oplus x.$$

Donc la loi $\oplus$ est commutative.

— Élément neutre : soit e l'élément neutre de $\oplus$.

$$\forall x \in E,\ x \oplus e = e \oplus x = x.$$

Comme la loi est commutative, seul l'égalité $x \oplus e = x$ est utile.

Soit $x \in E$. On a donc $\dfrac{1}{\frac{1}{x}+\frac{1}{e}} = x$ donc $\dfrac{ex}{e+x} = x$ donc $ex = x(e+x)$ et donc $\cancel{ex} = \cancel{ex} + x^2$. On en déduit que $x^2 = 0$, ce qui n'est pas possible car $x \in \mathbb{R}_\star^+$. Donc, il n'y a pas d'élément neutre pour $\oplus$.

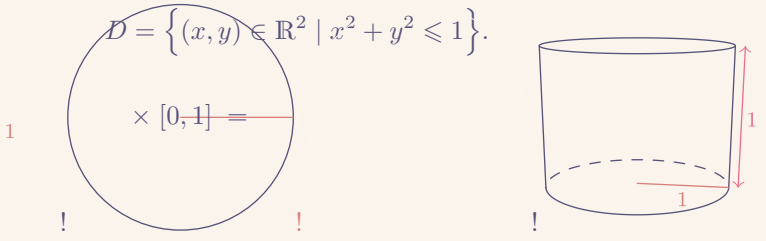
5 Divers

Définition : Soient E et F deux ensembles. Un couple (x, y) est la donnée d'un élément x de E et d'un élément y de F où

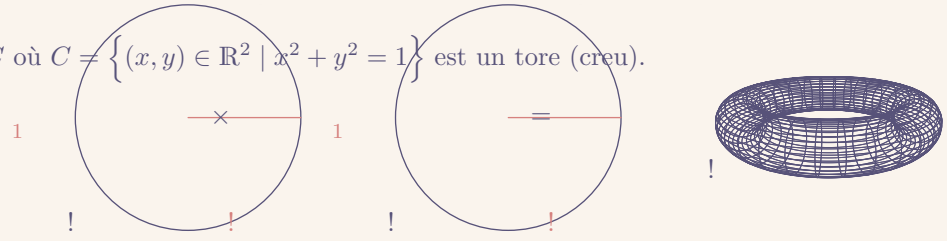
$$\forall x, x' \in E, \forall y, y' \in F, \qquad (x, y) = (x', y') \iff \begin{cases} x = x', \\ y = y'. \end{cases}$$

On note $E \times F$ l'ensemble des couples ; c'est le produit cartésien de E et F.

Exemple :
$D \times [0, 1]$ est un cylindre plein où D est le disque unité fermé i.e.



$C \times C$ où $C = \left\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\right\}$ est un tore (creu).



Définition : Soient E et F deux ensembles. On dit que E et F sont équipotents s'il existe une bijection de E dans F.

EXEMPLE : 1. $\mathbb{N}$ et $\mathbb{N}^\star$ sont équipotents car $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N}^\star \\ k & \longmapsto & k+1 \end{array}$ est bijective.

2. $P = \{n \in \mathbb{N} \mid n \text{ pair}\}$ et $I = \{n \in \mathbb{N} \mid n \text{ impair}\}$ sont équipotents car $f : \begin{array}{ccc} P & \longrightarrow & I \\ x & \longmapsto & x+1 \end{array}$ est bijective.
3. $\mathbb{N}$ et P sont équipotents car $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & P \\ k & \longmapsto & 2k \end{array}$ est bijective.
4. $[0,1]$ et $[0,1[$ sont équipotents car

$$f : [0,1] \longrightarrow [0,1[$$
$$x \longmapsto \begin{cases} \dfrac{1}{n+1} & \text{si } x = \dfrac{1}{n} \text{ avec } n \in \mathbb{N}^\star \\ x & \text{sinon} \end{cases}$$

est bijective.
5. De même, $]0,1[$ et $]0,1]$ sont équipotents.
6. $]0,1[$ et $[0,1[$ sont équipotents : $f : \begin{array}{ccc}]0,1] & \longrightarrow & [0,1[\\ x & \longmapsto & 1-x \end{array}$ est bijective.
7. $\forall a < b$, $[a,b]$ et $[0,1]$ sont équipotents :

$$f : [0,1] \longrightarrow [a,b]$$
$$\alpha \longmapsto \alpha b + (1-\alpha)a$$

est bijective (interpolation linéaire).
8. $\mathbb{R}$ et $]0,1[$ sont équipotents :

$$f : \mathbb{R} \longrightarrow]0,1[$$
$$x \longmapsto \frac{1}{2} + \frac{\operatorname{Arctan} x}{\pi}$$

est bijective.
9. $[0,1[$ et $\mathbb{N}$ ne sont pas équipotents (argument de Cantor). Soit $f : \mathbb{N} \to [0,1[$ une bijection :

k	$f(k)$
0	$0,\ 0\ 0\ 0\ 0\ \ldots$
1	$0, a_1 a_2 a_3 a_4 \ldots$
2	$0, b_1 b_2 b_3 b_4 \ldots$
$\vdots$	$\vdots \qquad \ddots$

On considère le nombre

$$x = 0,\ (a_0+1)(b_1+1)(c_2+1)\cdots$$

$f(1) \neq x$ car ils n'ont pas le même chiffre des dizaines.
$f(2) \neq x$ car ils n'ont pas le même chiffre des centaines.

Par le même raisonement, on en déduit que

$$\forall n \in \mathbb{N}, f(n) \neq x$$

donc x n'a pas d'antécédant : une contradiction.

10. On verra en exercice que E et $\mathscr{P}(E)$ ne sont pas équipotents. $\mathbb{R}$ et $\mathscr{P}(\mathbb{R})$ ne sont pas équipotents mais $\mathbb{R}$ et $\mathscr{P}(\mathbb{N})$ le sont (développement dyadique).
11. $\mathbb{R}^2$ et $\mathbb{R}$ sont équipotents ; $\mathbb{C}$ et $\mathbb{R}$ sont équipotents.

Exercice :
Soit E un ensemble. L'application

$$\begin{aligned} f : \mathscr{P}(E) &\longrightarrow 0,1^E \\ A &\longmapsto \mathbb{1}_A \end{aligned}$$

est bijective.

Soit $g : E \to \{0,1\}$.

Analyse Soit $A \in \mathscr{P}(E)$ tel que $f(A) = g$. Alors $g = \mathbb{1}_A$. donc

$$\forall x \in E,\ g(x) = \mathbb{1}_A(x)$$

et donc

$$\begin{cases} \forall x \in A,\ g(x) = 1 \\ \forall x \in E \setminus A,\ g(x) = 0 \end{cases}$$

On en déduit que

$$A = \{x \in E \mid g(x) = 1\} = g^{-1}\big(\{1\}\big).$$

Synthèse On pose $A = g^{-1}\big(\{1\}\big)$. Montrons que $f(A) = g$.

$$\forall x \in E,\ g(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} = \mathbb{1}_A$$

donc $g = \mathbb{1}_A$.

On aurait aussi pu rédiger de la façon suivante : on pose

$$\begin{aligned} u : \{0,1\}^E &\longrightarrow \mathscr{P}(E) \\ g &\longmapsto g^{-1}\big(\{1\}\big). \end{aligned}$$

On montre que u est la réciproque de f :

$$\begin{cases} f \circ u = \mathrm{id}_{\{0,1\}^E}, \\ u \circ f = \mathrm{id}_{\mathscr{P}(E)}\,. \end{cases}$$

Définition : Soit $f : E \to F$. L'image de f est

$$\mathrm{Im}(f) = f(E) = \big\{f(x) \mid x \in E\big\}.$$

Proposition : Soit $f : E \to F$.

$$f \text{ est surjective } \iff f(E) = F.$$

Définition : Une suite de E est une application de $\mathbb{N}$ dans E.

Remarque (Notation) :
Soit $u \in E^{\mathbb{N}}$. Pour $n \in \mathbb{N}$, on écrit u_n à la place de $u(n)$.

Définition : Soient E et I deux ensembles. Une famille de E indéxée par I est une application de I dans E.

À la place de $u(i)$ (avec $i \in I$), on écrit u_i.

Définition : Soit E un ensemble et $(A_i)_{i\in I}$ une famille de parties de E. On suppose $I \neq$. On pose

$$\bigcup_{i\in I} A_i = \{x \in E \mid \exists i \in I,\ x \in A_i\}$$

et

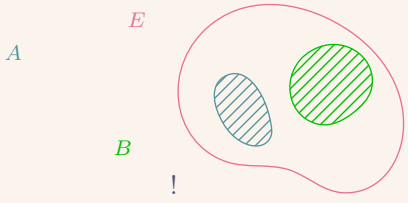
$$\bigcap_{i\in I} A_i = \{x \in E \mid \forall i \in I,\ x \in A_i\}.$$

On pose aussi $\bigcup_{i\in} A_i =$ et $\bigcap_{i\in} A_i = E$.

Remarque :
De même que pour les sommes et produits de complexes, on peut intervertir des réunions doubles.

Proposition : Soit E un ensemble, $(A, B) \in \mathcal{P}(E)^2$.

$$A \subset (E \setminus B) \iff A \cap B = .$$



Preuvë “ $\Longrightarrow$ ” Soit $x \in A \cap B$. Alors $x \in A$ et $x \in B$. Comme $x \in A \subset (E \setminus B)$, alors $x \in E \setminus B$ i.e. $x \notin B$: une contradiction. Donc $A \cap B = .$

“ $\Longleftarrow$ ” On suppose $A \cap B = .$ Soit $x \in A$. Si $x \in B$, alors $x \in A \cap B =$: faux. Donc $x \notin B$ et donc $x \in E \setminus B$.

□

Proposition : Si $f : E \to F$ et $g : F \to G$ sont bijectives, alors $g \circ f$ est bijective et

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

□

Remarque (B Attention) :
$g \circ f$ peut-être bijective alors que f et g ne le sont pas.

Chapitre 9

Inégalités dans $\mathbb{R}$

1

2

3

4 Bornes supérieures

Proposition (borne inférieure) **:** Toute partie minorée non vide de $\mathbb{R}$ admet une borne inférieure.

Preuve :
Soit $A \subset \mathbb{R}$ non vide minorée. On pose $B = \{-a \mid a \in A\} \neq$. Soit m un minorant de A :

$$\forall a \in A,\ m \leqslant a.$$

D'où,

$$\forall a \in A,\ -a \leqslant -m$$

donc B est majorée par $-m$.

D'après la propriété de la borne supérieure, B admet une borne supérieure. On pose $\beta = \sup(B)$, donc β majore B et donc

$$\forall a \in A,\ -a \leqslant \beta$$

et donc

$$\forall a \in A,\ -\beta \geqslant a.$$

Donc $-\beta$ est un minorant de A.

Soit x un minorant de A. Montrons que $x \leqslant -\beta$. On sait que $-x$ majore B et donc $-x \geqslant \beta$. On en déduit que $x \leqslant -\beta$ et donc $-\beta = \inf(A)$. □

Proposition (caractérisation de la borne supérieure) **:** Soit $A \subset \mathbb{R}$ non vide majorée et $M \in \mathbb{R}$.

$$M = \sup(A) \iff \begin{cases} \forall a \in A,\ a \leqslant M, \\ \forall \varepsilon > 0, \exists a_0 \in A, A_0 > M - \varepsilon. \end{cases}$$

Preuve $\Longleftarrow$ " On suppose $M = \sup(A)$. M est un majorant de a :

$$\forall a \in A,\ a \leqslant M.$$

Soit $\varepsilon > 0$, comme M est le plus petit majorant de A et que $M - \varepsilon < M$, $M - \varepsilon$ ne majore pas A. Donc

$$\exists a_0 \in A,\ a_0 > M - \varepsilon.$$

— On suppose

$$\begin{cases} \forall a \in A,\ a \leqslant M; & (1) \\ \forall \varepsilon > 0, \exists a_0 \in A, M - \varepsilon < a_0. & (2) \end{cases}$$

D'après (1), M est un majorant de A. Soit M' un majorant de A. Montrons que $M' \geqslant M$.

On suppose $M' < M$ et on pose $\varepsilon = M - M' > 0$. D'après (2), il existe $a_0 \in A$ tel que

$$a_0 > M - \varepsilon = M' \geqslant a_0$$

une contradiction. Donc $M' \geqslant M$ et donc M est le plus petit majorant de A : $M = \sup(A)$.

□

Proposition (caractérisation de la borne inférieure) **:** Soit $A \subset \mathbb{R}$, non vide minorée et $m \in \mathbb{R}$.

$$m = \inf(A) \iff \begin{cases} \forall a \in A,\ m \leqslant a; \\ \forall \varepsilon > 0,\ \exists a_0 \in A,\ a_0 < m + \varepsilon. \end{cases}$$

□

Proposition : Soit $A \subset \mathbb{R}$ non vide majorée et $M \in \mathbb{R}$.

$$M \geqslant \sup(A) \iff \forall a \in A,\ a \leqslant M.$$

Preuve " $\Longrightarrow$ " On suppose $M = \sup(A)$. Soit $a \in A$. On sait que $a \leqslant \sup(A)$ car $\sup(A)$ majore A. Donc $a \leqslant M$.
" $\Longleftarrow$ " On suppose $\forall a \in A,\ a \leqslant M$. Donc M majore A. Or, $\sup(A)$ est le plus petit majorant et donc $M \geqslant \sup(A)$.

□

Proposition : Soit $A \subset \mathbb{R}$ non vide minorée et $m \in \mathbb{R}$.

$$m \leqslant \inf(A) \iff \forall a \in A,\ m \leqslant a.$$

□

Proposition–Définition : $\mathbb{R}$ est archimédien :

$$\forall x \in \mathbb{R}_+^\star,\ \forall y \in \mathbb{R},\ \exists n \in \mathbb{N},\ nx \geqslant y.$$

Preuve :
Soit $x \in \mathbb{R}_+^\star$ et $y \in \mathbb{R}$. Supposons

$$(H) : \qquad \forall n \in \mathbb{N},\ nx < y.$$

On pose $A = \{nx \mid n \in \mathbb{N}\} \subset \mathbb{R}$. Comme $0 \in A$, $A \neq$. D'après (H), A est majorée par y.

Soit $\alpha = \sup(A)$ et $n \in \mathbb{N}$. On sait que $(n+1)x \in A$ donc $(n+1)x \leqslant \alpha$ et donc $nx \geqslant \alpha - x$. On remarque que $\alpha - x$ majore A mais que $\alpha - x < \alpha$: une contradiction car α est le plus petit majorant de A. Donc,

$$\exists n \in \mathbb{N},\ nx \geqslant y.$$

□

Théorème : Toute fonction continue sur un segment est bornée et atteint ses bornes : si $f : [a,b] \to \mathbb{R}$ (avec $a < b \in \mathbb{R}$) est continue, alors

$$\exists (\alpha, \beta) \in [a,b]^2,\ \forall x \in [a,b],\ f(\alpha) \leqslant f(x) \leqslant f(\beta).$$

Preuve :
c.f. Chapitre 14 : Continuité. □

Proposition : Soit $A \subset \mathbb{R}$ non vide majorée. Il existe une suite $(a_n) \in A^{\mathbb{N}}$ telle que $\lim\limits_{n\to+\infty} a_n = \sup(A)$.

Preuve :
On sait que

$$\forall \varepsilon > 0,\ \exists a \in A,\ a > \sup(A) - \varepsilon.$$

Donc,

$$\forall n \in \mathbb{N}^\star, \exists a_n \in A, a_n > \sup(A) - \frac{1}{n}.$$

On a

$$\forall n \in \mathbb{N}^\star, a_n \in A \ \text{ et } \ a_n \leqslant \sup(A).$$

Or

$$\forall n \in \mathbb{N}^\star,\ \sup(A) - \frac{1}{n} < a_n \leqslant \sup(A),$$

par encadrement, on en déduit que $a_n \xrightarrow[n\to+\infty]{} \sup(A)$. □

Proposition : Soit $A \subset \mathbb{R}$ non vide minorée. Il existe une suite $(a_n) \in A^{\mathbb{N}}$ telle que $\lim\limits_{n\to+\infty} a_n = \inf(A)$. □

5 Partie entière

Proposition–Définition : Soit $x \in \mathbb{R}$. Il existe un unique entier $n \in \mathbb{N}$ tel que

$$n \leqslant x < n + 1.$$

Cet entier n est appelé partie entière de x et est noté $\lfloor x \rfloor$.

Preuve :
Soit $A = \{p \in \mathbb{Z} \mid p > x\}$. $A \neq$ car $\mathbb{R}$ est archimédien.

Soit α la borne inférieure de A. Alors $\alpha \geqslant x$. Montrons que $\alpha \in A$. Soit $n \geqslant 2$. On a $\alpha + \dfrac{1}{n} > \alpha$ donc, il existe $a_n \in A$ tel que

$$\alpha < a_n < \alpha + \frac{1}{n}.$$

On sait que $\dfrac{1}{n} < 1$ donc, il y a au plus un entier dans le segment $\left[\alpha, \alpha + \dfrac{1}{n}\right]$.
Donc, tous les a_n sont égaux et $a_n \xrightarrow[n\to+\infty]{} \alpha$. On en déduit que

$$\forall n \geqslant 2,\ a_n = \alpha$$

et donc $\alpha \in A$. Ainsi, $\alpha = \min(A)$ et alors $\alpha - 1 \notin A$. On a donc

$$\alpha - 1 \leqslant x < \alpha$$

et, en posant $n = \alpha - 1$, on en déduit que

$$n \leqslant x < n + 1.$$

□

6 Densité

Définition : Soit $A \in \mathcal{P}(\mathbb{R})$. On dit que A est dense dans $\mathbb{R}$ si, pour tout intervalle I ouvert non vide de $\mathbb{R}$, $A \cap I \neq$.

Théorème : $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Preuve :
Soit I un intervalle ouvert non vide. Soient $a < b$ deux éléments de I. On cherche $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ tel que

$$a \leqslant \frac{p}{q} \leqslant b.$$

Comme $\mathbb{R}$ est archimédien, il existe $q \in \mathbb{N}^\star$ tel que

$$q(b - a) \geqslant 2 > 1.$$

Donc, l'intervalle $[qa, qb]$ a une longueur supérieure à 1, il contient donc au moins un entier p.

En effet, sinon on a $\lfloor qa \rfloor = \lfloor qb \rfloor$ et alors

$$\begin{cases} \lfloor qa \rfloor \leqslant qb < \lfloor qa \rfloor + 1 \\ \lfloor qa \rfloor \leqslant qa < \lfloor qa \rfloor + 1 \end{cases}$$

et alors

$$-1 < qb - qa < 1$$

une contradiction. On a donc $qa \leqslant p \leqslant qb$ et finalement

$$a \leqslant \frac{p}{q} \leqslant b.$$

□

Théorème : $\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$.

Il manque une partie du cours ici

7

8

Il manque une partie du cours ici

Preuve :
Soit $a \in I$ et

$$\begin{aligned} \tau_a : I \setminus \{a\} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{f(x) - f(a)}{x - a}. \end{aligned}$$

D'après le lemme des pentes, τ_a est croissante. En effet, soient $x, y \in I \setminus \{a\}$ tels que $x < y$.

Cas 1 $a < x < y$. On a alors

$$\frac{f(x) - f(a)}{x - a} \leqslant \frac{f(y) - f(a)}{y - a}$$

et donc $\tau_a(x) \leqslant \tau_a(y)$.

Cas 2 $x < a < y$. On a alors

$$\frac{f(x) - f(a)}{x - a} \leqslant \frac{f(x) - f(y)}{x - y} \leqslant \frac{f(y) - f(a)}{y - a}$$

et donc $\tau_a(x) \leqslant \tau_a(y)$.

Cas 3 $x < y < a$. On a alors

$$\frac{f(x) - f(y)}{x - y} \leqslant \frac{f(x) - f(a)}{x - a} \leqslant \frac{f(y) - f(a)}{y - a}$$

et donc $\tau_a(x) \leqslant \tau_a(y)$.

Soit $x > a$ avec $x \in I$. On fixe $z_0 < a$ un élément de I. z_0 existe car I est ouvert. On a alors... □

Il manque une partie du cours ici

La suite du cours provient d'Aubin. Je ne suis pas responsable pour les éventuelles bêtises qu'il a pu taper.

9 Propriétés de $(\mathbb{R}, \leq)$

Axiome (Propriétés de $(\mathbb{R}, \leq)$) **:** $\mathbb{R}$ est muni dune addition notée $+$ associative, commutative, délément neutre 0 et tout réel x a un symétrique pour $+$ noté $-x$
$\mathbb{R}$ est muni dune multiplication notée $\times$, associative, commutative, délément neutre 1 et tout réel x a un symétrique pour $\times$ noté x^{-1} ou $\frac{1}{x}$
(on la notera * dans ce document)
La multiplication est distributive sur laddition
$\forall (a, b, c) \in \mathbb{R}^3, a(b + c) = ab + ac$

$\leq$ est un ordre total sur $\mathbb{R}$
$\forall (x, y, a) \in \mathbb{R}^3, (x \leq y \Longrightarrow a + x \leq a + y)$
$\forall a \in \mathbb{R}_+^\star, \forall (x, y) \in \mathbb{R}^2, x \leq y \Longrightarrow ax \leq ay$

$\mathbb{Q} \subset \mathbb{R}$
Propriété de la borne supérieure : Tout partie non vide majorée de $\mathbb{R}$ admet une borne supérieure

Lemme (Opposé dun réel) **:** $\forall a \in \mathbb{R}, -a = -1 \star a$

Proposition (Inverse de $\leq$) **:** Soient $(x, y) \in \mathbb{R}^2$
$x \leq y \Longrightarrow -y \leq -x$

Preuve :
$x \leq y \Longrightarrow -x + x \leq -x + y$
$\Longrightarrow 0 \leq -x + y$
$\Longrightarrow -y \leq -x$

□

Corollaire ($\times$ et $\leq$) **:** $\forall a \in \mathbb{R}_-^\star, \forall (x, y) \in \mathbb{R}^2, x \leq y \Longrightarrow ay \leq ax$

Preuve :

Soient $a < 0, (x, y) \in \mathbb{R}^2$

On pose $b = -a$
$a < 0 \Longrightarrow -0 \leq -a \Longrightarrow 0 \leq b$

Si $b = 0, a = 0$
$x \leq y \Longrightarrow bx \leq by$
$\Longrightarrow -by \leq -bx$
$\Longrightarrow -1(by) \leq -1(bx)$
$\Longrightarrow (-1 \star b) \star y \leq (-1 \star b) \star x$
$\Longrightarrow -by \leq -bx$
$\Longrightarrow ay \leq ax$

□

Proposition (Elément Symétrique pour la Multiplication) **:** Soit $a \in \mathbb{R}, -a$ est le seul réel qui vérifie $a + (-a) = 0$

Preuve :
$a + (-a) = a + (-1) \star a$
$= a \star (1 + -1)$
$= a \star 0 = 0$

On a bien $a \star 0 = 0$ car :
$a \star 0 = a \star (0 + 0)$
$0 + 0 = (a \star 0) + (a \star 0) = 0$

□

Proposition ($+$ et $\leq$) **:** Soient $(a, b, x, y) \in \mathbb{R}^4$ tels que $\begin{cases} x \leq y \\ a \leq b \end{cases}$
Alors $a + x \leq b + y$

Preuve :
$a \leq b \Longrightarrow a + x \leq b + x$
$x \leq y \Longrightarrow b + x \leq b + y$
$\leq$ est transitive donc $a + x \leq b + y$

□

REMARQUE (Soustraire des Inégalités) :
On ne peut pas soustraire directement des inégalités

Si $\begin{cases} x \leq y \\ a \leq b \end{cases}$, alors $\begin{cases} x \leq y \\ -b \leq -a \end{cases}$

et alors, $x - b \leq y - a$

Proposition ($\times$ et $\leq$ dans $\mathbb{R}^{\star}$) **:** Soient $(x, y, a, b) \in (\mathbb{R}^{+})^4$

$$\begin{cases} 0 \leq x \leq y \\ 0 \leq a \leq b \end{cases} \Longrightarrow xa \leq yb$$

Preuve :
$\begin{cases} x \leq y \\ 0 \leq a \end{cases} \Longrightarrow ax \leq ay$ et $\begin{cases} a \leq b \\ 0 \leq y \end{cases} \Longrightarrow ay \leq bx$

□

Proposition (Inégalité des Inverses) **:** $\forall (x, y) \in (\mathbb{R}_{\star}^{+})^2, x \leq y \Longrightarrow \dfrac{1}{x} \leq \dfrac{1}{y}$

Preuve :
Soient $(x, y) \in (R_{\star}^{+})^2$
On suppose $x \leq y$

Si $\dfrac{1}{x} \leq 0$, alors $x\dfrac{1}{x} \leq 0 \star x$, alors $1 \leq 0$

Donc $\dfrac{1}{x} \geqslant 0$ donc $\dfrac{1}{x}x \leq \dfrac{1}{x}y$

Donc $\dfrac{1}{x} \leq \dfrac{1}{y}$

□

REMARQUE (Diviser des Inégalités) :

On ne peut pas diviser des inégalités

10 Inégalités Classiques

Proposition (Inégalité Triangulaire dans $\mathbb{R}$) **:** $\forall (x,y) \in \mathbb{R}^2, \begin{cases} |x+y| \leq |x| + |y| \\ |x| - |y| \leq |x-y| \end{cases}$

En changeant y en $-y$, on a aussi

$$\begin{cases} |x-y| \leq |x| + |y| \\ |x| - |y| \leq |x+y| \end{cases}$$

Preuve :
1 - Soient $(x,y) \in \mathbb{R}^2$
$|x| = \max(-x, x) \geq x$
$|y| \geq y$

Donc $x + y \leq |x+y|$

Si $x + y \leq 0$, alors $|x+y| \leq |x| + |y|$

On a aussi $|x| \geq -x$ et $|y| \geq -y$
Donc $-(x+y) \leq |x| + |y|$

Si $x + y \leqslant 0$, alors $|x| + |y| \geq |x+y|$

2 - Soient $(x,y) \in \mathbb{R}^2$

$|x| = |x - y + y| \leq |x-y| + |y|$
Donc $|x| - |y| \leq |x+y|$

Si $|x| - |y| \geq 0, |x| - |y| \leq |x-y|$

On a aussi $|y| = |y - x + x| \leq |y-x| + |x|$
Donc $|y| - |x| \leq |y-x|$

Si $|x| - |y| \leqslant 0, |x| - |y| \leq |x-y|$

□

Proposition (Inégalité Triangulaire dans $\mathbb{C}$) **:** $\forall (x,y) \in \mathbb{C}, \begin{cases} |x+y| \leq |x| + |y| \\ |x| - |y| \leq |x-y| \end{cases}$

Preuve :
$|x+y| \leq |x| + |y| \iff |x+y|^2 \leq (|x| + |y|)^2$
$\iff (x+y)(\overline{x} + \overline{y}) \leq |x|^2 + |y|^2 + 2|xy|$
$\iff |x|^2 + |y|^2 + (x\overline{y} + \overline{x}y) \leq |x|^2 + |y|^2 + 2|xy|$
$\iff 2\mathfrak{Re}(xy) \leq 2|xy|$

Or, pour tout $z \in \mathbb{C}, \mathfrak{Re}(e) \leq |z|$
En effet :
$|z| = \sqrt{\mathfrak{Re}(z)^2 + \mathfrak{Im}(z)^2} \geqslant \sqrt{\mathfrak{Re}(z)^2} = |\mathfrak{Re}(z)| \geqslant \mathfrak{Re}(z)$

□

Proposition (Inégalité Triangulaire à n Coefficients) **:** Soient $(z_1 ... z_n) \in \mathbb{C}^n$
Alors, $|\sum_{k=1}^{n} |z_k \leq \sum_{k=1}^{n} |z_k|$

Preuve :
Pour $n \in \mathbb{N}^\star, P(n) : \forall (z_1 ... z_n) \in \mathbb{C}^n, |\sum_{k=1}^{n} |z_k \leq \sum_{k=1}^{n} |z_k|$

$P(1)$ et $P(2)$ sont vraies

Soit $n \in \mathbb{N}^\star$, on suppose $P(n)$ vraie
Soient $(z_1 ... z_n + 1) \in \mathbb{C}^n + 1$
$|\sum_{k=1}^{n+1} |z_k = |\sum_{k=1}^{n} z_k + z_{n+1}| \leq \sum_{k=1}^{n} |z_k| + |z_{n+1}| = \sum_{k=1}^{n+1} |z_k|$

Donc $P(n+1)$ vraie
Par récurrence, $\forall n \in N^\star, P(n)$ vraie

□

Proposition (Inégalité Triangulaire des Intégrales) **:** Soit $f : [a,b] \longrightarrow \mathbb{R}$ continue

Alors $|\int_a^b f(x)dx| \leq \int_a^b |f(x)|dx$

Preuve :
$\forall x \in [a,b], -|f(x)| \leq f(x) \leq |f(x)|$

□

Proposition (Inégalité Triangulaire des Intégrales sur $\mathbb{C}$) **:** Soit $f : [a,b] \longrightarrow \mathbb{C}$ continue
Alors $|\int_a^b f(x)dx| \leq \int_a^b |f(x)|dx$

Preuve :
Cas 1 : $|\int_a^b f(x)dx| = 0$

On a $\forall x \in [a,b], |f(x)| \geqslant 0$
donc $\int_a^b |f(x)|dx \geqslant 0 = |\int_a^b f(x)dx|$

Cas 2 : $|\int_a^b f(x)dx| \neq 0$

On pose $r = |\int_a^b f(x)dx| \in \mathbb{R}_+^\star$
Soit θ un argument de $\int_a^b f(x)dx$
Doù $\int_a^b f(x)dx = re^{i\theta}$

$r = e^{-i\theta}\int_a^b f(x)dx = \int_a^b f(x)e^{-i\theta}dx$
$= \mathfrak{Re}(\int_a^b f(x)e^{-i\theta}dx)$

$$= \int_a^b \mathfrak{Re}(f(x)e^{-i\theta})dx \leq \int_a^b |f(x)e^{-i\theta}|dx$$
car $\forall x, \mathfrak{Re}(f(x)e^{-i\theta}) \leq |f(x)e^{-i\theta}|$
$$\leq \int_a^b |f(x)||e^{-i\theta}|dx = \int_a^b |f(x)|dx$$

□

Proposition (Inégalité de Cauchy-Schwartz) **:** Soient $f, g : [a, b] \longrightarrow \mathbb{R}$ continues

$$(\int_a^b f(t)g(t)dt)^2 \leq \int_a^b f^2(t)dt \int_a^b g^2(x)dt$$

Proposition (Inégalité des Accroissements Finis sur $\mathbb{R}$) **:** Soit $f : I \longrightarrow \mathbb{R}$ dérivable sur I telle quil existe $M \in \mathbb{R}$ vérifiant
$\forall t \in I, |f'(t)| \leq M$

Alors $\forall (a, b) \in I^2, |f(a) - f(b)| \leq M|a - b|$

Proposition (Inégalité des Accroissements Finis sur $\mathbb{C}$) **:** Soit $f : I \longrightarrow \mathbb{C}$ de classe C^1 et M tel que
$\forall t \in I, |f'(t)| \leq M$

Alors $\forall (a, b) \in I^2, |f(a) - f(b)| \leq M|a - b|$

Preuve :
On suppose $a \leq b$

$$|f(a) - f(b)| = |f(b) - f(a)| = |\int_a^b f'(t)dt|$$
$$\leq \int_a^b |f'(t)|dt$$
$$\leq \int_a^b Mdt = M(b - a) = M|b - a|$$

□

11 Valeur Absolue

Proposition (Inégalités avec la Valeur Absolue) **:** Soient $(a, b) \in \mathbb{R}^2$
$|a| \leq b \iff -b \leq a \leq b$
$|a| \geqslant b \iff a \geqslant b$ ou $a \leq -b$

Proposition (Partie Bornée et Valeur Absolue) **:** Soit $A \in \mathcal{P}(\mathbb{R})$
A est bornée $\iff \exists M \in \mathbb{R}, \forall a \in A, |a| \leq M$

Preuve :
$\Longleftarrow$:
On suppose quil existe $M \in \mathbb{R}$ tel que $\forall a \in A, |a| \leq M$

Donc $\forall a \in A, -M \leq a \leq M$
Donc A est majorée par M et minorée par $-M$
Donc A est bornée

$\Longrightarrow$:
On suppose A bornée

Soit M un majorant de A et m un minorant de A
On pose $\alpha = \max(M, -m)$
$\alpha \geqslant M$ et $\forall a \in A, a \leq \alpha$

On a aussi $\alpha \geqslant m$ donc $-a \leq -m$
donc $-m$ est un majorant

$\forall a \in A, -\alpha \leq a \leq \alpha$
donc $\forall a \in A, |a| \leq \alpha$

□

12 Bornes Inférieure / Supérieure

Proposition (Existence de la Borne Inférieure) **:** Toute partie minorée, non vide de $\mathbb{R}$ admet une borne inférieure

Preuve :
Soit $A \in \mathcal{P}(\mathbb{R})$ non vide et minorée
Soit $B = -a | a \in A \neq \varnothing$
Soit m un minorant de A

$\forall a \in A, m \leq a$
donc $\forall a \in A, -a \geqslant -m$
donc B est majoré par m

Daprès la propriété de la borne supérieure, B admet une borne supérieure
On suppose $\beta = \sup(B)$

β majore B donc $\forall a \in A, -a \leq \beta$
donc $\forall a \in A, -\beta \leq a$
donc $-\beta$ est un majorant de A

Soit x un minorant de A
Montrons que $x \leq -\beta$
$-x$ majore B donc $-x \geqslant \beta$ donc $x \leq -\beta$

Donc $-\beta = \inf(A)$

□

Proposition (Caractérisation de la Borne Supérieure) **:** Soient $A \in \mathcal{P}(\mathbb{R})$ non vide majorée et $M \in \mathbb{R}$

$$M = \sup(A) \iff \begin{cases} \forall a \in A, a \leq M \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 > M - \varepsilon \end{cases}$$

Preuve :
$\Longrightarrow$: On suppose $M = \sup(A)$

M est un majorant de A donc $\forall a \in A, a \leq M$
et cest le plus petit majorant

Soit $\varepsilon > 0$
$M - \varepsilon > M$ donc $M - \varepsilon$ ne majore pas A

$\exists a_0 \in A, a_0 > M - \varepsilon$

$\Longleftarrow$: On suppose $\begin{cases} \forall a \in A, a \leq M & 1 \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 > M - \varepsilon & 2 \end{cases}$

Daprès 1, M est un majorant de A
Soit M' un majorant de A, montrons $M' \geqslant M$
On suppose $M' \leq M$, on pose $\varepsilon = M - M' \geqslant 0$

Daprès 2, il existe $a_0 \in A$ tel que
$a_0 > M - \varepsilon = M' \geqslant a_0$ contradiction

Donc $M' \geqslant M$
Donc M est le plus petit majorant de A
Donc $M = \sup(A)$

□

Proposition (Caractérisation de la Borne Inférieure) **:** Soient $A \in \mathcal{P}(\mathbb{R})$ non vide minorée et $M \in \mathbb{R}$
$M = \inf(A) \iff \begin{cases} \forall a \in A, a > M \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 < M + \varepsilon \end{cases}$

Proposition (Inégalité et Borne Supérieure) **:** Soit $A \in \mathcal{P}(\mathbb{R})$ non vide majorée et $M \in \mathbb{R}$
$M \geqslant \sup(A) \iff \forall a \in A, M \geqslant a$

Preuve :
$\Longrightarrow$: On suppose $M \geqslant \sup(A)$
Soit $a \in A$, on sait que $a \leq \sup(A)$ car $\sup(A)$ majore A
Donc $a \leq M$

$\Longleftarrow$: On suppose $\forall a \in A, a \leq M$
Donc M majore A
Or, $\sup(A)$ est le plus petit majorant de A donc $M \geqslant \sup(A)$

□

Proposition (Inégalité et Borne Inférieure) **:** Soit $A \in \mathcal{P}(\mathbb{R})$ non vide minorée et $m \in \mathbb{R}$
$m \leq \inf(A) \iff \forall a \in A, a > m$

Proposition ($\mathbb{R}$ est archimédien) **:** $\mathbb{R}$ est archimédien :
$\forall x \in \mathbb{R}_\star^+, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx \geqslant y$

Preuve :
Soient $(x, y) \in \mathbb{R}_\star^+ \times \mathbb{R}$
Supposons $(H) : \forall n \in \mathbb{N}, nx \leq y$

On pose $A = \{nx | n \in \mathbb{N}\} \subset \mathbb{R}$
$A \neq \varnothing$ car $0 \in A$
Daprès (H), A est majoré par y
Soit $\alpha = \sup(A)$

Soit $n \in \mathbb{N}$
$(n+1)x \in A$ donc $(n+1)x \leq \alpha$
donc $nx \leq \alpha$

Donc $\begin{cases} \alpha - x \geqslant nx \\ \alpha - x < \alpha \end{cases}$ Contradiction avec le fait que α soit le plus petit majorant de A

Donc $\exists n \in \mathbb{N}, nx \geqslant y$

□

Proposition (Théorème des Valeurs Extrêmes) **:** Toute fonction continue sur un segment est bornée et atteint ses bornes

Si $f : [a, b] \longrightarrow \mathbb{R}$ est continue, alors
$\exists (\alpha, \beta) \in [a, b]^2, \forall x \in [a, b], \quad f(\alpha) \leq f(x) \leq f(\beta)$

Preuve :
Voir Chapitre 12 : Suites

□

Proposition (Limite de Suite et Borne Supérieure) **:** Soit $A \in \mathcal{P}(\mathbb{R})$ non vide majorée
Il existe une suite $(a_n) \subset A$ telle que
$\lim a_n = \sup(A)$

Preuve :
On sait que $\forall \varepsilon > 0, \exists a \in A, a > \sup(A) - \varepsilon$

Donc $\forall n \in \mathbb{N}^\star, \exists a_n > sup(A) - \dfrac{1}{n}$
$\forall n \in \mathbb{N}, a_n \in A$ donc $a_n < \sup(A)$
$\forall a \in \mathbb{N}^\star, \sup(A) - \dfrac{1}{n} < a_n < \sup(A)$

Par encadrement, $a_n \underset{n \longrightarrow +\infty}{\longrightarrow} \sup(A)$

□

Proposition (Limite de Suite et Borne Inférieure) **:** Soit $A \in \mathcal{P}(\mathbb{R})$ non vide minorée
Il existe une suite $(a_n) \subset A$ telle que
$\lim a_n = \inf(A)$

13 Partie Entière

Proposition (Définition) **:** Soit $x \in \mathbb{R}$
$\exists! n \in \mathbb{Z}, n \leq x < n + 1$
Cet entier est appelé partie entière de x et noté $\lfloor x \rfloor$

Preuve :
Soit $A = \{p \in \mathbb{Z} | p > x\}$
$A \neq \varnothing$ car $\mathbb{R}$ est archimédien
A est minoré par x

Soit α la borne inférieure de A, alors $\alpha \geqslant x$
Montrons que $\alpha \in \mathbb{Z}$

Soit $n \geqslant 2, \alpha + \dfrac{1}{n} \geqslant \alpha$
donc $\exists a_n \in A, \alpha \leq a_n \leq \alpha + \dfrac{1}{n}$

$\dfrac{1}{n} < 1$ car la distance entre deux entiers est $\geqslant 1$
Il y a au plus 1 entier dans $[\alpha, \alpha + \dfrac{1}{n}]$

Donc tous les a_n sont égaux et $a_n \longrightarrow \alpha$ donc $\forall n \geqslant 2, a_n = \alpha$
donc $\alpha \in A$, donc $\alpha = \min(A)$, alors $\alpha - 1 \notin A$
donc $\alpha - 1 \leq x \leq a$
On pose $n = \alpha - 1$

□

14 Densité

Définition (Densité) **:** Soit $A \in \mathcal{P}(\mathbb{R})$
On dit que A est dense dans $\mathbb{R}$ si :
Pour tout intervalle I ouvert non vide de $\mathbb{R}$, $A \cap I \neq \varnothing$

Théorème (Densité de $\mathbb{Q}$) **:** $\mathbb{Q}$ est dense dans $\mathbb{R}$

Preuve :
Soit I un intervalle ouvert non vide de $\mathbb{R}$
Soient $a < b$ deux éléments de I

On cherche $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ tels que $a < \dfrac{p}{q} < b$

Comme $\mathbb{R}$ est archimédien, $\exists q \in \mathbb{N}^\star, q(b-a) \geqslant 2 > 1$
Donc lintervalle $[qa, qb]$ a une longueur supérieure à 1
Il contient donc au moins 1 entier p

En effet, sinon on a $\lfloor qa \rfloor = \lfloor qb \rfloor$ et alors
$\begin{cases} \lfloor qa \rfloor \leq qb \leq \lfloor qa \rfloor + 1 \\ \lfloor qa \rfloor \leq qa \leq \lfloor qa \rfloor + 1 \end{cases}$

et alors $-1 < qb - qa < 1$ contradiction

On a donc $qa \leq p \leq qb$
et finalement $a \leq \dfrac{p}{q} \leq b$

□

Théorème (Densité de $\mathbb{RQ}$) **:** $\mathbb{RQ}$ est dense dans $\mathbb{R}$

Preuve :
Soit I un intervalle ouvert non vide de R

On pose $J = \{x - \sqrt{2} | x \in I\}$, J est ouvert et non vide
$\mathbb{Q}$ est dense dans $\mathbb{R}$ donc $J \cap \mathbb{Q} \neq \varnothing$

Soit $r \in J \cap \mathbb{Q}$, alors $r + \sqrt{2} \in I$
Soit $s \in Q = r + \sqrt{2}$, alors $\sqrt{2} = s - r \in \mathbb{Q}$
ce qui nest pas le cas
Ainsi, $r + \sqrt{2} \in I \cap (\mathbb{RQ})$

□

Remarque (Suite de Rationnels) :
Soit $x \in \mathbb{R}, \forall n \in \mathbb{N}^\star, I_n =]x - \dfrac{1}{n}, x + \dfrac{1}{n}[$
Pour tout $n \in \mathbb{N}^\star$, on choisit $r_n \in Q \cap I$
On a défini une suite de rationnels (r_n)
$\forall n \in \mathbb{N}^\star, x - \dfrac{1}{n} \leq r_n \leq x + \dfrac{1}{n}$
Par encadrement, $r_n \longrightarrow x$

Proposition (Approximation par Défaut et par Excès) **:** Soit $x \in \mathbb{R}$
Alors, $\forall n \in \mathbb{N}$, $\dfrac{\lfloor 10^n x \rfloor}{10^n} \leq x < \dfrac{\lfloor 10^n x \rfloor}{10^n} + \dfrac{1}{10^n}$

On démontrera que $\dfrac{\lfloor 10^n x \rfloor}{10^n} \underset{n \longrightarrow +\infty}{\longrightarrow} x$

Preuve :
$\forall n \in \mathbb{N}, \lfloor 10^n x \rfloor \leq 10^n x < \lfloor 10^n x \rfloor + 1$

□

Corollaire (Densité de $\boldsymbol{D}$) **:** Soit D lensemble des nombres décimaux
$D = \{\frac{p}{10^n} | p \in \mathbb{Z}, n \in \mathbb{N}\}$
D est dense dans $\mathbb{R}$

15 Intervalles

Définition (Intervalle de $\mathbb{R}$) **:** Un intervalle de $\mathbb{R}$ est une partie de $\mathbb{R}$ dune de ces formes :
$\{x \in \mathbb{R} | a \leq x \leq b\}, (a, b) \in \mathbb{R}^2$
$\{x \in \mathbb{R} | a \leq x < b\}, a \in \mathbb{R}, b \in \mathbb{R} \cup \{+\infty\}$
$\{x \in \mathbb{R} | a < x \leq b\}, a \in \mathbb{R} \cup \{-\infty\}, b \in \mathbb{R}$
$\{x \in \mathbb{R} | a < x < b\}, a \in \mathbb{R} \cup \{-\infty\}, b \in \mathbb{R} \cup \{+\infty\}$

Définition (Partie Convexe) **:** Soit D une partie de $\mathbb{R}$
On dit que D est convexe si $\forall (x, y) \in D^2, x \leq y \Longrightarrow [x, y] \in D$

Théorème (Intervalle et Convexité) **:** Soit $D \in \mathcal{P}(\mathbb{R})$
D est un intervalle $\iff$ D est convexe

Preuve :
$\Longrightarrow$: On suppose que D est un intervalle

Cas 1 : On suppose $D = [a, b]$ avec $(a, b) \in \mathbb{R}^2$ et $a \leq b$
Soient $(x, y) \in D^2$ avec $x \leq y$
Soit $z \in [x, y]$
On a donc $a \leq x \leq z \leq y \leq b$ donc $z \in [a, b]$
Donc D est convexe

Cas 2 : On suppose $D = [a, b[$ avec $a \in \mathbb{R}, b \in \mathbb{R} \cup \{+\infty\}$ et $a < b$

Soient $(x, y) \in D^2$ avec $x \leq y$
Soit $z \in [x, y]$
On a donc $a \leq x \leq z \leq y < b$ donc $z \in [a, b]$
Donc D est convexe

Les deux autres cas se traitent de la même façon

$\Longleftarrow$: On suppose que D est convexe et non vide

On pose $M = \begin{cases} \sup(D) \text{ si } D \text{ est majorée} \\ +\infty \text{ sinon} \end{cases}$ et $m = \begin{cases} \inf(D) \text{ si } D \text{ est minorée} \\ -\infty \text{ sinon} \end{cases}$

Montrons que
$]m, M[\subset D \subset [m, M]$ si $(m, M) \in \mathbb{R}^2$
$]m, M[\subset D \subset [m, M[$ si $m \in \mathbb{R}, M = +\infty$
$]m, M[\subset D \subset]m, M]$ si $m = -\infty, M \in \mathbb{R}$
$]m, M[\subset D \subset]m, M[$ si $m = -\infty, M = +\infty$

Soit $z \in]m, M[$
Si $M \in \mathbb{R}$, z ne majore pas D car $z \leq M$
Si $M = +\infty$, D nest pas majorée donc z nest pas un majorant
Donc $\exists y \in D, y \geqslant z$

Si $m \in \mathbb{R}$, z ne minore pas D car $m \leq z$
Si $m = -\infty$, D nest pas minorée donc z nest pas un minorant
Donc $\exists x \in D, x \leq z$

Donc $z \in [x, y] \subset D$ car $\begin{cases} (x, y) \in D^2 \\ D \text{ convexe} \end{cases}$

Donc $z \in D$, on a bien $]m, M[\subset D$

Cas 1 : On suppose $(m, M) \in \mathbb{R}^2$

Soit $z \in D$, $\begin{cases} m \text{ minore } D \text{ donc } m \leq z \\ M \text{ majore } D \text{ donc } z \leq M \end{cases}$ donc $z \in [m, M]$

Donc $D \in \{]m, M[,\ [m, M[,\ ]m, M],\ [m, M]\}$
Donc D est un intervalle

Cas 2 : On suppose $m \in \mathbb{R}, M = +\infty$

Soit $z \in D$, $\begin{cases} m \text{ minore } D \text{ donc } m \leq z \\ M = +\infty \end{cases}$ donc $z \in [m, +\infty[$

Donc $D \in \{]m, M[,\ [m, M[\}$
Donc D est un intervalle

Cas 3 : On suppose $m = -\infty, M \in \mathbb{R}$

Soit $z \in D, \begin{cases} m = -\infty \\ M \text{ majore } D \text{ donc } z \leq M \end{cases}$ donc $z \in]-\infty, M]$

Donc $D \in \{]m, M[,\ ]m, M]\}$
Donc D est un intervalle

Cas 4 : On suppose $m = -\infty, M = +\infty$

Soit $z \in \mathbb{R}$ donc $z \in]-\infty, +\infty[$

$D = \mathbb{R}$ donc D est un intervalle

□

Proposition (Bornes, Min et Max) **:** Soient $a, b \in \mathbb{R}$

$\inf([a, b]) = \min([a, b]) = a$
$\sup([a, b]) = \max([a, b]) = b$

$\inf(]a, b[) = a$
$\sup(]a, b[) = b$

$\inf([a, b[) = \min([a, b[) = a$
$\sup([a, b[) = b$

$\inf(]a, b]) = a$
$\sup(]a, b]) = \max(]a, b]) = b$

Proposition (Intersection dIntervalles) **:** Un intersection quelconque dintervalles est convexe

Preuve :

Soit $(I_a)_{a\in A}$ une famille dintervalles et $I = \bigcap_{a\in A} I_a$

Montrons que I est un intervalle
Montrons que I est convexe

Soit $(x, y) \in I^2, x \leq y$, montrons $[x, y] \subset I$

Soit $z \in [x, y]$
Soit $a \in A$

$x \in I$ donc $x \in I_a$
$y \in I$ donc $y \in I_a$

I_a est convexe
Donc $z \in I_a$

□

Remarque (Réunion dIntervalles) :
Un réunion dintervalles nest pas nécessairement un intervalle

16 Fonction Convexes

Définition (Fonction Convexe) **:** Soit $f : I \longrightarrow \mathbb{R}$ avec I un intervalle
On dit que f est convexe si
$\forall (x, y) \in I^2, \forall \lambda \in [0, 1], f((1-\lambda)x + \lambda y) \leq (1-\lambda)f(x) + \lambda f(y)$

Proposition (Expression dun Elément dun Intervalle selon les Bornes) **:**
Soit $(a, b) \in \mathbb{R}^2$ avec $a \leq b$
Soit $x \in \mathbb{R}$
$x \in [a, b] \iff \exists \lambda \in [0, 1], x = (1-\lambda)a + \lambda b$

Preuve :
$x \in [a, b] \iff a \leq x \leq b$
$\iff 0 \leq x - a \leq b - a$
$\iff 0 \leq \dfrac{x-a}{b-a} \leq 1$

$\iff \exists \lambda \in [0,1], \lambda = \dfrac{x-a}{b-a}$
$\iff \exists \lambda \in [0,1], x = \lambda(b-a)+a$
$\iff \exists \lambda \in [0,1], x = \lambda b - \lambda a + a$
$\iff \exists \lambda \in [0,1], x = (1-\lambda)a + \lambda b$

□

Proposition (Inégalité de Jansen) **:** Soit $f : I \longrightarrow \mathbb{R}$ convexe et $(x_1...x_n) \in I^n, (\lambda_1...\lambda_n) \in [0,1]^n$ tels que $\sum_{i=1}^{n} \lambda_i = 1$ et $n \geqslant 2$

Alors $f(\sum_{i=1}^{n} \lambda_i x_i) \leq \sum_{i=1}^{n} \lambda_i f(x_i)$

Preuve :
Soit $n \geqslant 2$
$\forall (x_1...x_n) \in I^n, (\lambda_1...\lambda_n) \in [0,1]^n$ tels que $\sum_{i=1}^{n} \lambda_i = 1$
On a $f(\sum_{i=1}^{n} \lambda_i x_i) \leq \sum_{i=1}^{n} \lambda_i f(x_i)$

Soient $(x_1...x_{n+1}) \in I^{n+1}, (\lambda_1...\lambda_{n+1}) \in [0,1]^{n+1}$
On suppose $\sum_{i=1}^{n+1} \lambda_i = 1$
On suppose $\lambda_{n+1} \neq 1$

On pose $\begin{cases} \lambda = \sum_{i=1}^{n} \lambda_i = 1 - \lambda_{n+1} \neq 0 \\ x = \dfrac{1}{\lambda} \sum_{i=1}^{n} \lambda_i x_i = \sum_{i=1}^{n} \dfrac{\lambda_i}{\lambda} x_i \in I \end{cases}$

Ainsi, $f(\sum_{i=1}^{n+1} \lambda_i x_i) = f(\lambda_{n+1} x_{n+1} + \sum_{i=1}^{n} \lambda_i x_i)$
$= f((1-\lambda)x_{n+1} + \lambda x) \leq (1-\lambda) f(x_{n+1}) + \lambda f(x)$

De plus, $f(x) = f(\sum_{i=1}^{n} \mu_i x_i)$ avec $\forall i \in [\![1,n]\!], \mu_i = \dfrac{\lambda_i}{\lambda}$
$\sum_{i=1}^{n} \mu_i = \sum_{i=1}^{n} \dfrac{\lambda_i}{\lambda} = \dfrac{1}{\lambda} + \lambda = 1$

Daprès lhypothèse de récurrence,
$f(x \leq \sum_{i=1}^{n} \frac{\lambda_i}{\lambda} f(x_i))$
Doù
$f(\sum_{i=1}^{n+1} \lambda_i x_i) = \lambda_{n+1} f(x_{n+1}) + \sum_{i=1}^{n} \lambda_i f(x_i)$

Montrons que $x \in I$
On pose $\begin{cases} \alpha = \min\{x_i | i \in [\![1, n]\!]\} \in I \\ \beta = \max\{x_i | i \in [\![1, n]\!]\} \in I \end{cases}$

$\forall i \in [\![1, n]\!], \alpha \leq x_i \leq \beta$
donc $\forall i \in [\![1, n]\!], \frac{\lambda_i}{\lambda}\alpha \leq \frac{\lambda_i}{\lambda} x_i \leq \frac{\lambda_i}{\lambda}\beta$
donc $\sum_{k=1}^{n} \frac{\lambda_i}{\lambda}\alpha \leq \sum_{k=1}^{n} \frac{\lambda_i}{\lambda} x_i \sum_{k=1}^{n} \frac{\lambda_i}{\lambda}\beta$
donc $\alpha \leq x \leq \beta$

Donc, par convexité de I,
On suppose $\lambda_{n+1} = 1$, alors $\sum_{i=1}^{n} \lambda_i = 0$

Or, $\forall i \in [\![1, n]\!], \lambda_i \geqslant 0$
Donc $\forall i \in [\![1, n]\!], \lambda_i = 0$
$f(\sum_{i=1}^{n} \lambda_i x_i) = f(x_{n+1}) \leq \sum_{i=1}^{n+1} \lambda_i f(x_i) = f(x_{n+1})$

□

Proposition (Lemme des Pentes) **:** Soit $f : I \longrightarrow \mathbb{R}$ convexe
Soient $x_1 < x_2 < x_3 \in I^3$
Alors $\frac{f(x_1) - f(x_2)}{x_1 - x_2} \leq \frac{f(x1) - f(x_3)}{x_1 - x_3} \leq \frac{f(x_2) - f(x_3)}{x_2 - x_3}$

Preuve :
Soit $\lambda \in]0, 1[$ tel que $x_2 = (1 - \lambda)x_1 + \lambda x_3$
$f(x_2) - f(x_1) \leq (1 - \lambda) f(x_1) + \lambda f(x_3) - f(x_1)$
$\leq \lambda(f(x_3) - f(x_1))$
$x_2 - x_1 = \lambda(x_3 - x_1) > 0$

Doù $\frac{f(x_2) - f(x_1)}{x_2 - x_1} \leq \frac{\lambda(f(x_3) - f(x_1))}{\lambda(x_3 - x_1)} \leq \frac{f(x_3) - f(x_1)}{x_3 - x_1}$

$f(x_2) - f(x_3) \leq (1-\lambda)f(x_1) + \lambda f(x_3) - f(x_3)$
$\leq (1-\lambda)(f(x_1) - f(x_3))$

$x_2 - x_3 = (1-\lambda)(x_1 - x_3) < 0$
$\frac{f(x_2) - f(x_3)}{x_2 - x_3} \geq \frac{(1-\lambda)(f(x1) - f(x_3))}{(1-\lambda)(x_1 - x_3)} \geq \frac{f(x_1) - f(x_3)}{x_1 - x_3}$

□

Proposition (Réciproque du Lemme des Pentes) **:** Soit $f : I \longrightarrow \mathbb{R}$

Si, $\forall x_1 < x_2 < x_3 \in I^3, \frac{f(x_1) - f(x_2)}{x_1 - x_2} \leq \frac{f(x_1) - f(x_3)}{x_1 - x_3}$
Alors f est convexe

Preuve :
Soient $x \leq y \in I^2$
Soient $\lambda \in]0,1[$ et $z = (1-\lambda)x + \lambda y$

Montrons que $f(z) \leq (1-\lambda)f(x) + \lambda f(y)$
On pose $\begin{cases} x_1 = x \\ x_2 = z \\ x_3 = y \end{cases}$ Ainsi, $x_1 < x_2 < x_3$
Donc $\frac{f(x) - f(z)}{x - z} \leq \frac{f(x) - f(y)}{x - y}$ $(\star)$ et $\lambda = \frac{z - x}{y - x}$

$(\star) \Longrightarrow \frac{f(z) - f(x)}{z - x} \leq \frac{f(y) - f(x)}{y - x}$
$\Longrightarrow f(z) - f(x) \leq \frac{f(y) - f(x)}{y - x}(z - x)$
$\Longrightarrow f(z) \leq \lambda(f(y) - f(x)) + f(x) = \lambda f(y) + (1-\lambda)f(x)$

□

Remarque (Autres Preuves Possible) :
Si on remplace $(\star)$ par $\frac{f(x_1) - f(x_3)}{x_1 - x_3} \leq \frac{f(x_2) - f(x_3)}{x_2 - x_3}$ ou par $\frac{f(x_1) - f(x_2)}{x_1 - x_2} \leq \frac{f(x_2) - f(x_3)}{x_2 - x_3}$
On peut aussi conclure que f est convexe

Proposition (Théorème Convexité / Dérivabilité) **:** Soit $f : I \longrightarrow \mathbb{R}$ convexe sur I ouvert
Alors f est dérivable à gauche et) droite en tout point de I et
$\forall x \in I, f'_{gauche}(x) \leq f'_{droite}(x)$

Preuve :
Soit $a \in I$ et $\tau_a : I\{a\} \longrightarrow \mathbb{R}$
$x \longmapsto \dfrac{f(x) - f(a)}{x - a}$

Daprès le Lemme des Pentes, τ_a est croissante
En effet, soient $(x, y) \in (I\{a\})^2$ et $x < y$

Cas 1 : $a < x < y$
On a alors $\dfrac{f(x) - f(a)}{x - a} \leq \dfrac{f(y) - f(a)}{y - a}$
Donc $\tau_a(x) \leq \tau_a(y)$

Cas 2 : $x \leq a \leq y$
On a alors $\dfrac{f(x) - f(a)}{x - a} \leq \dfrac{f(x) - f(y)}{x - y} \leq \dfrac{f(y) - f(a)}{y - a}$
Donc $\tau_a(x) \leq \tau_a(y)$

Cas 3 : $x \leq y \leq a$
On a alors $\dfrac{f(x) - f(y)}{x - y} \leq \dfrac{f(x) - f(a)}{x - a} \leq \dfrac{f(y) - f(a)}{y - a}$
Donc $\tau_a(x) \leq \tau_a(y)$

Donc $\tau_a(x) \leq \tau_a(x)$

Soit $x > a$ avec $x \in I$
On fixe $z_0 < a$ avec $z_0 \in I$

Alors $\tau_a(x) \geqslant \tau_a(z_0)$
τ_a est minorée sur $I \cap]a, +\infty[$ et croissante
Donc τ_a a une limite finie quand x tend vers a par valeur supérieure
Donc f est dérivable à droite et $f'_{droite}(a) \geqslant \tau_a(z_0)$

Soit $z_1 > a$ fixé
$\forall x \in I \cap]-\infty, a[, \tau_a(x) \leq \tau_a(z_1)$
Donc τ_a est majorée sur $I \cap]-\infty, a[$
Donc τ_a a une limite finie que x tend vers a par valeur inférieure

Donc f est dérivable à gauche et $f'_{gauche}(a) \leq \tau_a(z_1)$

De plus, $\forall x \in I \cap]-\infty, a[,\ \forall y \in]a, +\infty[,\ \tau_a(x) \leq \tau_a(y)$

Donc, si on fait tendre x vers a par valeur inférieure :
$\forall y \in I \cap]a, +\infty[, f'_{gauche}(a) \leq \tau_a(y)$
Si on fait tendre y par valeur supérieure :
$f'_{gauche}(x) \leq f'_{droite}(x)$

□

Corollaire : Soit $f : I \longrightarrow \mathbb{R}$ convexe où I est ouvert
Alors f est continue sur I

Preuve :
Soit $a \in I$

$\forall x \in I \cap]-\infty, a[, \dfrac{f(x) - f(a)}{x - a} = f'_g(a) + \underset{\substack{x \to a \\ <}}{o}(1)$
Donc $f(x) = f(a) + f'_g(a)(x - a) + \underset{\substack{x \to a \\ <}}{o}(x - a)$
Donc $f(x) \underset{\substack{x \to a \\ <}}{\longrightarrow} f(a)$

De même, $\forall x \in I \cap]a, +\infty[, f(x) = f(a) + f'_d(a) + \underset{\substack{x \to a \\ >}}{o}(x - a)$
Donc $f(x) \underset{\substack{x \to a \\ >}}{\longrightarrow} f(a)$
Donc f est continue en a

□

Proposition (Théorème Convexité / Croissance Dérivée) **:** Soit $f : I \longrightarrow \mathbb{R}$ dérivable
f est dérivable $\iff$ f' est croissance

Preuve :
$\Longrightarrow$: On suppose que I a au moins 2 éléments distincts, sinon le résultat

est trivial
On suppose f convexe

Soient $(x, y) \in I^2$, on suppose $x < y$
Soit $u \in]x, y[$
Soit $\tau_x : u \longmapsto \dfrac{f(u) - f(x)}{u - x}$

Comme τ_x est croissante sur $I\{x\}$, $f'(x) \leq \tau_x(u)$
Daprès le Lemme des Pentes,
$\dfrac{f(u) - f(x)}{u - x} \leq \dfrac{f(x) - f(y)}{x - y} \leq \dfrac{f(y) - f(u)}{y - u}$
et donc $\tau_x(u) \leq \tau_y(u)$

Comme τ_y est croissante, $\tau_y(u) \leq f'(y)$
Doù $f'(x) \leq \tau_x(u) \leq \tau_y(u) \leq f'(y)$
Donc f' est croissante

$\Longleftarrow$: On va exploiter le Théorème des Accroissements Finis

Soit $f : [a, b] \longrightarrow \mathbb{R}$ continue dérivable sur $]a, b[$
Alors $\exists c \in]a, b[, f'(c) = \dfrac{f(a) - f(b)}{a - b}$

Soient $x_1 < x_2 < x_3 \in I^3$
f est continue sur $[x_1, x_2]$ et dérivable sur $]x_1, x_2[$
$\exists c_1 \in]x_1, x_2[, \dfrac{f(x_1) - f(x_2)}{x_1 - x_2} = f'(c_1)$

f est continue sur $[x_2, x_3]$ et dérivable sur $]x_2, x_3[$
$\exists c_2 \in]x_2, x_3[, \dfrac{f(x_2) - f(x_3)}{x_2 - x_3} = f'(c_2)$

On remarque que $c_1 < x < c_2$
Comme f' est croissante, $f'(c_1) \leq f'(c_2)$

□

Corollaire : Soit $f : I \longrightarrow \mathbb{R}$ deux fois dérivable
f convexe sur $I \iff \forall x \in I, f''(x) > 0$

Proposition (Inégalité Image / Taux de Variation) **:** Soit $f : I \longrightarrow \mathbb{R}$

convexe, dérivable
$\forall (x,a) \in I^2, f(x) \geqslant f'(a)(x-a)+f(a)$

Preuve :
Soit $a \in I$
On pose $g : I \longrightarrow \mathbb{R}$
$x \longmapsto f(x) - f'(a)(x-a) + f(a)$

g est dérivable sur I et $g'(x) = f'(x) - f'(a)$
On sait que f' est croissante sur I

g est décroissante pour $x < a$, croissante pour $x > a$ et $g(a) = 0$
$\forall x \in I, g(x) \geqslant 0$

□

Définition (Concavité) **:** On dit que f est concave si $-f$ est convexe

Proposition (Concavité) **:** Soit $f : I \longrightarrow \mathbb{R}$
f concave $\iff \forall (x,y) \in I^2, \forall \lambda \in [0,1], f((1-\lambda)x + \lambda y) \geqslant (1-\lambda)f(x) + \lambda f(y)$

Si f est concave sur un intervalle I ouvert, f est continue

Si f est dérivable, f concave $\iff$ f' décroissante

Si f est deux fois dérivable, f concave $\iff$ f'' négative

Si f est dérivable et concave, $\forall (x,a) \in I^2, f(x) < f'(a)(x-a) + f(a)$

Chapitre 10

Nombres entiers - $\mathbb{N}$

1 Axiomatique de $\mathbb{N}$

Axiome : $(\mathbb{N}, \leqslant)$ est un ensemble non vide totalement ordonné vérifiant

- Toute partie non vide de $\mathbb{N}$ a un plus petit élément ;
- Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément ;
- $\mathbb{N}$ n'est pas majoré.

Définition :
- 0 est le plus petit élément de $\mathbb{N}$: $0 = \min(\mathbb{N})$.
- $1 = \min(\mathbb{N}^\star) = \min\big(\mathbb{N} \setminus \{0\}\big)$.
- Soit $n \in \mathbb{N}$. On pose $n+1 = \min\big(\{k \in \mathbb{N} \mid k > n\}\big)$. On dit que $n+1$ est le successeur de n.
- Soit $n \in \mathbb{N}^\star$. On pose $n-1 = \max\big(\{k \in \mathbb{N} \mid k < n\}\big)$. On dit que $n-1$ est le prédécesseur de n.

Proposition :

$$\begin{cases} \forall n \in \mathbb{N},\ (n+1) - 1 = n; \\ \forall n \in \mathbb{N}^\star,\ (n-1) + 1 = n. \end{cases}$$

Preuve :
Soit $n \in \mathbb{N}$. On pose $p = n+1$ et $q = p-1$. On a donc $n < p$ et $q < p$ et donc $n \leqslant q$ car $q = \max\big(\{k \in \mathbb{N} \mid k < p\}\big)$.

Si $q > n$, alors $q \geqslant p$ car $p = \min\big(\{k \in \mathbb{N} \mid k > n\}\big)$: une contradiction.

On a donc $q = n$. □

Proposition : Pour tout $n \in \mathbb{N}$, $\mathbb{N} \cap]n, n+1[= .$

Preuve :
Soit $n \in \mathbb{N}$. On sait que $n+1 > n$. Soit $p \in \mathbb{N}$ tel que $n < p < n+1$. Comme $p > n$, $p \geqslant n+1$: une contradiction. □

Théorème (récurrence) **:** Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ est vrai ,} \\ \forall n \geqslant n_0,\ P(n) \implies P(n+1), \end{cases}$$

alors

$$\forall n \geqslant n_0,\ P(n) \text{ est vrai.}$$

Preuve :
Soit $A = \{n \in \mathbb{N} \mid n \geqslant n_0 \text{ et } P(n) \text{ faux }\}$ Supposons $A \neq$; A a donc un plus petit élément. On pose $N = \min(A)$.

Cas 1 $N = 0$, alors, comme $N \in A$, on a $n_0 \leqslant 0$ et $P(0)$ fausse. On en déduit que $n_0 = 0$: une contradiction car $P(n_0) = P(0)$ est vraie.

Cas 2 $N \neq 0$. Alors $N-1 \in \mathbb{N}$ et $N-1 \notin A$ (car $N-1 < N$). On en déduit que $N-1 < n_0$ ou $P(N-1)$ vraie.

- Supposons $N-1 < n_0$. $N \in A$ donc $N \geqslant n_0$ et donc $N-1 < n_0 \leqslant N$ donc $N = n_0$. Or, $N \in A$ donc $P(N)$ fausse alors que $P(n_0)$ est vraie.
- Supposons $N-1 > n_0$ et $P(N-1)$ vraie. Comme $N-1 \geqslant n_0$, $P(N-1) \implies P(N)$ et donc $P(N)$ est vraie. Or, $N \in A$ et donc $P(N)$ est fausse.

On en déduit que $A = .$

□

2 Récurrence

Proposition (récurrence double) **:** Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ vraie} \\ P(n_0+1) \text{ vraie} \\ \forall n \in \mathbb{N} \text{ avec } n \geqslant n_0,\ P(n) \text{ et } P(n+1) \implies P(n+2) \end{cases}$$

Alors
$$\forall n \in \mathbb{N} \text{ avec } n \geqslant n_0,\ P(n) \text{ vraie.}$$

Preuve :
On pose, pour tout $n \geqslant n_0$,
$$Q(n) : \text{“}P(n) \text{ et } P(n+1)\text{”}.$$
— $Q(0)$ est vraie.
— Soit $n \geqslant n_0$. On suppose $Q(n)$ vraie. On sait alors que $P(n+2)$ est vraie. De plus, par hypothèse de récurrence, $P(n+1)$ est vraie. Donc $Q(n+1)$ est vraie.

□

Exemple :
On pose $u_0 = 0$, $u_1 = 1$ et
$$\forall n \in \mathbb{N},\ u_{n+2} = u_{n+1} + u_n$$
Montrons que $\forall n \in \mathbb{N}, u_n \geqslant 0$.
— $u_0 = 0 \geqslant 0$;
— $u_1 = 1 \geqslant 0$;
— Soit $n \in \mathbb{N}$. On suppose que $u_n \geqslant 0$ et $u_{n+1} \geqslant 0$. Alors $u_{n+2} = u_n + u_{n+1} \geqslant 0$.
Par récurrence double,
$$\forall n \in \mathbb{N},\ u_n \geqslant 0.$$

Proposition : Soit P un prédicat, $p \in \mathbb{N}^\star$ et $n_0 \in \mathbb{N}$. Si
$$\begin{cases} \forall k \in [\![0, p-1]\!],\ P(n_0+k) \text{ vraie;} \\ \forall n \geqslant n_0,\ \big(P(n) \text{ et } P(n+1) \text{ et } \cdots \text{ et } P(n+p-1)\big) \implies P(n+p). \end{cases}$$
Alors,
$$\forall n \geqslant n_0, P(n) \text{ vraie.}$$

□

Exemple :
On pose $u_0 = 0$, $u_1 = 1$, $u_2 = 2$, $u_3 = 3$ et
$$\forall n \in \mathbb{N},\ u_{n+4} = u_n + 2u_{n+1} + 3u_{n+2} + u_{n+3}.$$
Montrons que $\forall n \in \mathbb{N},\ u_n \geqslant 0$.
— $u_0 \geqslant 0$, $u_1 \geqslant 0$, $u_2 \geqslant 0$ et $u_3 \geqslant 0$.
— Soit $n \in \mathbb{N}$. On suppose $u_n \geqslant 0$, $u_{n+1} \geqslant 0$, $u_{n+2} \geqslant 0$ et $u_{n+3} \geqslant 0$. Comme u_{n+4} est la somme de réels positifs, $u_{n+4} \geqslant 0$.

Proposition (récurrence forte) **:** Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si $P(n_0)$ est vrai et

$$\forall n \geqslant n_0, \big(P(n_0) \text{ et } \ldots \text{ et } P(n-1) \text{ et } P(n)\big) \implies P(n+1).$$

Alors,

$$\forall n \geqslant n_0,\ P(n) \text{ est vraie.}$$

Preuve :
On pose, pour tout $n \in \mathbb{N}$,

$$Q(n) : \text{“}\forall k \in [\![n_0, n]\!],\ P(k) \text{ vraie”}.$$

— $Q(n_0)$ est vraie car $P(n_0)$ est vraie.
— Soit $n \geqslant n_0$. On suppose $Q(n)$ vraie. On sait donc que $\forall k \in [\![n_0, n]\!],\ P(k)$ vraie. Alors, $P(n+1)$ est vraie et donc

$$\forall k \in [\![n_0, n+1]\!],\ P(k) \text{ est vraie.}$$

Ainsi, $Q(n+1)$ est vraie.

□

Exemple :
Montrer que tout entier supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers. On prouve ce résultat par récurrence forte.

— Le nombre 2 est un nombre premier : $2 = 2$.
— Soit $n \geqslant 2$. On suppose que, tout entier $k \in [\![2, n]\!]$ est un produit de nombres premiers. On pose $N = n + 1$.
Cas 1 N est premier et donc, on peut l'exprimer comme un produit de nombres premiers : $N = N$.
Cas 2 N n'est pas un nombre premier. Alors, il existe p, q tels que $N = p \times q$ avec $1 < p < N$ et $1 < q < N$. Comme $p \in [\![2, n]\!]$, p est un produit de nombres premiers. De même pour q. Donc, le produit $N = p \times q$ est un produit de nombres premiers.

Exemple :
Avec $u_0 = 0$, $u_1 = 1$, $u_2 = 2$, $u_3 = 3$ et, pour tout $n \in \mathbb{N}$, $u_{n+4} = u_n + 2u_{n+1} + 3u_{n+2} + u_{n+3}$, montrer que, pour tout $n \in \mathbb{N}$, $u_n \geqslant 0$. On prouve ce résultat par récurrence forte.

— $u_0 = 0 \geqslant 0$.
— Soit $n \in \mathbb{N}$. On suppose que $\forall k \in [\![1, n]\!],\ u_k \geqslant 0$.
  — Si $n = 0$, $u_{n+1} = u_1 = 1 \geqslant 0$.
  — Si $n = 1$, $u_{n+1} = u_2 \geqslant 0$.
  — Si $n = 2$, $u_{n+1} = u_3 \geqslant 0$.
  — Si $n \geqslant 3$, $u_{n+1} = \underbrace{u_{n-3}}_{\geqslant 0} + 2\underbrace{u_{n-2}}_{\geqslant 0} + 2\underbrace{u_{n-1}}_{\geqslant 0} + 3\underbrace{u_n}_{\geqslant 0} \geqslant 0$.

3 Divisibilité

Définition : Soient $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = k \times a$. Dans ce cas, on écrit $a \mid b$. On dit aussi que a est un diviseur de b ; et que b est un multiple de a.

Exemple : — $\forall x \in \mathbb{Z},\ 1 \mid x$.
— $0 \mid 0$ mais $\forall x \in \mathbb{Z}^\star, 0 \nmid x$.
— $\forall x \in \mathbb{Z},\ x \mid 0$.

Proposition : " $\mid$ " est une relation d'ordre sur $\mathbb{Z}$. □

Proposition : Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$.

$$a \mid b \implies |a| \leqslant |b|.$$

□

Proposition : Soient $a, b, c \in \mathbb{Z}$.

$$\left.\begin{array}{l} a \mid b \\ a \mid c \end{array}\right\} \implies \big(\forall (k, \ell) \in \mathbb{Z}^2,\ a \mid (kb + \ell c)\big).$$

Preuve :
On pose $u, v \in \mathbb{Z}$ tels que

$$\begin{cases} b = au, \\ c = av. \end{cases}$$

Soient $k, \ell \in \mathbb{Z}$.

$$bk + \ell c = aku + a\ell v = a \underbrace{ku + \ell v}_{\in \mathbb{Z}}.$$

et donc $a \mid (ku + \ell v)$. □

Exemple :
Soient $n \in \mathbb{N}$.

$$\left.\begin{array}{l} a \mid n \\ a \mid n+1 \end{array}\right\} \implies a \mid \big((n+1) - n\big) \implies a \mid 1 \implies a = \pm 1.$$

Définition : Soient $a, b \in \mathbb{Z}$. On dit que a et b sont associés si

$$a = b \text{ ou } a = -b.$$

Proposition : Soient $a, b \in \mathbb{Z}$.

$$a \mid b \iff -a \mid b \iff a \mid -b.$$

Proposition (division euclidienne dans $\mathbb{N}$) **:** Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^\star$.

$$\exists!\,(q, r) \in \mathbb{N}^2,\ \begin{cases} a = bq + r, \\ 0 \leqslant r < q. \end{cases} \qquad \begin{array}{r|l} a & b \\ \hline & q \\ r & \end{array}$$

Preuve Existence On considère $A = \{q \in \mathbb{N} \mid qb \leqslant a\}$. $A \neq$ car $0 \in A$: $0 \times b = 0 \leqslant a$. A est majoré :

$$\forall q \in A,\ a \geqslant qb \geqslant q \text{ car } b \geqslant 1.$$

Soit $q = \max(A)$. On pose $r = a - bq$. Comme a, b et q sont des entiers positifs, $r \in \mathbb{Z}$. On sait que $q \in A$, donc $qb \leqslant a$ et donc $r \geqslant 0$. $q + 1 > \max A$ donc $q + 1 \notin A$ i.e. $(q + 1)b > a$ et donc $r < b$.

Unicité Soient $(q', r') \in \mathbb{N}^2$ tels que $\begin{cases} a = q'b + r', \\ 0 \leqslant r' < b. \end{cases}$ Or, $a = bq + r$ et donc, en soustrayant les deux égalités, on a

$$0 = b(q' - q) + r' - r.$$

De plus, $0 \leqslant r < b$ et $-b < -r' \leqslant 0$, et donc

$$r - r' = b\underbrace{(q' - q)}_{\in\mathbb{Z}}.$$

On en déduit que $-b < r - r' < b$. Le seul multiple de b dans $]\!]-b, b[\![$ est 0. Ainsi, $r' = r$ et donc $b(q' - q) = 0$. Or, $b > 0$, donc $q' = q$.

□

Proposition (division euclidienne dans $\mathbb{Z}$) **:** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$.

$$\exists!\,(q,r) \in \mathbb{Z}^2,\ \begin{cases} a = bq + r, \\ 0 \leqslant r \leqslant |b|\,. \end{cases}$$

Preuve Existence Cas 1 $a \in \mathbb{N}$ et $b \in \mathbb{N}^\star$. D'après la proposition précédente,

$$\exists!(q,r) \in \mathbb{N}^2,\ \begin{cases} a = bq + r \\ 0 \leqslant r < b. \end{cases}$$

Comme $b > 0$, on a bien $0 \leqslant r < |b| = b.$ et $q \in \mathbb{N} \subset \mathbb{Z}$.

Cas 2 $a \in \mathbb{Z}^-$ et $b \in \mathbb{N}^\star$. Comme $-a \in \mathbb{N}$,

$$\exists(q',r') \in \mathbb{N}^2,\ \begin{cases} -a = bq' + r', \\ 0 \leqslant r' < b \end{cases}$$

donc

$$\begin{aligned} a &= b(-q') - r' \\ &= b(q'-1) + b - r'. \end{aligned}$$

En posant,

$$q = \begin{cases} -q' - 1 & \text{si } r' \neq 0, \\ -q' & \text{si } r' = 0; \end{cases}$$

$$r = \begin{cases} b - r' & \text{si } r' \neq 0, \\ -r' & \text{si } r' = 0; \end{cases}$$

on a bien

$$\begin{cases} a = bq + r, \\ q \in \mathbb{Z}, \\ 0 \leqslant r < b. \end{cases}$$

Cas 3 $a \in \mathbb{N}$ et $b \in \mathbb{Z}_-^\star$. On sait que

$$\exists(q',r') \in \mathbb{N}^2,\ \begin{cases} a = (-b)q' + r', \\ 0 \leqslant r' < -b. \end{cases}$$

En posant $q = -q'$ et $r = r'$, on a bien $a = bq + r$ et $0 \leqslant r < |b|$.

Cas 4 $a \in \mathbb{Z}^-$ et $b \in \mathbb{Z}_-^\star$. On sait que

$$\exists(q',r') \in \mathbb{N}^2,\ \begin{cases} -a = -bq' + r' \\ 0 \leqslant r' < -b. \end{cases}$$

Donc,

$$\begin{aligned} a &= bq' - r' \\ &= b(q'+1) - r' - b. \end{aligned}$$

En posant

$$q = \begin{cases} q' & \text{si } r' = 0, \\ q'+1 & \text{si } r' \neq 0; \end{cases}$$

$$r = \begin{cases} r' & \text{si } r' = 0, \\ -r' - b & \text{si } r' \neq 0; \end{cases}$$

on a bien

$$\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leqslant r < |b|. \end{cases}$$

Unicité Soient $(q', r') \in \mathbb{Z}^2$ tels que

$$\begin{cases} a = bq' + r' \\ \check{\text{r}} \leqslant r' < |b|. \end{cases}$$

Or, on sait qye $a = bq + r$ et $0 \leqslant r < |b|$. D'où

$$\begin{cases} b(q'-q) = r' - r \\ -|b| < r - r' < |b| \end{cases}$$

donc $r - r' = 0$ et donc $q = q'$.

□

Définition : Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$. D'après le théorème précédent, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$\begin{cases} a = bq + r \\ 0 \leqslant r < |b|. \end{cases}$$

On dit que r est le quotient, et r le reste dans la division (euclidienne) de a par b.

Exemple :
Soit $n \in \mathbb{N}$ impair. On divise n par 2 : soient $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $\begin{cases} n = 2q + r \\ 0 \leqslant r < 2. \end{cases}$

Si $r = 0$, n est pair : une contradiction. Ainsi, $r \neq 0$ et donc $r = 1$. On a donc $n = 2q + 1$.

Proposition : Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$. On note r le reste de la division euclidienne de a par b.

$$r = 0 \iff a \mid b.$$

Preuve :
On pose $a = bq + r$ avec $q \in \mathbb{Z}$.
" $\Longrightarrow$ " Si $r = 0$, alors $a = bq$ avec $q \in \mathbb{Z}$ et donc $b \mid a$.
" $\Longleftarrow$ " Si $b \mid a$, il existe $k \in \mathbb{Z}$ tel que $a = bk$. Donc, $a = bk + 0$ et $0 \leqslant 0 < |b|$. Par unicité de la division euclidienne, $r = 0$.

□

4 Arithmétique modulaire

Définition : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^\star$. On dit que a est congrus à b modulo c si a et b ont le même reste dans la division euclidienne par c. Dans ce cas, on écrit $a \equiv b \ [c]$.

Proposition : La congruence modulo c est une relation d'équivalence.

□

Remarque (Notation) :
On note $\mathbb{Z}/c\mathbb{Z}$ l'ensemble des classes d'équivalences modulo c.

Par exemple, $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Proposition : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^\star$.

$$a \equiv b \ [c] \iff c \mid (b - a).$$

Preuve " $\Longrightarrow$ " Soient $q, q' \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que

$$\begin{cases} a = cq + r \\ b = cq' + r \end{cases}$$

avec $0 < r < c$. En soustrayant les égalités, on obtient

$$b - a = c\underbrace{(q' - q')}_{\in\mathbb{Z}}.$$

Ainsi, $c \mid (b - a)$.

“ $\Longleftarrow$ ” On pose $\begin{cases} a = cq + r \\ b = cq' + r' \end{cases}$ avec $(q, q') \in \mathbb{Z}$ et $\begin{cases} 0 \leqslant r < c \\ 0 \leqslant r' < c. \end{cases}$ En soustrayant les égalités et inégalités, on obtient

$$\begin{cases} b - a = c(q' - q) + r' - r \\ -c < r' - r < c. \end{cases}$$

□

La suite du cours provient d'Aubin. Je ne suis pas responsable pour les éventuelles bêtises qu'il a pu taper.

5 Axiomatique de $\mathbb{N}$

Axiome (Axiomatique de Von Neumann) **:** $(\mathbb{N}, \leq)$ est un ensemble totalement ordonné vérifiant
Toute partie non vide de $\mathbb{N}$ a un plus petit élément
Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément
$\mathbb{N}$ nest pas majoré

Définition (0) : $0 = \min(\mathbb{N})$

Définition (1) : $1 = \min(\mathbb{N}\{0\})$

Définition $(n+1)$: Soit $n \in \mathbb{N}$
On pose $n+1 = \min(\{k \in \mathbb{N} | k > n\})$
On dit que $n+1$ est le successeur de n

Proposition $(+1-1)$: $\forall n \in \mathbb{N}, (n+1)-1 = n$
$\forall n \in \mathbb{N}, (n-1)+1 = n$

Preuve :
Soient $n \in \mathbb{N},\ p = n+1,\ q = p-1$

$n < p$ et $q < p$
Donc $n \leq q$ car $q = \max(\{k \in \mathbb{N} | k < p\})$
Si $q > n$, alors $q \geqslant p$ car $p = \min(\{k \in \mathbb{N} | k > n\})$
Donc $q = n$

□

Proposition (Ensemble Ouvert Vide) **:** $\forall n \in \mathbb{N},]n, n+1[= \varnothing$

Preuve :
Soit $n \in \mathbb{N}$, on sait que $n+1 > n$
Soit $p > n$, on suppose $n < p < n+1$
Comme $p > n, p \geqslant n+1$ Contradiction

□

Proposition (Théorème de Récurrence) **:** Soit P un prédicat sur $\mathbb{N}$ et $n \in \mathbb{N}$
Si $\begin{cases} P(n_0) \text{ est vrai} \\ \forall n \geqslant n_0 n P(n) \Longrightarrow P(n+1) \end{cases}$
Alors $\forall n \geqslant n_0, P(n)$ est vrai

Preuve :
Soit $A = \{n \in \mathbb{N} | n \geqslant n_0\}$ et $P(n)$ faux
Supposons $A \neq \varnothing$
A a donc un plus petit élement, soit $N = \min(A)$

Cas 1 : $N = 0$
Alors, comme $N \in A$, on a $n_0 \leq 0$ et $P(0)$ est faux
Alors $n_0 = 0$ Contradiction avec $P(n)$ est vrai

Cas 2 : $N \neq 0$
Alors $N - 1 \in \mathbb{N}$
$N - 1 \notin A$ car $N - 1 < N$
Donc $N - 1 < n_0$ ou $P(n)$ vrai

Supposons $N - 1 < n_0$
$N \in A$ donc $N \geqslant n_0$
$N - 1 < n_0 < N$
Donc $N = n_0$
Or, $N \in A$ donc $P(n)$ est faux alors que $P(n)$ est vrai

Supposons $\begin{cases} P(n-1) \text{ vrai} \\ N - 1 \geqslant n_0 \end{cases}$ Comme $N - 1 \geqslant n_0, P(N-1) \Longrightarrow P(N)$

Donc $P(N)$ est vrai
Or, $N \in A$ donc $P(N)$ est faux

Donc $A = \varnothing$

□

6 Récurrences

Proposition (Récurrence Double) **:** Soient P un prédicat sur $\mathbb{N}$ et $n_0 \in N$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ P(n_0+1) \text{ est vrai} \\ \forall n > n_0, P(n) \text{ et } P(n+1) \Longrightarrow P(n+2) \end{cases}$

Alors $\forall n \geqslant n_0, P(n)$ est vrai

Preuve :
On pose $\forall n \in \mathbb{N}, Q(n) : P(n)$ et $P(n+1)$ vrais
$Q(n_0)$ est vrai

Soit $n \geqslant n_0$, on suppose $Q(n)$ vrai
On sait alors que $P(n+2)$ est vrai
On sait par hypothèse de récurrence que $P(n+1)$ est vrai
Donc $Q(n+1)$ est vrai

□

Proposition (Récurrence Multiple) **:** Soient P un prédicat sur $\mathbb{N}$ et $(p, n_0) \in \mathbb{N}^2$

Si $\begin{cases} \forall k \in [\![0, p]\!], P(n_0 - k) \text{ est vrai} \\ \forall n \geqslant n_0, (P(n) \text{ et } ... \ P(n+p-1)) \Longrightarrow P(n+p) \end{cases}$

Alors $\forall n \geqslant n_0, P(n)$ est vrai

Proposition (Récurrence Forte) **:** Soient P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ \forall n \geqslant n_0, (P(n_0) \text{ et } ... \ P(n-1)) \Longrightarrow P(n) \end{cases}$

Alors $\forall n \geqslant n_0, P(n)$ est vrai

Preuve :
On pose $\forall n \in N, Q(n) : \forall k \in [\![n_0, n]\!], P(k)$ vrai
$Q(n_0)$ est vrai car $P(n_0)$ est vrai

Soit $n \geqslant n_0$, on suppose $Q(n)$ vrai
On sait que $\forall k \in [\![n_0, n]\!], P(k)$ est vrai
Alors $P(n+1)$ est vrai
Donc $\forall k \in [\![n_0, n+1]\!], P(k)$ est vrai
Donc $Q(n+1)$ est vrai

□

Définition (Divisibilité) **:** Soient $(a, b) \in \mathbb{Z}^2$
On dit que a divise b si il existe $k \in \mathbb{Z}$ tel que $b = ka$
On écrit $a|b$ et on dit que $\begin{cases} a \text{ est un diviseur de } b \\ b \text{ est un multiple de } a \end{cases}$

Proposition (Caractéristiques de la Divisibilité) **:** $|$ est une relation dordre sur $\mathbb{Z}$
Ce nest pas une relation totale

Proposition (Ordonnancement et Divisibilité) **:** Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$
Si $a|b, |a| \leq |b|$

Proposition (Divisibilité et Combinaison Linéaire) **:** Soient $(a, b, c) \in (\mathbb{Z}^\star)^3$
$\begin{cases} a|b \\ a|c \end{cases} \implies \forall (k, l) \in \mathbb{Z}^2, a|(bk + cl)$

Preuve :
$\begin{cases} b = au \text{ avec } u \in \mathbb{Z} \\ c = av \text{ avec } v \in \mathbb{Z} \end{cases}$
Soient $(k, l) \in \mathbb{Z}^2$
$bk + cl = auk + avl = a(uk + vl)$
Donc $a|(bk + cl)$

□

Définition (Nombres Associés) **:** Soient $(a, b) \in \mathbb{Z}^2$

a et b sont associés si $a = b$ ou $a = -b$

Proposition (Nombres Associés et Divisibilité) **:** Soient $(a, b) \in \mathbb{Z}^2$
$a|b \iff -a|b \iff a|-b \iff -a|-b$

8 Division Euclidienne

Proposition (Division Euclidienne dans $\mathbb{N}$) **:** Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^\star$
$\exists!(q, r) \in \mathbb{N}^2, \begin{cases} a = bq + r \\ r \in [0, b[\end{cases}$

Preuve :
Existence : On considère$|$ $A = \{q \in \mathbb{N} | qb \leq a\}$ A est non vide car $0 \in A$
A est majoré : $\forall q \in A, q \leq a$ car $a \geqslant qb \geqslant q$

Soit $q = \max(A)$, on pose $r = a - bq$
Comme a, b et $q \in \mathbb{N}, r \in \mathbb{Z}$
$q \in A$ donc $qb \leq a$ donc $r \geqslant 0$
$q + 1 > \max(A)$ donc $q + 1 \notin A$ donc $(q + 1)b > a$
Donc $r < b$

Unicité : Soit $(q', r') \in \mathbb{N}^2$ tel que $\begin{cases} a + bq' + r' \\ 0 \leq r' < b \end{cases}$
On sait aussi que $a = bq + r$
Donc $0 = b(q' - q) + r' - r$
$-r' + r = b(q' - q)$

De plus, $\begin{cases} 0 \leq r < b \\ -b < -r \leq 0 \end{cases}$
Donc $-b < r' - r < b$

Le seul multiple de b dans $]\!]-b, b[\![$ est 0
Donc $r' - r = 0$, donc $r = r'$
et $b(q' - q) = 0$
Or, $b \neq 0$ donc $q' - q = 0$ donc $q = q'$

□

Proposition (Division Euclidienne dans $\mathbb{Z}$) **:** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$

$\exists!(q,r) \in \mathbb{Z}^2, \left\{ \begin{array}{l} a = bq + r \\ 0 \leq r < |b| \end{array} \right.$

Preuve :

Existence :

Cas 1 : $a \in \mathbb{N}, b \in \mathbb{N}^\star$

Daprès ce qui précède, $\exists!(q,r) \in \mathbb{N}^2, \left\{ \begin{array}{l} a = bq + r \\ 0 \leq r < b \end{array} \right.$

Comme $b \in \mathbb{N}^\star$, on a bien $0 \leq r < |b|$

$q \in \mathbb{N} \subset \mathbb{Z}$

Cas 2 : $a \in \mathbb{Z}, b \in \mathbb{N}^\star$

Comme $-a \in \mathbb{N}, \exists!(q',r') \in \mathbb{N}^2, \left\{ \begin{array}{l} -a = bq' + r' \\ 0 \leq r' < b \end{array} \right.$

Donc $a = b(-q') - r'$

$= b(-q' - 1) - r' + b$

On pose $q = \left\{ \begin{array}{l} -q' - 1 \text{ si } r \neq 0 \\ -q' \text{ si } r = 0 \end{array} \right.$ et $r = \left\{ \begin{array}{l} -r' + b \text{ si } r' \neq 0 \\ r' \text{ si } r' = 0 \end{array} \right.$

On a bien $\left\{ \begin{array}{l} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b| \end{array} \right.$

Cas 3 : $a \in \mathbb{N}, b \in \mathbb{Z}^\star_-$

$\exists!(q',r') \in \mathbb{N}^2, \left\{ \begin{array}{l} a = (-b)q' + r' \\ 0 \leq r' < -b \end{array} \right.$

On pose $\left\{ \begin{array}{l} q = -q' \\ r = r' \end{array} \right.$

Et on a bien $\left\{ \begin{array}{l} a = bq + r \\ 0 \leq r < |b| \end{array} \right.$

Cas 4 : $a \in \mathbb{Z}^-, b \in \mathbb{Z}^\star_-$

$\exists!(q',r') \in \mathbb{N}^2, \left\{ \begin{array}{l} -a = -bq' + r' \\ 0 \leq r' < -b \end{array} \right.$

Donc $a = bq' - r'$

$= b(q' + 1) - r' - b$

On pose $q = \left\{ \begin{array}{l} q' + 1 \text{ si } r \neq 0 \\ q' \text{ si } r = 0 \end{array} \right.$ et $r = \left\{ \begin{array}{l} -r - b' \text{ si } r' \neq 0 \\ r' \text{ si } r' = 0 \end{array} \right.$

On a bien $\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b| \end{cases}$

Unicité :
Soit $(q', r') \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq' + r' \\ 0 \leq r' < |b| \end{cases}$ et $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

Doù $\begin{cases} b(q' - q) = r' - r \\ -|b| < r - r' < |b| \end{cases}$
Donc $r - r' = 0$

Donc $r' = r$ et $q' = q$

□

Définition (Quotient et Reste) **:** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$
Daprès le théorème précédent, $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}$, $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$
On dit que q est le quotient et r le reste dans la division (euclidienne) de a par b

Proposition (Reste et Divisibilité) **:** Soient $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$
On note r le reste de la division de a par b
$r = 0 \iff b|a$

Preuve :
On pose $a = bq + r, q \in \mathbb{Z}$

$\Longrightarrow$: Si $r = 0$, alors $\begin{cases} a = bq \\ q \in \mathbb{Z} \end{cases}$ donc $b|a$

$\Longleftarrow$: Si $b|a$, $\exists k \in \mathbb{Z}, a = bk$
Donc $\begin{cases} a = bk + 0 \\ 0 \leq 0 < |b| \end{cases}$
Par unicité du reste, $r = 0$

□

9 Arithmétique Modulaire

Définition (Congruences) **:** Soient $(a,b) \in \mathbb{Z}^2, c \in \mathbb{N}^\star$
On dit que a et b sont congrus modulo c si a et b ont le même reste dans ma division par c
On note $a = b[c]$

Proposition (Congruence et Relation DEquivalence) **:** La relation de congruence modulo c est une relation déquivalence

Remarque (Classes dEquivalence Modulo c) :
On note $\mathbb{Z}/c\mathbb{Z}$ lensemble des classes déquivalence modulo c
$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Proposition (Modulo et Divisibilité) **:** Soient $(a,b) \in \mathbb{Z}^2$ et $c \in \mathbb{N}^\star$
$a \equiv b[c] \iff c|b-a$

Preuve :
$\Longrightarrow$: On pose $\begin{cases} a = cq + r, q \in \mathbb{Z}, 0 \leq r < c \\ b = cq' + r, q' \in \mathbb{Z} \end{cases}$
Donc $b - a = c(q' - q)$
Donc $c|b-a$

$\Longleftarrow$: On pose $\begin{cases} a = cq + r, q \in \mathbb{Z}, 0 \leq r < c \\ b = cq' + r', q' \in \mathbb{Z}, 0 \leq r' < c \end{cases}$
$b - a = c(q' - q) + r' - r$
$-c \leq r' - r \leq c$

Si $r' - r \geqslant 0, r' - r$ est le reste de la division de $a - b$ par c
Donc $r' = r$ donc $a \equiv b[c]$

Si $r' - r < 0, r - r'$ est le reste de la division de $a - b$ par c
Donc $r' = r$ donc $a \equiv b[c]$

□

Proposition (Addition et Multiplication de Congruences) **:** Soient $(a,b,x,y) \in \mathbb{Z}^4$ et $c \in \mathbb{N}^\star$

On suppose $\begin{cases} a \equiv b[c] \\ x \equiv y[c] \end{cases}$

Alors $\begin{cases} a+x \equiv b+y[c] \\ ax \equiv by[c] \end{cases}$

Preuve :
$c|b-a$ et $c|y-x$
Donc $c|(b-a+y-x)$
Donc $c|(b+y-(a+x))$
Donc $a+x \equiv b+y[c]$

On pose $\begin{cases} a = ck+b, k \in \mathbb{Z} \\ x = cl+y, l \in \mathbb{Z} \end{cases}$
$ax = (ck+b)(cl+y)$
$= by + cky + clk + c^2kl$
$= by + c(ky + bl + clk)$
Donc $ax \equiv by[c]$

□

Proposition (Critères de Divisibilité en Base 10) **:** Soit $N \in \mathbb{N}$, on notera ses chiffres $a_0...a_n$
$N = \sum_{k=0}^{n} 10^k a_k$

Divisibilité par 2 :
N pair $\iff N \equiv 0[2]$
$\iff \sum_{k=0}^{n} 10^k a_k \equiv 0[2]$
$\iff a_0 \equiv 0[2]$ car $\forall k \geqslant 1, 10^k \equiv 0[2]$
$10^0 = 1 \equiv 1[2]$

Divisibilité par 3 :
$\forall k \in \mathbb{N}, 10^k \equiv 1^k \equiv 1[3]$ car $10 \equiv 1[3]$
$3|N \iff N \equiv 0[3]$
$\iff \sum_{k=0}^{n} 10^k a_k \equiv 0[3]$

Divisibilité par 9 :
$\forall k \in N, 10^k \equiv 1[9]$
$9|N \iff N \equiv 0[9]$

$\iff \sum_{k=0}^{n} 10^k a_k \equiv 0[9]$

Divisibilité par 5 :
$\begin{cases} 10^0 \equiv 1[5] \\ \forall k \in \mathbb{N}^\star, 10^k \equiv 0[5] \end{cases}$
$5|N \iff a_0 \equiv 0[5]$
$\iff a_0 \in \{0,5\}$

Divisibilité par 11 :
$10^0 \equiv -1[11]$
Donc $\forall k \in \mathbb{N}, 10^k \equiv (-1)^k[11]$
$N \equiv 0[11] \iff \sum_{k=0}^{n} (-1)^k a_k \equiv 0[11]$
$\iff a_0 - a_1 + a_2 ... + (-1)^n a_n \equiv 0[11]$

Remarque (Réécriture en Classes dEquivalence) :
On peut réecrire le calcul précédent dans $\mathbb{Z}/11\mathbb{Z}$
$\overline{N} = \overline{\sum_{k=0}^{n} 10^k a_k} = \sum_{k=0}^{n} \overline{10^k}\ \overline{a_k} = \sum_{k=0}^{n} \overline{(-1)^k}\ \overline{a_k}$

Remarque (Opération dans $\mathbb{Z}/n\mathbb{Z}$) :
Dans $\mathbb{Z}/n\mathbb{Z}$, on dispose $\begin{cases} \text{dune addition :} & \overline{a} + \overline{b} = \overline{a+b} \\ \text{d'une multiplication :} & \overline{a} \star \overline{b} = \overline{a \star b} \end{cases}$

Laddition est commutative, associative, nélément neutre $\overline{0}$ et lopposé de $\overline{a}$ est $\overline{-a}$
La multiplication est commutative, associative, délément neutre $\overline{1}$ et distributive par rapport à $+$

10 PCGD et PPCM

Définition (PGCD) **:** Soient $(a,b) \in \mathbb{Z}^2$
Le PGCD de a et b est le plus grand diviseur commun à a et b
Il existe car $\mathcal{D} = \{d \in \mathbb{N} | d|a \text{ et } d|b\}$ est non vide car $a \in \mathcal{D}$
$\mathcal{D}$ est majoré par $|a|$
On le note PGCD(a,b) ou $a \wedge b$

Proposition (Théorème dEuclide) **:** Soient $a \in \mathbb{Z}, b \in \mathbb{N}^\star$
Soit r le reste de la division de a par b
$a \wedge b = b \wedge r$

Preuve :

On pose $\begin{cases} d = a \wedge b \\ \varsigma = b \wedge r \\ a = bq + r \end{cases}$

$$\begin{cases} d|a \\ d|b \end{cases} \Longrightarrow \begin{cases} d|a - bq \\ d|b \end{cases} \Longrightarrow \begin{cases} d|r \\ d|b \end{cases} \Longrightarrow d \leq \varsigma$$

$$\begin{cases} \varsigma|b \\ \varsigma|r \end{cases} \Longrightarrow \begin{cases} \varsigma|bq + r \\ \varsigma|b \end{cases} \Longrightarrow \begin{cases} \varsigma|a \\ \varsigma|b \end{cases} \Longrightarrow \varsigma \leq d$$

Donc $d = \varsigma$

□

Proposition (PGCD et Diviseurs) **:** Soient $(a, b) \in \mathbb{Z}^2$ et $d = a \wedge b$
$\mathcal{D} = \{k \in \mathbb{Z} |\ k|a, k|b\}$
$\forall k \in \mathbb{Z}, k \in \mathcal{D} \iff k|d$

Preuve :
$\Longleftarrow$: Soit $k \in \mathbb{Z}$, on suppose $k|d$
$d|a$ donc $k|a$
$d|b$ donc $k|b$

Donc $k \in \mathcal{D}$

$\Longrightarrow$: Soit $k \in \mathcal{D}$
On pose r_0 le reste de la division de a par b,
r_1 le reste de la division de b par r_0
et $\forall n \in \mathbb{N}, r_{n+1}$ le reste de la division de r_{n-1} par r_n si $r_n \neq 0$

La suite (r_n) est décroissante, minorée par 0 et à valeurs entières
Soit $N \in \mathbb{N}$ tel que $r_N = 0$ (si $N = 0$, on pose $r_{-1} = b$)

Daprès la poposition précédente,
$d = a \wedge b = b \wedge r_0 = r_0 \wedge r_1 ... r_{N-1} \wedge r_N$
$= r_{N-1} \wedge 0 = r_N$

On pose aussi $\forall n \in [\![1, N-1]\!], r_{n-1} = r_n q_n + r_{n+1}$

On en déduit que $\exists(\alpha_n, \beta_n) \in \mathbb{Z}^2, r_{N-1} = a\alpha_N + b\beta_N$
$\begin{cases} k|a \\ k|b \end{cases} \implies k|a\alpha_N + b\beta_N \implies k|r_{N-1} \implies k|d$

□

Définition (PPCM) **:** Soit $(a,b) \in \mathbb{Z}^2$, on pose $M = \{k \in \mathbb{N} |\ a|k, b|k\}$
$M \neq \varnothing$ car $ab \in M$
$M \neq \varnothing$ donc admet un plus petit élément noté PPCM(a,b) ou $a \vee b$

Proposition (Produit PGCD PPCM) **:** $\forall (a,b) \in \mathbb{Z}^2, (a \wedge b)(a \vee b) = ab$

Preuve :
Voir paragraphe Facteurs Premiers

□

Proposition (Propriétés de $\wedge$ et $\vee$) **:** $\wedge$ est commutative, associative sur $\mathbb{Z}^\star$
$\vee$ est commutative, associative sur $\mathbb{Z}^\star$

Preuve :
Soient $(a,b,c) \in (\mathbb{Z}^\star)^3, d = (a \wedge b) \wedge c, \varsigma = a \wedge (b \wedge c)$

$$\begin{cases} d|c \\ d|a \wedge b \end{cases} \implies \begin{cases} d|c \\ d|a \\ d|b \end{cases}$$

$$\begin{cases} \varsigma|a \\ \varsigma|b \wedge c \end{cases} \implies \begin{cases} \varsigma|a \\ \varsigma|b \\ \varsigma|c \end{cases}$$

On pose $\varepsilon = \text{PGCD}(a,b,c)$
On a $\begin{cases} d \leq \varepsilon \\ \varsigma \leq \varepsilon \end{cases}$

$$\left\{\begin{array}{l}\varepsilon|a\\ \varepsilon|b\\ \varepsilon|c\end{array}\right. \Longrightarrow \left\{\begin{array}{l}\varepsilon|a\\ \\ \varepsilon|b\wedge c\end{array}\right. \Longrightarrow \varepsilon|a\wedge(b\wedge c)\Longrightarrow \varepsilon\leq d$$

De même, on $\varepsilon\leq\varsigma$
Donc $d=\varepsilon=\varsigma$

□

Proposition (Théorème de Bézout) **:** Soient $(a,b)\in\mathbb{Z}\times\mathbb{Z}^\star, d=a\wedge b$
$\exists(u,v)\in\mathbb{Z}^2, d=au+bv$

Preuve :
On pose $A=\{au+bv|(u,v)\in\mathbb{Z}^2\}$
On veut montrer que $d\in A$
$a=a\star1+b\star0$ donc $a\in A$
$b=a\star0+b\star1$ donc $b\in A$
$0=a\star0+b\star0$ donc $0\in A$

Soit $(x,y)\in A^2$
$x=au_1+bv_1,(u_1,v_1)\in\mathbb{Z}^2$
$y=au_2+bv_2,(u_2,v_2)\in\mathbb{Z}^2$
$x+y=a(u_1+u_2)+b(v_1+v_2)\in A$

Soit $x\in A, k\in\mathbb{Z}$
$x=au+bv,(u,v)\in\mathbb{Z}^2$
$kx=aku+bkv\in A$

Soit $n=\min(A\cap\mathbb{N}^\star)$ $(|b|\in A\cap\mathbb{N}^\star)$
Soit $x\in A$

Par division euclidienne de x par n :
$\left\{\begin{array}{l}x=nq+r\\ q\in A, 0\leq r<n\end{array}\right.$

$$\left\{\begin{array}{l}x\in A\\ n\in A\end{array}\right. \Longrightarrow \left\{\begin{array}{l}x\in A\\ -qn\in A\end{array}\right. \Longrightarrow x-qn\in A\Longrightarrow r\in A$$

$$\left\{\begin{array}{l}r<n\\ r\in A\end{array}\right. \Longrightarrow r\leq 0$$

Donc $r=0$
Donc $n|x$

Doù $A = n\mathbb{Z}$
Or, $\begin{cases} a \in A \\ b \in A \end{cases} \Longrightarrow \begin{cases} n|a \\ n|b \end{cases}$

Cas particulier : $a \wedge b = d = 1$, alors 1 est le seul diviseur positif de a et b
Donc $n = 1$ donc $A = \mathbb{Z}$ donc $1 \in \mathbb{Z}$

Cas général : On pose $a' = \dfrac{a}{d} \in \mathbb{Z},\ b' = \dfrac{b}{d} \in \mathbb{Z},\ a' \wedge b' = 1$
Daprès le cas particulier, $\exists (u, v) \in \mathbb{Z}^2, a'u + b'v = 1$

Doù $au + bv = d$

□

Proposition (Réciproque du Théorème de Bézout) **:** Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$
On suppose quil existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$
Alors $a \wedge b = 1$

Preuve :
On pose $d = a \wedge b$
$\begin{cases} d|a \\ d|b \end{cases} \Longrightarrow d|au + bv \Longrightarrow d|1 \Longrightarrow d = 1$

□

Proposition (Théorème de Gauß) **:** Soient $(a, b, c) \in \mathbb{Z}^3$ tels que $\begin{cases} a \wedge b = 1 \\ a|bc \end{cases}$
Alors $a|c$

Preuve :
Daprès le théorème de Bézout,
$au + bv = 1$ avec $(u, v) \in \mathbb{Z}^2$
Doù $acu + bcv = c$

$\begin{cases} a|acu \\ a|bcv \end{cases}$
Donc $a|acu + bcv$
Donc $a|c$

□

REMARQUE (Inversion Modulo n) :
Soit $x \in \mathbb{Z}$
$\exists ? y \in \mathbb{Z}, xy \equiv 1[n]$
($\iff$ dans $\mathbb{Z}/n\mathbb{Z}, \overline{x} + \overline{y} = \overline{1}$?)

Avec $n = 4$:

x	0123
0	0000
1	0123
2	0202
3	0321

$\begin{cases} 1 \text{ et } 3 \text{ sont inversibles modulo } 4 \\ 2 \text{ n'est pas inversible modulo } 4 \end{cases}$

$3x \equiv 2[4]$
$\iff 3 \star 3x \equiv 3 \star 2[4]$
$\iff x \equiv 2[4]$

$2x \equiv 1[4]$
$\implies 2 \star 2x \equiv 2[4]$
$\implies 0 \equiv 2[4]$

Proposition (Congruences et Nombres Premiers) **:** Soit p un nombre premier
Alors $\forall x \in \mathbb{Z}, x \not\equiv 0[p] \implies \exists y \in \mathbb{Z}, xy \equiv 1[p]$

Preuve :
Soit $x \in \mathbb{Z}$ tel que $x \not\equiv 0[p]$
Soit $y \in \mathbb{Z}$
$xy \equiv 1[p] \iff \exists u \in \mathbb{Z}, xy = 1 + pu$
$\iff \exists u \in \mathbb{Z}, xy - pu = 1$

y existe $\iff x \wedge p = 1$
$\iff p \nmid x$

□

Proposition (Inversibilité Modulo n) **:** Soit $n \in \mathbb{N}^\star, x \in \mathbb{Z}$
x inversible modulo $n \iff x \wedge n = 1$

Preuve :
Voir précédent

□

Proposition (Petit Théorème de Fermat) **:** Soit p premier, $a \in \mathbb{Z}$
$a^p \equiv a[p]$

Preuve :
Cas 1 : $a \equiv 0[p]$
$a^p \equiv 0^p[p]$
$a^p \equiv 0[p] \equiv a[p]$

Cas 2 : $a \not\equiv 0[p]$
Alors $a \wedge p = 1$

On pose $\forall i \in \mathbb{N}^\star, r_i$ le reste de la division de ia par p
Soit $i \in [\![1, p-1]\!]$
$r_i = 0 \Longrightarrow p|ia \Longrightarrow p|i$ Contradiction
$\forall i \in \mathbb{N}^\star, r_i \neq 0$

Soit $(i, j) \in [\![1, p-1]\!]^2, i \neq j$
On suppose $r_i = r_j$, alors $ia \equiv ja[p]$
Or, $a \wedge p = 1$ donc a est inversible modulo p
Donc $a \equiv j[p]$ donc $i = j$ Contradiction

Ainsi, $r_1 ... r_{p-1} \in [\![1, p-1]\!]$ distincts donc ils prennent toutes les valeurs de $[\![1, p-1]\!]$
$i \longmapsto r_i$ est injective
$\{r_1 ... r_{p-1}\} = [\![1, p-1]\!]$

Donc $\prod_{k=1}^{p-1} r_i = (p-1)!$

Donc $\prod_{k=1}^{p-1} ia \equiv (p-1)![p]$
Donc $(p-1)!a^{p-1} \equiv (p-1)![p]$

Doù $(p-1)! \equiv 0[p] \iff p|1\star 2\star 3\cdots\star(p-1)$
$\iff \exists i \in [\![1, p-1]\!], p|i$
Donc $(p-1)! \not\equiv 0[p]$
Donc $(p-1)!$ est inversible modulo p
Donc $a^p \equiv 1[p]$
Donc $a^p \equiv a[p]$

□

11 Décomposition en Facteurs Premiers

Définition (Nombre Premier) **:** Soit $n \in \mathbb{N}$
On dit que n est premier si
$n \geqslant 2$
les seuls diviseurs entiers de n sont 1 et n

Proposition (Infinité de Nombres Premiers) **:** Il y a une infinité de nombres premiers

Preuve :
On suppose quil ny a quun nombre fini de nombres premiers
$p_1 < ... < p_n$

On pose $N = p_n\star...\star p_1 + 1$
$N > p_n$ donc N nest pas premier
N a dautres diviseurs positifs que 1 et N
N est divisible par un nombre entre 2 et $N-1$

Soit $p = \min(\{k \in [\![2, N-1]\!] | k|N\})$
p est premier (Tout diviseur de p divise aussi N)
$\exists i \in [\![1, n]\!], p_i = p$
$p_i|N$
$p_i|N - p_1...p_n$
$p_i|1$ Contradiction

Donc il y a une infinité de nombres premiers

□

Proposition (Théorème Fondamental de lArithmétique) **:** Tout entier se décompose en un unique produit de nombres premiers

Soient $n \in \mathbb{N}$ tel que $n \geqslant 2$ et $\mathcal{P}$ lensemble des nombres premiers
$\exists! \nu : \mathcal{P} \longrightarrow \mathbb{N}$ telle que $\begin{cases} \{p \in \mathcal{P} | \nu(p) \neq 0\} \text{ est fini} \\ n = \prod_{p \in \mathcal{P}} p^{\nu(p)} \end{cases}$

Preuve :
Existence : Déjà vue : Récurrence Forte (Chapitre 9)

Unicité : Soit $n \geqslant 2$ et $\nu : \mathcal{P} \longrightarrow \mathbb{N}$ telle que
$(\star) \prod_{p \in \mathcal{P}} p^{\mu(p)} = \prod_{p \in \mathcal{P}} p^{\nu(p)}$ avec $\begin{cases} \mu \neq \nu \\ M = \{p \in \mathcal{P} | \mu(p) \neq 0\} \text{ fini} \\ M = \{p \in \mathcal{P} | \nu(p) \neq 0\} \text{ fini} \\ n \text{ minimale pour cette propriété} \end{cases}$

Soit $p \in M, \mu(p) \neq 0$ donc $p|n$
Si $\nu(p) = 0, \forall q \in \mathbb{N}, p \wedge q = 1$ donc $p|1$ Contradiction avec le théorème de Gauß

Donc on peut simplifier $(\star)$ par p
On a alors 2 décompositions de $\dfrac{n}{p} < n$ Contradiction
Donc n nexiste pas

□

Proposition (Divisibilité et Nombres Premiers) **:** Soient $(, b, c) \in \mathbb{N}^3$ supérieurs à 2
On pose $a = \prod_{p \in \mathcal{P}} p^{\alpha(p)}$ et $b = \prod_{p \in \mathcal{P}} p^{\beta(p)}$
$a|b \iff \forall p \in \mathcal{P}, \alpha(p) \leq \beta(p)$

Preuve :

$\Longrightarrow$: On suppose $a|b, \exists k, b = ak$
On pose $k = \prod_{p\in\mathcal{P}} p^{\kappa(p)}$
et donc $b = \prod_{p\in\mathcal{P}} p^{\alpha(p)} \prod_{p\in\mathcal{P}} p^{\kappa(p)} = \prod_{p\in\mathcal{P}} p^{\alpha(p)+\kappa(p)}$

Par unicité de la décomposition en facteurs premiers,
$\forall p \in \mathcal{P}, \beta(p) = \alpha(p) + \kappa(p) \geqslant \alpha(p)$

$\Longleftarrow$: On suppose $\forall p \in \mathcal{P}, \beta(p) \geqslant \alpha(p)$
On pose $\forall p \in \mathcal{P}, \kappa(p) = \beta(p) - \alpha(p) \in \mathbb{N}$

Tous les $\alpha(p)$ et $\beta(p)$ sont nuls à partir dun certain rang
C'est donc le cas aussi pour les $\kappa(p)$
Donc on a le droit de former le produit
$\prod_{p\in\mathcal{P}} p^{\kappa(p)} \in \mathbb{N}$

On pose $k = \prod_{p\in\mathcal{P}} p^{\kappa(p)}$ et $ak = \prod_{p\in\mathcal{P}} p^{\alpha(p)} \prod_{p\in\mathcal{P}} p^{\kappa(p)} = \prod_{p\in\mathcal{P}} p^{\alpha(p)+\kappa(p)} = \prod_{p\in\mathcal{P}} p^{\beta(p)} = b$

□

Proposition (Produit de Facteurs Premiers, PGCD et PPCM) **:** Avec les notations précédentes,

$$a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(\alpha(p),\beta(p))} \text{ et } a \vee b = \prod_{p\in\mathcal{P}} p^{\max(\alpha(p),\beta(p))}$$

Corollaire : $(a \wedge b)(a \vee b) = ab$

Preuve :
$(a \wedge b)(a \vee b) = \prod_{p\in\mathcal{P}} p^{\min(\alpha(p),\beta(p))} \prod_{p\in\mathcal{P}} p^{\max(\alpha(p),\beta(p))}$
$= \prod_{p\in\mathcal{P}} p^{\min(\alpha(p),\beta(p))+\max(\alpha(p),\beta(p))}$
$= \prod_{p\in\mathcal{P}} p^{\alpha(p)+\beta(p)} = ab$

□

Chapitre 11

Suites numériques

1 Modes de définition

Définition : Une suite peut être définie

— Explicitement On dispose pour tout $n \in \mathbb{N}$ de l'expression de u_n en fonction de n.
ex $\forall n \in \mathbb{N}_\star, u_n = \dfrac{\ln(n)}{n} e^{-n}$

— Par récurrence On connait u_{n+1} en fonction de $u_0, u_1, \ldots, u_n$
ex $\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N}, u_{n+1} = \sin(u_n) \end{cases}$

— Implicitement $\forall n \in \mathbb{N}, u_n$ est le seul nombre vérifiant une certaine propriété
ex u_n est le seul réel vérifiant $x^5 + nx - 1 = 0$

2 Limites

Définition : Soit u une suite réelle et $\ell \in \mathbb{R}$. On dit que

— u converge vers ℓ
— u_n tends vers ℓ quand n tends vers $+\infty$
— ℓ est une limite de u

si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, \quad |u_n - \ell| \leqslant \varepsilon \quad (\ell - \varepsilon \leqslant u_n \leqslant \ell + \varepsilon)$$

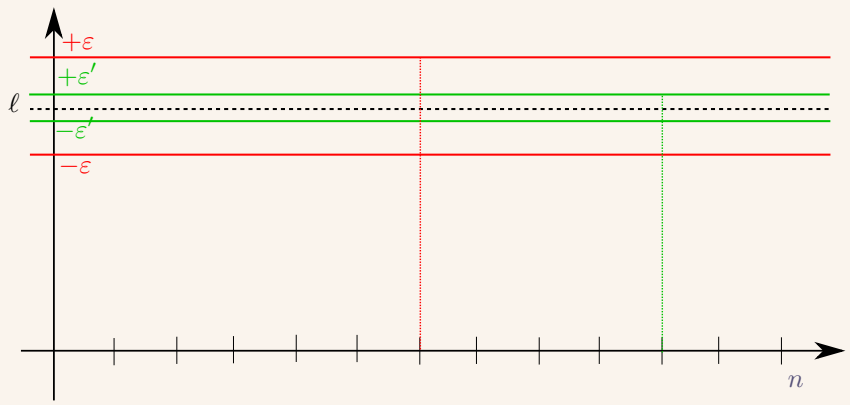


FIGURE 11.1 – Définition de la limite

EXEMPLE :
Montrer que $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ converge vers 0.
Soit $\varepsilon > 0$ quelconque. On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, -\varepsilon \leqslant \frac{1}{n} \leqslant \varepsilon$$

Analyse Soit $N \in \mathbb{N}^\star$ tel que $\forall n \geqslant N, -\varepsilon \leqslant \frac{1}{n} \leqslant \varepsilon$.
En particulier, $\frac{1}{N} \leqslant \varepsilon$ donc $N \geqslant \frac{1}{\varepsilon}$.

Synthèse On pose $N = \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1 \in \mathbb{N}^\star$ et $N > \frac{1}{\varepsilon}$. Soit $n \geqslant N$.

$$\frac{1}{n} > 0 > -\varepsilon \text{ donc } \frac{1}{n} \geqslant -\varepsilon$$

$$n \geqslant N > \frac{1}{\varepsilon} \text{ donc } n \geqslant \frac{1}{\varepsilon} \iff \frac{1}{n} \leqslant \varepsilon$$

Définition : Soit u une suite réelle.
On dit que u tends vers $+\infty$ si

$$\forall M \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geqslant N, u_n \geqslant M$$

On dit que u tends vers $-\infty$ si

$$\forall m \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geqslant N, u_n \leqslant m$$

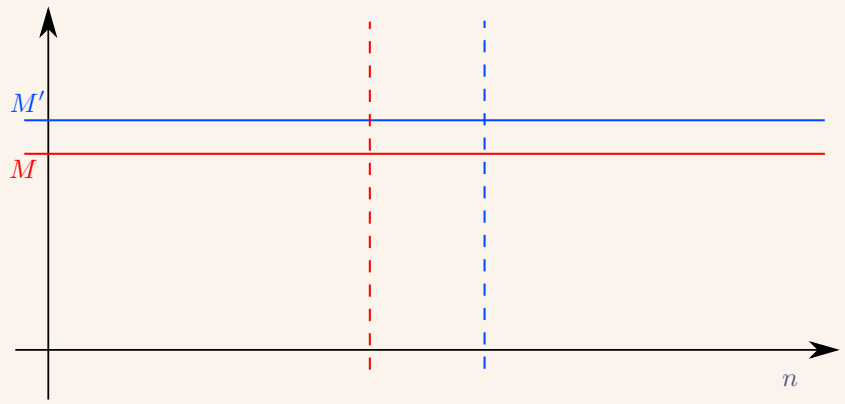


FIGURE 11.2 – Limites infinies

EXEMPLE :
Montrons que $n^2 \xrightarrow[n\to+\infty]{} +\infty$.
Soit $M \in \mathbb{R}$, on cherche $N \in \mathbb{N}$ tel que $\forall n \geqslant N, n^2 \geqslant M$.

Analyse Soit $N \in \mathbb{N}$ tel que $\forall n \geqslant N, n^2 \geqslant M$.
En particulier, $N^2 \geqslant M$ et dont $N \geqslant \sqrt{M}$ si $M \geqslant 0$

Synthèse On pose $N = \begin{cases} 0 & \text{si } M \leqslant 0 \\ \lfloor \sqrt{M} \rfloor + 1 & \text{sinon} \end{cases}$

Ainsi $N \in \mathbb{N}$ et $N^2 \geqslant M$. Soit $n \geqslant N$. On a $n^2 \geqslant N^2 \geqslant M$.

Définition : Une suite qui ne converge pas est dite divergente (on dit qu'elle diverge). C'est le cas si cette suite n'a pas de limite quand elle tends vers $\pm\infty$.

Théorème (Unicité de la limite (réelle)) **:** Soit $u \in \mathbb{R}^{\mathbb{N}}, (\ell_1, \ell_2) \in \overline{\mathbb{R}}^2$
Si $\begin{cases} u_n \xrightarrow[n\to+\infty]{} \ell_1 \\ u_n \xrightarrow[n\to+\infty]{} \ell_2 \end{cases}$ alors $\ell_1 = \ell_2$

*Preuve***Cas 1** $(\ell_1, \ell_2) \in \mathbb{R}^2$.
On suppose $\begin{cases} \ell_1 \neq \ell_2 \\ u_n \to l_1 \\ u_n \to l_2 \end{cases}$

Sans perte de généralité, on peut supposer $\ell_1 < \ell_2$

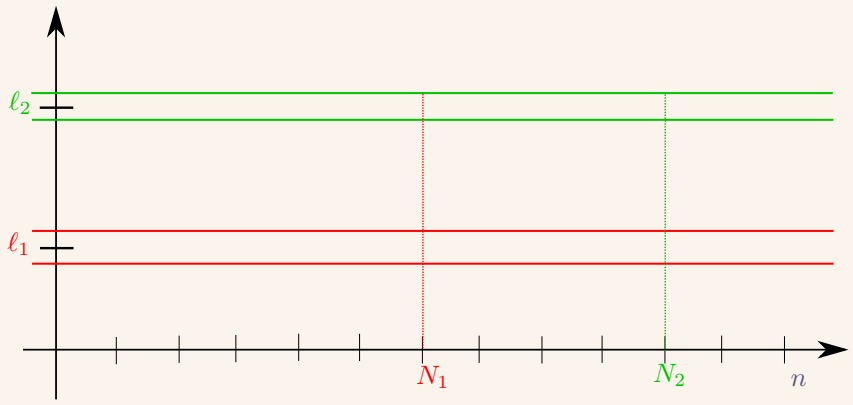


FIGURE 11.3 – Preuve unicité de la limite (cas 1)

On pose $\varepsilon = \dfrac{\ell_2 - \ell_1}{3} > 0$. On sait qu'il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, \ell_1 - \varepsilon \leqslant u_n \leqslant \ell_1 + \varepsilon$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, \ell_2 - \varepsilon \leqslant u_n \leqslant \ell_2 + \varepsilon$$

On pose $N = \max(N_1, N_2)$. On a alors

$$u_n \leqslant \ell_1 + \varepsilon < \ell_2 + \varepsilon \leqslant u_n$$

une contradiction ($u_n < u_n$). En effet,

$$\begin{aligned} \ell_1 + \varepsilon < \ell_2 + \varepsilon &\iff 2\varepsilon < \ell_2 - \ell_1 \\ &\iff \frac{2}{3}(\ell_2 - \ell_1) < \ell_2 - \ell_1 \\ &\iff \frac{2}{3} < 1 \end{aligned}$$

Ainsi $\ell_1 = \ell_2$

Cas 2 $\ell_1 \in \mathbb{R}, \ell_2 = +\infty$

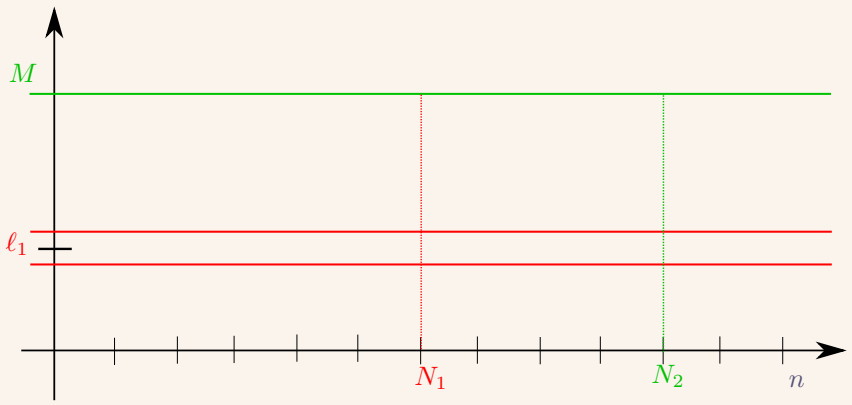


FIGURE 11.4 – Preuve unicité de la limite (cas 2)

$u_n \to \ell_1$ donc il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, \ell_1 - 1 \leqslant u_n \leqslant \ell_1 + 1$$

$u_n \to +\infty$ donc il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, u_n \geqslant \ell_1 + 2$$

On pose $N = \max(N_1, N_2)$. Ainsi

$$u_n \geqslant \ell_1 + 2 > \ell_1 + 1 \geqslant u_n$$

une contradiction

De la même manière, on peut prouver pour $(\mathbb{R}, -\infty)$ et $(+\infty, -\infty)$

□

REMARQUE :
Si u_n tends vers ℓ quand n tends vers $+\infty$, on écrit $u_n \xrightarrow[n\to+\infty]{} \ell$ ou $\lim\limits_{n\to+\infty} u_n = \ell$ ou $\lim u_n = \ell$

Proposition : Toute suite convergente est bornée

Preuve :
On pose $\ell = \lim u_n \in \mathbb{R}$. Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \ell - 1 \leqslant u_n \leqslant \ell + 1$$

L'ensemble $\{u_n \mid n \leqslant N\}$ est fini, il a donc un plus grand élément et un plus petit élément. On pose

$$\begin{cases} M_1 = \max\{u_n \mid n \leqslant N\} \\ m_1 = \min\{u_n \mid n \leqslant N\} \end{cases}$$

et

$$\begin{cases} M = \max(\ell_1 + 1, M_1) \\ m = \min(\ell_1 - 1, m_1) \end{cases}$$

Ainsi,

$$\forall n \in \mathbb{N}, \begin{cases} m \leqslant m_1 \leqslant u_n \leqslant M_1 \leqslant M & \text{si } n \leqslant N \\ m \leqslant \ell_1 - 1 \leqslant u_n \leqslant \ell_1 + 1 \leqslant M & \text{si } n > N \end{cases}$$

Donc

$$\forall n \in \mathbb{N}, m \leqslant u_n \leqslant M$$

□

Proposition : Soient $u \in \mathbb{R}^{\mathbb{N}}$ et $v \in \mathbb{R}^{\mathbb{N}}$. On pose $\ell_1 = \lim u_n$ et $\ell_2 = \lim v_n$

1. si $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$ alors $u_n + v_n \to \ell_1 + \ell_2$
2. si $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$ alors $u_n + v_n \to +\infty$
3. si $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$ alors $u_n + v_n \to -\infty$
4. si $\ell_1 = \ell_2 = +\infty$, alors $u_n + v_n \to +\infty$
5. si $\ell_1 = \ell_2 = -\infty$, alors $u_n + v_n \to -\infty$

Preuve : 1. On suppose $(\ell_1, \ell_2) \in \mathbb{R}^2$, on pose $\ell = \ell_1 + \ell_2$.
Soit $\varepsilon > 0$ quelconque. On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \ell - \varepsilon \leqslant u_n + v_n \leqslant \ell + \varepsilon$$

$\frac{\varepsilon}{2} > 0$ donc il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, \ell_1 - \frac{\varepsilon}{2} \leqslant u_n \leqslant \ell_1 + \frac{\varepsilon}{2}$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, \ell_2 - \frac{\varepsilon}{2} \leqslant v_n \leqslant \ell_2 + \frac{\varepsilon}{2}$$

On pose $N = \max(N_1, N_2)$. Soit $n \geqslant N$ quelconque.

$$n \geqslant N \geqslant N_1 \text{ donc } \ell_1 - \frac{\varepsilon}{2} \leqslant u_n \leqslant \ell_1 + \frac{\varepsilon}{2}$$

$$n \geqslant N \geqslant N_2 \text{ donc } \ell_2 - \frac{\varepsilon}{2} \leqslant v_n \leqslant \ell_2 + \frac{\varepsilon}{2}$$

D'où, en additionnant les inégalités

$$\ell - \varepsilon = \ell_1 + \ell_2 - \varepsilon \leqslant u_n + v_n \leqslant \ell_1 + \ell_2 + \varepsilon = \ell + \varepsilon$$

2. On suppose $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$. Soit $M \in \mathbb{R}$ quelconque.
Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, \ell_1 - 1 \leqslant u_n \leqslant \ell_1 + 1$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, v_n \geqslant M - \ell_1 + 1$$

On pose $N = \max(N_1, N_2)$. Soit $n \geqslant N$ quelconque

$$\begin{cases} n \geqslant N_1 \text{ donc } u_n \geqslant \ell_1 - 1 \\ n \geqslant N_2 \text{ donc } v_n \geqslant M - \ell_1 + 1 \end{cases}$$

D'où, $u_n + v_n \geqslant M$

□

Proposition : Soient u et v deux suites réelles. On pose $\ell_1 = \lim u_n$ et $\ell_2 = \lim v_n$

1. si $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$, alors $u_n v_n \to \ell_1 \ell_2$
2. si $\begin{cases} \ell_1 \in \mathbb{R}_\star^+, \ell_2 = +\infty \text{ alors } u_n v_n \to +\infty \\ \ell_1 \in \mathbb{R}_\star^-, \ell_2 = +\infty \text{ alors } u_n v_n \to -\infty \end{cases}$
3. si $\begin{cases} \ell_1 \in \mathbb{R}_\star^+, \ell_2 = -\infty \text{ alors } u_n v_n \to -\infty \\ \ell_1 \in \mathbb{R}_\star^-, \ell_2 = -\infty \text{ alors } u_n v_n \to +\infty \end{cases}$
4. si $\begin{cases} \ell_1 = -\infty, \ell_2 = +\infty \text{ alors } u_n v_n \to -\infty \\ \ell_1 = -\infty, \ell_2 = -\infty \text{ alors } u_n v_n \to +\infty \\ \ell_1 = +\infty, \ell_2 = +\infty \text{ alors } u_n v_n \to +\infty \end{cases}$

Preuve : 1. $(\ell_1, \ell_2) \in \mathbb{R}^2$
Soit $\varepsilon > 0$ quelconque. On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, |u_n v_n - \ell_1 \ell_2| \leqslant \varepsilon$$

$$\begin{aligned} \forall n \in \mathbb{N}, |u_n v_n - \ell_1 \ell_2| &= |(u_n - \ell_1) v_n + \ell_1 (v_n - \ell_2)| \\ &\leqslant |v_n| \, |u_n - \ell_1| + |\ell_1| \, |v_n - \ell_2| \end{aligned}$$

Comme v_n converge, elle est bornée,

$$\exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |v_n| \leqslant M$$

donc

$$|u_n v_n - \ell_1 \ell_2| \leqslant M \times |u_n - \ell_1| + |\ell_1| \, |v_n - \ell_2|$$

Cas 1 On suppose $M \neq 0$ et $\ell_1 \neq 0$. Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, |u_n - \ell_1| \leqslant \frac{\varepsilon}{2M}$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, |v_n - \ell_2| \leqslant \frac{\varepsilon}{2\,|\ell_1|}$$

On pose $N = \max(N_1, N_2)$.

$$\forall n \geqslant N, |u_n v_n - \ell_1 \ell_2| \leqslant \frac{\varepsilon}{2M} \times M + |\ell_1| \times \frac{\varepsilon}{2\,|\ell_1|} = \varepsilon$$

Cas 2 $M = 0$, $(\ell_1 \neq 0)$
Alors, $\forall n \in \mathbb{N}, v_n = 0$
Donc

$$\begin{cases} \forall n \in \mathbb{N}, u_n v_n = 0 \\ \ell_2 = 0 \\ \ell_1 \ell_2 = 0 = \lim\limits_{n \to +\infty} u_n v_n \end{cases}$$

Cas 3 $M \neq 0$ et $\ell_1 = 0$
Alors, $\forall n \in \mathbb{N}, |u_n v_n - 0| \leqslant M \, |u_n|$
$\dfrac{\varepsilon}{M} > 0$ donc il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, |u_n| \leqslant \frac{\varepsilon}{M}$$

Donc,

$$\forall n \geqslant N, |u_n v_n| \leqslant M \times \frac{\varepsilon}{M} = \varepsilon$$

Donc, $u_n v_n \xrightarrow[n \to +\infty]{} 0 = \ell_1 \ell_2$

2. $l_1 > 0$ et $l_2 = +\infty$
Soit $M \in \mathbb{R}_\star^+$ On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, u_n v_n \geqslant M$$

On pose $\varepsilon = \dfrac{\ell_1}{2} > 0$. Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, u_n \geqslant \ell_1 - \varepsilon = \frac{\ell_1}{2} > 0$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, v_n \geqslant \frac{2M}{\ell_1} > 0$$

On pose $N = \max(N_1, N_2)$. Alors,

$$\forall n \geqslant N, u_n v_n \geqslant \frac{2M}{\ell_1} \times \frac{\ell_1}{2} = M$$

Donc $u_n v_n \xrightarrow[n\to+\infty]{} +\infty$

□

Proposition : Soit $(u_n)_{n\in\mathbb{N}}$ une suite de $\mathbb{R}_\star$.Donc, $\forall n \in \mathbb{N}, u_n \neq 0$
On pose $\ell = \lim u_n$ (si elle existe).

1. si $\ell = +\infty$ alors, $\dfrac{1}{u_n} \to 0$
2. si $\ell = 0$ alors, $\left|\dfrac{1}{u_n}\right| \to +\infty$

   B Si le signe de u_n ne se stabilise pas $\dfrac{1}{u_n}$ n'a pas de limite

   ex $u_n = \dfrac{(-1)^n}{n}$
3. si $\ell \in \mathbb{R}^\star$, alors $\dfrac{1}{u_n} \xrightarrow[n\to+\infty]{} \dfrac{1}{\ell}$

Preuve : 3.

$$\forall n \in \mathbb{N}, \left|\frac{1}{u_n} - \frac{1}{\ell}\right| = \frac{|\ell - u_n|}{|u_n|\,|\ell|}$$

On pose $\varepsilon = \dfrac{|\ell|}{2} > 0$. Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \ell - \varepsilon \leqslant u_n \leqslant \ell + \varepsilon$$

Si $\ell > 0$ alors

$$\forall n \geqslant N, u_n \geqslant \ell - \varepsilon = \frac{\ell}{2} > 0$$

et donc

$$\forall n \geqslant N, |u_n| \geqslant \frac{|\ell|}{2}$$

Si $\ell < 0$ alors

$$\forall n \in \mathbb{N}, u_n \leqslant \ell + \varepsilon = \frac{\ell}{2} < 0$$

et donc

$$\forall n \in \mathbb{N}, |u_n| \geqslant \frac{|\ell|}{2}$$

Donc,

$$\forall n \geqslant N, \left|\frac{1}{u_n} - \frac{1}{\ell}\right| \leqslant \frac{|u_n| - \ell}{|\ell| \times \frac{|\ell|}{2}} = \frac{2\,|u_n - \ell|}{|\ell|^2}$$

Soit $\varepsilon' > 0$ quelconque. $\dfrac{\varepsilon'\,|\ell|^2}{2}$ donc il existe $N' \in \mathbb{N}$ tel que

$$\forall n \geqslant N', |u_n - \ell| \leqslant \frac{\varepsilon'}{2}\,|\ell|^2$$

On pose N'', $\left|\dfrac{1}{u_n} - \dfrac{1}{\ell}\right| \leqslant \dfrac{\varepsilon'}{2}\,|\ell|^2 \times \dfrac{2}{|\ell|^2} = \varepsilon'$

□

3 Limites et inégalités

Proposition : Soient u et v deux suites réelles convergentes de limites respectives ℓ_1 et ℓ_2. On suppose que

$$\forall n \in \mathbb{N}, u_n \leqslant v_n$$

Alors, $\ell_1 \leqslant \ell_2$

Preuve :
On suppose $\ell_1 < \ell_2$. On pose $\varepsilon = \dfrac{\ell_1 - \ell_2}{3} > 0$.
Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, u_n \geqslant \ell_1 - \varepsilon$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, v_n \leqslant \ell_2 + \varepsilon$$

Ainsi,

$$\forall n \geqslant \max(N_1, N_2), \ell_1 - \varepsilon \leqslant u_n \leqslant v_n \leqslant \ell_2 + \varepsilon$$

et donc

$$\ell_1 - \varepsilon \leqslant \ell_2 + \varepsilon$$

donc, $\ell_1 - \ell_2 \leqslant 2\varepsilon$
donc, $1 \leqslant \dfrac{2}{3}$ une contradiction □

REMARQUE :
Si $\begin{cases} u_n \to \ell_1 \in \mathbb{R} \\ v_n \to \ell_2 \in \mathbb{R} \\ \forall n \in \mathbb{N}, u_n < v_n \end{cases}$
on n'a pas forcément $\ell_1 < \ell_2$
ex $\forall n \in \mathbb{N}_\star, \dfrac{1}{n+1} < \dfrac{1}{n}$ mais les deux convergent vers 0

Proposition : Soient u et v deux suites réelles telles que

$$\forall n \in \mathbb{N}, u_n < v_n$$

1. si $u_n \to +\infty$,$v_n \to +\infty$
2. si $v_n \to -\infty$,$u_n \to -\infty$

Preuve : 1. On suppose $u_n \to +\infty$. Soit $M \in \mathbb{R}$, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, u_n \geqslant M$$

Donc

$$\forall n \geqslant N, v_n \geqslant u_n \geqslant M$$

Donc $v_n \to +\infty$

□

Théorème (Théorème des "gendarmes") **:** Soient u, v et w trois suites réelles telles que

$$\forall n \in \mathbb{N}, u_n \leqslant v_n \leqslant w_n$$

On suppose que u et w convergent vers la même limite $\ell \in \mathbb{R}$. Alors, v converge vers ℓ

Preuve :
Soit $\varepsilon > 0$. Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, w_n \leqslant \ell + \varepsilon$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, u_n \leqslant \ell - \varepsilon$$

On pose $N = \max(N_1, N_2)$. D'où,

$$\forall n \geqslant N, \ell - \varepsilon \leqslant u_n \leqslant v_n \leqslant w_n \leqslant \ell + \varepsilon$$

Donc, $v_n \xrightarrow[n\to+\infty]{} \ell$ □

Théorème (Limite monotone) **:**

1. Soit u une suite croissante majorée par M.
   Alors, u converge et $\lim u_n \leqslant M$
2. Soit u une suite croissante non majorée.
   Alors, $u_n \xrightarrow[n\to+\infty]{} +\infty$
3. Soit u une suite décroissante minorée par m.
   Alors, u converge et $\lim u_n \geqslant m$
4. Soit u une suite décroissante non minorée.
   Alors, $u_n \xrightarrow[n\to+\infty]{} -\infty$

Preuve :

1. $\{u_n \mid n \in \mathbb{N}\} \neq$ (u_0 y est) majorée (par hypothèse) par M.
   On pose $\ell = \sup_{n\in\mathbb{N}}(u_n)$. Soit $\varepsilon > 0$ quelconque
   $\ell - \varepsilon < \ell$ donc, $\exists N \in \mathbb{N}, u_N > \ell - \varepsilon$
   u est croissante donc

$$\forall n \geqslant N, u_n \geqslant u_N > \ell - \varepsilon$$

   donc,

$$\forall n \geqslant N, \ell - \varepsilon \leqslant u_n \leqslant \ell \leqslant \ell + \varepsilon$$

   Donc, $u_n \to \ell$
2. Soit $M \in \mathbb{R}$. M n'est pas un majorant de l'ensemble $\{u_n \mid n \in \mathbb{N}\}$ donc

$$\exists N \in \mathbb{N}, u_N > M$$

   Comme u est croissante

$$\forall n \geqslant N, u_n \geqslant u_N \geqslant M$$

   donc

$$u_n \xrightarrow[n\to+\infty]{} +\infty$$

□

Exemple :

$$\begin{cases} u_0 = a \in]0,1[\\ \forall n \in \mathbb{N}, u_{n+1} = u_n(1-u_n) \end{cases}$$

(suite logistique)

$u_{n+1} = f(u_n)$ avec $f : x \mapsto x(1-x)$

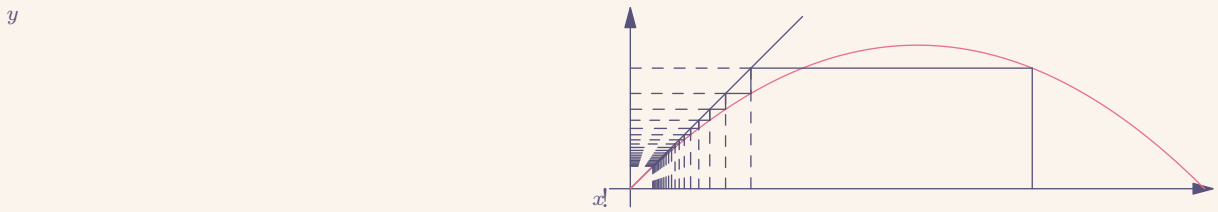


FIGURE 11.5 – Courbe logistique

— Soit $n \in \mathbb{N}$,

$$\begin{aligned} u_{n+1} - u_n &= u_n(1-u_n) - u_n \\ &= -{u_n}^2 \leqslant 0 \end{aligned}$$

Donc, u est décroissante.

— Montrons par récurrence que

$$\forall n \in \mathbb{N}, u_n \in [0,1]$$

— $u_0 = a \in]0,1[$ donc $u_0 \in [0,1]$

— Soit $n \in N$. On suppose $u_n \in [0,1]$

$$\begin{cases} 0 \leqslant u_n \leqslant 1 \\ 0 \leqslant 1 - u_n \leqslant 1 \end{cases}$$

donc

$$0 \leqslant u_{n+1} \leqslant 1$$

donc u minoré par 0

— D'après le théorème de la limite monotone, u converge. On pose ℓ sa limite :

$$\ell = \lim_{n \to +\infty} u_n$$

Alors, $u_{n+1} \xrightarrow[n \to +\infty]{} \ell$

$$u_n(1-u_n) \xrightarrow[n \to +\infty]{} \ell(1-\ell)$$

Par unicité de la limite,

$$\begin{aligned} &\ell = \ell(1-\ell) \\ \iff &1 = 1 - \ell \\ \iff &0 = -\ell \iff \ell = 0 \end{aligned}$$

EXEMPLE :

$$\begin{cases} u_0 = a \in]0,1[\\ u_{n+1} = 2u_n(1-u_n) \end{cases}$$

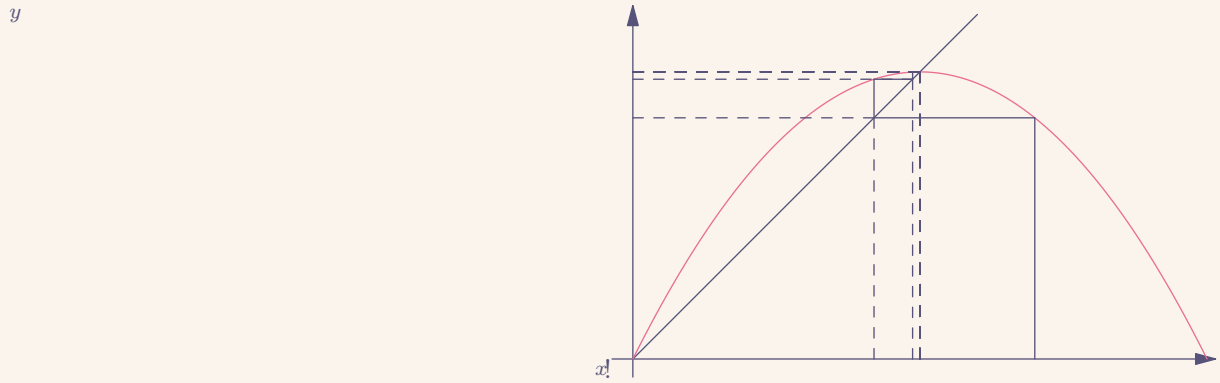


FIGURE 11.6 – Courbe logistique (2)

EXEMPLE :

$$\begin{cases} u_0 = a \in]0,1[\\ u_{n+1} = 3u_n(1-u_n) \end{cases}$$

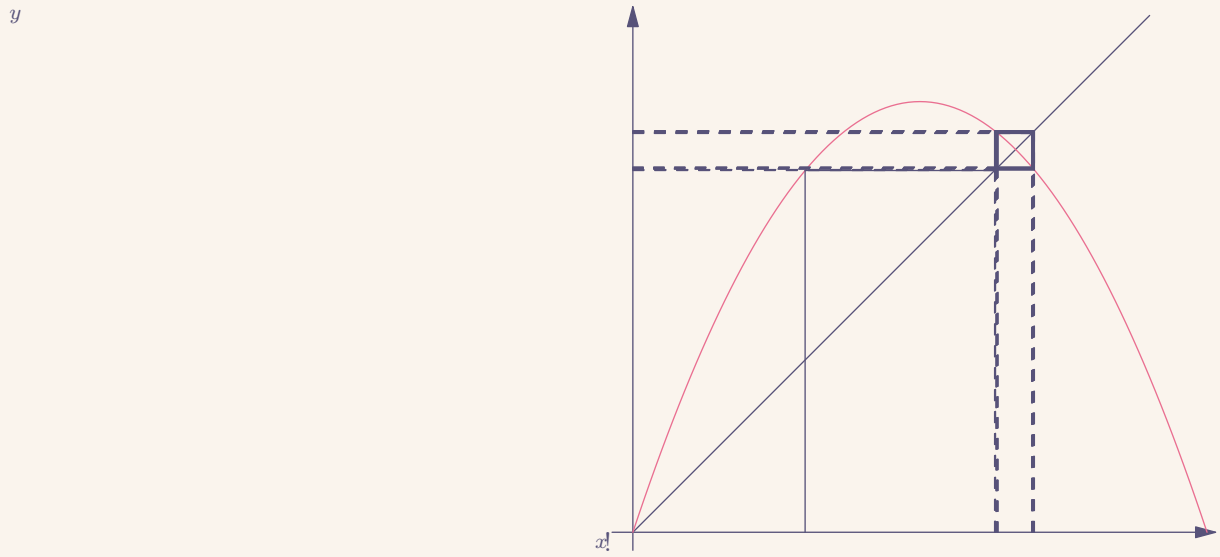


FIGURE 11.7 – Courbe logistique (3)

EXEMPLE :

$$\begin{cases} u_0 = a \in]0,1[\\ u_{n+1} = 4u_n(1-u_n) \end{cases}$$

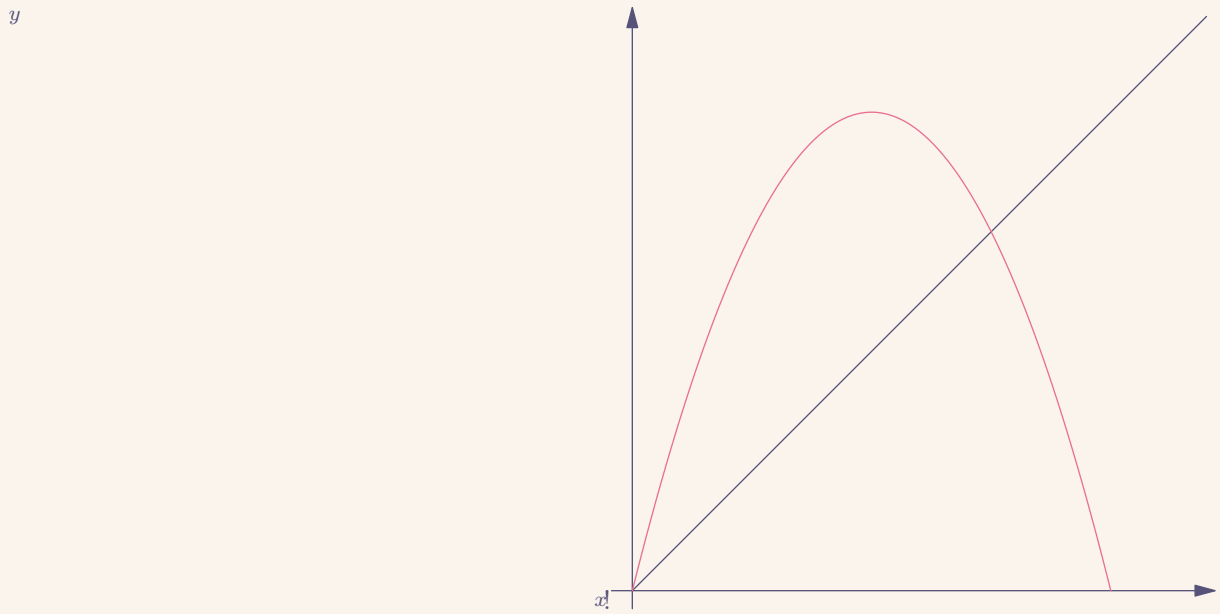


FIGURE 11.8 – Courbe logistique (4)

Définition : Soient u et v deux suites réelles. On dit que u et v sont adjacentes si

- u est croissante
- v est décroissante
- $u_n - v_n \xrightarrow[n\to+\infty]{} 0$

Théorème : Soient u et v deux suites adjacentes. Alors, u et v convergent vers la même limite.

Preuve :
$u - v$ est croissante donc,

$$\forall n \in \mathbb{N}, u_n - v_n \leqslant 0$$

v décroissante donc

$$\forall n \in \mathbb{N}, v_n \leqslant v_0$$

donc u majorée par v_0 donc u converge.
u est croissante donc,

$$\forall n \in \mathbb{N}, u_n \geqslant u_0$$

donc v est minorée par u_0 donc v converge.

Donc, $u_n - v_n \to \lim(u_n) - \lim(v_n)$ Par unicité de la limite,

$$\begin{aligned} & \lim(u_n) - \lim(v_n) = 0 \\ \iff & \lim(u_n) = \lim(v_n) \end{aligned}$$

□

Théorème (Théorème des segments emboîtés) **:** Soit (I_n) une suite de segments (non vide) décroissante

$$\forall n \in \mathbb{N}, I_{n+1} \subset I_n$$

On note $\ell(I)$ la longueur d'un intervalle I.
Si $\ell(I_n) \xrightarrow[n\to+\infty]{} 0$ alors $\bigcap_{n\in\mathbb{N}} I_n$ est un singleton.

Preuve :
On pose $\forall n \in \mathbb{N}, I_n = [a_n, b_n]$ avec $\forall n \in \mathbb{N}, a_n \leqslant b_n$. Soit $n \in \mathbb{N}$.
$I_{n+1} \subset I_n$ donc $a_{n+1} \in I_{n+1} \subset I_n$
donc $a_{n+1} \geqslant a_n$. De même, $b_{n+1} \in I_{n+1}$ donc $b_{n+1} \in I_n$ donc $b_{n+1} \leqslant b_n$.

$$\forall n \in \mathbb{N}, b_n - a_n = \ell(I_n) \xrightarrow[n\to+\infty]{} 0$$

donc (a_n) et (b_n) sont adjacentes, elles convergent donc vers la même limite $\ell \in \mathbb{R}$.
(a_n) croissante de limite ℓ donc

$$\forall n \in \mathbb{N}, a_n \leqslant \ell$$

(b_n) est décroissante de limite ℓ donc

$$\forall n \in \mathbb{N}, b_n \geqslant \ell$$

Donc, $\forall n \in \mathbb{N}, \ell \in I_n$ donc $\ell \in \bigcap_{n\in\mathbb{N}} I_n$.
Soit $\ell' \neq \ell$.

— Si $\ell' < \ell = \sup_{n\in\mathbb{N}}(a_n)$ donc ℓ' ne majore pas (a_n)

$$\exists N \in \mathbb{N}, a_N > \ell'$$

donc $\ell' \notin I_N$ donc $\ell' \notin \bigcap_{n\in\mathbb{N}} I_n$

— Si $\ell' > \ell = \inf_{n\in\mathbb{N}}(b_n)$ donc ℓ' ne minore pas (b_n)

$$\exists N' \in \mathbb{N}, b_{N'} < \ell'$$

et donc $\ell' \notin I_{N'}$ donc $\ell' \notin \bigcap_{n\in\mathbb{N}} I_n$

□

4 Suites extraites

Définition : Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante.
On dit que $\left(u_{\varphi(n)}\right)$ est une **suite extraite** de u ou une **sous suite** de u.
On dit alors que φ est une extractrice.

Exemple :
u_0 $\boxed{u_1}$ u_2 u_3 $\boxed{u_4}$ $\boxed{u_5}$ u_6 u_7 ...

$$\begin{cases} \varphi(0) = 1 \\ \varphi(1) = 4 \\ \varphi(2) = 5 \end{cases}$$

Lemme : Soit $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante. Alors,

$$\forall n \in \mathbb{N}, \varphi(n) \geqslant n$$

Preuve (par récurrence) *:* — $\varphi(0) \in \mathbb{N}$ donc $\varphi(0) \geqslant 0$
— Soit $n \in \mathbb{N}$. On suppose $(\varphi(n) \geqslant n$.
$n + 1 > n$ donc $\varphi(n + 1) > \varphi(n) \geqslant n$ donc $\varphi(n + 1) > n$
Comme $\varphi(n + 1) \in \mathbb{N}$, $\varphi(n + 1) \geqslant n + 1$

□

Proposition : Soit $u \in \mathbb{R}^{\mathbb{N}}$ de limite $\ell \in \overline{\mathbb{R}}$ et $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante
alors $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$.

Preuve Cas 1 $\ell \in \mathbb{R}$

Soit $\varepsilon > 0$ on sait qu'il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, |u_n - \ell| \leqslant \varepsilon$$

Soit $n \geqslant N$ alors $\varphi(n) \geqslant n \geqslant N$ donc

$$\left|u_{\varphi(n)} - \ell\right| \leqslant \varepsilon$$

Donc, $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$

Cas 2 $\ell = +\infty$

Soit $M \in \mathbb{R}$ et soit $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, u_n \geqslant M$$

Soit $n \geqslant N$, on a $\varphi(n) \geqslant n \geqslant N$ donc

$$u_{\varphi(n)} \geqslant M$$

Donc $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} +\infty$

Cas 3 $\ell = -\infty$ similaire au Cas 2

□

Exemple :
$\forall n \in \mathbb{N}, u_n = (-1)^n$

$$u_{2n} = 1 \xrightarrow[n\to+\infty]{} 1$$

$$u_{2n+1} = -1 \xrightarrow[n\to+\infty]{} -1$$

donc u_n n'a pas de limite.

Proposition : Si (u_{2n}) et (u_{2n+1}) ont la même limite ℓ alors $u_n \xrightarrow[n\to+\infty]{} \ell$

*Preuve*Cas 1 $\ell \in \mathbb{R}$

Soit $\varepsilon > 0$. Soit $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, |u_{2n} - \ell| \leqslant \varepsilon$$

Soit $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, |u_{2n+1} - \ell| \leqslant \varepsilon$$

On pose $N = \max(2N_1, 2N_2 + 1)$. Soit $n \geqslant N$.
Si n pair alors $n = 2k$ avec $k \geqslant N_1$ et donc, $|u_{2k} - \ell| \leqslant \varepsilon$, i.e.

$|u_n - \ell| \leqslant \varepsilon$
Si n impair alors $n = 2k+1$ avec $k \geqslant N_2$ et donc, $|u_{2k+1} - \ell| \leqslant \varepsilon$, i.e. $|u_n - \ell| \leqslant \varepsilon$
Donc,

$$\forall n \geqslant N, |u_n - \ell| \leqslant \varepsilon$$

Donc $u_n \xrightarrow[n\to+\infty]{} \ell$

□

Théorème (Théorème de Bolzano-Weierstrass) **:** Soit (u_n) une suite réelle bornée. Alors, il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $\left(u_{\varphi(n)}\right)$ converge.

Méthode 1 par dichotomie
Soitent $m, M \in \mathbb{R}$ tel que

$$\forall n \in \mathbb{N}, m \leqslant u_n \leqslant M$$

On pose

$$A_1 = \left\{ n \in \mathbb{N} \mid m \leqslant u_n \leqslant \frac{m+M}{2} \right\}$$
$$A_2 = \left\{ n \in \mathbb{N} \mid \frac{m+M}{2} \leqslant u_n \leqslant M \right\}$$

Comme $A_1 \cup A_2 = \mathbb{N}$, A_1 et A_2 ne peuvent pas être finis tous les deux.
On pose

$$B_0 = \begin{cases} A_1 & \text{si } A_1 \text{ est infini} \\ A_2 & \text{sinon} \end{cases}$$

B_0 est infini donc non vide. On pose $\varphi(0) = \min(B_0)$
On pose aussi

$$m_0 = \begin{cases} m & \text{si } B_0 = A_1 \\ \dfrac{m+M}{2} & \text{si } B_0 = A_2 \end{cases}$$

et

$$M_0 = \begin{cases} \dfrac{m+M}{2} & \text{si } B_0 = A_1 \\ M & \text{si } B_0 = A_2 \end{cases}$$

Ainsi, $B_0 = \{n \in \mathbb{N} \mid m_0 \leqslant u_n \leqslant M_0\}$. On pose

$$B'_1 = \left\{n \in B_0 \mid n > \varphi(0) \text{ et } m_0 \leqslant u_n \leqslant \frac{M_0 + m_0}{2}\right\}$$
$$B'_2 = \left\{n \in B_0 \mid n > \varphi(0) \text{ et } \frac{m_0 + M_0}{2} \leqslant u_n \leqslant M_0\right\}$$

$$B'_1 \cup B'_2 = \{n \in B \mid n > \varphi(0)\} = B_0 \setminus \{\varphi(0)\}$$

$B_0 \setminus \{\varphi(0)\}$ est infini donc B'_1 ou B'_2 est infini. On pose

$$B_1 = \begin{cases} B'_1 & \text{si } B'_1 \text{ est infini} \\ B'_2 & \text{sinon} \end{cases}$$

B_1 est infini donc non vide et admet un plus petit élément :

$$\varphi(1) = \min(B_1)$$

$\varphi(1) \in B_1$ donc $\varphi(1) > \varphi(0)$
On pose

$$m_1 = \begin{cases} m_0 & \text{si } B_1 = B'_1 \\ \dfrac{m_0 + M_0}{2} & \text{si } B_1 = B'_2 \end{cases}$$
$$M_1 = \begin{cases} \dfrac{m_0 + M_0}{2} & \text{si } B_1 = B'_1 \\ M_0 & \text{si } B_1 = B'_2 \end{cases}$$

On construit une suite décroissante (B_n), deux suites de réels (m_n) et (M_n) et une suite d'entiers $(\varphi(n))$ telles que

$$\forall n \in \mathbb{N}, \begin{cases} B_{n+1} = \{k \in B_n \mid k > \varphi(n) \text{ et } m_{n+1} \leqslant u_k \leqslant M_{n+1}\} \\ \varphi(n+1) = \min(B_{n+1}) > \varphi(n) \\ M_{n+1} - m_{n+1} = \dfrac{1}{2}(M_n - m_n) \end{cases}$$

La suite (m_n) est croissante, (M_n) est décroissante et

$$\lim_{n\to+\infty} M_n - m_n = \lim_{n\to+\infty} \left(\frac{1}{2}\right)^n (M_0 - m_0) = 0$$

Donc, (m_n) et (M_n) sont adjacentes donc convergentes avec la même limite $\ell \in \mathbb{R}$

$$\forall n \in \mathbb{N}, m_n \leqslant u_{\varphi(n)} \leqslant M_n$$

Par encadrement, $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$ □

Méthode 2 On pose $A = \{n \in \mathbb{N} \mid \forall k > n, u_n > u_k\}$

Cas 1 On suppose A infini.
On pose $\varphi(0) = \min(A)$. Soit $n \in \mathbb{N}$. On suppose $\varphi(0), \varphi(1), \ldots, \varphi(n)$ soient déjà construits. On pose

$$\varphi(n+1) = \min(A \setminus \{\varphi(0), \varphi(1), \ldots, \varphi(n)\})$$

Soit $n \in \mathbb{N}_\star$

$$\varphi(n+1) \in A \setminus \{\varphi(0), \varphi(1), \ldots, \varphi(n)\}$$

donc

$$\varphi(n+1) \in A \setminus \{\varphi(0), \varphi(1), \ldots, \varphi(n-1)\}$$

donc

$$\varphi(n+1) \geqslant \varphi(n)$$

Or, par définition, $\varphi(n+1) \neq \varphi(n)$ donc $\varphi(n+1) > \varphi(n)$
On a aussi $\varphi(1) \in A$ donc $\varphi(1) \geqslant \varphi(0)$ Or, on sait que $\varphi(1) \neq \varphi(0)$. Donc, $\varphi(1) > \varphi(0)$ Soit $n \in \mathbb{N}$, $\varphi(n) \in A$ donc

$$\forall k > \varphi(n), u_k < u_{\varphi(n)}$$

or $\varphi(n+1) > \varphi(n)$ donc $u_{\varphi(n+1)} < u_{\varphi(n)}$.
La sous suite $\left(u_{\varphi(n)}\right)$ est décroissante et minorée (car u est minorée) donc elle converge

Cas 2 On suppose A fini. Soit $N = \max(A)$,

$$\forall n > N, n \notin A$$

Donc $\forall n > N, \exists k > n, u_n \leqslant u_k$.
Par exemple, en posant $\varphi(0) = N + 1$, on a

$$A_1 = \{k > N+1 \mid u_{N+1} \leqslant u_k\} \neq$$

On pose $\varphi(1) = \min(A_1)$ donc $\begin{cases} \varphi(1) > N+1 = \varphi(0) \\ u_{\varphi(0)} < u_{\varphi(1)} \end{cases}$
Avec $n = \varphi(1)$

$$\exists k > n, u_{\varphi(1)} \leqslant u_k$$

Donc, $A_2 = \{k \in \mathbb{N} \mid k > \varphi(1) \text{ et } u_{\varphi ğ 1)} \leqslant u_k\} \neq$
On pose $\varphi(2) = \min(A_2)$. On a alors $\varphi(2) > \varphi(1)$. Soit $n \in \mathbb{N}$, on suppose $\varphi(n)$ déjà construit avec $\varphi(n) > N$. On sait alors que

$$A_{n+1} = \{k \in \mathbb{N} \mid k > \varphi(n) \text{ et } u_{\varphi(n)} \leqslant u_k\} \neq$$

On pose $\varphi(n+1) = \min(A_{n+1})$. Donc,

$$\begin{cases} \varphi(n+1) > \varphi(n) > N \\ u_{\varphi(n)} \leqslant u_{\varphi(n+1)} \end{cases}$$

On vient de construire une sous suite croissante majorée (car u est majorée) donc convergente.

□

5 Suites récurrentes

Définition : On dit que u est une suite récurrente linéaire d'ordre 2 à coefficients constants s'il existe $(a, b) \in \mathbb{C}$ tels que

$$\forall n \in \mathbb{N}, u_{n+2} = au_{n+1} + bu_n$$

L'équation caractéristique associée est

$$(C) : z^2 = az + b \text{ avec } z \in \mathbb{C}$$

Proposition : Avec les notations précédentes,

1. Si (C) a 2 racines simples $r_1 \neq r_2$ alors
$$\exists (A, B) \in \mathbb{C}^2, \forall n \in \mathbb{N}, u_n = A{r_1}^n + B{r_2}^n$$
2. Si (C) a une racine double $r \in \mathbb{C}$ alors
$$\exists (A, B) \in \mathbb{C}^2, \forall n \in \mathbb{N}, u_n = (An + B)r^n$$

Preuve (Récurrence double) *:*

□

Proposition : avec les notations précédentes et avec $(a, b) \in \mathbb{R}^2$ et $(u_n) \in \mathbb{R}^{\mathbb{N}}$

1. Si (C) a deux racines simples $r_1 \neq r_2$ alors
$$\exists (A, B) \in \mathbb{R}^2, \forall n \in \mathbb{N}, u_n = A{r_1}^n + B{r_2}^n$$
2. Si (C) a une racine simple $r \in \mathbb{R}$ alors
$$\exists (A, B) \in \mathbb{R}^2, \forall n \in \mathbb{N}, u_n = (An + B)r^n$$
3. Si (C) a deux racines complexes conjuguées $re^{i\theta}$ avec $r \in \mathbb{R}_\star^+$ et $\theta \in \left[0, \frac{\pi}{2}\right[$ alors
$$\exists (A, B) \in \mathbb{R}^2, \forall n \in \mathbb{N}, u_n = r^n(A\cos(n\theta) + B\sin(n\theta))$$

□

Remarque :
Étude de $u_{n+1} = f(u_n)$

1. On choisit rapidement la fonction f (au moins le tableau de variation)

1'. (optionnel) on représente graphiquement la fonction f et la droite d'équation $y = x$ pour conjecturer sa limite

2. On utilise le tableau de variation pour vérifier que (u_n) est bien définie par récurrence

$$P(n) : "u_n \text{ existe et } u_n \in \mathcal{D}_f"$$

3. On étudie le signe de $f(x) - x$

4. On cherche les intervalles stables par f :

$$f(I) \subset I$$

les plus petits possible (ça permet de montrer que la suite est majorée (minorée) en particulier ceux sur lesquels $f(x) - x$ ne change pas de signe

4'. Donc on utilise le théorème de la limite monotone

4". Sinon, on essaie l'inégalité (voir théorème) des accroissements finis :
Soit ℓ un point fixe de f : $f(\ell) = \ell$

$$\forall n \in \mathbb{N}, |u_{n+1} - \ell| = |f(u_n) - f(\ell)| = M\,|u_n - \ell|$$

où M est un majorant de $|f|$
Si $0 \leqslant M \leqslant 1$ alors

$$\forall n \in \mathbb{N}, |u_n - \ell| \leqslant M^n\,|u_n - \ell| \xrightarrow[n\to+\infty]{} 0$$

donc $u_n \xrightarrow[n\to+\infty]{} \ell$

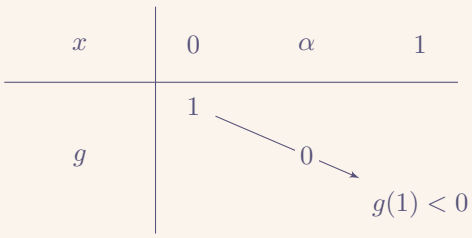
5. si (u_n) a une limite et si f continue alors $\lim(u_n)$ est une point fixe de f

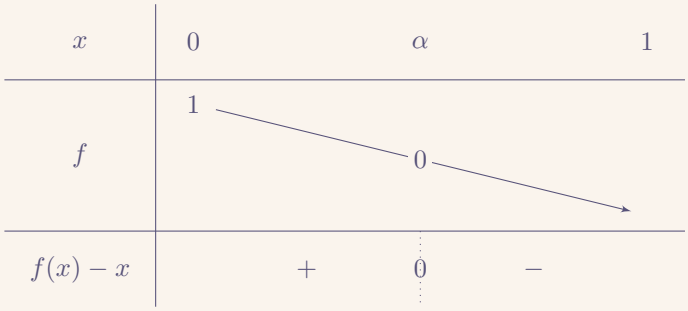
Exemple : 1.

$$\begin{cases} u_{n+1} = \cos(u_n) \\ u_0 \in]0, 1[\end{cases}$$

x	0		1		$\frac{\pi}{2}$
f	1	$\searrow$		$\searrow$	0

On pose $g : x \mapsto \cos(x) - x$ dérivable et
$\forall x \in [0, 1]\,, g'(x) = -\sin(x) - 1 \leqslant 0$





$$\forall x \in [0,1], |f'(x)| = |-\sin(x)| \\ = \sin(x) \leqslant \sin(1) < 1$$

$$\forall n, |u_{n+1} - \alpha| = |f(u_n) - f(\alpha)| \leqslant \sin(1)\,|u_n - \alpha|$$

donc

$$\forall n, |u_n - \alpha| \leqslant \underbrace{\sin^n(1)}_{\xrightarrow[n\to+\infty]{} 0} |u_0 - \alpha|$$

Donc, $u_n \xrightarrow[n\to+\infty]{} \alpha$

6 Comparaison de suites

Définition : Soient u et v deux suites réelles. On dit que u est dominée par v si

$$\exists M \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geqslant N, |u_n| \leqslant M\,|v_n|$$

Dans ce cas, on note $u = O(v)$ ou $u_n = O(v_n)$ et on dit que "u est un grand o de v"

Exemple :
En informatique, on dit qu'un algorithme a une complexité linéaire si son temps d'éxécution est un $O(n)$ Par exemple, on calcule a^n

— Approche naïve Complexité linéaire $O(n)$

```
1 : p ← 1
2 : pour i ∈ ⟦0, n − 1⟧ faire
3 :     p ← p × a
4 : retourner p
```

— Exponentiation rapide
On écrit n en binaire :

$$\begin{aligned} n &= \overline{a_k a_{k-1} \dots a_0}^{(2)} \\ &= \sum_{i=0}^{k} a_i 2^i \end{aligned}$$

avec $(a_i) \in \{0,1\}^{k+1}$

$$\begin{aligned} a^n &= a^{\sum_{i=0}^{k} a_i 2^i} \\ &= \prod_{i=0}^{k} a^{a_i 2^i} \end{aligned}$$

```
1 : s ← 0
2 : p ← a
3 : pour i ∈ ⟦0, log_2(n)⟧ faire
4 :     p ← p × p
5 :     si a[i] = 1 alors
6 :         s ← s + p
7 : retourner s
```

Compléxité logarithmique $O(\log_2(n))$

Proposition : O est une relation réfléctive et transitive.

Preuve : — Soit u une suite. On pose $M = 1$ et

$$\forall n \in \mathbb{N}, |u_n| \leqslant M\,|u_n|$$

Donc $u = O(u)$.
— Soient u, v, w trois suites telles que

$$\begin{cases} u = O(v) \\ v = O(w) \end{cases}$$

Soient $M_1, M_2 \in \mathbb{R}$ et $N_1, N_2 \in \mathbb{N}$ tels que

$$\begin{cases} \forall n \geqslant N_1, |u_n| \leqslant M_1 |v_n| \\ \forall n \geqslant N_2, |v_n| \leqslant M_2 |w_n| \end{cases}$$

Nécéssairement, $M_1 \geqslant 0$ et $M_2 \geqslant 0$.
Soit $N = \max(N_1, N_2)$.

$$\forall n \geqslant N, |u_n| \leqslant M_1 |v_n| \leqslant M_1 M_2 |w_n|$$

Donc $u = O(w)$

□

Définition : Soient u et v deux suites. On dit que u est négligeable devant v si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, |u_n| \leqslant \varepsilon |v_n|$$

Dans ce cas, on note $u = o(v)$ ou $u_n = o(v_n)$ ou on le lit "u est un petit o de v"

Proposition : o est une relation transitive, non-réfléctive

Preuve : — Soient u, v et w trois suites telles que

$$\begin{cases} u = o(v) \\ v = o(w) \end{cases}$$

Soit $\varepsilon > 0$. Soit $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, |u_n| \leqslant \sqrt{\varepsilon} |v_n|$$

Soit $N_2 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_2, |v_n| \leqslant \sqrt{\varepsilon} |w_n|$$

On pose $N = \max(N_1, N_2)$, alors

$$\forall n \geqslant N, |u_n| \leqslant \sqrt{\varepsilon} |v_n| \leqslant \underbrace{\sqrt{\varepsilon} \times \sqrt{\varepsilon}}_{\varepsilon} |w_n|$$

donc $u = o(w)$
— Soit u une suite tel qu'il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, u_n > 0$$

On suppose que $u = o(u)$, alors

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, |u_n| \leqslant \varepsilon |u_n|$$

On pose $\varepsilon = \dfrac{1}{2}$ alors

$$\exists N \in \mathbb{N}, \forall n \geqslant N, |u_n| \leqslant \frac{1}{2} |u_n|$$

une contradiction

□

Proposition : Soient u et v deux suites.

- $o(u) + o(u) = o(u)$
- $v \times o(u) = o(uv)$
- $o(u) \times o(v) = o(uv)$
- $o(o(u)) = o(u)$

□

Définition : Soient u et v deux suites. On dit que u et v sont équivalentes si

$$u = v + o(v)$$

i.e.

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, |u_n - v_n| \leqslant \varepsilon |v_n|$$

Dans ce cas, on le note $u \sim v$

Proposition : $\sim$ est une relation d'équivalence □

Proposition : Soient $(u, v) \in \mathbb{R}^{\mathbb{N}}$. On suppose que v ne s'annule pas à partir d'un certain rang

1. $u = o(v) \iff \left(\dfrac{u_n}{v_n}\right)$ bornée
2. $u = o(v) \iff \dfrac{u_n}{v_n} \xrightarrow[n \to +\infty]{} 0$
3. $u \sim v \iff \dfrac{u_n}{v_n} \xrightarrow[n \to +\infty]{} 1$

□

Proposition (Suites de références) **:**

1. $\ln^\alpha(n) = o(n^\beta)$ avec $(\alpha, \beta) \in \left(\mathbb{R}_\star^+\right)^2$
2. $n^\beta = o(a^n)$ avec $\beta > 0$ et $a > 1$
3. $a^n = o(n!)$ avec $a > 1$
4. $n! = o(n^n)$

Lemme (Exercice 10 du TD) **:** Soit $u \in \left(\mathbb{R}_\star^+\right)^{\mathbb{N}}$
Si $\dfrac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} \ell < 1$ avec $\ell \in \mathbb{R}$,
alors $u_n \xrightarrow[n\to+\infty]{} 0$

Preuve (de la proposition) *:*

1. par croissance comparée
2. On pose $\forall n \in \mathbb{N}^\star, u_n = \dfrac{n^\beta}{a^n}$.

$$\begin{aligned}\forall n \in \mathbb{N}^\star, \frac{u_{n+1}}{u_n} &= \left(\frac{n+1}{n}\right)^\beta \times \frac{1}{a} \\ &= \frac{1}{a}\left(1 + \frac{1}{n}\right)^\beta \\ &\xrightarrow[n\to+\infty]{} \frac{1}{a} < 1\end{aligned}$$

   Donc, $u_n \xrightarrow[n\to+\infty]{} 0$

3. On pose $\forall n \in \mathbb{N}, u_n = \dfrac{a^n}{n!}$

$$\forall n \in \mathbb{N}, \frac{u_{n+1}}{u_n} = \frac{a}{n+1} \xrightarrow[n\to+\infty]{} 0 < 1$$

   donc $u_n \xrightarrow[n\to+\infty]{} 0$

4. On pose $\forall n \in \mathbb{N}^\star, u_n = \dfrac{n!}{n^n}$.

$$\begin{aligned}\forall n \in \mathbb{N}^\star, \frac{u_{n+1}}{u_n} &= (n+1)\frac{n^n}{(n+1)^{n+1}}\\ &= \left(\frac{n}{n+1}\right)^n\\ &= e^{n\ln\left(\frac{n}{n+1}\right)}\\ &= e^{n\ln\left(1+\frac{1}{n+1}\right)}\\ &= e^{n\left(-\frac{1}{n}+o\left(\frac{1}{n}\right)\right)}\\ &= e^{-1+o(1)}\\ &\xrightarrow[n\to+\infty]{} e^{-1} < 1\end{aligned}$$

donc $u_n \xrightarrow[n\to+\infty]{} 0$

□

7 Suites complexes

Définition : Soit $(u_n) \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$. On dit que (u_n) converge vers ℓ si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, |u_n - \ell| \leqslant \varepsilon$$

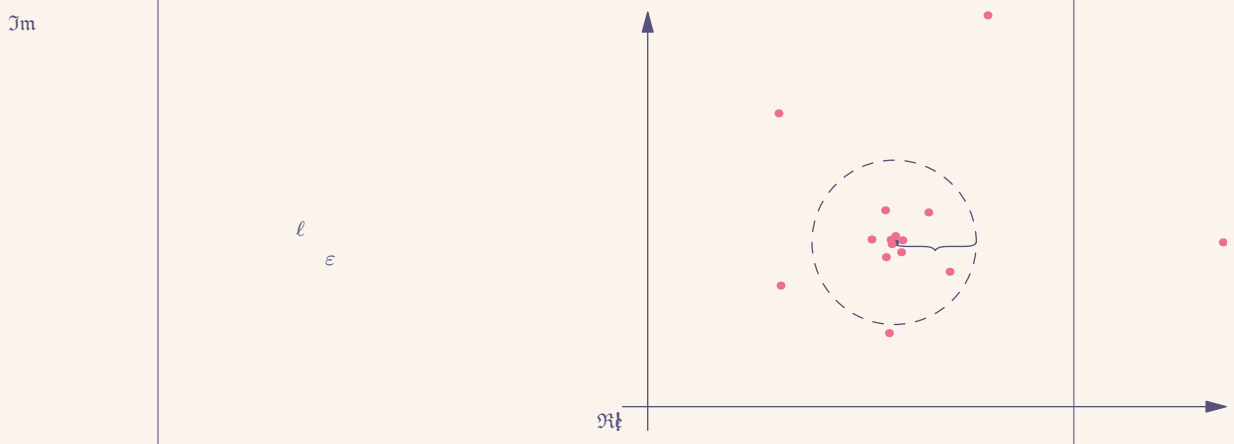


FIGURE 11.9 – Suite complexe convergente

Proposition : Si ℓ_1 et ℓ_2 sont deux limites de u alors $\ell_1 = \ell_2$

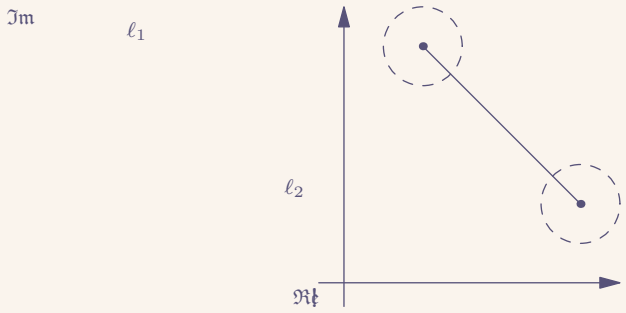


FIGURE 11.10 – Unicité de la limite de suites complexes

□

Proposition : Les limites de somme, produit, quotient de suites complexes respectent les mêmes lois que pour les suites réelles. □

Théorème : Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$.

$$u_n \xrightarrow[n\to+\infty]{} \ell \iff \begin{cases} \mathfrak{Re}(u_n) \xrightarrow[n\to+\infty]{} \mathfrak{Re}(\ell) \\ \mathfrak{Im}(u_n) \xrightarrow[n\to+\infty]{} \mathfrak{Im}(\ell) \end{cases}$$

Preuve : $\Longrightarrow$ On suppose $u_n \to \ell$.
Soit $\varepsilon > 0$. Soit $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, |u_n - \ell| \leqslant \varepsilon$$

Or,

$$\forall n \geqslant N, \begin{cases} \mathfrak{Re}(u_n) - \mathfrak{Re}(\ell) = \mathfrak{Re}(u_n - \ell) \leqslant |u_n - \ell| \leqslant \varepsilon \\ \mathfrak{Im}(u_n) - \mathfrak{Im}(\ell) = \mathfrak{Im}(u_n - \ell) \leqslant |u_n - \ell| \leqslant \varepsilon \end{cases}$$

donc

$$\begin{cases} \mathfrak{Re}(u_n) \to \mathfrak{Re}(\ell) \\ \mathfrak{Im}(u_n) \to \mathfrak{Im}(\ell) \end{cases}$$

$\Longleftarrow$ On suppose $\begin{cases} \mathfrak{Re}(u_n) \to \mathfrak{Re}(\ell) \\ \mathfrak{Im}(u_n) \to \mathfrak{Im}(\ell) \end{cases}$
Alors,

$$\forall n \in \mathbb{N}, u_n = \mathfrak{Re}(u_n) + i\mathfrak{Im}(u_n) \to \mathfrak{Re}(\ell) + i\mathfrak{Im}(\ell) = \ell$$

□

Proposition : Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$.
Si $u_n \to \ell$ alors $|u_n| \to |\ell|$

Preuve :
On suppose $u_n \to \ell$

$$\forall n \in \mathbb{N}, |u_n| = \sqrt{\mathfrak{Re}^2(u_n) + \mathfrak{Im}^2(u_n)} \to \sqrt{\mathfrak{Re}^2(\ell) + \mathfrak{Im}^2(\ell)} = |\ell|$$

□

Proposition : Tous les résultats (sauf ceux avec des limites infinies !) concernant les suites extraites sont encore valables dans $\mathbb{C}$ y compris le théorème de Bolzano-Weierstrass (mais avec une autre preuve).

Définition : Soit $u \in \mathbb{C}^{\mathbb{N}}$. On dit que u est bornée s'il existe $M \in \mathbb{R}^+$ tel que

$$\forall n \in \mathbb{N}, |u_n| \leqslant M$$

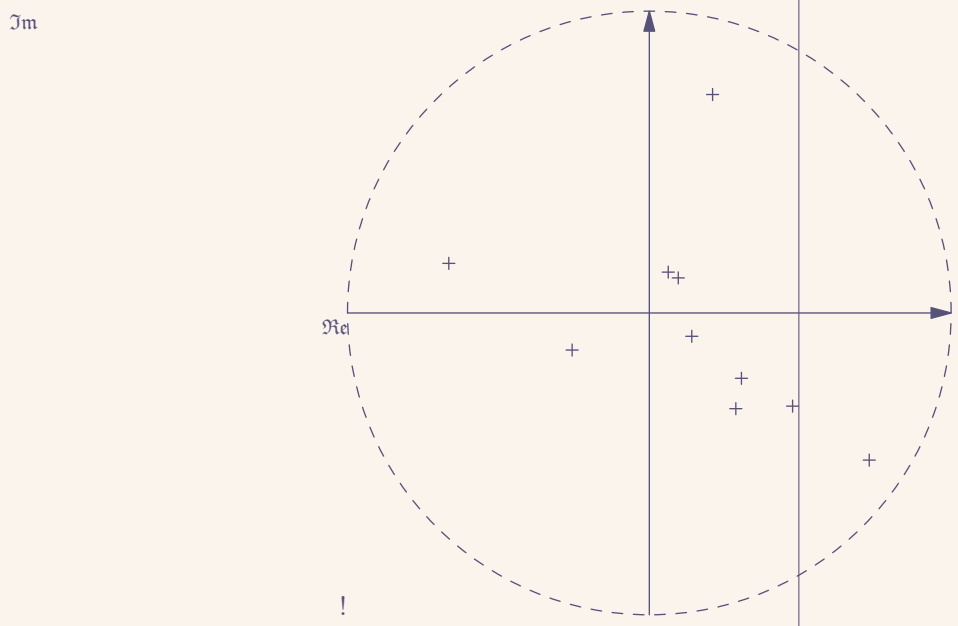


FIGURE 11.11 – Suite complexe bornée

Théorème (Bolzano Weierstrass) **:** Soit $u \in \mathbb{C}^{\mathbb{N}}$ bornée. Il existe φ :

$\mathbb{N} \to \mathbb{N}$ strictement croissante telle que $\left(u_{\varphi(n)}\right)$ converge.

Preuve :
Soit $M \in \mathbb{R}^+$ tel que

$$\forall n \in \mathbb{N}, |u_n| \leqslant M$$

Donc, $\forall n \in \mathbb{N}, |\mathfrak{Re}(u_n)| \leqslant |u_n| \leqslant M$ Donc $(\mathfrak{Re}(u_n))_{n\in\mathbb{N}}$ est bornée. Donc, il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $\left(\mathfrak{Re}\left(u_{\varphi(n)}\right)\right)$ converge.

$$\forall n \in \mathbb{N}, \left|\mathfrak{Im}\left(u_{\varphi(n)}\right)\right| \leqslant \left|u_{\varphi(n)}\right| \leqslant M$$

donc $\left(\mathfrak{Im}(u_{\varphi(n)}\right)$ est bornée. Soit $\psi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $\left(\mathfrak{Im}\left(u_{\varphi(\psi(n))}\right)\right)$ converge. Or, $\left(\mathfrak{Re}\left(u_{\varphi(\psi(n))}\right)\right)$ est une sous suite de la suite convergente $\left(\mathfrak{Re}\left(u_{\varphi(n)}\right)\right)$ donc $\left(\mathfrak{Re}\left(u_{\varphi(\psi(n))}\right)\right)$ converge.
Donc, $\left(u_{\varphi(\psi(n))}\right)$ converge.
Comme $\varphi \circ \psi$ est strictement croissante, $\left(u_{\varphi(\psi(n))}\right)$ est une sous suite de (u_n) □

8 Annexe

Proposition : Soit $f : I \to I$ continue et $(u_n)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} u_0 \in I \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

Si (u_n) converge vers $\ell \in \mathbb{R}$
alors $f(\ell) = \ell$ i.e. (ℓ est un point fixe de f)

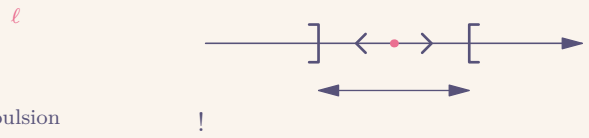
Preuve :
On suppose que (u_n) converge vers ℓ.
$\lim\limits_{n\to+\infty} u_{n+1} = \ell$ car (u_{n+1}) est une sous suite de (u_n).

$$\forall n \in \mathbb{N}, u_{n+1} = f(u_n)$$

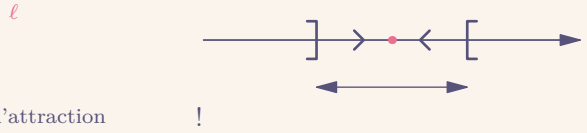
Comme f est continue alors $f(u_n) \xrightarrow[n\to+\infty]{} f(\ell)$. Par unicité de la limite, $\ell = f(\ell)$ □

Remarque :
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $f : \mathbb{R} \to \mathbb{R}$ dérivable telle que $u_{n+1} = f(u_n)$.
Soit $\ell \in \mathbb{R}$ un point fixe de f. Donc, $f(\ell) = \ell$.

$|f'(\ell)| > 1$:



$|f'(\ell)| < 1$:



Par contre, si $|f'(\ell)| = 1$, on ne sait pas.

Remarque (Suite arithético-géométrique) :

$$(\star) : \forall n \in \mathbb{N}, u_{n+1} = au_n + b = f(u_n)$$

Méthode 1

— On cherche v une suite constante solution de $(\star)$:

$$\exists C \in \mathbb{R}, \forall n \in \mathbb{N}, v_n = C$$

donc

$$\forall n \in \mathbb{N}, C = aC + b = f(C)$$

Si $a \neq 1$: $C = \dfrac{b}{1-a}$

— Soit u qui vérifie $(\star)$. On pose $w = u - v$.

$$\begin{aligned} \forall n \in \mathbb{N}, w_{n+1} &= u_{n+1} - v_{n+1} \\ &= au_n + b - av_n - b \\ &= a(u_n - v_n) \\ &= aw_n \end{aligned}$$

Donc $\forall n \in \mathbb{N}, w_{n+1} = aw_n + 0$: équation homogène associée à $(\star)$

(w_n) est géométrique donc

$$\forall n \in \mathbb{N}, w_n = w_0 a^n$$

et donc

$$\forall n \in \mathbb{N}, u_n = w_0 a^n + \frac{b}{1-a}$$

Méthode 2

$$\begin{aligned} \varphi : \mathbb{R}^{\mathbb{N}} &\longrightarrow \mathbb{R}^{\mathbb{N}} \\ (u_n) &\longmapsto (u_{n+1} - au_n) \end{aligned}$$

φ morphisme de groupes additifs

$$\varphi(u) = (b) \iff u = v + w \text{ avec } w \in \mathrm{Ker}(\varphi)$$

$$\begin{aligned} w \in \mathrm{Ker}(\varphi) &\iff \varphi(w) = 0 \\ &\iff \forall n \in \mathbb{N}, w_{n+1} - aw_n = 0 \\ &\iff \forall n \in \mathbb{N}, w_{n+1} = aw_n \end{aligned}$$

Chapitre 12

Structures algébriques usuelles

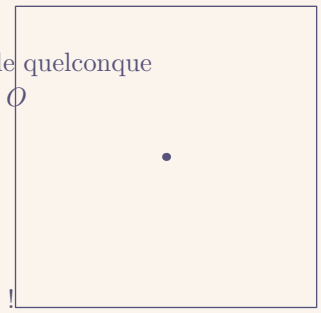
1 Groupes

Principe de symétrie (Pierre Curie)
La symétrie des causes se retrouvent dans les effets.

On fait tomber un caillou dans un plan d'eau ce qui crée une onde qui se propage.

— Symétries des "causes"
(conserver O en place)

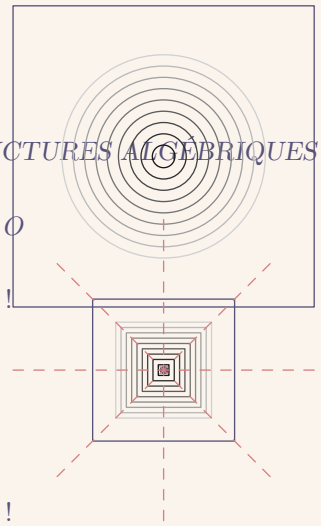
  — translation de vecteur $\vec{0}$
  — rotations de centre O d'angle quelconque
  — symétries d'axe passant par O



— Symétries des "effets" (conserver les ondes en place)

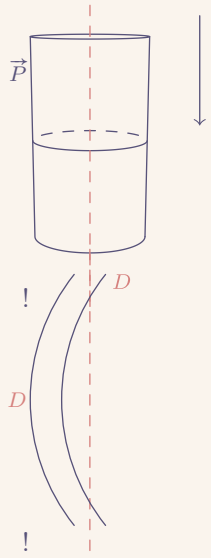
  — translation de vecteur $\vec{0}$
  — rotations de centre O d'angle quelconque

— symétries d'axe passant par O



— translation de vecteur $\vec{0}$
— 4 rotations de centre O d'angle $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$
— 4 symétries axiales

— Causes
  — translations de vecteur $\vec{u} \in \vec{D}$
  — rotations d'axe D



— Effet

Définition : Soit G un ensemble, muni d'une loi de composition interne $\diamond$.
On dit que $(G, \diamond)$ est un groupe si :
— $\diamond$ est associative
— $\diamond$ a un neutre $e \in G$
— $\forall x \in G, \exists y \in G, x \diamond y = y \diamond x = e$

Exemple ((À connaître)) : 1. E un ensemble. $S(E)$ l'ensemble des bijections de E dans E.
$(S(E), \circ)$ est un groupe appelé groupe symétrique de E.
Si, $E = [\![1, n]\!]$, alors noté $S(E)$ est noté S_n (ou parfois $\mathfrak{S}_n$)

2. $(\mathbb{Z},+)$ est un groupe mais $(\mathbb{N},+)$ n'est pas un groupe.
3. $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes
4. $(\mathbb{R},\times)$ n'est pas un groupe car 0 n'a pas d'inverse.
   $(\mathbb{Q}_\star,\times)$, $(\mathbb{R}_\star,\times)$, $(\mathbb{C}_\star,\times)$ sont des groupes.
   $(\mathbb{Z}_\star,\times)$ n'est pas un groupe.
5. $(\mathcal{M}_n(\mathbb{C}),+)$ est un groupe
   $(\mathcal{M}_n(\mathbb{C}),\times)$ n'est pas un groupe

Définition : On dit que $(G,\diamond)$ est un groupe commutatif ou abélien si c'est un groupe et $\diamond$ est une loi commutative.

Définition : Soit $(G,\cdot)$ un groupe (d'élément neutre e) et $H\subset G$. On dit que H est un sous groupe de G si

1. $\forall (x,y)\in H^2, x\cdot y\in H$
2. $e\in H$
3. $\forall x\in H, x^{-1}\in H$

Proposition : Soit H un sous groupe de $(G,\cdot)$. Alors, $(H,\cdot)$ est un groupe. □

Proposition : Soit $(G,\cdot)$ un groupe et $H\subset G$.

$$H \text{ est un sous groupe de } G \iff \begin{cases}\forall (x,y)\in H, x\cdot y^{-1}\in H\\ H\neq\end{cases}$$

Preuve $\Longrightarrow$ " $e\in H$ donc $H\neq$.
Soit $(x,y)\in H^2$.
$y\in H$ donc $y^{-1}\in H$.
$x\in H$ donc $x\cdot y^{-1}\in H$.

" $\Longleftarrow$ " $H\neq$.
Soit $a\in H$, $(a,a)\in H^2$ donc $a\cdot a^{-1}\in H$ donc $e\in H$.
Soit $x\in H$, $(e,x)\in H^2$ donc $e\cdot e^{-1}\in H$ donc $x^{-1}\in H$.
Soit $(x,y)\in H^2$. Comme $y\in H$, $y\in y^{-1}\in H$ donc $(x,y^{-1})\in H^2$.
Donc, $x\cdot\left(y^{-1}\right)^{-1}\in H$.
Donc, $x\cdot y\in H$.

□

Exemple :
$2\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$.
En effet,

— $2 \in 2\mathbb{Z}$ donc $2\mathbb{Z} \neq$

— Soit $(x, y) \in (2\mathbb{Z})^2$, $\begin{cases} x \equiv 0 \ [2] \\ y \equiv 0 \ [2] \end{cases}$

donc $x - y \equiv 0 \ [2]$ donc $x - y \in 2\mathbb{Z}$

Proposition : Soit $(G, \cdot)$ un groupe et $(H_i)_{i \in I}$ une famille non vide de sous groupes de G. Alors, $\bigcap_{i \in I} H_i$ est un sous groupe de G.

Preuve :
On sait que $\forall i \in I, e \in H_i$ et $I \neq$
Donc, $e \in \bigcap_{i \in I} H_i$ donc $\bigcap_{i \in I} H_i \neq$
Soit $(x, y) \in \left(\bigcap_{i \in I} H_i \right)^2$.

$$\forall i \in I, \begin{cases} x \in H_i \\ y \in H_i \end{cases}$$

donc,

$$\forall i \in I, x \cdot y^{-1} \in H_i$$

donc

$$x \cdot y^{-1} \in \bigcap_{i \in I} H_i$$

□

Proposition : Soit $(G, \cdot)$ un groupe.
$\{e\}$ et G sont des sous groupes de G

Remarque :
Une réunion de sous groupes n'est pas nécessairement un sous groupe.

$$(G, \cdot) = (\mathbb{Z}, +)$$

$2\mathbb{Z} \cup 3\mathbb{Z} = A$
$2 \in A$ et $3 \in A$ mais $2 + 3 = 5 \notin A$.
Donc, A n'est pas un sous groupe de $\mathbb{Z}$

Proposition–Définition : Soit $(G,\cdot)$ un groupe et $A \subset G$. Alors,

$$\bigcap_{\substack{H \text{ sous groupe de } G \\ A \subset H}} H$$

est le plus petit (au sens de l'inclusion) sous groupe de G qui contient A.
On dit que c'est le sous groupe engendré par A et on le note $\langle A \rangle$

Preuve :
On pose $\mathcal{G} = \{H \in \mathcal{P}(G) \mid H \text{ sous groupe contenant } A\}$.
$G \in \mathcal{G}$ donc $\mathcal{G} \neq$ donc $\bigcap_{H \in \mathcal{G}} H$ est un sous groupe de G.
Soit $a \in A$. Alors

$$\forall H \in \mathcal{G}, a \in A \subset H$$

et donc $a \in \bigcap_{H \in \mathcal{G}} H$.
Donc, $A \subset \bigcap_{H \in \mathcal{G}} H$.
Soit H un sous groupe de G qui contient A.
Alors, $H \in \mathcal{G}$ alors $H \supset \bigcap_{H \in \mathcal{G}} H$ □

Exemple :
$(G,\cdot) = (\mathbb{Z},+)$
$A = 2\mathbb{Z} \cup 3\mathbb{Z}$
$\langle A \rangle = \mathbb{Z}$ (d'après le théorème de Bézout).
On généralise $\langle a\mathbb{Z} \cup b\mathbb{Z} \rangle = (a \wedge b)\mathbb{Z}$

Définition : Soit $(G,\cdot)$ un groupe et $A \subset G$.
On dit que A est une partie génératrice de G ou que A engendre G si $G = \langle A \rangle$

Exemple (Rubik's cube) :

Exemple :
Soit $(G,\cdot)$ un groupe.

- $\langle \rangle = \{e\}$
  $\langle G \rangle = G$
- Soit $a \in G \setminus \{e\}$.
  $\langle a \rangle = \langle \{a\} \rangle = \{a^n \mid n \in \mathbb{Z}\}$

— Soit $a \neq b$ deux éléments de $G \setminus \{e\}$

$$\langle \{a,b\} \rangle = \{x \in G \mid \exists n \in \mathbb{N}, \exists (a_1, a_2, \ldots, a_n) \in \{a,b\}^n, \\ \exists (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \in \{-1,1\}^n, x = a_1^{\varepsilon_1} \times a_2^{\varepsilon_2} \times \ldots \times a_n^{\varepsilon_n}\}$$

Remarque (Notation) :
Soit $(G, \cdot)$ un groupe et $a \in G$.
Pour $n \in \mathbb{N}_\star$, on pose $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ fois}}$.
On pose $a^0 = e$ et pour $n \in Z_\star^-$,

$$a^n = \left(a^{-1}\right)^{-n}$$

Remarque :
Si le groupe est noté additivement. On note na $(n \in \mathbb{Z}, a \in G)$ à la place de a^n

Définition : On dit qu'un groupe $(G, \cdot)$ est monogène s'il existe $a \in G$ tel que

$$G = \langle a \rangle$$

On dit alors que a est un générateur de G

Exemple :
$(\mathbb{Z}, +)$ est engendré par 1.
$(2\mathbb{Z}, +)$ est engendré par 2

Définition : Un groupe monogène fini est cyclique.

Proposition : Soit $(G, \cdot)$ un groupe monogène fini. Soit a un générateur de G. Il existe $k \in \mathbb{N}$ tel que

$$G = \{e, a, a^2, \ldots a^{k-1}\}$$

Preuve :
G est fini donc il existe $p < q$ tels que $a^p = a^q$. On a alors $e = a^{q-p}$.
On pose alors, $k = \min \{n \in \mathbb{N}_\star \mid a^n = e\}$.
Soit $x \in G = \langle a \rangle$. Il existe $n \in \mathbb{Z}$ tel que $x = a^n$. On fait la division de n par k

$$\begin{cases} n = kq + r \\ q \in \mathbb{Z}, 0 \leqslant r < k \end{cases}$$

$$x = a^n = a^{kq+r} = \left(a^k\right)^q \times a^r = a^r$$

On a prouvé
$$G \subset \left\{e, a, \dots, e^{k-1}\right\}$$
On sait déjà que $\left\{e, a, \dots, a^{k-1}\right\} \subset G$. □

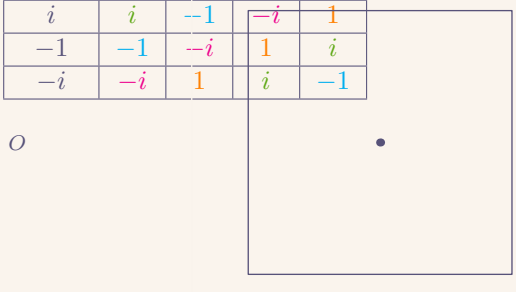
Exemple :
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique :
$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

Définition : Soit $(G, \cdot)$ un groupe et $a \in G$.
Si $\langle a \rangle$ est fini, le cardinal de $\langle a \rangle$ est appelé ordre de a : c'est le plus petit entier strictement positif n tel que $a^n = e$

Exemple :
$(S(\mathbb{C}_\star), \circ)$ est un groupe
$z \mapsto \overline{z}$ est d'ordre de 2
$z \mapsto -z$ est d'ordre de 2
$z \mapsto \dfrac{1}{z}$ est d'ordre de 2

Exemple : — $G_1 = (\mathbb{U}_4, \times)$ où
$$\begin{aligned}\mathbb{U}_4 &= \{z \in \mathbb{C} \mid z^4 = 1\} \\ &= \{1, i, -1, -i\}\end{aligned}$$

y \ x	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1



!

— G_2 l'ensemble des rotations planes qui laissent globalement invariant un carré.
$$G_2 = \left\{id, \rho_{\frac{\pi}{2}}, \rho_\pi, \rho_{\frac{3\pi}{2}}\right\}$$

y \ x	id	$\rho_{\frac{\pi}{2}}$	ρ_{π}	$\rho_{\frac{3\pi}{2}}$
id	id	$\rho_{\frac{\pi}{2}}$	ρ_{π}	$\rho_{\frac{3\pi}{2}}$
$\rho_{\frac{\pi}{2}}$	$\rho_{\frac{\pi}{2}}$	ρ_{π}	$\rho_{\frac{3\pi}{2}}$	id
ρ_{π}	ρ_{π}	$\rho_{\frac{3\pi}{2}}$	id	$\rho_{\frac{\pi}{2}}$
$\rho_{\frac{3\pi}{2}}$	$\rho_{\frac{3\pi}{2}}$	id	$\rho_{\frac{\pi}{2}}$	ρ_{π}

—

$$G_3 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$

Définition : Soient $(G_1, \cdot)$ et $(G_2, \star)$ deux groupes et $f : G_1 \to G_2$. On dit que f est un (homo)morphisme de groupes si

$$\forall (x, y) \in G_1, f(x \cdot y) = f(x) \star f(y)$$

Exemple :
$\exp : (\mathbb{R}, +) \to (\mathbb{R}_\star^+, \times)$ est un morphisme de groupes

Proposition : Avec les notations précédentes,
- l'image directe d'un sous groupe de G_1 est un sous groupe de G_2
- l'image réciproque d'un sous groupe de G_2 est un sous groupe de G_1

Preuve : — Soit H_1 un sous groupe de G_1.
$e_1 \in H_1$ donc $f(e_1) \in f(H_1)$ donc $H_1 \neq$ Soient $x \in f(H_1)$ et $y \in f(H_2)$.
On pose $\begin{cases} x = f(u) \text{ avec } u \in H_1 \\ y = f(v) \text{ avec } v \in H_1 \end{cases}$

$$\begin{aligned} x \star y^{-1} &= f(u) \star f(v)^{-1} \\ &= f(u) \star f\left(v^{-1}\right) \\ &= f\left(u \cdot v^{-1}\right) \end{aligned}$$

$\begin{cases} u \in H_1 \\ v \in H_1 \end{cases}$ donc $u \cdot v^{-1} \in H_1$ donc $x \star^{-1} \in f(H_1)$

— Soit H_2 un sous groupe de G_2.

$$(x,y) \in f^{-1}(H_2)^2$$

$$\begin{aligned} x \cdot y^{-1} \in f^{-1}(H_2) &\iff f\left(x \cdot y^{-1}\right) \in H_2 \\ &\iff f(x) \star f\left(y^{-1}\right) \in H_2 \\ &\iff f(x) \star f(y)^{-1} \in H_2 \end{aligned}$$

Or, $\begin{cases} f(x) \in H_2 \\ f(y) \in H_2 \end{cases}$
Comme H_2 est un sous groupe de G_2,

$$f(x) \star f(y)^{-1} \in H_2$$

et donc,

$$x \cdot y^{-1} \in f^{-1}(H_2)$$

□

Lemme :

$$\begin{cases} f(e_1) = e_2 \\ \forall u \in G_1, f\left(u^{-1}\right) = (f(u))^{-1} \end{cases}$$

Preuve :

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) \star f(e_1)$$

On multiplie par $f(e_1)^{-1}$ (possible car G_2 est un groupe) et on trouve $f(e_1) = e_2$.
Soit $u \in G_1$.

$$f(u) \star f(u^{-1}) = f(u \cdot u^{-1}) = f(e_1) = e_2 f(u^{-1}) \star f(u) = f(u^{-1} \cdot u) = f(e_1) = e_2$$

Donc, $f\left(u^{-1}\right) = (f(u))^{-1}$ □

Corollaire : Soit $f : (G_1, \cdot) \to (G_2, \star)$ un morphisme de groupes. Alors, $\mathrm{Im}(f)$ est un sous groupe de G_2.

$$\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\})$$

est un sous groupe de G_1. □

Théorème : Avec les notations précédentes,

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{e_1\}$$

Preuve " $\Longrightarrow$ " On suppose f injective.

$$f(e_1) = e_2 \text{ donc } e_1 \in \mathrm{Ker}(f)$$
$$\text{donc } \{e_1\} \subset \mathrm{Ker}(f)$$

Soit $x \in \mathrm{Ker}(f)$. On a alors $f(x) = e_2 = f(e_1)$
Comme f injective, $x = e_1$.

" $\Longleftarrow$ " On suppose $\mathrm{Ker}(f) = \{e_1\}$

Soient $\begin{cases} x \in G_1 \\ y \in G_1 \end{cases}$. On suppose $f(x) = f(y)$

$$\begin{aligned} f(x) = f(y) &\Longrightarrow f(x) \star f(y)^{-1} = e_2 \\ &\Longrightarrow f(x) \star f\left(y^{-1}\right) = e_2 \\ &\Longrightarrow f\left(x \cdot y^{-1}\right) \qquad \Longrightarrow x \cdot y^{-1} \in \mathrm{Ker}(f) = \{e_1\} \\ &\Longrightarrow x \cdot y^{-1} = e_1 \\ &\Longrightarrow x = y \end{aligned}$$

Donc, f est injective

□

Exemple ((équation diophantienne)) :

$$\begin{cases} 2x + 5y = 1 \\ (x, y) \in \mathbb{Z}^2 \end{cases}$$

On trouve une solution particulière (Bézout) : $(-1, 1) = (x_0, y_0)$

$$\begin{aligned} 2x + 5y = 1 &\iff 2x + 5y = 2x_0 + 5y_0 \\ &\iff 2(x - x_0) + 5(y - y_0) = 0 \\ &\iff 2(x - x_0) = 5(y_0 - y) \\ &\vdots \quad \text{(Gauß)} \end{aligned}$$

$$\begin{aligned} f : \mathbb{Z}^2 &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto 2x + 5y \end{aligned}$$

$(\mathbb{Z}^2, +)$ est un groupe avec $+$ qui est l'addition composante par composante.
f est un morphisme de groupes.

$$\begin{aligned} f(x,y) = 1 = f(x_0,y_0) &\iff f(x,y) - f(x_0,y_0) = 0 \\ &\iff f(x-x_0, y-y_0) = 0 \\ &\iff (x-x_0, y-y_0) \in \mathrm{Ker}(f) \end{aligned}$$

Théorème : Soit $f : (G_1, \cdot) \to (G_2, \star)$ un morphisme de groupes, $y \in G_2$ et $(\mathscr{E})$ l'équation

$$f(x) = y$$

d'inconnue $x \in G_1$.
Si $y \notin \mathrm{Im}(f)$, alors $(\mathscr{E})$ n'a pas de solution.
Sinon, soit $x_0 \in G_1$ tel que $f(x_0) = y$ (x_0 est une solution particulière de $(\mathscr{E})$)

$$f(x) = y \iff \exists h \in \mathrm{Ker}(f), x = x_0 \cdot h$$

Preuve :

$$\begin{aligned} f(x) = y &\iff f(x) = f(x_0) \\ &\iff f(x_0)^{-1} \star f(x) = e_2 \\ &\iff f\left(x_0^{-1}\right) \star f(x) = e_2 \\ &\iff f\left(x_0^{-1} \cdot x\right) = e_2 \\ &\iff x_0^{-1} \cdot x \in \mathrm{Ker}(f) \\ &\iff \exists h \in \mathrm{Ker}(f), x_0^{-1} \cdot x = h \\ &\iff \exists h \in \mathrm{Ker}(f), x = x_0 \cdot h \end{aligned}$$

□

Proposition : Soient $f : G_1 \to G_2$ et $g : G_2 \to G_3$ deux morphisme de groupes. Alors, $g \circ f$ est un morphisme de groupes.

Preuve :
Soient $x \in G_1$ et $y \in G_2$.

$$\begin{aligned} g \circ f(x \cdot y) &= g(f(x) \star f(y)) = g(f(x)) \times g(f(y)) \\ &= g \circ f(x) \times g \circ f(y) \end{aligned}$$

□

Définition : Soit G un groupe.

- Un endomorphisme de G est un morphisme de groupes de G dans G.
- Un isomorphisme de G dans H un morphisme de groupes $f : G \to H$ bijectif.
- Un automorphisme de G est un endomorphisme de G bijectif.

Proposition : Soit $f : G \to H$ un isomorphisme de groupes.
Alors, $f^{-1} : H \to G$ est aussi un isomorphisme.

Preuve :
Soit $(x, y) \in H^2$. On pose $\begin{cases} f(u) = x, u \in G \\ f(v) = y, v \in G \end{cases}$

$$\begin{aligned} f\left(f^{-1}\left(x \cdot y^{-1}\right)\right) &= x \cdot y^{-1} \\ &= f(u) \cdot f(v)^{-1} \\ &= f\left(u \cdot v^{-1}\right) \end{aligned}$$

Comme f injective,

$$f^{-1}\left(x \cdot y^{-1}\right) = u \cdot v^{-1} = f^{-1}(x)\left(f^{-1}(y)\right)^{-1}$$

□

Corollaire : On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.
$\mathrm{Aut}(G)$ est un sous groupe de $(S(G), \circ)$.

Définition : Soit $(G, \cdot)$ un groupe et $g \in G$. L'application

$$\begin{aligned} c_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est appelée conjugaison par g. On dit aussi que c'est un automorphisme intérieur.

Proposition : Avec les notations précédentes,

$$c_g \in \mathrm{Aut}(G)$$

Preuve :
Soient $x \in G$ et $y \in G$.

$$c_g(xy) = g \cdot xy \cdot g^{-1}$$
$$c_g(x) \cdot c_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = c_g(xy)$$

Donc, c_g est un morphisme de groupes.

De plus,

$$\forall x \in G, c_{g^{-1}} \circ c_g(x) = g^{-1}\left(gxg^{-1}g\right) = x$$

Donc, $c_{g^{-1}} \circ c_g = id_G$.
De même, $c_g \circ c_{g^{-1}} = id_G$
Donc, c_g bijective et $(c_g)^{-1} = c_{g^{-1}}$ □

Corollaire :

$$\forall x \in G, \forall n \in \mathbb{Z}, c_g(x^n) = (c_g(x))^n$$

□

Proposition : L'application

$$G \longrightarrow \mathrm{Aut}(G)$$
$$g \longmapsto c_g$$

est un morphisme de groupes.

Preuve :
Soient $(g, h) \in G^2$.

$$\begin{aligned}\forall x \in G, c_g \circ c_h(x) &= g\left(hxh^{-1}\right)g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= c_{gh}(x)\end{aligned}$$

Donc, $c_g \circ c_h = c_{gh}$ □

Proposition (Rappel) **:**

$$\forall g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$$

Preuve :

$$(gh)\left(h^{-1}g^{-1}\right) = e$$
$$\left(h^{-1}g^{-1}\right)(gh) = e$$

□

Proposition–Définition : Soient $(G_1, \star)$ et $(G_2, \star)$ deux groupes. On définit une loi sur $G_1 \times G_2$ en posant

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$$

Alors, $G_1 \times G_2$ est un groupe pour cette loi appelée groupe produit.

Preuve : — Soient $(x_1, y_1) \in {G_1}^2$ et $(x_2, y_2) \in {G_2}^2$.
On sait que $x_1 \star y_1 \in G_1$ et que $x_2 \star y_2 \in G_2$.
Donc, $(x_1, x_2) \cdot (y_1, y_2) = (x_1 x_2, y_1 y_2) \in G_1 \times G_2$

□

2 Anneaux

Définition : Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de compositions internes notées $+$ et $\times$ vérifiant

1. $(A, +)$ est un groupe commutatif (son neutre est noté 0_A)
2. $(A, \times)$ est un monoïde
   (a) $\times$ est associative
   (b) $\times$ a un neutre $1_A \in A$
3. distributivité à gauche et à droite :

$$\forall (a, b, c) \in A^3, \begin{cases} a \times (b + c) = (a \times b) + (a \times c) \\ (b + c) \times a = (b \times a) + (c \times a) \end{cases}$$

Remarque (Convention) :
Soit $(A, +, \times)$ un anneau.

On convient que la multiplication est prioritaire sur l'addition.

$$(a \times b) + (a \times c) = a \times b + a \times c$$

et l'exponentiation est prioritaire sur la multiplication ($n \in \mathbb{N}$)

$$\begin{aligned} a \times b^n &= a \times (\underbrace{b \times b \times \cdots \times b}_{n \text{ fois}}) \\ &\neq (a \times b)^n \end{aligned}$$

Proposition : Soit $(A, +, \times)$ un anneau. Alors, 0_A est absorbant

$$\forall a \in A, a \times 0_A = 0_A \times a = 0_A$$

Preuve :
Soit $a \in A$. On pose $b = a \times 0_A \in A$.

$$\begin{aligned} b = a \times 0_A &= a \times (0_A + 0_A) = a \times 0_A + a \times 0_A \\ &= b + b \ (= 2b) \end{aligned}$$

Donc,

$$-b + b = -b + b + b$$

donc $0_A = b$
De même, $0_A \times a = 0_A$. □

Remarque :

On peut imaginer $\begin{cases} a \times b = 0_A \\ a \neq 0_A \\ b \neq 0_A \end{cases}$

Exemple : — $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ est un anneau

$$\begin{cases} \overline{2} \times \overline{2} = \overline{0} & \text{car } 4 \equiv 0 \ [4] \\ \overline{2} \neq \overline{0} & \text{car } 2 \not\equiv 0 \ [4] \end{cases}$$

— $(\mathcal{M}_2(\mathbb{C}), +, \times)$ est un anneau (non commutatif)

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_A$$

$$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Définition : On dit qu'un anneau $(A, +, \times)$ est intègre si

$$\forall (a, b) \in A^2, (a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A)$$

Exemple : — $(\mathbb{Z}, +, \times)$ est intègre

— $\forall p$ premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est intègre (car tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible donc simplifiable)

Exemple :
Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$.

$$\begin{aligned}(a+b)^2 &= (a+b) \times (a+b) \\ &= (a+b) \times a + (a+b) \times b \\ &= a^2 + b \times a + a \times b + b^2\end{aligned}$$

Si a et b commutent, alors, $a \times b = b \times a$ et donc $(a+b)^2 = a^2 + b^2 + 2ab$

$$\begin{aligned}(a+b)^3 &= (a+b) \times (a+b) \times (a+b) \\ &= a^3 + a^2 \times b + a \times b \times a + b \times a^2 \\ &+ b^2 \times a + b \times a \times b + a \times b^2 + b^3\end{aligned}$$

Si a et b commutent,

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Proposition : Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{Z}$. Alors,

$$n(a \times b) = (na) \times b = a \times (nb)$$

Preuve : — Évident si $n = 0$

— On suppose $n > 0$.

$$\begin{aligned}(n(a \times b) &= \underbrace{a \times b + \cdots + a \times b}_{n \text{ fois}} \\ &= \sum_{k=1}^{n} (a \times b) \\ &= a \times \sum_{k=1}^{n} = a \times (nb) \\ &= \left(\sum_{k=1}^{n} a \right) \times b = (na) \times b\end{aligned}$$

— On suppose $n < 0$. On pose $n = -p$ avec $p = \mathbb{N}_\star$.

$$\begin{aligned}n(a \times b) &= (-p)(a \times b) = -\left(p(a \times b)\right) \\ &= -\left((pa) \times b\right) = (-p)a \times b = (na) \times b \\ &= -\left(a \times (pb)\right) = a \times (-pb) = a \times (nb)\end{aligned}$$

En effet,

$$\forall (a', b') \in A^2 (-a') \times b' + a' \times b' = (-a' + a') \times b' = 0_A \times b' = 0_A$$

donc $-(a' \times b') = (-a') \times b'$

□

Théorème (Formule du binôme de Newton) **:** Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{N}$.
Si a et b commutent alors

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Preuve (par récurrence sur n) *:*

□

Proposition : Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$ et $n \in \mathbb{N}_\star$.

Si a et b commutent, alors

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$$

□

Proposition : On note $A^\times$ l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$.
$(A^\times, \times)$ est un groupe. □

Exemple : — $\mathbb{Z}^\times = \{-1, 1\}$
— $\mathcal{M}_n(\mathbb{C})^\times = GL_n(\mathbb{C})$
— $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$

Définition : Soit $(A, +, \times)$ un anneau commutatif.

1. Soient $(a, b) \in A^2$. On dit que a divise b s'il existe $k \in A$ tel que $b = a \times k$. On dit aussi que a est un diviseur de b et que b est un multiple de a.
2. On dit que a et b sont associés s'il existe $k \in A^\times$ tel que $ak = b$ (dans ce cas, $a \mid b$ et $b \mid a$)

Remarque :
Le théorème des deux carrés peut se démontrer en exploitant les propriétés arithmétiques de l'anneau $(Z[i], +, \times)$ où $Z[i] = \{a + ib \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

Théorème des deux carrés :

1. Soit p un nombre premier.

$$\exists (a, b) \in \mathbb{N}^2, p = a^2 + b^2 \iff p \equiv 1\ [4]$$

2. Soit $n \in \mathbb{N}_\star$, $n = \prod_{p \in \mathcal{P}} p^{\alpha(p)}$

$$\exists (a, b) \in \mathbb{N}^2, n = a^2 + b^2 \iff \forall p \in \mathcal{P} \text{ tel que } \alpha(p) \neq 0, p \equiv 1\ [4]$$

Définition : Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un sous anneau de A si

1. B est un sous groupe de $(A, +)$
2. $\forall (a, b) \in B^2, a \times b \in B$

3. $1_A \in B$

Exemple :
$Z[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$

Proposition : Soit $(A, +, \times)$ un anneau et B un sous anneau de A. Alors, $(B, +, \times)$ est un anneau. □

Exercice (Exercice à connaître) :
Soit $(A, +, \times)$ un anneau. Le centre de A est

$$Z(A) = \{x \in A \mid \forall a \in A, a \times x = x \times a\}$$

$Z(A)$ est un sous anneau de A.

Proposition : Soit $(A, +, \times)$ un anneau.
Si $0_A = 1_A$ alors $A = \{0_A\}$. On dit alors que A est l'anneau nul.

Preuve :
Soit $a \in A$.

$$a = a \times 1_A = a \times 0_A = 0_A$$

□

Définition : Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux (les lois notés de la même façon mais ne sont pas forcément les mêmes !).
Soit $f : A \to B$. On dit que f est un (homo)morphisme d'anneaux si

1. $\forall (a, b) \in A^2, f(a + b) = f(a) + f(b)$
2. $\forall (a, b) \in A^2, f(a \times b) = f(a) \times f(b)$
3. $f(1_A) = 1_B$

Proposition : Avec les notations précédentes, **si** $a \in A^\times$ alors $f(a) \in B^\times$ et dans ce cas,

$$f(a)^{-1} = f\left(a^{-1}\right)$$

Preuve :

On suppose $a \in A^\times$.

$$\begin{cases} f\left(a^{-1}\right) \times f(a) = f\left(a^{-1} \times a\right) = f(1_A) = 1_B \\ f(a) \times f\left(a^{-1}\right) = f\left(a \times a^{-1}\right) = f(1_A) = 1_B \end{cases}$$

Donc, $f(a) \in B^\times$ et $f(a)^{-1} = f\left(a^{-1}\right)$ □

Définition : Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et $f : A \to B$ un morphisme d'anneaux.
On dit que f est un

- isomorphisme d'anneaux si f est bijective
- endomorphisme d'anneaux si $\begin{cases} A = B \\ + = + \\ \times = \times \end{cases}$
- automorphisme d'anneaux si f est à la fois un isomorphisme et un endomorphisme d'anneaux

Exemple : 1. Soit $a \in \mathbb{Z}$ et

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto ax \end{aligned}$$

f endomorphisme d'anneaux $\iff a = 1$

2.

$$\begin{aligned} f : \mathcal{M}_n(\mathbb{C}) &\longrightarrow \mathcal{M}_n(\mathbb{C}) \\ A &\longmapsto A^2 \end{aligned}$$

f n'est pas un morphisme d'anneaux car

$$(A+B)^2 \neq A^2 + B^2$$

3.

$$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \overline{z} \end{aligned}$$

est un automorphisme d'anneaux

4.

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{R} \\ x &\longmapsto x \end{aligned}$$

f est un morphisme d'anneaux mais ce n'est pas un endomorphisme.

5.

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto \overline{k} \end{aligned}$$

f est un morphisme d'anneaux surjectif.

Proposition : La composée de deux morphismes d'anneaux est un morphisme d'anneaux. □

Proposition : La réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux. □

Proposition : L'ensemble des automorphismes d'anneaux de A est un sous groupe de $(S(A), \circ)$. □

Proposition : L'image directe ou réciproque d'un sous anneau par un morphisme d'anneaux est un sous anneaux.

Définition : Soi $f : A \to B$ un morphisme d'anneaux. Le noyau de f est

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$$

Proposition : Avec les notations précédents,

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{0_A\}$$

□

Remarque :
$\mathrm{Ker}(f)$ n'est pas un sous anneau en général (car $1_A \notin \mathrm{Ker}(f)$ sauf si $A = \{0_A\}$)

Définition : Soit $(A, +, \times)$ un anneau et $a \in A \setminus \{0_A\}$.
On dit que a est un diviseur de zéro s'il existe $b \in A \setminus \{0_A\}$ tel que $a \times b = b \times a = 0_A$

Proposition : Les diviseurs de zéro ne sont pas inversibles. □

Exemple :
$A = \mathscr{M}_2(\mathbb{C})$
$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro
car $M \times M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

3 Corps

Exemple (Problème) : — avec $A = \mathbb{Z}/9\mathbb{Z}$, résoudre $\overline{x}^2 = \overline{0}$

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{x}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{0}$	$\overline{7}$	7	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

On a trouvé 3 solutions : $\overline{0}$, $\overline{3}$, $\overline{6}$.

— $\mathbb{Z}/8\mathbb{Z}$

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{x^2}$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{1}$

$\overline{x}^2 = 7$ a 4 solutions : $\overline{1}, \overline{7}, \overline{3},$ et $\overline{5}$

— $A = \mathbb{H} = \{a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{R}^4\}$
$i^2 = j^2 = k^2 = -1$

$$\begin{array}{ccc} ij = k & jk = i & ji = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

Dans cet anneau, -1 a 6 racines !

Définition : Soit $(\mathbb{K}, +, \times)$ un ensemble muni de deux lois de composition internes. On dit que c'est un corps si

1. $(\mathbb{K}, \times)$ est un groupe abélien
2. $(\mathbb{K}, \times)$ est un monoïde commutatif
3. $\forall x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}, \exists y \in \mathbb{K}, xy = 1_{\mathbb{K}}$
4. $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$

Exemple : — $(\mathbb{C}, +, \times)$ est un corps
— $(\mathbb{R}, +, \times)$ est un corps
— $(\mathbb{Q}, +, \times)$ est un corps
— $(\mathbb{Z}, +, \times)$ n'est pas un corps

Proposition : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Preuve :

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \left\{\overline{k} \mid k \wedge n = 1\right\}$$

□

Proposition : Tout corps est un anneau intègre.

Preuve :
Soit $(\mathbb{K}, +, \times)$ un corps. Soient $(a, b) \in \mathbb{K}^2$ tel que $a \times b = 0_{\mathbb{K}}$.
On suppose $a \neq 0_{\mathbb{K}}$. Alors, a est inversible et donc

$$b = a^{-1} \times a \times b = a^{-1} \times 0_{\mathbb{K}} = 0_{\mathbb{K}}$$

□

Exemple :
Soit $(\mathbb{K}, +, \times)$ un corps.
Résoudre

$$\begin{cases} x^2 = 1_{\mathbb{K}} \\ x \in \mathbb{K} \end{cases}$$

$$\begin{aligned} x^2 = 1_{\mathbb{K}} &\iff x^2 - 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ &\iff (x - 1_{\mathbb{K}})(x + 1_{\mathbb{K}}) = 0_{\mathbb{K}} \\ &\iff x - 1_{\mathbb{K}} = 0_{\mathbb{K}} \text{ ou } x + 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ &\iff x = 1_{\mathbb{K}} \text{ ou } x = -1_{\mathbb{K}} \end{aligned}$$

Il y a au plus 2 solutions.

Proposition : Soit $(\mathbb{K}, +, \times)$ un corps et P un polynôme à coefficients dans $\mathbb{K}$ de degré n. Alors, l'équation $P(x) = 0_{\mathbb{K}}$ a au plus n solutions dans $\mathbb{K}$ □

Corollaire ((Théorème de Wilson)) **:** voir exercice 16 du TD 12

Définition : Soit $(\mathbb{K}, +, \times)$ un corps et $L \subset \mathbb{K}$.
On dit que L est un sous corps de $\mathbb{K}$ si

1. L est un anneau de $(\mathbb{K}, +, \times)$ non nul
2. $\forall x \in L \setminus \{0_{\mathbb{K}}\}, x^{-1} \in L$

en d'autres termes si

1. $\forall (x, y) \in L^2, x - y \in L$
2. $\forall (x, y) \in L^2, x \times y^{-1} \in L$

On dit aussi que $\mathbb{K}$ est une extension de L.

Proposition : Tout sous corps est un corps. □

Définition : Soient $(\mathbb{K}_1, +, \times)$ et $(\mathbb{K}_2, +, \times)$ deux corps et $f : \mathbb{K}_1 \to \mathbb{K}_2$. On dit que f est un morphisme de corps si f est un morphisme d'anneaux. i.e. si

$$\begin{cases} \forall (x,y) \in {\mathbb{K}_1}^2, & f(x+y) = f(x) + f(y) \\ \forall (x,y) \in {\mathbb{K}_1}^2, & f(x \times y) = f(x) \times f(y) \end{cases}$$

Proposition : Tout morphisme de corps est injectif.

Preuve :
Soit $f : \mathbb{K}_1 \to \mathbb{K}_2$ un morphisme de corps.

- $\mathrm{Ker}(f)$ est un sous groupe de $(\mathbb{K}_1, +)$
- Soit $x \in \mathrm{Ker}(f)$ et $y \in \mathbb{K}_1$

$$f(x \times y) = f(x) \times f(y) = 0_{\mathbb{K}_2} \times f(y) = 0_{\mathbb{K}_2}$$

- Soit $x \in \mathrm{Ker}(f) \setminus \{0_{\mathbb{K}_1}\}$.
  Alors, x est inversible.

$$\left.\begin{array}{l} x \in \mathrm{Ker}(f) \\ x^{-1} \in \mathbb{K}_1 \end{array}\right\} \text{ donc } x \times x^{-1} \in \mathrm{Ker}(f)$$

$$\text{donc } 1_{\mathbb{K}_1} \in \mathrm{Ker}(f)$$

$$\text{donc } f(1_{\mathbb{K}_1}) = 0_{\mathbb{K}_2}$$

Or, $f(1_{\mathbb{K}_1}) = 1_{\mathbb{K}_2} \neq 0_{\mathbb{K}_2}$
Donc, $\mathrm{Ker}(f) = \{0_{\mathbb{K}_1}\}$ donc f est injective. □

Exemple :
$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$ est un morphisme de corps

4 Actions de groupes

Définition : Soit $(G, \cdot)$ un groupe et X un ensemble non vide. Une action de G sur X est une application

$$\begin{array}{rccc} \varphi : & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & \underbrace{g \cdot x}_{\text{ce n'est pas la loi de } G} \end{array}$$

qui vérifie

1. $\forall x \in X, \varphi(e,x) = e \cdot x = x$
2. $\forall x \in X, \forall g,h \in G, g \cdot (h \cdot x) = (g \cdot h) \cdot x$

Dans ce cas, $\begin{array}{ccc} G & \longrightarrow & S(X) \\ g & \longmapsto & \varphi(g,\cdot) \end{array} : \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$ est un morphisme de groupes.

Preuve :
$\forall g \in G \, (x \mapsto g \cdot x)^{-1} =$ □

5 Bilan

Groupe

On dit que $(G, \diamond)$ est un groupe si
- $\diamond$ est associative ;
- $\diamond$ a un neutre $e \in G$;
- tout élément $x \in E$ a un inverse $y \in E$:
  $x \diamond y = y \diamond x = e$.

Sous-groupe

On dit que $H \subset G$ est un sous-groupe de G si
- $e \in H$;
- $\forall x,y \in H,\ x \diamond y \in H$;
- $\forall x \in H,\ x^{-1} \in H$.

Si $\diamond$ est commutative, on dit que $(G, \diamond)$ est un groupe commutatif ou abélien.

Pour monter que H est un sous-groupe de G, on montre
- $H \neq$;
- $\forall x,y \in H,\ x \diamond y^{-1} \in H$.

L'intersection de sous-groupes est un sous-groupe. Attention, l'union de sous-groupes n'est pas forcément un sous-groupe.

Sous-groupe engendré

Le sous-groupe engendré par A, $\langle A \rangle$, est le plus petit sous groupe de G contenant A.

S'il existe $a \in G$ tel que $G = \langle a \rangle$, on dit que G est monogène et a est un générateur de G.

Soit $a \in G$. L'ordre de a est $\# \langle a \rangle$ i.e. $a^n = e$.

Morphisme de groupes

Soit $f : G_1 \to G_2$ où $(G_1, \cdot)$ et $(G_2, \times)$ sont des groupes. f est un morphisme de groupes si
$\forall x,y \in G_1,\ f(x \cdot y) = f(x) \times f(y)$.
L'image directe d'un sous-groupe de G_1 est un sous-groupe de G_2. L'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1.
$\forall u \in G_1;\ f\left(u^{-1}\right) = f(u)^{-1}$.

$$f \text{ injective} \iff \operatorname{Ker} f = \{e_1\}.$$

Chapitre 13

Systèmes linéaires et calculs matriciels

Exemple :

$$(S_1): \left\{ \begin{array}{cccccc} & \overbrace{}^{\text{pivot}} & & & & \\ \boxed{x} & +y & +z & -t & = 1 \\ x & +2y & +3z & +t & = 0 \\ x & & +z & = 2 & & \end{array} \right.$$

$$\begin{array}{c} \Longleftrightarrow \\ L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_3 - L_1 \end{array} \left\{ \begin{array}{cccccc} \boxed{x} & +y & +z & -t & = 1 \\ & y & +2z & +2t & = -1 \end{array} \right.$$

$$\begin{array}{c} \Longleftrightarrow \\ L_1 \leftarrow L_1 - L_2 \\ L_3 \leftarrow L_3 + L_2 \end{array} \left\{ \begin{array}{cccccc} \boxed{x} & & -z & -3t & = 2 \\ & \boxed{y} & +2z & +2t & = -1 \\ & & 2z & +3t & = 0 \end{array} \right.$$

$$\begin{array}{c} \Longleftrightarrow \\ L_1 \leftarrow L_1 + L_3 \\ L_2 \leftarrow L_2 + \dfrac{2}{3} L_3 \end{array} \left\{ \begin{array}{l} \boxed{x} + z = 2 \\ \boxed{y} + \dfrac{2}{3} z = -1 \\ \boxed{3t} + 2z = 0 \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{l} x = 2 - z \\ y - -1 - \dfrac{2}{3} z \\ t = -\dfrac{2}{3} z \end{array} \right.$$

L'ensemble des solutions est

$$\left\{ \left(2 - z, -1 - \frac{2}{3} z, z, -\frac{2}{3} z \right) \mid z \in \mathbb{K} \right\}$$

$$\begin{aligned}
&\left\{\begin{array}{l} x+y+z-t=1 \\ x+2y+3z+t=0 \\ x+\boxed{z}=2 \end{array}\right. \\
\underset{\substack{L_1 \leftarrow L_1-L_3 \\ L_2 \leftarrow L_2-3L_3}}{\iff} &\left\{\begin{array}{l} \boxed{y}-t=-1 \\ -2x+2y+t=-6 \\ x+\boxed{z}=2 \end{array}\right. \\
\underset{L_2 \leftarrow \frac{L_2-2L_1}{-2}}{\iff} &\left\{\begin{array}{l} \boxed{y}-t=-1 \\ \boxed{x}-\frac{3}{2}t=2 \\ x+\boxed{z}=2 \end{array}\right. \\
\underset{L_3 \leftarrow L_3-L_2}{\iff} &\left\{\begin{array}{l} \boxed{y}-t=-1 \\ \boxed{x}-\frac{3}{2}t=2 \\ \boxed{z}+\frac{3}{2}t=0 \end{array}\right. \\
\iff &\left\{\begin{array}{l} y=-1+t \\ x=2+\frac{3}{2}t \\ z=-\frac{3}{2}t \end{array}\right.
\end{aligned}$$

$$\begin{aligned}
\mathcal{S} &= \left\{(2+\frac{3}{2}t, -1+t, -\frac{3}{2}t, t \mid t \in \mathbb{K}\right\} \\
&= \{\underbrace{(2,-1,0,0)}_{A} + t\underbrace{\left(\frac{3}{2}, 1, -\frac{3}{2}, 1\right)}_{u} \mid t \in \mathbb{K}\}
\end{aligned}$$

Exemple :

$$\begin{cases} x+y+z=0 \\ x-y+z=1 \\ 2x-y+z=2 \\ x-y-z=3 \\ y+3z=1 \end{cases}$$

$$\begin{array}{c} \iff \\ L_2 \leftarrow \dfrac{L_2-L_1}{-2} \\ L_3 \leftarrow L_3-2L_1 \\ L_4 \leftarrow L_4-L_1 \end{array} \begin{cases} \boxed{x}+y+z=0 \\ \boxed{y}=\dfrac{1}{2} \\ -3y-z=2 \\ -2y-2z=3 \\ y+3z=1 \end{cases}$$

$$\begin{array}{c} \iff \\ L_1 \leftarrow L_1-L_2 \\ L_3 \leftarrow -(L_3-3L_2) \\ L_4 \leftarrow L_4+3L_2 \\ L_5 \leftarrow L_5-L_2 \end{array} \begin{cases} \boxed{x}+z=\dfrac{1}{2} \\ \boxed{y}=-\dfrac{1}{2} \\ \boxed{z}=-\dfrac{1}{2} \\ -2z=2 \\ 3z=\dfrac{3}{2} \end{cases}$$

$$\begin{array}{c} \iff \\ L_1 \leftarrow L_1-L_3 \\ L_4 \leftarrow L_4+2L_3 \\ L_5 \leftarrow L_5-3L_3 \end{array} \begin{cases} \boxed{x}=1 \\ \boxed{y}=-\dfrac{1}{2} \\ \boxed{z}=-\dfrac{1}{2} \\ \boxed{\begin{array}{l} 0=1 \\ 0=3 \end{array}} \end{cases} \text{ incompatibilité}$$

Il n'y a pas de solution !

Exemple :

$$(S_2): \begin{cases} \boxed{x}+y-z=1 \\ y+z=0 \\ x+2y=0 \end{cases}$$

$$\begin{array}{c} \iff \\ L_3 \leftarrow L_3-L_1 \end{array} (S_2'): \begin{cases} \boxed{x}+y-z=1 \\ \boxed{y}+z=0 \\ y+z=-1 \end{cases}$$

$$\begin{array}{c} \iff \\ L_1 \leftarrow L_1-L_2 \\ L_3 \leftarrow L_3-L_2 \end{array} \begin{cases} \boxed{x}-2z=1 \\ \boxed{y}+z=0 \\ \boxed{0=-1} \end{cases}$$

Exemple :

$$(S_1) \iff \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & -1 & 1 \\ 1 & -1 & -1 \\ 0 & 1 & 3 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x \\ y \\ z \end{pmatrix}}_{X} = \underbrace{\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 1 \end{pmatrix}}_{B}$$
$$\iff AX = B$$

$$(S_2) \iff \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}}_{A} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$(S_2') \iff \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{A'} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}}_{A} = \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{A'}$$

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}}_{\in \mathrm{GL}_3(\mathbb{K})} \underbrace{\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}}_{\in \mathrm{GL}_3(\mathbb{K})} A = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$A \in \mathrm{GL}_3(\mathbb{K}) \iff \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{K})$$

Exemple :

$$A = \begin{pmatrix} \boxed{1} & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$
\begin{array}{ll}
A & \\
\overset{\sim}{C_3 \leftarrow C_3 - C_1} & \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & \boxed{1} & -1 \end{pmatrix} \\
\overset{\sim}{C_1 \leftarrow C_1 - C_2} & \begin{pmatrix} \boxed{1} & 0 & 0 \\ -1 & 1 & \boxed{1} \\ 0 & \boxed{1} & 0 \end{pmatrix} \\
C_3 \leftarrow \dfrac{C_3 - C_2}{2} & \\
\overset{\sim}{C_1 \leftarrow C_1 + C_3} & \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & 0 & \boxed{1} \\ 0 & \boxed{1} & 0 \end{pmatrix} \\
C_2 \leftarrow C_2 - C_3 & \\
\overset{\sim}{C_2 \leftrightarrow C_3} & I_3
\end{array}
$$

$$
\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}
\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
=
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix}
$$

$$
I_3 = A \underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix}
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{B}
$$

$$
A \in \mathrm{GL}_3(\mathbb{K}) \text{ et } A^{-1} = I_3 \times B
$$

$$
\begin{array}{rl}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
C_3 \leftarrow C_3 - C_1 \overset{\sim}{} & \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\begin{array}{l} C_1 \leftarrow C_1 - C_2 \overset{\sim}{} \\ C_3 \leftarrow \dfrac{C_3 + C_2}{2} \end{array} & \begin{pmatrix} 1 & 0 & -\frac{1}{2} \\ -1 & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \\
\begin{array}{l} C_1 \leftarrow C_1 + C_3 \overset{\sim}{} \\ C_2 \leftarrow C_2 - C_3 \end{array} & \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \\
C_2 \leftrightarrow C_3 \overset{\sim}{} & \underbrace{\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}}_{A^{-1}}
\end{array}
$$

REMARQUE (Résumé) : — Méthode du pivot : opérations sur les lignes :

1. $L_i \leftarrow L_i + \lambda L_j$ ($\lambda \in \mathbb{K}$)
2. $L_i \leftarrow \mu L_i$ ($\mu \in \mathbb{K} \setminus \{0\}$)
3. $L_i \leftrightarrow L_j$

En appliquant la méthode du pivot on obtient

$$
(S) \iff \begin{cases} x_{i_1} & = \ell_1(x_{j_1}, \ldots, x_{j_n - r}) \\ x_{i_2} & = \ell_2(x_{j_1}, \ldots, x_{j_n - r}) \\ \vdots & \vdots \\ x_{i_r} & = \ell_r(x_{j_1}, \ldots, x_{j_n - r}) \\ 0 & = \star \end{cases}
$$

Les inconnues $x_{i_1}, \ldots, x_{i_r}$ sont les inconnues principales, les autres sont appelées paramètre.
On peut supprimer les équations $0 = 0$. S'il y a une équation $0 = \lambda$ avec $\lambda \neq 0$, il n'y a pas de solution : le système est incompatible.
Les inconnues principales dépendent des choix de pivots !

— Représentation matricielle

$$
(S) \iff AX = B
$$

où A est la matrice du système, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ et B est le second membre

(S) a n équations et p inconnues donc A a n lignes et p colonnes.
La matrice $(A \mid B)$ est la matrice augmentée du système.

— Faire un opération L sur les lignes d'une matrice M revient à multiplier M à gauche par une matrice R où R est obtenue en appliquant L sur I_n.

— La méthode du pivot matriciel par lignes :

Exemple :

$$A = \begin{pmatrix} 5 & 1 & 4 & 4 \\ 2 & 1 & 0 & 0 \\ 7 & 2 & 3 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 5 & \boxed{1} & 3 & 4 \\ 2 & 1 & 0 & 0 \\ 7 & 2 & 3 & 4 \end{pmatrix} \underset{\substack{L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_3 - 2L_1}}{\sim} \begin{pmatrix} 5 & \boxed{1} & 3 & 4 \\ -3 & 0 & -3 & -4 \\ -3 & 0 & -3 & -4 \end{pmatrix}$$

$$\underset{L_2 \leftarrow -\frac{1}{3}L_2}{\sim} \begin{pmatrix} 5 & \boxed{1} & 3 & 4 \\ \boxed{1} & 0 & 1 & \frac{4}{3} \\ -3 & 0 & -3 & -4 \end{pmatrix}$$

$$\underset{\substack{L_1 \leftarrow L_1 - 5L_2 \\ L_3 \leftarrow L_3 + 3L_2}}{\sim} \begin{pmatrix} 0 & \boxed{1} & -2 & -\frac{8}{3} \\ \boxed{1} & 0 & 1 & \frac{4}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\underset{L_1 \leftrightarrow L_2}{\sim} \underbrace{\begin{pmatrix} \boxed{1} & 0 & 1 & 4/3 \\ 0 & \boxed{1} & -2 & -8/3 \\ 0 & 0 & 0 & 0 \end{pmatrix}}_{\text{matrice échelonnée réduite par lignes}}$$

Définition (Rang d'une matrice) **:** Soit M une matrice et R la matrice échelonnée réduite par lignes associée à M. Le nombre de lignes non nulles de R (le nombre de pivots) est appelée rang de M.
Soit S un système de matrice augmentée $(A \mid B)$. Le rang de S est le rang de la matrice A.
Le rang est noté rg.

Proposition (Interprétation) **:**

— Soit S un système de n équations, p inconnues de rang r.
r est le nombre d'inconnues principales, il y a $p - r$ paramètres.

— Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$ de rang r.
r est le nombre de lignes indépendantes : il y a $n - r$ lignes

combinaisons linéaires des r lignes indépendantes.

Corollaire : Soit S un système de n équations, p inconnues de rang n.
Alors S a au moins une solution.
Si $n = p$ alors S a exactement une solution.
Si $p > n$, il y a une infinité de solutions.

□

Définition : Soit S un système à n équations, n inconnues et de rang n.
On dit que S est un système de Cramer (il a une unique solution)

Proposition : Soit S un système de n équations, p inconnues de rang r.

- Si $r < n$ alors le système peut-être incompatible : il y a $n-r$ équations de la forme $0 = \star$ après la méthode du pivot.
- Si $r < p$ alors il y a $p - r$ paramètres : si le système n'est pas incompatible, il y aura une infinité de solutions.

□

Exemple :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & \boxed{1} & 2 \\ 1 & 1 & 1 \end{pmatrix} \overset{\substack{L_1 \leftarrow L_1 - 2L_2 \\ L_3 \leftarrow L_3 + L_2}}{\sim} \begin{pmatrix} -9 & 0 & -1 \\ 5 & \boxed{1} & 2 \\ 4 & 0 & \boxed{1} \end{pmatrix}$$

$$\overset{L_1 \leftarrow L_1 + L_3}{\sim} \begin{pmatrix} \boxed{-5} & 0 & 0 \\ 5 & \boxed{1} & 2 \\ 4 & 0 & \boxed{1} \end{pmatrix}$$

$$\overset{L_1 \leftarrow -L_1/5}{\sim} \begin{pmatrix} \boxed{1} & 0 & 0 \\ 5 & \boxed{1} & 2 \\ 4 & 0 & \boxed{1} \end{pmatrix}$$

$$\overset{\substack{L_2 \leftarrow L_2 - 5L_1 \\ L_3 \leftarrow L_3 - 4L_1 \\ L_2 \leftarrow L_2 + 2L_3}}{\sim} \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & \boxed{1} & 0 \\ 0 & 0 & \boxed{1} \end{pmatrix}$$

Exemple :

$$(S) : \begin{cases} x+y+z+t=1 \\ x-y+z+2t=0 \\ 2y-t=1 \\ 2x+2z+3t=1 \end{cases}$$

$$\begin{cases} \boxed{x}+y+z+t=1 \\ x-y+z+2t=0 \\ 2y-t=1 \\ 2x+2z+3t=1 \end{cases} \underset{\substack{L_2 \leftarrow L_2 - L_1 \\ L_4 \leftarrow L_4 - 2L_1}}{\iff} \begin{cases} \boxed{x}+y+z+t=1 \\ -2y+\boxed{t}=-1 \\ 2y-t=1 \\ -2y+t=-1 \end{cases}$$

$$\underset{\substack{L_3 \leftarrow L_3 + L_2 \\ L_4 \leftarrow L_4 - L_2}}{\iff} \boxed{\begin{cases} \boxed{x}+y+z+t=1 \\ -2y+\boxed{t}=-1 \\ 0=0 \\ 0=0 \end{cases}} \text{ Système triangulaire}$$

$$\iff \begin{cases} t=-1+2y \\ x=2-3y-z \end{cases}$$

La matrice du système triangulaire est

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Elle n'est pas échelonnée réduite par lignes !

Proposition : Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et C une opération élémentaire sur les colonnes de A. On pose A' la matrice obtenue en appliquant C sur les colonnes de A.

$$\operatorname{rg}(A) = \operatorname{rg}(A')$$

□

Exemple :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & 1 & 2 \\ \boxed{1} & 1 & 1 \end{pmatrix} \underset{\substack{C_2 \leftarrow C_2 - C_1 \\ C_3 \leftarrow C_3 - C_1}}{\sim} \begin{pmatrix} 1 & \boxed{1} & 2 \\ 5 & -4 & -3 \\ \boxed{1} & 0 & 0 \end{pmatrix}$$

$$\underset{C_3 \leftarrow C_3 - 2C_2}{\sim} \begin{pmatrix} 1 & \boxed{1} & 0 \\ 5 & -4 & \boxed{5} \\ \boxed{1} & 0 & 0 \end{pmatrix}$$

Donc $\mathrm{rg}(A) = 3$

Exemple :

$$\mathrm{rg}\left(\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right) = 1$$

Proposition : Le rang d'une matrice est aussi le nombre de colonnes indépendantes. □

Définition : Une matrice triangulaire supérieure est une matrice carrée avec des coefficients nuls sous sa diagonale :

$$T = \begin{pmatrix} \star & \cdots & \star \\ & \ddots & \vdots \\ 0 & & \star \\ \vdots & \ddots & \\ 0 & \cdots & 0 \end{pmatrix}$$

et triangulaire inférieure si les coefficients au-dessus de la diagonale sont nuls :

$$T = \begin{pmatrix} \star & & 0 \\ \vdots & \ddots & \\ & & 0 \\ \vdots & \ddots & \\ \star & \cdots & \star \end{pmatrix}$$

Un système triangulaire est de la forme

$$\begin{cases} a_{11}x_1 & +a_{12}x_2 & +\ldots & +a_{1p}x_p & = & b_1 & +\ldots \\ & +a_{22}x_2 & +\ldots & +a_{2p}x_p & = & b_2 & +\ldots \\ & & \ddots & & \vdots & & \\ & & & a_{pp}x_p & = & b_p & +\ldots \\ & & & 0 & = & \ldots & \end{cases}$$

Remarque :

$$(S) \iff \begin{cases} AX = B \\ X \in \mathcal{M}_{p,1}(\mathbb{K}), B \in \mathcal{M}_{n,1}(\mathbb{K}), A \in \mathcal{M}_{n,p}(\mathbb{K}) \end{cases}$$

On pose

$$\begin{aligned} \varphi : \mathcal{M}_{p,1}(\mathbb{K}) &\longrightarrow \mathcal{M}_{n,1}(\mathbb{K}) \\ X &\longmapsto AX \end{aligned}$$

On cherche $\varphi^{-1}(\{B\})$

On sait que

- $(\mathcal{M}_{p,1}(\mathbb{K}), +)$ est un groupe
- $(\mathcal{M}_{n,1}(\mathbb{K}), +)$ aussi

Soient $X, Y \in \mathcal{M}_{p,1}(\mathbb{K})$

$$\varphi(X+Y) = A(X+Y) = AX + AY = \varphi(X) + \varphi(Y)$$

Donc φ est un morphisme de groupes.
On peut résoudre (S) de la façon suivante :

- On cherche $X_0 \in \mathcal{M}_{p,1}(\mathbb{K})$ tel que $\varphi(X_0) = B$
- On résout $\varphi(X) = 0$ $(X \in \mathrm{Ker}(\varphi))$

C'est le système homogène associé :

$$\varphi(X) = B \iff \exists H \in \mathrm{Ker}(\varphi), X = X_0 + H$$

Proposition :

$$A = (a_{i,j})_{\substack{1 \leqslant j \leqslant n \\ 1 \leqslant j \leqslant p}} \in \mathcal{M}_{n,p}(\mathbb{K})$$
$$B = (b_{k,\ell})_{\substack{1 \leqslant k \leqslant p \\ 1 \leqslant \ell \leqslant q}} \in \mathcal{M}_{p,q}(\mathbb{K})$$

$$AB = (c_{i,\ell})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant \ell \leqslant q}} \in \mathcal{M}_{n,q}(\mathbb{K})$$
$$c_{i,\ell} = \sum_{j=1}^{n} = a_{i,j} b_{j,\ell}$$

Chapitre 14

Continuité

1 Définition d'une limite de fonctions

Définition : Soit $a \in \overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$ et $V \in \mathcal{P}(\mathbb{R})$.

1. Si $a \in \mathbb{R}$, on dit que V est un voisinage si
$$\exists \eta > 0,\ ]a - \eta, a + \eta[\subset V.$$

2. Si $a = +\infty$, on dit que V est un voisinage de a si
$$\exists M \in \mathbb{R},\ ]M, +\infty[\subset V.$$

3. Si $a = -\infty$, on dit que V est un voisinage de a si
$$\exists m \in \mathbb{R},\ ]-\infty, m[\subset V.$$

On note $\mathcal{V}_a$ l'ensemble des voisinages de a.

L'utilisation des voisinages permet d'exprimer une limite finie ou infinie plus simplement, sans disjonction de cas.

Exemple :
Soit $u \in \mathbb{R}^{\mathbb{N}}$ de limite $a \in \overline{\mathbb{R}}$.

— Si $a \in \mathbb{R}$,

$$\begin{aligned} &\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ |u_n - a| \leqslant \varepsilon \\ \text{i.e. } &\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ a - \varepsilon \leqslant u_n \leqslant a + \varepsilon \\ \text{i.e. } &\forall V \in \mathscr{V}_a,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \in V. \end{aligned}$$

— Si $a = +\infty$,

$$\begin{aligned} &\forall M \in \mathbb{R},\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \geqslant M \\ \text{i.e. } &\forall M \in \mathbb{R},\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \in [M, +\infty[\\ \text{i.e. } &\forall V \in \mathscr{V}_a,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \in V. \end{aligned}$$

— Si $a = -\infty$,

$$\begin{aligned} &\forall m \in \mathbb{R},\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \leqslant m \\ \text{i.e. } &\forall m \in \mathbb{R},\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \in]-\infty, m] \\ \text{i.e. } &\forall V \in \mathscr{V}_a,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \in V. \end{aligned}$$

Même si, dans chacun des cas, la définition de limite de la suite u est différente, en utilisant les voisinages, la notation est identique :

$$\forall V \in \mathscr{V}_a,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ u_n \in V.$$

En utilisant cette nouvelle notation, on peut redéfinir la limite plus simplement.

Définition : Soit f une fonction définie sur $D \subset \mathbb{R}$ à valeurs réelles. Soit $a \in \overline{D} = \{x \in \overline{\mathbb{R}} \mid \forall V \in \mathscr{V}_x,\ V \cap D \neq \}$ (on "rajoute" chacune des bornes exclues des intervalles composant D) :

On dit que $f(x)$ tends vers ℓ si

$$\forall V \in \mathscr{V}_\ell,\ \exists W \in \mathscr{V}_a,\ \forall x \in W \cap D,\ f(x) \in V.$$

Exemple :
Soit $f : \mathbb{R} \to \mathbb{R}$ telle que $f(x) \xrightarrow[x \to -1]{} 1$.

$$\forall V \in \mathscr{V}_1,\ \exists W \in \mathscr{V}_{-1},\ \forall x \in W,\ f(x) \in V$$

donc

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in\ ]-1-\eta, -1+\eta[,\ f(x) \in [1-\varepsilon, 1+\varepsilon[$$

i.e.

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in \mathbb{R},\ \big(|x-(-1)| < \eta \implies |f(x)-1| \leqslant \varepsilon\big).$$

Si $f(x) \xrightarrow[x \to -\infty]{} +\infty$,

$$\forall V \in \mathscr{V}_{+\infty},\ \exists W \in \mathscr{V}_{-\infty},\ \forall x \in W,\ f(x) \in V$$

i.e.

$$\forall M \in \mathbb{R},\ \exists m \in \mathbb{R},\ \forall x \in]-\infty, m],\ f(x) \in [M, +\infty[$$

i.e.

$$\forall M \in \mathbb{R},\ \exists m \in \mathbb{R},\ \forall x \in \mathbb{R},\ \big(x \leqslant m \implies f(x) \geqslant M\big).$$

Définition : Soit $a \in \mathbb{R}$.

Un voisinage à gauche de a est une partie de $\mathbb{R}$ qui contient un inveralle $]a-\eta, a]$ avec $\eta > 0$.

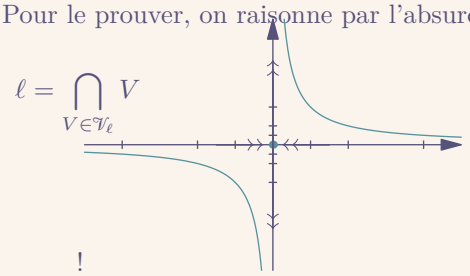
Un voisinage à droite de a est une partie de $\mathbb{R}$ qui contient un inveralle $[a, a+\eta[$ avec $\eta > 0$.

Exemple :

Soit $f : x \mapsto \begin{cases} \dfrac{1}{x} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases}$

1. $\lim\limits_{x \to 0} f(x)$ *existe ? Si oui, que vaut elle ?*
2. $\lim\limits_{\substack{x \to 0 \\ \leqslant}} f(x)$ *existe ? Si oui, que vaut elle ?*

Réponse : $\lim\limits_{x \to 0} f(x)$ n'existe pas. Pour le prouver, on raisonne par l'absurde.



Si ℓ existe, alors $\ell = f(0)$.
Or, $0 \neq \lim\limits_{x \to 0} f(x)$

Proposition : Si f admet une limite finie en $a \in I$, alors cette limite vaut $f(a)$.

Preuve :
Soit $\ell = \lim\limits_{x \to a}$ et $a \in \mathscr{D}$.

On sait que

$$\forall V \in \mathscr{V}_\ell, \exists W \in \mathscr{V}_a, \forall x \in W \cap \mathscr{D}, f(x) \in V.$$

Soit $V \in \mathscr{V}_\ell$. Alors, $f(a) \in V$.

$$f(a) \in \bigcap_{V \in \mathscr{V}_\ell} V = \begin{cases} \{\ell\} & \text{si } \ell \in \mathbb{R}, \\ & \text{si } \ell = \pm\infty. \end{cases}$$

Donc $\ell \in \mathbb{R}$ et $\ell = f(a)$. □

REMARQUE :
De même si $a \in \mathcal{D}$ et si $\lim\limits_{\substack{x\to a\\ \leqslant}} f(x)$ existe (resp. $\lim\limits_{\substack{x\to a\\ \leqslant}} f(x)$) alors $f(a) = \lim\limits_{\substack{x\to a\\ \leqslant}} f(x)$
(resp $f(a) = \lim\limits_{\substack{x\to a\\ \geqslant}} f(x)$)

EXEMPLE :
$\lim\limits_{x\to 0} \delta(x)$ n'existe pas
$\lim\limits_{x\to 0^+} \delta(x)$ et $\lim\limits_{x\to 0^-}$ n'existent pas non plus.

$\lim\limits_{\substack{x\to 0\\ \neq}} \delta(x)$

$\lim\limits_{\substack{x\to 0\\ <}} \delta(x) = 0,\ \lim\limits_{\substack{x\to 0\\ >}} \delta(x) = 0$

$$\lim_{x\to a} \frac{f(x)-f(a)}{x-a} = \lim_{\substack{x\to a\\ \neq}} \frac{f(x)-f(a)}{x-a}$$

Définition : Soit f définie sur D et $a \in D$. On dit que f est continue en a si $\lim\limits_{x\to a} f(x)$ existe ou si $\lim\limits_{\substack{x\to a\\ \neq}} f(x) = f(a)$.

EXEMPLE :
Soit $f : x \mapsto \begin{cases} \dfrac{\sin(x)}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases}$

$\lim\limits_{\substack{x\to 0\\ \neq}} f(x) = \lim\limits_{x\to 0} \dfrac{\sin(x)}{x} = 1 = f(0)$
Donc f est continue en 0.

Proposition : f est continue en a si et seulement si

$$\lim_{\substack{x\to a\\ <}} f(x) = \lim_{\substack{x\to a\\ >}} = f(a)$$

Preuve (unicité de la limite) *:*
On suppose que $f(x) \xrightarrow[x\to u]{} a$, $f(x) \xrightarrow[x\to u]{} b$ avec $a \neq b$.

Soient V et W conne dans le lemme (suivant),

$$\begin{cases}\exists W_1 \in \mathcal{V}_u, \forall x \in W_1 \cap \mathcal{D}, f(x) \in V \\ \exists W_2 \in \mathcal{V}_u, \forall x \in W_2 \cap \mathcal{D}, f(x) \in W\end{cases}$$

Donc

$$\forall x \in \underbrace{W_1 \cap W_2 \cap \mathcal{D}}_{\neq \text{ car } W_1 \cap W_2 \in \mathcal{V}_u} f(x) \in V \cap W =$$

□

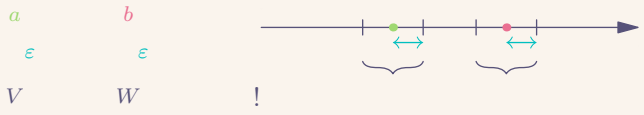
Lemme : Soient $a \neq b$ deux éléments de $\overline{\mathbb{R}}$
Alors $\exists V \in \mathcal{V}_a, \exists W \in \mathcal{V}_b, V \cap W =$

*Preuve*Cas 1 $(a, b) \in \mathbb{R}^2$. On suppose que $a < b$.

On pose $\varepsilon = \dfrac{b-a}{2}$,

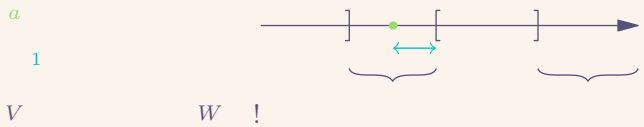
$$\begin{cases}V =]a - \varepsilon; a + \varepsilon[\\ W =]b - \varepsilon; b + \varepsilon[\end{cases}$$

On vérifie que $V \cap W =$



Cas 2 $a \in \mathbb{R}$ et $b = +\infty$

$$\begin{cases}V =]a - 1; a + 1[\\ W =]a + 2; +\infty[\end{cases}$$



Cas 3 $a = -\infty$, $b = +\infty$

$$\begin{cases}V =]-\infty; 0[\\ W =]0; +\infty[\end{cases}$$

□

Théorème : Soit f définie sur $\mathscr{D}$ et $a \in \overline{\mathscr{D}}$, $\ell \in \overline{\mathbb{R}}$

$$f(x) \xrightarrow[x\to a]{} \ell \iff \forall (x_n) \in \mathscr{D}^{\mathbb{N}} \left(x_n \xrightarrow[n\to+\infty]{} a \implies f(x_n) \xrightarrow[n\to+\infty]{} \ell \right)$$

Preuve “ $\implies$ ” On suppose que $f(x) \xrightarrow[x\to a]{} \ell$.

Soit $(x_n) \in \mathscr{D}^{\mathbb{N}}$ telle que $x_n \xrightarrow[n\to+\infty]{} \ell$

Soit $V \in \mathscr{V}_\ell$. Soit $W \in \mathscr{V}_a$ tel que

$$\forall x \in W \cap \mathscr{D}, f(x) \in V$$

$x_n \xrightarrow[n\to+\infty]{} a$ donc il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, x_n \in W \cap \mathscr{D}$$

Donc

$$\forall n \geqslant N, f(x_n) \in V$$

D'où, $f(x_n) \xrightarrow[n\to+\infty]{} \ell$

“ $\impliedby$ ” On suppose que $f(x) \not\xrightarrow[x\to a]{} \ell$

$$\exists V \in \mathscr{V}_\ell, \forall W \in \mathscr{V}_a, \exists x \in W \cap \mathscr{D}, f(x) \notin V$$

Soit V comme ci dessus. Soit $W_1 \in \mathscr{V}_a$.

Cas 1 $a \in \mathscr{D}$ et $\forall x \in W \cap \mathscr{D} \setminus \{a\}, f(x) \in V$.

On le prouve par la contraposée. On suppose $f(x) \not\xrightarrow[x\to a]{} \ell \in \mathbb{R}$

Donc,

$$\exists \varepsilon > 0, \forall \eta > 0, \exists x \in]a-\eta, a+\eta[, |f(x) - \ell| > \varepsilon$$

On considère un tel ε donc

$$\forall n \in \mathbb{N}_\star, \exists x_n \in \left]a - \frac{1}{n}, a + \frac{1}{n}\right[, |f(x_n) - \ell| > \varepsilon$$

Par encadrement, $x_n \xrightarrow[n\to+\infty]{} a$ et $f(x_n) \not\xrightarrow[n\to+\infty]{} \ell$

Cas 2 Soit $x_1 \in W_1 \cap \mathscr{D}$ tel que $f(x_1) \notin V$

$\begin{cases} x_1 \in \mathscr{D} \\ a \notin \mathscr{D} \end{cases}$ donc $x_1 \neq a$

Cas 3 $\exists x \in W_1 \cap \mathcal{D} \setminus \{a\}, f(x) \notin V$
Soit x_1 un tel élément :

$$x_1 \in W_1 \cap \mathcal{D}$$
$$x_1 \neq a$$
$$f(x_1) \notin V$$

Dans les cas 2 et 3, on pose $W_2 \in \mathcal{V}_a$ tel que

$$W_2 \subset W_1 \setminus \{x_1\}$$

En itérant ce procédé, on construit une suite (x_n) qui tend vers a et telle que

$$\forall n \in \mathbb{N}, f(x_n) \notin V$$

et donc $f(x_n) \xrightarrow[n\to+\infty]{\not\longrightarrow} \ell$

□

Proposition : Si $f(x) \xrightarrow[x\to a]{} \ell$ et $g(x) \xrightarrow[x\to a]{} \ell_2$
alors

1. $f(x) + g(x) \xrightarrow[x\to a]{} \ell_1 + \ell_2$
2. $f(x) \times g(x) \xrightarrow[x\to a]{} \ell_1 \times \ell_2$
3. Si $\ell_2 \neq 0$, $\dfrac{f(x)}{g(x)} \xrightarrow[x\to a]{} \dfrac{\ell_1}{\ell_2}$

Preuve : 1. Soit (x_n) une suite qui tends vers a alors $f(x_n) \xrightarrow[n\to+\infty]{} \ell_1$ et $g(x_n) \xrightarrow[n\to+\infty]{} \ell_2$
Donc, $f(x_n) + g(x_n) \xrightarrow[n\to+\infty]{} \ell_1 + \ell_2$
Donc $f(x) + g(x) \xrightarrow[n\to+\infty]{} \ell_1 + \ell_2$

□

Proposition : Si $f(x) \xrightarrow[x\to a]{} \ell_1$ et $g(x) \xrightarrow[x\to \ell_1]{} \ell_2$ alors $g(f(x)) \xrightarrow[x\to a]{} \ell_2$

Preuve :
Soit (x_n) une suite qui tend vers a. Alors, $f(x_n) \xrightarrow[n\to+\infty]{} \ell_1$ donc $g(f(x_n)) \xrightarrow[n\to+\infty]{} \ell_2$ donc $g(f(x)) \xrightarrow[x\to a]{} \ell_2$ □

Corollaire : Une somme, un produit, une composée de fonctions continues sont continues. □

Remarque :
Pour démontrer que $f(x)$ n'a pas de limite quands x tend vers a. On cherche deux suites (x_n) et (y_n) de limite a avec

$$\begin{cases} f(x_n) \longrightarrow \ell_1 \\ f(y_n) \longrightarrow \ell_2 \\ \ell_1 \neq \ell_2 \end{cases}$$

Exemple :

$$\forall n \in \mathbb{N}, \sin(2\pi n) = 0 \xrightarrow[n\to+\infty]{} 0$$
$$\sin\left(\frac{\pi}{2} + 2\pi n\right) = 1 \xrightarrow[n\to+\infty]{} 1$$

Or,

$$2\pi n \xrightarrow[n\to+\infty]{} +\infty$$
$$\frac{\pi}{2} + 2\pi n \xrightarrow[n\to+\infty]{} +\infty$$

Donc, sin n'a pas de limite en $+\infty$

Théorème (Limite monotone) **:** Soit f une fonction croissante sur $]a, b[$ avec $a \neq b \in \overline{\mathbb{R}}$.

1. Si f est majorée,
$$\exists M \in \mathbb{R}, \forall x \in]a, b[, f(x) \leqslant M$$
alors $\lim\limits_{\substack{x\to b \\ <}} f(x) = \sup\limits_{x\in]a,b[} f(x) \in \mathbb{R}$
2. Si f n'est pas majorée,
$$\lim_{\substack{x\to b \\ <}} f(x) = +\infty$$
3. Si f est minorée,
$$\exists m \in \mathbb{R}, \forall x \in]a, b[, f(x) \leqslant m$$
alors $\lim\limits_{\substack{x\to a \\ >}} f(x) = \inf\limits_{]a,b[} f \in \mathbb{R}$

4. Si f n'est pas minorée, $\lim\limits_{\substack{x\to a\\ >}} f(x) = -\infty$

Preuve : 1. $\sup\limits_{]a,b[} f$ existe

$$\forall \varepsilon > 0, \exists x \in]a,b[, f(x) > \sup_{]a,b[}(f) - \varepsilon$$

donc

$$\forall \varepsilon > 0, \exists x \in]a,b[, \forall y \in [x,b[, \sup_{]a,b[}(f) - \varepsilon < f(y) \leqslant \sup_{]a,b[}(f) < \sup_{]a,b[}(f) + \varepsilon$$

donc $f(x) \underset{\substack{x\to b\\ <}}{\longrightarrow} \sup\limits_{]a,b[}(f)$

2. f n'est pas majorée

$$\forall M \in \mathbb{R}, \exists x \in]a,b[, f(x) > M$$

donc

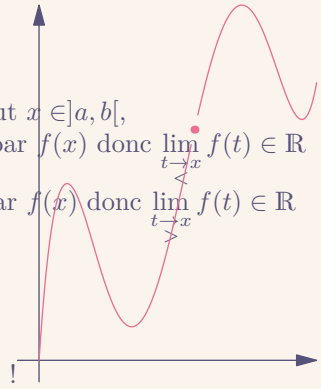
$$\forall M \in \mathbb{R}, \exists x \in]a,b[, \forall y \in [x,b[, f(y) \in [M, +\infty[$$

□

Remarque :
Avec les hypothèses ci-dessus, pour tout $x \in]a,b[$,
f est croissante sur $]a,x[$, et majorée par $f(x)$ donc $\lim\limits_{\substack{t\to x\\ <}} f(t) \in \mathbb{R}$

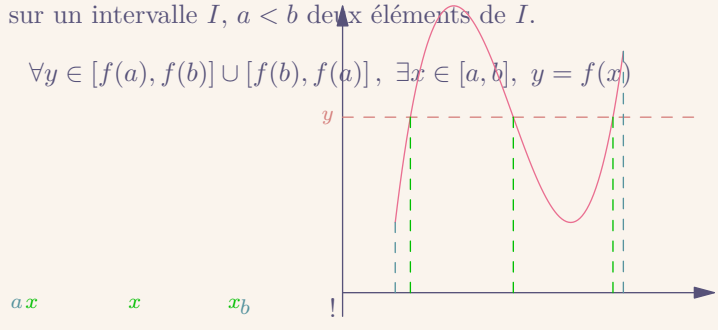
f est croissante sur $]x,b[$ et minorée par $f(x)$ donc $\lim\limits_{\substack{t\to x\\ >}} f(t) \in \mathbb{R}$

$\lim\limits_{\substack{t\to x\\ <}} f(t) \leqslant f(x) \leqslant \lim\limits_{\substack{t\to x\\ >}} f(t)$



Théorème (Théorème des valeurs intermédiaires) **:** Soit f une fonction continue sur un intervalle I, $a < b$ deux éléments de I.

$$\forall y \in [f(a), f(b)] \cup [f(b), f(a)], \ \exists x \in [a,b], \ y = f(x)$$



Lemme : Soit f une fonction continue sur un intervalle I, $a < b$ deux éléments de I tels que $f(a) \leqslant 0 \leqslant f(b)$. Alors,

$$\exists x \in [a,b], f(x) = 0$$

Preuve (du lemme) *:*
On pose $A = \{x \in [a,b] \mid f(x) \leqslant 0\}$
$A \neq$ car $a \in A$ et A est majorée par b.
On pose $u = \sup(A)$. Soit $(x_n) \in A^{\mathbb{N}}$ qui converge vers u.
$\forall n \in \mathbb{N}, x_n \in A$ donc $\forall n \in \mathbb{N}, \begin{cases} a \leqslant x_n \leqslant b \\ f(x_n) \leqslant 0 \end{cases}$
On sait que $x_n \longrightarrow u$ et $f(x_n) \longrightarrow f(u)$ par continuité de f.
Donc, $\begin{cases} a \leqslant u \leqslant b \\ f(u) \leqslant 0 \end{cases}$ (donc $u = \max(A)$)
De plus,

$$\forall x \in]u,b], f(x) > 0$$

donc

$$\begin{cases} \lim\limits_{\substack{x \to u \\ >}} f(x) = f(u) \\ \\ \lim\limits_{\substack{x \to u \\ >}} f(x) \geqslant 0 \end{cases}$$

Donc, $f(u) \geqslant 0$ donc $f(u) = 0$

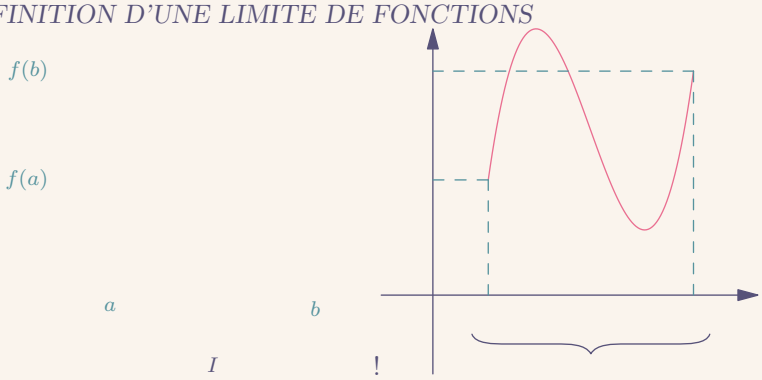
□

Preuve (du théorème) *:*
On pose $g : x \mapsto f(x) - y$. g est continue sur I.

Si $f(a) < f(b)$ alors $\begin{cases} g(a) \leqslant 0 \\ g(b) \geqslant 0 \end{cases}$
D'après le lemme, il existe $x \in [a,b]$ tel que $g(x) = 0$ et donc $f(x) = y$

Si $f(a) < f(b)$ alors $\begin{cases} h(a) \leqslant 0 \\ h(b) \geqslant 0 \end{cases}$ où $h : x \mapsto -g(x) = y - f(x)$ est continue
D'après le lemme, il existe $x \in [a,b]$ tel que $h(x) = 0$ et donc $f(x) = y$ □

Corollaire : Soit f continue sur un intervalle I. Alors, $f(I)$ est un intervalle.



Preuve :
Montrons que $f(I)$ est convexe
Soit $\alpha \in f(I), \beta \in f(I)$ avec $\alpha < \beta$. Montrons que

$$\forall \gamma \in [\alpha, \beta], f(\gamma) \in f(I)$$

Or, $\begin{cases} \alpha \in f(I) & \exists a \in I, \alpha = f(a) \\ \beta \in f(I) & \exists b \in I, \beta = f(b) \end{cases}$
D'après le théorème des valeurs intermédiaires, il existe $x \in [a, b]$ tel que $\gamma = f(x)$ donc, $f(\gamma) \in f(I)$ □

Corollaire : On peut généraliser le théorème des valeurs intermédiaires au cas où $\begin{cases} a \in \overline{R} \\ b \in \overline{\mathbb{R}} \end{cases}$ en remplaçant $f(a)$ par $\lim\limits_{\substack{x \to a \\ >}} f(x)$ et $f(b)$ par $\lim\limits_{\substack{x \to b \\ <}} f(x)$

□

Théorème (Théorème de la bijection) **:** Soit f continue, strictement monotone sur un intervalle I. Alors, $J = f(I)$ est un intervalle de même nature (ouvert, semi-ouvert ou fermé) et f établit une bijection de I sur J.

Preuve :
D'après le théorème des valeurs intermédiaires, J est un intervalle. f est strictement monotone donc f injective. Donc f établit une bijection de I sur J.

Cas 1 $I = [a, b]$ et f croissante
$\forall x \in I, a \leqslant x \leqslant b$
donc $\forall x \in I, f(a) \leqslant f(x) \leqslant f(b)$
donc $J \subset [f(a), f(b)]$

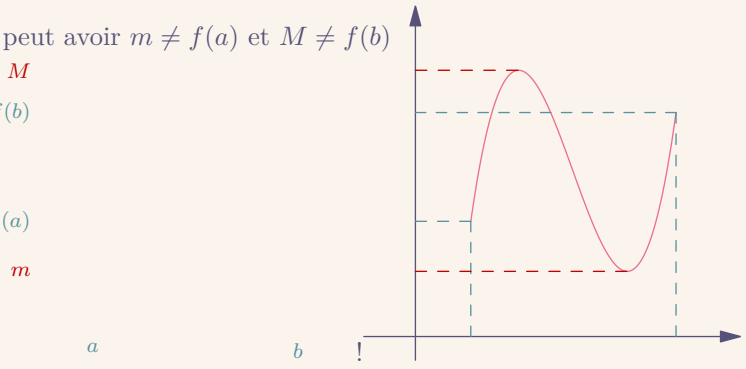
Or, $[f(a), f(b)] \subset J$ d'après le théorème des valeurs intermédiaires
Donc $J = [f(a), f(b)]$

Les autres cas se démontrent de la même façon. □

Théorème : Soit f continue sur un segment $[a, b]$. Alors, f est bornée et atteint ses bornes, i.e.

$$\exists (m, M) \in \mathbb{R}^2, f([a, b]) = [m, M]$$

B On peut avoir $m \neq f(a)$ et $M \neq f(b)$



Preuve :
On suppose que f n'est pas majorée :

$$\forall M \in \mathbb{R}, \exists x \in [a, b], f(x) \geqslant M$$

En particulier,

$$\forall n \in \mathbb{N}, \exists x_n \in [a, b], f(x_n) \geqslant n$$

Donc, $f(x_n) \xrightarrow[n \to +\infty]{} +\infty$
La suite $(x_n)_{n \in \mathbb{N}}$ est minorée apr a et majorée par b donc bornée.
D'après le théorème de Bolzano-Weierstrass, il existe $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que $(x_{\varphi(n)})_{\in \mathbb{N}}$ converge. On pose $\ell = \lim\limits_{n \to +\infty} x_{\varphi(n)}$. On a bien $\ell \in [a, b]$ et $f(\ell) = \lim\limits_{n \to +\infty} f\left(x_{\varphi(n)}\right)$ par continuité de f.
Or, $\left(f\left(x_{\varphi(n)}\right)\right)_{n \in \mathbb{N}}$ est une sous-suite de $(f(x_n))$ donc $f\left(x_{\varphi(n)}\right) \xrightarrow[n \to +\infty]{}$ $+\infty$: une contradiction
Donc f est majorée et on pose

$$M = \sup_{a \leqslant x \leqslant b} f(x)$$

On prouve de même que f est minorée. On pose donc

$$m = \inf_{a \leqslant x \leqslant b} f(x)$$

Soit $(y_n) \in [a,b]^{\mathbb{N}}$ telle que $f(y_n) \xrightarrow[n\to+\infty]{} M$.
(y_n) est bornée donc il existe une sous-suite $\left(y_{\psi(n)}\right)$ de (y_n) convergente.
On pose $y = \lim\limits_{n\to+\infty} y_{\psi(n)} \in [a,b]$
Comme f continue sur y,

$$f(y) = \lim_{n\to+\infty} f\left(y_{\psi(n)}\right)$$

Or, $\left(f\left(y_{\psi(n)}\right)\right)$ est une sous-suite de $(f(y_n))$ donc

$$M = \lim_{n\to+\infty} f\left(y_{\psi(n)}\right)$$

Par unicité de la limite, $M = f(y)$
Donc, $M = \max\limits_{a\leqslant x\leqslant b} f(x)$. De même, $m \in f([a,b])$
Enfin, en posant $\begin{cases} M = f(y) & \text{avec } y \in [a,b] \\ m = f(z) & \text{avec } z \in [a,b] \end{cases}$, on obtient

$$[m,M] = [f(z), f(y)] \underbrace{\subset}_{\substack{\text{théorème des valeurs intermédiaires}}} f([a,b]) \underbrace{\subset}_{\substack{m \text{ minimum} \\ M \text{ maximum}}} [m,M]$$

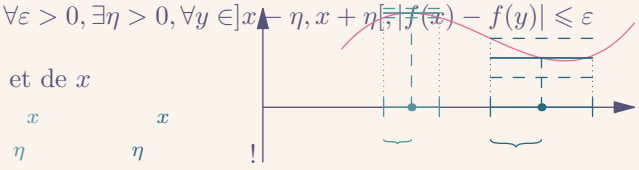
donc $f([a,b]) = [m,M]$ □

2 Continuité uniforme

Remarque :
$f : \mathbb{R} \to \mathbb{R}$ continue,

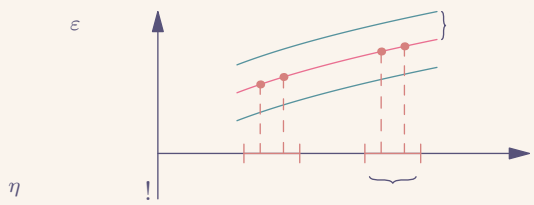
$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists \eta > 0, \forall y \in]x-\eta, x+\eta[, |f(x) - f(y)| \leqslant \varepsilon$$

Ici, η dépend de ε et de x



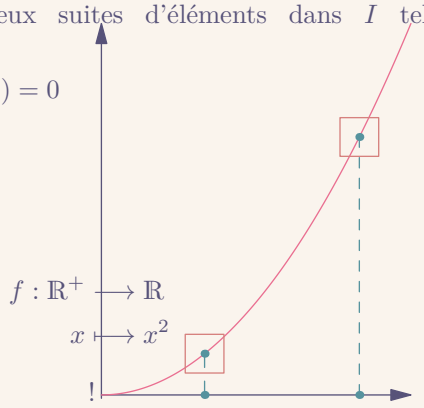
Dans certaines situations, il serait préférable d'avoir

$$\forall \varepsilon > 0, \exists \eta > 0, \forall (x,y) \in \mathbb{R}^2, |x-y| \leqslant \eta \implies |f(x) - f(y)| \leqslant \varepsilon$$



Lemme : Soit f uniformément continue sur un intervalle I. Soient $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}$ deux suites d'éléments dans I telles que $x_n - y_n \xrightarrow[n\to+\infty]{} 0$.
Alors, $\lim\limits_{n\to+\infty} (f(x_n) - f(y_n)) = 0$ □

EXEMPLE :



On pose $\forall n \in \mathbb{N}_\star, \begin{cases} x_n = n \\ y_n = n + \dfrac{1}{n} \end{cases}$. On a bien $\forall n \in \mathbb{N}_\star, x_n - y_n = \dfrac{1}{n} \xrightarrow[n\to+\infty]{} 0$.

$$\forall n \in \mathbb{N}_\star, {x_n}^2 - {y_n}^2 = n^2 - n^2 - \frac{1}{n^2} - 2 \xrightarrow[n\to+\infty]{} -2 \neq O$$

Donc, f n'est pas uniformément continue.

Théorème (Théorème de Heine) **:** Soit f une function continue sur $[a, b]$. Alors, f est uniformément continue sur $[a, b]$.

Preuve :
On suppose f continue sur $[a, b]$ mais pas uniformément continue.

$$\exists \varepsilon > 0, \forall \eta > 0, \exists (x, y) \in [a, b]^2 \text{ avec } |x - y| \leqslant \eta \text{ et } |f(x) - f(y)| > \varepsilon$$

Soit $\varepsilon > 0$ comme ci-dessus. Alors,

$$\forall n \in \mathbb{N}, \exists (x_n, y_n) \in [a, b]^2 \text{ avec } \left| x_n - y_n \leqslant \frac{1}{n+1} \right| \text{ et } |f(x_n) - f(y_n)| > \varepsilon$$

(x_n) est bornée donc il existe une sous-suite $\left(x_{\varphi(n)}\right)$ de (x_n) convergente. On note $\ell = \lim\limits_{n\to+\infty} x_{\varphi(n)} \in [a, b]$ $\left(y_{\varphi(n)}\right)$ est bornée, $\left(y_{\varphi(n)}\right)$ a une sous-suite $\left(y_{\varphi(\psi(n))}\right)$ convergente. On pose $\ell' = \lim\limits_{n\to+\infty} y_{\varphi(\psi(n))}$. $\left(x_{\varphi(\psi(n))}\right)_{n\in\mathbb{N}}$ est une autre sous-suite de $\left(x_{\varphi(n)}\right)$ donc $x_{\varphi(\psi(n))} \xrightarrow[n\to+\infty]{} \ell$.
De plus,

$$\forall n \in \mathbb{N}, \left|x_{\varphi(\psi(n))} - y_{\varphi(\psi(n))}\right| \leqslant \frac{1}{\varphi(\psi(n)) + 1}$$

On a vu que

$$\forall n \in \mathbb{N}, \varphi(\psi(n)) \geqslant n$$

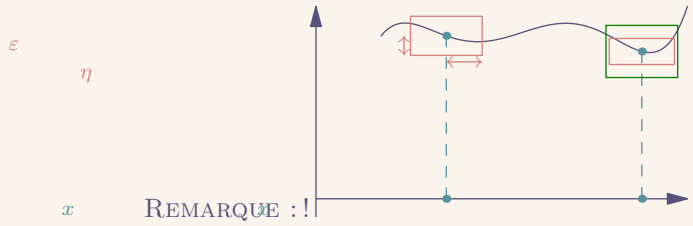
car $\varphi \circ \psi$ est strictement croissante à valeurs dans $\mathbb{N}$.
Donc, $x_{\varphi(\psi(n))} - y_{\varphi(\psi(n))} \xrightarrow[n\to+\infty]{} 0$.
On en déduit que $\ell - \ell' = 0$. De plus

$$\forall n \in \mathbb{N}, \left|f\left(x_{\varphi(\psi(n))}\right) - f\left(x_{\varphi(\psi(n))}\right)\right| > \varepsilon$$

En passant à la limite,

$$0 = |f(\ell) - f(\ell)| > \varepsilon > 0$$

car f continue en ℓ
On a obtenu une contradiction. $\lightning$ □



REMARQUE : !

$$\begin{cases} \eta > 0 \\ \varepsilon > 0 \end{cases}$$
$$\begin{cases} |x-y| \leqslant \eta \\ |f(x) - f(y)| \leqslant \varepsilon \end{cases}$$

Définition : Soit $f : I \to \mathbb{R}$ où I est un intervalle et $k \in \mathbb{R}$. On dit que f est k-lipschitzienne si

$$\forall (x,y) \in I^2, |f(x) - f(y)| \leqslant k\,|x-y|$$

On dit que f est lipschitzienne s'il existe $k \in \mathbb{R}$ tel que f soit k-lipschitzienne.

Proposition : Soit f une fonction lipschitzienne sur I. Alors, f est uniformément continue sur I donc continue sur I.

Preuve :
Soit $k \in \mathbb{R}$ tel que

$$\forall (x,y) \in I^2, |f(x) - f(y)| \leqslant k\,|x-y|$$

Soit $\varepsilon > 0$.
Si $k = 0$ alors f est constante donc uniformément continue.

On suppose $k \neq 0$. Soit $\varepsilon > 0$. On pose $\underbrace{\eta = \frac{\varepsilon}{k}}_{\text{ne dépend pas de } x} > 0$ car $k > 0$.

Soit $(x, y) \in I^2$. On suppose $|x - y \leqslant \eta|$. Alors,

$$|f(x) - f(y)| \leqslant k\,|x - y| \leqslant k\eta = \varepsilon$$

□

Exemple :
$x \mapsto |x|$ est 1-lipschitzienne sur $\mathbb{R}$.

$$\forall (x, y) \in \mathbb{R}^2, ||x| - |y|| \leqslant |x - y|$$

(inégalité triangulaire)

Théorème : Soit $f : I \to \mathbb{R}$ dérivable sur I telle qu'il existe $M \in \mathbb{R}$ vérifiant

$$\forall x \in I, |f'(x)| \leqslant M$$

Alors

$$\forall (a, b) \in I^2, |f(a) - f(b)| \leqslant M\,|a - b|$$

donc f est M-lipschitzienne.

Corollaire : Soit f de classe $\mathscr{C}^1$ sur $[a, b]$. Alors f est lipschitzienne.

Preuve :
f' est continue sur un segment donc bornée. □

Exemple :

$$\begin{aligned} f : \mathbb{R}^+ &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto \sqrt{x} \end{aligned}$$

$$\forall x > 0, |f'(x)| = \frac{1}{2\sqrt{x}} \xrightarrow[x \to 0^+]{} +\infty$$

Par contre,

$$\forall x \geqslant 1, |f'(x)| \leqslant \frac{1}{2}$$

Donc f est $\frac{1}{2}$-lipschitzienne sur $[1, +\infty[$ donc uniformément continue sur $[1, +\infty[$.
f est continue sur $[0, 1]$ donc uniformément continue sur $[0, 1]$ (théorème de

Heine).
Soit $\varepsilon > 0$. Soient $\eta_1, \eta_2 \in \mathbb{R}_\star^+$ tels que

$$\begin{cases} \forall (x,y) \in [0,1]^2, |x-y| \leqslant \eta_1 \implies \left|\sqrt{x} - \sqrt{y}\right| \leqslant \dfrac{\varepsilon}{2} \\ \forall (x,y) \in [1,+\infty[^2, |x-y| \leqslant \eta_2 \implies \left|\sqrt{x} - \sqrt{y}\right| \leqslant \dfrac{\varepsilon}{2} \end{cases}$$

On pose $\eta = \min(\eta_1, \eta_2)$. Soient $(x,y) \in \left(\mathbb{R}^+\right)^2$. On suppose $|x-y| \leqslant \eta$

Cas 1 $\begin{cases} x \leqslant 1 \\ y \leqslant 1 \end{cases}$
Alors, $|x-y| \leqslant \eta \leqslant \eta_1$ donc $\left|\sqrt{x} - \sqrt{y} \leqslant \varepsilon_2\right| \leqslant \varepsilon$

Cas 2 $\begin{cases} x \geqslant 1 \\ y \geqslant 1 \end{cases}$
Alors, $|x-y| \leqslant \eta \leqslant \eta_2$ donc $\left|\sqrt{x} - \sqrt{y} \leqslant \dfrac{\varepsilon}{2} \leqslant \varepsilon\right|$

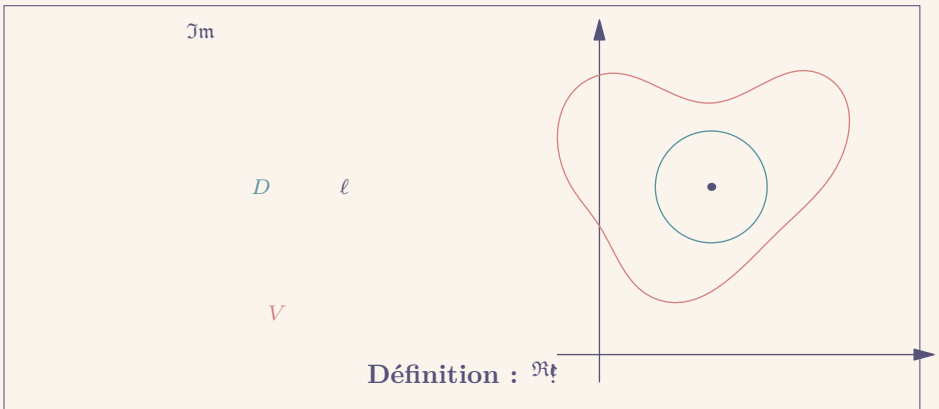
Cas 3 $x \leqslant 1 \leqslant y$

$$\begin{aligned} \left|\sqrt{x} - \sqrt{y}\right| &= \left|\sqrt{x} - \sqrt{1} + \sqrt{1} - \sqrt{y}\right| \\ &\leqslant \left|\sqrt{x} - \sqrt{1}\right| + \left|\sqrt{y} - \sqrt{1}\right| \end{aligned}$$

$$|x-1| \leqslant |x-y| \leqslant \eta \leqslant \eta_1 \text{ donc } \left|\sqrt{x} - \sqrt{1}\right| \leqslant \frac{\varepsilon}{2}$$
$$|y-1| \leqslant |x-y| \leqslant \eta \leqslant \eta_2 \text{ donc } \left|\sqrt{y} - \sqrt{1}\right| \leqslant \frac{\varepsilon}{2}$$

Donc $\left|\sqrt{x} - \sqrt{y}\right| \leqslant \dfrac{\varepsilon}{2} + \dfrac{\varepsilon}{2} = \varepsilon$

3 Fonctions à valeurs dans $\mathbb{C}$



V est un voisinage de ℓ s'il existe $r > 0$ tel que $V \supset D(\ell, r)$
où $D(l,r) = \{z \in \mathbb{C} \mid |z - \ell| < r\}$

Proposition : Soit $f : I \to \mathbb{C}$ et $a \in I$, $\ell \in \mathbb{C}$.

$$f(x) \xrightarrow[x\to a]{} \ell \iff \begin{cases} \mathfrak{Re}(f(x)) \xrightarrow[x\to a]{} \mathfrak{Re}(\ell) \\ \mathfrak{Im}(f(x)) \xrightarrow[x\to a]{} \mathfrak{Im}(\ell) \end{cases}$$

□

Remarque (Rappel) :
On dit que : $I \to \mathbb{C}$ est bornée s'il existe $M \in \mathbb{R}$ tel que

$$\forall x \in I, |f(x)| \leqslant M$$

4 Annexe

Théorème : *Théorème 2.11*
$f : I \to J$ bijective monotone avec I et J deux intervalles.
Alors, f^{-1} est continue (et f aussi)

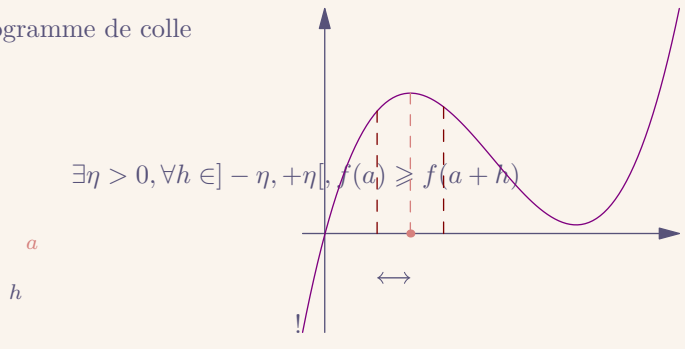
Preuve :
f monotone donc $f(I) = J$
donc f continue (d'après 2.10).
f^{-1} monotone, $f^{-1}(J) = I$
donc f^{-1} est continue □

Définition : Un homéomorphisme est une application bijective, continue dont la réciproque est continue.

Remarque :
Preuve du programme de colle

Preuve :

$$\exists \eta > 0, \forall h \in]-\eta, +\eta[, f(a) \geqslant f(a+h)$$



$$f'(a) = \lim_{h\to 0} \frac{f(a+h)-f(a)}{h} = \lim_{\substack{h\to 0 \\ >}} \frac{f(a+h)-f(a)}{h} \leqslant 0$$
$$= \lim_{\substack{h\to 0 \\ <}} \frac{f(a+h)-f(a)}{h} \geqslant 0$$

Donc, $f(a) = 0$ □

Chapitre 15

Espaces vectoriels

1 Définition et premières propriétés

Définition : Soit E un ensemble muni d'une loi interne $+$ et d'une loi $\cdot$ définie sur $\mathbb{K} \times E$ à valeurs dans E où $\mathbb{K}$ est un corps.
On dit que $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel (ou un espace vectoriel sur $\mathbb{K}$) si

1. $(E, +)$ est un groupe abélien
2. (a)

$$\forall u \in E, \forall (\lambda, \mu) \in \mathbb{K}^2,$$
$$\mu \cdot (\lambda \cdot u) = (\mu \underbrace{\times}_{\times \text{ de } \mathbb{K}} \lambda) \cdot u$$

   (b) $\forall u \in E, 1_{\mathbb{K}} \cdot u = u$
3. (a)

$$\forall u \in E, \forall (\lambda, \mu) \in \mathbb{K}^2$$
$$(\lambda \cdot u) \underbrace{+}_{+ \text{ de } E} (\mu \cdot u) = (\lambda \underbrace{+}_{+ \text{ de } \mathbb{K}} \mu) \cdot u$$

   (b)

$$\forall \lambda \in \mathbb{K}, \forall (u, v) \in E^2,$$
$$\lambda \cdot (u + v) = (\lambda \cdot u) + (\lambda \cdot v)$$

Les éléments de E sont alors appelés vecteurs et les éléments de $\mathbb{K}$ sont dits scalaires.
Par convention, $\cdot$ est prioritaire sur $+$.

Exemple :
Soit $\mathbb{K}$ corps, $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel

Exemple :
Soit $\vec{\mathcal{P}}$ l'ensemble des vecteurs du plan. $\vec{\mathcal{P}}$ est un $\mathbb{R}$-espace vectoriel.

Exemple :
$\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel.
En généralisant, tout corps $\mathbb{K}$ est un $\mathbb{L}$-espace vectoriel pour $\mathbb{L}$ un sous-corps de $\mathbb{K}$

Exemple :
$(\mathbb{K}^n, +, \cdot)$ avec

$$\begin{aligned}(x_1, \dots, x_n) + (y_1, \dots, y_n) &= (x_1 + y_1, \dots, x_n + y_n)\\ \lambda \cdot (y_1, \dots, y_n) &= (\lambda \cdot y_1, \dots, \lambda \cdot y_n)\end{aligned}$$

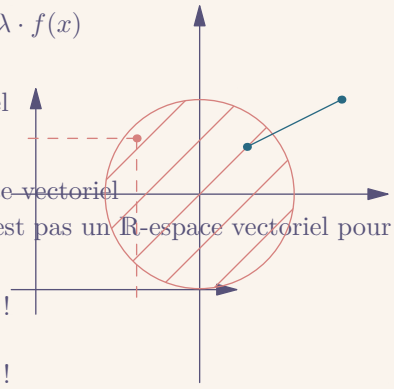
est un espace vectoriel.

Exemple :
Soient $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et $\mathcal{D}$ un ensemble non vide.
$(E^{\mathcal{D}}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel où pour $f, g \in E^{\mathcal{D}}$ et $\lambda \in \mathbb{K}$

$$\begin{aligned}f + g : \mathcal{D} &\longrightarrow E\\ x &\longmapsto f(x) + g(x)\end{aligned}$$

$$\begin{aligned}\lambda f : \mathcal{D} &\longrightarrow \mathbb{K}\\ x &\longmapsto \lambda \cdot f(x)\end{aligned}$$

Par exemple, $\mathbb{C}^{\mathbb{N}}$ est un $\mathbb{R}$-espace vectoriel
$\mathscr{C}^0(\mathcal{D}, \mathbb{R})$ est un $\mathbb{R}$-espace vectoriel



Exemple :
— $\mathbb{R}^+$ n'est pas un $\mathbb{R}$-espace vectoriel
— $\{(x, 0) \mid x \in \mathbb{R}\} \cup \{(0, y) \mid y \in \mathbb{R}\}$ n'est pas un $\mathbb{R}$-espace vectoriel pour les lois usuelles

!

!

Proposition : Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel.

1. $\forall u \in E, 0_{\mathbb{K}} \cdot u = 0_E$
2. $\forall \lambda \in \mathbb{K}, \lambda \cdot 0_E = 0_E$
3. $\forall \lambda \in \mathbb{K}, \forall u \in E, \lambda \cdot u = 0_E \implies \lambda = 0_{\mathbb{K}}$ ou $u = 0_E$

Preuve : 1. Soit $u \in E$.

$$\begin{aligned} 0_{\mathbb{K}} \cdot u &= (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot u \\ &= 0_{\mathbb{K}} \cdot u + 0_{\mathbb{K}} \cdot u \end{aligned}$$

$(E, +)$ est un groupe donc $0_E = 0_{\mathbb{K}} \cdot u$

2. Soit $\lambda \in \mathbb{K}$.

$$\lambda \cdot 0_E = \lambda \cdot (0_E + 0_E) = \lambda \cdot 0_E + \lambda \cdot 0_E$$

$\lambda \cdot 0_E$ est régulier pour $+$:

$$0_E = \lambda \cdot 0_E$$

3. Soit $\lambda \in \mathbb{K}$ et $u \in E$ tel que $\lambda \cdot u = 0_E$

Cas 1 $\lambda = 0_{\mathbb{K}}$
Cas 2 $\lambda \neq 0_{\mathbb{K}}$ Alors, $\lambda^{-1} \in \mathbb{K}$ et donc

$$\begin{aligned} \lambda \cdot u = 0_E &\implies \lambda^{-1}(\lambda \cdot u) = \lambda^{-1} \\ &\implies (\lambda^{-1} \times \lambda) \cdot u = 0_E \text{ d'après 2.} \\ &\implies 1_{\mathbb{K}} \cdot u = 0_E \\ &\implies u = 0_E \end{aligned}$$

□

Proposition : Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et $u \in E$. Alors, $-u = (-1_{\mathbb{K}}) \cdot u$

Preuve :

$$\begin{aligned} u + (-1_{\mathbb{K}}) \cdot u &= (1_{\mathbb{K}} \cdot u) + (-1_{\mathbb{K}}) \cdot u \\ &= (1_{\mathbb{K}} + (-1_{\mathbb{K}})) \cdot u \\ &= 0_{\mathbb{K}} u \\ &= 0_E \end{aligned}$$

Donc $-u = (-1_{\mathbb{K}}) \cdot u$ □

2 Sous-espaces vectoriels

Définition : Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel. Soit $F \subset E$.
On dit que F est un sous-$\mathbb{K}$-espace vectoriel de E si

1. $F \neq$
2. $\forall (u, v) \in F^2, u + v \in F$
3. $\forall \lambda \in \mathbb{K}, \forall u \in F, \lambda u \in F$

Proposition : Avec les notations précédentes, $(F, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel

Preuve :
— D'après 2., + est interne dans F
— $(E, +)$ est un groupe abélien donc + est associative et commutative dans E donc dans F
— $F \neq$. Soit $u \in F$. D'après 3.,

$$0_{\mathbb{K}} \cdot u \in F$$

Comme $u \in E$ et $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel,

$$0_{\mathbb{K}} \cdot u = 0_E$$

Donc, $0_E \in F$
— Soit $u \in F$. Comme $u \in E$,

$$-u = -(1_{\mathbb{K}}) \cdot u \in F \text{ d'après 3.}$$

— Les autres axiomes sont aisément vérifiés.

□

Proposition : Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et $F \subset E$.
F est un sous-espace vectoriel de $(E, +, \cdot)$ si et seulement si

1. $F \neq$
2. $\forall (\lambda, \mu) \in \mathbb{K}^2, \forall (u, v) \in F^2, \lambda \cdot u + \mu \cdot v \in F$

Preuve " $\Longrightarrow$ " On sait déjà que F est non vide.

$$\forall u, v \in F, \forall \lambda, \mu \in \mathbb{K}, \left.\begin{array}{l} \lambda u \in F \\ \mu v \in F \end{array}\right\} \text{ donc } \lambda u + \mu v \in F$$

" $\Longleftarrow$ " — On sait déjà que F est non-vide

— Soient $u, v \in F$

$$u + v = 1_{\mathbb{K}} \cdot u + 1_{\mathbb{K}} \cdot v \in F$$

— Soit $u \in F, \lambda \in \mathbb{K}$.

$$\lambda \cdot u = \lambda \cdot u + 0_{\mathbb{K}} \cdot u \in F$$

□

Définition : Soient $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et $(u_1, \dots, u_n) \in E^n$. Une combinaison linéaire de $(u_1, \dots, u_n)$ est un vecteur de E de la forme $\sum_{i=1}^{n} \lambda_i u_i$ où $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$

Remarque :
On peut aussi démontrer que F est un sous-espace vectoriel de E si et seulement si

$$F \neq \text{ et } \forall u, v \in F, \forall \lambda \in \mathbb{K}, \lambda u + v \in F$$

Exemple : 1. $F = \{z \in \mathbb{C} \mid \mathfrak{Re}(z) + \mathfrak{Im}(z) = 1\} \subset \mathbb{C}$
F est un sous-$\mathbb{R}$-espace vectoriel de $\mathbb{C}$?
Non car $0 \notin F$

2. $F = \{z \in \mathbb{C} \mid \mathfrak{Re}(z) + \mathfrak{Im}(z) = 0\}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathbb{C}$ mais pas un sous-$\mathbb{C}$-espace vectoriel.
En effet, $1 - i \in F$ $i(1 - i) = i + 1 \notin F$
3. $E = \mathbb{R}^{\mathbb{N}}$ est un $\mathbb{R}$-espace vectoriel.
$F = \left\{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N}, u_{n+1} = 3u_n\right\}$ est un sous-espace vectoriel de E.
$G = \left\{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N}, u_{n+1} = 3u_n + 2\right\}$ n'est pas un sous-espace vectoriel de E puique $0_E \notin G$.
4. $E = \mathbb{R}^D$ est un $\mathbb{R}$-espace vectoriel
$F = \mathscr{C}^0(D, \mathbb{R})$ est un sous-espace vectoriel de E (fonctions continues)
$G = \mathscr{D}(D, \mathbb{R})$ est un sous-espace vectoriel de E (fonctions dérivables)
Si $D =]-a, a[$ avec $a \in \mathbb{R}$, $H = \{f \in E \mid f \text{ impaire }\}$ est un sous-espace vectoriel de E
Si $D = \mathbb{R}$, $L = \{f \in E \mid f \text{ 1-périodique }\}$ est un sous-espace vectoriel de E
$M = \{f \in E \mid f \text{ périodique }\}$ n'est pas un sous-ensemble vectoriel de E
5. L'ensemble des solutions sur un intervalle I d'une équation différentielle linéaire est un sous-espace vectoriel de $\mathbb{R}^I$

Exercice (Exercice) :
Trouver tous les sous-$\mathbb{R}$-espaces vectoriels de $\mathbb{R}^2$

— $\{(0,0)\}$ est un sous-espace vectoriel de $\mathbb{R}^2$
— Les droites passant par O sont des sous-espaces vectoriels de $\mathbb{R}^2$
— $\mathbb{R}^2$ est un sous-espace vectoriel de $\mathbb{R}^2$

et rien d'autre !

Proposition : Soit $(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel et $\mathcal{F}$ une famille non vide de sous-espaces vectoriels de E. Alors $\bigcap_{F\in\mathcal{F}} F$ est un sous-espace vectoriel de E.

Preuve :
On pose $G = \bigcap_{F\in\mathcal{F}} F$.

— $\forall F \in \mathcal{F}, 0_E \in F$ car F est un sous espace vectoriel de E donc $0_E \in G$.
— Soient $u, v \in G$ et $\lambda, \mu \in \mathbb{K}$. On pose $w = \lambda u + \mu v$.

$$\forall F \in \mathcal{F}, \left.\begin{array}{l} u \in F \\ v \in F \end{array}\right\} \text{ donc } w \in F$$

donc $w \in G$

□

Remarque (Attention B) :
Une réunion de sous-espaces vectoriels n'est pas un sous-espace vectoriel en général.

Exercice :
$F \cup G$ est un sous-espace vectoriel de $E \iff F \subset G$ ou $G \subset F$

Définition : Soient F et G deux sous-espaces vectoriels de E. On définit leur somme $F+G$ par

$$F + G = \{x + y \mid x \in F, y \in G\}$$

Proposition : Avec les notations précédentes, $F+G$ est le plus petit

sous-espace vectoriel de E contenant $F \cup G$.

Preuve : — — $0_E = \underbrace{0_E}_{\in F} + \underbrace{0_E}_{\in G} \in F + G$

— Soient $u \in F + G, v \in F + G, \lambda, \mu \in \mathbb{K}$
On pose

$$\begin{cases} u = x + y \text{ avec } \begin{cases} x \in F \\ y \in G \end{cases} \\ v = a + b \text{ avec } \begin{cases} a \in F \\ b \in G \end{cases} \end{cases}$$

Donc,

$$\begin{aligned} \lambda u + \mu v &= \lambda(x + y) + \mu(a + b) \\ &= \lambda x + \lambda y + \mu a + \mu b \\ &= \underbrace{(\lambda x + \mu a)}_{\in F} + \underbrace{\lambda y + \mu b}_{\in G} \in F + G \end{aligned}$$

Ainsi $F + G$ est un sous-espace vectoriel de E.

— Soit $x \in F \cup G$.
Si $x \in F$ alors $x = \underbrace{x}_{\in F} + \underbrace{O_E}_{\in G} \in F + G$
Si $x \in G$ alors $x = \underbrace{0_E}_{\in F} + \underbrace{x}_{\in G} \in F + G$
Donc, $F \cup G \subset F + G$

— Soit H un sous-espace vectoriel de E tel que $F \cup G \subset H$
Soit $u \in F + G$. On pose $u = x + y$ avec $\begin{cases} x \in F \\ y \in G \end{cases}$

$$\begin{cases} x \in F \subset F \cup G \subset H \\ y \in G \subset F \cup G \subset H \end{cases}$$

H est un sous-espace vectoriel de E donc $x + y \in H$.
On a montré que $F + G \subset H$

□

Définition : Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et $(F_i)_{i \in I}$ une famille

quelconque non vide de sous-espaces vectoriels de E. On définit $\sum_{i\in I} F_i$ par

$$\sum_{i\in I} F_i = \left\{ \sum_{i\in I} x_i \mid (x_i)_{i\in I} \in \prod_{i\in I} F_i ; (x_i) \text{ presque nulle} \right\}$$
$$= \left\{ \sum_{i\in I} x_i \mid (x_i) \in \prod_{i\in I} F_i ; \{i \in I \mid x_i \neq 0_E\} \text{ est fini} \right\}$$

$\sum_{i\in I} F_i$ est l'ensemble de sommes finies obtenues à partir d'éléments de $\prod_{i\in I} F_i$

Exemple :
$E = \mathbb{R}^{\mathbb{R}}$
$\forall i \in \mathbb{N}, F_i = \{x \mapsto ax^i \mid a \in \mathbb{R}\}$
$\sum_{i\in\mathbb{N}} F_i$ est l'ensemble des fonctions polynomiales

Proposition : Une somme quelconque de sous-espaces vectoriels est le plus petit sous-espace vectoriel contenant leur réunion. □

Définition : Soient F et G deux sous-espaces vectoriels de E. On dit qu'ils sont en somme directe si

$$\forall u \in F + G, \exists!(x, y) \in F \times G, u = x + y$$

Dans ce cas, l'espace $F + G$ est noté $F \oplus G$

Exemple :
$E = \mathbb{R}^3$
$F = \{(x, 0, x) \mid x \in \mathbb{R}\}$

$$G = \left\{ (x, y, z) \mid (S) : \begin{cases} x + y + z = 0 \\ y - z = 0 \end{cases} \right\}$$

$F \oplus G$?

— $(0, 0, 0) \in F$ car $0 \in \mathbb{R}$
Soient $x, y \in \mathbb{R}$, $\begin{cases} u = (x, 0, x) \\ v = (y, 0, y) \end{cases}$
Soient $\lambda, \mu \in \mathbb{R}$

$$\begin{aligned}\lambda u+\mu v &= \lambda(x,0,0)+\mu(y,0,y)\\ &= (\lambda x,0,\lambda x)+(\mu y,0,\mu y)\\ &= (\lambda x+\mu y,0,\lambda x+\mu y)\in F\end{aligned}$$

Donc F est un sous-espace vectoriel de E

— $(0,0,0)\in G$ car (S) est homogène

$\begin{cases}u=(x,y,z)\in G\\ v=(a,b,c)\in G\end{cases}$

Soient $\lambda,\mu\in\mathbb{R}$

$$\begin{aligned}\lambda u+\mu v\in G &\iff \lambda(x,y,z)+\mu(a,b,c)\in G\\ &\iff (\lambda x+\mu a,\lambda y+\mu b,\lambda z+\mu c)\in G\\ &\iff \begin{cases}(\lambda x+\mu a)+(\lambda y+\mu b)+(\lambda z+\mu c)=0\\ (\lambda y+\mu b)-(\lambda z+\mu c)=0\end{cases}\\ &\iff \begin{cases}\lambda\overbrace{(x+y+z)}^{=0}+\mu\overbrace{(a+b+c)}^{=0}\\ \lambda\underbrace{(y-z)}_{=0}+\mu\underbrace{(b-c)}_{=0}=0\end{cases}\\ &\iff \begin{cases}0=0\\ 0=0\end{cases}\end{aligned}$$

— Soit $w\in E$. On pose $w=(x,y,z)$

$$\begin{aligned}w\in F+G &\iff \exists(u,v)\in F\times G, w=u+v\\ &\iff \exists x'\in\mathbb{R},\exists(a,b,c)\in\mathbb{R}^3,\begin{cases}w=(x',0,x')+(a,b,c)\\ a+b+c=0\\ b-c=0\end{cases}\\ &\iff \exists\,(x',a,b,c)\in\mathbb{R}^4,\begin{cases}(x,y,z)=(a+x',b,c+x')\\ a+b+c=0\\ b-c=0\end{cases}\\ &\iff \exists\,(x',a,b,c)\in\mathbb{R}^4,(S'):\begin{cases}a+x'=x\\ b=y\\ c+x'=z\\ a+b+c=0\\ b-c=0\end{cases}\end{aligned}$$

(S') est un système linéaire à 4 inconnues (x',a,b,c), 5 équations, 3 paramètres (x,y,z)

$$(S') \iff \begin{cases} b = y \\ c = y \\ x' = z - y \\ a = x - z + y \\ x + 3y - z = 0 \end{cases}$$

Si $x + 3y - z \neq 0$ alors (S') n'a pas de solutions et donc $w \notin F + G$
Si $x + 3y - z = 0$ alors (S') a une unique solution alors

$$\exists!(u, v) \in F \times G, w = u + v$$

On a montré que

$$F \oplus G = \left\{(x, y, z) \in \mathbb{R}^3 \mid x + 3y - z = 0\right\}$$

Proposition : Soient $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces vectoriels de E
F et G sont en somme directe si et seuelement si $F \cap G = \{0_E\}$

Preuve $\Longrightarrow$ " On suppose la somme directe.
Soit $x \in F \cap G$.
D'une part, $0_E = \underbrace{0_E}_{\in F} + \underbrace{0_E}_{\in G}$
D'autre part, $0_E = \underbrace{x}_{\in F} + \underbrace{(-x)}_{\in G}$
Par unicité, $x = 0_E$
" $\Longleftarrow$ " On suppose $F \cap G = \{0_E\}$
Soit $x \in F + G$ et on supoise que x a deux décompositions :

$$\begin{cases} x = u + v, & u \in F, v \in G \\ x = u' + v', & u' \in F, v' \in G \end{cases}$$

D'où, $u - u' = v' - v$
Or, $\begin{cases} u - u' \in F \\ v - v' \in G \end{cases}$
Donc, $u - u' \in F \cap G = \{0_E\}$
donc $u - u' = 0_E$ donc $u = u'$ donc $v' = v$

□

Remarque :
Ce résultat est inutile pour l'instant (en l'absence d'arguments dimensionnels) pour prouver un resultat de la forme $E = F \oplus G$

Exemple :
$E = \mathbb{R}^{\mathbb{R}}$
$F = \{f \in E \mid f \text{ paire}\}$ et $F = \{f \in E \mid f \text{ impaire}\}$
Prouvons que $E = F \oplus G$
Soit $f \in F \cap G$ donc

$$\forall x \in \mathbb{R}, f(-x) = f(x) = -f(x)$$

Donc

$$\forall x \in \mathbb{R}, f(x) = -f(x)$$

et donc

$$\forall x \in \mathbb{R}, f(x) = 0$$

donc $f = 0_E$
Ainsi, la somme de F est G est directe

$$F + G = F \oplus G$$

Montrons que $E = F + G$. Soit $f \in E$.

Analyse Soient $g \in G$ et $g \in F$ telles que

$$f = g + h$$

Donc

$$\forall x \in \mathbb{R}, \begin{cases} f(x) = g(x) + h(x) \\ f(-x) = -g(x) + h(x) \end{cases}$$

et donc

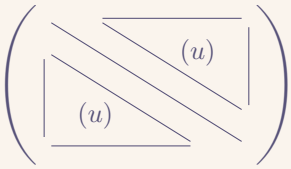
$$\begin{cases} h(x) = \dfrac{1}{2}(f(x) + f(-x)) \\ g(x) = \dfrac{1}{2}(f(x) - f(-x)) \end{cases}$$

Donc $F + G = F \oplus G$.
Synthèse On pose

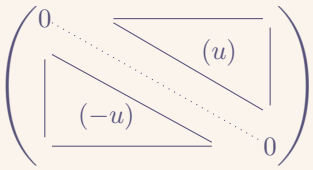
$$\begin{cases} g : x \longmapsto \dfrac{1}{2}(f(x) - f(-x)) \\ h : x \longmapsto \dfrac{1}{2}(f(x) + f(-x)) \end{cases}$$

On vérifie que $\begin{cases} g \in F \\ h \in F \\ g + h = f \end{cases}$
On a prouvé que $E = F + G$

Exemple :
$E = \mathcal{M}_2(\mathbb{C})$
$F = S_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{C} \right\}$



$$G = A_2(\mathbb{C}) = \left\{ \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \mid a \in \mathbb{C} \right\}$$



$E = F \oplus G$

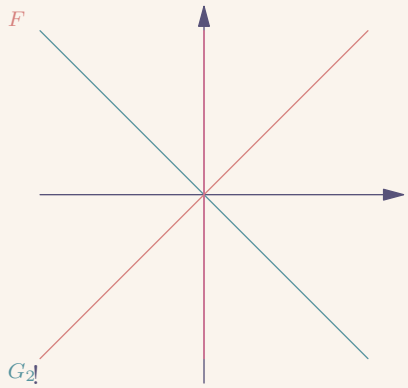
Définition : Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel. On dit que F et G sont supplémentaires dans E si

$$E = F \oplus G$$

en d'autres termes,

$$\forall x \in E, \exists! (y, z) \in F \times G, x = y + z$$

Exemple :
$E = \mathbb{R}^2$
$F = \{(x, y) \in \mathbb{R}^2, y = x\}$



$G_1 \oplus F = E$ et $G_2 \oplus F = E$
Soit $(x, y) \in E$

$$\begin{aligned}(x,y) &= \underbrace{(x,x)}_{\in F} + \underbrace{(0,y-x)}_{\in G_1} \\ &= \underbrace{\left(\frac{x+y}{2},\frac{x+y}{2}\right)}_{\in F} + \underbrace{\left(\frac{x+y}{2},\frac{x+y}{2}\right)}_{\in G_2}\end{aligned}$$

Définition : Soit $(F_i)_{i\in I}$ une famille non vide de sous-espaces vectoriels de $(E,+,\cdot)$. On dit qu'ils sont en somme directe si

$$\forall x \in \sum_{i\in I} F_i, \exists!(x_i)_{i\in I} \in \prod_{i\in I} F_i \text{ presque nulle telle que } x = \sum_{i\in I} x_i$$

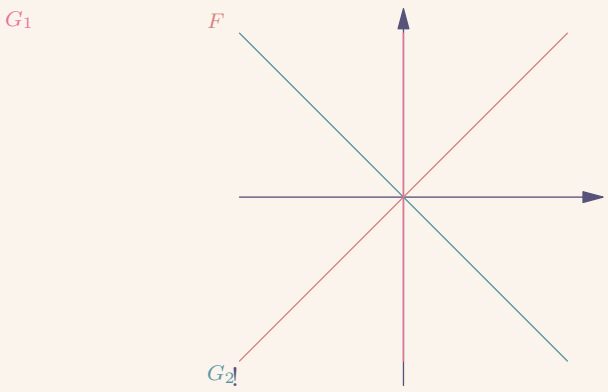
Dans ce cas, on écrit $\bigoplus_{i\in I} F_i$ à la place de $\sum_{i\in I} F_i$

Exemple :
E : l'espace des fonctions polynomiales

$$\forall i \in \mathbb{N}, F_i = \{x \mapsto ax^i \mid a \in \mathbb{K}\}$$

$E = \bigoplus_{i\in\mathbb{N}} F_i$

Exemple :
$E = \mathbb{R}^2$



$$\begin{cases} F = \{(x,x)ă \mid x \in \mathbb{R}\} \\ G = \{(0,x)ă \mid x \in \mathbb{R}\} \\ F = \{(x,-x)ă \mid x \in \mathbb{R}\} \end{cases}$$

On a $F \cap G \cap H = \{0_E\}$ mais leur somme n'est pas directe

$$\begin{aligned}(0,0) &= \overbrace{(1,1)}^{\in F} + \overbrace{(0,-2)}^{\in G} + \overbrace{(-1,1)}^{\in H} \\ &= \underbrace{(2,2)}_{\in F} + \underbrace{(0,-4)}_{\in G} + \underbrace{(-2,2)}_{\in H}\end{aligned}$$

3 Familles de vecteurs

Définition : Soit $(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel et $A \in \mathscr{P}(E)$. Le sous-espace vectoriel engendré par A est le plus petit sous espace vectoriel V de E tel que $A \subset V$.
On le note $\text{Vect}(A)$

Exemple :
E un $\mathbb{K}$-espace vectoriel.

- $\text{Vect}(\{0_E\}) = \{0_E\}$
- $\text{Vect}() = \{0_E\}$
- $\text{Vect}(E) = E$
- Soit $u \in E \setminus \{0_E\}$
  $\text{Vect}(\{u\}) = \{\lambda u \mid \lambda \in \mathbb{K}\} = \mathbb{K}u$
- Soient $u, v \in \exists \setminus \{0_E\}$
  $\text{Vect}(\{u,v\}) = \{\lambda u + \mu v \mid (\lambda,\mu) \in \mathbb{K}^2\} = \mathbb{K}u + \mathbb{K}v$

Définition : Soit $(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel et $u \in E \setminus \{0_E\}$. La droite (vectorielle) engendrée par u est $\mathbb{K}u = \text{Vect}(u) = \text{Vect}(\{u\})$. Soit $v \in E$. On dit que u et v sont colinéaires si $v \in \mathbb{K}u$. Si v n'est pas colinéaire à u alors, $\text{Vect}(u,v) = \mathbb{K}u + \mathbb{K}v$ est appelé plan (vectoriel) engendré par u et v.

Exemple :
L'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre 1 est une droite vectorielle.

L'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre 2 à coefficients constants est un plan vectoriel.

$$\{y \in \mathscr{C}^2(\mathbb{R}) \mid y'' + y = 0\} = \text{Vect}(\cos, \sin)$$

Proposition : Soit $(e_i)_{i\in I}$ un famille non vide de vecteurs d'un $\mathbb{K}$-espace

vectoriel $(E, +, \cdot)$. Alors,

$$\begin{aligned}\text{Vect}\left((e_i)_{i\in I}\right) &= \left\{ \sum_{i\in I} \lambda_i e_i \mid (\lambda_i)_{i\in I} \in \mathbb{K}^I \text{ et } (\lambda_i) \text{ presque nulle} \right\} \\ &= \sum_{i\in I} \mathbb{K}e_i\end{aligned}$$

Preuve :
On pose $F = \sum_{i\in I} \mathbb{K}e_i$
F est un sous espace vectoriel de E.

$$\forall i \in I, e_i = \underbrace{\sum_{j\in I} \lambda_j e_j}_{\in F} \text{ où } \lambda_j = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

$$= \delta_{i,j} \text{ (symbole de Kronecker)}$$

Soit G un sous espace vectoriel de E tel que

$$\forall i \in I, e_i \in G$$

Soit $u \in F$. Soit $(\lambda_i)_{i\in I}$ une famille presque nulle de scalaires telle que $u = \sum_{ii\in I} \lambda_i e_i$
Soit $\{i_1, \ldots, i_k\} = \{i \in I \mid \lambda_i \neq 0_{\mathbb{K}}\}$
Donc,

$$u = \sum_{j=1}^{k} \underbrace{\lambda_{ij} e_{ij}}_{\in G} \in G$$

Donc $F \subset G$ □

Définition : On dit que $(e_i)_{i\in I}$ est une famille génératrice de E si

$$E = \text{Vect}\left((e_i)_{i\in I}\right)$$

Exemple :

$$E = \mathbb{R}^3$$

$$\begin{cases} e_1 &= (1,0,1) \\ e_2 &= (0,1,1) \\ e_3 &= (1,1,1) \\ e_4 &= (1,0,0) \\ e_5 &= (0,1,2) \end{cases}$$

Soit $(x,y,z) \in \mathbb{R}^3$. On cherche $(\lambda_1, \dots, \lambda_5) \in \mathbb{R}^5$ tels que

$$(E): \quad (x,y,z) = \sum_{i=1}^{5} \lambda_i e_i$$

$$\begin{aligned} (E) &\iff (x,y,z) = (\lambda_1 + \lambda_3 + \lambda_4, \lambda_2 + \lambda_3 + \lambda_5, \lambda_1 + \lambda_2 + \lambda_3 + 2\lambda_5) \\ &\iff \begin{cases} \lambda_1 + \lambda_3 + \boxed{\lambda_4} = x \\ \lambda_2 + \boxed{\lambda_3} + \lambda_5 = y \\ \boxed{\lambda_1} + \lambda_2 + \lambda_3 + 2\lambda_5 = z \end{cases} \\ &\iff \begin{cases} \lambda_4 = x - \lambda_1 - \lambda_3 \\ \lambda_3 = y - \lambda_2 - \lambda_5 \\ \lambda_1 = z - \lambda_2 - \lambda_3 - 2\lambda_5 \end{cases} \end{aligned}$$

Par exemple, $(\lambda_1 = z - y, \lambda_2 = 0, \lambda_3 = y, \lambda_4 = x - z, \lambda_5 = 0)$ est solution

Donc

$$\text{Vect}(e_1, e_2, e_3, e_4, e_5) = E$$

Exemple :
$E = \mathbb{R}^4$

$$\begin{cases} e_1 = (1,0,1,0) \\ e_2 = (0,1,0,1) \\ e_3 = (1,1,1,1) \\ e_4 = (1,-1,1,-1) \\ e_5 = (1,1,0,0) \end{cases}$$

Soit $(x,y,z,t) \in \mathbb{R}^4$, $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) \in \mathbb{R}^5$

$$(E)\quad (x,y,z,t)=\sum_{i=1}^{5}\lambda_i e_i \iff \begin{cases} x=\lambda_1+\lambda_3+\lambda_4+\lambda_5\\ y=\lambda_2+\lambda_3-\lambda_4+\lambda_5\\ z=\lambda_1+\lambda_3+\lambda_4\\ t=\lambda_2+\lambda_3-\lambda_4\end{cases}$$

$$\underset{\substack{L_2\leftarrow L_2-L_4\\ L_1\leftarrow L_1-L_3}}{\iff} \begin{cases} \lambda_5=x-z\\ \lambda_5=y-t\\ \lambda_1+\lambda_3+\lambda_4=z\\ \lambda_2+\lambda_3-\lambda_4=t\end{cases}$$

$$\underset{L_2\leftarrow L_2-L_1}{\iff} \begin{cases} \lambda_5=x-z\\ \boxed{0=y-t-x+z}\\ \lambda_1+\lambda_3+\lambda_4=z\\ \lambda_1+\lambda_3-\lambda_4=t\end{cases}$$

Par exemple ; $(1,0,0,0)\notin \text{Vect}\,(e_1,e_2,e_3,e_4,e_5)$

Proposition : Soit $(e_i)_{i\in I}$ une famille génératrice de E et $(u_j)_{j\in J}$ une surfamille de $(e_i)_{i\in I}$ constituée de vecteurs de E :

$$\forall i\in I, \exists j\in J, e_i=u_j$$

Alors, $(u_j)_{j\in J}$ engendre E. □

Proposition : Soit $(e_i)_{i\in I}$ une famille génératrice de E et $i_0\in I$

$(e_i)_{i\in I\setminus\{i_0\}}$ engendre E $\iff$ $e_{i_0}\in \text{Vect}\left((e_i)_{i\in I\setminus\{i_0\}}\right)$
$\iff$ e_{i_0} est une combinaison linéaire des e_i $(i\in I, i\neq i_0)$

Preuve

“ $\Longrightarrow$ ” $E=\text{Vect}\,((e_i)_{i\neq i_0})$ et $e_{i_0}\in E$

“ $\Longleftarrow$ ” Soit $u\in E$. Soit $(\lambda_i)_{i\in I}$ une famille presque nulle de scalaires telle que

$$u=\sum_{i\in I}\lambda_i e_i$$

Soit $(\mu_i)_{i\neq i_0}$ une famille de scalaires telle que

$$e_{i_0}=\sum_{i\in I\setminus\{i_0\}}\mu_i e_i$$

D'où,

$$\begin{aligned} u &= \lambda_{i_0} e_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \lambda_{i_0} \sum_{i \in I \setminus \{i_0\}} \mu_i e_i + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \sum_{i \in I \setminus \{i_0\}} (\lambda_{i_0} \mu_i + \lambda_i)\, e_i \\ &\in \text{Vect}\left((e_i)_{i \in I \setminus \{i_0\}}\right) \end{aligned}$$

□

Proposition : Soit $(e_i)_{i \in I}$ une famille génératrice de E, $i_0 \in I$.

1. On pose $u_i = \begin{cases} e_i & \text{si } i \neq i_0 \\ \lambda e_{i_0} & \text{sinon} \end{cases}$ où $\lambda \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$
   Alors, $(u_i)_{i \in I}$ engendre E
2. Soit $v \in \text{Vect}\left((e_i)_{i \in I \setminus \check{a}\{i_0\}}\right)$.
   On pose $u_i = \begin{cases} e_i & \text{si } i \neq i_0 \\ e_{i_0} + v & \text{sinon} \end{cases}$ où $\lambda \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$
   Alors, $(u_i)_{i \in I}$ engendre E

Preuve : 1. Soit $u \in E$. On pose

$$u = \sum_{i \in I} \lambda_i e_i$$

où $(\lambda_i) \in \mathbb{K}^I$ presque nulle

$$\begin{aligned} u &= \lambda_{i_0} e_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \lambda_{i_0} \lambda^{-1} u_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i u_i \\ &\in \text{Vect}\left((u_i)_{i \in I}\right) \end{aligned}$$

2. Soit $u = \sum_{i \in I} \lambda_i e_i \in E$

$$\begin{aligned} u &= \lambda_{i_0} e_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \lambda_{i_0} (u_{i_0} - v) + \sum_{i \in I \setminus \{i_0\}} \lambda_i u_i \end{aligned}$$

Or, $v = \sum_{i \in I \setminus \{i_0\}} \mu_i e_i = \sum_{i \in I \setminus \{i_0\}} \mu_i u_i$ où $(\mu_i)_{i \in I} \in \mathbb{K}^I$ presque nulle
Donc, $u = \lambda_{i_0} + \sum_{i \in I \setminus \{i_0\}} (\lambda_i - \lambda_{i_0} \mu_i) u_i \in \text{Vect}\left((u_i)_{i \in I}\right)$

□

Définition : Soit $(e_i)_{i \in I}$ une famille de vecteurs. On dit que $(e_i)_{i \in I}$ est libre si aucun vecteur de cette famille n'est une combinaison linéaire des autres vecteurs de cette famille :

$$\forall i \in I, e_i \notin \text{Vect}\left((e_j)_{j \in I \setminus \{i\}}\right)$$

On dit aussi que les e_i sont linéairement indépendants

Proposition :

$$(e_i)_{i \in I} \text{ est libre } \iff \forall (\lambda_i) \in \mathbb{K}^I \text{ presque nulle }, \left(\sum_{i \in I} \lambda_i e_i = 0_E \implies \forall i \in I, \lambda_i = O_{\mathbb{K}} \right)$$

Preuve " $\implies$ " Soit $(\lambda_i) \in \mathbb{K}^I$ presque nulle. On suppose que

$$\sum_{i \in I} \lambda_i e_i = 0_E$$

On suppose aussi qu'il existe $i_0 \in I$ tel que $\lambda_{i_0} \neq 0_{\mathbb{K}}$
On a alors

$$\lambda_{i_0} e_{i_0} = - \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i$$

$\lambda_{i_0} \neq 0_{\mathbb{K}}$ donc il a un inverse $\lambda_{i_0}^{-1}$ donc

$$e_{i_0} = \sum_{i \in I \setminus \{i_0\}} \left(-\lambda_i \lambda_{i_0}^{-1}\right) e_i \in \text{Vect}\left((e_i)_{i \in I \setminus \{i_0\}}\right)$$

une contradiction ↯

" $\Longleftarrow$ " On suppose que $(e_i)_{i\in I}$ n'est pas libre. On considère $i_0 \in I$ tel que e_{i_0} soit une combinaison linéaire des $e_i, i \in I \setminus \{i_0\}$

$$e_{i_0} = \sum_{i\in I\setminus\{i_0\}} \mu_i e_i$$

avec $(\mu_i)_{i\in I\setminus\{i_0\}}$ famille presque nulle de scalaires.
Alors, $1_{\mathbb{K}} e_{i_0} - \sum_{i\in I\setminus\{i_0\}} \mu_i e_i = 0_E$ Par hypothèse

$$\begin{cases} 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ \forall i \neq i_0, -\mu_i = 0_{\mathbb{K}} \end{cases}$$

une contradiction ↯

□

Exemple :
$E = \mathbb{R}^3$ On pose $\begin{cases} e_1 = (1,1,0) \\ e_2 = (1,0,1) \end{cases}$
Soit $(\lambda_1, \lambda_2) \in \mathbb{R}^2$.

$$\begin{aligned} \lambda_1 e_1 + \lambda_2 e_2 = 0_E &\iff (\lambda_1 + \lambda_2, \lambda_1, \lambda_2) = (0,0,0) \\ &\iff \begin{cases} \lambda_1 + \lambda_2 = 0 \\ \lambda_1 = 0 \\ \lambda_2 = 0 \end{cases} \\ &\iff \lambda_1 = \lambda_2 = 0 \end{aligned}$$

Donc, (e_1, e_2) est libre.

Exemple :
$E = \mathbb{R}^{\mathbb{R}}, e_1 = \cos, e_2 = \sin$
Soit $(\lambda_1, \lambda_2) \in \mathbb{R}^2$.

$$\begin{aligned} \lambda_1 e_1 + \lambda_2 e_2 = 0_E &\iff \forall x \in \mathbb{R}, \lambda_1 \cos(x) + \lambda_2 \sin(x) = 0 \\ &\Longrightarrow \begin{cases} \lambda_1 = 0 & (x = 0) \\ \lambda_2 = 0 & (x = 0 \text{ dans la dérivée}) \end{cases} \end{aligned}$$

Donc (e_1, e_2) est libre.

Proposition : Soit $(e_i)_{i\in I}$ une famille libre de E. Alors

$$\sum_{i\in I} \mathbb{K} e_i = \bigoplus_{i\in I} \mathbb{K} e_i$$

i.e.

$$\forall u \in \sum_{i\in I} \mathbb{K}e_i, \exists!(\lambda_i) \in \mathbb{K}^I \text{ presque nulle telle que } u = \sum_{i\in I} \lambda_i e_i$$

En d'autres termes, tout vecteur de E a au plus une décomposition en combinaisons linéaires des $e_i, i \in I$

Preuve :
Soit $u \in \sum_{i\in I} \mathbb{K}e_i$
On suppose que u a au plus 2 décompositions

$$u = \sum_{i\in I} \lambda_i e_i = \sum_{i\in I} \mu_i e_i$$

avec (λ_i) et (μ_i) presque nulles.
Alors,

$$0_E = u - u = \sum_{i\in I} \lambda_i e_i - \sum_{i\in I} \mu_i e_i = \sum_{i\in I} (\lambda_i - \mu_i) e_i$$

Or, $(e_i)_{i\in I}$ est libre donc

$$\forall i \in I, \lambda_i \mu_i = 0_{\mathbb{K}}$$

□

Proposition : Soit $(e_i)_{i\in I}$ une famille libre de E.

1. Toute sous famille de (e_i) est encore libre
2. Soit $u \in E$, $\mathcal{F} = (e_i \mid i \in I) \cup \{u\}$.

$$\mathcal{F} \text{ est libre } \iff u \notin \text{Vect}(e_i \mid i \in I)$$

3. (a) Quand on remplace un vecteur e_i par λe_i avec $\lambda \neq 0_{\mathbb{K}}$, la famille obtenue est libre.
   (b) Quand on remplace un vecteur e_i par $v + e_i$ avec $v \in \text{Vect}(e_j \mid j \neq i)$, la famille obtenue est libre.

Définition : Soit $(e_i)_{i\in I}$ une famille de vecteurs de E. On dit que (e_i) est une base de E si c'est à la fois une famille libre et génératrice de E ; i.e. si

$$E = \bigoplus_{i\in I} \mathbb{K}e_i$$

i.e. si

$$\forall u \in E, \exists!(\lambda_i) \in \mathbb{K}^I \text{ presque nulle telle que } u = \sum_{i \in I} \lambda_i e_i$$

Dans ce cas, on dit que les λ_i sont les coordonnées de u dans la base $(e_i)_{i \in I}$

EXEMPLE : 1. $(1, i)$ est une base de $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel
2. (1) est une base de $\mathbb{C}$ en tant que $\mathbb{C}$-espace vectoriel
3.

$$\begin{cases} u = 1 + i \\ v = 1 - i \end{cases}$$

(u, v) est une $\mathbb{R}$-base de $\mathbb{C}$
En effet, soit $z = a + ib \in \mathbb{C}$ avec $(a, b) \in \mathbb{R}^2$. Soient $\lambda, \mu \in \mathbb{R}$.

$$\begin{aligned} z = \lambda u + \mu v &\iff a + ib = \lambda + \mu + i(\lambda - \mu) \\ &\iff \begin{cases} a = \lambda + \mu \\ b = \lambda - \mu \end{cases} \\ &\iff \begin{cases} \lambda = \dfrac{a+b}{2} \\ \mu = \dfrac{a-b}{2} \end{cases} \end{aligned}$$

AUTRE MÉTHODE

$$\begin{aligned} &(1, i) \text{ base} \\ \text{donc } &(1, 1 + i) \text{ base} \\ \text{donc } &(1 - (1 + i), 1 + i) \text{ base} \\ \text{donc } &(-2i, 1 + i) \text{ base} \\ \text{donc } &(1 + i - 2i, 1 + i) \text{ base} \\ \text{donc } &(1 - i, 1 + i) \text{ base} \end{aligned}$$

EXEMPLE (Bases canoniques) : 1. La base canonique de $\mathbb{K}^n$ est $(e_1, \ldots, e_n)$ où $\forall i, e_i = (0_\mathbb{K}, \ldots, 0_\mathbb{K}, \underbrace{1_\mathbb{K}}_{\text{en } i\text{ème} position}, 0_\mathbb{K}, \ldots, 0_\mathbb{K})$ car

$$\begin{aligned} \forall u \in \mathbb{K}^n, \exists!(x_1, \ldots, x_n) \in \mathbb{K}^n, u = (x_1, \ldots, x_n) &= x_1(1_\mathbb{K}, 0_\mathbb{K}, \ldots, 0_\mathbb{K}) \\ &+ x_2(0_\mathbb{K}, 1_\mathbb{K}, \ldots, 0_\mathbb{K}) \\ &\vdots \qquad\qquad \vdots \\ &+ x_n(0_\mathbb{K}, 0_\mathbb{K}, \ldots, 1_\mathbb{K}) \\ &= \sum_{i=1}^{n} x_i e_i \end{aligned}$$

2. E l'ensemble des fonctions polynomiales de $\mathbb{K}$ dans $\mathbb{K}$ à coefficiants dans $\mathbb{K}$ où $\mathbb{K}$ est infini.
La base canonique de E est $(x \mapsto x^n)_{n\in\mathbb{N}}$ car

$$\forall P \in E, \exists! n \in \mathbb{N}, \exists!(a_0,\dots,a_n) \in \mathbb{K}^{n+1}, \forall x \in \mathbb{K}, P(x) = \sum_{i=0}^{n} a_i x^i$$

3. $E = \mathcal{M}_{n,p}(\mathbb{K})$
La base canonique de E est $(E_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}}$ où

$$\forall i \in [\![1,n]\!], \forall j \in [\![1,p]\!], E_{i,j} = \left(\sigma_{i,j}^{k,\ell}\right)_{\substack{1\leqslant k\leqslant n\\ 1\leqslant \ell\leqslant p}}$$

i.e.

$$E_{i,j} = \begin{pmatrix} & & \overset{j}{\downarrow} & & \\ 0_{\mathbb{K}} & \cdots & \cdots & \cdots & 0_{\mathbb{K}} \\ \vdots & & & & \vdots \\ \vdots & & 1_{\mathbb{K}} & & \vdots \\ \vdots & & & & \vdots \\ 0_{\mathbb{K}} & \cdots & \cdots & \cdots & 0_{\mathbb{K}} \end{pmatrix} \leftarrow i$$

$$\forall A = (a_{i,j}) \in \mathcal{M}_{n,p}, A = \sum_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}} a_{i,j} E_{i,j}$$

Chapitre 16

Dérivation

1 Définition et premières propriétés

Dans ce paragraphe, f désigne une fonction définie sur un intervalle ouvert non vide I à valeurs réelles.

Définition : Soit $a \in I$. On dit que f est dérivable en a si $\dfrac{f(x)-f(a)}{x-a}$ a une limite qui est finie quand $x \to a$.
Dans ce cas, cette limite est notée $f'(a)$ et est appelée nombre dérivée de f en a
On dit que f est dérivable sur I si f est dérivable en tout $a \in I$.
L'application $\begin{array}{c} I \longrightarrow \mathbb{R} \\ a \longmapsto f'(a) \end{array}$ est la dérivée de f et est notée f'

Proposition :

f est dérivable en $a \iff f$ a un développement limité d'ordre 1 au voisinage de a

Preuve
" $\Longrightarrow$ " $f'(a) = \lim\limits_{x\to a} \dfrac{f(x)-f(a)}{x-a}$
donc $\dfrac{f(x)-f(a)}{x-a} = f'(a) + \underset{x\to a}{o}(1)$
donc $f(x)-f(a) = (x-a)f'(a) + \underset{x\to a}{o}(x-a)$
donc $f(x) = f(a) + (x-a)f'(a) + \underset{x\to a}{o}(x-a)$
" $\Longleftarrow$ " $f(x) = a_0 + a_1(x-a) + \underset{x\to a}{o}(x-a)$

Alors, avec $x = a$, $a_0 = f(a)$ et donc

$$\frac{f(x) - f(a)}{x - a} = \frac{a_1(x-a) + o(x-a)}{x-a} = a_1 + o(1) \xrightarrow[x \to a]{} a_1 \in \mathbb{R}$$

□

Proposition : Si f est dérivable en a alors f est continue en a.

Preuve :

$$\forall x, f(x) = f(a) + f'(a)(x-a) + \underset{x \to a}{o}(x-a)$$

donc

$$\lim_{\substack{x \to a \\ \neq}} f(x) = f(a) + f'(a) \times 0 + 0 = f(a)$$

□

Proposition : Soient f et g dérivables en a

1. $f + g$ est dérivable en a et $(f+g)'(a) = f'(a) + g'(a)$
2. $f \times g$ est dérivable en a et $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$
3. Si $g(a) \neq 0$, alors $\dfrac{f}{g}$ est dérivable en a et

$$\left(\frac{f}{g}\right)'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{(g(a))^2}$$

Preuve :

$$\begin{cases} f(x) = f(a) + f'(a)(x-a) + o(x-a) \\ g(x) = g(a) + g'(a)(x-a) + o(x-a) \end{cases}$$

$$f(x) + g(x) = f(a) + g(a) + (x-a)\underbrace{(f'(a) + g'(a))}_{(f+g)'(a)} + o(x-a)$$

2.

$$f(x) \times g(x) = f(a)g(a) + (x-a)\underbrace{(f(a)g'(a) + g(a)f'(a))}_{(fg)'(a)} + o(x-a)$$

3. On suppose $g(a) \neq 0$

$$\begin{aligned}\frac{1}{g(x)} &= \frac{1}{g(a)+(x-a)g'(a)+\mathop{o}_{x\to a}(x-a)}\\ &= \frac{1}{g(a)}\times\frac{1}{1+(x-a)\frac{g'(a)}{g(a)}+\mathop{o}_{x\to a}(x-a)}\\ &= \frac{1}{g(a)}\times\left(1-(x-a)\frac{g'(a)}{g(a)}+\mathop{o}_{x\to a}(x-a)\right)\end{aligned}$$

D'où,

$$\begin{aligned}\frac{f(x)}{g(x)} &= \frac{1}{g(a)}\left(f(a)+(x-a)\left(-\frac{f(a)g'(a)}{g(a)}+f'(a)\right)\right)\mathop{o}_{x\to a}(x-a)\\ &= \frac{f(a)}{g(a)}+(x-a)\frac{-f(a)g'(a)+f'(a)g(a)}{(g(a))^2}+\mathop{o}_{x\to a}(x-a)\end{aligned}$$

□

Proposition : Soit f dérivable en a et g dérivable en $f(a)$. Alors, $f\circ g$ est dérivable en a et

$$(g\circ f)'(a) = g'(f(a))f'(a)$$

Preuve :

$$\begin{cases}\forall x, f(x) = f(a)+(x-a)f'(a)+\mathop{o}_{x\to a}(x-a)\\ \forall y, g(y) = g(f(a))+(y-f(a))g'(f(a))+\mathop{o}_{y\to f(a)}(y\to f(a))\end{cases}$$

Donc,

$$\begin{aligned}g(f(x)) &= g(f(a))+(f(x)-f(a))g'(f(a))+\mathop{o}_{x\to a}(f(x)-f(a)) \text{ car } f \text{ est continue en } a\\ &= g(f(a))+(x-a)f'(a)g'(f(a))+\mathop{o}_{x\to a}\left((x-a)f'(a)+\mathop{o}_{x\to a}(x-a)\right)\\ &= g(f(a))+(x-a)f'(a)g'(f(a))+\mathop{o}_{x\to a}(x-a)\end{aligned}$$

□

Proposition : On suppose que f est bijective dérivable en a et $f'(a)\neq 0$.

Si f^{-1} est continue, alors f^{-1} est dérivable en $f(a)$ et

$$\left(f^{-1}\right)'(f(a)) = \frac{1}{f'(a)}$$

Preuve :
$\forall y \neq f(a)$ on pose $x = f^{-1}(y)$.
$y \xrightarrow[x\to a]{} f(a)$ et $x \xrightarrow[y\to f(a)]{} a$

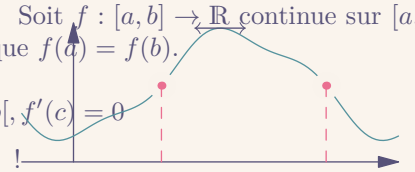
$$\frac{f^{-1}(y) - f^{-1}(f(a))}{y - f(a)} = \frac{x-a}{f(x)-f(a)} = \frac{1}{\frac{f(x)-f(a)}{x-a}} \xrightarrow[x\to a]{} \frac{1}{f'(a)}$$

□

2 Théorème de Rolle et accroissements finis

Théorème (Théorème de Rolle) **:** Soit $f : [a,b] \to \mathbb{R}$ continue sur $[a,b]$ et dérivable sur $]a,b[$. On suppose que $f(a) = f(b)$.
Alors,

$$\exists c \in]a,b[, f'(c) = 0$$



Preuve :
f est continue sur le segment $[a,b]$. On pose

$$\begin{cases} M = \max\limits_{[a,b]}(f) \\ m = \min\limits_{[a,b]}(f) \end{cases}$$

Cas 1

$$\exists c \in]a,b[, M = f(c)$$

$$f'(c) = \lim_{\substack{x\to c \\ <}} \frac{f(x)-f(c)}{x-c} \geqslant 0 \text{ car } \forall x < c, \begin{cases} f(x) - f(c) \leqslant 0 \\ x - c < 0 \end{cases}$$

$$= \lim_{\substack{x\to c \\ >}} \frac{f(x)-f(c)}{x-c} \leqslant 0 \text{ car } \forall x > c, \begin{cases} f(x) - f(c) \leqslant 0 \\ x - c > 0 \end{cases}$$

Donc, $f'(c) = 0$

Cas 2

$$\exists c \in]a,b[, m = f(c)$$

$$f'(c) = \lim_{\substack{x \to c \\ <}} \leqslant 0 \text{ car } \forall x < c \begin{cases} f(x) - f(c) \geqslant 0 \\ x - c < 0 \end{cases}$$
$$= \lim_{\substack{x \to c \\ >}} \frac{f(x) - f(c)}{x - c} \geqslant 0$$

Donc $f'(c) = 0$

Cas 3

$$\forall c \in]a, b[, f(c) \notin \{m, M\}$$

Alors

$$\begin{cases} M \in \{f(a), f(b)\} \\ m \in \{f(a), f(b)\} \end{cases}$$

Or, $f(a) = f(b)$ donc $M = m$ donc f est constante donc

$$\forall x \in [a, b], f'(x) = 0$$

□

Définition : On dit que f présente un maximum local en a s'il existe $\eta > 0$ tel que

$$\forall x \in]a - \eta, a + \eta[, f(x) \leqslant f(a)$$

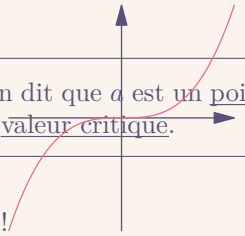
et un minimum local en a s'il existe $\eta > 0$ tel que

$$\forall x \in]a - \eta, a + \eta[, f(x) \geqslant f(a)$$

Un extremum local est un minimum local ou un maximum local.

Proposition : Soit $a \in I$ tel que $f(a)$ est un extremum local de f où f est dérivable en a. Alors, $f'(a) = 0$ □

Définition : Soit f dérivable et $a \in I$. On dit que a est un point critique de f si $f'(a) = 0$. On dit que $f(a)$ est une valeur critique.

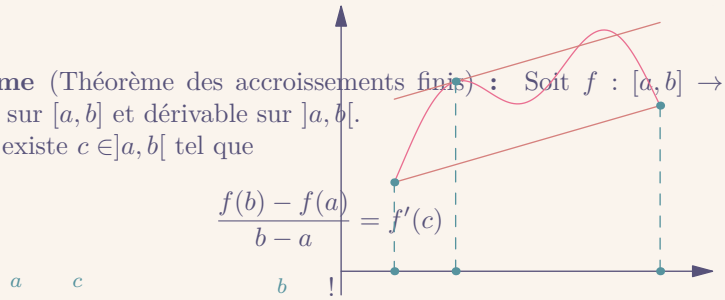


Exemple : !

$x \mapsto x^3$
$f'(0) = 0$ mais 0 n'est pas un extremum local

Théorème (Théorème des accroissements finis) **:** Soit $f : [a, b] \to \mathbb{R}$ continue sur $[a, b]$ et dérivable sur $]a, b[$.
Alors, il existe $c \in]a, b[$ tel que

$$\frac{f(b) - f(a)}{b - a} = f'(c)$$



Preuve :
On pose $\tau = \dfrac{f(b) - f(a)}{b - a}$
$g : x \mapsto f(x) - \tau x$ continue sur $[a, b]$ et dérivable sur $]a, b[$.
$g(a) - g(b) = f(a) - f(b) - \tau(a - b) = 0$
D'après le théorème de Rolle, il existe $c \in]a, b[$ tel que $g'(c) = 0$.

$$\forall x, g'(x) = f'(x) - \tau$$

Donc, $f'(c) = \tau$ □

Proposition : Soit $f : I \to \mathbb{R}$ dérivable avec I un intervalle non vide.

1. f est croissante sur $I \iff \forall x \in I, f'(x) \geqslant 0$
2. f est décroissante sur $I \iff \forall x \in I, f'(x) \leqslant 0$
3. $\forall x \in I, f'(x) > 0 \implies f$ strictement croissante
4. $\forall x \in I, f'(x) < 0 \implies f$ strictement décroissante
5. f constante $\iff \forall x \in I, f'(x) = 0$

Preuve : " $\not\Longrightarrow$ " On suppose f croissante.
Soit $x \in I$.

$$f'(x) = \lim_{y \to x} \frac{f(y) - f(x)}{y - x}$$

Or, $\forall y, f(y) - f(x)$ et $y - x$ sont de même signe donc $\dfrac{f(y) - f(x)}{y - x} \geqslant 0$.
Et donc $f'(x) \geqslant 0$.
" $\Longleftarrow$ " On suppose que

$$\forall x \in I, f'(x) \geqslant 0$$

Soit $(a, b) \in I^2$. On suppose que $a \leqslant b$.
f est continue sur $[a, b]$
f est dérivable sur $]a, b[$
donc, d'après le théorème des accroissements finis, il existe $c \in$

$]a,b[$ tel que

$$f(a)-f(b)=\underbrace{f'(c)}_{\geqslant 0}\underbrace{(a-b)}_{\leqslant 0}\leqslant 0$$

donc $f(a)\leqslant f(b)$
Donc f est croissante.

On procède de la même manière pour les autres propositions □

Théorème (Théorème de la limite de la dérivée) **:** Soit $f : I \to \mathbb{R}$ continue (sur I), $a \in I$. On suppose f dérivable sur $I\setminus\{a\}$ et que $\lim\limits_{\substack{x\to a\\ \neq}} f'(x)$ existe.
Alors,

$$\frac{f(x)-f(a)}{x-a} \xrightarrow[\substack{x\to a\\ \neq}]{} \lim_{\substack{x\to a\\ \neq}} f'(a)$$

Preuve :
On pose $\ell = \lim\limits_{\substack{x\to a\\ \neq}} f'(x) \in \overline{\mathbb{R}}$.
Soit $x \in I \setminus \{a\}$.
f est continue sur I donc sur $[a,x]$ si $x \geqslant a$ et sur $[x,a]$ si $x < a$
f est dérivable sur $I \setminus \{a\}$ donc sur $]a,x[$ si $x > a$ et sur $]x,a[$ si $x < a$
D'après le théorème des accroissements finis, il existe $c_x \in]a,x[\cup]x,a[$ tel que

$$\frac{f(x)-f(a)}{x-a} = f'(c_x)$$

— $\forall x < a$, on a $x < c_x < a$
Par encadrement, $c_x \xrightarrow[\substack{x\to a\\ <}]{} a$

— $\forall x > a$, on a $x > c_x > a$
Par encadrement, $c_x \xrightarrow[\substack{x\to a\\ >}]{} a$

Donc,

$$\lim_{\substack{x\to a\\ \neq}} c_x = a$$

donc

$$f'(c_x) \xrightarrow[\substack{x\to a\\ \neq}]{} \ell$$

(compositions des limites)

□

Proposition : Soit $f : I \to \mathbb{R}$ dérivable. On suppose qu'il existe $M \in \mathbb{R}$ tel que

$$\forall x \in I, |f'(x)| \leqslant M$$

Alors f est M-lipschitzienne sur I.

Preuve :
Soient $(a, b) \in I^2$.
D'après le théorème des accroissements finis, il existe $c \in I$ tel que

$$f(a) - f(b) = f'(c)(a - b)$$

donc

$$\begin{aligned} |f(a) - f(b)| &= |f'(c)|\,|a - b| \\ &\leqslant M\,|a - b| \end{aligned}$$

□

3 Dérivées n-ièmes

Définition : On dit que f est une fois dérivable si f est dérivable. Dans ce cas, on note $f^{(1)}$ la fonction f'.
Pour $n \in \mathbb{N}_\star$, on dit que f est dérivable n fois si f est dérivable $n-1$ fois et $f^{(n-1)}$ est dérivable une fois. Dans ce cas, $f^{(n)} = \left(f^{(n-1)}\right)'$.

Remarque (Convention) :

$$f^{(0)} = f$$

Définition : f est de classe $\mathscr{C}^n$ si f est dérivables n fois et $f^{(n)}$ est continue.

Proposition : Soit f dérivable n fois et $k \leqslant n$.
Alors f est dérivables k fois et $f^{(n)} = \left(f^{(k)}\right)^{(n-k)}$ □

Proposition : Soit f et g deux fonctions dérivables n fois en a.
Alors, $f + g$ est dérivable n fois en a et

$$(f + g)^{(n)}(a) = f^{(n)}(a) + g^{(n)}(a)$$

Si f et g sont de classe $\mathscr{C}^n$, alors, $f+g$ est de classe $\mathscr{C}^n$

Preuve (Récurrence immédiate sur n) *:*

□

Proposition (Leibniz) **:** Soient f et g dérivables n fois en a. Alors, $f\times g$ est dérivables n fois en a. et

$$(\star): \qquad (f\times g)^{(n)}(a)=\sum_{k=0}^{n}\binom{n}{k}f^{(n)}(a)g^{(n-k)}(a)$$

Si f et g sont de classe $\mathscr{C}^n$ alors $f\times g$ est de classe $\mathscr{C}^n$.

Preuve (par récurrence sur n) *:* — Soient f et g deux fonctions

$$(f\times g)^{(0)}(a)=(f\times g)(a)=f(a)g(a)$$

et

$$\sum_{k=0}^{0}\binom{0}{k}f^{(k)}(a)g^{(n-k)}(a)=f^{(0)}(a)g^{(0)}(a)=f(a)g(a)$$

— Soit $n\in\mathbb{N}$. On suppose $(\star)$ vraie quelles que soient les fonctions f et g dérivables n fois en a.
Soient f et g dérivables $n-1$ fois en a. En particulier, elles sont dérivables n fois en a. Donc

$$(f\times g)^{(n)}(a)=\sum_{k=0}^{n}\binom{n}{k}f^{(k)}(a)g^{(n-k)}(a)$$

$$\forall k\in[\![0,n]\!],\begin{cases}f^{(k)} \text{ est dérivables en } a\\ g^{(n-k)} \text{ est dérivables en } a\end{cases}$$

Donc, $(f\times g)^{(n)}$ est dérivable en a donc $f\times g$ est dérivables $n+1$ fois en a.

$$\begin{aligned}(f\times g)^{(n+1)}(a) &= \sum_{k=0}^{n}\binom{n}{k}\left(f^{(k+1)}(a)g^{(n-k)}(a)+f^{(k)}(a)g^{(n-k+1)}(a)\right)\\ &= \sum_{k=1}^{n}\binom{n}{k-1}f^{(k)}(a)\times g^{(n-k+1)}(a)+\sum_{k=0}^{n}\binom{n}{k}f^{(k)}(a)g^{(n-k+1)}(a)\\ &= \sum_{k=1}^{n}\binom{n+1}{k}f^{(k)}(a)g^{(n+1-k)}+f^{(n+1)}(a)g(a)+f(a)g^{(n+1)}(a)\\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}f^{(k)}(a)g^{(n+1-k)}(a)\end{aligned}$$

□

Proposition : Soient f et g dérivables n fois (resp. de classe $\mathscr{C}^n$). On suppose $g(a)\neq 0$.
Alors, $\dfrac{f}{g}$ est dérivables n fois (resp. $\mathscr{C}^n$) en a.

Preuve (par récurrence sur n) *:*
Le résultat est vrai pour $n=0$ et $n=1$.
Soit $n\in\mathbb{N}$ tel que pour toutes fonctions f et g dérivables n fois en a avec $g(a)\neq 0$, $\dfrac{f}{g}$ est aussi dérivables n fois en a.

Soient f et g dérivables $n+1$ fois en a telles que $g(a)\neq 0$. Alors, $\dfrac{f}{g}$ dérivable en a. et

$$\left(\frac{f}{g}\right)'(a)=\frac{f'(a)g(a)-f(a)g'(a)}{g(a)^2}$$

- f' est dérivables n fois en a
- g est dérivables n fois en a
- f est dérivables n fois en a
- g' est dérivables n fois en a

Donc, $f'\times g-f\times g'$ et g^2 sont dérivables n fois en a et $g(a)^2\neq 0$
D'après l'hypothèse de récurrence, $\dfrac{f'\times g-f\times g'}{g^2}$ est dérivable n fois en a
donc $\dfrac{f}{g}$ dérivable $n+1$ fois en a □

Proposition : Soit f dérivable n fois en a et g dérivable n fois en $f(a)$ (resp. f et g de classe $\mathscr{C}^n$).
Alors, $g \circ f$ est dérivable n fois en a (resp. de classe $\mathscr{C}^n$).

Preuve (similaire à la précédente) *:*

□

Définition : On dit que f est de classe $\mathscr{C}^\infty$ si f est de classe $\mathscr{C}^n$ pour tout $n \in \mathbb{N}$, i.e. f est dérivable une infinité de fois.

Proposition (formule de Taylor avec reste intégral) **:** Soit $f : I \to \mathbb{R}$ de classe $\mathscr{C}^{n+1}$ et $a \in I$. Alors

$$(\star) \qquad \forall x \in I, f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\, dt$$

Preuve (par récurrence sur n) *:* — Soit $f : I \to \mathbb{R}$ de classe $\mathscr{C}^1$ et $a \in I$.
Soit $x \in I$.

$$\begin{aligned}\sum_{k=0}^{0} \frac{f^{(k)}(a)}{k!}(x-a)^k + \int_a^x f^{(1)}(t)\frac{(x-t)^0}{0!}\, dt = f(a) + \int_a^x f'(t)\, dt \\ = f(a) + f(x) - f(a) \\ = f(x)\end{aligned}$$

— Soit $n \in \mathbb{N}$ tel que $(\star)$ est vraie pour toute fonction f de classe $\mathscr{C}^{n+1}$ sur $I \ni a$. Soit f de classe $\mathscr{C}^{n+2}$. Alors, f est de classe $\mathscr{C}^{n+1}$ donc

$$\forall x \in I, f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\, dt$$

Soit $x \in I$. On pose $\begin{cases} u : t \mapsto -\dfrac{(x-t)^{n+1}}{(n+1)!} \\ v = f^{(n+1)} \end{cases}$

Les fonctions u et v sont de classe $\mathscr{C}^1$ donc

$$\int_a^x u'(t)v(t)\, dt = [u(t)v(t)]_a^x - \int_a^x u(t)v'(t)\, dt$$

donc

$$\int_a^x f^{(n+1)}(t)\,dt = \left[-\frac{(x-t)^{n+1}}{(n+1)!}f^{(n+1)}(t)\right]_a^x + \int_a^x f^{(n+2)}(t)\frac{(x-t)^{n+1}}{(n+1)!}\,dt$$

D'où,

$$f(x) = \sum_{k=0}^{n}\frac{f^{(k)}}{k!}(x-a)^k + \frac{(x-a)^{n+1}}{(n+1)!}f^{(n+1)}(a) + \int_a^x f^{(x+2)}(t)\frac{(x-t)^{n+1}}{(n+1)!}\,dt$$

□

Proposition (Inégalité de Taylor-Lagrange) **:** Soit $f : I \to \mathbb{R}$ de classe $\mathscr{C}^{n+1}$ et $M \in \mathbb{R}$ tel que

$$\forall x \in I, \left|f^{(n+1)}(x)\right| \leqslant M$$

Alors, pour tout $a \in I$,

$$\forall x \in I, \left|f(x) - \sum_{k=0}^{n}\frac{(x-a)^k}{k!}f^{(k)}(a)\right| \leqslant M\frac{|x-a|^{n+1}}{(n+1)!}$$

Preuve :
D'après la formule de Taylor avec reste intégral,

$$\begin{aligned}\forall x \in I, \left|f(x) - \sum_{k=0}^{n}f^{(k)}(a)\frac{(x-a)^k}{k!}\right| &= \left|\int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\,dt\right| \\ &\leqslant \left|\int_a^x \left|f^{(n+1)}\right|(t)\frac{|x-t|^n}{n!}\,dt\right| \\ &\leqslant \left|\int_a^x M\frac{|x-t|^n}{n!}\,dt\right|\end{aligned}$$

On suppose $x \geqslant a$.

$$\begin{aligned}\left|f(x) - \sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(x-a)^k\right| &\leqslant M\int_a^x \frac{(x-t)^n}{n!}\,dt = M\left[-\frac{x-t)^{n+1}}{(n+1)!}\right]_a^x \\ &\leqslant M\frac{(x-a)^{n+1}}{(n+1)!}\end{aligned}$$

On suppose $x \leqslant a$.

$$\left|f(x)-\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(x-a)^k\right| \leqslant M\int_x^a \frac{(t-x)^n}{n!}\,dt$$
$$\leqslant M\left[\frac{(t-x)^{n+1}}{(n+1)!}\right]_x^a$$
$$\leqslant M\frac{(a-x)^{n+1}}{(n+1)!} = M\frac{|x-a|^{n+1}}{(n+1)!}$$

□

Exemple :

$$\forall x\in\mathbb{R}, e^x = \lim_{n\to+\infty}\sum_{k=0}^{n}\frac{x^k}{k!}$$

On pose

$$f:\mathbb{R}\longrightarrow\mathbb{R}$$
$$x\longmapsto e^x$$

. Soit $n\in\mathbb{N}$ et $a=0$.
f est de classe $\mathscr{C}^1$ sur $\mathbb{R}$. Soit $x\in\mathbb{R}^+$ et $I=[0,x]$

$$\forall t\in I, \left|f^{(n+1)}(t)\right| = \left|e^t\right| = e^t \leqslant e^x$$

$$\forall t\in I, \left|e^t-\sum_{k=0}^{n}\frac{t^k}{k!}\right| \leqslant e^x\frac{t^{n+1}}{(n+1)!} \xrightarrow[n\to+\infty]{} 0$$

donc

$$\forall t\in I, \lim_{n\to+\infty}\sum_{k=0}^{n}\frac{t^k}{k!} = e^t$$

donc

$$e^x = \lim_{n\to+\infty}\frac{x^k}{k!}$$

Exercice :
Montrer que $\ln 2 = \lim_{n\to+\infty}\sum_{k=1}^{n}\frac{(-1)^{k+1}}{k}$

4 Fonctions à valeurs complexes

Définition : Soient $f: I\to\mathbb{C}$, (I intervalle de $\mathbb{R}$) et $a\in I$.
f est dérivable en a si $\lim\limits_{\substack{x\to a\\ \neq}}\dfrac{f(x)-f(a)}{x-a}\in\mathbb{C}$

Proposition :

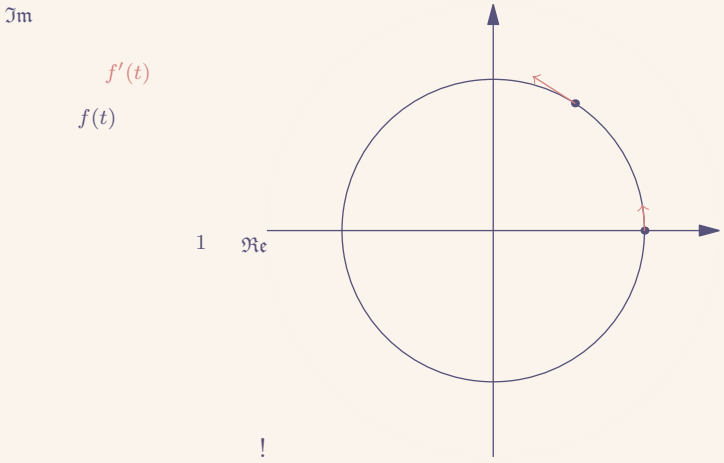
f est dérivable en $a \iff \mathfrak{Re}(f)$ et $\mathfrak{Im}(f)$ sont dérivables en a

Dans ce cas, $f'(a) = \mathfrak{Re}(f)'(a) + i\mathfrak{Im}(f)'(a)$ □

Proposition : La somme, le produit, de fonctions dérivables sont dérivables ; le quotient également si le dénominateur ne s'annule pas. □

Proposition : idem avec les dérivées n-ièmes □

Remarque (Attention B) :
Le théorème de Rolle n'est plus vraie.



$$f : \mathbb{R} \longrightarrow \mathbb{C}$$
$$t \longmapsto e^{it}$$

$f(0) = f(2\pi) = 1$
f est continue sur $[0, 2\pi]$ et dérivable sur $]0, 2\pi[$
$\forall t, f'(t) = ie^{it} \neq 0$

Proposition : La formule de Taylor avec reste intégral et l'inégalité de Taylor-Lagrange sont aussi vrais dans $\mathbb{C}$. □

Chapitre 17

Dimension finie

Définition : Soit E un $\mathbb{K}$-espace vectoriel. On dit que E est de dimension finie si E a au moins une famille génératrice finie. On dit que E est de dimension infinie sinon.

Théorème (Théorème de la base extraite) **:** Soit E un $\mathbb{K}$-espace vectoriel non nul de dimension finie. Soit $\mathcal{G}$ une famille génératrice finie de E. Alors, il existe une base $\mathcal{B}$ de $\mathcal{E}$ telle que $\mathcal{B} \subset \mathcal{G}$.

Preuve (par récurrence sur $\#G = \text{Card}(G)$) *:*

— Soit E un $\mathbb{K}$-espace vectoriel non nul engendré par $\mathcal{G} = (u)$.
Si $u = 0_E$, alors $E = \{0_E\}$: une contradiction $\lightning$
Donc $u \neq 0_E$ donc (u) est libre. En effet,

$$\forall \lambda \in \mathbb{K}, \lambda u = 0_E \implies \lambda = 0_{\mathbb{K}}$$

Donc $\mathcal{G}$ est une base de E.

— Soit $n \in \mathbb{N}_\star$. Soit E un $\mathbb{K}$-espace vectoriel. On suppose que si E a une famille génératrice constituée de n vecteurs, alors on peut extraire de cette famille une base de E.
Soit $\mathcal{G}$ une famille génératrice de E avec $n+1$ vecteurs.
Si $\mathcal{G}$ est libre, alors $\mathcal{G}$ est une base de E.
Si $\mathcal{G}$ n'est pas libre, alors il existe $u \in \mathcal{G}$ tel que $u \in \text{Vect}(\mathcal{G} \setminus \{u\})$
Donc $\mathcal{G} \setminus \{u\}$ engendre E. Or, $\mathcal{G} \setminus \{u\}$ possède n vecteurs. D'après l'hypothèse de récurrence, il existe une base $\mathcal{B}$ de E telle que

$$\mathcal{B} \subset \mathcal{G} \setminus \{u\} \subset \mathcal{G}$$

□

Corollaire : Tout espace de dimension finie a une base. □

Théorème (Théorème de la base incomplète) **:** Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $\mathcal{G}$ une famille génératrice finie de E. $\mathcal{L}$ une famille libre de E. Alors, il existe une base $\mathcal{B}$ de E telle que

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} \subset \mathcal{G}$$

Preuve (par récurrence sur $\#(\mathcal{G} \setminus \mathcal{L})$) *:* — Avec les notations précédentes, on suppose que $\mathcal{G} \setminus \mathcal{L} \neq$

$$\forall u \in \mathcal{G}, u \in \mathcal{L}$$

Donc $\mathcal{G} \subset \mathcal{L}$ donc $\mathcal{L}$ est génératrice donc $\mathcal{L}$ est une base de E. On pose $\mathcal{B} = \mathcal{L}$ et alors

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} = \subset \mathcal{G}$$

— Soit $n \in \mathbb{N}$. On suppose que si $\mathcal{G}$ est génératrice et $\mathcal{L}$ libre avec $\#(\mathcal{G} \setminus \mathcal{L}) = n$ alors il existe une base $\mathcal{B}$ de E telle que

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} \subset \mathcal{G}$$

Soient à présent $\mathcal{G}$ une famille génératrice de E et $\mathcal{L}$ une famille libre de E telles que $\#(\mathcal{G} \setminus \mathcal{L}) = n + 1 > 0$
Si $\mathcal{L}$ engendre E, alors $\mathcal{L}$ est une base de E. On pose $\mathcal{B} = \mathcal{L}$ et on a bien

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} = \subset \mathcal{G}$$

On suppose que $\mathcal{L}$ n'engendre pas E. Il existe $u \in \mathcal{G}$ tel que $u \notin \vec{(}\mathcal{L})$ (car sinon, $\mathcal{G} \subset \text{Vect}(\mathcal{L})$ et donc $\underbrace{\text{Vect}(\mathcal{G})}_{=E} \subset \underbrace{\text{Vect}(\mathcal{L})}_{\subset E}$
Donc $\mathcal{L} \cup \{u\}$ est libre. On pose $\mathcal{L}' = \mathcal{L} \cup \{u\}$

$$\mathcal{G} \setminus \mathcal{L}' = \mathcal{G} \setminus (\mathcal{L} \cup \{u\}) = (\mathcal{G} \setminus \mathcal{L}) \setminus \{u\}$$

donc $\#(\mathcal{G} \setminus \mathcal{L}') = n + 1 - 1 = n$
D'après l'hypothèse de récurrence, il existe $\mathcal{B}$ une base de E telle que

$$\mathcal{L} \subset \mathcal{L}' \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L}' \subset \mathcal{G}$$

$$\mathcal{B} \setminus \mathcal{L} = \underbrace{\mathcal{B} \setminus \mathcal{L}'}_{\subset \mathcal{G}} \cup \underbrace{\{u\}}_{\subset \mathcal{G} \text{ car } u \in \mathcal{G}}$$

On a $\mathcal{B} \setminus \mathcal{L} \subset \mathcal{G}$

□

Théorème : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Toutes les bases de E ont le même cardinal.

Preuve :
Soit $\mathcal{G}$ une famille génératrice finie de E et $\mathcal{B} \subset \mathcal{G}$ une base de E. On note $n = \#\mathcal{B}$
Soit $\mathcal{B}'$ une base de E. On pose $p = n - \#(\mathcal{B} \cap \mathcal{B}')$. Montrons par récurrence sur p que $\#\mathcal{B} = \#\mathcal{B}'$

— On suppose que $p = 0$. Alors, $\#(\mathcal{B} \cap \mathcal{B}') = n$
Or, $\mathcal{B}' \cap \mathcal{B} \subset \mathcal{B}$ donc $\mathcal{B} \cap \mathcal{B}' = \mathcal{B}$ donc $\mathcal{B} \subset \mathcal{B}'$ et donc $\mathcal{B} = \mathcal{B}'$

— Soit $p \in \mathbb{N}$. On suppose que si $\mathcal{B}'$ est une base de E telle que $n - \#(\mathcal{B} \cap \mathcal{B}') = p$, alors $\#\mathcal{B}' = n$
Aoit $\mathcal{B}'$ une base de E telle que $n - \#(\mathcal{B} \cap \mathcal{B}') = p + 1 > 0$
Donc $\mathcal{B} \cap \mathcal{B}' \neq \mathcal{B}$. Soit $u \in \mathcal{B}' \setminus \mathcal{B}$. D'après le lemme d'échange, il existe $v \in \mathcal{B} \setminus \mathcal{B}'$ tel que $\mathcal{B}' \setminus \{u\} \cup \{v\}$ est une base de E. On pose $\mathcal{B}'' = \mathcal{B}' \setminus \{u\} \cup \{v\}$

$$\begin{aligned} \mathcal{B}'' \cap \mathcal{B} &= ((\mathcal{B}' \setminus \{u\}) \cap \mathcal{B}) \cup \{v\} \\ &= (\mathcal{B}' \cap \mathcal{B}) \cup \{v\} \end{aligned}$$

donc,

$$\begin{aligned} n - \#(\mathcal{B}'' \cap \mathcal{B}) &= n - (\#(\mathcal{B}' \cap \mathcal{B}) + 1) \\ &= p + 1 - 1 \\ &= p \end{aligned}$$

D'après l'hypothèse de récurrence,

$$\#\mathcal{B}'' = n$$

Or, $\#\mathcal{B}'' = \#\mathcal{B}'$

□

Lemme : Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E telles que $\mathcal{B} \subset \mathcal{B}'$. Alors, $\mathcal{B} = \mathcal{B}'$.

Preuve :
On suppose $\mathcal{B}' \neq \mathcal{B}$. Soit $u \in \mathcal{B}' \setminus \mathcal{B}$ $u \in E = \text{Vect}(\mathcal{B})$ donc $\mathcal{B} \cup \{u\}$ n'est pas libre. Donc $\mathcal{B} \cup \{u\} \subset \mathcal{B}'$ et $\mathcal{B}'$ est libre donc $\mathcal{B} \cup \{u\}$ est libre : une contradiction $\lightning$ □

Lemme (Lemme d'échange) **:** Soient $\mathscr{B}_1$ et $\mathscr{B}_2$ deux bases de E et $u \in \mathscr{B}_1 \setminus \mathscr{B}_2$. Alors, il existe $v \in \mathscr{B}_2$ tel que $(\mathscr{B}_1 \setminus \{u\}) \cup \{v\}$ soit une base de E.

Preuve (1nde méthode) *:*
On suppose que pout tout $v \in \mathscr{B}_2$, $(\mathscr{B}_1 \setminus \{u\}) \cup \{v\}$ n'est pas une base de E Soit $v \in \mathscr{B}_2$.

— Supposons $(\mathscr{B}_1 \setminus \{u\}) \cup \{v\}$ non libre. $\mathscr{B}_1 \setminus \{u\}$ est libre. Donc $v \in \text{Vect}(\mathscr{B}_1 \setminus \{u\})$

— Supposons $(\mathscr{B}_1 \setminus \{u\}) \cup \{v\}$ non génératrice. Comme $\mathscr{B}_1$ engendre E, $u \notin \text{Vect}(\mathscr{B}_1 \setminus \{v\})$. On suppose que $\mathscr{B}_1 \neq \mathscr{B}_2$. $\forall v \in \mathscr{B}_2 \setminus \mathscr{B}_1, \text{Vect}(\mathscr{B}_1 \setminus \{v\}) = \text{Vect}(\mathscr{B}_1) = E \ni u$ donc, $(\mathscr{B}_1 \setminus \{u\}) \cup \{v\}$ engendre E et donc

$$v \in \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

On a aussi

$$\forall v \in \mathscr{B}_1 \setminus \{u\}, v \in \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

Comme $u \notin \mathscr{B}_2$, on a

$$\forall v \in \mathscr{B}_2, v \in \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

docn

$$E = \text{Vect}(\mathscr{B}_2) \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

donc $\mathscr{B}_1 \setminus \{u\}$ engendre E donc $\mathscr{B}_1 \setminus \{u\}$ est une base de E. Or, $\mathscr{B}_1 \setminus \{u\} \subset \mathscr{B}_1$, donc $\mathscr{B}_1 \setminus \{u\} = \mathscr{B}_1$

□

Preuve (2nde méthode) *:*
On suppose que pout tout $v \in \mathscr{B}_2$, $(\mathscr{B}_1 \setminus \{u\}) \cup \{v\}$ n'est pas une base de E

— Comme $u \in \mathscr{B}_1 \setminus \mathscr{B}_2$, nécéssairement $\mathscr{B}_1 \neq \mathscr{B}_2$ donc $\mathscr{B}_2 \not\subset \mathscr{B}_1$, donc $\mathscr{B}_2 \setminus \mathscr{B}_1 \neq$

— Soit $v \in \mathscr{B}_2 \setminus \mathscr{B}_1$. Il existe $(\lambda_w)_{w \in \mathscr{B}_1}$ une famille de scalaires presque nulle telle que

$$v = \sum_{w \in \mathscr{B}_1} \lambda_w w - \lambda_u u + + \sum_{w \in \mathscr{B}_1 \setminus \{u\}} \lambda_w w$$

Si $\lambda_u \neq 0_E$, alors

$$u = \lambda_u^{-1}\left(v - \sum_{w\in\mathscr{B}_1\setminus\{u\}} \lambda_w w\right)$$
$$\in \text{Vect}(\mathscr{B}_1 \setminus \{u\} \cup v)$$

donc $\mathscr{B}_1 \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\} \cup \{v\})$
et donc $E \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\} \cup \{v\})$
et donc $\mathscr{B}_1 \setminus \{u\} \cup \{v\}$ engendre E
donc $\mathscr{B}_1 \setminus \{u\} \cup \{v\}$ n'est pas libre
donc $v \in \text{Vect}(\mathscr{B}_1 \setminus \{u\})$ (car $\mathscr{B}_1 \setminus \{u\}$ est libre
donc $\lambda_u = 0_{\mathbb{K}}$ $\lightning$
‘

Donc, $\lambda_u = 0_{\mathbb{K}}$, docn $v \in \text{Vect}(\mathscr{B}_1 \setminus \{u\})$
On vient de prouver que

$$\mathscr{B}_2 \setminus \mathscr{B}_1 \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$
$$\mathscr{B}_1 \setminus \{u\} \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

Comme $u \notin \mathscr{B}_2$,

$$\mathscr{B}_2 \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

donc

$$E = \text{Vect}(\mathscr{B}_2) \subset \text{Vect}(\mathscr{B}_1 \setminus \{u\})$$

donc $\mathscr{B}_1 \setminus \{u\}$ engendre E. Donc, $\mathscr{B}_1 \setminus \{u\}$ est une base de E.
Or, $\mathscr{B}_1 \setminus \{u\} \subset \mathscr{B}_1$, donc $\mathscr{B}_1 \setminus \{u\} = \mathscr{B}_1$

□

Définition : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Le cardinal commun à toutes les bases de E est appelé dimension de E est notée $\dim(E)$ ou $\dim_{\mathbb{K}}(E)$
C'est donc aussi le nombre de coordonnées de n'importe quel vecteur dans n'importe quelle base.

Exemple : 1. $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ et $\dim_{\mathbb{C}}(\mathbb{C}) = 1$
2. $\dim_{\mathbb{K}}(\mathbb{K}^n) = n$
3. $\dim_{\mathbb{K}}(\mathscr{M}_{n,p}(\mathbb{K})) = np$

Corollaire : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $\mathscr{L}$ une famille libre de E, $\mathscr{G}$ une famille génératrice de E. On note $n = \dim(E)$
1. $\#\mathscr{G} \geqslant n$ et $(\#\mathscr{G} = n \implies \mathscr{G}$ est une base de $E)$
2. $\#\mathscr{L} \leqslant n$ et $(\#\mathscr{L} = n \implies \mathscr{L}$ est une base de $E)$

Corollaire : $\mathbb{R}^{\mathbb{R}}$ est de dimension infinie. $\forall i \in \mathbb{N}, e_i : x \mapsto x^i$
$(e_i)_{i\in\mathbb{N}}$ est libre dans $\mathbb{R}^{\mathbb{R}}$

Proposition : Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. Alors $E \times F$ est de dimension finie et $\dim(E \times F) = \dim(E) + \dim(F)$

Preuve :
Soit $(e_1, \dots, e_n)$ une base de E, $(f_1, \dots, f_p)$ une base de F. On pose

$$\begin{cases} u_1 &= (e_1, 0_F) \\ u_2 &= (e_2, 0_F) \\ &\vdots \\ u_n &= (e_n, 0_F) \\ u_{n+1} &= (0_E, f_1) \\ u_{n+2} &= (0_E, f_2) \\ &\vdots \\ u_{n+p} &= (0_E, f_p) \end{cases}$$

Soit $(x, y) \in E \times F$.

$$\left\{\exists (x_1, \dots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^{n} x_i e_i \exists (y_1, \dots, y_n) \in \mathbb{K}^n, x = \sum_{j=1}^{p} y_j f_j\right.$$

$$\begin{aligned} (x, y) &= \left(\sum_{i=1}^{n} x_i e_i, \sum_{i=1}^{p} y_j f_j\right) \\ &= \sum_{i=1}^{n} x_i (e_i + 0_F) + \sum_{j=1}^{p} y_j (0_E, f_j) \\ &= \sum_{i=1}^{n} x_i u_i + \sum_{j=1}^{p} y_j u_{n+j} \end{aligned}$$

Donc, $E \times F = \text{Vect}(u_1, \dots, u_{n+p})$ donc $E \times F$ est de dimension finie.
Soit $(\lambda_1, \dots, \lambda_{n+p}) \in \mathbb{K}^{n+p}$ tel que

$$(\star) : \quad \sum_{k=1}^{n+p} \lambda_k u_k = 0_{E\times F} = (0_E, 0_F)$$

$$
\begin{aligned}
(\star) &\iff \sum_{k=1}^{n} \lambda_k (e_k, 0_F) + \sum_{k=n+1}^{p} \lambda_k (0_E, f_{k-n}) = (0_E, 0_F) \\
&\iff \begin{cases} \displaystyle\sum_{k=1}^{n} \lambda_k e_k = 0_E \\ \displaystyle\sum_{k=n+1}^{p} \lambda_k f_{k-n} = 0_F \end{cases} \\
&\iff \begin{cases} \forall k \in [\![1, n]\!], \lambda_k = 0_{\mathbb{K}} & (\text{car } (e_1, \dots, e_n) \text{ est libre}) \\ \forall k \in [\![n+1, n+p]\!], \lambda_k = 0_{\mathbb{K}} & (\text{car } (f_1, \dots, f_n) \text{ est libre}) \end{cases}
\end{aligned}
$$

Donc $(u_1, \dots, u_{n+p})$ est une base de $E \times F$. Donc, $\dim(E \times F) = n + p = \dim(E) + \dim(F)$ □

Remarque (Convention) :

$$\dim\left(\{0_E\}\right) = 0$$

Théorème : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, F un sous-espace vectoriel de E. Alors, F est de dimension finie et $\dim(F) \leqslant \dim(E)$
Si $\dim(F) = \dim(E)$, alors $F = E$

Preuve :
On considère

$$A = \{k \in \mathbb{N} \mid \text{il existe une famille libre de } F \text{ à } k \text{ éléments}\}$$

On suppose $F \neq \{0_E\}$.

- Soit $u \in F \setminus \{0_E\}$. (u) est libre donc $1 \in A$ et donc $A \neq$
- Soit $\mathscr{L}$ une famille libre de F. Alors, $\mathscr{L}$ est une famille libre de E donc $\#\mathscr{L} \leqslant \dim(E)$
  Donc A est majorée par $\dim(E)$
  On en déduit que A a un plus grand élément p.
- Soit $\mathscr{L}$ une famille libre de F avec p éléments.
  Si $\mathscr{L}$ n'engendre pas F, alors il existe $u \in F$ tel que $u \notin \text{Vect}(\mathscr{L})$ et donc $\mathscr{L} \cup \{u\}$ est une famille libre de F, donc $p + 1 \in A$ en contradiction avec la maximalité de p.
  Donc $\mathscr{L}$ est une base de F donc F est de dimension finie et $\dim(F) = p \leqslant \dim(E)$

Soit $\mathscr{B}$ une base de F. Alors, $\mathscr{B}$ est aussi une famille de libre de de E. Donc $\#\mathscr{B} \leqslant \dim(E)$ donc $\dim(F) = \dim(E)$
Si $\dim(F) = \dim(E)$, alors $\mathscr{B}$ est une base de E, et donc $F = \text{Vect}(\mathscr{B}) = E$ □

Proposition (Formule de Grassmann) **:** Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, F et G deux sous-espace vectoriels de E. Alors,

$$\dim(F+G) = \dim(F) + \dim(G) - \dim(F \cap G)$$

Preuve :
Soit $(e_1, \dots, e_p)$ une base de $F \cap G$. $(e_1, \dots, e_p)$ est une famille libre de F. On complète $(e_1, \dots, e_p)$ en une base $(e_1, \dots, e_p, u_1, \dots, u_q)$ de F.
De même, on complète $(e_1, \dots, e_p)$ en une base $(e_1, \dots, e_p, v_1, \dots, v_r)$ de G.
On pose $\mathscr{B} = (e_1, \dots, e_p, u_1, \dots, u_q, v_1, \dots, v_r)$. Montrons que $\mathscr{B}$ est une base de $F+G$

— Soit $u \in F+G$
On pose $u = v + w$ avec $\begin{cases} v \in F \\ w \in G \end{cases}$.
On pose $v = \sum_{i=1}^{p} \lambda_i e_i + \sum_{i=1}^{q} \mu_i u_i$ avec $(\lambda_1, \dots, \lambda_p, \mu_1, \dots, \lambda_q) \in \mathbb{K}^{p+q}$
On pose aussi $w = \sum_{i=1}^{p} \lambda'_i e_i + \sum_{j=1}^{r} \nu_j v_j$ avec $(\lambda'_1, \dots, \lambda'_p, \nu_1, \dots, \nu_r) \in \mathbb{K}^{p+r}$
D'où,

$$u = \sum_{i=1}^{p} (\lambda_i + \lambda'_i) e_i + \sum_{j=1}^{q} \mu_j u_j + \sum_{k=1}^{r} \nu_k v_k \in \mathrm{Vect}(\mathscr{B})$$

— Soient $(\lambda_1, \dots, \lambda_p, \mu_1, \dots, \mu_q, \nu_1, \dots, \nu_r) \in \mathbb{K}^{p+q+r}$.
On suppose

$$(\star) \quad \sum_{i=1}^{p} \lambda_i e_i + \sum_{j=1}^{q} \mu_j u_j + \sum_{k=1}^{r} \nu_k v_k = 0_E$$

D'où,

$$\underbrace{\sum_{i=1}^{p} \lambda_i e_i + \sum_{j=1}^{q} \mu_j u_j}_{\in F} = \underbrace{-\sum_{k=1}^{r} \nu_j v_k}_{\in G}$$

Donc,

$$f = \sum_{i=1}^{p} \lambda_i e_i + \sum_{j=1}^{q} \mu_j u_j \in F \cap G$$

Comme $(e_1, \dots, e_p)$ est une base de $F \cap G$, $\exists!(\lambda'_1, \dots, \lambda'_p) \in \mathbb{K}^p$ tel

que

$$f = \sum_{i=1}^{p} \lambda_i' e_i = \sum_{i=1}^{p} \lambda_i' e_i + \sum_{j=1}^{q} 0_{\mathbb{K}} u_j$$

Comme $(e_1, \dots, e_p, u_1, \dots, u_q)$ est une base de F,

$$\forall k \in [\![1, q]\!], \mu_j = 0_{\mathbb{K}}$$

De même,

$$\forall k \in [\![1, r]\!], \nu_k = 0_{\mathbb{K}}$$

On remplace dans $(\star)$ pour trouver

$$\sum_{i=1}^{p} \lambda_i e_i = 0_E$$

Comme $(e_1, \dots, e_p)$ est libre,

$$\forall i \in [\![1, p]\!], \lambda_i = 0_{\mathbb{K}}$$

Donc $\mathscr{B}$ est libre.
Donc,

$$\begin{aligned} \dim(F+G) &= p + q + r \\ &= (p+q) + (p+r) - p \\ &= \dim(F) + \dim(G) - \dim(F \cap G) \end{aligned}$$

□

Corollaire : Avec les hypothèse précédentes,

$$E = F \oplus G \iff \begin{cases} F \cap G = \{0_E\} \\ \dim(E) = \dim(F) + \dim(G) \end{cases}$$

Preuvë " $\Longrightarrow$ " On suppose $E = F \oplus G$
Comme la somme est directe, $F \cap G = \{0_E\}$

$$\begin{aligned} \dim(E) &= \dim(F) \\ &= \dim(F) + \dim(G) - \dim(F \cap G) \\ &= \dim(F) + \dim(G) \end{aligned}$$

" $\Longleftarrow$ " On suppose $F \cap G = \{0_E\}$ et $\dim(E) = \dim(F) + \dim(G)$.
On sait déjà que $F + G = F \oplus G$

$$\dim(F+G) = \dim(F) + \dim(G) - \dim(F \cap G) = \dim(E)$$

Donc $F + G = E$

□

Proposition : Soit F un $\mathbb{K}$-espace vectoriel de dimension finie n. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de F. L'application

$$\begin{aligned} f : \mathbb{K}^n &\longrightarrow F \\ (\lambda_1, \ldots, \lambda_n) &\longmapsto \sum_{i=1}^{n} \lambda_i e_i \end{aligned}$$

est bijective.
Si $\mathbb{K}$ est infini, $\mathbb{K}^n$ aussi et donc F aussi.
Si $\#\mathbb{K} = p \in \mathbb{N}_\star$,

$$\begin{array}{c} \#\mathbb{K}^n = p^n \\ \| \\ \#F \end{array}$$

Chapitre 18

Polynômes formels

Dans ce chapitre, $\mathbb{K}$ désigne un corps

1 Définition

Définition : — Un polynôme à coefficients dans $\mathbb{K}$ est une suite presque nulle de $\mathbb{K}^{\mathbb{N}}$

— Le polynôme nul, noté 0 est la suite nulle.

— Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme non nul.
$\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$ est non-vide et majoré. Le degré de P est $\max\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$, et on le note $\deg(P)$ et $a_{\deg(P)}$ est le coefficient dominant de P, il est noté $\mathrm{dom}(P)$.

— Le degré du polynôme nul est $-\infty$

Proposition–Définition : Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$. Alors, $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$ est un polynôme appelé somme de P et Q.

Preuve :

$$\exists N_1 \in \mathbb{N}, \forall n \geqslant N_1, a_n = 0$$
$$\exists N_2 \in \mathbb{N}, \forall n \geqslant N_2, b_n = 0$$

On pose $N = \max(N_1, N_2)$ donc

$$\forall n \geqslant N, a_n + b_n = 0 + 0 = 0$$

donc $P + Q$ est une suite presque nulle. □

Proposition–Définition : Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$. On pose

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

La suite $(c_n)_{n\in\mathbb{N}}$ est presque nulle. Ce polynôme est appelé produit de P et Q et noté PQ.

Preuve :

$$\exists N_1 \in \mathbb{N}, \forall n \geqslant N_1, a_n = 0$$
$$\exists N_2 \in \mathbb{N}, \forall n \geqslant N_2, b_n = 0$$

On pose $N = N_1 + N_2$

$$\forall n \geqslant N, c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{N_1} a_k b_{n-k} + \sum_{k=N_1+1}^{n} a_k b_{n-k}$$

$\forall k \geqslant N_1 + 1$, $a_k = 0$ donc $\displaystyle\sum_{k=N_1+1}^{n} a_k b_{n-k} = 0$
$\forall k \leqslant N_1$, $b - k \geqslant n - N_1 \geqslant N_1 + N_2 - N_1 \geqslant N_2$ donc $\forall k \leqslant N_1, b_{n-k} = 0$
et donc $\displaystyle\sum_{k=0}^{N_1} a_k b_{n-k} = 0$
Donc

$$\forall n \geqslant N, c_n = 0$$

□

Remarque (Notation) :
Soit $P = (a_n)_{n\in\mathbb{N}}$, un polynôme à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. Le polynôme $(\lambda a_n)_{n\in\mathbb{N}}$ est noté λP

Remarque (Notation) :
On pose $X = (0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \ldots) = (\delta_{1,n})_{n\in\mathbb{N}}$

Exemple :

$$\begin{aligned} X^2 &= XX \\ &= (0\times 0, 0\times 1 + 1\times 0, 0\times 0 + 1\times 1 + 0\times 0, 0, \ldots) \\ &= (0, 0, 1, 0, \ldots) \end{aligned}$$

Théorème : Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme non nul à coefficients dans $\mathbb{K}$. Alors

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{où } n = \deg(P) \text{ et } X^0 = (1, 0, \ldots)$$

Preuve :

Pour $k \in \mathbb{N}$, $\mathscr{P}(n)$: "$X^k = (\delta_{k,n})_{\in\mathbb{N}}$" où $\delta_{k,n} = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{si } n \neq k \end{cases}$

— $\delta_{0,n} = (1, 0, \ldots) = X^0$ donc $\mathscr{P}(0)$ est vrai

— Soit $k \in \mathbb{N}$. On suppose $\mathscr{P}(k)$ vraie.

$$X^{k+1} = X^k\, X = (c_n)_{n\in\mathbb{N}}$$

où

$$\forall n \in \mathbb{N}, c_n = \sum_{j=0}^{n} \delta_{k,j}\delta_{1,n-j}$$

Donc, pour tout $n \in \mathbb{N}$ et pour tout $j \in [\![0, n]\!]$

$$\begin{aligned} \delta_{k,j}\delta_{1,n-j} \neq 0 &\iff \begin{cases} k = j \\ 1 = n - j \end{cases} \\ &\iff \begin{cases} k = j \\ n = k + 1 \end{cases} \end{aligned}$$

Donc, si $n \neq k + 1$, alors

$$\forall j \in [\![0, n]\!], \delta_{k,j}\delta_{1,n-j} = 0$$

et donc $c_n = 0$

$$c_{k+1} = \sum_{j=0}^{k+1} \delta_{k,j}\delta_{1,j+1-j} = \delta_{k,k}\delta_{1,1} = 1$$

Donc

$$\forall n \in \mathbb{N}, c_n = \delta_{k+1,n}$$

donc $\mathscr{P}(k + 1)$ est vraie

Ainsi, $\mathcal{P}(k)$ est vraie pour tout $k \in \mathbb{N}$. Soit $P = (a_0, \ldots, a_n, 0, \ldots)$ un polynôme de degré n.

$$\begin{aligned}\sum_{k=0}^{n} a_k X^k &= a_0(1,0,0,0,\ldots)\\ &\quad + a_1(0,1,0,0,\ldots)\\ &\quad + a_2(0,0,1,0,\ldots)\\ &\quad \vdots\\ &\quad + a_n(0,\ldots,0,1,0,\ldots)\\ &\quad = (a_0, a_1, \ldots, a_n, 0, \ldots)\\ &\quad = P\end{aligned}$$

□

Remarque (Notation) :
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ dont l'indéterminée $(0,1,0,\ldots)$ est notée X.

Proposition : $\big(\mathbb{K}[X], +, \times, \cdot\big)$ est une $\mathbb{K}$-algèbre commutative i.e.

1. $\big(\mathbb{K}[X], +, \times\big)$ est un anneau commutatif
2. $\big(\mathbb{K}[X], +, \cdot\big)$ est un $\mathbb{K}$-espace vectoriel
3. $\forall \lambda \in \mathbb{K}, \forall (P,Q) \in \big(\mathbb{K}[X]\big)^2, \lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$

Preuve : 1. $(\mathbb{K}[X], +)$ est un groupe abélien car $(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel

- $X^0 = (1, 0, \ldots)$ est le neutre de $\times$
  En effet, $\forall P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, en posant $(c_n)_{n\in\mathbb{N}} = PX^0$ on a
  $$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k \delta_{k,n-k} = a,$$
  donc $PX^0 = P$
- $\times$ est commutative : $\forall P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X], \forall Q = (b_n)_{n\in\mathbb{N}} \in$

$\mathbb{K}[X]$, on pose $R = (c_n)_{n\in\mathbb{N}} = PQ$, $S = (d_n)_{n\in\mathbb{N}} = QP$ alors

$$\begin{aligned}\forall n \in \mathbb{N}, c_n &= \sum_{k=0}^{n} a_k b_{n-k} \\ &= \sum_{j=0}^{n} a_{n-j} b_j \qquad (j = n-k) \\ &= \sum_{j=0}^{n} b_j a_{n-j} \\ &= d_n\end{aligned}$$

donc $PQ = QP$

— Soient

$$\begin{cases} P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \\ Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \\ R = (c_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \end{cases}$$

On pose

$$\begin{cases} S = (d_n)_{n\in\mathbb{N}} = PQ \\ T = (e_n)_{n\in\mathbb{N}} = SR = (PQ)R \\ U = (f_n)_{n\in\mathbb{N}} = QR \\ V = (g_n)_{n\in\mathbb{N}} = PU = P(QR) \end{cases}$$

Donc,

$$\begin{aligned}\forall n \in \mathbb{N}, e_n &= \sum_{k=0}^{n} d_k c_{n-k} \\ &= \sum_{k=0}^{n} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) c_{n-k} \\ &= \sum_{j=0}^{n} \sum_{k=j}^{n} a_j b_{k-j} c_{n-k} \\ &= \sum_{j=0}^{n} a_j \sum_{k=j}^{n} b_{k-j} c_{n-k} \\ &= \sum_{j=0}^{n} a_j \sum_{\ell=0}^{n-j} b_\ell c_{n-j-\ell} \qquad (\ell = k-j) \\ &= \sum_{j=0}^{n} a_j f_{n-j} \\ &= g_n\end{aligned}$$

Donc $T = V$

— Soient $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}, R = (C_n)_{n\in\mathbb{N}}$ trois polynômes et $P(Q+R) = (d_n)_{n\in\mathbb{N}}$ et $PQ + PR = (e_n)_{n\in\mathbb{N}}$.

$$\begin{aligned}\forall n \in \mathbb{N}, d_n &= \sum_{k=0}^{n} a_k(b_{n-k} + c_{n-k}) \\ &= \sum_{k=0}^{n} a_k b_{n-k} + \sum_{k=0}^{n} a_k c_{n-k} \\ &= e_n\end{aligned}$$

Donc, $\big(\mathbb{K}[X], +, \times\big)$ est un anneau commutatif

2. $\mathbb{K}[X] \subset \mathbb{K}^{\mathbb{N}}$
   $\big(\mathbb{K}^{\mathbb{N}}, +, \cdot\big)$ est un $\mathbb{K}$-espace vectoriel. D'après la propriété précédente,
   $$\mathbb{K}[X] = \text{Vect}\left((X^n \mid n \in \mathbb{N})\right)$$
   donc $\mathbb{K}[X]$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$
3. Soit $\lambda \in \mathbb{K}, P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes. On pose $(c_n)_{n\in\mathbb{N}} = PQ, R = (d_n)_{n\in\mathbb{N}} = \lambda(PQ), S = (e_n)_{n\in\mathbb{N}} = (\lambda P)Q, T = (f_n)_{n\in\mathbb{N}} = P(\lambda Q)$.
   $$\begin{aligned}\forall n \in \mathbb{N}, d_n = \lambda c_n &= \lambda \sum_{k=0}^{n} a_k b_{n-k} \\ &= \sum_{k=0}^{n} (\lambda a_k) b_{n-k} = e_n \\ &= \sum_{k=0}^{n} a_k (\lambda b_{n-k}) = f_n\end{aligned}$$

□

Remarque :
$(\mathscr{M}_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre non commutative (si $n > 1$)

Proposition : $i : \begin{array}{ccc}\mathbb{K} & \longrightarrow & \mathbb{K}[X] \\ \lambda & \longmapsto & \lambda X^0\end{array}$ est un morphisme d'algèbre injectif, i.e.

$$\forall \lambda, \mu \in \mathbb{K}, \begin{cases} i(\lambda + \mu) = i(\lambda) + i(\mu) \\ i(\lambda \cdot \mu) = i(\lambda) \times i(\mu) \end{cases}$$

et i est injective.

Remarque (Notation) :
On identifie $\lambda \in \mathbb{K}$ avec $\lambda X^0 \in \mathbb{K}[X]$. Ainsi, on peut écrire $X^0 = 1$, on peut écrire $2 + X + 3X^2$ au lieu de $2X^0 + X + 3X^2$

Proposition : Soient $P, Q \in \mathbb{K}[X]$

- $\deg(P+Q) \leqslant \max\big(\deg(P), deg(Q)\big)$
- Si $\deg(P) \neq \deg(Q)$, alors
  - $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big)$
  - $\mathrm{dom}(P+Q) = \begin{cases} \mathrm{dom}(P) & \text{si } \deg(P) > \deg(Q) \\ \mathrm{dom}(Q) & \text{si } \deg(P) < \deg(Q) \end{cases}$
- Si $\deg(P) = \deg(Q)$ et $\mathrm{dom}(P) + \mathrm{dom}(Q) \neq 0$,
  alors $\begin{cases} \deg(P+Q) = \deg(P) = \deg(Q) \\ \mathrm{dom}(P+Q) = \mathrm{dom}(P) + \mathrm{dom}(Q) \end{cases}$
- Si $\deg(P) = \deg(Q)$ et $\deg(P) + \deg(Q) = 0$, alors $\deg(P+Q) < \deg(P)$

Preuve :
- Si $P = 0$, alors $\deg(P+Q) = \deg(Q)$ et donc $\max\big(\deg(P), \deg(Q)\big) = \max\big(-\infty, \deg(Q)\big)$
  On a bien $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$
- De même avec $Q = 0$
- On suppose $P \neq 0$ et $Q \neq 0$
  On pose $\begin{cases} P = \sum_{k=0}^{p} a_k X^k & p = \deg(P) \\ Q = \sum_{k=0}^{q} b_k X^k & q = \deg(Q) \end{cases}$
  On peut supposer $p \geqslant q$. On pose $b_{q+1} = \ldots = b_p = 0$ si $p > q$
  Ainsi, $Q = \sum_{k=0}^{p} b_k X^k$
  $P + Q = \sum_{k=0}^{p} (a_k + b_k) X^k$ donc $\deg(P+Q) \leqslant p$ et $p = \max\big(\deg(P), \deg(Q)\big)$
  De plus, $a_p + b_p = \begin{cases} \underset{\neq 0}{\mathrm{dom}(P)} & \text{si } p > q \\ \mathrm{dom}(P) + \mathrm{dom}(Q) \text{ si } p = q \end{cases}$

□

Proposition : Soient $P, Q \in \mathbb{K}[X]$. Alors

$$\deg(PQ) = \deg(P) + \deg(Q)$$

Preuve :
Si P ou Q est nul, alors la formule est vraie car

$$\begin{cases} \deg(PQ) = -\infty \\ \deg(P) + \deg(Q) = \begin{cases} \text{cste} - \infty = -\infty \\ -\infty + \text{cste} = -\infty \\ -\infty - \infty = -\infty \end{cases} \end{cases}$$

On suppose $P \neq 0$ et $Q \neq 0$. On pose $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$ et $Q = \sum_{k=0}^{q} b_k X^k$ avec $b_q \neq 0$

$$\begin{aligned} PQ &= \left(\sum_{k=0}^{p} a_k X^k\right)\left(\sum_{\ell=0}^{q} b_\ell X^\ell\right) \\ &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell X^{k+\ell} \end{aligned}$$

donc $\deg(PQ) \leqslant p+q$ et le coefficient devant X^{p+q} est $a_p b_q \neq 0$ (car $\mathbb{K}$ est intègre)
donc $\deg(PQ) = p+q$ □

2 Évaluation

Définition : Soit A une $\mathbb{K}$-algèbre et $P \in \mathbb{K}[X]$. On pose $P = \sum_{k=0}^{n} e_k X^k$.
Soit $a \in A$.
On pose

$$\begin{aligned} P(a) &= \sum_{k=0}^{n} e_k a^k \\ &= e_0 1_A + e_1 a + e_2 a^2 + \cdots + e_n a^n \in A \end{aligned}$$

On dit qu'on a <u>évalué</u> P en a, ou <u>spécialisé</u> X avec la valeur de a, ou <u>remplacé</u> X par a, <u>substitué</u> a à X.

Définition : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
On dit que a est une <u>racine de P</u> si $P(a) = 0_{\mathbb{K}}$.

Définition : Soit $P \in \mathbb{K}[X] \in \mathscr{M}_n(\mathbb{K})$. On dit que c'est un polynôme de matrices.

Exemple :
$P = 1 + 2X - 3X^2$, $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$$\begin{aligned} P(A) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - 3\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} - 3\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ -4 & 0 \end{pmatrix} \end{aligned}$$

Définition : Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^{n} a_k X^k$.

Alors $P(Q) = \sum_{k=0}^{n} a_k Q^k \quad \in \mathbb{K}[X]$

C'est la composée de P et Q.

Remarque (B Attention) :
Ne pas confondre $\underbrace{P(X+1)}_{\text{composée}}$ et $\underbrace{P(X+1)}_{\text{produit}}$.
On a $\underbrace{P(X+1)}_{\text{produit}} = (X+1)\,P = P(X)\,(X+1) = P \times (X+1)$

Proposition : Soient $P, Q \in \mathbb{K}[X]$ avec $\begin{cases} Q \neq 0 \\ P \neq 0 \end{cases}$. On a

$$\deg\big(P(Q)\big) = \deg(P) \times \deg(Q)$$

□

Exemple :
$\mathbb{K} = {}^{\mathbb{Z}}/_{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$

$P = X^2 + X + 1 \in \mathbb{K}[X]$ et $Q = 1 \in \mathbb{K}[X]$
$P \neq Q$

$$\begin{aligned} f_P : {}^{\mathbb{Z}}/_{2\mathbb{Z}} &\longrightarrow {}^{\mathbb{Z}}/_{2\mathbb{Z}} \\ x &\longmapsto P(x) \end{aligned}$$

$$\begin{aligned} f_Q : {}^{\mathbb{Z}}/_{2\mathbb{Z}} &\longrightarrow {}^{\mathbb{Z}}/_{2\mathbb{Z}} \\ x &\longmapsto Q(x) \end{aligned}$$

$f_P\left(\overline{0}\right) = \overline{1} = f_Q\left(\overline{0}\right)$
$f_P\left(\overline{1}\right) = \overline{1} + \overline{1} + \overline{1} = \overline{1} = f_Q\left(\overline{1}\right)$
donc $f_P = f_Q$ alors que $P \neq Q$

Théorème : Soit A une $\mathbb{K}$-algèbre. L'application

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow A^A \\ P \longmapsto f_P : \begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & P(a) \end{array} & \end{aligned}$$

vérifie

1. $\forall P, Q \in \mathbb{K}[X], \varphi(P+Q) = \varphi(P) + \varphi(Q)$
2. $\forall P, Q \in \mathbb{K}[X], \varphi(PQ) = \varphi(P) \times \varphi(Q)$
3. $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X], \varphi(\lambda P) = \lambda\varphi(P)$

□

Exemple :
$\mathbb{K} = \mathbb{R}$
$X^2 - 1 = (X-1)(X+1)$

— $\mathbb{C}$ est une $\mathbb{R}$-algèbre donc

$$\forall z \in \mathbb{C}, z^2 - 1 = (z-1)(z+1)$$

— $\mathscr{M}_2(\mathbb{R})$ est une $\mathbb{R}$-algèbre

$$\forall A \in \mathscr{M}_2(\mathbb{R}), A^2 - I_2 = (A - I_2)(A + I_2)$$

Définition : Soit $P \in \mathbb{K}[X]$,

$$P = \sum_{k=0}^{n} a_k X^k$$

Le polynôme dérivé de P est

$$P' = \sum_{k=0}^{n} k a_k X^{k-1} = \sum_{k=1}^{n} k a_k X^{k-1}$$

où

$$\forall k \in [\![1, n]\!], ka_k = \underbrace{a_k + \cdots + a_k}_{k \text{ fois}}$$

$$0_{\mathbb{N}} a_k = 0_{\mathbb{K}}$$

Remarque :
Si $P \in \mathbb{R}[X]$, $f_p : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P(x) \end{array}$
$f_{P'} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P'(x) \end{array}$ alors $f_{P'} = f'_P$

Proposition :

$$\forall P \in \mathbb{K}[X], \deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg(P) > 0 \\ -\infty & \text{sinon} \end{cases}$$

Proposition : Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

1. $(P + Q)' = P' + Q'$
2. $(PQ)' = P'Q + PQ'$
3. $(\lambda P)' = \lambda P'$

Preuve :
On pose

$$P = \sum_{k=0}^{p} a_k X^k \qquad Q = \sum_{k=0}^{q} b_k X^k$$

1. On peut supposer $p \geqslant q$
   Si $p > q$, on pose $b_{q+1} = \cdots = b_p = 0$

   $$P + Q = \sum_{k=0}^{p} (a_k + b_k) X^k$$

   donc

   $$\begin{aligned} (P + Q)' &= \sum_{k=0}^{p} k(a_k + b_k) X^{k-1} \\ &= \sum_{k=0}^{p} k a_k X^{k-1} + \sum_{k=0}^{p} k b_k X^{k-1} \\ &= P' + Q' \end{aligned}$$

2.
$$PQ = \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell X^{k+\ell}$$
D'après 1.,
$$\begin{aligned}(PQ)' &= \sum_{k=0}^{p}\sum_{\ell=0}^{q}\left(a_k b_\ell X^{k+\ell}\right)' \\ &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell (k+\ell) X^{k+\ell-1} \\ &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} k a_k b_\ell X^{k-1+\ell} + \sum_{k=0}^{p}\sum_{\ell=0}^{q} \ell a_k b_\ell X^{k+\ell-1} \\ &= \sum_{k=0}^{p} k_k X^{l-1}\sum_{\ell=0}^{q} b_\ell X^{\ell} + \sum_{k=0}^{p} a_k X^k \sum_{\ell=0}^{q} \ell b_\ell X^{\ell-1} \\ &= P'Q + PQ'\end{aligned}$$

3.
$$\lambda P = \sum_{k=0}^{p} \lambda a_k X^k$$
donc
$$(\lambda P)' = \sum_{k=0}^{p} \lambda a_k k X^{k-1} = \lambda \sum_{k=0}^{p} k a_k X^{k-1} = \lambda P'$$

□

Définition : Pour $k \in \mathbb{N}$, on définit la dérivée k-ième d'un polynôme $P \in \mathbb{K}[X]$ par
- si $k = 0$, $P^{(k)} = P$
- si $k = 1$, $P^{(1)} = P'$
- si $k > 1$, $P^{(k)} = \left(P^{(k-1)}\right)'$

Proposition :
$$\forall k, j \in \mathbb{N}^2, \left(X^k\right)^{(j)} = \begin{cases} 0 & \text{si } j > k \\ k(k-1)\cdots(k-j+1)X^{k-j} = \dfrac{k!}{(k-j)!}X^k & \text{si } j \leqslant k \end{cases}$$

Preuve (par récurrence sur j à k fixé) *:*

□

Proposition : Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$

1. $\forall k \in \mathbb{N}, (P+Q)^{(k)} = P^{(k)} + Q^{(k)}$
2. $\forall k \in \mathbb{N}, (PQ)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} P^{(i)} Q^{(k-i)}$
3. $\forall k \in \mathbb{N}, (\lambda P)^{(k)} = \lambda P^{(k)}$

Preuve (par récurrence sur k) *:*

□

3 Arithmétique dans $\mathbb{K}[X]$

Définition : Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B (dans $\mathbb{K}[X]$) s'il existe $C \in \mathbb{K}[X]$ tel que

$$AC = B$$

On dit dans ce cas que A est un diviseur de B ou que B est un multiple de A. On le note alors $A \mid B$
On dit que A et B sont associés s'il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $A = \lambda B$. Il s'agit d'une relation d'équivalence.

Proposition : Soient $A, B \in \mathbb{K}[X]$.

$$\left.\begin{array}{l} A \mid B \\ B \mid A \end{array}\right\} \iff A \text{ et } B \text{ sont associés}$$

Preuve " $\Longrightarrow$ " Soit $C \in \mathbb{K}[X]$ tel que $AC = B$ et $D \in \mathbb{K}[X]$ tel que $BD = A$.
D'où,

$$A = BD = ACD$$

Or, $\mathbb{K}[X]$ est un anneau intègre.
D'où

$$A(1 - CD) = 0$$

donc $A = 0$ ou $CD = 1$
Si $A = 0$, alors $B = 0 \times C = 0 = 1 \times A$ donc A et B sont associés
Si $CD = 1$, on sait que $\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$
Alors, A et B sont associés.

" $\Longleftarrow$ " évident

□

Lemme : $\mathbb{K}[X]$ est un anneau intègre.

Preuve :
Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. On suppose que $P \neq 0$ et $Q \neq 0$
Alors $\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0$
Or, $PQ = 0$ et $\deg(0) = -\infty$: $\lightning$ une contradiction □

Lemme :

$$\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$$

Preuve :
Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 1$.
Alors, $0 = \deg(1) = \deg(PQ) = \deg(P) + \deg(Q)$
Comme $P \neq 0$, $\deg(P) \geqslant 0$. De même, $\deg(Q) \geqslant 0$
Done $\deg(P) = \deg(Q) = 0$ Donc, il existe $\lambda, \mu \in \mathbb{K}$ tels que $\lambda\mu = 1$
Donc $\lambda \in \mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ □

Proposition : $\mid$ est une relation réflexive et transitive. □

Proposition : Soient $A, B, C \in \mathbb{K}[X]$ tels que $A \mid B$ et $A \mid C$. Alors

$$\forall (P, Q) \in \mathbb{K}[X]^2, A \mid BQ + CP$$

□

Proposition–Définition : Soit $A \in \mathbb{K}[X], B \in \mathbb{K}[X] \setminus \{0\}$.

$$\exists ! (P, Q) \in \mathbb{K}[X]^2, \begin{cases} A = PQ + R \\ \deg(R) < \deg(B) \end{cases}$$

On dit que Q est le quotient et R le reste de la division (euclidienne) de A par B.

Preuve : — On prouve l'existence par récurrence sur le degré de A. On fixe $B \in \mathbb{K}[X] \setminus \{0\}$

$$\forall n \in \mathbb{N}, \mathscr{P}(n) : \text{“ } \forall A \in \mathbb{K}[X] \text{ tel que } \deg(A) = n,$$
$$\exists (Q,R) \in \mathbb{K}[X]^2, \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases} \text{ ”}$$

— Soit $A \in \mathbb{K}[X]$. On suppose $\deg(A) = 0$
Si $\deg(B) > 0$ alors on pose $Q = 0$ et $R = A$. Ainsi $\begin{cases} BQ + R = A \\ \deg(R) = 0 < \deg(B) \end{cases}$
Si $\deg(B) = 0$, alors $A = \lambda$ et $B = \mu$ avec $(\lambda, \mu) \in (\mathbb{K} \setminus \{0\})^2$.
On pose $\begin{cases} Q = \mu^{-1}\lambda \\ R = 0 \end{cases}$. Alors, $\begin{cases} BQ + R = \mu\mu^{-1}\lambda = \lambda = A \\ \deg(R) = -\infty < 0 = \deg(B) \end{cases}$

Donc $\mathscr{P}(0)$ est vraie.

— Soit $n \in \mathbb{N}$. On suppose $\mathscr{P}(k)$ pour tout $k \leqslant n$. Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) = n+1$. On pose $p = \deg(B)$
Si $p > n+1$, on pose $\begin{cases} Q = 0 \\ R = A \end{cases}$ et on a

$$\begin{cases} BQ + R = A \\ \deg(R) = n+1 < p = \deg(B) \end{cases}$$

Si $p \leqslant n+1$. On pose $\begin{cases} Q = a_{n+1} b_b^{-1} X^{n+1-p} \\ R = A - BQ \end{cases}$ où $\begin{cases} a_{n+1} = \mathrm{dom}(A) \\ a_p = \mathrm{dom}(b) \end{cases}$ On a $A = BQ + R$
Or, $\begin{cases} \deg(BQ) = p + n + 1 - p = n + 1 = \deg(A) \\ \mathrm{dom}(BQ) = b_p b_p^{-1} a_{n+1} = a_{n+1} = \mathrm{dom}(A) \end{cases}$
donc $\deg(R) < \deg(A)$ donc $\deg(R) \leqslant n$
D'après $\mathscr{P}(n)$,

$$\exists (Q_1, R_1) \in \mathbb{K}[X]^2, \begin{cases} R = BQ_1 + R_1 \\ \deg(R_1) < \deg(B) \end{cases}$$

D'où,

$$\begin{aligned} A &= BQ + R \\ &= BQ + BQ_1 + R_1 \\ &= B(Q + Q_1) + R_1 \end{aligned}$$

et $\deg(R_1) < \deg(B)$ donc $\mathcal{P}(n+1)$ est vraie.

Donc, $\mathcal{P}(n)$ est vraire pour tout $n \in \mathbb{N}$ par récurrence forte. Si $A = 0$, on pose $Q = R = 0$ et on a bien $BQ + R = 0 = A$ et $\deg(R) = -\infty < \deg(B)$

— Unicité

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On suppse que $A = BQ_1 + R_1 = BQ_2 + R_2$ avec $Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ et $\begin{cases}\deg(R_1) < \deg(B)\\ \deg(R_2) < \deg(B)\end{cases}$

D'où,

$$B(Q_1 - Q_2) = R_2 - R_1$$

Or,

$$\deg(R_2 - R_1) \leqslant \max\big(\deg(R_2), \deg(R_1)\big) < \deg(B)$$

Or,

$$\begin{aligned}\deg\big(B(Q_1 - Q_2)\big) &= \deg(B) + \deg(Q_1 - Q_2)\\ &\geqslant \deg(B) \text{ si } Q_1 - Q_2 \neq 0\end{aligned}$$

Donc,

$$\begin{cases}Q_1 - Q_2 = 0\\ R_2 - R_1 = B(Q_2 - Q_1) = 0\end{cases}$$

et donc

$$\begin{cases}Q_1 = Q_2\\ R_2 = R_1\end{cases}$$

□

Exemple :

Division euclidienne de $A = X^5 + X^3 - X^2 + 1$ par $B = X^2 + \frac{1}{2}X - 1$ dans $\mathbb{R}[X]$

$$
\begin{array}{r|l}
X^5+X^3-X^2+1 & X^2+\frac{1}{2}X-1 \\
\hline
-\quad X^5+\frac{1}{2}X^4-X^3 & X^3-\frac{1}{2}X^2+\frac{9}{4}X-\frac{21}{8} \\
\hline
-\frac{1}{2}X^4+2X^3-X^2+1 & \\
-\quad -\frac{1}{2}X^4-\frac{1}{4}X^3+\frac{1}{2}X^2 & \\
\hline
\frac{9}{4}X^3-\frac{3}{2}X^2+1 & \\
-\quad \frac{9}{4}X^3+\frac{9}{8}X^2-\frac{9}{4}X & \\
\hline
-\frac{21}{8}X^2+\frac{9}{4}X+1 & \\
-\quad -\frac{21}{8}X^2-\frac{21}{16}X+\frac{21}{8} & \\
\hline
\frac{57}{16}X-\frac{13}{8} &
\end{array}
$$

quotient

reste

Théorème : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$P(a) = 0 \iff X - a \mid P$$

Preuve " $\Longleftarrow$ " On suppose $P = (X - A) \times Q$ avec $Q \in \mathbb{K}[]$. On substitue a à X

$$P(a) = (a - a) \times Q(a) = 0_{\mathbb{K}} \times Q(a) = 0_{\mathbb{K}}$$

" $\Longrightarrow$ " On suppose que $P(a) = 0$. On réalise la division euclidienne de P par $X - a$:

$$\begin{cases} P = (X - a) \times Q + R \\ \deg(R) < \deg(X - a) = 1 \end{cases}$$

donc $R = \lambda$ avec $\lambda \in \mathbb{K}$
D'où,

$$0 = P(a) = (a - a) \times Q(a) + R(a) = \lambda$$

donc

$$P = (X - a) \times Q$$

et donc

$$X - a \mid P$$

□

Corollaire : Soit $P \in \mathbb{K}[X]$ non nul de degré n. Alors, P a au plus n racines distinctes dans $\mathbb{K}$

Preuve (par récurrence sur n) *:* — C'est évident pour $n = 0$

— Soit $n \in \mathbb{N}$. On suppose la proposition vraie pour les polynômes de degré n.
Soit $P \in \mathbb{K}[X]$ de degré $n+1$
Si P n'a pas de racine alors le résultat est trivialement vrai pour P
Si P a une racine a, alors il existe $Q \in \mathbb{K}[X]$ non nul tel que $P = (X-a) \times Q$
$n+1 = \deg(P) = 1 + \deg(Q)$ donc $\deg(Q) = n$
D'après l'hypothèse de récurrence, Q a au plus n racines distinctes
Soit b une racine de P différente de a. Alors,

$$0 = P(b) = \underbrace{(b-a)}_{\neq 0} \times Q(b)$$

donc $Q(b) = 0$

Donc P a bien au plus $n+1$ racines. □

Définition : Soient A et B deux polynômes dont l'un au moins est non nul, $D \in \mathbb{K}[X]$. On dit que D est un PGCD de A et B si D est un diviseur commun de A et B et de degré maximal.

Proposition : Avec les hypothèse précédents, deux PGCD quelconques de A et B sont nécessairement associés

Preuve :
On forme

$$E = \left\{ AU + BV \mid (U,V) \in \mathbb{K}[X]^2 \right\}$$

— E est un sous-groupe de $(\mathbb{K}[X], +)$
— $\forall P \in E, \forall Q \in \mathbb{K}[X], PQ \in E$

On dit que E est un *idéal* de $\mathbb{K}[X]$

Soit $D \in E$ un polynôme non nul de degré minimal. Soit $P \in E$ On divise

P par D :

$$\begin{cases} P = DQ + R \\ \deg(R) < \deg(D) \end{cases}$$

D'où

$$R = \underbrace{P}_{\in E} - \underbrace{DQ}_{\in E} \in E$$

$\deg(R) < \deg(D)$ donc $R = 0$
Donc,

$$\forall P \in E, D \mid P$$

$A \in E$ donc $D \mid A$
$B \in E$ donc $D \mid B$

Soit Δ un diviseur commun quelconque de A et B. On pose $D = AU + BV$
$\left.\begin{matrix} \Delta \mid A \\ \Delta \mid B \end{matrix}\right\}$ donc $\Delta \mid AU + BV$ donc $\Delta \mid D$
donc $\deg(\Delta) \leqslant \deg(D)$

Ainsi, D est un PGCD de A et B. De plus, Δ est un PGCD de A et B alors

$$\begin{cases} \Delta \mid D \\ \deg(\Delta) = \deg(D) \end{cases}$$

Donc $D = \Delta Q$ avec $\begin{cases} Q \in \mathbb{K}[X] \\ \deg(Q) = 0 \end{cases}$
donc D et Δ sont associés. □

Remarque :
Dans la preuve précédente, on a aussi montré les deux propositions suivantes.

Théorème (Théorème de Bézout) **:** Soient $A, B \in \mathbb{K}[X]$ tels que $A \neq 0$ ou $B \neq 0$
Soit D un PGCD de A et B. Alors

$$\exists (U, V) \in \mathbb{K}[X]^2, AU + BV = D$$

■

Proposition : Avec les hypothèses précédents,

$$\forall \Delta \in \mathbb{K}[X],$$
$$\left.\begin{matrix} \Delta \mid A \\ \Delta \mid B \end{matrix}\right\} \iff \Delta \mid D$$

■

Définition : On dit qu'un polynôme est unitaire si sont coefficient dominant vaut 1.

Proposition–Définition : Soient A et B deux polynômes dont l'un au moins est non nul. Parmi tous les PGCD de A et B, un seul est unitaire. On le note $A \wedge B$.

Preuve :
Soit D un PGCD de A et B. Alors $\mathrm{dom}(D)^{-1}D$ est associé à D, donc c'est un PGCD de A et B et il est unitaire. Soient D et Δ deux PGCD unitaires de A et B. Ils sont associés

$$\Delta = \lambda D \text{ avec } \lambda \in \mathbb{K} \setminus \{0\}$$

D'où,

$$1 = \mathrm{dom}(\Delta) = \lambda \,\mathrm{dom}(D) = \lambda$$

Donc $\Delta = D$ □

Proposition : Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Soit R le reste de la division de A par B. Alors,

$$A \wedge B = B \wedge R$$

Preuve (idem que dans $\mathbb{Z}$) *:*

□

Exemple :
$D = (5X^2 + 3X - 1) \wedge (X + 3)$

$$\begin{array}{r|l} X^2 + 3X - 1 & X + 3 \\ \hline -\ 5X^2 + 15X & 5X - 12 \\ \hline -12X - 1 & \\ -\ -12X - 36 & \\ \hline 35 & \end{array} \qquad \begin{array}{r|l} X + 3 & 35 \\ \hline -\ X & \frac{1}{35}X + \frac{3}{35} \\ \hline 3 & \\ -\ 3 & \\ \hline 0 & \end{array}$$

$$D = (X + 3) \wedge 35 = 1$$

Théorème (Théorème de Gauß) **:** Soient A, B, C trois polynômes non nuls tels que $\begin{cases} A \mid BC \\ A \wedge B = 1 \end{cases}$
Alors, $A \mid C$

Preuve (idem que dans $\mathbb{Z}$) *:*

□

Corollaire : Avec les notations précédentses,

$$\left.\begin{array}{l} A \mid B \\ B \mid C \\ A \wedge B = 1 \end{array}\right\} \Longrightarrow AB \mid C$$

Proposition : Soient A et B deux polynômes non nuls et D un PGCD de A et B. Soit $x \in \mathbb{K}$.

$$A(x) = B(x) = 0 \iff D(X) = 0$$

Preuve " $\Longrightarrow$ " On suppose $A(x) = B(x) = 0$
D'après le théorème de Bézout,

$$D = AU + BV \text{ avec } (U, V) \in \mathbb{K}[X]^2$$

Donc,

$$D(x) = A(x)U(x) + B(x)V(x) = 0 + 0 = 0$$

" $\Longleftarrow$ " On suppose $D(x) = 0$. On pose $\begin{cases} A = DA_1 \\ B = DB_1 \end{cases}$ avec $(A_1, B_1) \in \mathbb{K}[X]^2$
D'où,

$$\begin{cases} A(x) = D(x)A_1(x) = 0 \\ B(x) = D(x)B_1(x) = 0 \end{cases}$$

□

Définition : Soit $P \in \mathbb{K}[X]$.

On dit que P n'est pas irréductible si il existe $(Q, R) \in \mathbb{K}[X]^2$ non constants tels que $P = QR$ **ou** si P est constant.

Sinon, on dit que P est irréductible.

EXEMPLE : 1. X^2+1 est irréductible dans $\mathbb{R}[X]$
On suppose que

$$X^2+1 = QR \text{ avec } (Q,R) \in \mathbb{R}[X]^2$$

$$\begin{cases} \deg(Q) > 0 \\ \deg(R) > 0 \end{cases}$$

Donc, P et Q sont de degré 1, donc ont chacun une racine réelle donc X^2+1 a au moins une racine réelle : $\lightning$ une contradiction.

2. X^2+1 n'est pas irréductible dans $\mathbb{C}[X]$:

$$X^2+1 = (X-i)(X+i)$$

3. X^4+1 n'est pas irréductible dans $\mathbb{R}[X]$ et pourtant il n'a aucune racine réelle.

$$\begin{aligned} X^2+1 &= X^4+2X^2+1-2X^2 \\ &= \left(X^2+1\right)^2 - 2X^2 \\ &= \underbrace{\left(X^2+1-\sqrt{2}X\right)}_{\in\mathbb{R}[X]} \underbrace{\left(X^2+1+\sqrt{2}X\right)}_{\in\mathbb{R}[X]} \end{aligned}$$

Théorème (Théorème de D'Alembert - Gauß) **:**

$$\forall P \in \mathbb{C}[X] \text{ non constant}, \exists a \in \mathbb{C}, P(a) = 0$$

□

Corollaire : Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactemenent les polynômes de degré 1.

Preuve :
Les polynômes de degré 1 sont évidemment irréductibles.
Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) \geqslant 2$. Soit $a \in \mathbb{C}$ une racine de P.
Donc $X-a \mid P$.

$$\begin{cases} P = (X-a) \times Q \\ Q \in \mathbb{C}[X] \end{cases}$$

$\left.\begin{array}{l}\deg(Q) \geqslant 1 \\ \deg(X-a)=1\end{array}\right\}$ donc P n'est pas irréductible. □

Exemple :
Factoriser X^4+1 dans $\mathbb{C}$
Les racines complexes de X^4+1 sont $\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, $-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, $\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$ et $-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$
Donc,

$$\begin{aligned} X^4-1 = &\left(X-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right)\left(X+\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right) \\ &\times\left(X+\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)\left(X-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)\end{aligned}$$

Définition : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $\mu \in \mathbb{N}$.
On dit que a est une racine de P de multiplicité μ si

$$\begin{cases} (X-a)^\mu \mid P \\ (X-a)^{\mu+1} \nmid P \end{cases}$$

Si $\mu=1$, on dit que a est une racine simple.
Si $\mu=2$, on dit que a est une racine double.

Remarque :
a est une racine de multiplicité 0 si et seulement si $P(a) \neq 0$

Lemme : Soient $(A,B) \in \mathbb{R}[X]^2$ non nuls. On suppose que A divise B dans $\mathbb{C}[X]$
Alors, A divise B dans $\mathbb{R}[X]$

Preuve :
On suppose que

$$(\star) \qquad B = AQ \text{ avec } Q \in \mathbb{C}[X]$$

On divise B par A dans $\mathbb{R}[X]$:

$$(\star\star) \qquad B = AQ_1 + R_1 \text{ avec } \begin{cases}(Q_1,Q_2) \in \mathbb{R}[X]^2 \\ \deg(R_1) < \deg(A)\end{cases}$$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, $(\star\star)$ est aussi le résultat de la division euclidienne de B par A dans $\mathbb{C}[X]$.

($\star$) correspond aussi à une division euclidienne dans $\mathbb{C}[X]$
Par unicité, $\begin{cases} Q = Q_1 \in \mathbb{R}[X] \\ R_1 = 0 \end{cases}$
Donc A divise B dans $\mathbb{R}[X]$ □

Proposition : Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$, $\mu \in \mathbb{N}$.
Si a est une racine de P de multiplicité μ alors $\overline{a}$ est une racine de P de multiplicité μ.

Preuve (par récurrence sur μ) *:*
On pose

$\forall n \in \mathbb{N}, \mathcal{P}(n)$: "$\forall P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ racine de P de multiplicité μ, alors $\overline{a}$ est aussi une racine de P de multiplicité μ"

— Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ tel que $P(a) \neq 0$.
On pose $P = \sum_{i=0}^{p} \alpha_i X^i$ avec $\alpha_0, \dots, \alpha_p \in \mathbb{R}$

$$\begin{aligned} P(\overline{a}) &= \sum_{i=0}^{p} \alpha_i \overline{a}^i \\ &= \sum_{i=0}^{p} \overline{\alpha_i} \overline{a^i} \\ &= \sum_{i=0}^{p} \overline{\alpha_i a^i} \\ &= \overline{\left(\sum_{i=0}^{p} \alpha_i a^i \right)} \\ &= \overline{P(a)} \\ &\neq 0 \end{aligned}$$

Donc $\mathcal{P}(0)$ est vraie
— Soit $\mu \in \mathbb{N}$. On suppose $\mathcal{P}(\mu)$ vraie.
Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ une racine de P de multiplicité $\mu + 1$. On pose

$$\begin{cases} P = (X - a)^{\mu+1} Q \\ Q \in \mathbb{C}[X] \\ Q(a) \neq 0 \end{cases}$$

On pose aussi $P = \sum_{i=0}^{p} \alpha_i a^i$ avec $\alpha_0, \dots, \alpha_p \in \mathbb{R}$

$\mu+1 \geqslant 1$ donc $P(a)=0$. D'où, $P(\overline{a})=\overline{P(a)}=\overline{0}=0$
donc $\underbrace{(\overline{a}-a)^{\mu+1}}_{\neq 0} Q(\overline{a})=0$
Donc, $Q=(X-\overline{a})Q_1$ avec $Q_1 \in \mathbb{C}[X]$
D'où

$$\begin{aligned} P &= (X-a)^{\mu+1}(X-\overline{a})Q_1 \\ &= (X-a)(X-\overline{a})(X-a)^{\mu}Q_1 \end{aligned}$$

Or,

$$\begin{aligned} (X-a)(X-\overline{a}) &= X^2-(a+\overline{a})X+a\overline{a} \\ &= X^2-2\mathfrak{Re}(a)X=|a|^2 \in \mathbb{R}[X] \end{aligned}$$

D'après le lemme précédent, $(X-a)^{\mu}Q_1 \in \mathbb{R}[X]$
De plus,

$$0 \neq Q(a)=(\overline{a}-a)Q_1(a)$$

docn $Q_1(a) \neq 0$
Donc a est une racine de $(X-a)^{\mu}Q_1 \in \mathbb{R}[X]$ de multiplicité μ.
D'après $\mathcal{P}(\mu)$, $\overline{a}$ est aussi une racine de $(X-a)^{\mu}Q_1$ de multiplicité μ.
Donc, on peut écrire

$$(X-a)^{\mu}Q_1=(X-\overline{a})^{\mu}Q_2 \text{ avec } \begin{cases} Q_2 \in \mathbb{C}[X] \\ Q_2(\overline{a}) \neq 0 \end{cases}$$

Donc,

$$P=(X-a)(X-\overline{a})^{\mu+1}Q_2$$

Donc $\overline{a}$ est une racine de P de multiplicité $\mu+1$

□

Corollaire : Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatifs.

Preuve :
- Les polynômes de de degré 1 sont évidemment irréductibles
- Les polynômes constants ne sont pas irréductibles par définition
- Les polynômes de degré 2 ayant au moins une racine réelle peuvent s'écrire comme produit de deux polynômes réels de degré 1 à coefficients réels

— Réciproquement, si un polynôme de degré 2 n'est pas irreductible, c'est forcémet un produit de 2 polynômes de degré 1 à coefficients réels et donc ce polynôme a au moins une racine réelle

— Soit $P \in \mathbb{R}[X]$ tel que $\deg(P) \geqslant 3$
On note $a_1, \dots, a_r$ les racines réelles distictes de P,

$$a_{r+1}, \overline{a_{r+1}}, a_{r+2}, \overline{a_{r+2}}, \dots, a_s, \overline{a_s}$$

les récines non réelles distictes de P. On note aussi

$$\forall k \in [\![1, s]\!], \mu_k \text{ la multiplicité de } a_k$$

Donc

$$P = \mathrm{dom}(P)(X - a_1)^{\mu_1} \cdots (X - a_r)^{\mu_r}(X - a_{r+1})^{\mu_{r+1}}(X - \overline{a_{r+1}})^{\mu_{r+1}} \times \cdots \times (X - a_s)^{\mu_s}(X - \overline{a_s})^{\mu_s}$$

Or,

$$\begin{aligned} \forall k \geqslant r+1, (X - a_k)^{\mu_k}(X - \overline{a_k})^{\mu_k} &= ((x-a)(x-\overline{a}))^{\mu_k} \\ &= (X^2 - 2\mathfrak{Re}(a)X + |a|^2 \\ &\in \mathbb{R}[X] \end{aligned}$$

D'où,

$$P = \underbrace{\mathrm{dom}(P)}_{\in \mathbb{R}} \underbrace{\prod_{k=1}^{r}(X - a_k)^{\mu_k}}_{\in \mathbb{R}[X]} \prod_{k=r+1}^{s} \underbrace{\left(X^2 - 2\mathfrak{Re}(a_k)X + |a_k|^2\right)^{\mu_k}}_{\in \mathbb{R}[X]}$$

P irréductible $\iff$
- il y a une unique racine réelle simple et aucune racine non réelle
- OU
- il n'y a aucune racine réelle et 2 racines non réelles conjuguées simples

□

Théorème : Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Tout polynôme de $\mathbb{K}$ se découpe en produit de facteurs irréductibles dans $\mathbb{K}[X]$ et cette décomposition est unique à multiplication par une constante non nulle près. □

Proposition : Soient $A, B \in \mathbb{C}[X]$ non nuls.

$$A \mid B \iff \begin{array}{l}\forall a \in \mathbb{C},\ \text{si } a \text{ est une racine de } A \text{ de multiplicité } \mu \in \mathbb{N},\\ \text{alors } a \text{ est racine de } B \text{ avec une multiplicité} \geqslant \mu\end{array}$$

Preuve " $\Longrightarrow$ " On suppose $A \mid B$
Soit $a \in \mathbb{C}$ une racine de A de multiplicité μ
Alors, $(X-a)^{\mu} \mid A$ donc $(X-a)^{\mu} \mid B$
Donc a est une racine de B de multiplicité $\geqslant \mu$

" $\Longleftarrow$ " On décompose A et B en produit de facteurs irréductibles sur $\mathbb{C}[X]$:

$$B = \mathrm{dom}(B) \prod_{a \in \mathcal{R}} (X-a)^{\nu_a}$$

où $\mathcal{R}$ est l'ensemble des racines de B ; et

$$A = \mathrm{dom}(A) \prod_{a \in \mathcal{S}} (X-a)^{\mu_a}$$

où $\mathcal{S}$ est l'ensemble des racines de A
On suppose que $\begin{cases}\mathcal{S} \subset \mathcal{R}\\ \forall a \in \mathcal{S}, \mu_a \leqslant \nu_a\end{cases}$
D'où,

$$B = \frac{\mathrm{dom}(B)}{\mathrm{dom}(A)} \underbrace{\mathrm{dom}(A) \prod_{a \in \mathcal{S}} (X-a)^{\mu_a}}_{A} \times \underbrace{\prod_{a \in \mathcal{S}} (X-a)^{\nu_a - \mu_a} \times \prod_{a \in \mathcal{R} \setminus \mathcal{S}} (X-a)^{\nu_a}}_{\in \mathbb{C}[X]}$$

Donc, $A \mid B$

□

Exercice :
Montrer que $1 + X + X^2 \mid X^{3n} - 1$
Les racines de $1 + X + X^2$ sont j et j^2

$$j^{3n} - 1 = \left(j^3\right)^n - 1 = 1 - 1 = 0$$
$$\left(j^2\right)^{3n} = \left(j^3\right)^{2n} - 1 = 1 - 1 = 0$$

Proposition : Soit $P \in \mathbb{C}[X]$ de degré $n > 0$
Alors P a exactement n racines comptées avec multiplicité.

Preuve :

$$P = \mathrm{dom}(P) \times \prod_{a \in \mathscr{R}} (X-a)^{\mu_a}$$

où $\mathscr{R}$ est l'ensemble des racines distinctes de P
$n = \deg(P) = \sum_{a \in \mathscr{R}} \deg\left((X-a)^{\mu_a}\right) = \sum_{a \in \mathscr{R}} \mu_a$ □

4 L'espace vectoriel $\mathbb{K}[X]$

Remarque (Rappel) :
$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel engendré par $(1, X, X^2, \ldots)$

Proposition : La famille $(X^n)_{n \in \mathbb{N}}$ est libre.

Preuve :
Soit $(\lambda_n)_{n \in \mathbb{N}}$ une famille presque nulle de scalairees telle que $\sum_{n \in \mathbb{N}} \lambda_n X^n = 0$
$(\lambda_n)_{n \in \mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$: on le note P.
Or,

$$\sum_{n \in \mathbb{N}} \lambda_n X^n = (\lambda_0, \lambda_1, \ldots, \lambda_n, \ldots) = P$$

Donc $P = 0$ donc

$$\forall n \in \mathbb{N}, \lambda_n = 0$$

□

Corollaire :

$$\dim\left(\mathbb{K}[X]\right) = +\infty$$

□

Définition : Pour $n \in \mathbb{N}$, on note

$$\mathbb{K}_n[X] = \left\{P \in \mathbb{K}[X] \mid \deg(P) \leqslant n\right\}$$

Théorème : $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n+1$

Preuve :
$\mathbb{K}_n[X] = \text{Vect}\left(1, X, \ldots, X^n\right)$ □

Proposition : Soit $(P_i)_{i\in I}$ une famille de polynômes non nuls telle que

$$\forall i \neq j, \deg(P_i) \neq \deg(P_j)$$

Alors $(P_i)_{i\in I}$ est libre.

Preuve :
Soit $n \in \mathbb{N}$ et $i_1, \ldots, i_n$ des éléments distincts de I
Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$. On suppose

$$\lambda_1 P_{i_1} + \cdots + \lambda_n P_{i_n} = 0$$

Quitte à renuméroter les polynômes, on peut supposer que

$$\forall k \in [\![1, n]\!], \deg\left(P_{i_n}\right) > \deg\left(P_{i_k}\right)$$

Si $\lambda_n \neq 0$,

$$\deg\left(\lambda_1 P_{i_1} + \cdots + \lambda_n P_{i_n}\right) = \deg\left(P_{i_n}\right) \neq -\infty$$

Donc $\lambda_n = 0$
Donc $\lambda_1 P_{i_1} + \cdots + \lambda_{n-1} P_{i_{n-1}} = 0$

On conclut par récurrence sur n. □

Théorème (Formule de Taylor) **:** Soit $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$.

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Preuve :
$\left(1, X-a, \ldots, (X-a)^n\right)$ est libre.
Comme $\dim\left(\mathbb{K}_n[X]\right) = n+1$, c'est une base de $\mathbb{K}_n[X]$.
Donc, il existe $(\lambda_0, \ldots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que

$$P = \sum_{k=0}^{n} \lambda_k (X-a)^k$$

On remarque que

$$P(a) = \lambda_0$$

$$\forall i \in [\![1, n]\!], P^{(i)}(a) = \sum_{k=0}^{n} \lambda_k \underbrace{\left((X-a)^k\right)^{(i)}}_{=\begin{cases} 0 & \text{si } k < i \\ i! & \text{si } k = i \\ \frac{k!}{(k-i)!}(X-a)^{k+1} & \text{si } k > i \end{cases}}(a)$$

$$= \lambda_i i!$$

Donc $\lambda_i = \dfrac{P^{(i)}(a)}{i!}$ □

Proposition : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$\left.\begin{array}{r} a \text{ est une racine de } P \\ \text{de multiplicité } \mu \end{array}\right\} \iff \begin{cases} \forall k \leqslant \mu - 1, P^{(k)}(a) = 0 \\ P^{(\mu)}(a) \neq 0 \end{cases}$$

Preuve :
On pose $n = \deg(P)$

“ $\Longleftarrow$ ”

$$\begin{aligned} P &= \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \\ &= \sum_{k=\mu}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \\ &= (X-a)^\mu \underbrace{\sum_{k=\mu}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-\mu}}_{Q \in \mathbb{K}[X]} \end{aligned}$$

$$\text{Donc } \begin{cases} (X-a)^\mu \mid P \\ Q(a) = \dfrac{P^{(\mu)}(a)}{\mu!} \neq 0 \end{cases}$$

“ $\Longrightarrow$ ”

$$\begin{cases} P = (X-a)^\mu Q \\ Q(a) \neq 0 \end{cases}$$

$$\begin{aligned}\forall k \leqslant \mu - 1, P^{(k)}(a) &= \sum_{j=0}^{k} \binom{k}{j} \left((X-a)^{\mu}\right)^{(j)}(a) Q^{(k-j)}(a) \\ &= \sum_{j=0}^{k} \binom{k}{j} \frac{\mu!}{(\mu-j)!} \underbrace{(a-a)^{\mu-j}}_{=0} Q^{(k-j)}(a) \\ &= 0\end{aligned}$$

$$\begin{aligned}P^{(\mu)}(a) &= \binom{\mu}{\mu} \times \mu! \times 1 \times Q^{(0)}(a) \\ &= Q(a) \\ &\neq 0\end{aligned}$$

□

Corollaire : Avec les notations précédentes, si a est une racine de P de multiplicité μ, alors a est une racine de P' de multiplicité $\mu - 1$

□

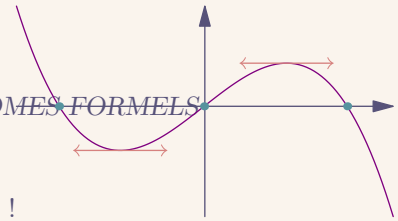
Définition : On dit qu'un polynôme P est scindé sur $\mathbb{K}$ si P est un produit de polynômes de $\mathbb{K}[X]$ de degré 1, i.e. toutes les racines de P sont dans $\mathbb{K}$

Exercice : 1. Soit $P \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$ à racines simples avec $\deg(P) \geqslant 2$. Montrer que P' est scindé sur $\mathbb{R}$ à racines simple.

2. Soit $P \in \mathbb{R}[X]$ scindé avec $\deg(P) \geqslant 2$. Montrer que P' est scindé.

tion

1.



Soit $P \in \mathbb{R}[X]$ avec $\deg(P) = n$ scindé sur $\mathbb{R}$.
On note $x_1 < x_2 < \cdots < x_n$ les n racines de P
Soit $f_P : \mathbb{R} \to \mathbb{R}$ la fonction polynomiale. Aussi, f_P est $\mathscr{C}^\infty$ sur $\mathbb{R}$.
D'après le théorème de Rolle,

$$\forall i \in [\![1, n-1]\!], \exists y_i \in]x_i, x_{i+1}[, f_P'(y_i) = 0$$

Donc $y_1, \ldots, y_{n-1}$ sont racines de P'.
De plus,

$$y_1 < x_2 < y_2 < x_3 < y_3 < \cdots < y_{n-1}$$

On a donc trouvé $n-1$ racines distinctes de P'. Or, $\deg(P') = n-1$.
Donc, on a trouvé TOUTES les racines complexes de P'. Donc P' est sciendé à racines simples.

2. On note $x_1 < \cdots < x_p$ les racines de P et $n = \deg(P)$. On note pour tout $i \in [\![1, p]\!]$, μ_i la multiplicité de x_i. Donc,

$$\sum_{i=1}^{p} \mu_i = n$$

D'après le théorème de Rolle,

$$\forall i \in [\![1, p-1]\!], \exists y_i \in]x_i, x_{i+1}[, P'(y_i) = 0$$

On a trouvé $p-1$ racines réelles de P'. $\forall i \in [\![1, p]\!], x_i$ est une racine de P' de multiplicité $\mu - 1$.
Ce qui fait, $\sum_{i=1}^{p}(\mu_i - 1) = n - p$ racines réelles de P' comptées avec multiplicité.
En tout, on a trouvé $n-1$ racines réelles de P' comptées avec multiplicité.
Comme $\deg(P') = n-1$, P' n'a pas d'autres racines donc P' est scindé.

Exercice (Problème) :
Soient $(x_1, \ldots, x_n) \in \mathbb{K}^n$ tels que

$$\forall i \neq j, x_i \neq x_j$$

Soient $(y_1, \ldots, y_n) \in \mathbb{K}^n$. On cherche $P \in \mathbb{K}[X]$ de <u>degré minimal</u> tel que

$$(\star) \quad \forall i \in [\![1, n]\!], P(x_i) = y_i$$

Soit φ : $\begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^n \\ P & \longmapsto & \big(P(x_1), \ldots, P(x_n)\big) \end{array}$

$$(\star) \iff \varphi(P) = (y_1, \ldots, y_n)$$

On cherche, parmi tous les antécédants de $(y_1, \ldots, y_n)$ celui de plus bas degré.

φ est linéaire :

$$\begin{aligned}\forall P, Q \in \mathbb{K}[X], \forall \alpha, \beta \in \mathbb{K},\\ \varphi(\alpha P + \beta Q) &= \big(\alpha P(x_1) + \beta Q(x_1), \dots, \alpha P(x_n) + \beta Q(x_n)\big)\\ &= \big(\alpha P(x_1), \dots, \alpha P(x_n)\big) + \big(\beta Q(x_1), \dots, \beta Q(x_n)\big)\\ &= \alpha\varphi(P) + \beta\varphi(Q)\end{aligned}$$

— Donc φ est un morphisme de groues additifs.

— $(y_1, \dots, y_n) = \displaystyle\sum_{i=0}^{n} y_i e_i$ où $(e_1, \dots, e_n)$ est la bade canonique de $\mathbb{K}^n$

Si on trouve $L_1, \dots, L_n \in \mathbb{K}[X]$ tels que $\varphi(L_1) = e_1, \ \dots \ \varphi(L_n) = e_n$, alors

$$\begin{aligned}\varphi\left(\sum_{i=1}^{n} y_i L_i\right) &= \sum_{i=0}^{n} y_i \varphi(L_i)\\ &= \sum_{i=1}^{n} y_i e_i\\ &= (y_1, \dots, y_n)\end{aligned}$$

—

$$\begin{aligned}P \in \operatorname{Ker}(\varphi) &\iff \varphi(P) = (0, \dots, 0)\\ &\iff \forall i \in [\![1, n]\!], P(x_i) = 0\\ &\iff \exists Q \in \mathbb{K}[X], P = (X - x_1) \cdots (X - x_n)Q\end{aligned}$$

Soit $i \in [\![1, n]\!]$ et $L_i \in \mathbb{K}[X]$.

$$\begin{aligned}\varphi(L_i) = e_i &\iff \big(L_i(x_1), L_i(x_2), \dots, L_i(x_n)\big) = (0, \dots, 0, \underbrace{1}_{i}, 0, \dots, 0)\\ &\iff \begin{cases} L_i(x_i) = 1 \\ \forall j \neq i, L_i(x_j) = 0 \end{cases}\\ &\iff \begin{cases} \exists Q \in \mathbb{K}[X], L_i = \displaystyle\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - x_j)Q \\ 1 = \displaystyle\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (x_i - x_j)Q(x_i) \end{cases}\\ &\impliedby L_i = \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}\end{aligned}$$

D'où,

$$\varphi(P) = (y_1, \dots, y_n) \iff \exists Q \in \mathbb{K}[X], P = \underbrace{\sum_{i=1}^{n} y_i L_i}_{\substack{\text{solution particulière} \\ \deg(\cdot) \leqslant n-1}} + \underbrace{\prod_{k=1}^{n} (X - x_k) Q}_{\substack{\text{solutions de l'équation} \\ \text{homogène associée} \\ \deg(\cdot) \geqslant n}}$$

Le polynôme de plus bas degré solution du problème d'interpolation est

$$\sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}$$

Définition : Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ avec

$$\forall i \neq j, x_i \neq x_j$$

On pose

$$\forall i \in [\![1, n]\!], L_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$$

L_i est le i-ème polynôme interpolateur de Lagrange associé à $(x_1, \dots, x_n)$:

$$\forall j \in [\![1, n]\!], L_i(x_j) = \delta_{i,j}$$

Proposition : Avec les notations précédentes, $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$.

Preuve :
— $\forall i \in [\![1, n]\!], \deg(L_i) = n - 1$
— Soit $P \in \mathbb{K}_{n-1}[X]$. On pose

$$\forall i \in [\![1, n]\!], y_i = P(x_i)$$

On pose $Q = \sum_{i=1}^{n-1} y_i L_i$. Q est le seul polynôme de degré $\leqslant n - 1$ tel que $Q(x_i) = y_i$ pour tout i.
Donc, $P = Q \in \text{Vect}(l_1, \dots, L_n)$. Donc $(L_1, \dots, L_n)$ est une famille génératrice de $\mathbb{K}_{n-1}[X]$. Or, $\dim\left(\mathbb{K}_{n-1}[X]\right) = n$. Donc $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$

□

Exemple :
$\mathbb{K} = {}^{\mathbb{Z}}/_{5\mathbb{Z}}$ et $n = 3$

$x_1 = \overline{2}$ $\quad$ $y_1 = \overline{1}$
$x_2 = \overline{0}$ $\quad$ $y_2 = \overline{1}$
$x_3 = \overline{-1}$ $\quad$ $y_3 = \overline{2}$

Le seul polynôme de degré $\leqslant 2$ tel que $P(x_i) = y_i$ pour tout $i \in [\![1, 2]\!]$ est
$\displaystyle\sum_{i=1}^{3} y_i \prod_{\substack{1\leqslant j\leqslant 3\\ j\neq i}} \frac{X - x_j}{x_i - x_j}$

$$\begin{aligned} L_1 &= (x_1 - x_2)^{-1}(x_1 - x_3)^{-1}(X - x_2)(X - x_3) \\ &= \overline{3} \times \overline{2} \times X\left(X + \overline{1}\right) = X\left(X + \overline{1}\right) = X^2 + X \end{aligned}$$

$$\begin{aligned} L_2 &= (x_2 - x_1)^{-1}(x_2 - x_3)^{-1}(X - x_1)(X - x_3) \\ &= \overline{2} \times \overline{1}\left(X - \overline{2}\right) \times \left(X - \overline{1}\right) \\ &= \overline{2}X^2 + \overline{3}X + \overline{1} \end{aligned}$$

$$\begin{aligned} L_3 &= (x_3 - x_1)^{-1}(x_3 - x_2)^{-1}(X - x_1)(X - x_2) \\ &= \overline{3} \times \overline{4} \times \left(X - \overline{2}\right) \times X \\ &= \overline{2}X\left(X - \overline{2}\right) \\ &= \overline{2}X^2 + X \end{aligned}$$

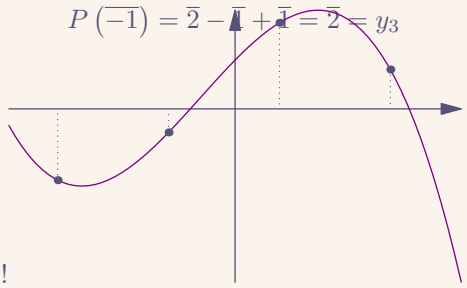
Donc,

$$\begin{aligned} P &= X^2 + X + \overline{2}X + \overline{3}X + \overline{1} + \overline{4}X^2 + \overline{2} \\ &= \overline{2}X^2 + X + \overline{1} \end{aligned}$$

Vérification :

$$\begin{aligned} P\left(\overline{2}\right) &= \overline{3} + \overline{2} + \overline{1} = \overline{1} = y_1 \\ P\left(\overline{0}\right) &= \overline{1} = y_2 \\ P\left(\overline{-1}\right) &= \overline{2} - \overline{1} + \overline{1} = \overline{2} = y_3 \end{aligned}$$

x_1 $\quad$ x_2 $\quad$ x_3 $\quad$ x_4



!

Chapitre 19

Applications linéaires

1 Premières propriétés

Définition : Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f : E \to F$. On dit que f est <u>linéaire</u> si

$$\forall (x,y) \in E^2, \forall (\alpha,\beta) \in \mathbb{K}^2, f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$$

Exemple : 1. $E = \mathscr{C}^0([a,b],\mathbb{C})$

$$\begin{aligned} \varphi : E &\longrightarrow \mathbb{C} \\ f &\longmapsto \int_a^b f(t)\,dt \end{aligned}$$

φ est linéaire

2. $E = \mathscr{D}(I,\mathbb{C})$ et $F = \mathbb{C}^I$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \end{aligned}$$

φ est linéaire

3. $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax \end{array}$ est linéaire.

$$f(\alpha x + \beta y) = \alpha a x + \beta a y = \alpha f(x) + \beta f(y)$$

4. $E = \mathscr{C}^1(I,\mathbb{C})$ et $F = \mathscr{C}^0(I,\mathbb{C})$. $a \in F$

$\varphi : \begin{array}{ccc} E & \longrightarrow & F \\ y & \longmapsto & y' + ay \end{array}$ est linéaire

$$y' + a(x)y = b(x) \iff \varphi(y) = b$$

5. $E = \mathbb{C}^{\mathbb{N}} = F$

$\varphi : \begin{array}{ccc} E & \longrightarrow & F \\ (u_n) & \longmapsto & (u_{n+2} - u_{n+1} - u_n) \end{array}$

$$\forall n, u_{n+2} = u_{n+1} + u_n \iff \varphi(u) = 0$$

6. $E = \mathcal{M}_{p,1}(\mathbb{K})$, $F = \mathcal{M}_{n,1}(\mathbb{K})$, $A \in \mathcal{M}_{n,p}(\mathbb{K})$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ X &\longmapsto AX \end{aligned}$$

$$AX = B \iff \varphi(X) = B$$

Définition : On dit qu'un problème est linéaire s'il se présente sous la forme :

$$\text{Résoudre } \varphi(x) = y$$

où l'inconnue est $x \in E$, y est un paramètre de F avec $\varphi : E \to F$ linéaire.

Exemple :
Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$\forall x \in \mathbb{R}, f(x+1) - f(x-1) = \lambda$$

où $\lambda \in \mathbb{R}$ est fixé.
On pose $E = \mathbb{R}^{\mathbb{R}}$,

$$\begin{aligned} \varphi : E &\longrightarrow E \\ f \longmapsto \varphi(f) : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x+1) - f(x-1) \end{array} \end{aligned}$$

et

$$\begin{aligned} y : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \lambda \end{aligned}$$

Le problème est équivalent à

$$\begin{cases} \varphi(f) = y \\ f \in E \end{cases}$$

Soient $f, g \in E$, $\lambda, \mu \in \mathbb{R}$.

$$\begin{aligned} \forall x \in \mathbb{R}, \varphi(\lambda f + \mu g)(x) &= (\lambda f + \mu g)(x+1) - (\lambda f + \mu g)(x-1) \\ &= \lambda f(x+1) - \mu g(x+1) - \lambda f(x-1) - \mu g(x-1) \\ &= \lambda\big(f(x+1) - f(x-1)\big) + \mu\big(g(x+1) - g(x-1)\big) \\ &= \lambda\varphi(f)(x) + \mu\varphi(g)(x) \end{aligned}$$

Donc, $\varphi(\lambda f + \mu g) = \lambda\varphi(f) + \mu\varphi(g)$

Remarque (Notation) :
Soient E et F deux $\mathbb{K}$-espaces vectoriels.
L'ensemble des applications linéaires de E dans F est $\mathscr{L}(E, F)$.
Si $F = E$, alors on note plus simplement $\mathscr{L}(E)$ à la place de $\mathscr{L}(E, E)$.
Les éléments de $\mathscr{L}(E)$ sont appelés endomorphismes (linéaires) de E.

Proposition : Soit $f \in \mathscr{L}(E,F)$, $g \in \mathscr{L}(F,G)$. Alors $g \circ f \in \mathscr{L}(E,G)$.

Preuve :
Soient $u, v \in E$ et $\alpha, \beta \in \mathbb{K}$.

$$\begin{aligned}(g \circ f)(\alpha u + \beta v) &= g\big(f(\alpha u + \beta v)\big)\\ &= g\big(\alpha f(u) + \beta f(v)\big)\\ &= \alpha g\big(f(u)\big) + \beta g\big(f(v)\big)\\ &= \alpha(g \circ f)(u) + \beta(g \circ f)(v)\end{aligned}$$

□

Proposition : $\mathscr{L}(E,F)$ est un sous-espace vectoriel de F^E.

Preuve :
Soient $f, g \in \mathscr{L}(E,F)$ et $\lambda, \mu \in \mathbb{K}$. Montrons que $\lambda f + \mu g \in \mathscr{L}(E,F)$.
Soient $u, v \in E$, $\alpha, \beta \in \mathbb{K}$.

$$\begin{aligned}(\lambda f + \mu g)(\alpha u + \mu v) &= \lambda f(\alpha u + \beta v) + \mu g(\alpha u + \beta v)\\ &= \lambda\big(\alpha f(u) + \beta f(v)\big) + \mu\big(\alpha g(u) + \beta g(v)\big)\\ &= \alpha\big(\lambda f(u) + \mu g(u)\big) + \beta\big(\lambda f(v) + \mu g(v)\big)\\ &= \alpha\big((\lambda f + \mu g)(u)\big) + \beta\big((\lambda f + \mu g)(v)\big)\end{aligned}$$

De plus, $\tilde{0} : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & 0_F \end{array}$ est linéaire donc $\mathscr{L}(E,F) \neq \emptyset$. □

Proposition : $\big(\mathscr{L}(E), +, \circ, \cdot\big)$ est une $\mathbb{K}$-algèbre (non commutative en général).

Preuve : — $\big(\mathscr{L}(E), +, \cdot\big)$ est un $\mathbb{K}$-espace vectoriel d'après la proposition précédente.
— $\big(\mathscr{L}(E), +\big)$ est un groupe abélien.
" $\circ$ " est associative et interne sur $\mathscr{L}(E)$.
$\mathrm{id}_E \in \mathscr{L}(E)$.

Soient $f, g, h \in \mathscr{L}(E)$.

$$\begin{aligned}\forall x \in E, f \circ (g+h)(x) &= f\big((g+h)(x)\big)\\ &= f\big(g(x)+h(x)\big)\\ &= f\big(g(x)\big)+f\big(h(x)\big) \text{ car } f \text{ est linéaire}\\ &= (f\circ g + f\circ h)(x)\end{aligned}$$

Donc,

$$f \circ (g+h) = f\circ g + f\circ h$$

$$\begin{aligned}\forall x \in E, (g+h)\circ f(x) &= (g+h)\big(f(x)\big)\\ &= g\big(f(x)\big)+h\big(f(x)\big)\\ &= (g\circ f + h\circ f)(x)\end{aligned}$$

Donc,

$$(g+h)\circ f = g\circ f + h\circ f$$

Donc, $\big(\mathscr{L}(E), +, \circ\big)$ est un anneau

— Soit $\lambda \in \mathbb{K}$, $f, g \in \mathscr{L}(E)$.

$$\forall x \in E, \lambda \cdot (f\circ g)(x) = \lambda f\big(g(x)\big)$$
$$(\lambda \cdot f)\circ g(x) = \lambda f\big(g(x)\big)$$

$$\begin{aligned}f\circ(\lambda\cdot g)(x) &= f\big(\lambda g(x)\big)\\ &= \lambda f\big(g(x)\big) \text{ car } f \in \mathscr{L}(E)\end{aligned}$$

□

Corollaire : Soit $P \in \mathbb{K}[X]$ et $u \in \mathscr{L}(E)$. On peut former $P(u) \in \mathscr{L}(X)$: on dit que $P(u)$ est un polynôme d'endomorphisme.

Proposition : Soit $f \in \mathscr{L}(E, F)$ bijective. Alors $f^{-1} \in \mathscr{L}(F, E)$.

Preuve :

Soit $u, v \in F$, $\alpha, \beta \in \mathbb{K}$.

$$\begin{aligned} & f^{-1}(\alpha u + \beta v) = \alpha f^{-1}(u) + \beta f^{-1}(v) \\ \iff & \alpha u + \beta v = f\big(\alpha f^{-1}(u) + \beta f^{-1}(v)\big) \\ \iff & \alpha u + \beta v = \alpha f\left(f^{-1}(u)\right) + \beta f\left(f^{-1}(v)\right) \\ \iff & \alpha u + \beta v = \alpha u + \beta v \end{aligned}$$

Donc, $f^{-1} \in \mathscr{L}(F, E)$ □

Remarque (Notation) :
On note $\mathrm{GL}(E)$ l'ensemble des endomorphismes de E bijectifs, $\mathrm{GL}(E, F)$ l'ensemble des applications linéaires de E dans F bijectives.
Les éléments de $\mathrm{GL}(E)$ sont appelés automorphismes (linéaires) de E.

Corollaire : $\mathrm{GL}(E)$ est un sous-groupe de $\big(S(E), \circ\big)$

Définition : $\mathrm{GL}(E)$ est dit " le groupe linéaire de E".

2 Noyau et image

Proposition : Soit $f \in \mathscr{L}(E, F)$, U un sous-espace vectoriel de E et V un sous-espace vectoriel de F.

1. $f(U)$ est un sous-espace vectoriel de F.
2. $f^{-1}(V)$ est un sous-espace vectoriel de E.

Preuve : 1. $0_F = f(0_E)$ et $0_E \in U$ donc $0_F \in f(U)$ donc $f(U) \neq$
Soient $(x, y) \in f(U)^2$, $(\lambda, \mu) \in \mathbb{K}^2$. Soient $a, b \in U$ tels que $\begin{cases} x = f(a) \\ y = f(b) \end{cases}$.

$$\lambda x + \mu y = \lambda f(a) + \mu f(b) = f(\lambda a + \mu b) \text{ car } f \in \mathscr{L}(E, F)$$

U est un sous-espace vectoriel de E.
Donc $\lambda a + \mu v \in U$
donc $f(\lambda u + \mu v) \in f(U)$
donc $\lambda x + \mu y \in f(U)$.

2. $f(0_E) = 0_F \in V$ donc $0_E \in f^{-1}(V)$. Donc $f^{-1}(V) \neq$.
Soient $x, y \in f^{-1}(V)$, $\lambda, \mu \in \mathbb{K}$.

$$f(\lambda x + \mu y) = \lambda \underbrace{f(x)}_{\in V} + \mu \underbrace{f(y)}_{\in V} \in V$$

donc $\lambda x + \mu y \in f^{-1}(V)$.

□

Corollaire : Soit $f \in \mathscr{L}(E, F)$.

1. $\mathrm{Ker}(f) = f^{-1}(\{0_F\}) = \{x \in E \mid f(x) = 0_E\}$ est un sous-espace vectoriel de E.
2. $\mathrm{Im}(f) = f(E) = \{f(u) \mid u \in E\}$ est un sous-espace vectoriel de E.

□

REMARQUE (Rappel) :
Soit $f \in \mathscr{L}(E, F)$

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{0_E\}$$
$$f \text{ surjective} \iff \mathrm{Im}(f) = F$$

EXEMPLE : 1. Soit I un intervalle, $E = \mathscr{D}(I, \mathbb{R})$ et $F = \mathbb{R}^I$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \end{aligned}$$

$$\mathrm{Ker}(\varphi) = \{f : I \to \mathbb{R} \mid f \text{ constante } \}$$
$$\mathrm{Im}(\varphi) \supset \mathscr{C}^0(I, \mathbb{R})$$

2. $E = \mathbb{R}_2[X]$, $F = \mathbb{R}$, $\varphi : \begin{array}{ccc} E & \longrightarrow & F \\ P & \longmapsto & \displaystyle\int_0^1 P(t)\, dt \end{array}$

$$\begin{aligned} \mathrm{Ker}(\varphi) &= \left\{ P = a + bX + cX^2 \mid (a, b, c) \in \mathbb{R}^3 \text{ et } \int_0^1 P(t)\, dt = 0 \right\} \\ &= \left\{ a + bX + cX^2 \mid a + \frac{b}{2} + \frac{c}{3} = 0 \right\} \\ &= \left\{ a + bX + cX^2 \mid a = -\frac{b}{2} - \frac{c}{3} \right\} \\ &= \left\{ -\frac{b}{2} - \frac{c}{3} + bX + cX^2 \mid b, c \in \mathbb{R} \right\} \\ &= \left\{ b\left(-\frac{1}{2} + X\right) + c\left(-\frac{1}{3} + X^2\right) \mid b, c \in \mathbb{R} \right\} \\ &= \mathrm{Vect}\left(-\frac{1}{2} + X, -\frac{1}{3} + X^2\right) \end{aligned}$$

$\mathrm{Im}(\varphi) = \mathbb{R}$.

3 Théorème du rang

Dans ce paragraphe, E est un $\mathbb{K}$-espace vectoriel de dimension finie.

Proposition : Soit $f : E \to F$ un isomorphisme (i.e. une application linéaire bijective). Alors, $\dim(E) = \dim(F)$

Preuve :
Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. On pose

$$\forall i \in [\![1, n]\!], u_i = f(e_i) \in F$$

— Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$. On suppose que $\sum_{i=0}^{n} \lambda_i u_i = 0_F$. D'où,

$$\begin{aligned} \sum_{i=1}^{n} \lambda_i f(e_i) \text{ donc } f\left(\sum_{i=1}^{n} \lambda_i e_i\right) &= 0_F \\ \text{donc } \sum_{i=1}^{n} \lambda_i e_i &\in \operatorname{Ker}(f) = \{0_E\} \\ \text{donc } \sum_{i=1}^{n} \lambda_i e_i &= 0_E \\ \text{donc } \forall i \in [\![1, n]\!], \lambda_i &= 0 \end{aligned}$$

Donc $(u_1, \dots, u_n)$ est libre.
Soit $y \in F$. Comme f est surjective, il existe $x \in E$ tel que $f(x) = y$.
Comme $\mathcal{B}$ engendre E, il existe $\lambda_1, \dots, \lambda_n \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^{n} \lambda_i e_i$.
Comme f est linéaire,

$$y = f(x) = \sum_{i=1}^{n} \lambda_i f(e_i) = \sum_{i=1}^{n} \lambda_i e_i$$

Donc, $F = \operatorname{Vect}(u_1, \dots, u_n)$
Donc $(u_1, \dots, u_n)$ est une base de F donc

$$\dim(E) = n = \dim(F)$$

□

La première partie de la preuve précédente justifie le résultat suivant.

Proposition : Soit $f \in \mathscr{L}(E,F)$ injective. $\mathscr{L} = (e_1, \ldots, e_p)$ une famille libre de E. Alors $\big(f(e_1), \ldots, f(e_n)\big)$ est une famille libre de F. En particulier, $\dim(F) \geqslant \dim(E)$. □

La deuxième partie de la preuve prouve :

Proposition : Soit $f \in \mathscr{L}(E,F)$ surjective et $\mathscr{G} = (e_1, \ldots, e_p)$ une famille génératrice de E. Alors $\big(f(e_1), \ldots, f(e_p)\big)$ est une famille génératrice de F. En particulier,

$$\dim(F) \leqslant \dim(E)$$

□

Théorème (Théorème du rang) **:** Soit $f \in \mathscr{L}(E,F)$.

$$\dim(E) = \dim\big(\operatorname{Ker}(f)\big) + \dim\big(\operatorname{Im}(f)\big)$$

Preuve (À connaître) *:*
On pose

$$\begin{aligned} u : U &\longrightarrow \operatorname{Im}(f) \\ x &\longmapsto f(x) \end{aligned}$$

où U est un supplémentaire de $\operatorname{Ker}(f)$ dans E.
(U existe : voir remarque qui suit)

— $u \in \mathscr{L}\big(U, \operatorname{Im}(f)\big)$, en effet, soient $x, y \in U, \lambda, \mu \in \mathbb{K}$

$$\begin{aligned} u(\lambda x + \mu v) &= f(\lambda x + \mu v) \\ &= \lambda f(x) + \mu f(y) \\ &= \lambda u(x) + \mu u(y) \end{aligned}$$

— Soit $y \in \operatorname{Im}(f)$. Soit $x \in E$ tel que $y = f(x)$. Comme $E = U \oplus \operatorname{Ker}(f)$. On peut écrire

$$\begin{cases} x = a + b \\ a \in U, b \in \operatorname{Ker}(f) \end{cases}$$

D'où,

$$y = f(x) = f(a+b) = f(a) + f(b) = u(a) + 0_E = u(a)$$

Donc u est surjective.
Soit $x \in U$.

$$\begin{aligned} x \in \mathrm{Ker}(u) &\iff u(x) = 0_F \\ &\iff f(x) = 0_F \\ &\iff x \in \mathrm{Ker}(f) \\ &\iff x = 0_E \text{ car } U \cap \mathrm{Ker}(f) = \{0_E\} \end{aligned}$$

Donc u est injective.
Ainsi, $\dim(U) = \dim\big(\mathrm{Im}(f)\big)$
Or,

$$\begin{aligned} \dim(E) &= \dim\big(U \oplus \mathrm{Ker}(f)\big) \\ &= \dim(U) + \dim\big(\mathrm{Ker}(f)\big) \end{aligned}$$

donc

$$\dim(U) = \dim(E) - \dim\big(\mathrm{Ker}(f)\big)$$

Donc,

$$\dim(E) = \dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big)$$

□

Remarque :
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, et F un sous-espace vectoriel de E.

Cas 1 $F = \{0_E\}$, alors E est un supplémentaire de F.

Cas 2 $F \neq \{0_E\}$. Soit $\mathscr{B} = (e_1, \ldots, e_p)$ une base de F. Alors $\mathscr{B}$ est une famille libre de E. On complète $\mathscr{B}$ en une base $(e_1, \ldots, e_p, e_{p+1}, \ldots, e_n)$ de E. On pose $G = \mathrm{Vect}(e_{p+1}, \ldots, e_n)$. On démontre que

$$F \oplus G = E$$

Corollaire : Soient E et F deux $\mathbb{K}$-espaces vectoriels de même dimension finie et $f \in \mathscr{L}(E, F)$.

$$\begin{aligned} f \text{ injective} &\iff f \text{ surjective} \\ &\iff f \text{ bijective} \end{aligned}$$

Preuve :
D'après le théorème du rang,

$$\dim(E) = \dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big)$$

Si f est injective, alors $\mathrm{Ker}(f) = \{0_E\}$

et donc $\dim\big(\mathrm{Ker}(f)\big) = 0$
et donc $\dim\big(\mathrm{Im}(f)\big) = \dim(F)$
et donc $\mathrm{Im}(f) = F$
et donc f est surjective.

Si f est surjective, alors $\mathrm{Im}(f) = F$
et donc $\dim\big(\mathrm{Im}(f)\big) = \dim(F) = \dim(E)$
et donc $\dim\big(\mathrm{Ker}(f)\big) = 0$
et donc $\mathrm{Ker}(f) = \{0\}$
et donc f est injective □

Exemple :
Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ tel que

$$\forall i \neq j, x_i \neq x_j$$

Soit $(y_1, \dots, y_n) \in \mathbb{K}^n$. On pose $\varphi : \begin{array}{ccc} \mathbb{K}_{n-1}[X] & \longrightarrow & \mathbb{K}^n \\ P & \longmapsto & \big(P(x_1), \dots, P(x_n)\big) \end{array}$

$$\begin{aligned} P \in \mathrm{Ker}(\varphi) &\iff \varphi(P) = 0 \\ &\iff \forall i \in [\![1, n]\!], P(x_i) = 0 \\ &\iff P = 0 \text{ car } \deg(P) \leqslant n-1 \end{aligned}$$

Donc φ est injective et donc φ est bijective.
Donc,

$$\exists! P \in \mathbb{K}_{n-1}[X], \forall i \in [\![1, n]\!], P(x_i) = y_i$$

De plus, $\varphi^{-1} : \mathbb{K}^n \to \mathbb{K}_{n-1}[X]$ est un isomorphisme.
Soit $(e_1, \dots, e_n)$ la base canonique d $\mathbb{K}^n$. $\big(\varphi^{-1}(e_1) \dots, \varphi^{-1}(e_n)\big)$ est une base de $\mathbb{K}_{n-1}[X]$.
$\forall i \in [\![1, n]\!], \varphi^{-1}(e_i) = L_i$ es tle i-ème polynôme interpolateur de Lagrange.

$$\begin{aligned} P &= \varphi^{-1}(y_1, \dots, y_n) \\ &= \varphi^{-1}\left(\sum_{i=1}^{n} y_i e_i\right) \\ &= \sum_{i=1}^{n} y_i \varphi^{-1}(e_i) \\ &= \sum_{i=1}^{n} y_i L_i \end{aligned}$$

Exercice (Interpolation de Hermite) :
Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ avec

$$\forall i \neq j, x_i \neq x_j$$

Soit $(y_1, \dots, y_n) \in \mathbb{K}^n$ et $(z_1, \dots, z_n) \in \mathbb{K}^n$.
Trouver un polynôme de plus bas degré tel que

$$(\star) \qquad \forall i \in [\![1, n]\!], \begin{cases} P(x_i) = y_i \\ P'(x_i) = z_i \end{cases}$$

Soit $\varphi : \begin{array}{ccc} \mathbb{K}_{2n-1}[X] & \longrightarrow & \mathbb{K}^{2n} \\ P & \longmapsto & \big(P(x_1), \dots, P(x_n), P'(x_1), \dots, P'(x_n)\big) \end{array}$

$$(\star) \iff \varphi(P) = (y_1, \dots, y_n, z_1, \dots, z_n)$$

$$\begin{aligned} P \in \mathrm{Ker}(\varphi) &\iff \forall i, \begin{cases} P(x_i) = 0 \\ P'(x_i) = 0 \end{cases} \\ &\iff P = 0 \text{ car } \deg(P) \leqslant 2n - 1 \end{aligned}$$

Donc φ est un isomorphisme.

Corollaire : Soit $f \in \mathscr{L}(E)$ avec E de dimension finie. Alors,

$$f \in \mathrm{GL}(E) \iff f \text{ injective} \iff f \text{ surjective}$$

□

Remarque :
Soit $f \in \mathscr{L}(E, F)$, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Alors

$$\boxed{\mathrm{Im}(f) = \mathrm{Vect}\big(f(e_1), \dots, f(e_n)\big)}$$

$\dim\big(\mathrm{Im}(f)\big) = \mathrm{rg}\big(f(e_1), \dots, f(e_n)\big)$

Définition : Soit $f \in \mathscr{L}(E, F)$. Le rang de f est

$$\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big)$$

4 Formes linéaires

Définition : Soit E un $\mathbb{K}$-espace vectoriel. Une forme linéaire sur E est une application linéaire de E dans $\mathbb{K}$.
L'ensemble des formes linéaires est noté $E^\star = \mathscr{L}(E, \mathbb{K})$. $E^\star$ est appelé espace dual de E.

Proposition : Toute forme linéaire est soit nulle, soit surjective.

Preuve :
Soit $f \in E^\star$.
$\mathrm{Im}(f)$ est un sous-espace vectoriel de $\mathbb{K}$ donc $\mathrm{rg}(f) \leqslant \dim(\mathbb{K}) = 1$.
Si $\mathrm{rg}(f) = 0$, alors $\mathrm{Im}(f) = \{0\}$ et donc

$$\forall x \in E, f(x) = 0$$

Si $\mathrm{rg}(f) = 1$, alors $\mathrm{Im}(f) = \mathbb{K}$ et donc f est surjective. □

Proposition : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et $f \in E^\star \setminus \{0\}$. Alors $\mathrm{Ker}(f)$ est de dimension $n-1$.

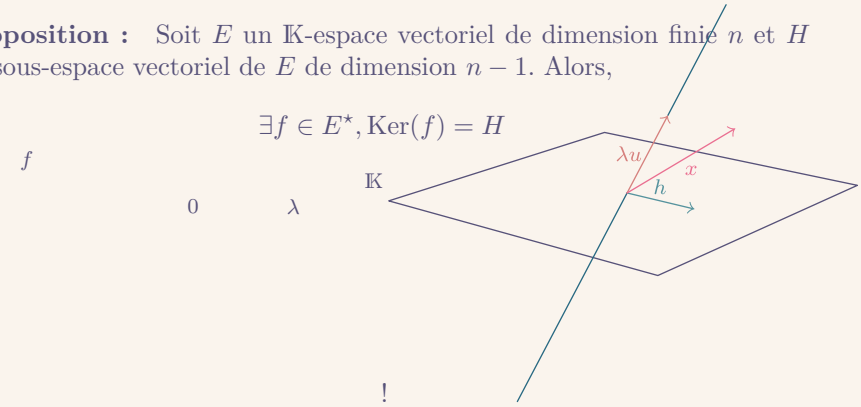
Preuve :
Comme $f \neq 0$, donc $\mathrm{rg}(f) = 1$
D'après le théorème du rang,

$$\dim\big(\mathrm{Ker}(f)\big) = \dim(E) - \mathrm{rg}(f) = n - 1$$

□

Proposition : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et H un sous-espace vectoriel de E de dimension $n-1$. Alors,

$$\exists f \in E^\star, \mathrm{Ker}(f) = H$$



Preuve :
Soit D un supplémentaire de H dans E :

$$E = H \oplus D$$

Nécessairement,

$$\dim(D) = \dim(E) - \dim(H) = 1$$

Soit $u \in D \setminus \{0\}$. $D = \mathrm{Vect}(u)$

On pose $f : \begin{array}{ccc} E & \longrightarrow & \mathbb{K} \\ x = h + \lambda u & \longmapsto & \lambda \\ (h \in H, \lambda \in \mathbb{K}) & & \end{array}$

Montrons que $f \in E^\star$.

Soient $(x, y) \in E^2, (\alpha, \beta) \in \mathbb{K}^2$.

On pose

$$\begin{cases} x = h + \lambda u, & h \in H, \lambda \in \mathbb{K} \\ y = h' + \lambda' u, & h' \in H, \lambda' \in \mathbb{K} \end{cases}$$

D'où,

$$\begin{aligned} \alpha x + \beta y &= \alpha(h + \lambda u) + \beta(h' + \lambda' u) \\ &= \underbrace{(\alpha h + \beta h')}_{\in H} + \underbrace{(\alpha\lambda + \beta\lambda')}_{\in \mathbb{K}} u \end{aligned}$$

Donc,

$$\begin{aligned} f(\alpha x + \beta y) &= \alpha\lambda + \beta\lambda' \\ &= \alpha f(x) + \beta f(y) \end{aligned}$$

Soit $x \in E$. On pose $x = h + \lambda u$ avec $h \in H$ et $\lambda \in \mathbb{K}$

$$\begin{aligned} x \in \mathrm{Ker}(f) &\iff f(x) = 0 \\ &\iff \lambda = 0 \\ &\iff x = y \\ &\iff x \in H \end{aligned}$$

Donc, $H = \mathrm{Ker}(f)$.

□

Exemple :

$E = \mathbb{R}^4$, $H = \mathrm{Vect}\big((1,0,0,1),(1,1,0,0),(0,1,1,0)\big)$

Soit $u = (1,2,1,1) \notin H$.

Soit $(x, y, z, t) \in E$. On cherche $(\alpha, \beta, \gamma, \lambda) \in \mathbb{R}^4$ tels que

$$(\star) \qquad (x, y, z, t) = \alpha(1,0,0,1) + \beta(1,1,0,0) + \gamma(0,1,1,0) + \lambda(1,2,1,1)$$

Plus précisément, on cherche à exprimer λ en fonction de x, y, z, t.

$$
\begin{aligned}
(\star) &\iff \begin{cases} \alpha+\beta+\gamma = x \\ \beta+\gamma+2\lambda = y \\ \gamma+\lambda = z \\ \alpha+\lambda = t \end{cases} \\
&\iff \begin{cases} \boxed{\alpha}+\beta+\lambda = x \\ \beta+\gamma+2\lambda = y \\ \boxed{\gamma}+\lambda = z \\ -\beta = t-x \end{cases} \\
&\iff \begin{cases} \boxed{\alpha}+\beta+\lambda = x \\ \beta+\lambda = y-z \\ \boxed{\gamma}+\lambda = z \\ \beta = x-t \end{cases} \\
&\iff \begin{cases} \lambda = y-z-x+t \\ \vdots \end{cases}
\end{aligned}
$$

Donc,

$$(x, y, z, t) \in H \iff y - z - x + t = 0$$

Soit $f : \begin{array}{ccc} \mathbb{R}^4 & \longrightarrow & \mathbb{R} \\ (x, y, z, t) & \longmapsto & x - y + z - t \end{array}$ et $H = \mathrm{Ker}(f)$

Proposition : Avec les notations précédentes,
$\{f \in E^\star \mid \mathrm{Ker}(f) = H\}$ est une droite de $E^\star$ privée de l'application nulle.
En d'autres termes, les équations de H sont 2 à 2 proportionelles.

Preuve :
Soient $f, g \in E^\star$ telles que

$$\mathrm{Ker}(f) = \mathrm{Ker}(g)$$

On pose $H = \mathrm{Ker}(f)$. Soit $u \notin H$ de sorte que

$$H \oplus \mathrm{Vect}(u) = E$$

$u \notin H$ donc $f(u) \neq 0$.
On pose $\alpha = \dfrac{g(u)}{f(u)}$. Montrons que $g = \alpha f$.
Soit $x \in E$. On pose $x = h + \lambda u$ avec $\begin{cases} h \in H \\ \lambda \in \mathbb{K} \end{cases}$

$$g(x) = g(h) + \lambda g(u) = 0 + \lambda\alpha f(u)$$
$$\alpha f(x) = \alpha\big(f(h) + \lambda f(u)\big) = \lambda\alpha f(u)$$

□

Définition : Soit E un $\mathbb{K}$-espace vectoriel et H un sous-espace vectoriel de E. On dit que H est un hyperplan de E s'il existe une droite D de E telle que
$$H \oplus D = E$$

En reprenant les démonstrations précédentes, on a encore les résultats suivants :

Proposition : Soit H un hyperplan de E. Alors, $\{f \in E^\star \mid \mathrm{Ker}(f) = H\}$ est une droite de $E^\star$ privée de l'application nulle. □

Proposition : Soit $f \in E^\star$ non nulle. Alors $\mathrm{Ker}(f)$ est un hyperplan de E.

Preuve :
f non nulle. Soit $x \in E$ tel que
$$f(x) \neq 0$$
On pose $H = \mathrm{Ker}(f)$ et $D = \mathrm{Vect}(x)$. Montrons que $H \oplus D = E$.

Analyse Soit $y \in E$. On suppose $y = h + \lambda x$ avec $h \in H$ et $\lambda \in \mathbb{K}$. Alors,
$$f(y) = f(h) + \lambda f(x) = \lambda f(x) \text{ donc } \begin{cases} \lambda = f(y)f(x)^{-1} \\ h = y - f(y)f(x)^{-1}x \end{cases}$$

Synthèse Soit $y \in E$. On pose $\begin{cases} \lambda = f(y)f(x)^{-1} \\ h = y - \lambda x \end{cases}$.

Évidemment, $\begin{cases} h + \lambda x = y \\ \lambda \in \mathbb{K} \end{cases}$

$$\begin{aligned} f(h) &= f(y - \lambda x) \\ &= f(y) - \lambda f(x) \\ &= f(y) - f(y)f(x)^{-1}f(x) \\ &= 0 \end{aligned}$$

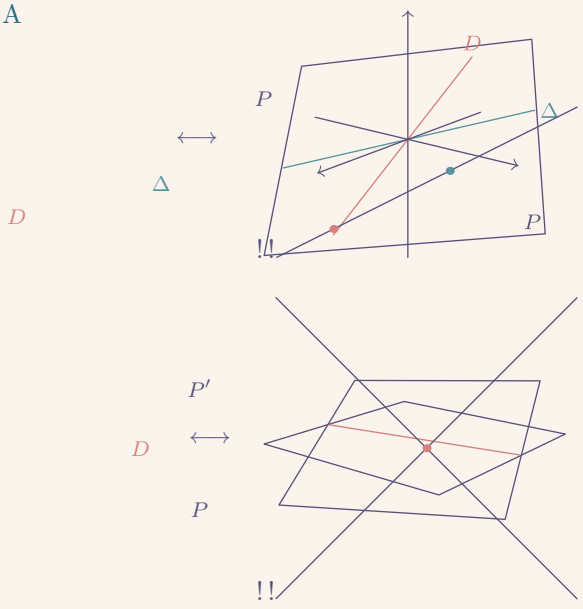
□

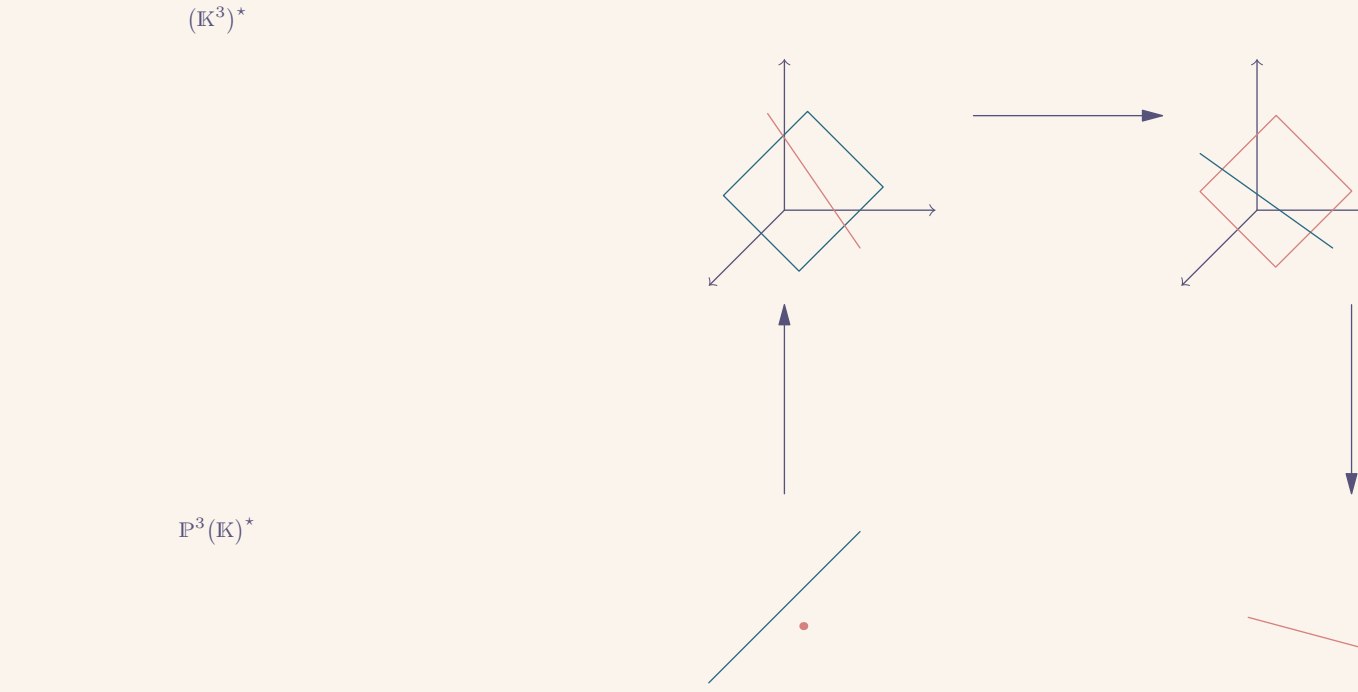
Hors-Programme

$$\mathbb{P}^3(\mathbb{K}) = \{D \setminus \{0\} \mid D \text{ droite vectorielle de } \mathbb{K}^3\}$$

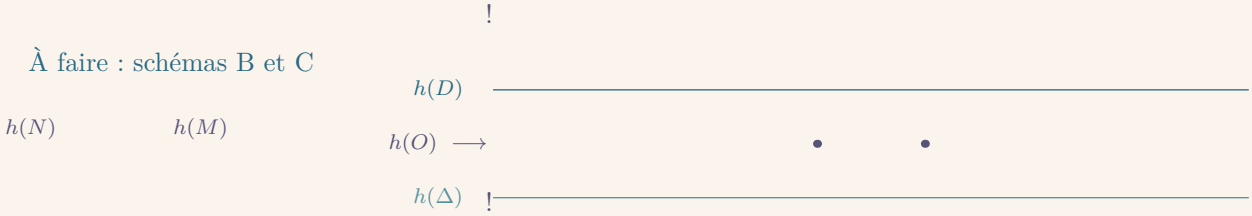
Une droite projective de $\mathbb{P}^3(\mathbb{K})$ est un plan vectoriel de $\mathbb{K}^3$ privé de 0.

À faire : schéma A





À faire : schémas B et C



5 Projections et symétries

Définition : Soit E un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces de E supplémentaires :

$$E = F \oplus G$$

Soit $x \in E$.

$$\exists!(a,b) \in F \times G, x = a + b$$

Le vecteur a est appelé projeté de x sur F parallèlement à G.
Le vecteur b est appelé projeté de x sur G parallèlement à F.
La projection sur F parallèlement à G est l'application qui à $x \in E$ associe

son projeté sur F parallèlement à G.

Exemple :
$E = \mathbb{R}^{\mathbb{R}}$, $F = \{f \in E \mid f \text{ paire}\}$ et $G = \{f \in E \mid f \text{ impaire}\}$
On a $E = F \oplus G$.
Soient p la projection sur F parallèlement à G et q la projection sur G parallèlement à F.

$$\forall x \in E, \begin{cases} p(f) : x \mapsto \dfrac{1}{2}\big(f(x) + f(-x)\big) \\ q(f) : x \mapsto \dfrac{1}{2}\big(f(x) - f(-x)\big) \end{cases}$$

Proposition : Soient F et G deux sous-espaces vectoriels de E supplémentaires et p la projection sur F parallèlement à G.

1. $p \in \mathscr{L}(E)$
2. $p_{|F} = \mathrm{id}_F$ et $p_{|G} = 0$
3. $p \circ p = p$
4. $\mathrm{id}_E - p$ est la projection sur G parallèlement à F.

Preuve : 1. $\forall x \in E, p(x) \in F \subset E$
Soit $(x, y) \in E^2$, $(\lambda, \mu) \in \mathbb{K}^2$.
On pose $x = a + b$ avec $\begin{cases} a \in F \\ b \in G \end{cases}$ et $y = c + d$ avec $\begin{cases} c \in F \\ d \in G \end{cases}$
donc,

$$\begin{aligned} \lambda x + \mu y &= \lambda(a + b) + \mu(c + d) \\ &= \underbrace{(\lambda a + \mu c)}_{\in F} + \underbrace{(\lambda b + \mu d)}_{\in G} \end{aligned}$$

Donc,

$$p(\lambda x + \mu y) = \lambda a + \mu b = \lambda p(x) + \mu p(y)$$

2. $\forall x \in F, x = \underbrace{x}_{\in F} + \underbrace{0}_{\in G}$ donc $p(x) = x$
   $\forall x \in G, x = \underbrace{0}_{\in F} + \underbrace{x}_{\in G}$ donc $p(x) = 0$
3. $\forall x \in E, p(x) \in F$ donc $p(p(x)) = p(x)$
4. Soit $x \in E$. On pose $x = a + b$ avec $\begin{cases} a \in F \\ b \in G \end{cases}$. Donc $p(x) = a$. D'où, $x - p(x) = b$ est le projeté de x sur G parallèlement à F.

□

Définition : Soit $f \in \mathscr{L}(E)$. On dit que f est un projecteur si $f \circ f = f$

Proposition : Soit f un projecteur de E. Alors f est la projection sur $\mathrm{Im}(f)$ parallèlement à $\mathrm{Ker}(f)$. En particulier,

$$\mathrm{Im}(f) \oplus \mathrm{Ker}(f) = E$$

Preuve :

Analyse Soit $x \in E$. On suppose que $x = a + b$ avec $\begin{cases} a \in \mathrm{Ker}(f) \\ b \in \mathrm{Im}(f) \end{cases}$.

D'où,

$$\begin{aligned} f(x) &= f(a) + f(b) \\ &= 0 + f(b) \\ &= f(b) \end{aligned}$$

Soit $y \in E$ tel que $b = f(y)$. Donc,

$$f(b) = f\big(f(y)\big) = f(y) = b$$

Donc, $f(x) = b$ et donc $a = x - b = x - f(x)$

Synthèse Soit $x \in E$. On pose $\begin{cases} a = x - f(x) \\ b = f(x) \end{cases}$. Évidemment, $\begin{cases} a + b = x \\ b \in \mathrm{Im}(f) \end{cases}$

$$\begin{aligned} f(a) &= f\big(x - f(x)\big) \\ &= f(x) - f\big(f(x)\big) \\ &= f(x) - f(x) \\ &= 0 \end{aligned}$$

Donc $a \in \mathrm{Ker}(f)$. On a montré

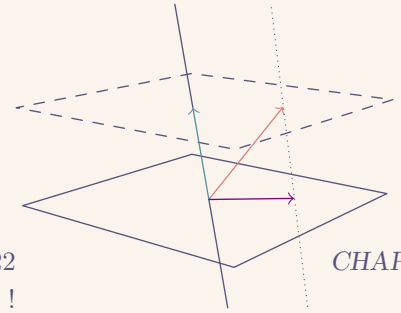
$$\mathrm{Im}(f) \oplus \mathrm{Ker}(f) = E$$

On considère la projection p sur $\mathrm{Im}(f)$ parallèlement à $\mathrm{Ker}(f)$.
Soit $x \in E$. On a montré que

$$x = \underbrace{f(x)}_{\in \mathrm{Im}(f)} + \underbrace{x - f(x)}_{\in \mathrm{Ker}(f)}$$

donc $p(x) = f(x)$ et donc $p = f$

□



!

Définition : Soient F et G supplémentaires dans E : $E = F \oplus G$

Soit $x \in E$. On décompose x :

$$x = a + b \text{ avec } \begin{cases} a \in F \\ b \in G \end{cases}$$

et on forme

$$y = a - b$$

On dit que y est le symétrique de x par rapport à F parallèlement à G
La symétrie par rapport à F parallèlement à G est l'application qui à tout $x \in E$ associe son symétrique parallèlement à G par rapport à F.

Proposition : Soient F et G supplémentaires dans E, s la symétrie par rapport à F parallèlement à G.

1. $s \in \mathscr{L}(E)$
2. $s_{|E} = \mathrm{id}_F$ et $s_{|G} = -\mathrm{id}_G$
3. $s \circ s = \mathrm{id}_E$

Preuve :
Soient p la projection sur F parallèlement à G et q la projection sur G parallèlement à F.
On remarque que $s = p - q$.

1. p et q sont des endomorphismes donc s aussi
2. $\forall x \in E, s(x) = p(x) - q(x) = x - 0 = x$
   $\forall x \in G, s(x) = p(x) - q(x) = 0 - x = -x$
3. $$\begin{aligned} \forall x \in E, s\big(s(x)\big) &= s\big(p(x) - q(x)\big) \\ &= s\big(\underbrace{p(x)}_{\in F}\big) - s\big(\underbrace{q(x)}_{\in G}\big) \\ &= p(x) - \big(-q(x)\big) \\ &= x \end{aligned}$$

□

Définition : Soit $f \in \mathscr{L}(E)$. On dit que f est involutive si $f \circ f = \mathrm{id}_E$.

Proposition : Soit $f \in \mathscr{L}(E)$ involutif. Alors f est la symétrie par rapport à $\mathrm{Ker}(f - \mathrm{id}_E)$ parallèlement à $\mathrm{Ker}(f + \mathrm{id}_E)$. En particulier,

$$\mathrm{Ker}(f - \mathrm{id}_E) \oplus \mathrm{Ker}(f + \mathrm{id}_E) = E$$

Preuve.

Analyse Soit $x \in E$. On suppose que $x = a+b$ avec $\begin{cases} a \in \mathrm{Ker}(f - \mathrm{id}_E) \\ b \in \mathrm{Ker}(f + \mathrm{id}_E) \end{cases}$

$$\begin{aligned} a \in \mathrm{Ker}(f - \mathrm{id}_E) &\iff (f - \mathrm{id}_E)(a) = 0 \\ &\iff f(a) - a = 0 \\ &\iff a = f(a) \end{aligned}$$

$$\begin{aligned} b \in \mathrm{Ker}(f + \mathrm{id}_E) &\iff f + \mathrm{id}_E)(b) = 0 \\ &\iff f(b) + b = 0 \\ &\iff f(b) = -b \end{aligned}$$

On sait que $x = a + b$ et $f(x) = f(a) + f(b) = a - b$
D'où,

$$\begin{aligned} a &= \frac{1}{2}\big(x + f(x)\big) \\ b &= \frac{1}{2}\big(x - f(x)\big) \end{aligned}$$

Synthèse Soit $x \in E$. On pose

$$\begin{aligned} a &= \frac{1}{2}\big(x + f(x)\big) \\ b &= \frac{1}{2}\big(x - f(x)\big) \end{aligned}$$

Alors $a + b = x$

$$\begin{aligned} f(a) &= f\left(\frac{1}{2}\big(x + f(x)\big)\right) \\ &= \frac{1}{2}\left(f(x) + f\big(f(x)\big)\right) \\ &= \frac{1}{2}\big(f(x) + x\big) \\ &= a \end{aligned}$$

Donc $a \in \operatorname{Ker}(f - \mathrm{id}_E)$

$$\begin{aligned} f(b) &= f\left(\frac{1}{2}\big(x - f(x)\big)\right) \\ &= \frac{1}{2}\left(f(x) - f\big(f(x)\big)\right) \\ &= \frac{1}{2}\big(f(x) - x\big) \\ &= -b \end{aligned}$$

donc $b \in \operatorname{Ker}(f + \mathrm{id}_E)$
Ainsi,

$$\operatorname{Ker}(f - \mathrm{id}_E) \oplus \operatorname{Ker}(f + \mathrm{id}_E) = E$$

Soit s la symétrie par rapport à $\operatorname{Ker}(f - \mathrm{id}_E)$ parallèlement à $\operatorname{Ker}(f + \mathrm{id}_E)$.
Soit $x \in E$. On a vu que

$$x = \underbrace{\frac{1}{2}\big(x + f(x)\big)}_{\in \operatorname{Ker}(f - \mathrm{id}_E)} + \underbrace{\frac{1}{2}\big(x - f(x)\big)}_{\in \operatorname{Ker}(f + \mathrm{id}_E)}$$

Donc,

$$s(x) = \frac{1}{2}\big(x + f(x)\big) - \frac{1}{2}\big(x - f(x)\big) = f(x)$$

Donc $s = f$ □

Exemple :
$E = \mathbb{R}^{\mathbb{R}}$ et

$$\begin{aligned} s : E &\longrightarrow E \\ f &\longmapsto s(f) : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(-x) \end{array} \end{aligned}$$

$s(f) = f \circ (-\mathrm{id}_{\mathbb{R}})$
$s \in \mathscr{L}(E)$, en effet :

$$\begin{aligned} \forall f, g \in \mathscr{L}(E), \forall \alpha, \beta \in \mathbb{R}, \\ s(\alpha f + \beta g) &= (\alpha f + \beta g) \circ (-\mathrm{id}_{\mathbb{R}}) \\ &= \alpha\big(f \circ (-\mathrm{id}_{\mathbb{R}})\big) + \beta\big(g \circ (-\mathrm{id}_{\mathbb{R}})\big) \\ &= \alpha s(f) + \beta s(g) \end{aligned}$$

De plus, $s \circ s = \mathrm{id}_E$. Donc s est une symétrie.

$$\begin{aligned} \operatorname{Ker}(s - \mathrm{id}_E) &= \{f \in E \mid f \text{ paire}\} = \mathscr{P} \\ \operatorname{Ker}(s + \mathrm{id}_E) &= \{f \in E \mid f \text{ impaire}\} = \mathscr{I} \end{aligned}$$

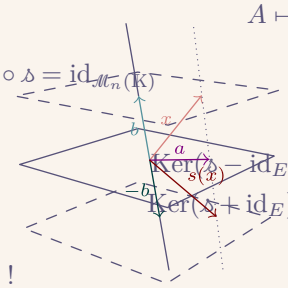
D'où,

$$\mathscr{P} \oplus \mathscr{I} = E$$

Exemple :
$E = \mathcal{M}_n(\mathbb{K})$
Pour $A \in E$, on note ${}^tA$ la transposée de A la matrice obtenue en écrivant en ligne les colonnes de A.
Soit

$$\begin{aligned} \mathcal{s} : \mathcal{M}_n(\mathbb{K}) &\longrightarrow \mathcal{M}_n(\mathbb{K}) \\ A &\longmapsto {}^tA \end{aligned}$$

$\mathcal{s}$ est linéaire, $\mathcal{s} \circ \mathcal{s} = \mathrm{id}_{\mathcal{M}_n(\mathbb{K})}$



$\mathrm{Ker}(\mathcal{s} - \mathrm{id}_E) = S_n(\mathbb{K})$
$\mathrm{Ker}(\mathcal{s} + \mathrm{id}_E) = A_n(\mathbb{K})$

!

Chapitre 20

Fractions rationnelles

1 Construction de $\mathbb{K}(X)$

Proposition–Définition : On définit la relation $\sim$ sur $\mathbb{K}[X] \times \big(\mathbb{K}[X] \setminus \{0\}\big)$ par

$$(P,Q) \sim (A,B) \iff PB = QA$$

Cette relation est une relation d'équivalence. On note $\big(\mathbb{K}[X] \times \big(\mathbb{K}[X] \setminus \{0\}\big)\big)/_\sim$. Les éléments de $\mathbb{K}(X)$ sont appelés fractions rationnelles.
On note $\dfrac{P}{Q}$ la classe d'équivalence du couple (P,Q).

Preuve :
On note $E = \mathbb{K}[X]\big(\mathbb{K}[X] \setminus \{0\}\big)$.

- Soit $(P,Q) \in E$. $PQ = QP$ car $\times$ est commutative dans $\mathbb{K}[X]$. Donc $(P,Q) \sim (P,Q)$
- Soient $(P,Q) \in E, (A,B) \in E$. On suppose que $(P,Q) \sim (A,B)$. Donc $PB = QA$
  Donc, $(A,B) \sim (P,Q)$
- Soit $\big((P,Q),(A,B),(C,D)\big) \in E^3$. On suppose

$$\begin{cases} (P,Q) \sim (A,B) \\ (A,B) \sim (C,D) \end{cases}$$

D'où,

$$\begin{cases} PB = QA \\ AD = BC \end{cases}$$

Donc

$$PBD = QAD = QBC$$

donc $B(PD - QC) = 0$
Comme $B \neq 0$ et comme $\mathbb{K}[X]$ est intègre,

$$PD - QC = 0$$

et donc $(P, Q) \sim (C, D)$

□

Proposition : Soient $(P, Q) \in \mathbb{K}[X] \times \big(\mathbb{K}[X] \setminus \{0\}\big)$ et $R \in \mathbb{K}[X] \setminus \{0\}$. Alors

$$\frac{PR}{QR} = \frac{P}{Q}$$

Preuve :

$$\begin{aligned} \frac{PR}{QR} = \frac{P}{Q} &\iff (PQ, QR) \sim (P, Q) \\ &\iff PRQ = QRP \end{aligned}$$

□

Définition : Soit $(P, Q) \in \mathbb{K}[X] \setminus \big(\mathbb{K}[X] \setminus \{0\}\big)$. On dit que la fraction $\dfrac{P}{Q}$ est sous forme irréductible si $P \wedge Q = 1$.

Proposition–Définition : Soient $(P, Q) \sim (A, B)$. Alors

$$\deg(P) - \deg(Q) = \deg(A) - \deg(B)$$

Le degré de $\dfrac{P}{Q}$ est $\deg(P) - \deg(Q)$. On note ce "nombre" $\deg\left(\dfrac{P}{Q}\right)$.

Preuve :
On sait que $PB = QA$ donc

$$\deg(P) + \deg(Q) = \deg(Q) + \deg(A)$$

et donc

$$\deg(P) - \deg(Q) = \deg(A) - \deg(B)$$

□

Proposition–Définition : Soient $(P,Q) \sim (A,B)$ et $(R,S) \sim (C,D)$. Alors, $(PR,QS) \sim (AC,BD)$.
Le produit de $\dfrac{P}{Q}$ avec $\dfrac{R}{S}$ est $\dfrac{PR}{QS}$

Preuve :
On sait que $\begin{cases} PB = QA \\ RD = SC \end{cases}$. D'où,

$$PBRD = QASC$$

et donc

$$(PR)(BD) = (QS)(AC)$$

donc

$$(PR,QS) \sim (AC,BD)$$

□

Proposition–Définition : Avec les notations précédentes,

$$(PS+RQ,QS) \sim (AD+BC,BD)$$

On définit la somme de $\dfrac{P}{Q}$ et $\dfrac{R}{S}$ par

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS+RQ}{QS}$$

Preuve :
On sait que $\begin{cases} PB = QA \\ RD = SC \end{cases}$. Donc,

$$\begin{aligned} (PS+RQ)BD &= PSBD + RQBD \\ &= QASD + SCQB \\ &= QS(AD+BC) \end{aligned}$$

□

Théorème : $\big(\mathbb{K}(X),+,\times\big)$ est un corps.

Preuve (partielle) *:* 1. “+” est associative : soient $\left(\frac{P}{Q}, \frac{R}{S}, \frac{A}{B}\right) \in \mathbb{K}(X)^3$.

$$\frac{P}{Q} + \left(\frac{R}{S} + \frac{A}{B}\right) = \frac{P}{Q} + \frac{RB + AS}{SB} = \frac{PSB + QRB + QAS}{QSB}$$

$$\left(\frac{P}{Q} + \frac{R}{S}\right) + \frac{A}{B} = \frac{PS + RQ}{QS} + \frac{A}{B} = \frac{PSB + RQB + AQS}{QSB}$$

2. “ + ” est commutative
3. $\frac{0}{1}$ est neutre pour “ + ”

$$\frac{P}{Q} + \frac{0}{1} = \frac{P \times 1 + 0 \times Q}{Q \times 1} = \frac{P}{Q}$$

4. Soit $\frac{P}{Q} \in \mathbb{K}(X)$.

$$\frac{P}{Q} + \frac{-P}{Q} = \frac{PQ - QP}{Q^2} = \frac{0}{Q^2} = \frac{0}{1}$$

5. “ × ” est associative
6. “ × ” est commutative
7. $\frac{1}{1}$ est le neutre pour “ × ”
8. Soient $\left(\frac{P}{Q}, \frac{R}{S}, \frac{A}{B}\right) \in \mathbb{K}(X)^3$

$$\frac{P}{Q}\left(\frac{R}{S} + \frac{A}{B}\right) = \frac{P}{Q} \times \frac{RB + AS}{SB} = \frac{PRB + PAS}{QSB}$$

et

$$\begin{aligned} \frac{P}{Q} \times \frac{R}{S} + \frac{P}{Q} \times \frac{A}{B} &= \frac{PR}{QS} + \frac{PA}{QB} \\ &= \frac{PRQB + QSPA}{Q^2SB} \\ &= \frac{PRB + SPA}{QSB} \end{aligned}$$

9. Soit $\frac{P}{Q} \neq \frac{0}{1}$ donc $P \times 1 \neq Q \times 0$ donc $P \neq 0$.

$$\frac{P}{Q} \times \frac{Q}{P} = \frac{PQ}{PQ} = \frac{1}{1}$$

10. $\dfrac{1}{1} \neq \dfrac{0}{1}$ car $1 \times 1 \neq 0 \times 1$

□

Proposition :

$$\forall P, A \in \mathbb{K}[X], \forall Q \in \mathbb{K}[X] \setminus \{0\}, \qquad \frac{P}{Q} + \frac{A}{Q} = \frac{P + A}{Q}$$

Proposition : $i : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \dfrac{P}{1} \end{array}$ est un morphisme d'anneaux injectif.

Preuve :
Soient $P, Q \in \mathbb{K}[X]$.

$$\begin{aligned} i(P+Q) &= \frac{P+Q}{1} = \frac{P}{1} + \frac{Q}{1} = i(P) + i(Q) \\ i(PQ) &= \frac{PQ}{1} = \frac{PQ}{1 \times 1} = \frac{P}{1} \times \frac{Q}{1} = i(P) \times i(Q) \\ i(1) &= \frac{1}{1} \end{aligned}$$

Donc i est un morphisme d'anneaux.

$$\begin{aligned} P \in \mathrm{Ker}(i) &\iff i(P) = \frac{0}{1} \\ &\iff \frac{P}{1} = \frac{0}{1} \\ &\iff P \times 1 = 0 \times 1 \\ &\iff P = 0 \end{aligned}$$

donc i est injective. □

Définition : Soient $\lambda \in \mathbb{K}$ et $F = \dfrac{P}{Q} \in \mathbb{K}(X)$. On pose

$$\lambda F = \frac{\lambda P}{Q} = \frac{\lambda}{1} \times \frac{P}{Q}$$

Proposition : $\big(\mathbb{K}(X),+,\cdot\big)$ est un $\mathbb{K}$-espace vectoriel et i : $\begin{array}{ccc}\mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \dfrac{P}{1}\end{array}$ est linéaire. □

Remarque :
On peut identifier $P \in \mathbb{K}[X]$ avec $\dfrac{P}{1} \in \mathbb{K}(X)$ i.e. écrire $P = \dfrac{P}{1}$ et alors
$\begin{cases}\mathbb{K}[X] \text{ est un sous-anneau de } \mathbb{K}(X) \\ \mathbb{K}[X] \text{ est un sous-espace vectoriel de } \mathbb{K}(X)\end{cases}$
De plus, les deux définitions de degré coïncident.

Proposition : Soit $F, G \in \mathbb{K}(X)$.

1. $\deg(F+G) \leqslant \max(\deg F, \deg G)$
   Si $\deg(F) \neq \deg(G)$ alors $\deg(F+G) = \max(\deg F, \deg G)$;
2. $\deg(FG) = \deg(F) + \deg(G)$;
3. Si $F \neq 0$, $\deg\left(\dfrac{1}{F}\right) = -\deg(F)$.

Preuve :
On pose $F = \dfrac{A}{B}$ et $G = \dfrac{P}{Q}$.

1. $F + G = \dfrac{AQ+PB}{BQ}$. On suppose que $\deg(F) \geqslant \deg(G)$ i.e. $\deg A - \deg B \geqslant \deg P - \deg Q$.

$$\deg(F+G) = \deg(QA+PB) - \deg(BQ)$$

On a

$$\deg(AQ) = \deg(A) + \deg(Q) \geqslant \deg(P) + \deg(B) = \deg(PB).$$

D'où

$$\deg(F+G) \leqslant \deg(AQ) - \deg(BQ) = \deg\left(\frac{AQ}{BQ}\right) = \deg(F).$$

Si $\deg(F) > \deg(G)$, alors $\deg(AQ) > \deg(PB)$ et donc

$$\deg(F+G) = \deg(AQ) - \deg(BQ) = \deg(F).$$

2.

$$\begin{aligned}\deg(FG) &= \deg\left(\frac{AP}{BQ}\right)\\ &= \deg(AP) - \deg(BQ)\\ &= \deg(A) + \deg(P) - \deg(B) - \deg(Q)\\ &= \deg F + \deg G.\end{aligned}$$

3. $\deg\left(\frac{1}{F}\right) = \deg(1) - \deg(F) = -\deg(F)$

□

2 Décomposition en éléments simples

nition

Lemme :

$$\forall F \in \mathbb{K}(X), \exists!(E,G) \in \mathbb{K}[X] \times \mathbb{K}(X), \begin{cases} F = E + G \\ \deg(G) < 0 \end{cases}$$

On dit que E est la partie entière de F.

Preuve :
On pose $F = \frac{P}{Q}$ avec $P \in \mathbb{K}[X], Q \in \mathbb{K}[X] \setminus \{0\}$.

Analyse Soit $E \in \mathbb{K}[X]$ et $G \in \mathbb{K}(X)$ tels que

$$F = E + G \deg(G) < 0.$$

On pose $G = \frac{A}{Q}$ avec $A \in \mathbb{K}[X]$.

$$\begin{aligned} F = E + G &\iff \frac{P}{Q} = E + \frac{A}{Q}\\ &\iff P = EQ + A.\end{aligned}$$

$\deg G < 0, \deg A < \deg Q$.

Don E est le quotient de la division euclidienne de P par Q et A sont reste.

Synthèse Soient E le quotient et A le reste de la division euclidienne de P par Q. On a alors

$$\begin{cases} P = EQ + A \\ \deg(A) < \deg(Q) \end{cases}$$

et donc

$$F = E + \frac{A}{Q}\deg\left(\frac{A}{Q}\right) < 0.$$

□

EXEMPLE :
$F = \dfrac{X^3 + X - 1}{X^2 + 2}$, $\deg F = 1$.

$$\begin{array}{r|l} X^3 + X - 1 & X^2 + 2 \\ \hline -\quad X^3 + 2X & X \\ \hline -X - 1 & \end{array}$$

Donc,

$$F = \frac{X(X^2+2) - (X+1)}{X^2+2} = X - \frac{X+1}{X^2+2}.$$

Lemme : Soit $F = \dfrac{P}{AB}$ avec

$$\begin{cases} (P, A, B) \in \mathbb{K}[X]^3; \\ A \neq 0; B \neq 0; \\ A \wedge B = 1; \deg F < 0. \end{cases}$$

Alors,

$$\exists!(U, V) \in \mathbb{K}[X]^2, \begin{cases} F = \dfrac{U}{A} + \dfrac{V}{B} \\ \deg\left(\dfrac{U}{A}\right) < 0 \text{ et } \deg\left(\dfrac{V}{R}\right). \end{cases}$$

Preuve ANALYSE On suppose que

$$\begin{cases} F = \dfrac{U}{A} + \dfrac{V}{B} \\ U \in \mathbb{K}[X], \deg U < \deg A \\ V \in \mathbb{K}[X], \deg V < \deg B. \end{cases}$$

D'où

$$\frac{P}{AB} = \frac{UB + VA}{AB}$$

et donc $P = UB + VA$. D'après le théorème de Bézout, il existe $(R, S) \in \mathbb{K}[X]^2$ tel que

$$RB + SA = P.$$

On a alors

$$0 = B(R-U) + A(S-V)$$

donc

$$A(S-V) = B(U-R)$$

donc

$$A \mid B(U-R) \qquad \text{dans } \mathbb{K}[X].$$

D'après le théorème de Gauß,

$$A \mid U-R$$

Donc $U-R = AT$ avec $T \in \mathbb{K}[X]$ donc

$$A(S-V) = BAT$$

donc

$$S-V = BT$$

donc

$$\begin{cases} R = -AT+U \\ S = BT+V \end{cases}.$$

On a

$$\begin{cases} S = BT+V \\ \deg V < \deg B \end{cases}$$

donc V est le reste de la division euclidienne de S par B et U est le reste de la division euclidienne de R par A.

Synthèse Soit $(R,S) \in \mathbb{K}[X]^2$ tel que

$$P = RB + SA.$$

Soit V le reste de la division euclidienne de S par B.

$$\begin{cases} S = BT+V, T \in \mathbb{K}[X] \\ \deg V < \deg B \end{cases}$$

D'où,

$$\frac{P}{AB} = \frac{R}{A} + T + \frac{V}{B} = \frac{R+AT}{A} + \frac{V}{B}$$

et

$$\deg\left(\frac{V}{B}\right) = \deg(V) - \deg(B) < 0.$$

Si $\deg\left(\dfrac{R+AT}{A}\right) \geqslant 0$, alors

$$\deg\left(\frac{R+AT}{A}\right) > \deg\left(\frac{V}{B}\right)$$

et alors
$$\deg\left(\frac{P}{AB}\right) = \deg\left(\frac{R+AT}{A}\right) \geqslant 0.$$
Or,
$$\deg\left(\frac{P}{AB}\right) < 0.$$
Donc
$$\deg\left(\frac{R+AT}{A}\right) < 0.$$
On pose $U = R + AT$. On a bien
$$\frac{P}{AB} = \frac{U}{A} + \frac{V}{B} \text{ avec } \deg\left(\frac{U}{V}\right) < 0 \text{ et } \deg\left(\frac{V}{R}\right) < 0.$$

□

Lemme : Soit $H \in \mathbb{K}[X]$ irréductible, $n \in \mathbb{N}_\star$, $P \in \mathbb{K}[X]$, $F = \dfrac{P}{H^n}$ et $\deg F < 0$. Alors,
$$\begin{cases} \exists!(U,V) \in \mathbb{K}[X]^2, F = \dfrac{U}{H^n} + \dfrac{V}{H^{n-1}}; \\ \deg U < \deg H; \\ \deg\left(\dfrac{V}{H^{n+1}}\right) < 0. \end{cases}$$

Preuve :

Analyse $F = \dfrac{U}{H^n} + \dfrac{V}{H^{n-1}}$ avec
$$\begin{cases} \deg U < \deg H, \\ U \in \mathbb{K}[X], V \in \mathbb{K}[X], \\ \deg\left(\dfrac{V}{H^{n-1}}\right) < 0. \end{cases}$$
D'où
$$P = U + VH,\ \deg U < \deg H.$$
Donc V est le quotient et U le reste de la division euclidienne de P par H.

Synthèse Soient V et U le quotient et le reste de la division euclidienne de P par H :
$$\begin{cases} P = U + VH \\ \deg U < \deg H. \end{cases}$$

D'où

$$F = \frac{U}{H^n} + \frac{V}{H^{n-1}}$$
$$\deg U < \deg H$$

Si $\deg\left(\frac{V}{H^{n-1}}\right) \geqslant 0$, alors $\deg F = \deg\left(\frac{V}{H^{n-1}}\right) \geqslant 0$: une contradiction. Donc $\deg\left(\frac{V}{H^{n-1}}\right) < 0$.

□

Théorème (Théorème de décomposition en éléments simples sur $\mathbb{C}(\mathbf{X})$) **:**
Soit $F \in \mathbb{K}(X)$, $F = \frac{P}{Q}$ la forme irréductible de F. On note $(z_1, \ldots, z_p)$ les racines complexes de Q et $(\mu_1, \ldots, \mu_p)$ leur multiplicité.

Alors,

$$\exists!(E, a_{1,1}, \ldots, a_{1,\mu_1}, a_{2,1}, \ldots, a_{2,\mu_2}, \ldots, a_{p,1}, \ldots, a_{p,\mu_p}) \in \mathbb{C}[X] \times \mathbb{C}^{\deg Q},$$
$$F = E + \sum_{i=1}^{p}\left(\sum_{j=1}^{\mu_i} \frac{a_{i,j}}{(X - z_i)^j}\right).$$

Exemple :
$F = \dfrac{X^7 - 1}{X^5 + 2X^3 + X} \in \mathbb{C}(X)$

$$\begin{array}{rr|l} X^7 - 1 & & X^5 + 2X^3 + X \\ -\ X^7 + 2X^5 + X^3 & & \hline X^2 - 2 \\ \hline -2X^5 - X^3 - 1 & & \\ -\ 2X^5 - 4X^3 - 2X & & \\ \hline 3X^3 + 2X - 1 & & \end{array}$$

$$F = (X^2 - 2) + \frac{3X^3 + 2X - 1}{X^5 + 2X^3 + X}$$

$$\begin{aligned} X^5 + 2X^3 + X &= X(X^4 + 2X^2 + 1) \\ &= X(X^2 + 1)^2 \\ &= X(X - i)^2(X + i)^2 \end{aligned}$$

D'après le 2ème lemme,

$$\frac{3X^3 + 2X - 1}{X^5 + 2X^3 + X} = \frac{a}{X} + \frac{bX + c}{(X - i)^2}$$

D'après le 3ème lemme,

$$\frac{bX+c}{(X-i)^2} = \frac{f}{(X-i)^2} + \frac{g}{X-i}$$
$$\frac{dX+e}{(X+i)^2} = \frac{h}{(X+i)^2} + \frac{h}{X+i}$$

$$F = (X^2-2) + \frac{a}{X} + \frac{f}{(X-i)^2} + \frac{g}{X-i} + \frac{h}{(X-i)^2} + \frac{k}{X+i}.$$

On multiplie par X :

$$\frac{X^7-1}{X^4+2X^2+1} = a + X\left(X^2 - 2 + \frac{f}{(X-i)^2} + \frac{g}{X-i} + \frac{h}{(X-i)^2} + \frac{k}{X+1}\right).$$

En remplaçant X par 0, on obtient

$$a = \frac{-1}{1} = -1.$$

On multiplie par $(X-i)^2$ et on remplace X par i :

$$\frac{3i^2+2i-1}{i(2i)^2} = f.$$

Donc,

$$f = \frac{-i-1}{-4i} = \frac{1}{4} - \frac{i}{4}$$

De même,

$$h = \frac{3(-i)^3+2(-i)-1}{-i(-2i)^2} = \overline{f} = \frac{1}{4} + \frac{i}{4}$$

$$\frac{3X^2+2X-1}{X^5+2X^3}+\frac{1}{X}-\left(\frac{1}{4}-\frac{i}{4}\right)\frac{1}{(X-i)^2}-\left(\frac{1}{4}+\frac{i}{4}\right)\frac{1}{(X+i)^2}=\frac{g}{X-i}+\frac{h}{X+i}$$

$$\begin{aligned}
\frac{g}{X-i}+\frac{h}{X+i} &= \frac{3X^3+2X-1+X^4+2X^2+1+X(X+i)^2\left(-\frac{1}{4}+\frac{i}{4}\right)-X(X-i)^2\left(\frac{1}{4}-\frac{i}{4}\right)}{X^5+2X^3+X}\\
&= \frac{12X^3+8X-4+4X^4+8X^2+4+X^3(-1+i)+(1-i)X-X^3(1+i)-2X^2(1-i)+X(1+i)}{4(X^5+2X^3+X)}\\
&= \frac{4X^4+10X^3+8X^2+10X}{4\left(X^5+2X^3+X\right)}\\
&= \frac{2X^3+5X^2+2X+5}{2(X^4+2X^2+1)}\\
&= \frac{(X-i)(X+i)(2X+5)}{2(X-i)^2(X+i)^2}\\
&= \frac{2X+5}{2(X-i)(X+i)}
\end{aligned}$$

Donc,

$$\begin{cases} g=\dfrac{2i+5}{2\times 2i}=\dfrac{(2i+5)i}{-4}=\dfrac{2-5i}{4} \\ h=\dfrac{2(-i)+5}{2(-2i)}=\dfrac{2+5i}{4} \end{cases}$$

Preuve :
On suppose $\frac{P}{Q} \notin \mathbb{C}[X]$. On peut supposer Q unitaire.

Existence D'après le lemme 1, il existe $E \in \mathbb{C}[X]$, $G \in \mathbb{C}(X)$ tels que

$$\begin{cases} \frac{P}{Q} = E + G \\ \deg(G) < 0 \end{cases}$$

Soit $\frac{A}{B}$ la forme irréductible de G avec B unitaire ($A \wedge B = 1$ et $A \neq 0$).

$$\frac{P}{Q} = E + \frac{A}{B}$$

donc

$$PB = EBQ + AQ \qquad (\star)$$

donc

$$AQ = PB - EBQ$$

donc

$$A \mid B(P - EQ)$$

D'après le théorème de Gauß,

$$A \mid P - EQ$$

Soit $R \in \mathbb{C}[X]$ tel que

$$AR = P - EQ$$

D'où

$$\frac{AR}{Q} = \frac{P}{Q} - E = \frac{A}{B}$$

D'où

$$\frac{R}{Q} = \frac{1}{B}$$

donc $B \mid Q$.
De $(\star)$, on a aussi

$$P \mid Q(EB + A)$$

Or, $P \wedge Q = 1$. Donc

$$P \mid EB + A$$

Soit $S \in \mathbb{C}[X]$ tel que

$$PS = EB + A$$

Donc

$$\frac{PS}{B} = E + \frac{A}{B} = \frac{P}{Q}$$

Donc
$$\frac{S}{B} = \frac{1}{Q}$$
et donc $Q \mid B$
Donc $Q = B$ (car ils sont unitaires).
Donc $G = \dfrac{A}{Q}$.
Or,
$$Q = \prod_{j=1}^{p} (X - z_j)^{\mu_j}$$
$$\forall j \neq k, (X - z_j)^{\mu_j} \wedge (X - z_k)^{\mu_k} = 1$$
D'après le lemme 2, il existe $(A_1, \ldots, A_p) \in \mathbb{C}[X]^p$ tel que
$$\begin{cases} \dfrac{A}{Q} = \displaystyle\sum_{j=1}^{p} \frac{A_j}{(X - z_j)^{\mu_j}} \\ \forall j \in [\![1, p]\!], \deg(A_j) < \mu_j \end{cases}$$
Soit $j \in [\![1, p]\!]$. D'après le lemme 3,
$$\frac{A_j}{(X - z_j)^{\mu_j}} = \frac{a_{j,\mu_j}}{(X - z_j)^{\mu_j}} + \frac{A_{j,1}}{(X - z_j)^{\mu_j - 1}}$$
avec
$$\begin{cases} a_{j,\mu_j} \in \mathbb{C} \\ A_{j,1} \in \mathbb{C}_{\mu_j - 2}[X] \end{cases}$$
En itérant ce procédé, on trouve $(a_{j,\mu_j}, \ldots, a_{j,1}) \in \mathbb{C}^{\mu_j}$ tel que
$$\frac{A_j}{(X - z_j)^{\mu_j}} = \sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X - z_j)^k}$$
D'où
$$\frac{P}{Q} = E + \underbrace{\sum_{j=1}^{p} \sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X - z_j)^k}}_{\deg(\quad) < 0}$$

Unicité Soit $E_1 \in \mathbb{C}[X]$ et $(b_{j,k})_{\substack{1 \leqslant j \leqslant p \\ 1 \leqslant k \leqslant \mu_j}} \in \mathbb{C}^{\sum_{j=1}^{p} \mu_j}$ tels que
$$\frac{P}{Q} = E_1 + \underbrace{\sum_{j=1}^{p} \sum_{k=1}^{\mu_j} \frac{b_{j,k}}{(X - z_j)^k}}_{\deg(\quad) < 0}$$

D'après le lemme 1,

$$E = E_1 \text{ et } \sum_{j=1}^{p}\sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X-z_j)^k} = \sum_{j=1}^{p}\sum_{k=1}^{\mu_j} \frac{b_{j,k}}{(X-z_j)^k}$$

$$\forall j \in [\![1,p]\!],$$
$$\sum_{k=0}^{\mu_j} \frac{b_{j,k}}{(X-z_j)^k} = \frac{\sum_{k=1}^{\mu_j} b_{j,k}(X-z_j)^{\mu_j-k}}{(X-z_j)^{\mu_j}}$$
$$\|$$
$$\sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X-z_j)^k} = \frac{\sum_{k=1}^{\mu_j} a_{j,k}(X-z_j)^{\mu_j-k}}{(X-z_j)^{\mu_j}}$$

Donc,

$$\sum_{k=1}^{\mu_j} a_{j,k}(X-z_j)^k = \sum_{k=1}^{\mu_j} b_{j,k}(X-z_j)^k$$

Comme $\left(X-z_j, (X-z_j)^2, \dots, (X-z_j)^{\mu_j}\right)$ est libre dans $\mathbb{C}[X]$,

$$\forall k \in [\![1,\mu_j]\!], b_{j,k} = a_{j,k}$$

□

Théorème (Théorème de décomposition en éléments simples sur $\mathbb{R}(\boldsymbol{X})$) **:**
Soit $(P,Q) \in \mathbb{R}[X]^2$, $P \wedge Q = 1$, Q unitaire, $Q \notin \{0,1\}$. On pose

$$Q = \prod_{i=1}^{p}(X-a_i)^{\mu_i} \prod_{k=1}^{q}(X^2+\alpha_k X+\beta_k)^{\nu_k}$$

avec

$$\begin{cases} p \in \mathbb{N}, q \in \mathbb{N}, \\ (a_1,\dots,a_p) \in \mathbb{R}^p \\ (\alpha_1,\dots,\alpha_q,\beta_1,\dots,\beta_q) \in \mathbb{R}^{2q} \\ (\mu_1,\dots,\mu_p,\nu_1,\dots,\nu_p) \in \mathbb{N}^{p+q} \\ \forall j \in [\![1,q]\!], \alpha_k^2 - 4\beta_k < 0 \end{cases}$$

Alors

$$\begin{aligned} \exists!(E, &\gamma_{1,1},\dots,\gamma_{1,\mu_1},\gamma_{2,1},\dots,\gamma_{2,\mu_2},\dots,\gamma_{p,1},\dots,\gamma_{p,\mu_p}, \\ &\delta_{1,1},\dots,\delta_{1,\nu_1},\delta_{2,1},\dots,\delta_{2,\nu_2},\dots,\delta_{q,1},\dots,\delta_{q,\nu_q}, \\ &\varepsilon_{1,1},\dots,\varepsilon_{1,\nu_1},\varepsilon_{2,1},\dots,\varepsilon_{2,\nu_2},\dots,\varepsilon_{q,1},\dots,\varepsilon_{q,\nu_q}) \\ &\in \mathbb{R}[X] \times \mathbb{R}^{\mu_1+\dots+\mu_p} \times \mathbb{R}^{2(\nu_1+\dots+\nu_q)} \end{aligned}$$

$$\frac{P}{Q} = E + \sum_{i=1}^{p}\sum_{j=1}^{\mu_i} \frac{\gamma_{i,j}}{(X-a_i)^j} + \sum_{k=1}^{q}\sum_{j=1}^{\nu_k} \frac{\delta_{k,j}X + \varepsilon_{k,j}}{(X^2+\alpha_k X+\beta_k)^j}$$

□

Définition : Soit $F \in \mathbb{C}(X)$. Soient $(P,Q) \in \mathbb{C}[X]^2$ tels que $\begin{cases} P \wedge Q = 1 \\ F = \dfrac{P}{Q} \end{cases}$.
Les racines de P sont appelées zéros de F
Les racines de Q sont appelées pôles de F

Proposition : Soit $F \in \mathbb{C}(X)$ et $z \in \mathbb{C}$ un pôle simple de F. Le coefficient devant $\dfrac{1}{X-z}$ dans la décomposition en éléments simples de F est $\dfrac{P(z)}{Q'(z)}$.

Preuve :
Soit $(P,Q) \in \mathbb{C}[X]^2$ tels que

$$\begin{cases} F = \dfrac{P}{Q} \\ P \wedge Q = 1 \\ Q \text{ unitaire} \end{cases}$$

On pose

$$Q = (X-z)\prod_{i=1}^{q}(X-z_i)^{\mu_i}$$

où $z_1, \ldots, z_q$ sont les racines distinctes de z du polynôme Q. Donc,

$$\frac{P}{Q} = F = \frac{a}{X-z} + \sum_{i=1}^{q}\sum_{k=1}^{\mu_i} \frac{b_{i,k}}{(X-z_i)^k}$$

avec $a, (b_{i,k})_{\substack{1\leqslant i\leqslant q \\ 1\leqslant k\leqslant \mu_i}}$ des nombres complexes.

On muliplie par $X - z$.

$$\frac{P}{\prod_{i=1}^{q}(X-z_i)^{\mu_i}} = a + (X-z)\sum_{i=1}^{q}\sum_{k=1}^{\mu_i}\frac{b_{i,k}}{(X-z_i)^k}$$

On remplace X par z.

$$\frac{P(z)}{\prod_{i=1}^{q}(z-z_i)^{\mu_i}} = a$$

Or,

$$Q = (X-z)\prod_{i=1}^{q}(X-z_i)^{\mu_i}$$

D'où

$$Q' = \prod_{i=1}^{q}(X-z_i)^{\mu_i} + (X-z)\left(\prod_{i=1}^{q}(X-z_i)^{\mu_i}\right)'$$

Don

$$Q'(z) = \prod_{i=1}^{q}(z-z_i)^{\mu_i}$$

Donc

$$a = \frac{P(z)}{Q'(z)}$$

□

Proposition : Soit $P \in \mathbb{C}[X]$ avec $\deg(P) \geqslant 1$, $(z_1, \ldots, z_p)$ les racines de P, $\mu_1, \ldots, \mu_p$ leur multiplicité. Alors

$$\frac{P'}{P} = \sum_{i=1}^{p}\frac{\mu_i}{X-z_i}$$

Preuve :
On pose

$$P = \alpha\prod_{i=1}^{p}(X-z_i)^{\mu_i}$$

Donc

$$P' = \alpha\sum_{i=1}^{p}\left(\prod_{j\neq i}(X-z_j)^{\mu_j}\right)\mu_i(X-z_i)^{\mu_i-1}$$

D'où

$$\begin{aligned}\frac{P'}{P} &= \frac{\cancel{\alpha}\sum_{i=1}^{p}\mu_i(X-z_i)^{\mu_i-1}\prod_{j\neq i}(X-z_j)^{\mu_j}}{\cancel{\alpha}\prod_{i=1}^{p}(X-z_i)^{\mu_i}}\\ &= \sum_{i=1}^{p}\mu_i\frac{(X-z_i)^{\mu_i-1}\prod j\neq i)(X-z_j)^{\mu_j}}{\prod_{j=1}^{p}(X-z_j)^{\mu_j}}\\ &= \sum_{i=1}^{p}\mu_i\frac{1}{X-z_i}\end{aligned}$$

□

Remarque :
Il existe un "truc" pour retenir cette formule :

$$\frac{P'}{P} = \underbrace{\ln(P)'}_{\text{n'existe pas !}} = \left(\ln\left(\alpha\prod_{i=1}^{p}(X-z_i)^{\mu_i}\right)\right)' = \left(\sum_{i=1}^{p}\mu_i\ln(X-z_i)\right)' = \sum_{i=1}^{p}\mu_i\frac{1}{X-z_i}$$

Chapitre 21

Matrices et applications linéaires

1 Matrices d'un vecteur

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

Définition : Soit $x \in E$. On sait qu'il existe un unique n-uplet $(x_1, \dots, x_n) \in \mathbb{K}^n$ tel que

$$x = \sum_{i=1}^{n} x_i e_i$$

La matrice de x dans la base $\mathcal{B}$ est la colonne

$$\mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Remarque :
En général, si $\mathcal{B}$ et $\mathcal{B}'$ sont 2 bases différentes, alors $\mathrm{Mat}_{\mathcal{B}}(x) \neq \mathrm{Mat}_{\mathcal{B}'}(x)$.

Exemple :
$E = \mathbb{R}_3[X]$, $\mathbb{K} = \mathbb{R}$, $\mathcal{B} = (1, X, X^2, X^3)$ et

$$\mathscr{C} = \left(\frac{X(X-1)(X-2)}{6}, -\frac{X(X-1)(X-3)}{2}, \frac{X(X-2)(X-3)}{2}, -\frac{(X-1)(X-2)(X-3)}{6}\right)$$

$$P = X^2 - X + 1$$

$$\mathrm{Mat}_{\mathscr{B}}(P) = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix}$$

$$P = P(3)\frac{X(X-1)(X-2)}{6} + P(2)\frac{-X(X-1)(X-3)}{2} + P(1)\frac{X(X-2)(X-3)}{2} + P(0)\frac{-(X-1)(X-2)(X-3)}{6}$$

$$\mathrm{Mat}_{\mathscr{B}'}(P) = \begin{pmatrix} 7 \\ 3 \\ 1 \\ 1 \end{pmatrix}$$

2 Matrice d'une famille de vecteurs

Soient E est un $\mathbb{K}$-espace vectoriel de dimension finie n, $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E, $\mathscr{F} = (u_1, \ldots, u_p)$ une famille de vecteurs de E.

Définition : La matrice de $\mathscr{F}$ dans la base $\mathscr{B}$ est la matrice M telle que, pour tout $j \in [\![1, p]\!]$, la j-ème colonne de M est $\mathrm{Mat}_{\mathscr{B}}(u_j)$.

Exemple :

$$\mathrm{Mat}_{\mathscr{C}}(\mathscr{B}) = \begin{pmatrix} 1 & 3 & 9 & 27 \\ 1 & 2 & 4 & 8 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Proposition : Soit $\mathscr{F}$ une famille de vecteurs de E.

$$\mathrm{rg}(\mathscr{F}) = \mathrm{rg}\left(\mathrm{Mat}_{\mathscr{B}}(\mathscr{F})\right)$$

Preuve :
Dans ce chapitre, on définit le rang d'une matrices comme le nombre maximale de colonnes linéairement idépendantes. □

Corollaire : Soit $\mathscr{F} = (u_1, \dots, u_p) \in E^p$ et $\mathscr{B} = (e_1, \dots, e_n)$ une base de E, et $M = \mathrm{Mat}_{\mathscr{B}}(\mathscr{F})$.

1. $\mathscr{F}$ est libre $\iff \mathrm{rg}(M) = p$
2. $E = \mathrm{Vect}(\mathscr{F}) \iff \mathrm{rg}(M) = n$
3. $\mathscr{F}$ base de $E \iff n = p = \mathrm{rg}(M) \iff M \in \mathrm{GL}_n(\mathbb{K})$
   Dans ce cas,
   $$\left(\mathrm{Mat}_{\mathscr{B}}(\mathscr{F})\right)^{-1} = \mathrm{Mat}_{\mathscr{F}}(\mathscr{B})$$

Exemple :

$$\mathrm{Mat}_{\mathscr{C}}(\mathscr{B}) = \begin{pmatrix} 1 & 3 & 9 & 27 \\ 1 & 2 & 4 & 8 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = M$$

On sait que $\mathscr{B}$ est une base donc $M \in \mathrm{GL}_4(\mathbb{R})$. Donc,

$$M^{-1} = \mathrm{Mat}_{\mathscr{B}}(\mathscr{C}) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ \frac{1}{3} & -\frac{3}{2} & 3 & -\frac{11}{6} \\ -\frac{1}{2} & 2 & -\frac{5}{2} & 1 \\ \frac{1}{6} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{6} \end{pmatrix}$$

Preuve : 1.

$$\begin{aligned} \mathscr{F} \text{ est libre} &\iff (u_1, \dots, u_p) \text{ base de } \mathrm{Vect}(u_1, \dots, u_p) \\ &\iff \dim\left(\mathrm{Vect}(u_1, \dots, u_p)\right) = p \\ &\iff \mathrm{rg}\left((u_1, \dots, u_p)\right) = p \\ &\iff \mathrm{rg}(M) = p \end{aligned}$$

2.

$$\begin{aligned}\mathscr{F} \text{ engendre } E &\iff E = \mathrm{Vect}(u_1, \dots, u_p)\\ &\iff \dim(E) = \dim\big(\mathrm{Vect}(u_1, \dots, u_p)\big)\\ &\iff n = \mathrm{rg}(M)\end{aligned}$$

3.

$$\mathscr{F} \text{ base de } E \iff \begin{cases}\mathrm{rg}(M) = p\\ \mathrm{rg}(M) = n\end{cases}$$

On suppose que $\mathscr{F}$ est une base de E.

$$M = \mathrm{Mat}_{\mathscr{B}}(\mathscr{F}) = \begin{pmatrix} m_{11} & \dots & m_{1,n}\\ m_{21} & \dots & m_{2,n}\\ \vdots & \ddots & \vdots\\ m_{n,1} & \dots & m_{n,n}\end{pmatrix}$$

Soit $A = \mathrm{Mat}_{\mathscr{F}}(\mathscr{B}) = \begin{pmatrix} a_{11} & \dots & a_{1,n}\\ a_{21} & \dots & a_{2,n}\\ \vdots & \ddots & \vdots\\ a_{n,1} & \dots & a_{n,n}\end{pmatrix}$. Montrons que $AM = I_n$.
La première colonne de AM est

$$A\begin{pmatrix} m_{11}\\ \vdots\\ m_{n,1}\end{pmatrix} = m_{11}\begin{pmatrix} a_{11}\\ \vdots\\ a_{n,1}\end{pmatrix} + m_{21}\begin{pmatrix} a_{12}\\ \vdots\\ a_{n,2}\end{pmatrix} + \dots + m_{n,1}\begin{pmatrix} a_{1,n}\\ \vdots\\ a_{n,n}\end{pmatrix}$$

Or, $\forall i \in [\![1, n]\!]$, $\begin{pmatrix} a_{1,i}\\ \vdots\\ a_{n,i}\end{pmatrix} = \mathrm{Mat}_{\mathscr{F}}(e_i)$.
Donc, la première colonne de AM est la colonne des coordonées du vecteur $m_{11}e_1 + m_{21}e_2 + \dots + m_{n,1}e_n$ dans la base $\mathscr{F}$.
Or,

$$\mathrm{Mat}_{\mathscr{B}}(u_1) = \begin{pmatrix} m_{11}\\ m_{21}\\ \vdots\\ m_{n,1}\end{pmatrix}$$

donc $u_1 = m_{11}e_1 + m_{21}e_2 + \dots + m_{n,1}e_n$.

Comme $u_1 = 1 \cdot u_1 + 0 \cdot u_2 + \cdots + 0 \cdot u_n$,

$$\mathrm{Mat}_{\mathscr{F}}(u_1) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

La j-ème colonne de AM est

$$A \begin{pmatrix} m_{1,j} \\ \vdots \\ m_{n,j} \end{pmatrix} = m_{1,j} \begin{pmatrix} a_{11} \\ \vdots \\ a_{n,1} \end{pmatrix} + m_{2,j} \begin{pmatrix} a_{12} \\ \vdots \\ a_{n,2} \end{pmatrix} + \cdots + m_{n,j} \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{n,n} \end{pmatrix}$$

Or, $\forall i \in [\![1, n]\!]$, $\begin{pmatrix} a_{1,i} \\ \vdots \\ a_{n,i} \end{pmatrix} = \mathrm{Mat}_{\mathscr{F}}(e_i)$.
Donc, la j-ème colonne de AM est la colonne des coordonées du vecteur $m_{1,j}e_1 + m_{2,j}e_2 + \cdots + m_{n,j}e_n$ dans la base $\mathscr{F}$.
Or,

$$\mathrm{Mat}_{\mathscr{B}}(u_1) = \begin{pmatrix} m_{1,j} \\ m_{2,j} \\ \vdots \\ m_{n,j} \end{pmatrix}$$

donc $u_j = m_{1,j}e_1 + m_{2,j}e_2 + \cdots + m_{n,j}e_n$.
Comme $u_j = 0 \cdot u_1 + \cdots + 1 \cdot u_j + \cdots + 0 \cdot u_n$,

$$\mathrm{Mat}_{\mathscr{F}}(u_1) = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow j \\ \vdots \\ 0 \end{pmatrix}$$

Donc,

$$AM = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ & \ddots & \ddots & & \vdots \\ 0 & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} = I_n$$

En inversant les rôles de $\mathscr{F}$ et $\mathscr{B}$, on prouve que $MA = I_n$.

On suppose maintenant que $M \in \mathrm{GL}_n(\mathbb{K})$. Montrons que $\mathscr{F}$ est une

base de E. On pose

$$M^{-1} = \begin{pmatrix} a_{11} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix}$$

On sait que

$$M\,M^{-1} = I_n$$

Donc

$$\forall j \in [\![1,n]\!], a_{1,j} \begin{pmatrix} m_{11} \\ \vdots \\ m_{n,1} \end{pmatrix} + \dots + a_{n,j} \begin{pmatrix} m_{1,n} \\ \vdots \\ m_{n,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow j \\ \vdots \\ 0 \end{pmatrix}$$

donc

$$\forall j \in [\![1,n]\!], \mathrm{Mat}_{\mathscr{B}}\left(\sum_{i=1}^{n} a_{i,j} u_i\right) = \mathrm{Mat}_{\mathscr{B}}(e_j)$$

donc

$$\forall j \in [\![1,n]\!], e_j = \sum_{i=1}^{n} a_{i,j} u_i \in \mathrm{Vect}(\mathscr{F})$$

Donc $\mathscr{F}$ engendre E.

$$\mathrm{Card}(\mathscr{F}) = n = \dim(E)$$

donc $\mathscr{F}$ est une base de E.

□

3 Matrices d'une application linéaire

Soit $f \in \mathscr{L}(E,F)$, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E et $\mathscr{C} = (f_1, \dots, f_p)$ une base de F.

Proposition–Définition : Soit $x \in E$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathrm{Mat}_{\mathscr{B}}(x)$. Soit $y \in F$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix} = \mathrm{Mat}_{\mathscr{C}}(y)$. On pose $A = \begin{pmatrix} a_{11} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{p,1} & \dots & a_{p,n} \end{pmatrix} \in$

$\mathcal{M}_{p,n}(\mathbb{K})$ telle que

$$\forall j \in [\![1,n]\!], \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix} = \mathrm{Mat}_{\mathscr{C}}\left(f(e_j)\right)$$

Alors

$$y = f(x) \iff Y = AX$$

On dit que A est la matrice de f dans les bases $\mathscr{B}$ et $\mathscr{C}$. On la note $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f)$.

Preuve :

$$x = \sum_{j=1}^{n} x_j e_j \qquad y = \sum_{i=1}^{p} y_i f_i$$

$$\begin{aligned} y = f(x) &\iff \sum_{i=1}^{p} y_i f_i = f\left(\sum_{j=1}^{n} x_j e_j\right) \\ &\iff \sum_{i=1}^{p} y_i f_i = \sum_{j=1}^{n} x_j f(e_j) \end{aligned}$$

Or,

$$\forall j \in [\![1,n]\!], f(e_j) = \sum_{i=1}^{p} a_{i,j} f_i$$

D'où,

$$\begin{aligned} y = f(x) &\iff \sum_{i=1}^{p} y_i f_i = \sum_{j=1}^{n} x_j \sum_{i=1}^{p} a_{i,j} f_i \\ &= \sum_{i=1}^{p} \left(\sum_{j=1}^{n} a_{i,j} x_j\right) f_i \\ &\iff \forall i \in [\![1,p]\!], \sum_{j=1}^{n} a_{i,j} x_i = y_i \\ &\iff AX = Y \end{aligned}$$

□

Exemple :
$E = \mathbb{R}^3$ et f la projection sur $R = \{(x,y,z) \mid x+y=0\}$ parallèlement à $G = \mathrm{Vect}\big((1,1,1)\big)$.

— $\mathscr{B} = (e_1, e_2, e_3)$ base canonique.

$$\mathrm{Mat}_{\mathscr{B},\mathscr{B}}(f) = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$

$$e_1 = (1,0,0) = \underbrace{\left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right)}_{\in F} + \underbrace{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)}_{\in G}$$

$$f(e_1) = \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) = \frac{1}{2}e_1 - \frac{1}{2}e_2 - \frac{1}{2}e_3$$

$$e_2 = (0,1,0) = \left(-\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right) + \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

$$e_3 = (0,0,1) = (0,0,1) + (0,0,0)$$

Donc

$$\mathrm{Mat}_{\mathscr{B},\mathscr{B}}(f) = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix}$$

— $\mathscr{C} = (e_3, e_1 - e_2, e_1 + e_2 + e_3) = (u_1, u_2, u_3)$

$$\mathrm{Mat}_{\mathscr{C},\mathscr{C}}(f) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

car

$$f(u_1) = u_1 f(u_2) = u_2 f(u_3) = 0$$

—

$$\mathrm{Mat}_{\mathscr{C},\mathscr{B}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

—

$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f) = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

— Soit $(x,y,z)\in\mathbb{R}^3$

$$\begin{aligned}\mathrm{Mat}_{\mathscr{B}}\left(f\big((x,y,z)\big)\right) &= \mathrm{Mat}_{\mathscr{B},\mathscr{B}}(f)\times\mathrm{Mat}_{\mathscr{B}}\left((x,y,z)\right)\\ &= \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1\\ \frac{1}{2} & -\frac{1}{2} & 0\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}\\ &= \begin{pmatrix} \frac{x-y}{2}\\ \frac{y-x}{2}\\ \frac{-x-y}{2}+z\end{pmatrix}\end{aligned}$$

Donc

$$f\big((x,y,z)\big)=\Big(\frac{x-y}{2},\frac{y-x}{2},z-\frac{x+y}{2}\Big)$$

$$\begin{aligned}\mathrm{Mat}_{\mathscr{C}}\left(f(x,y,z)\right) &= \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f)\times\mathrm{Mat}_{\mathscr{B}}\left((x,y,z)\right)\\ &= \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1\\ \frac{1}{2} & -\frac{1}{2} & 0\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}\\ &= \begin{pmatrix} \frac{-x-y}{2}+z\\ \frac{x-y}{2}\\ 0\end{pmatrix}\end{aligned}$$

Donc

$$f\big((x,y,z)\big)=\Big(z-\frac{x+y}{2}\Big)u_1+\Big(\frac{x-y}{2}\Big)u_2$$

Exemple :
Soient $E=\mathbb{C}$, $\mathscr{B}=(1,i)$, $\theta\in\mathbb{R}$ et f la rotation de centre O et d'angle θ.

$$\begin{aligned} f:\mathbb{C}&\longrightarrow\mathbb{C}\\ z&\longmapsto e^{i\theta}z\end{aligned}$$

f est linéaire :

$$\begin{aligned}\forall(\lambda,\mu)\in\mathbb{R}^2,\forall(z,w)\in\mathbb{C}^2 f(\lambda z+\mu w) &= e^{i\theta}(\lambda z+\mu w)\\ &= \lambda e^{i\theta}z+\mu e^{i\theta}w\\ &= \lambda f(z)+\mu f(w)\end{aligned}$$

$$\mathrm{Mat}_{\mathscr{B}}(f)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$$

car

$$\begin{cases} f(1) = e^{i\theta} = \cos\theta + i\sin\theta \\ f(i) = ie^{i\theta} = -\sin\theta + i\cos\theta \end{cases}$$

$$z = x + iy \text{ avec } x, y \in \mathbb{R}$$

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta & -y\sin\theta \\ x\sin\theta & y\cos\theta \end{pmatrix}$$

Théorème : Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E et $\mathscr{C} = (f_1, \dots, f_p)$ une base de F.

$$\begin{aligned} \Phi : \mathscr{L}(E,F) &\longrightarrow \mathscr{M}_{p,n}(\mathbb{K}) \\ f &\longmapsto \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f) \end{aligned}$$

Φ est un $\mathbb{K}$-isomorphisme linéaire.

Preuve : — Soient $(f,g) \in \mathscr{L}(E,F)^2$ et $(\lambda,\mu) \in \mathbb{K}^2$. On pose $A = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f) = \Phi(f) = (a_{i,j})$ et $B = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(g) = \Phi(g) = (b_{i,j})$. On pose également $C = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(\lambda f + \mu g) = \Phi(\lambda f + \mu g) = (c_{i,j})$.

$$\begin{aligned} \forall j \in [\![1,n]\!], \begin{pmatrix} c_{1,j} \\ \vdots \\ c_{p,j} \end{pmatrix} &= \mathrm{Mat}_{\mathscr{C}}\left((\lambda f + \mu g)(e_j)\right) \\ &= \mathrm{Mat}_{\mathscr{C}}\left(\lambda f(e_j) + \mu g(e_j)\right) \end{aligned}$$

Or,

$$\mathrm{Mat}_{\mathscr{C}}\left(f(e_j)\right) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix}$$

et

$$\mathrm{Mat}_{\mathscr{C}}\left(g(e_j)\right) = \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{p,j} \end{pmatrix}$$

Donc

$$\mathrm{Mat}_{\mathscr{C}}\left(\lambda f(e_j) + \mu g(e_j)\right) = \lambda \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix} + \mu \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{p,j} \end{pmatrix}$$

Donc $C = \lambda A + \mu B$ et donc Φ est linéaire.

— Soit $f \in \operatorname{Ker}\Phi$:

$$\operatorname{Mat}_{\mathscr{B},\mathscr{C}}(f) = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

Donc

$$\forall j \in [\![1, n]\!], f(e_j) = \sum_{i=1}^{p} 0 \cdot f_i = 0_F$$

Soit $x \in E$. On pose $x = \sum_{j=1}^{n} x_j e_j$.

$$f(x) = \sum_{j=1}^{n} x_j f(e_j) = 0_F$$

Donc $f = 0$. Donc Φ est injective.
Soit $A \in \mathscr{M}_{p,n}(\mathbb{K})$. On pose $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}}$.
On définit $F : E \to F$ de la façon suivante : pour tout $x \in E$, on décompose $x = \sum_{j=1}^{n} x_j e_j$. On pose alors

$$\begin{aligned} f(x) &= \sum_{j=1}^{n} x_j \sum_{i=1}^{p} a_{i,j} f_i \\ &= \sum_{i=1}^{p} \sum_{j=1}^{n} a_{i,j} x_j f_i \end{aligned}$$

Montrons que $f \in \mathscr{L}(E, F)$ et $\Phi(f) = A$
— Soit $(x, y) \in E^2$ et $(\alpha, \beta) \in \mathbb{K}^2$. On pose

$$\begin{cases} x = \sum_{j=1}^{n} x_j e_j & \text{avec } (x_1, \ldots, x_n) \in \mathbb{K}^n \\ y = \sum_{j=1}^{n} y_j e_j & \text{avec } (y_1, \ldots, y_n) \in \mathbb{K}^n \end{cases}$$

Donc

$$\alpha x + \beta y = \sum_{j=1}^{n} (\alpha x_j + \beta y_j)(e_j$$

D'où

$$\begin{aligned} f(\alpha x+\beta y) &= \sum_{i=1}^{p}\sum_{j=1}^{n} a_{i,j}(\alpha x_j+\beta x_j)f_i \\ &= \alpha\sum_{i=1}^{p}\sum_{j=1}^{n} a_{i,j}x_j f_i + \beta\sum_{i=1}^{p}\sum_{j=1}^{n} b_{i,j}y_j f_i \\ &= \alpha f(x)+\beta f(y) \end{aligned}$$

Soit $j \in [\![1,p]\!]$.

$$f(e_j) = \sum_{i=1}^{p} a_{i,j} f_i$$

et

$$\mathrm{Mat}_{\mathscr{C}}\left(f(e_j)\right) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix}$$

donc

$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f) = A$$

□

Corollaire : Si E et F sont deux $\mathbb{K}$-espaces vectoriels de dimension finie, alors

$$\dim\left(\mathscr{L}(E,F)\right) = \dim(E)\times\dim(F)$$

□

Exemple (*Trouver tous les endomorphismes de* $\mathbb{R}^2$) :
Soit $\mathscr{B} = (e_1, e_2)$ la base canonique de $\mathbb{R}^2$.

$$\begin{aligned} \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (ax+cy, bx+dy) \end{aligned}$$

avec $(a,b,c,d) \in \mathbb{R}^4$.
Une base de $\mathscr{L}(\mathbb{R}^2)$ est (f_1, f_2, f_3, f_4) où

$$\begin{cases} f_1 : (x,y) \mapsto (x,0) \\ f_2 : (x,y) \mapsto (0,x) \\ f_3 : (x,y) \mapsto (y,0) \\ f_4 : (x,y) \mapsto (0,y) \end{cases}$$

Théorème : Soient $f \in \mathscr{L}(E,F)$ et $g \in \mathscr{L}(F,G)$, $\mathscr{B}$ une base de E, $\mathscr{C}$ une base de F et $\mathscr{D}$ une base de G. Alors

$$\mathrm{Mat}_{\mathscr{B},\mathscr{D}}(g \circ f) = \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(g) \times \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f)$$

Preuve :
On pose

$$\begin{aligned}\mathscr{B} &= (e_1, \dots, e_n)\\ \mathscr{C} &= (f_1, \dots, f_p)\\ \mathscr{D} &= (g_1, \dots, g_q).\end{aligned}$$

et

$$\begin{aligned}A = (a_{i,j})_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant n}} &= \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f)\\ B = (b_{k,i})_{\substack{1\leqslant k\leqslant q\\ 1\leqslant i\leqslant p}} &= \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(g)\\ C = (c_{k,j})_{\substack{1\leqslant k\leqslant q\\ 1\leqslant j\leqslant n}} &= \mathrm{Mat}_{\mathscr{B},\mathscr{D}}(g \circ f)\end{aligned}$$

Soit $j \in [\![1, n]\!]$. La j-ième colonne de C est

$$\begin{aligned}\mathrm{Mat}_{\mathscr{D}}\left(g \circ f(e_j)\right) &= \mathrm{Mat}_{\mathscr{D}}\left(g\big(f(e_j)\big)\right)\\ &= \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(g) \times \mathrm{Mat}_{\mathscr{C}}\left(f(e_j)\right)\\ &= BA_j\end{aligned}$$

où A_j est la j-ème colonne de A.
Or, la j-ème colonne de BA est aussi BA_j.
Donc, $C = BA$. □

4 Formules de changement de bases

Proposition : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.
Soient $\mathscr{B}_1$ et $\mathscr{B}_2$ deux bases de E et $x \in E$. Soit $P = P_{\mathscr{B}_1 \to \mathscr{B}_2} = \mathrm{Mat}_{\mathscr{B}_1}(\mathscr{B}_2)$.
Alors

$$\mathrm{Mat}_{\mathscr{B}_2}(x) = P^{-1}\,\mathrm{Mat}_{\mathscr{B}_1}(x)$$

Preuve :

$$P = \mathrm{Mat}_{\mathscr{B}_2,\mathscr{B}_1}(\mathrm{id}_E) = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$

si $\begin{cases} \mathscr{B}_1 = (e_1, \dots, e_n) \\ \mathscr{B}_2 = (u_1, \dots, u_n) \end{cases}$

$$\begin{aligned} P\,\mathrm{Mat}_{\mathscr{B}_2}(x) &= \mathrm{Mat}_{\mathscr{B}_2,\mathscr{B}_1}(\mathrm{id}_E) \times \mathrm{Mat}_{\mathscr{B}_2}(x) \\ &= \mathrm{Mat}_{\mathscr{B}_1}\left(\mathrm{id}_E(x)\right) \\ &= \mathrm{Mat}_{\mathscr{B}_1}(x) \end{aligned}$$

$$\begin{array}{ccccc} E_{\mathscr{B}_2} & & \overset{x}{X} & \xrightarrow[P]{\mathrm{id}_E} & \overset{\mathrm{id}_E(x)}{PX} \\ & & & & E_{\mathscr{B}_1} \end{array}$$

□

Proposition : Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie $\mathscr{B}_1$ et $\mathscr{B}_2$ deux bases de E, et $\mathscr{C}_1, \mathscr{C}_2$ deux bases de F et $f \in \mathscr{L}(E,F)$.

Soient $\begin{cases} P = P_{\mathscr{B}_1 \to \mathscr{B}_2} = \mathrm{Mat}_{\mathscr{B}_1}(\mathscr{B}_2) \\ Q = P_{\mathscr{C}_1 \to \mathscr{C}_2} = \mathrm{Mat}_{\mathscr{C}_1}(\mathscr{C}_2) \\ A = \mathrm{Mat}_{\mathscr{B}_1,\mathscr{C}_1}(f) \end{cases}$ Alors,

$$\mathrm{Mat}_{\mathscr{B}_2,\mathscr{C}_2}(f) = Q^{-1}AP$$

Preuve :

$$\begin{array}{ccccc} E_{\mathscr{B}_1} & \overset{f}{\underset{A}{}} & F_{\mathscr{C}_1} & \longrightarrow & \\ \mathrm{id}_E \;\; P & & \mathrm{id}_F \;\; Q^{-1} & \uparrow \quad \downarrow & \\ E_{\mathscr{B}_2} & \overset{f}{\underset{A'}{}} & F_{\mathscr{C}_2} & \longrightarrow & \\ & & ! & & \end{array}$$

$f = \mathrm{id}_F \circ f \circ \mathrm{id}_E$ donc

$$\mathrm{Mat}_{\mathscr{B}_2,\mathscr{C}_2}(f) = \mathrm{Mat}_{\mathscr{C}_1,\mathscr{C}_2}(\mathrm{id}_F)\,\mathrm{Mat}_{\mathscr{B}_1,\mathscr{C}_1}(f)\,\mathrm{Mat}_{\mathscr{B}_2,\mathscr{B}_1}(\mathrm{id}_E)$$

□

Exemple :
$E = \mathbb{R}^3$, $F = \{(x,y,z) \in \mathbb{R}^3 \mid x+y=0\}$, $G = \text{Vect}\big((1,1,1)\big)$ et f la projection sur F parallèlement à G.
Soient $\mathscr{B} = (e_1, e_2, e_3)$ base canonique de E et $\mathscr{C} = (u_1, u_2, u_3)$ avec $\begin{cases} u_1 = (0,0,1) \\ u_2 = (1,-1,0) \\ u_3 = (1,1,1) \end{cases}$.

$$\text{Mat}_{\mathscr{C}}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Donc

$$\text{Mat}_{\mathscr{B}}(f) = \begin{pmatrix} 0 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix}^{-1}$$

Proposition–Définition : Soient $(A,B) \in \mathscr{M}_{p,n}(\mathbb{K})^2$.
On dit que A et B sont équivalentes si

$$\exists (P,Q) \in \text{GL}_n(\mathbb{K}) \times \text{GL}_p(\mathbb{K}), B = Q^{-1}AP$$

Cette relation est une relation d'équivalence. □

Théorème : Soit $f \in \mathscr{L}(E)$, $\mathscr{B}$ et $\mathscr{C}$ deux bases de E, $P = P_{\mathscr{B}\to\mathscr{C}} = \text{Mat}_{\mathscr{B}}(\mathscr{C})$, $A = \text{Mat}_{\mathscr{B}}(f)$ et $B = \text{Mat}_{\mathscr{C}}(f)$.
Alors

$$B = P^{-1}AP.$$

□

Définition : Soit $(A,B) \in \mathscr{M}_n(\mathbb{K})^2$. On dit que A et B sont semblables s'il existe $P \in \text{GL}_n(\mathbb{K})$ telle que

$$B = P^{-1}AP.$$

L'ensemble $\{P^{-1}AP \mid P \in \text{GL}_n(\mathbb{K})\}$ est la classe de similitude de A.

Exemple :

$$\begin{cases} \forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n \\ u_0 = 0 \\ u_1 = 1 \end{cases}$$

On pose

$$\forall n \in \mathbb{N}, X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} \text{ et } X_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

On a

$$\begin{aligned} \forall n \in \mathbb{N}, X_{n+1} &= \begin{pmatrix} u_{n+1} \\ u_{n+2} \end{pmatrix} \\ &= \begin{pmatrix} u_{n+1} \\ u_n + u_{n+1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} \\ &= AX_n \text{ avec } A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

D'où

$$\forall n \in \mathbb{N}, X_n = A^n X_0$$

On aimerait trouver D diagonale et $P \in \mathrm{GL}_2(\mathbb{C})$ telles que

$$A = PDP^{-1}.$$

Soit $f : \begin{array}{ccc} \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 \\ (z_1, z_2) & \longmapsto & (z_2, z_1 + z_2) \end{array}$ telle que $\mathrm{Mat}_{\mathcal{B}}(f) = A$ où $\mathcal{B} = (e_1, e_2)$ est la base canonique de $\mathbb{C}^2$.

On cherche $\mathcal{C} = (u_1, u_2)$ une base de $\mathbb{C}^2$ telle que $\mathrm{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D$ avec $(\lambda_1, \lambda_2) \in \mathbb{C}^2$.

Analyse On suppose que $\mathcal{C}$ existe. Dans ce cas,

$$\begin{cases} f(u_1) = \lambda_1 u_1, \\ f(u_2) = \lambda_2 u_2, \\ (\lambda_1, \lambda_2) \text{ libre.} \end{cases}$$

Soit $u = (x, y) \in \mathbb{C}^2$ et $\lambda \in \mathbb{C}$.

$$\begin{aligned} f(u) = \lambda u &\iff \begin{cases} y = \lambda x \\ x + y = \lambda y \end{cases} \\ &\iff \begin{cases} y = \lambda x \\ x + \lambda x - \lambda^2 x = 0 \end{cases} \\ &\iff \begin{cases} y = \lambda x \\ x(1 + \lambda - \lambda^2) = 0 \end{cases} \\ &\iff \begin{cases} x = 0 \\ y = 0 \end{cases} \text{ ou } \begin{cases} A + \lambda - \lambda^2 = 0 \\ y = \lambda x \end{cases} \\ &\iff u = (0,0) \text{ ou } \begin{cases} \lambda = \dfrac{-1+\sqrt{5}}{2} \\ y = \dfrac{-1+\sqrt{5}}{2} x \end{cases} \quad \text{ou} \quad \begin{cases} \lambda = \dfrac{-1-\sqrt{5}}{2} \\ y = \dfrac{-1-\sqrt{5}}{2} x \end{cases} \end{aligned}$$

Synthèse On pose $\begin{cases}\lambda_1 = \dfrac{-1+\sqrt{5}}{2} = \varphi \\ u_1 = (1, \varphi)\end{cases}$ et $\begin{cases}\lambda_2 = \dfrac{-1-\sqrt{5}}{2} = -\dfrac{1}{\varphi} \\ u_2 = \left(1, -\dfrac{1}{\varphi}\right)\end{cases}$.

Ainsi, $\begin{cases}f(u_1) = \lambda_1 u1 \\ f(u_2) = \lambda_2 u_2.\end{cases}$

u_1 et u_2 ne sont pas colinéaires, ils forment une famille libre donc une base.

On pose $\mathscr{C} = (u_1, u_2)$ et $\mathrm{Mat}_{\mathscr{C}}(f) = \begin{pmatrix}\varphi & 0 \\ 0 & -\dfrac{1}{\varphi}\end{pmatrix} = D.$

$$A = PDP^{-1}$$

et

$$\begin{cases}P^{-1} = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(\mathrm{id}_{\mathbb{C}^2}) = P_{\mathscr{C}\to\mathscr{B}} \\ P = \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(\mathrm{id}_{\mathbb{C}^2}) = P_{\mathscr{B}\to\mathscr{C}}\end{cases}$$

On a $P = \begin{pmatrix}1 & 1 \\ \varphi & -\dfrac{1}{\varphi}\end{pmatrix}$ donc

$$P^{-1} = -\frac{1}{\sqrt{5}}\begin{pmatrix}-\dfrac{1}{\varphi} & -1 \\ -\varphi & 1\end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix}\dfrac{1}{\varphi} & 1 \\ \varphi & -1\end{pmatrix}$$

Donc $A = PDP^{-1}$ et donc

$$\forall n \in \mathbb{N},\ A^n = PD^nP^{-1} = \frac{1}{\sqrt{5}}\begin{pmatrix}1 & 1 \\ \varphi & -\dfrac{1}{\varphi}\end{pmatrix}\begin{pmatrix}\varphi^n & 0 \\ 0 & \left(-\dfrac{1}{\varphi}\right)^n\end{pmatrix}\begin{pmatrix}\dfrac{1}{\varphi} & 1 \\ \varphi & -1\end{pmatrix}$$

$$\begin{pmatrix}\star & u_n \\ \star & \star\end{pmatrix}$$

Exemple :

$$y'' + \omega^2 y = 0 \qquad \omega \in \mathbb{R}_\star^+$$

$$\forall t, Y(t) = \begin{pmatrix}y(t) \\ y'(t)\end{pmatrix}$$

$$\begin{aligned}\forall t, Y'(t) &= \begin{pmatrix} y'(t) \\ y''(t) \end{pmatrix} \\ &= \begin{pmatrix} y'(t) \\ -\omega^2 y(t) \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -\omega^2 & 0 \end{pmatrix} \begin{pmatrix} y(t) \\ y'(t) \end{pmatrix} \\ &= AY(t)\end{aligned}$$

Soit $f : \begin{array}{ccc} \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 \\ (a,b) & \longmapsto & (b, -\omega^2 a) \end{array}$.
$A = \mathrm{Mat}_{\mathscr{B}}(f)$ où $\mathscr{B} = (e_1, e_2)$ base canonique de $\mathbb{C}^2$. On cherche $\mathscr{C} = (u_1, u_2)$ une base de $\mathbb{C}^2$ telle que $\mathrm{Mat}_{\mathscr{C}}(f) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D$.

Analyse Si $\mathscr{C}$ existe,

$$\begin{cases} f(u_1) = \lambda_1 u_1 \\ f(u_2) = \lambda_2 u_2 \end{cases}$$

Soit $u = (a, b) \in \mathbb{C}^2$ et $\lambda \in C$.

$$\begin{aligned} f(u) = \lambda u &\iff \begin{cases} b = \lambda a \\ -\omega^2 a = \lambda b \end{cases} \\ &\iff \begin{cases} b = \lambda a \\ -\omega^2 a = \lambda^2 a \end{cases} \\ &\iff \begin{cases} a = 0 \\ b = 0 \end{cases} \quad \text{ou} \quad \begin{cases} \lambda^2 = -\omega^2 \\ b = \lambda a \end{cases}\end{aligned}$$

$$\begin{array}{ccc} \mathbb{C}^2_{\mathscr{B}} & \xrightarrow{f} & \mathbb{C}^2_{\mathscr{B}} \\ {\scriptstyle \mathrm{id}_{\mathbb{C}^2}}\uparrow {\scriptstyle P} & & {\scriptstyle \mathrm{id}_{\mathbb{C}^2}}\uparrow {\scriptstyle P^{-1}} \\ \mathbb{C}^2_{\mathscr{C}} & \xrightarrow{D} & \mathbb{C}^2_{\mathscr{C}} \end{array}$$

Synthèse On pose $\begin{cases} \lambda_1 = i\omega \\ u_1 = (1, i\omega) \end{cases}$ et $\begin{cases} \lambda_2 = -i\omega \\ u_2 = (1, -i\omega) \end{cases}$. (u_1, u_2) est bien une base de $\mathbb{C}^2$ et $\mathrm{Mat}_{\mathscr{C}}(f) = \begin{pmatrix} i\omega & 0 \\ 0 & -i\omega \end{pmatrix} = D$

!

$$AP = PD \iff P^{-1}A = DP^{-1}$$

On a

$$P = P_{\mathscr{B} \to \mathscr{C}} = \begin{pmatrix} 1 & 1 \\ i\omega & -i\omega \end{pmatrix}$$

On pose

$$\forall t, X(t) = P^{-1} \times Y(t)$$

Donc

$$\begin{aligned}\forall t, X'(t) = P^{-1}Y'(t) &= P^{-1}AY(t)\\ &= DP^{-1}Y(t)\\ &= DX(t)\end{aligned}$$

On pose

$$\forall t, X(t) = \begin{pmatrix} a(t) \\ b(t) \end{pmatrix}$$

$$\begin{aligned} X'(t) = DX(t) &\iff \begin{cases} a'(t) = i\omega a(t) \\ b'(t) = -i\omega b(t) \end{cases} \\ &\iff \begin{cases} a(t) = \lambda e^{i\omega t} \\ b(t) = \mu e^{-i\omega t} \end{cases} \qquad (\lambda, \mu) \in \mathbb{C}^2. \end{aligned}$$

$$\begin{aligned}\forall t, Y(t) &= P \times X(t)\\ &= \begin{pmatrix} 1 & 1 \\ i\omega & -i\omega \end{pmatrix} \begin{pmatrix} \lambda e^{i\omega t} \\ \mu e^{-i\omega t} \end{pmatrix}\\ &= \begin{pmatrix} \lambda e^{i\omega t} + \mu e^{-i\omega t} \\ \star \end{pmatrix}\end{aligned}$$

Donc,

$$\forall t, y(t) = \lambda e^{i\omega t} + \mu e^{-i\omega t}$$

Définition : Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$.
La trace de A est

$$\operatorname{tr}(A) = \sum_{i=1}^{n} a_{i,i}$$

Proposition : 1. $\operatorname{tr} \in \mathcal{L}\big(\mathcal{M}_n(\mathbb{K}), \mathbb{K}\big) = \mathcal{M}_n(\mathbb{K})^\star$
2. $\forall A, B \in \mathcal{M}_n(\mathbb{K}), \operatorname{tr}(AB) = \operatorname{tr}(BA)$

Preuve : 1. Soient $(A, B) \in \mathcal{M}_n(\mathbb{K})$ et $(\alpha, \beta) \in \mathbb{K}^2$. On pose $A = (a_{i,j})$

et $B = (b_{i,j})$.

$$\begin{aligned}\operatorname{tr}(\alpha A + \beta B) &= \sum_{i=1}^{n} (\alpha a_{i,i} \beta b_{i,i}) \\ &= \alpha \sum_{i=1}^{n} a_{i,i} + \beta \sum_{i=1}^{n} b_{i,i} \\ &= \alpha \operatorname{tr}(A) + \beta \operatorname{tr}(B)\end{aligned}$$

2. Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$. On pose $A = (a_{i,j})$, $B = (b_{i,j})$, $AB = (c_{i,j})$ et $BA = (d_{i,j})$.

$$\begin{aligned}\operatorname{tr}(AB) = \sum_{i=1}^{n} c_{i,i} &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} b_{j,i} \\ &= \sum_{j=1}^{n} \sum_{i=1}^{n} b_{j,i} a_{i,j} \\ &= \sum_{j=1}^{n} d_{j,j} \\ &= \operatorname{tr}(BA)\end{aligned}$$

□

Proposition : Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$.

$$A \text{ et } B \text{ semblables} \implies \operatorname{tr}(A) = \operatorname{tr}(B)$$

Preuve :
On suppose A et B semblables. Soit $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $A = P^{-1}BP$. Donc

$$\operatorname{tr}(A) = \operatorname{tr}\left(P^{-1}(BP)\right) = \operatorname{tr}\left((BP)P^{-1}\right) = \operatorname{tr}(B)$$

□

Remarque (Attention) :
$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\operatorname{tr}(A) = 2 = \operatorname{tr}(B)$

Or, A et B ne sont pas semblables, sinon

$$\begin{aligned} A = P^{-1}BP \text{ avec } P \in \mathrm{GL}_2(\mathbb{K}) \qquad & = P^{-1}I_2P \\ = P^{-1}P & \\ = I_2 \neq A & \end{aligned}$$

nition

Corollaire : Soit $f \in \mathscr{L}(E)$ et $\mathscr{B}$ une base de E. $A = \mathrm{Mat}_{\mathscr{B}}(f)$. La trace de f est $\mathrm{tr}(A)$.
Ce nombre ne dépend pas de la base $\mathscr{B}$ choisie. On note ce nombre $\mathrm{tr}(f)$.
□

Proposition : Soit p un projecteur de E de dimension finie. Alors

$$\mathrm{tr}(p) = \mathrm{rg}(p)$$

Preuve :
On sait que

$$E = \mathrm{Ker}(p) \oplus \mathrm{Im}(p)$$

Soit $\mathscr{B}_1 = (e_1, \dots, e_k)$ une base $\mathrm{Ker}(p)$ et $\mathscr{B}_2 = (e_{k+1}, \dots, e_n)$ une base de $\mathrm{Im}(p)$.
On pose $\mathscr{B} = (e_1, \dots, e_k, e_{k+1}, \dots, e_n)$. $\mathscr{B}$ est une base de E et

$$A = \mathrm{Mat}_{\mathscr{B}}(p)$$

$$\mathrm{tr}(p) = \mathrm{tr}(A) = n - k = \#\mathscr{B}_2 = \dim(\mathrm{Im}\, p) = \mathrm{rg}(p)$$

□

Exemple :
$F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y = 0\}$
$G = \mathrm{Vect}\big((1, 1, 1)\big)$
f la projection sur F parallèlement à G.
$\mathscr{B} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{R}^3$.

$$\mathrm{Mat}_{\mathscr{B}}(f) = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} = A$$

$$\mathrm{tr}(A) = 2 = \dim(F)$$

5 Conséquences

Proposition : La multiplication matricielle est associative.

Preuve :

$$\begin{cases} A \in \mathscr{M}_{n,p}(\mathbb{K}) \\ B \in \mathscr{M}_{p,q}(\mathbb{K}) \\ C \in \mathscr{M}_{q,r}(\mathbb{K}) \end{cases}$$

Soient $f \in \mathscr{L}(\mathbb{K}^p, \mathbb{K}^n)$, $g \in \mathscr{L}(\mathbb{K}^q, \mathbb{K}^p)$ et $h \in \mathscr{L}(\mathbb{K}^r, \mathbb{K}^q)$ telles que

$$\begin{cases} A = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f) \\ B = \mathrm{Mat}_{\mathscr{E},\mathscr{B}}(g) \\ C = \mathrm{Mat}_{\mathscr{D},\mathscr{E}}(h) \end{cases}$$

où $\mathscr{B}$ est la base canonique de $\mathbb{K}^p$, $\mathscr{C}$ est la base canonique de $\mathbb{K}^n$, $\mathscr{D}$ est la base canonique de $\mathbb{K}^r$, $\mathscr{E}$ est la base canonique de $\mathbb{K}^q$.

$$\begin{aligned} A(BC) &= \mathrm{Mat}_{\mathscr{D}\mathscr{C}}\left(f \circ (g \circ h)\right) \\ &= \mathrm{Mat}_{\mathscr{D},\mathscr{C}}\left((f \circ g) \circ h\right) \\ &= (AB)C \end{aligned}$$

□

Proposition : Soit $(A, B) \in \mathscr{M}_n(\mathbb{K})^2$. On suppose que $AB = I_n$. Alors $(A, B) \in \mathrm{GL}_n(\mathbb{K})^2$ et $A^{-1} = B$.

Preuve :
Soit $\mathscr{B}$ la base canonique de $\mathbb{K}^n$, $f \in \mathscr{L}(\mathbb{K}^n)$ telle que $\mathrm{Mat}_{\mathscr{B}}(f) = A$, $g \in \mathscr{L}(\mathbb{K}^n)$ telle que $\mathrm{Mat}_{\mathscr{B}}(g) = B$.

$AB = I_n$ donc $\mathrm{Mat}_{\mathscr{B}}(f \circ g) = \mathrm{Mat}_{\mathscr{B}}(\mathrm{id}_{\mathbb{K}^n})$ donc $f \circ g = \mathrm{id}_{\mathbb{K}^n}$
donc $f \circ g$ est injective
donc g est injective
donc g est un isomorphisme

Or, $f \circ g = \mathrm{id}$ donc $f = f \circ g \circ g^{-1} = g^{-1}$

$$\begin{aligned} BA &= \mathrm{Mat}_{\mathscr{B}}(g) = \mathrm{Mat}_{\mathscr{B}}(f) \\ &= \mathrm{Mat}_{\mathscr{B}}(g \circ f) \\ &= \mathrm{Mat}_{\mathscr{B}}(g \circ g^{-1}) \\ &= \mathrm{Mat}_{\mathscr{B}}(\mathrm{id}_{\mathbb{K}^n}) \\ &= I_n \end{aligned}$$

Donc $A = B^{-1}$. □

Remarque :
Au passage, on a montré que

$$f \in \mathrm{GL}(E) \iff \mathrm{Mat}_{\mathscr{B}}(f) \in \mathrm{GL}_n(\mathbb{K})$$

et, dans ce cas,

$$\mathrm{Mat}_{\mathscr{B}}(f^{-1}) = \mathrm{Mat}_{\mathscr{B}}(f)^{-1}$$

Proposition : Soit $A \in \mathscr{M}_{p,n}(\mathbb{K})$.

Le nombre maximal de lignes linéairement indépendantes de A est égal au rang de A.

Preuve :
On appelle rang par lignes le nombre exact de lignes linéairement indépendantes.

Ce rang par ligne est invariant quand on effectue une opération élémentaire sur les lignes.

En appliquant la méthode du pivot de Gauß, on obtient une matrice de la forme

$$\left(\begin{array}{ccccccccc} 0 & \dots & 0 & \boxed{1} & \star & \dots & \dots & \star \\ 0 & \dots & \dots & 0 & \boxed{1} & \star & \dots & \star \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \end{array}\right)$$

qui a le même rang par lignes que A.

On obsèrve que ce rang r est égal au nombre de pivots.

Soit S le système homogène

$$AX = 0$$

où $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. D'après l'algorithme du pivot, la résolution de ce système fournit r inconnues principales et $n - r$ paramètres.

Sans perte de généralité, on peut supposer que $x_1, \dots, x_{n-r}$ sont les paramètres et $x_{n-r+1}, \dots, x_n$ les inconnues principales.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$ et $\mathcal{C} = (f_1, \dots, f_p)$ la base canonique de $\mathbb{K}^p$ et $f \in \mathscr{L}(\mathbb{K}^n, \mathbb{K}^p)$ telle que

$$A = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f).$$

Soit $x = (x_1, \dots, x_n) \in \mathbb{K}^n$ et $X = \mathrm{Mat}_{\mathcal{B}}(x)$.

$$\begin{aligned} AX = 0 &\iff \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)\,\mathrm{Mat}_{\mathcal{B}}(f) = \mathrm{Mat}_{\mathcal{C}}(0) \\ &\iff \mathrm{Mat}_{\mathcal{C}}\left(f(x)\right) = \mathrm{Mat}_{\mathcal{C}}(0) \\ &\iff f(x) = 0 \\ &\iff x \in \mathrm{Ker}\, f \end{aligned}$$

Ainsi, l'ensemble E des solutions de (S) est un $\mathbb{K}$-espace vectoriel isomorphe à $\mathrm{Ker}(f)$.

De plus,

$$\begin{aligned} g : E &\longrightarrow \mathbb{K}^{n-r} \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} &\longmapsto (x_1, \dots, x_{n-r}) \end{aligned}$$

est un isomorphisme. Donc, $\dim(\mathrm{Ker}\, f) = \dim(E) = n - r$.

D'après le théorème du rang,

$$\mathrm{rg}(A) = \mathrm{rg}(f) = \dim(\mathbb{K}^n) - \dim(\mathrm{Ker}\, f) = n - (n - r) = r.$$

□

Définition : Soit $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}} \in \mathscr{M}_{p,n}(\mathbb{K})$.

La transposée de A, notée ${}^tA = (b_{j,i})_{\substack{1 \leqslant j \leqslant n \\ 1 \leqslant i \leqslant p}} \in \mathscr{M}_{n,p}(\mathbb{K})$ est définie par

$$\forall i \in [\![1, p]\!], \forall j \in [\![1, n]\!], b_{j,i} = a_{i,j}.$$

Les lignes de ${}^tA$ sont les colonnes de A. Les colonnes de ${}^tA$ sont les lignes de A.

Exemple :
$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 3 & -1 \end{pmatrix}$ donc ${}^tA = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \end{pmatrix}$.

Corollaire :

$$\forall A \in \mathcal{M}_{n,p}(\mathbb{K}), \operatorname{rg}(A) = \operatorname{rg}({}^tA)$$

□

Proposition : $\begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ A & \longmapsto & {}^tA \end{array}$ est la symétrie par rapport à $S_n(\mathbb{K})$ parallèlement à $A_n(\mathbb{K})$ où

$$S_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^tA = A\} = \begin{pmatrix} & & \\ & (u) & \\ (u) & & \end{pmatrix}$$

et

$$A_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^tA = -A\} = \begin{pmatrix} 0 & & \\ & (u) & \\ (-u) & & 0 \end{pmatrix}$$

et donc

$$S_n(\mathbb{K}) \oplus A_n(\mathbb{K}) = \mathcal{M}_n(\mathbb{K}).$$

Preuve :
Soient $A = (a_{i,j})$, $B = (b_{i,j})$ et $(\alpha, \beta) \in \mathbb{K}^2$.

$$\begin{aligned} {}^t(\alpha A + \beta B) &= (\alpha a_{j,i} + \beta b_{j,i})_{1 \leqslant i,j \leqslant n} = \alpha(a_{j,i}) + \beta(b_{j,i}) \\ &= \alpha {}^tA + \beta {}^tB \end{aligned}$$

Clairement,

$$\forall A \in \mathcal{M}_n(\mathbb{K}), {}^t\left({}^tA\right) = A$$

donc $f : A \mapsto {}^tA$ est la symétrie par rapport à $\operatorname{Ker}(f - \mathrm{id}_{\mathcal{M}_n(\mathbb{K})})$ parallèlement à $\operatorname{Ker}(f + \mathrm{id}_{\mathcal{M}_n(\mathbb{K})})$.

Or,

$$\begin{aligned} \operatorname{Ker}(f - \mathrm{id}_{\mathcal{M}_n(\mathbb{K})}) &= \{A \in \mathcal{M}_n(\mathbb{K}) \mid f(A) - A = 0\} \\ &= \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^tA = A\} \\ &= S_n(\mathbb{K}) \end{aligned}$$

et

$$\begin{aligned}\mathrm{Ker}(f+\mathrm{id}_{\mathscr{M}_n(\mathbb{K})}) &= \{A\in\mathscr{M}_n(\mathbb{K}) \mid f(A)+A=0\}\\ &= \{A\in\mathscr{M}_n(\mathbb{K}) \mid {}^tA=A\}\\ &= A_n(\mathbb{K})\end{aligned}$$

□

Proposition : Soit $A\in\mathscr{M}_{n,p}(\mathbb{K})$ et $B\in\mathscr{M}_{p,q}(\mathbb{K})$.

$$^t(AB) = {}^tB{}^tA$$

Preuve :
On pose

$$\begin{cases} A=(a_{i,j})_{\substack{1\leqslant i\leqslant n,\\ 1\leqslant j\leqslant p}}\\ B=(b_{j,k})_{\substack{1\leqslant j\leqslant p,\\ 1\leqslant k\leqslant q}}\\ {}^tB{}^tA=(c_{k,i})_{\substack{1\leqslant k\leqslant q.\\ 1\leqslant i\leqslant n}}\end{cases}$$

$$\begin{aligned}\forall k\in[\![1,q]\!],\forall i\in[\![1,n]\!], c_{k,i} &= \sum_{j=1}^{p}({}^tB)_{k,j}({}^tA)_{j,i}\\ &= \sum_{j=1}^{p} b_{j,k}a_{i,j}\\ &= \sum_{j=1}^{p} a_{i,j}b_{j,k}\\ &= (AB)_{i,k}\\ &= \left({}^t(AB)_{k,i}\right)\end{aligned}$$

Donc, $^t(AB) = {}^tB{}^tA$. □

Corollaire : Si $A\in\mathrm{GL}_n(\mathbb{K})$ alors ${}^tA\in\mathrm{GL}_n(\mathbb{K})$ et

$$\left({}^tA\right)^{-1} = {}^t\left(A^{-1}\right)$$

Preuve :
On suppose $A \in \mathrm{GL}_n(\mathbb{K})$.

$AA^{-1} = I_n$ donc ${}^t(AA^{-1}) = {}^tI_n$

donc ${}^t(A^{-1}){}^tA = I_n$

donc

$$ {}^tA \in \mathrm{GL}_n(\mathbb{K}){}^t(A^{-1}) = ({}^tA)^{-1}$$

□

6 Matrices par blocs

Exemple :
Soit p un projecteur de E :

$$E = \mathrm{Ker}\, p \oplus \mathrm{Im}\ p$$

Soit $\mathcal{B} = (e_1, \dots, e_k, e_{k+1}, \dots, e_n)$ une base de E avec $\begin{cases} \mathrm{Im}(p) = \mathrm{Vect}(e_1, \dots, e_k) \\ \mathrm{Ker}(p) = \mathrm{Vect}(e_{k+1}, \dots, e_n) \end{cases}$

Alors,

$$\mathrm{Mat}_{\mathcal{B}}(p) = \left(\begin{array}{ccc|ccc} 1 & & & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ & & 1 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right) = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & 0 \end{array}\right)$$

De même, si s est une symétrie de E,

$$E = \mathrm{Ker}(s - \mathrm{id}_E) \oplus \mathrm{Ker}(s + \mathrm{id}_E).$$

Soit $\mathcal{C} = (e'_1, \dots, e'_\ell, e'_{\ell+1}, \dots, e'_n)$ avec $\begin{cases} \mathrm{Vect}(e'_1, \dots, e'_\ell) = \mathrm{Ker}(s - \mathrm{id}_E), \\ \mathrm{Vect}(e'_{\ell+1}, \dots, e'_n) = \mathrm{Ker}(s + \mathrm{id}_E). \end{cases}$

Alors

$$\mathrm{Mat}_{\mathcal{C}}(s) = \left(\begin{array}{c|c} I_\ell & 0 \\ \hline 0 & -I_{n-\ell} \end{array}\right)$$

Proposition : Soient F et G supplémentaires dans E :

$$E = F \oplus G.$$

Soit $f \in \mathscr{L}(F)$ et $g \in \mathscr{L}(G)$. Alors

$$\exists! h \in \mathscr{L}(E) h_{|F} = f,\ h_{|G} = g \ \text{ et } \ h = f \circ p + g \circ q$$

où $\begin{cases} p \text{ est la projection sur } F \text{ parallèlement à } G \\ q \text{ est la projection sur } G \text{ parallèlement à } F \end{cases}$.

On a aussi $q = \mathrm{id}_E - p$.

Preuve

Analyse Soit $h \in \mathscr{L}(E)$ tel que $\begin{cases} h_{|F} = f \\ h_{|G} = g \end{cases}$.

Soit $x \in E$. Alors

$$x = \underbrace{p(x)}_{\in F} + \underbrace{q(x)}_{\in G}$$

Donc,

$$\begin{aligned} h(x) &= h\big(p(x)\big) + h\big(q(x)\big) \\ &= f\big(p(x)\big) + g\big(q(x)\big) \\ &= (f \circ p + g \circ q)(x) \end{aligned}$$

Si h existe, alors

$$h = f \circ p + g \circ q$$

Synthèse On pose $h = f \circ p + g \circ q$.

p, q, f et g sont linéaires donc h aussi.

Soit $x \in E$.

$$\begin{aligned} h(x) &= f\big(p(x)\big) + g\big(q(x)\big) \\ &= f(x) + g(0_E) \\ &= f(x) \end{aligned}$$

donc $h_{|F} = f$ et de même $h_{|G} = g$.

□

Proposition : On reprend les notations et hypothèses précédentes. Soit $(e_1, \dots, e_p)$ une base de F, et $(f_1, \dots, f_q)$ une base de G. Alors, $\mathscr{B} = (e_1, \dots, e_p, f_1, \dots, f_q)$ est une base de E et

$$\mathrm{Mat}_{\mathscr{B}}(h) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$$

où $\begin{cases} A = \mathrm{Mat}_{(e_1,\dots e_p)}(f) \\ B = \mathrm{Mat}_{(f_1,\dots,f_q)}(g) \end{cases}$

□

Proposition : Soient $(A, A') \in \mathcal{M}_n(\mathbb{K})^2$ et $(B, B') \in \mathcal{M}_p(\mathbb{K})^2$.

1. $$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array}\right) = \left(\begin{array}{c|c} AA' & 0 \\ \hline 0 & BB' \end{array}\right)$$

2. $$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) \in \mathrm{GL}_{n+p}(\mathbb{K}) \iff \begin{cases} A \in \mathrm{GL}_n(\mathbb{K}) \\ B \in \mathrm{GL}_p(\mathbb{K}) \end{cases}$$

   et dans ce cas,

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)^{-1} = \left(\begin{array}{c|c} A^{-1} & 0 \\ \hline 0 & B^{-1} \end{array}\right)$$

3. $$\mathrm{tr}\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) = \mathrm{tr}\, A + \mathrm{tr}\, B$$

Preuve : 1. Soit $\Big\{ f \in \mathcal{L}(F)$ tel que $\mathrm{Mat}_{\mathcal{B}}(f) = A, f' \in \mathcal{L}(F)$ tel que $\mathrm{Mat}_{\mathcal{B}}(f') = A', g \in \mathcal{L}(G)$ tel que $\mathrm{Mat}_{\mathcal{C}}$

où $\begin{cases} F \oplus G = \mathbb{K}^{n+p}, \\ \dim(F) = n, \dim(G) = p, \\ \mathcal{B} \text{ base de } F, \\ \mathcal{C} \text{ base de } G. \end{cases}$ Soit $\begin{cases} h \in \mathcal{L}(\mathbb{K}^{n+p}) \text{ tel que } \begin{cases} h_{|F} = f \\ h_{|G} = g \end{cases} \\ h' \in \mathcal{L}(\mathbb{K}^{n+p}) \text{ tel que } \begin{cases} h'_{|F} = f' \\ h'_{|G} = g' \end{cases} \end{cases}$

Soit $\mathcal{D} = \mathcal{B} \cup \mathcal{C}$ une base de $\mathbb{K}^{n+p}$.

$$\begin{aligned} \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array}\right) &= \mathrm{Mat}_{\mathcal{D}}(h)\,\mathrm{Mat}_{\mathcal{D}}(h') \\ &= \mathrm{Mat}_{\mathcal{D}}(h \circ h') \end{aligned}$$

Or, $(h \circ h')_{|F} = f \circ f'$ et $(h \circ h')_{|G} = g \circ g'$.

Donc,

$$\begin{aligned} \mathrm{Mat}_{\mathcal{D}}(h \circ h') &= \left(\begin{array}{c|c} \mathrm{Mat}_{\mathcal{B}}(f \circ f') & 0 \\ \hline 0 & \mathrm{Mat}_{\mathcal{C}}(g \circ g') \end{array}\right) \\ &= \left(\begin{array}{c|c} AA' & 0 \\ \hline 0 & BB' \end{array}\right). \end{aligned}$$

□

Proposition : Soient $A, A' \in \mathcal{M}_n(\mathbb{K})$, $B, B' \in \mathcal{M}_{n,p}(\mathbb{K})$, $C, C' \in \mathcal{M}_{p,n}(\mathbb{K})$ et $D, D' \in \mathcal{M}_p(\mathbb{K})$.

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)\left(\begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array}\right) = \left(\begin{array}{c|c} AA'+BC' & AB'+BD' \\ \hline CA'+DC' & CB'+DD' \end{array}\right)$$

Cette formule se généralise à un nombre quelconque de blocs :

$$\left(\begin{array}{c|c|c|c} A_{11} & A_{12} & \cdots & A_{1,n} \\ \hline A_{21} & A_{22} & \cdots & A_{2,n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A_{p,1} & A_{p,2} & \cdots & A_{p,n} \end{array}\right)\left(\begin{array}{c|c|c|c} A'_{11} & A'_{12} & \cdots & A'_{1,n} \\ \hline A'_{21} & A'_{22} & \cdots & A'_{2,n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A'_{p,1} & A'_{p,2} & \cdots & A'_{p,n} \end{array}\right)$$

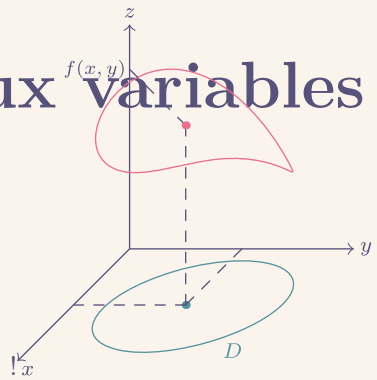
Cette matrice se calcyle comme on s'y attend si les dimensions des blocs autorisent les produits.

$$\begin{array}{ccc} \mathbb{C}^2_{\mathscr{B}} & \overset{f}{\longrightarrow} & \mathbb{C}^2_{\mathscr{B}} \\ \| & & \| \\ A & & A \\ \| & & \| \\ \mathbb{C}^2_{\mathscr{C}} & \underset{!}{\overset{f}{\longrightarrow}} & \mathbb{C}^2_{\mathscr{C}} \\ D & & D \end{array} \qquad \begin{array}{ccc} \mathbb{C}^2 & \overset{\mathrm{id}_{\mathbb{C}^2}}{\longrightarrow} & \mathbb{C}^2 \\ \downarrow P & \nearrow & \downarrow P \\ \mathbb{C}^2 & \underset{!}{\overset{\mathrm{id}_{\mathbb{C}^2}}{\longrightarrow}} & \mathbb{C}^2 \end{array}$$

Proposition : Le rang d'une matrice A, c'est la taille de la plus grande matrice carrée inversible que l'on peut extraire de A. □

Chapitre 22

Fonctions de deux variables



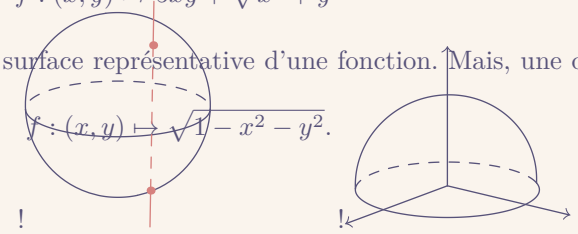
1 Quelques généralités

On s'interesse dans ce chapitre à des fonctions définies sur une partie D de $\mathbb{R}^2$ à valeurs dans $\mathbb{R}$.

Par exemple,

$$f : (x, y) \mapsto 5xy + \sqrt{x^2 + y^2}$$

Une sphère n'est pas la surface représentative d'une fonction. Mais, une demi-sphère oui :



$$f : (x, y) \mapsto \sqrt{1 - x^2 - y^2}.$$

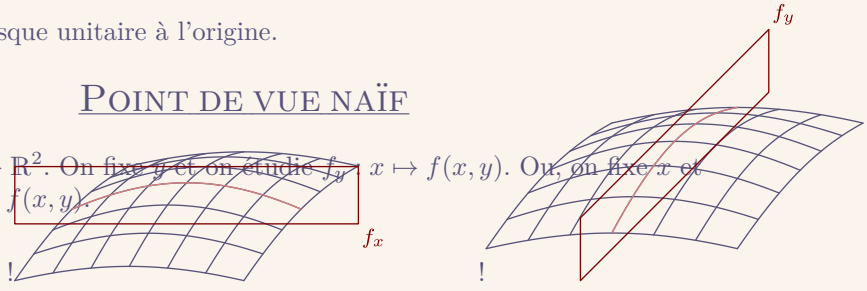
La surface de la demisphère est

$$S = \big\{\big(x, y, f(x, y)\big) \mid (x, y) \in D_O(1)\big\}.$$

où $D_O(1)$ est le disque unitaire à l'origine.

Point de vue naïf

Soit $f : D \subset \mathbb{R}^2 \to \mathbb{R}^2$. On fixe y et on étudie $f_y : x \mapsto f(x, y)$. Ou, on fixe x et on étudie $f_x : y \mapsto f(x, y)$.



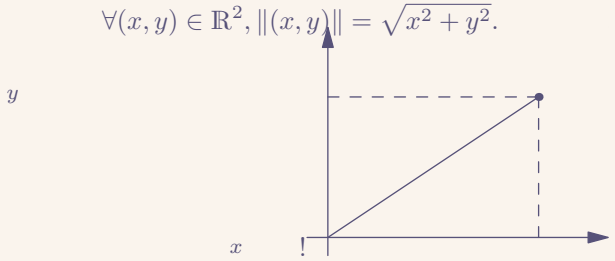
Le bon point de vue

On reprend les notions d'une fonction d'une seule variable (limite, continuité, développement limité, ...) que l'on adapte aux fonctions à deux variables.

2 Topologie de $\mathbb{R}^2$

Définition : La norme (euclidienne) de $\mathbb{R}^2$ est l'application définie par

$$\forall (x,y) \in \mathbb{R}^2, \|(x,y)\| = \sqrt{x^2+y^2}.$$



Proposition : La norme euclidienne vérifie :

1. (séparation)
$$\forall (x,y) \in \mathbb{R}^2, \|(x,y)\| = 0 \iff x = y = 0,$$
2. (homogénéité positive)
$$\forall \lambda \in \mathbb{R}, \forall (x,y) \in \mathbb{R}^2, \|\lambda(x,y)\| = |\lambda| \, \|(x,y)\|$$
3. (inégalité triangulaire)
$$\forall (x,y),(a,b) \in \mathbb{R}^2, \|(x,y)+(a,b)\| \leqslant \|(x,y)\| + \|(a,b)\|.$$

Preuve :
Déjà vue en replaçant (x,y) par $x+iy \in \mathbb{C}$ et $\|(x,y)\|$ par |x+iy| □

Définition : Soit $(a,b) \in \mathbb{R}^2$ et $r \in \mathbb{R}_+$.

La boule ouverte (ou disque ouvert) de centre (a,b) et de rayon r est

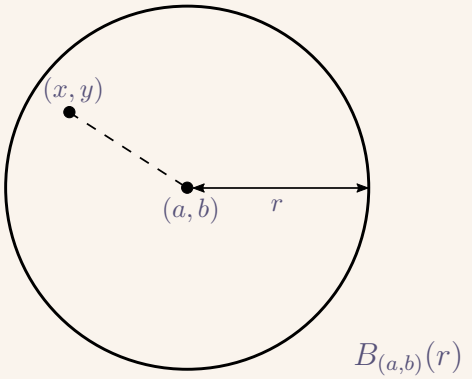
$$B_{(a,b)}(r) = \big\{(x,y) \in \mathbb{R}^2 \mid \|(x,y)-(a,b)\| < r\big\}.$$

La boule fermée (ou disque fermé) de centre (a,b) et de rayon r est

$$\overline{B_{(a,b)}}(r) = \big\{(x,y) \in \mathbb{R}^2 \mid \|(x,y)-(a,b)\| \leqslant r\big\}.$$

La sphère (ou boule) de centre (a,b) et de rayon r est

$$S_{(a,b)}(r) = \partial\overline{B_{(a,b)}}(r) = \big\{(x,y) \in \mathbb{R}^2 \mid \|(x,y)-(a,b)\| = r\big\}.$$

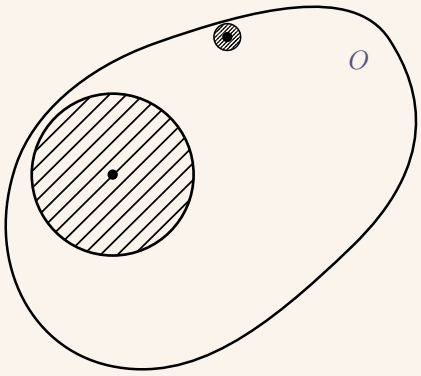


Remarque :
On parle de boule en dimension quelconque.

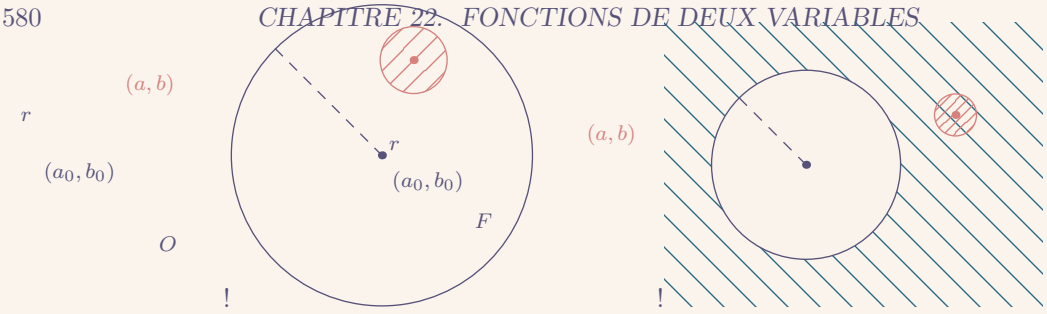
Définition : Une partie ouverte O de $\mathbb{R}^2$ (ou un ouvert) si

$$\forall (x, y) \in O, \exists r > 0, B_{(a,b)}(r) \subset O.$$

Une partie F est fermée su $\mathbb{R}^2 \setminus F$ est ouverte.



Proposition : Une boule ouverte est ouverte. Une boule fermée est fermée.



Preuve :
est un ouvert.

Soit B la boule ouverte de centre $(a_0, b_0) \in \mathbb{R}^2$ et de rayon $r > 0$.

On pose $\rho = \dfrac{1}{2}\big(r - \|(a,b) - (a_0,b_0)\|\big)$. Montrons que

$$B_{(a,b)}(\rho) \subset B_{(a,b)}(r).$$

Soit $(x, y) \in B_{(a,b)}(\rho)$.

$$\begin{aligned}
\|(x,y) - (a_0,b_0)\| &= \|(x,y) - (a,b) + (a,b) - (a_0,b_0)\| \\
&\leqslant \|(x,y) - (a,b)\| + \|(a,b) - (a_0,b_0)\| \\
&< \rho + \|(a,b) - (a_0,b_0)\| = \frac{1}{2}r + \frac{1}{2}\|(a,b) - (a_0,b_0)\| \\
&< r
\end{aligned}$$

Soit F la boule fermée de centre (a_0, b_0) et de rayon $r \geqslant 0$.

Soit $(a, b) \notin F$. On pose

$$\rho = \frac{1}{2}\big(\|(a,b) - (a_0,b_0)\| - r\big) > 0.$$

Montrons que $B_{(a,b)}(\rho) \subset \mathbb{R}^2 \setminus F$.

Soit $(x, y) \in B_{(a,b)}(\rho)$.

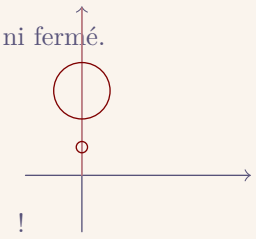
$$\begin{aligned}
\|(x,y) - (a_0,b_0)\| &= \|(x,y) - (a,b) + (a,b) - (a_0,b_0)\| \\
&\geqslant \Big| \underbrace{\|(x,y) - (a,b)\|}_{\leqslant \rho} - \underbrace{\|(a,b) - (a_0,b_0)\|}_{> r} \Big| \\
&\geqslant \|(a,b) - (a_0,b_0)\| - \|(x,y) - (a,b)\| \\
&> \|(a,b) - (a_0,b_0)\| - \rho \\
&> \frac{1}{2}\|(a,b) - (a_0,b_0)\| + \frac{1}{2}r \\
&> r
\end{aligned}$$

donc $(x, y) \notin F$. □

EXEMPLE : 1. est ouvert.
$\mathbb{R}^2$ est ouvert.

2. est fermé.
$\mathbb{R}^2$ est fermé.

3. $\{(x, 0) \mid x > 0\}$ n'est ni ouverte ni fermé.



Définition : Soit $(a, b) \in \mathbb{R}^2$ et $V \in \mathcal{P}(\mathbb{R}^2)$.

On dit que V est un voisinage de (a, b) s'il existe $r > 0$ tel que

$$B_{(a,b)}(r) \subset V.$$

Proposition : Un ouvert non vide est un voisinage en chacun de ces points. □

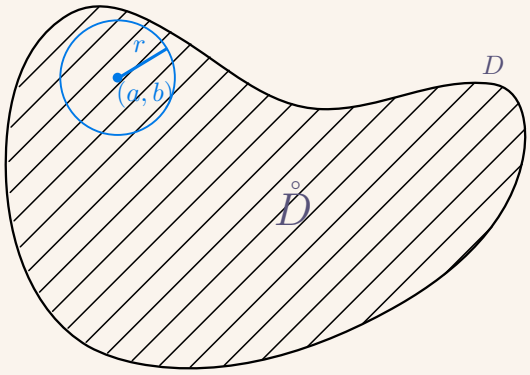
Définition : Soit $D \subset \mathbb{R}^2$. Un point intérieur de D est un couple $(a, b) \in D$ tel que

$$\exists r > 0, B_{(a,b)}(r) \subset D.$$

en d'autres termes, si D est un voisinage de (a, b).

On note $\mathring{D}$ l'ensemble des points intérieurs à D. C'est l'intérieur de D.

Proposition : $\mathring{D}$ est le plus grand ouvert O de $\mathbb{R}^2$ tel que $O \subset D$.



Preuve :
Soit $(a,b) \in \mathring{D}$.

Par définition, il existe $r > 0$ tel que

$$B_{(a,b)}(r) \subset D.$$

Montrons que $B_{(a,b)}(r) \subset \mathring{D}$.

Soit $(x,y) \in B_{(a,b)}(r)$. Comme $B_{(a,b)}(r)$ est un ouvert de $\mathbb{R}^2$, il existe $\rho > 0$ tel que

$$B_{(x,y)}(\rho) \subset B_{(a,b)}(r)$$

donc $(x,y) \in \mathring{D}$.

Donc $\mathring{D}$ est ouvert, $\mathring{D} \subset D$.

Soit O un ouvert de $\mathbb{R}^2$ tel que $O \subset D$. Montrons que $O \subset \mathring{D}$.

Soit $(x,y) \in O$. Soit $r > 0$ tel que

$$B_{(x,y)}(r) \subset O \subset D$$

donc $(x,y) \in \mathring{D}$. □

Définition : Soit $f : D \subset \mathbb{R}^2 \to \mathbb{R}$, $\ell \in \mathbb{R}$, $(a,b) \in \mathring{D}$.

On dit que $f(x,y)$ tend vers ℓ quand (x,y) tend vers (a,b) ou que ℓ est une limite de f en (a,b) si

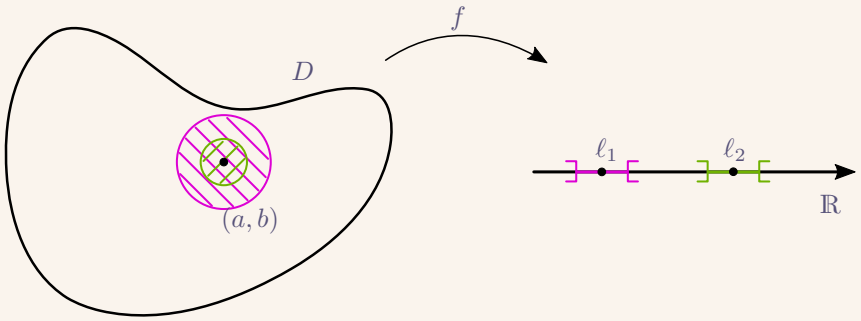
$$\forall \varepsilon > 0, \exists r > 0, \forall (x,y) \in D, \|(x,y) - (a,b)\| < r \implies |f(x,y) - \ell| \leqslant \varepsilon.$$

en d'autres termes si

$$\forall V \in \mathscr{V}_\ell, \exists W \in \mathscr{V}_{(a,b)}, \forall (x,y) \in W \cap D, f(x,y) \in V.$$

Proposition (unicité de la limite) **:** Soit $f : D \to \mathbb{R}$, $(a,b) \in \mathring{D}$, $\ell_1, \ell_2 \in \mathbb{R}$ telles que ℓ_1 et ℓ_2 sont des limites de f en (a,b).

Alors $\ell_1 = \ell_2$.



Preuve :
On suppose $\ell_1 < \ell_2$. On pose $\varepsilon = \dfrac{\ell_2 - \ell_1}{2} > 0$.

Soit $r_1 > 0$ tel que

$$f\big(B_{(a,b)}(r_1)\big) \subset]\ell_1 - \varepsilon, \ell_1 + \varepsilon[.$$

Soit $r_2 > 0$ tel que

$$f\big(B_{(a,b)}(r_2)\big) \subset]\ell_2 - \varepsilon, \ell_2 + \varepsilon[.$$

On pose $r = \min(r_1, r_2)$ donc

$$B_{(a,b)}(r_1) \cap B_{(a,b)}(r_2) = B_{(a,b)}(r) \neq .$$

Soit $(x,y) \in B_{(a,b)}(r)$. Alors,

$$f(x,y) \in]\ell_1 - \varepsilon, \ell_1 + \varepsilon[\cap]\ell_2 - \varepsilon, \ell_2 + \varepsilon[= .$$

↯ □

Définition : Soit $f : D \to \mathbb{R}$, $(a,b) \in \mathring{D}$.

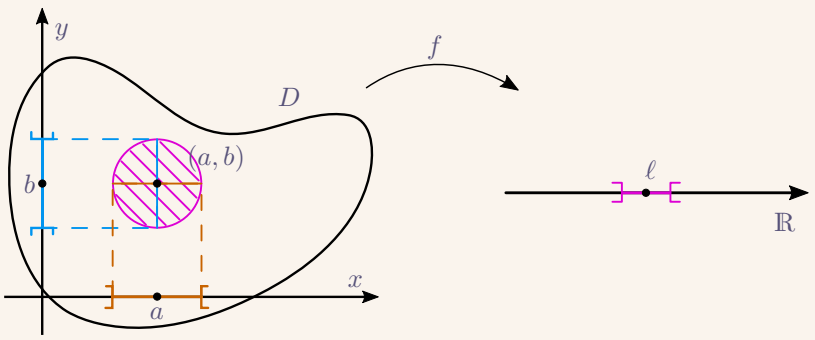
On dit que f est continue en (a,b) si

$$f(x,y) \xrightarrow[(x,y)\to(a,b)]{} f(a,b).$$

Proposition : Si $f(x,y) \xrightarrow[(x,y)\to(a,b)]{} \ell$

alors $\begin{cases} f(x,b) \xrightarrow[x\to a]{} \ell \\ f(a,y) \xrightarrow[y\to b]{} \ell. \end{cases}$

Preuve :



□

Contre-exemple : exercice 3.

EXEMPLE : 1. $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x \end{array}$ limite en $(0,0)$?

Soit $\varepsilon > 0$. On pose $r = \varepsilon$.

$$\forall (x,y) \in B_{(0,0)}(r), |f(x,y)| = |x| \leqslant \|(x,y)\| < r = \varepsilon$$

Donc $f(x,y) \xrightarrow[(x,y)\to(a,b)]{} 0$.

2. limite $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x^3 \end{array}$ en $(0,0)$?

Soit $\varepsilon > 0$. On pose $r = \sqrt[3]{r} > 0$.

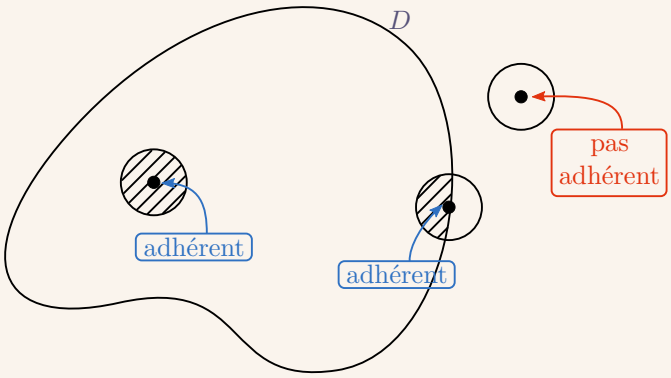
$$\forall (x,y) \in B_{(0,0)}(r), |f(x,y)| = \left|x^3\right| \leqslant \|(x,y)\|^3 < r^3 = \varepsilon.$$

3. limite de $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x^3y^2 \end{array}$ en $(0,0)$?

Soit $\varepsilon > 0$. On pose $r = \sqrt[5]{\varepsilon} > 0$.

$$\forall (x,y) \in B_{(0,0)}(r), |f(x,y)| = \left|x^3y^2\right| \leqslant \|(x,y)\|^3 \|(x,y)\|^2 < r^5 = \varepsilon.$$

Définition : Soient $D \subset \mathbb{R}^2$ et $(x,y) \in \mathbb{R}^2$.



On dit que (x,y) est adhérent à D si

$$\forall r > 0, B_{(x,y)}(r) \cap D \neq .$$

L'ensemble des points adhérents à D est noté $\overline{D}$. On dit que $\overline{D}$ est l'adhérence de D.

Définition : Soit $f : D \subset \mathbb{R}^2 \to \mathbb{R}$ et $(a,b) \in \overline{D}$, $\ell \in \mathbb{R}$. On dit que f tend vers ℓ quand (x,y) tend vers (a,b) si

$$\forall \varepsilon > 0, \exists r > 0, \forall (x,y) \in B_{(a,b)}(r) \cap D, |f(x,y) - \ell| \leqslant \varepsilon.$$

Proposition :
1. Dans ce contexte, il y a unicité de la limite
2. La limite d'une somme, d'un produit, d'un quotien, d'une composée se comporte comme dans le cas d'une seule variable.
3. Soit $f : D \to \mathbb{R}$ continue. Soient $g : I \to \mathbb{R}$ et $h : I \to \mathbb{R}$ continues

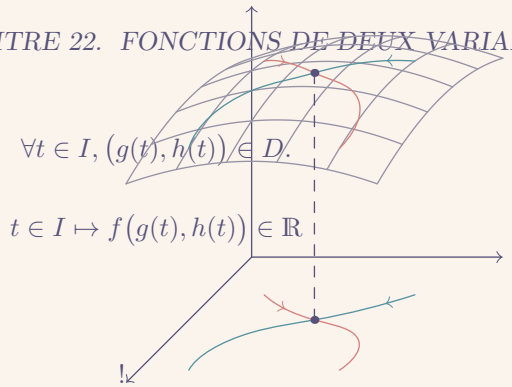
telles que

$\forall t \in I, \big(g(t), h(t)\big) \in D.$

Alors

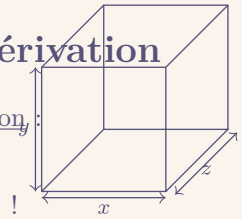
$t \in I \mapsto f\big(g(t), h(t)\big) \in \mathbb{R}$

est continue.



3 Dérivation

Motivation :



$$S(x,y,z) = 2(xy + xz + yz)$$
$$V(x,y,z) = xyz$$

On cherche à minimiser S avec la contrainte $V = 1$.

Soit f : $\begin{array}{ccc} \left(\mathbb{R}_\star^+\right)^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & S\left(x,y,\dfrac{1}{xy}\right) = 2\left(xy + \dfrac{1}{y} + \dfrac{1}{x}\right). \end{array}$

On cherche $(a,b) \in \left(\mathbb{R}_\star^+\right)^2$ tel que

$$\forall (x,y) \in (\mathbb{R}_\star^+), f(x,y) \geqslant f(a,b).$$

Définition : Soit $f : U \to \mathbb{R}$ où U est un ouvert de $\mathbb{R}^2$. Soit $(a,b) \in U$.

Si $\lim\limits_{x \to a} \dfrac{f(x,b) - f(a,b)}{x - a} \in \mathbb{R}$, alors on dit que f a une dérivée partielle suivant x en (a,b) et cette limite est notée

$$\partial f_1(a,b) = \frac{\partial f}{\partial x}(a,b).$$

Si $\lim\limits_{y \to b} \dfrac{f(a,y) - f(a,b)}{y - b} \in \mathbb{R}$, alors on dit que f a une dérivée partielle suivant y en (a,b) et la limite est notée

$$\partial f_2(a,b) = \frac{\partial f}{\partial y}(a,b).$$

Exemple : 1. $f : (x,y) \mapsto xy + x - y$.

$$\frac{\partial f}{\partial x} : (x,y) \mapsto y+1,$$
$$\frac{\partial f}{\partial y} : (x,y) \mapsto x-1.$$

2. $f : (x,y) \mapsto xy + \dfrac{1}{y} + \dfrac{1}{x}$.

$$\frac{\partial f}{\partial x} : (x,y) \mapsto y - \frac{1}{x^2},$$
$$\frac{\partial f}{\partial y} : (x,y) \mapsto x - \frac{1}{y^2}.$$

3. Trouver f telle que $\begin{cases} (1) : & \dfrac{\partial f}{\partial x} = y, \\ (2) : & \dfrac{\partial f}{\partial y} = x. \end{cases}$

   D'après (1) :

$$\forall (x,y), \exists C(y) \in \mathbb{R}, f(x,y) = xy + C(y)$$

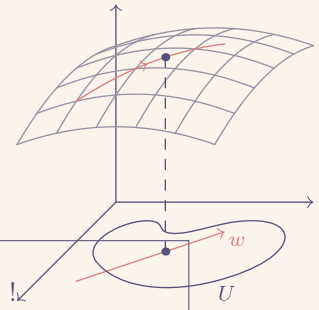
   et donc

$$\frac{\partial f}{\partial y}(x,y) = x + C'(y)$$

   donc $C'(y) = 0$ et donc C est constante.

4. Trouver f telle que $\begin{cases} \dfrac{\partial f}{\partial x} = -y, \\ \dfrac{\partial f}{\partial y} = x. \end{cases}$

   Ce n'est pas possible !



Définition :
Soit $f : U \to \mathbb{R}$ où U est un ouvert. Soit $(a,b) \in U$. Soit $w = (w_1, w_2) \in \mathbb{R}^2$.
Si

$$\lim_{t \to 0} \frac{f(a+tw_1, b+tw_2) - f(a,b)}{t}$$

existe et est réelle, alors on dit que f a une dérivée dans la direction de w et la limite est notée

$$\mathrm{d}f(w)\,(a,b) = D_w(f)\,(a,b).$$

Exemple :

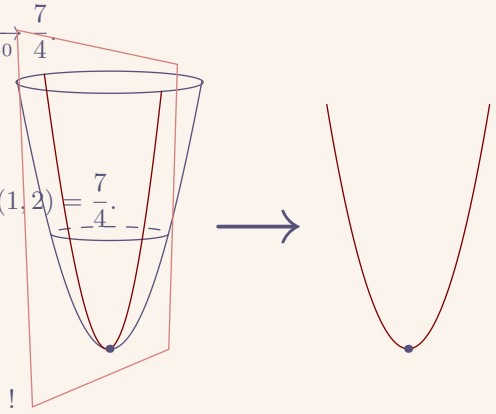
$$f : \left(\mathbb{R}_\star^+\right)^2 \longrightarrow \mathbb{R}$$
$$(x,y) \longmapsto xy + \frac{1}{x} + \frac{1}{y}.$$

On pose $(a,b)=(1,2)$, $w=(w_1,w_2)=(1,1)$.

$$\begin{aligned}\frac{f(1+t,2+t)-f(1,2)}{t} &= \frac{1}{t}\left((1+t)(2+t)+\frac{1}{1+t}+\frac{1}{2+t}-3-\frac{1}{2}\right)\\ &= \frac{1}{t}\left(\cancel{2}+3t+\wp(t)+\cancel{1}-t+\wp(t)+\frac{1}{2}\left(\cancel{1}-\frac{t}{2}+\wp(t)\right)-\cancel{3}-\cancel{\frac{1}{2}}\right)\\ &= \frac{1}{t}\left(\frac{7}{4}t+\wp(t)\right)\\ &= \frac{7}{4}+\wp(1) \xrightarrow[t\to 0]{} \frac{7}{4}.\end{aligned}$$

Donc,

$$\mathrm{d}f(1,1)\,(1,2)=\frac{7}{4}.$$



Remarque :

Théorème : Soit $f : U \to \mathbb{R}$, $(a,b) \in U$. On suppose que $\dfrac{\partial f}{\partial x}$ et $\dfrac{\partial f}{\partial y}$ existent en (a,b) et sont **continues** en (a,b). Alors,

$\forall (h,k) \in \mathbb{R}^2$ tel que $(a+h,b+k) \in U$,

$$f(a+h,b+k)=f(a,b)+h\frac{\partial f}{\partial x}(a,b)+k\frac{\partial f}{\partial y}(a,b)+\underset{(h,k)\to(0,0)}{\wp}\big(\|(h,k)\|\big).$$

On dit que f est de classe $\mathscr{C}^1$ si $\dfrac{\partial f}{\partial x}$ et $\dfrac{\partial f}{\partial y}$ existent et sont continues.

□

Remarque :
En physique, cette formule correspond à :

$$\mathrm{d}f=\frac{\partial f}{\partial x}\mathrm{d}x+\frac{\partial f}{\partial y}\mathrm{d}y.$$

En effet :

$$\begin{aligned}\mathrm{d}f &= f(x+\mathrm{d}x,y+\mathrm{d}y)-f(x,y)\\ &= \frac{\partial f}{\partial x}\mathrm{d}x+\frac{\partial f}{\partial y}\mathrm{d}y.\end{aligned}$$

Proposition : Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^1$ en $(a,b) \in U$. Alors,

$$\forall w = (w_1, w_2) \in \mathbb{R}^2, \mathrm{d}f(w)\,(a,b) = w_1 \frac{\partial f}{\partial x}(a,b) + w_2 \frac{\partial f}{\partial y}(a,b).$$

Preuve :
Soit $w = (w_1, w_2) \in \mathbb{R}^2$. Soit $t \in \mathbb{R}^\star$.

$$\begin{aligned}\frac{1}{t}\big(f(a+tw_1, b+tw_2) - f(a,b)\big) &= \frac{1}{t}\left(tw_1 \frac{\partial f}{\partial x}(a,b) + tw_2 \frac{\partial f}{\partial y}(a,b) + \underset{t\to 0}{o}\big(\|tw\|\big)\right) \\ &= w_1 \frac{\partial f}{\partial x}(a,b) + w_2 \frac{\partial f}{\partial y}(a,b) + \underset{t\to 0}{o}(1) \\ &\xrightarrow[t\to 0]{} w_1 \frac{\partial f}{\partial x}(a,b) + w_2 \frac{\partial f}{\partial y}(a,b).\end{aligned}$$

□

Définition : Avec les hypothèses précédentes, en posant

$$\nabla f(a,b) = \left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)\right)$$

on obtient

$$\mathrm{d}f(w)\,(a,b) = \langle w \mid \nabla f(a,b)\rangle$$

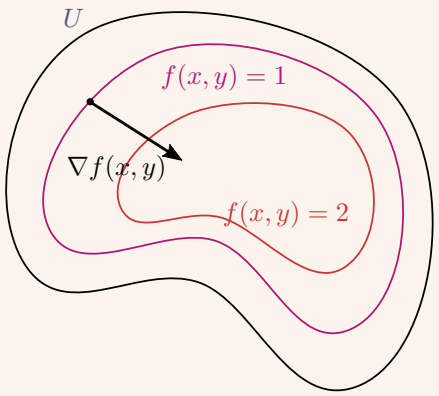
où $\langle \cdot | \cdot \rangle$ est le produit scalaire.

Le vecteur $\nabla f(a,b)$ est appelé gradient de f en (a,b).

Le développement limité à l'ordre 1 de f devient

$$f\big((a,b)+w\big) = f(a,b) + \langle w \mid \nabla f(a,b)\rangle + \underset{w\to 0}{o}(\|w\|)$$

Proposition : Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^1$.



∇f est orthogonal au lignes de niveaux de f, son orientation va dans le sens d'une augmentation de f.

Preuve :
Soit $\gamma : I \to U$ une courbe de niveau :

$$\forall t \in I, f\big(\gamma(t)\big) = \text{cste}.$$

D'après le lemme suivant :

$$\forall t \in I, 0 = (f \circ \gamma)'(t) = \mathrm{d}f\big(\gamma'(t)\big)\big(\gamma(t)\big) = \big\langle \gamma'(t) \mid \nabla f\big(\gamma(t)\big)\big\rangle$$

Donc $\nabla f\big(\gamma(t)\big)$ est orthogonal à $\gamma'(t)$.

Pour tout $t \in I$, on pose $w(t) = t\,\nabla f\big(\gamma(t)\big)$. Donc

$$f\big(\gamma(t) + w(t)\big) = f\big(\gamma(t)\big) + t\|\nabla f(\gamma(t))\|^2 + \underset{t\to 0}{\mathcal{O}}(t)$$

Pour t assez petit, $f\big(\gamma(t) + w(t)\big) - f\big(\gamma(t)\big)$ est du même signe que t. □

Remarque :

$$\begin{aligned} V : \mathbb{R}^3 &\longrightarrow \mathbb{R} \\ (x,y,z) &\longmapsto -mgz \end{aligned}$$

l'énerge potentielle de pesenteur

On a donc

$$\nabla V(x,y,z) = \left(\frac{\partial V}{\partial x}, \frac{\partial V}{\partial y}, \frac{\partial V}{\partial z}\right) = (0,0,-mg) = \vec{P}.$$

Lemme : Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^1$, $\gamma : \begin{array}{ccc} I & \longrightarrow & U \\ t & \longmapsto & \big(x(t), y(t)\big) \end{array}$ où x et y sont dérivables.

On pose

$$\forall t \in I, \gamma'(t) = \big(x'(t), y'(t)\big).$$

Alors $f \circ \gamma : I \to \mathbb{R}$ est dérivable et

$$\begin{aligned} \forall t \in I, (f \circ \gamma)'(t) &= \mathrm{d}f\big(\gamma'(t)\big)\big(\gamma(t)\big) \\ &= \big\langle \gamma'(t) \mid \nabla f\big(\gamma(t)\big)\big\rangle \\ &= x'(t)\frac{\partial f}{\partial x}\big(x(t), y(t)\big) + y'(t)\frac{\partial f}{\partial y}\big(x(t), y(t)\big). \end{aligned}$$

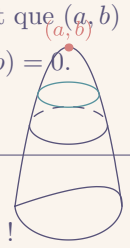
Preuve :
On fixe $t \in I$.

$$\begin{aligned} \forall h \neq 0, \frac{f \circ \gamma(t+h) - f \circ \gamma(t)}{h} &= \frac{1}{h}\big(f(\gamma(t)) + h\gamma'(t) + \underset{h\to 0}{o}(h) - f(\gamma(t))\big) \\ &= \frac{1}{h}\Big(\cancel{f(\gamma(t))} + \langle h\gamma'(t) \mid \nabla f(\gamma(t))\rangle + \underset{h\to 0}{o}(\|h\gamma'(t)\|) - \cancel{f(\gamma(t))}\Big) \\ &= \langle \gamma'(t) \mid \nabla f(\gamma(t))\rangle + \underset{h\to 0}{o}(1) \\ &\xrightarrow[h\to 0]{} \langle \gamma'(t) \mid \nabla f(\gamma(t))\rangle \end{aligned}$$

□

Définition : Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^1$ et $(a, b) \in U$. On dit que (a, b) est un point critique de f si $\nabla f(a, b) = 0$ i.e. $\dfrac{\partial f}{\partial x}(a, b) = \dfrac{\partial f}{\partial y}(a, b) = 0$.

Dans ce cas, $f(a, b)$ est appelé valeur critique de f.



Proposition :
Soit $f : U \to \mathbb{R}$ de classe $\mathscr{C}^1$ et $(a, b) \in U$ tel que

$$\exists r > 0, \forall (x, y) \in B_{(a,b)}(r), f(x, y) \leqslant f(a, b)$$

Alors $\nabla f(a, b) = (0, 0)$.

Preuve :
Soit $g : x \mapsto f(x,b)$. $g(a)$ est un maximum local de g donc $g'(a) = 0$.

Or, $g'(a) = \dfrac{\partial f}{\partial x}(a,b)$

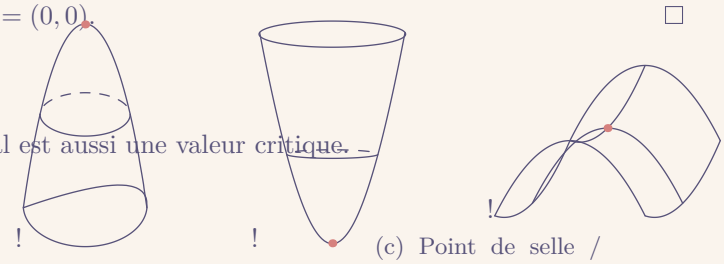
donc $\dfrac{\partial f}{\partial x}(a,b) = 0$.

Soit $h : y \mapsto f(a,y)$. On a de même $h'(b) = 0$.

Or, $h'(b) = \dfrac{\partial f}{\partial y}(a,b)$.

Donc, $\nabla f(a,b) = (0,0)$. □

REMARQUE :
Un minimum local est aussi une valeur critique.



(a) Maximum local (b) Minimum local (c) Point de selle / Point col

EXEMPLE :
On revient à l'exemple donné en introduction :

$$\begin{aligned} f : \left(\mathbb{R}_+^\star\right)^2 &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto 2\left(xy + \frac{1}{x} + \frac{1}{y}\right). \end{aligned}$$

$\left(\mathbb{R}_\star^+\right)^2$ est un ouvert de $\mathbb{R}^2$. Soit $(x,y) \in \left(\mathbb{R}_\star^+\right)^2$.

On a

$$\begin{cases} \dfrac{\partial f}{\partial x}(x,y) = 2\left(y - \dfrac{1}{x^2}\right), \\ \dfrac{\partial f}{\partial y}(x,y) = 2\left(x - \dfrac{1}{y^2}\right). \end{cases}$$

$$\begin{aligned} & \frac{\partial f}{\partial x}(x,y) = \frac{\partial f}{\partial y}(x,y) = 0 \\ \iff & \begin{cases} y = \dfrac{1}{x^2} \\ x = \dfrac{1}{y^2} \end{cases} \\ \iff & \begin{cases} y = \dfrac{1}{x^2} \\ x = x^4 \end{cases} \\ \iff & \begin{cases} x = 1 \\ y = 1 \end{cases} \end{aligned}$$

On vérifie que f présente en effet un minium local en $(1,1)$.

$$f(1,1)=6$$

On fixe $y\in\mathbb{R}_\star^+$ et

$$g:x\mapsto 2\left(xy+\frac{1}{x}+\frac{1}{y}\right).$$

Donc

$$\forall x\in\mathbb{R}_\star^+, g'(x)=2\left(y-\frac{1}{x^2}\right).$$

x	0		$\frac{1}{\sqrt{y}}$		$+\infty$
$g'(x)$		$-$	0	$+$	
g		$\searrow$	$2\left(2\sqrt{y}+\frac{1}{y}\right)$	$\nearrow$	

Ainsi,

$$\forall x\in\mathbb{R}_\star^+,\forall y\in\mathbb{R}_\star^+, f(x,y)\geqslant 2\left(2\sqrt{y}+\frac{1}{y}\right)$$

Soit $h:y\mapsto 2\sqrt{y}+\dfrac{1}{y}$. On a

$$\forall y>0, h'(y)=\frac{1}{\sqrt{y}}-\frac{1}{y^2}=\frac{y\sqrt{y}-1}{y^2}=\frac{y^{\frac{3}{2}}-1}{y^2}$$

y	0		1		$+\infty$
$h'(y)$		$-$	0	$+$	
h		$\searrow$	3	$\nearrow$	

Donc,

$$\forall x,y>0, f(x,y)\geqslant 2\times 3=6=f(1,1).$$

Proposition (règle de la chaîne) **:** Soit $f:\begin{array}{ccc}U&\longrightarrow&\mathbb{R}^2\\(x,y)&\longmapsto&f(x,y)\end{array}$ de classe $\mathscr{C}^1$ et U,V deux ouverts de $\mathbb{R}^2$.

Soit $\varphi:\begin{array}{ccc}V&\longrightarrow&U\\(u,v)&\longmapsto&\varphi(u,v)=\big(x(u,v),y(u,v)\big)\end{array}$.

On suppose que x et y sont de classe $\mathscr{C}^1$ sur V.

Alors, $f\circ\varphi : \begin{array}{ccc} V & \longrightarrow & \mathbb{R} \\ (u,v) & \longmapsto & f\big(\varphi(u,v)\big) \end{array}$ est de classe $\mathscr{C}^1$ et

$$\forall (u_0,v_0)\in V,\ \frac{\partial(f\circ\varphi)}{\partial u}(u_0,v_0) = \frac{\partial f}{\partial x}\big(\varphi(u_0,v_0)\big)\times\frac{\partial x}{\partial u}(u_0,v_0) + \frac{\partial f}{\partial y}\big(\varphi(u_0,v_0)\big)\frac{\partial y}{\partial u}(u_0,v_0)$$

$$\forall (u_0,v_0)\in V,\ \frac{\partial(f\circ\varphi)}{\partial v}(u_0,v_0) = \frac{\partial f}{\partial x}\big(\varphi(u_0,v_0)\big)\times\frac{\partial x}{\partial v}(u_0,v_0) + \frac{\partial f}{\partial y}\big(\varphi(u_0,v_0)\big)\frac{\partial y}{\partial v}(u_0,v_0)$$

Exemple (changement de coordonnées polaires) :
On pose

$$\begin{aligned} \varphi : \mathbb{R}_\star^+\times]0,2\pi[&\longrightarrow \mathbb{R}^2\setminus\big(R_\star^+\times\{0\}\big) \\ (r,\theta) &\longmapsto (r\cos\theta, r\sin\theta), \end{aligned}$$

$$\begin{aligned} f : \mathbb{R}^2\setminus\big(R_\star^+\times\{0\}\big) &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto f(x,y), \end{aligned}$$

$$\begin{aligned} g : \overbrace{\mathbb{R}_\star^+\times]0,2\pi[}^{=V} &\longrightarrow \mathbb{R} \\ (r,\theta) &\longmapsto f(r\cos\theta, r\sin\theta). \end{aligned}$$

$\forall (r_0,\theta_0)\in V,$

$$\begin{aligned} \frac{\partial g}{\partial r}(r_0,\theta_0) &= \frac{\partial f}{\partial x}(r_0\cos\theta_0, r_0\sin\theta_0)\cos\theta_0 \\ &\quad + \frac{\partial f}{\partial y}(r_0\cos\theta_0, r_0\sin\theta_0)\sin\theta_0 \\ &= 2r_0\cos^2\theta_0 + 2r_0\sin^2(\theta_0) \\ &= 2r_0 \end{aligned}$$

$$\begin{aligned} \frac{\partial g}{\partial \theta}(r_0,\theta_0) &= \frac{\partial f}{\partial x}(r_0\cos\theta_0, r_0\sin\theta_0)r_0\sin\theta_0 \\ &\quad + \frac{\partial f}{\partial y}(r_0\cos\theta_0, r_0\sin\theta_0)r_0\cos\theta_0 \\ &= -2{r_0}^2\cos(\theta_0)\sin(\theta_0) + 2{r_0}^2\sin(\theta_0)\cos(\theta_0) \\ &= 0 \end{aligned}$$

Donc,

$$g(r,\theta) = r^2.$$

Exemple :
Résoudre

$$\begin{cases} \dfrac{\partial f}{\partial x} = \dfrac{x}{x^2+y^2}, \\ \dfrac{\partial f}{\partial y} = \dfrac{y}{x^2+y^2}. \end{cases}$$

On pose $g : (r,\theta) \mapsto f(r\cos\theta, r\sin\theta)$.

$$\begin{aligned} \frac{\partial g}{\partial r} &= \frac{1}{r}\cos^2\theta + \frac{1}{r}\sin^2\theta = \frac{1}{r}, \\ \frac{\partial g}{\partial \theta} &= -\cos(\theta)\sin(\theta) + \sin(\theta)\cos(\theta) = 0. \end{aligned}$$

Donc,

$$\exists C \in \mathbb{R}, g : (r,\theta) \mapsto \ln r + C$$

d'où,

$$\begin{aligned} \forall (x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}, f(x,y) &= \ln\left(\sqrt{x^2+y^2}\right) + C \\ &= \frac{1}{2}\ln(x^2+y^2) + C. \end{aligned}$$

Remarque :
Soit $\mathscr{B} = (e_1, e_2)$ la base canonique de $\mathbb{R}^2$, $f : U \to \mathbb{R}$ de classe $\mathscr{C}^1$ avec U un ouvert de $\mathbb{R}^2$.

Soit $(x,y) \in U$.

$$\mathrm{Mat}_{\mathscr{B}}\left(\nabla f(x,y)\right) = \begin{pmatrix} \dfrac{\partial f}{\partial x}(x,y) \\ \dfrac{\partial f}{\partial y}(x,y) \end{pmatrix}$$

Soit

$$\begin{aligned} \varphi : V &\longrightarrow U \\ (u,v) &\longmapsto \big(x(u,v), y(u,v)\big) \end{aligned}$$

avec x, y de classe $\mathscr{C}^1$. Soit $g = f \circ \varphi$.

$$\begin{aligned}
\mathrm{Mat}_{\mathscr{B}}\big(\nabla g(u,v)\big) &= \begin{pmatrix} \dfrac{\partial g}{\partial u}(u,v) \\ \dfrac{\partial g}{\partial v}(u,v) \end{pmatrix} \\
&= \begin{pmatrix} \dfrac{\partial x}{\partial u}(u,v)\dfrac{\partial f}{\partial x}(x,y) + \dfrac{\partial y}{\partial u}(u,v)\dfrac{\partial f}{\partial y}(x,y) \\ \dfrac{\partial x}{\partial v}(u,v)\dfrac{\partial f}{\partial x}(x,y) + \dfrac{\partial y}{\partial v}(u,v)\dfrac{\partial f}{\partial y}(x,y) \end{pmatrix} \\
&= \underbrace{\begin{pmatrix} \dfrac{\partial x}{\partial u}(u,v) & \dfrac{\partial y}{\partial u}(u,v) \\ \dfrac{\partial x}{\partial v}(u,v) & \dfrac{\partial y}{\partial v}(u,v) \end{pmatrix}}_{J(u,v)} \begin{pmatrix} \dfrac{\partial f}{\partial x}(x,y) \\ \dfrac{\partial f}{\partial y}(x,y) \end{pmatrix} \\
&= J(u,v)\,\mathrm{Mat}_{\mathscr{B}}\big(\nabla f(x,y)\big)
\end{aligned}$$

où $J(u,v) = \big(\mathrm{Mat}_{\mathscr{B}}\big(\nabla x(u,v)\big) : \mathrm{Mat}_{\mathscr{B}}\big(\nabla y(u,v)\big)\big)$.

On dit que $J(u,v)$ est <u>la jacobienne</u> de φ en (u,v). L'application linéaire canoniquement associée à $J(u,v)$ est la <u>différentielle de φ</u> en (u,v) noté $\mathrm{d}\varphi(u,v)$.

On a $\mathrm{d}\varphi(u,v) \in \mathscr{L}(R^2)$ et $\mathrm{Mat}_{\mathscr{B}}\big(\mathrm{d}\varphi(u,v)\big) = J(u,v)$.

Par exemple, la jacobienne du changement de coordonnées polaires est

$$J = \begin{pmatrix} \dfrac{\partial x}{\partial r} & \dfrac{\partial y}{\partial r} \\ \dfrac{\partial x}{\partial \theta} & \dfrac{\partial y}{\partial \theta} \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -r\sin\theta & r\cos\theta \end{pmatrix}.$$

$$\underbrace{\det(J)}_{\text{le jacobien}} = r\cos^2\theta + r\sin^2\theta = r$$

Dans une intégrale double, si $(x,y) = \varphi(u,v)$, alors $\mathrm{d}x\mathrm{d}y = \det(J)\mathrm{d}u\mathrm{d}v$.

Ici,

$$\mathrm{d}x\ \mathrm{d}y = r\ \mathrm{d}r\ \mathrm{d}\theta.$$

Preuve :
On pose $(x_0, y_0) = \varphi(u_0, v_0)$. Pour tout $(h,k) \in \mathbb{R}^2$ tels que $(u_0+h, v_0+k) \in V$, en posant $g = f \circ \varphi$.

$$
\begin{aligned}
g(u_0+h,v_0+h) &= f\big(x(u_0+h,v_0+k),y(u_0+h,v_0+k)\big)\\
&= f\left(x(u_0,v_0)+h\frac{\partial x}{\partial u}(u_0,v_0)+k\frac{\partial x}{\partial v}(u_0,v_0)+\circ\left(\|(h,k)\|\right),\right.\\
&\qquad \left. y(u_0,v_0)+h\frac{\partial y}{\partial u}(u_0,v_0)+k\frac{\partial y}{\partial v}(u_0,v_0)+\circ\left(\|(h,k)\|\right)\right)\\
&= f(x_0,y_0)\\
&\quad +\left(h\frac{\partial x}{\partial u}(u_0,v_0)+k\frac{\partial x}{\partial v}(u_0,v_0)+\circ(\|(h,k)\|)\right)\frac{\partial f}{\partial x}(x_0,y_0)\\
&\quad +\left(h\frac{\partial y}{\partial u}(u_0,v_0)+k\frac{\partial y}{\partial v}(u_0,v_0)+\circ(\|(h,k)\|)\right)\frac{\partial f}{\partial y}(x_0,y_0)\\
&\quad +\circ(\|(h,k)\|)\\
&= f(x_0,y_0)\\
&\quad +h\left(\frac{\partial x}{\partial u}(u_0,v_0)\frac{\partial f}{\partial x}(x_0,y_0)+\frac{\partial y}{\partial u}(u_0,v_0)\frac{\partial f}{\partial y}(x_0,y_0)\right)\\
&\quad +k\left(\frac{\partial x}{\partial v}(u_0,v_0)\frac{\partial f}{\partial x}(x_0,y_0)+\frac{\partial y}{\partial v}(u_0,v_0)\frac{\partial f}{\partial y}(x_0,y_0)\right) \qquad +\circ(\|(h,k)\|)\\
&= g(u_0,v_0)+h\frac{\partial g}{\partial u}(u_0,v_0)+k\frac{\partial g}{\partial v}(u_0,v_0)+\circ(\|(h,k)\|)
\end{aligned}
$$

Par identification,

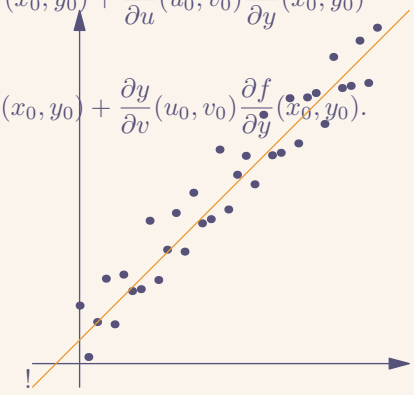
$$\frac{\partial g}{\partial u}(u_0,v_0)=\frac{\partial x}{\partial u}(u_0,v_0)\frac{\partial f}{\partial x}(x_0,y_0)+\frac{\partial y}{\partial u}(u_0,v_0)\frac{\partial f}{\partial y}(x_0,y_0)$$

et

$$\frac{\partial g}{\partial v}(u_0,v_0)=\frac{\partial x}{\partial v}(u_0,v_0)\frac{\partial f}{\partial x}(x_0,y_0)+\frac{\partial y}{\partial v}(u_0,v_0)\frac{\partial f}{\partial y}(x_0,y_0).$$

□

Exemple (Régression linéaire) :



$$y=ax+b$$

On fixe $(a,b)\in\mathbb{R}^2$.

$$\varepsilon(a,b)=\sum_{i=1}^{n}\big(y_i-(ax_i+b)\big)^2$$

l'erreur totale.

On veut minimiser $\varepsilon(a,b)$. On a

$$\forall (a,b)\in\mathbb{R}^2,\ \begin{cases}\dfrac{\partial\varepsilon}{\partial a}(a,b)=-2\displaystyle\sum_{i=1}^{n}(y_i-ax_i-b)x_i,\\ \dfrac{\partial\varepsilon}{\partial b}(a,b)=-2\displaystyle\sum_{i=1}^{n}(y_i-ax_i-b).\end{cases}$$

Donc,

$$\begin{aligned}(a,b)\text{ point critique de }\varepsilon &\iff \begin{cases}a\displaystyle\sum_{i=1}^{n}{x_i}^2+b\sum_{i=1}^{n}x_i=\sum_{i=1}^{n}y_ix_i\\ a\displaystyle\sum_{i=1}^{n}x_i+nb=\sum_{i=1}^{n}y_i\end{cases}\\ &\iff \begin{cases}a\left(\dfrac{1}{n}\displaystyle\sum_{i=1}^{n}{x_i}^2-\overline{x}^2\right)=\overline{y}-\overline{xy}\\ b=\dfrac{1}{n}\displaystyle\sum_{i=1}^{n}y_i-\dfrac{a}{n}\sum_{i=1}^{n}x_i=\dfrac{1}{n}\sum_{i=1}^{n}x_iy_i-\overline{xy}\end{cases}\\ &\qquad\text{où }\overline{x}=\frac{1}{n}\sum_{i=1}^{n}x_i,\ \overline{y}=\frac{1}{n}\sum_{i=1}^{n}y_i\\ &\iff \begin{cases}a=\dfrac{\mathrm{Cov}(x,y)}{V(x)}\\ b=\overline{y}-a\overline{x}\end{cases}\end{aligned}$$

Coefficient de corrélation : $\dfrac{\mathrm{Cov}(x,y)}{\sigma_x\sigma_y}\in[-1,1]$

Chapitre 23

Dénombrement

1 Cardinal d'un ensemble

Lemme : Soit $n \in \mathbb{N}^\star$, $n \geqslant 2$, et $X \subsetneq [\![1, n]\!]$ avec $X \neq$ ($\subsetneq$ signifie inclus et différent).

Alors

$$\exists\ 0 < p < n, \exists f : X \to [\![1, p]\!] \text{ bijective .}$$

Preuve (par récurrence sur n) *:*
On pose, pour $n \geqslant 2$,

$\mathscr{P}(n)$: "$\forall X \subsetneq [\![1, n]\!]$ tel que $X \neq$, $\exists\ 0 < p < n, \exists f : X \to [\![1, p]\!]$ bijective"

— Soit $X \subsetneq [\![1, 2]\!]$ avec $X \neq$. Par définition d'une inclusion,

$$X = \{1\} \text{ ou } X = \{2\}.$$

On pose $p = 1$.

Si $X = \{1\}$, alors on pose

$$\begin{aligned} f : X &\longrightarrow [\![1, 1]\!] = \{1\} \\ 1 &\longmapsto 1 \end{aligned}$$

f est bien bijective.

Si $X = \{2\}$, alors on pose

$$\begin{aligned} f : X &\longrightarrow \{1\} \\ 2 &\longmapsto 1 \end{aligned}$$

De nouveau, f est bijective.

Ainsi, $\mathscr{P}(2)$ est vraie.

— Soit $n \geqslant 2$. On suppose $\mathscr{P}(n)$ vraie. Soit $X \subsetneq [\![1, n+1]\!]$ avex $X \neq .$

Cas 1 On suppose que $n+1 \notin X$.

Alors $X \subset [\![1, n]\!]$.

— Si $X = [\![1, n]\!]$, alors on pose $p = n < n+1$ et $f : \begin{array}{ccc} X & \longrightarrow & [\![1,p]\!] = X \\ i & \longmapsto & i \end{array}$ est bijective.

— Si $X \subsetneq [\![1, n]\!]$, d'après $\mathscr{P}(n)$, il existe $p \in [\![1, n-1]\!]$ et une bijection $f : X \to [\![1, p]\!]$.

On a bien $p < n+1$.

Cas 2 $n+1 \in X$. On pose $Y = X \setminus \{n+1\}$. Ainsi $Y \subset [\![1, n+1]\!]$.

— Si $Y = [\![1, n]\!]$, alors $X = [\![1, n]\!] \cup \{n+1\}$: $\lightning$

— Si $Y = $, alors $X = \{n+1\}$. On pose donc $p = 1 < n+1$ et $f : \begin{array}{ccc} X & \longrightarrow & [\![1,p]\!] = \{1\} \\ n+1 & \longmapsto & 1 \end{array}$ est bijective.

— On suppose $Y \neq .$ D'après $\mathscr{P}(n)$, il existe $q \in [\![1, n-1]\!]$ et $g : Y \to [\![1, q]\!]$ bijective.

On pose $f : \begin{array}{ccc} X & \longrightarrow & [\![1, q+1]\!] \\ x & \longmapsto & \begin{cases} g(x) & \text{si } x \neq n+1, \\ q+1 & \text{si } x = n+1. \end{cases} \end{array}$

On pose aussi $p = q+1 \leqslant n < n+1$. f est bijective.

On pose

$$h : [\![1, q+1]\!] \longrightarrow X$$
$$i \longmapsto \begin{cases} g^{-1}(i) & \text{si } i \leqslant q, \\ n+1 & \text{si } i = q+1. \end{cases}$$

$$\forall i \in [\![1, q+1]\!], f\big(h(i)\big) = \begin{cases} f\big(g^{-1}(i)\big) & \text{si } i \leqslant q \\ f(n+1) & \text{si } i = q+1 \end{cases}$$
$$= \begin{cases} g\big(g^{-1}(i)\big) & \text{si } i \leqslant q \\ q+1 & \text{si } i = q+1 \end{cases}$$
$$= i$$

$$\begin{aligned}\forall x \in X, h\big(f(x)\big) &= \begin{cases} h\big(g(x)\big) & \text{si } x \neq n+1 \\ h(q+1) & \text{si } x = n+1 \end{cases} \\ &= \begin{cases} g^{-1}\big(g(x)\big) & \text{si } x \neq n+1 \\ n+1 & \text{si } x = n+1 \end{cases} \\ &= x\end{aligned}$$

□

Lemme : Soient n, p deux entiers non-nuls et $f : [\![1,p]\!] \to [\![1,n]\!]$ une surjection. Alors $p \geqslant n$.

Preuve (par récurrence sur n) *:*
Pour $n \in \mathbb{N}^\star$, on pose

$$\mathcal{P}(n) : \text{“ } \forall p \in \mathbb{N}^\star, \forall f : [\![1,p]\!] \to [\![1,n]\!], f \text{ surjective } \implies p \geqslant n.\text{”}$$

— Soit $p \in \mathbb{N}^\star$ et $f : [\![1,p]\!] \to [\![1,1]\!] = \{1\}$. On suppose f surjetive. Nécessairement, $p \geqslant 1$.
— Soit $n \in \mathbb{N}^\star$. On suppose $\mathcal{P}(n)$ vraie. Soit $p \in \mathbb{N}^\star$ et $f : [\![1,p]\!] \to [\![1,n+1]\!]$. On suppose f surjective. On veut montrer que $p \geqslant n+1$.

On pose

$$X = f^{-1}\big([\![1,n]\!]\big) = \{i \in [\![1,p]\!] \mid f(i) \neq n+1\}.$$

Commme f est surjective, $X \neq$ et $X \neq [\![1,p]\!]$. D'après le lemme précédent, il existe $0 < q < p$ et $g : X \to [\![1,q]\!]$ bijective.

Ainsi $f \circ g^{-1} : [\![1,q]\!] \to [\![1,n]\!]$ est surjective.

D'après $\mathcal{P}(n)$, $q \geqslant n$.

Si $p \leqslant n$, alors $q < p \leqslant n$: ↯

Donc $p > n$ et donc $p \geqslant n+1$.

□

Lemme : Soient $n \geqslant 1$ et $p \geqslant 1$, $f : [\![1,p]\!] \to [\![1,n]\!]$. Alors $p \leqslant n$.

Preuve :

On pose

$$g : [\![1,n]\!] \longrightarrow [\![1,p]\!]$$
$$i \longmapsto \begin{cases} 1 & \text{si } f^{-1}\big(\{i\}\big) = , \\ j & \text{si } f^{-1}\big(\{i\}\big) = \{j\}. \end{cases}$$

g est surjective. Soit $k \in [\![1,p]\!]$, alors $g\big(f(k)\big) = k$ car k est un antécédant de $f(k)$ par f.

D'après le lemme précédent, $n \geqslant p$. □

Corollaire : Soient $n, p \in \mathbb{N}^\star$ et $f : [\![1,n]\!] \to [\![1,p]\!]$ bijective. Alors $n = p$

Définition : Soit X un ensemble. On dit que X est fini si $X =$ ou s'il existe $n \in \mathbb{N}^\star$ et une bijection $f : X \to [\![1,n]\!]$.

Soit X un ensemble fini. Le cardinal de X est

- 0 si $X =$
- sinon, c'est le seul entier $n \in \mathbb{N}^\star$ pour lequel il existe une bijection de X dans $[\![1,n]\!]$.

On le note $\mathrm{Card}(X)$, $\#X$ ou $|X|$.

Proposition : Soit E un ensemble fini et $X \in \mathcal{P}(E)$.

Alors X est fini et $\#X \leqslant \#E$.

Si $\#X = \#E$, alors $X = E$.

Preuve Cas 1 Si $E =$, alors $X =$.

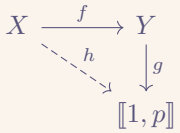
Cas 2 $E \neq$. On pose $n = \#E \in \mathbb{N}^\star$. Soit $f : E \to [\![1,n]\!]$ une bijection.

On suppose $X \neq$. On pose $Y = f(X) \subset [\![1,n]\!]$

- Si $Y = [\![1,n]\!]$, alors $X = E$ et donc $\#X = n \leqslant \#E$.
- Si $Y \subsetneq [\![1,n]\!]$, comme $Y \neq$, il existe $p \in [\![1,n-1]\!]$ et $g : Y \to [\![1,p]\!]$: une bijection.

$$g : X \longrightarrow [\![1,p]\!]$$
$$x \longmapsto g\big(f(x)\big)$$

D'où



Montrons que h est bijective. On pose

$$\begin{aligned} k : [\![1,p]\!] &\longrightarrow X \\ i &\longmapsto f^{-1}\big(g^{-1}(i)\big). \end{aligned}$$

h et k sont réciproques l'une de l'autre, donc $\#X = p \leqslant n$.

On suppose $X = $, alors $\#X = 0 < n$.

□

Proposition : Soit E un ensemble fini, $(A, B) \in \mathcal{P}(E)^2$ tel que $A \cap B = $.

Alors

$$\#(A \cup B) = \#A + \#B.$$

Preuve :

Le résultat est évident si $A = $ et $B = $.

On suppose $A \neq $ et $B \neq $. On pose $a = \#A$ et $\#B$. Soient

$$\begin{cases} f : A \to [\![1,a]\!] \text{ une bijection} \\ g : B \to [\![1,b]\!] \text{ une bijection} \end{cases}$$

On pose

$$\begin{aligned} h : A \cup B &\longrightarrow [\![a+b]\!] \\ x &\longmapsto \begin{cases} f(x) & \text{si } x \in A, \\ a + g(x) & \text{si } x \in B. \end{cases} \end{aligned}$$

Comme $A \cap B = $, h est bien définie.

Soit

$$\begin{aligned} k : [\![1,a+b]\!] &\longrightarrow A \cup B \\ i &\longmapsto \begin{cases} f^{-1}(i) & \text{si } i \leqslant a \\ g^{-1}(i-a) & \text{si } i > a. \end{cases} \end{aligned}$$

On vérifie que h et k sont réciproques l'une de l'autre.

Donc $\#(A \cup B) = a + b$. □

Proposition : Soient E un ensemble fini, $n \in \mathbb{N}^\star$, $(A_1, \dots, A_n) \in \mathscr{P}(E)^n$ telles que

$$\forall i \neq j, A_i \cap A_j = .$$

Alors

$$\#\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \#A_i$$

Preuve (par récurrence sur n) *:*
On a traité le cas $n = 2$ précédemment.

Soit $n \geqslant 2$ pour lequel le résultat est vrai. Soit $(A_1, \dots, A_{n+1}) \in \mathscr{P}(E)^{n+1}$ telles que

$$\forall i \neq j, A_i \cap A_j = .$$

On pose $A = \bigcup_{i=1}^{n} A_i$. Alors

$$\begin{aligned} A \cap A_{n+1} &= \left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1} \\ &= \bigcup_{i=1}^{n} (A_i \cap A_{n+1}) \\ &= \bigcup_{i=1}^{n} \\ &= . \end{aligned}$$

Donc,

$$\begin{aligned} \#(\bigcup_{i=1}^{n+1} A_i) &= \#(A \cup A_{n+1}) \\ &= \#A = \#A_{n+1} \\ &= \sum_{i=1}^{n} \#A_i + \#A_{n+1} \\ &= \sum_{i=1}^{n+1} \#A. \end{aligned}$$

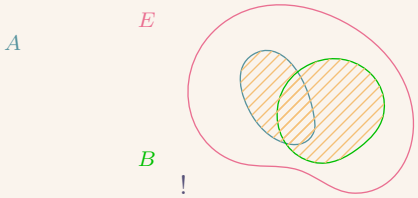
□

Proposition : Soient E un ensemble fini, $(A,B) \in \mathcal{P}(E)^2$. Alors

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

Preuve :

On pose $\begin{cases} C = A \cap B \\ A' = A \setminus C \\ B' = B \setminus C. \end{cases}$



Alors

$$\begin{cases} A' \cup B' \cup C = A \cup B, \\ A' \cap B' = A' \cap C = B' \cap C = . \end{cases}$$

D'où

$$\begin{aligned} \#(A \cup B) &= \#(A' \cup B' \cup C) \\ &= \#A' + \#B' + \#C. \end{aligned}$$

Or,

$$\begin{cases} A = A' \cup C \\ A' \cap C = \end{cases}$$

donc

$$\#A = \#A' + \#C$$

donc

$$\#A' = \#A - \#C.$$

De même,

$$\#B' = \#B - \#C.$$

D'où

$$\begin{aligned} \#(A \cup B) &= \#A - \#C + \#B - \#C + \#C \\ &= \#A + \#B - \#C \end{aligned}$$

□

Au passage, on a prouvé la proposition suivante :

Proposition : Soient E un ensemble fini, $(A,B) \in \mathcal{P}(E)^2$ avec $B \subset A$. Alors

$$\#(A \setminus B) = \#A - \#B.$$

□

Exemple :
Soit E un ensemble fini, $(A,B,C) \in \mathcal{P}(E)^3$.

$$\begin{aligned}\#(A\cup B\cup C) = &\#A+\#B+\#C\\ &-\#(A\cap B)-\#(B\cap C)-\#(A\cap C)\\ &+\#(A\cap B\cap C).\end{aligned}$$

Soit $(A,B,C,D) \in \mathcal{P}(E)^4$.

$$\begin{aligned}\#(A\cup B\cup C\cup D) = &\#A+\#B+\#C+\#D\\ &-\#(A\cap B)-\#(A\cap C)-\#(A\cap D)-\#(B\cap C)-\#(B\cap D)-\#(C\cap D)\\ &+\#(A\cap B\cap C)+\#(A\cap B\cap D)+\#(B\cap C\cap D)+\#(A\cap C\cap D)\\ &-\#(A\cap B\cap C\cap D).\end{aligned}$$

En généralisant, on obtient la formule du crible :

$$\#\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n}(-1)^{k+1}\sum_{1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant n}\#(A_{i_1}\cap\cdots\cap A_{i_k}).$$

Proposition : Soient E et F deux ensembles finis et $f : E \to F$.
1. Si f est injective, alors $\#E \leqslant \#F$,
2. Si f est surjective, alors $\#E \geqslant \#F$,
3. Si f est bijective, alors $\#E = \#F$,

Preuve : 1.
$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle bij}\uparrow & & \downarrow{\scriptstyle bij} \\ [\![1,n]\!] & \xrightarrow{inj} & [\![1,p]\!] \end{array}$$

2.
$$\begin{array}{ccc} E & \xrightarrow{surj} & F \\ {\scriptstyle bij}\uparrow & & \downarrow{\scriptstyle bij} \\ [\![1,n]\!] & \xrightarrow{surj} & [\![1,p]\!] \end{array}$$

□

Proposition (principe des tiroirs – pigeonhole principle) **:** Soit $f : E \to F$ telle que $\#E > \#F$. Alors

$$\exists (x,y)\in E^2, \begin{cases} x\neq y, \\ f(x)=f(y)\end{cases}$$

Preuve :
C'est la contraposée du point 1. de la proposition précédente. □

Proposition : Soit $E \to F$ où E et F sont finis et $\#E = \#F$.

$$f \text{ injective} \iff f \text{ surjective} \iff f \text{ bijective .}$$

Preuve : — On suppose f injective. Soit

$$\begin{aligned} g : E &\longrightarrow \mathrm{Im}(f) \\ x &\longmapsto f(x) \end{aligned}$$

g est bijective donc $\#E = \#\mathrm{Im}\, f$. Or, $\#E = \#F$ donc $\mathrm{Im}\, f = F$ et donc f est surjective.

— On suppose f surjective. Alors

$$E = \bigcup_{y \in F}^{\cdot} f^{-1}(\{y\})$$

donc

$$\#E = \sum_{y \in F} \#f^{-1}(\{y\}) \geqslant \sum_{y \in F} 1 = \#F$$

donc

$$\forall y \in F, \#f^{-1}(\{y\}) = 1$$

donc f est bijective.

□

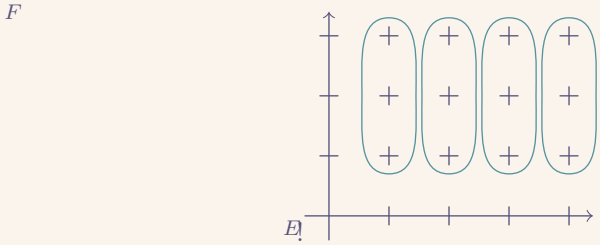
2 Dénombrement

Proposition : Soient E et F deux ensembles finis. Alors $E \times F$ est fini et

$$\#(E \times F) = \#E \times \#F.$$

Preuve :

$$E \times F = \bigcup_{x \in E}^{\cdot} \underbrace{\{(x, y) \mid y \in F\}}_{F_x}.$$



Donc,

$$\#(E \times F) = \sum_{x \in E} (\#F_x)$$

Pour $x \in E$, soit

$$\begin{aligned} \varphi_x : F_x &\longrightarrow F \\ (x, y) &\longmapsto y. \end{aligned}$$

φ_x est bijective donc $\#F_x = \#F$. D'où

$$\#(E \times F) = \sum_{x \in E} (\#F) = \#(E) \times (\#F).$$

□

Proposition : Soit $n \in \mathbb{N}^\star$ et $E_1, \ldots, E_n$ des ensembles finis. Alors $\prod_{i=1}^{n} E_i$ est fini et

$$\# \left(\prod_{i=1}^{n} E_i \right) = \prod_{i=1}^{n} (\#E_i).$$

Preuve :
par récurrence sur n. □

Corollaire : Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}^\star$. Alors

$$\#(E^p) = n^p.$$

En d'autres termes, il y a n^p p-listes de E, où une p-lise de E est un $(x_1, \ldots, x_p)$ de E^p.

Définition : Soit E un ensemble fini et $p \in \mathbb{N}^\star$. Un p-arrangement de E

est une p-liste de E d'éléments deux à deux distincts :

$$(x_1, \dots, x_p) \in E^p \text{ est un } p\text{-arrangement} \iff \forall i \neq j, x_i \neq x_j.$$

Proposition : Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}^\star$. Il y a exactement $\dfrac{n!}{(n-p)!}$ p-arrangements si $p \leqslant n$ et 0 si $p > n$.

Preuve (par récurrence sur p) *:*

— Il y a n 1-arrangements de E. Or, $\dfrac{n!}{(n-1)!} = n$.

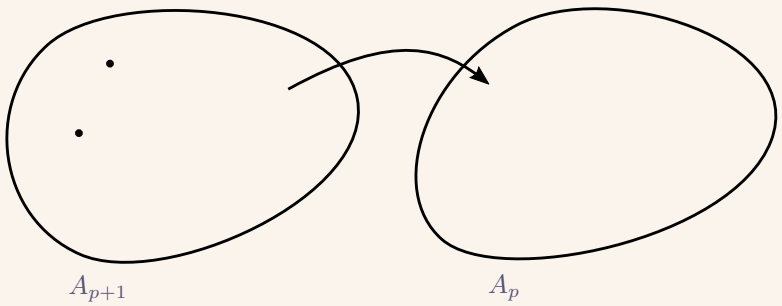
— Soit $p \in \mathbb{N}^\star$. On suppose qu'il y a $\dfrac{n!}{(n-p)!}$ p-arrangements.

Soit

$$\begin{aligned} f : \mathscr{A}_{p+1} &\longrightarrow \mathscr{A}_p \\ (x_1, \dots, x_{p+1}) &\longmapsto (x_1, \dots, x_p) \end{aligned}$$

où $\mathscr{A}_{p+1}$ est l'ensemble des $(p+1)$-arrangements et $\mathscr{A}_p$ est l'ensemble des p-arrangements.

Soit $x = (x_1, \dots, x_p) \in \mathscr{A}_p$. x a exactement $n - p$ antécédants par f.



D'après le principe des bergers,

$$\begin{aligned}\#\mathscr{A}_{p+1} &= (n-p)\#\mathscr{A}_p \\ &= (n-p) \times \frac{n!}{(n-p)!} \\ &= \frac{n!}{(n-p-1)!} \\ &= \frac{n!}{\big(n-(p+1)\big)!}\end{aligned}$$

□

Dans la preuve précédente, on a utilisé principe des bergers :

Lemme (principe des bergers) **:** Soit $f : E \to F$ surjective telle que

$$\exists k, \forall y \in F, \#\big(f^{-1}(\{-1\})\big) = k$$

En d'autres termes, tous les éléments de F ont le même nombre d'antécédants.

Si F est fini, alors

$$\#E = k\,\#F.$$

Preuve :
On définit $\sim$ sur E :

$$x \sim y \iff f(x) = f(y).$$

"$\sim$" est une relation d'équivalence sur E. Soit $\mathscr{R}$ un système de représentants :

$$E = \bigcup_{x \in \mathscr{R}}^{\cdot} \mathscr{C}\ell(x).$$

On a donc

$$\forall x \in E, \exists! u \in \mathscr{R}, x \sim u.$$

L'application $\begin{array}{ccc} \mathscr{R} & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array}$ est bijective donc $\#\mathscr{R} = \#F$.

Soit $x \in \mathscr{R}$.

$$\begin{aligned}\forall y \in E, y \in \mathscr{C}\ell(x) &\iff f(y) = f(x) \\ &\iff y \text{ est un antécédant de } f(x)\end{aligned}$$

donc $\#\mathscr{C}\ell(x) = k$.

Finalement,

$$\begin{aligned}\#E &= \sum_{x\in\mathscr{R}} \#\big(\mathscr{C}\ell(x)\big)\\ &= \sum_{x\in\mathscr{R}} k\\ &= k(\#\mathscr{R})\\ &= k(\#F).\end{aligned}$$

□

Proposition : Soit E un ensemble fini de cardinal n. Il y a $n!$ permutations de E.

Preuve :
On note $S(E)$ l'ensemble des permutations de E, $\mathscr{A}_n(E)$ l'ensemble des n arrangements de E. On pose $E = \{a_1, \dots, a_n\}$ et

$$\begin{aligned}f : S(E) &\longrightarrow \mathscr{A}_n(E)\\ \sigma &\longmapsto \big(\sigma(a_1), \dots, \sigma(a_n)\big).\end{aligned}$$

et

$$\begin{aligned}g : \mathscr{A}_n(E) &\longrightarrow S(E)\\ (b_1, \dots, b_n) &\longmapsto \left(\sigma : \begin{array}{ccc} E & \longrightarrow & E \\ a_i & \longmapsto & b_i \end{array}\right).\end{aligned}$$

f et g sont réciproques l'une de l'autre donc

$$\#S(E) = \#\mathscr{A}_n(E) = \frac{n!}{0!} = n!.$$

□

Exemple :
On pose $E = \left\{\pi, e, \sqrt{2}\right\}$. Alors,

$$S(E) = \left\{\mathrm{id}, \begin{pmatrix} \pi \mapsto e \\ e \mapsto \pi \\ \sqrt{2} \mapsto \sqrt{2} \end{pmatrix}, \dots\right\}$$

Donc,

$$f(\sigma) = \left(e, \pi, \sqrt{2}\right).$$

et alors

$$\begin{aligned} g\left(\sqrt{2},\pi,e\right) : E &\longrightarrow E \\ \pi &\longmapsto \sqrt{2} \\ e &\longmapsto \pi \\ \sqrt{2} &\longmapsto e. \end{aligned}$$

Définition : Soit E un ensemble fini et $p \in \mathbb{N}^\star$. Une p-combinaison de E est une partie de E de cardinal p.

Proposition : Soit E fini de cardinal n et $p \in \mathbb{N}^\star$. Il y a exactement $\binom{n}{p}$ parties de E de cardinal p.

Preuve :
On note $\mathscr{A}_p(E)$ l'ensemble des p-arrangements et $\mathscr{C}_p(E)$ l'ensemble des p-combinaisons de E.

Soit

$$\begin{aligned} f : \mathscr{A}_p(E) &\longrightarrow \mathscr{C}_p(E) \\ (x_1,\dots,x_p) &\longmapsto \{x_1,\dots,x_p\}. \end{aligned}$$

f est surjective et

$$\forall X \in \mathscr{C}_p(E),\ X \text{ a } p! \text{ antécédants.}$$

D'après le lemme des bergers :

$$\#\mathscr{A}_p(E) = p!\,\#\mathscr{C}_p(E)$$

et donc

$$\#\mathscr{C}_p(E) = \frac{n!}{(n-p)!\,p!} = \binom{n}{p}.$$

□

Corollaire :

$$\forall (n,p) \in \mathbb{N}^2, \binom{n}{p} \in \mathbb{N}.$$

□

Proposition : Soit E et F deux ensembles finis. Alors F^E est fini et

$$\#(F^E) = (\#F)^{\#E}.$$

Preuve :
Soit

$$\begin{aligned} \varphi : F^E &\longrightarrow F^n \\ f &\longmapsto \big(f(x_1), \dots, f(x_n)\big) \end{aligned}$$

où $E = \{x_1, \dots, x_n\}$ et $n = \#E$.

Soit

$$\begin{aligned} \psi : F^n &\longrightarrow F^E \\ (y_1, \dots, y_n) &\longmapsto \begin{array}{ccc} E & \longrightarrow & F \\ x_i & \longmapsto & y_i. \end{array} \end{aligned}$$

On a $\varphi \circ \psi = \mathrm{id}_{F^n}$ et $\psi \circ \varphi = \mathrm{id}_{F^E}$.

Donc

$$\#(F^E) = (\#F)^n.$$

□

Proposition : Soit E fini de cardinal n. Alors $\#\mathscr{P}(E) = 2^n$.

Méthode 1 Soit

$$\begin{aligned} \varphi : \mathscr{P}(E) &\longrightarrow \{0,1\}^E \\ A \longmapsto \mathbb{1}_A : & \begin{array}{ccc} E & \longrightarrow & \{0,1\} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon.} \end{cases} \end{array} \end{aligned}$$

φ est bijective :

$$\begin{aligned} \varphi^{-1} : \{0,1\}^E &\longrightarrow \mathscr{P}(E) \\ f &\longmapsto \{x \in E \mid f(x) = 1\}. \end{aligned}$$

On a donc $\#\mathscr{P}(E) = 2^n$.

Méthode 2

$$\mathscr{P}(E) = \bigcup_{p=0}^{n}{}^{\cdot} \mathscr{C}_p(E)$$

donc

$$\#\mathscr{P}(E) = \sum_{p=0}^{n} \binom{n}{p} = (1+1)^n = 2^n$$

Méthode 3 (par récurrence sur n).

— $n = 0$ donc $E = $ et $\mathscr{P}() = \{\}$. donc $\#\mathscr{P}(E) = 1 = 2^n$.

— Soit $n \in \mathbb{N}$. On suppose que

$$\forall E \text{ de cardinal } n,\ \#\mathscr{P}(E) = 2^n$$

Soit E de cardinal $n+1 > 0$. Soit $a \in E$ et $F = E \setminus \{a\}$.

— Les parties de E qui ne contienent pas a sont des parties de F et réciproquement : il y en a 2^n.

— A chaque partie de E contenant a, on peut faire correspondre une partie de F en supprimant a de la partie, et réciproquement : il y en a 2^n.

Donc,

$$\#\mathscr{P}(E) = 2^n + 2^n = 2 \times 2^n = 2^{n+1}.$$

□

Proposition :

$$\forall k \leqslant n \in \mathbb{N}, \binom{n}{k} = \binom{n}{n-k}.$$

Preuve :
Il y a autant de façons de choisir k éléments parmi n que d'en choisir $n-k$ à exclure.

Formellement :
L'application

$$\begin{aligned} f : \mathscr{C}_k(\llbracket 1, n \rrbracket) &\longrightarrow \mathscr{C}_{n-k}(\llbracket 1, n \rrbracket) \\ X &\longmapsto \llbracket 1, n \rrbracket \setminus X \end{aligned}$$

est bijective. □

Proposition :

$$\forall k \leqslant n,\ \binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}.$$

Preuve :
On pose

$$A_{n+1} = \Big\{ X \in \mathscr{C}_{k+1}\big(\,[\![1, n+1]\!]\,\big) \mid n{+}1 \in X \Big\}, B_{n+1} = \Big\{ X \in \mathscr{C}_{k+1}\big(\,[\![1, n+1]\!]\,\big) \mid n{+}1 \notin X \Big\}.$$

donc

$$\mathscr{C}_{k+1}\big(\,[\![1, n+1]\!]\,\big) = A_{n+1} \uplus B_{n+1}.$$

L'application f : $\begin{array}{ccc} A_{n+1} & \longrightarrow & \mathscr{C}_k\big(\,[\![1,n]\!]\,\big) \\ X & \longmapsto & X \setminus \{n+1\} \end{array}$ est bijective

Donc

$$B_{n+1} = \mathscr{C}_{k+1}\big(\,[\![1, n]\!]\,\big)$$

et donc

$$\begin{aligned} \binom{n+1}{k+1} &= \#A_{n+1} + \#B_{n+1} \\ &= \binom{n}{k} + \binom{n}{k+1}. \end{aligned}$$

□

Proposition : Soit $(A, +, \times)$ un anneau, $(a, b) \in A^2$ tel que $a \times b = b \times a$.
Alors

$$\forall n \in \mathbb{N}^\star, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Preuve :

Soit $n \in \mathbb{N}^\star$. On pose $a_1 = a$ et $a_2 = b$. Alors

$$\begin{aligned}
(a+b)^n &= (a_1+a_2)(a_1+a_2)\cdots(a_1+a_2) \\
&= \sum_{i_1=1}^{2} a_{i_1} \sum_{i_2=1}^{2} a_{i_2} \cdots \sum_{i_n=1}^{2} a_{i_n} \\
&= \sum_{(i_1,\dots,i_n)\in\{1,2\}^n} a_{i_1}\, a_{i_2} \cdots a_{i_n} \\
&= \sum_{k=0}^{n} \sum_{\substack{(i_1,\dots,i_n)\in\{1,2\}^n \\ \#\{j\in[\![1,n]\!]\,|\,i_j=1\}=k}} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \sum_{\substack{(i_1,\dots,i_n)\in\{1,2\}^n \\ \#\{j\in[\![1,n]\!]\,|\,i_j=1\}=k}} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.
\end{aligned}$$

□

4 Bilan

Principe des tiroirs

Soit $f : E \to F$ avec $\#E > \#F$. Alors

$$\exists x \neq y \in E,\ f(x) = f(y).$$

Soit $f : E \to F$ avec $\#E = \#F$. Alors

$$f \text{ injective} \iff f \text{ surjective} \iff f \text{ bijective.}$$

$$\#\left(\prod_{i=1}^{n} E_i\right) = \prod_{i=1}^{n} (\#E_i).$$

$$\#(E^n) = (\#E)^n.$$

Une p-liste est de la forme $(x_1, \dots, x_p) \in E^p$.

Un p-arrangement est une p-liste d'éléments de E distincts. Il y en a, avec $n = \#E$,

$$\frac{n!}{(n-p)!}.$$

Principe des bergers

Soit $f : E \to F$ telle que chaque élément $y \in F$ ait exactement k antécédants dans F. Alors,

$$\#E = k\#F.$$

Une permutation est une bijection de E dans E. Il y en a $n!$ si $\#E = n$.

Une p-combinaision de E est une partie de E de cardinal p. Il y en

a $\binom{n}{p}$ si $n = \#E$.

$\#(F^E) = (\#F)^{\#E}$.

$\#\mathcal{P}(E) = 2^{\#E}$.

Chapitre 24

Groupe symétrique

Définition : Soit $n \in \mathbb{N}^\star$.

Le groupe symétrique est noté S_n : l'ensemble des permutations de $[\![1, n]\!]$ muni de $\circ$.

$$\#S_n = n!$$

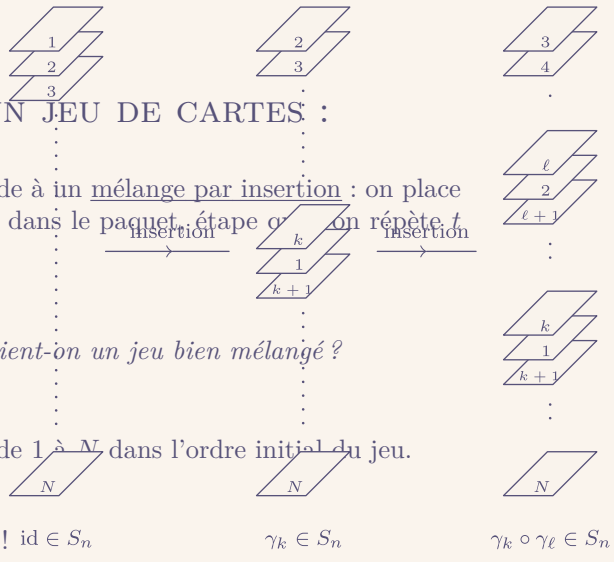
1 Mise en situation

Bon mélange d'un jeu de cartes :

Soit un jeu neuf de N cartes. On procède à un mélange par insertion : on place la carte qui est au-dessus n'importe où dans le paquet, étape que l'on répète t fois.

Pour quelles valeurs de t obtient-on un jeu bien mélangé ?

Modélisation : On numérote les cartes de 1 à N dans l'ordre initial du jeu.



On peut modéliser par un arbre le mélange dont les nœuds sont des permutations des éléments de S_N.

On dit que le jeu est bien mélangé après t insertions si chaque élément de S_N est une <u>feuille</u> de cet arbre et la probabilité d'obtenir cette permutation est $\frac{1}{N!}$.

Avec $N = 4$, on a

$$\gamma_1 = \mathrm{id} \qquad \gamma_2 = \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}2\\1\\3\\4\end{matrix}$$

$$\gamma_3 = \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}3\\1\\2\\4\end{matrix} \qquad \gamma_4 = \begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}4\\1\\2\\3\end{matrix}.$$

Avec $k = 2$ et $\ell = 1$,

$$\begin{matrix}1\\2\\3\\4\end{matrix} \xrightarrow{\gamma_2\circ} \underbrace{\begin{matrix}2\\1\\3\\4\end{matrix}}_{\gamma_2} \xrightarrow{\gamma_1\circ} \underbrace{\begin{matrix}2\\1\\3\\4\end{matrix}}_{\gamma_2}$$

Avec $k = 2$ et $\ell = 2$, on a

$$\begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}2\\1\\3\\4\end{matrix} \to \begin{matrix}1\\2\\3\\4\end{matrix}.$$

Et avec $k = 2$ et $\ell = 3$, on a

$$\begin{matrix}1\\2\\3\\4\end{matrix} \to \begin{matrix}2\\1\\3\\4\end{matrix} \to \begin{matrix}1\\3\\2\\4\end{matrix}.$$

$$\gamma_2 \circ \gamma_3 : \begin{matrix}1 \mapsto 1\\2 \mapsto 3\\3 \mapsto 2\\4 \mapsto 4\end{matrix}$$

Est-ce-que toute permutation peut s'écrire comme un produit des γ_k avec $k \in [\![1, N]\!]$?

2 Cycles

Remarque (Notation) :
Soit $\sigma \in S_n$.

$$\sigma : [\![1, N]\!] \longrightarrow [\![1, N]\!]$$
$$i \longmapsto \begin{cases} \star & \text{si } i = 1 \\ \star & \text{si } i = 2 \\ \vdots & \\ \star & \text{si } i = N. \end{cases}$$

On écrit plutôt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & N \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(N) \end{pmatrix}$$

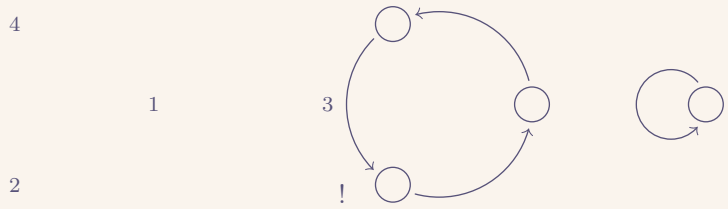
Exemple :
Avec $N = 4$, on a donc

$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\gamma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \gamma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

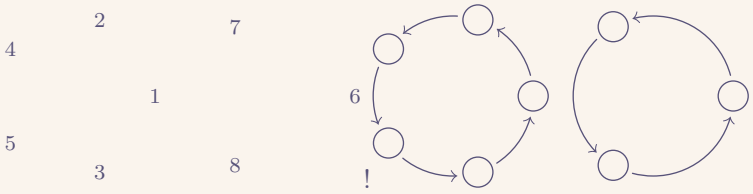
Remarque :
Avec $N = 4$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$



Avec $N = 8$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 5 & 3 & 7 & 8 & 6 \end{pmatrix}$$



Définition : Soit $\sigma \in S_N$ et $x \in [\![1, N]\!]$.

L'orbite de x pour σ est

$$\{x, \sigma(x), \sigma^2(x), \ldots\} = \{\sigma^i(x) \mid i \in \mathbb{N}\}.$$

On note l'ordre d de σ : si $\sigma \neq \mathrm{id}$, $\begin{cases}\sigma^d = \mathrm{id}, \\ \sigma^{d-1} \neq \mathrm{id}\,.\end{cases}$ L'orbite de x est

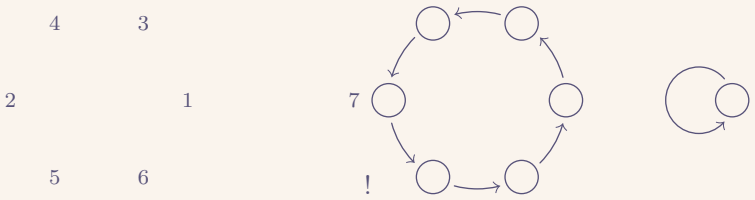
$$\{x, \sigma(x), \ldots, \sigma^{d-1}(x)\}.$$

Les orbites de σ partitionnent $[\![1, N]\!]$.

Définition : Soit $\gamma \in S_N$. On dit que γ est un k-cycle si γ a $N-k$ points fixes et les k autres éléments sont dans une même orbite.

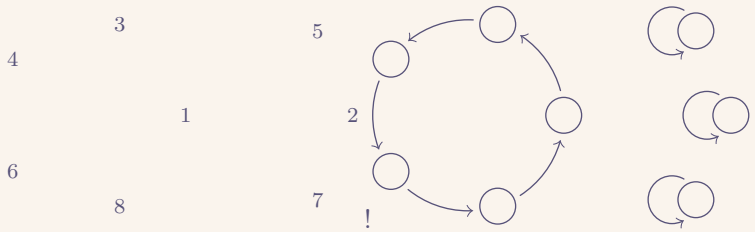
Exemple :

$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 5 & 4 & 2 & 6 & 1 & 7\end{pmatrix}$$



σ est un 6-cycle.

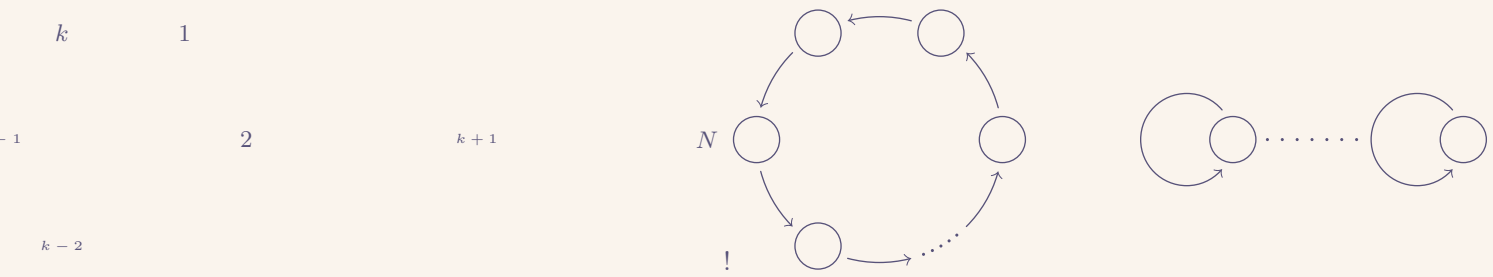
$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 3 & 2 & 4 & 6 & 5 & 8 & 7 & 1\end{pmatrix}$$



σ est un 5-cycle.

Exemple :

$$\gamma_k = \begin{pmatrix}1 & 2 & 3 & \cdots & k & k+1 & \cdots & N\\ k & 1 & 2 & \cdots & k-1 & k+1 & \cdots & N\end{pmatrix}$$



γ_k est un k-cycle.

Remarque (Notation) :
Soit γ un k-cycle tel que $\gamma(x) \neq x$. On note

$$\gamma = \begin{pmatrix} x & \gamma(x) & \gamma^2(x) & \cdots & \gamma^{k-1}(x) \end{pmatrix}.$$

Exemple :
Avec

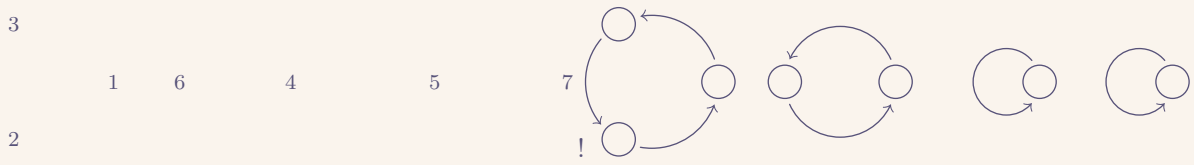
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 6 & 5 & 8 & 7 & 1 \end{pmatrix}$$

On a donc

$$\begin{aligned} \sigma &= \begin{pmatrix} 6 & 8 & 1 & 3 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 4 & 6 & 8 & 1 \end{pmatrix} \end{aligned}$$

Exemple :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix} = \sigma.$$

$$\begin{pmatrix} 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix} = \sigma.$$

Exemple :
Avec $N = 4$,

$$(1\ \ 2\ \ 3)(1\ \ 3\ \ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$(1\ \ 3\ \ 4)(1\ \ 2\ \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Définition : Soit $\sigma \in S_n$. Le support de σ est

$$\mathrm{Supp}(\sigma) = \{x \in [\![1, n]\!] \mid \sigma(x) \neq x\}.$$

Théorème : Toute permutation de S_n est une composée de cycles à supports disjoints et ces cycles sont uniques.

Exemple :

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 1 & 7 & 11 & 3 & 2 & 12 & 5 & 4 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 10 & 5 & 7 & 3 & 8 & 2 & 9 & 12 & 6 & 11 & 4 \end{pmatrix} \end{aligned}$$

Exemple :

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 8 & 2 & 1 & 6 & 3 & 7 \end{pmatrix} \\ &= (1\ \ 4\ \ 2\ \ 5)(3\ \ 8\ \ 7) \end{aligned}$$

Preuve :
Soit $\sigma \in S_n$.

Analyse On suppose que

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_p$$

où $\forall i \in [\![1, p]\!]$, γ_i est un cycle et $\forall i \neq j, \mathrm{Supp}(\gamma_i) \cap \mathrm{Supp}(\gamma_j) = .$

On pose $\gamma_1 = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}$. Donc

$$\begin{aligned}\sigma(a_1) &= \gamma_1 \circ \cdots \circ \gamma_p(a_1)\\ &= \gamma_1 \circ \cdot \circ \gamma_{p-1}(a_1)(\text{ car } a_1 \in \text{Supp}(\gamma_1) \text{ donc } a_1 \notin \text{Supp}(\gamma_p))\\ &\vdots\\ &= \gamma_1(a_1) = a_2.\end{aligned}$$

De même,

$$\sigma(a_2) = \gamma_1(a_2) = a_3$$
$$\vdots$$
$$\sigma(a_{k-1}) = \gamma_1(a_{k-1}) = a_k$$
$$\sigma(a_k) = \gamma_1(a_k) = a_1$$

De même,

$$\forall i \in [\![1, p]\!],\ \text{Supp}(\gamma_i) \text{ est un orbite de } \sigma.$$

En d'autres termes, si σ a pour orbites $O(x_1), O(x_2), \ldots, O(x_p), \{\{x_{p+1}\}, \ldots, \{x_q\}\}$ avec $x_1, \ldots, x_p \in \text{Supp}(\sigma)$ alors

$$\begin{cases}\gamma_1 = \begin{pmatrix} x_1 & \sigma(x_1) & \sigma^2(x_1) & \cdots \end{pmatrix}\\ \gamma_2 = \begin{pmatrix} x_2 & \sigma(x_2) & \sigma^2(x_2) & \cdots \end{pmatrix}\\ \quad\vdots\\ \gamma_p = \begin{pmatrix} x_p & \sigma(x_p) & \sigma^2(x_p) & \cdots \end{pmatrix}\end{cases}$$

Synthèse ok !

□

Proposition : Soit γ un k-cycle.

Alors l'ordre de γ est k :

$$\begin{cases}\gamma^k = \text{id}\\ \forall \ell \in [\![1, k-1]\!], \gamma^\ell \neq \text{id}\end{cases}$$

Preuve :

On pose $\gamma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}$ avec

$$\forall i \neq j, a_i \neq a_j.$$

Soit $\ell \in [\![1, k-1]\!]$. Alors

$$\gamma^\ell = a_{1+\ell} \neq a_1 \text{ car } 1 + \ell \leqslant k$$

donc $\gamma^\ell \neq \text{id}$.

Soit $i \in [\![1, k]\!]$. Alors

$$\gamma^k(a_i) = a_j$$

avec $\begin{cases} j \in [\![1, k]\!] \\ j \equiv i + k \ [k] \end{cases}$ donc $a_j = a_i$.

$$\forall x \notin \{a_1, \ldots, a_k\}, \gamma(x) = x$$

donc $\gamma^k(x) = x$ et donc $\gamma^k = \text{id}$. □

Proposition : Soit $\gamma = \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix}$ un k-cycle et $\sigma \in S_n$. Alors

$$\sigma\gamma\sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \cdots & \sigma(a_k) \end{pmatrix}$$

est un k-cycle.

Preuve :
Soit $x \notin \{\sigma(a_1), \ldots, \sigma(a_k)\}$. σ est bijective : soit $y \in [\![1, n]\!]$ tel que $\sigma(y) = x$.

De plus, $y \notin \{a_1, \ldots, a_k\}$.

D'où

$$\begin{aligned} \sigma\gamma\sigma^{-1} &= \sigma\gamma\sigma^{-1}\big(\sigma(y)\big) \\ &= \sigma\gamma(y) \\ &= \sigma(y) \\ &= x. \end{aligned}$$

Soit $i \in [\![1, k-1]\!]$.

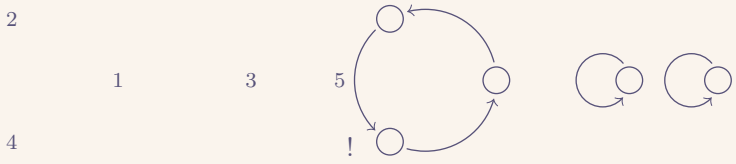
$$\begin{aligned} \sigma\gamma\sigma^{-1}\big(\sigma(a_i)\big) &= \sigma\gamma(a_i) = \sigma(a_{i+1}) \\ \sigma\gamma\sigma^{-1}\big(\sigma(a_k)\big) &= \sigma\gamma(a_k) = \sigma(a_1). \end{aligned}$$

□

3 Transpositions

Définition : Une transposition est un cycle de longueur 2 : $(a \quad b)$ avec $a \neq b$.

Exemple :
Avec $n = 5$ et $\gamma = (2 \quad 4 \quad 1)$.



$$\gamma = (1 \quad 4)(1 \quad 2)$$

Avec $n = 6$ et $\gamma = (1 \quad 3 \quad 5 \quad 6 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$.

Donc,

$$\gamma = (1 \quad 2)(1 \quad 6)(1 \quad 5)(1 \quad 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$$

Et,

$$\gamma = (1 \quad 3)(2 \quad 3)(3 \quad 5)(5 \quad 6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \\ 1 & 2 & 5 & 4 & 6 & 3 \\ 1 & 3 & 5 & 4 & 6 & 2 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$$

Exemple :

$$(1 \quad 4) = (1 \quad 2)(2 \quad 3)(3 \quad 4)(2 \quad 3)(1 \quad 2)$$

On n'a pas toujours le même nombre de transpositions mais la parité du nombre reste la même (proposition plus loin).

Théorème : Toute permutation se décompose en produit de transpositions.

Preuve :
Soit $\gamma = \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix}$ un k-cycle.

On remarque que

$$\gamma = \begin{pmatrix} a_1 & a_k \end{pmatrix} \cdots \begin{pmatrix} a_1 & a_4 \end{pmatrix} \begin{pmatrix} a_1 & a_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \end{pmatrix}$$

C'est un produit de transpositions. □

Exemple :
Avec $n = 10$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 8 & 1 & 7 & 2 & 3 & 4 & 5 & 10 & 6 \end{pmatrix}$.

On a

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 9 & 10 & 6 & 3 \end{pmatrix} \begin{pmatrix} 2 & 8 & 5 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 10 \end{pmatrix} \begin{pmatrix} 1 & 9 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 2 & 8 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix} \end{aligned}$$

Vérification :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 7 & 5 & 6 & 4 & 8 & 9 & 10 \\ 1 & 8 & 3 & 7 & 5 & 6 & 4 & 2 & 9 & 10 \\ 1 & 8 & 3 & 7 & 2 & 6 & 4 & 5 & 9 & 10 \\ 9 & 8 & 3 & 7 & 2 & 6 & 4 & 5 & 1 & 10 \\ 9 & 8 & 3 & 7 & 2 & 6 & 4 & 5 & 10 & 1 \\ 9 & 8 & 3 & 7 & 2 & 1 & 4 & 5 & 10 & 6 \\ 9 & 8 & 1 & 7 & 2 & 3 & 4 & 5 & 10 & 6 \end{pmatrix}$$

4 Signature d'une permutation

Définition : Soit $\sigma \in S_n$.

Un inversion de σ est $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$.

La signature de σ, notée $\varepsilon(\sigma)$ vaut $(-1)^k$ où k est le nombre d'inversions de σ.

Exemple :
Avec $n = 10$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 8 & 1 & 7 & 2 & 3 & 4 & 5 & 10 & 6 \end{pmatrix}$.

Les inversions de σ sont $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(1,6)$, $(1,7)$, $(1,8)$, $(1,10)$, $(2,3)$, $(2,4)$, $(2,5)$, $(2,6)$, $(2,7)$, $(2,8)$, $(2,10)$, $(4,5)$, $(4,6)$, $(4,7)$, $(4,8)$, $(4,10)$, $(9,10)$.

Donc, $\varepsilon(\sigma) = (-1)^{21} = -1$.

Proposition : Soit τ un transposition. Alors $\varepsilon(\tau) = -1$.

Preuve :
On pose $\tau = \begin{pmatrix} a & b \end{pmatrix}$ avec $a < b$.

Donc

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & a & \cdots & b & \cdots & n \\ 1 & 2 & \cdots & b & \cdots & a & \cdots & n \end{pmatrix}$$

τ a pour inversion $(a, a+1)$, $(a, a+2)$, $\ldots$, (a, b), $(a+1, b)$, $(a+2, b)$, $\ldots$, $(b-1, b)$.

Donc

$$\varepsilon(\tau) = (-1)^{b-a+b-a+1} = (-1)^{2(b-a)+1} = -1.$$

□

Théorème : $\varepsilon : (S_n, \circ) \to \big(\{-1, 1\}, \times\big)$ est un morphisme de groupes.

Preuve :
Soient $(\sigma_1, \sigma_2) \in (S_n)^2$. On a

$$\varepsilon(\sigma_1) = \prod_{i<j} \frac{\sigma_1(i) - \sigma_1(j)}{i - j}$$

donc

$$\begin{aligned}
\varepsilon(\sigma_1\sigma_2) &= \prod_{i<j} \frac{\sigma_1\sigma_2(i) - \sigma_1\sigma_2(j)}{i - j} \\
&= \prod_{i<j} \frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma_2(i) - \sigma_2(j)} \times \frac{\sigma_2(i) - \sigma_2(j)}{i - j} \\
&= \prod_{\substack{k,\ell \\ {\sigma_2}^{-1}(k)<\sigma_2)^{-1}(\ell)}} \frac{\sigma_1(k) - \sigma_1(\ell)}{k - \ell} \times \varepsilon(\sigma_2) \\
&= \prod_{i<j} \frac{\sigma_1(i) - \sigma_1(j)}{i - j} \times \varepsilon(\sigma_2) \\
&= \varepsilon(\sigma_1)\varepsilon(\sigma_2).
\end{aligned}$$

□

Définition : On dit qu'une permutation σ est paire si $\varepsilon(\sigma) = 1$, impaire si $\varepsilon(\sigma) = -1$.

Proposition–Définition : On note

$$A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}.$$

C'est un sous-groupe de S_n : on l'appelle groupe alterné.

Preuve :
$A_n = \mathrm{Ker}(\varepsilon)$ □

Exemple :
Avec

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

donc

$$\begin{aligned} \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} &= \frac{\cancel{(3-1)(2-1)(5-1)(4-1)}}{\cancel{(2-1)(3-1)(4-1)(5-1)}} \\ &\times \frac{\cancel{(2-3)(5-3)(4-3)}}{\cancel{(3-2)(4-2)(5-2)}} \\ &\times \frac{\cancel{(5-2)(4-2)}}{\cancel{(4-3)(5-3)}} \\ &\times \frac{4-5}{5-4} \\ &= -1. \end{aligned}$$

Remarque :
$\#A_n = \dfrac{n!}{2}$. En effet :

$$\begin{aligned} A_n &\longrightarrow \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} \\ \sigma &\longmapsto (1 \quad 2)\,\sigma \end{aligned}$$

est une bijection.

Exercice :
Problème :

Soit $\sigma \in S_n$. σ est-il un produit des cycles $\gamma_k = (k \quad k-1 \quad k-2 \quad \cdots \quad 1)$ avec $k \in [\![1, N]\!]$?

Avec $N = 5$ et $\gamma = \begin{pmatrix} 2 & 3 & 5 \end{pmatrix}$, $\begin{cases} \gamma_2 &= \begin{pmatrix} 1 & 2 \end{pmatrix} \\ \gamma_3 &= \begin{pmatrix} 3 & 2 & 1 \end{pmatrix} \\ \gamma_4 &= \begin{pmatrix} 4 & 3 & 2 & 1 \end{pmatrix} \\ \gamma_5 &= \begin{pmatrix} 5 & 4 & 3 & 2 & 1 \end{pmatrix} \end{cases}$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \\ 1 & 3 & 5 & 2 & 4 \\ 2 & 3 & 5 & 1 & 4 \\ 1 & 2 & 5 & 4 & 3 \\ 3 & 1 & 5 & 4 & 2 \\ 2 & 3 & 5 & 4 & 1 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \begin{matrix} \gamma_3 \\ \gamma_2 \\ \gamma_5 \\ \gamma_3 \\ \gamma_2 \\ \gamma_4 \\ \gamma_3 \\ \gamma_3 \\ \gamma_2 \end{matrix}$$

5 Bilan

$\#S_n = n!$.

$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

On dit que d est l'ordre de σ si
$\begin{cases} \sigma^d = \mathrm{id}; \\ \forall i \in [\![1, d-1]\!],\ \sigma^i \neq \mathrm{id}\,. \end{cases}$

L'orbite de σ pour $x \in [\![1, n]\!]$ est

$$\left\{ x, \sigma(x), \ldots, \sigma^{d-1}(x) \right\}$$

où d est l'ordre de σ.

On dit que σ est un k-cycle si
- σ a $n-k$ points fixes ;
- les autres éléments sont dans une même orbite.

Dans ce cas, σ est noté
$\sigma = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \cdots & \sigma^{k-1}(x) \end{pmatrix}$
et l'ordre de σ est k.

Le support de σ est l'ensemble des éléments qui "changent" après l'application de σ :
$\mathrm{Supp}(\sigma) = \left\{ x \in [\![1, n]\!] \mid \sigma(x) \neq x \right\}$.

Toute permutation peut être décomposée, de manière unique, en cycles à supports disjoints.

Soit γ un k-cycle :
$$\gamma = \begin{pmatrix} a_1 & \cdots & a_n - k \end{pmatrix}.$$
Alors, pour toute permutation σ,
$$\sigma\gamma\sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \cdots & \sigma(a_k) \end{pmatrix} I$$
et c'est un k-cycle.

Une transposition est un cycle de longueur 2.

Toute permutation se décompose en produit de transpositions mais cette décomposition n'est pas unique.

Une inversion est un couple (i, j) avec $i < j$ mais $\sigma(i) > \sigma(j)$.

La signature d'une permutation σ est $\varepsilon(\sigma) = (-1)^k$ où k est le nombre d'inversions. C'est un morphisme de groupes donc
$$\varepsilon\left(\prod_{i=1}^{N} \sigma_i\right) = \prod_{i=1}^{N} \varepsilon(\sigma_i).$$
La signature d'une transposition est -1.

Une permutation paire est une permutation de signature 1.

Une permutation impaire est une permutation de signature -1.

L'ensemble des permutations paires forment un sous-groupe : le groupe alterné.

Chapitre 25

Séries numériques

1 Défintions et premières propriétés

Définition : Soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$. La suite des sommes partielles associée à (u_n) est

$$\forall n \in \mathbb{N}, S_n = \sum_{k=0}^{n} u_k.$$

Étudier la série des (u_n), c'est étudier la convergence de la suite (S_n).

On dit que la série $\sum u_n$ converge si (S_n) converge. Dans ce cas, $\lim\limits_{n\to+\infty} S_n$ est notée $\sum\limits_{n=0}^{+\infty} u_n$ et on l'appelle la somme de la série, et la suite définie par

$$\forall n \in \mathbb{N}, R_n = \sum_{k=n+1}^{+\infty} u_k$$

est appelée suite des restes partiels.

Exemple (À connaître : série géométrique) :
Soit $q \in \mathbb{C}$.

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} q_k = \begin{cases} \dfrac{1-q^{n+1}}{1-q} & \text{si } q \neq 1 \\ n+1 & \text{si } q = 1 \end{cases}$$

Cette série converge si et seulement si $|q| < 1$, et dans ce cas $\sum\limits_{k=0}^{+\infty} q^n = \dfrac{1}{1-q}$.

Par exemple, avec $q = 1/2$, on a

$$\sum_{n=0}^{+\infty} \left(\frac{1}{2}\right)^n = \frac{1}{1-\frac{1}{2}} = 2$$

et

$$\begin{aligned} R_n &= 2 - \sum_{k=0}^{n} \left(\frac{1}{2}\right)^k \\ &= 2 - \frac{1 - \left(\frac{1}{2}\right)^{n+1}}{1 - \frac{1}{2}} \\ &= 2 - 2\left(1 - \left(\frac{1}{2}\right)^{n+1}\right) \\ &= \frac{1}{2^n} \end{aligned}$$

Proposition : Soit $(v_n) \in \mathbb{C}^{\mathbb{N}}$.
La série $\sum(v_{n+1} - v_n)$ converge si et seulement si (v_n).

Preuve :

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n}(v_{k+1} - v_k) = v_{n+1} - v_k.$$

□

Proposition : Soit $\sum u_n$ une série.
Si $\sum u_n$ converge Alors $u_n \longrightarrow 0$.

Remarque :
La réciproque est Fausse.

Contre-exemple (série harmonique) :
La série $\sum \frac{1}{n}$ diverge. En effet, on a vu en T.D. :

$$\forall n \in \mathbb{N}^\star, \sum_{k=1}^{n} \frac{1}{k} = \ln(n) + \gamma + \underset{n\to+\infty}{o}(1)$$

où γ est la constante d'Euler.

Preuve :
On pose

$$\forall n \in \mathbb{N},\ S_n = \sum_{k=0}^{n} u_k.$$

On suppose que (S_n) converge vers $S \in \mathbb{C}$. On a donc

$$\forall n \in \mathbb{N}^\star, u_n = S_n - S_{n-1} \xrightarrow[n\to+\infty]{} S - S = 0.$$

□

Remarque :
Avec les notations précédentes, si $u_n \not\longrightarrow 0$, alors $\sum u_n$ diverge. On dit qu'elle diverge grossièrement.

2 Séries à termes positifs

Proposition : Soit $(u_n) \in \left(\mathbb{R}^+\right)^{\mathbb{N}}$. Alors $\left(\sum_{k=0}^{n} u_k\right)_{n\in\mathbb{N}}$ est croissante.

Preuve :

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n+1} u_k - \sum_{k=0}^{n} u_k = u_{n+1} \geqslant 0.$$

□

Théorème : Soient u et v deux suites réelles telles que

$$\forall n \in \mathbb{N}, \boxed{0 \leqslant u_n} \leqslant v_n.$$

1. Si $\sum v_n$ converge, Alors $\sum u_n$ converge
2. Si $\sum u_n$ diverge, Alors $\sum v_n$ diverge.

Preuve : 1. On suppose que $\sum v_n$ converge. On note

$$\forall n \in \mathbb{N}, S_n(v) = \sum_{k=0}^{n} v_k.$$

Donc $\left(S_n(v)\right)$ est majorée. Soit V un majorant et $n \in \mathbb{N}$.

$$\forall k, 0 \leqslant u_k \leqslant v_k$$

donc
$$\sum_{k=0}^{n} u_k \leqslant \sum_{k=0}^{n} v_k = S_n(v) \leqslant V$$
donc $\left(\sum_{k=0}^{n} u_k\right)_{n\in\mathbb{N}}$ est majorée. Or, elle est croissante, donc elle converge.

2. C'est la contraposée du 1.

□

Contre-exemple :
$\sum \frac{1}{n}$ diverge, $\sum \frac{1}{n^2}$ converge (vers $\frac{\pi^2}{6}$) et
$$\forall n \in \mathbb{N},\ 0 \leqslant \frac{1}{n^2} \leqslant \frac{1}{n}.$$

Corollaire : Soient u, v deux suites réelles POSITIVES telles que $u = O(v)$.

1. Si $\sum v_n$ converge, alors $\sum u_n$ converge.
2. Si $\sum u_n$ diverge, alors $\sum v_n$ diverge.

□

Théorème : Soient u et v deux suites réelles POSITIVES telles que $u = o(v)$.

1. Si $\sum v_n$ converge, alors $\sum u_n$ converge.
2. Si $\sum u_n$ diverge, alors $\sum v_n$ diverge.

□

Théorème (règle des équivalents) **:** Soient u et v deux suites réelles POSITIVES telles que $u \sim v$. Alors
$$\sum u_n \text{ converge} \iff \sum v_n \text{ converge}.$$

Preuve :
On suppose
$$u_n = v_n + o(v_n)$$
et donc
$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, |u_n - v_n| \leqslant \varepsilon |v_n|$$

En particulier, on peut considerer $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, -\frac{1}{2}v_n \leqslant u_n - v_n \leqslant \frac{1}{2}v_n$$

et donc

$$\forall n \geqslant N, \frac{1}{2}v_n \leqslant u_n \leqslant \frac{3}{2}v_n$$

et donc $\begin{cases} u = O(v), \\ v = O(u). \end{cases}$

Si $\sum v_n$ converge, alors $\sum u_n$ converge car $u = O(v)$.

Si $\sum u_n$ converge, alors $\sum v_n$ converge car $v = O(u)$. □

Exemple :
Déterminer la nature de $\displaystyle\sum \frac{1}{n^3 + n\ln(n)}$ *?*

$$\forall n \geqslant 3, \frac{1}{n^3 + n\ln n} \geqslant 0.$$

et

$$\frac{1}{n^3 + n\ln n} \underset{n\to+\infty}{\sim} \frac{1}{n^3}.$$

$$\forall n \geqslant 1, \frac{1}{n^3} \leqslant \frac{1}{n^2}$$

$\sum \frac{1}{n^2}$ converge donc $\sum \frac{1}{n^3}$ converge donc $\displaystyle\sum \frac{1}{n^3 + n\ln n}$ converge.

3 Comparaison avec une intégrale

Théorème : Soit $\alpha \in \mathbb{R}$.

$$\sum \frac{1}{n^\alpha} \text{ converge } \iff \alpha > 1$$

Dans ce cas, on note

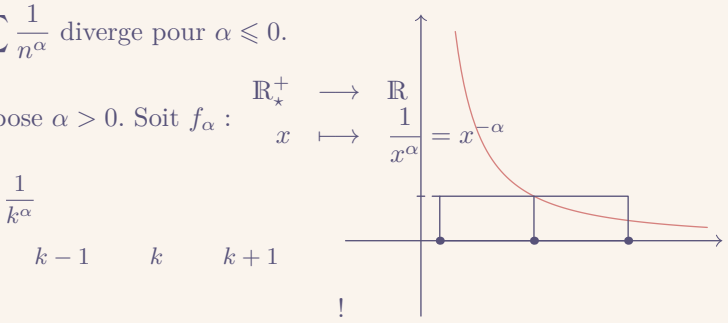
$$\zeta(\alpha) = \sum_{n=1}^{+\infty} \frac{1}{n^\alpha}.$$

Preuve :

$$\frac{1}{n^\alpha} \xrightarrow[n\to+\infty]{} \begin{cases} 0 & \text{si } \alpha > 0 \\ 1 & \text{si } \alpha = 0 \\ +\infty & \text{si } \alpha < 0 \end{cases}$$

donc $\sum \frac{1}{n^\alpha}$ diverge pour $\alpha \leqslant 0$.

On suppose $\alpha > 0$. Soit f_α : $\begin{array}{ccc} \mathbb{R}_\star^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{1}{x^\alpha} = x^{-\alpha} \end{array}$



Soit $k \in \mathbb{N}$ avec $k \geqslant 2$. comme f_α est décroissante,

$$\forall k \in [k, k+1], f_\alpha(x) \leqslant f_\alpha(k)$$

et donc

$$\int_k^{k+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leqslant \int_k^{k+1} \frac{1}{k^\alpha}\,\mathrm{d}x = \frac{1}{k^\alpha}.$$

De même,

$$\forall k \in [k-1, k], f_\alpha(x) \geqslant f_\alpha(k)$$

et donc

$$\int_{k-1}^{k} \frac{1}{x^\alpha}\,\mathrm{d}x \geqslant \int_{k-1}^{k} \frac{1}{k^\alpha}\,\mathrm{d}x = \frac{1}{k^\alpha}.$$

Soit $n \in \mathbb{N}$ avec $n \geqslant 2$.

$$\forall k \in [\![2, n]\!], \int_k^{k+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leqslant \frac{1}{k^\alpha} \leqslant \int_{k-1}^{k} \frac{1}{x^\alpha}\,\mathrm{d}x$$

donc

$$\int_2^{n+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leqslant \sum_{k=2}^{n} \frac{1}{k^\alpha} \leqslant \int_1^n \frac{1}{x^\alpha}\,\mathrm{d}x$$

Cas 1 On suppose $\alpha > 1$. Alors

$$\begin{aligned} \forall n \geqslant 2, \sum_{k=1}^{n} \frac{1}{k^\alpha} &\leqslant 1 + \int_1^n \frac{1}{x^\alpha}\,\mathrm{d}x = 1 + \left[\frac{x^{-\alpha+1}}{-\alpha+1}\right]_1^n \\ &\leqslant 1 + \frac{1}{1-\alpha}\left(\frac{1}{n^{\alpha-1}} - 1\right) \\ &\leqslant 1 + \frac{1}{\alpha-1}\left(1 - \frac{1}{n^{\alpha-1}}\right) \\ &\leqslant 1 + \frac{1}{\alpha-1}. \end{aligned}$$

La suite $\left(\sum_{k=1}^{n} \frac{1}{k^\alpha}\right)_n$ est croissante et majorée donc elle converge.

Cas 2 On suppose $\alpha = 1$.

$$\forall n \geqslant 2, \sum_{k=1}^{n} \frac{1}{k} \geqslant 1 + \int_2^{n+1} \frac{1}{x}\,\mathrm{d}x \geqslant \underbrace{1 + \ln(n+1) - \ln 2}_{\xrightarrow[n\to+\infty]{} +\infty}$$

Par comparaison, $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \xrightarrow[n\to+\infty]{} +\infty$.

Cas 3 On suppose $\alpha > 1$.

$$\begin{aligned}\forall n \geqslant 2, \sum_{k=1}^{n} \frac{1}{k^\alpha} &\geqslant 1 + \int_2^{n+1} \frac{1}{x^\alpha}\,\mathrm{d}x \\ &\geqslant 1 + \left[\frac{x^{-\alpha+1}}{-\alpha+1}\right]_2^{n+1} \\ &\geqslant \underbrace{1 + \frac{1}{1-\alpha}\left(\frac{1}{(n+1)^{\alpha-1}} - \frac{1}{2^{\alpha-1}}\right)}_{\xrightarrow[n\to+\infty]{} +\infty \text{ car } \alpha<1}\end{aligned}$$

Donc, $\displaystyle\sum_{k=1}^{n} \frac{1}{k^\alpha} \xrightarrow[n\to+\infty]{} +\infty$.

□

Théorème : Soit $f : [a, +\infty[\longrightarrow \mathbb{R}^+$ continue, décroissante de limite nulle, avec $a \in \mathbb{N}$. Alors,

$$\sum_{n\geqslant a} f(n) \text{ converge} \iff \left(\int_a^n f(x)\,\mathrm{d}x\right)_n \text{ converge.}$$

Preuve :
Soit $k \in \mathbb{N}$ tel que $k \geqslant a + 1$.

$$\forall x \in [k, k+1], f(x) \leqslant f(k)$$

donc

$$\int_k^{k+1} f(x)\,\mathrm{d}x \leqslant \int_k^{k+1} f(k)\,\mathrm{d}x = f(k)$$

et

$$\forall x \in [k-1, k], f(x) \geqslant f(k)$$

et donc

$$\int_{k-1}^{k} f(x)\,\mathrm{d}x \geqslant \int_{k-1}^{k} f(k)\,\mathrm{d}x = f(k).$$

Donc, $\forall n \in \mathbb{N}$ avec $n \geqslant a+1$

$$\int_{a+1}^{n+1} f(x)\,\mathrm{d}x \leqslant \sum_{a+1\leqslant k\leqslant n} f(k) \leqslant \int_{a}^{n} f(x)\,\mathrm{d}x.$$

Cas 1 On suppose que $\left(\int_a^n f(x)\,\mathrm{d}x\right)_n$ converge. Cette suite est croissante, donc majorée. Soit M un majorant donc

$$\forall n \geqslant a+1,\ \sum_{a\leqslant k\leqslant n} f(k) \leqslant f(a) + M.$$

donc la série converge.

— On suppose que $\left(\int_a^n f(x)\,\mathrm{d}x\right)_n$ diverge donc, par croissance de cette suire,

$$\lim_{n\to+\infty} \int_a^n f(x)\,\mathrm{d}x = +\infty$$

et donc

$$\forall n \geqslant a+1, \sum_{k=a}^{n} f(k) = f(a) + \sum_{k=a+1}^{n} f(k)$$
$$\geqslant \underbrace{f(a) + \int_a^n f(x)\,\mathrm{d}x - \int_a^{a+1} f(x)\,\mathrm{d}x}_{\xrightarrow[n\to+\infty]{} +\infty}$$

donc la série diverge.

□

Exercice :
Quelle est la nature de la série $\sum \dfrac{1}{n\ln(n)}$ *?*

Exercice :
Quelle est la nature de la série $\sum \dfrac{\ln^\alpha(n)}{n^\beta}$ *en fonction de* α *et* β *?*

4 Opérations sur les séries

Proposition : L'ensemble $E = \{u \in \mathbb{C}^{\mathbb{N}} \mid \sum u_n \text{ converge}\}$ est un sous-

espace vectoriel de $\mathbb{C}^{\mathbb{N}}$ et

$$\begin{aligned} S : E &\longrightarrow \mathbb{C} \\ u &\longmapsto \sum_{n=0}^{+\infty} u_n \end{aligned}$$

est une forme linéaire. □

Remarque :
La somme d'une série convergente et d'une série divergente diverge. Le produit d'une série divergente par un scalaire non nul diverge.

5 Séries absolument convergente

Théorème : Soit $(u_n) \in \mathbb{C}^{\mathbb{N}}$. Si $\sum |u_n|$ converge, alors $\sum u_n$ converge.

Remarque :
La réciproque est FAUSSE. On a vu en exercice que la série harmonique alternée $\sum \frac{(-1)^{n+1}}{n}$ converge vers $\ln 2$, alors que $\sum \frac{1}{n}$ diverge.

Preuve Cas 1 On suppose $u \in \mathbb{R}^{\mathbb{N}}$. On pose

$$\forall n \in \mathbb{N}, u_n^+ = \begin{cases} u_n & \text{si } u_n \geqslant 0 \\ 0 & \text{si } u_n < 0 \end{cases}$$

et

$$u_n^- = \begin{cases} -u_n & \text{si } u_n \leqslant 0 \\ 0 & \text{si } u_n > 0. \end{cases}$$

Ainsi,

$$\forall n \in \mathbb{N}, \begin{cases} u_n^+ \geqslant 0, \\ u_n^- \geqslant 0, \\ u_n = u_n^+ - u_n^-, \\ |u_n| = u_n^+ + u_n^-. \end{cases}$$

On suppose que $\sum |u_n|$ converge. Or,

$$\forall n \in \mathbb{N}, 0 \leqslant u_n^+ \leqslant u_n^+ + u_n^- = |u_n|$$

donc $\sum u_n^+$ converge. De même,

$$\forall n \in \mathbb{N}, 0 \leqslant u_n^- \leqslant u_n^- + u_n^+ = |u_n|$$

donc $\sum u_n^-$ converge. Par linéarité, $\sum u_n$ converge.

CAS 2 $u \in \mathbb{C}^{\mathbb{N}}$. On suppose que $\sum |u_n|$ converge. On pose

$$\forall n \in \mathbb{N}, \begin{cases} v_n = \mathfrak{Re}(u_n) \in \mathbb{R} \\ w_n = \mathfrak{Im}(u_n) \in \mathbb{R} \end{cases}$$

Or,

$$\forall n \in \mathbb{N}, 0 \leqslant |v_n| \leqslant |u_n|$$

donc $\sum |v_n|$ converge donc d'après le CAS 1, $\sum v_n$ converge.

De même,

$$\forall n \in \mathbb{N}, 0 \leqslant |w_n| \leqslant |u_n|$$

donc $\sum w_n$ converge.

Par linéarité, $\sum u_n$ converge.

□

Définition : Soit $u \in \mathbb{C}^{\mathbb{N}}$. On dit que $\sum u_n$ converge absolument si $\sum |u_n|$ converge. On dit que $\sum u_n$ est semi-convergente si

$$\begin{cases} \sum u_n \text{ converge,} \\ \sum |u_n| \text{ diverge.} \end{cases}$$

Corollaire : Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $v \in \left(\mathbb{R}^+\right)^{\mathbb{N}}$ telles que $u = O(v)$.

Si $\sum v_n$ converge, alors $\sum u_n$ converge absolument. □

EXEMPLE :

Quelle est la nature de la série $\displaystyle\sum_{n \geqslant 1} \frac{(-1)^n}{n^2} \sin\left(\frac{1}{n}\right)$ *?*

$$\left|\frac{(-1)^n}{n^2} \sin\left(\frac{1}{n}\right)\right| = \frac{1}{n^2} \left|\sin \frac{1}{n}\right| \sim \frac{1}{n^3}$$

donc $\displaystyle\sum \frac{(-1)^n}{n^2} \sin\left(\frac{1}{n}\right)$ converge.

EXEMPLE :

Quelle est la nature de $\displaystyle\sum (-1)^n \sin\left(\frac{1}{n}\right)$ *?*

$$\sin \frac{1}{n} = \frac{1}{n} + O\left(\frac{1}{n^2}\right)$$

donc

$$(-1)^n \sin \frac{1}{n} = \frac{(-1)^n}{n} + O\left(\frac{1}{n^2}\right).$$

$\sum O\left(\frac{1}{n^2}\right)$ converge absolument donc converge.

$\sum \frac{(-1)^n}{n}$ converge.

Par linéarité, $\sum (-1)^n \sin\frac{1}{n}$ converge.

6 Séries alternées

Théorème : Soit $u \in \left(\mathbb{R}^+\right)^{\mathbb{N}}$ décroissante de limite nulle. Alors $\sum (-1)^n u_n$ converge.

Preuve :
On pose

$$\forall n \in \mathbb{N}, S_n = \sum_{k=0}^{n} (-1)^k u_k$$

Montrons que (S_{2n}) et (S_{2n+1}) sont adjacentes.

— Soit $n \in \mathbb{N}$.

$$\begin{aligned} S_{2n+2} - S_{2n} &= (-1)^{2n+1} u_{2n+1} + (-1)^{2n+2} u_{2n+2} \\ &= u_{2n+2} - u_{2n+1} \leqslant 0 \end{aligned}$$

Donc $(S_{2n})_n$ est décroissante.

— Soit $n \in \mathbb{N}$.

$$S_{2n+3} - S_{2n+1} = u_{2n+2} - u_{2n+3} \geqslant 0$$

Donc la suite $(S_{2n+1})_n$ est croissante.

— $\forall n \in \mathbb{N}, S_{2n+1} - S_{2n} = -u_{2n+1} \xrightarrow[n\to+\infty]{} 0$.

Ainsi, (S_{2n}) et (S_{2n+1}) convergent et ont la même limite, donc (S_n) converge. On note $S = \lim\limits_{n\to+\infty} S_n$:

$$\forall n \in \mathbb{N}, S_{2n+1} \leqslant S \leqslant S_{2n}$$

donc

$$\forall n \in \mathbb{N}, R_{2n+1} \geqslant 0 \geqslant R_{2n}.$$

Soit $n \in \mathbb{N}$:

$$|R_{2n+1}| = R_{2n+1} = S - S_{2n+1} \leqslant S_{2n} - S_{2n+1} = u_{2n+1},$$

$$|R_{2n}| = -R_{2n} = S_{2n} - S \leqslant S_{2n} - S_{2n+1} \leqslant u_{2n+1} \leqslant u_{2n}.$$

Ainsi,

$$\forall n \in \mathbb{N}, |R_n| \leqslant u_n.$$

□

Proposition : Soit u une suite de signe constant telle que $\big(|u_n|\big)_n$ est décroissante de limite nulle. Alors, $\sum(-1)^n u_n$ converge et

$$\forall n \in \mathbb{N}, R_n \text{ est du signe de } (-1)^{n+1}u_{n+1} \text{ et } |R_n| \leqslant |u_n|$$

□

7 Résumé et exemples

$\sum u_n$ diverge
Comparer avec une intégrale
$v_n = O(w_n)$ $\sum w_n$ converge ?
OUI
$\sum u_n$ converge
NON
On remplace (u_n)par un équivalentplus simple
$u_n = O(v_n)$ $\sum w_n$ diverge ?
OUI
$\sum u_n$ diverge
NON
OUI
onstant à partird'un certain rang ?
NON
$\sum u_n$ converge
OUI
$\sum u_n$ alternée$(|u_n|) \searrow 0(|u_n|)$ décroissante ?
NON
$\sum |u_n|$ converge ?
OUI
$\sum u_n$ converge
NON
On forme un dévelop-pement asymptotiquede u_n
!

EXERCICE : 1. $\forall n \in \mathbb{N}^\star$, $u_n = \sqrt[n]{n+1} - \sqrt[n]{n}$,

2. $\forall n \geqslant 2$, $u_n = u_n = \ln\left(1 + \dfrac{(-1)^n}{n}\right)$,
3. $\forall n \in \mathbb{N}^\star$, $u_n = \sin\left(\dfrac{\pi}{2n}\right)$,
4. $\forall n \in \mathbb{N}^\star, u_n = \dfrac{1}{\sum_{k=1}^{n} \frac{1}{k^\alpha}}$.

1. Pour $n \in \mathbb{N}^\star$,
$$f_n : x \mapsto x^{\frac{1}{n}} = e^{\frac{1}{n}\ln x}$$
donc
$$\forall x > 0, f_n'(x) = \frac{1}{nx} e^{\frac{1}{n}\ln(x)} = \frac{1}{nx} e^{\frac{1}{n}\ln x}.$$
D'après le théorème des accroissements finis,
$$\exists c_n \in [n, n+1], f_n(n+1) - f(n) = f_n'(c_n)$$
donc
$$u_n = \frac{1}{c_n} e^{\frac{1}{n}\ln c_n}.$$

$$\forall n, 1 \leqslant \frac{c_n}{n} \leqslant 1 + \frac{1}{n}$$
donc $c_n \underset{n\to+\infty}{\sim} n$ donc $c_n = n + \mathrm{o}(n)$:
$$\begin{aligned}\ln c_n &= \ln\big(n + \mathrm{o}(n)\big)\\ &= \ln\Big(n\big(1 + \mathrm{o}(1)\big)\Big)\\ &= \ln n + \ln\big(1 + \mathrm{o}(1)\big)\\ &= \ln(n) + \mathrm{o}(1)\\ &\sim \ln n\end{aligned}$$
donc $\dfrac{\ln c_n}{n} \sim \dfrac{\ln n}{n} \xrightarrow[n\to+\infty]{} 0$
donc $e^{\frac{1}{n}\ln c_n} \underset{n\to+\infty}{\sim} 1$
donc $u_n \sim \dfrac{1}{n^2}$
donc $\sum u_n$ converve.
2. $$\forall n \geqslant 2, u_n = \frac{(-1)^n}{n} + O\left(\frac{1}{n^2}\right)$$
$\sum \dfrac{(-1)^n}{n}$ converge et $\sum O\left(\dfrac{1}{n^2}\right)$ converge absolument. Donc, $\sum u_n$ converge.
3. $u_n \underset{n\to+\infty}{\sim} \dfrac{\pi}{2n} \geqslant 0$ donc $\sum u_n$ diverge.
4. $$\lim_{n\to+\infty} \sum_{k=1}^{n} \frac{1}{k^\alpha} = \begin{cases} \underbrace{\zeta(\alpha)}_{>0} & \text{si } \alpha > 1,\\ +\infty & \text{si } \alpha \leqslant 1,\end{cases}$$

donc

$$u_n \longrightarrow \begin{cases} \dfrac{1}{\zeta(\alpha)} \neq 0 & \text{si } \alpha > 1, \\ 0 & \text{si } \alpha \leqslant 1 \end{cases}$$

Si $\alpha > 1$, alors $\sum u_n$ diverge. On suppose $\alpha \leqslant 1$.

Équivalent de $\displaystyle\sum_{k=1}^{n} \frac{1}{k^\alpha}$?

Si $\alpha < 1$,

$$\underbrace{\frac{1}{1-\alpha}\left((n+1)^{1-\alpha} - 2^{1-\alpha}\right)}_{\frac{n^{1-\alpha}}{1-\alpha}} = \int_2^{n+1} \frac{1}{x^\alpha}\,\mathrm{d}x \leqslant \sum_{k=2}^{n} \frac{1}{k^\alpha} \leqslant \int_1^n \frac{1}{x^\alpha}\,\mathrm{d}x = \underbrace{\frac{1}{1-\alpha}\left(n^{1-\alpha} - 1\right)}_{\sim \frac{n^{1-\alpha}}{1-\alpha}}$$

donc

$$\sum_{k=1}^{n} \frac{1}{k^\alpha} \sim \frac{n^{1-\alpha}}{1-\alpha}$$

donc

$$u_n \sim \frac{1-\alpha}{n^{1-\alpha}}$$

$$\begin{aligned} \textstyle\sum u_n \text{ converge} &\iff 1-\alpha > 1 \\ &\iff \alpha < 0 \end{aligned}$$

Si $\alpha = 1$, $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \sim \ln n$ et donc $u_n \sim \dfrac{1}{\ln n}$.

A-t-on $u_n = \mathrm{o}\left(\dfrac{1}{n^\beta}\right)$ avec $\beta > 1$ ou $\dfrac{1}{n^\beta} = \mathrm{o}(u_n)$ avec $\beta \leqslant 1$?

Si $\beta \geqslant 0$,

$$n^\beta u_n \sim \frac{n^\beta}{\ln(n)} \longrightarrow +\infty$$

En particulier avec $\beta = \dfrac{1}{2}$:

$$\frac{1}{n^{\frac{1}{2}}} = \mathrm{o}(u_n)$$

et $\displaystyle\sum \frac{1}{n^{\frac{1}{2}}}$ diverge car $\dfrac{1}{2} < 1$. Donc, $\sum u_n$ diverge.

On a donc

— avec $\alpha \leqslant 0$, $\sum u_n$ converge,
— avec $\alpha > 0$, $\sum u_n$ diverge.

8 Applications

8.1 Formule de Stirling

Proposition : On a :

$$n! \underset{n\to+\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{e}\right)^n ?.$$

Preuve :

$$\forall n \in \mathbb{N}^\star, \ln(n!) = \sum_{k=1}^{n} \ln k.$$

$x \mapsto \ln x$ est strictement croissante sur $[1, +\infty[$ donc

$$\forall k \in \mathbb{N}^\star, \forall x \in [k, k+1], \ln x \geqslant \ln k$$

donc

$$\forall k \in \mathbb{N}^\star, \int_k^{k+1} \ln x \, \mathrm{d}x \geqslant \int_k^{k+1} \ln k \, \mathrm{d}x = \ln k$$

et

$$\forall k \geqslant 2, \forall x \in [k-1, k], \ln x \leqslant \ln k$$

et docn

$$\forall k \geqslant 2, \int_{k-1}^{k} \ln x \, \mathrm{d}x \leqslant \int_{k-1}^{k} \ln k \, \mathrm{d}x = \ln k$$

Ainsi

$$\forall n \geqslant 2, \int_1^n \ln x \, \mathrm{d}x \geqslant \sum_{k=2}^{n} \leqslant \int_2^{n+1} \ln x \, \mathrm{d}x$$

Or

$$\begin{aligned}
\forall n \geqslant 2, \int_1^n \ln x \, \mathrm{d}x &= [x \ln x]_0^n \\
&= n\ln(n) - n + 1 \\
&\underset{n\to+\infty}{\sim} n \ln n \\
\int_2^{n+1} \ln x \, \mathrm{d}x &= (n+1)\ln(n+1) - (n+1) - 2\ln(2) + 2 \\
&\underset{n\to+\infty}{\sim} (n+1)\ln(n+1) \\
&\underset{n\to+\infty}{\sim} n \ln n
\end{aligned}$$

car

$$\begin{aligned}\ln(n+1) &= \ln\left(n\left(1+\frac{1}{n}\right)\right)\\ &= \ln n + \ln\left(1+\frac{1}{n}\right)\\ &= \ln n + \frac{1}{n} + o\left(\frac{1}{n}\right)\\ &\sim \ln n\end{aligned}$$

Donc

$$\ln(n!)) \underset{n\to+\infty}{\sim} n\ln n$$

Cependant, on a un problème :

$$\ln(n!) = n\ln n + o(n\ln n)$$
$$\text{donc } n! = n^n \underbrace{e^{o(n\ln n)}}_{?}$$

On pose

$$\forall n \in \mathbb{N}^\star, u_n = \ln(n!) - n\ln n$$

(u_n) a même nature que $\sum(u_{n+1}-u_n)$ et

$$\begin{aligned}\forall n \in \mathbb{N}^\star, u_{n+1}-u_n &= \ln\left(\frac{(n+1)!}{n!}\right) - (n+1)\ln(n+1) + n\ln n\\ &= n\big(\ln n - \ln(n+1)\big)\\ &= n\ln\left(\frac{n}{n+1}\right)\\ &= n\ln\left(1-\frac{1}{n+1}\right)\\ &\sim -\frac{n}{n+1} \sim -1 < 0\end{aligned}$$

$\sum(-1)$ diverge donc (u_n) diverge.

Conjecture

$$u_n = \sum_{k=1}^{n-1}(u_{k+1}-u_k) \underbrace{\sim}_{\downarrow} \sum_{k=1}^{n-1}(-1) = -(n-1) \sim -n$$

On n'a absolument pas le droit !

On pose

$$\forall n \in \mathbb{N}^\star, v_n = u_n + n$$

et donc

$$\begin{aligned}\forall n\in\mathbb{N}^\star, v_{n+1}-v_n &= n\ln\left(1-\frac{1}{n+1}\right)+1\\ &= n\left(-\frac{1}{n+1}-\frac{1}{2(n+1)^2}+o\left(\left(\frac{1}{n+1}\right)^2\right)\right)+1\\ &= n\left(-\frac{1}{n\left(1+\frac{1}{n}\right)}-\frac{1}{2n^2\left(1+\frac{1}{n^2}\right)}+o\left(\frac{1}{n^2}\right)\right)+1\\ &= -\left(\frac{1}{1+\frac{1}{n}}-\frac{1}{2n}\times\frac{1}{\left(1+\frac{1}{n}\right)^2}+o\left(\frac{1}{n}\right)\right)\\ &= -\left(1-\frac{1}{n}+\frac{1}{2n}+o\left(\frac{1}{n}\right)\right)+1\\ &= \frac{1}{2n}+o\left(\frac{1}{n}\right)\\ &\sim \frac{1}{2n}>0.\end{aligned}$$

$$v_n\sim\sum_{k=1}^{n-1}(v_{k-1}-v_k)\sim\sum_{k=1}^{n-1}\frac{1}{2k}\sim\frac{1}{2}\ln(n)$$

On pose

$$\forall n\in\mathbb{N}^\star, w_n=v_n-\frac{1}{2}\ln n$$

et donc

$$\begin{aligned}\forall n\in\mathbb{N}^\star, w_{n+1}-w_n &= n\ln\left(1+\frac{1}{n+1}\right)-\frac{1}{2}\ln(n+1)+\frac{1}{2}\ln(n)+1\\ &= n\left(-\frac{1}{n+1}-\frac{1}{2(n+1)^2}-\frac{1}{3(n+1)^3}+o\left(\frac{1}{(n+1)^3}\right)\right)\\ &\quad+1+\frac{1}{2}\ln\left(1-\frac{1}{n+1}\right)\\ &= -1-\frac{1}{2(n+1)}-\frac{1}{3(n+1)^2}+o\left(\frac{1}{(n+1)^2}\right)\\ &\quad+\frac{1}{n+1}+\frac{1}{2(n+1)^2}+1\\ &\quad+\frac{1}{2}\left(-\frac{1}{n+1}-\frac{1}{2(n+1)^2}+o\left(\frac{1}{(n+1)^2}\right)\right) \qquad \sim -\frac{1}{12(n+1)^2}\\ &\sim -\frac{1}{12n^2}<0\end{aligned}$$

donc $\sum(w_{n+1}-w_n)$ converge et donc (w_n) converge.

On pose $\ell = \lim\limits_{n\to+\infty} w_n$. Ainsi,

$$\forall n \in \mathbb{N}^\star, w_n = \ell + o(1)$$

et donc

$$\forall n \in \mathbb{N}^\star, \ln(n!) = n\ln n - n + \frac{1}{2}\ln(n) + \ell + o(1)$$

et alors

$$\begin{aligned}\forall n \in \mathbb{N}^\star, n! &= n^n e^{-n}\sqrt{n}e^{\ell}\underbrace{e^{o(1)}}_{\xrightarrow[n\to+\infty]{}1}\\ &\sim \left(\frac{n}{e}\right)^n \sqrt{n} \times K\end{aligned}$$

avec $K = e^{\ell}$.

On pose

$$\forall n \in \mathbb{N}^\star, I_n = \int_0^{\frac{\pi}{2}} \sin^n x \, \mathrm{d}x \sim \sqrt{\frac{\pi}{2n}}$$

et (c.f. TD5 / Exercice 8)

$$I_{2n} = \frac{(2n)!}{\left(2^n n!\right)^2} \times \frac{\pi}{2}.$$

$$\begin{aligned}I_{2n} &\sim \frac{\pi}{2}\cancel{\left(\frac{2n}{2e}\right)^{2n}}\sqrt{2n}K\cancel{\left(\frac{e}{n}\right)^{2n}}\frac{1}{n} \times \frac{1}{K^2}\\ &\sim \frac{\pi}{K\sqrt{2n}}.\end{aligned}$$

Or

$$I_{2n} \sim \sqrt{\frac{\pi}{4n}}.$$

Donc

$$\frac{\sqrt{\frac{\pi}{4n}}}{\frac{\pi}{K\sqrt{2n}}} \xrightarrow[n\to+\infty]{} 1$$

donc

$$\frac{K}{\sqrt{2\pi}} \xrightarrow[n\to+\infty]{} 1$$

et donc $K = \sqrt{2\pi}$. □

8.2 Développement décimal

Exemple : — Avec $x = 0,54\underline{54}\ldots$, que vaut $2x$?

— Avec $x = 0,333\underline{3}\ldots$, que vaut $3x$?

— $0.999\underline{9}\ldots$?

— $3 \times \frac{1}{3} = 1$?

Proposition : Soit $(a_n)_{n\in\mathbb{N}}$ telle que

$$\begin{cases} a_0 \in \mathbb{Z}, \\ \forall n \geqslant 1, a_n \in [\![0,9]\!] \end{cases}$$

La série $\sum \frac{a_n}{10^n}$ converge.

Preuve :

$$\forall n \geqslant 1, 0 \leqslant \frac{a_n}{10^n} \leqslant \frac{9}{10^n}$$

$\sum \frac{1}{10^n}$ converge car $\frac{1}{10} \in [0,1[$. Donc $\sum_{n\geqslant 1} \frac{a_n}{10^n}$ converge donc $\sum_{n\geqslant 1} \frac{a_n}{10^n}$ converge. □

Définition : Soit $x \in \mathbb{R}$. On dit que x admet un <u>développement décimal</u> si

$$\exists a_0 \in \mathbb{Z}, (a_n)_{n\geqslant 1} \in [\![0,9]\!]^N, x = \sum_{n=0}^{+\infty} \frac{a_n}{10^n}.$$

Théorème : Tou réel $x \in [0,1[$ admet un développement décimal :

$$x = \sum_{n=1}^{+\infty} \frac{\lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor}{10^n}$$

Preuve :

$$\begin{aligned} \forall n \geqslant 1, \quad & 10^n x - 1 < \lfloor 10^n x \rfloor \leqslant 10^n x \\ & -10^n x + 10 > -10 \lfloor 10^{n-1} x \rfloor \geqslant -10^n x \end{aligned}$$

donc

$$-1 < \lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor < 10$$

et donc

$$\lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor \in [\![0,9]\!].$$

De plus,

$$\begin{aligned}\sum_{k=1}^{n}\frac{\lfloor 10^k x\rfloor - 10\lfloor 10^{k-1}x\rfloor}{10^k} &= \sum_{k=1}^{n}\left(\frac{\lfloor 10^k x\rfloor}{10^k} - \frac{\lfloor 10^{k-1}x\rfloor}{10^{k-1}}\right)\\ &= \frac{\lfloor 10^n x\rfloor}{10^n} - \underbrace{\lfloor x\rfloor}_{=0}\\ &\xrightarrow[n\to+\infty]{} x.\end{aligned}$$

□

Théorème : Soit $x \in]0,1[$.

1. Si x n'est pas décimal (i.e. on ne peut pas l'écrire comme $p/10^n$ avec $p \in \mathbb{Z}$ et $n \in \mathbb{N}$), alors x a un unique développement décimal.
2. Si x est décimal, alors x a exactement 2 développements décimaux :
   — il y en a un où, à partir d'un certain rang, tous les chiffres sont nuls,
   — et un autre où tous les chiffres sont égaux à 9 à parir d'un certain rang.

Preuve :
Soit $(a_n)_{n\geqslant 1} \in [\![0,9]\!]^{\mathbb{N}^\star}$ et $(b_n)_{n\geqslant 1} \in [\![0,9]\!]^{\mathbb{N}^\star}$ telles que

$$x = \sum_{n=1}^{+\infty}\frac{a_n}{10^n} = \sum_{n=1}^{+\infty}\frac{b_n}{10^n}$$

On pose $n_0 = \min\{n \in \mathbb{N}^\star \mid a_n \neq b_n\}$:

$$\begin{cases}\forall n < n_0, a_n = b_n,\\ a_{n_0} \neq b_{n_0}.\end{cases}$$

Sans perte de généralité, on suppose $a_{n_0} < b_{n_0}$. On a donc

$$0 < \frac{b_{n_0} - a_{n_0}}{10^{n_0}} = \sum_{n=n_0+1}^{+\infty}\frac{a_n - b_n}{10^n}$$

$$\forall n \geqslant n_0, \begin{cases}0 \leqslant a_n \leqslant 9\\ 0 \leqslant b_n \leqslant 9\end{cases}$$

donc

$$\forall n \geqslant n_0, -9 \leqslant a_n - b_n \leqslant 9$$

donc

$$-9\sum_{n=n_0+1}^{+\infty}\frac{1}{10^n} \leqslant \sum_{n=n_0+1}^{+\infty}\frac{a_n-b_n}{10^n} \leqslant 9\sum_{n=1}^{+\infty}\frac{1}{10^n}.$$

Or,

$$\begin{aligned}\sum_{n=n_0+1}^{+\infty}\frac{1}{10^n} &= \frac{1}{10^{n_0+1}}\sum_{n=0}^{+\infty}\frac{1}{10^n}\\ &= \frac{1}{10^{n_0+1}}\times\frac{1}{1-\frac{1}{10}}\\ &= \frac{1}{9\times 10^{n_0}}\end{aligned}$$

D'où,

$$0 < \frac{b_{n_0}-a_{n_0}}{10^{n_0}} \leqslant \frac{1}{10^{n_0}}$$

donc

$$0 < \underbrace{b_{n_0}-a_{n_0}}_{\in\mathbb{Z}} \leqslant 1$$

donc $b_{n_0} - a_{n_0} = 1$ et donc

$$\sum_{n=n_0+1}^{+\infty}\frac{a_n-b_n}{10^n} = \frac{1}{10^{n_0}}$$

donc

$$\forall n > n_0, a_n - b_n = 9$$

et donc

$$\forall n > n_0, \begin{cases} a_n = 9\\ b_n = 0\end{cases}$$

Comme

$$\forall n > n_0, b_n = 0$$

x est décimal et les deux développements de x sont alors

$$\begin{aligned}x &= 0, a_1 \dots a_{n_0-1}a_{n_0}\underline{9}\dots\\ &= 0, a_1 \dots a_{n_0-1}(a_{n_0}+1)\underline{0}\dots\end{aligned}$$

□

Remarque :
Avec $x = 0{,}5\underline{454}\dots$, $100x = 54{,}5\underline{454}\dots = 54 + x$. On a donc $x = \dfrac{54}{99}$.

Avec $x = 0{,}987\,123\,\underline{123}\ldots$, on a

$$\begin{aligned} x &= \frac{987}{1000} + 0{,}000\,\underline{123}\ldots \\ &= \frac{987}{1000} + \frac{1}{10^3}\underbrace{(0{,}\underline{123}\ldots)}_{y} \end{aligned}$$

On a $1000y = 123 + y$ et donc $y = \dfrac{123}{999}$ et donc $x = \dfrac{987 + \frac{123}{999}}{1000}$.

8.3 Exponentielle

Proposition :

$$\forall x \in \mathbb{R},\ \sum_{n=0}^{+\infty} \frac{x^n}{n!} = e^x$$

Preuve :
(formule de Taylor avec reste intégral)

$$e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + \int_0^x e^t \frac{(x-t)^n}{n}\ \mathrm{d}t$$

$$\begin{aligned} \left| e^x - \sum_{k=0}^{n} \frac{x^k}{k!} \right| &\leqslant \int_0^x e^t \frac{|x-t|^n}{n!}\ \mathrm{d}t \\ &\leqslant \int_0^x e^x \frac{(x-t)^n}{n!}\ \mathrm{d}t \\ &\leqslant e^x \left[-\frac{(x-t)^{n+1}}{(n+1)!} \right]_0^x \\ &\leqslant e^x \frac{x^{n+1}}{(n+1)!} \xrightarrow[n\to+\infty]{} 0 \end{aligned}$$

car

Méthode 1

$$\begin{aligned} \frac{x^n}{n!} \sim \frac{x^n}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} &= \frac{1}{\sqrt{2\pi n}}\left(\frac{ex}{n}\right)^n \\ &= \frac{1}{\sqrt{2\pi n}} e^{n\ln\left(\frac{ex}{n}\right)} \xrightarrow[n\to+\infty]{} 0 \end{aligned}$$

Méthode 2

$$\frac{\frac{x^{n+1}}{(n+1)!}}{\frac{x^n}{n!}} = \frac{x}{n+1} \xrightarrow[n\to+\infty]{} 0 < 1.$$

□

Proposition :

$$\forall z \in \mathbb{C},\ \sum_{n=0}^{+\infty} \frac{z^n}{n!} = e^z$$

□

Chapitre 26

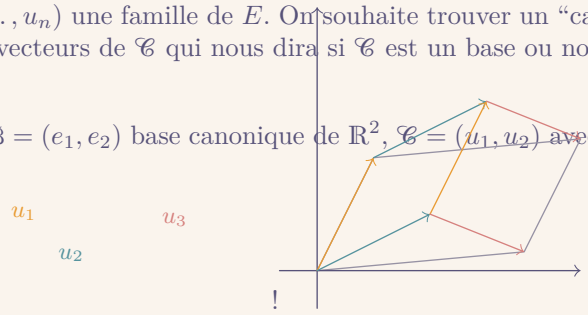
Déterminant

1 Motivation

Soit E un espace vectoriel de dimension n, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E.

Soit $\mathscr{C} = (u_1, \dots, u_n)$ une famille de E. On souhaite trouver un "calcul" sur les coordonées des vecteurs de $\mathscr{C}$ qui nous dira si $\mathscr{C}$ est un base ou non de E.

Exemple :
Avec $E = \mathbb{R}^2$, $\mathscr{B} = (e_1, e_2)$ base canonique de $\mathbb{R}^2$, $\mathscr{C} = (u_1, u_2)$ avec $u_1 = (x, y)$ et $u_2 = (x', y')$.



On note A l'aire orientée (ou algébrique) du parallélogramme engendré par u_1 et u_2.

Cette aire vérifie :

$$\begin{cases} A(u_1 + u_3, u_2) = A(u_1, u_2) + A(u_3, u_2) \\ A(\lambda u_1, u_2) = \lambda A(u_1, u_2) \\ A(u_2, u_1) = -A(u_1, u_2) \\ A(e_1, e_2) = 1 \end{cases}$$

$$\begin{aligned} A(u_1, u_2) &= A(xe_1 + ye_2, u_2) \\ &= xA(e_1, u_2) + yA(e_2, u_2) \\ &= xA(e_1, x'e_1 + y'e_2) + yA(e_2, x'e_1 + y'e_2) \\ &= xx'A(e_1, e_1) + xy'A(e_1, e_2) + yx'A(e_2, e_1) + yy'A(e_2, e_2) \\ &= xy' - yx' \end{aligned}$$

$$(u_1, u_2) \text{ base de } \mathbb{R}^2 \iff xy' - yx' \neq 0$$

REMARQUE :

$$\mathrm{Mat}_{\mathscr{B}}(\mathscr{C}) = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$$

EXEMPLE :
$E = \mathbb{R}^3$, (e_1, e_2, e_3) base canonique, $\mathscr{C} = (u_1, u_2, u_3)$ famille de E.

Soit V le volume algébrique du parallélépipède orienté engendré par u_1, u_2 et u_3.

V est trilinéaire et

$$\begin{cases} V(u_2, u_1, u_3) = -V(u_1, u_2, u_3) \\ V(u_3, u_1, u_2) = V(u_1, u_2, u_3) \\ V(e_1, e_2, e_3) = 1 \end{cases}$$

$$\text{On pose } \begin{cases} u_1 = (x_1, y_1, z_1) \\ u_2 = (x_2, y_2, z_2) \\ u_3 = (x_3, y_3, z_3). \end{cases}$$

$$\begin{aligned} V(u_1, u_2, u_3) &= V(x_1e_1 + y_1e_2 + z_1e_3, u_2, u_3) \\ &= x_1V(e_1, u_2, u_3) + y_1V(e_2, u_2, u_3) + z_1V(e_3, u_2, u_3) \\ &= \quad x_1y_2z_3V(e_1, e_2, e_3) + x_1z_2y_3V(e_1, e_3, e_2) + y_1x_2z_3V(e_2, e_1, e_3) \\ &\quad + y_1z_2x_3V(e_2, e_3, e_1) + z_1x_2y_3V(e_3, e_1, e_2) + z_1y_2x_3V(e_3, e_2, e_1) \\ &= x_1y_2z_3 + y_1z_2x_3 + z_1x_2y_3 - x_1z_2y_3 - y_1x_2z_3 - z_1y_2x_3 \end{aligned}$$

C'est la formule de Sarrus (hors-programme).

2 Définitions

Définition : Soit E un $\mathbb{K}$-espace vectoriel de dimension $n < +\infty$ et $f : E^n \longrightarrow \mathbb{K}$. On dit que f est multilinéaire si

$$\forall i \in [\![1, n]\!], \forall (u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n) \in E^{n-1},$$

l'application $\begin{array}{ccc} E & \longrightarrow & \mathbb{K} \\ u & \longmapsto & f(u_1, \ldots, u_{i-1}, u, u_{i+1}, \ldots, u_n) \end{array}$ est linéaire.

On dit que f est antisymétrique si

$$\begin{gathered}\forall i<j, \forall (u_1,\dots,u_n)\in E^n,\\ f(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_{j-1},u_i,u_{j+1},\dots,u_n)\\ =-f(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_{j-1},u_j,u_{j+1},\dots,u_n).\end{gathered}$$

On dit que f est alternée si

$$\forall (u_1,\dots,u_n)\in E^n, \big(\exists i<j, u_i=u_j \implies f(u_1,\dots,u_n)=0\big).$$

Proposition : Soit $\mathbb{K}$ un corps tel que $1+1\neq 0$, E un $\mathbb{K}$-espace vectoriel de dimension n et $f : E^n \to \mathbb{K}$ une forme multilinéaire.

Alors,

$$f \text{ alternée} \iff f \text{ antisymétrique}.$$

Preuve " $\implies$ " On suppose f alternée.

Soit $(u_1,\dots,u_n)\in E^n$ et $(i,j)\in [\![1,n]\!]^2$ avec $i<j$.

$$\begin{aligned}0 &= f(u_1,\dots,u_{i-1},u_i+u_j,u_{i+1},\dots,u_{j-1},u_i+u_j,u_{j+1},\dots,u_n)\\ &= f(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_{j-1},u_i+u_j,u_{j+1},\dots,u_n)\\ &\quad + f(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_{j-1},u_i+u_j,u_{j+1},\dots,u_n)\\ &= f(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_{j-1},u_i,u_{j+1},\dots,u_n)\\ &\quad + f(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_{j-1},u_j,u_{j+1},\dots,u_n)\\ &\quad + f(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_{j-1},u_i,u_{j+1},\dots,u_n)\\ &\quad + f(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_{j-1},u_j,u_{j+1},\dots,u_n)\end{aligned}$$

donc

$$\begin{aligned}&f(u_1,\dots,u_{i-1},u_j,u_{i+1},u_{i+1},\dots,u_{j-1},u_i,u_{j+1},\dots,u_n)\\ &=-f(u_1,\dots,u_{i-1},u_i,u_{i+1},u_{i+1},\dots,u_{j-1},u_j,u_{j+1},\dots,u_n).\end{aligned}$$

Donc, f est antisymétrique.

" $\impliedby$ " On suppose f antisymétrique. Soit $(u_1,\dots,u_n)\in E^n$ et $(i,j)\in [\![1,n]\!]^2$ tels que $i<j$ et $u_i<u_j$.

$$\begin{aligned} & f(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_{j-1},u_j,u_{j+1},\dots,u_n) \\ =& f(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_{j-1},u_i,u_{j+1},\dots,u_n) \\ =& -f(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_{j-1},u_j,u_{j+1},\dots,u_n) \end{aligned}$$

D'où,

$$f(u_1,\dots,u_n)\underbrace{(1+1)}_{\neq 0}=0$$

donc $f(u_1,\dots,u_n)=0$.

□

Dans le reste du chapitre, $\mathbb{K}$ est un corps avec $1+1\neq 0$.

Théorème : Soit E un $\mathbb{K}$-espace vectoriel de dimension n. L'ensemble des formes multilinéaires alternées de E est un sous-espace vectoriel de $\mathbb{K}^{(E^n)}$ de dimension 1.

Preuve (pas exigible) *:*
Soit $\mathcal{B}=(e_1,\dots,e_n)$ une base de E. Soit f une forme multilinéaire alternée.
Soit $(u_1,\dots,u_n)\in E^n$.

$$\forall j\in[\![1,n]\!],\ \exists (a_{i,j})_{1\leqslant i\leqslant n},\ u_j=\sum_{i=1}^{n}a_{i,j}e_i$$

$$\begin{aligned}
f(u_1,\dots,u_n) &= f\left(\sum_{i=1}^{n} a_{i,1}e_i, u_2,\dots,u_n\right)\\
&= \sum_{i=1}^{n} a_{i,1} f(e_i,u_2,\dots,u_n)\\
&= \sum_{i_1=1}^{n} a_{i_1,1} f\left(e_{i_1}, \sum_{i_2=1}^{n} a_{i_2,2}e_{i_2}, u_3,\dots,u_n\right)\\
&= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} a_{i_1,1}a_{i_2,2}, f(e_{i_1},e_{i_2},u_3,\dots,u_n)\\
&\vdots\\
&= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n} a_{i_1,1}a_{i_2,2}\cdots a_{i_n,n} f(e_{i_1},e_{i_2},\dots,e_{i_n})\\
&= \sum_{\sigma\in S_n} a_{\sigma(1),1}a_{\sigma(2),2}\cdots a_{\sigma(n),n} f(e_{\sigma(1)},e_{\sigma(2)},\dots,e_{\sigma(n)})\\
&= \underbrace{\sum_{\sigma\in S_n}\left(\varepsilon(\sigma)\prod_{j=1}^{n} a_{\sigma(j),j}\right)}_{A(u_1,\dots,u_n)} \underbrace{f(e_1,\dots,e_n)}_{\in\mathbb{K}}
\end{aligned}$$

D'où, $f = f(e_1,\dots,e_n)\ A$.

Donc, l'ensemble des formes multilinéaires alternées est $\mathrm{Vect}(A)$. De plus,

$$\begin{aligned}
A(e_1,\dots,e_n) &= \sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^{n}\delta_{\sigma(j),j}\\
&= \varepsilon(\mathrm{id})\prod_{j=1}^{n} 1 = 1 \neq 0.
\end{aligned}$$

□

Définition : Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathcal{B} = (e_1,\dots,e_n)$ une base de E.

Il existe une unique forme f multilinéaire alternée sur E telle que

$f(e_1, \dots, e_n) = 1$. Elle est donnée par la formule

$$\forall (u_1, \dots, u_n) \in E^n, f(u_1, \dots, u_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j}$$

où

$$\forall i, j,\ a_{i,j} \text{ est la } i\text{-ème coordonnée de } u_j \text{ dans la base } \mathscr{B}.$$

Cette application est appelée déterminant dans la base $\mathscr{B}$ et noté $\det_{\mathscr{B}}$.

Proposition : Soient $\mathscr{B} = (e_1, \dots, e_n)$ et $\mathscr{C} = (u_1, \dots, u_n)$ deux bases de E. Alors

$$\det_{\mathscr{C}} = \det_{\mathscr{C}}(e_1, \dots, e_n)\ \det_{\mathscr{B}}$$

i.e.

$$\forall (v_1, \dots, v_n) \in E^n, \det_{\mathscr{C}}(v_1, \dots, v_n) = \det_{\mathscr{C}}(e_1, \dots, e_n)\ \det_{\mathscr{B}}(v_1, \dots, v_n).$$

Preuve :
On sait que $\det_{\mathscr{B}}$ et $\det_{\mathscr{C}}$ sont colinéaires :

$$\exists \lambda \in \mathbb{K},\ \forall (v_1, \dots, v_n) \in E^n,\ \det_{\mathscr{C}}(v_1, \dots, v_n) = \lambda \det_{\mathscr{B}}(v_1, \dots, v_n).$$

En particulier,

$$\det_{\mathscr{C}}(e_1, \dots, e_n) = \lambda \det_{\mathscr{B}}(e_1, \dots, e_n) = \lambda.$$

□

Remarque (notation) :
Avec les notations précédentes, on note $\det_{\mathscr{B}}(\mathscr{C})$ au lieu de $\det_{\mathscr{B}}(u_1, \dots, u_n)$.

Corollaire : Avec les notations précédentes, $\det_{\mathscr{B}}(\mathscr{C}) \neq 0$ et

$$\det_{\mathscr{B}}(\mathscr{C}) = (\det_{\mathscr{C}}(\mathscr{B}))^{-1}$$

Preuve :
On sait que

$$\forall (v_1, \dots, v_n) \in E^n, \det_{\mathscr{C}}(v_1, \dots, v_n) = \det_{\mathscr{B}}(\mathscr{C})\ \det_{\mathscr{B}}(v_1, \dots, v_n).$$

En particulier,

$$1 = \det_{\mathscr{C}}(\mathscr{C}) = \det_{\mathscr{C}}(\mathscr{B})\ \det_{\mathscr{B}}(\mathscr{C}).$$

□

Théorème : Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E, $\mathscr{C} = (u_1, \dots, u_n)$ une famille liée (i.e. $\mathscr{C}$ n'est pas libre). Alors $\det_{\mathscr{B}}(\mathscr{C}) = 0$.

Preuve :
Sans perte de généralité, on peut supposer que $u_n \in \text{Vect}(u_1, \dots, u_{n-1})$:

$$u_n = \sum_{k=1}^{n-1} \lambda_k u_k \text{ où } \lambda_1, \dots, \lambda_{n-1} \in \mathbb{K}.$$

$$\begin{aligned}\det_{\mathscr{B}}(u_1, \dots, u_{n-1}, u_n) &= \sum_{k=1}^{n-1} \lambda_k \underbrace{\det_{\mathscr{B}}(u_1, \dots, u_{n-1}, u_k)}_{=0} \\ &= 0\end{aligned}$$

□

3 Déterminant d'un endomorphisme

Proposition : Soit $f \in \mathscr{L}(E)$, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Alors,

$$\exists! \lambda \in \mathbb{K}, \forall (u_1, \dots, u_n) \in E, \det_{\mathscr{B}}\big(f(u_1), \dots, f(u_n)\big) = \lambda \det_{\mathscr{B}}(u_1, \dots, u_n).$$

Preuve :
Soit $g : \begin{array}{ccc} E^n & \longrightarrow & \mathbb{K} \\ (u_1, \dots, u_n) & \longmapsto & \det_{\mathscr{B}}\big(f(u_1), \dots, f(u_n)\big) \end{array}$. g est clairement alternée.

Soit $i \in [\![1, n]\!]$, $(u_1, \dots, u_i, u_{i+1}, \dots, u_n) \in E^{n-1}$. L'application $u \mapsto g(u_1, \dots, u_{i-1}, u, u_{i+1}, \dots, u_n)$ est la composée de f et de $v \mapsto \det_{\mathscr{B}}\big(f(u_1), \dots, f(u_{i-1}), v, f(u_{i+1}), \dots, f(u_n)\big)$ donc elle est linéaire.

Donc, g est une forme multilinéaire alternée donc colinéaire à $\det_{\mathscr{B}}$. □

Proposition : Soit $f \in \mathscr{L}(E)$, $\mathscr{B}$ et $\mathscr{C}$ deux bases de E. Soient $(\lambda, \mu) \in \mathbb{K}^2$ tel que

$$\forall (u_1, \dots, u_n) \in E^n, \begin{cases} \det_{\mathscr{B}}\big(f(u_1), \dots, f(u_n)\big) = \lambda \det_{\mathscr{B}}(u_1, \dots, u_n), \\ \det_{\mathscr{C}}\big(f(u_1), \dots, f(u_n)\big) = \mu \det_{\mathscr{C}}(u_1, \dots, u_n). \end{cases}$$

Alors, $\lambda = \mu$.

Preuve :
On pose $\mathscr{B} = (e_1, \dots, e_n)$.

$$\det_{\mathscr{C}}\big(f(e_1), \dots, f(e_n)\big) = \mu \det_{\mathscr{C}}(e_1, \dots, e_n) = \mu \det_{\mathscr{C}}(\mathscr{B})$$

$$\| $$

$$\det_{\mathscr{C}}(\mathscr{B}) \det_{\mathscr{B}}\big(f(e_1), \dots, f(e_n)\big)$$

$$\| $$

$$\lambda \underbrace{\det_{\mathscr{C}}(\mathscr{B})}_{\neq 0} \underbrace{\det_{\mathscr{B}}(\mathscr{B})}_{=1}$$

donc $\lambda = \mu$. □

Définition : Soit $f \in \mathscr{L}(E)$. Le <u>déterminant</u> de f est le seul scalaire vérifiant,

$\forall \mathscr{B}$ base de E, $\forall (u_1, \dots, u_n), \det_{\mathscr{B}}\big(f(u_1), \dots, f(u_n)\big) = \lambda \det_{\mathscr{B}}(u_1, \dots, u_n)$

et on le note $\lambda = \det(f)$.

Remarque :
Si $n = 2$,

$$\text{Aire}\big(f(u_1), f(u_2)\big) = \det(f)\, \text{Aire}(u_1, u_2).$$

Proposition : Soient f et g deux endomorphismes de E. Alors,

$$\det(f \circ g) = \det f \times \det g.$$

Preuve :
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E.

$$\det_{\mathscr{B}}\big(f \circ g(e_1), \dots, f \circ g(e_n)\big) = \det(f \circ g) \det_{\mathscr{B}}(e_1, \dots, e_n) = \det(f \circ g)$$

$$\| $$

$$\det_{\mathscr{B}}\Big(f\big(g(e_1)\big), \dots, f\big(g(e_n)\big)\Big)$$

$$\| $$

$$(\det f)\ \det_{\mathscr{B}}\big(g(e_1), \dots, g(e_n)\big)$$

$$\| $$

$$(\det f)\,(\det g)\ \underbrace{\det_{\mathscr{B}}(e_1, \dots, e_n)}_{=1}.$$

□

Corollaire : Si $f \in \mathrm{GL}(E)$, alors $\det(f) \neq 0$ et $\det(f^{-1}) = \det(f)^{-1}$.

Preuve :
On suppose $f \in \mathrm{GL}(E)$:
$$f \circ f^{-1} = \mathrm{id}_E\,.$$
Donc,
$$\det(f)\ \det(f^{-1}) = \det(f \circ f^{-1}) = \det(\mathrm{id}_E).$$
Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E.
$$\det_{\mathscr{B}}\left(\mathrm{id}_E(e_1), \ldots, \mathrm{id}_E(e_n)\right) = \det(id_E) \times 1$$
$$\|$$
$$\det_{\mathscr{B}}(\mathscr{B}) = 1$$
□

Proposition : Soit $f \in \mathscr{L}(E)$. On suppose $f \notin \mathrm{GL}(E)$. Alors $\det(f) = 0$.

Preuve :
Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E.
$$\det(f) = \det_{\mathscr{B}}\left(f(e_1), \ldots, f(e_n)\right).$$
f n'est pas surjective donc $\mathrm{rg}\left(f(e_1), \ldots, f(e_n)\right) < n$ donc $\left(f(e_1), \ldots, f(e_n)\right)$ est liée donc $\det_{\mathscr{B}}\left(f(e_1), \ldots, f(e_n)\right) = 0$. □

Définition : Soit $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \in \mathscr{M}_n(\mathbb{K})$.

Le <u>déterminant</u> de A est
$$\det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j}$$

Proposition : Soit E un $\mathbb{K}$-espace vectoriel de dimension n, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E, $(u_1, \dots, u_n) \in E^n$ et $A = \mathrm{Mat}_{\mathscr{B}}(u_1, \dots, u_n)$.

Alors,

$$\det_{\mathscr{B}}(u_1, \dots, u_n) = \det(A).$$

Proposition : Soit E un $\mathbb{K}$-espace vectoriel de dimension n, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E, $f \in \mathscr{L}(E)$ et $A = \mathrm{Mat}_{\mathscr{B}}(f)$. Alors, $\det(A) = \det(f)$.

Preuve :
$\det(f) = \det_{\mathscr{B}}\big(f(e_1), \dots, f(e_n)\big)$, $A = \mathrm{Mat}_{\mathscr{B}}\big(f(e_1), \dots, f(e_n)\big)$.

$$\begin{aligned} \det A &= \det_{\mathscr{B}}\big(f(e_1), \dots, f(e_n)\big) \\ &= \det(f). \end{aligned}$$

□

Proposition : Soit $(A, B) \in \mathscr{M}_n(\mathbb{K})^2$.

$$\det(AB) = \det(A)\,\det(B).$$

Preuve :
Soit $E = \mathbb{K}^n$, $\mathscr{B} = (e_1, \dots, e_n)$ la base canonique de E, $f \in \mathscr{L}(E)$ tel que $A = \mathrm{Mat}_{\mathscr{B}}(f)$ et $g \in \mathscr{L}(E)$ tel que $B = \mathrm{Mat}_{\mathscr{B}}(g)$.

$$\begin{aligned} \det(AB) = \det(f \circ g) &= (\det f)\,(\deg g) \\ &= \det(A)\,\det(B). \end{aligned}$$

□

Proposition : Soit $A \in \mathscr{M}_n(\mathbb{K})$.

$$A \in \mathrm{GL}_n(\mathbb{K}) \iff \det(A) \neq 0$$

Dans ce cas, $\det(A^{-1}) = \det(A)^{-1}$. □

Proposition :

$$\forall A \in \mathscr{M}_n(\mathbb{K}), \det({}^tA) = \det(A).$$

Preuve :
Soit $A \in \mathscr{M}_n(\mathbb{K})$.

$$\begin{aligned}
\det({}^tA) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j,\sigma(j)} \\
&= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{\sigma^{-1}(k),k} \\
&= \sum_{\sigma' \in S_n} \varepsilon\left(\sigma'^{-1}\right) \prod_{k=1}^{n} a_{\sigma'(k),k} \\
&= \sum_{\sigma' \in S_n} \varepsilon(\sigma') \prod_{k=1}^{n} a_{\sigma'(k),k} \\
&= \det(A)
\end{aligned}$$

car

$$\forall \sigma' \in S_n, \varepsilon\left(\sigma'^{-1}\right) = \varepsilon(\sigma')^{-1} = \begin{cases} 1 & \text{si } \varepsilon(\sigma') = 1 \\ -1 & \text{si } \varepsilon(\sigma') = -1 \end{cases} = \varepsilon(\sigma').$$

□

Proposition : Soit $A \in \mathscr{M}_n(\mathbb{K})$, C une opération sur les colonnes et A' la matrice obtenue en appliquant C sur les colonnes A.

1. Si $C = c_i \longleftrightarrow c_j$ (avec $i \neq j$), alors $\det(A') = -\det(A)$.
2. Si $C = c_i \longleftrightarrow \lambda c_i$, alors $\det(A') = \lambda \det(A)$.
3. Si $C = c_i \longleftrightarrow c_i + \lambda c_j$ (avec $i \neq j$), alors $\det(A') = \det(A)$.

Preuve :
Soit $(u_1, \ldots, u_n) \in (\mathbb{K}^n)^n$ tel que

$$\forall i \in [\![1, n]\!], c_i = \mathrm{Mat}_{\mathscr{B}}(u_i)$$

où $\mathscr{B}$ est la base canonique de $\mathbb{K}^n$ et c_i la i-ème colonne de A.

1.
$$\begin{array}{rl} -\det(A) = -\det_{\mathscr{B}}(u_1,\dots,u_n) & \\ & \| \\ \det(A') = \det_{\mathscr{B}}(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_{j-1},u_i,u_{j+1},\dots,u_n). & \end{array}$$

2.
$$\begin{aligned} \det(A') &= \det_{\mathscr{B}}(u_1,\dots,u_{i-1},\lambda u_i,u_{i+1},\dots,u_n) \\ &= \lambda \det_{\mathscr{B}}(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_n) \\ &= \lambda \ \det(A). \end{aligned}$$

3.
$$\begin{aligned} \det(A') &= \det_{\mathscr{B}}(u_1,\dots,u_{i-1},u_i+\lambda u_j,u_{i+1},\dots,u_n) \\ &= \det_{\mathscr{B}}(u_1,\dots,u_{i-1},u_i,u_{i+1},\dots,u_n) + \lambda \det_{\mathscr{B}}(u_1,\dots,u_{i-1},u_j,u_{i+1},\dots,u_n) \\ &= \det(A) \end{aligned}$$

car, comme u_j apparaît deux fois dans le second détermiant, il vaut 0.

□

Corollaire : Le déterminant d'une matrice triangulaire est le produit de ses coefficients diagonaux.

Preuve :

Soit $T = \begin{pmatrix} \lambda_1 & \star & \cdots & \star \\ & \ddots & \ddots & \vdots \\ (0) & & & \star \\ & & \lambda_n & \end{pmatrix}$. S'il existe $i \in [\![1,n]\!]$, avec $\lambda_i = 0$, alors $\mathrm{rg}(T) < n$ et donc $T \notin \mathrm{GL}_n(\mathbb{K})$ et donc $\det(T) = 0 = \prod_{k=1}^{n} \lambda_k$.

On suppose que $\forall i, \lambda_i \neq 0$. On a

$$\frac{1}{\lambda_1}\det(T) = \det \begin{pmatrix} 1 & \star & \cdots & \star \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

et

$$\frac{1}{\lambda_1\lambda_2}\det(T)=\det\begin{pmatrix}1&\star&\cdots&\cdots&\star\\0&1&\ddots&&\vdots\\\vdots&0&\lambda_3&\ddots&\vdots\\\vdots&\vdots&\ddots&\ddots&\star\\0&0&\cdots&0&\lambda_n\end{pmatrix}$$

D'où

$$\begin{aligned}\frac{1}{\lambda_1\cdots\lambda_n}\det(T)&=\begin{vmatrix}1&&&\star\\&\ddots&&\\&&\ddots&\\(0)&&&1\end{vmatrix}\\&=\begin{vmatrix}1&&&(0)\\&\ddots&&\\&&\ddots&\\(0)&&&1\end{vmatrix}\\&=1\end{aligned}$$

donc $\det(T)=\lambda_1\cdots\lambda_n$. □

Proposition : Soit $A\in\mathscr{M}_n(\mathbb{K})$, L une opération sur les lignes, A' la matrice obtenue en appliquant L sur les lignes de A.

1. Si $L=\ell_i\longleftrightarrow\ell_j$ (avec $i\neq j$), $\det(A')=-\det(A)$.
2. Si $L=\ell_i\longleftrightarrow\lambda\ell_i$, $\det(A')=\lambda\det(A)$.
3. Si $L=\ell_i\longleftrightarrow\ell_i+\lambda\ell_j$ (avec $i\neq j$), $\det(A')=\det(A)$.

□

Exemple :
$(a,b,c)\in\mathbb{C}^3$

$$\begin{aligned}\begin{vmatrix} a & b & c \\ b & a & c \\ c & a & b \end{vmatrix} &= \begin{vmatrix} a+b+c & b & c \\ a+b+c & a & c \\ a+b+c & a & b \end{vmatrix} \\ &= (a+b+c)\begin{vmatrix} 1 & b & c \\ 1 & a & c \\ 1 & a & b \end{vmatrix} \\ &= (a+b+c)\begin{vmatrix} 1 & b & c \\ 0 & a-b & 0 \\ 0 & 0 & b-c \end{vmatrix} \\ &= (a+b+c)(a-b)(b-c)\end{aligned}$$

5 Développement suivant une ligne ou une colonne

Exemple :

$$\begin{vmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{vmatrix}$$

$$\begin{vmatrix} 1 & \boxed{2} & 3 & 0 \\ 4 & 5 & 6 & -1 \\ 7 & 8 & 9 & -2 \\ 3 & 2 & 1 & 0 \end{vmatrix} = -2\begin{vmatrix} 4 & 6 & -1 \\ 7 & 9 & -2 \\ 3 & 1 & 0 \end{vmatrix} + 5\begin{vmatrix} 1 & 3 & 0 \\ 7 & 9 & -2 \\ 3 & 1 & 0 \end{vmatrix} - 8\begin{vmatrix} 1 & 3 & 0 \\ 4 & 6 & -1 \\ 3 & 1 & 0 \end{vmatrix} + 2\begin{vmatrix} 1 & 3 & 0 \\ 4 & 6 & -1 \\ 7 & 9 & -2 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & \boxed{0} \\ 4 & 5 & 6 & \boxed{-1} \\ 7 & 8 & 9 & \boxed{-2} \\ 3 & 2 & 1 & \boxed{0} \end{vmatrix} = -1\begin{vmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 3 & 2 & 1 \end{vmatrix} + 2\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 3 & 2 & 1 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 0 \\ 4 & 5 & 6 & -1 \\ 7 & 8 & 9 & -2 \\ \boxed{3} & \boxed{2} & \boxed{1} & \boxed{0} \end{vmatrix} = -3\begin{vmatrix} 2 & 3 & 0 \\ 5 & 6 & -1 \\ 8 & 9 & -1 \end{vmatrix} + 2\begin{vmatrix} 1 & 3 & 0 \\ 4 & 6 & -1 \\ 7 & 9 & -2 \end{vmatrix} - \begin{vmatrix} 1 & 2 & 0 \\ 4 & 5 & -1 \\ 7 & 8 & 9 \end{vmatrix}$$

$E = \mathbb{C}^4$ et $\mathscr{B} = (e_1, e_2, e_3, e_4)$ base canonique de E.

On pose $\begin{cases} u_1 = (1,4,7,3), \\ u_2 = (2,5,8,2), \\ u_3 = (3,6,9,1), \\ u_4 = (0,-1,-2,0). \end{cases}$ et $A = \mathrm{Mat}_{\mathscr{B}}(u_1,u_2,u_3,u_4) = \mathrm{Mat}_{\mathscr{B}}(u_1, 2e_1 + 5e_2 + 8e_3 + 2e_4, u_3, u_4)$.

Donc,

$$\begin{aligned}\det A &= \det_{\mathscr{B}}(u_1, 2e_1 + 5e_2 + 8e_3 + 2e_4, u_3, u_4)\\ &= \quad 2\det_{\mathscr{B}}(u_1, e_1, u_3, u_4)\\ &\quad + 5\det_{\mathscr{B}}(u_1, e_2, u_3, u_4)\\ &\quad + 9\det_{\mathscr{B}}(u_1, e_3, u_3, u_4)\\ &\quad + 2\det_{\mathscr{B}}(u_1, e_4, u_3, u_4).\end{aligned}$$

$$\begin{aligned}\det_{\mathscr{B}}(u_1, e_1, u_3, u_4) &= \begin{vmatrix} 1 & 1 & 3 & 0\\ 4 & 0 & 6 & -1\\ 7 & 0 & 9 & -2\\ 3 & 0 & 1 & 0 \end{vmatrix}\\ &= -\begin{vmatrix} \boxed{1} & 1 & 3 & 0\\ 0 & 4 & 6 & -1\\ 0 & 7 & 9 & -2\\ 0 & 3 & 1 & 0 \end{vmatrix}\\ &= -\left|\begin{array}{c|ccc} 1 & 0 & 0 & 0\\ \hline 0 & 4 & 6 & -1\\ 0 & 7 & 9 & -2\\ 0 & 3 & 1 & 0 \end{array}\right|\\ &= \dots\\ &= -\left|\begin{array}{c|c} 1 & 0\\ \hline 0 & \begin{array}{cc} & \star\\ (0) & \end{array} \end{array}\right|\end{aligned}$$

Idem pour e_2, e_3, e_4.

Proposition (Laplace) **:** Soit $A = (a_{ij}) \in \mathscr{M}_n(\mathbb{K})$.

$$\forall j \in [\![1, n]\!]\,,\ \det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} m_{i,j}$$

où $m_{i,j}$ est le mineur d'indices (i, j), i.e. le déterminant de la matrice obtenue en supprimant la ligne i et la colonne j de la matrice A.

$$\forall i \in [\![1, n]\!]\,,\ \det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} m_{i,j}.$$

□

Proposition (Vandermonde) **:** Soient $(a_1, \dots, a_n) \in \mathbb{K}^n$.

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{j<i} (a_j - a_i)$$

Preuve (par récurrence sur n) *:* — Soit $n \in \mathbb{N}$. Soient $a_1, \dots, a_{n+1} \in \mathbb{K}$.
On pose

$$\Delta_{n+1} = \begin{vmatrix} 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n+1} & \cdots & a_{n+1}^n \end{vmatrix}$$

On développe Δ_{n+1} suivant la dernière ligne et on obtient une expression polynomial en a_{n+1} :

$$\Delta_{n+1} = P(a_{n+1}) \text{ avec } P \in \mathbb{K}_n[X]$$

et le coefficent devant X^n est Δ_n.

Cas 1 On suppose $\Delta_n \neq 0$. D'après l'hypothèse de récurrence :

$$\begin{cases} \forall i, j \in [\![1, n]\!],\ i \neq j \implies a_i \neq a_j \\ \deg(P_n) = \Delta_n = \displaystyle\prod_{n \geqslant j > i \geqslant 1} (a_j - a_i) \\ \deg(P_n) = n \\ \forall i \in [\![1, n]\!], P(a_i) = 0 \end{cases}$$

donc

$$P = \Delta_n (X - a_1) \cdots (X - a_n)$$

donc

$$\begin{aligned} \Delta_{n+1} &= \prod_{n \geqslant j > i \geqslant 1} (a_j - a_i)\,(a_{n+1} - a_1) \cdots (a_{n+1} - a_n) \\ &= \prod_{n+1 \geqslant j > i \geqslant 1} (a_j - a_i) \end{aligned}$$

Cas 2 On suppose $\Delta_n = 0$:

$$\exists i, j \in [\![1, n]\!],\ i \neq j \text{ et } a_i = a_j.$$

Alors,

$$\Delta_{n+1} = 0 = \prod_{n+1 \geqslant j > i \geqslant 1} (a_j - a_i).$$

□

Proposition–Définition : Soit $A \in \mathcal{M}_n(\mathbb{K})$, et $\mathrm{com}(A)$ la comatrice de A : c'est la matrice

$$\left((-1)^{i+j}\, m_{i,j}\right)_{1\leqslant i,j\leqslant n}$$

où $m_{i,j}$ est le mineur d'indices (i,j) de A.

On a

$$A\ {}^t\mathrm{com}(A) = {}^t\mathrm{com}(A)\ A = \det(A)\ I_n.$$

Si $\det A \neq 0$, alors

$$A^{-1} = \frac{1}{\det(A)}\ {}^t\mathrm{com}(A).$$

Exemple :
Avec $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, on a $\det A = ad - bc$.

$$\mathrm{com}\, A = \begin{pmatrix} +d & -b \\ -c & +a \end{pmatrix} \text{ donc } {}^t\mathrm{com}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Si $\det(A) \neq 0$,

$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Exemple :
Avec $A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$, on a

$$\mathrm{com}\, A = \begin{pmatrix} b_2c_3 - b_3c_2 & a_3c_2 - a_2c_3 & a_2b_3 - a_3b_2 \\ c_1b_3 - b_1c_3 & a_1c_3 - a_3c_1 & a_3b_1 - a_1b_3 \\ b_1c_2 - b_2c_1 & a_2c_1 - a_1c_2 & a_1b_2 - a_2b_1 \end{pmatrix}$$

Preuve :
On note $C = A\ {}^t\mathrm{com}(A) = (c_{i,j})$.

$$\forall i \in [\![1,n]\!]\,, c_{ii} = \sum_{j=1}^{n} a_{ij}(-1)^{i+j} m_{ij} = \det(A).$$

Soient $i \in [\![1,n]\!]$, $j \in [\![1,n]\!]$ avec $i \neq j$.

$$c_{ij} = \sum_{k=1}^{n} a_{ik}(-1)^{j+k} m_{jk}.$$

C'est le déterminant de la matrice obtenue en remplaçant la j-ème ligne de A par la i-ème, qui a donc 2 lignes identiques donc $c_{ij} = 0$.

L'autre formule " ${}^t\mathrm{com}(A)\ A = \det(A) I_n$" se démontre de la même façon. □

Remarque :
En pratique, on n'utilise jamais cette formule pour trouver A^{-1} (sauf si $n = 2$).

Exercice (Formules de Cramer) :

Inutiles et Hors-Programme

Soit S le système $AX = B$ avec $A \in \mathrm{GL}_n(\mathbb{K})$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$.

L'unique solution du système S est donnée par

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ où } \forall i,\ x_i = \frac{\det A_i}{\det A}$$

où A_i est obtenue en replaçant la i-ème colonne de A par B.

Solution : Soit $(x_1, \dots, x_n)$ l'unique solution de S.

$$\sum_{i=1}^{n} x_i C_i(A) = B$$

où $C_i(A)$ est la i-ème colonne de A.

$$\begin{aligned} \forall j, \det(A_j) &= \det\big(C_1(A), C_2(A), \dots, C_{j-1}(A), B, C_{j+1}(A), \dots, C_n(A)\big) \\ &= \sum_{i=1}^{n} x_i \det\big(C_1(A), \dots, C_{j-1}(A), C_i(A), C_{j+1}(A), \dots, c_n(A)\big) \\ &= x_j \det(A) \end{aligned}$$

Retour sur la diagonalisation

Soit $A \in \mathcal{M}_n(\mathbb{K})$. On cherche $P \in \mathrm{GL}_n(\mathbb{K})$ telle que

$$P\ A\ P^{-1} = \begin{pmatrix} \lambda_1 & \ddots & (0) \\ & \ddots & \\ (0) & \ddots & \lambda_n \end{pmatrix}$$

Soit $f \in \mathcal{L}(\mathbb{K}^n)$ telle que $\mathrm{Mat}_{\mathcal{B}}(f) = A$ où $\mathcal{B}$ est la base canonique de $\mathbb{K}^n$. On cherche $\mathcal{C} = (u_1, \dots, u_n) \in \mathbb{K}^n$ telle que

$$\exists \lambda_i, f(u_i) = \lambda_i u_i$$

$$
\begin{aligned}
& \exists \lambda \in \mathbb{K},\ \exists u \neq 0,\ f(u) = \lambda u \\
\iff & \exists \lambda \in \mathbb{K},\ \exists u \neq 0,\ u \in \operatorname{Ker}(f - \lambda \operatorname{id}_{\mathbb{K}^n}) \\
\iff & \exists \lambda \in \mathbb{K},\ f - \lambda \operatorname{id}_{\mathbb{K}^n} \text{ n'est pas injective} \\
\iff & \exists \lambda \in \mathbb{K},\ f - \lambda \operatorname{id}_{\mathbb{K}^n} \notin \mathrm{GL}(\mathbb{K}^n) \\
\iff & \exists \lambda \in \mathbb{K},\ \det(\lambda - \operatorname{id}_{\mathbb{K}^n}) = 0 \\
\iff & \exists \lambda \in \mathbb{K},\ \underbrace{\det(A - \lambda I_n)}_{\text{polynôme caractéristique de } A} = 0
\end{aligned}
$$

Chapitre 27

Espace probabilisé fini

1 Définitions

Définition : Soit Ω un ensemble fini. Une probabilité sur Ω est une application

$$P : \mathcal{P}(\Omega) \longrightarrow [0,1]$$

telle que

1. $P(\Omega) = 1$,
2. $\forall A, B \in \mathcal{P}(W),\ A \cap B = \implies P(A \cup B) = P(A) + P(B)$.

Dans ce cas, on dit que (Ω, P) est un espace probabilisé.

Exemple (équiprobabilité) :
Soit Ω un ensemble fini non vide. Soit

$$\begin{aligned} P : \mathcal{P}(\Omega) &\longrightarrow [0,1] \\ A &\longmapsto \frac{\#A}{\#\Omega}. \end{aligned}$$

En effet,

1. $P(\Omega) = \dfrac{\#\Omega}{\#\Omega} = 1$.
2. Soient $A, B \in \mathcal{P}(\Omega)$ avec $A \cap B = .$

$$\begin{aligned} P(A \cup B) &= \frac{\#(A \cup B)}{\#\Omega} \\ &= \frac{\#A + \#B}{\#\Omega} \\ &= P(A) + P(B) \end{aligned}$$

De plus, on pose $n = \#\Omega$.

$$\forall \omega \in \Omega, P\big(\{\omega\}\big) = \frac{1}{n} \text{ et ne dépend pas de } \omega.$$

Définition : Soit (Ω, P) un espace probabilisé.

L'ensemble Ω est appelé univers, les singletons $\{\omega\}$ avec $\omega \in \Omega$ sont appelés événements élémentaires, les parties de Ω sont appelées événements, est appelé événement impossible et Ω est appelé événement certain.

Soient $A, B \in \mathcal{P}(\Omega)$. On dit que A et B sont incompatibles si $A \cap B = .$

Proposition : Soit $\Omega = \{\omega_1, \dots, \omega_n\}$ un ensemble de cardinal n et $(p_1, \dots, p_n) \in [0,1]^n$ tel que $\sum_{i=1}^{n} p_i = 1$. Il existe une unique probabilité P sur Ω que

$$\forall i \in [\![1, n]\!],\ P\big(\{\omega_i\}\big) = p_i.$$

Preuve

Existence On pose

$$\begin{aligned} P : \mathcal{P}(\Omega) &\longrightarrow [0,1] \\ A &\longmapsto \sum_{i \in I_A} p_i \end{aligned}$$

où $I_A = \big\{i \in [\![1, n]\!] \mid \omega_i \in A\big\}$.

— Soit $a \in \mathcal{P}(\Omega)$.

$$0 \leqslant P(A) = \sum_{i \in I_A} p_i \leqslant \sum_{i=1}^{n} p_i = 1$$

— $P(\Omega) = \sum_{i \in I_\Omega} p_i = \sum_{i=1}^{n} p_i = 1.$

— Soient $A, B \in \mathcal{P}(\Omega)$ incompatibles.

$$\begin{aligned} I_{A \cup B} &= \{i \in [\![1, n]\!], \omega_i \in A \cup B\} \\ &= I_A \cup I_B \end{aligned}$$

$$P(A \cup B) = \sum_{i \in I_{A \cup B}} p_i = \sum_{i \in I_A} p_i + \sum_{i \in I_B} p_i = P(A) + P(B).$$

Unicité Soit Q une probabilité sur Ω tel que

$$\forall i \in [\![1, n]\!], Q\big(\{\omega_i\}\big) = p_i.$$

Soit $A \in \mathcal{P}(\Omega)$.

$$A = \bigcup_{\omega \in A}^{\cdot} \{\omega\} = \bigcup_{i \in I_A}^{\cdot} \{\omega_i\}.$$

En utilisant le lemme suivant,

$$Q(A) = Q\left(\bigcup_{i\in I_A}^{\cdot}\{\omega_i\}\right) = \sum_{i\in I_A} Q\big(\{\omega_i\}\big)$$
$$= \sum_{i\in I_A} p_i = P(A).$$

□

Lemme : Soit P une probabilité sur Ω et $(A_i)_{1\leqslant i\leqslant n}$ une famille d'événements 2 à 2 incompatibles. Alors

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i).$$

Preuve :
par récurrence sur n. □

Proposition : Soit P une probabilitésur Ω.

1. $P() = 0$;
2. $\forall A, B \in \mathscr{P}(\Omega),\ A \subset B \implies P(A) \leqslant P(B)$;
3. $\forall A, B \in \mathscr{P}(\Omega),\ P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Preuve : 1. $\Omega = \cup\,\Omega$ donc $P(\Omega) = P() + P(\Omega)$ donc $P() = 0$.

2. Soient $A, B \in \mathscr{P}(\Omega)$ avec $A \subset B$. On pose $C = B \setminus A$:

$$\begin{cases} B = A \cup C; \\ A \cap C = . \end{cases}$$

Donc, $P(B) = P(A) + \underbrace{P(C)}_{\geqslant 0} \geqslant P(A)$.

3. On pose $\begin{cases} A' = A \setminus (A \cap B), \\ B' = B \setminus (A \cap B), \\ C = A \cap B. \end{cases}$

$$\begin{cases} A' \cup B' \cup C = A \cup B \\ A' \cap C = B' \cap C = A' \cap B' = \end{cases}$$

donc

$$P(A \cup B) = P(A') + P(B') + P(C).$$

De plus,

$$\begin{cases} A = A' \uplus C \text{ donc } P(A) = P(A') + P(C); \\ B = B' \uplus C \text{ donc } P(B) = P(B') + P(C). \end{cases}$$

D'où

$$\begin{aligned} P(A \cup B) &= P(A) - P(C) + P(B) - \cancel{P(C)} + \cancel{P(C)} \\ &= P(A) + P(B) - P(A \cap B). \end{aligned}$$

□

2 Probabilité conditionnelle

Proposition–Définition : Soit (Ω, P) un espace probabilisé et $A \in \mathscr{P}(\Omega)$ tel que $P(A) \neq 0$.

L'application

$$\begin{aligned} \mathscr{P}(\Omega) &\longrightarrow [0,1] \\ X &\longmapsto \frac{P(A \cap X)}{P(A)} \end{aligned}$$

est une probabilité. Elle est notée P_A et est appelée probabilité sachant A.

Elle est parfois notée $P(A \mid B)$.

Preuve : — Soit $X \in P(\Omega)$.

$$0 \leqslant P(A \cap X) \leqslant P(A) \text{ car } A \cap X \subset A$$

Comme $P(A) > 0$,

$$0 \leqslant \frac{P(A \cap X)}{P(A)} \leqslant 1$$

—

$$\frac{P(A \cap \Omega)}{P(A)} = \frac{P(A)}{P(A)} = 1$$

— Soient $X, Y \in P(\Omega)$ avec $X \cap Y = .$

$$\begin{aligned}\frac{P\big(A \cap (X \cup Y)\big)}{P(A)} &= \frac{P\big((X \cap A) \uplus (Y \cap A)\big)}{P(A)} \\ &= \frac{P(A \cap X) + P(A \cap Y)}{P(A)}\end{aligned}$$

□

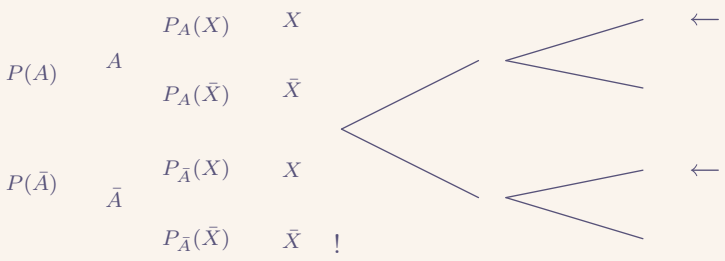
Proposition : Soit (Ω, P) un espace probabilisé et $A \in \mathscr{P}(\Omega)$ tel que $P(A) \neq 0$.

$$\forall X \in \mathscr{P}(\Omega),\ P(A \cap X) = P(A)\ P_A(X).$$

□

Proposition : Soit (Ω, P) un espace probabilisé, $A \in \mathscr{P}(\Omega)$ tel que $P(A) \in]0, 1[$.

$$\forall X \in \mathscr{P}(\Omega),\ P(X) = P(A)\,P_A(X) + P\left(\bar{A}\right)\ P_{\bar{A}}(X).$$



Preuve :
Soit $X \in \mathscr{P}(\Omega)$.

$$\begin{aligned}X &= X \cap \Omega \\ &= X \cap \left(A \uplus \bar{A}\right) \\ &= (X \cap A) \uplus \left(X \cap \bar{A}\right)\end{aligned}$$

donc

$$\begin{aligned} P(X) &= P(X \cap A) + P\left(X \cap \bar{A}\right) \\ &= P(A)\, P_A(X) + P\left(\bar{A}\right)\, P_{\bar{A}}(X). \end{aligned}$$

□

Définition : Soit (Ω, P) un espace probabilisé. Un système complet d'événements est une partition de Ω.

Proposition (probabilités totales) **:** Soit (Ω, P) un espace probabilisé, $(A_i)_{1\leqslant i\leqslant n}$ un système complet d'événements tel que

$$\forall i \in [\![1, n]\!]\,,\ P(A_i) > 0.$$

Alors,

$$\forall x \in \mathscr{P}(\Omega),\ P(X) = \sum_{i=1}^{n} P(A_i) P_{A_i}(X).$$

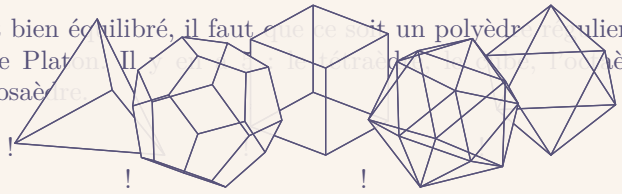
Preuve :
Soit $X \in \mathscr{P}(\Omega)$.

$$\begin{aligned} P(X) &= P(X \cap \Omega) \\ &= P\left(X \cap \left(\bigcup_{i=1}^{n}{}^{\cdot} A_i\right)\right) \\ &= P\left(\bigcup_{i=1}^{n}{}^{\cdot} (X \cap A_i)\right) \\ &= \sum_{i=1}^{n} P(X \cap A_i) \\ &= \sum_{i=1}^{n} P(A_i) P_{A_i}(X) \end{aligned}$$

□

Exemple :
On dispose de 5 dés : un à 4 faces, un à 6 faces, un à 8 faces, un à 8 faces, un à 12 faces et un à 20 faces que l'on suppose bien équilibré.

Pour qu'un dé soit bien équilibré, il faut que ce soit un polyèdre régulier, aussi appelé polyèdre de Platon. Il y a cinq tels polyèdres : le tétraèdre, le cube, l'octaèdre, le dodécaèdre, et l'icosaèdre.



On choisit au hasard l'un de ces dés, on le lance et on note le résultat.

Quelle est la probabilité que ce résultat soit égal à 7 ?

Modélisation 1 : $\Omega = [\![1, 20]\!]$, $P = ?$.

Modélisation 2 : $\Omega = \big\{(x, y) \mid x \in \{4, 6, 8, 12, 20\} \text{ et } y \in [\![1, x]\!]\big\}$ et P une probabilité sur Ω. On pose $\forall x \in \overbrace{\{4, 6, 8, 12, 20\}}^{X}$, $A_x = \{x\} \times [\![1, x]\!]$. On suppose que

$$\forall x \in X,\ P(A_x) = \frac{1}{5}.$$

On note

$$\forall y \in [\![1, 20]\!]\,,\ B_y = \big\{(x, y) \mid x \in X \text{ et } y \leqslant x\big\}$$

et donc

$$\forall x \in X,\ \forall y \in [\![1, x]\!]\,,\ P_{A_x}(B_y) = \begin{cases} \dfrac{1}{x} & \text{si } y \leqslant x, \\ 0 & \text{si } y > x. \end{cases}$$

Implémentation en Python de l'experience :

```
import random as rd

def exp():
  faces = rd.choice([4, 6, 8, 12, 20])
  result = rd.randint(1, faces)
  return result == 7

def proba(N = 1000):
  cpt = 0
  for _ in range(N):
    if exp():
      cpt += 1
  return cpt / N
```

Solution :

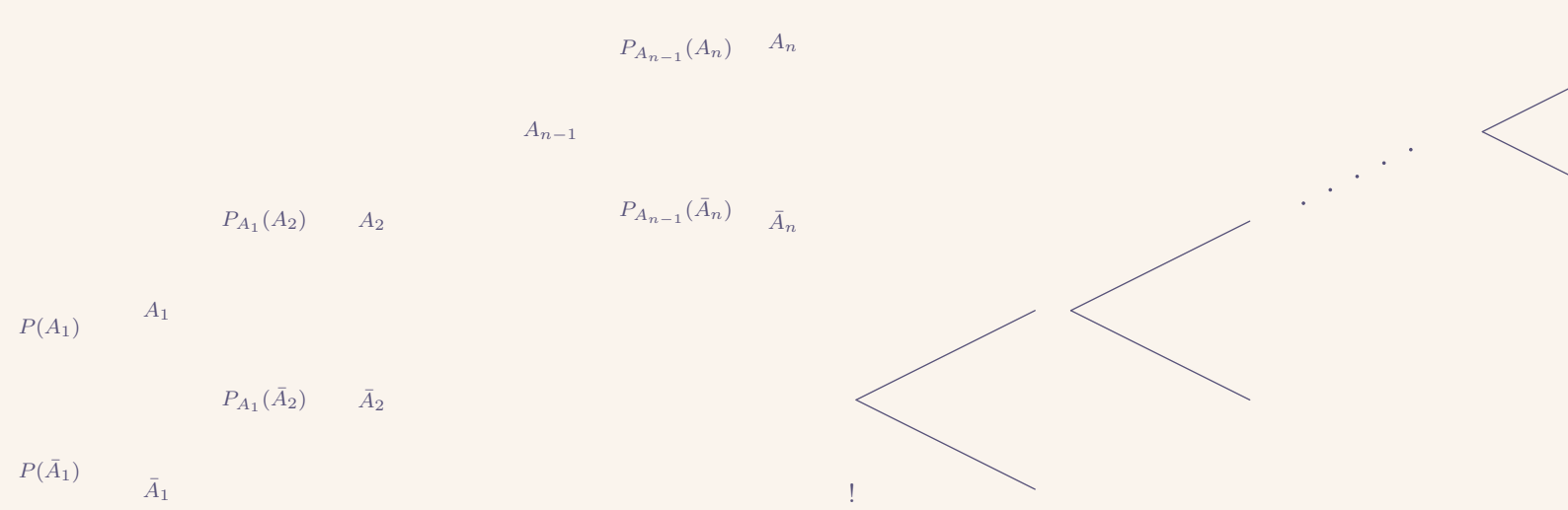
$$\begin{aligned} P(B_7) &= \sum_{x \in X} P_{A_x}(B_7) P(A_x) \\ &= \frac{1}{5}\left(P_{A_8}(B_7) + P_{A_{12}}(B_7) + P_{A_{20}}(B_7)\right) \\ &= \frac{1}{5}\left(\frac{1}{8} + \frac{1}{12} + \frac{1}{20}\right). \end{aligned}$$

Proposition (probabilités composées) **:** Soit (Ω, P) un espace probabilisé, $(A_i)_{1\leqslant i\leqslant n}$ des événements tels que

$$P(A_1 \cap \cdots \cap A_{n-1}) \neq 0.$$

Alors,

$$P(A_1 \cap \cdots \cap A_n) = P(A_1)\, P_{A_1}(A_2)\, P_{A_1\cap A_2}(A_3) \cdots P_{A_1\cap\cdots\cap A_{n-1}}(A_n)$$



Preuve :

$$\forall i, A_1 \cap \cdots \cap A_i \supset A_1 \cap \cdots \cap A_n \text{ donc } P(A_1 \cap \cdots \cap A_i) > 0.$$

$$\begin{aligned} &P(A_1)\, P_{A_1}(A_2)\, P_{A_1\cap A_2}(A_3) \cdots P_{A_1\cap\cdots\cap A_{n-1}}(A_n) \\ &= P(A_1)\frac{P(A_2\cap A_1)}{P(A_1)}\frac{P(A_3\cap A_2\cap A_1)}{P(A_1\cap A_2)} \cdots \frac{P(A_n\cap A_{n-1}\cap\cdots\cap A_1)}{P(A_1\cap\cdots\cap A_{n-1})} \\ &= P(A_1\cap\cdots\cap A_n) \end{aligned}$$

□

Exemple :
On reprend l'expérience précédente aléatoire précédente. On sait qu'on a obtenu 7.

Quel dé a été utilisé ?

On veut calculer $P_{B_7}(A_x)$ pour tout x. Soit $x \in X$.

$$\begin{aligned} P_{B_7}(A_x) &= \frac{P(A_x \cap B_7)}{P(B_7)} \\ &= \frac{P_{A_x}(B_7)\, P(A_x)}{P(B_7)} \\ &= \begin{cases} 0 & \text{si } x \in \{4, 6\} \\ \dfrac{\frac{1}{8} \times \frac{1}{5}}{P(B_7)} & \text{si } x = 8 \\ \dfrac{\frac{1}{2} \times \frac{1}{5}}{P(B_7)} & \text{si } x = 12 \\ \dfrac{\frac{1}{20} \times \frac{1}{5}}{P(B_7)} & \text{si } x = 20 \end{cases} \end{aligned}$$

On a utilisé la formule de Bayes.

Proposition (Bayes) **:** Soit (Ω, P) un espace probabilisé, $A, B \in \mathcal{P}(\Omega)$ tels que $P(A) \neq 0$ et $P(B) \in]0, 1[$.

$$P_A(B) = \frac{P_B(A)\, P(B)}{P(A)} = \frac{P_B(A)\, P(B)}{P_B(A)\, P(B) + P_{\bar{B}}(A)\, P\left(\bar{B}\right)}.$$

□

Remarque :
On appèle $P_A(B)$ la vraissemblance (*likelyhood* en anglais), $P(A)$ la probabilité a-priori (*prior distribution*), et $P_B(A)$ la probabilité a-posteriori (*posterior distribution*).

Exemple (filtre bayésien) :
On peut utiliser cette formule pour filtrer les SPAMs dans les emails. On utilise des données de la forme :

	mot 1	mot 2	$\cdots$	mot p	spam ?
mail 1					
mail 2					
$\vdots$					
mail n					

.

On peut donc calculer la probabilité qu'un email soit un SPAM en fonction des

mots qu'il contient :

$$P_{(\text{mot } 1,\overline{\text{mot } 2},\ldots)}(\text{spam}) = \frac{P(\text{spam})\,P_{\text{spam}}(\text{mot } 1,\overline{\text{mot } 2},\ldots)}{P(\text{mot } 1,\overline{\text{mot } 2},\ldots)} \simeq \frac{P_{\text{spam}}(\text{mot } 1)\times P_{\text{spam}}(\overline{\text{mot } 2})\times\cdots}{P(\text{mot } 1,\overline{\text{mot } 2},\ldots)}.$$

Exemple (Test médical) :
On estime qu'une personne sur 10 000 est atteinte d'une certaine maladie. On invente un test T.

$$\begin{cases} P_{\text{malade}}(T = \text{ positif}) = \dfrac{99}{100}, \\ P_{\overline{\text{malade}}}(T = \text{ positif}) = \dfrac{1}{1000}. \end{cases}$$

On fait un test et il revient positif. Quelle est la probabilité d'avoir la maladie : $P_{T^+}(M)$?

$$\begin{aligned} P_{T^+}(M) &= \frac{P_M(T^+)\,P(M)}{P(T)} \\ &= \frac{\frac{99}{100}\times\frac{1}{10\,000}}{\frac{99}{100}\times\frac{1}{10\,000}\times\frac{9\,999}{10\,000}} \\ &= \frac{990}{990+9999} \simeq 9\,\% \end{aligned}$$

On a 9 % d'avoir la maladie : le test n'est pas très précis.

Exemple (QCM) :
On a un QCM de 20 questions où l'on peut répondre par vrai ou faux (donc c'est pas vraiment un QCM). Si un étudiant connaît la réponse, il réponds correctement. Sinon, il choisit l'une des réponses au hasard.

Soit p la probabilité qu'il connaisse la réponse à une question. Cela représente le niveau du candidat : un élève ayant travaillé aura une valeur de p plus importante qu'un élève n'ayant pas travaillé.

L'étudiant obtient $^{13}/_{20}$. Estimer p.

Comme $p \in [0,1]$, on découpe l'intervalle en 10 : on pose

$$\forall k \in [\![0,9]\!],\ A_k : \text{“ } p = \frac{k+0,5}{10}\text{ ”}.$$

On pose aussi

$$\begin{cases} \forall i \in [\![1,20]\!],\ B_i : \text{“ la } i\text{-ème réponse est correcte”}, \\ \forall j \in [\![0,20]\!],\ C_j : \text{“ l'étudiant a } {}^{j}/_{20}\text{”}, \end{cases}$$

On cherche donc $P_{C_{13}}(A_k)$. S'il n'y a pas de “pic” de probabilité (en fonction de k), il faut changer le QCM : augmenter le nombre de questions, mettre des questions plus faciles / difficiles...

On utilise la formule de Bayes :

$$P_{C_{13}}(A_k) = \frac{P_{A_k}(C_{13})\, P(A_k)}{P(C_{13})}.$$

On peut choisir $P(A_k)$: c'est subjectif. On peut avoir une distribution uniforme, ou suivant une courbe de Gauß, ...

On choisit $P(A_k) = \dfrac{1}{10}$: distribution uniforme.

$$P(C_{13}) = \sum_{k=0}^{9} P_{A_k}(C_{13})\, P(A_k);$$

$$P_{A_k}(C_{13}) = \binom{20}{13} \left(\frac{p+1}{2}\right)^{13} \left(1 - \frac{p+1}{2}\right)^{7}.$$

Proposition (Bayes) **:** Soit (Ω, P) un espace probabilisé et $(A_k)_{k\in K}$ un système complet d'événements tel que

$$\forall k \in K,\ P(A_k) \neq 0.$$

Soit $X \in \mathcal{P}(\Omega)$ tel que $P(X) \neq 0$. On a

$$\forall k \in K,\ P_X(A_k) = \frac{P_{A_k}(X)\, P(A_k)}{\sum_{j\in K} P_{A_j}(X) P(A_j)}.$$

□

3 Événements indépendants

Définition : Soient A et B deux événements d'un espace probabilisé (Ω, P). On dit que A et B sont indépendants si

$$P(A \cap B) = P(A)\, P(B).$$

Remarque :
L'indépendance d'événements au sens mathématique n'est pas la même chose que l'indépendance dans le sens commun : elle dépend de la probabilité utilisé !

Exemple :
On considère un objet, qui est défectueux avec une probabilité $p \in]0,1[$. On effectue deux contrôles indépendants. Chaque contrôle permet de détecter un défaut (s'il y en a un) avec une probabilité q (il n'y a pas de faux positifs : on ne peut pas trouver un défaut s'il n'y en a pas).

Les deux contrôles sont négatifs. Quelle est la probabilité qu'il y ait quand même un défaut ?

```python
import random as rd

def experience(p, q):
  defaut = bernoulli(p)
  controles = [False, False]

  for i in range(2):
    if defaut:
      controles[i] = bernoulli(q)

  return (controles, defaut)

def proba(p, q, N = 10000):
  cpt = 0
  pr = 0
  while cpt < N:
    c, d = experience(p, q)
    if not any(c): # deux controles negatifs
      cpt += 1

      if d:
        pr += 1
  return pr / N
```

Simulation en Python :

Pour générer une variable aléatoire de probabilité p en Python, on génère un réel $x \in [0,1]$ et on le compare à p :

```python
def bernoulli(p):
  return rd.random() < p
```

Modélisation : $\Omega = \{0,1\}^3$;
$D = \{0,1\}^2 \times \{1\}$ et $P(D) = p$;
$C_1 = \{1\} \times \{0,1\}^2$ et $P_D(C_1) = q$;
$C_2 = \{0,1\} \times \{1\} \times \{0,1\}$ et $P_D(C_2) = q$.

On sait que $P_{\bar{D}}(C_1) = P_{\bar{D}}(C_2) = 0$.

On suppose que C_1 et C_2 indépendants relativement à P_D.

$$P_{\bar{C}_1 \cap \bar{C}_2}(D) = \frac{P_D\left(\bar{C}_1 \cap \bar{C}_2\right) P(D)}{P\left(\bar{C}_1 \cap \bar{C}_2\right)}.$$

On a :

$$\begin{aligned} P_D\left(\bar{C}_1 \cap \bar{C}_2\right) &= P_D\left(\bar{C}_1\right) P_D\left(\bar{C}_2\right) \\ &= (1-q)^2, \end{aligned}$$

$$P(D) = p,$$

et

$$\begin{aligned} P\left(\bar{C}_1 \cap \bar{C}_2\right) &= P_D(\bar{C}_1 \cap \bar{C}_2)\, P(D) + P_{\bar{D}}(\bar{C}_1 \cap \bar{C}_2)\, P(\bar{D}). \\ &= p(1-q)^2 + 1 - p. \end{aligned}$$

Or,

$$\begin{aligned} P\left(\bar{C}_1\right)\, P\left(\bar{C}_2\right) &= \big((1-q)p + 1 - p\big)^2 \\ &\neq P\big(\bar{C}_1 \cap \bar{C}_2\big) \text{ en général.} \end{aligned}$$

Finalement,

$$P_{\bar{C}_1 \cap \bar{C}_2}(D) = \frac{p(1-q)^2}{p(1-q)^2 + 1 - p}.$$

Si $q = 1$, on a $P_{\bar{C}_1 \cap \bar{C}_2}(D) = 0$. Si $q = 0$, on a $P_{\bar{C}_1 \cap \bar{C}_2}(D) = p$.

Définition : Soit (Ω, P) un espace probabilisé et $(A_i)_{i \in I}$ une famille finie d'événements.

1. On dit que ces événements sont 2 à 2 indépendants si
$$\forall i \neq j, \quad P(A_i \cap A_j) = P(A_i)\, P(A_j)$$
2. On dit qu'ils sont mutuellement indépendants si
$$\forall J \in \mathcal{P}(I) \setminus \{\}, \quad P\Big(\bigcap_{j \in J} A_j\Big) = \prod_{j \in J} P(A_j).$$

Exemple :

À faire

$\Omega = \ldots$, $P = \ldots$, $A, B, C = \ldots$ tels que

$$\begin{cases} P(A \cap B) = P(A)\, P(B) \\ P(A \cap C) = P(A)\, P(C) \\ P(B \cap C) = P(B)\, P(C) \end{cases}$$

mais

$$P(A \cap B \cap C) \neq P(A)\, P(B)\, P(C).$$

Exercice :
Soit (Ω, P) un espace probabilisé fini, A et B deux événements indépendants (par rapport à P).

1. *Montrer que A et $\bar{B}$ sont indépendants.*
2. *Montrer que $\bar{A}$ et $\bar{B}$ sont indépendants.*

Solution :

1. On suppose $P(A) \neq 0$.

$$\begin{aligned} P\left(A \cap \bar{B}\right) &= P_A\left(\bar{B}\right) P(A) \\ &= P(A)\left(1 - P_A(B)\right) \\ &= P(A)\big(1 - P(B)\big) \\ &= P(A)\, P\left(\bar{B}\right) \end{aligned}$$

   On suppose $P(A) = 0$. $A \cap \bar{B} \subset A$ donc

$$0 \leqslant P\left(A \cap \bar{B}\right) \leqslant P(A) = 0$$

   et donc

$$P\left(A \cap \bar{B}\right) = 0 = P(A)\, P\left(\bar{B}\right).$$

2. C'est une conséquence du 1. : on remplace B par A et A par $\bar{B}$.

Proposition : Soit (Ω, P) un espace probabilisé et $(A_i)_{i\in I}$ une famille d'événements mutuellement indépendants. Soit $J \in \mathscr{P}(I)$ et on pose

$$\forall i \in I,\ B_i = \begin{cases} \bar{A}_i & \text{si } i \in J \\ A_i & \text{sinon.} \end{cases}$$

Alors, $(B_i)_{i\in I}$ est une famille d'événements mutuellement indépendants.

Preuve :
Pour $n \in \mathbb{N}^\star$, on pose

$$\mathscr{P}(n) : \text{“}\forall K \subset I \text{ avec } \#K = n,\ P\left(\bigcap_{i\in K} B_i\right) = \prod_{i\in K} P(B_i)\text{”}.$$

□

4 Bilan

Une probabilité est une application de la forme

$$P : \mathscr{P}(\Omega) \longrightarrow [0,1]$$

vérifiant

1. $P(\Omega) = 1$;
2. $\forall A, B,\ P(A \cup B) = P(A) + P(B)$.

Équiprobabilité

$$P : \mathcal{P}(\Omega) \longrightarrow [0,1]$$
$$A \longmapsto \frac{\#A}{\#\Omega}.$$

Si $A \cap B = $, on dit qu'il sont incompatibles.

Si on associe à chaque événement élémentaire ω_i une "valeur" ($\simeq$ probabilité) p_i, alors il existe une unique probabilité P sur Ω vérifiant $P(\omega_i) = p_i$.

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i).$$

$\forall A, B, P(A \cup B) = P(A) + P(B) - P(A \cap$

Probabilité conditionnelle

Pour tout événement A de Ω de probabilité non nulle,

$$P_A : \mathcal{P}(\Omega) \longrightarrow [0,1]$$
$$X \longmapsto \frac{P(A \cap X)}{P(A)}.$$

Un système complet d'événements est une partition de Ω.

Probabilités totales

$$\forall X \in \mathcal{P}(\Omega), P(X) = \sum_{i=1}^{n} P(A_i)\, P_{A_i}(X).$$

A et B sont deux événements indépendants si

$$P(A \cap B) = P(A)\, P(B).$$

$(A_i)_{i \in I}$ est une famille finie d'événements mutuellement indépendants si

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

Probabilités composées

$$P(A_1 \cap \cdots \cap A_n) = P(A_1)\, P_{A_1}(A_2)\, P_{A_1 \cap A_2}(A_3) \cdots P_{A_1 \cap \cdots \cap A_{n-1}}(A_n).$$

Bayes

$$P_A(B) = \frac{P_B(A)\, P(B)}{P(A)}.$$

Pour plusieurs événements

$$\forall k \in K,\ P_X(A_k) = \frac{P_{A_k}(X)\ P(A_k)}{\sum_{j\in K} P_{A_j}(X)\, P(A_j)}.$$

Chapitre 28

Sous-espaces affines d'un espace vectoriel

1 Espace affine (Hors Programme)

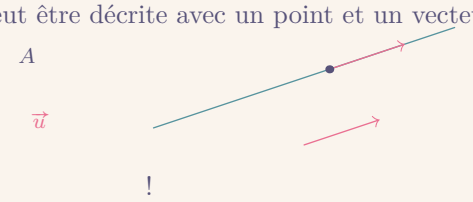
Motivation géométrique :

Dans les petites classes, la géométrie du plan distingue deux types d'objets élémentaires :

— le point
— le vecteur

reliés par la notion de translation.

Par exemple, une droite peut être décrite avec un point et un vecteur :



!

Soit $\mathbb{K}$ un corps.

Définition : Un $\mathbb{K}$-espace affine est un triplet $\left(E, \vec{E}, \tau\right)$ où

— E est un ensemble ;

— $\vec{E}$ est un $\mathbb{K}$-espace vectoriel ;

— $\tau : E \times \vec{E} \longrightarrow E$ telle que

$$\begin{cases} \forall M \in E,\ \tau\left(M, \vec{0}\right) = M, \\ \forall M \in E,\ \forall (\vec{u}, \vec{v}) \in \vec{E}^2, \tau\Big(\tau\left(M, \vec{u}\right), \vec{v}\Big) = \tau\left(M, \vec{u} + \vec{v}\right), \\ \forall (A, B) \in E^2,\ \exists! \vec{u} \in \vec{E}, \tau\left(A, \vec{u}\right) = B. \end{cases}$$

Les éléments de E sont appelés points, ceux de $\vec{E}$ vecteurs.

Pour tout $\vec{u} \in \vec{E}$, l'application

$$\begin{array}{ccc} E & \longrightarrow & E \\ M & \longmapsto & \tau\left(M, \vec{u}\right) \end{array}$$

est la translation de vecteur $\vec{u}$.

En général, pour $M \in E$ et $\vec{u} \in \vec{E}$, au lieu d'écrire $\tau\left(M + \vec{u}\right)$, on écrit $M + \vec{u}$. Soient $(A, B) \in E^2$. L'unique vecteur $\vec{u}$ tel que $A + \vec{u} = B$ est noté $\overrightarrow{AB} = B - A$.

Exemple : 1. On pose

$$(\mathscr{E}) : \quad y' = xy + xe^x$$

Soit E l'ensemble des solutions de $(\mathscr{E})$, $\vec{E}$ le $\mathbb{R}$-espace vectoriel des solutions de

$$(\mathscr{H}) : \quad y' = xy,$$

et

$$\begin{array}{c} \tau : E \times \vec{E} \longrightarrow E \\ (f, \vec{u}) \longmapsto f + \vec{u} \end{array}$$

où $+$ correspond à l'addition de fonctions.

— $\forall f \in E,\ \tau\left(f, \vec{0}\right) = f + 0 = f.$

—

$$\begin{aligned} \forall f \in E,\ \forall (h_1, h_2) \in \vec{E}^2,\ \tau\big(\tau(f, h_1), h_2\big) &= \tau(f + h_1, h_2) \\ &= (f + h_1) + h_2 \\ &= f + (h_1 + h_2) \\ &= \tau\big(f, \tau(h_1, h_2)\big) \end{aligned}$$

— Soient $(f_1, f_2) \in E^2$. On pose $h = f_2 - f_1 \in \vec{E}$ ($-$ est la soustraction de fonctions) et alors $\tau(f_1, h) = f_2$ et h est unique.

2. On pose $E = \mathbb{R}^2$, $\vec{E} = \mathbb{R}^2$ et

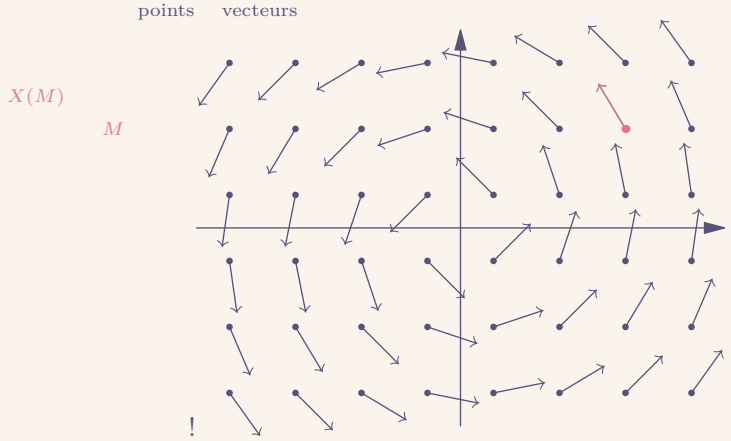
$$\begin{array}{c} \tau : E \times \vec{E} \longrightarrow E \\ \big((x, y), (u, v)\big) \longmapsto (x + u, y + v). \end{array}$$

$\left(E, \vec{E}, \tau\right)$ est un $\mathbb{R}$-espace affine.

Proposition : Soit E un $\mathbb{K}$-espace vectoriel. Alors $(E, E, +)$ est un $\mathbb{K}$-espace affine. □

Exemple :
Soit E un $\mathbb{K}$-espace vectoriel. Un champ de vecteur est une application

$$X : \underset{\text{points}}{E} \longrightarrow \underset{\text{vecteurs}}{E}.$$



Exemple :
Avec $F = \mathbb{R}^2$ et $E = \{(x, y) \in F \mid 2x + 3y = 5\}$, $(E, +, \cdot)$ n'est pas un $\mathbb{R}$-espace vectoriel : $(0, 0) \notin E$.

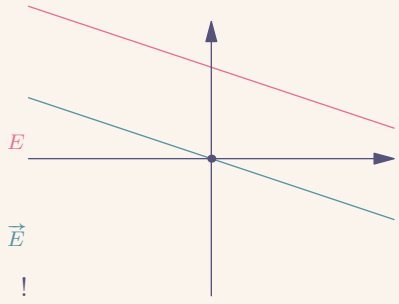
On pose $\vec{E} = \{(x, y) \in F \mid 2x + 3y = 0\}$, c'est un sous-espace vectoriel de F.
On pose

$$\begin{aligned} \tau : E \times \vec{E} &\longrightarrow E \\ \big((x, y), (u, v)\big) &\longmapsto (x + u, y + v). \end{aligned}$$

En effet,

$$\begin{aligned} \forall (x, y) \in E, \forall (u, v) \in \vec{E}, 2(x + u) + 3(y + v) &= 2x + 3y + 2u + 3v \\ &= 5 + 0 = 5 \end{aligned}$$

donc $\tau\big((x, y), (u, v)\big) \in E$.



Exemple :
Avec E les solutions de $y' = 3y + e^x$, $\vec{E} = \mathbb{R}$, et

$$\begin{aligned} \tau : E \times \vec{E} &\longrightarrow E \\ (y, \lambda) &\longmapsto \left(x \mapsto y(x) + \lambda e^{3x}\right). \end{aligned}$$

Proposition : Soit $\left(E, \vec{E}, \tau\right)$ un $\mathbb{K}$-espace affine. Si $E \neq$,

$$\vec{E} = \left\{\overrightarrow{AB} \mid (A, B) \in \vec{E}\right\}.$$

Preuve :
— $\forall A, B \in E,\ \overrightarrow{AB} \in \vec{E}$.
— Soit $\vec{u} \in \vec{E}$. Comme $E \neq$, on choisit $A \in E$. On pose $B = A + \vec{u}$. D'où $\vec{u} = \overrightarrow{AB}$.

□

Remarque :
On a même démontré que, pour tout $A \in E$, l'application

$$\begin{aligned} \varphi_A : \vec{E} &\longrightarrow E \\ \vec{u} &\longmapsto A + \vec{u} \end{aligned}$$

est bijective. On dit qu'on a vectorialisé E au point A :

$$\begin{cases} M + N := A + \overrightarrow{AM} + \overrightarrow{AN} \\ \lambda N := A + \lambda \overrightarrow{AM} \end{cases}$$

Proposition : Soit $\left(E, \vec{E}, \tau\right)$ un $\mathbb{K}$-espace affine.

1. $\forall A \in E,\ \overrightarrow{AA} = \vec{0}$;
2. $\forall A, B, C \in E,\ \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$;
3. $\forall A, B \in E,\ \overrightarrow{BA} = -\overrightarrow{AB}$.

Preuve :
1. Soit $A \in E$. $\tau\left(A, \overrightarrow{AA}\right) = A = \tau\left(A, \vec{0}\right)$ donc $\overrightarrow{AA} = \vec{0}$.
2. Soient $A, B, C \in E$. On pose $\vec{u} = \overrightarrow{AB}$ et $\vec{v} = \overrightarrow{BC}$.

$$\begin{array}{ccc} \tau\left(\tau\left(A, \vec{u}\right), \vec{v}\right) = \tau\left(B, \vec{v}\right) = C = \tau\left(A, \overrightarrow{AC}\right) \\ \| \\ \tau\left(A, \vec{u} + \vec{v}\right) \end{array}$$

3. Soient $A, B \in E$. D'après 1. $\overrightarrow{AA} = \vec{0}$ et, d'après 2. $\overrightarrow{AA} = \overrightarrow{AB} + \overrightarrow{BA}$. Donc $\overrightarrow{AB} = -\overrightarrow{BA}$.

□

2 Sous-espaces affines

Définition : Soit $\left(E, \vec{E}, \tau\right)$ un $\mathbb{K}$-espace affine et $F \in \mathcal{P}(E) \setminus \{\}$.

Pour tout $A \in F$, on pose $\overrightarrow{F_A} = \left\{\overrightarrow{AB} \mid B \in F\right\}$. On dit que F est un sous-espace affine de $\left(E, \vec{E}, \tau\right)$ s'il existe $A \in F$ tel que $\overrightarrow{F_A}$ est un sous-espace vectoriel de $\vec{E}$.

Proposition : Avec les notations précédentes, $\left(F, \overrightarrow{F_A}, \tau_{|F \times \overrightarrow{F_A}}\right)$ est un espace affine.

Preuve : — Soit $M \in F$, $\vec{u} \in \overrightarrow{F_A}$.

$$M + \vec{u} = A + \underbrace{\underbrace{\overrightarrow{AM}}_{\in \overrightarrow{F_A}} \underbrace{\vec{u}}_{\in \overrightarrow{F_A}}}_{\in \overrightarrow{F_A}} = A + \underbrace{\overrightarrow{AB}}_{B \in F} = B \in F.$$

— Soit $M \in F$, $\vec{u}, \vec{v} \in \overrightarrow{F_A}$.

$$(M + \vec{u}) + \vec{v} = M + (\vec{u} + \vec{v})$$

car $M \in E$ et $\vec{u}, \vec{v} \in \vec{E}$.

— Soient $M, N \in F \subset E$. On sait que

$$\exists! \vec{u} \in \vec{E},\ M + \vec{u} = N.$$

$$\begin{aligned} \vec{u} = \overrightarrow{MN} &= \overrightarrow{MA} + \overrightarrow{AN} \\ &= \underbrace{\overrightarrow{AN}}_{\in \overrightarrow{F_A}} - \underbrace{\overrightarrow{AM}}_{\in \overrightarrow{F_A}} \in \overrightarrow{F_A} \end{aligned}$$

□

Proposition : Soit F un sous-espace affine de $\left(E, \vec{E}, \tau\right)$. Alors

$$\forall (A, B) \in F^2,\ \overrightarrow{F_A} = \overrightarrow{F_B}.$$

Preuve :
Soit A comme dans la définition ($\overrightarrow{F_A}$ sous-espace vectoriel de $\vec{E}$) et $B \in F$.
Soit $\vec{u} \in \overrightarrow{F_B}$. Alors $\vec{u} = \overrightarrow{BM}$ avec $M \in F$.

$$\vec{u} = \overrightarrow{BA} + \overrightarrow{AM} = \overrightarrow{AM} - \overrightarrow{AB} \in \overrightarrow{F_A}.$$

Soit $\vec{v} \in \overrightarrow{F_A}$. On pose $M = \underbrace{M}_{} + \underbrace{\vec{v}}_{\in \overrightarrow{F_A}} \in F$. Donc $\vec{v} = \overrightarrow{BM} \in \overrightarrow{F_B}$. □

Corollaire : Soit $f \in \mathscr{L}(E, F)$ et $y \in F$.

Les solutions de l'équation $f(x) = y$ est un sous-espace affine de direction $\operatorname{Ker} f$. □

Proposition : Soit $(F_i)_{i \in I}$ une famille de sous-espaces affines de F. Alors, $\bigcap_{i \in I} F_i$ est soit vide, soit un sous-espace affine de F.

De même que pour les groupes et les espaces vectoriels, on peut définir le sous-espace engendré par une partie de E.

Proposition–Définition : Soit $A \in \mathscr{P}(E)$. Le sous-espace affine engendré par A est

$$\bigcap_{\substack{F \text{ sous-espace affine de } E \\ A \subset F}} F.$$

C'est le plus petit (au sens de l'inclusion) sous-espace affine contenant A.

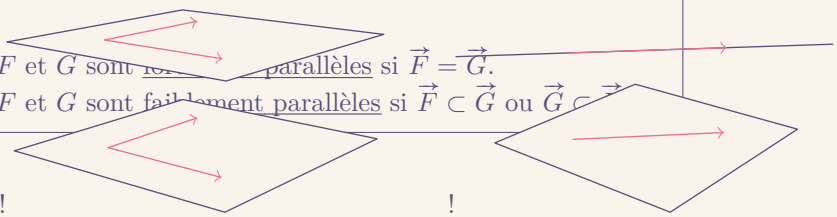
Remarque :
Si E est un $\mathbb{K}$-espace vectoriel et F un sous-espace affine de E, alors

$$\begin{cases} \forall A \in F,\ F = A + \vec{F} = \{A + \vec{u} \mid \vec{u} \in \vec{F}\}, \\ \vec{F} \text{ sous-espace vectoriel de } E. \end{cases}$$

3 Parallèlisme et hyperplans

Définition : Soit $\left(E, \vec{E}, \tau\right)$ un espace affine, F et G deux sous-espaces affines de E.

1. On dit que F et G sont fortement parallèles si $\vec{F} = \vec{G}$.
2. On dit que F et G sont faiblement parallèles si $\vec{F} \subset \vec{G}$ ou $\vec{G} \subset \vec{F}$.



!

(a) parallélisme fort

!

(b) parallélisme faible

Définition : Soit F un sous-espace affine de $\left(E, \vec{E}, \tau\right)$. L'espace

$$\vec{F} = \left\{\overrightarrow{AB} \mid A, B \in F\right\}$$

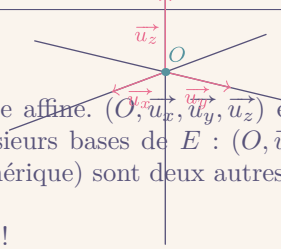
est appelé direction de F.

On dit que

- F est une droite affine si $\vec{F}$ est une droite vectorielle,
- F est une plan affine si $\vec{F}$ est un plan vectorielle,
- F est une hyperplan affine si $\vec{F}$ est un hyperplan vectorielle.

4 Repère affine

Définition : Soit F un sous-espaca affine de E. Un repère de F est la donnée d'un point $A \in F$ ("l'origine du repère") et d'une base $\mathcal{B} = (\vec{e_i})_{i \in I}$ de $\vec{F}$ ("vecteurs direction").



Exemple (mécanique – physique) :
On pose $E = (\mathbb{R}^3, \mathbb{R}^3, +)$, un $\mathbb{R}$-espace affine. $(O, \overrightarrow{u_x}, \overrightarrow{u_y}, \overrightarrow{u_z})$ est une base de E : la base carthésienne. Il existe plusieurs bases de E : $(O, \overrightarrow{u_r}, \overrightarrow{u_\theta}, \overrightarrow{u_z})$ (base cylindrique) et $(O, \overrightarrow{u_r}, \overrightarrow{u_\theta}, \overrightarrow{u_\varphi})$ (base sphérique) sont deux autres bases de E.

!

Proposition–Définition : Soit F un sous-espace affine de E, et $\mathcal{R} = (A, \vec{e_1}, \ldots, \vec{e_n})$ un repère de F. Alors, pour tout $B \in F$,

$$\exists!(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n,\ B = A + \sum_{i=1}^{n} \lambda_i \vec{e_i}.$$

On dit que $(\lambda_1, \ldots, \lambda_n)$ sont les coordonées de B.

Remarque :
Les solutions d'un problème linéaire forment un espace sous-affine de direction les solutions du système homogène associé.

Chapitre 29

Produit scalaire

Dans ce chapitre, E désigne un $\mathbb{R}$-espace vectoriel.

On sait déjà calculer le produit scalaire en dimension 2 et 3 mais l'objectif de ce chapitre est de le généraliser en dimension potentiellement infinie.

1 Définitions

Définition : Un produit scalaire sur E est une forme bilinéaire symétrique définie positive :

$$f : E \times E \longrightarrow \mathbb{R}$$

1. $\forall (u_1, u_2, v) \in E^3, \forall (\alpha, \beta) \in \mathbb{R}^2, f(\alpha u_1 + \beta u_2, v) = \alpha f(u_1, v) + \beta f(u_2, v)$, (bilinéaire)
2. $\forall (u, v) \in E^2,\ f(u, v) = f(v, u)$, (symétrie)
3. $\forall u \in E,\ f(u, u) \geqslant 0$, (positive)
4. $\forall u \in E,\ \big(f(u, u) = 0 \iff u = 0_E\big)$. (définie)

On dit alors que (E, f) est un espace préhilbertien. Si, de plus, E est de dimension finie, alors on dit que (E, f) est un espace euclidien.

En général, on note $\langle u \mid v \rangle$, $\langle u, v \rangle$ ou $(u \mid v)$ à la place de $f(u, v)$.

Remarque :
Même si elle est utilisée (notament au lycée), la notation $u \cdot v$ est dangeureuse car elle peut être facilement confondue par la multiplication.

Exemple : 1. Avec $E = \mathbb{R}^2$, on a $\big\langle (x, y) \mid (x', y') \big\rangle = xx' + yy'$.

2. Avec $E = \mathbb{R}^n$, on a $\big\langle (x_1, \dots, x_n) \mid (y_1, \dots, y_n) \big\rangle = \sum_{i=1}^{n} x_i y_i$.

3. Avec $E = \mathscr{C}^0\big([a, b], \mathbb{R}\big)$, on a $\langle f \mid g \rangle = \displaystyle\int_a^b f(t)g(t)\ \mathrm{d}t$.

4. Avec $E = \ell^1(\mathbb{R}) = \{u \in \mathbb{R}^{\mathbb{N}} \mid \sum |u_n| \text{ converge}\}$, on a $\langle u \mid v\rangle = \sum_{n=0}^{+\infty} u_n v_n$.
   En effet, $v \in E$ donc $\sum |v_n|$ converge et donc $v_n \xrightarrow[n\to+\infty]{} 0$. On a donc
   $$\exists N \in \mathbb{N},\ \forall n \geqslant N,\ |v_n| \leqslant 1$$
   donc
   $$\exists N \in \mathbb{N},\ \forall n \geqslant N,\ |u_n v_n| \leqslant |u_n|.$$
   Comme $\sum |u_n|$ converge, on en déduit que $\sum |u_n v_n|$ aussi.
5. Avec $E = \mathbb{R}^2$, on a $\big\langle (x,y) \mid (x',y')\big\rangle = xx' + 2xy' + 2yx' + 5yy'$.
   — On fixe $(x',y') \in E$. Soient $(x_1,y_1) \in E$, $(x_2,y_2) \in E$ et $(\lambda_1,\lambda_2) \in \mathbb{R}^2$.
   $$\begin{aligned}\big\langle \lambda_1(x_1,y_1) + \lambda_2(x_2,y_2) \mid (x',y')\big\rangle &= \big\langle (\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2) \mid (x',y')\big\rangle \\ &= \quad (\lambda_1 x_1 + \lambda_2 x_2)x' + 2(\lambda_1 x_1 + \lambda_2 x_2)y' \\ &\quad + 2(\lambda y_1 + \lambda_2 y_2)x' + 5(\lambda_1 y_1 + \lambda_2 y_2)y' \\ &= \quad \lambda_1(x_1 x' + 2x_1 y' + 2y_1 x' + 5y_1 y') \\ &\quad + \lambda_2(x_2 x' + 2x_2 y' + 2y_2 x' + 5y_2 y') \\ &= \lambda_1\big\langle (x_1,y_1) \mid (x',y')\big\rangle + \lambda_2\big\langle (x_2,y_2) \mid (x',y')\big\rangle\end{aligned}$$
   — Soit $(x,y) \in E$ et $(x',y') \in E$.
   $$\begin{aligned}\big\langle (x',y') \mid (x,y)\big\rangle &= x'x + 2x'y + 2y'x + 3y'y \\ &= \big\langle (x,y) \mid (x',y')\big\rangle\end{aligned}$$
   — Soit $(x,y) \in E$.
   $$\begin{aligned}\big\langle (x,y) \mid (x,y)\big\rangle &= x^2 + 4xy + 5y^2 \\ &= (x+2y)^2 + y^2 \geqslant 0\end{aligned}$$
   — Soit $(x,y) \in E$.
   $$\begin{aligned}\big\langle (x,y) \mid (x,y)\big\rangle = 0 &\iff (x+2y)^2 + y^2 = 0 \\ &\iff \begin{cases} y^2 = 0 \\ (x+2y)^2 = 0 \end{cases} \\ &\iff \begin{cases} y = 0 \\ x = 0 \end{cases}\end{aligned}$$

Définition : Soit $(E, \langle \cdot \mid \cdot \rangle)$ un esapce préhilbertien. Soit $x \in E$.

La norme (euclidienne) de x est

$$\sqrt{\langle x \mid x\rangle} = \|x\|.$$

Proposition :
1. $\forall x \in E,\ \|x\| = 0 \iff x = 0_E$ (séparation)
2. $\forall x \in E,\ \forall \lambda \in \mathbb{R},\ \|\lambda x\| = |\lambda|\,\|x\|$ (homogénéité positive)
3. $\forall (x,y) \in E^2,\ \|x+y\| \leqslant \|x\| + \|y\|$ (inégalité triangulaire)

□

L'inégalité triangulaire sera prouvée dans la suite du chapitre (paragraphe 2.).

Définition : Soit $(x,y) \in E^2$. On dit que x et y sont orthogonaux si $\langle x \mid y\rangle = 0$. On note cette situation $x \perp y$.

Exemple :
Avec $E = \mathscr{C}^0\big([-1,1],\mathbb{R}\big)$ et $\langle f \mid g\rangle = \displaystyle\int_{-1}^{1} f(t)\,g(t)\,\mathrm{d}t$. Soit f paire et g impaire. Alors $f \perp g$. Dans ce cas, on peut appliquer le théorème de Pythagore (vu dans la suite du chapitre) :

$$\|f+g\|^2 = \|f\|^2 + \|g\|^2.$$

2 Quelques formules

Dans ce paragraphe, $\big(E, \langle\cdot \mid \cdot\rangle\big)$ est un espace préhilbertien.

Proposition : Soient $x, y \in E$.
1. $\|x+y\|^2 = \|x\|^2 + \|y\|^2 + 2\,\langle x \mid y\rangle$.
2. $\|x+y\|^2 + \|x-y\|^2 = 2\big(\|x\|^2 + \|y\|^2\big)$. (identité du parallélogramme)
3. $\langle x \mid y\rangle = \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right)$. (polarisation)

Preuve : 1.

$$\begin{aligned}\|x+y\|^2 &= \langle x+y \mid x+y\rangle\\ &= \langle x \mid x+y\rangle + \langle y \mid x+y\rangle\\ &= \langle x \mid x\rangle + \langle x \mid y\rangle + \langle y \mid x\rangle + \langle y \mid y\rangle\\ &= \|x\|^2 + \|y\|^2 + 2\,\langle x \mid y\rangle\end{aligned}$$

2.

$$\begin{aligned}\|x+y\|^2+\|x-y\|^2 &= \|x\|^2+\|y\|^2+2\langle x \mid y\rangle \\ &\quad +\|x\|^2+\|-y\|^2+2\langle x \mid -y\rangle \\ &= 2\|x\|^2+2\|y\|^2\end{aligned}$$

3.

□

Théorème (inégalité de Cauchy–Schwarz) **:** Soient $x, y \in E$. Alors

$$\left|\langle x \mid y\rangle\right| \leqslant \|x\|\,\|y\|$$

et

$$\left|\langle x \mid y\rangle\right| = \|x\|\,\|y\| \iff x \text{ et } y \text{ sont colinéaires.}$$

Preuve :
On fixe $(x, y) \in E^2$.

— On suppose $y \neq 0_E$. Soit

$$\begin{aligned}f : \mathbb{R} &\longrightarrow \mathbb{R} \\ t &\longmapsto \|x+ty\|.\end{aligned}$$

$$\begin{aligned}\forall t \in \mathbb{R},\ f(t) &= \|x\|^2+2\langle x \mid ty\rangle+\|ty\|^2 \\ &= \|x\|^2+2t\langle x \mid y\rangle+t^2\|y\|^2.\end{aligned}$$

Comme $y \neq 0_E$, $\|y\|^2 \neq 0$ et f est donc une fonction polynomiale de degré 2.

En outre,

$$\forall t \in \mathbb{R},\ f(t) \geqslant 0.$$

Donc le discriminant Δ de f est négatif ou nul. Or,

$$\Delta = 4\langle x \mid y\rangle^2 - 4\|x\|^2\|y\|^2.$$

Ainsi

$$\langle x \mid y\rangle^2 \leqslant \|x\|^2\|y\|^2$$

et donc

$$\left|\langle x \mid y\rangle\right| \leqslant \|x\|\,\|y\|.$$

On suppose que $|\langle x \mid y\rangle| = \|x\|\,\|y\|$. Dans ce cas, $\Delta = 0$. Soit $\lambda \in \mathbb{R}$ tel que $f(\lambda) = 0$, i.e. $\|x+\lambda y\| = 0$ et donc $x = -\lambda y$, donc x et y sont colinéaires.

La réciproque est immédiate.

— On suppose $y = 0_E$.

$$|\langle x \mid y\rangle| = |\langle x \mid 0_E\rangle| = 0 \qquad \text{et} \qquad \|x\|\,\|y\| = \|x\| \times 0 = 0.$$

On a bien

$$\begin{cases} |\langle x \mid y\rangle| \leqslant \|x\|\,\|y\|; \\ y \text{ et } x \text{ sont colinéaires.} \end{cases}$$

□

Corollaire (inégalité triangulaire) **:** Soit $(x, y) \in E^2$.

1. $\|x+y\| \leqslant \|x\| + \|y\|$.
2. $\|x+y\| = \|x\| + \|y\| \iff \exists \lambda \in \mathbb{R}^+,\ \big(x = \lambda y \text{ ou } y = \lambda x\big)$.

Preuve : 1.

$$\begin{aligned} \|x+y\|^2 &= \|x\|^2 + \|y\|^2 + 2\langle x \mid y\rangle \\ &\leqslant \|x\|^2 + \|y\|^2 + 2|\langle x \mid y\rangle| \\ &\leqslant \|x\|^2 + \|y\|^2 + 2\|x\|\,\|y\| \\ &\leqslant \big(\|x\| + \|y\|\big)^2. \end{aligned}$$

D'où

$$\|x+y\| \leqslant \|x\| + \|y\|.$$

2.

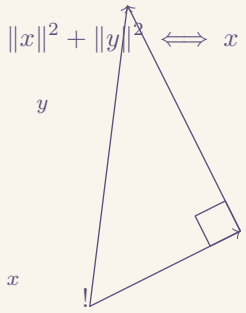
$$\begin{aligned} \|x+y\| = \|x\| + \|y\| &\iff \|x+y\|^2 = \big(\|x\| + \|y\|\big)^2 \\ &\iff \|x\|^2 + \|y\|^2 + 2\langle x \mid y\rangle = \|x\|^2 + \|y\|^2 + 2\|x\|\,\|y\| \\ &\iff \langle x \mid y\rangle = \|x\|\|y\| \\ &\iff \begin{cases} \langle x \mid y\rangle \geqslant 0 \\ |\langle x \mid y\rangle| = \|x\|\|y\| \end{cases} \\ &\iff \begin{cases} \exists \lambda \in \mathbb{R},\ x = \lambda y \text{ ou } y = \lambda x \\ \langle x \mid y\rangle \geqslant 0 \end{cases} \\ &\iff \exists \lambda \in \mathbb{R}^+,\ x = \lambda y \text{ ou } y = \lambda x. \end{aligned}$$

□

3 Familles orthogonales

Théorème (Pythagore) **:** Soit $(x, y) \in E^2$.

$$\|x+y\|^2 = \|x\|^2 + \|y\|^2 \iff x \perp y.$$



Preuve :

$$\|x+y\|^2 = \|x\|^2 + \|y\|^2 \iff 2\langle x \mid y\rangle = 0 \iff x \perp y.$$

□

Définition : Soit $(e_i)_{i\in I}$ une famille de vecteurs. On dit que cette famille est orthogonale si

$$\forall i \neq j \; e_i \perp e_j.$$

Si, en plus, on a

$$\forall i \in I, \; \|e_i\| = 1,$$

alors on dit que la famille est orthonormale ou orthonormée.

Proposition (Pythagore) **:** Soit $(e_1, \ldots, e_n)$ une famille orthogonale. Alors

$$\left\| \sum_{i=1}^{n} e_i \right\|^2 = \sum_{i=1}^{n} \|e_i\|^2.$$

Théorème : Toute famille orthogonale de vecteurs non nuls est libre.

Preuve :
Soit $(e_i)_{i\in I}$ une famille orthogonale telle que

$$\forall i \in I, \; e_i \neq 0_E.$$

Soit $n \in \mathbb{N}^\star$, $(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n$. On suppose

$$\sum_{k=1}^{n} \lambda_k e_{i_k} = 0_E.$$

Soit $j \in [\![1, n]\!]$.

$$\begin{aligned} 0 &= \left\langle \sum_{k=1}^{n} \lambda_k e_{i_k} \mid e_{i_j} \right\rangle \\ &= \sum_{k=1}^{n} \lambda_k \left\langle e_{i_k} \mid e_{i_j} \right\rangle \\ &= \lambda_j \underbrace{\|e_{i_j}\|^2}_{\neq 0} \end{aligned}$$

donc $\lambda_j = 0$. □

Algorithme (Orthonormalisation de Gran–Schmidt) **:** On suppose E de dimension finie. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

— *Étape 1* : On pose $v_1 = \dfrac{e_1}{\|e_1\|}$ de sorte que $\|v_1\| = 1$.

— *Étape 2* : On pose

$$u_2 = e_2 - \langle e_2 \mid v_1 \rangle v_1.$$

Ainsi,

$$\begin{aligned} \langle u_2 \mid v_1 \rangle &= \langle e_2 - \langle e_2 \mid v_1 \rangle v_1 \mid v_1 \rangle \\ &= \langle e_2 \mid v_1 \rangle - \langle e_2 \mid v_1 \rangle \langle v_1 \mid v_1 \rangle \\ &= 0. \end{aligned}$$

On pose $v_2 = \dfrac{u_2}{\|u_2\|}$ donc $v_2 \perp v_1$ et $\|v_2\| = 1$.

— *Étape 3* : On pose

$$u_2 = e_3 - \langle e_3 \mid v_1 \rangle v_1 - \langle e_3 \mid v_2 \rangle v_2.$$

Ainsi,

$$\begin{aligned} \langle u_3 \mid v_1 \rangle &= \langle e_3 \mid v_1 \rangle - \langle e_3 \mid v_1 \rangle \underbrace{\langle v_1 \mid v_1 \rangle}_{=1} - \langle e_3 \mid v_2 \rangle \underbrace{\langle v_2 \mid v_1 \rangle}_{=0} \\ &= 0 \end{aligned}$$

et

$$\begin{aligned}\langle u_3 \mid v_2\rangle &= \langle e_3 \mid v_2\rangle - \langle e_3 \mid v_1\rangle \underbrace{\langle v_1 \mid v_2\rangle}_{=0} - \langle e_3 \mid v_2\rangle \underbrace{\langle v_2 \mid v_2\rangle}_{=1}\\ &= 0.\end{aligned}$$

On pose $v_3 = \dfrac{u_3}{\|u_3\|}$ de sorte que $v_3 \perp v_1$, $v_3 \perp v_2$ et $\|v_3\| = 1$.

— *Étape $i+1$* : On pose

$$u_{i+1} = e_{i+1} - \sum_{k=1}^{i} \langle e_{i+1} \mid v_k\rangle\, v_k.$$

Ainsi, pour tout $j \in [\![1, i]\!]$, on a

$$\begin{aligned}\langle u_{i+1} \mid v_j\rangle &= \langle e_{i+1} \mid v_j\rangle - \sum_{k=1}^{i} \langle e_{i+1} \mid v_k\rangle \langle v_k \mid v_j\rangle\\ &= \langle e_{i+1} \mid v_j\rangle - \langle e_{i+1} \mid v_j\rangle \|v_j\|^2\\ &= 0.\end{aligned}$$

On pose $v_{i+1} = \dfrac{u_{i+1}}{\|u_{i+1}\|}$.

Exemple :
Avec $E = \mathbb{R}_3[X]$, $\langle P \mid Q\rangle = \displaystyle\int_0^1 P(t)\,Q(t)\,\mathrm{d}t$ et $\mathcal{B} = (1, X, X^2, X^3)$.

1. $\|1\|^2 = \langle 1 \mid 1\rangle = \displaystyle\int_0^1 1\,\mathrm{d}t = 1$ et donc $v_1 = 1$.
2. $u_2 = X - \langle X \mid v_1\rangle\, v_1$. Or, $\langle X \mid v_1\rangle = \displaystyle\int_0^1 t\,\mathrm{d}t = \frac{1}{2}$. D'où $u_2 = X - \frac{1}{2}$.

$$\begin{aligned}\|u_2\|^2 &= \int_0^1 \left(t - \frac{1}{2}\right)^2 \mathrm{d}t\\ &= \int_0^1 \left(t^2 - t + \frac{1}{4}\right) \mathrm{d}t\\ &= \frac{1}{3} - \frac{1}{2} + \frac{1}{4}\\ &= \frac{1}{12}\end{aligned}$$

On en déduit que $v_2 = \sqrt{12}\left(X - \dfrac{1}{2}\right)$.

3. $u_3 = X^2 - \langle X^2 \mid v_1 \rangle v_1 - \langle X^2 \mid v_2 \rangle v_2$. On a

$$\langle X^2 \mid v_1 \rangle = \int_0^1 t^2 \, \mathrm{d}t = \frac{1}{3}$$

et

$$\begin{aligned} \langle X^2 \mid v_2 \rangle &= \sqrt{12} \int_0^1 t^2 \left(t - \frac{1}{2} \right) \, \mathrm{d}t \\ &= \frac{\sqrt{12}}{12}. \end{aligned}$$

D'où

$$\begin{aligned} u_3 &= X^2 - \frac{1}{3} - \frac{\sqrt{12}}{12}\sqrt{12}\left(X - \frac{1}{2} \right) \\ &= X^2 - \frac{1}{3} - X + \frac{1}{2} \\ &= X^2 - X + \frac{1}{6}. \end{aligned}$$

$$\begin{aligned} \|u_3\|^2 &= \int_0^1 \left(t^2 - t + \frac{1}{6} \right) \, \mathrm{d}t \\ &= \int_0^1 \left(t^4 + t^2 + \frac{1}{36} - 2t^3 + \frac{t^2}{3} - \frac{t}{3} \right) \, \mathrm{d}t \\ &= \frac{1}{5} + \frac{1}{3} + \frac{1}{36} - \frac{1}{2} + \frac{1}{9} - \frac{1}{6} \\ &= \frac{36 + 60 + 5 - 90 + 20 - 30}{180} \\ &= \frac{1}{180} \end{aligned}$$

On en déduit que

$$v_3 = 6\sqrt{5}\left(X^2 - X + \frac{1}{6} \right).$$

4. Exercice : calculer v_4.

Proposition : Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E et $\mathscr{C}$ la base obtenue par le procédé d'orthonormalisation de Gram–Schmidt. Alors,

$$\forall i \in [\![1, n]\!], \ \mathrm{Vect}(e_1, \ldots, e_i) = \mathrm{Vect}(v_1, \ldots, v_i).$$

□

Exemple (orthogonalisation) : — $u_1 = 1$.

—
$$\left.\begin{array}{l} u_2 \in \mathrm{Vect}(e_1, e_2) \\ u_2 \perp u_1 \end{array}\right\} \iff \begin{cases} u_2 = ae_1 + be_2 \quad (a,b) \in \mathbb{R}^2 \\ \langle u_1 \mid u_2 \rangle = 0 \end{cases}$$
$$\iff \begin{cases} u_2 = a + bX \\ \displaystyle\int_0^1 (a+bt)\ \mathrm{d}t = 0. \end{cases}$$

$$\int_0^1 (a+bt)\ \mathrm{d}t = 0 \iff a + \frac{b}{2} = 0$$
$$\iff a = -\frac{b}{2}$$
$$\iff u_2 = -\frac{b}{2} + bX.$$

Par exemple, $u_2 = -1 + 2X$.

— $\begin{cases} u_3 \in \mathrm{Vect}(e_1, e_2, e_3) \\ u_3 \perp u_1 \\ u_3 \perp u_2 \end{cases}$

On pose $u_3 = a + bX + cX^2$ avec $(a,b,c) \in \mathbb{R}^3$.

$$\left.\begin{array}{l} \displaystyle\int_0^1 \left(a + bt + ct^2\right)\ \mathrm{d}t = 0 \\ \displaystyle\int_0^1 \left(a + bt + ct^2\right)(2t-1)\ \mathrm{d}t = 0 \end{array}\right\} \iff \begin{cases} a + \dfrac{b}{2} + \dfrac{c}{3} = 0 \\ \displaystyle\int_0^1 \left(2ct^3 + (-c+2b)t^2 + (2a-b)t - a\right)\ \mathrm{d}t = 0 \end{cases}$$
$$\iff \begin{cases} a + \dfrac{b}{2} + \dfrac{c}{3} = 0 \\ \dfrac{c}{2} + \dfrac{2b-c}{3} + \dfrac{2a-b}{2} - a = 0 \end{cases}$$
$$\iff \begin{cases} a = -\dfrac{b}{2} - \dfrac{c}{3} = \dfrac{c}{2} - \dfrac{c}{3} = \dfrac{c}{6} \\ b = -c. \end{cases}$$

On en déduit que
$$u_3 = 1 - 6X + 6X^2.$$

Corollaire (théorème de la base orthonormée incomplète) **:** Soit $(e_1, \ldots, e_k)$ une base orthonormée d'un espace euclidien. On peut trouver $e_{k+1}, \ldots, e_n$ tels que $(e_1, \ldots, e_k, e_{k+1}, \ldots, e_n)$ soit une base orthonormée de E.

Preuve :
On sait que $(e_1, \ldots, e_k)$ est libre. On complète $(e_1, \ldots, e_k)$ en une base $\mathscr{B}$ de E. On orthonormalise $\mathscr{B}$: on obtient une base orthonormée $\mathscr{C}$ de E. En

détaillant l'algorithme de Gram–Schmidt, on s'aperçoit que les k premiers vecteurs de $\mathscr{C}$ sont ceux de $\mathscr{B}$. □

Théorème : Soit E un espace euclidien et $\mathscr{B} = (e_1, \dots, e_n)$ une base orthonormée de E. Soit $(x, y) \in E^2$. On pose $(x_1, \dots, x_n) \in \mathbb{R}^n$ et $(y_1, \dots, y_n) \in \mathbb{R}^n$ tels que

$$x = \sum_{i=1}^{n} x_i e_i \qquad\qquad y = \sum_{i=1}^{n} y_i e_i.$$

Alors

$$\langle x \mid y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Alors,

$$\langle x \mid y \rangle = X^\top Y.$$

Preuve :

$$\begin{aligned}
\langle x \mid y \rangle &= \left\langle \sum_{i=1}^{n} x_i e_i \mid y \right\rangle \\
&= \sum_{i=1}^{n} x_i \langle e_i \mid y \rangle \\
&= \sum_{i=1}^{n} x_i \left\langle e_i \mid \sum_{j=1}^{n} y_j e_j \right\rangle \\
&= \sum_{i=1}^{n} x_i \sum_{j=1}^{n} y_j \underbrace{\langle e_i \mid e_j \rangle}_{\delta_i^j} \\
&= \sum_{i=1}^{n} x_i y_i.
\end{aligned}$$

□

Proposition : Soit E un espace euclidien et $\mathscr{B} = (e_1, \dots, e_n)$ une base

orthonormée de E. Alors,

$$\forall x \in E,\ x = \sum_{i=1}^{n} \langle x \mid e_i \rangle\, e_i.$$

Preuve :
Soit $x \in E$. On pose

$$x = \sum_{i=1}^{n} x_i e_i$$

avec $(x_1, \dots, x_n) \in \mathbb{R}^n$. Soit $j \in [\![1, n]\!]$. On a

$$\begin{aligned}\langle x \mid e_j \rangle &= \left\langle \sum_{i=1}^{n} x_i e_i \mid e_j \right\rangle \\ &= \sum_{i=1}^{n} x_i \langle e_i \mid e_j \rangle \\ &= x_j.\end{aligned}$$

□

4 Projection orthogonale

Dans ce paragraphe, $\big(E, \langle \cdot \mid \cdot \rangle\big)$ est un espace préhilbertien (de dimension quelconque).

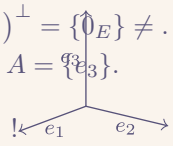
Définition : Soit $A \in \mathcal{P}(E)$. L'orthogonal de A est

$$A^{\perp} = \{u \in E \mid \forall a \in A,\ a \perp u\}.$$

Exemple : 1. $^{\perp} = E$; $\{0_E\}^{\perp} = E$; $E^{\perp} = \{0_E\}$.

Attention B , $\left(^{\perp}\right)^{\perp} = \{0_E\} \neq$.

2. Avec $E = \mathbb{R}^3$, et $A = \{e_3\}$.



et

$$A^{\perp} = \mathrm{Vect}(e_1, e_2)$$

$$A^{\perp\perp} = \mathrm{Vect}(e_1, e_2)^{\perp} = \mathrm{Vect}(e_3) \neq A.$$

Proposition :

$\forall A \in \mathscr{P}(E)$, $A^\perp$ est un sous-espace vectoriel de E.

Preuve :
Soit $A \in \mathscr{P}(E)$.

— $\forall a \in A, \langle a \mid 0_E \rangle = 0$ donc $0_E \in A^\perp$ et donc $A^\perp \neq \emptyset$.

— Soient $(u, v) \in A^\perp$, $(\alpha, \beta) \in \mathbb{R}^2$. Soit $a \in A$.

$$\begin{aligned}\langle \alpha u + \beta v \mid a \rangle &= \alpha \langle u \mid a \rangle + \beta \langle v \mid a \rangle \\ &= \alpha \times 0 + \beta \times 0 \\ &= 0.\end{aligned}$$

□

Théorème : Soit F un sous-espace vectoriel de dimension finie de E. Alors

$$F \oplus F^\perp = E.$$

Preuve :
Soit $\mathscr{B} = (e_1, \ldots, e_p)$ une base orthonormée de F.

Analyse Soit $x \in E$. On suppose $x = u + v$ avec $u \in F$ et $v \in F^\perp$. On pose $u = \sum_{i=1}^{p} u_i e_i$. De plus,

$$\forall i \in [\![1, p]\!], \langle v \mid e_i \rangle = 0.$$

Soit $i \in [\![1, p]\!]$.

$$\begin{aligned}\langle x \mid e_i \rangle &= \langle u + v \mid e_i \rangle \\ &= \langle u \mid e_i \rangle + \langle v \mid e_i \rangle \\ &= \left\langle \sum_{j=1}^{p} u_j e_j \mid e_i \right\rangle \\ &= \sum_{j=1}^{p} u_j \langle e_j \mid e_i \rangle \\ &= u_i\end{aligned}$$

D'où

$$\begin{cases} u = \displaystyle\sum_{i=1}^{p} \langle x \mid e_i \rangle e_i \\ v = x - \displaystyle\sum_{i=1}^{p} \langle x \mid e_i \rangle e_i. \end{cases}$$

Synthèse Soit $x \in E$. On pose

$$\begin{cases} u = \displaystyle\sum_{i=1}^{p} \langle x \mid e_i \rangle e_i \\ v = x - \displaystyle\sum_{i=1}^{p} \langle x \mid e_i \rangle e_i \end{cases}$$

On a clairement $u + v = x$ et $u \in F$.

Soit $a \in F$. On pose $a = \displaystyle\sum_{i=1}^{p} a_i e_i$.

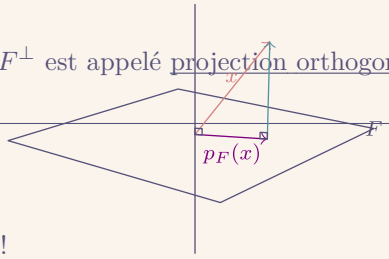
$$\begin{aligned} \langle v \mid a \rangle &= \langle x \mid a \rangle - \sum_{i=1}^{p} \langle x \mid e_i \rangle \underbrace{\langle e_i \mid a \rangle}_{=a_i} \\ &= \sum_{i=1}^{p} a_i \langle x \mid e_i \rangle - \sum_{i=1}^{p} a_i \langle x \mid e_i \rangle \\ &= 0 \end{aligned}$$

donc $v \in F^{\perp}$.

□

Définition : Dans le conditions précédentes, $F^{\perp}$ est appelé le supplémentaire orthogonal de F.

La projection sur F parallèlement à $F^{\perp}$ est appelé projection orthogonale sur F. On la note p_F.



!

Proposition (inégalité de Bessel) **:** Soit F de dimension finie. Alors,

$$\forall x \in E,\ \|p_F(x)\| \leqslant \|x\|.$$

Preuve :
Comme F est de dimension finie :

$$F \oplus F^\perp = E.$$

Soit $x \in E$. On a

$$x = p_F(x) + \big(x - p_F(x)\big)p_F(x) \in Fx - p_F(x) \in F^\perp.$$

Donc, $x - p_F(x) \perp p_F(x)$ car $p_F(x) \in F$ et $x - p_F(x) \in F^\perp$.

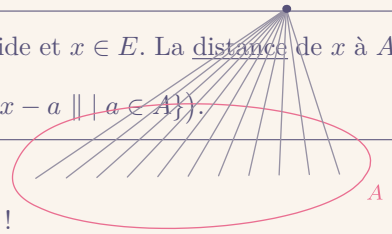
D'après le théorème de Pythagore,

$$\begin{aligned}\|x\|^2 &= \|p_F(x)\|^2 + \underbrace{\|x - p_F(x)\|^2}_{\geqslant 0} \\ &\geqslant \|p_F(x)\|^2.\end{aligned}$$

□

Définition : Soit $A \in \mathscr{P}(E)$ non vide et $x \in E$. La distance de x à A est

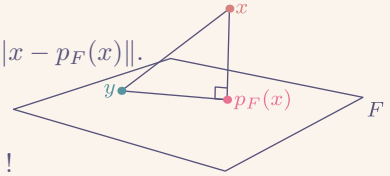
$$d(x, A) = \inf\big(\{\|x - a\| \mid a \in A\}\big).$$



!

Théorème : Soit F un sous-espace vectoriel de E de dimension finie et $x \in E$. Alors,

$$d(x, F) = \|x - p_F(x)\|.$$

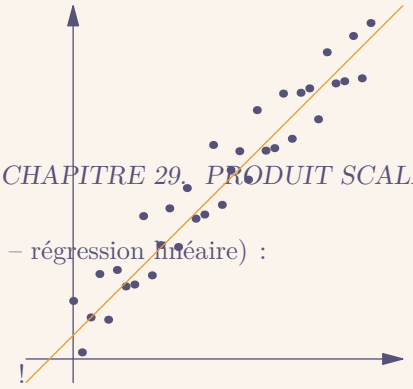


!

Preuve :
Soit $y \in F$.

$$\begin{aligned}\|x - y\|^2 &= \|\underbrace{x - p_F(x)}_{\in F^\perp} + \underbrace{p_F(x) - y}_{\in F}\|^2 \\ &= \|x - p_F(x)\|^2 + \|p_F(x) - y\|^2 \\ &\geqslant \|x - p_F(x)\|^2.\end{aligned}$$

□



Exemple (droite des moindres carrés – régression linéaire) :

On cherche $(a,b) \in \mathbb{R}^2$ qui minimise $\sum_{i=1}^{n}(y_i - (ax_i - b))^2$.

On pose $y = (y_1, \dots, y_n) \in \mathbb{R}^n$, $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ et $\mathbb{1} = (1, \dots, 1) \in \mathbb{R}^n$. On suppose que x et $\mathbb{1}$ ne sont pas colinéaires.

Soit $\langle \cdot \mid \cdot \rangle$ le produit scalaire canonique de $\mathbb{R}^n$.

$$\sum_{i=1}^{n}(y_i - (ax_i - b))^2 = \|y - \underbrace{(ax - b\mathbb{1})}_{\in \mathrm{Vect}(x,\mathbb{1}) = F}\|^2.$$

$$\min_{(a,b)\in\mathbb{R}^2} \sum_{i=1}^{n}(y_i - (ax_i + b))^2 = \|y - p_F(y)\|^2.$$

On veut les coordonnées de $p_F(y)$ dans la base $(x, \mathbb{1})$ de F.

Proposition : Soit F un sous-espace vectoriel de E de dimension finie et $\mathscr{B} = (e_1, \dots, e_p)$ une base orthonormée de F. Alors,

$$\forall x \in E,\ p_F(x) = \sum_{i=1}^{p} \langle x \mid e_i \rangle\, e_i.$$

Preuve : — $\sum_{i=1}^{p} \langle x \mid e_i \rangle\, e_i \in F$ car $e_1, \dots, e_p \in F$.

— On pose $u = x - \sum_{i=1}^{p} \langle x \mid e_i \rangle\, e_i$. Montrons que $u \in F^\perp$. Soit $a \in F$.

On peut écrire $a = \sum_{i=1}^{p} \langle a \mid e_i \rangle\, e_i$.

$$\begin{aligned}
\langle u \mid a \rangle &= \langle x \mid a \rangle - \langle p_F(x) \mid a \rangle \\
&= \sum_{i=1}^{p} \langle a \mid e_i \rangle \langle x \mid e_i \rangle - \sum_{i=1}^{p}\sum_{j=1}^{p} \langle a \mid e_i \rangle \langle x \mid e_j \rangle \langle e_i \mid e_j \rangle \\
&= \sum_{i=1}^{p} \langle a \mid e_i \rangle \langle x \mid e_i \rangle - \sum_{i=1}^{p} \langle a \mid e_i \rangle \langle x \mid e_i \rangle \\
&= 0.
\end{aligned}$$

□

Exemple (suite de l'exemple précédent – régression linéaire) :
On orthonormalise la base $(\mathbb{1}, x)$ de F.

$$\|\mathbb{1}\|^2 = \sum_{i=1}^{n} 1^2 = n.$$

On pose donc $v_1 = \dfrac{\mathbb{1}}{\|\mathbb{1}\|} = \dfrac{1}{\sqrt{n}}(1, \dots, 1)$.

Soit $u_2 = x - \langle x \mid v_1 \rangle v_1$.

$$\langle x \mid v_1 \rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} x_i = \sqrt{n}\bar{x} \text{ où } \bar{x} = \frac{1}{n} = \frac{1}{n} \sum_{i=1}^{n} x_i.$$

D'où,

$$\begin{aligned} u_2 &= (x_1, \dots, x_n) - \bar{x}(1, \dots, 1) \\ &= (x_1 - \bar{x}, \dots, x_n - \bar{x}). \end{aligned}$$

On a $\|u_2\|^2 = \sum_{i=1}^{n} (x_i - \bar{x})^2 = n\sigma_x^2$. On en déduit donc que

$$v_2 = \frac{u_2}{\|u_2\|} = \frac{1}{\sqrt{n}\sigma_x}(x_1 - \bar{x}, \dots, x_n - \bar{x}).$$

$$\begin{aligned} p_F(y) &= \langle y \mid v_1 \rangle v_1 + \langle y \mid v_2 \rangle v_2 \\ &= \frac{1}{n} \sum_{i=1}^{n} y_i (1, \dots, 1) + \frac{1}{n\sigma_x^2} \sum_{i=1}^{n} y_i (x_i - \bar{x})(x_1 - \bar{x}, \dots, x_n - \bar{x}) \\ &= (\bar{y}, \dots, \bar{y}) - \frac{1}{n\sigma_x^2} \left(\sum_{i=1}^{n} (y_i - \bar{y})(x_i - \bar{x}) + \bar{y} \sum_{i=1}^{n} (x_i - \bar{x}) \right) (x_1 - \bar{x}, \dots, x_n - \bar{x}) \\ &= (\bar{y}, \dots, \bar{y}) + \frac{1}{\sigma_x^2} \operatorname{Cov}(x, y)(x_1 - \bar{x}, \dots, x_n - \bar{x}) \\ &= \left(\bar{y} - \frac{\operatorname{Cov}(x, y)}{\sigma_x^2} \bar{x} \right) (1, \dots, 1) + \frac{\operatorname{Cov}(x, y)}{\sigma_x^2} (x_1, \dots, x_n). \end{aligned}$$

Donc,

$$\begin{cases} a = \dfrac{\operatorname{Cov}(x, y)}{\sigma_x^2}; \\ b = \bar{y} - a\bar{x}. \end{cases}$$

Proposition : Soit F un sous-espace vectoriel de E de dimension finie. Alors,

$$\left(F^\perp\right)^\perp = F.$$

Preuve :
Clairement, $F \subset \left(F^\perp\right)^\perp$.

Soit $\mathscr{B} = (e_1, \dots, e_p)$ une base orthonormée de F et $x \in \left(F^\perp\right)^\perp$.

On sait que

$$\begin{cases} x = \underbrace{p_F(x)}_{\in F} + \underbrace{x - p_F(x)}_{\in F^\perp} \\ p_F(x) = \displaystyle\sum_{i=1}^{p} \langle x \mid e_i \rangle \, e_i \end{cases}.$$

$$\begin{aligned} x - p_F(x) \in F^\perp &\text{ donc } x \perp (x - p_F(x)) \\ &\text{donc } \langle x \mid x - p_F(x) \rangle = 0 \\ &\text{donc } \|x\|^2 - \langle x \mid p_F(x) \rangle = 0 \\ &\text{donc } \|x\|^2 = \sum_{i=1}^{p} \langle x \mid e_i \rangle \langle x \mid e_i \rangle = \|p_F(x)\|^2 \end{aligned}$$

Or,

$$\begin{aligned} \|x\|^2 &= \|p_F(x)\|^2 + \|x - p_F(x)\|^2 \\ \text{donc } \|x - p_F(x)\| &= 0 \\ \text{donc } x = p_F(x) &\in F. \end{aligned}$$

□

5 Annexe

Dans ce chapitre, beaucoup des résultats ne seront pas prouvés, et sont, en grande majorité, hors-programme (pour l'année de *MP2I*).

5.1 Produit vectoriel

Théorème (Riesz) **:** Soit $(E, \langle \cdot \mid \cdot \rangle)$ un espace euclidien. L'application

$$\begin{aligned} \varphi : E &\longrightarrow E^\star \\ a &\longmapsto \langle a \mid \cdot \rangle \end{aligned}$$

est un isomorphisme.

Preuve :
Soient $(a,b) \in E^2$ et $(\alpha,\beta) \in \mathbb{R}^2$.

$$\begin{aligned}\forall x \in E,\ \varphi(\alpha a+\beta b)(x) &= \langle \alpha a+\beta b \mid x\rangle \\ &= \alpha\langle a \mid x\rangle + \beta\langle b \mid x\rangle \\ &= \alpha\varphi(a)(x)+\beta\varphi(b)(x) \\ &= \big(\alpha\varphi(a)+\beta\varphi(b)\big)(x)\end{aligned}$$

Donc $\varphi \in \mathscr{L}(E,E^\star)$.

Soit $a \in \mathrm{Ker}(\varphi)$, alors $\varphi(a) = 0_{E^\star}$ et donc,

$$\forall x \in E,\ \varphi(a)(x) = 0$$

donc

$$\forall x \in E,\ \langle a \mid x\rangle = 0.$$

On a donc $\langle a \mid a\rangle = 0$ et donc $a = 0_E$.

On en déduit que φ est injective.

Comme $\dim(E) = \dim(E^\star) < +\infty$ et donc $\varphi \in \mathrm{GL}(E,E^\star)$. □

Exemple :
Soit P un plan de $\mathbb{R}^3$ et $n \in P^\perp$.

$$\begin{aligned}u \in P &\iff u \perp n \\ &\iff \langle u \mid n\rangle = 0.\end{aligned}$$

Ici, $E = \mathbb{R}^3$ muni de son produit scalaire canonique.

Définition : Soient u et v linéairement indépendants dans E. Soit $\mathscr{B} = (e_1,e_2,e_3)$ la base canonique de E.

L'application

$$\begin{aligned}f : E &\longrightarrow \mathbb{R} \\ w &\longmapsto \det_{\mathscr{B}}(u,v,w)\end{aligned}$$

est linéaire. D'après le théorème de Riesz,

$$\exists!\, a \in E,\ f = \langle a \mid \cdot\rangle .$$

On considère un tel vecteur $a \in E$. Donc,

$$\forall w \in E,\ \det_{\mathscr{B}}(u,v,w) = \langle a \mid w\rangle .$$

On en déduit que

$$\begin{aligned}(u,v,w) \text{ base de } E &\iff \langle a \mid w\rangle \neq 0\\ &\iff w \not\perp a.\end{aligned}$$

Comme $a \not\perp a$, (u,v,a) est une base de E. a est le produit vectoriel de u et v et est noté $u \wedge v$.

$$\forall w \in E,\ \det_{\mathcal{B}}(u,v,w) = \underbrace{\langle u \wedge v \mid w\rangle}_{\substack{\text{produit mixte}\\ \text{noté } [u,v,w]}}.$$

Proposition : Soit $(u,v) \in E^2$ avec u et v linéairement indépendants.

1. $(u \wedge v) \perp u$;
2. $(u \wedge v) \perp v$;
3. $(u, v, u \wedge v)$ est une base directe (i.e. $\det(u, v, u \wedge v) > 0$) ;
4. $\|u \wedge v\| = \|u\|\,\|v\|\,\sin(\widehat{u,v})$.

Preuve : 1. $\langle u \wedge v \mid u\rangle = \det_{\mathcal{B}}(u,v,u) = 0$.
2. $\langle u \wedge v \mid v\rangle = \det_{\mathcal{B}}(u,v,v) = 0$.
3. $\det_{\mathcal{B}}(u,v,u \wedge v) = \langle u \wedge v \mid u \wedge v\rangle = \|u \wedge v\|^2 > 0$.
4. $\|u \wedge v\|^2 = \det_{\mathcal{B}}(u,v,u \wedge v) = \|u \wedge v\|\,\|u\|\,\|v\|\,\sin(\widehat{u,v})$.

□

Proposition : Soient $u = (a,b,c)$ et $v = (\alpha,\beta,\gamma)$. Alors,

$$u \wedge v = (b\gamma - c\beta, \alpha c - \gamma a, a\beta - b\alpha).$$

Preuve :

On pose $u \wedge v = (x, y, z)$. Comme (e_1, e_2, e_3) est orthonormée, on a

$$x = \langle u \wedge v \mid e_1 \rangle = \det_{\mathscr{B}}(u, v, e_1) = \begin{vmatrix} a & \alpha & 1 \\ b & \beta & 0 \\ c & \gamma & 0 \end{vmatrix} = \begin{vmatrix} b & \beta \\ c & \gamma \end{vmatrix};$$

$$y = \langle u \wedge v \mid e_2 \rangle = \begin{vmatrix} a & \alpha & 0 \\ b & \beta & 1 \\ c & \gamma & 0 \end{vmatrix} = -\begin{vmatrix} a & \alpha \\ c & \gamma \end{vmatrix};$$

$$z = \langle u \wedge v \mid e_3 \rangle = \begin{vmatrix} a & \alpha & 0 \\ b & \beta & 0 \\ c & \gamma & 1 \end{vmatrix} = a\beta - b\alpha.$$

□

5.2 Calcul différentiel

Définition : Soit $f : D \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ où D est un ouvert. Soit $a \in D$. S'il existe $\ell_a \in \mathscr{L}(\mathbb{R}^n, \mathbb{R})$ telle que

$$\forall h \in \mathbb{R}^n \text{ avec } \|h\| \text{ assez petite, } f(a+h) = f(a) + \ell_a(h) + \wr\left(\|h\|\right)$$

alors on dit que f est <u>différentiable</u> en a et ℓ_a est la <u>différentielle</u> de f en a. Si c'est le cas, alors

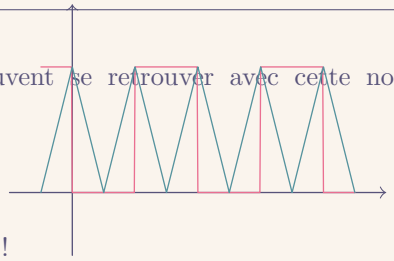
$$\exists!\, g_a \in \mathbb{R}^n,\ \forall h,\ \ell_a(h) = \langle g_a \mid h \rangle .$$

On dit que g_a est le <u>gradient</u> de f au point a.

Donc,

$$f(a+h) - f(a) \simeq \langle g_a \mid h \rangle .$$

Les résultats vus au chapitre 22 peuvent se retrouver avec cette nouvelle définition du gradient.



5.3 Séries de Fourier

Soit E un $\mathbb{C}$-espace vectoriel de dimension infinie et $\langle \cdot \mid \cdot \rangle$ une application de E^2 dans $\mathbb{C}$ vérifiant

1. linéarité à gauche ;
2. $\forall (u, v) \in E^2,\ \langle v \mid u \rangle = \overline{\langle u \mid v \rangle}$; (symétrie hermitienne)
3. $\forall u \in E,\ \langle u \mid u \rangle \geqslant 0$;
4. $\forall u \in E,\ \langle u \mid u \rangle = 0 \iff u = 0_E$.

Proposition : $\langle \cdot \mid \cdot \rangle$ est semi-linéaire à droite :

$$\langle u \mid \alpha v + \beta w \rangle = \bar{\alpha} \langle u \mid v \rangle + \bar{\beta} \langle u \mid w \rangle .$$

$\langle \cdot \mid \cdot \rangle$ est donc sesquilinéaire.

$\langle \cdot \mid \cdot \rangle$ est dit produit héermitien.

Exemple :
Avec $E = \mathscr{C}^0\big([a,b], \mathbb{C}\big)$, on a $\langle f \mid g \rangle = \dfrac{1}{b-a} \displaystyle\int_a^b f(t)\,\overline{g(t)}\,\mathrm{d}t$.

Définition : Soit $\mathscr{B} = (e_n)_{n\in\mathbb{Z}}$ une famille de E. On dit que $\mathscr{B}$ est une base hilbertienne si

$$\begin{cases} \forall x \in E,\ \exists!\,(c_n)_{n\in\mathbb{Z}},\ x = \displaystyle\sum_{n=-\infty}^{+\infty} c_n e_n; \\ \forall n \in \mathbb{Z},\ \|e_n\| = 1; \\ \forall p \neq q,\ \langle e_p \mid e_q \rangle = 0. \end{cases} .$$

Dans ce cas, $c_n = \langle x \mid e_n \rangle$.

Exemple :
On pose

$$\begin{aligned} \forall n \in \mathbb{Z}, \qquad e_n : [0, 2\pi] &\longrightarrow \mathbb{C} \\ t &\longmapsto e^{int} \end{aligned}$$

$$\begin{aligned} \langle e_p \mid e_q \rangle &= \frac{1}{2\pi} \int_0^{2\pi} e^{ipt}\, e^{-iqt}\, \mathrm{d}t \\ &= \frac{1}{2\pi} \int_0^{2\pi} e^{i(p-q)t}\, \mathrm{d}t \\ &= \begin{cases} 1 & \text{si } p = q \\ \dfrac{1}{2\pi} \left[\dfrac{e^{i(p-q)t}}{i(p-q)} \right]_0^{2\pi} = 0 \text{ si } p \neq q \end{cases} \end{aligned}$$

Soit

$$F = \left\{ \sum_{n\in\mathbb{Z}} c_n e_n \mid (c_n) \in \mathbb{C}^{\mathbb{Z}} \text{ tel que } \forall t,\ \sum c_n e_n(t) \text{ converge} \right\}.$$

Soit f 2π-périodique. On a

$$p_F(f) = \sum_{n=-\infty}^{+\infty} c_n e_n$$

où $c_n = \langle f \mid e_n \rangle = \dfrac{1}{2\pi} \displaystyle\int_0^{2\pi} f(t)\, e^{-int}\, \mathrm{d}t$.

On en déduit que

$$\mathfrak{Re}(c_n) = \frac{1}{2\pi} \int_0^{2\pi} f(t)\, \cos(nt)\, \mathrm{d}t$$

5.4 Espace-temps de Minkowsky

On modélise l'espace-temps par $E = \mathbb{R}^4$; c'est un espace affine et on y crée un "produit scalaire" (en utilisant une "norme") :

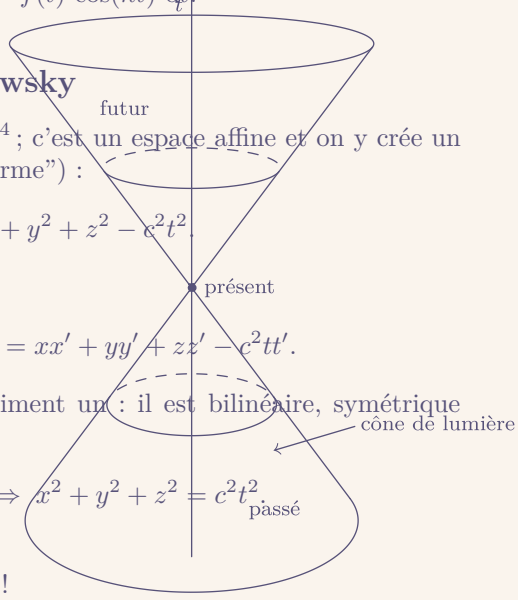
$$q(x, y, z, t) = x^2 + y^2 + z^2 - c^2 t^2.$$

On en déduit que

$$\langle (x, y, z, t) \mid (x', y', z', t') \rangle = xx' + yy' + zz' - c^2 tt'.$$

Ce "produit scalaire" n'en est pas vraiment un : il est bilinéaire, symétrique MAIS pas positif.

$$(x, y, z, t) \text{ isotrope} \iff x^2 + y^2 + z^2 = c^2 t^2$$



!

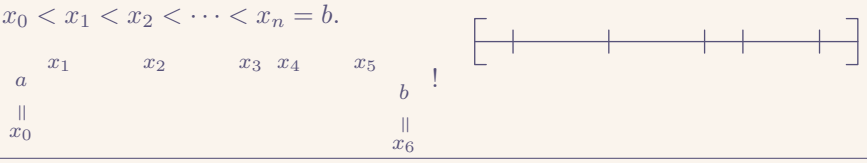
Toute information contenue dans le cône passé nous est accessible ; s'il est sur sa surface, il faut que l'information y voyage à la vitesse de la lumière. Par contre, comme le temps n'est pas symétrique, on ne peut pas voir l'information future.

Chapitre 30

Intégrale de Riemann

1 Intégrale d'une fonction en escaliers

Définition : Une subdivision du segment $[a,b]$ est une suite finie $a = x_0 < x_1 < x_2 < \cdots < x_n = b$.



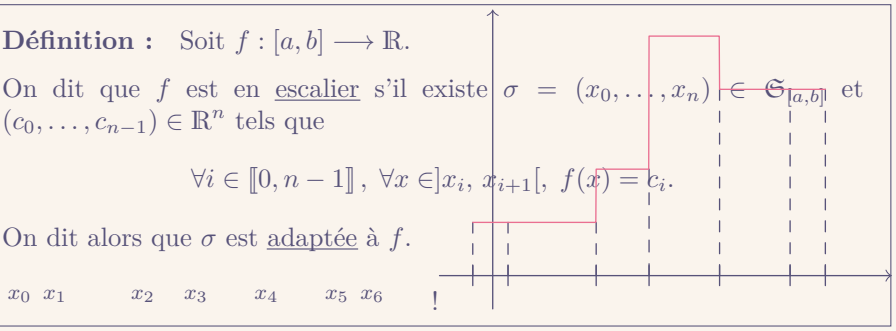
Remarque (Notation) :
Dans ce chapitre, l'ensemble des subdivisions de $[a,b]$ est noté $\mathfrak{S}_{[a,b]}$.

Définition : Soit $f : [a,b] \longrightarrow \mathbb{R}$.

On dit que f est en escalier s'il existe $\sigma = (x_0, \ldots, x_n) \in \mathfrak{S}_{[a,b]}$ et $(c_0, \ldots, c_{n-1}) \in \mathbb{R}^n$ tels que

$$\forall i \in [\![0, n-1]\!],\ \forall x \in]x_i, x_{i+1}[,\ f(x) = c_i.$$

On dit alors que σ est adaptée à f.



Définition : Soient $\sigma = (x_0, x_1, \ldots, x_n) \in \mathfrak{S}_{[a,b]}$ et $\sigma' = (x'_0, x'_1, \ldots, x'_p) \in \mathfrak{S}_{[a,b]}$. On dit alors que σ' est plus fine que σ si $\{x_0, x_1, \ldots, x_n\} \subset \{x'_0, x'_1, \ldots, x'_n\}$. On note alors $\sigma' \prec \sigma$.

Proposition : Soient σ_1, σ_2 deux subdivisions de $[a,b]$. Alors il existe une subdivision σ_3 plus fine que σ_1 et σ_2.

Preuve :
Soit $\sigma_1 = (x_0, x_1, \dots, x_n) \in \mathfrak{S}_{[a,b]}$ et $\sigma_2 = (x'_0, x'_1, \dots, x'_p) \in \mathfrak{S}_{[a,b]}$.

On pose $A = \{x_0, \dots, x_n\} \cup \{x'_0, \dots, x'_p\}$. On ordonne dans l'ordre croissant les éléments de A :

$$A = \{x''_0, x''_1, \dots, x''_q\}$$

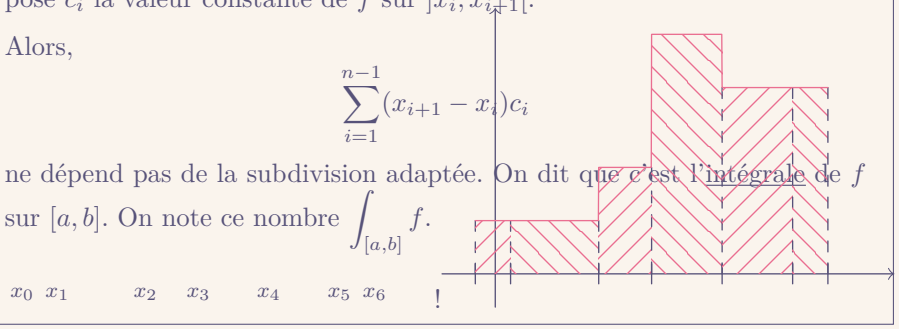
avec $a = x''_0 < x''_1 < \cdots < x''_q = b$. On pose $\sigma_3 = (x''_0, x''_1, \dots, x''_q) \in \mathfrak{S}_{[a,b]}$. On a bien $\sigma_3 \prec \sigma_2$ et $\sigma_3 \prec \sigma_1$. □

Proposition–Définition : Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction en escaliers. Soit $\sigma = (x_0, \dots, x_n)$ une subdivision adaptée à f. Pour $i \in [\![0, n-1]\!]$, on pose c_i la valeur constante de f sur $]x_i, x_{i+1}[$.

Alors,

$$\sum_{i=1}^{n-1} (x_{i+1} - x_i) c_i$$

ne dépend pas de la subdivision adaptée. On dit que c'est l'intégrale de f sur $[a,b]$. On note ce nombre $\displaystyle\int_{[a,b]} f$.



Preuve :
Soit $\sigma' = (x'_0, \dots, x'_p)$ une subdivision adaptée à f. On considère σ'' une subdivision de $[a,b]$ plus fine que σ et σ'. On pose

$$\sigma'' = (a, x_{1,1}, x_{1,2}, \dots, \underset{\|}{x_{1,i_1}}, x_{2,1}, \dots, \underset{\|}{x_{2,i_2}}, \dots, b)$$
$$\begin{matrix} x_{2,0} & & x_{3,0} \\ \| & & \| \\ x_1 & & x_2 \end{matrix}$$

On a

$$\forall k \in [\![0, n-1]\!], \forall j \in [\![0, u_k - 1]\!], \forall x \in]x_{k,j}, x_{k,j+1}[, \ f(x) = c_k.$$

$$\sum_{k=0}^{n-1}\sum_{j=0}^{i_k-1}(x_{k,j+1}-x_{k,j})c_k = \sum_{k=0}^{n-1} c_k \sum_{j=0}^{i_k-1}(x_{k,j+1}-x_{k,j})$$
$$= \sum_{k=0}^{n-1}(x_{k,i_k}-x_{k,0})$$
$$= \sum_{k=0}^{n-1} c_k(x_{k+1}-x_k)$$

De même, comme $\sigma \prec \sigma'$, on a aussi l'égalité avec $\sum_{k=0}^{p-1} c'_k(x'_{k+1}-x'_k)$ où c'_k est la valeur de f sur $]x'_k, x'_{k+1}[$. □

Pour définir l'intégrale d'une fonction continue, on peut utiliser deux méthodes :

1. L'intégrale d'une fonction continue est la limite d'une suite de fonctions en escaliers. Ces résultats seront vus l'année prochaine en *MPI*.
2. Les sommes de Darboux ; c'est la définition que l'on va utiliser.

2 Sommes de Darboux

Définition : Soit $f : [a,b] \longrightarrow \mathbb{R}$. Soit $\sigma = (x_0, x_1, \dots, x_n) \in \mathfrak{S}_{[a,b]}$. La somme de Darboux supérieur de f associé à σ est

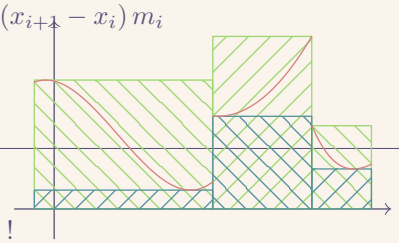
$$S^+_\sigma(f) = \sum_{i=1}^{n-1}(x_{i+1}-x_i)\,M_i$$

où $\forall i \in [\![0, n-1]\!]$, $M_i = \sup_{]x_i,x_{i+1}[} f$.

La somme de Darboux inférieure de f associé à σ est

$$S^-_\sigma(f) = \sum_{i=0}^{n-1}(x_{i+1}-x_i)\,m_i$$

où $m_i = \inf_{]x_i,x_{i+1}[} f$.



Proposition : Soit $f : [a,b] \longrightarrow \mathbb{R}$ bornée, σ et σ' deux subdivisions de

$[a,b]$ avec $\sigma' \prec \sigma$. Alors

$$\begin{cases} S^+_{\sigma'}(f) \leqslant S^+_\sigma(f); \\ S^-_{\sigma'}(f) \geqslant S^-_\sigma(f). \end{cases}$$

Preuve :
On pose $\sigma = (x_0, \dots, x_n)$.

$$\forall i \in [\![0, n-1]\!]\,,\ ]x_i, x_{i+1}[= \bigcup_{k=0}^{\ell-1}]y_k, y_{k+1}[$$

avec $y_k \in \sigma'$ pour tout k.

$$\forall x \in]y_k, y_{k+1}[,\ f(x) \leqslant M_i.$$

donc M_i majore $f\big(]y_k, y_{k+1}[\big)$ et donc $\sup\limits_{]y_k, y_{k+1}[} f \leqslant M_i$. Donc,

$$\sum_{k=0}^{\ell-1}(y_{k+1}-y_k) \sup_{]y_k,y_{k+1}[} \leqslant M_i \sum_{k=0}^{\ell-1}(y_{k+1}-y_k) = M_i(x_{i+1}-x_i).$$

Ainsi,

$$S^+_{\sigma'}(f) \leqslant \sum_{i=0}^{n-1} M_i(x_{i+1}-x_i) = S^+_\sigma(f).$$

De même pour la somme de Darboux inférieure. □

Définition : Soit $f : [a,b] \longrightarrow \mathbb{R}$ bornée.

L'intégrale supérieure de f est

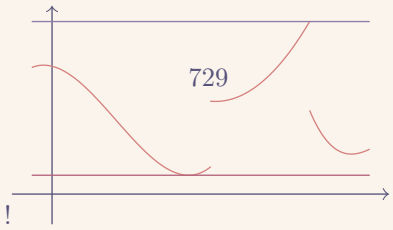
$$I^+_{[a,b]}(f) = \inf_{\sigma \in \mathfrak{S}_{[a,b]}} \big(S^+_\sigma(f)\big).$$

L'intégrale inférieure de f est

$$I^-_{[a,b]}(f) = \sup_{\sigma \in \mathfrak{S}_{[a,b]}} \big(S^-_\sigma(f)\big).$$

Remarque (justification de l'existence des bornes inférieures et supérieures) :
Soit $m = \inf\limits_{[a,b]} f$. $\forall i \in [\![0, n-1]\!]\,,\ M_i \geqslant m$ et donc

$$\begin{aligned} S^+_\sigma(f) &= \sum_{i=0}^{n-1}(x_{i+1}-x_i)M_i \\ &\geqslant \sum_{i=0}^{n-1}(x_{i+1}-x_i)m \\ &\geqslant m(b-a). \end{aligned}$$



De même, avec $M = \sup_{[a,b]} f$, $\forall \sigma \in \mathfrak{S}_{[a,b]}$, $S^-_\sigma(f) \leqslant M(b-a)$.

EXEMPLE : 1. Soit $f : [a,b] \longrightarrow \mathbb{R}$ en escaliers.

$$I^+_{[a,b]}(f) = \int_{[a,b]} f = I^-_{[a,b]}(f).$$

2. On pose

$$f : [0,1] \longrightarrow \mathbb{R}$$
$$x \longmapsto \begin{cases} 0 & \text{si } x \notin \mathbb{Q} \\ 1 & \text{si } x \in \mathbb{Q}. \end{cases}$$

Rappel : on a $f = \mathbb{1}_{\mathbb{Q}}$.

On a $I^+_{[0,1]}(f) = 1$ et $I^-_{[0,1]}(f) = 0$.

3. On pose

$$f : [0,1] \longrightarrow \mathbb{R}$$
$$x \longmapsto x$$

Soit $\sigma_n = \left(0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1\right)$.

$$S^+_{\sigma_n}(f) = \sum_{i=0}^{n} \frac{1+1}{n} \times \frac{i}{n} = \frac{1}{n^2} \times \frac{n(n+1)}{2} = \frac{n-1}{2n}.$$

On a, pour tout n non nul, $I^+_{[0,1]} f \leqslant \frac{n+1}{n}$ donc $I^+_{[a,b]} \leqslant \frac{1}{2}$.

De même,

$$S^-_{\sigma_n}(f) = \sum_{i=0}^{n-1} \frac{1}{n} \times \frac{i}{n} = \frac{n(n-1)}{2} = \frac{n-1}{2n}.$$

D'où, pour tout n non nul, $I^-_{[0,1]}(f) \geqslant \frac{n-1}{2n}$ et docn $I^-_{[0,1]}(f) \geqslant \frac{1}{2}$.

Or, $\frac{1}{2} \leqslant I^-_{[0,1]}(f) \leqslant I^+_{[0,1]}(f) \leqslant \frac{1}{2}$ (voir ci-après). Et donc,

$$I^-_{[0,1]}(f) = I^+_{[0,1]}(f) = \frac{1}{2}.$$

Proposition : Soit $f : [a,b] \to \mathbb{R}$ bornée. Alors

$$I^-_{[a,b]}(f) \leqslant I^+_{[a,b]}(f).$$

[]

Preuve :
Soit $\sigma \in \mathfrak{S}_{[a,b]}$. Soit $\sigma' \in \mathfrak{S}_{[a,b]}$. On considère $\sigma'' \in \mathfrak{S}_{[a,b]}$ telle que $\sigma'' \prec \sigma$ et $\sigma'' \prec \sigma'$. On a donc

$$S^-_{\sigma'}(f) \leqslant S^-_{\sigma''}(f) \leqslant S^+_{\sigma''}(f) \leqslant S^+_{\sigma}(f).$$

On fixe $\sigma \in \mathfrak{S}_{[a,b]}$.

$$\forall \sigma' \in \mathfrak{S}_{[a,b]},\ S^-_{\sigma'}(f) \leqslant S^+_{\sigma}(f)$$

donc $S^+_\sigma(f)$ majore toutes les sommes de Darboux inférieures de f donc

$$I^-_{[a,b]}(f) \leqslant S_\sigma(f)$$

donc $I^-_{[a,b]}(f)$ minore toutes les sommes de Darboux supérieures de f. On a donc

$$I^+_{[a,b]}(f) \geqslant I^-_{[a,b]}(f).$$

□

Définition : Soit $f : [a,b] \to \mathbb{R}$ bornée. On dit que f est Riemann-intégrable si $I^-_{[a,b]}(f) = I^+_{[a,b]}(f)$. Dans ce cas, ce nombre est noté $\displaystyle\int_{[a,b]} f$.

3 Propriétés de l'intégrale

Proposition : Soient f et g deux fonctions définies de $[a,b]$ à valeurs dans $\mathbb{R}$. Si $f \leqslant g$, alors

$$I^-_{[a,b]}(f) \leqslant I^-_{[a,b]}(g).$$

Preuve :
On suppose $f \leqslant g$.

$$\begin{aligned} I^-(f) \leqslant I^-(g) &\iff \sup_{\sigma\in\mathfrak{S}} S^-_\sigma(f) \leqslant \sup_{\sigma\in\mathfrak{S}} S^-_\sigma(g) \\ &\iff \forall \sigma \in \mathfrak{S},\ S^-_\sigma(f) \leqslant \sup_{\sigma'\in\mathcal{S}} I^-_{\sigma'}(g) \end{aligned}$$

Soit $\sigma \in \mathfrak{S}$. On pose $\sigma = (x_0, x_1, \ldots, x_n)$ et, pour tout $i \in [\![0, n-1]\!]$,

$m_i = \inf_{]x_i,x_{i+1}[} f$). Alors,

$$S_\sigma^-(f) = \sum_{i=1}^{n-1}(x_{i+1} - x_i)m_i.$$

On pose aussi, pour tout $i \in [\![0, n-1]\!]$, $m_i' = \inf_{]x_i,x_{i+1}[}(g)$.

Soit $i \in [\![0, n-1]\!]$.

$$\begin{aligned} m_i \leqslant m_i' &\iff \inf_{]x_i,x_{i+1}[}(f) \leqslant \inf_{]x_i,x_{i+1}[}(g) \\ &\iff \forall x \in]x_i, x_{i+1}[, \inf_{]x_i,x_{i+1}[}(f) \leqslant g(x) \end{aligned}$$

Soit $x \in]x_i, x_{i+1}[$. On sait que

$$\inf_{]x_i,x_{i+1}[}(f) \leqslant f(g) \leqslant g(x).$$

On en déduit que

$$S_\sigma^-(f) \leqslant \sum_{i=0}^{n-1}(x_i - x_{i+1})m_i' = S_\sigma^-(g) \leqslant \sup_{\sigma' \in \mathfrak{S}} S_{\sigma'}^-(g).$$

□

Exercice :
Démontrer le même résultat avec les sommes de Darboux supérieures :

$$I_{[a,b]}^+(f) \leqslant I_{[a,b]}^+(g).$$

Corollaire : Soient f et g deux fonctions intégrables définies sur $[a, b]$ à valeurs dans $\mathbb{R}$. Si $f \leqslant g$, alors

$$\int_{[a,b]} f \leqslant \int_{[a,b]} g.$$

□

Proposition (Chasles) **:** Soit f une fonction définie sur $[a, b]$ à valeurs dans $\mathbb{R}$. Soit $c \in]a, b[$. Alors,

$$\begin{cases} I_{[a,b]}^-(f) = I_{[a,c]}^-(f) + I_{[c,b]}^-(f) \\ I_{[a,b]}^+(f) = I_{[a,c]}^+(f) + I_{[c,b]}^+(f). \end{cases}$$

Preuve :

— $I^-_{[a,b]}(f) \leqslant I^-_{[a,c]}(f) + I^-_{[c,b]}(f) \iff \forall \sigma \in \mathfrak{S}_{[a,b]},\ S^-_\sigma(f) \leqslant I^-_{[a,c]}(f) + I^-_{[c,b]}(f)$.

Soit $\sigma \in \mathfrak{S}_{[a,b]}$. On pose $\sigma = (x_0, x_1, \dots, x_n)$. On note $k \in [\![0, n-1]\!]$ tel que $x_k \leqslant c \leqslant x_{k+1}$.

On pose aussi $\sigma_1 = (x_0, x_1, \dots, x_k, c) \in \mathfrak{S}_{[a,c]}$ et $\sigma_2 = (c, x_{k+1}, \dots, x_n) \in \mathfrak{S}_{[c,b]}$.

$\sigma_1 \cup \sigma_2$ est une subdivision plus fine que σ. On en déduit que

$$S^-_\sigma(f) \leqslant S^-_{\sigma_1 \cup \sigma_2}(f) = \underbrace{S^-_{\sigma_1}(f)}_{\geqslant I^-_{[a,c]}(f)} + \underbrace{S^-_{\sigma_2}(f)}_{\geqslant I^-_{[c,b]}(f)}.$$

—

$$\begin{aligned} I^-_{[a,b]}(f) \geqslant I^-_{[a,c]}(f) + I^-_{[c,b]}(f) &\iff I^-_{[a,c]}(f) \geqslant I^-_{[a,b]}(f) - I^-_{[c,b]}(f) \\ &\iff \forall \sigma_1 \in \mathfrak{S}_{[a,c]},\ S^-_{\sigma_1} \leqslant I^-_{[a,b]}(f) - I^-_{[c,b]}(f) \\ &\iff \forall \sigma_1 \in \mathfrak{S}_{[a,c]},\ I^-_{[c,b]}(f) \leqslant I^-_{[a,b]}(f) - S^-_{\sigma_1}(f) \\ &\iff \forall \sigma_1 \in \mathfrak{S}_{[a,c]},\ \forall \sigma_2 \in \mathfrak{S}_{[c,b]},\ S^-_{\sigma_2}(f) \leqslant I^-_{[a,b]}(f) - S^-_{\sigma_1}(f). \end{aligned}$$

Soient $\sigma \in \mathcal{S}_{[a,c]}$ et $\sigma_2 \in \mathfrak{S}_{[c,b]}$.

$$S^-_{\sigma_1}(f) + S^-_{\sigma_2}(f) = S^-_{\sigma_1 \cup \sigma_2}(f) \leqslant I^-_{[a,b]}(f).$$

□

Corollaire : Soit f une fonction définie sur $[a, b]$ à valeurs dans $\mathbb{R}$. Soit $c \in]a, b[$. Alors,

$$\int_{[a,b]} f = \int_{[a,c]} f + \int_{[c,b]} f.$$

□

Proposition : Soient f et g deux fonctions intégrables définies sur $[a, b]$ à valeurs dans $\mathbb{R}$. Alors,

$$\begin{cases} I^-_{[a,b]}(f+g) \geqslant I^-_{[a,b]}(f) + I^-_{[a,b]}(f) \\ I^+_{[a,b]}(f+g) \leqslant I^+_{[a,b]}(f) + I^+_{[a,b]}(f) \end{cases}$$

Preuve :

$$\begin{aligned}
I^-(f+g) \geqslant I^-(f) + I^-(g) &\iff I^-(f) \leqslant I^-(f+g) - I^-(g)\\
&\iff \forall \sigma \in \mathfrak{S}_{[a,b]}, S^-_\sigma(f) \leqslant I^-(f+g) - I^-(g)\\
&\iff \forall \sigma \in \mathfrak{S},\ I^-(g) \leqslant I^-(f+g) - S^-_\sigma(f)\\
&\iff \forall \sigma \in \mathfrak{S}, \forall \sigma' \in \mathfrak{S},\ S^-_{\sigma'}(g) \leqslant I^-(f+g) - I^-_\sigma(f)\\
&\iff \forall \sigma \in \mathfrak{S}, \forall \sigma' \in \mathfrak{S}, S^-_\sigma(f) + S^-_{\sigma'}(g) \leqslant I^-(f+g)
\end{aligned}$$

Soit $\sigma, \sigma' \in \mathfrak{S}$. On considère $\sigma'' \in \mathfrak{S}$ telle que $\sigma'' \prec \sigma'$ et $\sigma'' \prec \sigma$. On a

$$\begin{cases} S^-_\sigma(f) \geqslant S^-_{\sigma''}(f) \\ S^-_{\sigma'}(g) \leqslant S^-_{\sigma''}(g) \end{cases}$$

donc

$$S^-_\sigma(f) + S^-_{\sigma'}(g) \leqslant S^-_{\sigma''}(f) + S^-_{\sigma''}(g).$$

On pose $\sigma'' = (x_0, \dots, x_n)$ et, pour $i \in [\![0, n-1]\!]$,

$$\begin{cases} m_i(f) = \inf\limits_{]x_i, x_{i+1}[}(f) \\ m_i(g) = \inf\limits_{]x_i, x_{i+1}[}(g) \\ m_i(f+g) = \inf\limits_{]x_i, x_{i+1}[}(f+g). \end{cases}$$

Alors,

$$\begin{aligned}
S^-_{\sigma''}(f) + S^-_{\sigma''}(g) &= \sum_{i=0}^{n-1}(x_{i+1} - x_i)m_i(f) + \sum_{i=0}^{n-1}(x_{i+1} - x_i)m_i(g)\\
&= \sum_{i=0}^{n-1}(x_{i+1} - x_i)\big(m_i(f) + m_i(g)\big).
\end{aligned}$$

Soit $i \in [\![0, n-1]\!]$.

$$\begin{aligned}
m_i(f) + m_i(g) \leqslant m_i(f+g) &\iff \inf_{]x_i, x_{i+1}[}(f) + \inf_{]x_i, x_{i+1}[}(g) \leqslant \inf_{]x_i, x_{i+1}[}(f+g)\\
&\iff \forall x \in]x_i, x_{i+1}[, \inf_{]x_i, x_{i+1}[}(f) + \inf_{]x_i, x_{i+1}[}(g) \leqslant (f+g)(x)
\end{aligned}$$

Soit $x \in]x_i, x_{i+1}[$.

$$\begin{aligned}
(f+g)(x) &= f(x) + g(x)\\
&\geqslant \inf_{]x_i, x_{i+1}[}(f) + \inf_{]x_i, x_{i+1}[}(g).
\end{aligned}$$

D'où

$$\begin{aligned} S^-_{\sigma''}(f)+S^-_{\sigma''}(g) &\leqslant \sum_{i=0}^{n-1}(x_{i+1}-x_i)m_i(f+g)\\ &\leqslant S^-_{\sigma''}(f+g)\leqslant I^-(f+g). \end{aligned}$$

□

Proposition : Soit $\lambda\in\mathbb{R}$. On a

$$I^-_{[a,b]}(\lambda f)=\begin{cases}\lambda I^-_{[a,b]}(f) & \text{si } \lambda\geqslant 0\\ \lambda I^+_{[a,b]}(f) & \text{si } \lambda\leqslant 0\end{cases}$$

et

$$I^+_{[a,b]}(\lambda f)=\begin{cases}\lambda I^+_{[a,b]}(f) & \text{si } \lambda\geqslant 0\\ \lambda I^-_{[a,b]}(f) & \text{si } \lambda\leqslant 0\end{cases}.$$

Preuve : — On suppose $\lambda>0$.

$$I^-(\lambda f)\leqslant\lambda I^-(f)\iff\forall\sigma\in\mathfrak{S},\ S^-_\sigma(\lambda f)\leqslant\lambda I^-(f).$$

Soit $\sigma=(x_0,\dots,x_n)\in\mathfrak{S}$. On pose, pour $i\in[\![0,n-1]\!]$, $m_i(f)=\inf_{]x_i,x_{i+1}[}(f)$ et $m_i(\lambda f)=\inf_{]x_i,x_{i+1}[}(\lambda f)$.

Soit $i\in[\![0,n-1]\!]$.

$$\begin{aligned} m_i(\lambda f)\leqslant\lambda m_i(f) &\iff m_i(f)\geqslant m_i(f)\geqslant\frac{1}{\lambda}m_i(\lambda f)\\ &\iff\forall x\in\,]x_i,x_{i+1}[,\ \frac{1}{\lambda}m_i(\lambda f)\leqslant f(x)\end{aligned}$$

Soit $x\in\,]x_i,x_{i+1}[$. On a

$$f(x)=\frac{1}{\lambda}\big(\lambda f(x)\big)\geqslant\frac{1}{\lambda}m_i(\lambda f).$$

Donc,

$$\begin{aligned} S^-_\sigma(\lambda f)&=\sum_{i=0}^{n-1}(x_{i+1}-x_i)m_i(\lambda f)\\ &\leqslant\sum_{i=0}^{n-1}\lambda(x_{i+1}-x_i)m_i(f)\\ &\leqslant\lambda S^-_\sigma(f)\\ &\leqslant\lambda I^-(f).\end{aligned}$$

En outre,

$$\begin{aligned} I^-(f) &= I^-\left(\frac{1}{\lambda}\lambda f\right) \\ &\leqslant \frac{1}{\lambda} I^-(\lambda f) \end{aligned}$$

donc

$$\lambda I^-(f) \leqslant I^-(\lambda f).$$

— On suppose $\lambda < 0$.

$$I^-(\lambda f) \leqslant \lambda I^-(f) \iff \forall \sigma \in \mathfrak{S},\ S_\sigma^-(\lambda f) \leqslant \lambda I^+(f).$$

Soit $\sigma \in \mathfrak{S}$. On pose $\sigma = (x_0, \dots, x_n)$. Alors,

$$S_\sigma^-(\lambda f) = \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i(\lambda f).$$

Soit $i \in [\![0, n-1]\!]$. Soit $x \in]x_i, x_{i+1}[$.

$$f(x) = \frac{1}{\lambda}\Big(\underbrace{\lambda f(x)}_{\geqslant \inf(\lambda f)} \Big) \leqslant \frac{1}{\lambda} m_i(\lambda f)$$

$$\text{donc } \frac{1}{\lambda} m_i(\lambda f) \text{ majore } f \text{ sur }]x_i, x_{i+1}[$$

$$\text{donc } \frac{1}{\lambda} m_i(\lambda f) \geqslant \sup_{]x_i, x_{i+1}[} (f) = M_i(f)$$

$$\text{et donc } m_i(\lambda f) \leqslant \lambda M_i(f).$$

D'où

$$\begin{aligned} S_\sigma^-(\lambda f) &\leqslant \sum_{i=0}^{n-1} \lambda (x_{i+1} - x_i) M_i(f) \\ &\leqslant \lambda S_\sigma^+(f) \\ &\leqslant \lambda I^+(f) \end{aligned}$$

car $\lambda < 0$ et $I^+(f) \leqslant S_\sigma^+(f)$.

De plus,

$$I^-\left(\frac{1}{\lambda}\lambda f\right) \leqslant \frac{1}{\lambda} I^+(\lambda f)$$

donc

$$\lambda I^-(f) \geqslant I^+(\lambda f).$$

Il reste à prouver (pour $\lambda < 0$) que

$$\begin{cases} I^-(\lambda f) \geqslant \lambda I^+(f) \\ I^+(\lambda f) \geqslant \lambda I^-(f). \end{cases}$$

□

4 Théorème fondamental de l'Analyse

Théorème : Soit $f : [a,b] \to \mathbb{R}$ continue. Alors f est Riemann-intégrable.

Preuve :
f est continue sur $[a,b]$; elle est donc bornée. Soient

$$\begin{aligned} \varphi^- : [a,b] &\longrightarrow \mathbb{R} \\ x &\longmapsto I^-_{[a,x]}(f) \end{aligned}$$

et

$$\begin{aligned} \varphi^+ : [a,b] &\longrightarrow \mathbb{R} \\ x &\longmapsto I^+_{[a,x]}(f). \end{aligned}$$

Soit $x \in]a,b[$ et $h > 0$ tel que $x + h \in [a,b]$.

$$\varphi^-(x+h) - \varphi^-(x) = I^-_{[x,x+h]}(f) \leqslant I^+_{[x,x+h]}(f) = \varphi^+(x+h) - \varphi^+(x)$$

donc

$$\begin{cases} \dfrac{1}{h}\big(\varphi^-(x+h) - \varphi^-(x)\big) = \dfrac{1}{h} I^-_{[x,x+h]}(f) \geqslant \dfrac{1}{h} \inf\limits_{[x,x+h]} f \times (x+h-x); \\ \dfrac{1}{h}\big(\varphi^+(x+h) - \varphi^-(x)\big) = \dfrac{1}{h} I^+_{[x,x+h]}(f) \leqslant \dfrac{1}{h} \sup\limits_{[x,x+h]} (f) \times (x+h-x); \end{cases}$$

d'où

$$\inf_{[x,x+h]}(f) = \frac{1}{h} I^-_{[x,x+h]}(f) \leqslant \frac{1}{h} I^+_{[x,x+h]}(f) \leqslant \sup_{[x,x+h]}(f).$$

f est continue sur $[x,x+h]$ donc $\inf\limits_{[x,x+h]}(f) = f(c_h)$ avec $c_h \in [x,x+h]$. $x \leqslant c_h \leqslant x+h$ donc $c_h \xrightarrow[h\to 0]{>} x$. Comme f est continue, $f(c_h) \xrightarrow[h\to 0]{>} f(x)$.

De même, $\sup\limits_{[x,x+h]}(f) = f(d_h)$ avec $d_h \in [x,x+h]$ donc $d_h \xrightarrow[h\to 0]{>} x$ et donc $f(d_h) \xrightarrow[h\to 0]{>} f(x)$.

On en déduit que

$$\begin{cases} \dfrac{\varphi^-(x+h)-\varphi^-(x)}{h} \xrightarrow[\substack{h\to 0\\ >}]{} f(x) \\ \dfrac{\varphi^+(x+h)-\varphi^+(x)}{h} \xrightarrow[\substack{h\to 0\\ >}]{} f(x). \end{cases}$$

De même,

$$\begin{cases} \dfrac{\varphi^-(x+h)-\varphi^-(x)}{h} \xrightarrow[\substack{h\to 0\\ <}]{} f(x) \\ \dfrac{\varphi^+(x+h)-\varphi^+(x)}{h} \xrightarrow[\substack{h\to 0\\ <}]{} f(x). \end{cases}$$

Donc φ^- et φ^+ sont deux primitives de f sur l'intervalle $[a,b]$.

Donc,

$$\exists C \in \mathbb{R},\ \forall x \in [a,b],\ \varphi^-(x) = \varphi^+(x) + C.$$

En évaluant en $x = a$, on a

$$\underbrace{\varphi^-(a)}_{=0} = \underbrace{\varphi^+(a)}_{=0} + C$$

et donc $C = 0$ donc $\varphi^-(b) = \varphi^+(b)$ et donc f est intégrable. □

On a aussi démontré le théorème suivant :

Théorème : Soit $f : [a,b] \longrightarrow \mathbb{R}$ conitnue. Alors

$$x \mapsto \int_{[a,x]} f$$

est une primitive de f. □

Remarque (Notation) :

Soit $f : [a,b] \longrightarrow \mathbb{R}$ continue. On note plutôt $\displaystyle\int_a^b f(t)\ \mathrm{d}t$ à la place de $\displaystyle\int_{[a,b]} f$.

On note aussi $\displaystyle\int_b^a f(t)\ \mathrm{d}t = -\int_{[a,b]} f$.

Corollaire : Soit $f : [a,b] \longrightarrow \mathbb{R}$ continue et F une primitive de f. Alors

$$\int_a^b f(t)\ \mathrm{d}t = F(b) - F(a).$$

Preuve :
Soit $\varphi : x \mapsto \displaystyle\int_a^x f(t)\ \mathrm{d}t$. On sait que φ est une primitive de f. Or,

$$\varphi' = f = F' \text{ donc } (\varphi - F)' = 0$$

On en déduit que

$$\exists C \in \mathbb{R},\ \forall x \in [a,b],\ \varphi(x) = F(x) + C.$$

En particulier,

$$0 = \varphi(a) = F(a) + C$$

donc $C = -F(a)$.

D'où

$$\int_a^b f(t)\ \mathrm{d}t = \varphi(b) = F(b) + C = F(b) - F(a).$$

□

5 Fonctions continues par morceaux

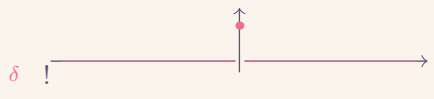
Définition : Soit $f : [a,b] \longrightarrow \mathbb{R}$. On dit que f est continue par morceaux si,

$$\exists \sigma = (x_0, \dots, x_n) \in \mathfrak{S}_{[a,b]},\ \begin{cases} \forall i \in [\![0, n-1]\!]\,,\ f_{\left|]x_i, x_{i+1}[\right.} \text{ est continue;} \\ \forall i \in [\![1, n-1]\!]\,,\ \lim\limits_{\substack{x \to x_i \\ <}} f(x) \in \mathbb{R} \text{ et } \lim\limits_{\substack{x \to x_i \\ >}} f(x) \in \mathbb{R}; \\ \lim\limits_{\substack{x \to a \\ >}} f(x) \in \mathbb{R};\ \lim\limits_{\substack{x \to b \\ <}} f(x) \in \mathbb{R}. \end{cases}$$

Théorème : Toute fonction continue par morceaux sur un segment est Riemann-intégrable sur ce segment. □

Définition : Soit $f : I \subset \mathbb{R} \longrightarrow \mathbb{R}$. On dit que f est continue par morceaux sur I si f est continue par morceaux sur tout segment inclus dans I.

Remarque :



$$\begin{aligned}\delta : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 0 & \text{si } x \neq 0, \\ 1 & \text{si } x = 0. \end{cases}\end{aligned}$$

δ est continue par morceaux sur $\mathbb{R}$. On a $\displaystyle\int_{[0,1]} \delta = 0$, et $\forall x \in [0,1],\ f(x) \geqslant 0$. Mais, $\delta \neq 0$.

6 Sommes de Riemann

Théorème : Soit $f : [a,b] \longrightarrow \mathbb{R}$ continue par morceaux.

À faire : schéma 1

$$\lim_{n\to+\infty} \left(\sum_{i=0}^{n-1} \frac{b-a}{n} f\left(a + i\frac{b-a}{n}\right)\right) = \int_a^b f(t)\,\mathrm{d}t.$$

Preuve (dans le cas où f est continue) *:*

$$\begin{aligned}\forall n \in \mathbb{N}^\star, 0 &\leqslant \left| \int_a^b f(t)\,\mathrm{d}t - \sum_{i=0}^{n-1} \frac{b-a}{n} f\Big(\overbrace{a + i\frac{b-a}{n}}^{x_i}\Big)\right| \\ &= \left| \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} f(t)\,\mathrm{d}t - \sum_{i=0}^{n-1} \frac{b-a}{n} f(x_i)\right| \\ &= \left| \sum_{i=0}^{n-1} \left(\int_{x_i}^{x_{i+1}} f(t)\,\mathrm{d}t - \frac{b-a}{n} f(x_i)\right)\right| \\ &= \left| \sum_{i=0}^{n-1} \left(\int_{x_i}^{x_{i+1}} f(t)\,\mathrm{d}t - \int_{x_i}^{x_{i+1}} f(x_i)\,\mathrm{d}t\right)\right| \\ &= \left| \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} \big(f(t) - f(x_i)\big)\,\mathrm{d}t\right| \\ &\leqslant \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} \big|f(t) - f(x_i)\big|\,\mathrm{d}t.\end{aligned}$$

f est continue sur $[a,b]$, donc uniformément continue sur $[a,b]$:

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x, y \in \mathscr{D}_f,\ |x-y| \leqslant \eta \implies \big|f(x) - f(y)\big| \leqslant \varepsilon.$$

Soit $\varepsilon > 0$. On considère $\eta > 0$ comme ci-dessus. On a $\dfrac{b-a}{n} \longrightarrow 0$ donc, il

existe $N \in \mathbb{N}^\star$ tel que

$$\forall n \geqslant N,\ \frac{b-a}{n} \leqslant \eta.$$

On considère un tel $N \in \mathbb{N}^\star$. On suppose $n \geqslant N$.

$$\forall i \in [\![0, n-1]\!],\ \forall x \in [x_i, x_{i+1}],\ |x - x_i| \leqslant x_{i+1} - x_i = \frac{b-a}{n} \leqslant \eta$$

et donc

$$\big|f(x) - f(x_i)\big| \leqslant \varepsilon.$$

Donc,

$$\forall n \geqslant N,\ \left|\int_a^b f(x)\ \mathrm{d}x - \frac{b-a}{n}\sum_{i=0}^{n-1} f(x_i)\right| \leqslant \sum_{i=0}^{n-1}\int_{x_i}^{x_{i+1}} \varepsilon\ \mathrm{d}t = \varepsilon(b-a).$$

□

Proposition : Soit $f : [a,b] \to \mathbb{R}$ continue par morceaux et $n \in \mathbb{N}^\star$.

$$\frac{b-a}{n}\sum_{i=1}^{n} f\big(\underbrace{a + i\tfrac{b-a}{n}}_{x_i}\big) \xrightarrow[n\to+\infty]{} \int_a^b f(t)\ \mathrm{d}t.$$

□

Remarque :
On suppose à présent f de classe $\mathscr{C}^1$ sur $[a,b]$. f' est continue sur $[a,b]$: on considère

$$M = \max_{x\in[a,b]} \big|f'(x)\big|.$$

$$\begin{aligned}
\forall n \in \mathbb{N}^\star,\ \left|\int_a^b f(t)\ \mathrm{d}t - \frac{b-a}{n}\sum_{i=0}^{n-1} f(x_i)\right| &= \left|\sum_{i=0}^{n-1}\int_{x_i}^{x_{i+1}} \big(f(t) - f(x_i)\big)\ \mathrm{d}t\right| \\
&\leqslant \sum_{i=0}^{n-1}\int_{x_i}^{x_{i+1}} \big|f(t) - f(x_i)\big|\ \mathrm{d}t \\
&\leqslant \sum_{i=0}^{n-1}\int_{x_i}^{x_{i+1}} M|t - x_i|\ \mathrm{d}t \\
&\leqslant M\sum_{i=0}^{n-1}\frac{(x_{i+1}-x_i)^2}{2} \\
&\leqslant \frac{M}{2}\left(\frac{b-a}{n}\right)^2 n \\
&= \frac{M(b-a)^2}{2n}.
\end{aligned}$$

Par exemple, on veut calculer une valeur approchée de $\ln 2$ à 10^{-3} près :

$$\ln 2 = \int_1^2 \frac{1}{t}\,\mathrm{d}t.$$

Soit $f : t \mapsto \dfrac{1}{t}$ de classe $\mathscr{C}^1$ sur $[1,2]$.

$$\forall t \in [1,2],\ |f'(t)| = \frac{1}{t^2} \leqslant 1$$

d'où $M = 1$.

On cherche $n \in \mathbb{N}^\star$ tel que

$$\frac{1(2-1)^2}{2n} \leqslant 10^{-3}$$

i.e. $n \geqslant 500$.

Donc, $\dfrac{1}{500}\displaystyle\sum_{i=0}^{499} \frac{1}{1+\frac{i}{500}} \simeq 0{,}693$ est une valeur approchée de $\ln 2$ à 10^{-3} près.

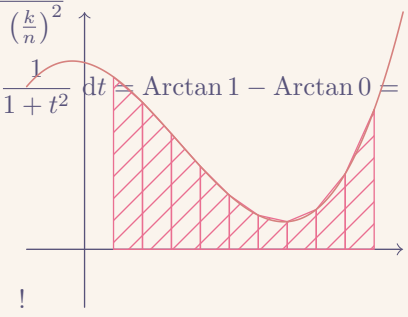
Exemple :

$$\textit{Que vaut } \lim_{n\to+\infty} \sum_{i=1}^{n} \frac{n}{n^2+k^2} \textit{ ?}$$

$\displaystyle\sum_{1\leqslant k\leqslant n} \frac{n}{n^2+k^2}$ n'est pas une série ! En effet, en passant de n à $n+1$, on modifie les termes précédents.

$$\begin{aligned}\forall n \in \mathbb{N}^\star,\ \sum_{k=1}^{n} \frac{n}{n^2+k^2} &= \sum_{k=1}^{n} \frac{\frac{1}{n}}{1+\left(\frac{k}{n}\right)^2} \\ &= \frac{1}{n}\sum_{k=1}^{n} \frac{1}{1+\left(\frac{k}{n}\right)^2} \\ &\xrightarrow[n\to+\infty]{} \int_0^1 \frac{1}{1+t^2}\,\mathrm{d}t = \operatorname{Arctan} 1 - \operatorname{Arctan} 0 = \frac{\pi}{4}.\end{aligned}$$

Remarque (Méthode des trapèzes) :



!

Au lieu d'approximer l'intégrale par des rectangles, on utilise des trapèzes.

7 Retour sur les formules de Taylor

Proposition : Soit $f : I \subset \mathbb{R} \longrightarrow \mathbb{R}$ continue et F une primitive de f. On suppose

$$f(x) = \sum_{i=0}^{n} \alpha_i (x-a)^i + \underset{x\to a}{o}\left((x-a)^n\right).$$

Alors,

$$F(x) = F(a) + \sum_{i=0}^{n} \alpha_i \frac{(x-a)^{i+1}}{i+1} + \underset{x\to a}{o}\left((x-a)^{n+1}\right).$$

Preuve :
Soit $\varepsilon > 0$. On sait qu'il existe $\eta > 0$ tel que

$$\forall x \in [a-\eta, a+\eta],\ \left| f(x) - \sum_{i=0}^{n} \alpha_i (x-a)^i \right| \leqslant \varepsilon\, |x-a|^n.$$

On considère un tel $\eta > 0$. Soit $x \in [a-\eta, a+\eta]$.

$$\overbrace{\left| F(x) - F(a) - \sum_{i=0}^{n} \alpha_i \frac{(x-a)^{i+1}}{i+1} \right|}^{(\star)} = \left| \int_a^x f(t)\ \mathrm{d}t - \sum_{i=0}^{n} \alpha_i \int_a^x (t-a)^i\ \mathrm{d}t \right|$$
$$= \left| \int_a^x \left(f(t) - \sum_{i=0}^{n} \alpha_i (t-a)^i \right)\ \mathrm{d}t \right|$$

On suppose $x \geqslant a$, donc

$$\begin{aligned}(\star) &\leqslant \int_a^x \left| f(t) - \sum_{i=0}^{n} \alpha_i (t-a)^i \right|\ \mathrm{d}t \\ &\leqslant \int_a^x \varepsilon |t-a|^n\ \mathrm{d}t \\ &\leqslant \varepsilon \int_a^x (t-a)^n\ \mathrm{d}t \\ &= \frac{\varepsilon}{n+1}(x-a)^{n+1}\end{aligned}$$

On suppose $x < a$.

$$\begin{aligned}
(\star) &= \left| \int_x^a \left(f(t) - \sum_{i=0}^{n} \alpha_i (t-a)^i \right) \, \mathrm{d}t \right| \\
&\leqslant \int_x^a \left| f(t) - \sum_{i=0}^{n} \alpha_i (t-a)^i \right| \, \mathrm{d}t \\
&\leqslant \int_x^a \varepsilon |t-a|^n \, \mathrm{d}t \\
&\leqslant \alpha \int_x^a (a-t)^n \, \mathrm{d}t \\
&\leqslant \varepsilon \left[-\frac{(a-t)^{n+1}}{n+1} \right]_x^a \\
&\leqslant \varepsilon \frac{(a-x)^{n+1}}{n+1} \\
&= \frac{\varepsilon}{n+1} |x-a|^{n+1}
\end{aligned}$$

□

Corollaire : Soit $f : \overset{a}{\curvearrowright} I \longrightarrow \mathbb{R}$ de classe $\mathscr{C}^n$. Alors,

$$f(x) = \sum_{i=0}^{n} \frac{f^{(i)}(a)}{i!} (x-a)^i + \underset{x \to a}{\wp} \left((x-a)^n \right).$$

Preuve :
par récurrence sur n. □

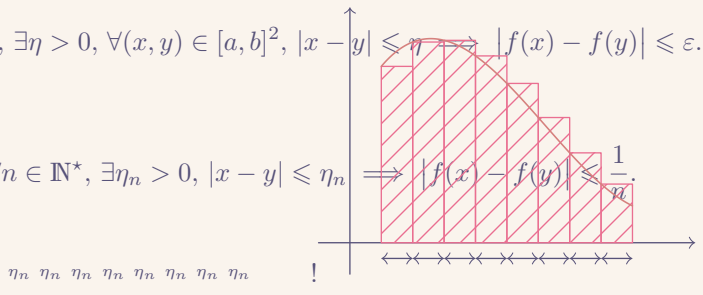
8 Fonctions réglées

Soit $f : [a,b] \to \mathbb{R}$ continue. Cette fonction est donc uniformément continue (théorème de Heine) :

$$\forall \varepsilon > 0, \exists \eta > 0, \forall (x,y) \in [a,b]^2, |x-y| \leqslant \eta \Longrightarrow \left| f(x) - f(y) \right| \leqslant \varepsilon.$$

D'où

$$\forall n \in \mathbb{N}^\star, \exists \eta_n > 0, |x-y| \leqslant \eta_n \Longrightarrow \left| f(x) - f(y) \right| \leqslant \frac{1}{n}.$$

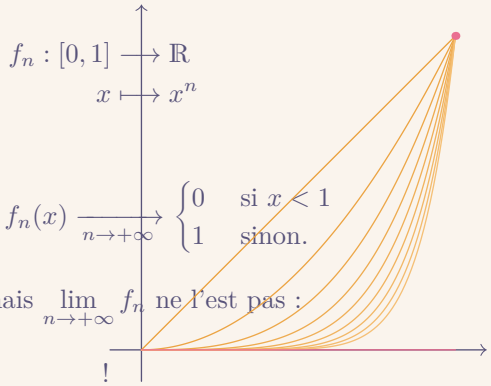


Cependant, contrairement au sommes de Darboux, cette construction utilise des notions que l'on admet : notamment, la convergence d'une suite de fonctions.

Exemple (convergence d'une suite de fonctions) :
Pour $n \in \mathbb{N}$, on pose

$$f_n : [0,1] \longrightarrow \mathbb{R}, \quad x \longmapsto x^n$$

$$\forall x \in [0,1],\ f_n(x) \xrightarrow[n\to+\infty]{} \begin{cases} 0 & \text{si } x < 1 \\ 1 & \text{sinon.} \end{cases}$$



Pour $n \in \mathbb{N}$, f_n est continue mais $\lim\limits_{n\to+\infty} f_n$ ne l'est pas : !

Chapitre 31

Variables aléatoires

1 Définitions

Définition : Une variable aléatoire est une application sur un espace probabilisé (Ω, P) dans E où E est un ensemble quelconque :

$$X : \Omega \longrightarrow E.$$

Si $E \subset \mathbb{R}$, on dit que X est réelle.

Si E est un espace vectoriel, on dit que X est un vecteur aléatoire.

Si $E \subset \mathscr{M}_{n,p}(\mathbb{K})$, on dit que X est une matrice aléatoire.

Exemple :
On lance 2 dés bien équilibrés et on note S la somme des points sur ces deux dés.

On pose $\Omega = [\![1,6]\!]^2$, P l'équiprobabilité et

$$\begin{aligned} S : \Omega &\longrightarrow \mathbb{R} \\ (\omega_1, \omega_2) &\longmapsto \omega_1 + \omega_2. \end{aligned}$$

$S(\Omega) = [\![2,12]\!]$.

s	2	3	4	5	6	7	8	9	10	11	12
$P(S=s)$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Dans la suite du chapitre, (Ω, P) est un espace probabilisé.

Proposition : Soit $X : \Omega \to E$ une variable aléatoire avec $E = X(\Omega)$. L'application

$$\begin{aligned} P_X : \mathscr{P}(E) &\longrightarrow [0,1] \\ A &\longmapsto P\left(X^{-1}(A)\right) \end{aligned}$$

est une probabilité sur E.

Preuve :
- $\forall A \in \mathscr{P}(E)$, $X^{-1}(A) \in \mathscr{P}(\Omega)$ donc $P\big(X^{-1}(A)\big) \in [0,1]$.
- $P_X(E) = P\big(X^{-1}(E)\big) = P(\Omega) = 1$.
- Soient $A, B \in \mathscr{P}(E)$ avec $A \cap B = .$

$$\begin{aligned} P_X(A \cup B) &= P\big(X^{-1}(A \cup B)\big) \\ &= P\big(X^{-1}(A) \cup X^{-1}(B)\big) \\ &= P\big(X^{-1}(A)\big) + P\big(X^{-1}(B)\big) \\ &= P_X(A) + P_X(B). \end{aligned}$$

□

Définition : Soit $X : \Omega \to E$ une variable aléatoire. P_X est la loi de X.

Remarque (Notations) :
Soit $X : \Omega \to E$ une variable aléatoire.

- Soit $A \in \mathscr{P}(E)$. $X^{-1}(A)$ est noté $(X \in A)$. D'où $P_X(A) = P(X \in A)$.
- Soit $x \in E$. $X^{-1}\big(\{x\}\big)$ est noté $(X = x)$; $P_X\big(\{x\}\big) = P(X = x)$.
- Si $E \subset \mathbb{R}$, $X^{-1}\big(]-\infty, x]\big)$ est noté $(X \leqslant x)$ et donc $P\big(X^{-1}\big(]-\infty, x]\big)\big) = P(X \leqslant x)$.
  De même avec les autres inégalités strictes et larges.

Remarque (Notation) :
On note $X \sim Y$ si X et Y suivent la même loi, i.e. $P_X = P_Y$.

2 Exemples de lois

Définition : Soit $X : \Omega \to E$ une variable aléatoire. On dit que X suit une loi uniforme si P_X est l'équiprobabilité sur $X(\Omega)$. On note alors $X \sim \mathcal{U}\big(X(\Omega)\big)$.

Définition : Soit $X : \Omega \to \{0, 1\}$. On note $p = P(X = 1) \in [0, 1]$. On dit que X suit la loi de Bernoulli de paramètre p. On note alors $X \sim \mathcal{B}(p)$.

Définition : Soit $X : \Omega \to [\![0, n]\!]$. On dit que X suit la loi binomiale de paramètres n et p si

$$\forall k \in [\![0, n]\!] \, , \, P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

On note alors $X \sim \mathcal{B}(n, p)$.

Théorème : On considère une expérience aléatoire qui n'a que deux issues possibles : succès ou échec. On répète n fois à l'identique cette expérience, et on note X le nombre de succès. Alors $X \sim \mathcal{B}(n, p)$ où P est la probabilité de succès. □

3 Couples de variables aléatoires

Exemple :
On lance 2 dés bien équilibrés ; on note S la somme des points sur ces deux dés et M le maximum.

S \ M	1	2	3	4	5	6	loi de S
2	$1/36$	0	0	0	0	0	$1/36$
3	0	$2/36$	0	0	0	0	$2/36$
4	0	$1/36$	$2/36$	0	0	0	$3/36$
5	0	0	$2/36$	$2/36$	0	0	$4/36$
6	0	0	$1/36$	$2/36$	$2/36$	0	$5/36$
7	0	0	0	$0/36$	$2/36$	$2/36$	$6/36$
8	0	0	0	$1/36$	$2/36$	$2/36$	$5/36$
9	0	0	0	0	$2/36$	$2/36$	$4/36$
10	0	0	0	0	$1/36$	$2/36$	$3/36$
11	0	0	0	0	0	$2/36$	$2/36$
12	0	0	0	0	0	$1/36$	$1/36$
loi de M	$1/36$	$3/36$	$5/36$	$7/36$	$9/36$	$11/36$	

Définition : Soient $X : \Omega \to E$ et $Y : \Omega \to F$ deux variables aléatoires.

La loi du couple (X, Y) est P_Z où

$$\begin{aligned} Z : \Omega &\longrightarrow E \times F \\ \omega &\longmapsto \big(X(\omega), Y(\omega)\big) \end{aligned}$$

i.e. c'est la donnée de

$$\forall x \in X(\Omega), \forall y \in Y(\Omega), P(X = x, Y = y) = P\big((X = x) \cap (Y = y)\big).$$

Définition : Soient $X : \Omega \to E$ et $Y : \Omega \to F$. Les lois marginales du couple (X, Y) sont P_X et P_Y.

Proposition : Avec les notations précédentes,

$$\forall x \in X(\Omega),\ P(X = x) = \sum_{y \in Y(\Omega)} P(X = x, Y = y);$$
$$\forall y \in Y(\Omega),\ P(Y = y) = \sum_{x \in X(\Omega)} P(X = x, Y = y).$$

Preuve :
probabilités totales □

Remarque :
Si

$$\forall y \in Y(\Omega),\ P(Y = y) \neq 0$$

alors

$$\forall x \in X(\Omega),\ P(X = x) = \sum_{y \in Y(\Omega)} P_{(Y=y)}(X = x)\ P(Y = y).$$

Définition : Soient $X : \Omega \to E$ et $Y : \Omega \to F$ deux variables aléatoires. On dit que X et Y sont indépendantes si

$$\forall A \subset X(\Omega), \forall B \subset Y(\Omega),\ P(X \in A, Y \in B) = P(X \in A)\ P(Y \in B).$$

On note alors $X \perp\!\!\!\perp Y$.

Proposition : Avec les notations précédentes,

$$X \perp Y \iff \forall x \in X(\Omega), \forall y \in Y(\Omega),\ P(X = x, Y = y) = P(X = x)P(Y = y).$$

Preuve " $\Longrightarrow$ " immédiat
" $\Longleftarrow$ " Soient $A = \{x_1, \ldots, x_n\} \subset X(\Omega)$ et $B = \{y_1, \ldots, y_p\} \subset Y(\Omega)$.

$$\begin{aligned}
P(X \in A, Y \in B) &= P\left(\left(\bigcup_{i=1}^{n}{}^{\cdot}(X = x_i)\right) \cap (Y \in B)\right) \\
&= P\left(\bigcup_{i=1}^{n}{}^{\cdot}\left((X = x_i) \cap (Y \in B)\right)\right) \\
&= \sum_{i=1}^{n} P\big((X = x_i) \cap (Y \in B)\big) \\
&= \sum_{i=1}^{n} P\left((X = x_i) \cap \left(\bigcup_{j=1}^{p}{}^{\cdot}(Y = y_j)\right)\right) \\
&= \sum_{i=1}^{n} P\left(\bigcup_{j=1}^{p}{}^{\cdot}\left((X = x_i) \cap (Y = y_i)\right)\right) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{p} P(X = x_i, Y = y_j) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{p} P(X = x_i)\, P(Y = y_j) \\
&= \sum_{i=1}^{n} P(X = x_i \sum_{j=1}^{p} P(Y = y_j) \\
&= P(X \in A)\ P(Y \in B).
\end{aligned}$$

□

4 Familles de variables aléatoires

Définition : Soit $(X_i)_{i\in I} \in \prod_{i\in I} E_i^{\Omega}$ une famille de variables aléatoires. On dit que ces variables sont indépendantes si, pour toute partie finie J de I, et pour tout $(A_j)_{j\in J} \in \prod_{j\in J} \mathcal{P}(E_j)$,

$$P\left(\bigcap_{j\in J}(X_j \in A_j)\right) = \prod_{j\in J} P(X_j \in A_j).$$

Proposition : Avec les notations précédentes, $(X_i)_{i\in I}$ est une famille de

variables aléatoires indédpendantes si et seulement si

$$\forall J \subset I,\ J \text{ finie},\ \forall (x_j)_{j\in J} \in \prod_{j\in J} X_j(\Omega),\ P\left(\bigcap_{j\in J}(X_j = x_j)\right) = \prod_{j\in J} P(X_j = x_j).$$

□

Proposition : Soit $(X_i)_{i\in\mathbb{N}}$ une suite de variables aléatoires suivant la même loi de Bernoulli $\mathscr{B}(p)$. Alors,

$$\forall n \in \mathbb{N}^\star,\ \sum_{i=1}^{n} X_i \sim \mathscr{B}(n,p).$$

Proposition : Soient $X \sim \mathscr{B}(n,p)$ et $Y \sim \mathscr{B}(m,p)$.
Si $X \perp\!\!\!\perp Y$, alors $X + Y \sim \mathscr{B}(n+m,p)$. □

5 Espérance d'une variable aléatoire

Dans ce paragrape, toutes les variables aléatoires sont à valeurs réelles.

Définition : Soit $X : \Omega \to \mathbb{R}$. L'espérance de X est

$$E(X) = \sum_{x\in X(\Omega)} x\, P(X = x).$$

Exemple (À connaître) : 1. Avec $X \sim \mathscr{B}(p)$, on a $E(X) = \sum_{x\in\{0,1\}} xP(X = x) = p$.

2. Avec $X \sim \mathcal{B}(n,p)$, on a

$$\begin{aligned}
E(X) &= \sum_{k=0}^{n} k\,P(X=k) \\
&= \sum_{k=1}^{n} k\binom{n}{k}p^k(1-p)^{n-k} \\
&= n\sum_{k=1}^{n}\binom{n-1}{k-1}p^k(1-p)^{n-k} \\
&= np\sum_{k=0}^{n-1}\binom{n-1}{k}p^k(1-p)^{n-k-1} \\
&= np(p+1-p)^{n-1} \\
&= np
\end{aligned}$$

Lemme : Soit $X : \Omega \to \mathbb{R}$.

$$E(X) = \sum_{\omega\in\Omega} X(\omega)\,P\big(\{\omega\}\big).$$

Preuve :

$$\begin{aligned}
\sum_{w\in\Omega} X(\omega)\,P\big(\{\omega\}\big) &= \sum_{x\in X(\Omega)}\ \sum_{\substack{\omega\in\Omega\\ X(\omega)=x}} X(\omega)\,P\big(\{\omega\}\big) \\
&= \sum_{x\in X(\Omega)}\ \sum_{\substack{\omega\in\Omega\\ X(\omega)=x}} xP\big(\{\omega\}\big) \\
&= \sum_{x\in X(\omega)} x\sum_{\substack{\omega\in\Omega\\ X(\omega)=x}} P\big(\{\omega\}\big) \\
&= \sum_{x\in X(\Omega)} xP\left(\bigcup_{\substack{\omega\in\Omega\\ X(\omega)=x}}^{\cdot}\{\omega\}\right) \\
&= \sum_{x\in X(\Omega)} x\,P(X=x)
\end{aligned}$$

□

Théorème (linéarité de l'espérance) **:** Soient X et Y deux variables aléatoires réelles, et α, β deux réels. Alors,

$$E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y).$$

Preuve :

$$\begin{aligned}\alpha E(X) + \beta E(Y) &= \alpha \sum_{\omega\in\Omega} X(\omega)P\big(\{\omega\}\big) = \beta \sum_{\omega\in\Omega} Y(\omega)P\big(\{\omega\}\big)\\ &= \sum_{\omega\in\Omega} \big(\alpha X(\omega) + \beta Y(\omega)\big)P\big(\{\omega\}\big)\\ &= E(\alpha X + \beta Y).\end{aligned}$$

□

Corollaire : Soit X une variable aléatoire suivant la loi binomiale $\mathscr{B}(n,p)$. On a $E(X) = np$.

Preuve :
Soient $X_1, \ldots, X_n$ des variables indépendantes suivant toutes $\mathscr{B}(p)$.

On a

$$X \sim \sum_{i=1}^{n} X_i$$

donc

$$\begin{aligned}E(X) &= E\left(\sum_{i=1}^{n} X_i\right)\\ &= \sum_{i=1}^{n} E(X_i)\\ &= np\end{aligned}$$

□

Exemple :

On pose $\Omega = S_n$ le groupe symétrique ; P l'équiprobabilité sur Ω et

$$\begin{aligned} X : \Omega &\longrightarrow [\![0, n]\!] \\ \omega &\longmapsto \text{le nombre de points fixes de } \omega \end{aligned}$$

Que vaut $E(X)$?

On pose, pour tout $\omega \in \Omega$, pour tout $i \in [\![0, n]\!]$, $X_i(\omega) = \begin{cases} 1 & \text{si } \omega(i) = i \\ 0 & \text{sinon.} \end{cases}$

Ainsi,

$$\forall \omega \in \Omega, \sum_{i=1}^{n} X_i(\omega) = X(\omega).$$

D'où

$$\begin{aligned} E(X) &= E\left(\sum_{i=1}^{n} X_i\right) \\ &= \sum_{i=1}^{n} E(X_i) \\ &= \sum_{i=1}^{n} P(X_i = 1) \\ &= \sum_{i=1}^{n} \frac{(n-1)!}{n!} \\ &= \sum_{i=1}^{n} \frac{1}{n} \\ &= \frac{n}{n} \\ &= 1 \end{aligned}$$

On n'a pas eu besoin de déterminer la loi de X pour déterminer l'espérance de X.

Définition : Soient $X : \Omega \to \mathbb{R}$ une variable aléatoire et $f : \mathbb{R} \to \mathbb{R}$.

$$\begin{array}{ccc} \Omega & \xrightarrow{X} & \mathbb{R} \\ & \searrow & \downarrow f \\ & & \mathbb{R} \end{array}$$

La composée $f \circ X$ est notée $f(X)$.

Théorème (formule de transfert) **:** Avec les notations précédentes,

$$E\big(f(X)\big) = \sum_{x\in X(\Omega)} f(x)\,P(X=x).$$

Preuve :

$$\begin{aligned} E\big(f(X)\big) &= \sum_{\omega\in\Omega} f\big(X(\omega)\big)\,P\big(\{\omega\}\big) \\ &= \sum_{x\in X(\Omega)} \sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} f\big(X(\omega)\big)\,P\big(\{\omega\}\big) \\ &= \sum_{x\in X(\Omega)} f(x) \sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P\big(\{\omega\}\big) \\ &= \sum_{x\in X(\Omega)} f(x)\,P(X=x). \end{aligned}$$

□

Exemple :
Avec $X(\Omega)=\{-1,0,1\}$, $P(X=-1)=\dfrac{1}{2}$, $P(X=0)=\dfrac{1}{4}$, $P(X=1)=\dfrac{1}{4}$, *que vaut* $E(X^2)$ *?*

— Loi de X^2 : $X^2(\Omega)=\{0,1\}$ avec $P(X^2=0)=\dfrac{1}{4}$ et $P(X^2=1)=\dfrac{3}{4}$; d'où $E(X^2)=\dfrac{3}{4}$.

— Formule de transfert : $E(X^2)=\displaystyle\sum_{x=-1}^{1} x^2 P(X=x)=\frac{3}{4}$.

6 Variance

Dans ce paragrape, toutes les variables aléatoires sont à valeurs réelles.

Définition : Soit $X:\Omega\to\mathbb{R}$ une variable aléatoire. La variance de X est

$$V(X)=E\left(\big(X-E(X)\big)^2\right).$$

Proposition : Avec les notations précédentes,

$$V(X) \geqslant 0.$$

Preuve :
On pose $\mu = E(X)$.

$$V(X) = \sum_{x \in X(\Omega)} \underbrace{(x-\mu)^2 \, P(X=x)}_{\geqslant 0} \geqslant 0.$$

□

Définition : L'écart-type de X est

$$\sigma_X = \sqrt{V(X)}.$$

Définition : On dit que X vérifie presque sûrement une propriété si la probabilité que X vérifie cette propriété vaut 1.

Proposition :

$$V(X) = 0 \iff X \text{ est presque sûrement constante..}$$

□

Proposition (Kœnig-Huygens) **:**

$$V(X) = E(X^2) - E(X)^2.$$

Preuve :

On pose $\mu = E(X)$

$$\begin{aligned} V(X) &= E\big((X-\mu)^2\big) \\ &= E(X^2 - 2\mu X + \mu^2) \\ &= E(X^2) - 2\mu E(X) + \mu^2 E(1) \\ &= E(X^2) - 2\mu^2 + \mu^2 \\ &= E(X^2) - \mu^2 \end{aligned}$$

□

EXEMPLE : 1. Avec $X \sim \mathcal{B}(p)$, on a $X^2 \sim \mathcal{B}(p)$ d'où

$$V(X) = p - p^2 = p(1-p) = pq \leqslant \frac{1}{4} \text{ avec } q = 1-p$$

2. Avec $X \sim \mathcal{B}(n,p)$.

$$\begin{aligned} E(X^2) &= \sum_{k=0}^{n} k^2 \binom{n}{k} p^k q^{n-k} \\ &= \cdots\cdots\cdots \end{aligned}$$

En faisant le calcul, on trouve $V(X) = npq$.

Théorème : Soit $X, Y : \Omega \to \mathbb{R}$.

$$V(X+Y) = V(X) + V(Y) + 2\,\mathrm{Cov}(X,Y)$$

où $\mathrm{Cov}(X,Y) = E(XY) - E(X)\,E(Y)$ est la covariance de X et Y.

Preuve :

$$\begin{aligned} E\big((X+Y)^2\big) &= E(X^2 + Y^2 + 2XY) \\ &= E(X^2) + E(Y^2) + 2E(XY) \end{aligned}$$

et

$$\begin{aligned} \big(E(X+Y)\big)^2 &= \big(E(X) + E(Y)\big)^2 \\ &= E(X)^2 + E(Y)^2 + 2E(X)E(Y). \end{aligned}$$

D'où

$$V(X+Y) = V(X) + V(Y) + 2\,\mathrm{Cov}(X,Y).$$

□

Proposition : Si $X \perp\!\!\!\perp Y$, alors $\mathrm{Cov}(X,Y) = 0$. D'où

$$V(X+Y) = V(X) + V(Y).$$

Preuve :

$$\begin{aligned} E(XY) &= \sum_{\substack{x\in X(\Omega)\\ y\in Y(\Omega)}} xy\,P(X=x, Y=y) \\ &= \sum_{x\in X(\Omega)} \sum_{y\in Y(\Omega)} xyP(X=x)P(Y=y) \\ &= \sum_{x\in X(\Omega)} x\,P(X=x) \sum_{y\in Y(\Omega)} y\,P(Y=y) \\ &= E(X)E(Y) \end{aligned}$$

□

Proposition : Soit $(X_i)_{1\leqslant i\leqslant n}$ des variabls aléatoires définies sur le même espace probabilisé (Ω, P). Alors

$$\begin{aligned} V\left(\sum_{i=1}^{n} X_i\right) &= \sum_{1\leqslant i,j\leqslant n} \mathrm{Cov}(X_i, X_j) \\ &= \sum_{i=1}^{n} V(X_i) + 2 \sum_{1\leqslant i<j\leqslant n} \mathrm{Cov}(X_i, X_j) \end{aligned}$$

□

Corollaire : Avec les notations précédentes, si les X_i sont deux à deux non corrélés (i.e. $\mathrm{Cov}(X_i, X_j) = 0$ pour $i \neq j$), alors

$$V\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} V(X_i).$$

□

Corollaire : Avec les notations précédentes, si les X_i sont indépendantes deux à deux, alors

$$V\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} V(X_i).$$

□

Corollaire : Soit $X \sim \mathcal{B}(n,p)$. Alors,

$$V(X) = np(1-p).$$

Preuve :
On pose $X \sim \sum_{i=1}^{n} X_i$ où les (X_i) sont mutuellement indépendants et $\forall i$, $X_i \sim \mathcal{B}(p)$.

$$\begin{aligned} V(X) &= V\left(\sum_{i=1}^{n} X_i\right) \\ &= \sum_{i=1}^{n} V(X_i) \\ &= \sum_{i=1}^{n} p(1-p) \\ &= np(1-p) \end{aligned}$$

□

Proposition (transfert) **:** Soient $X_1, \ldots, X_n$ des variables aléatoires à valeurs réelles toutes définies sur un même espace probabilisé (Ω, P) et $f : \mathbb{R}^n \longrightarrow \mathbb{R}$

$$E\big(f(X_1,\ldots,X_n)\big) = \sum_{x_1 \in X_1(\Omega)} \cdots \sum_{x_n \in X_n(\Omega)} f(x_1,\ldots,x_n) P(X_1 = x_1, \ldots, X_n = x_n).$$

Preuve :

$$\begin{aligned}
E\big(f(X_1,\dots,X_n)\big) &= \sum_{\omega\in\Omega} f\big(X_1(\omega),\dots,X_n(\omega)\big)\,P\big(\{\omega\}\big)\\
&= \sum_{x_1\in X_1(\Omega)}\cdots\sum_{x_n\in X_n(\Omega)}\sum_{\substack{\omega\in\Omega\\ \forall i,\,X_i(\omega)=x_i}} f\big(X_1(\omega),\dots,X_n(\omega)\big)\,P\big(\{\omega\}\big)\\
&= \sum_{x_1\in X_1(\Omega)}\cdots\sum_{x_n\in X_n(\Omega)} f(x_1,\dots,x_n)\sum_{\substack{\omega\in\Omega\\ \forall i,\,X_i(\omega)=x_i}} P\big(\{\omega\}\big)\\
&= \sum_{x_1\in X_1(\Omega)}\cdots\sum_{x_n\in X_n} f(x_1,\dots,x_n)P(X_1=x_1,\dots,X_n=x_n)
\end{aligned}$$

□

7 Covariance (Hors-Programme)

On se place dans une optique de Big Data. On dispose d'un tableau à N lignes : chaque ligne correspond à une observation et chaque colonne à une "mesure" (ou caractéristique).

Ces caractéristiques peuvent être corrélées plus ou moins fortement et contenir plus ou moins d'information.

Plus la variance est grande, plus il y a d'information.

Soient X et Y deux colonnes. D'après l'inégalité de Cauchy-Schwarz :

$$\big|\operatorname{Cov}(X,Y)\big| \leqslant \sigma_X\,\sigma_Y \quad \text{donc} \quad -1 \leqslant \frac{\operatorname{Cov}(X,Y)}{\sigma_X\,\sigma_Y} \leqslant 1.$$

Si $Y=\alpha X+\beta$: $$\left|\frac{\operatorname{Cov}(X,Y)}{\sigma_X,\sigma_Y}\right| = 1.$$

L'objectif est de modifier les colonnes de façon à extraire le plus d'informations possible sur le moins de colonnes possibles.

La matrice de covariance est

$$A = \big(\operatorname{Cov}(X_i,X_j)\big)_{\substack{1\leqslant i\leqslant N\\ 1\leqslant j\leqslant N}}.$$

On aimerait que la matrice A soit diagonale avec de grands coefficients diagonaux.

L'année prochaine, nous verrons le théorème suivant :

Théorème (théorème spectral) **:** Toute matrice symétrique réelle est diagonalisable dans une base orthonormée de vecteurs propres.

Il existe donc des variables aléatoires $Y_1, \dots, Y_k$ combinaisons linéaires des $X_1, \dots, X_k$ telles que

$$\big(\mathrm{Cov}(Y_i, Y_j)\big) = \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & (0) \\ & & \ddots & \\ & (0) & & \lambda_k \end{pmatrix}.$$

De plus, le maximum de $V(\alpha_1 X_1 + \cdots + \alpha_k X_k)$ avec la condition que $\alpha_1^2 + \cdots + \alpha_k^2 = 1$ est $V(Y_1) = \lambda_1$.

Définition (Multiplicateurs de Lagrange) **:** Soit $f : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ où U est un ouvert de $\mathbb{R}^n$. On cherche $\max\limits_{(x_i)_{i\in[\![1,n]\!]}\in R^n} f(x_1, \dots, x_n)$ avec la contrainte $g(x_1, \dots, x_n)$.

On pose

$$\begin{aligned} F : \mathbb{R}^{n+1} &\longrightarrow \mathbb{R} \\ (x_1, \dots, x_n, \lambda) &\longmapsto f(x_1, \dots, x_n) + \lambda g(x_1, \dots, x_n). \end{aligned}$$

On cherche les points critiques de F :

$$\begin{aligned} \nabla F(x_1, \dots, x_n, \lambda) = 0 &\iff \begin{cases} \forall i,\ \dfrac{\partial F}{\partial x_i}(x_1, \dots, x_n, \lambda) = 0 \\ \dfrac{\partial F}{\partial \lambda}(x_1, \dots, x_n, \lambda) = 0 \end{cases} \\ &\iff \begin{cases} \forall i,\ \dfrac{\partial f}{\partial x_i}(x_1, \dots, x_n) + \lambda \dfrac{\partial g}{\partial x_i}(x_1, \dots, x_n) = 0 \\ g(x_1, \dots, x_n) = 0 \end{cases} \end{aligned}$$

Si $(x_1, \dots, x_n, \lambda)$ est le maximum de F, alors
$\forall y_1, \dots, y_n, \mu \in \mathbb{R}^{n+1}$ $\quad F(x_1, \dots, x_n, \lambda) \geqslant F(y_1, \dots, y_n, \mu)$

$$f(x_1, \dots, x_n) + \underbrace{\lambda g(x_1, \dots, x_n)}_{=0} \geqslant f(y_1, \dots, y_n)$$

8 Loi des grands nombres

Lemme (inégalité de Марков [a]) **:** Soit $X : \Omega \to \mathbb{R}^+$ une variable aléatoire positive.

$$\forall t \in \mathbb{R}_+^\star,\ P(X \geqslant t) \leqslant \frac{E(X)}{t}$$

ou encore,

$$\forall u \in \mathbb{R}_+^\star,\ P\big(X \geqslant u\, E(X)\big) \leqslant \frac{1}{u}.$$

a. Марков : Markov

Preuve :
Soit $t \in \mathbb{R}_+^\star$.

$$\begin{aligned} E(X) &= \sum_{x \in X(\Omega)} x\, P(X = x) \\ &= \sum_{\substack{x \in X(\Omega) \\ x \geqslant t}} x\, P(X = x) + \sum_{\substack{x \in X(\Omega) \\ x < t}} x\, P(X = x) \\ &\geqslant \sum_{\substack{x \in X(\Omega) \\ x \geqslant t}} t\, P(X = x) + \sum_{\substack{x \in X(\Omega) \\ x < t}} 0 \\ &\geqslant t\, P(X \geqslant t). \end{aligned}$$

□

Lemme (inégalté de Bienaymé-чебышёв [a]) **:** Soit $X : \Omega \to \mathbb{R}$ une variable aléatoire réelle. On pose $\mu = E(X)$ et $\sigma = \sigma_X$. Alors,

$$\forall t \in \mathbb{R}_+^\star,\ P\big(|X - \mu| \geqslant t\big) \leqslant \frac{\sigma^2}{t^2}$$

ou encore

$$\forall u \in \mathbb{R}_\star^+,\ P\big(|X - \mu| \geqslant u\sigma\big) \leqslant \frac{1}{u^2}.$$

a. чебышёв : Tchebychev

Preuve :
On pose $Y = |X - \mu|^2$, Y est positive.

$$E(Y) = E\left((X - \mu)^2\right) = V(X) = \sigma^2.$$

Donc, d'après l'inégalité de Марков :

$$\forall y \in \mathbb{R}_+^\star,\ P(Y \geqslant y) \leqslant \frac{\sigma^2}{y}$$

donc

$$\forall t > 0,\ P\left((X - \mu)^2 \geqslant t^2\right) \leqslant \frac{\sigma^2}{t^2}.$$

Or, $\big(|X - \mu| \geqslant t\big) = \big((X - \mu)^2 \geqslant t^2\big)$, donc

$$P\big(|X - \mu) \geqslant t\big) \leqslant \frac{\sigma^2}{t^2}.$$

□

Remarque (Application) :
On considère une expérience de Bernoulli de paramètre $p \in]0,1[$. On répète n fois cette expérience à l'identique et on note Y_n le nombre moyen de succès.

On pose, pour $i \in [\![1,n]\!]$,

$$X_i = \begin{cases} 1 & \text{si la } i\text{-ème expérience est un succès} \\ 0 & \text{sinon.} \end{cases}$$

Les (X_i) sont mutuellement indépendants ; d'où

$$Y_n = \frac{1}{n}\sum_{i=1}^{n} X_i.$$

Et donc

$$E(Y_n) = \frac{1}{n}\sum_{i=1}^{n} E(X_i) = \frac{1}{n}np = p.$$

Comme les (X_i) sont deux à deux indépendantes,

$$V(Y_n) = \frac{1}{n^2}\sum_{i=1}^{n} V(X_i) = \frac{1}{n^2}npq = \frac{pq}{n} \text{ où } q = 1-p.$$

D'où, d'après l'inégalité de Bienaymé-чебышёв,

$$\forall \varepsilon > 0,\ P(|Y_n - p| \geqslant \varepsilon) \leqslant \frac{pq}{n\varepsilon^2} \xrightarrow[n\to+\infty]{} 0.$$

On en déduit que

$$\forall \varepsilon > 0,\ P(|Y_n - p| < \varepsilon) \geqslant \underbrace{1 - \frac{pq}{n\varepsilon^2}}_{\substack{\mathscr{s} \\ \text{“seuil”}}}.$$

— Par exemple, avec $\varepsilon = 10^{-2}$ et $\mathscr{s} = 95\,\%$, on a

$$\begin{aligned} \frac{95}{100} = \mathscr{s} = 1 - \frac{pq}{n \times 10^{-4}} &\iff \frac{5}{100} = \frac{pq}{n\,10^{-4}} \\ &\iff 20 = \frac{n\,10^{-4}}{pq} \\ &\iff n = 20\underbrace{pq}_{\leqslant \frac{1}{4}}10^4 \leqslant 5 \times 10^4. \end{aligned}$$

En répétant 50 000 fois l'expérience, on est sûr à 95% que la valeur observée de $Y_{50\,000}$ est dans l'intervalle $\left[p - 10^{-2}, p + 10^{-2}\right]$.

— Avec $n = 12$ et $\text{ɔ} = 95\,\%$, on a

$$\begin{aligned}\frac{95}{100} = \text{ɔ} = 1 - \frac{pq}{n\varepsilon^2} &\iff \frac{pq}{n\varepsilon^2} = \frac{5}{100}\\ &\iff \frac{\varepsilon^2 n}{pq} = 20\\ &\iff \varepsilon^2 = \frac{20}{n}pq \leqslant \frac{5}{12}.\end{aligned}$$

Donc, $\varepsilon = \sqrt{\dfrac{5}{12}} \simeq 0{,}65$.

— Avec $n = 12$ et $\varepsilon = 10^{-2}$,

$$\begin{aligned}P\big(|Y_{12} - p| < \varepsilon\big) &\geqslant 1 - \frac{pq}{12 \cdot 10^{-4}}\\ &\geqslant 1 - \frac{1}{48 \cdot 10^{-4}}\\ &\geqslant \underbrace{1 - \frac{1}{48} \times 10^4}_{<0}\end{aligned}$$

Théorème (loi faible des grands nombres — HORS-PROGRAMME) **:** Soit $(X_n)_{n\in\mathbb{N}}$ une suite de varialbe aléatoires indépedantes de même loi définies sur le même espace probabilisé (Ω, P). On note μ leur espérance commune.

$$\forall \varepsilon > 0,\ \lim_{n\to+\infty} P\Big(\big|\bar{X}_n - \mu\big| > \varepsilon\Big) = 0$$

où $\forall n,\ \bar{X}_n = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} X_i$.

Preuve :

$$\begin{aligned}\forall n \in \mathbb{N}^\star, E\big(\bar{X}_n\big) &= \frac{1}{n}\sum_{i=1}^{n} E(X_i) = \mu\\ V\big(\bar{X}_n\big) &= \frac{1}{n^2}\sum_{i=1}^{n} V(X_i) = \frac{n\sigma^2}{n^2} = \frac{\sigma^2}{n}\end{aligned}$$

où σ^2 est la variance commune aux X_i.

Soit $\varepsilon > 0$.

$$0 \leqslant P\Big(\big|\bar{X}_n - \mu\big| > \varepsilon\Big) \leqslant \frac{\sigma^2}{n\varepsilon^2} \xrightarrow[n\to+\infty]{} 0..$$

□

Proposition (lemme des coalitions) **:** Soient $X_1, \dots, X_n$ des variables aléatoires à valeurs réelles d'un même ensemble probabilisé mutuellement indépendantes. Soient $f : \mathbb{R}^p \to \mathbb{R}$ et $g : \mathbb{R}^{n-p} \to \mathbb{R}$. Alors, $f(X_{i_1}, \dots, X_{i_p})$ et $g(X_{j_1}, \dots, X_{j_{n-p}})$ sont indépendantes si

$$\begin{cases} \{i_1, \dots, i_p\} \cap \{j_1, \dots, j_{n-p}\} = \\ \forall k \neq \ell,\ i_k \neq i_\ell \text{ et } j_k \neq j_\ell. \end{cases}$$

Chapitre 32

Familles sommables

1 Motivation

La série $\sum \dfrac{(-1)^n}{n}$ est semi-convergente. On a $\displaystyle\sum_{n=1}^{+\infty} \frac{(-1)^n}{n} = -\ln 2$, d'où,

$$-1+\frac{1}{2}-\frac{1}{3}+\frac{1}{4}-\frac{1}{5}+\frac{1}{6}+\cdots = -\ln 2.$$

On change l'ordre :

$$\begin{aligned}
&\overbrace{-1+\frac{1}{2}+\frac{1}{4}}^{-\frac{1}{2}+\frac{1}{4}}-\overbrace{\frac{1}{3}+\frac{1}{6}+\frac{1}{8}}^{-\frac{1}{6}+\frac{1}{8}}-\overbrace{\frac{1}{5}+\frac{1}{10}+\frac{1}{12}}^{-\frac{1}{10}+\frac{1}{12}}+\cdots\\
&=\frac{1}{2}\left(-1+\frac{1}{2}-\frac{1}{3}+\frac{1}{4}-\frac{1}{5}+\frac{1}{6}+\cdots\right)\\
&=\frac{-\ln 2}{2}
\end{aligned}$$

> **Théorème** (réarrangement de Riemann) **:** Soit $\sum u_n$ une série semi-convergente réelle.
>
> $$\forall \ell \in \mathbb{R},\ \exists \sigma : \mathbb{N} \xrightarrow{\text{bij}} \mathbb{N},\ \sum_{n=1}^{+\infty} u_{\sigma(n)} = \ell.$$

2 Familles sommables positives

Dans ce paragraphe, toutes les familles considérées sont positives.

Définition : Soit $(u_i)_{i\in I} \in \left(\mathbb{R}^+\right)^I$.

Si $\left\{ \sum_{i\in J} u_i \;\middle|\; \begin{array}{c} J\subset I \\ J \text{ fini} \end{array} \right\}$ est majorée, alors on dit qu'elle est sommable et on définit la somme des $(u_i)_{i\in I}$ par

$$\sum_{i\in I} u_i = \sup_{\substack{J\subset I \\ J \text{ fini}}} \sum_{j\in J} u_j.$$

Sinon, la famille n'est pas sommable et on définit

$$\sum_{i\in I} u_i = +\infty.$$

EXEMPLE : 1. Toute famille finie positive est sommable : avec $I = [\![1, n]\!]$, on a

$$\sum_{i\in I} u_i = \sum_{i=1}^{n} u_i.$$

2. Soit $(u_n)_{n\in\mathbb{N}} \in \left(\mathbb{R}^+\right)^{\mathbb{N}}$.

CAS 1 $\sum u_n$ converge. Soit $J \subset I = \mathbb{N}$ finie et

$$\sum_{j\in J} u_j \leqslant \sum_{i=0}^{\max(J)} u_i \leqslant \sum_{i=0}^{+\infty} u_i = S.$$

Or,

$$\forall \varepsilon > 0\, \exists N \in \mathbb{N}\, \forall n \geqslant N,\ S - \varepsilon \leqslant \sum_{i=1}^{n} u_i$$

donc $S - \varepsilon$ ne majore pas $\left\{ \sum_{i\in J} u_i \;\middle|\; \begin{array}{c} J\subset I \\ J \text{ fini} \end{array} \right\}$. Ainsi,

$$S = \sup_{\substack{J\subset I \\ J \text{ finie}}} \sum_{j\in J} u_j = \sum_{i\in\mathbb{N}} u_i.$$

CAS 2 $\sum u_n$ diverge. Alors $\lim\limits_{N\to+\infty} \sum\limits_{i=0}^{N} u_i = +\infty$ et donc $\left\{ \sum_{i\in J} u_i \;\middle|\; \begin{array}{c} J\subset I \\ J \text{ fini} \end{array} \right\}$ n'est pas majorée et donc $(u_n)_{n\in\mathbb{N}}$ n'est pas sommable et

$$\sum_{n\in\mathbb{N}} u_n = +\infty.$$

Théorème : Soit $(u_i)_{i\in I} \in \left(\mathbb{R}^+\right)^I$ sommable et soit $\sigma : I \to I$ une bijection. Alors

$$\sum_{i\in I} u_{\sigma(I)} = \sum_{i\in I} u_i.$$

Preuve :

$$\left\{ \sum_{j\in J} u_{\sigma(j)} \;\middle|\; \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\} = \left\{ \sum_{k\in\sigma(J)} u_i \;\middle|\; \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$$
$$= \left\{ \sum_{k\in K} u_k \;\middle|\; \begin{array}{l} K \subset I \\ K \text{ fini} \end{array} \right\}$$

□

Corollaire (sommation par paquets) **:** Soit $(u_i)_{i\in I} \in \left(\mathbb{R}^+\right)^I$ et $(I_j)_{j\in J}$ une partition de I :

$$I = \bigcup_{j\in J} I_j.$$

$$(u_i)_{i\in I} \text{ est sommable} \iff \begin{cases} \forall j \in J,\ (u_i)_{i\in I_j} \text{ est sommable,} \\ \left(\sum_{i\in I_j} u_i\right)_{j\in J} \text{ est sommable.} \end{cases}.$$

Dans ce cas,

$$\sum_{i\in I} u_i = \sum_{j\in J}\sum_{i\in I_j} u_i.$$

□

Corollaire (Fubini positif) **:** Soit $(u_{i,j})_{\substack{i\in I \\ j\in J}} \in \left(\mathbb{R}^+\right)^{I\times J}$.

$$\sum_{i\in I}\sum_{j\in J} u_{i,j} = \sum_{j\in J}\sum_{i\in I} u_{i,j}.$$

Preuve : — On suppose $(u_{i,j})_{\substack{i\in I \\ j\in J}}$ sommable. On pose $I \times J = \bigcup_{i\in I} K_i$ où $K_i = \{i\} \times J = \{(i,j) \mid j \in J\}$.

Donc, $\forall i \in I$, $(u_{i,j})_{j\in J}$ est sommable, $\left(\sum_{j\in J} u_{i,j}\right)_{i\in I}$ est sommable et

$$\sum_{(i,j)\in I\times J} u_{i,j} = \sum_{i\in I}\sum_{j\in J} u_{i,j}.$$

On a aussi

$$I \times J = \bigcup_{j\in J} L_j \qquad \text{où } L_j = I \times \{j\}.$$

$\forall j \in J$, $(u_{i,j})_{i\in I}$ est sommable, $\left(\sum_{i\in I} u_{i,j}\right)_{j\in J}$ est sommable et

$$\sum_{(i,j)\in I\times J} u_{i,j} = \sum_{j\in J}\sum_{i\in I} u_{i,j}.$$

— On suppose $(u_i)_{\substack{i\in I\\ j\in J}}$ non sommable et donc

$$\sum_{i\in I}\sum_{j\in I} u_{i,j} = +\infty = \sum_{j\in J}\sum_{i\in I} u_{i,j}.$$

□

Corollaire : Soient $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ deux familles sommables de réels positifs.

$$\sum_{\substack{i\in I\\ j\in J}} a_i b_j = \left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right).$$

Preuve :
On pose, pour $i \in I$, pour $j \in J$, $u_{i,j} = a_i b_j$.

$$\begin{aligned}\sum_{\substack{i\in I\\ j\in J}} a_i b_j &= \sum_{(i,j)\in I\times J} u_{i,j}\\ &= \sum_{i\in I}\sum_{j\in J} u_{i,j}\\ &= \sum_{i\in I}\sum_{j\in J} a_i b_j\\ &= \sum_{i\in I} a_i \sum_{j\in J} b_j\end{aligned}$$

□

Dans la preuve précédente, on a utilisé la linéarité de la somme :

Proposition : Soient $(a_i)_{i\in I} \in \left(\mathbb{R}^+\right)^I$, $(b_i)_{i\in I} \in \left(\mathbb{R}^+\right)^I$ et $\lambda \in \mathbb{R}^+$.

1. $\displaystyle\sum_{i\in I}(a_i+b_i) = \sum_{i\in I} a_i + \sum_{i\in I} b_i$;
2. $\displaystyle\sum_{i\in I}(\lambda a_i) = \lambda \sum_{i\in I} a_i$.

Preuve Cas 1 On suppose (a_i) et (b_i) sommables. Soit $J \subset I$ finie.

$$\sum_{i\in J}(a_i+b_i) = \sum_{i\in J} a_i + \sum_{i\in J} b_i \leqslant \sum_{i\in I} a_i + \sum_{i\in I} b_i.$$

Donc, $S = \displaystyle\sum_{i\in I} a_i + \sum_{i\in I} b_i$ majore $\left\{ \displaystyle\sum_{i\in J}(a_i+b_i) \;\middle|\; \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$ et donc $(a_i+b_i)_{i\in I}$ est sommable.

Soit $\varepsilon > 0$. Il existe $J \subset I$ finie telle que

$$\sum_{j\in J} a_j \geqslant \sum_{i\in I} a_i - \frac{\varepsilon}{2}.$$

Également, il existe $J \subset I$ finie telle que

$$\sum_{i\in K} b_i \geqslant \sum_{i\in J} b_i - \frac{\varepsilon}{2}.$$

On pose $L = J \cup K$. $L \subset I$ et L est un ensemble fini.

$$\begin{aligned}\sum_{i\in L}(a_i+bi) &= \sum_{i\in L} a_i + \sum_{i\in L} b_i \\ &\geqslant \sum_{i\in J} a_i + \sum_{i\in K} b_i \\ &\geqslant \sum_{i\in I} a_i - \frac{\varepsilon}{2} + \sum_{i\in I} b_i - \frac{\varepsilon}{2} \\ &\geqslant S - \varepsilon.\end{aligned}$$

Donc,

$$S = \sup_{\substack{J\subset I \\ J \text{ finie}}} \sum_{i\in J}(a_i+b_i) = \sum_{i\in I}(a_i+b_i).$$

□

Proposition : Soient $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$ deux familles de réels positifs telles que

$$\forall i \in I,\ 0 \leqslant a_i \leqslant b_i.$$

Si $(b_i)_{i\in I}$ est sommable, alors $(a_i)_{i\in I}$ aussi, et, dans ce cas,

$$\sum_{i\in I} a_i \leqslant \sum_{i\in I} b_i.$$

Preuve :
Soit $J \subset I$ finie.

$$\sum_{i\in J} a_i \leqslant \sum_{i\in J} b_i \leqslant \sum_{i\in I} b_i$$

$$\text{donc } \sum_{i\in I} b_i \text{ majore } \left\{ \sum_{i\in J} a_i \;\middle|\; \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$$

donc (a_i) est sommable et

$$\sum_{i\in I} a_i \leqslant \sum_{i\in I} b_i.$$

□

3 Familles sommables réelles

Définition : Soit $(u_i)_{i\in I} \in \mathbb{R}^I$. On dit que $(u_i)_{i\in I}$ est sommable si $\left(|u_i|\right)_{i\in I}$ est sommable.

Exemple : 1. Toute famille finie de réels est sommable.
2. Avec $I = \mathbb{N}$ et $(u_n) \in \mathbb{R}^{\mathbb{N}}$,

$$\begin{aligned} (u_n)_{n\in\mathbb{N}} \text{ sommable} &\iff \sum |u_n| \text{ converge} \\ &\iff \sum u_n \text{ converge absolument.} \end{aligned}$$

Remarque :
Une famille sommable n'est pas une famille dont on peut calculer la somme mais la somme des valeurs absolues.

Proposition–Définition : Soit $(u_i)_{i\in I} \in \mathbb{R}^I$. On pose, pour tout $i \in I$,

$$u_i^+ = \begin{cases} u_i & \text{si } u_i \geqslant 0, \\ 0 & \text{sinon;} \end{cases}$$

$$u_i^- = \begin{cases} -u_i & \text{si } u_i \leqslant 0, \\ 0 & \text{sinon.} \end{cases}$$

Alors,

$$(u_i) \text{ sommable} \iff (u_i^+) \text{ et } (u_i^-) \text{ sont sommables.}$$

Dans ce cas, on définit

$$\sum_{i\in I} u_i = \sum_{i\in I} u_i^+ - \sum_{i\in I} u_i^-.$$

Preuve " $\Longrightarrow$ " On suppose (u_i) sommable. Par définition, $\big(|u_i|\big)_{i\in I}$ est sommable.

$$\forall i \in I,\ 0 \leqslant u_i^+ \leqslant |u_i|.$$

On en déduit que (u_i^+) est sommable. De même,

$$\forall i \in I,\ 0 \leqslant u_i^- \leqslant |u_i|$$

et donc (u_i^-) est sommable.

" $\Longleftarrow$ " On suppose (u_i^+) et (u_i^-) sommables.

$$\forall i \in I,\ |u_i| = u_i^+ + u_i^-.$$

Par linéarité, $\big(|u_i|\big)_{i\in I}$ est sommable et donc $(u_i)_{i\in I}$ est sommable.

□

Proposition : Soient $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$ deux familles sommables et $\lambda \in \mathbb{R}$. Alors, $(a_i + b_i)_{i\in I}$ est sommable, $(\lambda a_i)_{i\in I}$ aussi et

$$\sum_{i\in I}(a_i + b_i) = \sum_{i\in I} a_i + \sum_{i\in I} b_i,$$

$$\sum_{i\in I} \lambda a_i = \lambda \sum_{i\in I} a_i.$$

En d'autres termes, $\ell^1(I)$ est un sous-espace vectoriel de $\mathbb{R}^I$ et

$$\begin{aligned} S : \ell^1(I) &\longrightarrow \mathbb{R} \\ (u_i)_{i\in I} &\longmapsto \sum_{i\in I} u_i \end{aligned}$$

est linéaire où $\ell^1(I) = \{(u_i) \in \mathbb{R}^I \mid (u_i) \text{ sommable}\}$.

Preuve : — $\forall i \in I$, $|u_i + v_i| \leqslant |u_i| + |v_i|$. Or, par hypothèse, $\big(|u_i|\big)_{i\in i}$ et $\big(|v_i|\big)_{i\in i}$ sont sommables et positives donc $\big(|u_i|+|v_i|\big)_{i\in I}$ est sommable donc $\big(|u_i + v_i|\big)_{i\in I}$ est sommable et donc $(u_i + v_i)_{i\in I}$ est sommable.

Et,

$$\sum_{i\in I}(u_i + v_i) = \sum_{i\in I}(u_i + v_i)^+ - \sum_{i\in I}(u_i + v_i)^-.$$

Or,

$$\begin{aligned}
&\sum_{i\in I}(u_i + v_i) = \sum_{i\in I} u_i + \sum_{i\in I} v_i \\
\iff &\sum_{i\in I}(u_i + v_i)^+ - \sum_{i\in I}(u_i + v_i)^- = \sum_{i\in I} u_i^+ - \sum_{i\in I} u_i^- + \sum_{i\in I} v_i^+ - \sum_{i\in I} v_i^- \\
\iff &\sum_{i\in I}(u_i + v_i)^+ + \sum_{i\in I} u_i^- + \sum_{i\in I} v_i^- = \sum_{i\in I}(u_i + v_i)^- + \sum_{i\in I} u_i^+ + \sum_{i\in I} v_i^+ \\
\iff &\sum_{i\in I}\big((u_i + v_i)^+ + u_i^- + v_i^-\big) = \sum_{i\in I}\big((u_i + v_i)^- + u_i^+ + v_i^+\big).
\end{aligned}$$

On réalise une disjonction de cas : soit $i \in I$.

u_i	v_i	$u_i + v_i$	$(u_i + v_i)^+ + u_i^- + v_i^-$	$(u_i + v_i)^- + u_i^+ + v_i^+$
$+$	$+$	$+$	$u_i + v_i$	$u_i + v_i$
$+$	$-$	$+$	u_i	u_i
$+$	$-$	$-$	$-v_i$	$-v_i$
$-$	$+$	$+$	v_i	v_i
$-$	$+$	$-$	$-u_i$	$-u_i$
$-$	$-$	$-$	$-u_i - v_i$	$-u_i - v_i$

On remarque que, pour tout $i \in I$,

$$(u_i + v_i)^+ + u_i^- + v_i^- = (u_i + v_i)^- + u_i^+ + v_i^+.$$

— $\forall i \in I$, $|\lambda u_i| = |\lambda|\,|u_i|$, $\big(|u_i|\big)_{i\in I}$ est sommable, $|\lambda| \geqslant 0$ et donc $\big(|\lambda u_i|\big)_{i\in I}$ est sommable et donc $(\lambda u_i)_{i\in I}$ est sommable.

Cas 1 $\lambda \geqslant 0$:

$$\begin{aligned}\sum_{i\in I}\lambda u_i &= \sum_{i\in I}(\lambda u_i)^+ - \sum_{i\in I}(\lambda u_i)^- \\ &= \sum_{i\in I}\lambda u_i^+ - \sum_{i\in I}\lambda u_i^- \\ &= \lambda\left(\sum_{i\in I}u_i^+ - \sum_{i\in I}u_i^-\right) \\ &= \lambda\sum_{i\in I}u_i.\end{aligned}$$

Cas 2 $\lambda < 0$:

$$\begin{aligned}\sum_{i\in I}\lambda u_i &= \sum_{i\in I}(\lambda u_i)^+ - \sum_{i\in I}^{-} \\ &= \sum_{i\in I}\underbrace{(-\lambda)}_{\geqslant 0}u_i^- - \sum_{i\in I}\underbrace{(-\lambda)}_{\geqslant 0}u_i^+ \\ &= (-\lambda)\left(\sum_{i\in I}u_i^- - \sum_{i\in I}u_i^+\right).\end{aligned}$$

Or,

$$\lambda\sum_{i\in I}u_i = \lambda\left(\sum_{i\in I}u_i^+ - \sum_{i\in I}u_i^-\right) = (-\lambda)\left(\sum_{i\in I}u_i^- - \sum_{i\in I}u_i^+\right).$$

□

Proposition : Soit $(u_i)_{i\in I} \in \mathbb{R}^I$ sommable et $\sigma : I \to I$ une bijection. Alors $(u_{\sigma(i)})_{i\in I}$ est sommable et

$$\sum_{i\in I}u_{\sigma(i)} = \sum_{i\in I}u_i.$$

Preuve :

D'après le paragraphe 1, $\big(|u_{\sigma(i)}|\big)_{i\in I}$ est sommable.

$$\begin{aligned}\sum_{i\in I} u_{\sigma(i)} &= \sum_{i\in I} u^+_{\sigma(i)} - \sum_{i\in I} u^-_{\sigma(i)}\\ &= \sum_{i\in I} u_i^+ - \sum_{i\in I} u_i^-\\ &= \sum_{i\in I} u_i\end{aligned}$$

□

Corollaire (sommation par paquets) **:** Soit $(u_i)_{i\in I}\in\mathbb{R}^I$ et $(I_j)_{j\in J}$ une partition de I.

$$(u_i)_{i\in I} \text{ sommable} \implies \begin{cases}\forall j\in J,\ (u_i)_{i\in I_j} \text{ sommable},\\ \Big(\displaystyle\sum_{i\in I_j} u_i\Big)_{j\in J} \text{ sommable.}\end{cases}$$

Dans ce cas,

$$\sum_{i\in I} u_i = \sum_{j\in J}\sum_{i\in I_j} u_i.$$

Corollaire (Fubini) **:** Soit $(u_{i,j})_{\substack{i\in I\\ j\in J}}\in\mathbb{R}^{I\times J}$ sommable. Alors,

$$\sum_{i\in I}\sum_{j\in J} u_{i,j} = \sum_{j\in J}\sum_{i\in I} u_{i,j}.$$

Corollaire : Soient $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ deux familles sommables. Alors $(a_ib_j)_{\substack{i\in I\\ j\in J}}$ est sommable et

$$\sum_{i\in I}\sum_{j\in J} a_ib_j = \Big(\sum_{i\in I} a_i\Big)\Big(\sum_{j\in J} b_j\Big).$$

Preuve :
On a $I\times J = \bigcup\limits_{i\in I}^{\cdot}\big(\{i\}\times J\big)$.

Alors,

$$(a_ib_j)_{\substack{i\in I\\ j\in J}} \text{ sommable } \iff \begin{cases} \forall i\in I,\ (a_ib_j)_{j\in J} \text{ sommable} \\ \left(\sum_{j\in J} a_ib_j\right)_{i\in I} \text{ sommable} \end{cases}$$
$$\impliedby \left\{(b_j)_{j\in J} \text{ sommable}, (a_i)_{i\in I} \text{ sommable}.\right.$$

De plus,

$$\begin{aligned}\sum_{(i,j)\in I\times J} &= \sum_{i\in I}\sum_{j\in J}(a_ib_j)\\ &= \sum_{i\in I}\left(a_i\sum_{j\in J}b_j\right)\\ &= \left(\sum_{i\in I}a_i\right)\left(\sum_{j\in J}b_j\right).\end{aligned}$$

□

4 Familles sommables de nombres complexes

Définition : Soit $(u_i)_{i\in I}\in\mathbb{C}^I$. On dit qu'elle est sommable si $\left(|u_i|\right)_{i\in I}$ est sommable.

Proposition : Soit $(u_i)_{i\in I}\in\mathbb{C}^I$.

$(u_i)_{i\in I}$ sommable $\iff \left(\mathfrak{Re}(u_i)\right)_{i\in I}$ et $\left(\mathfrak{Im}(u_i)\right)_{i\in I}$ sont sommables.

Preuve " $\Longrightarrow$ " Pour tout $i\in I$, $|\mathfrak{Re}(u_i)|\leqslant|u_i|$ et $|\mathfrak{Im}(u_i)|\leqslant|u_i|$ donc $\left(\mathfrak{Re}(u_i)\right)_{i\in I}$ et $\left(\mathfrak{Im}(u_i)\right)_{i\in I}$ sont sommables.
" $\Longleftarrow$ " $\forall i\in I$, $|u_i|\leqslant|\mathfrak{Re}(u_i)|+|\mathfrak{Im}(u_i)|$ donc $\left(|u_i|\right)_{i\in I}$ est sommable.

□

Définition : Soit $(u_k)_{k\in I}\in\mathbb{C}^I$ sommable. On définit

$$\sum_{k\in I}u_k=\sum_{k\in I}\mathfrak{Re}(u_k)+i\sum_{k\in I}\mathfrak{Im}(u_k).$$

On a exactement les mêmes propriétés que pour des familles réelles. □

5 Produit de Cauchy de deux séries

RAPPEL :
Avec $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{\ell=0}^{q} b_\ell X^\ell$, on a

$$\begin{aligned} PQ &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell X^{k+\ell} \\ &= \sum_{m=0}^{p+q}\left(\sum_{k=0}^{\min(p,m)} a_k b_{m-k}\right) X^m. \end{aligned}$$

Définition : Soient $(u_n), (v_n) \in \mathbb{C}^{\mathbb{N}}$. Le produit de Cauchy des séries $\sum u_n$ et $\sum v_n$ est la série $\sum w_n$ où

$$\forall n \in \mathbb{N},\ w_n = \sum_{k=0}^{n} u_k v_{n-k}.$$

Théorème : Soient $(u_n), (v_n) \in \mathbb{C}^{\mathbb{N}}$. Si $\sum u_n$ et $\sum v_n$ convergent absolument, alors leur produit $\sum w_n$ converge absolument et

$$\sum_{n=0}^{+\infty} w_n = \left(\sum_{n=0}^{+\infty} u_n\right)\left(\sum_{n=0}^{+\infty} v_n\right).$$

Preuve :
On sait que (u_n) et (v_n) sont sommables. On pose

$$\forall n \in \mathbb{N},\ w_n = \sum_{k=0}^{n} u_k v_{n-k}.$$

$(u_n\, v_m)_{(n,m)\in\mathbb{N}^2}$ est donc sommable et

$$\begin{aligned}\left(\sum_{k=0}^{+\infty} u_n\right)\left(\sum_{k=0}^{+\infty} v_n\right) &= \sum_{(n,m)\in\mathbb{N}^2} u_n v_m \\ &= \sum_{n=0}^{+\infty}\sum_{a=n}^{+\infty} u_n v_{a-n} \\ &= \sum_{a=0}^{+\infty}\sum_{n=0}^{a} u_n v_{a-n} \\ &= \sum_{n=0}^{+\infty}\sum_{k=0}^{n} u_k v_{n-k} \\ &= \sum_{n=0}^{+\infty} w_n.\end{aligned}$$

□

Exemple :
On préfère définir l'exponentielle complexe par

$$\forall z\in\mathbb{C},\ e^z = \sum_{n=0}^{+\infty}\frac{z^n}{n!}$$

(au lieu de la définition du chapitre 4)

Par définition, $e^0 = \sum_{n=0}^{+\infty}\frac{0^n}{n!} = 1$.

Soient $(x,y)\in\mathbb{C}^2$. $\left(\frac{x^n}{n!}\right)_{n\in\mathbb{N}}$ et $\left(\frac{y^n}{n!}\right)_{n\in\mathbb{N}}$ sont sommables donc

$$\begin{aligned}e^x e^y &= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}\frac{x^k}{k!}\times\frac{y^{n-k}}{(n-k)!}\right) \\ &= \sum_{n=0}^{+\infty}\frac{1}{n!}\left(\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right) \\ &= \sum_{n=0}^{+\infty}\frac{1}{n!}(x+y)^n \\ &= e^{x+y}.\end{aligned}$$

Chapitre 33

Annexe

1 Algorithme de Metropolis-Hastings

On a un texte à déchiffrer. Il a été codé par substitution : on a remplacé une lettre par une autre (par exemple, "$A \to W$" et "$B \to U$"). L'algorithme de Metropolis-Hastings permet de déchiffrer ce type de message.

Cet algorithme fonctionne itérativement, et, pour chaque lettre, il tente de la permuter avec une autre et il conserve la meilleur.

Pour comparer deux permutations, il utilise des *bigrammes* : un couple de deux lettres consécutives (où l'on a supprimé les espaces). Avec un entrainement sur un autre texte de la même langue, l'algorithme determine la *plausibilité* de chaque bigramme. Au moment de comparer deux permutations, il compare les plausibilités des bigrammes obtenus à la suite des deux permutations.

On se place dans le groupe symétrique et la fonction qui donne la plausibilité associée à une permutation est une fonction du groupe symétrique dans les réels : $p : S_n \longrightarrow \mathbb{R}$ (en français, $n = 26$).

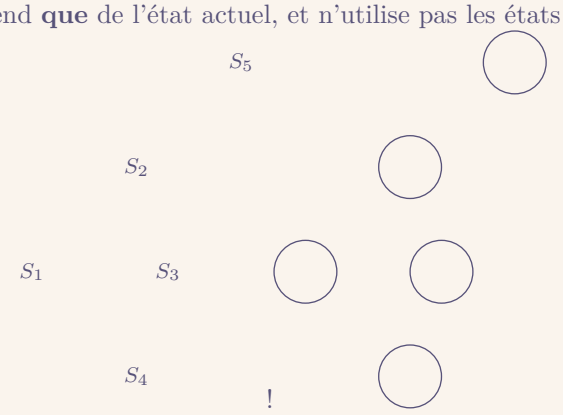
L'algorithme ressemble donc à :

> On choisit une permutation.
>
> Si, en l'appliquant au texte, la plausibilité augmente, on conserve cette permutation. Sinon, on ne la conserve pas.
>
> Et on répète.

Cet algorithme utilise donc une marche aléatoire, il ne teste pas *toutes* les permutations (avec $n = 26$, on a $\#S_n \geqslant 10^{61}$).

> **Définition** (Chaîne de Марков) **:** Le système est dans un état E et peut passer dans d'autres états avec des probabilités associées. Ce changement

d'état ne dépend **que** de l'état actuel, et n'utilise pas les états passés.



On associe à une chaîne de Марков une matrice de transition :

$$\begin{matrix} & i \\ & \downarrow \\ \left(\right. & P(S_j \mid S_i) & \left. \right) \leftarrow j \end{matrix}$$

On souhaite trouver $\max_{x \in S} f(x)$. Pour cela, on considère le changement $x \longrightarrow x'$ et on pose $\alpha = \frac{f(x')}{f(x)}$. On ne conserve x' avec une probabilité de α, sinon, on revient à x.

Mais, la probabilité de transition est proportionnelle à $f(x')$ et donc, pour que ce choix soit marqué, il faut que la fonction f ait une grande variance.

Cette méthode de choix ne peut être appliquée que si la chaîne de Марков est symétrique et connexe. La symétrie de la chaîne de Марков est assurée par le fait qu'une permutation est bijective, on peut donc appliquer sont inverse pour revenir à un état précédent.

2 Gradient automatique

On considère l'ensemble

$$D = \{a + b\varepsilon \mid (a, b) \in \mathbb{R}^2\}$$

où $\varepsilon \notin \mathbb{R}$ donc $\varepsilon \neq 0$ mais $\varepsilon^2 = 0$ (similaire à i dans les complexes).

Cet ensemble peut existe : avec $D = {}^{\mathbb{R}[X]}/_{\sim}$ où

$$\begin{aligned} P \sim Q &\iff P \equiv Q \ \left[X^2\right] \\ &\iff X^2 \mid P - Q. \end{aligned}$$

On définit donc $\varepsilon = \overline{X} \neq 0 : \varepsilon^2 = \overline{X^2} = \overline{0} = 0$. En appliquant la division euclidienne de P par X^2, on a $P = X^2Q + R$ et donc $\overline{P} = \overline{R} = \overline{a + bX} = a + b\varepsilon$.

C'est comme ça que l'on a définit $\mathbb{C}$: en effet, on a $\mathbb{C} = {}^{\mathbb{R}[X]}\!/_{(X^2+1)}$.

On essaie de multiplier deux *duaux* avec la distributivité du produit :

$$(1+2\varepsilon)(3+4\varepsilon) = 3+4\varepsilon+6\varepsilon+8\varepsilon^2 = 3+10\varepsilon.$$

On considère maintenant une fonction réelle

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 3x^2-5x^2+2x+6 \end{aligned}$$

et on pose F l'extension de f dans l'anneau des nombres duaux.

$$\begin{aligned} F(x+\varepsilon) &= 3(x+\varepsilon)^3 - 5(x+\varepsilon)^2 + 2(x+\varepsilon) + 6 \\ &= 3(x^3+3x^2\varepsilon+\cancel{3x\varepsilon^2}+\cancel{\varepsilon^2}) - 5(x^2+2x\varepsilon+\cancel{\varepsilon^2}) + 2x + 2\varepsilon + 6 \\ &= \underbrace{(3x^3-5x^2+2x+6)}_{f(x)} + \varepsilon \underbrace{(9x^2-10x+2)}_{f'(x)} \\ &= f(x) + \varepsilon f'(x) \end{aligned}$$

On généralise : soient f et g deux fonctions définies et dérivables sur $I \subset \mathbb{R}$ à valeurs réelles. On pose

$$\forall x \in I,\ \forall y \in \mathbb{R},\ \begin{cases} F(x+y\varepsilon) = f(x) + y\varepsilon f'(x), \\ G(x+y\varepsilon) = g(x) + y\varepsilon g'(x). \end{cases}$$

Soit $x \in I$ et $y \in \mathbb{R}$.

$$\begin{aligned} F(x+\varepsilon) + G(x+\varepsilon) &= \big(f(x)+g(x)\big) + \varepsilon\big(f'(x)+g'(x)\big); \\ F(x+\varepsilon) \times G(x+\varepsilon) &= \big(f(x)+\varepsilon f'(x)\big)\big(g(x)+\varepsilon g'(x)\big) \\ &= f(x)\,g(x) + \varepsilon\big(f'(x)\,g(x) + f(x)\,g'(x)\big) \\ &= (f\times g)(x) + \varepsilon(f\times g)'(x) \\ F\big(G(x+\varepsilon)\big) &= F\big(g(x)+\varepsilon g'(x)\big) \\ &= f\big(g(x)\big) + g'(x)\varepsilon f'\big(g(x)\big) \end{aligned}$$

Ces opérations sur les fonctions dans l'anneau dual sont compatibles avec les règles de dérivation habituelles.

Exemple :
On calcule

$$\frac{\mathrm{d}}{\mathrm{d}x}\big(e^x\cos x - \cos(\ln x)\big).$$

On pose

$$\begin{cases} F(x+y\varepsilon) = e^x + y\varepsilon e^x, \\ G(x+y\varepsilon) = \cos(x) - y\varepsilon \sin x, \\ H(x+y\varepsilon) = \ln x + \dfrac{y\varepsilon}{x}. \end{cases}$$

$$\begin{aligned} & F(x+\varepsilon)G(x+\varepsilon) - G(H(x+\varepsilon)) \\ &= (e^x + \varepsilon e^x)\big(\cos x - \varepsilon \sin x\big) - G\left(\ln x + \frac{\varepsilon}{x}\right) \\ &= e^x \cos x - \varepsilon \sin(x) e^x + \varepsilon \cos(x) e^x - \left(\cos(\ln x) - \frac{\varepsilon}{x} \times \sin(\ln x)\right) \\ &= e^x \cos(x) - \cos(\ln x) + \varepsilon \left(-\sin(x)e^x + \cos(x)e^x + \frac{1}{x}\sin(\ln x)\right) \end{aligned}$$

On peut calculer les dérivées de fonctions. À la main, ça prend autant de temps que d'utiliser les techniques habituelles. Cependant, informatiquement, le calcul de dérivée est simple ; en Python on peut le faire avec :

```
class Dual:
  def __init__(self, x, y):
    self.x = x
    self.y = y

  def __add__(self, other):
    return Dual(self.x + other.x, self.y + other.y)

  def __mul__(self, other):
    return Dual(self.x * other.x, self.x * other.y +
        ↪ self.y * other.x)

  def exp(self):
    return Dual(exp(self.x), self.y * exp(self.x))
```

Par example, pour chercher $\min_{x\in\mathbb{R}} \big(x^4 + 3x^3 - 5x^2 + 2\big)$, on pose $f(x_0) = f(x_0 + \varepsilon f'(x_0)$ et $x_{n+1} = x_n - hf'(x_n)$ où $h > 0$. La suite (x_n) tends vers $x^\star$ où $x^\star$ est un minimum local.

Ce calcul de dérivée est exact, on ne calcule pas $f'(x) \simeq \dfrac{f(x+h) - f(x)}{h}$.

Pour le calcul de gradient dans le cas de deux dimensions, on considère deux nombres vérifiant les propriétés de "ε" : ε_1 et ε_2.

Partie III

MP2I – Mathématiques – TDs

Chapitre 11

TD 11

Exercice 3

a.

$$\begin{aligned}\forall n \in \mathbb{N}, u_n &= \sqrt{n\left(1+\frac{1}{n}\right)} - \sqrt{n} \\ &= \sqrt{n}\left(1 - \frac{1}{2n} + o\left(\frac{1}{n}\right) - 1\right) \\ &\sim -\frac{1}{2\sqrt{n}} \xrightarrow[n\to+\infty]{} 0\end{aligned}$$

b. $\forall n \in \mathbb{N}_\star$

$n - (-1)^n = n\left(1 - \dfrac{(-1)^n}{n}\right) \sim n$

car $\left|\dfrac{(-1)^n}{n}\right| = \dfrac{1}{n} \xrightarrow[n\to+\infty]{} 0$

De même, $n + (-1)^n \sim n$ donc $u_n \sim \dfrac{n}{n} = 1 \xrightarrow[n\to+\infty]{} 1$

c. $\forall n \in \mathbb{N}_\star$

$$\begin{aligned}u_n &= (2 + (-1)^n)^{\frac{1}{n}} \\ &= e^{\frac{1}{n}\ln(2+(-1)^n)} \\ &= e^{\frac{1}{n}+O(1)} \xrightarrow[n\to+\infty]{} 1 \\ &\text{car } \frac{1}{n}O(1) \xrightarrow[n\to+\infty]{} 0\end{aligned}$$

e. $\forall k \in \mathbb{N}$,

$$kx - 1 < \lfloor kx \rfloor \leqslant kx$$

Donc $\forall n \in \mathbb{N}_\star$,

$$\frac{1}{n^2}\sum_{k=1}^{n}(kx-1) < u_n \leqslant \frac{1}{n^2}\sum_{k=1}^{n} kx$$

Donc $\forall n \in \mathbb{N}_\star$,

$$\underbrace{\frac{1}{n^2}\left(\frac{xn(n+1)}{2} - n\right)}_{\sim \frac{x}{2}} \leqslant u_n \leqslant \underbrace{\frac{x}{n^2} \times \frac{n(n+1)}{2}}_{\sim \frac{x}{2}}$$

Donc, $u_n \xrightarrow[n\to+\infty]{} \frac{x}{2}$

g. $\forall n \in \mathbb{N}_\star$

$$\sum_{k=1}^{2n+1} \frac{1}{n+1} \leqslant \sum_{k=1}^{2n+1} \frac{1}{\sqrt{n^2+k}} \leqslant \sum_{k=1}^{2n+1} \frac{1}{n}$$

donc, $\forall n \in \mathbb{N}_\star$,

$$\underbrace{\frac{2n+1}{n+1}}_{\xrightarrow[n\to+\infty]{} 2} \leqslant u_n \leqslant \underbrace{\frac{2n+1}{n}}_{\xrightarrow[n\to+\infty]{} 2}$$

donc $u_n \xrightarrow[n\to+\infty]{} 2$

l. $\forall n \in \mathbb{N}_\star, u_n = \dfrac{n!}{n^n}$

$$\begin{aligned}
\forall n \geqslant 2, 0 \leqslant u_n &= \frac{1 \times 2 \times 3 \times \ldots \times n}{n \times n \times n \times \ldots \times n} \\
&= \frac{1}{n} \times \frac{2}{n} \times \ldots \times \frac{n}{n} \\
&= \frac{1}{n} \prod_{k=2}^{n} \frac{k}{n} \leqslant \frac{1}{n} \xrightarrow[n\to+\infty]{} 0
\end{aligned}$$

Exercice 6

5)

$$\forall n \in \mathbb{N}_\star u_n = e^{n \ln\left(\frac{2^{\frac{1}{n}}+3^{\frac{1}{n}}+4^{\frac{1}{n}}}{3}\right)}$$

$$\begin{aligned}
\ln\left(\frac{2^{\frac{1}{n}}+3^{\frac{1}{n}}+4^{\frac{1}{n}}}{3}\right) &= \ln\left(\frac{1}{3}\left(3 + \frac{1}{n}(\ln 2 + \ln 3 + \ln 4) + o\left(\frac{1}{n}\right)\right)\right) \\
&= \ln\left(1 + \frac{1}{3n}\ln 24 + o\left(\frac{1}{n}\right)\right) \\
&\sim \frac{\ln 24}{3n}
\end{aligned}$$

Donc, $\ln\left(\dfrac{2^{\frac{1}{n}}+3^{\frac{1}{n}}+4^{\frac{1}{n}}}{3}\right) \sim \dfrac{\ln 24}{3} \to \dfrac{\ln 24}{3}$

$u_n \xrightarrow[n\to+\infty]{} e^{\frac{1}{3}\ln 24} = \sqrt[3]{24}$

6) $\forall n \in \mathbb{N}_\star$,

$$u_n = e^{n^2 \ln\left(\frac{\text{Arctan}(n+1)}{\text{Arctan}(n)}\right)}$$

$$\frac{\text{Arctan}(n+1)}{\text{Arctan}(n)} = \frac{\frac{\pi}{2} - \text{Arctan}\left(\frac{1}{n+1}\right)}{\frac{\pi}{2} - \text{Arctan}\left(\frac{1}{n}\right)}$$

$$\frac{\pi}{2} - \text{Arctan}\left(\frac{1}{n}\right) = \frac{\pi}{2} - \frac{1}{n} + o\left(\frac{1}{n}\right)$$

$$\begin{aligned}\frac{1}{\frac{\pi}{2} - \text{Arctan}\left(\frac{1}{n}\right)} &= \frac{2}{\pi} \times \frac{1}{1 - \frac{2}{\pi n} + o\left(\frac{1}{n}\right)} \\ &= \frac{2}{\pi}\left(1 + \frac{2}{\pi n} + o\left(\frac{1}{n^2}\right) + \frac{4}{\pi^2 n^2}\right)\end{aligned}$$

$$\begin{aligned}\frac{\pi}{2} - \text{Arctan}\left(\frac{1}{n+1}\right) &= \frac{\pi}{2} - \frac{1}{n+1} + o\left(\frac{1}{(n+1)^2}\right) \\ &= \frac{\pi}{2} - \frac{1}{n} + o\left(\frac{1}{n^2}\right) + \frac{1}{n^2}\end{aligned}$$

$$\begin{aligned}\frac{\text{Arctan}(n+1)}{\text{Arctan}(n)} &= \left(\frac{\pi}{2} - \frac{1}{n} + o\left(\frac{1}{n^2}\right) + \frac{1}{n^2}\right) \times \left(1 + \frac{2}{\pi n} + \frac{4}{\pi^2 n^2} + o\left(\frac{1}{n^2}\right)\right) \\ &= 1 + \frac{2}{\pi n} - \frac{2}{\pi n} + \frac{4}{\pi^2 n^2} - \frac{4}{\pi^2 n^2} + \frac{2}{\pi n^2} + o\left(\frac{1}{n^2}\right) \\ &= 1 + \frac{2}{\pi n^2} + o\left(\frac{1}{n^2}\right)\end{aligned}$$

$$\ln\left(\frac{\text{Arctan}(n+1)}{\text{Arctan}(n)}\right) \sim \frac{2}{\pi n^2}$$

$$n^2 \ln\left(\frac{\text{Arctan}(n+1)}{\text{Arctan}(n)}\right) \sim \frac{2}{\pi}$$

Donc, $u_n \to e^{\frac{2}{\pi}}$

Exercice 7

$$\forall n \in \mathbb{N}, a^n - 1 < \lfloor a^n \rfloor \leqslant a^n$$

Cas 1 : $a > 1$ Alors, $a^n - 1 > 0$ et donc,

$$(a^n-1)^{\frac{1}{n}} < u_n \leqslant a$$

$$\begin{aligned}(a^n-1)^{\frac{1}{n}} &= e^{\frac{1}{n}\ln(a^n-1)}\\ &= e^{\frac{1}{n}\ln\left(a^n\left(1-\frac{1}{a^n}\right)\right)}\\ &= \ln(a)+\frac{1}{n}\ln\left(1-\frac{1}{a^n}\right)\\ &\xrightarrow[n\to+\infty]{} e^{\ln a} = a\end{aligned}$$

Cas 2 : $a = 1$ $\forall n \in \mathbb{N}_\star, u_n = 1 \xrightarrow[n\to+\infty]{} 1 = a$

Cas 3 : $0 < a < 1$ donc

$$\forall n \in \mathbb{N}_\star, a^n \in]0,1[$$

donc

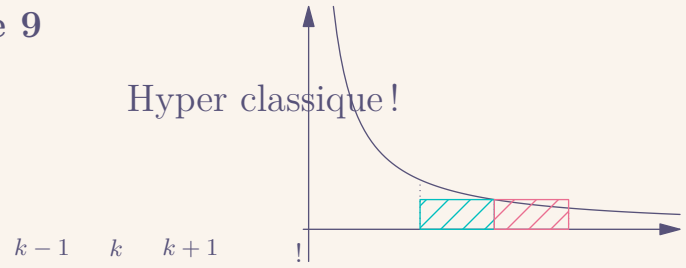
$$\forall n \in \mathbb{N}_\star \lfloor a^n \rfloor = 0$$

donc u_n n'existe pas (car $\forall n \in \mathbb{N}_\star, u_n = e^{\frac{1}{n}\ln(\lfloor a^n \rfloor)}$ et $\ln(0)$ n'existe pas)

Exercice 9

Hyper classique !

1. $f : x \mapsto \frac{1}{x}$



$$\forall k > 2, \int_k^{k+1} \frac{1}{x}dx \leqslant \frac{1}{k} \leqslant \int_{k-1}^{k} \frac{1}{x}dx$$

Or,

$$\ln(k+1) - \ln(k) \leqslant \frac{1}{k} \leqslant \ln(k) - \ln(k-1)$$

donc

$$\forall k \geqslant 2, \ln\left(\frac{k-1}{k}\right) \leqslant \frac{1}{k}$$

et

$$\forall k \geqslant 1, \frac{1}{k+1} \leqslant \ln\left(\frac{k+1}{k}\right)$$

2. Soit $n \in \mathbb{N}_\star$

$$\begin{aligned}u_{n+1} - u_n &= \sum_{k=1}^{n+1}\frac{1}{k} - \ln(n+1) - \sum_{k=1}^{n}\frac{1}{k} + \ln(n)\\ &= \frac{1}{n+1} - \ln\left(\frac{n+1}{n}\right) \leqslant 0\end{aligned}$$

$$\begin{aligned} v_{n+1} - v_n &= \sum_{k=1}^{n+1} \frac{1}{k} - \ln(n+2) + \sum_{k=1}^{n} \frac{1}{k} + \ln(n+1) \\ &= \frac{1}{n+1} - \ln\left(\frac{n+2}{n+1}\right) \end{aligned}$$

$$u_n - v_n = -\ln(n+1) + \ln(n) = \ln\left(\frac{n}{n+1}\right) \xrightarrow[n\to+\infty]{} 0$$

3. (u_n) converge, on note γ sa limite :

$$u_n = \gamma + o(1)$$

donc

$$\sum_{k=1}^{n} \frac{1}{k} - \ln(n) = \gamma + o(1)$$

donc

$$\boxed{\sum_{k=1}^{n} \frac{1}{k} = \ln(n) + \gamma + o(1)}$$

4. $S_n \sim \ln(n) \xrightarrow[n\to+\infty]{} +\infty$
5.

$$\begin{aligned} \sum_{k=n}^{2n} \frac{1}{k} &= \sum_{k=1}^{2n} \frac{1}{k} - \sum_{k=1}^{n-1} \frac{1}{k} \\ &= \ln(2n) + \gamma + o(1) - \ln(n-1) - \gamma + o(1) \\ &= \ln\left(\frac{2n}{n-1} + o(1)\right) \\ &\xrightarrow[n\to+\infty]{} \ln 2 \end{aligned}$$

Exercice 10

1. On sait que

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, \ell - \varepsilon \leqslant \frac{u_{n+1}}{u_n} \leqslant \ell + \varepsilon$$

.1 Méthode 1

En particulier, avec $\varepsilon = \dfrac{1-\ell}{2} > 0$.
Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \frac{u_{n+1}}{u_n} \leqslant \ell - \varepsilon = \frac{1+\ell}{2} < 1$$

$$\forall n \in \mathbb{N}, u_{n+1} \leqslant$$

La suite $(u_n)_{n\geqslant N}$ est décroissante minorée par 0 donc converge.
On pose $M = \lim\limits_{n\to+\infty} u_n$. Alors, $u_{n+1} \xrightarrow[n\to+\infty]{} L$
Si $L \neq 0$ alors $\dfrac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} \dfrac{L}{L} = 1 \neq \ell$: une contradiction
Donc $L = 0$

.2 Méthode 2

On pose $\varepsilon = \dfrac{1-\ell}{2} > 0$. Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \frac{u_{n+1}}{u_n} \leqslant \ell + \varepsilon = \frac{1+\varepsilon}{2}$$

Donc

$$\forall n \geqslant N, \prod_{k=N}^{n} \frac{u_{k+1}}{u_k} \leqslant \prod_{k=N}^{n} \frac{1+\ell}{2}$$

donc

$$\forall n \geqslant N, \frac{u_{n+1}}{u_n} \leqslant \left(\frac{1+\ell}{2}\right)^{n-N+1}$$

et donc

$$\forall n \geqslant N, u_{n+1} \leqslant \left(\frac{1+\ell}{2}\right)^{n-N+1} u_n$$

$\dfrac{1+\ell}{2} \in]0,1[$ donc $\left(\dfrac{1+\ell}{2}\right)^{n-N+1} \xrightarrow[n\to+\infty]{} 0$.
Par encadrement, $u_n \xrightarrow[n\to+\infty]{} 0$

2.

3. $\forall n \in \mathbb{N}, u_n = n$, $\dfrac{n+1}{n} \xrightarrow[n\to+\infty]{} 1$ mais $u_n \to +\infty$.
$\forall n \in \mathbb{N}, u_n = \dfrac{1}{n}$, $\dfrac{\frac{1}{n+1}}{\frac{1}{n}} = \dfrac{n}{n+1} \to 1$ mais $u_n \to 0$

Exercice 11

1. Soit $\varepsilon > 0$ (quelconque fixé). On cherche $N \in \mathbb{N}_\star$ tel que

$$\forall n \geqslant N, \left|\frac{1}{n}\sum_{i=1}^{n} u_i\right| \leqslant \varepsilon$$

Soit $\varepsilon' = \dfrac{\varepsilon}{2} > 0$ Il existe $N' \in \mathbb{N}_\star$ tel que

$$\forall n \geqslant N', |u_n| \leqslant \varepsilon'$$

La suite $\left(\dfrac{1}{n}\sum_{i=1}^{N'-1} |u_i|\right)$ converge vers 0.

Il existe $N'' \in \mathbb{N}$ tel que

$$\forall n \geqslant N'', \frac{1}{n}\sum_{i=1}^{N'-1}|u_i| \leqslant \frac{\varepsilon}{2}$$

On pose $N = \max(N', N'') \in \mathbb{N}$

$$\begin{aligned}\forall n \geqslant N, \left|\frac{1}{n}\sum_{i=1}^{n} u_i\right| &\leqslant \frac{1}{n}\sum_{i=1}^{n}|u_i| = \frac{1}{n}\left(\sum_{i=1}^{N-1}|u_i| + \sum_{i=1}^{n}|u_i|\right)\\ &\leqslant \frac{1}{n}\sum_{i=1}^{N'-1}|u_i| + \frac{n-N'+1}{n}\varepsilon'\\ &\leqslant \varepsilon' + \frac{1}{n}\sum_{i=1}^{N'-1}|u_i|\\ &\leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon\end{aligned}$$

2. On pose

$$\forall n \in \mathbb{N}, w_n = u_n - \ell \xrightarrow[n\to+\infty]{} 0$$

D'après la 1. ,

$$\frac{1}{n}\sum_{i=1}^{n} w_i \xrightarrow[n\to+\infty]{} 0$$

Or,

$$\begin{aligned}\forall n \in \mathbb{N}_\star, \frac{1}{n}\sum_{i=1}^{n} w_i &= \frac{1}{n}\sum_{i=1}^{n}(u_i - \ell)\\ &= \frac{1}{n}\sum_{i=1}^{n} u_i - \frac{1}{n}\sum_{i=1}^{n}\ell\\ &= \frac{1}{n}\sum_{i=1}^{n} u_i - \ell\end{aligned}$$

Donc $\frac{1}{n}\sum_{i=1}^{n} u_i = \ell + \frac{1}{n}\sum_{i=1}^{n} w_i \xrightarrow[n\to+\infty]{} \ell$

3. La réciproque est fausse : contre exemple

$$\forall n \in \mathbb{N}_\star, u_n = (-1)^n$$

$$\forall n \in \mathbb{N}_\star, \left|\frac{1}{n}\sum_{i=1}^{n} u_i\right| = \frac{1}{n}\left|\sum_{i=1}^{n}(-1)^i\right| \leqslant \frac{1}{n} \xrightarrow[n\to+\infty]{} 0$$

donc $\frac{1}{n}\sum_{i=1}^{n} u_i \xrightarrow[n\to+\infty]{} 0$

Exercice 12

$$\forall n \in \mathbb{N}_\star, \forall k \in \mathbb{N}_\star, 0 \leqslant u_n \leqslant \frac{1}{k} + \frac{k}{n}$$

Soit $\varepsilon > 0$. Il existe $k \in \mathbb{N}_\star$ tel que $\frac{1}{k} \leqslant \frac{\varepsilon}{2}$ (par exemple $k = \left\lfloor \frac{2}{\varepsilon} \right\rfloor + 1$)
La suite $\left(\frac{k}{n}\right)_{n\in\mathbb{N}_\star}$ tends vers 0. Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \frac{k}{n} \leqslant \frac{\varepsilon}{2}$$

Donc,

$$\forall n \geqslant N, 0 \leqslant u_n \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

Donc $u_n \xrightarrow[n\to+\infty]{} 0$

Exercice 3

On pose

$$\begin{cases} \ell_1 = \lim u_{2n} \\ \ell_2 = \lim u_{2n+1} \\ \ell_3 = \lim u_{3n} \end{cases}$$

$(u_{6n})_{n\in\mathbb{N}}$ est une sous-suite de (u_{2n}) et de (u_{3n}) donc

$$u_{6n} \xrightarrow[n\to+\infty]{} \ell_1$$
$$u_{6n} \xrightarrow[n\to+\infty]{} \ell_3$$

Par unicité de la limite, $\ell_1 = \ell_3$.
$(u_{6n+3})_{n\in\mathbb{N}}$ est une sous suite de (u_{2n+1}) et de (u_{3n}) donc $\ell_2 = \ell_3$

D'où $\ell_1 = \ell_2$, (u_n) converge.

Exercice 14

Méthode 1

Soit $n \in \mathbb{N}_\star$

$$\begin{aligned}
u_n &= \sqrt{n^2+3n+7} - \sqrt{n^2+an+b} \\
&= n\sqrt{1+\frac{3}{n}+\frac{7}{n^2}} - n\sqrt{1+\frac{a}{n}+\frac{b}{n^2}} \\
&= n\left(1+\frac{1}{2}\left(\frac{3}{n}+\frac{7}{n^2}\right)-\frac{1}{8}\times\frac{9}{n^2}+o\left(\frac{1}{n^2}\right)\right) \\
&- n\left(1+\frac{1}{2}\left(\frac{a}{n}+\frac{b}{n^2}\right)-\frac{1}{8}\times\frac{a^2}{n^2}+o\left(\frac{1}{n^2}\right)\right) \\
&= \frac{3-a}{2}+\left(\frac{7}{2}-\frac{9}{8}-\frac{b}{2}+\frac{a^2}{8}\right)\times\frac{1}{n}+o\left(\frac{1}{n}\right) \\
&\xrightarrow[n\to+\infty]{} \frac{3-a}{2}
\end{aligned}$$

Méthode 2

$$\begin{aligned}
u_n &= \frac{(n^2+3n+7)-(n^2+an+b)}{\sqrt{n^2+3n+7}+\sqrt{n^2+an+b}} \\
&\sim \begin{cases} \dfrac{(3-a)n}{2n} & \text{si } a \neq 3 \to \dfrac{3-a}{2} \\ \dfrac{7-b}{2n} & \text{si } a = 3 \to 0 = \dfrac{3-a}{2} \end{cases}
\end{aligned}$$

$\sqrt{n^2+3n+7} = n + o(n)$ car $\dfrac{\sqrt{n^2+3n+7}}{n} = \sqrt{1+\dfrac{3}{n}+\dfrac{7}{n^2}} \to 1$
pour la même raison, $\sqrt{n^2+an+b} = n + o(n)$

Donc, $\sqrt{n^2+3n+7}+\sqrt{n^2+an+b} = 2n + o(n) \sim 2n$

Exercice 19

1. Soit $\varepsilon > 0$. On sait qu'il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, |u_n - \ell| \leqslant \frac{\varepsilon}{2}$$

Soient $p \geqslant N$ et $q \geqslant N$.

$$\begin{aligned}
|u_p - u_q| &= |u_p - \ell + \ell - u_q| \\
&\leqslant |u_p - \ell| + |u_q - \ell| \\
&\leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon
\end{aligned}$$

2. Soit u une suite de Cauchy.
On sait qu'il existe $N \in \mathbb{N}$ tel que

$$\forall p > N, \forall q > N, |u_p - u_q| \leqslant 1$$

En particulier,

$$\forall n > N, |u_n - u_{N+1}| \leqslant 1$$

donc

$$\forall n > N, u_{N+1} - 1 \leqslant u_n \leqslant 1 + u_{N+1}$$

donc $(u_n)_{n>N}$ est bornée. Il existe $M_1 \in \mathbb{R}$ tel que

$$\forall n > N, |u_n| \leqslant M_1$$

La famille $(u_n)_{n\leqslant N}$ est finie. On pose

$$M_2 = \max_{n\in[\![0,N]\!]} |u_n|$$

On pose $M = \max(M_1, M_2)$.

$$\forall n \in \mathbb{N}, |u_n| \leqslant M$$

Donc (u_n) est bornée.

3. Comme a est bornée, (b_n) est bien définie.
   (a) Soit $n \in \mathbb{N}$.

$$\begin{cases} b_{n+1} = \sup\{a_p \mid p \geqslant n+1\} \\ b_n = \sup\{a_p \mid p \geqslant n\} \end{cases}$$

$$\forall p \geqslant n+1, a_p \leqslant b_n (\text{car } p \geqslant n)$$

Donc, b_n majore $\{a_p \mid p \geqslant n+1\}$ donc $b_{n+1} \leqslant b_n$
La suite (b_n) est décroissante.
Comme (a_n) est bornée, il existe $m \in \mathbb{R}$ tel que

$$\forall n \in \mathbb{N}, m \leqslant a_n$$

En particulier,

$$\forall p \geqslant n, b_n \leqslant a_p \geqslant m$$

Ainsi, (b_n) est minorée.
Donc, (b_n) converge.

   (b) Comme (b_n) converge vers a, il existe donc $N_1 \in \mathbb{N}$ tel que

$$\forall n \geqslant N_1, |b_n - a| \leqslant \varepsilon$$

et donc

$$\forall n \geqslant N_1, b_n \leqslant a + \varepsilon$$

Comme (a_n) est de Cauchy, il existe $N_2 \in \mathbb{N}$ tel que

$$\forall p > N_2, \forall n > N_2, |a_p - a_n| \leqslant \frac{\varepsilon}{2}$$

et donc

$$\forall p > N_1, \forall n > N_2, a_p \leqslant a_n + \frac{\varepsilon}{2}$$

On pose $N = \max(N_1, N_2) + 1$.
Comme $N \geqslant N_1$, on a $\boxed{b_n \leqslant a + \varepsilon}$
De plus,

$$\forall n \geqslant N, n > N_2$$

et donc $\boxed{\forall n \geqslant N, \forall p \geqslant N, a_p \leqslant a_n + \frac{\varepsilon}{2}}$

(c) On sait déjà que $b_N \leqslant a+\varepsilon$
Soit $n \geqslant N$
— $b_n = \sup\{a_p \mid p \geqslant N\} \geqslant a_n$
— $\forall p \geqslant N, a_p \leqslant a_n + \dfrac{\varepsilon}{2}$
donc $a_n + \dfrac{\varepsilon}{2}$ majore $\{a_p \mid p \geqslant N\}$.
donc $a_n + \dfrac{\varepsilon}{2} \geqslant b_N$

Enfin, (b_n) est décroissante de limite a donc $b_N \geqslant a$ donc $b_N - \dfrac{\varepsilon}{2} \geqslant a - \dfrac{\varepsilon}{2} > a - \varepsilon$.
En particulier

$$\forall n \geqslant N, a-\varepsilon \leqslant a_n \leqslant a+\varepsilon$$

Donc (a_n) converge vers a par définition de la limite

Exercice 21

1. $\{\lim u_n\}$
2. $\forall n \in \mathbb{N}, u_n = \begin{cases} 1 & \text{si } n \text{ pair} \\ n & \text{si } n \text{ impair} \end{cases}$

(u_n) diverge car $u_{2n+1} \xrightarrow[n\to+\infty]{} +\infty$
1 est la valeur d'adhérence de (u_n) car $u_{2n} \xrightarrow[n\to+\infty]{} 1$

Soit $\ell \neq 1$ un autre valeur d'adhérence.
Soit $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$
Comme $\ell \neq 1$, il existe $\varepsilon > 0$ tel que

$$1 \notin [\ell-\varepsilon, \ell+\varepsilon]$$

$$\exists N \in \mathbb{N}, \forall n \geqslant N, u_{\varphi(n)} \in [\ell-\varepsilon, \ell+\varepsilon]$$

Donc

$$\forall n \geqslant N, \varphi(n) \text{ impair}$$

Donc,

$$\forall n \geqslant N, u_{\varphi(n)} = \varphi(n) \geqslant n \xrightarrow[n\to+\infty]{} +\infty$$

Donc $u_{\varphi(n)} \xrightarrow[n\to+\infty]{} \ell$

3. Soit u bornée divergente. D'après le théorème de Bolzano Weierstrass, u a au moins une valeur d'adhérence ℓ.
u diverge donc $u_n \xrightarrow[n\to+\infty]{\not\longrightarrow} \ell$ donc

$$\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \geqslant N, |u_n - \ell| > \varepsilon$$

Ainsi,

$$\begin{aligned}(N=1):&\exists n_1 \geqslant 1, |u_{n_1}-\ell|>\varepsilon\\(N=n_1+1):&\exists n_2 \geqslant n_1+1, |u_{n_2}-\ell|>\varepsilon\\(N=n_2+1):&\exists n_3 \geqslant n_2+1, |u_{n_3}-\ell|>\varepsilon\end{aligned}$$

On construit de cette façon $(n_k)_k$ strictement croissante telle que

$$\forall k, |u_{n_k}-\ell|>\varepsilon$$

(u_{n_k}) est une sous suite de u donc bornée.
D'après le théorème de Bolzano Weierstrass, $(u_{n_k})_k$ a une sous suite $\left(u_{n_{\varphi(k)}}\right)_k$ convergente vers ℓ' ($\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante).
Or, $\forall k, \left|u_{n_{\varphi(k)}}-\ell\right|>\varepsilon$
Donc, $u_{n_{\varphi(k)}} \xrightarrow[k\to+\infty]{} \ell$. Donc, $\ell' \neq \ell$.
Or, $\left(u_{n_{\varphi(k)}}\right)$ est une sous suite de (u_n) donc ℓ' est une valeur d'adhérence de u.

Exercice 23

4.

$$\begin{cases}u_0 \in \mathbb{R}\\ \forall n \in \mathbb{N}, u_{n+1}=u_n^2+1\end{cases}$$

On pose

$$\begin{aligned}f : \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longmapsto x^2+1\end{aligned}$$

et

$$\begin{aligned}g : \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longmapsto x^2+1-x\end{aligned}$$

x	$-\infty$		0		$+\infty$
f	$+\infty$	$\searrow$	1	$\nearrow$	$+\infty$
$g(x)$		$+$			

x	$-\infty$	$\frac{1}{2}$	$+\infty$
g	$\searrow$	$\frac{3}{4}$	$\nearrow$

$[0,+\infty[$ est stable par f,

$$u_1 = f(u_0) \geqslant 1$$

donc $u_1 \in [0,+\infty[$

!

Donc, $\forall n \geqslant 1, u_n \in [0,+\infty[$.
De plus,

$$\forall n \geqslant 1, u_{n+1} - u_n = g(u_n) > 0$$

Donc, (u_n) croissante donc elle a une limite finie ou $+\infty$.

On suppose que $u_n \xrightarrow[n\to+\infty]{} \ell \in \mathbb{R}$.
Comme f est continue, $f(\ell) = \ell$. Alors, $g(\ell) = 0$: une contradiction

8.

$$u_0 \in [-2,2] \forall n \in \mathbb{N}, u_{n+1} = \sqrt{2-u_n}$$

Soit $f : x \mapsto \sqrt{2-x}$

x	-2		1		2
f	2	$\searrow$	1	$\searrow$	0
$g(x)$		$+$	0	$-$	

On pose $g : x \mapsto f(x) - x$

x	-2		α		2
g	4	$\searrow$	0	$\searrow$	-2

$$\begin{aligned} g(\alpha) = 0 &\iff \alpha = \sqrt{2-\alpha} \\ &\iff \begin{cases} \alpha^2 = 2 - \alpha \\ \alpha \geqslant 0 \end{cases} \\ &\iff \alpha = 1 \end{aligned}$$

On pose

$$\forall n \in \mathbb{N}, \begin{cases} v_n = u_{2n} \\ w_n = u_{2n+1} \end{cases}$$

$$\forall n \in \mathbb{N}, \begin{cases} v_{n+1} = u_{2n+2} = f(f(u_{2n})) = f \circ f(v_n) \\ w_{n+1} = u_{2n+3} = f \circ f(w_n) \end{cases}$$

x	-2		1		2
$f \circ f$	0	$\nearrow$		$\nearrow$	$\sqrt{2}$

On pose $h : x \mapsto f(f(x)) - x = \sqrt{2 - \sqrt{2-x}} - x$

$$\begin{aligned}\forall x \in]-2,2[, h'(x) &= \frac{-\frac{-1}{2\sqrt{2-x}}}{2\sqrt{2-\sqrt{2-x}}} - 1 \\ &= \frac{1}{4\sqrt{2-x}\sqrt{2-\sqrt{2-x}}} - 1 \\ &= \frac{1 - 4\sqrt{4-2x-(2-x)\sqrt{2-x}}}{4\sqrt{2-x}\sqrt{2-\sqrt{2-x}}}\end{aligned}$$

$1 - 4\sqrt{4-2x-(2-x)\sqrt{2-x}}$ a le même signe que
$\left(1 - 4\sqrt{4-2x-(2-x)\sqrt{2-x}}\right)\left(1 + 4\sqrt{4-2x-(2-x)\sqrt{2-x}}\right)$
donc que $1 - 16\left(4-2x-(2-x)\sqrt{2-x}\right)$.

On décide de passer par l'inégalité des accroissements finis.

$$\begin{aligned}\forall x \in]-2,2[, |f'(x)| = \left|-\frac{1}{2\sqrt{2-x}}\right| = \frac{1}{2\sqrt{2-x}} &< 1 \\ \iff \sqrt{2-x} &> \frac{1}{2} \\ \iff 2-x &> \frac{1}{4} \\ \iff x &< \frac{7}{4}\end{aligned}$$

— Si $u_0 < \frac{7}{4}$ alors,

$$\forall n \in \mathbb{N}, |u_{n+1}| < M\,|u_n - 1|$$

avec $M = \sup_{x \in]-2, u_n[} |f'(x)| < 1$
Donc, $|u_n - 1| < M^n\,|u_0 - 1| \xrightarrow[n\to+\infty]{} 0$

— Si $u_0 > \frac{7}{4}$ alors $u_1 < \frac{7}{4} \cdots$ (pas prouvé rigoureusement)

Exercice 23

5. Soit $f : x \mapsto \dfrac{1}{2+x}$.
f est dérivable sur $\mathbb{R} \setminus \{2\}$ et décroissante sur $]-\infty; 2[$ et sur $]2; +\infty[$.

x	$-\infty$		-2		$+\infty$
f	0	$\searrow$	$-\infty$ / $+\infty$	$\searrow$	0

On pose $g : x \mapsto f(x) - x = \dfrac{1}{2+x} - x$ dérivable sur $\mathbb{R} \setminus \{2\}$ et

$$\forall x \neq 2, g'(x) = -\frac{1}{(2+x)^2} - 1 < 0$$

x	$-\infty$		α		-2		β		$+\infty$
g	$-\infty$	$\searrow$	0	$\searrow$	$-\infty$ / $+\infty$	$\searrow$	0	$\searrow$	$-\infty$

x	$-\infty$		α		-2		β		$+\infty$
f	0	$\searrow$	α	$\searrow$	$-\infty$ / $+\infty$	$\searrow$	β	$\searrow$	0
$f(x) - x$		$+$	0	$-$	‖	$+$	0	$-$	

(u_n) n'est pas définie s'il existe $k \in \mathbb{N}$ tel que

$$f^k(u_0) = -2$$

$(f^k(x) \neq (f(x))^k,\ f^k = f \circ \cdots \circ f)$

— On suppose la suite bien définie,

$$\begin{aligned} \forall x \neq -2, |f'(x)| &= \left| -\frac{1}{(2+x)^2} \right| \\ &= \frac{1}{(2+x)^2} \end{aligned}$$

En particulier si $x > 0$, alors $f'(x) \leqslant \dfrac{1}{4}$

— On suppose $u_0 > -2$ alors $u_1 > 0$ et donc

$$\forall n \in \mathbb{N}_\star, u_n > 0$$

Donc

$$\forall n \in \mathbb{N}_\star, |u_{n+1} - \beta| = |f(u_n) - f(\beta)| \leqslant \frac{1}{4} |u_n - \beta|$$

On en déduit par récurrence que

$$\forall n \in \mathbb{N}_\star, |u_n - \beta| \leqslant \left(\frac{1}{4}\right)^{n-1} |u_1 - \beta|$$

Or, $\left(\frac{1}{4}\right)^{n-1} \xrightarrow[n\to+\infty]{} 0$
Donc, $u_n \xrightarrow[n\to+\infty]{} \beta$

— Si $u_0 = \alpha$ alors
$$\forall n \in \mathbb{N}, u_n = \alpha \xrightarrow[n\to+\infty]{} \alpha$$

— Si, $u_0 < -2$ et $u_0 \neq \alpha$, je conjecture qu'il existe $p \in \mathbb{N}_\star$ tel que $u_p > -2$ et alors $u_n \xrightarrow[n\to+\infty]{} \beta$

Exercice

Pour $n \in \mathbb{N}$,
$$(E_n) : x^5 + nx - 1 = 0$$
On pose $\forall n \in \mathbb{N}, f_n : x \mapsto x^5 + nx - 1$.
$\forall n \in \mathbb{R}, f_n'(x) = 5x^4 + n > 0$ sauf si $\begin{cases} x = 0 \\ n = 0 \end{cases}$

u_n est le seul réel tel que $f_n(u_n) = 0$.

x	$-\infty$	0	u_n	$+\infty$
f_n	$-\infty$	-1	0	$+\infty$

Soit $n \in \mathbb{N}$.

$$\begin{aligned} f_n(u_{n+1}) &= u_{n+1}^5 + nu_{n+1} - 1 \\ &= \underbrace{u_{n+1}^5 (n+1) u_{n+1} - 1}_{f_{n+1}(u_{n+1})} - u_{n+1} \\ &= -u_{n+1} < 0 \end{aligned}$$

Donc $u_{n+1} < u_n$.
Les suites (u_n) est décroissante minorée par 0 donc elle converge.

On pose $\ell = \lim\limits_{n\to+\infty} u_n$.
On sait que

$$\forall n \in \mathbb{N}, u_n^5 + nu_n - 1 = 0$$

Or,

$$u_n^5 \xrightarrow[n\to+\infty]{} \ell^5$$
$$nu_n \xrightarrow[n\to+\infty]{} \begin{cases} -\infty \text{ si } \ell < 0 \\ +\infty \text{ si } \ell > 0 \end{cases}$$

Si, $\ell < 0$ alors $u_n^5 + nu_n - 1 \to -\infty \neq 0$.
Si, $\ell > 0$ alors $u_n^5 + nu_n - 1 \to +\infty \neq 0$.
Donc, $\boxed{\ell = 0}$

Or,

$$\forall n \in \mathbb{N}, nu_n = 1 - u_n^5 \xrightarrow[n\to+\infty]{} 1$$

donc $\boxed{u_n \sim_{n\to+\infty} \frac{1}{n}}$

$u_n = \frac{1}{n} + o_{n\to+\infty}\left(\frac{1}{n}\right)$
Donc,

$$\begin{aligned} \forall n \in \mathbb{N}, nu_n &= 1 - \left(\frac{1}{n} + o\left(\frac{1}{n}\right)\right) \\ &= 1 - \frac{1}{n^5}(1 + o(1))^5 \\ &= 1 - \frac{1}{n^5}(1 + o(1)) \\ &= 1 - \frac{1}{n^5} + o\left(\frac{1}{n^5}\right) \end{aligned}$$

Donc,

$$u_n = \frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6}\right)$$

$$\begin{aligned} \forall n \in \mathbb{N}_\star, nu_n &= 1 - \left(\frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6}\right)\right)^5 \\ &= 1 - \frac{1}{n^5}\left(1 - \frac{1}{n^5} + o\left(\frac{1}{n^5}\right)\right)^5 \\ &= 1 - \frac{1}{n^5}\left(1 - \frac{5}{n^5} + o\left(\frac{1}{n^5}\right)\right) \\ &= 1 - \frac{1}{n^5} + \frac{5}{n^{10}} + o\left(\frac{1}{n^10}\right) \end{aligned}$$

Donc,

$$u_n = \frac{1}{n} - \frac{1}{n^6} + \frac{5}{n^{11}} + o\left(\frac{1}{n^{11}}\right)$$

Exercice

$$\begin{cases} u_0 > 0 \\ \forall n \in \mathbb{N}, u_{n+1} = \dfrac{1}{2}\left(u_n + \dfrac{a}{u_n}\right) \end{cases}$$

On pose

$$\begin{aligned} f : \mathbb{R}_\star^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{2}\left(x + \frac{a}{x}\right) \end{aligned}$$

f est définie et dérivable sur $\mathbb{R}_\star^+$ et

$$\forall x > 0, f'(x) = \frac{1}{2}\left(1 - \frac{a}{x^2}\right)$$

x	0		$\sqrt{a}$		$+\infty$
f	$\|\|$ $+\infty$	$\searrow$	$\sqrt{a}$	$\nearrow$	$+\infty$
$f(x)-x$	$\|\|$	$+$	0	$-$	

On pose

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) - x \end{aligned}$$

$$\forall x > 0, g'(x) = f'(x) - 1 = -\frac{1}{2} - \frac{a}{2x^2} < 0$$

x	0		$\sqrt{a}$		$+\infty$
g	$+\infty$	$\searrow$	0	$\searrow$	$-\infty$

$$\forall x > 0, g(x) = -\frac{x}{2} + \frac{a}{2x}$$

— Pour $n \in \mathbb{N}$, $\mathscr{P}(n)$: "u_n existe et $u_n > 0$"
  — D'après l'énoncé, u_0 existe et $u_0 > 0$. Donc, $\mathscr{P}(0)$ est vraie.
  — Soit $n \in \mathbb{N}$, on suppose $\mathscr{P}(n)$ vraie.
  $u_n > 0$ donc u_n appartient au domaine de définition de f donc u_{n+1} existe. De plus, $u_{n+1} = f(u_n) \geqslant \sqrt{a} > 0$
  Donc, $\mathscr{P}(n+1)$ est vraie
— Pour $n \in \mathbb{N}_\star$, $\mathbb{Q}(n)$: "$u_n \geqslant \sqrt{a}$"
  — $u_1 = f(u_0) \geqslant \sqrt{a}$
  — Soit $n \in \mathbb{N}_\star$ tel que $u_n \geqslant \sqrt{a}$. Alors, $u_{n+1} = f(u_n) \geqslant \sqrt{a}$

De plus,

$$\forall n \in \mathbb{N}_\star, u_n \geqslant \sqrt{a}$$

donc,

$$\forall n \in \mathbb{N}_\star, u_{n+1} - u_n = g(u_n) \leqslant 0$$

Donc, (u_n) est décroissante, minorée par $\sqrt{a}$ donc (u_n) converge vers un point fixe de f (car f est continue).
Or, $\sqrt{a}$ est le seul point fixe de f. Donc,

$$u_n \xrightarrow[n\to+\infty]{} \sqrt{a}$$

Chapitre 12

TD 12

Exercice 2

"$i \not\Longrightarrow ii$"

$$\begin{aligned}\forall a, b \in G, (ab)^2 &= abab \\ &= aabb \\ &= a^2b^2\end{aligned}$$

"$ii \implies i$"

$$\begin{aligned}\forall (a, b) \in G^2, abab &= a^2b^2 \\ \text{donc } bab &= ab^2 \\ \text{donc } ba &= ab\end{aligned}$$

"$ \implies iii$"

$$\forall a, b \in G, (a, b)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$$

"$iii \implies i$"

$$\forall a, b \in G, ab = \left(b^{-1}a^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1} = ba$$

2. Soit $a, b \in G$

   — $(a, b)^2 = e$
   — $a^2b^2 = e \cdot e = e$

   Donc, $(a, b)^2 = a^2b^2$ donc G est abélien

Exercice 3

Soit $f : \mathbb{C}_\star \to \mathbb{R}_\star$ un isomorphisme.
$i^2 = -1$ donc $f(i^2) = f(-1)$ donc $f(i)^2 = f(-1)$
$(-1)^2 = 1$ donc $f\left((-1)^2\right) = f(1) = 1$ donc $f(-1)^2 = 1$ donc $f(-1) = \pm 1$
Or, $f(-1) = 1 \iff f(-1) = f(1) \iff -1 = 1$: une contradiction
Donc, $\underbrace{f(i)^2}_{>0} = -1$ une contradiction aussi

Exercice 6

$\langle 1 \rangle = \mathbb{Z}$ à prouver avec $\mathbb{Z} \subset \langle 1 \rangle \subset \mathbb{Z}$
$\langle 2 \rangle = 2\mathbb{Z}$

Exercice 7

Soit $f : (\mathbb{Q}, +) \to (\mathbb{Q}_\star, \times)$ un isomorphisme.

On pose

$$\begin{cases} a = f^{-1}(2) \in \mathbb{Q} \\ b = \dfrac{a}{2} \in \mathbb{Q} \end{cases}$$

Domme $a = 2b$, on a $2 = f(a) = f(b+b) = f(b) \times f(b) = f(b)^2$
Donc, $f(b) = \pm\sqrt{2}$. Or, $f(b) \in \mathbb{Q}_\star$. $\lightning$

Exercice 10

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$$

— $\mathbb{Z}[i] \subset \mathbb{C}$
— Soient $u, v \in \mathbb{Z}[i]$. On pose $u = a + ib$ et $v = c + id$ avec $(a, b, c, d) \in \mathbb{Z}^4$.

$$u + v = \underbrace{(a+c)}_{\in\mathbb{Z}} + i\underbrace{(b+d)}_{\in\mathbb{Z}} \in \mathbb{Z}[i]$$
$$uv = \underbrace{(ac - bd)}_{\in\mathbb{Z}} + i\underbrace{(ad + bc)}_{\in\mathbb{Z}} \in \mathbb{Z}[i]$$

$$-u = -a - ib \in \mathbb{Z}[i]$$
$$0 = 0 + i \times 0 \in \mathbb{Z}[i]1 \qquad = 1 + i \times 0 \in \mathbb{Z}[i]$$

— Soit $u \in \mathbb{Z}[i]^\times$. On sait qu'il existe $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
Donc, $|u|^2 |v|^2 = |uv|^2 = 1^2 = 1$
Comme $u \in \mathbb{Z}[i]$, $|u|^2 = \mathfrak{Re}(u)^2 + \mathfrak{Im}(u)^2 \in \mathbb{N}$
De même, $|v|^2 \in \mathbb{N}$
Donc, $|u|^2 = 1$.

On pose $u = a + ib, (a, b) \in \mathbb{Z}^2$. On a $a^2 + b^2 = 1$
donc $\begin{cases} 0 \leqslant a^2 \leqslant 1 \\ 0 \leqslant b^2 \leqslant 1 \end{cases}$
Donc, $\begin{cases} a^2 \in \{0, 1\} \\ b^2 \in \{0, 1\} \\ a^2 + b^2 = 1 \end{cases}$
Donc, $u \in \{\pm i, \pm 1\}$

—

$$\begin{aligned} 1^{-1} &= 1 \in \mathbb{Z}[i] \\ (-1)^{-1} &= -1 \in \mathbb{Z}[i] \\ i^{-1} &= -i \in \mathbb{Z}[i] \\ (-i)^{-1} &= i \in \mathbb{Z}[i] \end{aligned}$$

Autre méthode $u \in \mathbb{Z}[i] \setminus \{0\}$. $u = a + ib$ avec $a, b \in \mathbb{Z}$.

$$\begin{aligned} \frac{1}{u} \in \mathbb{Z}[i] &\iff \frac{1}{a+ib} \in \mathbb{Z}[i] \\ &\iff \frac{a-ib}{a^2-b^2} \in \mathbb{Z}[i] \\ &\iff \begin{cases} \dfrac{a}{a^2+b^2} \in \mathbb{Z} \\ \dfrac{-b}{a^2+b^2} \in \mathbb{Z} \end{cases} \qquad \iff \begin{cases} a^2+b^2 \mid a \\ a^2+b^2 \mid b \end{cases} \\ &\implies \begin{cases} a^2+b^2 \leqslant |a| \\ a^2+b^2 \leqslant |b| \end{cases} \qquad \implies \begin{cases} a \in \{0, 1, -1\} \\ b \in \{0, 1, -1\} \\ a^2+b^2 = 1 \end{cases} \end{aligned}$$

Exercice 12

$G \cap \mathbb{R}_\star^+ \neq$ minoré par 0 donc a existe

1. $a = \min(G \cap \mathbb{R}_\star^+)$. On adapte l'exercice 5. Soit $g \in G$
On pose $q = \left\lfloor \dfrac{g}{a} \right\rfloor \in \mathbb{Z}$ et $r = g - qa \in G$
Or, $q \leqslant \dfrac{g}{a}$ donc $aq \leqslant g$ donc $r \geqslant 0$
$\dfrac{g}{a} < q + 1$ donc $g < aq + a$ donc $r < a$

Si $r > 0$, alors $\begin{cases} r \in G \cap \mathbb{R}_\star^+ \\ r < a \leqslant r : \text{une contradiction } \lightning \end{cases}$
Donc $r = 0$ donc $g = aq$ avec $q \in \mathbb{Z}$ donc $g \in a\mathbb{Z}$
Donc, $G \subset a\mathbb{Z}$
$a \in G$ donc $a\mathbb{Z} \subset G$
Donc $G = a\mathbb{Z}$

2. Soit $g \in G \cap \mathbb{R}_\star^+$. Comme $a \notin \left(G \cap \mathbb{R}_\star^+\right)$, $g \neq a$
Or, $g \geqslant a$ donc $g > a$ donc g ne minore pas $G \cap \mathbb{R}_\star^+$ donc il existe $g_1 \in G \cap \mathbb{R}_\star^+$ tel que $g_1 < g$
De cette façon, on fabrique une suite (g_n) strictement décroissante minorée par a. Donc (g_n) converge. On pose $\ell = \lim\limits_{n \to +\infty} g_n$
Donc $\underbrace{g_{n+1} - g_n}_{\in G} \xrightarrow[n \to +\infty]{} \ell - \ell = 0$
On vient de trouver une suite $(g_{n+1} - g_n)_{n \in \mathbb{N}_\star}$ de G qui converge vers 0.
Donc $a = 0$
Soit $I =]a, b[$ et $g \in G$ tel que $0 < g < b - a$
On pose $n = \left\lfloor \dfrac{a}{g} \right\rfloor$. On a donc

$$n \leqslant \frac{a}{g} < n + 1$$

donc $ng \leqslant a < g(n+1)$.
Or,

$$g(n+1) = ng + g \leqslant a + g < a + b - a < b$$

donc $(n+1) \in]a, b[\cap G$

Exercice 15

$f : \mathbb{C} \longrightarrow \mathbb{C}$ morphisme d'anneaux
$f_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$
Soit $z \in \mathbb{C}$. On pose $z = a + ib$, $(a, b) \in \mathbb{R}^2$

$$\begin{aligned} f(z) &= f(a + ib) \\ &= f(a) + f(ib) \\ &= a + f(i)f(b) \\ &= a + bf(i) \end{aligned}$$

$i^2 = -1$ donc $f\left(i^2\right) = f(-1) = -1$ donc $f(i)^2 = -1$ donc $f(i) \in \{i, -i\}$
Donc $f \in \{\mathrm{id}_{\mathbb{C}}, z \mapsto \overline{z}\}$

Exercice 19

Soit $a \in A \setminus \{0\}$

$$\begin{aligned} f : A &\longrightarrow A \\ x &\longmapsto ax \end{aligned}$$

$1 \in \mathrm{Im}(f)$?

— Soient $x, y \in A$

$$f(x+y) = a(x+y)ax + ay = f(x) + f(y)$$

donc f est un endomorphisme de $(A, +)$

— Soit $x \in A$

$$\begin{aligned} x \in \mathrm{Ker}(f) &\iff f(x) = 0 \\ &\iff ax = 0 \\ &\iff a = 0 \text{ ou } x = 0 \\ &\iff x = 0 \end{aligned}$$

$\mathrm{Ker}(f) = \{0\}$ donc f est injective.
Comme A est fini, f est bijective donc $\mathrm{Im} = A \ni 1$

Exercice 20

Analyse : Soit $\mathbb{K} = (\{0, 1, a, b\}, +, \times)$ un corps à 4 éléments.

$+$	0	1	a	b
0	0	1	a	b
1	1	0 / b	b / 0	a / a
a	a	b / 0	1 / b	/ 1
b	b	a / a	/ 1	/ 0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$$\begin{aligned} & a^2 = b \neq 1 \\ & b^2 = a \neq 1 \\ \implies & -1 \notin \{0, a, b\} \\ \implies & -1 = 1 \\ \implies & 1 + 1 = 0 \end{aligned}$$

$$\begin{aligned} a+a &= a(1+1) \\ &= a \times 0 \\ &= 0 \end{aligned}$$

Donc, $\mathbb{K} = \left\{0, 1, a, a^{-1}\right\}$: le sous-corps engendré par a

$+$	0	1	a	a^{-1}
0	0	1	a	a^{-1}
1	1	0	a^{-1}	a
a	a	a^{-1}	0	1
a^{-1}	a^{-1}	a	1	0

$\times$	0	1	a	a^{-1}
0	0	0	0	0
1	0	1	a	a^{-1}
a	0	a	a^{-1}	1
a^{-1}	0	a^{-1}	1	a

Synthèse : Il faut vérifier que

— $+$ est associative
— $\times$ est associative
— la distributivité

Chapitre 13

TD 13

Exercice 5

$$(S) : AX = 0 \text{ où } X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\begin{aligned} A = \mathrm{GL}_n(\mathbb{C}) &\iff \mathrm{rg}(A) = n \\ &\iff \mathrm{rg}(S) = n \\ &\iff S \text{ est de Cramer} \\ &\iff X = 0 \text{ est la seule solution de } (S) \end{aligned}$$

On suppose $X \neq 0$ tel que $AX = 0$ et on cherche une contradiction.

$$\begin{aligned} (S) &\iff \forall i \in [\![1, n]\!], \sum_{j=1}^{n} a_{ij} x_j = 0 \\ &\implies \forall i \in [\![1, n]\!] - a_{ii} x_i = \sum_{j \neq i} a_{ij} x_j \\ &\implies \forall i \in [\![1, n]\!], |a_{ii}| \, |x_i| = \left| \sum_{j \neq i} a_{ij} x_j \right| \\ &\implies \forall i \in [\![1, n]\!] \, |a_{ii}| \, |x_i| \leqslant \sum_{j \neq i} |a_{ij}| \, |x_j| \end{aligned}$$

Soit i_0 tel que $|x_{i_0}| = \max\limits_{i \leqslant j \leqslant n} (|x_j|)$ ($i_0 = \mathrm{argmax}\, 1 \leqslant j \leqslant n \, (|x_j|)$)
Comme $X \neq 0$, $x_{i_0} > 0$, donc

$$|a_{i_0,i_0}| \leqslant \sum_{j \neq i_0} |a_{i_0,j}| \frac{|x_j|}{|x_{i_0}|} \leqslant \sum_{j \neq i_0} |a_{i_0,j}|$$

une contradiction $\lightning$

Exercice 9

$$\left(\begin{array}{ccc|c} \boxed{1} & a & -a^2 & a^4 \\ 1 & b & -b^2 & b^4 \\ 1 & c & -c^2 & c^4 \end{array}\right) \underset{\substack{L_2 \leftarrow \frac{L_2-L_1}{b-a} \\ L_3 \leftarrow \frac{L_3-L_1}{c-a}}}{\sim} \left(\begin{array}{ccc|c} \boxed{1} & a & -a^2 & a^4 \\ 0 & \boxed{1} & -(a+b) & b^3+ab^2+a^2b+a^3 \\ 0 & 1 & -(a+c) & c^3+ac^2+a^2c+a^3 \end{array}\right)$$

$$\underset{L_3 \leftarrow \frac{L_3-L_2}{b-c}}{\sim} \left(\begin{array}{ccc|c} \boxed{1} & a & -a^2 & a^4 \\ 0 & \boxed{1} & -(a+b) & b^3+ab^2+a^2b+a^3 \\ 0 & 0 & \boxed{1} & -c^2-bc-b^2-ac-ab-a^2 \end{array}\right)$$

$$\underset{\substack{L_2 \leftarrow L_2+(a+b)L_3 \\ L_1 \leftarrow L_1-aL_2+a^2L_3}}{\sim} \left(\begin{array}{ccc|c} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \end{array}\right)$$

Exercice 10

Soient a, b, c, d différents de -1.

$$(S) : \begin{cases} x = by + cz + dt \\ y = cz + dt + ax \\ z + dt + ax + by \\ t = ax + by + cz \end{cases} \iff \begin{cases} x = by + cz + dt \\ y - x = ax - by \\ z - y = by - cz \\ t - z = cz - dt \end{cases}$$

$$\iff \begin{cases} z = \dfrac{d+1}{c+1}t \\ y = \dfrac{c+1}{b+1}z = \dfrac{d+1}{b+1}t \\ x = \dfrac{b+1}{a+1}y = \dfrac{d+1}{a+1}t \\ \dfrac{d+1}{a+1}t = \dfrac{b}{b+1}(d+1)t + \dfrac{c}{c+1}(d+1)t + dt \end{cases}$$

$$\iff \begin{cases} x = \dfrac{d+1}{a+1}t \\ y = \dfrac{d+1}{b+1}t \\ z = \dfrac{d+1}{c+1}t \\ t\left(\dfrac{b}{b+1} + \dfrac{c}{c+1} + \dfrac{d}{d+1} - \dfrac{1}{a+1}\right) = 0 \end{cases}$$

(S) a des solutions non nulles ssi

$$\frac{b}{b+1} + \frac{c}{c+1} + \frac{d}{d+1} - \frac{1}{a+1} = 0$$

ssi

$$\frac{b}{b+1}+\frac{c}{c+1}+\frac{d}{d+1}-\frac{a+1-a}{a+1}=0$$

ssi

$$\frac{a}{a+1}+\frac{b}{b+1}+\frac{c}{c+1}+\frac{d}{d+1}=1$$

Chapitre 14

TD 14

Exercice 1

Pour $t \in [0,1]$, on note $d(t)$ la distance en km parcourue en t heure.

$$d : [0,1] \longrightarrow \mathbb{R}^+$$

On suppose $\begin{cases} d(0) = 0 \\ d(1) = 4 \\ d \text{ continue et croissante} \end{cases}$

On veut prouver qu'il existe t te lque

$$d\left(t + \frac{1}{2}\right) - d(t) = 2$$

On pose $\delta : t \mapsto d\left(t + \frac{1}{2}\right) - d(t)$ continue.

$$\begin{cases} \delta(0) = d\left(\frac{1}{2}\right) \\ \delta\left(\frac{1}{2}\right) = 4 - d\left(\frac{1}{2}\right) \leqslant d(1) \end{cases}$$

— Si $d\left(\frac{1}{2}\right) > 2$, alors $\delta\left(\frac{1}{2}\right) < 2 < \delta(0)$ donc il existe t tel que $\delta(t) = 2$

— Si $d\left(\frac{1}{2}\right) \leqslant 2$, alors $\delta\left(\frac{1}{2}\right) \geqslant 2 \geqslant \delta(0)$ donc il existe t tel que $\delta(t) = 2$

Donc il exite t tel que $\delta(t) = 2$ i.e. $d\left(t + \frac{1}{2}\right) = 2 + d(t)$

Exercice 2

On pose $\begin{cases} M : x \mapsto \max(f(x), g(x)) \\ m : x \mapsto \min(f(x), g(x)) \end{cases}$
On remarque que

$$\forall x \in \mathbb{R}, \begin{cases} M(x) + m(x) = f(x) + g(x) \\ M(x) - m(x) = |f(x) - g(x)| \end{cases}$$

Donc

$$\forall x \in \mathbb{R}, M(x) = \frac{1}{2}\left(f(x) + g(x) + |f(x) - g(x)|\right)$$

et

$$\left(\forall x \in \mathbb{R}, m(x) = \frac{1}{2}\left(f(x) + g(x) - |f(x) - g(x)|\right)\right)$$

On a bien M continue

Exercice 3

$\forall n \in \mathbb{Z}, x \mapsto \lfloor x \rfloor$ est constante sur $[n, n+1[$ donc $\begin{cases} \text{continue sur }]n, n+1[\\ \text{et continue à droite en } n \end{cases}$

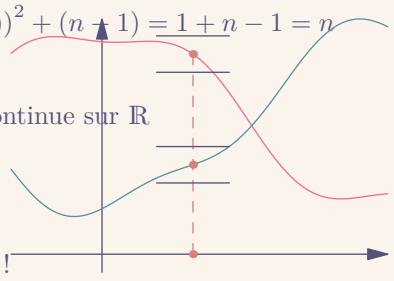
Soit $f : x \mapsto (x - \lfloor x \rfloor)^2 + \lfloor x \rfloor$
Soit $n \in \mathbb{Z}$. f est continue sur $]n, n+1[$
Donc f est continue sur $\mathbb{R} \setminus \mathbb{Z}$.

$$f(n) = 0^2 + n = n$$

$$\lim_{\substack{x \to n \\ >}} f(x) = \lim_{\substack{x \to n \\ >}} (x - n)^2 + n = n$$

$$\lim_{\substack{x \to n \\ <}} f(x) = \lim_{\substack{x \to n \\ <}} (x - (n-1))^2 + (n+1) = 1 + n - 1 = n$$

Donc f est continue en n donc f est continue sur $\mathbb{R}$



Exercice 4

On suppose, sans perte de généralité, $f(a) < g(a)$.
On pose $\varepsilon = \dfrac{g(a) - f(a)}{3} > 0$.
$g(x) \xrightarrow[x \to a]{} g(a)$ donc il existe $\eta_1 > 0$ tel que

$$\forall x \in]a - \eta_1, a + \eta_1[\cap I, |g(x) - g(a)| \leqslant \varepsilon$$

De même, il existe $\eta_2 > 0$ tel que

$$\forall x \in]a - \eta_2, a + \eta_2[\cap I, |f(x) - f(a)| \leqslant \varepsilon$$

On suppose $a \in \mathring{A}$ (sinon $J = \{a\}$ conviendrait...)
donc il existe $\eta_3 > 0$ tel que $]a - \eta_3, a + \eta_3[\subset I$.
On pose $J =]a - \eta_1, a + \eta_1[\cap]a - \eta_2, a + \eta_2[\cap]a - \eta_3, a + \eta_3[$.
J est un intervalle ouvert non vide (car $a \in J$) inclus dans I.

$$\begin{aligned} \forall x \in J, f(x) \leqslant f(a) + \varepsilon &= \frac{2f(a) + g(a)}{3} \\ &< \frac{f(a) + 2g(a)}{3} \\ &\leqslant g(a) - \varepsilon \\ &\leqslant g(x) \end{aligned}$$

Donc,

$$\forall x \in J, f(x) \neq g(x)$$

Exercice 5

On pose

$$\begin{aligned} g : [0,1] &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) - x \end{aligned}$$

g est continue

$$\begin{cases} g(0) = f(0) \geqslant 0 \\ g(1) = f(1) - 1 \leqslant 0 \end{cases}$$

D'après le théorème des valeurs intermédiaires,

$$\exists a \in [0,1], g(a) = 0 \text{ i.e. } f(a) = a$$

Exercice 6

—

$$\forall x \in \mathbb{R}, |f(x)| \leqslant x^2 \, |x - 2| \xrightarrow[\substack{x \to 0 \\ x \to 2}]{} 0$$

Par encadrement,

$$\begin{cases} f(x) \xrightarrow[\substack{x \to 0 \\ \neq}]{} 0 & = f(0) \\ f(x) \xrightarrow[\substack{x \to 2 \\ \neq}]{} 0 & = f(2) \end{cases}$$

Donc f est continue en 0 et en 2

— Soit $a \in \mathbb{R} \setminus \{0, 2\}$.
$\mathbb{Q}$ est dense dans $\mathbb{R}$ dnc il existe $(x_n) \in \mathbb{Q}^{\mathbb{N}}$ telle que $x_n \xrightarrow[n \to +\infty]{} a$

$\mathbb{R}\backslash\mathbb{Q}$ est dense dans $\mathbb{R}$ donc il existe $(y_n) \in (\mathbb{R} \setminus \mathbb{Q})^{\mathbb{N}}$ telle que $y_n \xrightarrow[n\to+\infty]{} a$

$$\begin{cases} \forall n \in \mathbb{N}, \begin{cases} f(x_n) = {x_n}^2(x_n - 2) \times 0 = 0 \xrightarrow[n\to+\infty]{} 0 \\ f(y_n) = {y_n}^2(y_n - 2) \times 1 \xrightarrow[n\to+\infty]{} a^2(a-2) \end{cases} \end{cases}$$

Comme $a \notin \{0, 2\}, a^2(a-2) \neq 0$ donc f n'est pas continue en a

Exercice 7

Cas 1 $\forall x \geqslant a, f(x) = 0$
Alors,

$$0 = f(a) = \max_{[a,+\infty[} f$$

Cas 2 $\exists x_0 \geqslant a, f(x_0) > 0$.
On pose $\varepsilon = \dfrac{f(x_0)}{2} > 0$
Il existe $\eta \geqslant x_0$ tel que

$$\forall x \geqslant \eta, f(x) \leqslant \varepsilon$$

f est continue sur $[a, \eta]$ donc elle a un maximum

$$\max_{[a,\eta]} f = f(b) \text{ avec } b \in [a, \eta]$$

D'où,

$$\forall x \geqslant a, f(x) \leqslant \begin{cases} \varepsilon < f(x_0) \underbrace{\leqslant}_{\text{car } x_0 \in [a,\eta]} f(b) & \text{si } x \geqslant \eta \\ f(b) & \text{si } x \leqslant \eta \end{cases}$$

Exercice 8

Preuve du " $\Longleftarrow$ " de la proposition 2.10 du cours

Soit $y \in]a, b[$. f est croissante sur $]a, y[$ et majorée par $f(y)$ donc

$$\lim_{\substack{x\to y \\ <}} f(x) = \sup_{]a,y[} f \leqslant f(y)$$

f est croissante sur $]y, b[$ minorée par $f(b)$ donc

$$\lim_{\substack{x\to y \\ >}} f(x) = \inf_{]y,b[} f \geqslant f(y)$$

Supposons $\sup\limits_{]a,y[} f < f(y)$.
Soit $t \in]a, y[$, $f(t) \leqslant \sup\limits_{]a,y[} f < f(y)$
donc $\sup\limits_{]a,y[} f \in [f(t), f(y)] \subset [f(a), f(b)] = f([a, b])$
donc

$$\exists u \in]a, b[, \sup_{]a,y[} f = f(u)$$

Donc $f(u) < f(y)$
Soit $w \in]f(u), f(y)[\subset [f(a), f(b)] = f([a,b])$ donc $w = f(r)$ avec $r \in [a,b]$.

$$f(r) > f(u) \text{ donc } r > u$$
$$f(r) < f(y) \text{ donc } r < y$$

donc $r \in]a, y[$ donc $f(u) < w = f(r) \leqslant f(u)$ ↯

Exercice 9

1. Récurrence :
   - $f\left(a^{\frac{1}{a^0}}\right) = f(a)$
   - $f\left(a^{\frac{1}{2^{n+1}}}\right) = f\left(\left(a^{\frac{1}{2^n}}\right)^2\right) = f\left(a^{\frac{1}{2n}}\right) = f(a)$
2. $\forall a > 0, a^{\frac{1}{2^n}} \xrightarrow[n\to+\infty]{} 1$
   f est continue donc

$$f\left(a^{\frac{1}{2^n}}\right) \xrightarrow[n\to+\infty]{} f(1)$$
$$\| \qquad\qquad\qquad$$
$$f(a) \quad \xrightarrow[n\to+\infty]{} f(a)$$

   Donc $f(a) = f(1)$
   $f(0) = \lim\limits_{\substack{a\to 0 \\ >}} f(a) = f(1)$ car f est continue en 0
   donc $\forall a \in \mathbb{R}^+, f(a) = f(1)$, f est constant

Exercice 10

— Soit $x \in E_f$. $f(x) = x$ donc $x \in \mathrm{Im}(f)$
— Soit $x \in \mathrm{Im}(f), x = f(u)$.
Alors, $f(x) = f(f(u)) = f(u) = x$ donc $x \in E_f$
D'ou $\boxed{E_f = \mathrm{Im}(f) = f([0,1])}$
Comme f est continue, $f([0,1])$ est un segment non vide car $f(1) \in \mathrm{Im}(f) = E_f$
Soient $a \leqslant b$ dans $[0,1]$
$g : [0,a] \to [a,b]$ continue telle que $g(a) = a$
$h : [b,1] \to [a,b]$ continue telle que $h(b) = b$
On pose

$$f : [0,1] \longrightarrow [0,1]$$
$$x \longmapsto \begin{cases} g(x) & \text{si } x \leqslant a \\ x & \text{si } a \leqslant x \leqslant b \\ h(x) & \text{si } x \geqslant b \end{cases}$$

Montrer que f est continue est $f \circ f = f$

Exercice 11

On suppose $A \neq$ et on pose

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \inf\{|x-a| \mid a \in A\} \end{aligned}$$

$$\forall x \in \mathbb{R}, \Big(\forall a \in A, |x-a| \geqslant 0 \text{ donc } f(x) \text{ existe}\Big)$$

Soient $x, y \in \mathbb{R}$.

$$\begin{aligned} \forall a \in A, f(x) = \inf_{a\in A}(|x-a|) &\leqslant |x-a| = |x-y+y-a| \\ &\leqslant |x-y| + |y-a| \end{aligned}$$

donc

$$\forall a \in A, |y-a| \geqslant f(x) - |x-y|$$

donc

$$f(y) \geqslant f(x) - |x-y|$$

donc

$$f(x) - f(y) \leqslant |x-y|$$

On peut prouver de même que

$$f(y) - f(x) \leqslant |y-x| = |x-y|$$

D'où,

$$-|x-y| \leqslant f(x) - f(y) \leqslant |x-y|$$

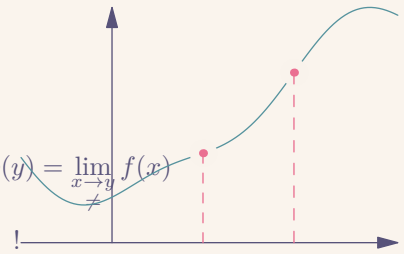
donc

$$|f(x) - f(y)| \leqslant |x-y|$$

donc f est 1-lipschitzienne donc continue

Exercice 12

$$\forall y \in [0,1], \varphi(y) = \lim_{\substack{x\to y \\ \neq}} f(x)$$



1. Soit $y \in [0,1]$. Soit $\varepsilon > 0$. Il existe $\eta_1 > 0$ tel que

$$\forall x \in [0,1] \cap]y-\eta_1, y+\eta_1[\setminus \{y\}, -\frac{\varepsilon}{2} \leqslant -f(x) + \varphi(y) \leqslant \frac{\varepsilon}{2}$$

2. Soit $z \in [0,1] \cap \left]y - \dfrac{\eta_1}{2}, y + \dfrac{\eta_1}{2}\right[$. Il exite $\eta_2 > 0$ tel que

$$\forall x \in [0,1] \cap]z-\eta_2, z+\eta_2[\setminus \{z\} - \frac{\varepsilon}{2} \leqslant f(x) - \varphi(z) \leqslant \frac{\varepsilon}{2}$$

3. Soit $x \in [0,1] \cap]z-\eta, z+\eta[\setminus \{y,z\}$ où $\eta = \dfrac{1}{2}\min(\eta_1, \eta_2)$.

$$|x-y| \leqslant |x-z| + |z-y| \leqslant \eta + \frac{\eta_1}{2} \leqslant \frac{\eta_1}{2} + \frac{\eta_1}{2} = \eta_1$$

$$\varphi(y) - \varphi(z) = \underbrace{\varphi(y) - f(x)}_{\in\left[-\frac{\varepsilon}{2}, \frac{\varepsilon}{2}\right]} \underbrace{f(x) - \varphi(z)}_{\in\left[-\frac{\varepsilon}{2}, \frac{\varepsilon}{2}\right]} \in [-\varepsilon, \varepsilon]$$

Exercice 13

$$\forall x \in \mathbb{R}, \varphi(x) = \sup_{t \in [a,b]} (f(t) + xg(t))$$

Soit $x \in \mathbb{R}$. $t \mapsto f(t) + xg(t)$ est continue sur $[a,b]$ donc $\varphi(x)$ existe. φ est définie sur $\mathbb{R}$. On pose

$$\begin{cases} m = \min\limits_{t \in [a,b]} (g(t)) \\ M = \max\limits_{t \in [a,b]} (g(t)) \end{cases}$$

Soit $(x,y) \in \mathbb{R}^2$.

$$\begin{aligned} \forall t \in [a,b], \varphi(x) &\geqslant f(t) + xg(t) \\ &\geqslant f(t) + yg(t) + (x-y)g(t) \end{aligned}$$

Si $x \geqslant y$, $g(t) \geqslant m$ donc $(x-y)g(t) \geqslant m(x-y)$
Si $x \leqslant y$, $g(t) \leqslant M$ donc $(x-y)g(t) \leqslant M(x-y)$

Dans les deux cas, il exite $\mu \in \mathbb{R}$ tel que

$$\forall t \in [a,b], \varphi(x) - \mu(x-y) \geqslant f(t) + yg(t)$$

donc

$$\varphi(x) - \mu(x-y) \geqslant \varphi(y)$$

donc

$$\varphi(x) - \varphi(y) \geqslant \mu(x-y)$$

En échangant les rôles de x et y, il existe $\nu \in \mathbb{R}$ tel que

$$\varphi(y) - \varphi(x) \geqslant \nu(y-x)$$

Donc

$$\mu(x-y) < \varphi(x) - \varphi(y) \leqslant \nu(x-y)$$

Par encadrement, $\varphi(x) - \varphi(y) \underset{\substack{x \to y \\ \neq}}{\longrightarrow} 0$

donc $\varphi(x) \underset{\substack{x \to y \\ \neq}}{\longrightarrow} \varphi(y)$

donc φ est continue en y

Chapitre 15

TD 15

Exercice 3

1. $0 \in F$.
   Soit $P, Q \in F, \lambda, \mu \in \mathbb{K}$. On pose $R = \lambda P + \mu Q$. Montrons que $R \in F$.

$$\begin{aligned} 2R'(1) + R(0) &= 2(\lambda P'(1) + \mu Q'(1)) + \lambda P(0) + \mu Q(0) \\ &= \lambda(2P'(1) + P(0)) + \mu(2Q'(1) + Q'(0)) \\ &= 0 \end{aligned}$$

   Donc $R \in F$ et donc F est un sous-espace vectoriel de E.
2.

$$\begin{aligned} P \in F &\iff 2P'(1) + P(0) \\ &\iff 2(b + 2c) + a = 0 \\ &\iff a + 2b + 4c = 0 \end{aligned}$$

3. *Touver une famille génératrice de E*

$$\begin{aligned} P \in F &\iff a + 2b + 4c = 0 \\ &\iff a = -2b - 4c \\ &\iff \forall x, P(x) = (-2b - 4c) + bx + cx^2 \\ &\iff \forall x, P(x) = b\underbrace{(-2 + x)}_{\in E} + c\underbrace{(-4 + x^2)}_{\in E} \end{aligned}$$

   Donc, $F = \text{Vect}(P_1, P_2)$ où $\begin{cases} P_1 : x \mapsto -2 + x \\ P_2 : x \mapsto -4 + x^2 \end{cases}$
4. *Cette famille est-elle une base ?*
   P_1 et P_2 ne sont pas colinéaires car ils n'ont pas le même degré donc (P_1, P_2) est une base de F. On a $\dim(F) = 2$.

Exercise 7

Let $(\lambda, \mu, \nu) \in \mathbb{R}^3$ such that

$$\lambda(u_n) + \mu(v_n) + \nu(w_n) = (0)$$

Thus,

$$\forall n \in \mathbb{N}, \lambda 2^n + \mu 3^n + \nu 4^n = 0$$

1ST METHOD In particular, with $n \in \{0, 1, 2\}$, we have

$$(S): \quad \begin{cases} \lambda + \mu + \nu = 0 \\ 2\lambda + 3\mu + 4\nu = 0 \\ 4\lambda + 9\mu + 16\nu = 0 \end{cases}$$

$$\begin{aligned} (S) &\iff \begin{cases} \lambda + \mu + \nu = 0 \\ \mu + 2\nu = 0 \\ 5\mu + 12\nu = 0 \end{cases} \\ &\iff \begin{cases} \lambda + \mu + \nu = 0 \\ \mu + 2\nu = 0 \\ 2\nu = 0 \end{cases} \\ &\iff \lambda = \mu = \nu = 0 \end{aligned}$$

Therefore, u, v and w are linearly independant.

2ND METHOD Suppose $\nu \neq 0$. Then,

$$0 = \lambda u_n + \mu v_n + \nu w_n \sim \nu 4^n \xrightarrow[n \to +\infty]{} \pm\infty$$

Hence, $\nu = 0$.
Suppose $\nu \neq 0$, then $0 = \lambda 2^n + \mu 3^n \sim \mu 3^n \xrightarrow[n \to +\infty]{} \pm\infty$
Thus, $\mu = 0$. Also, $\lambda = 0$

Exercice 8

Soit $P \in E$. On pose

$$P : x \mapsto ax^2 + bx + c$$

avec $(a,b,c) \in \mathbb{R}^3$

$$\begin{aligned}
P \in F &\iff \begin{cases} P(1) = 0 \\ \displaystyle\int_0^1 P(t)\ dt = 0 \end{cases} \\
&\iff \begin{cases} a+b+c=0 \\ \dfrac{a}{3}+\dfrac{b}{2}+c=0 \end{cases} \\
&\iff \begin{cases} a+b+c=0 \\ \dfrac{2}{3}a+\dfrac{1}{2}b=0 \end{cases} \\
&\iff \begin{cases} a=-\dfrac{3}{4}b \\ c=-\dfrac{1}{4}b \end{cases} \\
&\iff \forall x \in \mathbb{R}, P(x) = -\frac{3}{4}bx^2+bx-\frac{1}{4}b = b\left(-\frac{3}{4}x^2+x-\frac{1}{4}\right) \\
&\iff P \in \mathrm{Vect}(Q)
\end{aligned}$$

où $Q : x \mapsto -\dfrac{3}{4}x^2+x-\dfrac{1}{4}$
Donc, $F = \mathrm{Vect}(Q)$ est un sous-corps vectoriel de E. De plus, $Q \neq 0$ donc (Q) est une base de F.

Exercice 9

Soit $(x,y,z,t) \in \mathbb{R}^4$.

$$\begin{aligned}
(x,y,z,t) \in H_2 &\iff \begin{cases} x+y+z+t=0 \\ x-y-z+t=0 \end{cases} \\
&\iff \begin{cases} x+y+z+t=0 \\ 2y+2z=0 \end{cases} \\
&\iff \begin{cases} y=-z \\ x=-t \end{cases} \\
&\iff (x,y,z,t) = (-t,-z,z,t) = z(0,-1,1,0)+t(-1,0,0,1) \\
&\iff (x,y,z,t) \in \mathrm{Vect}(u_1,u_2) \\
&\qquad \text{où } \begin{cases} u_1 = (0,-1,1,0) \\ u_2 = (-1,0,0,1) \end{cases}
\end{aligned}$$

$H_2 = \mathrm{Vect}(u_1,u_2)$ est un sous-espace vectoriel de $\mathbb{R}^4$
u_1 et u_2 ne sont pas colinéaires donc (u_1,u_2) est une base de H_2.

Exercise 10

We need to show that $F \subset G$. Let $n \in \mathbb{N}$.

$$\forall x \in \mathbb{R}, \cos(nx) = T_n(\cos x)$$

where T_n is the n-th чебышёвpolynomial.
Thus,

$$\left(x \mapsto \cos(nx)\right) \in G$$

. In fact,

$$\begin{aligned}
\forall x \in \mathbb{R}, \cos(nx) &= \mathfrak{Re}\left(e^{inx}\right) \\
&= \mathfrak{Re}\left(\left(e^{ix}\right)^n\right) \\
&= \mathfrak{Re}\left((\cos x + i \sin x)^n\right) \\
&= \mathfrak{Re}\left(\sum_{k=0}^{n} i^k \sin^k x \cos^{n-k} x \binom{n}{k}\right) \\
&= \sum_{\substack{0 \leqslant k \leqslant n \\ k \text{ even}}} \binom{n}{k} \cos^{n-k} x \sin^k x i^k \\
&= \sum_{0 \leqslant p \leqslant \frac{n}{2}} \binom{n}{2p} \cos^{n-2p} x \left(\sin^2 x\right)^p (-1)^p \\
&= \sum_{0 \leqslant p \leqslant \frac{n}{2}} (-1)^p \binom{n}{2p} \cos^{n-2p} x \left(1 - \cos^2 x\right)^p
\end{aligned}$$

And,

$$T_n : u \mapsto \sum_{0 \leqslant p \leqslant \frac{n}{2}} (-1)^p \binom{n}{2p} u^{n-2p} \left(1 - u^2\right)^p$$

$$\begin{aligned}
\forall x \in \mathbb{R}, \cos^n x &= \left(\frac{e^{ix} + e^{-ix}}{2}\right)^n \\
&= \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} e^{ikx} e^{-i(n-k)x} \\
&= \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} e^{i(2k-n)x} \\
&= \mathfrak{Re}\left(\frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} e^{i(2k-n)x}\right) \\
&= \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} \cos\left(|2k-n|x\right)
\end{aligned}$$

So, $(x \mapsto \cos^n x) \in F$.

Exercice 11

Partie 1

1. En replacant t par 0, par $\frac{\pi}{8}$ et par $-\frac{\pi}{\sqrt{3}}$, on obtient

$$(S): \quad \begin{cases} a+b=0 \\ ae^{\frac{\pi}{\sqrt{3}}} + be^{-\frac{\pi}{2\sqrt{3}}} = 0 \\ ae^{-\frac{\pi}{\sqrt{3}}} - be^{\frac{\pi}{2\sqrt{3}}} = 0 \end{cases}$$

$$\begin{vmatrix} e^{\frac{\pi}{\sqrt{3}}} & e^{-\frac{\pi}{2\sqrt{3}}} \\ e^{-\frac{\pi}{\sqrt{3}}} & -e^{-\frac{\pi}{2\sqrt{3}}} \end{vmatrix} = -e^{\frac{3\pi}{2\sqrt{3}}} - e^{-\frac{3\pi}{2\sqrt{3}}} \neq 0$$

donc

$$\begin{pmatrix} e^{\frac{\pi}{\sqrt{3}}} & e^{-\frac{\pi}{2\sqrt{3}}} \\ e^{-\frac{\pi}{\sqrt{3}}} & -e^{-\frac{\pi}{2\sqrt{3}}} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

donc le système $\begin{cases} ae^{\frac{\pi}{\sqrt{3}}} be^{-\frac{\pi}{2\sqrt{3}}} = 0 \\ ae^{-\frac{\pi}{\sqrt{3}}} - be^{-\frac{\pi}{2\sqrt{3}}} = 0 \end{cases}$ est de Cramer. Son unique solution est $\begin{cases} a=0 \\ b=0 \end{cases}$

2.

$$\begin{aligned} af_1(t) = bf_2(t) + cf_3(c) &= a\left(1+t+\frac{t^2}{2}+\wp(t^2)\right) \\ &\quad + b\left(1-\frac{t}{2}+\wp(t)\right)\left(\frac{t\sqrt{3}}{2}+\wp(t^2)\right) \\ &\quad + c\left(1-\frac{t}{2}+\frac{t^2}{8}+\wp(t^2)\right)\left(1-\frac{3t^2}{8}+\wp(t^2)\right) \\ &= (a+c) + t\left(a+\frac{b\sqrt{3}}{2}-\frac{c}{2}\right) + t^2\left(\frac{a}{2}-\frac{b\sqrt{3}}{2}-\frac{c}{4}\right)+\wp(t^2) \end{aligned}$$

Par unicité du développement limité,

$$(S): \quad \begin{cases} a+c=0 \\ a+\dfrac{b\sqrt{3}}{2}-\dfrac{c}{2}=0 \\ a-\dfrac{b\sqrt{3}}{2}-\dfrac{c}{2}=0 \end{cases}$$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ 1 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \quad L_3 \leftarrow -L_3 + L_2 \sim \quad \begin{pmatrix} 1 & 0 & 1 \\ 1 & \frac{\sqrt{3}}{2} & \frac{1}{2} \\ 0 & \sqrt{3} & 0 \end{pmatrix}$$

$\mathrm{rg}(A) = 3$ donc $A \in \mathrm{GL}_3(\mathbb{R})$ donc S est de Cramer donc $a=b=c=0$

3.
$$\forall t, |f_2(t)| \leqslant e^{-\frac{t}{2}} \xrightarrow[t\to+\infty]{} 0$$
donc $f_2(t) \xrightarrow[t\to+\infty]{} 0$
De même, $f_3(t) \xrightarrow[t\to+\infty]{} 0$ et $f_1(t) \xrightarrow[t\to+\infty]{} = 0$
Si $a \neq 0$, alors, $0 = af_1(t) + bf_2(t) + cf_3(t) \xrightarrow[n\to+\infty]{} \pm\infty$
Donc $a = 0$.
$$\forall t, b\sin\left(\frac{t\sqrt{3}}{2}\right) + c\cos\left(\frac{t\sqrt{3}}{2}\right) = 0$$
Si $c \neq 0$,
$$\forall t \not\equiv \frac{\pi}{\sqrt{3}}\left[\frac{2\pi}{\sqrt{3}}\right], \frac{b}{c}\tan\left(\frac{t\sqrt{3}}{2}\right) = 1$$
donc $c = 0$ et donc $b = 0$

4. $f_1' = f_1 \in G$
$$\begin{aligned}\forall t, f_2'(t) &= -\frac{1}{2}e^{-\frac{t}{2}}\sin\left(\frac{t\sqrt{3}}{2}\right) + \frac{\sqrt{3}}{2}e^{-\frac{t}{2}}\cos\left(\frac{t\sqrt{3}}{2}\right)\\ &= -\frac{1}{2}f_2(t) + \frac{\sqrt{3}}{2}f_3(t)\end{aligned}$$

donc $f_2' \in \mathrm{Vect}(\mathscr{B}) = G$
$$\forall t, f_3'(t) = -\frac{1}{2}e^{-\frac{t}{2}}\cos\left(\frac{t\sqrt{3}}{2}\right) - \frac{\sqrt{3}}{2}e^{-\frac{t}{2}}\sin\left(\frac{t\sqrt{3}}{2}\right)$$
Soit $f : t \mapsto af_1(t) + bf_2(t) + cf_3(t)$

$$\begin{aligned}f' &= af_1 - \frac{b}{2}f_2 + b\frac{\sqrt{3}}{2}f_3 - \frac{c}{2}f_3 - c\frac{\sqrt{3}}{2}f_2\\ &= af_1 - \left(\frac{b}{2} - \frac{c\sqrt{3}}{2}f_2\right) + \left(\frac{b\sqrt{3}}{2} - \frac{c}{2}\right)f_3 \in G\end{aligned}$$

5. Les coordonnées de f est dans la base $\mathscr{B}$ sont $\left(a, -\frac{b}{2}, -\frac{c\sqrt{3}}{2}, \frac{b\sqrt{3}}{2}, -\frac{c}{2}\right)$
Les coordonnées de f_1 sont $(1, 0, 0)$
Les coordonnées de f_2 sont $\left(0, -\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$
Les coordonnées de f_2 sont $\left(0, \frac{\sqrt{3}}{2}, -\frac{1}{2}\right)$

Partie 2

3. — $0 \in \mathcal{S}$ d'après 2.

— Soient $f, g \in \mathcal{S}$, et $\lambda, \mu \in \mathbb{R}$
$\lambda f + \mu g$ est dérivable 3 fois,

$$\begin{aligned}(\lambda f + \mu g)^{(3)} &= \lambda f^{(3)} + \mu g^{(3)} \\ &= \lambda f + \mu g\end{aligned}$$

donc $\lambda f + \mu g \in \mathcal{S}$
Donc $\mathcal{S}$ est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{R}}$

$f_1' = f_1$ donc $f_1^{(3)} = f_1$ donc $f_1 \in \mathcal{S}$

$$\begin{aligned}f_2' &= -\frac{1}{2}f_2 + \frac{\sqrt{3}}{2}f_3 \\ f_2'' &= -\frac{1}{2}\left(-\frac{1}{2}f_2 + \frac{\sqrt{3}}{2}f_3\right) + \frac{\sqrt{3}}{2\left(-\frac{1}{2}f_3 - \frac{\sqrt{3}}{2}f_2\right)} \\ &= -\frac{1}{2}f_2 - \frac{\sqrt{3}}{2}f_3 \\ f_2^{(3)} &= -\frac{1}{2}\left(-\frac{1}{2}f_2 + \frac{\sqrt{3}}{2}f_3\right) - \frac{\sqrt{3}}{2}\left(-\frac{1}{2}f_3 + \frac{\sqrt{3}}{2}f_2\right) \\ &= f_2\end{aligned}$$

De même, $f_3^{(3)} = f_3$ $\mathcal{S}$ est stable par combinaison linéaire donc

$$G = \text{Vect}(f_1, f_2, f_3) \subset \mathcal{S}$$

4. $g' = f' + f'' + f^{(3)} = f + f' + f'' = g$
5.

$$\begin{aligned}y' - y = 0 &\iff \exists \lambda \in \mathbb{R}, \forall t, y(t) = \lambda e^t \\ &\iff y \in \text{Vect}(f_1)\end{aligned}$$

6. (f_1, f_2) car j et j^2 sont toujours solutions de $1 + z + z^2$
7. $\frac{\lambda}{3}f_1$ est une solution particulière

$$\frac{\lambda}{3}f_1 + \text{Vect}(f_2, f_3)$$

8.

$$\begin{aligned}f \in \mathcal{S} &\implies f + f' + f'' \in \text{Vect}(f_1) \\ &\implies \exists \lambda, f + f' + f'' = \lambda f_1 \\ &\implies \exists (\lambda, a, b), f = \frac{\lambda}{3}f_1 + af_2 + bf_3 \in G\end{aligned}$$

Exercice 12

$$\begin{array}{|c|c|c|}\hline a_{11} & a_{12} & a_{13} \\ \hline a_{21} & a_{22} & a_{23} \\ \hline a_{31} & a_{32} & a_{33} \\ \hline \end{array}$$

$$\underbrace{\frac{S}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{C_1}$$

$$\left.\begin{cases} a_{11}+a_{12}+a_{13}=0 \\ \vdots \\ a_{11}+a_{22}+a_{33}=0 \end{cases}\right\} \begin{array}{l} 8 \text{ équations} \\ 9 \text{ inconnues} \end{array}$$

$$\begin{array}{|c|c|c|}\hline a & -a-b & b \\ \hline b-a & 0 & -b+a \\ \hline -b & a+b & -a \\ \hline \end{array} = a\begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} + b\begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$$

L'ensemble $\mathscr{C}$ des carrés magiques est $\left\{\frac{S}{3}C_1 + aC_2 + bC_3 \mid (a,b,S) \in \mathbb{K}\right\} = \text{Vect}(C_1, C_2, C_3)$.

Montrons que (C_1, C_2, C_3) est libre. Soit $(\lambda, a, b) \in \mathbb{K}^3$

$$\begin{aligned} &\lambda C_1 + aC_2 + bC_3 = 0 \\ &\iff \begin{array}{|c|c|c|}\hline \lambda+a & \lambda-a-b & \lambda+b \\ \hline \lambda+b-a & \lambda & \lambda-b+a \\ \hline \lambda-b & \lambda+a+b & \lambda-a \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 0 & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline \end{array} \\ &\iff \begin{cases} \lambda = 0 \\ a = 0 \\ b = 0 \end{cases} \end{aligned}$$

Chapitre 16

TD 16

Exercice 1

$$\cos\left(\sqrt{x}\right) = 1 - \frac{x}{2} + o(x)$$

Donc, $f : x \mapsto \cos\left(\sqrt{x}\right)$ est dérivable en 0 et $f'(0) = -\dfrac{1}{2}$

Exercice 2

$$\begin{aligned}\frac{xf(a) - af(x)}{x-a} &= \frac{xf(a) - a\big(f(a) + (x-a)f'(a) + o(x-a)\big)}{x-a} \\ &= f(a) - af'(a) + o(1) \\ &\xrightarrow[x\to a]{} f(a) - af'(a)\end{aligned}$$

Exercice 3

Soit $x \geqslant 1$. f est continue sur $[x, x+1]$ et dérivable sur $]x, x+1[$. Donc

$$\exists c \in]x, x+1[, f(x+1) - f(x) = f'(c) < f'(x)$$

De même,

$$\exists d \in]x-1, x[, f(x) - f(x-1) = f'(d) > f'(x)$$

On pose $\ell = \lim\limits_{x\to+\infty} f(x) \in \mathbb{R}$ donc

- $f(x+1) - f(x) \xrightarrow[x\to+\infty]{} \ell - \ell = 0$
- $f(x) - f(x-1) \xrightarrow[x\to+\infty]{} \ell - \ell = 0$

Par encadrement, $f'(x) \xrightarrow[x\to+\infty]{} 0$

Exercice 4

Soit

$$g_M : x \mapsto f(x) - f(a) - \frac{x-a}{2}\big(f'(x) + f'(a)\big) - (x-a)^3 M$$

g_M est continue sur $[a,b]$ et dérivable sur $]a,b[$
$g_M(a) = 0$
$g_M(b) = f(b) - f(a) - \dfrac{b-a}{2}\big(f'(b) - f'(a)\big) - (b-a)^3 M$
On pose $M = \dfrac{1}{(b-a)^3}\left(f(b) - f(a) - \dfrac{b-a}{2}\big(f'(b) + f'(a)\big)\right)$
Ainsi, $g_M(b) = 0$
D'après le théorème de Rolle, il existe $\gamma \in]a,b[$ tel que $g'_M(\gamma) = 0$
D'où,

$$\begin{aligned} 0 &= f'(\gamma) - \frac{1}{2}\big(f'(\gamma) + f'(a)\big) - \frac{\gamma - a}{2} f''(\gamma) - 3(\gamma - a)^2 M \\ &= \frac{1}{2}\big(f'(\gamma) - f'(a)\big) - \frac{\gamma - a}{2} f''(\gamma) - 3(\gamma - a)^2 M \end{aligned}$$

Or,

$$g'_M(a) = 0$$

- g'_M est continue sur $[a,\gamma]$
- g'_M est dérivable sur $]a,\gamma[$
- $g'_M(a) = g'_M(\gamma)$

Donc, il existe $c \in]a,\gamma[\subset]a,b[$ tel que

$$g''_M(c) = 0$$

d'où $M = -\dfrac{1}{12} f^{(3)}(c)$
On en déduit

$$f(b) = f(a) + \frac{b-a}{2}\big(f'(b) + f'(a)\big) - \frac{(b-a)^3}{12} f^{(3)}(c)$$

Exercice 5

1. On pose $\varepsilon_1 = \dfrac{1}{2}\big(z - f'(a)\big) > 0$.
   Il existe $\eta_1 > 0$ tel que

   $$\forall k \in]-\eta_1, \eta_1[\setminus\{0\}, a + h \in I, \left|\frac{f(a+h) - f(a)}{h} - f'(a)\right| \leqslant \varepsilon_1$$

   En particulier,

   $$\forall kh \in]0, \eta_1[, \frac{f(a+h) - f(a)}{h} \leqslant f'(a) + \varepsilon_1 < z$$

De même, il existe $\eta_2 > 0$ tel que

$$\forall h \in]0, \eta_2[, \left| \frac{f(b+h) - f(b)}{h} - f'(b) \right| \leqslant \varepsilon_2 = \frac{1}{2}\big(f'(b) - z\big)$$

donc

$$\forall h \in]0, \eta_2[, \frac{f(b+h) - f(b)}{h} \geqslant f'(b) - \varepsilon_2 > z$$

On pose $\eta = \min(\eta_1, \eta_2) > 0$,

$$\forall h \in]0, \eta[, \frac{f(a+h) - f(a)}{h} < z < \frac{f(b+h) - f(b)}{h}$$

2. On fixe $h \in]0, \eta[$ et $g_h : x \mapsto \dfrac{f(x+h) - f(x)}{h}$
g_h est continue sur son domaine de définition, et d'après 1.,

$$g_h(a) < z < g_h(b)$$

D'après le théorème des valeurs intermédiaires, il existe $y \in I$ tel que $y + h \in I$ et $z = g_h(y) = \dfrac{f(y+h) - f(y)}{h}$
D'après le théorème des accroissements finis,

$$\exists x \in]y, y+h[, f'(x) = \frac{f(y+h) - f(y)}{h} = z$$

Exercice 7

de la solution

$$f(2x) = f(x) + ax + \mathrm{o}(x)$$

$$\begin{aligned} f(x) \xleftarrow[n\to+\infty]{} f(x) &= f\left(\frac{x}{2}\right) a\frac{x}{2} + \mathrm{o}(x) \\ &= f\left(\frac{x}{4}\right) + a\frac{x}{2} + a\frac{x}{4} + \mathrm{o}(x) \\ &= f\left(\frac{x}{2^n}\right) + a\sum_{k=1}^{n} \frac{x}{2^k} + \mathrm{o}(x) \\ &\xrightarrow[n\to+\infty]{} f(0) + ax + \mathrm{o}(x) \end{aligned}$$

ion

Donc, $f(x) = f(0) + ax + \mathrm{o}(x)$

$\varepsilon(x) \to 0$

$$f(2x) = f(x) + ax + x\varepsilon(x)$$

$$\begin{aligned} f(x) \xleftarrow[n\to+\infty]{} f(x) &= f\left(\frac{x}{2}\right) a\frac{x}{2} + \frac{x}{2}\varepsilon\left(\frac{x}{2}\right) \\ &= f\left(\frac{x}{4}\right) + a\frac{x}{2} + a\frac{x}{4} + \frac{x}{4}\varepsilon\left(\frac{x}{4}\right) + \frac{x}{2}\varepsilon\left(\frac{x}{2}\right) \\ &= f\left(\frac{x}{2^n}\right) + a\sum_{k=1}^{n} \frac{x}{2^k} + \underbrace{x\sum_{k=1}^{n} \frac{1}{2^k}\varepsilon\left(\frac{x}{2^k}\right)}_{\xrightarrow[n\to+\infty]{} ?} \\ &\xrightarrow[n\to+\infty]{} f(0) + ax + ? \end{aligned}$$

On pose

$$\forall x > 0, \varepsilon(x) = \frac{f(2x) - f(x)}{x} - a$$

D'après l'énoncé, $\varepsilon(x) \xrightarrow[\substack{x\to 0\\ >}]{} $ et

$$(\mathscr{E}) : \quad \forall x > 0, f(2x) = f(x) + ax + x\varepsilon(x)$$

On en déduit par récurrence que

$$\forall n \in \mathbb{N}_\star, P(n) \text{ est vraie, avec}$$

$$P(n) : \text{“}\forall x > 0, f(x) = f\left(\frac{x}{2^n}\right) + ax\sum_{k=1}^{n}\frac{1}{2^k} + x\sum_{k=1}^{n}\frac{1}{2^k}\varepsilon\left(\frac{x}{2^k}\right)\text{”}$$

— D'après $(\mathscr{E})$,

$$\forall x > 0, f(x) = f\left(\frac{x}{2}\right) + \frac{ax}{2} + \frac{x}{2}\varepsilon\left(\frac{x}{2}\right)$$

donc $P(1)$ est vraie

— Soit $n \in \mathbb{N}_\star$. On suppose $P(n)$ vraie.

$$\begin{aligned}
\forall x > 0, f(x) &= f\left(\frac{x}{2^n}\right) + ax\sum_{k=1}^{n}\frac{1}{2^k} + x\sum_{k=1}^{n}\frac{1}{2^k}\varepsilon\left(\frac{x}{2^k}\right)\\
&= f\left(\frac{x}{2^{n+1}}\right) + a\frac{x}{2^{n+1}} + \frac{x}{2^{n+1}}\varepsilon\left(\frac{x}{2^{n+1}}\right)\\
&+ ax\sum_{k=1}^{n}\frac{1}{2^k} + x\sum_{k=1}^{n}\frac{1}{2^k}\varepsilon\left(\frac{x}{2^k}\right)\\
&= f\left(\frac{x}{2^{n+1}}\right) + ax\sum_{k=1}^{n+1}\frac{1}{2^k} + x\sum_{k=1}^{n+1}\frac{1}{2^k}\varepsilon\left(\frac{x}{2^k}\right)
\end{aligned}$$

Donc, $P(n+1)$ est vraie

On fixe $x > 0$.

$$f\left(\frac{x}{2^n}\right) \xrightarrow[n\to+\infty]{} f(0) \text{ car } f \text{ est continue en } 0$$

$$\forall n \in \mathbb{N}_\star, \sum_{k=1}^{n}\frac{1}{2^k} = \frac{1}{2} \times \frac{1 - \left(\frac{1}{2}\right)^n}{1 - \frac{1}{2}} \qquad = 1 - \frac{1}{2^n} \xrightarrow[n\to+\infty]{} 1$$

Comme $\lim\limits_{\substack{x\to 0\\ >}} \varepsilon(x)0$, on sait que

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in]0, \eta[, |\varepsilon(x)| \leqslant \varepsilon$$

Soit $\varepsilon > 0$. On considère $\eta > 0$ tel que

$$\forall x \in]0, \eta[, |\varepsilon(x)| \leqslant \varepsilon$$

Soit $x \in]0, \eta[$.

$$\forall k \in \mathbb{N}, \frac{x}{2^k} \leqslant x$$

donc

$$\forall k \in \mathbb{N}, \frac{x}{2^k} \in]0, \eta[$$

donc

$$\forall x \in \mathbb{N}, \left|\varepsilon\left(\frac{x}{2}\right)\right| \leqslant \varepsilon$$

Donc

$$\begin{aligned}\forall n \in \mathbb{N}_\star, \left|\sum_{k=1}^{n} \frac{1}{2^k}\varepsilon\left(\frac{x}{2^k}\right)\right| &\leqslant \sum_{k=1}^{n} \frac{1}{2^k}\left|\varepsilon\left(\frac{x}{2^k}\right)\right| \\ &\leqslant \sum_{k=1}^{n} \frac{1}{2^k}\varepsilon \\ &\leqslant \left(1 - \frac{1}{2^n}\right)\varepsilon \\ &\leqslant \varepsilon\end{aligned}$$

De plus, pour tout $x > 0$, il existe $N'_x \in \mathbb{N}_\star$ tel que

$$\forall n \in \mathbb{N}'_\star, \left|f\left(\frac{x}{2^n}\right) - f(0)\right| \leqslant \varepsilon x$$

et il existe $N_x \in \mathbb{N}_\star$ tel que

$$\forall n \geqslant N_x, \left|a\sum_{k=1}^{n} \frac{1}{2^k} - a\right| \leqslant \varepsilon$$

donc

$$\forall n \geqslant N, ax - \varepsilon x \leqslant ax\sum_{k=1}^{n} \frac{1}{2^k} \leqslant ax + \varepsilon x$$

$$\begin{aligned}\forall x \in]0, \eta''[, \forall n \geqslant \max(N, N'_x), \\ f(0) - \varepsilon x + ax - \varepsilon x - \varepsilon x \leqslant f(x) \leqslant f(0) + \varepsilon x + ax + \varepsilon x + \varepsilon x\end{aligned}$$

donc

$$-3\varepsilon \leqslant \frac{f(x) - f(0)}{x} - a \leqslant 3\varepsilon$$

Donc $\lim\limits_{\substack{x \to 0 \\ >}} \dfrac{f(x) - f(0)}{x} - a = 0$ et donc f est dérivable à droite en 0 et $f'(0) = a$

Chapitre 17

TD 17

Exercice 4

$E = \mathbb{R}^4$
$a = (0, 1, -1, 2)$
$b = (1, 3, 0, 2)$
$c = (2, 1, -3, 4)$
$d = (0, 0, 2, 1)$
$e = (-1, 1, 0, 3)$

$F = \text{Vect}(a, b, c)$ et $G = \text{Vect}(d, e)$

Soient $(\lambda, \mu, \nu) \in \mathbb{R}^3$.

$$\lambda a + \mu b + \nu c = 0 \iff \begin{cases} \mu + 2\nu = 0 \\ \lambda + 3\mu + \nu = 0 \\ -\lambda - 3\nu = 0 \\ 2\lambda + 2\mu + 4\nu = 0 \end{cases}$$

$$\iff \begin{cases} \mu = -2\nu \\ \lambda = -3\nu \\ -8\nu = 0 \\ -6\nu = 0 \end{cases}$$

$$\iff \begin{cases} \nu = 0 \\ \lambda = 0 \\ \mu = 0 \end{cases}$$

Donc (a, b, c) est libre et donc (a, b, c) est une base de F. Donc, $\boxed{\dim(F) = 3}$

d, e ne sont pas colinéaires donc (d,e) est une base de G. Donc, $\boxed{\dim(G)=2}$

$F+G=\text{Vect}(a,b,c,d,e)$

MÉTHODE 1 Soient $\lambda,\mu,\nu,\alpha,\beta\in\mathbb{R}$.

$$\lambda a+\mu b+\nu c+\alpha d+\beta e=0 \iff \begin{cases}\boxed{\mu}+2\nu-\beta=0\\ \lambda+3\mu+\nu+\beta=0\\ -\lambda-3\nu+2\alpha=0\\ 2\lambda+2\mu+4\nu+\alpha+3\beta=0\end{cases}$$

$$\begin{matrix}\iff\\ L_2\leftarrow L_2-3L_1\\ L_4\leftarrow L_4-2L_1\end{matrix}\begin{cases}\boxed{\mu}+2\nu-\beta=0\\ \lambda-5\nu+4\beta=0\\ -\lambda-3\nu+2\alpha=0\\ 2\lambda+\boxed{\alpha}+5\beta=0\end{cases}$$

$$\begin{matrix}\iff\\ L_3\leftarrow L_3-2L_4\end{matrix}\begin{cases}\boxed{\mu}+2\nu-\beta=0\\ \boxed{\lambda}-5\nu+4\beta=0\\ -5\lambda-3\nu-10\beta=0\\ 2\lambda+\boxed{\alpha}+5\beta=0\end{cases}$$

$$\begin{matrix}\iff\\ L_3\leftarrow L_3+5L_2\\ L_4\leftarrow L_4-2L_2\end{matrix}\begin{cases}\boxed{\mu}+2\nu-\beta=0\\ \boxed{\lambda}-5\nu+4\beta=0\\ -28\nu+\boxed{10\beta}=0\\ \boxed{\alpha}+10\nu-3\beta=0\end{cases}$$

$$\iff\begin{cases}\beta=\dfrac{28}{10}\nu\\ \mu=\cdots\\ \lambda=\cdots\\ \alpha=\cdots\end{cases}$$

Avec $\nu=1$, on a $\lambda a+\mu b+c+\alpha d+\beta e=0$ et donc $c=-\lambda a-\mu b-\alpha d-\beta e$ donc $c\in\text{Vect}(a,b,d,e)$
Avec $\nu=0$, on a $\lambda a+\mu b+\alpha d+\beta e=0 \iff \beta=\mu=\lambda=\alpha=0$ et docnc (a,b,d,e) est libre.
Donc, (a,b,d,e) est une base de $F+G$ et donc $\boxed{\dim(F+G)=4}$ (donc $F+G=\mathbb{R}^4$
D'après la formule de Grassmann,

$$\boxed{\dim(F\cap G)=3+2-4=1}$$

MÉTHODE 2 $\dim(F+G)=\text{rg}(a,b,c,d,e)$

$$M=\begin{pmatrix}0&1&2&0&-1\\ \boxed{1}&3&1&0&1\\ -1&0&-3&2&0\\ 2&2&4&1&3\end{pmatrix}$$

$$\mathrm{rg}(a,b,c,d,e) = \mathrm{rg}(M)$$

$$M \begin{array}{c} \sim \\ C_2 \leftarrow C_2 - 3C_1 \\ C_3 \leftarrow C_3 - C_1 \\ C_5 \leftarrow C_5 - C_1 \end{array} \begin{pmatrix} 0 & 1 & 2 & 0 & -1 \\ \boxed{1} & 0 & 0 & 0 & 0 \\ -1 & 2 & -2 & 2 & \boxed{1} \\ 2 & -4 & 2 & 1 & 1 \end{pmatrix}$$

$$\begin{array}{c} \sim \\ C_2 \leftarrow C_2 - 3C_5 \\ C_3 \leftarrow C_3 + 2C_5 \\ C_4 \leftarrow C_4 + 2C_5 \end{array} \begin{pmatrix} 0 & 4 & 0 & -2 & 1 \\ \boxed{1} & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & \boxed{1} \\ 2 & -7 & 4 & \boxed{1} & 1 \end{pmatrix}$$

$$\begin{array}{c} \sim \\ C_2 \leftarrow C_2 + 7C_4 \\ C_3 \leftarrow C_3 - 4C_4 \end{array} \begin{pmatrix} 0 & -10 & \boxed{8} & -2 & -1 \\ \boxed{1} & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & \boxed{1} \\ 2 & 0 & 0 & \boxed{1} & 1 \end{pmatrix}$$

Donc $\mathrm{rg}(M) = 4$

$$\boxed{\begin{array}{c} \dim(F+G) = 4 \\ \dim(F \cap G) = 1 \end{array}}$$

MÉTHODE 3 $F + G \subset R^4$ donc $\dim(F+G) \leqslant 4$
$F \subset F + G$ donc $\dim(F+G) \geqslant 3$
Donc $\dim(F+G) \in \{3, 4\}$

On suppose $\dim(F+G) = 3$. Alors $F = F + G$. Or, $G \subset F + G = F$
On va caractériser F par un système d'équations.

Soit $u = (x, y, z, t) \in \mathbb{R}^4$

$$
\begin{aligned}
u \in F &\iff \exists (\lambda, \mu, \nu) \in \mathbb{R}^3, u = \lambda a + \mu b + \nu c \\
&\iff \exists (\lambda, \mu, \nu) \in \mathbb{R}^3 \begin{cases} x = \mu + 2\nu \\ y = \boxed{\lambda} + 3\mu + \nu \\ z = -\lambda - 3\nu \\ t = 2\lambda + 2\mu + 4\nu \end{cases} \\
&\underset{\substack{L_3 \leftarrow L_3 + L_2 \\ L_4 \leftarrow L_4 - 2L_2}}{\iff} \exists (\lambda, \mu, \nu) \in \mathbb{R}^3, \begin{cases} \boxed{\mu} + 2\nu = x \\ \boxed{\lambda} + 3\mu + \nu = y \\ 3\mu - 2\nu = y + z \\ -4\mu + 2\nu = t - 2y \end{cases} \\
&\underset{\substack{L_2 \leftarrow L_2 - 3L_1 \\ L_3 \leftarrow L_3 - 3L_1 \\ L_4 \leftarrow \dfrac{L_4 + 4L_2}{10}}}{\iff} \exists (\lambda, \mu, \nu) \in \mathbb{R}^3, \begin{cases} \boxed{\mu} + 2\nu = x \\ \boxed{\lambda} - 5\nu = y - 3x \\ -8\nu = y + z - 3x \\ \boxed{\nu} = \dfrac{t - 2y + 4x}{10} \end{cases} \\
&\underset{L_3 \leftarrow L_3 + 8L_4}{\iff} \exists (\lambda, \mu, \nu) \in \mathbb{R}^3, \begin{cases} \mu = \cdots \\ \lambda = \cdots \\ 0 = \dfrac{1}{5}x - \dfrac{3}{5}y + z + \dfrac{16}{5}t \\ \nu = \cdots \end{cases} \\
&\iff x + 3y + 5z + 16t = 0
\end{aligned}
$$

$$(x, y, z, t) \in F \iff x - 3y + 5z + 16t = 0$$

Or, $0 - 3 \times 0 + 5 \times 2 + 16 = 26 \neq 0$ donc $d \notin F$ ↯
Donc $\dim(F + G) = 4$ et domc $\dim(F \cap G) = 1$

MÉTHODE 4 On caractérise F et G par des équations. On reprend les calculs de la méthode 3.

$$(x, y, z, t) \in F \iff x - 3y + 5z + 16t = 0$$

$$
\begin{aligned}
(x,y,z,t)\in G &\iff \exists(\alpha,\beta)\in\mathbb{R}^2,(x,y,z,t)=\alpha d+\beta e\\
&\iff \exists(\alpha,\beta)\in\mathbb{R}^2,\begin{cases}-\beta=x\\ \beta=y\\ 2\alpha=z\\ \alpha+3\beta=t\end{cases}\\
&\iff \exists(\alpha,\beta)\in\mathbb{R}^2,\begin{cases}\alpha=\dfrac{1}{2}z\\ \beta=y\\ x+y=0\\ \dfrac{1}{2}z+3y=t\end{cases}\\
&\iff \begin{cases}x+y=0\\ z+6y-2t=0\end{cases}
\end{aligned}
$$

$$
\begin{aligned}
(x,y,z,t)\in F\cap G &\iff \begin{cases}x-3y+5z+16t=0\\ \boxed{x}+y=0\\ z+6y-2t=0\end{cases}\\
&\underset{L_1\leftarrow L_1-L_2}{\iff} \begin{cases}-4y+5z+16t=0\\ \boxed{x}+y=0\\ \boxed{z}+6y-2t=0\end{cases}\\
&\underset{L_1\leftarrow \frac{L_1-5L_3}{26}}{\iff} \begin{cases}-\dfrac{34}{26}y+t=0\\ \boxed{x}+y=0\\ \boxed{z}+6y-2t=0\end{cases}\\
&\underset{L_3\leftarrow L_3+2L_1}{\iff} \begin{cases}t=\dfrac{17}{13}y\\ x=-y\\ z=-\dfrac{44}{13}y\end{cases}\\
&\iff (x,y,z,t)=\left(-y,y,-\frac{44}{13}y,\frac{17}{13}\right)\\
&\iff (x,y,z,t)=\frac{y}{13}(-13,13,-44,17)
\end{aligned}
$$

Donc, $F\cap G=\text{Vect}((-13,13,-44,17))$ donc $\dim(F\cap G)=1$
Et donc, $\dim(F+G)=4$

Exercice 5

1. — On pose $G = \text{Vect}(e_1, \dots, e_k)$. On sait que $F \oplus G = E$
Soit $x \in F \cap G_a$. On considère $(\lambda_1, \dots, \lambda_k) \in \mathbb{K}^k$ tel que

$$\begin{aligned} x &= \sum_{i=1}^{k} \lambda_i (a + e_i) \\ &= \left(\sum_{i=1}^{k} \lambda_i \right) a + \sum_{i=1}^{k} \lambda_i e_i \end{aligned}$$

D'où,

$$\underbrace{x - \left(\sum_{i=1}^{k} \lambda_i \right) a}_{\in F} = \underbrace{\sum_{i=1}^{k} \lambda_i e_i}_{\in G}$$

Or, $F \cap G = \{0\}$ Donc $\sum_{i=1}^{k} \lambda_i e_i = 0$
Comme $(e_1, \dots, e_k)$ est libre,

$$\forall i \in [\![1, k]\!], \lambda_i = 0$$

Donc, $x = \sum_{i=1}^{k} \lambda_i (a + e_i) = 0$
On a prouvé que $F \cap G_a = \{0\}$.
— $(e_1, \dots, e_k)$ est une base de G donc $\dim(G) = k$, donc $\dim(F) = \dim(E) - k$
— Soitent $(\lambda_1, \dots, \lambda_k) \in K^k$. On suppose que

$$\sum_{i=1}^{k} \lambda_i (a + e_i) = 0$$

D'où,

$$\underbrace{\left(\sum_{i=1}^{k} \lambda_i \right) a}_{\in F} = \underbrace{-\sum_{i=1}^{k} \lambda_i e_i}_{\in G}$$

Donc,

$$\sum_{i=1}^{k} \lambda_i e_i \in F \cap G = \{0\}$$

donc

$$\forall i \in [\![1, k]\!], \lambda_i = 0$$

Donc $(a + e_1, \dots, a + e_k)$ est libre, c'est donc une base de G_a, donc

$$\dim(G_a) = k$$

D'où,

$$\dim(F) + \dim(G_a) = \dim(E) - k + k = \dim(E)$$

Ainsi,

$$F \oplus G_a = E$$

2. On suppose K infini. Dans ce cas, F contient une infinité de vecteurs.
Soient $a, b \in F$ avec $a \neq b$ et $a \neq 0$. Montrons que $G_a \neq G_b$.
Soit $x \in G_a \cap G_b$ donc

$$\begin{aligned} x &= \sum_{i=1}^{k} \mu_i (a + e_i) \\ &= \sum_{i=1}^{k} \lambda_i (b + e_i) \end{aligned}$$

D'où,

$$\underbrace{\left(\sum_{i=1}^{k} \mu_i\right) a - \left(\sum_{i=1}^{k} \lambda_i\right) b}_{\in F} = \underbrace{\sum_{i=1}^{k} (\lambda_i - \mu_i) e_i}_{\in G}$$

Donc,

$$\begin{cases} \left(\sum_{i=1}^{k} \mu_i\right) a = \left(\sum_{i=1}^{k} \lambda_i\right) b \\ \sum_{i=1}^{k} (\lambda_i - \mu_i) e_i = 0 \end{cases}$$

Donc,

$$a = b \text{ ou } \sum_{i=1}^{k} \lambda_i = 0 \forall i \in [\![1, k]\!], \lambda_i = \mu_i$$

Or, $a \neq b$, donc $\sum_{i=1}^{k} \lambda_i = 0$ donc $x \in G$
Si $G_a = G_b$, alors

$$G_a = G_a \cap G_b \subset G$$

donc

$$G_a = G$$

Or,

$$\sum_{i=1}^{k} (a + e_i) \in G_a \setminus G$$

En effet, si $\sum_{i=1}^{k} (a + e_i) = y \in G$, alors

$$\underbrace{ka}_{\in F} = \underbrace{g - \sum_{i=1}^{k} e_i}_{\in G}$$

donc $ka = 0$ Or $l \neq 0$ et $a \neq 0$.

Exercice 6

Soient $\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5 \in \mathbb{R}$. On suppose

$$\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 + \lambda_4 f_4 + \lambda_5 f_5 = 0$$

$$\forall x > 0, f(x) = \lambda_1 \ln x + \lambda_2 x + \lambda_3 e^x + \lambda_4 e^{x+3} + \lambda_5 \frac{1}{x} = 0$$

Si $\lambda_5 \neq 0$, alors $f(x) \sim_{x\to 0^+} \dfrac{\lambda_5}{x} \xrightarrow[x\to 0^+]{} \pm\infty$ ↯

Donc $\boxed{\lambda_5 = 0}$

Si $\lambda_1 \neq 0$, alors $f(x) \sim_{x\to 0^+} \lambda_1 \ln(x) \xrightarrow[x\to 0^+]{} \pm\infty$ ↯

Donc $\boxed{\lambda_1 = 0}$

Si $\lambda_3 + e^3\lambda_4 \neq 0$, alors $f(x) \sim_{x\to+\infty} \left(\lambda_3 + e^3\lambda_4\right) e^x \xrightarrow[x\to+\infty]{} \pm\infty$

Donc $\boxed{\lambda_3 + e^3\lambda_4 = 0}$

D'où,

$$\forall x > 0, \lambda_2 x = 0$$

donc $\boxed{\lambda_2 = 0}$

$f_4 = e^3 f_3$ donc $(f_1, f_2, f_3, f_4, f_5)$ n'est pas libre
Mais, (f_1, f_2, f_3, f_5) est libre $(\lambda_4 = 0)$

Exercice 7

F et G deux hyperplans

$F \cap G \subset F$ donc $\dim(F \cap G) \leqslant n - 1$

$$\begin{aligned} \dim(F \cap G) = n - 1 &\iff F \cap G = F \\ &\iff F \subset G \\ &\iff F = G \end{aligned}$$

$$\dim(F \cap G) = \dim(F) + \dim(G) - \dim(F+G)$$

$$\begin{aligned} & F + G \subset \mathbb{R}^n \\ \text{donc } & \dim(F+G) \leqslant n \\ \text{donc } & -\dim(F+G) \geqslant -n \\ \text{donc } & \dim(F \cap G) \geqslant 2(n-1) - n = n-2 \end{aligned}$$

Si $F = G$, alors $\dim(F \cap G) = n - 1$
Si $F \neq G$, alors $\dim(F \cap G) = n - 2$

Exercice 8

" $\Longleftarrow$ " Soient F, G, U tels que

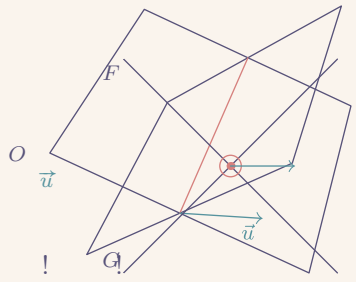
$$F \oplus U = E = G \oplus U$$

Donc,

$$\begin{aligned} \dim(F) + \dim(U) &= \dim(E) \\ \dim(G) + \dim(U) &= \dim(E) \end{aligned}$$

Donc, $\dim(F) = \dim(G)$

" $\Longrightarrow$ "



On raisonne par récurrence sur la $\text{codim}(F) = \dim(E) - \dim(F)$

— Soient F et G deux hyperplans de E
$F \cup G \neq E$ d'après l'exercice classique suivant :

$$F \cup G \text{ sous-espace vectoriel de } E \iff F \subset G \text{ ou } G \subset F$$

Solution de l'exercice :

" $\Longleftarrow$ "

$$\begin{aligned} F \subset G &\implies F \cup G = G \\ G \subset F &\implies F \cup G = F \end{aligned}$$

" $\Longrightarrow$ " On suppose $G \not\subset F$. Soit $u \in F$. Soit $v \in G \setminus F$.
$u+v \in F \cup G$ car $F \cup G$ est un sous-espace vectoriel de E.
Si $u+v \in F$, alors $v = \underbrace{u+v}_{\in F} - \underbrace{u}_{\in F} \in F$ ↯
Si $u+v \in G$, alors $u = \underbrace{u+v}_{\in G} - \underbrace{v}_{\in G} \in G$ ↯
Donc $F \subset G$

Soit $u \in E \setminus (F \cup G)$. $u \neq 0$ donc $\langle u \rangle$ est de dimension 1. $\langle u \rangle \cap F = \{0\}$ donc $F \oplus \langle u \rangle = E$
$\langle u \rangle \cap G = \{0\}$ donc $G \oplus \langle u \rangle = E$

— Soit $n \in \mathbb{N}_\star$ tels que pour tous F et G sous-espaces vectoriels de E de codimension n, F et G ont un supplémentaire commun.
Soient F et G de codimension $n+1$. De nouveau, $F \cup G \neq E$. Soit $u \in E \setminus (F \cup G)$. $\langle u \rangle \cap F = \{0\}$. On pose $F' = F \oplus \langle u \rangle$.
$\dim(F') = \dim(F) + 1$ donc $\operatorname{codim}(F') = n$
De même, $\langle u \rangle \cap G = \{0\}$. On pose $G' = G \oplus \langle u \rangle$ donc $\operatorname{codim}(G') = n$
Soit U un supplémentaire commun à F' et G'. On pose $U' = \langle u \rangle \oplus U$

$$\begin{aligned} E &= F' \oplus U \\ &= F \oplus \langle u \rangle \oplus U \\ &= F \oplus U' \end{aligned}$$

$$\begin{aligned} E &= G' \oplus U \\ &= G \oplus \langle u \rangle \oplus U \\ &= G \oplus U' \end{aligned}$$

Exercice 9

Soit $u \in E$.

$$\forall n, u_n = u_r \text{ où } r \text{ est le reste de la division de } n \text{ par } p$$

$$\begin{aligned} (u_n) &= (u_0, u_1, \ldots, u_{p-1}, u_0, u_1, \ldots, u_{p-1}, u_0, u_1, \ldots) \\ &= u_0(1, 0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots) \\ &+ u_1(0, 1, \ldots, 0, 0, 1, \ldots, 0, 0, 1, \ldots) \\ &\vdots \\ &+ u_{p-1}(0, 0, \ldots, 1, 0, 0, \ldots, 1, 0, 0, \ldots) \end{aligned}$$

$$\forall k \in [\![0, p-1]\!], v_k = (v_{k,n}) \text{ où } \forall n, v_{k,n} = \begin{cases} 1 & \text{si } n \equiv k \ [p] \\ 0 & \text{sinon} \end{cases}$$

On vient de montrer que

$$E \subset \text{Vect}(v_0, v_1, \dots, \vee_{p-1})$$

Or,

$$\forall k \in [\![0, p-1]\!], v_k \in E$$

car

$$\begin{aligned}\forall k \in [\![0, p-1]\!], \forall n \in \mathbb{N}, v_{k,n+p} &= \begin{cases} 1 & \text{si } p+n \equiv k \ [p] \\ 0 & \text{sinon} \end{cases} \\ &= \begin{cases} 1 & \text{si } n \equiv k \ [p] \\ 0 & \text{sinon} \end{cases} \\ &= v_{k,n}\end{aligned}$$

Donc $E = \text{Vect}(v_0, \dots, v_{p-1})$

Donc $\begin{cases} E \text{ sous-espace vectoriel de } \mathbb{C}^{\mathbb{N}} \\ \dim(E) \leqslant p \end{cases}$

Soit $q \in \mathbb{C} \setminus \{0\}$

$$\begin{aligned}\forall n \in \mathbb{N}, & q^{n+p} = q^n q^p = q^n \\ &\iff q^p = 1 \\ &\iff \exists k \in [\![0, p-1]\!], q = e^{\frac{2ik\pi}{p}}\end{aligned}$$

On pose

$$\forall k \in [\![0, p-1]\!], w_k = \left(e^{\frac{2ik\pi n}{p}}\right)_{n \in \mathbb{N}}$$

Montrons que $(w_0, \dots, w_{p-1})$ est libre.
Soient $(\lambda_0, \dots, \lambda_{p-1}) \in \mathbb{C}^p$. On suppose

$$\forall n \in \mathbb{N}, \sum_{k=0}^{p-1} \lambda_k e^{\frac{2ik\pi n}{p}} = 0$$

On pose

$$P(X) = \sum_{k=0}^{p-1} \lambda_k X^k \qquad \deg(P) \leqslant p-1$$

On a donc

$$\forall n \in \mathbb{N}, P\left(e^{\frac{2i\pi n}{p}}\right) = 0$$

donc P a au moins p racines : $1, e^{\frac{2i\pi}{p}}, e^{\frac{4i\pi}{p}}, \dots, e^{\frac{2i(p-1)\pi}{p}}$
Donc $P = 0$, donc $\forall k \in [\![0, p-1]\!], \lambda_k = 0$
Donc $(w_0, \dots, w_{p-1})$ est libre donc $\dim(E) \geqslant p$
Donc $\dim(E) = p$
Donc $(w_0, \dots, w_{p-1})$ est une base de E.

Chapitre 18

TD 18

Exercice 1

$$\begin{cases} P = (X-a)(X-b)Q + R \\ \deg R < 2 \end{cases}$$

Donc, $R = \alpha X + \beta$ avec $\alpha, \beta \in \mathbb{K}$.

$$\begin{cases} P(a) = R(a) = \alpha a + \beta \\ P(b) = R(b) = \alpha b + \beta \end{cases}$$

$$\begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} P(a) \\ P(b) \end{pmatrix}$$

On a

$$\begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix}^{-1} = \frac{1}{a-b} \begin{pmatrix} 1 & -1 \\ -b & a \end{pmatrix}$$

Donc,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{a-b} \begin{pmatrix} P(a) - P(b) \\ -bP(a) + aP(b) \end{pmatrix}$$

Exercice 2

1.

$$\begin{aligned} z^4 + 1 = 0 &\iff z^4 = -1 = e^{i\pi} \\ &\iff z \in \left\{ e^{\frac{i\pi}{4}}, e^{\frac{3i\pi}{4}}, e^{\frac{5i\pi}{4}}, e^{\frac{7i\pi}{4}} \right\} \end{aligned}$$

Dans $\mathbb{C}[X]$,

$$\begin{aligned}X^4-1 &= \left(X-e^{\frac{i\pi}{4}}\right)\left(X-e^{\frac{3i\pi}{4}}\right)\left(X-e^{\frac{5i\pi}{4}}\right)\left(X-e^{\frac{7i\pi}{4}}\right)\\ &= \left(X-e^{\frac{i\pi}{4}}\right)\left(X-e^{\frac{7i\pi}{4}}\left(X-e^{\frac{3i\pi}{4}}\right)\left(X-e^{\frac{5i\pi}{4}}\right)\right)\\ &= \left(X^2-2\cos\left(\frac{\pi}{4}\right)X+1\right)\left(X^2-2\cos\left(\frac{3\pi}{4}\right)X+1\right)\\ &= \left(X^2-\sqrt{X}X+1\right)\left(X^2+\sqrt{2}X+1\right)\in\mathbb{R}[X]\end{aligned}$$

2. $P=\left(X^2-X+1\right)^2+1$

$$\begin{aligned}\left(z^2-z+1\right)^2+1=0 &\iff \left(z^2-z+1\right)^2=-1\\ &\iff z^2-z+1=i \text{ ou } z^2-z+1=-i\\ &\iff z=\frac{1\pm(1+2i)}{2} \text{ ou } z=\frac{1\pm(1-2i)}{2}\end{aligned}$$

Dans $\mathbb{C}$,

$$\begin{aligned}P &= \big(X-(1+i)\big)\big(X-(-i)\big)\big(X-(1-i)\big)\big(X-i\big)\\ &= \left(X^2-2X+2\right)\left(X^2+1\right)\in\mathbb{R}[X]\end{aligned}$$

Exercice 4

$$A=\prod_{i=1}^{r}P_i \qquad P_i \text{ irreductible}$$
$$B=\prod_{j=1}^{\delta}Q_i \qquad Q_i \text{ irreductible}$$

donc

$$A^2=\prod_{i=1}^{r}P_i^2$$
$$B^2=\prod_{j=1}^{\delta}Q_i^2$$

$$\begin{aligned}A^2 \mid B^2 &\iff \forall i\in[\![1,r]\!],\exists j\in[\![1,\delta]\!],P_i=P_j\\ &\iff A\mid b\end{aligned}$$

Exercice 5

$$\begin{aligned} z^{2n} - 2\cos(na)z^n + 1 = 0 &\iff z^n = e^{\pm ina} \\ &\iff z \in \left\{e^{ia} \times e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!]\right\} \cup \left\{e^{-ia} \times e^{\frac{2ik\pi}{n}} \mid k \in [\![-(n-1), 0]\!]\right\} \end{aligned}$$

$$\begin{aligned} X^{2n} - 2\cos(na)X^n + 1 &= \prod_{k=0}^{n-1} \left(X - e^{i\left(a + \frac{2k\pi}{n}\right)}\right) \prod_{k=0}^{n-1} \left(X - e^{i\left(-a + \frac{2k\pi}{n}\right)}\right) \\ &= \prod_{k=0}^{n-1} \left(X^2 - 2\cos\left(a + \frac{2k\pi}{n}\right) X + 1\right) \end{aligned}$$

Exercice 7

$$\begin{aligned} f : \mathbb{K}_n[X] &\longrightarrow \mathbb{K}_n[X] \\ P &\longmapsto P - P' \end{aligned}$$

f est linéaire

$$\begin{aligned} P \in \mathrm{Ker}(f) &\iff P - P' = 0 \\ &\iff P = 0 \end{aligned}$$

Donc $f \in \mathrm{GL}\big(\mathbb{K}_n[X]\big)$ et $P_n = f^{-1}(X^n)$

$$P_n = \sum_{k=0}^{n} \alpha_k X^k$$

$$P_n' = \sum_{k=1}^{n} k\alpha_k X^{k-1} = \sum_{k=0}^{n-1} (k+1)\alpha_{k+1} X^k$$

$$P_n - P_n' = \alpha_n X^n + \sum_{k=0}^{n-1} \big(\alpha_k - (k+1)\alpha_{l+1}\big) X^k$$

$$\begin{cases} \alpha_n = 1 \\ \forall k \in [\![0, n-1]\!], \alpha_k = (k+1)\alpha_{k+1} \end{cases}$$

$$\alpha_n = 1 = \frac{n!}{n!}$$
$$\alpha_{n-1} = n\alpha_n = n = \frac{n!}{(n-1)!}$$
$$\alpha_{n-2} = (n-1)\alpha_{n-1} = (n-1)n = \frac{n!}{(n-2)!}$$

Preuve par récurrence :

$$\alpha_{n-k} = \frac{n!}{(n-k)!}$$

Donc,

$$P_n = \sum_{k=0}^{n} \frac{n!}{k!} X^k$$

Exercice 8

— On suppose $a \neq b$.

$P \mid P(X^3) \iff a$ et b sont racines de $P(X^3)$
$\iff P(a^3) = P(b^3) = 0 \iff \quad (a^3 = a \text{ ou } a^3 = b) \text{ et } (b^3 = a \text{ ou } b^3 = b)$

Or,

$$\begin{cases} a^3 = a \\ b^3 = a \end{cases} \iff \begin{cases} a = 0 \\ b = 0 \end{cases} \text{ ou } \begin{cases} a = 1 \\ b \in \{1, j, j^2\} \end{cases} \text{ ou } \begin{cases} a = -1 \\ b \in \{-1, -j, -j^2\} \end{cases}$$
$$\iff P \in \left\{(X-1)(X-j), (X-1)(X-j^2), (X+1)(X+j), (X+1)(X+j^2)\right\}$$

$\begin{cases} a^3 = a \\ b^3 = b \end{cases}$ donne des polynômes (en plus des précédents) dans

$$\left\{X(X-1), X(X+1), (X-1)(X+1)\right\}$$

$$\begin{cases} a^3 = b \\ b^3 = a \end{cases} \iff \begin{cases} a^3 = b \\ a^9 = a \end{cases} \iff \exists k \in [\![0, 7]\!], \begin{cases} a = e^{\frac{ik\pi}{4}} \\ b = e^{\frac{3ik\pi}{4}} \end{cases}$$

On a donc,

$$\left\{ \left(X - e^{i\frac{\pi}{4}}\right)\left(X - e^{\frac{3i\pi}{4}}\right), \underbrace{(X-i)(X+i)}_{\in \mathbb{R}[X]}, \left(X - e^{\frac{5i\pi}{4}}\right)\left(X - e^{\frac{-i\pi}{4}}\right) \right\}$$

— On suppose $a = b$.

$$P \mid P(X^3) \iff \begin{cases} P(a^3) = 0 \\ 3a^2 P'(a^3) = 0 \end{cases}$$
$$\iff a^3 = a$$
$$\iff a \in \{0, 1, -1\}$$
$$\iff P \in \left\{X^2, (X-1)^2, (X+1)^2\right\}$$

Exercice 10

On pose

$$\begin{aligned} P &= (X-x)(X-y)(X-z) \\ &= X^3 - (x+y+z)X^2 + (xy+xz+yz)X - xyz \end{aligned}$$

On pose

$$\begin{cases} \lambda = x+y+z \\ p = xyz \\ q = xy+xz+yz \end{cases}$$

On sait que $\lambda = 0$.

$$\begin{aligned} \lambda^2 &= (x+y+z)^2 \\ &= x^2+y^2+z^2 + \underbrace{2xy+2yz+2xz}_{2q} \end{aligned}$$

donc,

$$\frac{x^2+y^2+z^2}{2} = -q$$

$$\begin{aligned} 0 = P(x) &= x^3 - \lambda x^2 + qx - p \\ 0 = P(y) &= y^3 - \lambda y^2 + qy - p \\ 0 = P(z) &= z^3 - \lambda z^2 + qz - p \end{aligned}$$

D'où,

$$x^3+y^3+z^3 = -q\lambda + 3p = 3q$$

donc

$$\frac{x^3+y^3+z^3}{3} = p$$

On a aussi

$$\begin{aligned} 0 &= x^5 + qx^3 - px^2 \\ 0 &= y^5 + qy^3 - py^2 \\ 0 &= z^5 + qz^3 - pz^2 \end{aligned}$$

et donc

$$x^5+y^5+z^5 = -3qp - 2qp = -5qp$$

donc

$$\frac{x^5+y^5+z^5}{5} = -qp = \frac{x^2+y^2+z^2}{2} \times \frac{x^3+y^3+z^3}{3}$$

Exercice 11

$$L_n = \frac{n!}{(2n)!}\left((X^2-1)^n\right)^{(n)}$$

1. $\deg(L_n) = 2n - n = n$ et $\mathrm{dom}(L_n) = 1$ car

$$\begin{aligned} L_n &= \frac{n!}{(2n)!}\sum_{k=0}^{n}\binom{n}{k}\left(X^{2k}\right)^{(n)}(-1)^{n-k} \\ &= \frac{n!}{(2n)!}\sum_{k=0}^{n}\binom{n}{k}\frac{(2k)!}{(2k-n)!}X^{2k-n}(-1)^{n-k} \end{aligned}$$

2. Soit $Q \in \mathbb{R}_{n-1}[X]$.
On pose $f_n : t \mapsto \dfrac{n!}{(2n)!}\left(t^2-1\right)^n$

$$\begin{aligned} \int_{-1}^{1} L_n(t)Q(t)\,dt &= f_n^{(n)}(t)Q(t)\,dt \\ &= \left[f_n^{(n-1)}(t)Q(t)\right]_{-1}^{1} - \int_{-1}^{1} f_n^{(n-1)}(t)Q'(d)\,dt \end{aligned}$$

$f_n^{(n-1)}(1) = 0$ car 1 est racine de $\left(X^2-1\right)^n$ avec multiplicité n. De même, $f_n^{(n-1)}(-1) = 0$. Par récurence, à n fixé,

$\forall k \in [\![0, n-1]\!], \mathscr{P}(k) :$ " $\displaystyle\int_{-1}^{1} L_n(t)Q(t)\,dt = (-1)^k \int_{-1}^{1} f_n^{(n-k)}(t)Q^{(k)}(t)\,dt$"

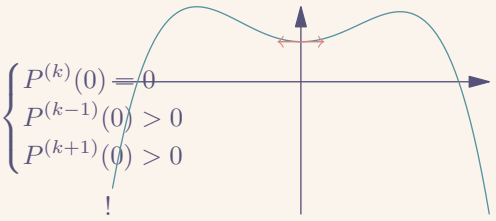
3. $\displaystyle\int_{-1}^{1} L_n\,dt = 0$, $t \mapsto L_n(t)$ est continue sur $[-1,1]$ et n'est pas l'application nulle.
donc L_n change de signe sur $[-1,1]$ donc L_n a au moins une racine dans $[-1,1]$.
Supposons que L_n a une unique racine a dans $[-1,1]$ et qu'elle change de signes en a. Donc, $t \mapsto L_n(t)(t-a)$ ne change pas de signes sur $[-1,1]$, est continue et d'intégrale nulle. Donc c'est l'application nulle $\lightning$.
On prouve par récurrence sur k que $t \mapsto L_n(t)$ change de signe au moins k-fois. Avec $k = n$, on trouve n racines disctinctes dans $[-1,1]$ et comme $\deg(L_n) = n$ donc, il n'y a pas plus de n racines.

Exercice 12

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}X^k$$

Soit $k \in \mathbb{N}$ tel que

$$\begin{cases} P^{(k)}(0) = 0 \\ P^{(k-1)}(0) > 0 \\ P^{(k+1)}(0) > 0 \end{cases}$$



!

Exercice 13

$P^2 + \alpha^2$ n'a pas de racines réelles.

Soit x une racine de $P^2 + \alpha^2$ de multiplicité au moins 2. Donc x est une racine de $2P'P$.

$x \notin \mathbb{R}$ donc $\begin{cases} P(x) \neq 0 \\ P'(x) \neq 0 \end{cases}$ car P et P' sont scindés sur $\mathbb{R}$. $\lightning$

Exercice 15

On suppose $\deg(A) \geqslant \deg(B)$.

$$\deg(A - B) \leqslant \deg(A)$$

Soient $a_1, \ldots, a_p$ les racines distinctes de A (et donc de B) avec $\alpha_1, \ldots, \alpha_p$ leur multiplicité en tant que racine de A et $\beta_1, \ldots, \beta_p$ leur multiplicité en tant que racine de B.
Donc,

$$\begin{cases} \sum_{i=1}^{p} \alpha_i = \deg(A) \\ \sum_{i=1}^{p} \beta_i = \deg(B) \end{cases}$$

$\forall i, a_i$ est une racine de $A - B$ de multiplicité $\min(\alpha_i, \beta_i)$

$$A - B = (A - 1) - (B - 1)$$

Soient $a'_1, \ldots, a'_q$ les racines de $A - 1$ (et donc de $B - 1$) avec $\alpha'_1, \ldots, \alpha'_q$ leur multiplicité en tant que racine de $A - 1$, et $\beta'_1, \ldots, \beta'_q$ leur multiplicité en tant que racine de $B - 1$.
On remarque que $\{a_1, \ldots, a_p\} \cap \{a'_1, \ldots, a'_q\} =$

$\forall j \in [\![1, q]\!], a'_j$ est racine de $A - B$ avec multiplicité $\min(\alpha'_j, \beta'_j)$.
$\forall i, a_i$ racone de A' avec multiplicité $\alpha_i - 1$. $\forall i, a'_i$ racone de A' avec multiplicité $\alpha'_i - 1$.

$$\sum_{i=1}^{p} (\alpha_i - 1) + \sum_{i=1}^{q} (\alpha'_j - 1) \leqslant \deg(A') = \deg(A) - 1$$

D'où,

$$\deg(A) - p + \deg(A)q \leqslant \deg(A) - 1$$

Donc

$$p + q \geqslant \deg(A) + 1$$

On a donc trouvé au moins $p + q$ racines différentes de $A - B$ avec $p + q > \deg(A - B)$. Donc $A - B = 0$

Exercice 17

Soient $x, y, z \in \mathbb{C}$. On pose

$$\begin{cases} \lambda = x + y + z \\ q = xy + xz + yz \\ p = xyz \end{cases}$$

et

$$\begin{aligned} P &= (X - x)(X - y)(X - z) \\ &= X^3 - \lambda X^2 + qX - p \end{aligned}$$

$$\begin{aligned} \lambda^2 &= (x + y + z)^2 \\ &= x^2 + y^2 + z^2 + 2q \end{aligned}$$

donc $x^2 + y^2 + z^2 = \lambda^2 - 2q$
De plus,

$$\begin{cases} 0 = P(x) & = x^3 - \lambda x^2 + qx - p \\ 0 = P(y) & = y^3 - \lambda y^2 + qy - p \\ 0 = P(z) & = z^3 - \lambda z^2 + qz - p \end{cases}$$

D'où,

$$\begin{aligned} x^3 + y^3 + z^3 &= \lambda(x^2 + y^2 + z^2) - q(x + y + z) + 3p \\ &= \lambda(\lambda^2 - 2q) - q\lambda + 3p \\ &= \lambda^3 - 3q\lambda + 3p \end{aligned}$$

et

$$\begin{aligned} x^4 + y^4 + z^4 &= \lambda(x^3 + y^3 + z^3) - q(x^2 + y^2 + z^2) + p(x + y + z) \\ &= \lambda(\lambda^3 - 3q\lambda + 3p) - q(\lambda^2 - 2q) + ps \end{aligned}$$

et

$$x^5+y^5+z^5=s(x^4+y^4+z^4)-q(x^3+y^3+z^3)+p(x^2+y^2+z^2)$$

$$\begin{aligned}
\begin{cases} x^2+y^2+z^2=0 \\ x^4+y^4+z^4=0 \\ x^5+y^5+z^5=0 \end{cases} &\iff \begin{cases} s^2-2q=0 \\ s(s^3-3qs+4p)=0 \\ -qs+3p=0 \end{cases} \\
&\iff \begin{cases} 0=0 \\ s=0 \\ q=0 \end{cases} \quad \text{ou} \quad \begin{cases} s^2=2q \\ s\neq 0 \\ q\neq 0 \\ 3p=qs \\ s^3-3qs+4p=0 \end{cases} \\
&\iff s=q=0 \ \text{ ou } \begin{cases} s^2=2q \\ 3p=qs \\ qs\left(2-3+\dfrac{4}{3}\right)=0 \end{cases} \\
&\iff s=q=0 \\
&\iff x,y,z \text{ sont racines de } X^3-p=0 \text{ avec } p\in\mathbb{C} \text{ quelconque} \\
&\iff \begin{cases} y=xj \\ z=xj^2 \end{cases} \quad \text{ou} \quad \begin{cases} y=xj^2 \\ z=xj \end{cases} \quad \text{avec } x\in\mathbb{C} \text{ quelconque}
\end{aligned}$$

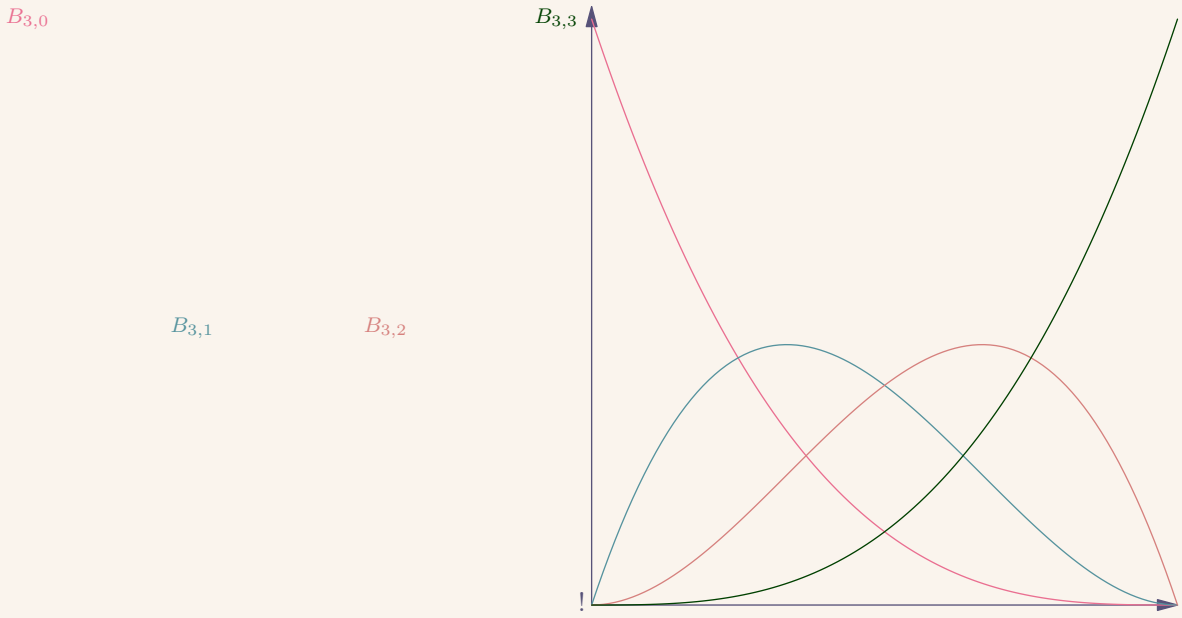
Vérification :

$$\begin{aligned}
x^2+y^2+z^2 &= x^2(1+j^2+j^4)=x^2(1+j+j^2)=0 \\
x^4+y^4+z^4 &= x^4(1+j^4+j^8)=x^4(1+j+j^2)=0 \\
x^5+y^5+z^5 &= x^5(1+j^5+j^{10})=x^5(1+j+j^2)=0
\end{aligned}$$

Exercice 18

1.

$$\begin{aligned}
\forall x, B_{3,0}(x) &= (1-x)^3 \\
B_{3,1}(x) &= 3x(1-x)^2 \\
B_{3,2}(x) &= 3x^2(1-x) \\
B_{3,3}(x) &= x^3
\end{aligned}$$



2. (a)

$$\begin{aligned}\sum_{k=0}^{n} b_{n,k} &= \sum_{k=0}^{n} \binom{n}{k} X^k (1-X)^{n-k} \\ &= (X+1-X)^n \\ &= 1\end{aligned}$$

$$\forall x \in [0,1], B_{n,k}(x) = \binom{n}{k} x^k (1-x)^{n-k} \geqslant 0$$

$$\sum_{k=0}^{n} B_{n,k}(x) = 1$$

donc

$$\forall x \in [\![0,1]\!], B_{n,k}(x) \leqslant 1$$

(b)

$$\begin{aligned}\sum_{k=1}^{n} kB_{n,k} &= \sum_{k=1}^{n} k\binom{n}{k}X^k(1-X)^{n-k}\\ &= \sum_{k=1}^{n}\frac{n!}{(k-1)!(n-k)!}X^k(1-X)^{n-k}\\ &= n\sum_{k=1}^{n}\binom{n-1}{k-1}X^k(1-X)^{n-k}\\ &= n\sum_{j=0}^{n-1}\binom{n-1}{j}X^{j+1}(1-X)^{n-1-j}\\ &= nX\sum_{j=0}^{n-1}\binom{n-1}{j}X^{j}(1-X)^{n-1-k}\\ &= nX(X+1-X)^{n-1}\\ &= nX\end{aligned}$$

$$\begin{aligned}\sum_{k=2}^{n} k(k-1)\binom{n}{k}X^k(1-X)^{n-k} &= \sum_{k=2}^{n}\frac{n!}{(k-2)!(n-k)!}X^k(1-X)^{n-k}\\ &= n(n-1)\sum_{k=2}^{n}\binom{n-2}{k-2}X^k(1-X)^{n-k}\\ &= n(n-1)\sum_{j=0}^{n-2}\binom{n-2}{j}X^{j+2}(1-X)^{n-2-j}\\ &= n(n-1)X^2\big(X+(1-X)\big)^{n-2}\\ &= n(n-1)X^2\end{aligned}$$

$$\begin{aligned}\forall k\in[\![1,n-1]\!],\sum_{k=1}^{n} k^2B_{n,k} &= \sum_{k=1}^{n} k\big((k-1)+1\big)B_{n,k}\\ &= \sum_{k=1}^{n} k(k-1)B_{n,k}+\sum_{k=1}^{n} kB_{n,k}\\ &= n(n-1)X^2+nX\\ &= n^2X^2+n(X-X^2)\end{aligned}$$

$$\begin{aligned}B'_{n,0} &= -n(1-X)^{n-1} = -nB_{n-1,0}\\ B'_{n,n} &= nX^{n-1} = nB_{n-1,n-1}\end{aligned}$$

3.

$$\begin{aligned}B'_{n-k} &= \binom{n}{k}\left(kX^{k-1}(1-X)^{n-k} - (n-k)X^k(1-X)^{n-k-1}\right)\\ &= n\binom{n-1}{k-1}X^{k-1}(1-X)^{n-k} - n\binom{n-1}{n-k-1}X^k(1-X)^{n-k-1}\\ &= nB_{n-1,k-1} - nB_{n-1,k}\end{aligned}$$

4. On montre par récurrence sur n que $(B_{n,k})_{0\leqslant k\leqslant n}$ est libre.
Soient $(\lambda_k)_{0\leqslant k\leqslant n} \in \mathbb{R}^{n+1}$. On suppose que

$$\sum_{k=0}^{n} \lambda_k B_{n,k} = 0$$

Donc

$$-n\lambda_0 B_{n-1,0} + n\lambda_n B_{n-1,n-1} + \sum_{k=1}^{n-1} n\lambda_k (B_{n-1,k-1} - B_{n-1,k}) = 0$$

Donc

$$-\lambda_0 B_{n-1,0} + \lambda_n B_{n-1,n-1} + \sum_{j=0}^{n-2} \lambda_{j+1} B_{n-1,j+1} - \sum_{k=1}^{n-1} \lambda_k B_{n-1,k} = 0$$

Donc

$$(\lambda_1 - \lambda_0)B_{n-1,0} = (\lambda_n - \lambda_{n-1})B_{n-1,n-1} + \sum_{k=1}^{n-2}(\lambda_{k+1} - \lambda_k)B_{n-1,k} = 0$$

D'après l'hypothèse de récurrence,

$$\lambda_1 - \lambda_0 = 0\lambda_n - \lambda_{n-1} = 0\forall k \in [\![1, n-2]\!], \lambda_{k+1} - \lambda_k = \check{\mathrm{r}}0$$

Donc

$$\forall k \in [\![0, n]\!], \lambda_k = \lambda_0$$

D'où

$$\sum_{k=0}^{n} \lambda_0 B_{n,k} = 0$$

donc

$$\lambda_0 \times 1 = 0$$

et donc

$$\lambda_0 = 0$$

Donc

$$\forall k \in [\![0, n]\!], \lambda_k = 0$$

5. (a) Soient $P, Q \in \mathbb{R}_n[X], \lambda, \mu \in \mathbb{R}$.

$$\begin{aligned} B(\lambda P + \mu Q) &= \sum_{k=0}^{n} (\lambda P + \mu Q)\left(\frac{k}{n}\right) B_{n,k} \\ &= \sum_{k=0}^{n} \left(\lambda P\left(\frac{k}{n}\right) + \mu Q\left(\frac{k}{n}\right)\right) B_{n,k} \\ &= \lambda \sum_{k=0}^{n} P\left(\frac{k}{n}\right) B_{n,k} + \mu \sum_{k=0}^{n} Q\left(\frac{k}{n}\right) B_{n,k} \\ &= \lambda B(P) + \mu B(Q) \end{aligned}$$

$$\forall k, \deg(B_{n,k}) \leqslant n$$

donc

$$\forall P \in \mathbb{R}[X], \deg\big(B(P)\big) \leqslant n$$

(b)

$$\begin{aligned} \mathrm{Ker}(B) &= \left\{ P \in \mathbb{R}_n[X] \mid \sum_{k=0}^{n} P\left(\frac{k}{n}\right) B_{n,k} = 0 \right\} \\ &= \left\{ P \in \mathbb{R}_n[X] \mid \forall k \in [\![0, n]\!], P\left(\frac{k}{n}\right) = 0 \right\} \\ &= \{0\} \end{aligned}$$

donc B injective et donc B est bijective.

Exercice 19 (supplémentaire)

Trouver tous les $P \in \mathbb{R}[X]$ tels que

$$XP(X+1) = (X+4)P(X)$$

Analyse Soit $P \in \mathbb{R}[X]$ tel que

$$XP(X+1) = (X+4)P(X)$$

En remplaçant X par 0, on obtient

$$4P(0) = 0$$

donc 0 est racine de P.
En replaçant X par -4, on obtient

$$-4P(-3) = 0$$

donc -3 est une racine de P.
En remplaçant X par -3, on obtient

$$-3P(-2) = -P(-3) = 0$$

donc -2 est racine de P.
En replaçant X par -2, on obtient

$$-2P(-1) = -2P(-2) = 0$$

donc -1 est racine de P.
D'où,

$$P = X(X+1)(X+2)(X+3)\,Q(X)$$

avec $Q \in \mathbb{R}[X]$.
Donc,

$$\begin{aligned} &X(X+1)(X+2)(X+3)(X+4)\,Q(X+1) \\ &= (X+4)X(X+1)(X+2)(X+3)\,Q(X). \end{aligned}$$

Comme $\mathbb{R}[X]$ est intègre,

$$Q(X) = Q(X+1).$$

Si Q n'est pas constant, alors Q a au moins une racine $a \in \mathbb{C}$ et alors

$$\forall k \in \mathbb{N}, Q(a+k) = Q(a) = 0.$$

Donc, Q a une infinité de racines donc $Q = 0$.
Donc Q est constant.

Synthèse Soit $\lambda \in \mathbb{R}$ et

$$P = \lambda X(X+1)(X+2)(X+3).$$

On vérifie aisément que

$$XP(X+1) = (X+4)P(X).$$

Chapitre 19

TD 19

Exercice 1

$E = \mathbb{K}_3[X]$ et $\varphi : \begin{array}{ccc} E & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & XP' - P \end{array}$

1. Soit $P \in E$.

$$\begin{aligned} \deg(XP') &= 1 + \deg(P) - 1 = \deg(P) \\ \deg(XP' - P) &\leqslant \deg(P) \leqslant 3 \end{aligned}$$

donc $\varphi(P) \in E$.
Soient $P, Q \in E$, $\lambda, \mu \in \mathbb{K}$.

$$\begin{aligned} \varphi(\lambda P + \mu Q) &= X(\lambda P + \mu Q)' - (\lambda P + \mu Q) \\ &= X(\lambda P' + \mu Q') - \lambda P - \mu Q \\ &= \lambda(XP' - P) + \mu(XQ' - Q) \\ &= \lambda\varphi(P) + \mu\varphi(Q) \end{aligned}$$

Donc $\varphi \in \mathscr{L}(E)$.

2. Soit $P \in E$. On pose $P = aX^3 + bX^2 + cX + d$ avec $(a, b, c, d) \in \mathbb{K}^4$.

$$\begin{aligned} P \in \operatorname{Ker}\varphi &\iff \varphi(P) = 0 \\ &\iff X(3aX^2 + 2bX + c) - (aX^3 + bX^2 + cX + d) = 0 \\ &\iff 2aX^3 + bX^2 + d = 0 \\ &\iff \begin{cases} a = 0 \\ b = 0 \\ d = 0 \end{cases} \\ &\iff P = cX \\ &\iff P \in \operatorname{Vect}(X) \end{aligned}$$

$\mathrm{Ker}(\varphi) = \mathrm{Vect}(X)$ et $X \neq 0$ donc (X) est une base de $\mathrm{Ker}\,\varphi$.

$$\begin{aligned}\mathrm{Im}(\varphi) &= \mathrm{Vect}\left(\varphi(1), \varphi(X), \varphi(X^2), \varphi(X^3)\right)\\ &= \mathrm{Vect}(-1, X^2, 2X^3)\end{aligned}$$

D'après le théorème du rang,

$$\begin{aligned}\dim\left(\mathrm{Im}(\varphi)\right) &= \dim E - \dim(\mathrm{Ker}\,\varphi)\\ &= 4 - 1\\ &= 3\end{aligned}$$

Donc $(1, X^2, X^3)$ est une base de $\mathrm{Im}(\varphi)$.

Exercice 3

$E = \mathbb{R}^4$ et $f : E \to E$ linéaire.

1. $u = (x, y, z, t) \in E$ donc

$$u = xe_1 + ye_2 + ze_3 + te_4$$

donc

$$\begin{aligned}f(u) &= f(xe_1 + ye_2 + ze_3 + te_4)\\ &= xf(e_1) + yf(e_2) + zf(e_3) + tf(e_4)\\ &= x(1,1,1,1) + y(1,2,1,1) + z(2,3,2,2) + t(-1,-2,-1,-1)\\ &= (x + y + 2z - t, x + 2y + 3z - 2t, x + y + 2z - t, x + y + 2z - t)\end{aligned}$$

Remarque :

$$\begin{pmatrix}1 & 1 & 2 & -1\\ 1 & 2 & 3 & -2\\ 1 & 1 & 2 & -1\\ 1 & 1 & 2 & -1\end{pmatrix}\begin{pmatrix}x\\ y\\ z\\ t\end{pmatrix} = \begin{pmatrix}x + y + 2z - t\\ x + 2y + 3z - 2t\\ x + y + 2z - t\\ x + y + 2z - t\end{pmatrix}$$

2. Soit $u = (x, y, z, t) \in E$.

$$\begin{aligned}
u \in \mathrm{Ker}(f) &\iff f(u) = (0,0,0,0) \\
&\iff \begin{cases} x + y + 2z - t = 0 \\ x + 2y + 3z - 2t = 0 \\ x + y + 2z - t = 0 \\ x + y + 2z - t = 0 \end{cases} \\
&\iff \begin{cases} x + 2y + 3z - 2t = 0 \\ x + y + 2z - t = 0 \end{cases} \\
&\underset{L_2 \leftarrow L_2 - L_1}{\iff} \begin{cases} \boxed{x} + y + 2z - t = 0 \\ \boxed{y} + z - t = 0 \end{cases} \\
&\iff \begin{cases} x = -z \\ y = -z + t \end{cases} \\
&\iff u = (-z, -z + t, z, t) \\
&\qquad = z\underbrace{(-1,-1,1,0)}_{v_1} + t\underbrace{(0,1,0,1)}_{v_2} \\
&\iff u \in \mathrm{Vect}(v_1, v_2)
\end{aligned}$$

Or, (v_1, v_2) est libre donc c'est une base de $\mathrm{Ker}(f)$.

$$\mathrm{Im}(f) = \mathrm{Vect}\left(f(e_1), f(e_2), f(e_3), f(e_4)\right)$$

Or, $\mathrm{rg}(f) = 4 - 2 = 2$
Donc $\left(f(e_1), f(e_2)\right)$ est libre dans $\mathrm{Im}(f)$ donc c'est une base de $\mathrm{Im}(f)$

3. $\mathrm{Ker}(f) \neq \{0\}$ donc f n'est pas injective donc pas bijective.

4.

$$\begin{aligned}
\forall (x, y, z, t) \in E, f((x, y, z, t)) = (&x + y + 2z - t, x + 2y + 3z - 2t, \\
&x + y + 2z - t, x + y + 2z - t)
\end{aligned}$$

Soit $(\alpha,\beta,\gamma,\delta)$.

$$\begin{aligned}(\alpha,\beta,\gamma,\delta)\in\mathrm{Im}(f) &\iff \exists(x,y,z,t)\in E,(\alpha,\beta,\gamma,\delta)=f\big((x,y,z,t)\big)\\ &\iff \exists(x,y,z,t)\in E,\begin{cases}x+y+2z-t=\alpha\\ x+2y+3z-2t=\beta\\ x+y+2z-t=\gamma\\ x+y+2z-t=\delta\end{cases}\\ &\iff \exists(x,y,z,t)\in E\begin{cases}\boxed{x}+y+2z-t=\alpha\\ \boxed{y}+z-t=\beta-\alpha\\ 0=\gamma-\alpha\\ 0=\delta-\alpha\end{cases}\\ &\iff \begin{cases}\gamma-\alpha=0\\ \delta-\alpha=0\end{cases}\\ &\iff (\alpha,\beta,\gamma,\delta)=(\alpha,\beta,\alpha,\alpha)\\ &\qquad\qquad =\alpha(1,0,1,1)+\beta(0,1,0,0)\end{aligned}$$

Une base de $\mathrm{Im}(f)$ est $\big((1,0,1,1),(0,1,0,0)\big)$.

Exercice 6

1.
$$S=\{u\in\mathbb{R}^{\mathbb{N}}\mid\forall n\in\mathbb{N},u_{n+2}=au_{n+1}+bu_n\}$$

— $S\neq$ car $0\in S$.

— Soient $u,v\in S$ et $\lambda,\mu\in\mathbb{R}$. Soit $n\in\mathbb{N}$.

$$\begin{aligned}(\lambda u+\mu v)(n+2)&=\lambda u_{n+2}+\mu v_{n+2}\\ &=\lambda(au_{n+1}+bu_n)+\mu(av_{n+1}+bv_n)\\ &=a(\lambda u_n+\mu v_n)+b(\lambda u+\mu v)\\ &=a(\lambda u+\mu v)(n+1)+b(\lambda u+\mu v)(n)\end{aligned}$$

Donc $(\lambda u+\mu v)\in S$.

2.
$$\begin{aligned}\Phi:S&\longrightarrow\mathbb{R}^2\\ (x_n)&\longmapsto(x_0,x_1)\end{aligned}$$

Soit $(u,v)\in S^2$ et $(\lambda,\mu)\in\mathbb{R}^2$.

$$\begin{aligned}\Phi(\lambda u+\mu v)&=(\lambda u_0+\mu v_0,\lambda u_1+\mu v_1)\\ &=\lambda(u_0,u_1)+\mu(v_0,v_1)\\ &=\lambda\Phi(u)+\mu\Phi(v)\end{aligned}$$

Donc Φ est linéaire.

$$\begin{aligned}\forall n \in \mathbb{N}, \quad a\alpha^{n+1} + b\alpha^n &= \alpha^n(a\alpha + b) \\ &= \alpha^n + \alpha^2 \quad \text{car solution de l'équation caractéristique} \\ &= \alpha^{n+2}\end{aligned}$$

Donc, $(\alpha^n)_{n\in\mathbb{N}} \in S$ et $\Phi(\alpha^n) = (1, \alpha) \neq (0, 0)$ Donc $\dim\big(\mathrm{Im}(\varphi)\big) > 0$.
De même, $(\beta_n)_{n\in\mathbb{N}} \in S$ et $\Phi(\beta^n) = (1, \beta) \neq (0, 0)$.
On a deux vecteurs non colinéaires dans Im Φ donc $\dim(\mathrm{Im}\ \Phi) = 2$.
Donc Im $\Phi = \mathbb{R}^2$ et donc Φ est bijective.

Exercise 7

—

$$\forall f \in \mathscr{L}(E), \begin{cases} f \circ p \in \mathscr{L}(E) \\ p \circ f \in \mathscr{L}(E) \end{cases}$$

so

$$\frac{1}{2}(f \circ p + p \circ f) \in \mathscr{L}(E)$$

— Let $(f, g) \in \mathscr{L}(E)^2$, $(\lambda, \mu) \in \mathbb{K}^2$.

$$\begin{aligned}\Phi(\lambda f + \mu g) = \frac{1}{2}\big((\lambda f + \mu g) \circ p + p \circ (\lambda f + \mu g)\big) \quad &= \frac{1}{2}(\lambda f \circ p + \mu g \circ p + \lambda p \circ f + \mu p \circ g) \\ = \lambda\Phi(f) + \mu\Phi(g)\end{aligned}$$

Thus,

$$\Phi \in \mathscr{L}\big(\mathscr{L}(E)\big)$$

—

$$\begin{aligned}E &= \mathrm{Ker}(p) \oplus \mathrm{Im}(p) \\ P_{|\,\mathrm{Ker}(p)} &= 0 \\ P_{|\mathrm{Im}(p)} &= \mathrm{id}\end{aligned}$$

Analysis Let $f \in \mathrm{Ker}(\Phi)$ so

$$\Phi(f) = 0_{\mathscr{L}(E)}$$

thus

$$\forall x \in E, \Phi(f)(x) = 0_E$$

so

$$\forall x \in \mathrm{Ker}(p), \Phi(f)(x) = 0_E$$

so

$$\forall x \in \mathrm{Ker}(p), f(0_E) + p\big(f(x)\big) = 0_E$$

thus

$$\forall x \in \mathrm{Ker}(p), f(x) \in \mathrm{Ker}(p)$$

Let $x \in \mathrm{Im}(p)$

$$\begin{aligned}\Phi(f)(x) = 0_E \text{ so } & f(x) + p\big(f(x)\big) = 0_E \\ \text{so } & p\big(f(x)\big) = -f(x) \\ \text{so } & -f(x) \in \mathrm{Im}(p) \\ \text{so } & f(x) \in \mathrm{Im}(p) \\ \text{so } & p\big(f(x)\big) = f(x) \\ \text{so } & f(x) = 0_E\end{aligned}$$

Synthesis Let $u \in \mathscr{L}(\mathrm{Ker}\, p)$. We set $f : E \to E$ defined by

$$\forall x \in E, f(x) = u\big(x - p(x)\big)$$

—

$$\forall x \in E, p\big(x - p(x)\big) = p(x) - p(x) = 0_E$$

so f is well-defined.

— Let $(x, y) \in E^2$ and $(\alpha, \beta) \in \mathbb{K}^2$.

$$\begin{aligned}f(\alpha x + \beta y) &= u\big(\alpha x + \beta y - p(\alpha x + \beta y)\big) \\ &= u\big(\alpha x + \beta y - \alpha p(x) - \beta p(y)\big) \\ &= u\big(\alpha\big(x - p(x)\big) + \beta\big(y - p(y)\big)\big) \\ &= \alpha u\big(x - p(x)\big) + \beta u\big(y - p(y)\big) \\ &= \alpha f(x) + \beta f(y)\end{aligned}$$

Thus,

$$f \in \mathscr{L}(E)$$

— Let $x \in E$.

$$\begin{aligned}\Phi(f)(x) &= \frac{1}{2}\big(f\big(p(x)\big) + \underbrace{p\big(f(x)\big)}_{=0_E \text{ car } f(x) \in \mathrm{Ker}(p)}\big) \\ &= \frac{1}{2}\big(p(x) - p\big(p(x)\big)\big) \\ &= \frac{1}{2}u\big(p(x) - p(x)\big) \\ &= 0_E\end{aligned}$$

So,

$$\Phi(f) = 0_{\mathscr{L}(E)}$$

Thus,

$$f \in \mathrm{Ker}\, \Phi$$

Exercice 9

1. $E^\star = \mathscr{L}(E, \mathbb{K})$
2. Soit $i \in [\![1, n]\!]$. Soient $(x, y) \in E^2$ et $(\lambda, \mu) \in \mathbb{K}^2$.
   On pose $x = \sum_{j=1}^{n} x_j e_j$ avec $(x_1, \ldots, x_n) \in \mathbb{K}^n$ et $y = \sum_{j=1}^{n} y_j e_j$ avec $(y_1, \ldots, y_n) \in \mathbb{K}^n$.
   D'où,

$$\begin{aligned}\lambda x + \mu y &= \lambda \sum_{j=1}^{n} x_j e_j + \mu \sum_{j=1}^{n} y_j e_j \\ &= \sum_{j=1}^{n} (\lambda x_j + \mu y_j) e_j\end{aligned}$$

$$\begin{aligned}e_i^\star(\lambda x + \mu y) &= \lambda x_i + \mu y_i \\ &= \lambda e_i^\star(x) + \mu e_i^\star(y)\end{aligned}$$

   Donc, $e_i^\star \in E^\star$.
   Soit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$. On suppose que

$$\sum_{i=1}^{n} \lambda_i e_i^\star = 0_{E^\star}$$

   Donc

$$\forall x \in E, \sum_{i=1}^{n} \lambda_i e_i^\star(x) = 0_{\mathbb{K}}$$

$$\forall j \in [\![1, n]\!], \sum_{i=1}^{n} \lambda_i \underbrace{e_i^\star(e_j)}_{\delta_{i,j}} = 0_{\mathbb{K}} \text{ donc } \lambda_j = 0_{\mathbb{K}}$$

   Donc $(e_1^\star, \ldots, e_n^\star)$ est libre.
3. Soit $f \in E^\star$. On va montrer que

$$f = \sum_{i=1}^{n} f(e_i) e_i^\star$$

   En effet, pour tout $x \in E$:

$$\begin{aligned}f(x) = f\left(\sum_{i=1}^{n} e_i^\star(x) e_i\right) &= \sum_{i=1}^{n} f(e_i) e_i^\star(x) \\ &= \left(\sum_{i=1}^{n} f(e_i) e_i^\star\right)(x)\end{aligned}$$

   Donc $E^\star = \mathrm{Vect}(e_1^\star, \ldots, e_n^\star)$. Donc $\dim(E^\star) = \dim(E)$.

4.

$$\begin{aligned}\Phi(u) : E^\star &\longrightarrow \mathbb{K}\\ f &\longmapsto f(u)\end{aligned}$$

Soient $f, g \in E^\star$ et $\lambda, \mu \in \mathbb{K}$.

$$\begin{aligned}\Phi(u)(\lambda f + \mu g) &= (\lambda f + \mu g)(u)\\ &= \lambda f(u) + \mu g(u)\\ &= \lambda\Phi(f) + \mu\Phi(g)\end{aligned}$$

Donc $\Phi(u) = \mathscr{L}(E^\star, \mathbb{K}) = (E^\star)^\star = E^{\star\star}$.

5.

$$\begin{aligned}\Phi : E &\longrightarrow E^{\star\star}\\ u &\longmapsto \Phi(u)\end{aligned}$$

Soient $(u, v) \in E^2$ et $(\lambda, \mu) \in \mathbb{K}^2$.

$$\begin{aligned}\Phi(\lambda u + \mu v) &: E^\star \longrightarrow \mathbb{K}\\ \lambda\Phi(u) + \mu\Phi(v) &: E^\star \longrightarrow \mathbb{K}\end{aligned}$$

Soit $f \in E^\star$.

$$\begin{aligned}\Phi(\lambda u + \mu v)(f) &= f(\lambda u + \mu v)\\ &= \lambda f(u) + \mu f(v)\\ &= \lambda\Phi(u)(f) + \mu\Phi(v)(f)\\ &= \big(\lambda\Phi(u) + \mu\Phi(v)\big)(f)\end{aligned}$$

Donc $\Phi \in \mathscr{L}(E, E^{\star\star})$.

Soit $u \in E$.

$$\begin{aligned}\Phi(u) = 0_{E^{\star\star}} &\iff \forall f \in E^\star, \Phi(u)(f) = 0_{\mathbb{K}}\\ &\iff \forall f \in E^\star, f(u) = 0_{\mathbb{K}} \implies \quad \forall i \in [\![1, n]\!], e_i^\star(u) = 0_{\mathbb{K}}\\ &\implies u = \sum_{i=1}^{n} e_i^\star(u) e_i = 0_E\end{aligned}$$

Donc, $\operatorname{Ker}\Phi = \{0_E\}$ donc Φ est injective.

6.

$$\dim(E^{\star\star}) = \dim(E^\star) = \dim(E)$$

donc

$$\Phi \in \mathrm{GL}(E, E^{\star\star})$$

Exercise 10

$\dim(\operatorname{Ker} f \cap F) \geqslant \dim F - \operatorname{rk} f$

Let $g : \begin{array}{ccc} ? & \longrightarrow & ? \\ x & \longmapsto & ? \end{array}$. We need to find g such that $\operatorname{Ker}(g) = \operatorname{Ker}(f) \cap F$.

$$\begin{aligned} g(x) = 0 \iff x \in \operatorname{Ker}(g) &\iff x \in \operatorname{Ker}(f) \cap F \\ &\iff x \in \operatorname{Ker}(f) \text{ and } x \in F \\ &\iff f(x) = 0 \text{ and } x \in F \end{aligned}$$

So,

$$\begin{aligned} g : F &\longrightarrow E \\ x &\longmapsto f(x) \end{aligned}$$

f is linear, so, g is also linear.

Thus,

$$\begin{aligned} \dim(F) &= \dim(\operatorname{Ker} g) - \dim(\operatorname{Im} f) \\ &= \dim\big(\operatorname{Ker}(f) \cap F\big) - \dim(\operatorname{Im} f) \end{aligned}$$

We know that

$$\operatorname{Im} f \supset \operatorname{Im} g$$

So,

$$\dim(\operatorname{Im} f) \leqslant \dim(\operatorname{Im} g)$$

So,

$$\dim F \leqslant \dim(\operatorname{Ker}(f) \cap F) + \dim(\operatorname{Im}, f)$$

and so

$$\dim\big(\operatorname{Ker}(f) \cap F\big) \geqslant \dim F - \dim(\operatorname{Im} f)$$

Exercice 11

1. Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n et $f, g \in \mathscr{L}(E)$.

$$\begin{aligned} f_{|\operatorname{Im}(g)} : \operatorname{Im}(g) &\longrightarrow E \\ x &\longmapsto f(x) \end{aligned}$$

Soit $x \in \mathrm{Im}(g)$.

$$\begin{aligned} x \in \mathrm{Ker}(f_{|\mathrm{Im}(g)}) &\iff f_{|\mathrm{Im}(g)}(x) = 0 \\ &\iff \begin{cases} f(x) = 0 \\ x \in \mathrm{Im}(g) \end{cases} \\ &\iff x \in \mathrm{Ker}(f) \cap \mathrm{Im}(g) \end{aligned}$$

$$\mathrm{Ker}(f_{|\mathrm{Im}(g)}) = \mathrm{Ker}(f) \cap \mathrm{Im}(g)$$
$$\dim(\mathrm{Im}\ g) = \dim\big(f(\mathrm{Im}\ g)\big) + \dim(\mathrm{Ker}\, f \cap \mathrm{Im}\ g)$$
$$\dim\big(f(\mathrm{Im}\ g)\big) = \dim\big(\mathrm{Im}(f \circ g)\big) = \mathrm{rg}(f \circ g)$$
$$\mathrm{rg}(f \circ g) = \mathrm{rg}(g) - \dim(\mathrm{Im}\ g \cap \mathrm{Ker}\, f)$$
$$\dim(E) = n = \mathrm{rg}(g) + \dim(\mathrm{Ker}\, f)$$

donc

$$-n + \mathrm{rg}(f) = \dim(\mathrm{Ker}\, f) \leqslant -\dim(\mathrm{Im}\ g \cap \mathrm{Ker}\, f)$$
$$\mathrm{rg}(f \circ g) \geqslant \mathrm{rg}(g) + \mathrm{rg}(f) - n$$

Analyse Soit $f \in \mathscr{L}(E)$ et $\dim(E) = 3$. On suppose $f \circ f = 0$.

$$\mathrm{rg}(0) = \mathrm{rg}(f \circ f) \geqslant \mathrm{rg}(f) = \mathrm{rg}(f) + \mathrm{rg}(f) - n$$

Donc

$$0 \leqslant 2\,\mathrm{rg}(f) - n$$
$$3 = n \geqslant 2\,\mathrm{rg}(f)$$

Donc,

$$\mathrm{rg}(f) \in \{0, 1\}$$

et donc

$$\dim(\mathrm{Im}\ f) \in \{1, 0\}$$

Soit $u \in \mathrm{Im}(f) \setminus \{0\}$ donc Vect $u = \mathrm{Im}\ f$.

$$\forall x \in K, \exists \lambda(x) \in \mathbb{K}, f(x) = \lambda(x) \cdot u$$

Synthèse

— $f = 0$
— On suppose $f \neq 0$. Soit $u \in E$, $\lambda \in \mathscr{L}(E, \mathbb{K}) = E^\star$.

$$\begin{aligned} f : E &\longrightarrow E \\ x &\longmapsto \lambda(x) \cdot u \end{aligned}$$

Soit $x \in E$.

$$\begin{aligned} (f \circ f)(x) &= f\big(\lambda(x) \cdot u\big) \\ &= \lambda\big(\lambda(x) \cdot u\big) \\ &= \lambda(x)\lambda(u) \cdot u \end{aligned}$$

Soient $(x, y) \in E^2$ et $\alpha, \beta \in \mathbb{K}^2$.

$$f(\alpha a + \beta y) = \lambda(\alpha x + \beta y) \cdot u$$

$$||$$

$$\alpha f(x) + \beta f(y) = \alpha\lambda(x) \cdot u + \beta\lambda(y) \cdot u$$

Donc,

$$\lambda(\alpha x + \beta y) \cdot u = \big(\alpha\lambda(x) + \beta\lambda(y)\big) \cdot u$$

et donc

$$\lambda(\alpha x + \beta y) = \alpha\lambda(x) + \beta\lambda(y)$$

$$f(u) = u$$

Soit $v \in E$ tel que $f(v) = u$.

$$f(u) = f\big(f(v)\big) = 0 = \lambda(u) \cdot u$$

Donc $\lambda(u) = 0$ et donc $u \in \mathrm{Ker}(\lambda)$.

Exercice 12

Partie I.

Soit $N \in \mathbb{N}_\star$. On pose

$$\forall P \in \mathbb{R}_N[X], \Delta(P) = P(X+1) - P(X).$$

1. Soit $P \in \mathbb{R}_N[X]$. On pose

$$P = \sum_{k=0}^{N} a_k X^k$$

On pose $N' = \deg P$. Donc,

$$\begin{aligned} P(X+1) &= \sum_{k=0}^{N'} a_k (X+1)^k \\ &= \sum_{k=0}^{N'} a_k \sum_{i=0}^{k} \binom{k}{i} X^i \\ &= \sum_{i=0}^{N'} \left(\sum_{k=i}^{N'} a_k \binom{k}{i} \right) X^i \\ &= \sum_{k=0}^{N'} \left(\sum_{i=k}^{N'} a_i \binom{i}{k} \right) X^k \end{aligned}$$

Donc,

$$\Delta(P) = P(X+1) - P(X) = \sum_{k=0}^{N'} \left(\sum_{i=k}^{N'} a_i \binom{i}{k} \right) X^k - \sum_{k=0}^{N'} a_k X^k$$
$$= \sum_{k=0}^{N'} \left(\sum_{i=k}^{N'} a_i \binom{i}{k} - a_k \right) X^k$$

Pour $k = N'$, $a_{N'} \binom{N'}{N'} - a_{N'} = 0$.

Pour $k = N' - 1$,

$$a_{N'-1} \binom{N'-1}{N'-1} + a_{N'} \binom{N'}{N'-1} - a_{N'-1} \leqslant N' a_{N'} \neq 0 \text{ si } N' \neq 0.$$

Si $\deg P > 0$, alors $\deg\big(\Delta(P)\big) = \deg(P) - 1$.

Si $\deg P \leqslant 0$, alors $\deg \Delta(P) = -\infty$.

2. $\deg\big(\Delta(P)\big) \leqslant \deg(P) \leqslant N$ donc $\Delta(P) \in \mathbb{R}_N[X]$.
Soient $(P, Q) \in \mathbb{R}_N[X]^2$ et $(\lambda, \mu) \in \mathbb{R}^2$.

$$\begin{aligned}\Delta(\lambda P + \mu Q) &= (\lambda P + \mu Q)(X+1) - (\lambda P + \mu Q)(X) \\ &= \lambda P(X+1) + \mu Q(X+1) - \lambda P(X) - \mu Q(X) \\ &= \lambda \Delta(P) + \mu \Delta(Q)\end{aligned}$$

Donc $\Delta \in \mathscr{L}\big(\mathbb{R}_n[X]\big)$.

3.

$$\begin{aligned}P \in \operatorname{Ker}(\Delta) &\iff \Delta(P) = 0 \\ &\iff P(X+1) - P(X) = 0 \\ &\iff \deg(P) \leqslant 0 \\ &\iff P \in \operatorname{Vect}(1)\end{aligned}$$

(1) est libre donc c'est une base.

4. D'après le théorème du rang,

$$\dim\big(\mathbb{R}_N[X]\big) = \dim(\operatorname{Ker}\Delta) + \dim(\operatorname{Im}\Delta)$$

$$\dim(\operatorname{Im}\Delta) = N$$

donc

$$\operatorname{Im}\Delta \neq \mathbb{R}_N[X]$$

donc Δ n'est pas surjective.

Partie II.

1. Soit $n \in \mathbb{N}_\star$.

$$\begin{aligned}
\Delta(P_n) &= P_n(X+1) - P_n(X) \\
&= \frac{1}{n!}\prod_{k=0}^{n-1}(X+1-k) - \frac{1}{n!}\prod_{k=0}^{n-1}(X-k) \\
&= \frac{1}{n!}\left(\prod_{k=0}^{n-1}(X+1-k) - \prod_{k=0}^{n-1}(X-k)\right) \\
&= \frac{1}{n!}\left(\prod_{i=-1}^{n-2}(X-i) - \prod_{k=0}^{n-1}(X-k)\right) \\
&= \frac{1}{n!}\left(\prod_{i=0}^{n-2}(X-i)\big((\cancel{X}+\cancel{1}) - (\cancel{X}-n+\cancel{1})\big)\right) \\
&= \frac{1}{(n-1)!}\prod_{i=0}^{n-2}(X-i) \\
&= P_{n-1}
\end{aligned}$$

   Si $n = 0$, $P_n = 1$ donc $\Delta(P_0) = 0$.

2. $$\forall i \neq j, \deg(P_i) \neq \deg(P_j)$$

   donc $(P_0, \ldots, P_n)$ est libre.

   Or, il y a $n+1$ vecteurs et

$$\dim\left(\mathbb{R}_n[X]\right) = n+1$$

   donc $(P_0, \ldots, P_N)$ est une base de $\mathbb{R}_N[X]$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1/2 & 1/3 \\ 0 & 0 & 1/2 & -1/2 \\ 0 & 0 & 0 & 1/6 \end{pmatrix}$$

   car

$$\begin{aligned}
P_0 &= 1 \\
P_1 &= X \\
P_2 &= \frac{1}{2}X^2 - \frac{1}{2}X \\
P_3 &= -\frac{1}{6}(X^3 - 3X^2 + 2X)
\end{aligned}$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1/2 & 1/3 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1/2 & -1/2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1/6 & 0 & 0 & 0 & 1 \end{array}\right) \underset{\substack{L_2\leftarrow L_2+L_3\\ L_3\leftarrow 2L_3\\ L_4\leftarrow 6L_4}}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1/6 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 \end{array}\right)$$

$$\underset{\substack{L_3\leftarrow L_3+L_4\\ L_2\leftarrow L_2+\frac{1}{6}L_4}}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 \end{array}\right)$$

Donc,

$$A^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

On a

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 6 \\ 6 \end{pmatrix}$$

Donc $X^3 = P_1 + 6P_2 + 6P_3$. Donc, $Q = P_2 + 6P_3 + 6P_4$ et aussi $\Delta(P) = X^3$.
donc

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} k^3 = \sum_{k=0}^{n} \big(Q(n+k) - Q(k)\big)$$

Donc

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} k^3 = Q(n+1) - Q(0)$$

Chapitre 20

TD 20

Exercice 2

6.

$$\begin{aligned}\frac{4}{(X^2+1)^2} &= \frac{4}{(X-i)^2(X+i^2)} \\ &= \frac{a}{X-i} + \frac{b}{(X-i)^2} + \frac{c}{X+i} + \frac{d}{(X+i)^2}\end{aligned}$$

avec $(a,b,c,d) \in \mathbb{C}^4$.

$$\frac{4}{(X+i)^2} = b + a(X-i) + (X-i)^2\left(\frac{c}{X+i} + \frac{d}{(X+i)^2}\right)$$

On remplace X par i :

$$-1 = \frac{4}{(2i)^2} = b$$

$$\frac{4}{(X-i)^2} = d + c(X+i) + (X+i)^2\left(\frac{a}{X-i} + \frac{b}{(X-i)^2}\right)$$

On remplace X par $-i$:

$$-1 = \frac{4}{(2i)^2} = d$$

donc

$$\frac{4}{(X-i)^2(X+i)^2} + \frac{1}{(X-i)^2} + \frac{1}{(X+i)^2} = \frac{a}{X-i} + \frac{c}{X+i}$$

donc
$$\frac{4+(X+i)^2+(X-i)^2}{(X-i)^2(X+i)^2}=\frac{a}{X-i}+\frac{c}{X+i}$$
donc
$$\frac{4+X^2+\cancel{2iX}-1+X^2-\cancel{2iX}-1}{(X-i)^2(X+i)^2}=\frac{a}{X-i}+\frac{b}{X+i}$$
donc
$$\frac{\cancel{2(X-i)(X+i)}}{(X-i)^{\cancel{2}}(X+i)^{\cancel{2}}}=\frac{a}{X-i}+\frac{c}{X+i}$$
donc
$$\frac{2}{(X-i)(X+i)}=\frac{a}{X-i}+\frac{c}{X+i}$$
donc
$$\frac{2}{X+i}=a+c\frac{X-i}{X+i}$$
et donc
$$-i=\frac{2}{2i}=a$$
On a aussi
$$\frac{2}{X-i}=c+a\frac{X+i}{X-i}$$
donc
$$i=\frac{2}{-2i}=c$$
Donc,
$$\frac{4}{(X^2+1)^2}=-\frac{i}{X-i}-\frac{1}{(X-i)^2}+\frac{i}{X+i}-\frac{1}{(X+i)^2}$$

3.
$$\frac{1}{X(X-1)^2}=\frac{a}{X}+\frac{b}{X-1}+\frac{c}{(X-1)^2}\text{ avec }a,b,c\in\mathbb{C}$$
$a=1$, $c=1$
$$\begin{aligned}\frac{1}{X(X-1)^2}-\frac{1}{X}-\frac{1}{(X-1)^2}&=\frac{1-(X-1)^2-X}{X(X-1)^2}\\&=\frac{\cancel{1}-X^2+2X-\cancel{1}-X}{X(X-1)^2}\\&=\frac{X(1-X)}{X(X-1)^2}\\&=-\frac{1}{X-1}=\frac{b}{X-1}\end{aligned}$$

Donc, $b=-1$.
$$f:x\longmapsto\frac{1}{x(x-1)^2}=\frac{1}{x}-\frac{1}{x-1}+\frac{1}{(x-1)^2}$$
Une primitive de f est
$$x\mapsto\ln(|x|)-\ln(|x-1|)-\frac{1}{x-1}$$

9.

$$A = \frac{3}{(X^3-1)^2}$$

Racines du dénominateur : 1, j et j^2

$$A = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{(X-j)^2} + \frac{d}{X-j} + \frac{e}{(X-j^2)^2} + \frac{f}{X-j^2}$$

On a $a = \frac{1}{3}$.

$$\begin{aligned} c &= \frac{3}{(X-1)^2(X-j^2)^2} \\ &= \frac{3}{(j-1)^2(j-j^2)^2} \\ &= \frac{3}{(j^2-2j+1)(j^2-2+j)} \\ &= \frac{3}{(-3j)(-3)} \\ &= \frac{1}{3j} = \frac{1}{3}j^2 \end{aligned}$$

$$\begin{aligned} e &= \frac{3}{(j^2-1)^2(j^2-j)^2} \\ &= \frac{3}{(j-2j^2+1)(j-2+j^2)} \\ &= \frac{3}{(-3j^2)(-3)} \\ &= \frac{1}{3j^2} = \frac{1}{3}j \end{aligned}$$

$$\begin{aligned}
\frac{3}{(X-1)^2}-\frac{a}{(X-1)^2}-\frac{c}{(X-j)^2}-\frac{e}{(X-j^2)^2} &= \frac{b}{X-1}+\frac{d}{X-j}+\frac{f}{X-j^2} \\
&= \frac{3-\frac{1}{3}(X-j^2)(X-j^2)^2-\frac{1}{3}j^2(X-1)^2(X-j^2)^2-\frac{1}{3}j(X-1)^2(X-j)^2}{(X^3-1)^2} \\
&= -2\left(\frac{X^3-1}{(X^3-1)^2}\right) \\
&= -\frac{2}{X^3-1}
\end{aligned}$$

$$\begin{aligned}
b &= -\frac{2}{(1-j)(1-j^2)} \\
d &= -\frac{2}{(j-1)(j-j^2)} = -2j \\
b &= -\frac{2}{(j^2-1)(j^2)} = -2j^2
\end{aligned}$$

Exercice 5

1. $\deg\left(\dfrac{P''}{P}\right) < 0.$

$$\frac{P''}{P} = \sum_{i=1}^{n} \frac{a_i}{X - x_i}$$

donc

$$\forall i \in [\![1, n]\!], a_i = \frac{P''(x_i)}{P'(x_i)}.$$

2.

$$\sum_{k=1}^{n} \frac{P''(x_k)}{P'(x_k)}.$$

donc

$$\frac{P''}{P} = \lambda \frac{\sum_{i=1}^{n} a_i \prod_{j \neq i}^{n} (X - x_j)}{P} \quad \lambda \in \mathbb{C}^\star$$

Les coefficiants de X^{n-1} est $\sum_{i=1}^{n} a_i$ en développant l'expression.

Or,

$$\deg(P'') < n - 1$$

Donc

$$\sum_{i=1}^{n} a_i = 0$$

Exercice 6

$$\forall i \in [\![1, n]\!], \sum_{j=1}^{n} \frac{x_j}{a_j + \alpha_j} = 1$$

On pose

$$F = \sum_{j=1}^{n} \frac{x_j}{a_j + X} \in \mathbb{C}(X).$$

Donc,

$$(S) \iff \forall i \in [\![1, n]\!], F(\alpha_i) = 0.$$

De plus, $-1 + \sum_{j=1}^{n} \dfrac{x_j}{X + a_j}$ est la décomposition en éléments simples d'une fraction rationelle ayant pour pôles simples $-a_1, -a_2, \ldots, -a_n$.

Donc,

$$\begin{cases} F = \dfrac{P}{(X+a_1)(X+a_2)\cdots(X+a_n)} \text{ avec } P \in \mathbb{C}[X] \\ \\ \forall i \in [\![1,n]\!], F(\alpha_i) = 0. \end{cases}$$

Comme $\deg(F) = 0$, $\deg(P) = n$.

De plus,

$$\forall i \in [\![1,n]\!], P(\alpha_i) = 0$$

Donc

$$\exists \lambda \in \mathbb{C}, P = \lambda(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n).$$

Donc

$$\begin{aligned} \forall j \in [\![1,n]\!], x_j &= \frac{P(-a_j)}{\prod_{i\neq j}(-a_j+a_i} \\ &= \frac{\lambda\prod_{i=1}^{n}(-a_j-\alpha_i)}{\prod_{i\neq j}(a_i-a_j)}. \end{aligned}$$

De plus, -1 est le quotient de la division euclidienne de P par $\prod_{i=1}^{n}(X+a_i)$ c'est-à-dire λ. Donc, $\lambda = -1$.

$$\forall j \in [\![1,n]\!], x_j = \frac{(-1)^{n+1}\prod_{i=1}^{n}(a_j+\alpha_i)}{\prod\limits_{\substack{1\leqslant i\leqslant n \\ i\neq j}}(a_i-a_j)}.$$

Exercice 7

1. $$\left(\frac{P'}{P}\right)' = \frac{P''P - P'^2}{P^2}.$$

   On note $x_1 \leqslant \cdots \leqslant x_n$ les racines (réelles) de P. Pour tout $x \notin \{x_1,\ldots,x_n\}$, $P'(x)^2 - P''(x)P(x)$ est du signe opposé à $f'(x)$ où $f : x \mapsto \dfrac{P'(x)}{P(x)}$.

   Or,

   $$\forall x \notin \{x_1,\ldots,x_n)\}, f(x) = \sum_{i=1}^{n}\frac{1}{x-x_i}$$

   et donc

   $$\forall x \notin \{x_1,\ldots,x_n\}, f'(x) = \sum_{i=1}^{n}\frac{-1}{(x-x_i)^2} < 0$$

donc

$$\forall x \notin \{x_1, \ldots, x_n\}, P'(x)^2 - P''(x)P(x) > 0$$

par continuuité, on a donc

$$\forall x \in \mathbb{R}, P'(x)^2 - P''(x)P(x) \geqslant 0.$$

2. D'après la formule de Taylor,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k.$$

D'où

$$\forall k \in [\![0, n]\!], a_k = \frac{P^{(k)}(0)}{k!}.$$

D'où, d'après 1. :

$${a_1}^2 - 2a_2a_0 \geqslant 0$$

Donc si $a_0a_2 \geqslant 0$,

$$a_0a_2 \leqslant 2a_0a_2 \leqslant {a_0}^2$$

et si $a_0a_2 \leqslant 0$,

$$a_0a_2 \leqslant 0 \leqslant {a_0}^2$$

Soit $k \in \mathbb{N}^\star$. On a aussi, comme $P^{(k-1)}$ est scindé on a

$$P^{(k)}(0)^2 - P^{(k+1)}(0)P^{(k-1)}(0) \geqslant 0$$

donc

$$(k!)^2 a_k^2 - (k+1)!(k-1)!a_{k+1}a_{k-1} \geqslant 0$$

$$a_k^2 \geqslant \frac{k}{k+1} a_k^2 \geqslant a_{k+1}a_{k-1}$$

Chapitre 21

TD 21

Exercice 1

Soit φ l'endomorphisme de $\mathbb{R}_n[X]$ défini par $\varphi(P) = P(X+1)$.

1. La base canonique de $\mathbb{R}_n[X]$ est $\mathcal{B} = (1, X, X^2, \ldots, X^n)$.

$$\begin{aligned}\forall k \in [\![1, n]\!],\ \varphi(X^k) &= (X+1)^k \\ &= \sum_{i=0}^{k} \binom{k}{i} X^i\end{aligned}$$

Donc,

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

2.

$$A \text{ est inversible} \iff \varphi \text{ bijective}$$

On pose $\psi : \begin{array}{ccc} \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}_n[X] \\ P & \longmapsto & P(X-1) \end{array}$

φ et ψ sont réciproques l'une de l'autre donc

$$A^{-1} = \mathrm{Mat}_{\mathcal{B}}(\psi).$$

$$\begin{aligned}\forall k \in [\![1,n]\!]\,,\ \psi(X^k) &= (X-1)^k \\ &= \sum_{i=0}^{k} \binom{k}{i} X^i (-1)^{k-i}\end{aligned}$$

Donc,

$$A^{-1} = \begin{pmatrix} 1 & -1 & 1 & \cdots & (-1)^n \\ 0 & 1 & -2 & \cdots & (-1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Exercice 2

Soit $a \in \mathbb{C}^\star$ et $f : z \mapsto z + a\overline{z}$.

1. $\forall x \in \mathbb{C}, f(x) \in \mathbb{C}$.

   Soient $(x,y) \in \mathbb{C}^2$ et $(\lambda,\mu) \in \mathbb{R}^2$.

   $$\begin{aligned} f(\lambda x + \mu y) &= (\lambda x + \mu y) + a\overline{(\lambda x + \mu y)} \\ &= \lambda x + \mu y + a\lambda\overline{x} + a\mu\overline{y} \\ &= \lambda(x + a\overline{x}) + \mu(y + a\overline{y}) \\ &= \lambda f(x) + \mu f(y) \end{aligned}$$

   Donc $f \in \mathscr{L}(\mathbb{C})$.
2. $f(1) = 1 + a \times 1 = a + 1$
   $f(i) = i + a \times (-i) = i(a-1)$

   $$M = \mathrm{Mat}_{(1,i)}(f) = \begin{pmatrix} 1 + \mathfrak{Re}(a) & \mathfrak{Im}(a) \\ \mathfrak{Im}(a) & \mathfrak{Re}(a) - 1 \end{pmatrix}$$
3. Soit $z \in \mathbb{C}$. On pose $z = x + iy$ avec $x, y \in \mathbb{R}$.

   $$M \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + x\,\mathfrak{Re}(a) + y\,\mathfrak{Im}(a) \\ x\,\mathfrak{Im}(a) + y - y\,\mathfrak{Re}(a) \end{pmatrix}$$

   $$\begin{aligned} \det(M) &= \big(1 + \mathfrak{Re}(a)\big)\big(-\mathfrak{Re}(a) + 1\big) - \mathfrak{Im}(a)^2 \\ &= 1 - \mathfrak{Re}(a)^2 - \mathfrak{Im}(a)^2 \\ &= 1 - |a|^2 \end{aligned}$$

   Si $a \neq 1$, $\mathrm{Ker}(f) = \{0\}$. Si $a = 1$,

Cas 1 $\mathfrak{Re}(a) = -1$, alors

$$\begin{cases} 0 = 0 \\ y = 0. \end{cases}$$

On a

$$\mathrm{Ker}(f) = \mathrm{Vect}(e_1) = \mathrm{Vect}(1) = \mathbb{R}$$

Cas 2 $\mathfrak{Re}(a) \neq -1$, alors

$$\left\{ x = \frac{-y\mathfrak{Im}(a)}{1 + \mathfrak{Re}(a)} \right.$$

et donc

$$z = y\left(\frac{-\mathfrak{Im}(a)}{1 + \mathfrak{Re}(a)} - i\right)$$

On a

$$\mathrm{Ker}(f) = \mathrm{Vect}\left(-\mathfrak{Im}(a) + i(1 + \mathfrak{Re}(a))\right)$$

4.

$$\begin{aligned} \dim(\mathrm{Im}\, f) &= \dim(\mathbb{C}) - \dim(\mathrm{Ker}\, f) \\ &= 1 \end{aligned}$$

Donc, si $\mathfrak{Re}(a) \neq -1$,

$$\mathfrak{Im}(f) = \mathrm{Vect}(1 + a)$$

sinon

$$\mathfrak{Im}(f) = \mathrm{Vect}(2i) = i\mathbb{R}$$

Exercice 4

$$\forall P \in \mathbb{R}_n[X], \int_0^1 P(t)\, dt = \sum_{i=0}^{n} \lambda_i P(a_i)$$

On pose

$$\begin{aligned} f : \mathbb{R}_n[X] &\longrightarrow \mathbb{R} \\ P &\longmapsto \int_0^1 P(t)\, dt. \end{aligned}$$

$$\forall P \in \mathbb{R}_n[X],\ f(P) = \sum_{i=0}^{n} \lambda_i P(a_i)$$

On pose

$$\begin{aligned} g_i : \mathbb{R}_n[X] &\longrightarrow \mathbb{R} \\ P &\longmapsto P(a_i). \end{aligned}$$

On doit montrer : $\boxed{\forall P \in \mathbb{R}_n[X], f(P) = \sum_{i=0}^{n} \lambda_i \, g_i(P).}$

$\mathscr{B} = (g_0, \ldots, g_n)$ est une base de $\mathbb{R}_n[X]^\star$. Soit $\mathscr{C} = (1, X, \ldots, X^n)$ la base canonique de $\mathbb{K}_n[X]$.

On a $g_1(1) = 1$, $g_1(X) = a_1$, …, $g_1(X^n) = {a_1}^n$

Donc,

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ {a_0}^n & {a_1}^n & \cdots & {a_n}^n \end{pmatrix}$$

${}^tA = \mathrm{Mat}_{\mathscr{C}}(D)$ où D est la base des polynômes interpolateurs de Lagrange.

Donc ${}^tA$ inversible et donc A inversible.

Exercice 5

$\dim(E) = n$ et $f \in \mathscr{L}(E)$. On suppose $f \circ f = 0$.

Anaylyse Soit $\mathscr{B} = (u_1, \ldots, u_n)$ une base de E telle que

$$\mathrm{Mat}_{\mathscr{B}}(f) = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ & & & 0 & & 0 \\ & & & \vdots & & \vdots \\ & & & & \ddots & \\ & & & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & & & 0 \\ \vdots & & \vdots & & & \vdots \\ 0 & \cdots & 0 & & & 0 \end{array}\right)$$

$$\forall i \leqslant n - p, f(u_i) = 0$$

$$\forall i > n - p, f(u_i) = u_{i-n+p}$$

i.e.

$$\begin{cases} u_1 = f(u_{n-p+1}) \\ u_2 = f(u_{n-p+2}) \\ \vdots \\ u_p = f(u_n) \end{cases}$$

Synthèse Soit F tel que $\mathrm{Ker}(f) \oplus F = E$. On pose $p = \dim(F)$ et $\mathscr{C} = (v_1, \ldots, v_p)$ une base de F.

$$\forall i, u_{n-p+i} = v_i$$

$u_i = f(u_{n-p+i})$ pour $i \in [\![1, p]\!]$

La famille $(u_1, \dots, u_p, u_{n-p+1}, \dots, u_n)$ est-elle libre ?

Soit F un supplémentaire de $\mathrm{Ker}(f)$:

$$\mathrm{Ker}(f) \oplus F = E$$

On pose $p = \dim(F)$ et $(v_1, \dots, v_p)$ une base de F.

$$\begin{cases} u_{n-p+1} = v_1 \\ u_{n-p+2} = v_2 \\ \vdots \\ u_n = v_p \end{cases}$$

On pose aussi

$$\begin{cases} u_1 = f(u_{n-p+1}) = f(v_1) \\ u_2 = f(u_{n-p+2}) = f(v_2) \\ \vdots \\ u_p = f(u_n) = f(v_p). \end{cases}$$

$$\forall i \in [\![1, p]\!], f(u_i) = f\big(f(v_i)\big) = 0$$

donc

$$\forall i \in [\![1, p]\!], u_i \in \mathrm{Ker}(f).$$

Montrons que $(u_1, \dots, u_p)$ est libre. Soit $(\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p$. On suppose

$$\sum_{i=1}^{p} \lambda_i u_i = 0.$$

Donc

$$\sum_{i=0}^{p} \lambda_i f(v_i) = 0$$

donc

$$f\left(\sum_{i=1}^{p} \lambda_i v_i\right) = 0$$

donc

$$\sum_{i=0}^{p} \lambda_i v_i \in \mathrm{Ker}(f).$$

Or,

$$\sum_{i=1}^{p} \lambda_i v_i \in F.$$

Comme $F \cap \mathrm{Ker}(f) = \{0\}$:

$$\sum_{i=1}^{p} \lambda_i v_i = 0.$$

Comme $(v_1, \dots, v_p)$ est libre,

$$\forall i \in [\![1, p]\!], \lambda_i = 0.$$

On complète $(u_1,\dots,u_p)$ en une base $(u_1,\dots,u_p,u_{p+1},\dots,u_{n-p})$ de $\mathrm{Ker}(f)$ ($\dim(\mathrm{Ker}\, f)=\dim E-\dim F=n-p$. Montrons que $(u_1,\dots,u_n)$ est libre. Soit $(\mu_1,\dots,\mu_n)\in\mathbb{K}^n$. On suppose

$$\sum_{i=1}^{n}\mu_i u_i=0.$$

Donc,

$$\underbrace{\sum_{i=1}^{n-p}\mu_i u_i}_{\in\mathrm{Ker}\, f}=-\underbrace{\sum_{i=n-p+1}^{n}\mu_i u_i}_{\in F}.$$

Donc

$$\begin{cases}\displaystyle\sum_{i=1}^{n-p}\mu_i u_i=0\\ \displaystyle\sum_{i=n-p+1}^{n}\mu_i u_i=0.\end{cases}$$

Comme $(u_1,\dots,u_{n-p})$ est libre :

$$\forall i\in[\![1,n-p]\!],\mu_i=0.$$

Comme $(u_{n-p+1},\dots,u_n)$ est libre :

$$\forall i\in[\![n-p+1,n]\!],\mu_i=0.$$

Donc $(u_1,\dots,u_n)$ est libre. donc, c'est une base de E.

$$\mathrm{Mat}_{(u_1,\dots,u_n)}(f)=\left(\begin{array}{c|c}(0)&I_p\\(0)&(0)\end{array}\right)$$

Exercice 7

$\dim(E)=n$ donc $\dim\left(\mathscr{L}(E)\right)=n^2$.

On cherche $M\in\mathscr{M}_n(\mathbb{K})$ telle que $M^2=M$.

$$\forall i\in[\![1,n]\!],e_{i,i}^2=e_{i,i}$$

$$(e_{k,\ell}+e_{i,i})^2=e_{i,i}+e_{k,\ell}e_{i,i}+e_{k,\ell}^2+e_{i,i}e_{k,\ell}$$

$$e_{i,j}e_{k,\ell}=\begin{cases}0 & \text{si } k\neq j\\ e_{i,\ell} & \text{sinon}\end{cases}$$

Cas 1 $\ell\neq k$ et $i\neq k$

Cas 2 $\ell \neq k$ et $i = k$ donc, $e_{i,i} + e_{i,\ell}$

$$n(n-1) = n^2 - n$$

$(e_{i,j})$ libre

$(e_{11}, \ldots, e_{1,n}, e_{12} + e_{11}, \ldots, e_{i,1}, \ldots, e_{i,i}, \ldots)$.

Exercice 8

Partie I.

1. (a) Soit $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$.

$$\begin{aligned}
x \in \operatorname{Ker} f &\iff f(x) = 0 \\
&\iff \operatorname{Mat}_{\mathcal{B}}\big(f(x)\big) = \operatorname{Mat}_{\mathcal{B}}(0) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\
&\iff A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\
&\iff \begin{pmatrix} x_n \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\
&\iff x_n = 0 \\
&\iff x = (x_1, \ldots, x_{n-1}, 0) \\
&\qquad = \sum_{i=1}^{n-1} x_i e_i
\end{aligned}$$

Donc $\boxed{\operatorname{Ker} f = \operatorname{Vect}(e_1, \ldots, e_{n-1})}$.

D'après le théorème du rang,

$$\begin{aligned}
\operatorname{rg} f &= \dim \mathbb{R}^n - \dim(\operatorname{Ker} f) \\
&= n - (n-1) = 1.
\end{aligned}$$

De plus,

$$\operatorname{Mat}_{\mathcal{B}}\big(f(e_n)\big) = A \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \operatorname{Mat}_{\mathcal{B}}(e_1)$$

donc $f(e_n) = e_1 \neq 0$.

Donc, $\boxed{\operatorname{Im} f = \operatorname{Vect}\big(f(e_n)\big) = \operatorname{Vect}(e_1)}$.

On constate que

$$\boxed{\operatorname{Im} f \subset \operatorname{Ker} f}.$$

Soit $x \in \mathbb{R}^n$. Comme $f(x) \in \operatorname{Im} f \subset \operatorname{Ker} f$,

$$f\big(f(x)\big) = 0 \text{ donc } f^2 = 0.$$

donc $\boxed{f \text{ est nilpotent}}$. Comme $A \neq 0$, f est nilpotent $\boxed{\text{d'indice 2}}$.

Soit $x = (x_1, \dots, x_n) \in \mathbb{R}^n$.

$$\begin{aligned} x \in \operatorname{Ker} g &\iff B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\ &\iff \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\ &\iff x_1 = 0 \end{aligned}$$

On en déduit que

$$\boxed{\operatorname{Ker} g = \operatorname{Vect}(e_2, \dots, e_n)}.$$

De plus, $g(e_1) = e_n \neq 0$ donc

$$\boxed{\operatorname{Im} g = \operatorname{Vect}(e_n)}$$

et

$$\boxed{\operatorname{Im} g \subset \operatorname{Ker} g}$$

donc $\boxed{g \text{ est nilpotente d'indice 2}}$.

(b)

$$\begin{aligned} A^2 &= \operatorname{Mat}_{\mathcal{B}}(f)^2 \\ &= \operatorname{Mat}_{\mathcal{B}}(f \circ f) \\ &= \operatorname{Mat}_{\mathcal{B}}(0) \\ &= 0 \end{aligned}$$

Par récurrence,

$$\boxed{\forall k \geqslant 2, A^k = 0}, \; A^1 = \begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ et } A^0 = I_n.$$

De même,

$$\boxed{\forall k \geqslant 2, B^k = 0}, \; B^1 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 0 \end{pmatrix} \text{ et } B^0 = I_n.$$

(c) Soit $k \in \mathbb{N}^\star$.

$$(A+B)^k = \mathrm{Mat}_{\mathscr{B}}\left((f+g)^k\right)$$

Soit $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$.

$$\begin{aligned}(f+g)(x) &= (x_n, 0, \ldots, 0) + (0, \ldots, 0, x_1) \\ &= (x_n, 0, \ldots, 0, x_1)\end{aligned}$$

.

$$\begin{aligned}(f+g)^2(x) &= (f+g)(x_n, 0, \ldots, x_1) \\ &= (x_1, 0, \ldots, 0, x_n)\end{aligned}$$

On en déduit par récurrence que

$$\forall k \in \mathbb{N}^\star, \forall x = (x_1, \ldots, x_n) \in \mathbb{R}^n, \begin{cases}(f+g)^{2k}(x) = (x_1, 0, \ldots, 0, x_n) \\ (f+g)^{2k+1}(x) = (x_n, 0, \ldots, 0, x_1)\end{cases}$$

D'où

$$\boxed{\forall k \in \mathbb{N}^\star, \begin{cases}(A+B)^{2k} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \neq 0 \\ (A+B)^{2k+1} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ & & & & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & & & & \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} \neq 0.\end{cases}}$$

Donc, $\boxed{A+B \text{ n'est pas nilpotente}}$.

(d)

$$\boxed{AB = \mathrm{Mat}_{\mathscr{B}}(f \circ g) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}}$$

car $f \circ g(e_1) = f(e_n) = e_1$
et $\forall k \geqslant 2, f(e_k) = 0$.

$$\boxed{BA = \mathrm{Mat}_{\mathcal{B}}(g \circ f) = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdot & 1 \end{pmatrix}}$$

car $\forall k < n, g \circ f(e_k) = g(0) = 0$
et $g \circ f(e_n) = g(e_1) = e_n$.

De plus,

$$\begin{aligned} \forall x = (x_1, \ldots, x_n) \in \mathbb{R}^n, (f \circ g)^2(x) &= f \circ g(x_1, 0, \ldots, 0) \\ &= (x_1, 0, \ldots, 0) \\ &= f \circ g(x) \end{aligned}$$

donc $(AB)^2 = AB$ et donc

$$\boxed{\forall k \geqslant 1, (AB)^k = AB \neq 0}.$$

De même,

$$(g \circ f)^2 = g \circ f$$

et donc

$$\boxed{\forall k \geqslant 1, (BA)^k = BA \neq 0}.$$

Ainsi, $\boxed{\text{ni } AB \text{ ni } BA \text{ ne sont nilpotentes}}$.

(e) $N_n(\mathbb{R})$ n'est pas stable par somme, donc ce n'est pas un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ et a fortiori ce n'est pas une sous-algèbre.

2. (a) Soit $(\lambda_0, \ldots, \lambda_{p-1}) \in \mathbb{R}^p$. On suppose

$$\sum_{i=0}^{p-1} \lambda_i f^i(e_1) = 0.$$

Pour $k \in [\![0, p-1]\!]$,

$$f^k \left(\sum_{i=0}^{p-1} \lambda_i f^i(e_1) \right) = 0$$

i.e.

$$\sum_{i=0}^{p-1} \lambda_i \underbrace{f^{k+i}(e_1)}_{=0 \text{ si } k+1 \geqslant p} = 0$$

i.e.

$$\sum_{i=0}^{p-k-1} \lambda_i f^{k+i}(e_1) = 0.$$

En particulier, avec $k = p-1$:

$$\lambda_0 \underbrace{f^{p-1}(e_1)}_{\neq 0} = 0$$

donc $\lambda_0 = 0$. Avec $k = p-2$:

$$\underbrace{\lambda_0 f^{p-2}(e_1)}_{=0} + \lambda_1 \underbrace{f^{p-1}(e_1)}_{\neq 0} = 0$$

donc $\lambda_1 = 0$.

De proche en proche,

$$\forall i \in [\![0, p-1]\!], \lambda_i = 0.$$

La famille $\left(f^{p-1}(e_1), \dots, f(e_1), e_1\right)$ a p vecteurs et $\dim(\mathbb{R}^n) = n$ donc $\boxed{p \leqslant n}$.

(b) Soit g nilpotent d'indice p. D'après 2.(a), $p \leqslant n$.

D'où

$$\begin{aligned} g^n &= g^p \circ g^{n-p} \\ &= 0 \circ g^{n-p} \\ &= 0 \end{aligned}$$

3. (a) On sait que $\mathscr{C} = \left(f^2(e_1), f(e_1), e_1\right)$ est libre. Elle a $\dim(\mathbb{R}^3)$ vecteurs donc c'est une base de $\mathbb{R}^3$.

$$\boxed{\mathrm{Mat}_{\mathscr{C}}(f) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}}$$

car $f\left(f^2(e_1)\right) = 0$, $f\left(f(e_1)\right) = f^2(e_1)$, $f(e_1) = 0 \cdot f^2(e_1) + 1 \cdot f(e_1) + 0 \cdot e_1$

(b) Soit $x \in \mathrm{Im}\, f$. On considère $a \in \mathbb{R}^n$ tel que $x = f(a)$.

D'où $f(x) = f\left(f(a)\right) = f^2(a) = 0$ et donc $x \in \mathrm{Ker}\, f$.

On a montré $\underline{\mathrm{Im}\, f \subset \mathrm{Ker}\, f}$. et donc

$$\dim(\mathrm{Im} f) \leqslant \dim(\mathrm{Ker}\, f)$$

D'après le théorème du rang,

$$3 = \dim(\mathrm{Im}\, f) + \dim(\mathrm{Ker}\, f)$$

$f \neq 0$ donc $\dim(\mathrm{Im}\, f) > 0$. Donc, $\boxed{\dim(\mathrm{Im}\, f) = 1 \text{ et } \dim(\mathrm{Ker}\, f) = 2}$.

$f(e_1) \neq 0$ et $f(e_1) \in \mathrm{Ker}\, f$ donc $\left(f(e_1)\right)$ est une famille libre de $\mathrm{Ker}\, f$. Comme $\dim(\mathrm{Ker}\, f) = 2$, d'après le théorème de la base incomplète, il existe $e_3 \in \mathrm{Ker}\, f$ tel que $\left(f(e_1), e_3\right)$ soit une base de $\mathrm{Ker}\, f$.

Soit $(\alpha,\beta,\gamma)\in\mathbb{R}^3$. On suppose

$$\alpha f(e_1)+\beta e_1+\gamma e_3=0$$

donc, en applicant f,

$$\beta\underbrace{f(e_1)}_{\neq 0}=0$$

donc $\beta=0$ et donc

$$\alpha f(e_1)+\gamma e_3=0.$$

Or, $\big(f(e_1),e_3\big)$ est libre donc $\alpha=\gamma=0$.

Donc, $\mathcal{D}=\big(f(e_1),e_1,e_3\big)$ est une base de $\mathbb{R}^3$ et

$$\boxed{\mathrm{Mat}_{\mathcal{D}}(f)=\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}}.$$

4.

5. (c) Soit $M\in N_n(\mathbb{R})$. D'après 4., il existe $P\in \mathrm{GL}_n(\mathbb{R})$ tel que

$$PMP^{-1}=\left(\begin{array}{c|ccc}0&\star&\dots&\star\\\hline\star&\ddots&\ddots&\vdots\\\hline\vdots&\ddots&\ddots&\star\\\hline\star&\dots&\star&0\end{array}\right)$$

De plus, d'après (2b),

$$\mathrm{tr}\left(P(MP^{-1})\right)=\mathrm{tr}\left((MP^{-1})P\right)=\mathrm{tr}(M).$$

Comme les blocs diagonaux de PMP^{-1} sont nuls, $\mathrm{tr}(PMP^{-1})=0$.

Donc $M\in\mathrm{Ker}(\mathrm{tr})$. On a prouvé

$$N_n(\mathbb{R})\subset\mathrm{Ker}(\mathrm{tr})$$

Ker(tr) est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ donc

$$\mathrm{Vect}\left(N_n(\mathbb{R})\right)\subset\mathrm{Ker}(\mathrm{tr})$$

6. (a) $E_{12}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ donc $E_{12}\in N_2(\mathbb{R})$.

$E_{12}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ donc $E_{12}\in N_2(\mathbb{R})$.

$N^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ donc $N\in N_2(\mathbb{R})$.

(b)

$$M=a\begin{pmatrix}1&-1\\1&-1\end{pmatrix}+(b-a)\begin{pmatrix}0&1\\0&0\end{pmatrix}+(c+a)\begin{pmatrix}0&0\\1&0\end{pmatrix}$$

$\in\mathrm{Vect}(N,E_{12},E_{21})$

(c)
$$\mathrm{Ker}(\mathrm{tr}) \subset \mathrm{Vect}(N, E_{12}, E_{21}) \subset \mathrm{Vect}\left(N_2(\mathbb{R})\right) \subset \mathrm{Ker}(\mathrm{tr})$$

7. (a)
$$E_{ij}^2 = (a_{k,\ell})$$
où
$$\forall k,\ell,\ a_{k,\ell} = \sum_{m=0}^{n} \underbrace{\delta_{i,j}^{k,m}}\ \delta_{i,j}^{m,\ell} = \begin{cases} 0 & \text{si } i \neq k \text{ et } j \neq m \\ 1 & \text{sinon} \end{cases}$$

Soit $m \in [\![0, n]\!]$.

$$\delta_{i,j}^{k,m}\,\delta_{i,j}^{m,\ell} \neq 0 \iff \begin{cases} k = i\ m = j \\ m = i \\ \ell = j \end{cases} \implies i = j$$

Comme $i \neq j$, $E_{ij}^2 = 0$.

$$\begin{aligned} N_i^2 &= E_{11}^2 - E_{11}E_{1i} + E_{11}E_{i1} - E_{11}E_{ii} - E_{1i}E_{11} + E_{1i}^2 - E_{1i}E_{i1} \\ &\quad + E_{1i}E_{ii} + E_{i1}E_{i1} + E_{i1}^2 - E_{i1}E_{ii} - E_{ii}E_{11} + E_{ii}E_{1i} - E_{ii}E_{i1} \\ &\quad + E_{ii}^2 \\ &= \cancel{E_{11}} - \cancel{E_{1i}} - \cancel{E_{11}} + \cancel{E_{1i}} + \cancel{E_{i1}} - \cancel{E_{ii}} - \cancel{E_{i1}} + \cancel{E_{ii}} \\ &= 0 \end{aligned}$$

(b) Soit $(\lambda_{i,j})_{i\neq j} \in \mathbb{R}^{n^2-n}$ et $(\mu_i)_{2\leqslant u\leqslant n} \in \mathbb{R}^{n-1}$.

On suppose que
$$\sum_{1\leqslant i\neq j\leqslant n} \lambda_{i,j}E_{i,j} + \sum_{i=2}^{n} \mu_i N_i = 0.$$

Soit $(k,\ell) \in [\![1,n]\!]^2$. Le coefficient en position (k,ℓ) de la combinaison ci-dessus est :

$$\begin{aligned} &\sum_{1\leqslant i\neq j\leqslant n} \lambda_{i,j}\delta_{i,j}^{k,\ell} + \sum_{i=2}^{n} \mu_i \left(\delta_{1,1}^{k,\ell} - \delta_{1,i}^{k,\ell} + \delta_{1,i}^{k,\ell} - \delta_{i,i}^{k,\ell}\right) \\ &= \delta_{11}^{k,\ell}\left(\sum_{i=2}^{n} \mu_i\right) - \sum_{i=2}^{n} \mu_i \delta_{i,i}^{k,\ell} + \sum_{i=2}^{n} (\lambda_{1,i} - \mu_i)\delta_{1i}^{k\ell} + \sum_{i=2}^{n} (\lambda_{i,1} + \mu_i)\delta_{i,1}^{k,\ell} + \sum_{2\leqslant i\neq j\leqslant n} \lambda_{i,j}\delta_{i,j}^{k,\ell} \end{aligned}$$

Soit (k,ℓ) avec $\begin{cases} 2 \leqslant k \leqslant n, \\ 2 \leqslant \ell \leqslant n, \\ k \neq \ell. \end{cases}$

Alors

$$\begin{cases} \delta_{11}^{k,\ell} = 0 \\ \forall i \in [\![2,n]\!], \delta_{i,i}^{k,\ell} = 0 \\ \forall i \in [\![2,n]\!], \delta_{1,i}^{k,\ell} = 0 \\ \forall i \in [\![2,n]\!], \delta_{i,1}^{k,\ell} = 0 \\ \forall i \neq j \in [\![2,n]\!], \delta_{i,j}^{k,\ell} = 0 \text{ sauf si } \begin{cases} k = i \\ j = \ell \end{cases} \end{cases}$$

et donc $\lambda_{k,\ell} = 0$.

Soit $\ell \in [\![2,n]\!]$ et $k = 1$.

$$\begin{cases} \delta_{11}^{k,\ell} = 0 \\ \forall i \in [\![2,n]\!], \delta_{i,i}^{k,\ell} = 0 \\ \forall i \in [\![2,n]\!], \delta_{1,i}^{k,\ell} \neq 0 \iff i = \ell \\ \forall i \in [\![2,n]\!], \delta_{i,1}^{k,\ell} = 0 \\ \forall i \neq j \in [\![2,n]\!], \delta_{i,j}^{k,\ell} = 0 \end{cases}$$

donc $\lambda_{1,\ell} - \mu_\ell = 0$.

De même,

$$\begin{cases} \forall k \in [\![2,n]\!], \lambda_{k1} + \mu_k = 0 \\ \forall k \in [\![2,n]\!], -\mu_k = 0 \end{cases}$$

Ainsi

$$\begin{cases} \forall k \neq \ell, \lambda_{k,\ell} = 0 \\ \forall k \geqslant 2, \mu_k = 0 \end{cases}$$

donc la famille est libre.

On a trouvé une famille libre consituée de $n^2 - n + n - 1 = n^2 - 1$ matrices dans $\text{Vect}\left(N_n(\mathbb{R})\right)$ donc

(c)

$$\dim\left(\text{Vect}\left(N_n(\mathbb{R})\right)\right) \geqslant n^2 - 1.$$

Or

$$\text{Vect}\left(N_n(\mathbb{R})\right) \subset \text{Ker}(\text{tr})$$

donc

$$\dim\left(\text{Vect}\left(N_n(\mathbb{R})\right)\right) \leqslant \dim(\text{Ker}\,\text{tr}) = n^2 - 1.$$

Donc

$$\dim\left(\text{Vect}\left(N_n(\mathbb{R})\right)\right) = n^2 - 1 = \dim(\text{Ker}\,\text{tr})$$

Comme $\text{Vect}\left(N_n(\mathbb{R})\right) \subset \text{Ker}(\text{tr})$,

$$\boxed{\text{Vect}\left(N_n(\mathbb{R})\right) = \text{Ker}(\text{tr}).}$$

(d) $\text{Card}(\mathscr{F}_n) = \dim\left(\text{Vect}\left(N_n(\mathbb{R})\right)\right)$ et $\mathscr{F}_n$ est libre, donc $\mathscr{F}_n$ est une base de $\text{Vect}\left(N_n(\mathbb{R})\right)$.

Chapitre 22

TD 22

Exercice 2

$$f(x,y) = \frac{3x^2+xy}{\sqrt{x^2+y^2}}.$$

Soit $\varepsilon > 0$. On cherche $r > 0$ tel que

$$\underbrace{\forall (x,y) \in B_{(0,0)}(r) \setminus \{(0,0)\}}_{0<\sqrt{x^2+y^2}<r}, |f(x,y) - 0| \leqslant \varepsilon.$$

Soit $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$.

$$\begin{aligned} |3x^2+xy| &\leqslant 3x^2 + |xy| \\ &\leqslant 3(x^2+y^2) + \frac{1}{2}(x^2+y^2) \\ &\leqslant \frac{7}{2}\|(x,y)\|^2 \end{aligned}$$

donc

$$\left|\frac{3x^2+xy}{\sqrt{x^2+y^2}}\right| \leqslant \frac{7}{2}\|(x,y)\|.$$

On pose $r = \dfrac{2}{7}\varepsilon > 0$. Soit $(x,y) \in B_{(0,0)}(r) \setminus \{(0,0)\}$.

Alors

$$|f(x,y)| \leqslant \frac{7}{2}\|(x,y)\| < \frac{7}{2}r = \varepsilon.$$

Donc

$$f(x,y) \xrightarrow[(x,y)\to(0,0)]{} 0.$$

Exercice 3

$$f : (x,y) \mapsto \begin{cases} \dfrac{xy}{x^2+y^2} & \text{si } (x,y) \neq (0,0) \\ 0 & \text{sinon .} \end{cases}$$

Si $f(x,y) \xrightarrow[(x,y)\to(0,0)]{} 0$, alors si $x, y : I \to \mathbb{R}$ telles que $\begin{cases} x(t) \xrightarrow[t\to 0]{} 0 \\ y(t) \xrightarrow[t\to 0]{} 0 \end{cases}$ alors $f\big(x(t), y(t)\big) \xrightarrow[t\to 0]{} 0$.

On a $x(t) = t$ et $y(t) = t$. On calcule donc

$$f(x,x) = \frac{x^2}{2x^2} = \frac{1}{2} \xrightarrow[x\to 0]{} \frac{1}{2} \neq 0.$$

Donc

$$f(x,y) \xrightarrow[(x,y)\to(0,0)]{\not\longrightarrow} (0,0)$$

et donc f n'est pas continue en $(0,0)$.

Exercice 4

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto \begin{cases} 2x^2 + y^2 - 1 & \text{si } x^2 + y^2 > 1 \\ x^2 & \text{sinon} \end{cases} \end{aligned}$$

On regarde la continuité sur chacun des morceaux ouverts, puis sur les points du bord.

Soit $(x_0, y_0) \in \mathbb{R}^2$.

Cas 1 On suppose que ${x_0}^2 + {y_0}^2 > 1$.

On doit montrer :

$$\boxed{\forall \varepsilon > 0, \exists r > 0, \forall (x,y) \in \mathbb{R}^2, \quad \|(x,y) - (x_0,y_0)\| \leqslant r \implies |f(x,y) - f(x_0,y_0)| \leqslant \varepsilon}$$

Soit (x,y) vérifiant $x^2 + y^2 > 1$.

$$\begin{aligned} |f(x,y) - f(x_0,y_0)| &= \big|2x^2 + y^2 - 1 - 2x_0^2 - y_0^2 + 1\big| \\ &= \big|2(x^2 - x_0^2) + (y^2 - y_0^2)\big| \\ &\leqslant 2|x^2 - x_0^2| + |y^2 - y_0^2| \\ &\leqslant 2\|(x,y) - (x_0,y_0)\| + \|(x,y) - (x_0,y_0)\| \quad \leqslant 3\|(x,y) - (x_0,y_0)\| \end{aligned}$$

On pose $R = \sqrt{x_0^2 + y_0^2} - 1$. Soit $\varepsilon > 0$. On pose $r = \frac{1}{2}\min\left(\frac{\varepsilon}{3}, R\right)$.

Ainsi, $r < R$ et $r < \frac{\varepsilon}{3}$.

Soit $(x, y) \in B_{(x_0,y_0)}(r)$. Alors, comme $r < R$, $x^2 + y^2 > 1$ et donc

$$\left|f(x, y) - f(x_0, y_0)\right| \leqslant 3r < \varepsilon.$$

Cas 2 $x_0^2 + y_0^2 < 1$.

Cas 3 On suppose que $x_0^2 + y_0^2 = 1$. Soit $(x, y) \in \mathbb{R}^2$.

Si (x, y) vérifie $x^2 + y^2 > 1$:

$$\begin{aligned}\left|f(x, y) - f(x_0, y_0)\right| &= \left|2x^2 + y^2 - 1 - x_0^2\right| \\ &\leqslant \left|2x^2 + y^2 - x_0^2 - y_0^2 - x_0^2\right| \\ &\leqslant \left|2(x^2 - x_0^2) + y^2 - y_0^2\right| \\ &\leqslant 3\|(x, y) - (x_0, y_0)\|.\end{aligned}$$

Si $x^2 + y^2 \leqslant 1$:

$$\left|f(x, y) - f(x_0, y_0)\right| = \left|x^2 - x_0^2\right| \leqslant \|(x, y) - (x_0, y_0)\|$$

Soit $\varepsilon > 0$. On pose $r = \frac{\varepsilon}{6} < \frac{\varepsilon}{3}$ et donc

$$\forall (x, y) \in B_{(x_0,y_0)}(r), \left|f(x, y) - f(x_0, y_0)\right| \leqslant \varepsilon.$$

Exercice 6

1. On pose $g : (x, y) \mapsto f(y, x)$.

$$\begin{aligned}\frac{\partial g}{\partial x}(x, y) &= \frac{\partial f}{\partial x}(y, x)\,\frac{\partial y}{\partial x}(x, y) + \frac{\partial f}{\partial y}(y, x)\,\frac{\partial x}{\partial x}(x, y) \\ &= \frac{\partial f}{\partial y}(y, x)\end{aligned}$$

$$\begin{aligned}\frac{\partial g}{\partial y}(x, y) &= \frac{\partial f}{\partial x}(y, x)\,\frac{\partial x}{\partial x}(x, y) + \frac{\partial f}{\partial y}(y, x)\,\frac{\partial y}{\partial x}(x, y) \\ &= \frac{\partial f}{\partial x}(y, x)\end{aligned}$$

2. On pose $h : (x, y) \mapsto f\big(y, f(x, x)\big)$ et $k : x \mapsto f(x, x)$

$$\begin{aligned}\frac{\partial h}{\partial x}(x,y) &= \frac{\partial f}{\partial x}\big(y, f(x,x)\big)\ \frac{\partial y}{\partial x}(x,y) + \frac{\partial f}{\partial y}\big(y, f(x,x)\big)k'(x)\\ &= \frac{\partial f}{\partial y}\big(y, f(x,x)\big)\left(\frac{\partial f}{\partial x}(x,x) + \frac{\partial f}{\partial y}(x,x)\right)\end{aligned}$$

En effet, on a $\gamma : x \mapsto (x,x)$ et $\gamma'(x) = (1,1)$.

Donc $f \circ \gamma : x \mapsto f(x,x) = k(x)$.

$$\begin{aligned}k'(x) &= \langle \nabla f(x,x) \mid \gamma'(x)\rangle\\ &= \frac{\partial f}{\partial x}(x,x) + \frac{\partial f}{\partial y}(x,x).\end{aligned}$$

$$\begin{aligned}\frac{\partial h}{\partial y}(x,y) &= \frac{\partial f}{\partial x}\big(y, f(x,x)\big)\frac{\partial f}{\partial y}(x,y) + \frac{\partial f}{\partial y}\big(y, f(x,x)\big) \times 0\\ &= \frac{\partial f}{\partial x}\big(y, f(x,x)\big).\end{aligned}$$

Exercice 7

Soit $u = (a,b) \in \mathbb{R}^2$.

$$\forall t \neq 0, \Delta f(t) = \frac{f\big((0,0) - tu\big) - f(0,0)}{t} = \frac{1}{t} f(ta, tb).$$

Cas 1 $a \neq 0$. Alors,

$$\forall t \neq 0, \Delta f(t) = \frac{1}{t} t^2 b^2 \ln\big(|ta|\big) = tb^2 \ln\big(|ta|\big) \xrightarrow[t\to 0]{} 0.$$

Cas 2 $a = 0$. Alors,

$$\Delta f(t) = \frac{1}{t} \times 0 = 0 \xrightarrow[t\to 0]{} 0.$$

On trouve que

$$\forall u \in \mathbb{R}^2, \mathrm{d}f(u)(0,0) = 0.$$

On pose

$$\begin{cases} x(t) = t \\ y(t) = \begin{cases} 0 & \text{si } t = 0 \\ \sqrt{\dfrac{1}{\big|\ln\big(|t|\big)\big|}} & \text{si } t \neq 0 \end{cases} \end{cases}$$

et on a bien

$$\begin{cases} x(t) \xrightarrow[t\to 0]{} 0 \\ y(t) \xrightarrow[t\to 0]{} 0 \end{cases}$$

On a

$$\lim_{t\to 0} f\big(x(t),y(t)\big) = -1 \xrightarrow[t\to 0]{} -1 \neq f(0,0)$$

***

On a

$$\begin{cases} \dfrac{\partial f}{\partial x}(0,0) = \mathrm{d}f(1,0)(0,0) = 0, \\ \dfrac{\partial f}{\partial y} = \mathrm{d}f(0,1)(0,0) = 0. \end{cases}$$

et

$$\forall (x,y) \in \mathbb{R}^\star \times \mathbb{R}, \begin{cases} \dfrac{\partial f}{\partial x}(x,y) = \dfrac{y^2}{|x|} \times \operatorname{sgn}(x) \xrightarrow[x\to 0]{} \pm\infty \\ \dfrac{\partial f}{\partial y}(x,y) = 2y \ln\big(|x|\big). \end{cases}$$

Exercice 8

On a

$$\begin{cases} \dfrac{\partial g}{\partial x}(x,y) = \dfrac{1}{y}\left(e^{-x} - xe^{-x}\right) = \dfrac{e^{-x}}{y}(1-x) \\ \dfrac{\partial g}{\partial y}(x,y) = \dfrac{-xe^{-x}}{y^2} + \dfrac{1}{e} \end{cases}$$

$$\left.\begin{array}{l} \dfrac{\partial g}{\partial x}(x,y) = 0 \\ \dfrac{\partial g}{\partial y}(x,y) = 0 \end{array}\right\} \iff \begin{cases} x = 1 \\ y = 1 \end{cases}$$

$$\iff \begin{cases} x = 1 \\ y = 1 \end{cases}$$

On a

$$g(1,1) = \frac{1}{e} + \frac{1}{e} = \frac{2}{e}.$$

Or,

$$g(1,2) = \frac{1}{2e} + \frac{2}{e} > \frac{2}{e}$$

et

$$g\left(\frac{1}{2},1\right) = \frac{1}{2}e^{-\frac{1}{2}} + \frac{1}{e} < \frac{2}{e}$$

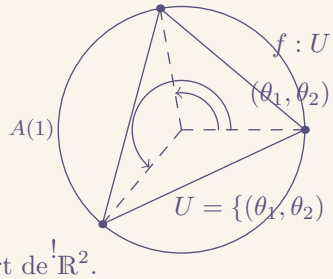
car $\dfrac{1}{2}e^{-\frac{1}{2}} < e^{-1} \iff \dfrac{1}{2} < e^{-\frac{1}{2}} \iff 2 > e^{\frac{1}{2}} \iff 4 > e.$

Donc, $(1,1)$ n'est ni un minimum, ni un maximum pour g.

Exercice 9

1. f est $\mathscr{C}^2$ donc
$$\forall h \in \mathbb{R}, f(h) = f(0) + hf'(0) + \underset{h\to 0}{o}(h)$$
donc
$$\forall (x,y) \in \mathbb{R}^2, f(x^2+y^2) = f(0) + (x^2+y^2)\, f'(0) + \underset{(x,y)\to(0,0)}{o}(x^2+y^2)$$
donc
$$\forall (x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}, F(x,y) = f'(0) + \underset{(x,y)\to(0,0)}{o}(1) \xrightarrow[(x,y)\to(0,0)]{} f'(0).$$
On pose donc $F(0,0) = f'(0)$.
2. f est de classe $\mathscr{C}^2$ donc
$$\forall (x,y) \in \mathbb{R}^2, f(x^2+y^2) = f(0)+(x^2+y^2)f'(0)+\frac{(x^2+y^2)^2}{2}f''(0)+\underset{(x,y)\to(0,0)}{o}\left(\left(x^2+y^2\right)^2\right).$$
Donc
$$\forall (x,y) \in \mathbb{R}^2\setminus\{(0,0)\}, F(x,y) = f'(0)+\frac{1}{2}(x^2+y^2)f''(0)+\underset{(x,y)\to(0,0)}{o}\left(x^2+y^2\right).$$
On en déduit que
$$\frac{\partial F}{\partial x}(0,0) = \lim_{\substack{x\to 0\\ \neq}} \frac{F(x,0)-F(0,0)}{x} = \lim_{\substack{x\to 0\\ \neq}} \left(\frac{1}{2}xf''(0) + \underset{x\to 0}{o}(x)\right) = 0$$
et
$$\frac{\partial F}{\partial y}(0,0) = \lim_{\substack{y\to 0\\ \neq}} \frac{F(0,y)-F(0,0)}{y} = 0.$$
Soit $(x,y) \neq (0,0)$.
$$\frac{\partial F}{\partial x}(x,y) = \frac{2xf'(x^2+y^2)(x^2+y^2) - 2x\big(f(x^2+y^2)-f(0)\big)}{(x^2+y^2)^2}$$
donc $\dfrac{\partial F}{\partial x}$ est continue sur $\mathbb{R}^2\setminus\{(0,0)\}$. Or, f' est $\mathscr{C}^1$ donc
$$f'(x^2+y^2) = f'(0) + (x^2+y^2)f''(0) + o(x^2+y^2)$$
d'où
$$\frac{\partial F}{\partial x}(x,y) = \frac{2x\big(f'(0)+(x^2+y^2)f''(0)+o(x^2+y^2)\big)}{x^2+y^2} - \frac{2x}{x^2+y^2}\big(f'(0)+\frac{x^2+y^2}{2}f''(0)+o(x^2+y$$
$$= x\frac{f''(0)}{2} + o(1) \xrightarrow[(x,y)\to(0,1)]{} 0 = \frac{\partial F}{\partial x}(0,0)$$
donc $\dfrac{\partial F}{\partial x}$ est continue en $(0,0)$. De même, $\dfrac{\partial F}{\partial y}$ est continue sur $\mathbb{R}^2$.
On en déduit que F est $\mathscr{C}^1$.

Exercice 10



$$f : U \longrightarrow \mathbb{R}$$
$$(\theta_1, \theta_2) \longmapsto \left|1 - e^{i\theta_1}\right| + \left|e^{i\theta_1} - e^{i\theta_2}\right| + \left|1 - e^{i\theta_2}\right|$$

où

$$U = \{(\theta_1, \theta_2) \in]0, 2\pi[^2 |\ \theta_1 < \theta_2\}$$

un ouvert de $\mathbb{R}^2$.

On a

$$\begin{cases} \left|1 - e^{i\theta_1}\right| = 2\left|\sin\dfrac{\theta_1}{2}\right|, \\ \left|1 - e^{i\theta_2}\right| = 2\left|\sin\dfrac{\theta_2}{2}\right|, \\ \left|e^{i\theta_1} - e^{i\theta_2}\right| = 2\left|\sin\dfrac{\theta_1 - \theta_2}{2}\right|. \end{cases}$$

Soit $(\theta_1, \theta_2) \in U$. Donc,

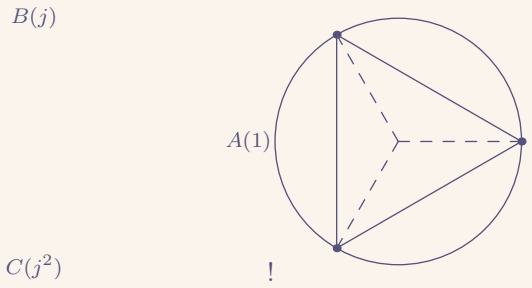
$$f(\theta_1, \theta_2) = 2\left(\sin\left(\frac{\theta_1}{2}\right) + \sin\left(\frac{\theta_2}{2}\right) + \sin\left(\frac{\theta_2 - \theta_1}{2}\right)\right)$$

On a

$$\begin{cases} \dfrac{\partial f}{\partial \theta_1}(\theta_1, \theta_2) = 2\left(\dfrac{1}{2}\cos\left(\dfrac{\theta_1}{2}\right) - \dfrac{1}{2}\cos\left(\dfrac{\theta_2 - \theta_1}{2}\right)\right), \\ \dfrac{\partial f}{\partial \theta_2}(\theta_1, \theta_2) = 2\left(\dfrac{1}{2}\cos\left(\dfrac{\theta_2}{2}\right) + \dfrac{1}{2}\cos\left(\dfrac{\theta_2 - \theta_1}{2}\right)\right). \end{cases}$$

On cherche (θ_1, θ_2) tel que

$$\begin{cases} \cos\dfrac{\theta_1}{2} - \cos\dfrac{\theta_2 - \theta_1}{2} = 0 \\ \cos\dfrac{\theta_2}{2} + \cos\dfrac{\theta_2 - \theta_1}{2} = 0 \end{cases}$$
$$\iff \begin{cases} \dfrac{\theta_2}{2} = \dfrac{\theta_2 - \theta_1}{2} \\ \pi - \dfrac{\theta_2}{2} = \dfrac{\theta_2 - \theta_1}{2} \end{cases}$$
$$\iff \begin{cases} 2\theta_1 = \theta_2 \\ 2\theta_2 - \theta_1 = 2\pi \end{cases}$$
$$\iff \begin{cases} \theta_1 = \dfrac{2\pi}{3} \\ \theta_2 = \dfrac{4\pi}{3} \end{cases}$$



Exercice 11

Il existe 4 dérivées secondes :

$$\begin{aligned}
\frac{\partial^2 f}{\partial x^2} &= \frac{\partial}{\partial x}\left(\frac{\partial f}{\partial x}\right) \\
\frac{\partial^2 f}{\partial y^2} &= \frac{\partial}{\partial y}\left(\frac{\partial f}{\partial y}\right) \\
\frac{\partial^2 f}{\partial x\,\partial y} &= \frac{\partial}{\partial x}\left(\frac{\partial f}{\partial y}\right) \\
\frac{\partial^2 f}{\partial y\,\partial x} &= \frac{\partial}{\partial y}\left(\frac{\partial f}{\partial x}\right)
\end{aligned}$$

On pose

$$\begin{aligned}
g : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\
(u,v) &\longmapsto f\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right).
\end{aligned}$$

Ainsi, $\forall (x,y) \in \mathbb{R}^2, g(x+y, x-y) = f(x,y)$.

Donc,

$$\begin{aligned}
\frac{\partial g}{\partial u}(u,v) &= \frac{\partial f}{\partial x} \times \frac{\partial x}{\partial u} + \frac{\partial f}{\partial y} \times \frac{\partial y}{\partial u} \\
&= \frac{\partial f}{\partial x} \times \frac{1}{2} + \frac{\partial f}{\partial y} \times \frac{1}{2}
\end{aligned}$$

On en déduit que

$$\begin{aligned}
\frac{\partial^2 g}{\partial v\,\partial u} &= \frac{1}{2}\left(\frac{\partial^2 f}{\partial x^2} \times \frac{\partial x}{\partial v} + \frac{\partial^2 f}{\partial y\,\partial x} \times \frac{\partial y}{\partial v} + \frac{\partial^2 f}{\partial x\,\partial y}\frac{\partial x}{\partial v} + \frac{\partial^2 f}{\partial y^2}\frac{\partial y}{\partial v}\right) \\
&= \frac{1}{2}\left(\frac{1}{2}\frac{\partial^2 f}{\partial x^2} - \frac{1}{2}\frac{\partial^2 f}{\partial y\,\partial x} + \frac{1}{2}\frac{\partial^2 f}{\partial x\,\partial y} - \frac{1}{2}\frac{\partial^2 f}{\partial y^2}\right)
\end{aligned}$$

Théorème (Schwarz) : Si f est $\mathscr{C}^2$ alors $\dfrac{\partial^2 f}{\partial x\,\partial y} = \dfrac{\partial^2 f}{\partial y\,\partial x}$.

(vu l'année prochaine)

Donc $\dfrac{\partial^2 g}{\partial u\,\partial v} = 0$.

$$\frac{\partial g}{\partial v} = F(v)$$
$$g(u,v) = G(v) + H(u)$$
$$f(x,y) = G(x-y) + H(x+y)$$

Exercice 12

1. $\begin{cases} \dfrac{\partial f}{\partial x} = xy^2 \\ \dfrac{\partial f}{\partial y} = x^2 y \end{cases}$

   Donc $f(x,y) = \dfrac{x^2y^2}{2} + \lambda$.

2. $\begin{cases} \dfrac{\partial f}{\partial x} = \dfrac{x}{\sqrt{x^2+y^2}} \\ \dfrac{\partial f}{\partial y} = \dfrac{y}{\sqrt{x^2+y^2}} \end{cases}$

   Donc $f(x,y) = \sqrt{x^2+y^2} + \lambda$.

3. $\begin{cases} \dfrac{\partial f}{\partial x} = \dfrac{x}{x^2+y^2} \\ \dfrac{\partial f}{\partial y} = -\dfrac{y}{x^2+y^2} \end{cases}$

   D'après (E_1), $f(x,y) = \dfrac{1}{2}\ln\left(x^2+y^2\right) + g(y)$

   Or,

   $\dfrac{\partial f}{\partial y} = \dfrac{y}{x^2+y^2} + g'(y) = -\dfrac{y}{x^2+y^2} \iff g'(y) = \dfrac{2y}{x^2+y^2}$ dépend de x ↯

Chapitre 23

TD 23

Exercice 1

Cours : $\#(E^n) = (\#E)^n$

On peut représenter un octet par un élément de $\{0,1\}^8$. Il y a donc $2^8 = 256$ octets.

Exercice 2

0. On peut représenter un nombre de 4 chiffres comme un élément de $[\![0,9]\!]^4$; il y en a donc $10^4 = 10\,000$.

   On peut aussi représenter un tel nombre par un entier de $[\![0,9\,999]\!]$; il y en a donc $10\,000$.
1. On représente un tel nombre par un élément de $[\![1,9]\!] \times [\![0,9]\!]^3$; il y en a $9 \times 10^3 = 9\,000$.
2. Cours :

$$A^n_{\#E} = \#\{(x_1,\dots,x_n) \in E^n \mid \forall i \neq j, x_i \neq x_j\} = (\#E)(\#E-1)\cdots(\#E-n+1)$$
$$= \frac{(\#E)!}{(\#E-n)!}$$

$$\bigcup_{x_1=1}^{9} \underbrace{\{(x_1,x_2,x_3,x_4) \mid (x_2,x_3,x_4) \in \mathcal{A}_3([\![0,9]\!] \setminus \{x_1\})\}}_{F_{x_1}}$$

On a $\#F = \sum_{x_1=1}^{9} \#F_{x_1}$.

Soit φ : $\begin{array}{rcl} F_{x_1} & \longrightarrow & \mathcal{A}_3(\llbracket 0,9\rrbracket \setminus \{x_1\}) \\ (x_1,x_2,x_3,x_4) & \longmapsto & (x_2,x_3,x_4), \end{array}$

et sa réciproque ψ : $\begin{array}{rcl} \mathcal{A}_3(\llbracket 0,9\rrbracket \setminus \{x_1\}) & \longrightarrow & F_{x_1} \\ (x_2,x_3,x_4) & \longmapsto & (x_1,x_2,x_3,x_4). \end{array}$

Donc

$$\#F_1 = A_9^3 = \frac{9!}{6!} = 7\times 8\times 9$$

et donc

$$\#F = \sum_{x_1=1}^{9} 504 = 9\times 504 = 4\,536.$$

8. Méthode 1 On note

$$F_1 = \{(x_1,x_2,x_3,x_4)\in \llbracket 1,9\rrbracket\times\llbracket 0,9\rrbracket^3 \mid \text{ parmi } (x_1,x_2,x_3,x_4), \text{ il y a 2 valeurs identiques exa}$$

$$F_2 = \{(x_1,x_2,x_3,x_4)\in \llbracket 1,9\rrbracket\times\llbracket 0,9\rrbracket^3 \mid \text{ parmi } (x_1,x_2,x_3,x_4), \text{ il y a 3 valeurs identiques exa}$$

$$F_3 = \{(x_1,x_2,x_3,x_4)\in \llbracket 1,9\rrbracket\times\llbracket 0,9\rrbracket^3 \mid \text{ parmi } (x_1,x_2,x_3,x_4), \text{ il y a 4 valeurs identiques exa}$$

$\begin{array}{rcl} F_3 & \longrightarrow & \llbracket 1,9\rrbracket \\ (x_1,x_2,x_3,x_4) & \longmapsto & x_1 \end{array}$ est une bijection donc $\#F_3 = 9$.

$$\begin{aligned} F_2 = {} & \{(x_1,x_1,x_1,x_4) \mid x_1\in\llbracket 1,9\rrbracket \text{ et } x_4\in\llbracket 0,9\rrbracket \text{ avec } x_1\neq x_4\} \\ & \cup \{(x_1,x_1,x_3,x_1) \mid x_1\in\llbracket 1,9\rrbracket \text{ et } x_3\in\llbracket 0,9\rrbracket \text{ avec } x_1\neq x_3\} \\ & \cup \{(x_1,x_2,x_1,x_1) \mid x_1\in\llbracket 1,9\rrbracket \text{ et } x_2\in\llbracket 0,9\rrbracket \text{ avec } x_1\neq x_2\} \\ & \cup \{(x_1,x_2,x_2,x_2) \mid x_1\in\llbracket 1,9\rrbracket \text{ et } x_2\in\llbracket 0,9\rrbracket \text{ avec } x_1\neq x_2\} \end{aligned}$$

On a

$$\begin{aligned} \#F_2 &= 9\times 9 + 9\times 9 + 9\times 9 + 9\times 9 \\ &= 4\times 9\times 9 = 324. \end{aligned}$$

De même,

$$\begin{aligned} \#F_1 &= 6\times 9\times 9\times 8 + 3\times 9\times 9 \\ &= 4\,131? \end{aligned}$$

Il y en a 4464.

Méthode 2 On passe au complémentaire :

$$9\,000 - 4\,536 = 4\,464.$$

Méthode 3 (fausse)

$$6\times 9\times 10\times 10 = 5\,400 \neq 4\,464.$$

4.

$$7\times 7\times 6\times 5 = 1470.$$

Exercice 3

$$\underbrace{\frac{13!}{2!\,11!}}_{M}\times\underbrace{\frac{11!}{2!\,9!}}_{A}\times\underbrace{\frac{9!}{2!\,7!}}_{T}\times\underbrace{\frac{7!}{1!\,6!}}_{H}\times\underbrace{\frac{6!}{1!\,5!}}_{I}\times\underbrace{\frac{5!}{1!\,4!}}_{Q}\times\underbrace{\frac{4!}{1!\,3!}}_{U}\times\underbrace{\frac{3!}{2!\,1!}}_{E}\times\underbrace{\frac{1!}{1!\,1!}}_{S}=\frac{13!}{2^4}.$$

Coefficient multinomial :

$$\frac{n!}{k_1!\,k_2!\,k_3!\cdots k_p!}=\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3}\cdots\binom{k_p}{k_p}$$

avec $k_1+k_2+\cdots+k_p=n$.

$$(a_1+a_2+\cdots+a_p)^n=\sum_{k_1,\cdots,k_p}\frac{n!}{k_1!\cdots k_p!}a_1^{k_1}\,a_2^{k_2}\,\cdots\,a_p^{k_p}.$$

Exercice 4

simultanément = on ne tient pas compte de l'ordre

1. Il y en a
$$\begin{aligned}\binom{32}{5}&=\frac{32!}{5!27!}\\&=\frac{23\times29\times30\times31\times32}{2\times3\times4\times5}\\&=14\times29\times2\times31\times8\\&=201\,376.\end{aligned}$$

2. (a) On en a $8\times28=224$.
   (b) On en a $\binom{8}{2}\times\binom{4}{2}\times\binom{4}{2}\times6\times4=24\,192$.
   (c) On en a $8\times\binom{4}{3}\times7\times\binom{4}{2}=8\times4\times7\times6=1\,344$.
   (d) On en a $8\times\binom{4}{3}\times\binom{7}{2}\times4\times4=8\times4\times21\times16=10\,752$.
   (e) On en a $4\times4=16$.

Exercice 5

1. $\binom{45}{2}$
2. 11×34
3. $\binom{34}{2}$

Exercice 6

On numérote les pays de 1 à N. On pose

$$\begin{aligned} f : [\![1, N]\!] &\longrightarrow [\![0, N-1]\!] \\ p &\longmapsto \text{ le nombre de voisins du pays numéro } p \end{aligned}$$

On suppose f injective. Alors f est surjective : $\exists p, f(p) = 0$ et $\exists q, f(q) = N-1$. Donc p est isolé est q est voisin de tous les pays. Donc p et q sont voisins. $\lightning$.

Donc f n'est pas injective donc

$$\exists p \neq q, f(p) = f(q).$$

Exercice 7

$$\begin{aligned} \sum_{X \in \mathcal{P}(E)} (\#E) &= \sum_{k=0}^{n} \sum_{\substack{X \in \mathcal{P}(E) \\ \#X = k}} \#X \\ &= \sum_{k=0}^{n} k \binom{n}{k} \\ &= \sum_{k=1}^{n} \frac{n!}{(k-1)!\,(n-k)!} \\ &= n \sum_{k=1}^{n} \binom{n-1}{k-1} \\ &= n \sum_{k=0}^{n-1} \binom{n-1}{k} \\ &= n 2^{n-1} \end{aligned}$$

$$\begin{aligned}\sum_{X,Y\in\mathcal{P}(E)}\#(X\cap Y) &= \sum_{X\in\mathcal{P}(E)}\ \sum_{Y\in\mathcal{P}(E)}\#(X\cap Y)\\ &= \sum_{X\in\mathcal{P}(E)}\ \sum_{(Z,T)\in\mathcal{P}(X)\times\mathcal{P}(E\setminus X)}\#Z\\ &= \sum_{X\in\mathcal{P}(E)}\ \sum_{T\in\mathcal{P}(E\setminus X)}\ \sum_{Z\in\mathcal{P}(X)}\#Z\\ &= \sum_{X\in\mathcal{P}(E)}\ \sum_{T\in\mathcal{P}(E)}\#X2^{\#X-1}\\ &= \sum_{X\in\mathcal{P}(E)}\#X2^{\#X-1}2^{n-\#X}\\ &= \sum_{X\in\mathcal{P}(E)}\#X2^{n-1}\\ &= n\left(2^{n-1}\right)^2\\ &= n2^{2n-2}\end{aligned}$$

$$\begin{aligned}\sum_{X,Y\in\mathcal{P}(E)}\#(X\cup Y) &= \sum_{X,Y\in\mathcal{P}(E)}\left(\#X+\#Y-\#(X\cap Y)\right)\\ &= 2\sum_{Y\in\mathcal{P}(E)}\ \sum_{X\in\mathcal{P}(E)}\#X-\sum_{X,Y\in\mathcal{P}(E)}\#(X\cap Y)\\ &= 2\times 2^n\times n2^{n-1}-n2^{2n-2}\\ &= 3n2^{2n-2}\end{aligned}$$

Exercice 8

$$A=\{(X,Y)\in\mathcal{P}(E)^2\mid X\subset Y\}.$$

Méthode 1 $A=\bigcup_{y=0}^{n}{\cdot}\,A_y$ où

$$\forall y\in[\![0,n]\!],A_y=\{(X,Y)\in\mathcal{P}(E)^2\mid X\subset Y\ \text{ et }\ \#Y=y\}.$$

Soit $y\in[\![0,n]\!]$.

On note C_y l'ensemble

$$C_y=\{Y\in\mathcal{P}(E)\mid \#Y=y\}.$$

On a $\#C_y=\binom{n}{y}$. Soit $Y\in C_y$. On pose

$$B_Y=\{X\in\mathcal{P}(E)\mid X\subset Y\}.$$

Donc,

$$A_y = \bigcup_{Y \in C_y}^{\cdot} B_Y.$$

Soit $f : \begin{array}{ccc} B_Y & \longrightarrow & \mathcal{P}(Y) \\ (X,Y) & \longmapsto & X. \end{array}$

Donc,

$$\#B_y = \#\mathcal{P}(Y) = 2^y.$$

D'où,

$$\begin{aligned} \#A &= \sum_{y=0}^{n} \sum_{Y \in C_y} 2^y \\ &= \sum_{y=0}^{n} \binom{n}{y} 2^y = 3^n. \end{aligned}$$

Méthode 2

$$A = \bigcup_{X \in \mathcal{P}(E)}^{\cdot} \underbrace{\{(X,Y) \mid Y \supset X\}}_{B_X}.$$

On pose $f : \begin{array}{ccc} B_X & \longrightarrow & \{Y \in \mathcal{P}(E) \mid Y \supset X\} = C_X \\ (X,Y) & \longmapsto & Y, \end{array}$

$g : \begin{array}{ccc} C_X & \longrightarrow & \mathcal{P}(E \setminus X) \\ Y & \longmapsto & Y \setminus X, \end{array}$

et $h : \begin{array}{ccc} \mathcal{P}(E \setminus X) & \longrightarrow & C_X \\ Z & \longmapsto & Z \cup X. \end{array}$

Les applications g et h sont réciproques donc

$$\begin{aligned} \#C_X &= \#\mathcal{P}(E \setminus X) \\ &= 2^{\#(E \setminus X)} \\ &= 2^{n - \#X}. \end{aligned}$$

Donc

$$\begin{aligned} \#A &= \sum_{X \in \mathcal{P}(E)} 2^{n-\#X} \\ &= \sum_{k=0}^{n} \sum_{\substack{X \in \mathcal{P}(E) \\ \#X = k}} 2^{n-k} \\ &= \sum_{k=0}^{n} 2^{n-k} \binom{n}{k} = 3^n. \end{aligned}$$

MÉTHODE 3 On note $x_1, \dots, x_n$ les élements de E. Soit $(X, Y) \in A$. On pose

$$\forall i \in [\![1, n]\!], a_i^{(X,Y)} = \begin{cases} 0 & \text{si } x_i \in X, \\ 1 & \text{si } x_i \in Y \setminus X, \\ 2 & \text{si } x_i \notin Y. \end{cases}$$

On dispose donc de

$$\begin{aligned} f : A &\longrightarrow [\![0, 2]\!]^n \\ (X, Y) &\longmapsto \big(a_1(X, Y), a_2(X, Y), \dots, a_n(X, Y)\big). \end{aligned}$$

Soit

$$\begin{aligned} g : [\![0, 2]\!]^n &\longrightarrow A \\ (a_1, \dots, a_n) &\longmapsto \big(\{x_i \mid i \in [\![1, n]\!] \text{ et } a_i = 0\}, \{x_i \mid i \in [\![1, n]\!] \text{ et } a_i \neq 2\}\big) \end{aligned}$$

Les applications f et g sont réciproques donc

$$\#A = \#\big([\![0, 2]\!]\big)^n = 3^n.$$

Exercice 10

CAS PARTICULIER : $p = 2$, $n = 15$ donc $x_1 + x_2 = 15$.

$$\left.\begin{array}{ccc} 0 & + & 15 \\ 1 & + & 14 \\ & \vdots & \\ 15 & + & 0 \end{array}\right\} 16$$

Avec $p = 3$ et $n = 15$, on a donc $x_1 + x_2 + x_3 = 15$.

$$\begin{aligned} 15 &= 1+1+1+1+1+1 \neq 1+1+1+1+1+1+1+1 \neq 1+1+1 \\ &= 5+7+3 \end{aligned}$$

Avec $(x_1, x_2, \dots, x_p) \in (\mathbb{N}^\star)^p$, on en a $\binom{n-1}{p-1}$.

$$\begin{aligned} 15 &= 12+0+3 \\ &\uparrow \\ 18 &= 13+1+4 \end{aligned}$$

On a donc $\binom{n+p-1}{p-1}$.

Exercice 11

1. $S_n^1 = 1$, $S_n^n = n!$ et $p > n$ donc $S_n^p = 0$.
2. $p\,S_{n-1}^p + pS_{n-1}^{p-1}$. En effet, on note

$$A = \{f : E \to F \text{ surjective } \mid f_{|E\setminus\{a\}} \text{ surjective}\}$$

et

$$\begin{aligned}\varphi : A &\longrightarrow F \times \{f : E \setminus \{a\} \to F \text{ surjective}\} \\ f &\longmapsto f_{|E\setminus\{a\}}\end{aligned}$$

est bijective car

$$\psi : F \times \{E \setminus \{a\} \to F \text{ surjective}\} \longrightarrow A$$
$$(y, g) \longmapsto \begin{pmatrix} E & \longrightarrow & F \\ x & \longmapsto & \begin{cases} y & \text{si } x = a \\ g(x) & \text{sinon} \end{cases} \end{pmatrix}$$

est la réciproque de φ et donc

$$\#A = \#F \times \#\{E \setminus \{a\} \to F \text{ surjective}\} = pS_{n-1}^p.$$

3. On pose

$$\forall n \in \mathbb{N}^\star, \mathcal{P}(n) : \text{“}\forall p \in \mathbb{N}^\star, S_n^p = \sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} k^n \text{”}.$$

— Avec $n = 1$ et $p = 1$, On a $S_1^1 = 1$ et

$$\sum_{k=0}^{1} (-1)^{1-k} \binom{1}{k} k^1 = 0 + 1 = 1.$$

Avec $n = 1$ et $p \geqslant 2$, montrons que

$$0 = \sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} k$$

$$\begin{aligned}\sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} k &= \sum_{k=1}^{p} (-1)^{p-k} \frac{p!}{(k-1)!\,(p-k)!} \\ &= p \sum_{k=1}^{p} (-1)^{p-k} \binom{p-1}{k-1} \\ &= p \sum_{j=0}^{p-1} (-1)^{p-1-k} \binom{p-1}{j} \\ &= p(1-1)^{p-1} = 0 \text{ car } p - 1 \geqslant 1.\end{aligned}$$

— Soit $n \geqslant 1$. On suppose $\mathscr{P}(n)$. Soit $p \in \mathbb{N}^\star$.

$$\begin{aligned}
S_{n+1}^p &= p\left(S_n^p + S_n^{p-1}\right) \\
&= \left(\sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}k^n + \sum_{k=0}^{p-1}(-1)^{p-1-k}\binom{p-1}{k}k^n\right) \\
&= p\left(\sum_{k=0}^{p-1}(-1)^{p-k}\left(\binom{p}{k} - \binom{p-1}{k}\right)k^n + p^n\right) \\
&= p\left(p^n + \sum_{k=1}^{p-1}(-1)^{p-k}\binom{p-1}{k-1}k^n\right) \\
&= p^{n+1} + \sum_{k=1}^{p-1}(-1)^{p-k}\frac{p!}{(k-1)!\,(p-k)!}k^n \\
&= p^{n+1} + \sum_{k=1}^{p-1}(-1)^{p-k}\binom{p}{k}k^{n+1} \\
&= \sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}k^{n+1}
\end{aligned}$$

Exercice 12

1. Déjà faite dans le TD du chapitre 8.

2. On prends $X = [\![1, p]\!]$, $Y = [\![p+1, p+q]\!]$. On a $\#E = p + q$.
   On a $X \uplus Y = [\![1, p+q]\!]$ et on pose

$$A_r = \{Z \in \mathscr{P}(E) \mid \#Z = r\}.$$

et

$$\begin{aligned}
f : A_r &\longrightarrow \mathscr{P}(X) \times \mathscr{P}(Y) \\
Z &\longmapsto (Z \cap X, Z \cap Y)
\end{aligned}$$

$$\begin{aligned}
\#\big\{(X',Y')\in\mathscr{P}(X)\times\mathscr{P}(Y)\mid \#X'+\#Y'=r\big\} &= \sum_{\substack{X'\in\mathscr{P}(X)\\ \#Y'\in\mathscr{P}(Y)\\ \#X'+\#Y'=r}} 1\\
&= \sum_{X'\in\mathscr{P}(X)} \sum_{\substack{Y'\in\mathscr{P}(Y)\\ \#Y'=r-\#X'}} 1\\
&= \sum_{k=0}^{p} \sum_{\substack{X'\in\mathscr{P}(X)\\ \#X'=k}} \sum_{\substack{Y'\in\mathscr{P}(Y)\\ \#Y'=r-k}} 1\\
&= \sum_{k=0}^{p} \sum_{\substack{X'\in\mathscr{P}(X)\\ \#'=k}} \binom{q}{r-k}\\
&= \sum_{k=0}^{p} \binom{p}{k}\binom{q}{r-k}\\
&= \sum_{\substack{i,j\\ i+j=r}} \binom{p}{i}\binom{q}{j}
\end{aligned}$$

Exercice 13

1. $f\circ f=\mathrm{id}_{\mathscr{P}(E)}$.
2. $g:\begin{array}{ccc}\mathscr{P}_0 & \longrightarrow & \mathscr{P}_1\\ X & \longmapsto & f(X)\end{array}$ bijective donc $\#\mathscr{P}_0=\#\mathscr{P}_1$.
3. On en déduit que si $n>0$

$$\#\mathscr{P}_0=\frac{1}{2}\#\mathscr{P}(E)=\frac{2^n}{2}=2^{n-1}.$$

On a

$$\#\mathscr{P}_0=\sum_{\substack{0\leqslant i\leqslant n\\ i \text{ pair}}}\binom{n}{i}$$

et

$$\#\mathscr{P}_1=\sum_{\substack{0\leqslant i\leqslant n\\ i \text{ impair}}}\binom{n}{i}.$$

$$\begin{aligned}
\sum_{k=0}^{n}(-1)^k\binom{n}{k} &= \sum_{\substack{0\leqslant k\leqslant n\\ k \text{ pair}}}\binom{n}{k}+\sum_{\substack{0\leqslant k\leqslant n\\ k \text{ impair}}}\left(-\binom{n}{k}\right)\\
&= \#\mathscr{P}_0-\#\mathscr{P}_1\\
&= 0
\end{aligned}$$

Exercice 14

Partie I. Les nombres de Bell

1. On a $b_3 = 1 + 3 + 1 = 5$.

2. (a) par définition d'une partition !

   (b) On pose $B(E)$ l'ensemble des partitions de E. Donc,

$$B([\![1, n+1]\!]) = \bigcup_{\substack{P \in \mathcal{P}([\![1,n+1]\!]) \\ n+1 \in P}} \Big(\underbrace{\big\{ \{P_1, \dots, P_\diamond\} \in B_n \mid \exists i, P = P_i \big\}}_{A_p^{n+1}} \Big)$$

L'application $\begin{array}{ccc} A_p^{n+1} & \longrightarrow & B\big([\![1, n+1]\!] \setminus P\big) \\ \{P_1, \dots, P_\diamond\} & \longmapsto & \{P_i \mid P_i \neq P\} \end{array}$ est une bijection.

On a donc

$$\begin{aligned} b_{n+1} &= \sum_{\substack{P \in \mathcal{P}([\![1,n+1]\!]) \\ n+1 \in P}} b_{n+1-\#P} \\ &= \sum_{i=1}^{n+1} \sum_{\substack{P \in \mathcal{P}([\![1,n+1]\!]) \\ n+1 \in P \\ \#P = i}} b_{n+1-i} \\ &= \sum_{i=1}^{n+1} \binom{n}{i-1} b_{n+1-i} \\ &= \sum_{k=0}^{n} \binom{n}{k} b_{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{n-k} b_{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} b_k. \end{aligned}$$

(c)

$$\begin{aligned} b_3 &= \sum_{k=0}^{2} \binom{2}{k} b_k \\ &= b_0 + 2b_1 + b_2 \\ &= 1 + 2 \times 1 + 2 = 5 \end{aligned}$$

$$\begin{aligned} b_4 &= \sum_{k=0}^{3} \binom{3}{k} b_k = b_0 + 3b_1 + 3b_2 + b_3 \\ &= 1 + 3 + 3 \times 2 + 5 \\ &= 15 \end{aligned}$$

$$\begin{aligned} b_5 &= \sum_{k=0}^{4} \binom{4}{k} b_k \\ &= b_0 + 4b_1 + 6b_2 + 4b_3 + b_4 \\ &= 1 + 4 + 12 + 20 + 15 \\ &= 52. \end{aligned}$$

(d)

$$b_{n+1} = \sum_{k=0}^{n} \binom{n}{k} b_k \geqslant \binom{n}{n-1} b_{n-1} = n b_{n-1}$$

$b_{2k+1}^2 \geqslant b_{2k} b_{2k+1} \geqslant (2k)!$
$b_{2k+1} = \sqrt{(2k)!}$

Chapitre 24

TD 24

Exercice 2

1. Soit $i < j$ avec $i, j \in [\![2, n]\!]$.

$$(i \quad j) = (1 \quad i)\,(1 \quad j)\,(1 \quad i)$$

2.

$$(1 \quad 3) = (1 \quad 2)\,\underbrace{\gamma\,(1 \quad 2)\,\gamma^{-1}}_{(2 \quad 3)}\,(1 \quad 2)$$

avec $\gamma = (1 \quad 2 \quad \cdots \quad n)$.

On pose

$$\begin{aligned}\sigma &= (1 \quad 2)\,\gamma \\ &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \\ 1 & 3 & \cdots & n & 2 \end{pmatrix} \\ &= (2 \quad 3 \quad 4 \quad \cdots \quad n)\end{aligned}$$

$$\begin{aligned}\sigma\,(1 \quad 2)\,\sigma^{-1} &= (\sigma(1) \quad \sigma(2)) \\ &= (1 \quad 3)\end{aligned}$$

$$\begin{aligned}\sigma^k\,(1 \quad 2)\,\sigma^{-k} &= (\sigma^k(1) \quad \sigma^k(2)) \\ &= (1 \quad 2+k)\end{aligned}$$

Exercice 3

1. On pose $\sigma = \begin{pmatrix} a & b & c \end{pmatrix}\begin{pmatrix} b & c & d \end{pmatrix} \in S_n$.

$$\forall k \notin \{a,b,c,d\}, \sigma(k) = k.$$

On suppose $a \neq d$.

$$\begin{cases} \sigma(a) = b \\ \sigma(b) = a \\ \sigma(c) = d \\ \sigma(d) = c \end{cases}$$

On suppose $a = d$: $\sigma = \begin{pmatrix} a & b & c \end{pmatrix}^2$. Donc,

$$\begin{cases} \sigma(a) = c \\ \sigma(b) = a \\ \sigma(c) = b \end{cases}$$

Si $a \neq d$, $\sigma = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}$.
Si $a = d$, $\sigma = \begin{pmatrix} a & c & b \end{pmatrix}$.

2. Soit $\sigma \in A_n$. On pose $\sigma = \tau_1 \cdot \tau_{2p}$ où $\forall i$, τ_i est un transposition.

Soit i impaire. Si $\mathrm{Supp}(\tau_i) = \mathrm{Supp}(\tau_{i+1})$, alors $\tau_i = \tau_{i+1}$ et donc $\tau_i\tau_{i+1} = \mathrm{id}$.

Si $\#\big(\mathrm{Supp}(\tau_i) \cap \mathrm{Supp}(\tau_{i+1})\big) = 1$, alors on peut écrire $\begin{cases} \tau_i = \begin{pmatrix} a & b \end{pmatrix} \\ \tau_{i+1} = \begin{pmatrix} b & c \end{pmatrix} \end{cases}$

avec $\begin{cases} a \neq b \\ b \neq c \\ a \neq c \end{cases}$ et alors

$$\tau_i\tau_{i+1} \text{ est un 3-cycle.}$$

Si $\mathrm{Supp}(\tau_i) \cap \mathrm{Supp}(\tau_{i+1}) =$, alors on peut écrire $\begin{cases} \tau_i = \begin{pmatrix} a & b \end{pmatrix} \\ \tau_{i+1} = \begin{pmatrix} c & d \end{pmatrix} \end{cases}$ avec

$\begin{cases} a \neq b \\ c \neq d \\ a \neq c \\ a \neq d \\ b \neq c \\ b \neq d \end{cases}$ et alors $\tau_i\tau_{i+1} = \begin{pmatrix} a & b & c \end{pmatrix}\begin{pmatrix} b & c & d \end{pmatrix}$. Donc σ est un produit de 3-cycles.

Réciproquement, comme ε est un morphisme de groupes, et comme un 3-cycle est de signature 1, tout produit de 3-cycles appartient à A_n.

Exercice 4

$$\begin{cases} 5 \vee 3 \vee 2 = 30 \\ 5 + 3 + 2 = 10 \end{cases}$$

Exercice 5

On note $\mathcal{O}_1, \ldots, \mathcal{O}_k$ les orbites de σ :

$$[\![1, n]\!] = \bigcup_{j=1}^{k} \mathcal{O}_j$$

On pose aussi $\sigma = \gamma_1 \cdots \gamma_k$ où

$$\forall j \in [\![1, k]\!], \begin{cases} \gamma_j \text{ est un cycle,} \\ \mathrm{Supp}(\gamma_j) = \mathcal{O}_j \text{ si } \#\mathcal{O}_j \geqslant 2. \end{cases}$$

$$\begin{aligned} \varepsilon(\sigma) &= \prod_{j=1}^{k} \varepsilon(\gamma_j) \\ &= \prod_{j=1}^{k} (-1)^{\#\mathcal{O}_j - 1} \\ &= (-1)^{\sum_{j=1}^{k} (\#\mathcal{O}_j - 1)} \\ &= (-1)^{n-k} \end{aligned}$$

Exercice 6

Il y en a $\dfrac{A_n^k}{k}$. On applique le principe des berges sur l'application suivante :

$$\begin{aligned} f : \mathcal{A}_{n,k} &\longrightarrow \{k\text{-cycles}\} \\ (a_1, \ldots, a_k) &\longmapsto \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix}. \end{aligned}$$

Exercice 7

On suppose $n > 2$. Soit $\sigma \in Z(S_n)$:

$$\forall \sigma' \in S_n, \sigma\ \sigma' = \sigma'\ \sigma.$$

En particulier,

$$\forall k \in [\![2,n]\!], \sigma \begin{pmatrix} 1 & k \end{pmatrix} \sigma^{-1} = \begin{pmatrix} 1 & k \end{pmatrix}$$

$$\| $$

$$\begin{pmatrix} \sigma(1) & \sigma(k) \end{pmatrix}$$

Donc $\sigma(1) \in \{1,k\}$ $\forall k$ et donc $\sigma(1) = 1$. On en déduit que

$$\forall k \geqslant 2, \sigma(k) = k$$

et donc $\sigma = \mathrm{id}$.

S_2 est commutatif : $\begin{pmatrix} 1 & 2 \end{pmatrix}$ commute avec id et $\begin{pmatrix} 1 & 2 \end{pmatrix}$.

Exercice 8

Analyse Soient $n \in \mathbb{N}^\star$ et $f \in S_n$ tels que $g : \begin{array}{ccc} [\![1,b]\!] & \longrightarrow & [\![0,n-1]\!] \\ k & \longmapsto & |f(k)-k| \end{array}$ injective.

Donc g est bijective et donc

$$\sum_{k=1}^{n} g(k) = \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}.$$

$$\forall k,\ g(k) \equiv f(k) - k \ [2]$$

donc

$$\begin{aligned} \sum_{k=1}^{n} g(k) &\equiv \sum_{k=1}^{n} \big(f(k)-k\big) \ [2] \\ &\equiv 0 \ [2] \end{aligned}$$

donc

$$n(n-1) \equiv 0 \ [4]$$

donc $\begin{cases} n \equiv 0 \ [4] \\ n-1 \equiv 0 \ [4] \end{cases}$

Synthèse On suppose $n \equiv 0 \ [4]$: $n = 4p$.

$$f = \left(\begin{array}{cccc|cccc|cccc|c} 1 & 2 & \cdots & p & p+1 & p+2 & \cdots & 2p & 2p+1 & 2p+2 & \cdots & 3p-1 & 3p & 3p \\ 4p & 4p-1 & \cdots & 3p+1 & p+1 & 3p & \cdots & 2p+2 & 2p & 2p-1 & \cdots & p+2 & p & p \end{array} \right.$$

$$g = \left(\begin{array}{cccc|cccc|cccc|c} 1 & 2 & \cdots & p & p+1 & p+2 & \cdots & 2p & 2p+1 & 2p+2 & \cdots & 3p-1 & 3p & 3p \\ 4p-1 & 4p-3 & \cdots & 2p+1 & 0 & 2p-2 & \cdots & 2 & 1 & 3 & \cdots & 2p-3 & 2p & 2p \end{array} \right.$$

Chapitre 25

TD 25

Exercice 1

1.

$$\begin{aligned}\forall n \in \mathbb{N}^\star, \sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) \\ &= 1 - \frac{1}{n+1} \xrightarrow[n\to+\infty]{} 1.\end{aligned}$$

2. $e : \sum_{n=0}^{+\infty} \frac{1}{n!}$ donc

$$\begin{aligned}\forall n \in \mathbb{N}, \sum_{k=0}^{n} \frac{k^2+1}{k!} &= \sum_{k=0}^{n} \frac{1}{k!} + \sum_{k=1}^{n} \frac{k-1+1}{(k-1)!} \\ &= \sum_{k=0}^{n} \frac{1}{k!} + \sum_{k=1}^{n} \frac{1}{(k-1)!} + \sum_{k=2}^{n} \frac{1}{(k-2)!} \\ &\xrightarrow[n\to+\infty]{} e + e + e = 3e.\end{aligned}$$

3. Soit $n \in \mathbb{N}$ avec $n \geqslant 2$.

$$\begin{aligned}\sum_{k=2}^{n} \ln\left(1 - \frac{1}{k^2}\right) &= \sum_{k=2}^{n} \ln\left(\frac{(k-1)(k+1)}{k^2}\right) \\ &= \sum_{k=2}^{n} \big(\ln(k-1) - \ln(k)\big) + \sum_{k=2}^{n} \big(\ln(k+1) - \ln(k)\big) \\ &= -\ln(n) + \ln(n+1) - \ln(2) \\ &= \ln\left(1 + \frac{1}{n}\right) - \ln(2) \\ &\xrightarrow[n\to+\infty]{} -\ln(2).\end{aligned}$$

Exercice 2

$$\forall n \in \mathbb{N},\ \frac{1}{1+n+n^2} = \frac{n+1-n}{1+n(n+1)}$$

On pose

$$\forall n \in \mathbb{N},\ u_n = \operatorname{Arctan} n$$

et alors

$$\forall n \in \mathbb{N},\ \frac{1}{1+n+n^2} = \frac{\tan u_{n+1} - \tan u_n}{1+\tan(u_{n+1})\tan(u_n)} = \tan(u_{n+1}-u_n).$$

En effet,

$$\begin{cases} 0 < u_{n+1} < \dfrac{\pi}{2} \\ -\dfrac{\pi}{2} < -u_n \leqslant 0 \end{cases}$$

donc

$$-\frac{\pi}{2} < u_{n+1} - u_n < \frac{\pi}{2}$$

et donc $u_{n+1} - u_n \not\equiv \dfrac{\pi}{2}\ [\pi]$ et $\operatorname{Arctan}\big(\tan(u_{n+1}-u_n)\big) = u_{n+1}-u_n$.

$$\begin{aligned} \forall n \in \mathbb{N}, \sum_{k=0}^{n} \operatorname{Arctan}\left(\frac{1}{1+k+k^2}\right) &= \sum_{k=0}^{n} (u_{k+1}-u_k) \\ &= u_{n+1} - u_n \\ &\xrightarrow[n\to+\infty]{} \frac{\pi}{2} \end{aligned}$$

On a donc

$$\frac{\pi}{2} = \sum_{n=0}^{+\infty} \operatorname{Arctan}\left(\frac{1}{1+n+n^2}\right)$$

Exercice 3

1. $$\forall n \in \mathbb{N}, 0 \leqslant u_n \leqslant \frac{n\,n!}{(n+3)!} = \frac{n}{(n+1)(n+2)(n+3)} \sim \frac{1}{n^2}$$

   $\sum u_n$ converge.

2. $$\forall n \geqslant 2, 0 \leqslant \frac{\ln n}{n^3} = \mathcal{o}\left(\frac{n}{n^3}\right) = \mathcal{o}\left(\frac{1}{n^2}\right)$$

   $\sum \dfrac{1}{n^2}$ converge donc $\sum \dfrac{\ln n}{n^3}$ converge.

3. $\forall \alpha, \ln n = \mathop{o}(n^\alpha)$. Avec $\alpha = \dfrac{1}{2}$, on a

$$0 \leqslant \frac{\ln n}{n^2} = \mathop{o}\left(\frac{1}{n^{\frac{3}{2}}}\right)$$

donc $\sum \dfrac{\ln n}{n^2}$ converge.

4. $\forall n \geqslant 3, \dfrac{\ln n}{n} \geqslant \dfrac{1}{n} \geqslant 0$ donc $\sum \dfrac{\ln n}{n}$ diverge.

5. $\left|\dfrac{(-1)^n}{n^2}\right| = \dfrac{1}{n^2}$ donc $\sum \dfrac{(-1)^n}{n^2}$ converge absolument donc $\sum \dfrac{(-1)^n}{n^2}$ converge.

Exercice 4

$$\forall n,\ 0 < u_n = \left(\frac{1}{n}\right)^{1+\frac{1}{n}} = \frac{1}{n} \times e^{\frac{1}{n}\ln\frac{1}{n}} = \frac{1}{n}^{-\frac{\ln n}{n}} \sim \frac{1}{n}.$$

Donc, $\sum u_n$ diverge.

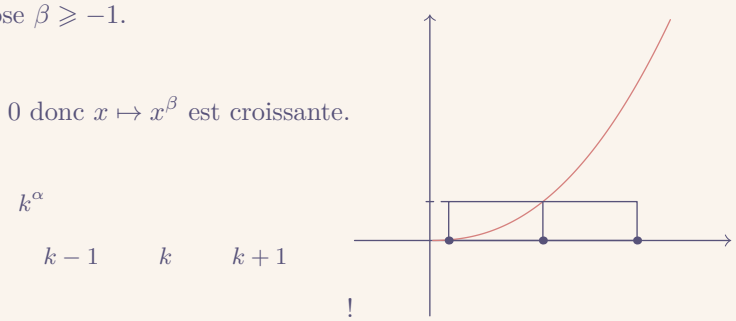
Exercice 5

$$\forall n \in \mathbb{N}^\star,\ \sum_{k=1}^{n} k^\beta = \sum_{k=1}^{n} \frac{1}{k^{-\beta}} \xrightarrow[n\to+\infty]{} \begin{cases} \zeta(-\beta) & \text{si } -\beta > 1 \\ +\infty & \text{sinon.} \end{cases}$$

On suppose $\beta < -1$. Alors, $0 < u_n \sim \dfrac{\zeta(-\beta)}{n^\alpha}$ et donc $\sum u_n$ converge si et seulement si $\alpha > 1$.

On suppose $\beta \geqslant -1$.

Cas 1 $\beta > 0$ donc $x \mapsto x^\beta$ est croissante.



!

Soit $n \in \mathbb{N}^\star$.

$$\forall k \in [\![1, n]\!], \int_{k-1}^{k} x^\beta \, \mathrm{d}x \leqslant k^\beta \leqslant \int_{k}^{k+1} x^\beta \, \mathrm{d}x$$

$$\text{donc } \int_0^n x^\beta \, \mathrm{d}x \leqslant \sum_{k=0}^{n} k^\beta \leqslant \int_1^{n+1} x^\beta \, \mathrm{d}x$$

$$\text{donc } \frac{n^{\beta+1}}{\beta+1} \leqslant \sum_{k=1}^{n} \leqslant \frac{(n+1)^{\beta+1}-1}{\beta+1} \sim \frac{n^{\beta+1}}{\beta+1}$$

et donc

$$0 < u_n \sim \frac{1}{n^\alpha} \times \frac{n^{\beta+1}}{\beta+1} = \frac{1}{\beta+1} \times \frac{1}{n^{\alpha-\beta-1}}.$$

Donc,

$$\begin{aligned} \sum u_n \text{ converge} &\iff \alpha - \beta - 1 > 1 \\ &\iff \alpha > \beta + 2. \end{aligned}$$

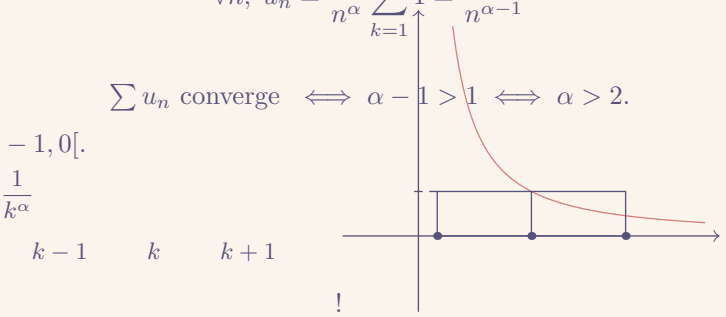
Cas 2 $\beta = 0$.

$$\forall n, \; u_n = \frac{1}{n^\alpha} \sum_{k=1}^{n} 1 = \frac{1}{n^{\alpha-1}}$$

donc

$$\sum u_n \text{ converge} \iff \alpha - 1 > 1 \iff \alpha > 2.$$

Cas 3 $\beta \in]-1, 0[$.



Soit $n \geqslant 2$.

$$\forall k \in [\![2, n]\!], \int_{k}^{k+1} x^\beta \, \mathrm{d}x \leqslant k^\beta \leqslant \int_{k-1}^{k} x^\beta \, \mathrm{d}x$$

donc

$$\int_2^{n+1} x^\beta \, \mathrm{d}x \leqslant \sum_{k=2}^{n} k^\beta \leqslant \int_1^n x^\beta \, \mathrm{d}x$$

et donc

$$\frac{(n+1)^{\beta+1} - 2^{\beta+1}}{\beta+1} \leqslant \sum_{k=2}^{n} k^\beta \leqslant \frac{n^{\beta+1}-1}{\beta+1}$$

donc

$$\sum_{k=2}^{n} b^\beta \sim \frac{n^{\beta+1}}{\beta+1}$$

et donc

$$\sum u_n \text{ converge} \iff \alpha > \beta + 2.$$

Cas 4 $\beta = -1$.

$$\int_2^{n+1} \frac{1}{x}\,\mathrm{d}x \leqslant \sum_{k=2}^{n} k^{\beta} \leqslant \int_1^n \frac{1}{x}\,\mathrm{d}x$$

$$\underbrace{\ln(n+1) - \ln 2}_{\sim \ln n} \leqslant \sum_{k=2}^{n} k^{-1} \leqslant \ln n.$$

$$0 < u_n \sim \frac{1}{n^{\alpha}} \ln n$$

Pour $n \geqslant 3$, $\dfrac{\ln n}{n^{\alpha}} > \dfrac{1}{n^{\alpha}}$.

Si $\alpha \leqslant 1$, alors $\sum u_n$ diverge.

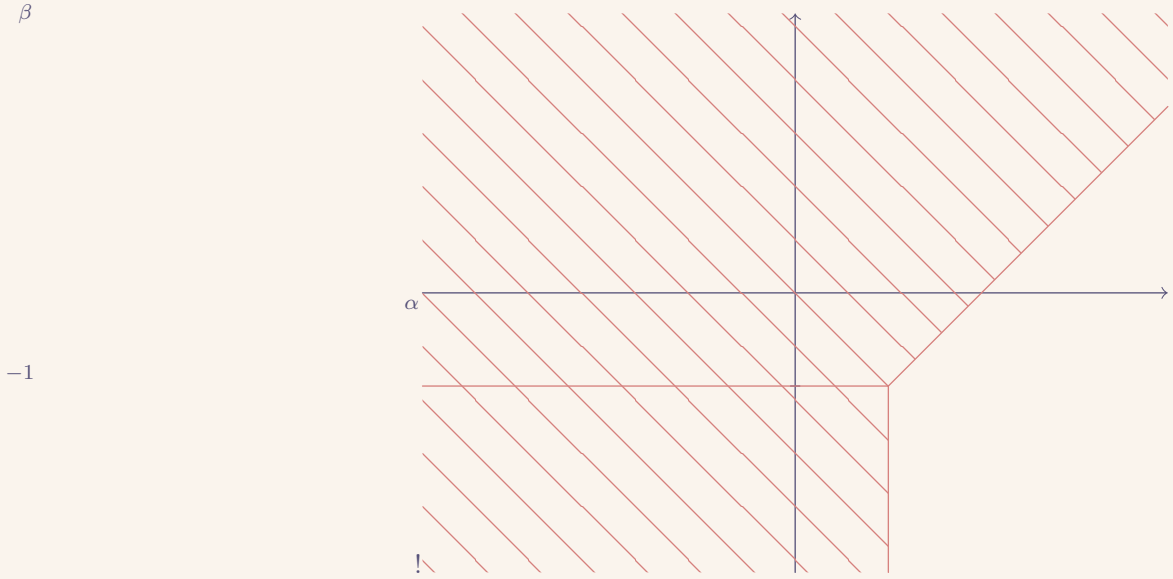
Si $\alpha > 1$,

$$\ln n = \mathop{o}(n^{\gamma}) \text{ avec } \gamma = \frac{\alpha - 1}{2} > 0.$$

donc

$$\frac{\ln n}{n^{\alpha}} = \mathop{o}\left(\frac{1}{n^{\alpha-\beta}}\right) = \mathop{o}\left(\frac{1}{n^{\frac{1+\alpha}{2}}}\right)$$

et donc $\sum \dfrac{\ln n}{n}$ converge.



Exercice 6

Nature de $\sum u_n$ où

$$\forall n, u_n = \ln\left(\frac{\sqrt{n} + (-1)^n}{\sqrt{n+a}}\right)$$

$$\begin{aligned} u_n &= \ln\left(\frac{1+\frac{(-1)^n}{\sqrt{n}}}{\sqrt{1+\frac{a}{n}}}\right) \\ &= \ln\left(1+\frac{(-1)^n}{\sqrt{n}}\right) - \frac{1}{2}\ln\left(1+\frac{a}{n}\right) \\ &= \frac{(-1)^n}{\sqrt{n}} - \frac{1}{2n} + \mathcal{O}\left(\frac{1}{n^{3/2}}\right) - \frac{a}{2n} + \frac{a^2}{4n^2} + \mathcal{O}\left(\frac{1}{n^2}\right) \\ &= \frac{(-1)^n}{\sqrt{n}} - \frac{1+a}{2n} + \mathcal{O}\left(\frac{1}{n^{3/2}}\right) \end{aligned}$$

La série $\sum \frac{(-1)^n}{\sqrt{n}}$ converge (théorème des séries alternées). La série $\sum \frac{1+a}{2n}$ diverge sauf si $a=-1$. La série $\sum \mathcal{O}\left(\frac{1}{n^{3/2}}\right)$ converge absolument (car $3/2>1$).

Donc,

$$\sum u_n \text{ converge} \iff a=-1$$

$$\begin{aligned} u_n &= \frac{(-1)^n}{\sqrt{n}} - \frac{1}{2n} + \frac{1}{3}\times\frac{(-1)^{3n}}{n^{3/2}} + o\left(\frac{1}{n^{3/2}}\right) - \frac{1}{2}\left(\frac{a}{n} - \frac{a^2}{2n^2} + o\left(\frac{1}{n^2}\right)\right) \\ &= \frac{(-1)^n}{\sqrt{n}} - \frac{1+a}{2n} + \frac{1}{3}\frac{(-1)^{3n}}{n^{3/2}} + o\left(\frac{1}{n^{3/2}}\right) \end{aligned}$$

Exercice 7

1. — On suppose que $\sum u_n$ converge. Donc $u_n \xrightarrow[n\to+\infty]{} 0$ et donc $v_n \sim u_n > 0$. Donc, $\sum v_n$ converge.
   — On suppose que $\sum v_n$ converge donc $v_n \xrightarrow[n\to+\infty]{} 0$.

$$\forall n,\ u_n = \frac{v_n}{1-v_n} \sim v_n$$

   donc $\sum u_n$ converge.
2. — On suppose $\sum u_n$ convergente.

$$0 \leqslant v_n \leqslant \frac{u_n}{u_1} \qquad \left(v_n \sim \frac{u_n}{\sum_{k=1}^{+\infty} u_k}\right)$$

   donc $\sum v_n$ converge.
   — On suppose que $\sum u_n$ diverge.

$$\begin{aligned} \forall n\in\mathbb{N},\ \ln(1-v_n) &= \ln\left(\frac{u_1+\cdots+u_{n-1}}{u_1+\cdots+u_n}\right) \\ &= \ln\left(\sum_{k=1}^{n-1} u_k\right) - \ln\left(\sum_{k=1}^{n} u_k\right) \end{aligned}$$

donc $\sum \ln(1-v_n)$ a même nature que $\left(\ln\left(\sum_{k=1}^{n} u_k\right)\right)_n$, donc $\sum \ln(1-v_n)$ diverge.

Si $\sum v_n$ converge, alors $v_n \longrightarrow 0$ et donc $\ln(1-v) \underset{n\to+\infty}{\sim} -v_n \leqslant 0$ et donc $\sum \ln(1-v_n)$ converge $\lightning$.

Donc $\sum v_n$ diverge.

Exercice 8

$$\begin{aligned}\forall n \in \mathbb{N},\ 0 \leqslant u_n &\leqslant \int_{n^2}^{n^2+1} \frac{1}{x^\alpha}\,\mathrm{d}x \\ &\leqslant \begin{cases} \underbrace{\ln\left(1+\frac{1}{n^2}\right)}_{\sim \frac{1}{n^2}} & \text{si } \alpha = 1 \\ \underbrace{\frac{1}{1-\alpha}\left(\left(n^2+1\right)^{-\alpha+1} - \left(n^2\right)^{-\alpha=1}\right)}_{v_n} & \text{si } \alpha \neq 1 \end{cases}\end{aligned}$$

Pour $\alpha \neq -1$,

$$\begin{aligned}(n^2+1)^{1-\alpha} &= n^{2(1-\alpha)}\left(1+\frac{1}{n^2}\right)^{1-\alpha} \\ &= n^{2(1-\alpha)}\left(1+\frac{1-\alpha}{n^2}+\wp\left(\frac{1}{n^2}\right)\right)\end{aligned}$$

$$0 < v_n \sim n^{-2\alpha} = \frac{1}{n^{2\alpha}}$$

Si $\alpha > \dfrac{1}{2}$, alors $\sum v_n$ converge et donc $\sum u_n$ converge.

On suppose $0 \leqslant \alpha \leqslant \dfrac{1}{2}$.

$$\begin{aligned}\forall n \in \mathbb{N},\ u_n &\geqslant \int_{n^2}^{n^2+1} \frac{\sin^2(\pi x)}{(n^2+1)^\alpha}\,\mathrm{d}x \\ &\geqslant \frac{1}{(n^2+1)^\alpha}\int_{n^2}^{n^2}\left(\frac{1}{2}\big(1-\cos(2\pi x)\big)\right)\,\mathrm{d}x \\ &\geqslant \frac{1}{2(n^2+1)^\alpha} \sim \frac{1}{2n^{2\alpha}}\end{aligned}$$

$2\alpha < 1$ donv $\displaystyle\sum \frac{1}{2n^{2\alpha}}$ diverge et donc $\sum u_n$ diverge.

Si $\alpha = 0$,

$$u_n = \int_{n^2}^{n^2+1} \sin^2(\pi x)\,\mathrm{d}x = \frac{1}{2}$$

donc $\sum u_n$ diverge.

Si $\alpha < 0$,

$$u_n \geqslant \int_{n^2}^{n^2+1} \frac{\sin^2(\pi x)}{n^{2\alpha}}\,\mathrm{d}x \geqslant \frac{1}{2n^{2\alpha}}$$

donc $\sum u_n$ diverge.

En fait, dans tous les cas, $u_n \sim \dfrac{1}{2n^{2\alpha}}$.

Exercice 9

Pour $n \in \mathbb{N}$, on pose

$$\mathscr{P}(n) : \text{“}u_n \text{ existe et } u_n > 0\text{”}.$$

— $\mathscr{P}(0)$ est vraie.

— Soit $n \in \mathbb{N}$. On suppose $\mathscr{P}(n)$. $u_n + \dfrac{a_n}{u_n}$ existe car $u_n \neq 0$ donc u_{n+1} existe. On a $a_n \geqslant 0$ et $u_n > 0$ donc $u_{n+1} \geqslant u_n > 0$.

$$\begin{aligned}(u_n) \text{ converge} &\iff \sum u_{n-1} - u_n \text{ convege} \\ &\iff \sum \frac{a_n}{u_n} \text{ converge}\end{aligned}$$

— On suppose que $u_n \xrightarrow[n\to+\infty]{} \ell > 0$ car (u_n) est *croissante*. Donc

$$\frac{a_n}{u_n} \sim \frac{a_n}{\ell}$$

donc $a_n \sim \ell \dfrac{a_n}{u_n}$.

Par compairaison de séries à termes positifs, $\sum u_n$ converge.

— On suppose que $u_n \longrightarrow +\infty$ alors $a_n \geqslant \dfrac{a_n}{u_n}$ à partir d'un certain rang donc $\sum a_n$ diverge.

Exercice 10

1. Oups, j'ai supprimé cette partie.

2. Si $\alpha > 0$,

$$\begin{aligned} u_n &= \frac{(-1)^n}{n^\alpha (-1)^n} = \frac{(-1)^n}{n^\alpha} \times \frac{1}{1+\frac{(-1)^n}{n^\alpha}} \\ &= \frac{(-1)^n}{n^\alpha}\left(1 - \frac{(-1)^n}{n^\alpha} + o\left(\frac{1}{n^\alpha}\right)\right) \\ &= \underbrace{\frac{(-1)^n}{n^\alpha}}_{\substack{\text{série alternée} \\ \text{convergente}}} \underbrace{- \frac{1}{n^{2\alpha}} + o\left(\frac{1}{n^{2\alpha}}\right)}_{\sim \frac{1}{n^{2\alpha}} > 0} \end{aligned}$$

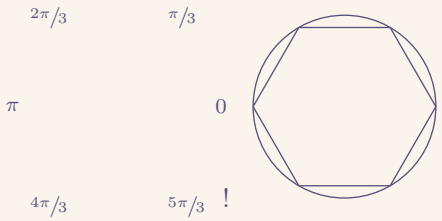
$\sum \dfrac{1}{n^{2\alpha}}$ converge si et seulement si $\alpha > \dfrac{1}{2}$.

Si $\alpha < 0$,

$$u_n = \frac{1}{1+(-1)^n n^\alpha} \xrightarrow[n\to+\infty]{} 1 \neq 0$$

donc u_n diverge.

3.



$$\begin{aligned} S_{6n} &= \sum_{k=1}^{6n} \ln\left(1 + \frac{\sin(k\pi/3)}{k}\right) \\ &= \sum_{a=0}^{n-1}\sum_{k=1}^{6} \ln\left(1 + \frac{\sin\left(\frac{(6a+k)\pi}{3}\right)}{6a+k}\right) \\ &= \sum_{a=0}^{n-1}\left(\ln\left(1+\frac{\sqrt{3}}{2(6a+1)}\right) + \ln\left(1+\frac{\sqrt{3}}{2(6a+2)}\right) + \ln\left(1-\frac{\sqrt{3}}{2(6a+4)}\right) + \ln\left(1-\frac{\sqrt{3}}{2(6a+5)}\right)\right) \\ &= \sum_{a=0}^{n-1}\left(\ln\left(1 - \frac{\sqrt{3}}{2(6a+4)} + \frac{\sqrt{3}}{2(6a+1)} - \frac{3}{4(6a+1)(6a+4)}\right)\right. \\ &\quad \left. + \left(\ln\left(1 - \frac{\sqrt{3}}{2(6a+5)} + \frac{\sqrt{3}}{2(6a+2)} - \frac{3}{4(6a+2)(6a+5)}\right)\right)\right) \\ &= \sum_{a=0}^{n-1} \ln\left(1 + \frac{6\sqrt{3}-3}{4(6a+1)(6a+4)}\right) + \sum_{a=0}^{n-1} \ln\left(1 + \frac{6\sqrt{3}-3}{4(6a+2)(6a+5)}\right) \end{aligned}$$

$$\ln\left(1+\frac{6\sqrt{3}-3}{4(6a+1)(6a+4)}\right)\underset{a\to+\infty}{\sim}\frac{6\sqrt{3}-3}{4\times 36a^2}>0.$$

$\sum\frac{6\sqrt{3}-3}{4\times 36a^2}$ converge donc $\sum\ln\left(1+\frac{6\sqrt{3}-3}{4(6a+4)(6a+1)}\right)$ converge.

Donc (S_{6n}) converge.
$S_{6n+1}=S_{6n}+\underbrace{u_{6n+1}}_{\to 0}\longrightarrow\lim S_{6n}$
$S_{6n+2},\dots,S_{6n+5}\longrightarrow\lim S_{6n}$
donc (S_n) converge et donc $\sum u_n$ converge.

Exercice 11

$$(k_n)=(1,2,3,4,5,6,7,8,10,11,12,\dots,18,20,\dots,).$$

$\forall n, k_n\geqslant n$ donc $\frac{1}{k_n}\leqslant\frac{1}{n}$.
Soit $n\in\mathbb{N}^\star$. Soit $N\in\mathbb{N}$ tel que

$$10^{N-1}\leqslant n<10^N.$$

$$\begin{aligned}\sum_{p=1}^{n}\frac{1}{k_p}&\leqslant\sum_{p=1}^{10^N}\frac{1}{k^p}=\sum_{i=1}^{N}\sum_{\substack{p\\10^{i-1}\leqslant k_p<10^i}}\frac{1}{k^p}\\&\leqslant\sum_{i=1}^{N}\sum_{\substack{p\\10^{i-1}\leqslant k_p<10^i}}\frac{1}{k^p}\\&\leqslant\sum_{i=1}^{N}\frac{8\times 9^{i-1}}{10^{i-1}}=8\sum_{i=1}^{N}\left(\frac{9}{10}\right)^{i-1}\\&\leqslant 8\times\frac{1-\left(\frac{9}{10}\right)^N}{1-\frac{9}{10}}\leqslant 80\end{aligned}$$

(S_n) croissante et majorée donc elle converge.

Exercice 12

1. Soit $f:t\mapsto\frac{\ln t}{t}$. f est dérivable sur $\mathbb{R}_\star^+$ et

$$\forall x>0,\ f'(t)=\frac{1}{t^2}-\frac{\ln t}{t}=\frac{1-\ln t}{t^2}$$

On a $\forall t > e, f'(t) < 0$ et donc f est strictement décroissante sur $[e, +\infty[$.

Soit $n \in \mathbb{N}$, $n \geqslant 4$.

$$\forall k \in [\![4, n]\!], \int_k^{k+1} \frac{\ln t}{t}\,\mathrm{d}t \leqslant \frac{\ln k}{k} \leqslant \int_{k-1}^{k} \frac{\ln t}{t}\,\mathrm{d}t$$

et donc

$$\int_4^{n+1} \frac{\ln t}{t}\,\mathrm{d}t \leqslant \sum_{k=4}^{n} \frac{\ln k}{k} \leqslant \int_3^{n} \frac{\ln t}{t}\,\mathrm{d}t$$

$$\frac{1}{2}\left(\ln^2(n+1) - \ln^2 4\right) \leqslant \sum_{k=4}^{n} \frac{\ln k}{k} \leqslant \frac{1}{2}\left(\ln^2 n - \ln^2 3\right).$$

Donc

$$\sum_{k=4}^{n} \frac{\ln k}{k} = \frac{1}{2}\ln^2 n + \mathcal{o}\left(\ln^2 n\right)$$

et donc

$$\sum_{k=1}^{n} \frac{\ln k}{k} = \frac{1}{2}\ln^2 n + \mathcal{o}\left(\ln^2 n\right).$$

On pose

$$\forall n \in \mathbb{N}^\star,\ u_n = \sum_{k=1}^{n} \frac{\ln k}{k} - \frac{1}{2}\ln^2 n$$

Soit $n \in \mathbb{N}^\star$.

$$\begin{aligned}
u_{n+1} - u_n &= \frac{\ln(n+1)}{n+1} - \frac{1}{2}\ln^2(n+1) + \frac{1}{2}\ln^2(n) \\
&= \frac{\ln n + \ln\left(1+\frac{1}{n}\right)}{n\left(1+\frac{1}{n}\right)} + \frac{1}{2}\ln^2 n - \frac{1}{2}\left(\ln n + \ln\left(1+\frac{1}{n}\right)\right)^2 \\
&= \left(\ln n + \frac{1}{n} + \mathcal{o}\left(\frac{1}{n}\right)\right)\left(\frac{1}{n} - \frac{1}{n^2} + \mathcal{o}\left(\frac{1}{n^2}\right)\right) \\
&\quad + \frac{1}{2}\ln^2 n - \frac{1}{2}\ln^2 n - \ln n\,\left(\frac{1}{n} - \frac{1}{2n^2} + \mathcal{o}\left(\frac{1}{n^2}\right)\right) - \frac{1}{2}\left(\frac{1}{n} + \mathcal{o}\left(\frac{1}{n}\right)\right)^2 \\
&= \frac{\ln n}{n} - \frac{\ln n}{n^2} - \frac{\ln n}{n} + \frac{1}{2}\frac{\ln n}{n^2} + \mathcal{o}\left(\frac{\ln n}{n^2}\right) \\
&= -\frac{1}{2}\frac{\ln n}{n^2} + \mathcal{o}\left(\frac{\ln n}{n^2}\right) \\
&\sim \underbrace{-\frac{\ln n}{2n^2}}_{=\mathcal{o}\left(\frac{1}{n^{3/2}}\right)} < 0 \text{ pour } n \geqslant 2
\end{aligned}$$

Donc $\sum \dfrac{1}{n^{3/2}}$ converge et donc $\sum(u_{n+1} - u_n)$ converge donc (u_n) converge. On note $\ell = \lim u_n$. D'où

$$\boxed{\sum_{k=1}^{n} \frac{\ln k}{k} = \frac{1}{2}\ln^2 n + \ell + \mathcal{o}(1)}.$$

2. Soit $n \in \mathbb{N}^\star$. On pose $N = \left\lfloor \frac{n}{2} \right\rfloor$.

$$\sum_{k=1}^{n} (-1)^k \frac{\ln k}{k} = \sum_{1 \leqslant i \leqslant N} \frac{\ln 2i}{2i} - \sum_{0 \leqslant i \leqslant N} \frac{\ln(2i+1)}{2i+1}$$

$$\begin{aligned}
\sum_{i=1}^{N} \frac{\ln 2i}{2i} &= \frac{1}{2} \sum_{i=1}^{N} \frac{\ln 2 + \ln i}{i} \\
&= \frac{1}{2} \left(\ln 2 \sum_{i=1}^{N} \frac{1}{i} + \sum_{i=1}^{N} \frac{\ln i}{i} \right) \\
&= \frac{1}{2} \left(\ln 2 \times \left(\ln N + \gamma + o(1) \right) + \frac{1}{2} \ln^2 N + \ell + o(1) \right) \\
&= \frac{1}{4} \ln^2 N + \frac{\ln 2}{2} \ln N + \frac{\gamma \ln 2}{2} + \frac{\ell}{2} + o(1)
\end{aligned}$$

$$\begin{aligned}
\sum_{i=0}^{N} \frac{\ln(2i+1)}{2i+1} &= \sum_{k=1}^{n} \frac{\ln k}{k} - \sum_{i=1}^{N} \frac{\ln 2i}{2i} \\
&= \frac{1}{2} \ln^2 n + \ell + o(1) - \left(\frac{1}{4} \ln^2 N + \frac{\ln 2}{2} \ln N + \frac{\gamma \ln 2}{2} + \frac{\ell}{2} + o(1) \right)
\end{aligned}$$

D'où

$$\sum_{k=1}^{n} (-1)^k \frac{\ln k}{k} = \frac{1}{2} \ln^2 N + \ln 2 \times \ln N + \gamma \ln 2 + \ell - \frac{1}{2} \ln^2 n - \ell + o(1).$$

$$N \leqslant \frac{n}{2} \leqslant N + 1$$

donc

$$\frac{n}{2} - 1 < N \leqslant \frac{n}{2}$$

et donc

$$N \underset{n \to +\infty}{\sim} \frac{n}{2}$$

$$\begin{aligned}
\ln N &= \ln \left(\frac{n}{2} + o\left(\frac{n}{2} \right) \right) \\
&= \ln \left(\left(\frac{n}{2} \right) \left(1 + o(1) \right) \right) \\
&= \ln \left(\frac{n}{2} \right) + \ln \left(1 + o(1) \right) \\
&= \ln \left(\frac{n}{2} \right) + o(1) \\
&\sim \frac{n}{2}
\end{aligned}$$

$$N \leqslant \frac{n}{2} \leqslant N+1$$

donc

$$\ln(n-2) - \ln 2 = \ln\left(\frac{n}{2}-1\right) \leqslant \ln N \leqslant \ln\left(\frac{n}{2}\right) = \ln n - \ln 2$$

et donc

$$\ln^2\left(\frac{n}{2}-1\right) \leqslant \ln^2 N \leqslant \ln^2\left(\frac{n}{2}\right)$$

On a, d'une part,

$$\begin{aligned}\sum_{k=1}^{n}(-1)^k\frac{\ln k}{k} &\leqslant \frac{1}{2}\left(\ln^2 n - 2\ln n\ln 2 + \ln^2 2\right) + \ln 2\left(\ln n - \ln 2\right) + \gamma\ln 2 - \frac{1}{2}\ln^2 n + o(1)\\ &\leqslant -\frac{1}{2}\ln^2 2 + \gamma\ln 2 + o(1).\end{aligned}$$

D'autre part, on a

$$\begin{aligned}\sum_{k=1}^{n}(-1)^k\frac{\ln k}{k} &\geqslant \frac{1}{2}\big(\ln(n-2) - \ln 2\big)^2 + \ln 2\big(\ln(n-2) - \ln 2\big) + \gamma\ln 2 - \frac{1}{2}\ln^2 n + o(1)\\ &\frac{1}{2}\left(\ln^2(n-2) - \ln^2 n\right) - \frac{1}{2}\ln^2 2 + \gamma\ln 2 + o(1).\end{aligned}$$

Or,

$$\begin{aligned}\ln^2(n-2) - \ln^2 n &= \left(\ln n + \ln\left(1-\frac{2}{n}\right)\right)^2 - \ln^2 n\\ &= \underbrace{2\ln n\ln\left(1-\frac{2}{n}\right)}_{\sim -4\frac{\ln n}{n}\longrightarrow 0} + \underbrace{\ln^2\left(1-\frac{2}{n}\right)}_{\longrightarrow 0}.\end{aligned}$$

Par encadrement,

$$\sum_{k=1}^{+\infty}(-1)^k\frac{\ln k}{k} = \gamma\ln 2 - \frac{1}{2}\ln^2 2.$$

Exercice

$$\sum_{k=0}^{+\infty}\frac{1}{(2k+1)^2} = \frac{\pi^2}{8}$$

En effet

$$\begin{aligned}\frac{\pi^2}{6} = \sum_{k=1}^{+\infty} \frac{1}{k^2} &= \sum_{k=1}^{+\infty} \frac{1}{(2k)^2} + \sum_{k=0}^{+\infty} \frac{1}{(2k+1)^2} \\ &= \frac{1}{4} \times \frac{\pi^2}{6} + \sum_{k=0}^{+\infty} \frac{1}{(2k+1)^2}\end{aligned}$$

Chapitre 26

TD 26

Exercice 2

Fait à l'oral.

Exercice 3

$$\Delta_n(x) = \begin{vmatrix} \lambda_1 + x & a + x & \cdots & a + x \\ b + x & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a + x \\ b + x & \cdots & b + x & \lambda_n + x \end{vmatrix}$$

1. On fixe $x \in \mathbb{R}$. On note $C_1, \dots, C_n$ les colonnes de la matrice

$$\begin{pmatrix} \lambda_1 + x & a + x & \cdots & a + x \\ b + x & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a + x \\ b + x & \cdots & b + x & \lambda_n + x \end{pmatrix}.$$

   Le déterminant n'est pas modifié suite aux opérations $C_i \leftarrow C_i - C_1$ pour $i \in [\![2, n]\!]$. Les colonnes 2 à n de la matrice obtenue ne font plus intervenir x. En développant le déterminant suivant la première colonne, on obtient alors une expression polynomiale en x de degré au plus 1.

2. $$\Delta_n(-a) = \begin{vmatrix} \lambda_1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ & \star & \ddots & 0 \\ & & & \lambda_n - a \end{vmatrix} = \prod_{i=1}^{n} (\lambda_i - a).$$

   De même,

$$\Delta_n(-b) = \prod_{i=1}^{n} (\lambda_i - b).$$

Or,

$$\Delta_n(x) = \Delta_n(-a) + (x+a)\frac{\Delta_n(-b) - \Delta_n(-a)}{-b+a}$$

et donc

$$\begin{aligned}\Delta_n(0) &= \prod_{i=1}^{n}(\lambda_i - a) + \frac{a}{a-b}\left(\prod_{i=1}^{n}(\lambda_i - b) - \prod_{i=1}^{n}(\lambda_i - a)\right) \\ &= \frac{1}{a-b}\left(-b\prod_{i=1}^{n}(\lambda_i - a) + a\prod_{i=1}^{n}(\lambda_i - b)\right)\end{aligned}$$

Exercice 4

$$\Delta_{n+2} = \begin{vmatrix} a & b & 0 & \cdots & 0 \\ c & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & b \\ 0 & \cdots & 0 & c & a \end{vmatrix}$$

$$= a\Delta_{n+1} - c\begin{vmatrix} b & 0 & \cdots & \cdots & 0 \\ c & a & b & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & b \\ \vdots & \ddots & \ddots & \ddots & \\ 0 & \cdots & 0 & c & a \end{vmatrix}$$

$$= a\Delta_{n+1} - bc\Delta_n$$

L'équation caractéristique est

$$z^2 = az - bc$$

Son discriminant vaut

$$a^2 - 4bc = 0$$

L'unique racine est $z = \dfrac{a}{2}$.

$$\exists \alpha, \beta \in \mathbb{R},\ \forall n \in \mathbb{N},\ \Delta_n(\alpha n + \beta)\left(\frac{a}{2}\right)^n$$

Cas 1 $a \neq 0$.

$$\Delta_1 = \det\big((a)\big) = a = (\alpha + \beta)\frac{a}{2}$$

$$\Delta_2 = \begin{vmatrix} a & b \\ c & a \end{vmatrix} = \frac{3}{4}a^2 = (2\alpha + \beta)\frac{a^2}{4}$$

Cas 2 $a = 0$.

$$\forall n, \Delta_n = 0 = (n+1)\frac{a^n}{2^n}$$

Exercice 6

$$C_n(a_0,\dots,a_{n-1}) = \begin{vmatrix} -x & 0 & \cdots & 0 & a_0 \\ 1 & -x & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1}-x \end{vmatrix}$$

$$= -x \begin{vmatrix} -x & 0 & \cdots & 0 & a_1 \\ 1 & -x & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1}-x \end{vmatrix} - \begin{vmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & -x & \ddots & \vdots & a_2 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1}-x \end{vmatrix}$$

$$\begin{aligned} &= -xC_{n-1}(a_1,\dots,a_{n-1}) + (-1)^n a_0 \\ &= -x\big(-xC_{n-2}(a_2,\dots,a_{n-1}) + (-1)^{n-1}a_1\big) + (-1)^n a_0 \\ &= x^2 C_{n-2}(a_2,\dots,a_{n-1}) + (-1)^n a_1 x + (-1)^n a_0 \\ &= \cdots\cdots\cdots \\ &= (-1)^n x^n + (-1)^{n+1}\sum_{k=0}^{n-1} a_k x^k \end{aligned}$$

Exercice 7

On a

$$\begin{cases} P = \displaystyle\sum_{i=0}^{p} a_i X^i \ a_p \neq 0 \\ Q = \displaystyle\sum_{i=0}^{q} b_i X^i \ b_p \neq 0 \end{cases}$$

et

$$\begin{aligned} \varphi : \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X] &\longrightarrow \mathbb{C}_{p+q-1}[X] \\ (U,V) &\longmapsto UP + VQ. \end{aligned}$$

4. $P = X^3 + aX + b$, $p = 3$; $Q = P' = 3X^2 + a$, $q = 2$.

$$\begin{aligned} \varphi : \mathbb{C}_1[X] \times \mathbb{C}_2[X] &\longrightarrow \mathbb{C}_4[X] \\ (U,V) &\longmapsto UP + VP'. \end{aligned}$$

La base canonique de $\mathbb{C}_4[X]$ est $\big(1, X, X^2, X^3, X^4\big)$. Une base de $\mathbb{C}_1[X] \times$

$\mathbb{C}_2[X]$ est $\Big((1,0),(X,0),(0,1),(0,X),(0,X^2)\Big)$.

$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(\varphi)=\begin{pmatrix} b & 0 & a & 0 & 0\\ a & b & 0 & a & 0\\ 0 & a & 3 & 0 & a\\ 1 & 0 & 0 & 3 & 0\\ 0 & 1 & 0 & 0 & 3\end{pmatrix}$$

car

$$\begin{cases}\varphi\big((1,0)\big) &= 1\times P+0\times P'=b+aX+X^3,\\ \varphi\big((X,0)\big) &= XP=bX+aX^2+X^4,\\ &\vdots\end{cases}$$

$$\begin{vmatrix} b & 0 & a & 0 & 0\\ a & b & 0 & a & 0\\ 0 & a & 3 & 0 & a\\ 1 & 0 & 0 & 3 & 0\\ 0 & 1 & 0 & 0 & 3\end{vmatrix} = \begin{vmatrix} b & 0 & a & 0 & 0\\ a & b & 0 & a & -3b\\ 0 & a & 3 & 0 & -2a\\ 1 & 0 & 0 & 3 & 0\\ 0 & 1 & 0 & 0 & 0\end{vmatrix}$$

$$= -\begin{vmatrix} b & a & 0 & 0\\ a & 0 & a & -3b\\ 0 & 3 & 0 & -2a\\ 1 & 0 & 3 & 0\end{vmatrix}$$

$$= -\begin{vmatrix} b & a & -3b & 0\\ a & 0 & -2a & -3b\\ 0 & 3 & 0 & -2a\\ 1 & 0 & 0 & 0\end{vmatrix}$$

$$= \begin{vmatrix} a & -3b & 0\\ 0 & -2a & -3b\\ 3 & 0 & -2a\end{vmatrix}$$

$$= a\begin{vmatrix}-2a & -3b\\ 0 & -2a\end{vmatrix}+3\begin{vmatrix}-3b & 0\\ -2a & -3b\end{vmatrix}$$

$$= 4a^3+27b^2$$

$$\begin{aligned} P \text{ a une racine multiple} &\iff P \text{ et } P' \text{ ont une racine commune}\\ &\iff \text{le resultant de } P \text{ et } P' \text{ est nul}\\ &\iff 4a^3+27b^2=0.\end{aligned}$$

1. Soit $(U,V)\in\mathbb{C}_{q-1}[X]\times\mathbb{C}_{p-1}[X]$.

$$\begin{aligned}\deg(U) &\leqslant q-1\\ \text{donc } \deg(UP) &= \deg(U)+\deg(P)\\ &\leqslant q-1+p\end{aligned}$$

De même, $\deg(V) \leqslant p-1$ et donc $\deg(VQ) = \deg(V)+\deg(Q) \leqslant p-1+q$. On en déduit que $\deg(UP+VQ) \leqslant p-1+q$. Ainsi, φ est bien définie.

Soient $(U_1, V_1) \in \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$, $(U_2, V_2) \in \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$, et $(\lambda_1, \lambda_2) \in \mathbb{C}^2$.

$$\begin{aligned}
\varphi\big(\lambda(U_1,V_1)+\lambda_2(U_2,V_2)\big) &= \varphi\big((\lambda_1U_1+\lambda_2U_2),(\lambda_1V_1+\lambda_2V_2)\big)\\
&= (\lambda_1U_1+\lambda_2U_2)\,P+(\lambda_1V_1+\lambda_2V_2)\,Q\\
&= \lambda_1U_1P+\lambda_2V_2P+\lambda_1V_1Q+\lambda_2V_2Q\\
&= \lambda_1(U_1P+V_1Q)+\lambda_2(U_2P+V_2Q)\\
&= \lambda_1\varphi(U_1,V_1)+\lambda_2\varphi(U_2,V_2)
\end{aligned}$$

Ainsi φ est linéaire.

On pose, pour $k \in [\![0, p+q-1]\!]$,

$$P_k = \begin{cases} \big(X^k, 0\big) & \text{si } k < q, \\ \big(0, X^{k-q}\big) & \text{si } k \geqslant q. \end{cases}$$

Soit $k \in [\![0, p+q-1]\!]$.

$$\begin{aligned}
\varphi(P_k) &= \begin{cases} X^kP & \text{si } k < q \\ X^{k-q}Q & \text{si } k \geqslant q \end{cases}\\
&= \begin{cases} \displaystyle\sum_{i=0}^{p} a_iX^{k+i} & \text{si } k < q \\ \displaystyle\sum_{i=0}^{q} b_iX^{k-q+i} & \text{si } k \geqslant q \end{cases}\\
&= \begin{cases} \displaystyle\sum_{j=k}^{k+q} a_{j-k}X^j & \text{si } k < q \\ \displaystyle\sum_{j=k-q}^{k} b_{j-k+q}X^j & \text{si } k \geqslant q. \end{cases}
\end{aligned}$$

Donc,

$$\mathrm{Mat}_{\mathscr{B}_1,\mathscr{B}_2}(\varphi) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & & b_0 \\ a_p & a_{p-1} & \cdots & a_0 & b_q & & & \\ 0 & a_q & \ddots & \vdots & 0 & & & \\ \vdots & \ddots & \ddots & 0 & & & & \\ 0 & 0 & \cdots & a_p & & & b_q & \end{pmatrix}$$

2. On sait que $P(a) = Q(a) = 0$. Supposons φ surjective. $1 \in \mathbb{C}_{p+q-1}[X]$. Soit (U, V) un antécédent de 1 par φ. Ainsi

$$1 = UP + VQ$$

En évaluant en a l'égalité précédente fournit

$$\begin{aligned} 1 &= U(A)P(A + V(a)Q(a) \\ &= U(a) \times 0 + V(a) \times 0 \\ &= 0. \end{aligned}$$

Donc $1 \notin \mathrm{Im}(\varphi)$ et donc φ n'est pas surjective.

Enfin,

$$\begin{aligned} \dim\left(\mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]\right) &= \dim\left(\mathbb{C}_{q-1}[X]\right) + \dim\left(\mathbb{C}_{p-1}[X]\right) \\ &= q - 1 + 1 + p - 1 + 1 \\ &= p + q \\ &= \dim\left(\mathbb{C}_{p+q-1}[X]\right) \end{aligned}$$

Ainsi $\mathrm{Mat}_{\mathscr{B}_1,\mathscr{B}_2}(\varphi)$ est carrée.

Comme φ n'est pas bijective, $\mathrm{Mat}_{\mathscr{B}_1,\mathscr{B}_2}(\varphi) \notin \mathrm{GL}_{p+q}(\mathbb{C})$ et donc $\det\left(\mathrm{Mat}_{\mathscr{B}_1,\mathscr{B}_2}(\varphi)\right) = 0$.

3. On suppose que le résultant de P et Q est nul. Donc φ n'est pas injective et donc $\mathrm{Ker}(\varphi) \neq \{(0,0)\}$.

Soit $(U, V) \in \mathrm{Ker}(\varphi) \setminus \{(0,0)\}$. Ainsi

$$UP + VQ = 0$$

et donc

$$P \mid VQ.$$

Supposons $P \wedge Q = 1$. D'après le théorème de Gauß, $P \mid V$.

Or $\deg P = p$ (car $a_p \neq 0$) et $\deg V \leqslant p-1$.

Donc $V = 0$ et donc $UP = 0$, donc $U = 0$ i.e. $(U,V) = (0,0)$: une contradiction.

On vient de prouver que P et Q ne sont pas premiers entre eux. Soit $D = P \wedge Q$. D'après ce qui précède, $\deg(D) \geqslant 1$, et donc D a au moins une racine $a \in \mathbb{C}$ par le théorème d'Alambert–Gauß.

Comme $D \mid P$ et $D(a) = 0$, on peut conclure que $P(a) = 0$. De même $Q(a) = 0$.

Exercice 8

1. On a :
$$\det u = \begin{array}{c} \begin{matrix} f(1) & f(X) & f(X^2) & \cdots & f(X^{n-1}) & f(X^n) \end{matrix} \\ \left|\begin{matrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 2 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & n \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{matrix}\right| \end{array} \begin{matrix} 1 \\ X \\ X^2 \\ \vdots \\ X^{n-1} \\ X^n \end{matrix} = 1.$$
2. On a $\det u = 0$ car $\operatorname{Ker} u \ni 1$.
3. On a
$$\det u = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & n \end{vmatrix} = n!.$$

Exercice 9

$\det(f)^2 = (-1)^n$ donc $\det f \in \mathbb{R} \iff n \in 2\mathbb{Z}$.

Exercice 10

$\mathscr{B} = (E_{11}, E_{12}, E_{13}, \ldots, E_{1n}, E_{21}, E_{22}, \ldots, E_{2n}, \ldots, E_{nn})$

$$\det u = ❀ = (-1)^{\frac{n(n-1)}{2}}.$$

Exercice

On a $2n+1$ cailloux et, à chaque fois qu'on retire un caillou quelconque, on divise le tas de cailloux en deux tas de même masse. Montrer que tous les cailloux ont

la même masse.

$$A = \begin{pmatrix} 0 & -1 & 1 & -1 & -1 & \cdots & \cdots & 1 \\ 1 & 0 & \ddots & \ddots & 1 & 1 & \cdots & -1 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & \ddots & & \\ & & & & \ddots & \ddots & & \\ & & & & & \ddots & \ddots & \\ & & & & & & & 0 \end{pmatrix} \in \mathscr{M}_{2n+1}(\mathbb{R}).$$

$$A \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$A \begin{pmatrix} m_1 \\ \vdots \\ m_{2n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\left.\begin{array}{l} \exists B \text{ extraite de } A \\ B \in \mathrm{GL}_{2n}(\mathbb{R}). \end{array}\right\} \implies \operatorname{rg} A = 2n \implies \dim(\operatorname{Ker} A) = 1 \implies \begin{pmatrix} m_1 \\ \vdots \\ m_{2n+1} \end{pmatrix} \text{ colinéaire à } \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & \ddots & \pm 1 \\ & \ddots & \\ \pm 1 & & 0 \end{pmatrix}$$

$\det B \in \mathbb{Z}$. Montrons que $\det B \equiv 1 \ [2]$.

$$\begin{aligned} \det B &\equiv \begin{vmatrix} 0 & \ddots & 1 \\ & \ddots & \\ -1 & & 0 \end{vmatrix} \ [2] \\ &\equiv 1 \ [2]\,. \end{aligned}$$

Chapitre 27

TD 27

Exercice 1

Analyse Soient P une probabilité sur $[\![1,n]\!]$ et $\alpha \in \mathbb{R}$ tels que

$$\forall k,\, P(\{k\}) = \alpha k.$$

D'où,

$$\begin{aligned} 1 = P\big([\![1,n]\!]\big) &= P\left(\bigcup_{k=1}^{n}{\cdot}\{k\}\right) \\ &= \sum_{k=1}^{n} P(\{k\}) = \alpha \sum_{k=1}^{n} k \\ &= \alpha \frac{n(n+1)}{2} \end{aligned}$$

et donc

$$\alpha = \frac{2}{n(n+1)}.$$

Synthèse On pose $\alpha = \dfrac{2}{n(n+1)}$ et

$$\forall k \in [\![1,n]\!], p_k = \alpha k.$$

On remarque que

$$\forall k \in [\![1,n]\!], p_k \geqslant 0$$

et

$$\sum_{k=1}^{n} p_k = \frac{2}{n(n+1)} \sum_{k=1}^{n} k = \frac{2}{n(n+1)} \times \frac{n(n+1)}{2} = 1.$$

D'après un résultat du cours, il existe une probabilité P sur $[\![1,n]\!]$ telle que

$$\forall k \in [\![1,n]\!],\, P(\{k\}) = p_k = \alpha k.$$

Exercice 2

On pose $\Omega = \Big\{A \in \mathcal{P}\big(\llbracket 1, N \rrbracket\big) \mid \#A = k\Big\}$. On a $\#\Omega = \binom{N}{k}$.

Soient $d_1, \dots, d_n$ les pièces défectueuses. On pose

$$A_k = \Big\{\omega \in \Omega \mid \#\big(\omega \cap \{d_1, \dots, d_n\}\big) = j\Big\}$$

et P l'équiprobabilité.

$$P(A_j) = \frac{\#A_j}{\#\Omega} = \frac{\binom{n}{j}\binom{N-n}{k-j}}{\binom{N}{k}}$$

Exercice 3

1.

$$\begin{aligned} P(A \cap B) &= P(A) + P(B) - \overbrace{P(A \cup B)}^{\in[0,1]} \\ &\geqslant P(A) + P(B) - 1 \end{aligned}$$

2. par récurrence sur n :

$$\begin{aligned} P\left(\bigcap_{i=1}^{n+1} A_i\right) &= P\left(\bigcap_{i=1}^{n} A_i \cap A_{n+1}\right) \\ &\geqslant P\left(\bigcap_{i=1}^{n} a_i\right) + P(A_{n+1}) - 1 \\ &\geqslant \sum_{i=1}^{n} P(A_i) - (n-1) + P(A_{n+1}) - 1 \\ &\geqslant \sum_{i=1}^{n+1} P(A_i) - n. \end{aligned}$$

Exercice 4

On pose $\Omega_n = \llbracket 1, 365 \rrbracket^n$, P_n l'équiprobabilité sur Ω_n et

$$\overline{A}_n = \big\{(\omega_1, \dots, \omega_n) \in \Omega_n \mid \forall i \neq j, \omega_i \neq \omega_j\big\}.$$

$$\begin{aligned} P_n(A_n) &= 1 - P_n(\overline{A}_n) \\ &= 1 - \frac{365!}{(365-n)!\ 365^n} \end{aligned}$$

On a

$$P_n(A_n) \geqslant \frac{1}{2} \iff n \geqslant 23$$
$$P_n(A_n) \geqslant 0{,}95 \iff n \geqslant 47.$$

Exercice 5

1. On a
$$\overline{A} = \{f\}^n \cup \{g\}^n$$
donc
$$\begin{aligned} P(A) &= 1 - P(\overline{A}) \\ &= 1 - \frac{2}{2^n} \\ &= \frac{2^n - 2}{2^n}. \end{aligned}$$

Et,
$$B = \{g\}^n \cup \{(f, g, \ldots, g)\} \cup \{(g, f, g, \ldots, g)\} \cup \cdots \cup \{(g, \ldots, g, f)\}$$
donc $P(B) = \dfrac{n+1}{2^n}$.

2. $P(A \cap B) = \dfrac{n}{2^n}$ et $P(A)\,P(B) = \dfrac{2^n - 2}{2} \times \dfrac{n+1}{2^n}$ d'où
$$\begin{aligned} & P(A \cap B) = P(A)\,P(B) \\ \iff & n2^n = (2^n - 2)(n+1) \\ \iff & 2^n - 2n - 2 = 0 \\ \iff & 2^{n-1} - n - 1 = 0? \end{aligned}$$

Soit $f : x \mapsto 2^{x-1} - x - 1$ dérivable sur $\mathbb{R}$ et
$$\forall x \in \mathbb{R},\ f'(x) = \ln(2)2^{x-1} - 1.$$

Soit $x \in \mathbb{R}$.
$$\begin{aligned} f'(x) > 0 &\iff 2^{x-1} > \frac{1}{\ln 2} \\ &\iff (x-1)\ln 2 > \ln\left(\frac{1}{\ln 2}\right) \\ &\iff x > \frac{-\ln(\ln 2)}{\ln 2} + 1 \simeq 1{,}5. \end{aligned}$$

Donc, f est strictement croissante sur $[2, +\infty[$.

x	0		$-\dfrac{\ln(\ln 2)}{\ln 2}$		3		$+\infty$
f	<0	↘		↗	0	↗	$+\infty$

Donc $n = 3$ est la seule solution de $(\star)$.

Exercice 6

Soit (Ω, P) un espace probabilisé qui modélise cette situation.

$$\forall i \in \{1,2,3\},\ \begin{cases} P(A_i) = \dfrac{1}{3} \\ P_{A_i}(R_i) = 1 - \alpha_i. \end{cases}$$

1. Soit $i \in \{1,2,3\}$.

$$\begin{aligned} P_{\overline{R}_i}(A_i) &= \frac{P_{A_i}(\overline{R}_i)\, P(A_i)}{P_{A_i}(\overline{R}_i)\, P(A_i) + P_{\overline{A}_i}(\overline{R}_i)\, P(\overline{A}_i)} \\ &= \frac{\frac{\alpha_i}{3}}{\frac{\alpha_i}{3} + \frac{2}{3}} \\ &= \frac{\alpha_i}{2+\alpha_i} \end{aligned}$$

2. Soit $f : x \mapsto \dfrac{x}{2+x}$ dérivable sur $[0,1]$ et

$$\forall x \in [0,1],\ f'(x) = \frac{2 + \not{x} - \not{x}}{(2+x)^2} > 0.$$

x	0		1
f	0	↗	$\dfrac{1}{3}$

Exercice 7

1. On pose $\Omega = \left\{\omega \in \mathcal{P}(\llbracket 1, n+m \rrbracket) \mid \#\omega = n\right\}$, P l'équiprobabilité.

Soit $A \in \mathcal{P}(\Omega)$ qui représente l'événement considéré. On a

$$P(A) = \frac{\#A}{\#\Omega} = \frac{\#A}{\binom{n+m}{n}}.$$

Par exemple, avec $n = 5$, $m = 4$ et $r = 3$. On cherche

_____.

On place i_1 "L" avec $i_1 \geqslant 0$.
Puis, j_1 "O" avec $j_1 > 0$.
Puis, i_2 "L" avec $i_1 > 0$.
Puis, j_2 "O" avec $j_2 > 0$.
$\vdots$
Puis, j_r "O" avec $j_r > 0$.
Enfin, on place i_{r+1} "L" avec $i_{r+1} \geqslant 0$.

On doit avoir

$$\begin{cases} \sum_{k=1}^{r+1} i_k = m \\ \sum_{k=1}^{r} j_k = n \end{cases}$$

On a

$$\#A = \binom{n-1}{r-1}\binom{m+1}{r}$$

d'où

$$P(A) = \frac{\binom{n-1}{r-1}\binom{m+1}{r}}{\binom{m+n}{n}}.$$

2.

$$\frac{\binom{6}{6}\binom{10}{7}}{\binom{16}{7}} \simeq 0{,}01$$

Exercice 8

Soit (Ω, P) un espace probabilisé qui modélise cette situation,

$$\forall i \in [\![1, 10]\!],\ D_i : \text{"le wagon } i \text{ a un défaut"}.$$

On a

$$\forall i \in [\![1, 10]\!],\ P(D_i).$$

Les événements $(D_i)_{i \in [\![1,10]\!]}$ sont mutuellement indépendants pour P.

On pose

$\forall i \in [\![1, 10]\!]$, $\forall j \in \{1, 2\}$, $C_{i,j}$: "le contrôleur j détecte un défaut dans le wagon i",

$$\forall i \in [\![1, 10]\!],\ \forall j \in \{1, 2\},\ P_{D_i}(C_{i,j}) = \frac{7}{10}$$

et, pour tout $i \in [\![1, 10]\!]$, $C_{i,1}$ et $C_{i,2}$ sont indépendants pour P_{D_i}.

1. On note R : “le train est retardé”. On a

$$\overline{R} = \bigcap_{\substack{i\in[\![1,10]\!]\\ j\in\{1,2\}}} \overline{C}_{i,j}.$$

On note, pour $I \in \mathscr{P}\big([\![1,10]\!]\big)$,

$$\mathscr{D}_I = \left(\bigcap_{i\in I} D_i\right) \cap \left(\bigcap_{i\notin I} \overline{D}_i\right).$$

$(\mathscr{D}_I)_{I\in\mathscr{P}([\![1,10]\!])}$ est un système complet d'événements.

$$P(\overline{R}) = \sum_{I\in\mathscr{P}([\![1,10]\!])} P_{\mathscr{D}_I}(\overline{R})P(\mathscr{D}_I).$$

Soit $I \in \mathscr{P}([\![1,10]\!])$.

$$\begin{aligned} P(\mathscr{D}_i) &= \prod_{i\in I}\frac{1}{10}\prod_{i\notin I}\frac{9}{10} \\ &= \left(\frac{1}{10}\right)^{\#I}\left(\frac{9}{10}\right)^{10-\#I} \\ &= \frac{9^{10-\#I}}{10^{10}} \end{aligned}$$

$$\begin{aligned} P_{\mathscr{D}_I}(\overline{R}) &= P_{\mathscr{D}_I}\left(\bigcap_{i\in I}\overline{C}_{i,j}\right) \\ &= \left(\left(\frac{3}{10}\right)^{\#I}\right)^2 \\ &= \left(\frac{3}{10}\right)^{2\#I}. \end{aligned}$$

D'où

$$\begin{aligned}
P(\overline{R}) &= \sum_{I\in\mathscr{P}([\![1,10]\!])} \left(\frac{3}{10}\right)^{2\#I} \frac{9^{10-\#I}}{10^{10}} \\
&= \left(\frac{9}{10}\right)^{10} \sum_{I\in\mathscr{P}([\![1,10]\!])} \frac{1}{100^{\#I}} \\
&= \left(\frac{9}{10}\right)^{10} \sum_{k=0}^{10} \sum_{\substack{I\in\mathscr{P}([\![1,10]\!]) \\ \#I=k}} \frac{1}{100^k} \\
&= \left(\frac{9}{10}\right)^{10} \sum_{k=0}^{10} \frac{1}{100^k} \binom{10}{k} \\
&= \left(\frac{9}{10}\right)^{10} \left(1+\frac{1}{100}\right)^{k} \\
&= \left(\frac{909}{1000}\right)^{10}.
\end{aligned}$$

On en déduit que

$$\begin{aligned}
P(R) &= 1 - P(\overline{R}) \\
&= 1 - \left(\frac{909}{1000}\right)^{10} \\
&\simeq 0{,}615
\end{aligned}$$

2. On pose $\mathscr{D} = \bigcup_{\substack{I\subset[\![1,10]\!] \\ I\neq}} \mathscr{D}_I$.

Exercice 9

$$\begin{aligned}
&\left(\frac{5}{6}\right)^n \leqslant \frac{1}{2} \\
\iff & n\ln\left(\frac{5}{6}\right) \leqslant \ln(\frac{1}{2}) \\
\iff & n \geqslant \frac{\ln\left(\frac{1}{2}\right)}{\ln\left(\frac{5}{6}\right)} \\
\iff & n \geqslant 4
\end{aligned}$$

Exercice 10

On condisère un espace probabilisé (Ω, P) qui modélise la situation. On pose

$$A : \text{“on a caché le trésor”}$$
$$\forall i \in [\![1, N]\!], T_i : \text{“le trésor est dans le coffre } i\text{”}.$$

On suppose que

$$P(A) = p$$
$$P_A(T_i) = \frac{1}{N}$$
$$P_{\overline{A}}(T_i) = 0.$$

On cherche $P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}}(T_N)$.

$$\begin{aligned}
P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}} &= P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}}(A)\, P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1} \cap A}(T_n) + P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}}(\overline{A}) P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1} \cap \overline{A}}(T_n) \\
&= P_{\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}}(A) \\
&= \frac{P_A(\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}) P(A)}{P_A(\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}) P(A) P_{\overline{A}}(\overline{T}_1 \cap \cdots \cap \overline{T}_{N-1}) P(\overline{A})} \\
&= \frac{p\frac{1}{N}}{p\frac{1}{N}(1-p)} \\
&= \frac{p}{p + N(1-p)} \xrightarrow[N \to +\infty]{} 0.
\end{aligned}$$

```python
def experience(p, N):
  coffres = [True] * N
  if rd.random() < p:
    k = rd.randint(0, N-1)
    coffres[k] = True
  else:
    k = -1
  return k == N - 1

def proba(p, N, n):
  cases = 0
  for i in range(n):
    if experience(p, N):
      cases += 1
  return cases / n
```

Exercice 11

1. On pose, pour tout $k \in [\![1, N]\!]$, U_k : “l'urne k a été choisie” ; et, pour tout $n \in \mathbb{N}^\star$, B_n : “la n-ième boule tirée est blanche”.

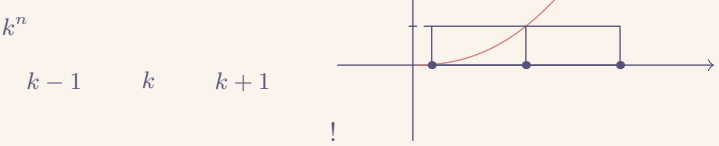
$$P\left(B_{n+1} \mid \bigcap_{i=1}^{n} B_i\right) = \frac{P(B_{n+1} \cap B_1 \cap \cdots \cap B_n)}{P(B_1 \cap \cdots \cap B_n)}.$$

$$\begin{aligned} P(B_1 \cap \cdots \cap B_n) &= \sum_{k=0}^{N} P_{U_k}(B_1 \cap \cdots \cap B_n)\, P_(U_k) \\ &= \frac{1}{N+1} \sum_{k=0}^{N} \left(\frac{k}{N}\right)^n ; \end{aligned}$$

$$P(B_1 \cap \cdots \cap B_{n+1}) = \frac{1}{N+1} \sum_{k=0}^{N} \left(\frac{k}{N}\right)^{n+1} ;$$

$$P_{B_1 \cap \cdots \cap B_n}(B_{n+1}) = \frac{1}{N} \times \frac{\sum_{k=1}^{N} k^{n+1}}{\sum_{k=1}^{N} k^n}.$$

On pose $f : x \mapsto x^n$.



$$\sum_{k=1}^{N} k^n \underset{N\to+\infty}{\sim} \frac{N^{n+1}}{n+1}$$

et donc

$$P_{B_1 \cap \cdots \cap B_n}(B_{n+1}) \underset{N\to+\infty}{\sim} \frac{1}{N} \times N \times \frac{n+1}{n+2} = \frac{n+1}{n+1} \xrightarrow[N\to+\infty]{} \frac{n+1}{n+2}.$$

Exercice 12

$$\begin{aligned} p_{n+1} &= q(1-p_n) + pp_n \\ &= (1-p)(1-p_n) + pp_n \\ &= p_n(2p-1) + 1 - p \end{aligned}$$

On a

$$p_n = \alpha(2p-1)^n + \frac{1}{2}$$

car

$$\begin{aligned} & x = x(2p-1) + 1 - p \\ \iff & x(2p-2) = p - 1 \\ \iff & x = \frac{1}{2} \end{aligned}$$

On a $p_1 = 1$ donc

$$\alpha(2p-1) + \frac{1}{2} = 1$$
$$\iff \alpha = \frac{\frac{1}{2}}{2p-1} = \frac{1}{4p-2}$$

On a donc

$$p_n = \frac{1}{4p-2}(2p-1)^n + \frac{1}{2} = \frac{1}{2}(2p-1)^{n_1} + \frac{1}{2} \xrightarrow[n\to+\infty]{} \frac{1}{2}.$$

Méthode : suites arithmético-géométriques

On a

$$\forall n,\ u_{n+1} = au_n + b.$$

L'application

$$\begin{aligned} \varphi : \mathbb{C}^{\mathbb{N}} &\longrightarrow \mathbb{C}^{\mathbb{N}} \\ (u_n) &\longmapsto (u_{n+1} - au_n) \end{aligned}$$

est linéaire. On a donc,

$$\varphi(u) = (b)_{n\in\mathbb{N}} \iff \overset{\operatorname{Ker}\varphi}{\underset{\cap}{u}} + \underbrace{u_0}_{\text{suite constante}}.$$

On a $\operatorname{Ker}\varphi = \operatorname{Vect}\big((a^n)\big)$.

Exercice 13

L'indicatrice d'Euler $\varphi(n)$ est le nombres de nombres premiers inférieurs à n :

$$\varphi(n) = \#\{k \in [\![1,n]\!] \mid k \wedge n = 1\} = \#\{\mathbb{Z}/n\mathbb{Z}^\times\}.$$

1. On a
$$P(A_p) = \frac{\#A_p}{\#\Omega} = \frac{n/p}{n} = \frac{1}{p}.$$

2. On suppose $p \wedge q = 1$.
$$P(A_p \cap A_q) = \frac{\#(A_p \cap A_q)}{\#\Omega} = \frac{\frac{n}{pq}}{n} = \frac{1}{pq} = \frac{1}{p} \times \frac{1}{q} = P(A_p) \times P(A_q).$$

3.
$$\overline{B} = \bigcup_{\substack{p \text{ premier} \\ p|n}} A_p$$

donc

$$B = \bigcap_{\substack{p \text{ premier} \\ p|n}} \overline{A}_p.$$

Montrons que les $\left(\overline{A}_p\right)_{\substack{p \text{ premier} \\ p|n}}$ sont muntuellement indépendants.

Soient $p_1, \dots, p_r$ des nombres premiers divisant n distincts 2 à 2.

$$\begin{aligned} P(A_{p_1} \cap \cdots \cap A_{p_r}) &= \frac{\frac{n}{p_1 \times \cdots \times p_r}}{n} \\ &= \frac{1}{p_1 \times \cdots \times p_r} \\ &= \prod_{i=1}^{r} P(A_{p_i}) \end{aligned}$$

Donc,

$$P(B) = \prod_{\substack{p \text{ premier} \\ p|n}} P(\overline{A}_p) = \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

On en déduit que

$$\#B = \#\Omega\, P(B) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

Exercice 14

Pour la question 1, la question est simple donc la rédaction doit être propre. Pour la question 2, il faut lire l'énoncé. Pour la question 2a, on développe. Pour la question 2b, on passe (E) au carré, donc le membre de droit de l'expression de la question a. D'après la question 1, on sait que les termes sont positifs donc tous les termes sont nuls et donc les coordonées de V sont de même signe.
Pour la question 3, on utilise le même procédé que pour la 2 :

$$\begin{aligned} \left(\sum_{i=1}^{N} v_i\right)^2 &= \left(\sum_{i=1}^{N} v_i\right)\left(\sum_{j=1}^{N} v_j\right) \\ &= \sum_{1 \leqslant i,j \leqslant N} v_i v_j \\ &= \sum_{i=1}^{N} v_i^2 + 2 \sum_{1 \leqslant i < j < N} v_i v_j. \end{aligned}$$

Pour la question 4, on a $\dfrac{1-\rho}{N} > 0$ donc $G_{i,j} > 0$ pour tout i, j.
Pour les questions 5 et 6, on a une disjonction de cas. Pour la question 5, on

utilise la définition de $A_{i,j}$ ce qui annule des termes. Pour la question 6, on remplace $A_{i,j}$ et on simplifie.
Pour la question 7, G est une matrice stochastique.
Pour la question 8, on développe la matrice et on utilise la défintion du PageRank.

La notation $P(A \mid B)$ représente $P_B(A)$; $1-\rho$ représente la probabilité de rentrer une nouvelle URL.
Pour la question 9, on utilise les propriétés de la probabilité P et que $A_n^1, \dots, A_n^N$ représente un système complet d'événements.
Pour la question 10,

$$\begin{aligned} P(A_n^i \cap A_{n-1}^j) &= P(A_n^i \mid A_{n-1}^j)\, P(A_{n-1}^j) \\ &= G_{i,j}(V_{n-1})_j. \end{aligned}$$

Pour la question 11, on utilise les probabilités totales et le calcul précédent ; on obitient un produit matriciel.
Pour la question 12, pour le faire proprement, on peut faire une récurrence.

On cherche la limite de V_k et donc la limite de G^n.

Pour la question 13, on pose $V = \begin{pmatrix} x \\ y \end{pmatrix}$ et on résout le système associé.
Pour la question 14, on trouve parmi les solutions de la question 13 le vecteur de probabilité.

Pour retrouver le résultat de la question 15, on peut utiliser une équation polynomiale. Par exemple, avec

$$A = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix},$$

on pose

$$P = X^2 - 5X + 6.$$

En évaluant $X = A$, on a

$$A^2 - 5A + 6I_2 = (0).$$

Pour trouver P, on a

$$P = X^2 - \operatorname{tr}(A)X + \det(A).$$

On a

$$X^n = (X^2 - 5X + 6)Q_n(X) + (a_n X + b_n).$$

et $A^n = a_n A + b_n I_n$.

Chapitre 28

TD 28

Exercice 1

$$F = A + V$$

où $A = (0,1,0)$ et $V = \text{Vect}\left((0,1,-1)\right)$ donc F est une droite affine.

Exercice 2

On a $\overrightarrow{OM} = \alpha\,\vec{\imath} + \beta\,\vec{\jmath}$ donc $\text{Mat}_{\mathscr{B}}\left(\overrightarrow{OM}\right) = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ et $\overrightarrow{O'M} = \alpha'\,\vec{u} + \beta'\,\vec{v}$ donc $\text{Mat}_{\mathscr{C}}\left(\overrightarrow{O'M}\right) = \begin{pmatrix}\alpha'\\ \beta'\end{pmatrix}$.

On a $\overrightarrow{O'M} = \overrightarrow{O'O} + \overrightarrow{OM}$ et $\text{Mat}_{\mathscr{C}}\left(\overrightarrow{O'O}\right) = -\,\text{Mat}_{\mathscr{C}}\left(\overrightarrow{OO'}\right)$.

$\overrightarrow{OO'} = a\,\vec{\imath} + b\,\vec{\jmath}$ donc $\text{Mat}_{\mathscr{B}}\left(\overrightarrow{OO'}\right) = \begin{pmatrix}a\\ b\end{pmatrix}$.

On a $P = P_{\mathscr{B}\to\mathscr{C}} = \begin{pmatrix}x & x'\\ y & y'\end{pmatrix}$ et donc $P^{-1} = \dfrac{1}{xy' - yx'}\begin{pmatrix}y' & -x'\\ -y & x\end{pmatrix}$.

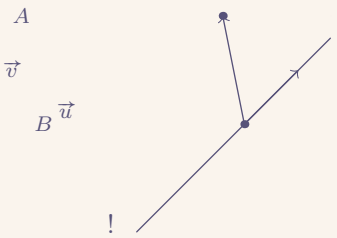
Or,

$$\forall \vec{w} \in \vec{E},\ \text{Mat}_{\mathscr{C}}\left(\vec{w}\right) = P^{-1}\,\text{Mat}_{\mathscr{B}}\left(\vec{w}\right).$$

Donc,

$$\begin{aligned}\begin{pmatrix}\alpha'\\ \beta'\end{pmatrix} &= -P^{-1}\begin{pmatrix}a\\ b\end{pmatrix} + P^{-1}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\\ &= P^{-1}\begin{pmatrix}\alpha - a\\ \beta - b\end{pmatrix}\\ &= \frac{1}{xy' - yx'}\begin{pmatrix}y'(\alpha - x) - x'(\beta - b)\\ -y(\alpha - a) + x(\beta - b)\end{pmatrix}.\end{aligned}$$

Exercice 3



$$\left.\begin{matrix} x-3y+2z=1 \\ 2x+y-3z=-1 \end{matrix}\right\} \iff \begin{cases} x-3y+2z=1 \\ 7y-7z=-3 \end{cases}$$
$$\iff \begin{cases} y=-\dfrac{3}{7}+z \\ x=-\dfrac{2}{7}+z \end{cases}$$
$$\iff (x,y,z)=\left(-\frac{2}{7}+z,-\frac{3}{7}+z,z\right)$$
$$=\left(-\frac{2}{7},-\frac{3}{7},0\right)+z(1,1,1)$$

On pose B le point de coordonnées $\left(-\frac{2}{7},-\frac{3}{7},0\right)$ et $\vec{u}$ le vecteur de coordonnées $(1,1,1)$. On a $B \in D$. On pose $\vec{D}=\text{Vect}\,(\vec{u})$.

On pose $\vec{v}=\overrightarrow{BA}$: ses coordonnées sont $\left(1+\frac{2}{7},-1+\frac{3}{7},1-0\right)=\left(\frac{9}{7},-\frac{4}{7},1\right)$.

Soit M de coordonnées (x,y,z).

$$\begin{aligned} M \in P &\iff \overrightarrow{AM} \in \text{Vect}\,(\vec{u}+\vec{v}) \\ &\iff \text{la famille } \left(\overrightarrow{AM},\vec{u},\vec{v}\right) \text{ est liée} \\ &\iff \det_{\mathscr{B}}\left(\overrightarrow{AM},\vec{u},\vec{v}\right)=0 \\ &\iff \begin{vmatrix} x-1 & 1 & \frac{9}{7} \\ y+1 & 1 & -\frac{4}{7} \\ z-1 & 1 & 1 \end{vmatrix}=0 \\ &\iff \frac{11}{7}(x-1)+\frac{2}{7}(y+1)-\frac{13}{7}(z-1)=0 \\ &\iff 11x+2y-13z+4=0 \end{aligned}$$

Exercice 4

1.

$$D \text{ et } D' \text{ sont complanaires} \iff \begin{cases} D \cap D' \neq \\ \text{ ou} \\ \vec{D} = \vec{D'}. \end{cases}$$

$$\begin{aligned} D \cap D' \neq \emptyset &\iff \begin{cases} \boxed{x} - 2z = 1 \\ y - z = 2 \\ x + y + z = 1 \\ x - 2y + 2z = a \end{cases} \\ &\iff \begin{cases} \boxed{x} - 2z = 1 \\ \boxed{y} - z = 2 \\ y + 3z = 0 \\ -2y + 4z = a - 1 \end{cases} \\ &\iff \begin{cases} x - 2z = 1 \\ y - z = 2 \\ z = -\dfrac{1}{2} \\ 0 = a + 4 \end{cases} \end{aligned}$$

Si $a = -4$, D et D' sont sécantes donc coplanaires.

On suppose maintenant $a \neq -4$. On a

$$\vec{D} : \begin{cases} x - 2z = 0 \\ y - z = 0 \end{cases}$$

et donc $\vec{D} = \text{Vect}\big(\underbrace{(2,1,1)}_{\vec{u}}\big)$.

On a

$$\vec{D'} : \begin{cases} x + y + z = 0 \\ x - 2y + 2z = 0 \end{cases} .$$

Or, $\vec{u} \notin \vec{D'}$ et donc $\vec{D} \neq \vec{D'}$. Les droites ne sont jamais parallèles.

2. On suppose $a = -4$. On pose A le point de coordonnées de $\left(0, \dfrac{3}{2}, -\dfrac{1}{2}\right)$.
On a $A \in D \cap D'$. On pose $\vec{u}$ le vecteur de coordonnées $(2,1,1)$ et $\vec{v}$ le vecteur de coordonnées $(-4,1,3)$.

Soit M un point de coordonnées (x, y, z).

$$\begin{aligned} M \in P &\iff \overrightarrow{AM} \in \text{Vect}\,(\vec{u}, \vec{v}) \\ &\iff \begin{vmatrix} x & 2 & -4 \\ y - \dfrac{3}{2} & 1 & 1 \\ z + \dfrac{1}{2} & 1 & 3 \end{vmatrix} = 0 \\ &\iff 2x - 10\left(y - \frac{3}{2}\right) + 6\left(z + \frac{1}{2}\right) = 0 \\ &\iff 2x - 10y + 6z + 18 = 0. \end{aligned}$$

Exercice 5

On a

$$P : \quad ax + by + cz + d = 0 \quad \text{avec } a, b, c, d \neq 0.$$

$$\forall i, \quad ax_i + by_i + cz_i + d = 0 \iff \begin{pmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Chapitre 29

TD 29

Exercice 1

— $\forall P, Q \in \mathbb{R}_n[X],\ \varphi(P,Q) \in \mathbb{R}$;

—

$$\begin{aligned}\forall P, Q, R \in \mathbb{R}_n[X], \forall \alpha, \beta \in \mathbb{R},\ \varphi(\alpha P + \beta Q, R) &= \sum_{k=0}^{n} \big(\alpha P(k) + \beta Q(k)\big)\, R(k) \\ &= \alpha \sum_{k=0}^{n} P(k)\, R(k) + \beta \sum_{k=0}^{n} Q(k)\, R(k) \\ &= \alpha\varphi(P,R) + \beta\varphi(Q,R);\end{aligned}$$

—

$$\begin{aligned}\forall P, Q \in \mathbb{R}_n[X],\ \varphi(Q,P) &= \sum_{k=0}^{n} Q(k)P(k) \\ &= \sum_{k=0}^{n} P(k)Q(k) \\ &= \varphi(P,Q);\end{aligned}$$

— $\forall P \in \mathbb{R}_n[X],\ \varphi(P,P) = \displaystyle\sum_{k=0}^{n} P(k)^2 \geqslant 0$;

—

$$\begin{aligned}\forall P \in \mathbb{R}_n[X],\ \varphi(P,P) = 0 &\iff \sum_{k=0}^{n} P(k)^2 = 0 \\ &\iff \forall k \in [\![0,n]\!]\,,\ P(k) = 0 \\ &\iff P = 0 \text{ car } \deg P \leqslant n.\end{aligned}$$

Exercice 2

— $\forall f, g \in E,\ \varphi(f,g) \in \mathbb{R}$;

—

$$\begin{aligned}\forall f,g,h \in E \forall \alpha,\beta \in \mathbb{R},\ \varphi(\alpha f + \beta g, h) &= \big(\alpha f(0) + \beta g(0)\big)h(0) \\ &\quad + \int_0^1 \big(\alpha f'(t) + \beta g'(t)\big)\, h'(t)\ \mathrm{d}t \\ &= \cdots\cdots\cdots \\ &= \alpha\varphi(f,h) + \beta\varphi(g,h);\end{aligned}$$

— $\forall f, g \in E,\ \varphi(g,f) = \varphi(f,g)$;

— $\forall f \in E,\ \varphi(f,f) = \underbrace{f(0)^2}_{\geqslant 0} + \underbrace{\int_0^1 f'(t)\ \mathrm{d}t}_{\geqslant 0}$;

— Soit $f \in E$.

$$\begin{aligned}\varphi(f,f) = 0 &\iff \begin{cases} f(0)^2 = 0 \\ \displaystyle\int_0^1 f'(t)^2\ \mathrm{d}t = 0 \end{cases} \\ &\iff \begin{cases} f(0) = 0 \\ \forall t,\ f'(t) = 0 \text{ car } (f')^2 \text{ est continue positive} \end{cases} \\ &\iff \begin{cases} f \text{ constante} \\ f(0) = 0 \end{cases} \\ &\iff f = 0\end{aligned}$$

Exercice 3

On pose

$$\begin{aligned}\varphi : \mathbb{R}^2 \times \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ \big((x,y),(x',y')\big) &\longmapsto x'(ax+cy) + y'(bx+dy) \\ &\quad \begin{pmatrix} x' & y' \end{pmatrix} \begin{pmatrix} ax+cy \\ bx+dy \end{pmatrix} \\ &\quad \begin{pmatrix} x' & y' \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}\end{aligned}$$

— φ est bilinéaire (multiplication matricielle).

—

$$\varphi \text{ symétrique} \iff \forall (x,y),(x',y') \in \mathbb{R}^2, \begin{pmatrix} x' & y' \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

$$\iff \forall (x,y),(x',y') \in \mathbb{R}^2, cx'y + by'x = cxy' + byx'$$

$$\iff b = c \text{ avec } \begin{cases} x = 1 \\ y = 0 \\ x' = 0 \\ y' = 1 \end{cases}$$

— On suppose $b = c$.

$$\varphi \text{ positive} \iff \forall (x,y) \in \mathbb{R}^2,\ ax^2 + 2bxy + dy^2 \geqslant 0$$

$$\iff \begin{cases} \forall y \in \mathbb{R},\ 4b^2y^2 - 4ady^2 \leqslant 0 \\ a \geqslant 0 \end{cases}$$

$$\iff \begin{cases} b^2 - 4ad \leqslant 0 \\ a \geqslant 0 \end{cases}$$

—

$$\varphi \text{ définie positive} \iff \forall (x,y) \in \mathbb{R}^2,\ \left(ax^2 + 2bxy + dy^2 = 0 \implies x = y = 0\right)$$

$$\iff \begin{cases} \forall y \neq 0,\ 4y^2(b^2 - ad) < 0 \\ a \neq 0 \end{cases}$$

$$\iff \begin{cases} b^2 - ad < 0 \\ a \neq 0 \end{cases}$$

On en déduit que φ est un produit scalaire si et seulement si

$$\begin{cases} b = c, \\ b^2 - ad < 0, \\ a > 0. \end{cases}$$

Exercice 4

On a $\|u\|^2 = 2$ d'où $e_1 = \dfrac{1}{\sqrt{2}}(1,0,1)$.

$$\begin{aligned} v - \langle v \mid e_1 \rangle e_1 &= (1,1,1) - \frac{1}{\sqrt{2}} \times 2 \times \frac{1}{\sqrt{2}}(1,0,1) \\ &= (0,1,0) \end{aligned}$$

D'où $e_2 = \dfrac{(0,1,0)}{\|(0,1,0)\|} = (0,1,0)$.

$$\begin{aligned} w - \langle w \mid e_1\rangle e_1 - \langle w \mid e_2\rangle e_2 &= (-1,1,0) + \frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} \times (1,0,1) - (0,1,0) \\ &= \left(-\frac{1}{2}, 0, \frac{1}{2}\right) \end{aligned}$$

On a $\left\|\left(-\frac{1}{2}, 0, \frac{1}{2}\right)\right\|^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ d'où

$$e_3 = \frac{\left(-\frac{1}{2}, 0, \frac{1}{2}\right)}{\left\|\left(-\frac{1}{2}, 0, \frac{1}{2}\right)\right\|} = \left(-\frac{\sqrt{2}}{2}, 0, \frac{\sqrt{2}}{2}\right).$$

Exercice 5

Conjecture : $(F \cap G)^\perp = F^\perp + G^\perp$.

— Soit $x \in F^\perp + G^\perp$. Montrons que $x \in (F \cap G)^\perp$. Soit $y \in F \cap G$. On décompose x en $u + v$ avec $u \in F^\perp$ et $g \in G^\perp$.

$$\begin{aligned} \langle x \mid y\rangle &= \langle u + v \mid y\rangle \\ &= \langle u \mid y\rangle + \langle v \mid y\rangle \\ &= 0 \end{aligned}$$

donc $x \perp y$ et donc $x \in (F \cap G)^\perp$.

On a prouvé

$$F^\perp + G^\perp \subset (F \cap G)^\perp.$$

— E est euclidien donc

$$\dim\left((F \cap G)^\perp\right) = \dim E - \dim(F \cap G).$$

$$\dim(F^\perp + G^\perp) = \dim(F^\perp) + \dim(G^\perp) - \dim(F^\perp \cap G^\perp)$$

Conjecture 2 : $F^\perp \cap G^\perp = (F + G)^\perp$.

— Soit $x \in F^\perp \cap G^\perp$. Soit y un élément de $F + G$ que l'on décompose en $u + v$ avec $u \in F$ et $v \in G$.

$$\begin{aligned} \langle x \mid y\rangle &= \langle x \mid u + v\rangle \\ &= \langle x \mid u\rangle + \langle x \mid v\rangle \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

— Soit $x \in (F+G)^\perp$.
  — $\forall y \in F$, $\langle x \mid y \rangle = 0$;
  — $\forall y \in G$, $\langle x \mid y \rangle = 0$.
  Donc, $x \in F^\perp \cap G^\perp$.

Retour au calcul précédent :

$$\begin{aligned}\dim(F^\perp + G^\perp) &= \dim(F^\perp) + \dim(G^\perp) - \dim(F^\perp \cap G^\perp)\\ &= \dim E - \dim F + \dim E - \dim G - \big(\dim E - \dim(F+G)\big)\\ &= \dim E - \big(\dim F + \dim G - \dim(F+G)\big)\\ &= \dim E - \dim(F+G)\end{aligned}$$

Exercice 6

1. $F^\perp = \mathrm{Vect}\big(\overbrace{(1,1,1,1)}^{v_1}, \overbrace{(1,-1,1,-1)}^{v_2}\big)$.

   En effet, soit $u = (x,y,z,t) \in \mathbb{R}^4$.

$$\begin{aligned}u \in F &\iff \begin{cases} x+y+z+t = 0 \\ x-y+z-t = 0 \end{cases}\\ &\iff \begin{cases} \langle u \mid v_1 \rangle = 0 \\ \langle u \mid v_2 \rangle = 0 \end{cases}\end{aligned}$$

   D'où $F = \mathrm{Vect}(v_1, v_2)^\perp$.

2. Méthode 1 Soit $u = (x,y,z,t) \in \mathbb{R}^4$. On sait que l'on peut décomposer u en $v + w$ avec $v \in F$ et $w \in F^\perp$. On pose $u = (a,b,c,d)$ avec
$\begin{cases} a+b+c+d = 0 \\ a-b+c-d = 0. \end{cases}$

   et $w = \alpha v_1 + \beta v_2$ avec $\alpha, \beta \in \mathbb{R}$.

   On calcule les valeurs de a,b,c,d,α,β et, on trouve v en fonction de (x,y,z,t) :

$$(a,b,c,d) = \underbrace{\begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}}_{\mathrm{Mat}_{\mathscr{B}}(p)} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}.$$

   Méthode 2 On orthonormalise une base de F :
   — on cherche (u_1, u_2) une base de F ;
   — on orthonormalise (u_1, u_2) en (v_1, v_2) ;
   — $\forall u$, $p_F(u) = \langle u \mid v_1 \rangle v_1 + \langle u \mid v_2 \rangle v_2$.

Méthode 3

$$\left.\begin{matrix} x+y+z+t=0 \\ x-y+z-t=0 \end{matrix}\right\} \iff \begin{cases} x=-z \\ y=-t. \end{cases}.$$

D'où $F = \text{Vect}\big(\underbrace{(-1,0,1,0)}_{u_1}, \underbrace{(0,-1,0,1)}_{u_2}\big)$.

Donc $\mathscr{C} = (u_1, u_2, v_1, v_2)$ est une base de $\mathbb{R}^4$. On en déduit que

$$\text{Mat}_{\mathscr{C}}(p_F) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

On applique les formules de changement de bases...

3. $d(u,F) = \|u - p_F(u)\|$.

Exercice 7

On montre que p est une projection : on montre $p \circ p = p$ et on calcule donc M^2 :

$$\begin{aligned} M^2 &= \frac{1}{36}\begin{pmatrix} 5 & -2 & 1 \\ -2 & 2 & 2 \\ 1 & 2 & 5 \end{pmatrix} \\ &= \frac{1}{36}\begin{pmatrix} 30 & -12 & 6 \\ -12 & 12 & 12 \\ 6 & 12 & 30 \end{pmatrix} \\ &= M \end{aligned}$$

Donc $p \circ p = p$ et donc p est la projection sur $\text{Im}(p)$ parallèlement à $\text{Ker}(p)$.

$$\text{rg}(p) = \text{tr}(p) = \frac{1}{6}(5+2+5) = 2.$$

$$\begin{aligned} \text{Donc, } \text{Im}(p) &= \text{Vect}\big(p(e_1), p(e_2)\big) \\ &= \text{Vect}\big((5,-2,1),(-1,1,1)\big). \end{aligned}$$

On remarque que $p(e_1 + 2e_2 - e_3) = 0$. D'où $\text{Ker}(p) = \text{Vect}(e_1 + 2e_2 - e_3)$.

$$\begin{aligned} \langle e_1 + 2e_2 - e_3 \mid 5e_1 - 2e_2 + e_3 \rangle &= 5 - 4 - 1 = 0 \\ \langle e_1 + 2e_2 - e_3 \mid -e_1 + e_2 + e_3 \rangle &= -1 + 2 - 1 = 0 \end{aligned}$$

donc $\underbrace{\text{Ker}\, p}_{\dim(\cdot)=1} \subset \underbrace{(\text{Im}\, p)^\perp}_{\dim(\cdot)=3-2=1}$ donc $\text{Ker}\, p = (\text{Im}\, p)^\perp$.

$$\begin{aligned}(x,y,z) \in \operatorname{Im} p &\iff (x,y,z) \in (\operatorname{Ker} p)^\perp \\ &\iff (x,y,z) \perp (1,2,-1) \\ &\iff x+2y-z=0\end{aligned}$$

Exercice 8

1. On sait déjà que $E = \mathscr{M}_n(\mathbb{R})$ est un $\mathbb{R}$-espace vectoriel.

   Soient $A, B \in E^2$.

   $$\operatorname{tr}({}^tB\,A) = \operatorname{tr}\left({}^t\left({}^tB\,A\right)\right) = \operatorname{tr}\left({}^tA\,{}^{tt}B\right) = \operatorname{tr}({}^tA\,B).$$

   La transposée est linéaire, la multiplication matricielle est linéaire et la trace est linéaire ; l'application $(A,B) \mapsto \operatorname{tr}({}^tA\,B)$ est linéaire.

   $\operatorname{tr}({}^tA\,A) \geqslant 0$ (c'est une somme de carrés) et $\operatorname{tr}({}^tAA) = 0 \iff A = 0$.
2. Soit $M = (m_{i,j}) \in S_n$.

   $$\begin{aligned}d(A,M)^2 &= \|M-A\|^2 \\ &= \operatorname{tr}\left({}^t(M-A)(M-A)\right) \\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n}(m_{ji}-a_{ji})^2\right) \\ &= \sum_{j=1}^{n}\left(\sum_{i=1}^{n}(m_{ij}-a_{ij})^2\right) \\ &= \sum_{1\leqslant i,j\leqslant n}(m_{ij}-a_{ij})^2\end{aligned}$$

   D'après le cours, on sait que $d(a,S_n)^2 = \|A - p_{S_n}(A)\|^2$.

   On pose

   $$A_n = \{M \in \mathscr{M}_n(\mathbb{R}) \mid {}^tM = -M\}.$$

   On montre $A_n \subset S_n^\perp$. Soient $M \in A_n$ et $S \in S_n$.

   $$\begin{aligned}\langle M \mid S\rangle &= \operatorname{tr}({}^tM\,S) = \operatorname{tr}(-M\,S) = -\operatorname{tr}(MS) \\ \langle S \mid M\rangle &= \operatorname{tr}({}^tS\,M) = \operatorname{tr}(SM) = \operatorname{tr}(MS)\end{aligned}$$

   D'où $\langle M \mid S\rangle = 0$.

   On sait que $S_n \oplus A_n = \mathscr{M}_n(\mathbb{R})$ donc $\dim A_n = \dim \mathscr{M}_n(\mathbb{R}) - \dim S_n$. Comme $\dim S_n < +\infty$,

   $$S_n \oplus S_n^\perp = \mathscr{M}_n(\mathbb{R})$$

donc

$$\begin{aligned}\dim S_n^\perp &= \dim \mathcal{M}_n(\mathbb{R}) - \dim S_n \\ &= \dim A_n.\end{aligned}$$

Donc $A_n = S_n^\perp$ et donc

$$A - p_{S_n}(A) = \frac{1}{2}\left(A - {}^tA\right)$$

En effet,

$$A = \underbrace{\frac{1}{2}\left(A + {}^tA\right)}_{\in S_n} + \underbrace{\frac{1}{2}\left(A - {}^tA\right)}_{\in A_n}.$$

On en déduit que

$$\inf_{M\in S_n} \sum_{1\leqslant i,j\leqslant n} (m_{ij} - a_{ij})^2 = \frac{1}{4} \sum_{i\leqslant i,j\leqslant n} (a_{ij} - a_{ji})^2.$$

On peut également prouver ce résultat avec les dérivées partielles : soit f telle que

$$f(m_{11}, \dots, m_{nn}) = \sum_{1\leqslant i,j\leqslant n} (m_{ij} - a_{ij})^2.$$

Soit $i \leqslant j$.

$$\frac{\partial f}{\partial m_{ij}} = 2(m_{ij} - a_{ij}) + 2(m_{ji} - a_{ji}) = 0 \iff m_{ij} = \frac{a_{ij} + a_{ji}}{2}.$$

D'où $M = \dfrac{A + {}^tA}{2}$. On a prouvé que c'est une valeur critique mais pas que c'est un minimum.

Exercice 9

" $\Longrightarrow$ " C'est du cours.

" $\Longleftarrow$ " par contraposée : soit G un supplémentaire de F tel que $F \neq F^\perp$, et p la projection sur F parallèlement à G.

Soit $u \in F \setminus \{0\}$, $v \in G \setminus \{0\}$ et

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ \lambda &\longmapsto \|u + \lambda v\|^2 - \|u\|^2 \\ &= 2\lambda \langle u \mid v\rangle + \lambda^2 \|v\|^2 \qquad = \lambda(2\langle u \mid v\rangle + \lambda\|v\|^2)\end{aligned}$$

λ	$-\infty$		0		λ_0		$+\infty$
f		$+$	0	$-$	0	$+$	

ou

λ	$-\infty$		λ_0		0		$+\infty$
f		$+$	0	$-$	0	$+$	

$$\forall \mu \in [0, \lambda_0],\ f(\mu) = \| \underbrace{u + \mu v}_{x} \| - \| \underbrace{u}_{p(x)} \| < 0$$

donc $\|x\| < \|p(x)\|$

Exercice 10

1. Soit $M = (m_{i,j}) = \mathrm{Mat}_{\mathscr{B}}(f)$.

   $\forall i, j$, $m_{i,j}$ est la i-ème coordonnée de $f(e_j)$:

$$\begin{aligned} m_{i,j} &= \langle f(e_j) \mid e_i \rangle \\ &= \langle e_j \mid f(e_i) \rangle \\ &= \langle f(e_i) \mid e_j \rangle \\ &= m_{j,i} \end{aligned}$$

2. Soient $u \in \mathrm{Ker}(f)$ et $v \in \mathrm{Im}(f)$. Soit $w \in E$ tel que $v = f(w)$.

$$\begin{aligned} \langle u \mid v \rangle &= \langle u \mid f(w) \rangle \\ &= \langle f(u) \mid w \rangle \\ &= \langle 0 \mid w \rangle \\ &= 0 \end{aligned}$$

   D'où $\mathrm{Ker}(f) \subset \mathrm{Im}(f)^{\perp}$.

$$\begin{aligned} \dim(\mathrm{Ker}\, f) &= \dim E - \dim(\mathrm{Im}\ f) \\ &= \dim\left((\mathrm{Im}\ f)^{\perp}\right) \end{aligned}$$

   On en déduit que $\mathrm{Ker}\, f = (\mathrm{Im}\ f)^{\perp}$.

Exercice 11

Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base orthonormée de E.

$$\begin{aligned}\forall i \neq j,\ \|f(e_i)\|^2 - \|f(e_j)\|^2 &= \langle f(e_i) + f(e_j) \mid f(e_i) - f(e_j)\rangle \\ &= \langle f(e_i + e_j) \mid f(e_i - e_j)\rangle\end{aligned}$$

Or, $\|e_i\|^2 = \|e_j\|^2 = 1$ et donc $\langle e_i + e_j \mid e_i - e_j\rangle = 0$ et donc $\langle f(e_i + e_j) \mid f(e_i - e_j)\rangle = 0$. D'où

$$\forall i \in [\![1, n]\!]\,,\ \|f(e_i)\| = \|f(e_1)\| =: \lambda.$$

Soit $x \in E$. On pose

$$x = \sum_{i=1}^{n} \langle x \mid e_i\rangle\, f(e_i)$$

d'où

$$f(x) = \sum_{i=1}^{n} \langle x \mid e_i\rangle\, f(e_i).$$

D'après le théorème de Pythagore,

$$\|f(x)\|^2 = \sum_{i=1}^{n} \langle x \mid e_i\rangle^2 \|f(e_i)\|^2 = \lambda^2 \sum_{i=1}^{n} \langle x \mid e_i\rangle^2\,.$$

Comme $(e_1, \dots, e_n)$ est orthonormée, on a

$$\|x\|^2 = \sum_{i=1}^{n} \langle x \mid e_i\rangle^2 \text{ donc } \|f(x)\| = \lambda\|x\|.$$

Exercice 12

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E.

$$\forall i, j,\ \langle f(e_i) \mid f(e_j)\rangle = \langle e_i \mid e_j\rangle = \delta_{i,j}$$

donc $\big(f(e_1), \dots, f(e_n)\big)$ est orthonormée, elle est donc libre ; c'est donc une base orthonormée.

D'où

$$\begin{aligned}\forall x \in E,\ f(x) &= \sum_{i=1}^{n} \langle f(x) \mid f(e_i)\rangle\, f(e_i) \\ &= \sum_{i=1}^{n} \langle x \mid e_i\rangle\, f(e_i).\end{aligned}$$

Donc,

$$\begin{aligned}\forall (x,y)\in E^2, \forall(\lambda,\mu)\in\mathbb{R}^2,\ f(\lambda x+\mu y) &= \sum_{i=1}^{n}\langle \lambda x+\mu y \mid e_i\rangle\, f(e_i)\\ &= \sum_{i=1}^{n}\big(\lambda\langle x\mid e_i\rangle+\mu\langle x\mid e_i\rangle\big) f(e_i)\\ &= \lambda\sum_{i=1}^{n}\langle x\mid e_i\rangle\, f(e_i)+\mu\sum_{i=1}^{n}\langle y\mid e_i\rangle\, f(e_i)\\ &= \lambda f(x)+\mu f(y).\end{aligned}$$

Exercice 13

Comme l'exercice 9.

Exercice 14

$G\subset F^\perp$ Soit $f\in F$ et $g\in G$.

$$\begin{aligned}\langle g\mid f\rangle &= \int_{-1}^{1} g(t)f(t)\ \mathrm{d}t\\ &= \int_{-1}^{0} g(t)f(t)\ \mathrm{d}t+\int_{0}^{1} g(t)f(t)\ \mathrm{d}x\\ &= 0\end{aligned}$$

$F^\perp\subset G$ Soit $h\in F^\perp$. Montrons que $h\in G$.

$$\forall f\in F\ \int_{-1}^{1} h(t)f(t)\ \mathrm{d}t=0.$$

Montrons que

$$\forall t\in[0,1],\ h(t)=0.$$

$$\exists\eta>0\,\forall t\in\,]t_0-\eta,t_0+\eta[, h(t)>0$$

Or,

$$\int_{-1}^{1} f(t)h(t)\ \mathrm{d}t=0.$$

Mais,

$$\int_{t_0-\eta}^{t_0+\eta} f(t)\underbrace{h(t)}_{>0}\ \mathrm{d}t=0.$$

↯

Exercice 15

1. Soit $t \in [0,1]$. On a $f(t) = \displaystyle\int_0^t f'(u)\ \mathrm{d}u$. D'où,

$$f^2(t) = \left(\int_0^t f'(u)\ \mathrm{d}u\right)^2 = \langle f' \mid 1\rangle^2 .$$

On applique l'inégalité de Cauchy-Schwarz :

$$f^2(t) \leqslant \int_0^t f'(u)^2\ \mathrm{d}u \int_0^t 1^2\ \mathrm{d}u \leqslant t\int_0^1 f'(u)^2\ \mathrm{d}u.$$

Donc,

$$\int_0^1 f^2(t)\ \mathrm{d}t \leqslant \int_0^1 \left(t\int_0^1 f'(u)^2\ \mathrm{d}u\right)\ \mathrm{d}t = \int_0^1 f'(u)^2\ \mathrm{d}u \int_0^1 t\ \mathrm{d}t = \frac{1}{2}\int_0^1 f'(t)^2\ \mathrm{d}t.$$

2. On suppose $f(0) = 0$ et $f(1) = 0$.

$$\begin{aligned}\forall t \in \left[\frac{1}{2}, 1\right],\ f^2(t) &= \int_t^1 f'(u)\ \mathrm{d}u \\ &\leqslant \int_t^1 f'(u)^2\ \mathrm{d}u \int_t^1 1^2\ \mathrm{d}u \\ &\leqslant \int_0^1 f'(u)^2\ \mathrm{d}u(1-t).\end{aligned}$$

$$\begin{aligned}\int_{\frac{1}{2}}^1 f^2(t)\ \mathrm{d}t &\leqslant \int_{\frac{1}{2}}^1 (1-t)\ \mathrm{d}t \int_0^1 f'(u)^2\ \mathrm{d}u \\ &\leqslant \frac{1}{8}\int_0^1 f'(u)^2\ \mathrm{d}u\end{aligned}$$

$$\begin{aligned}\int_0^{\frac{1}{2}} f^2(t)\ \mathrm{d}t &\leqslant \int_0^1 f'(u)\ \mathrm{d}u \int_0^{\frac{1}{2}} t\ \mathrm{d}t \\ &\leqslant \frac{1}{8}\int_0^1 f'(u)^2\ \mathrm{d}u\end{aligned}$$

On en déduit que

$$\int_0^1 f^2(t)\ \mathrm{d}t \leqslant \frac{1}{4}\int_0^1 f'(t)^2\ \mathrm{d}t.$$

Chapitre 30

TD 30

Exercice 1

Notons $\varphi : x \mapsto \displaystyle\int_x^{x+T} f(t)\ \mathrm{d}t$.

On pose F une primitive de f (f est continue). D'où

$$\forall x,\ \varphi(X) = F(x+T) - F(x).$$

On dérive cette expression :

$$0 = \varphi'(x) = f(x+T) - f(x).$$

Ainsi, f est T-périodique.

Exercice 2

Soit $f : [a,b] \to \mathbb{R}$ continue. Déterminer une condition nécessaire et suffisante poour que

$$\left|\int_a^b f(t)\ \mathrm{d}t\right| = \int_a^b \left|f(t)\right|\ \mathrm{d}t.$$

Condition suffisante : f est de signe constant sur $[a,b]$.

On démontre que c'est une condition nécessaire. On suppose donc

$$\left|\int_a^b f(t)\ \mathrm{d}t\right| = \int_a^b \left|f(t)\right|\ \mathrm{d}t.$$

— Cas 1 On suppose $\displaystyle\int_a^b f(t)\ \mathrm{d}t \geqslant 0$. On sait que

$$\int_a^b f(t)\ \mathrm{d}t = \int_a^b \left|f(t)\right|\ \mathrm{d}t$$

donc

$$\int_a^b \underbrace{\big(|f(t)| - f(t)\big)}_{\substack{\geqslant 0 \\ \text{de classe } \mathscr{C}^0}} \,\mathrm{d}t = 0.$$

On en déduit que

$$\forall t \in [a,b],\ f(t) = |f(t)| \geqslant 0.$$

— Cas 2 On suppose $\displaystyle\int_a^b f(t)\,\mathrm{d}t \leqslant 0$. On sait que

$$-\int_a^b f(t)\,\mathrm{d}t = \int_a^b \big|f(t)\big|\,\mathrm{d}t$$

donc

$$\int_a^b \underbrace{\big(|f(t)| + f(t)\big)}_{\substack{\geqslant 0 \\ \text{de classe } \mathscr{C}^0}} \,\mathrm{d}t = 0.$$

On en déduit que

$$\forall t \in [a,b],\ f(t) = -|f(t)| \leqslant 0.$$

Exercice 3

Soit $f : [0,1] \to \mathbb{R}$ continue. On suppose $\displaystyle\int_0^1 f(t)\,\mathrm{d}t = 0$. On note $m = \min_{[0,1]} f$ et $M = \max_{[0,1]} f$. Montrer que

$$\int_0^1 f^2(t)\,\mathrm{d}t \leqslant -mM.$$

$$\forall t \in [0,1],\ \big(M - f(t)\big)\big(f(t) - m\big) \geqslant 0$$

donc

$$\int_0^1 \big(M - f(t)\big)\big(f(t) - m\big)\,\mathrm{d}t \geqslant 0$$

et donc

$$-mM - \int_0^1 f^2(t)\,\mathrm{d}t \geqslant 0.$$

On en déduit que

$$\int_0^1 f^2(t)\,\mathrm{d}t \leqslant -mM.$$

Exercice 4

Soit $f : t \mapsto \begin{cases} \sin\left(\frac{1}{t}\right) & \text{si } t \neq 0 \\ 0 & \text{sinon.} \end{cases}$

On suppose f continue par morceaux. Soit $I = [-1, 1]$ et $\sigma = (a_0, \ldots, a_n)$ une subdivision de I telle que

$$\begin{cases} \forall i \in [\![1, n-1]\!]\,,\ f_{|]a_i, a_{i+1}[} \text{ continue;} \\ \forall i \in [\![1, n-1]\!]\,,\ f \text{ a une limite réelle à gauche et à droite.} \end{cases}$$

Comme f n'est pas continue en 0,

$$\exists i,\ 0 = a_i.$$

Or, f n'a pas de limite en 0 à droite : une contradiction.

En effet, les suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ ne convergent pas vers la même limite avec

$$\forall n \in \mathbb{N}^\star,\ \begin{cases} x_n = \dfrac{1}{n\pi} \xrightarrow[n\to+\infty]{} 0^+ \\ y_n = \dfrac{1}{2n\pi + \frac{\pi}{2}} \xrightarrow[n\to+\infty]{} 0^+ \end{cases}$$

car

$$\forall n \in \mathbb{N}^\star,\ \begin{cases} f(x_n) = \sin(n\pi) = 0 \xrightarrow[n\to+\infty]{} 0 \\ f(y_n) = \sin\left(\dfrac{\pi}{2} + 2n\pi\right) = 1 \xrightarrow[n\to+\infty]{} 1 \neq 0. \end{cases}$$

Donc f n'a pas de limite en 0^+.

Exercice 5

1.

$$\begin{aligned} \sum_{k=1}^{n} \frac{n}{n^2 + k^2} &= \sum_{k=1}^{n} \frac{\frac{1}{n}}{1 + \left(\frac{k}{n}\right)^2} \\ &= \frac{1}{n} \sum_{k=1}^{n} \frac{1}{1 + \left(\frac{k}{n}\right)^2} \\ &\xrightarrow[n\to+\infty]{} \int_0^1 \frac{1}{1+t^2}\,\mathrm{d}t = \frac{\pi}{4}. \end{aligned}$$

2.

$$\begin{aligned}\sum_{k=1}^{n}\frac{k}{k^2+n^2} &= \sum_{k=1}^{n}\frac{\frac{1}{n}\times\frac{k}{n}}{\left(\frac{k}{n}\right)^2+1}\\ &= \frac{1}{n}\sum_{k=1}^{n}\frac{\frac{k}{n}}{1+\left(\frac{k}{n}\right)^2}\\ &\xrightarrow[n\to+\infty]{} \int_0^1 \frac{x}{1+x^2}\,\mathrm{d}x = \frac{1}{2}\ln 2.\end{aligned}$$

3.

$$\begin{aligned}\sum_{k=1}^{n}\frac{1}{\sqrt{n^2+2kn}} &= \frac{1}{n}\sum_{k=1}^{n}\frac{1}{\sqrt{1+2\frac{k}{n}}}\\ &\xrightarrow[n\to+\infty]{} \int_0^1 \frac{1}{\sqrt{1+2t}}\,\mathrm{d}t = \sqrt{3}-1.\end{aligned}$$

Exercice 6

$$\lim_{n\to+\infty}\underbrace{\left(\frac{(2n)!}{n^n\,n!}\right)^{\frac{1}{n}}}_{u_n} = ?$$

$$\begin{aligned}\forall n\in\mathbb{N}^\star,\ \ln(u_n) &= \frac{1}{n}\ln\left(\frac{(2n)!}{n^n\,n!}\right)\\ &= \frac{1}{n}\ln\left(\prod_{k=1}^{n}\frac{n+k}{n}\right)\\ &= \frac{1}{n}\sum_{k=1}^{n}\ln\left(1+\frac{k}{n}\right)\end{aligned}$$

Si $f\in\mathscr{C}^0_{\mathrm{pm}}$ sur $[0,1]$ (continue par morceaux), alors

$$\frac{1}{n}\sum_{k=1}^{n} f\left(\frac{k}{n}\right) \xrightarrow[n\to+\infty]{} \int_0^1 f(t)\,\mathrm{d}t.$$

La fonction $t \mapsto \ln(1+t)$ est $\mathscr{C}^0$ sur $[0,1]$ donc,

$$\begin{aligned}\ln(u_n) \xrightarrow[n\to+\infty]{} \int_0^1 \ln(1+t)\,\mathrm{d}t &= [(1+t)\ln(1+t)-(1+t)]_0^1 \\ &= 2\ln 2 - 2 + 1 \\ &= 2\ln 2 - 1\end{aligned}$$

Exercice 7

—

$$\sum_{k=1}^{n} \sin\left(\frac{k}{n}\right)\sin\left(\frac{k}{n^2}\right).$$

Pour calculer cette somme, on utilise l'encadrement

$$\forall x \in \left[0, \frac{\pi}{2}\right],\ x - \frac{x^3}{6} \leqslant \sin x \leqslant x.$$

D'où,

$$\forall n \in \mathbb{N}\,\forall k \in [\![1,n]\!],\ \frac{k}{n^2} - \frac{k^3}{6n^6} \leqslant \sin\left(\frac{k}{n^2}\right) \leqslant \frac{k}{n^2}$$

et donc

$$\sum_{k=1}^{n}\left(\frac{k}{n^2} - \frac{k^3}{6n^6}\right)\sin\left(\frac{k}{n}\right) \leqslant \sum_{k=1}^{n}\sin\left(\frac{k}{n}\right)\sin\left(\frac{k}{n^2}\right) \leqslant \sum_{k=1}^{n}\frac{k}{n^2}\sin\left(\frac{k}{n}\right).$$

Or,

$$\begin{aligned}\sum_{k=1}^{n}\frac{k}{n^2}\sin\left(\frac{k}{n}\right) &= \frac{1}{n}\sum_{k=1}^{n}\frac{k}{n}\sin\left(\frac{k}{n}\right) \\ &\xrightarrow[n\to+\infty]{} \int_0^1 x\sin x\,\mathrm{d}x = [-x\cos x]_0^1 + \int_0^1 \cos x\,\mathrm{d}x \\ &= -\cos 1 + \sin 1.\end{aligned}$$

Et,

$$\sum_{k=1}^{n}\frac{k^3}{6n^6}\sin\left(\frac{k}{n}\right) = \underbrace{\frac{1}{6n^2}}_{\to 0} \times \underbrace{\frac{1}{n}\sum_{k=1}^{n}\left(\frac{k}{n}\right)^3\sin\left(\frac{k}{n}\right)}_{\text{limite finie}}$$

Par encadrement,

$$\sum_{k=1}^{n}\sin\left(\frac{k}{n}\right)\sin\left(\frac{k}{n^2}\right) \xrightarrow[n\to+\infty]{} \sin 1 - \cos 1.$$

— À essayer

Exercice 8

On pose

$$f_n : x \mapsto \sum_{k=1}^{n} \frac{\sin(kx)}{k}.$$

Soit $x \not\equiv 0 \ [2\pi]$.

$$\begin{aligned}
\forall x,\ f_n'(x) = \sum_{k=1}^{n} \cos(kx) &= \mathfrak{Re}\left(\sum_{k=1}^{n} e^{ikx}\right) \\
&= \mathfrak{Re}\left(e^{ix}\,\frac{1-\left(e^{ix}\right)^n}{1-e^{ix}}\right) \\
&= \mathfrak{Re}\left(e^{ix}\frac{e^{inx/2}}{e^{ix/2}}\frac{\cancel{2i}\sin(nx/2)}{\cancel{2i}\sin(x/2)}\right) \\
&= \frac{\sin(nx/2)}{\sin(x/2)}\cos\left((n+1)\,\frac{x}{2}\right).
\end{aligned}$$

À faire : Tableau de variations / de signes

Donc $x_n = \dfrac{\pi}{n+1}$.

$$\begin{aligned}
\forall n,\ f_n(x_n) &= \sum_{k=1}^{n} \frac{\sin\left(\frac{k\pi}{n+1}\right)}{k} \\
&= \frac{\pi}{n+1}\sum_{k=1}^{n} \frac{\sin\left(\frac{k\pi}{n+1}\right)}{\frac{k\pi}{n+1}} \\
&= \frac{\pi}{n+1}\sum_{k=1}^{n+1} g\left(\frac{k}{n+1}\right) - \cancel{\frac{\pi}{n+1}}\cancel{\sin(\pi)} \\
&\xrightarrow[n\to+\infty]{} \pi\int_0^1 g(x)\ \mathrm{d}x
\end{aligned}$$

où

$$g : x \mapsto \begin{cases} \dfrac{\sin(\pi x)}{\pi x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0. \end{cases}$$

Exercice 9

Montrer que

$$\forall x \in \left[0, \frac{\pi}{2}\right],\ x - \frac{x^3}{6} \leqslant \sin x \leqslant x - \frac{x^3}{6} + \frac{x^5}{120}.$$

On sait que sin est de classe $\mathscr{C}^\infty$ d'où sin est de classe $\mathscr{C}^5$.

On a

$$\begin{aligned}\sin x &= x - \frac{x^3}{6} + \int_0^x \frac{(x-t)^4}{4!} \sin^{(5)}(t)\ \mathrm{d}t \\ &= x - \frac{x^3}{6} + \int_0^x \frac{(x-t)^4}{4!} \underbrace{\cos(t)}_{\in[0,1]}\ \mathrm{d}t\end{aligned}$$

On en déduit que $\sin x \geqslant x - \dfrac{x^3}{6}$.

$$\begin{aligned}\sin x &\leqslant x - \frac{x^3}{6} + \int_0^x \frac{(x-t)^4}{24}\ \mathrm{d}t \\ &\leqslant x - \frac{x^3}{6} + \left[-\frac{(x-t)^5}{120}\right]_0^x \\ &\leqslant x - \frac{x^3}{6} + \frac{x^5}{120}.\end{aligned}$$

Exercice 10

Soit $x \in \mathbb{R}$. f est de classe $\mathscr{C}^2$ sur $[x, x+1]$.

$$f(x+1) = f(x) + f'(x) + \int_x^{x+1} f''(t)\ (x+1-t)\ \mathrm{d}t.$$

$$(\star) : \qquad \left|\int_x^{x+1} f''(t)\ (x+1-t)\ \mathrm{d}t\right| \leqslant \int_x^{x+1} \left|f''(t)\right|\ |x+1-t|\ \mathrm{d}t.$$

On note $M(X) = \max\limits_{t\in[x,x+1]} \left|f''(t)\right|$ et donc

$$(\star) \leqslant M(x) \int_x^{x+1} (x+1-t)\ \mathrm{d}t = \frac{M(x)}{2}.$$

$$\exists c_x \in [x, x+1],\ M(x) = \left|f''(c_x)\right|.$$

Or, $c_x \geqslant x$ donc $c_x \xrightarrow[x\to+\infty]{} +\infty$ et donc $f''(c_x) \xrightarrow[x\to+\infty]{} 0$.

Par encadrement, $\displaystyle\int_x^{x+1} f''(t)\ (x+1-t)\ \mathrm{d}t \xrightarrow[x\to+\infty]{} 0$.

Or, $f(x+1) - f(x) \xrightarrow[n\to+\infty]{} 0$ donc $f'(x) \xrightarrow[n\to+\infty]{} 0$.

Chapitre 31

TD 31

Exercice 1

1. On pose $\Omega = S_n$ muni de l'équiprobabilité P. On a donc

$$\begin{aligned}\forall i \in [\![1,n]\!]\,,\ (X=i) &= \{\omega \in \Omega \mid X(\omega) = i\} \\ &= \left\{\omega = \begin{pmatrix} 1 & \cdots & n \\ \omega_1 & \cdots & \omega_n \end{pmatrix} \in \Omega \;\middle|\; \omega_i = 1\right\}\end{aligned}$$

$$P(X=i) = \frac{\#(X=i)}{n!} = \frac{(n-1)!}{n!} = \frac{1}{n}.$$

2. $X \sim \mathcal{U}([\![1,n]\!])$.

Autre rédaction : On note $Y_i = j$ si on a tiré le jeton j lors du tour i. D'où

$$(X=i) = (Y_1 \neq 1) \cap \cdots \cap (Y_{i-1} \neq i) \cap (Y_i = 1).$$

Et donc,

$$P(X=i) = P(Y_1 \neq 1) P_{(Y_1 \neq 1)}(Y_2 \neq 2) \cdots P_{(Y_1 \neq 1, \ldots, Y_{i-2} \neq 1)}(Y_{i-1} \neq 1) P_{(Y_1 \neq 1, \ldots, Y_{i-1} \neq 1)}(Y_i = 1).$$

Exercice 2

Soit (Ω, P) un espace probabilisé modélisant la situation.

1. On a $X(\Omega) = [\![2, n-1]\!]$.

$$\forall k \in [\![2,n-1]\!]\,,\ P(X=k) = \frac{(k-1)(n-k)}{\binom{n}{3}}.$$

Vérification :

$$\begin{aligned}\sum_{k=0}^{n} P(X=k) &= \frac{3!\,(n-3)!}{n!}\sum_{k=2}^{n-1}\big(-k^2+(n+1)k-n\big)\\ &= \frac{6}{n(n-1)(n-2)}\left(-\frac{(n-1)\,n\,(2n-1)}{6}+1+(n+1)\frac{(n-2)(n+1)}{2}-n\,(n-2)\right)\\ &= \frac{6}{n(n-1)(n-2)}\times\frac{-n(n-1)(2n-1)+6+3(n+1)^2+(n-2)-6n(n-2)}{6}\\ &= \frac{1}{n^3-3n^2+2n}\times\big(n^3-3n^2+2n\big)\\ &= 1.\end{aligned}$$

2.

$$E(X)=\sum_{k=2}^{n-1} k\frac{(k-1)(n-k)}{\binom{n}{3}}=\cdots\cdots\cdots$$

Exercice 3

1. Pour tout i, $Y_i\sim\mathscr{B}\left(m,\frac{1}{n}\right)$ et $X_i\sim\mathscr{B}\left(1-\left(\frac{n-1}{n}\right)^m\right)$.
2. $X=\sum_{i=1}^{n}X_i$ d'où $E(X)=n\underbrace{\left(1-\left(\frac{n-1}{n}\right)^m\right)}_{E(X_i)}$.

Exercice 4

1. $T_n(\Omega)=[\![1,n]\!]$. On a

$$\forall k\in[\![1,n-1]\!]\,,\ P(T_n=k)=q^{k-1}\,p$$

et $P(T_n=n)=q^n+q^{n-1}p=q^{n-1}$.

Vérification :

$$\begin{aligned}\sum_{k=1}^{n}P(T_n=k) &= \sum_{k=1}^{n-1}q^{k-1}\,p+q^{n-1}\\ &= \not{p}\times\frac{1-q^{n-1}}{\not{1-q}}+q^{n-1}\\ &= 1.\end{aligned}$$

$$\begin{aligned}
E(T_n) &= \sum_{k=1}^{n} k\, P(T_n = k) \\
&= \sum_{k=1}^{n-1} k\, q^{k-1}\, p + n q^{n-1} \\
&= p\, \frac{\mathrm{d}}{\mathrm{d}q} \left(\sum_{k=0}^{n-1} q^k \right) + n q^{n-1} \\
&= p \frac{-n q^{n-1} + (1-q^n)}{(1-q)^2} + n q^{n-1} \\
&= \frac{1 - q^n - n p q^{n-1}}{p} + n q^{n-1} \\
&= \frac{1-q^n}{p}.
\end{aligned}$$

2. $X_n \sim \mathcal{B}(1-q^n)$. $E(X_n) = 1 - q^n$.
3. $X_n + Y_n = T_n$ d'où, par linéarité de l'espérance,

$$E(X_n) + E(Y_n) = E(T_n).$$

On en déduit que

$$\begin{aligned}
E(Y_n) &= E(T_n) - E(X_n) \\
&= \frac{1-q^n}{p} - (1-q^n) \\
&= (1-q^n) \left(\frac{1-p}{p} \right) \\
&= \frac{q}{p}(1-q^n).
\end{aligned}$$

Exercice 5

1.

v \ u	0	1	2
-1	0	qp	0
0	q^2	0	p^2
1	0	qp	0

2. $P(U=2, V=1) = 0 \neq P(U=2)\, P(V=1) = qp^3$.

Exercice 6

$(X,Y) \sim \mathcal{U}\left(\llbracket 1,6 \rrbracket^2\right)$;

z \ x	1	2	3	4	5	6	
1	$1/6$	0	0	0	0	0	$1/6$
2	0	$1/6$	0	0	0	0	$1/6$
3	0	0	$1/6$	0	0	0	$1/6$
4	0	0	0	$1/18$	$1/18$	$1/18$	$1/6$
5	0	0	0	$1/18$	$1/18$	$1/18$	$1/6$
6	0	0	0	$1/18$	$1/18$	$1/18$	$1/6$
	$1/6$	$1/6$	$1/6$	$1/6$	$1/6$	$1/6$	

Exercice 7

$$X = \sum_{i=1}^{Np} X_i \quad \text{d'où} \quad E(X) = \sum_{i=1}^{Np} E(X_i).$$

Or, $X_i \sim \mathcal{B}\left(\frac{\binom{N-1}{n-1}}{\binom{N}{n}}\right)$.

On en déduit que

$$\begin{aligned} E(X) &= \sum_{i=1}^{Np} \frac{\binom{N-1}{n-1}}{\binom{N}{n}} \\ &= \frac{n!\,\cancel{(N-n)!}\,(N-1)!\,Np}{N!\,(n-1)!\,\cancel{(N-n)!}} \\ &= \frac{n}{N} Np \\ &= np. \end{aligned}$$

$$V(X) = \sum_{i=1}^{Np} V(x_i) + 2 \sum_{1 \leqslant i < j} \mathrm{Cov}(X_i, X_j)$$

où

$$\mathrm{Cov}(X_i, X_j) = E(X_i X_j) - E(X_i)E(X_j).$$

1. $X_i \sim \mathcal{B}\left(\frac{\binom{N-1}{n-1}}{\binom{N}{n}}\right)$.

$$E(X_i) = \frac{n!\,(N-n)!}{N!} \times \frac{(N-1)!}{(n-1)!\,(N-n)!} = \frac{n}{N}.$$

$$V(X_i) = \frac{n}{N}\left(1 - \frac{n}{N}\right) = \frac{n(N-n)}{N^2}.$$

2. $\mathrm{Cov}(X_i, X_j) = E(X_iX_j) - E(X_i)E(X_j)$. Or, $X_iX_j \sim \mathscr{B}\big(P(X_i = 1, X_j = 1)\big)$ et

$$\begin{aligned} P(X_i = 1, X_j = 1) &= \frac{\binom{N-2}{n-2}}{\binom{N}{n}} \\ &= \frac{(N-2)!}{(n-2)!\,\cancel{(N-n)!}} \times \frac{n!\,(N-n)!}{N!} \\ &= \frac{n(n-1)}{N(N-1)}. \end{aligned}$$

3. On a $X = \sum_{i=1}^{Np} X_i$ et donc

$$E(X) = \sum_{i=1}^{Np} E(X_i) = \frac{n}{N} \times Np = np$$

et

$$\begin{aligned} V(X) &= \sum_{i=1}^{Np} V(X_i) + \sum_{1 \leqslant i \neq j \leqslant Np} \mathrm{Cov}(X_i, X_j) \\ &= p\frac{n}{N}(N-n) + \cancel{N}p(Np-1)\frac{n(n-1)}{\cancel{N}(N-1)}. \end{aligned}$$

Loi de X :

$$P(X = k) = \frac{\binom{Np}{k}\binom{Nq}{n-k}}{\binom{N}{n}}.$$

Exercice 8

1. $X(\Omega) = [\![1, n+1]\!]$.

$$\forall k \in [\![1, n]\!]\,,\ P(X = k) = q^{k-1}\,p.$$

(cela correspond, à quelques détails près, à la loi géométrique)

Également, $P(X = n+1) = q^n$.

Vérification : $\sum_{k=1}^{n} q^{k-1}p + q^n = p\frac{1-q^n}{1-q}q^n = 1.$

2.

$$\begin{aligned}
E(X) &= \sum_{k=1}^{n+1} k\, P(X=k) \\
&= \sum_{k=1}^{n} kq^{k-1}p + (n+1)q^n \\
&= p\,\frac{\mathrm{d}}{\mathrm{d}q}\left(\sum_{k=0}^{n} q^k\right) + (n+1)q^n \\
&= p\,\frac{\mathrm{d}}{\mathrm{d}q}\left(\frac{1-q^n}{1-q}\right) + (n+1)q^n \\
&= p\frac{-(n+1)q^n(1-q)+(1-q^{n+1})}{(1-q)^2} + (n+1)q^n \\
&= -(n+1)q^n\frac{1-q^{n+1}}{p} + (n+1)q^n \\
&= \frac{1-q^{n+1}}{p}
\end{aligned}$$

3. On cherche p tel que

$$\begin{aligned}
P(X=n+1) \leqslant \frac{1}{2} &\iff q^n \leqslant \frac{1}{2} \\
&\iff q \leqslant \frac{1}{\sqrt[n]{2}}
\end{aligned}$$

Exercice 9

On pose $q = 1-p$.

La probabilité que l'avion à deux moteurs arrive à destination est $P_A(D) = q^2 + 2pq = 1-p^2$.

La probabilité que l'avion à quatre moteurs arrive à destination est $P_B(D) = q^4 + 4pq^3 + 6p^2q^2$.

On pose $f : p \mapsto (1-p)^4 + 4p(1-p)^3 + 6p^2(1-p)^2 - 1 + p^2$.

B erreur de calcul probable.

$\forall p \in [0,1]$, $f(p) = 3p^4 - 4p^3 + p^2 = p^2 \underbrace{(3p^2 - 4p + 1)}_{\Delta = 16-4\times3\times1=4}$

p	0		$\frac{1}{3}$		1
$f(p)$		$+$	0	$-$	0

Exercice 10

C'est la loi trinomiale.

1. p^2qr^2 ; $\binom{5}{2}\binom{3}{1}p^2qr^2$
2. $$\binom{n}{i}\binom{n-i}{j}p^iq^jr^k = \frac{n!}{i!\,\cancel{(n-i)!}} \times \frac{\cancel{(n-i)!}}{j!\,(n-i-j)!}p^iq^jr^k$$
$$= \frac{n!}{i!\,j!\,k!}p^i\,q^j\,r^k$$

3. *Application* On a $p = q = \frac{7}{10} \times \frac{3}{10} = \frac{21}{100}$; $r = \left(\frac{3}{10}\right)^2 + \left(\frac{7}{10}\right)^2 = \frac{58}{100}$.

   On note X le nombre de succès de A, et Y le nombre de succès de B.

$$\begin{aligned} P(X > Y) &= \sum_{x=0}^{5} P(X = x, Y < x) \\ &= \sum_{x=0}^{5}\sum_{y=0}^{x-1} P(X = x, Y = y) \\ &= \sum_{i=0}^{5}\sum_{j=0}^{i-1} \frac{5!}{i!\,j!\,(5-i-j)!}\left(\frac{21}{100}\right)^i\left(\frac{21}{100}\right)^j\left(\frac{58}{100}\right)^{5-i-j}. \end{aligned}$$

Chapitre 32

TD 32

Exercice 1

$$\begin{aligned}\sum_{k=0}^{+\infty}\sum_{k=n}^{+\infty}\frac{1}{k!} &\overset{\text{B}}{=} \sum_{k=0}^{+\infty}\sum_{n=0}^{k}\frac{1}{k!}\\ &= \sum_{k=0}^{+\infty}\frac{k+1}{k!}\\ &= \sum_{k=0}^{+\infty}\frac{1}{(k-1)!}+\sum_{k=0}^{+\infty}\frac{1}{k!}\\ &= 2e\end{aligned}$$

On pose

$$I=\{(n,k)\in\mathbb{N}^2 \mid k\geqslant n\} \qquad \text{et} \qquad \forall (n,k)\in I,\ u_{n,k}=\frac{1}{k!}.$$

D'où

$$\sum_{k=0}^{+\infty}\sum_{k=n}^{+\infty}\frac{1}{k!}=\sum_{(n,k)\in I}u_{n,k}.$$

On pose $I=\bigcup_{k\in\mathbb{N}} I_k$ où $I_k=\{(n,k)\in\mathbb{N}^2 \mid n\leqslant k\}$.

D'après le théorème de sommation par paquets,

$$\sum_{(n,k)\in I}u_{n,k}=\sum_{k\in\mathbb{N}}\sum_{(n,k)\in I_k}u_{n,k}=\sum_{k=0}^{+\infty}\sum_{n=0}^{k}\frac{1}{k!}.$$

Exercice 2

On pose

$$I = \{(p,q) \in (\mathbb{N}^\star)^2 \mid p \geqslant q\} \text{ et } \forall (p,q) \in I,\ u_{p,q} = \frac{(-1)^p}{q^3}.$$

$$\forall (p,q) \in I,\ |u_{p,q}| = \frac{1}{q^3}.$$

$$\begin{aligned}\sum_{(p,q)\in I} |u_{p,q}| &= \sum_{p=1}^{+\infty}\sum_{q=p}^{+\infty} \frac{1}{q^3} \\ &= \sum_{q=1}^{+\infty}\sum_{p=1}^{q} \frac{1}{q^3} \\ &= \sum_{q=1}^{+\infty} \frac{1}{q^2} = \frac{\pi^2}{6} < +\infty\end{aligned}$$

Donc $(u_{p,q})_{(p,q)\in I}$ est sommable.

Donc,

$$\begin{aligned}\sum_{k=0}^{+\infty}\sum_{q=p}^{+\infty} \frac{(-1)^p}{q^3} &= \sum_{q=1}^{+\infty}\sum_{p=1}^{q} \frac{(-1)^p}{q^3} \\ &= \sum_{q=1}^{+\infty} \frac{1}{q^3} \underbrace{\sum_{p=1}^{q}(-1)^p}_{=\begin{cases}0 & \text{si } q \text{ pair} \\ -1 & \text{si } q \text{ impair.}\end{cases}} \\ &= \sum_{k=0}^{+\infty} -\frac{1}{(2k+1)^3}\end{aligned}$$

Or,

$$\zeta(3) = \sum_{p=1}^{+\infty} \frac{1}{p^3} = \sum_{\substack{p\in\mathbb{N}^\star \\ p \text{ pair}}} \frac{1}{p^3} + \sum_{\substack{p\in\mathbb{N}^\star \\ p \text{ impair}}} \frac{1}{p^3}$$

et

$$\sum_{\substack{p\in\mathbb{N}^\star \\ p \text{ pair}}} \frac{1}{p^3} = \sum_{k=1}^{+\infty} \frac{1}{(2k)^3} = \frac{1}{8}\zeta(3).$$

On en déduit que

$$\sum_{p=1}^{+\infty}\sum_{q=p}^{+\infty}\frac{(-1)^p}{q^3}=-\frac{7}{8}\zeta(3).$$

Exercice 4

1.

$$\begin{aligned}\sum_{(p,q)\in(\mathbb{N}^\star)^2}\frac{1}{p^2\,q^2}&=\sum_{p=1}^{\infty}\frac{1}{p^2}\sum_{q=1}^{+\infty}\frac{1}{q^2}\\&=\frac{\pi^4}{36}\end{aligned}$$

2.

$$\begin{aligned}\sum_{\substack{(p,q)\in(\mathbb{N}^\star)^2\\p|q}}\frac{1}{p^2\,q^2}&=\sum_{p=1}^{+\infty}\sum_{\substack{q\in\mathbb{N}^\star\\p|q}}\frac{1}{p^2q^2}\\&=\sum_{p=1}^{+\infty}\sum_{k=1}^{+\infty}\frac{1}{p^2(pk)^2}\\&=\sum_{p=1}^{+\infty}\frac{1}{p^4}\sum_{k=1}^{+\infty}\frac{1}{k^2}\\&=\zeta(4)\times\zeta(2)\\&=\frac{\pi^4}{90}\times\frac{\pi^2}{6}\\&=\frac{\pi^6}{540}.\end{aligned}$$

3.

$$\begin{aligned}\sum_{(p,q)\in(\mathbb{N}^\star)^2}\frac{1}{p^2\,q^2}&=\sum_{d\in\mathbb{N}^\star}\sum_{\substack{(p,q)\in\mathbb{N}^\star\\p\wedge q=d}}\frac{1}{p^2\,q^2}\\&=\sum_{d\in\mathbb{N}^\star}\sum_{\substack{(p',q')\in(\mathbb{N}^\star)^2\\p'\wedge q'=1}}\frac{1}{(dp')^2(dq')^2}\\&=\left(\sum_{d=1}^{+\infty}\frac{1}{d^4}\right)\left(\sum_{p'\wedge q'=1}\frac{1}{p'^2q'^2}\right)\end{aligned}$$

On en déduit que

$$\sum_{p\wedge q=1}\frac{1}{p^2\,q^2}=\frac{\frac{\pi^4}{36}}{\frac{\pi^4}{90}}=\frac{90}{36}=\frac{5}{2}.$$

Partie IV

MPI – Informatique – Cours

Chapitre -1

Ordres et induction

IV.1 Motivation

```
let rec fact n =
  if n = 0 then 1
  else n * (fact (n-1));;
```

Code 1 – Calcul de factorielle

Ce programme calcule la factorielle d'un nombre ? En développant, l'expression de `fact 3`, on a

$$\begin{aligned}(\texttt{fact } 3) &= 3 \times (\texttt{fact } 2) \\ &= 3 \times (2 \times (1 \times 1))\end{aligned}$$

On en déduit que ce programme calcule la factorielle car ce développement s'arrête à un certain point. Comment en être sûr ? En effet, avec `n` $= -1$, on obtient une `Stack Overflow Error` ; on n'a plus de mémoire. Pour en être sûr, il faut définir un *invariant*.

À faire : Ajouter 2ème exemple

Un autre exemple :

```
let mystere2 n m =
  let rec aux c b =
    if c = 0 and b = m then 0
    else if c = 0 then aux (b * m) (b + 1)
    else 1 + aux (c - 1) b
  in aux n 0;;
```

Code 2 – Un programme mystère (2)

Ce programme a beaucoup plus de variables : les variables augmentent dans certains cas, puis diminuent… On peut représenter l'état des variables `b` et `c` dans une figure :

À faire : Figure à faire

FIGURE 1 – État des variables `b` et `c`

On en conclut que ce programme calcule la valeur de

$$\mathtt{n}+\mathtt{m}+2\mathtt{m}+\cdots+\mathtt{m}^2=\mathtt{n}+\frac{\mathtt{m}^2\times(\mathtt{m}-1)}{2}.$$

Cherchons un variant. On peut penser à $\mathtt{b}-\mathtt{m}$ mais il ne diminue pas à chaque étape. Nous verrons quel est ce variant plus tard dans le chapitre.

Nouvel exemple : retourner une liste. Essayons de distinguer les différents cas possibles : si la liste est vide, on la renvoie ; sinon, on extrait un élément `x` et on note le reste de la liste `xs`, on retourne `xs` puis on concatène à droite `x`. On peut donc écrire

```
let rec rev l =
  match l with
  | [] -> []
  | x :: xs -> (rev xs) @ [x];;
```

CODE 3 – Inverser une liste

Cependant, le `@` est une opération lente en OCamL. En effet ce programme a une complexité en $\mathcal{O}(n^2)$, où n est la taille de la liste. Cette complexité est douteuse pour une opération aussi simple. On peut également se demander si cette opération se termine. Cela paraît très simple : la taille de la liste diminue mais nous n'avons pas le coté mathématique d'une liste. En effet, qu'est ce qu'une liste et la taille de cette liste ? On doit formaliser l'explication de pourquoi cet algorithme se termine.

Continuons avec un autre exemple :

```
let rec mystere3 m n =
  if m = 0 then n + 1
  else if n = 1 then mystere (n - 1) 1
  else mystere (m - 1) (mystere m (n-1));;
```

CODE 4 – Un programme mystère (3)

Il s'agit de la fonction ACKERMANN. Sa complexité est très importante mais ce n'est pas le sujet de cette introduction. En effet, on a

$$A_{0,m}=n+1$$
$$A_{m,0}=A_{n-1,1}$$
$$A_{m,n}=A_{m-1,A_{m,\dots}}$$

Malgré ce que l'on peut penser, cette fonction se termine mais comment le prouver ?

À faire : Exemple arbres binaires

On en conclut que, avec les outils de l'année passée, il est difficile de prouver que ces algorithmes se terminent rigoureusement.

IV.2 Ordre

Définition (Élements minimaux) **:** Lorsque $(E, \preccurlyeq)$ est un espace ordonné, et $A \subseteq E$ ("inclut ou égal") est une partie de E, on appelle *élément minimal* de A un élément $x \in A$ tel que

$$\forall y \in A,\ y \preccurlyeq x \implies y = x.$$

Exemple :
La figure ci-dessous est un diagramme de Hasse : c'est un diagramme où les points représente les éléments de l'ensemble E et où les segments représentent une comparaison entre les deux éléments connectés : l'élément inférieur est représenté plus bas. Dans l'exemple ci-dessous, les éléments minimaux de A sont les points b et f.

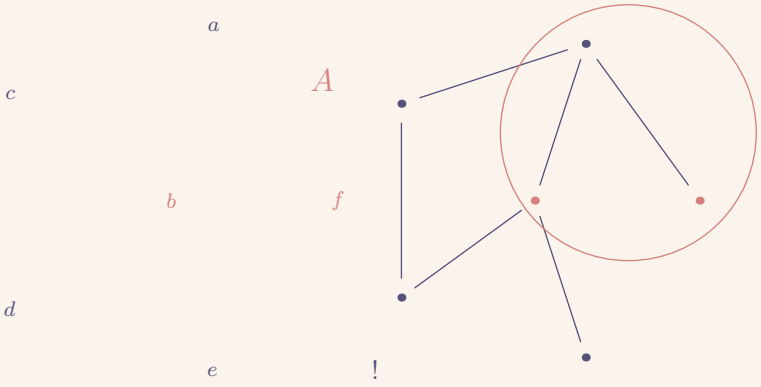


Figure 2 – Diagramme de Hasse

Définition (Ordre bien fondé) **:** Un ordre est *bien fondé* s'il n'existe pas de suite infiniment strictement croissante.

Exemple :

Oui	Non
$(\mathbb{N}, \leqslant)$	$(\mathbb{Z}, \leqslant)$
	$(\mathbb{R}, \leqslant)$
	$(\mathbb{R}^+, \leqslant)$ $(1/2^n)$
$(E, \subseteq)$ (si E est fini)	$(E, \subseteq)$ (en général)

Table 1 – Exemples et non-exemples d'ordres bien fondés

Proposition : Une relation d'ordre $\preccurlyeq$ sur un ensemble E bien fondé si et seulement si toute partie non vide de E admet un élément minimal.

Preuve “ $\Longleftarrow$ ” Supposons que toute partie non vide de E admet un élément minimal. Supposons, de plus, qu'il existe une suite $(x_n)_{n\in\mathbb{N}}$ infiniment strictement décroissante. Soit alors $A = \{u_n \mid n \in \mathbb{N}\}$ qui admet un élément minimal ; soit n_0 son indice. Or, $x_{n_0+1} \preccurlyeq x_{n_0}$ ce qui est absurde.

“ $\Longrightarrow$ ” Supposons que $(E, \preccurlyeq)$ est un ensemble bien fondé. Supposons également qu'il existe un sous-ensemble A de E non vide n'admettant pas d'élément minimal. Comme A est non vide, on pose alors $x_0 \in A$. Et, comme A n'admet pas d'élément minimal, donc il existe $x \in A$ tel que $x \preccurlyeq x_0$. Notons un tel x, x_1. En itérant ce procédé, on crée la suite $(x_i)_{i\in\mathbb{N}}$ qui est infiniment strictement décroissante ; ce qui est absurde.

□

Théorème (Induction bien fondée) **:** Soit $(E, \preccurlyeq)$ un ensemble ordonné et bien fondé. Soit P une propriété sur les éléments de E. Si $x \in E$, on note $E^{\preccurlyeq x} = \{y \in E \mid y \preccurlyeq x\}$. Si $\forall x \in E$, $\big(\forall y \in E^{\preccurlyeq x}, P(y)\big) \implies P(x)$, alors $\forall x \in E$, $P(x)$.

Remarque :
Si $(E, \preccurlyeq) = (\mathbb{N}, \leqslant)$, alors le théorème précédent se traduit par :

$$\text{si } \forall n \in \mathbb{N},\ \big(\forall p < n,\ P(p)\big) \implies P(n), \text{ alors } \forall n \in \mathbb{N}, P(n).$$

Ce résultat correspond à la “récurrence forte.” Décomposons ce “$\forall$” : on extrait le cas où $n = 0$

$$\text{si } P(0) \text{ et } \forall n \in \mathbb{N}^\star,\ \big(\forall p < n, P(p)\big) \implies P(n), \text{ alors } \forall n \in \mathbb{N}, P(n).$$

On peut donc utiliser le principe de la récurrence pour tout ensemble ordonné bien fondé.

Preuve :
Soit $A = \{x \in E \mid P(x) \text{ n'est pas vrai}\}$.

Cas 1 $A = $, alors OK.
Cas 2 $A \neq$. Soit alors $x \in A$ un élément minimal de A (c.f. proposition d'avant). On a que $\forall y \in E$, $y \preccurlyeq x$, $P(y)$ est vrai donc $P(x)$ est vrai par hypothèse. Ce qui est absurde.

□

IV.2.1 Ordre produit

Définition : Soit $(A, \preccurlyeq_A)$ et $(B, \preccurlyeq_B)$ deux ensembles ordonnés on définit alors $\preccurlyeq_\times$ sur $A \times B$ par

$$\forall (a,b),(a',b') \in A \times B,\ (a,b) \preccurlyeq_\times (a',b') \overset{\text{def.}}{\iff} (a \preccurlyeq_A a' \text{ et } b \preccurlyeq_B b').$$

Proposition : $\preccurlyeq_\times$ est une relation d'ordre. □

La proposition précédente est facilement vérifiée comme $\preccurlyeq_A$ et $\preccurlyeq_B$ sont, elles aussi, des relations d'ordre.

Remarque (B) :
Si $\preccurlyeq_A$ et $\preccurlyeq_B$ sont des ordres totaux, $\preccurlyeq_\times$ ne l'est pas forcément.

Proposition : Soient $(A, \preccurlyeq_A)$ et $(B, \preccurlyeq_B)$ bien fondés, alors $(A \times B, \preccurlyeq_\times)$ l'est aussi.

Preuve :
Supposons alors que $(A \times B, \preccurlyeq_\times)$ ne soit pas bien fondée. Nous avons donc une suite infiniment strictement décroissante

$$(a_0,b_0) \succ_\times (a_1,b_1) \succ_\times (a_2,b_2) \succ_\times \cdots.$$

On a donc $a_0 \succcurlyeq_A a_1 \succcurlyeq_A a_2 \succcurlyeq \cdots$. Or, $(A, \preccurlyeq_A)$ est bien fondée donc il existe $n_0 \in \mathbb{N}$ tel que $\forall i \geqslant n_0, a_i = a_{n_0}$. On a donc $\forall i \geqslant n_0,\ b_i \prec_B b_{i-1}$. Considérons $(b_i)_{i \geqslant n_0}$ est infiniment strictement décroissante dans $(B, \preccurlyeq_B)$, ce qui est absurde. □

Remarque :
On a défini une relation "produit," on peut se demander si ces résultats s'appliquent aussi si la relation est "somme." Ce n'est pas le cas : soit $\preccurlyeq_+$ définie comme

$$(a,b) \preccurlyeq_+ (a',b') \overset{\text{def.}}{\iff} a \preccurlyeq_A a' \text{ ou } b \preccurlyeq_B b'.$$

On peut démontrer que ce n'est pas une relation d'ordre.

Remarque :
Si $(A, \preccurlyeq_A)$ est une relation d'ordre alors $(A^n, \preccurlyeq_\times)$ a les même propriétés.

Remarque :
Sur $A^{\mathbb{N}}$, on définit $(u_n)_{n\in\mathbb{N}} \preccurlyeq_\times (v_n)_{n\in\mathbb{N}}$ si et seulement si

$$\forall i,\ u_i \preccurlyeq_A v_i.$$

L'ensemble ordonné $(A^{\mathbb{N}}, \preccurlyeq_\times)$ est il bien fondé ? La réponse est non.

Voici un contre-exemple : on pose $A = \{0,1\}$.

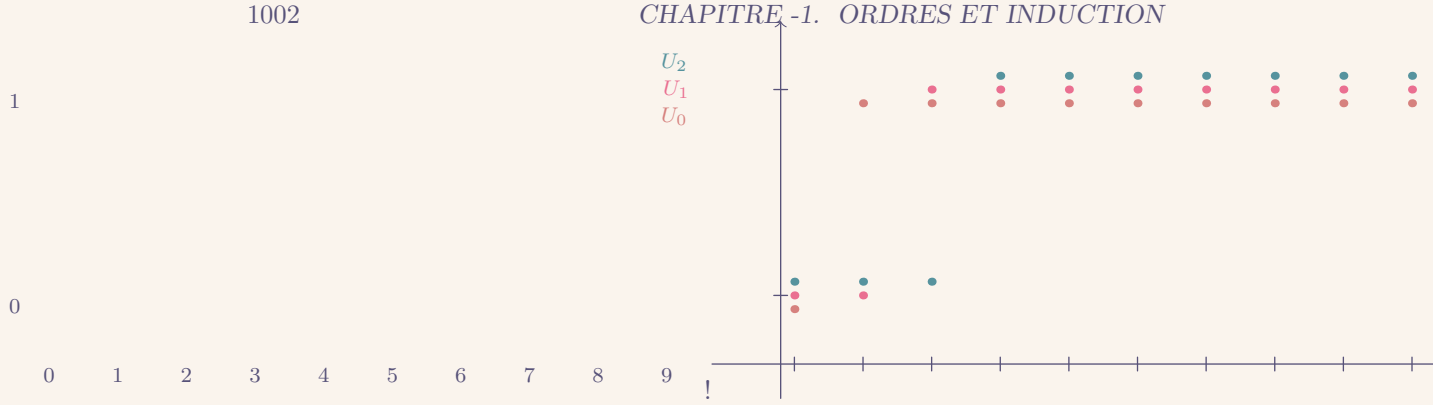


FIGURE 3 – Contre exemple : $(A^{\mathbb{N}}, \preccurlyeq_\times)$ est il bien fondé ?

On considère la suite U_0 qui a pour tout $n \in \mathbb{N}$ la valeur de 1. Puis, on considère la suite U_1 qui a, pour $n = 0$, la valeur de 0 puis pour les autres valeurs de n, la valeur de 1. Ensuite, on considère la suite U_2 qui, pour $n = 0, 1$, la valeur de 0 puis, pour les autres valeurs de n, la valeur de 1. En itérant ce procédé, on crée une suite de suite $(U_n)_{n\in\mathbb{N}}$ infiniment strictement décroissante :

$$U_0 \succcurlyeq_\times U_1 \succcurlyeq_\times U_2 \succcurlyeq_\times \cdots .$$

On considère le programme suivant :

```
let rec pgcd a b =
  if a = b then a
  else if a > b then pgcd (a-b) b
  else pgcd a (b-a);;
```

CODE 5 – Calcul du PGCD

Étudions ce programme. Ce programme se termine si et seulement si `a` $= 0$ et `b` $= 0$ où si `a` > 0 et `b` > 0. Prouvons-le rigoureusement. On choisit comme variant (a, b) vivant dans l'ensemble ordonné $(\mathbb{N}^\star \times \mathbb{N}^\star, \preccurlyeq_\times)$ où $\preccurlyeq_\times$ est la relation d'ordre produit. À faire : Recopier une partie du cours ici. On a donc bien une décroissance stricte de la valeur de l'expression (a, b)) valeurs dans un espace bien fondé. D'où terminaison.

Démontrons maintenant la correction, c'est-à-dire, démontrons que

$$\forall (a, b) \in \mathbb{N}^\star \times \mathbb{N}^\star, (\texttt{pgcd}\ a\ b) = a \wedge b.$$

Pour cela, on procède par induction sur $\left((\mathbb{N}^\star)^2, \preccurlyeq_\times\right)$ pour démontrer la proposition

$$P(a, b) = (\texttt{pgcd}\ a\ b) = a \wedge b.$$

— Soit $(a, b) = (1, 1)$. On a

$$(\texttt{pgcd}\ a\ b) \underset{\text{(code)}}{=} a = a \wedge b.$$

— Soit $(a, b) \neq (1, 1) \in (\mathbb{N}^\star)^2$ tel que pour tout $(c, d) \in (\mathbb{N}^\star)^2$ tel que $(c, d) \prec_\times (a, b)$ on ait $P(c, d)$. Montrons donc $P(a, b)$.

— Si $a = b$:

$$(\texttt{pgcd}\ a\ b) \underset{\text{(code)}}{=} a = a \wedge b.$$

— Si $a > b$:

$$\begin{aligned}(\texttt{pgcd}\ a\ b) &\underset{\text{(code)}}{=} (\texttt{pgcd}\ (a-b)\ b)\\ &\underset{\text{(hypothèse)}}{=} (a-b) \wedge b\\ &\underset{\text{(maths)}}{=} a \wedge b.\end{aligned}$$

IV.2.2 Ordre lexicographique

Définition : Soit $(A, \preccurlyeq_A)$ et $(B, \preccurlyeq_B)$ deux ensembles ordonnés, on définit alors sur $A \times B$ l'ordre

$$(a,b) \preccurlyeq_\ell (a',b') \overset{\text{def.}}{\iff} (a \prec_A a') \text{ ou } (a = a' \text{ et } b \preccurlyeq_B b').$$

Exemple :
Dans $(\mathbb{N}^2, \preccurlyeq_\times)$, on cherche les éléments $(x,y) \in \mathbb{N}^2$ tels que $(x,y) \preccurlyeq_\ell (3,4)$:

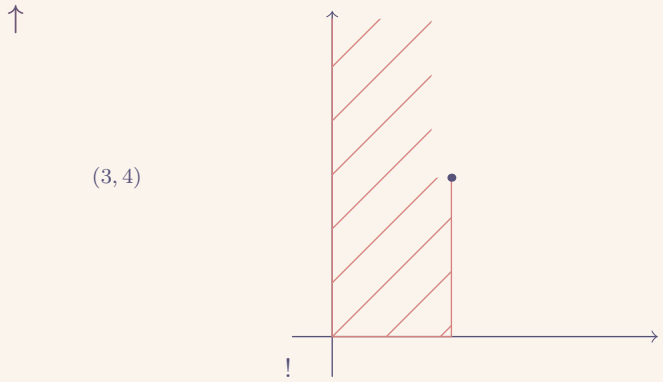


Figure 4 – Ordre lexicographique sur $\mathbb{N}^2$

Proposition : $\preccurlyeq_\ell$ est une relation d'équivalence.

Preuve :
À faire □

Proposition : Si $\preccurlyeq_A$ est totale et $\preccurlyeq_b$ est totale alors $\preccurlyeq_\ell$ est totale.

Preuve :
Soit (a,b) et $(c,d) \in (A \times B)$.

- Si $a \prec_A c$, alors $(a,b) \prec_\ell (c,d)$.
- Si $a = c$,
  - si $b \preccurlyeq_B d$ alors $(a,b) \preccurlyeq_\ell (c,d)$.
  - sinon $(b \succcurlyeq_B d)$ alors $(a,b) \succ_\ell (c,d)$.
- si $a \succ_A c$ alors $(c,d) \prec_\ell (a,b)$.

□

Proposition : Si $(A, \preccurlyeq_A)$ et $(B, \preccurlyeq_B)$ sont bien fondés, alors $(A \times B, \preccurlyeq_\ell)$ l'est aussi.

Preuve :
À rédiger. □

Remarque :
On peut généraliser à un ensemble $(A^n, \preccurlyeq_\ell)$.

Par exemple, avec $n = 3$, on a

$$(a,b,c) \preccurlyeq_\ell (a',b',c') \overset{\text{def.}}{\iff} a \prec_A a' \text{ ou } (a = a' \text{ et } b \prec_B b') \text{ ou } (a = a' \text{ et } b = b' \text{ et } c \prec_C c').$$

Même question qu'avec l'ordre produit, l'ensemble $(A^{\mathbb{N}}, \preccurlyeq_\ell)$ est-il bien fondé ?
De même, la réponse est non, la même suite de suite est un contre-exemple.

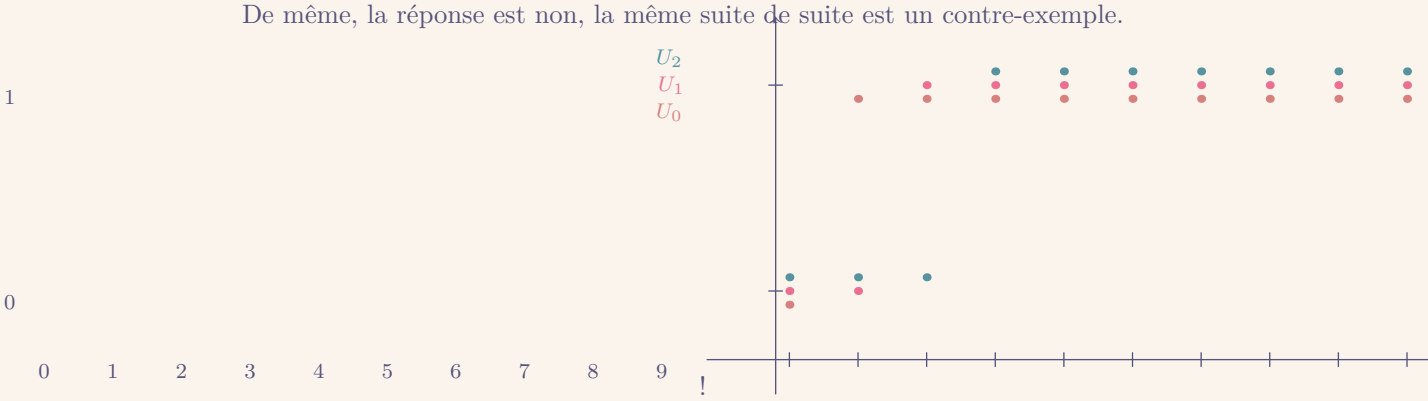


Figure 5 – Contre exemple : $(A^{\mathbb{N}}, \preccurlyeq_\ell)$ est il bien fondé ?

L'ordre lexicographique est, comme son nom l'indique, l'ordre utilisé dans le dictionnaire. La seule différence est que l'on peut comparer des mots de longueurs différentes.

Rappel :
Si A est un ensemble, alors $A^\star = \bigcup_{n\in\mathbb{N}} A^n$. L'ensemble $A^\star$ contient toutes les suites finies d'éléments de A.

Par exemple, avec $A = \{0, 1\}$, on a

$$A^\star \supseteq \big\{(\,), (1), (0), (0,1), (1,0), (1,1), (0,0), (1,1,0), (0,0,0), \dots\big\}.$$

Définition : Si $(A, \preccurlyeq_A)$ est un ensemble ordonné, on définit sur $A^\star$:

$$(u_p)_{p\in[\![1,n]\!]} \prec_\ell (v_p)_{p\in[\![1,m]\!]} \overset{\text{def.}}{\iff} \begin{array}{l} \exists i \in [\![1, \min(n,m)+1]\!], \\ \big(\forall j \in [\![1, i-1]\!],\ u_j = v_j\big) \\ \text{et } (i = n+1 \text{ ou } u_i \prec_A v_i). \end{array}$$

Proposition : C'est une relation d'ordre. Elle est totale si $\preccurlyeq_A$ est totale. □

Même question avec cette nouvelle définition de l'ordre lexicographique, l'ensemble $\big((A^\star)^{\mathbb{N}}, \preccurlyeq_\ell\big)$ est-il bien fondé ? De même, la réponse est non. Voici un contre-exemple : on considère la suite de suite $U_0 = (1)$, $U_1 = (0,1)$, $U_2 = (0,0,1)$. On crée une suite infiniment strictement décroissante.

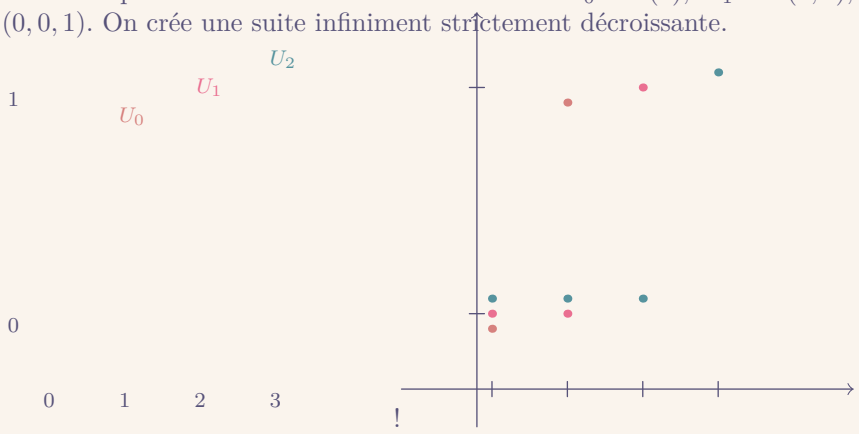


Figure 6 – Contre exemple : $\big((A^\star)^{\mathbb{N}}, \preccurlyeq_\ell\big)$ est il bien fondé ? (2)

```
let rec mystere3 m n =
  if m = 0 then n + 1
  else if n = 1 then mystere (n - 1) 1
  else mystere (m - 1) (mystere m (n-1));;
```

Code 6 – La fonction Ackermann

La fonction Ackermann utilise l'ordre lexicographique ; dans ce cas ci, l'ensemble ordonné est bien fondé. C'est comme cela que l'on a la terminaison de cette fonction.

Prenons un autre exemple :

```
let rec mystere n m p =
  if m > 0 then 1 + mystere n (m - 1) p
  else if m = 0 && n > 0 then 1 + mystere (n-1) p (p
      ↪ +1)
  else 0
```

CODE 7 – Une fonction mystère (5)

À faire :

— s'assurer de la terminaison (comme celle du PGCD)

— démontrer (par induction) que

$$\forall (m,n,p) \in \mathbb{N}^3,\ (\texttt{mystere}\ n\ m\ p) = \frac{n(n+1)}{2} + pn + m.$$

Les preuves de correction et de terminaison sont basées sur la supposition qu'un entier en OCamL est identique à un entier mathématique.

IV.3 Induction nommée

Définition (Règle de Construction nommée) **:** On appelle *règle de construction nommée* la donnée de

— un symbole S,

— un entier $r \in \mathbb{N}$,

— un ensemble non vide C.

On écrira alors cette règle

$$\text{“ } S\Big|_C^r \text{ ”} \qquad \text{ou encore} \qquad \text{“}S(y, \underbrace{\square, \square, \ldots, \square}_{r}) \text{ pour } y \in C.\text{”}$$

REMARQUE :
On a parfois besoin d'un ensemble C trivial (de taille 1 et contenant un objet inutile), on note alors la règle $S\Big|^r$.

EXEMPLE :
Les symboles sont écrits en rouge afin de les différencier.

$$0\Big|^0 \qquad S\Big|^1$$
$$[\,]\Big|^0 \qquad ::\Big|^1_{\mathbb{N}}$$
$$V\Big|^0 \qquad N\Big|^2_{\mathbb{N}}$$

Définition : — On appelle *règle de base* une règle de la forme $S\big|_C^0$.
— On appelle *règle d'induction* une règle de la forme $S\big|_C^n$.

Définition : Étant donné un ensemble <u>fini</u> de règles $R = \underbrace{B}_{\text{règle de base}} \cup \overbrace{I}^{\text{règle d'induction}}$ avec $B \neq$, on définit alors

$$X_0 = \left\{ (S, a) \;\middle|\; S\big|_C^r \text{ et } a \in C \right\}$$

puis, pour tout $n \in \mathbb{N}$,

$$X_{n+1} = X_n \cup \left\{ (S, a, t_1, t_2, \ldots, t_r) \middle| S\big|_C^r \in \underbrace{R}_{C},\, a \in C,\, t_1 \in X_n,\, t_2 \in X_n, \ldots, t_r \in X_n \right\}.$$

On appelle alors $\bigcup_{n\in\mathbb{N}} X_n$ l'ensemble défini par induction nommée à partir des règles de R.

Remarque (Notation) :
On note un n-uplet ayant pour premier élément un symbole S puis $n-1$ éléments $(a_1, \ldots, a_{n-1})$. Au lieu de $(S, a_1, \ldots, a_{n-1})$, on note $S(a_1, \ldots, a_{n-1})$.

Exemple :
On pose

$$R = \left\{ A\big|_{\mathbb{N}}^0, B\big|^1, C^2_{\{0,1\}} \right\}.$$

À faire : À finir

Remarque :
Pour l'ensemble A défini par induction à partir de $R = \left\{ 0\big|^0, S\big|^1 \right\}$, on dira plutôt

"Soit A l'ensemble défini par induction tel que $0 \in A$ et $\forall a \in A$, $S(a) \in A$."

Définition : Soit R un ensemble fini de règles et A l'ensemble défini par induction à partir de ces règles. Sur A, on définit la relation binaire $\diamond$ par

$$x \diamond y \overset{\text{def.}}{\iff} y = S(\ldots, x, \ldots) \text{ avec } S\big|_C^r \in R.$$

On définit alors

$$x \preccurlyeq y \overset{\text{def.}}{\iff} \exists p \in \mathbb{N}, \exists (a_1, \ldots, a_p) \in A^p,\, x \diamond a_1 \text{ et } a_1 \diamond a_2 \text{ et } \ldots \text{ et } a_p \diamond y \text{ ou } x = y.$$

Définition (hauteur) **:** Soit R un ensemble fini de règles d'induction nommée définissant un ensemble $A = \bigcup_{n\in\mathbb{N}} X_n$. On définit alors

$$\begin{aligned} h : A &\longrightarrow \mathbb{N} \\ x &\longmapsto \min\{n \in \mathbb{N} \mid x \in X_n\}. \end{aligned}$$

Remarque :
Si $x \in a$, il existe alors $n_0 \in \mathbb{N}$ tel que $x \in X_{n_0}$ donc $\{n \in \mathbb{N} \mid x \in X_n\} \neq$ donc le minimum existe.

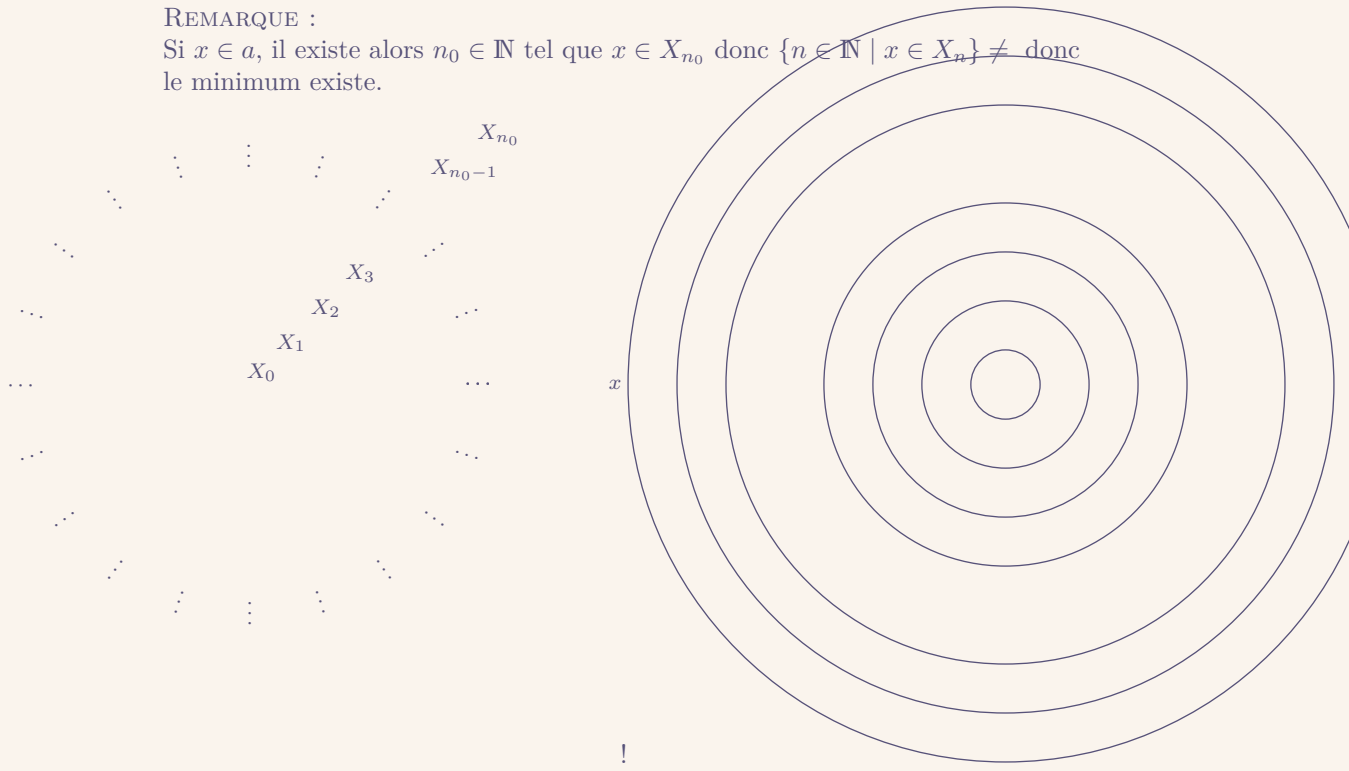


Figure 7 – Structure des ensembles $X_1, \ldots, X_n$

Proposition : Si $x \diamond y$, alors $h(x) < h(y)$.

Preuve :
Soit $x \diamond y$. Alors, $y \in A$. Soit $n_0 = h(y) \neq 0$, on a donc $y \in X_{n_0}$.

- Si $y \in X_{n_0-1}$ ce qui est absurde par définition de h.
- Si $y \in \left\{ S(a, t_1, \ldots, t_r) \;\middle|\; S|_C^r \in R \text{ et } a \in C \text{ et } t_1 \in X_{n_0-1} \text{ et } \ldots \text{ et } t_r \in X_{n_0-1} \right\}$. Or, soit i_0 tel que $x = t_{i_0}$ donc $x \in X_{n_0-1}$ et donc $h(x) \leqslant n_0 - 1$.

□

Corollaire : Si $n \leqslant y$, alors $h(x) = h(y) \iff x = y$ et $h(x) < h(y) \iff x \prec y$.

Corollaire : La relation $\preccurlyeq$ est antisymétrique.

Remarque :
La relation $\preccurlyeq$ est trivialement transitive et reflective. Elle est donc d'ordre.

Exemple :
On prend $R = \left\{ A\big|^0, B\big|^0 \right\}$ et $X_0 = \{A, B\}$, $X_1 = X_0, \ldots$ L'ensemble S défini par induction sur R est $\{A, B\}$. On en déduit que $\preccurlyeq$ n'est pas totale.

Exemple :
On prend $R = \left\{ 0\big|^0, S\big|^1 \right\}$, $X_0 = \{0\}$, $X_1 = \{0, S(0)\}$ (on a $0 \prec S(0)$), $X_2 = \{0, S(0), S(S(0))\}$ (on a $0 \prec S(0) \prec S(S(0))$). L'ensemble obtenu est

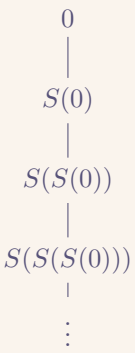


Figure 8 – Ensemble obtenu avec les règles S et 0

Exemple :
On pose $R = \left\{ ::\big|^1_{\mathbb{N}}, [\,]\big|^0 \right\}$ et $X_0 = \{[\,]\}$, $X_1 = \{::(0, [\,]), [\,], ::(1, [\,], ::(2, [\,])\}$, et $X_2 = \{[\,], ::(0, [\,]), ::(1, ::(0, [\,]))\}$. L'ensemble obtenu est

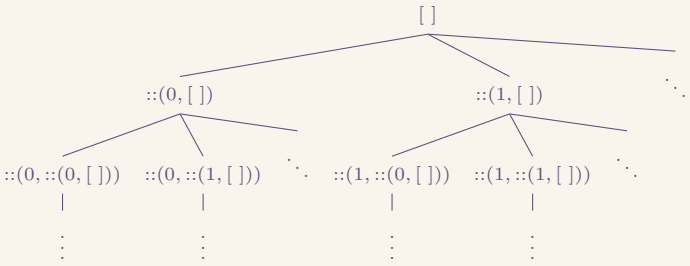


Figure 9 – Ensemble obtenu avec les règles :: et [ ]

Proposition : La relation $\preccurlyeq$ est bien fondée.

Preuve :
Soit $(x_n)_{n\in\mathbb{N}}$ une suite telle que $x_0 \succ x_1 \succ x_2 \succ \cdots \succ x_n \succ \cdots$ alors

$$\underbrace{h(x_0) > h(x_1) > \cdots > h(x_n) > \cdots}_{\in(\mathbb{N},\leqslant)}.$$

Or, $(\mathbb{N}, \leqslant)$ est bien fondé, c'est donc absurde. □

Remarque :
On peut faire des preuves par induction bien fondée.

Exemple : — Soit l'ensemble trivial défini par $\left\{A\big|^0, B\big|^0\right\}$, le théorème est trivial.

— Soit $\mathcal{N}$ défini par $\mathcal{N} = \left\{0\big|^0, S\big|^1\right\}$. Le théorème donne :

si $P(0)$ vrai et $\forall n \in \mathbb{N}$, $(\forall p \in \mathbb{N}, p < n-1, P(\underbrace{S(S(\cdots(S}_{p}(0)\cdots)))) \implies P(\underbrace{S(S(\cdots(S}_{n}(0)\cdots))))$

alors

$$\forall n \in \mathbb{N},\ P(\underbrace{S(S(\cdots(S}_{n}(0)\cdots))).$$

— Soit $\mathscr{L}$ défini par $\mathscr{L} = \left\{[\,]\big|^0, ::\big|^1_{\mathbb{N}}\right\}$. Si $P([\,])$, et $\forall \ell \in \mathscr{L}, \forall n \in \mathbb{N}, P(\ell) \implies P(::(n,\ell))$ alors $\forall \ell \in \mathscr{L}$, $P(\ell)$.

Proposition : Étant donné,
- un ensemble A défini par induction à partir d'un ensemble de règles nommé R,
- un ensemble $\mathbb{I}$,
- une fonction $f_T : C \times \mathbb{I}^r \to \mathbb{I}$ pour chaque règle $T = S\big|^r_C \in R$,

on défini de manière unique une fonction $f : A \to \mathbb{I}$ telle que, pour tout $x = S(a, t_1, \ldots, t_r) \in A$, soit $T = S\big|^r_C \in R$ alors $f(x) = f_T\big(a, f(t_1), \ldots, f(t_r)\big)$.

Exemple :
Sur $\mathscr{L}$ défini par $\Big\{\underbrace{[\,]\big|^0}_{R_1}, \underbrace{::\big|^1_{\mathbb{N}}}_{R_2}\Big\}$, on choisit $\mathbb{I} = \mathbb{N}$ et

$$\begin{aligned} f_{R_1} :\ & \overbrace{(\_,\_)}^{\in \text{Inutile}\times\mathbb{N}^0} \mapsto 0 \\ f_{R_2} :\ & (\underbrace{t}_{\mathbb{N}}, i) \mapsto t + i. \end{aligned}$$

On définit alors la fonction

$$\begin{aligned} f : \mathscr{L} &\longrightarrow \mathbb{N} \\ ::(a_1, ::(a_2, :: \cdots ::(a_n, [\,]) \cdots) &\longmapsto \sum_{i=1}^{n} a_i. \end{aligned}$$

IV.4 Synthèse du chapitre

— Ordre —

Ordre bien fondé

Un ordre est *bien fondé* s'il n'existe pas de suite infiniment strictement décroissante, *i.e.* toute partie non vide de E admet un élément minimal.

Le théorème de l'induction bien fondée nous autorise à faire une récurrence forte sur un ensemble ayant un ordre bien fondé.

Ordre produit

On définit l'*ordre produit* $\preccurlyeq_\times$ de $(A, \preccurlyeq_A)$ et $(B, \preccurlyeq_B)$ comme

$$(a,b) \preccurlyeq_\times (a',b') \overset{\text{def.}}{\iff} a \preccurlyeq_A a' \text{ et } b \preccurlyeq_B b'$$

Cet ordre préserve le caractère bien fondé de $\preccurlyeq_A$ et $\preccurlyeq_B$, mais pas le caractère total de la relation. On étend cet ordre à l'ensemble $(A^n, \preccurlyeq_\times)$, en itérant l'ordre produit.

Ordre lexicographique

On définit l'*ordre lexicographique* $\preccurlyeq_\ell$ de $(A, \preccurlyeq_A)$ et $(B, \preccurlyeq_B)$ comme

$$(a,b) \preccurlyeq_\ell (a',b') \overset{\text{def.}}{\iff} \left| \begin{array}{l} (a \prec_A a') \\ \text{ou} \\ (a = a' \text{ et } b \preccurlyeq_B b'). \end{array} \right.$$

Cet ordre conserve le caractère bien fondé de $\preccurlyeq_A$ et $\preccurlyeq_B$, ainsi que le caractère total. On peut également étendre cet ordre à un ensemble $(A^n, \preccurlyeq_\ell)$. On étend également cet ordre à l'ensemble $(A^\star, \preccurlyeq_\ell)$ comme

$$\begin{array}{c} u \prec_\ell v \\ \cap \quad \cap \\ A^n \quad A^{n+m} \end{array} \overset{\text{def.}}{\iff} \left| \begin{array}{l} \exists i \in [\![1, n+1]\!], \\ (\forall j < i,\ u_j = u_i) \text{ et} \\ (i = n+1 \text{ ou } u_i \prec_A v_i). \end{array} \right.$$

— Induction nommée —

Une *règle de construction nommée* est de la forme

$$\mathbf{S}\Big|_C^r \quad \text{ou} \quad \mathbf{S}(y, \underbrace{\square, \dots, \square}_{r})$$

où $\mathbf{S}$ est un symbole, $r \in \mathbb{N}$ est l'arité de $\mathbf{S}$, et C est un ensemble non vide. On omettra parfois l'ensemble C s'il est trivial (*i.e.* de taille 1). Une *règle de base* est de la forme $\mathbf{S}\big|_C^0$; une *règle d'induction* est de la forme $\mathbf{S}\big|_C^n$.

On définit la *hauteur* h comme

$$h : \bigcup_{n \in \mathbb{N}} X_n \longrightarrow \mathbb{N}$$
$$x \longmapsto \min\{n \in \mathbb{N} \mid x \in X_n\}.$$

On définit la relation $\preccurlyeq$ bien fondée telle que $x \preccurlyeq y$ si x est défini à partir de y. Si $x \preccurlyeq y$, alors $h(x) \leqslant h(y)$.

Un ensemble $\bigcup_{n\in\mathbb{N}} X_n$ est dit *défini par induction nommée* à partir des règles R, si $X_0 = \{\mathbf{S}(a) \mid \mathbf{S}^0_C \in R,\ a \in C\}$, et

$$X_{n+1} = X_n \cup \{\mathbf{S}(a, t_1, \ldots, t_r) \mid \mathbf{S}^r_C \in R,\ a \in C, (t_1, \ldots, t_r) \in (X_n)^r\}.$$

Chapitre 0

Logique

IV.1 Motivation

Considérons la grille de Sudoku 2×2 ci-dessous.

3			2
	4	1	
	3	2	
4			1

Figure 1 – Grille de Sudoku 2×2

On modélise ce problème : on considère $P_{i,j,k}$ une variable booléenne, c'est à dire un élément de $\{\mathbf{V}, \mathbf{F}\}$, définie telle que

$$P_{i,j,k} : \text{“}m(i,j) \stackrel{?}{=} k\text{” avec } (i,j,k) \in [\![1,4]\!]^3 \text{ ..}$$

On peut définir des contraintes logiques (des expressions logiques) pour résoudre le Sudoku. Les opérateurs ci-dessous seront définis plus tard.

$$\begin{aligned} & P_{113} \\ \wedge\ & P_{1,4,2} \\ \wedge\ & P_{2,2,4} \\ \wedge\ & P_{2,3,1} \\ & \vdots \\ \wedge\ & P_{1,2,1} \to (\neg P_{1,2,2} \wedge \neg P_{1,2,3} \wedge \neg P_{1,2,4}) \\ & \vdots \end{aligned}$$

Pour résoudre le Sudoku, on peut essayer chaque cas possible. Mais, ces possibilités sont très nombreuses.

En mathématiques, on utilise une certaine logique. Il en existe d'autre, certaines où tout est vrai, certaines où il est plus facile de montrer des théorèmes, etc. On va définir une logique ayant le moins d'opérateurs possibles.

IV.2 Syntaxe

Définition : On suppose donné un ensemble $\mathscr{P}$ de variables propositionnelles.

Définition : On définit alors l'ensemble des formules de la logique propositionnelle par induction nommée avec les règles :

- $\neg\big|^1$;
- $\wedge\big|^2$;
- $\vee\big|^2$;
- $\to\big|^2$;
- $\leftrightarrow\big|^2$;
- $\top\big|^0$;
- $\bot\big|^0$;
- $V\big|^0_{\mathscr{P}}$.

On nomme l'ensemble des formules $\mathscr{F}$.

Exemple :

$$\vee(\wedge(\to(V(P),\top(\,),\neg(\bot(\,))),\vee(\leftrightarrow(\top(\,),\top(\,)),V(r)).$$

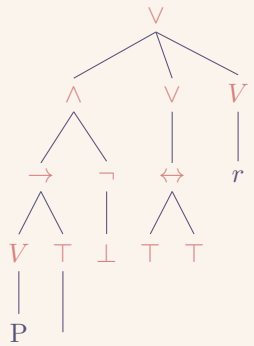


Figure 2 – Arbre syntaxique d'une expression logique

Pour simplifier la syntaxe, on écrit plutôt

$$\big((p \to \top) \wedge \neg\bot\big) \vee \big((\top \leftrightarrow \top) \vee r\big).$$

Définition (taille d'une formule) **:** On définit, par induction, la taille notée "taille" comme

$$\begin{aligned}
\text{taille} : \mathscr{F} &\longrightarrow \mathbb{N} \\
p \in \mathscr{P} &\longmapsto 1 \\
\top &\longmapsto 1 \\
\bot &\longmapsto 1 \\
\neg G &\longmapsto 1 + \text{taille}(G) \\
G \to H &\longmapsto 1 + \text{taille}(G) + \text{taille}(H) \\
G \leftrightarrow H &\longmapsto 1 + \text{taille}(G) + \text{taille}(H) \\
G \wedge H &\longmapsto 1 + \text{taille}(G) + \text{taille}(H) \\
G \vee H &\longmapsto 1 + \text{taille}(G) + \text{taille}(H).
\end{aligned}$$

Définition (Ensemble des variables propositionnelles) **:** On définit inductivement

$$\begin{aligned}
\text{vars} : \mathscr{F} &\longrightarrow \wp(\mathscr{P}) \quad {}^{1} \\
p \in \mathscr{P} &\longmapsto \{p\} \\
\top, \bot &\longmapsto \\
\neg G &\longmapsto \text{vars}(G) \\
G \odot H &\longmapsto \text{vars}(G) \cup \text{vars}(H)
\end{aligned}$$

où $\odot$ correspond à $\cup$, $\cap$, $\to$ ou $\leftrightarrow$.

Définition : On appelle *substitution* une fonction de $\mathscr{P}$ dans $\mathscr{F}$ qui est l'identité partout sauf sur un ensemble fini de variables. On la note alors

$$(p_1 \mapsto H_1, p_2 \mapsto H_2, \ldots, p_n \mapsto H_n)$$

qui est la substitution

$$\begin{aligned}
\mathscr{P} &\longrightarrow \mathscr{F} \\
p &\longmapsto \begin{cases} H_i & \text{si } p = p_i \\ p & \text{sinon.} \end{cases}
\end{aligned}$$

Exemple :
La fonction

$$\sigma = (p \mapsto p \vee q,\ r \mapsto p \wedge \top)$$

1. Le $\wp(E)$ représente ici l'ensemble des parties de E.

est une substitution. On a $\sigma(p) = p \vee q$, $\sigma(r) = p \wedge \top$, $\sigma(q) = q$ et, pour toute autre variable logique a, $\sigma(a) = a$.

Définition (Application d'une substitution à une formule) **:** Étant donné une formule $G \in \mathcal{F}$ et une substitution σ, on définit inductivement $G[\sigma]$ par

$$\begin{cases} \top[\sigma] = \top \\ \bot[\sigma] = \bot \\ p[\sigma] = \sigma(p) \\ (\neg G)[\sigma] = \neg(G[\sigma]) \\ (G \odot H)[\sigma] = (G[\sigma]) \odot H[\sigma] \end{cases}$$

où $\odot$ correspond à $\cup$, $\cap$, $\to$ ou $\leftrightarrow$.

Exemple :
Avec $G = p \wedge (q \vee \top)$ et $\sigma = (p \mapsto p,\, q \mapsto r \wedge \top)$, on a

$$G[\sigma] = q \wedge \big((r \wedge \top) \vee \bot\big).$$

Définition : On appelle parfois *clés* d'une substitution de σ, l'ensemble des variables propositionnelles sur lequel elle n'est pas l'identité.

Définition : On définit la *composée* de deux substitutions σ et σ' par

$$\begin{aligned} \sigma \cdot \sigma' : \mathcal{P} &\longrightarrow \mathcal{F} \\ p &\longmapsto \big(p[\sigma]\big)[\sigma]. \end{aligned}$$

Exemple :
Avec $\sigma = (p \mapsto q)$ et $\sigma = (q \mapsto r)$, on a

$$\sigma' \cdot \sigma = (p \mapsto r,\, q \mapsto r).$$

En effet,

$$\sigma' \cdot \sigma(x) = \begin{cases} r & \text{si } x = p \\ r & \text{si } x = q \\ x & \text{sinon.} \end{cases}$$

Exemple :

Avec $\sigma = (p \mapsto q \wedge \top)$, $\sigma' = (q \mapsto \bot,\ r \mapsto p)$, on a

$$\sigma' \cdot \sigma(x) = \begin{cases} \bot \wedge \top & \text{si } x = p \\ \bot & \text{si} x = q \\ p & \text{si } x = r \\ x & \text{sinon} \end{cases}$$
$$= (p \mapsto \bot \wedge \top,\ q \mapsto \bot,\ r \mapsto p).$$

Remarque :
L'opération $\cdot$ est associative.

Proposition : Soient σ et σ' deux substitutions, on a, pour toute formule $H \in \mathcal{F}$,

$$\big(H[\sigma]\big)[\sigma'] = H[\sigma' \cdot \sigma].$$

Preuve :
Notons P_G la propriété "$(G[\sigma])[\sigma'] = G[\sigma' \cdot \sigma]$"

Montrons que, pour toute formule $G \in \mathcal{F}$, P_G est vraie par induction :
- $\big(\top[\sigma]\big)[\sigma'] =^{(\text{def})} \top = \top[\sigma' \cdot]$
- $\big(p[\sigma]\big)[\sigma'] = p[\sigma' \cdot \sigma]$
- à faire à la maison : le cas $\neg$ et un cas $\wedge$.

□

Définition : On appelle *relation sous-formule*, la relation $\diamond$ définie dans la section 3 du chapitre -1.

IV.3 Sémantique

IV.3.1 Algèbre de Boole

Définition : On note $\mathbb{B} = \{\mathbf{V}, \mathbf{F}\}$ l'*ensemble des booléens.*

Définition : Sur $\mathbb{B}$, on définit les opérateurs

a	b	$a \cdot b$
F	**F**	**F**
F	**V**	**F**
V	**F**	**F**
V	**V**	**V**

TABLE 1 – Opération $\cdot$ sur les booléens

a	b	$a + b$
F	**F**	**F**
F	**V**	**V**
V	**F**	**V**
V	**V**	**V**

TABLE 2 – Opération $+$ sur les booléens

a	$\bar{a}$
F	**V**
V	**F**

TABLE 3 – Opération $\bar{\square}$ sur les booléens

REMARQUE :

NOM	$\cdot$	$+$
Commutativité	$a \cdot b = b \cdot a$	$a + b = b + a$
Neutre	$\mathbf{V} \cdot a = a$	$\mathbf{F} + a = a$
Absorbant	$\mathbf{F} \cdot a = \mathbf{F}$	$\mathbf{V} \cdot a = \mathbf{V}$
Associativité	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	$a + (b + c) = (a + b) + c$
Idempotence	$a \cdot a = a$	$a + a = a$
Distributivité	$a \cdot (b + c) = a \cdot b + a \cdot c$	$a + (b \cdot c) = (a + b) \cdot (a + c)$
Complémentaire	$a \cdot \bar{a} = \mathbf{F}$	$a + \bar{a} = \mathbf{V}$
MORGAN	$\overline{a \cdot b} = \bar{a} + \bar{b}$	$\overline{a + b} = \bar{a} \cdot \bar{b}$

TABLE 4 – Règles dans $\mathbb{B}$

IV.3.2 Fonctions booléennes

Définition (Environnement propositionnel) **:** On appelle *environnement propositionnel* une fonction de $\mathscr{P}$ dans $\mathbb{B}$.

Définition : On appelle *fonction booléenne* une fonction de $\mathbb{B}^{\mathscr{P}}$ dans $\mathbb{B}$. On note l'ensemble des fonctions booléennes $\mathbb{F}$.

Remarque :
Si $|\mathscr{P}| = n$, alors $\left|\mathbb{B}^{\mathscr{P}}\right| = 2^n$ et donc $|\mathbb{F}| = 2^{2^n}$.

Exemple :
La fonction

$$f : \begin{pmatrix} (p \mapsto \mathbf{F},\, q \mapsto \mathbf{F}) \mapsto \mathbf{F} \\ (p \mapsto \mathbf{F},\, q \mapsto \mathbf{V}) \mapsto \mathbf{V} \\ (p \mapsto \mathbf{V},\, q \mapsto \mathbf{F}) \mapsto \mathbf{V} \\ (p \mapsto \mathbf{V},\, q \mapsto \mathbf{V}) \mapsto \mathbf{V} \end{pmatrix} \in \mathbb{F}$$

est une fonction booléenne.

IV.3.3 Interprétation d'une formule comme une fonction booléenne

Définition (Interprétation) **:** Étant donné une formule $G \in \mathscr{F}$ et un environnement propositionnel $\rho \in \mathbb{B}^{\mathscr{P}}$, on définit l'*interprétation* de G dans l'environnement ρ par

- $[\![\top]\!]^\rho = \mathbf{V}$;
- $[\![\bot]\!]^\rho = \mathbf{F}$;
- $[\![p]\!]^\rho = \rho(p)$ où $p \in \mathscr{P}$;
- $[\![\neg G]\!]^\rho = \overline{[\![G]\!]^\rho}$;
- $[\![G \wedge H]\!]^\rho = [\![G]\!]^\rho \cdot [\![H]\!]^\rho$;
- $[\![G \vee H]\!]^\rho = [\![G]\!]^\rho + [\![H]\!]^\rho$;
- $[\![G \to H]\!]^\rho = \overline{[\![G]\!]^\rho} + [\![H]\!]^\rho$;
- $[\![G \leftrightarrow H]\!]^\rho = \left(\overline{[\![G]\!]^\rho} + [\![H]\!]^\rho\right) \cdot \left(\overline{[\![H]\!]^\rho} + [\![G]\!]^\rho\right)$.

Exemple :
Avec $\rho = (p \mapsto \mathbf{V}, q \mapsto \mathbf{F})$, et $G = (p \wedge \top) \vee (q \wedge \bot)$, on a

$$\begin{aligned} [\![G]\!]^\rho &= [\![(p \wedge \top) \vee (q \wedge \bot)]\!]^\rho \\ &= [\![p \wedge \top]\!]^\rho + [\![q \wedge \bot]\!]^\rho \\ &= [\![p]\!]^\rho \cdot [\![\top]\!]^\rho + [\![q]\!]^\rho \cdot [\![\bot]\!]^\rho \\ &= \rho(p) \cdot \mathbf{V} + \rho(q) \cdot \mathbf{F} \\ &= \mathbf{V} + \mathbf{F} \\ &= \mathbf{V}. \end{aligned}$$

Définition (Fonction booléenne associée à une formule) **:** Étant donné une formule G, on note

$$\begin{aligned} \mathbb{F} \ni [\![G]\!] : \mathbb{B}^{\mathscr{P}} &\longrightarrow \mathbb{B} \\ \rho &\longmapsto [\![G]\!]^\rho . \end{aligned}$$

Exemple :
La fonction booléenne associée à $p \vee q$ est

$$f : \begin{pmatrix} (p \mapsto \mathbf{F},\, q \mapsto \mathbf{F}) \mapsto \mathbf{F} \\ (p \mapsto \mathbf{F},\, q \mapsto \mathbf{V}) \mapsto \mathbf{V} \\ (p \mapsto \mathbf{V},\, q \mapsto \mathbf{F}) \mapsto \mathbf{V} \\ (p \mapsto \mathbf{V},\, q \mapsto \mathbf{V}) \mapsto \mathbf{V} \end{pmatrix} \in \mathbb{F}.$$

La fonction booléenne associée à $p \vee (q \wedge \top)$ est aussi f ; tout comme $(p \vee \bot) \vee (q \wedge \top)$.

IV.3.4 Liens sémantiques

Définition : On dit que G et H sont *équivalents* si et seulement si $[\![G]\!] = [\![H]\!]$. On note alors $G \equiv H$.

Définition (Conséquence sémantique) **:** On dit que H est *conséquence sémantique* de G dès lors que

$$\forall \rho \in \mathbb{B}^{\mathscr{P}},\ \big([\![G]\!]^\rho = \mathbf{V}\big) \implies \big([\![H]\!]^\rho = \mathbf{V}\big).$$

On le note $G \models H$.

Proposition : On a

$$G \equiv H \iff \big(G \models H \text{ et } H \models G\big).$$

Preuve “ $\Longrightarrow$ ” On suppose $G \equiv H$. Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. On suppose $[\![G]\!]^\rho = \mathbf{V}$ alors $[\![H]\!]^\rho = \mathbf{V}$ car $[\![G]\!] = [\![H]\!]$. On suppose maintenant $[\![H]\!]^\rho = \mathbf{V}$, et alors $[\![G]\!]^\rho = \mathbf{V}$ car $[\![G]\!] = [\![H]\!]$.
“ $\Longleftarrow$ ” On suppose $G \models H$ et $H \models G$. Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. On suppose $[\![G]\!]^\rho = \mathbf{V}$ alors $[\![H]\!]^\rho = \mathbf{V}$ car $H \models H$ et donc $[\![G]\!] = [\![H]\!]$. On suppose maintenant $[\![H]\!]^\rho = \mathbf{V}$ alors $[\![G]\!]^\rho = \mathbf{V}$ car $G \models H$. Par contraposée, si $[\![G]\!]^\rho = \mathbf{F}$, alors $[\![H]\!]^\rho = \mathbf{F}$. On en déduit que $[\![G]\!] = [\![H]\!]$.

□

Remarque :
$\models$ n’est pas une relation d’ordre.

Remarque :
La relation $\equiv$ est une relation d’équivalence. De plus, si $G \equiv G'$ et $H \equiv H'$, alors

— $G \wedge H \equiv G' \wedge H'$; — $G \vee H \equiv G' \vee H'$; — $G \to H \equiv G' \to H'$; — $G \leftrightarrow H \equiv G' \leftrightarrow H'$; — $\neg G \equiv \neg G'$.

Une telle relation est parfois appelée une *congruence*.

Définition : On dit d'une formule $H \in \mathscr{F}$ qu'elle est
- *valide* ou *tautologique* dès lors que $\forall \rho \in \mathbb{B}^{\mathscr{P}}$, $[\![H]\!]^\rho = \mathbf{V}$;
- *satisfiable* dès lors qu'il existe $\rho \in \mathbb{B}^{\mathscr{P}}$, $[\![H]\!]^\rho = \mathbf{V}$;
- *insatisfiable* dès lors qu'il n'est pas satisfiable.

On dit de $\rho \in \mathbb{B}^{\mathscr{P}}$ tel que $[\![H]\!]^\rho = \mathbf{V}$ que ρ est un *modèle* de H.

Exemple : — $p \vee \neg p$ est une tautologie. En effet, soit $\rho \in \mathscr{B}^{\mathscr{P}}$, on a

$$[\![p \vee \neg p]\!]^\rho = [\![p]\!]^\rho + \overline{[\![p]\!]^\rho} = \mathbf{V}.$$

— p est satisfiable mais non valide. En effet,

$$[\![p]\!]^{(p \mapsto \mathbf{V})} = \mathbf{V} \qquad \text{et} \qquad [\![p]\!]^{(p \mapsto \mathbf{F})} = \mathbf{F}.$$

— $p \wedge \neg p$ est insatisfiable. En effet, soit $\rho \in \mathbb{B}^{\mathscr{P}}$, on a

$$[\![p \wedge \neg p]\!]^\rho = [\![p]\!]^\rho \cdot \overline{[\![p]\!]^\rho} = \mathbf{F}.$$

Définition : Si Γ est un ensemble de formules, on écrit $\Gamma \models H$ pour dire que

$$\forall \rho \in \mathbb{B}^{\mathscr{P}}, (\forall G \in \Gamma, [\![G]\!]^\rho = \mathbf{V}) \implies [\![H]\!]^\rho = \mathbf{V}.$$

Remarque :
Si Γ est fini, alors on a

$$\Gamma \models H \iff \Big(\bigwedge_{G \in \Gamma} G \Big) \models H.$$

On doit faire la preuve, pour $n \geqslant 1$,

$$\{G_1, G_2, \ldots, G_n\} \models H \iff (\cdots((G_1 \wedge G_2) \wedge G_3) \cdots \wedge G_n) \models H.$$

IV.4 Le problème Sat – Le problème Validité

On définit le problème Sat comme ayant pour donnée une formule H et pour question "H est-elle satisfiable ?" et le problème Valide comme ayant pour donnée une formule H et pour question "H est-elle valide ?"

IV.4.1 Résolution par tables de vérité

a	b	c	$a \wedge b$	$\neg b$	$\neg c$	$\neg b \vee \neg c$	$(a \wedge b) \rightarrow (\neg b \vee \neg c)$
V	**V**	**V**	**V**	**F**	**F**	**F**	**F**
V	**F**	**V**	**F**	**V**	**F**	**V**	**V**
V	**F**	**F**	**F**	**V**	**V**	**V**	**V**
V	**V**	**F**	**V**	**F**	**V**	**V**	**V**
F	**V**	**V**	**F**	**F**	**F**	**F**	**V**
F	**F**	**V**	**F**	**V**	**F**	**V**	**V**
F	**F**	**F**	**F**	**V**	**V**	**V**	**V**
F	**V**	**F**	**V**	**F**	**V**	**V**	**V**

TABLE 5 – Table de vérité de $(a \wedge b) \rightarrow (\neg b \vee \neg c)$

EXEMPLE :

Le problème SAT lit la colonne résultat, on cherche un **V**. Le problème Valide lit la colonne résultat et vérifie qu'il n'y a que des **V**.

REMARQUE :
Deux formules sont équivalent si et seulement si elles ont la même colonne résultat.

On essaie d'énumérer toutes les possibilités : si $|\mathscr{P}| = n \in \mathbb{N}$, alors le nombre de classes d'équivalences pour $\equiv$ est au plus 2^{2^n}. On cherche donc un meilleur algorithme.

IV.5 Représentation des fonction booléennes

IV.5.1 Par des formules ?

p	q	r	S
F	**F**	**F**	**V**
F	**F**	**V**	**F**
F	**V**	**F**	**F**
F	**V**	**V**	**V**
V	**F**	**F**	**V**
V	**F**	**V**	**F**
V	**V**	**F**	**V**
V	**V**	**V**	**F**

TABLE 6 – Table de vérité d'une formule inconnue

On regarde les cas où la sortie est **V** et on crée une formule permettant de tester cette combinaison de p, q et r uniquement. On unie toutes ces formules par des

$\vee$. Dans l'exemple ci-dessus, on obtient

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r).$$

Théorème : Soit $f : \mathbb{B}^{\mathscr{P}} \to \mathbb{B}$ une fonction booléenne avec $\mathscr{P}$ fini. Il existe une formule $H \in \mathscr{F}$ telle que $[\![H]\!] = f$.

Avant de prouver ce théorème, on démontre d'abord les deux lemme suivants et on définit lit_ρ.

Définition : Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. On définit

$$\mathrm{lit}_\rho(p) = \begin{cases} p & \text{si } \rho(p) = \mathbf{V}; \\ \neg p & \text{sinon.} \end{cases}$$

Lemme :

$$\forall \rho \in \mathbb{B}^{\mathscr{P}}, \exists G \in \mathscr{F}, \left(\forall \rho' \in \mathbb{B}^{\mathscr{P}}, [\![G]\!]^{\rho'} = \mathbf{V} \iff \rho = \rho'\right).$$

On prouve ce lemme :

Preuve :
$\mathscr{P}$ est fini. Notons donc $\mathscr{P} = \{p_1, \ldots, p_n\}$ ses variables. Soit alors $\rho \in \mathbb{B}^{\mathscr{P}}$, on définit

$$H_\rho = \bigwedge_{i=1}^{n} \mathrm{lit}_\rho(p_i).$$

Montrons que $[\![H_\rho]\!]^{\rho'} = \mathbf{V} \iff \rho = \rho'$. Soit $\rho' \in \mathbb{B}^{\mathscr{P}}$.

— Si $\rho = \rho'$, alors

$$\begin{aligned} [\![H_\rho]\!]^{\rho'} &= \Big[\!\Big[\bigwedge_{i=1}^{n} \mathrm{lit}_\rho(p_i) \Big]\!\Big]^{\rho'} \\ &= \bigbullet_{i=1}^{n} [\![\mathrm{lit}_\rho(p_i)]\!]^{\rho'} \end{aligned}$$

Soit $i \in [\![1, n]\!]$. Si $\rho(p_i) = \mathbf{V}$ alors $\rho'(p_i) = \mathbf{V}$, or, $\mathrm{lit}_\rho(p_i) = p_i$ et donc $[\![\mathrm{lit}_\rho(p_i)]\!]^{\rho'} = [\![p_i]\!]^{\rho'} = \mathbf{V}$; sinon si $\rho(p_i) = \mathbf{F}$, alors $\rho'(p_i) = \mathbf{F}$, or, $\mathrm{lit}_\rho(p_i) = \neg p_i$ et donc

$$[\![\mathrm{lit}_\rho(p_i)]\!]^{\rho'} = [\![\neg p_i]\!]^{\rho'} = [\![p_i]\!]^{\rho'} = \rho'(p_i) = \bar{\mathbf{F}} = \mathbf{V}.$$

et comme ceci étant vrai pour tout $i \in [\![1, n]\!]$, on a

$$\bigbullet_{i=1}^{n} [\![\mathrm{lit}_\rho(p_i)]\!]^{\rho'} = \mathbf{V}.$$

— Sinon ($\rho \neq \rho'$), soit donc $p_i \in \mathscr{P}$ tel que $\rho(p_i) \neq \rho'(p_i)$. Si $\rho(p_i) = \mathbf{V}$ alors $\rho'(p_i) = \mathbf{F}$ et donc $\mathrm{lit}_\rho(p_i) = p_i$ et $[\![\mathrm{lit}_\rho\, p_i]\!]^{\rho'} = \rho'(p_i) = \mathbf{F}$; sinon si $\rho(p_i) = \mathbf{F}$, alors $\rho'(p_i) = \mathbf{V}$ et donc $\mathrm{lit}_\rho(p_i) = \neg p_i$ et $[\![\mathrm{lit}_\rho(p_i)]\!]^{\rho'} = [\![\neg p_i]\!]^{\rho'} = \overline{[\![p_i]\!]^{\rho'}} = \bar{\mathbf{V}} = \mathbf{F}$.

On en déduit donc que

$$[\![H_\rho]\!]^{\rho'} = \bigbullet_{j=1}^{n} [\![\mathrm{lit}_\rho(p_j)]\!]^{\rho'} = \mathbf{F}$$

car il existe $i \in [\![1, n]\!]$ tel que $[\![\mathrm{lit}_\rho(p_i)]\!]^{\rho'} = \mathbf{F}$. □

On peut donc maintenant prouver le théorème :

Lemme : Considérons alors la formule

$$H = \bigvee_{\substack{\rho \in \mathbb{B}^{\mathscr{P}} \\ f(\rho) = \mathbf{V}}} H_\rho.$$

On a $[\![H]\!] = f$.

Preuve : — Soit $\rho \in \mathbb{B}^{\mathscr{P}}$ tel que $f(\rho) = \mathbf{V}$, on a donc

$$[\![H]\!]^\rho = \Big[\!\Big[\bigvee_{\substack{\rho' \in \mathbb{B}^{\mathscr{P}} \\ f(\rho') = \mathbf{V}}} H_{\rho'} \Big]\!\Big]^\rho.$$

H_ρ apparaît donc dans cette disjonction. Or, $[\![H_\rho]\!] = \mathbf{V}$ et donc $[\![H]\!]^\rho = \mathbf{V}$.

Si $f(\rho) = \mathbf{F}$, alors on a vu que $\forall \rho'$ tel que $f(\rho') = \mathbf{V}$, alors $\rho' \neq \rho$ et donc $[\![H_{\rho'}]\!]^\rho = \mathbf{F}$ et donc

$$\Big[\!\Big[\bigvee_{\substack{\rho' \in \mathbb{B}^{\mathscr{P}} \\ f(\rho') = \mathbf{V}}} H_{\rho'} \Big]\!\Big] = \mathbf{F}.$$

Finalement $[\![H]\!] = f$.

□

Le théorème est prouvé directement à l'aide des deux lemmes précédents.

On connaît donc la réponse à la question du nom de ce paragraphe, à savoir "peut-on représenter les fonctions booléennes par des formules ?" Oui.

IV.5.2 Par des formules sous formes normales ?

Définition : On dit d'une formule de la forme

- p ou $\neg p$ avec $p \in \mathcal{P}$, que c'est un *littéral* ;
- $\bigwedge_{i=1}^{n} \ell_i$ où les ℓ_i sont des littéraux que c'est une *clause conjonctive* ;
- $\bigvee_{i=1}^{n} \ell_i$ où les ℓ_i sont des littéraux que c'est une *clause disjonctive* ;
- $\bigwedge_{i=1}^{n} D_i$ où les D_i qui sont des clauses disjonctives est appelée une *forme normale conjonctive* ;
- $\bigvee_{i=1}^{n} C_i$ où les C_i qui sont des clauses conjonctives est appelée une *forme normale disjonctive*.

Remarque :
On prend, comme convention, que $\bigwedge_{i=1}^{0} G_i = \top$ et $\bigvee_{i=1}^{0} G_i = \bot$.

Exemple :
La formule $\overbrace{(p \wedge \neg q)}^{\text{clause conjonctive}} \vee \overbrace{(r \wedge p)}^{\text{clause conjonctive}}$ est donc une clause normale disjonctive.

Remarque :
On écrit FMD pour une forme normale disjonctive et FNC pour une forme normale conjonctive.

Exemple :
La formule $p \wedge q \wedge \neg r$ est une clause conjonctive donc une FNC mais c'est aussi une FND.

Exemple :
La formule $\top$ est une clause conjonctive de taille 0, donc c'est une FND. Mais, c'est aussi une clause conjonctive de taille 0, donc c'est une FNC. De même, la formule $\bot$ est une FNC et une FND.

Théorème : Toute formule est équivalente à une formule sous FND et à une formule sous FNC.

Preuve :
Soit $G \in \mathcal{F}$ une formule. Soit $[\![G]\!]$ la fonction booléenne associée à G. Alors, par le théorème précédent, il existe une formule H telle que $[\![H]\!] = [\![G]\!]$ (i.e. $H \equiv G$) avec H construit dans la preuve précédente sous forme normale disjonctive. □

Exemple :
La formule $G = p \wedge (\neg q \vee p)$ a pour table de vérité la table suivante.

p	q	$[\![G]\!]$
F	**F**	**F**
F	**V**	**F**
V	**F**	**V**
V	**V**	**V**

Table 7 – Table de vérité de $p \wedge (\neg q \vee p)$

La forme normale disjonctive équivalente à G est $(p \wedge \neg q) \vee (p \wedge q)$.

Nous n'avons pas encore prouvé la deuxième partie du théorème mais, on essaie de trouver une formule sous fnc :

Exemple :
On reprend l'exemple de la table de vérité d'une fonction inconnue.

p	q	r	f	$\bar{f}$
F	**F**	**F**	**V**	**F**
F	**F**	**V**	**F**	**V**
F	**V**	**F**	**F**	**V**
F	**V**	**V**	**V**	**F**
V	**F**	**F**	**V**	**F**
V	**F**	**V**	**F**	**V**
V	**V**	**F**	**V**	**F**
V	**V**	**V**	**F**	**V**

Table 8 – Table de vérité d'une formule inconnue (2)

On analyse la formule $\bar{f}$ au lieu de f. Grâce à la première partie du théorème (et de la méthode pour générer cette fnd), on a

$$\bar{f} = (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r).$$

Et, à l'aide des lois de De Morgan, on a

$$\bar{f} = (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee \neg r),$$

ce qui est une fnc.

À l'aide de cet algorithme, on prouve facilement la $2^{\underline{\text{nde}}}$ partie du théorème.

Remarque :
Il est en fait possible de transformer une formule en fnd en appliquant les règles suivantes à toutes les sous-formules jusqu'à obtention d'un point fixe.

— $\neg\neg H \rightsquigarrow H$;
— $\neg(G \wedge H) \rightsquigarrow G \vee H$;
— $\neg(G \vee H) \rightsquigarrow G \wedge H$;
— $(G \vee H) \wedge I \rightsquigarrow (G \wedge I) \vee (H \wedge I)$;
— $I \wedge (G \vee H) \rightsquigarrow (I \wedge G) \vee (I \wedge H)$;

— $H \wedge \top \rightsquigarrow H$;
— $\top \wedge H \rightsquigarrow H$;
— $H \vee \bot \rightsquigarrow H$;
— $\bot \vee H \rightsquigarrow H$;
— $\neg\top \rightsquigarrow \bot$;
— $\bot \wedge H \rightsquigarrow \bot$;
— $H \wedge \bot \rightsquigarrow \bot$;
— $\neg\bot \rightsquigarrow \top$;
— $\top \vee H \rightsquigarrow \top$;
— $H \vee \top \rightsquigarrow \top$.

Proposition : Soit $n \geqslant 2$ et H_n la formule $H_n = (a_1 \vee b_1) \wedge (a_2 \vee b_2) \wedge \cdots \wedge (a_n \vee b_n)$ avec $\mathcal{P}_n = \{a_1, b_1, a_2, b_2, \ldots, a_n, b_n\}$. Alors, par application de l'algorithme précédent on obtient

$$\bigvee_{P \in \wp([\![1,n]\!])} \left(\bigwedge_{j=1}^{n} \begin{cases} a_j \text{ si } j \in P \\ b_j \text{ sinon} \end{cases} \right).$$

À faire :

Preuve (par récurrence) *:*

□

Remarque :
Qu'en est-il du problème Sat ? Le problème est-il simplifié pour les fnd ou les fnc ?

Oui, pour les fnd, le problème se simplifie. On considère, par exemple, la formule

$$\begin{array}{ll} & (\ell_{11} \wedge \ell_{12} \wedge \cdots \wedge \ell_{1,n_1}) \\ \vee & (\ell_{21} \wedge \ell_{22} \wedge \cdots \wedge \ell_{2,n_2}) \\ \vdots & \qquad\qquad \vdots \\ \vee & (\ell_{m,1} \wedge \ell_{m,2} \cdots \ell_{m,n_m}). \end{array}$$

On procède en suivant l'algorithme suivant : (À faire : Mettre l'algorithme à part) Pour i fixé, je lis la ligne i, puis je fabrique un environnement ρ.

Par exemple, pour $(p \wedge \neg q \wedge r \wedge \neg p) \vee (q \wedge r \wedge \neg q) \vee (p \wedge r)$, on a $\rho = (p \mapsto \mathbf{V}, r \mapsto \mathbf{V})$.

On en conclut que Sat peut être résolu en temps linéaire dans le cas d'une forme normale disjonctive. Le problème est de construire cette fnd.

Remarque :
Après s'être intéressé au problème Sat, on s'intéresse au problème Valide.

Par exemple, on considère la formule $(p \vee q \vee \neg r \vee \neg p) \wedge (p \vee \neg r \vee p \vee r) \wedge (q \vee r)$. On peut construire $\rho = (q \mapsto \mathbf{F}, r \mapsto \mathbf{F})$ est tel que $[\![H]\!]^\rho = \mathbf{F}$.

Si on ne peut pas construire un tel environnement propositionnel, la formule vérifie le problème Valide.

On en conclut que Valide peut être résolu en temps linéaire dans le cas d'une forme normale conjonctive. Le problème est de construire cette FNC.

IV.6 Algorithme de Quine

L'objectif de cet algorithme est de résoudre le problème SAT. On commence par poser quelques lemmes, puis on donne l'algorithme.

REMARQUE :
Une forme normale peut être vue comme un ensemble d'ensembles de littéraux (c'est la représentation que nous allons utiliser en OCamL).

EXEMPLE :

L'ensemble $\big\{\{p,q\},\{p,r\},\big\}$, a pour formule sous FNC associée $(p \vee \neg q) \wedge (q \vee r) \wedge \bot$.

L'ensemble $\big\{\{p,\neg q\},\{q,r\},\big\}$ a pour formule sous FND associée $(p \wedge \neg q) \vee (q \wedge r) \vee \top$.

L'ensemble a pour formule sous FNC associée $\top$.

L'ensemble a pour formule sous FND associée $\bot$.

Lemme : Pour toute formule H, pour tout variable propositionnelle p et pour tout environnement propositionnel ρ, tel que $\rho(p) = \mathbf{V}$, alors

$$\Big[\!\Big[H[p \mapsto \top]\Big]\!\Big]^{\rho} = [\![H]\!]^{\rho}.$$

Preuve (par induction sur les formules) *:* — Si $H = p$, avec $p \in \mathscr{P}$, alors

$$\Big[\!\Big[H[p \mapsto \top]\Big]\!\Big]^{\rho} = [\![\top]\!]^{\rho} = \mathbf{V} = [\![H]\!]^{\rho}.$$

— Si $H = \top$, alors $H[p \mapsto \top] = H$.
— Si $H = \neg H_1$ tel que $\Big[\!\Big[H_1[p \mapsto \top]\Big]\!\Big]^{\rho} = [\![H_1]\!]^{\rho}$, alors,

$$\begin{aligned}
\Big[\!\Big[H[p \mapsto \top]\Big]\!\Big]^{\rho} &= \Big[\!\Big[\neg\big(H_1[p \mapsto \top]\big)\Big]\!\Big]^{\rho} \\
&= \overline{\Big[\!\Big[H_1[p \mapsto \top]\Big]\!\Big]^{\rho}} \\
&= \overline{[\![H_1]\!]^{\rho}} \\
&= [\![\neg H_1]\!]^{\rho} \\
&= [\![H]\!]^{\rho}.
\end{aligned}$$

— Si $H = H_1 \wedge H_2$ avec H_1 et H_2 vérifiant l'hypothèse d'induction, alors

$$\begin{aligned}\Big[\!\Big[H[p \mapsto \top]\Big]\!\Big]^\rho &= \Big[\!\Big[\big(H_1[p \mapsto \top]\big) \wedge \big(H_2[p \mapsto \top]\big)\Big]\!\Big]^\rho \\ &= \Big[\!\Big[H_1[p \mapsto \top]\Big]\!\Big]^\rho \cdot \Big[\!\Big[H_2[p \mapsto \top]\Big]\!\Big]^\rho \\ &= [\![H_1]\!]^\rho \cdot [\![H_2]\!]^\rho \\ &= [\![H_1 \wedge H_2]\!]^\rho.\end{aligned}$$

□

Remarque :
Le résultat reste vrai en remplaçant **V** par **F** et $\top$ par $\bot$.

Lemme : Pour toute formule H, et pour toute variable propositionnelle p, H est satisfiable si, et seulement si $H[p \mapsto \top]$ est satisfiable ou $H[p \mapsto \bot]$ est satisfiable.

Preuve " $\Longrightarrow$ " Soit $H \in \mathscr{F}$ une formule satisfiable. Il existe donc un environnement propositionnel ρ défini sur $\text{vars}(H)$ tel que $[\![H]\!]^\rho = \mathbf{V}$.

— Si $\rho(p) = \mathbf{V}$, alors $\Big[\!\Big[H[p \mapsto \top]\Big]\!\Big]^\rho = \mathbf{V}$, d'après le lemme précédent. Donc, $H[p \mapsto \top]$ est satisfiable.

— Sinon, $\rho(p) = \mathbf{F}$ et donc, d'après le lemme précédent, $\Big[\!\Big[H[p \mapsto \bot]\Big]\!\Big]^\rho = \mathbf{V}$. La formule $H[p \mapsto \bot]$ est satisfiable.

" $\Longleftarrow$ " Supposons $H[p \mapsto \top]$ satisfiable. Il existe donc un environnement propositionnel μ défini sur $\text{vars}(H[p \mapsto \top])$ tel que $[\![H[p \mapsto \top]]\!]^\mu = \mathbf{V}$. Or, $\text{vars}(H[p \mapsto \top]) = \text{vars}(H) \setminus \{p\}$. On peut donc étendre μ en

$$\begin{aligned}\rho : \text{vars}(H) &\longrightarrow \mathbb{B} \\ x &\longmapsto \begin{cases}\mu(x) & \text{si } x \neq p \\ \mathbf{V} & \text{sinon.}\end{cases}\end{aligned}$$

Ainsi, $[\![H]\!]^\mu = [\![H[p \mapsto \top]]\!]^\rho = [\![H]\!]^\rho$ car $p \notin \text{vars}(H[p \mapsto \top])$.

□

Lemme : Une formule sans variables est

— satisfiable si et seulement si elle est équivalente à $\top$;

— insatisfiable si et seulement si elle est équivalente à $\bot$;

```
1 type formule =
2   | Top | Bot
```

```
  | Var   of string
  | Not   of formule
  | And   of formule * formule
  | Or    of formule * formule
  | Imply of formule * formule
  | Equiv of formule * formule

let substitution (f: formule) (x: string) (g: string): formule =
  ⟨code déjà fait en TP⟩

exception Found of string (* arret de la boucle *)
let get_var (f: formule): string option =
  let rec aux (f: formule): unit =
    match f with
    | Top | Bot      -> ()
    | Var(y)         -> raise(Found(y))
    | Not(f1)        -> aux f1
    | And(f1, f2)
    | Or(f1, f2)
    | Imply(f1, f2)
    | Equiv(f1, f2)  -> (aux f1; aux f2)
  in try
    aux f;
    None
  with
  | Found(y) -> Some(y)

let rec test_equiv (f: formule): bool option =
  match f with
  | Var(_) -> None
  | Top    -> Some(true)
  | Bot    -> Some(false)
  | Not(h) ->
            begin
              match test_equiv h with
              | None    -> None
              | Some(b) -> Some(not b)
            end
  | And(h1, h2) ->
            begin
              match test_equiv h1, test_equiv h2 with
              | Some(false), _ | _, Some(false) -> Some(false)
              | Some(true), Some(true)          -> Some(true)
              | _                               -> None
            end
  | Or(h1, h2) ->
            begin
              match test_equiv h1, test_equiv h2 with
              | Some(true), _ | _, Some(true) -> Some(true)
              | Some(false), Some(false)      -> Some(true)
              | _                             -> None
            end
  | Imply(h1, h2) ->
            begin
              match test_equiv h1, test_equiv h2 with
              | Some(false), _
```

```
59              | Some(true), Some(true)       -> Some(
                    ↪ true)
60              | Some(true), Some(false)      -> Some(
                    ↪ false)
61              | _                            -> None
62            end
63    | Equiv(h1, h2) ->
64            begin
65              match test_equiv h1, test_equiv h2 with
66              | Some(true), Some(true)
67              | Some(false), Some(false)     -> Some(
                    ↪ true)
68              | Some(true), Some(false)
69              | Some(false), Some(true)      -> Some(
                    ↪ false)
70              | _                            -> None
71            end
72
73  let rec quine (f: formule): bool =
74    match get_var f, test_equiv f with
75    | _, Some(b)     -> b
76    | None, _        -> failswith "cas impossible"
77    | Some(p), None -> ?
```

CODE 1 – Algorithme de QUINE *version zéro*

REMARQUE :
Dans la suite, on s'intéresse aux formules sous forme CNF. Une CNF (ou même une DNF) peut être représentée au moyen d'un ensemble d'ensemble de littéraux. Ces ensembles sont finis. Par exemple, la formule $(p \vee \neg q) \wedge (r \vee p \vee p)$ est représenté par

$$\big\{\{p, \neg q\}, \{r, p\}\big\}.$$

Algorithme 0.1 Algorithme *Assume*

Entrée G une CNF, p une variable propositionnelle, et $b \in \mathbb{B}$.
Sortie Une CNF équivalente à $G[p \mapsto b]$.

```
1 : Soit ℓ_V le littéral p si b = V, ¬p sinon.
2 : Soit ℓ_F le littéral ¬p si b = V, p sinon.
3 : pour C ∈ G faire
4 :     si ℓ_V ∈ C alors
5 :         On retire C de G.
6 :     sinon
7 :         si ℓ_F ∈ C alors
8 :             On retire ℓ_F de C.
```

On peut donc donner l'algorithme de QUINE final :

Algorithme 0.2 Algorithme de QUINE

Entrée Une CNF G

```
1 : si G =  alors
2 :     retourner OUI
3 : sinon
4 :     si  ∈ G alors
5 :         retourner NON
6 :     sinon si ∃{ℓ} ∈ G alors
7 :         si ℓ = p, avec p ∈ vars(G) alors
8 :             QUINE(Assume(G, p, V))
9 :         sinon si ℓ = ¬p, avec p ∈ vars(G)  alors
10 :            QUINE(Assume(G, p, F))
11 :    sinon
12 :        p ← h(G)
13 :        On essaie QUINE(Assume(G, p, V))
14 :        On essaie QUINE(Assume(G, p, F))
```

IV.7 Synthèse du chapitre

— Formules —

On définit l'ensemble des formules $\mathscr{F}$ par induction nommé avec les règles

- $\neg\big|^1$;
- $\wedge\big|^2$;
- $\vee\big|^2$;
- $\to\big|^2$;
- $\leftrightarrow\big|^2$;
- $\top\big|^0$;
- $\bot\big|^0$;
- $V\big|^0_{\mathscr{P}}$.

On définit inductivement taille(F), pour $F \in \mathscr{F}$, la taille de cette formule, *i.e.* le nombre d'opérateurs dans cette formule. On définit également l'ensemble des variables vars(F) d'une formule $F \in \mathscr{F}$.

Une *substitution* est une fonction de $\mathscr{P}$ dans $\mathscr{F}$, où elle est l'identité partout, sauf en nombre fini de variables, alors nommés *clés* de cette substitution. On note $F[\sigma]$ l'application d'une substitution σ à une formule $F \in \mathscr{F}$. On définit la composée de deux substitutions $\sigma \cdot \sigma'$, comme $\sigma \cdot \sigma' : p \mapsto (p[\sigma])[\sigma']$, cela ne correspond pas à la définition mathématique d'une composition de fonctions.

— Fonctions booléennes —

Un *environnement propositionnel* est une fonction de $\mathscr{P}$ dans $\mathbb{B}$. Une *fonction booléenne* est une fonction de $\mathbb{B}^{\mathscr{P}}$ dans $\mathbb{B}$. L'ensemble $\mathbb{F}$ est l'ensemble des fonctions booléennes.

On définit inductivement l'*interprétation* d'une formule $F \in \mathscr{F}$ dans un environment ρ. On note ce booléen $[\![F]\!]^\rho$. On note également $[\![F]\!]$ l'application $\rho \mapsto [\![F]\!]^\rho$.

— Liens sémantiques —

On note $G \equiv H$ si, et seulement si $[\![G]\!] = [\![H]\!]$. On note $G \models H$ dès lors que, pour $\rho \in \mathbb{B}^{\mathscr{P}}$, si $[\![G]\!]^\rho = \mathbf{V}$, alors $[\![H]\!]^\rho = \mathbf{V}$. On étend cette définition pour un ensemble Γ de formules G. On a $G \equiv H$ si, et seulement si $G \models H$ et $H \models G$.

Une formule *valide* ou *tautologique* est une formule dont l'interprétation vaut toujours $\mathbf{V}$, peu importe l'environnement propositionnel. Une formule satisfiable est une formule dont l'interprétation vaut $\mathbf{V}$, pour un certain environnement propositionnel. Si $\rho \in \mathbb{B}^{\mathscr{P}}$ vérifie $[\![F]\!]^\rho = \mathbf{V}$, on dit que ρ est un *modèle* de F.

Chapitre 1

Langages réguliers et Automates

IV.1 Motivation

IV.1.1 1ère motivation

Il y a une grande différence entre les mathématiques et l'informatique : la gestion de l'infini. On n'a pas de mémoire infinie sur un ordinateur. Par exemple, pour représenter π ou $\sqrt{2}$, on ne peut pas stocker un nombre infini de décimales. Ce n'est pas une question de base, ces nombres ont aussi des décimales infinies dans une base 2.

Par exemple, si on ne veut utiliser $\sqrt{2}$ seulement pour plus tard le mettre au carré. On peut définir une structure en `C` comme celle qui suit

```c
typedef struct {
  int carre;
  bool sign;
};
```

Code 1.1 – $\sqrt{2}$ sous forme de structure

On a pu décrire $\sqrt{2}$ comme cela car il y a une certaine régularité dans ce nombre.

On définit des relations entre ces objets. Dans ce chapitre, on va commencer par étudier autre chose : les mots. Les mots sont utilisés, tout d'abord, pour entrer une liste de lettres mais aussi le programme lui-même. En effet, il y a une liste infinie de code possibles en `C`.

IV.1.2 2nde motivation

Les ordinateurs sont complexes ; il peut être dans une multitude d'états. On représente une succession de tâches (le symbole 🔵 représente une tâche) :

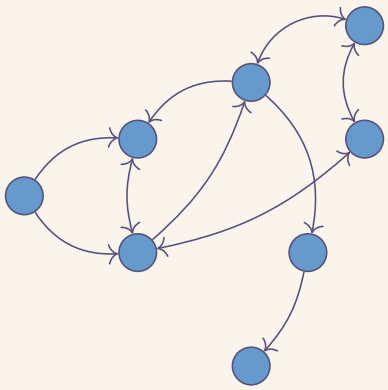


FIGURE 1.1 – États d'un ordinateur

Par exemple, pour une boucle infinie, on a un cycle dans le graphe ci-dessus. Ou, s'il atteint un certain nœud, on a un *bug*.

Mais, pour résoudre ce problème, on peut forcer le nombre d'état d'un ordinateur ; par exemple, dire qu'un ordinateur a 17 états.

On décide donc de représenter mathématiquement un ordinateur afin de pouvoir faire des preuves avec. Et, c'est l'objet de ce chapitre.

IV.2 Mots et langages, rappels

Définition : On appelle *alphabet* un ensemble fini, d'éléments qu'on appelle *lettres*.

Définition : On appelle une *mot* sur Σ (où Σ est un alphabet) une suite finie de lettres de Σ.

La *longueur* d'un mot est le nombre de lettres, comptées avec leurs multiplicité. On la note $|w|$ pour un mot w. Si $|w| = n \in \mathbb{N}^\star$, on indexe les lettres de w pour $(w_i)_{i\in[\![1,n]\!]}$ et on écrit alors

$$w = w_1 w_2 w_3 \dots w_n.$$

Il existe un unique mot de longueur 0 appelé *mot vide*, on le note ε.

Définition : Si Σ est un alphabet, on note

- Σ^n les mots de longueur n ;
- $\Sigma^\star$ les mots de longueurs positives ou nulle ;
- Σ^+ les mots de longueurs strictement positives.

Remarque :

$$\Sigma^\star = \bigcup_{n\in\mathbb{N}} \Sigma^n \qquad \Sigma^+ = \bigcup_{n\in\mathbb{N}^\star} \Sigma^n.$$

Définition : Soit Σ un alphabet. Soit x et y deux mots de $\Sigma^\star$. Notons

$$x = x_1x_2x_3\dots x_n$$
$$y = y_1y_2y_3\dots y_n.$$

On définit alors *concaténation* notée $x \cdot y$ l'opération définie comme

$$x \cdot y = x_1x_2x_3\dots x_ny_1y_2\dots y_n.$$

Remarque : — $\cdot$ est une opération interne ;
— ε est neutre pour $\cdot$: $\forall n \in \Sigma^\star,\ \varepsilon \cdot x = x \cdot \varepsilon = x.$
— $\cdot$ est associatif.

(On dit que c'est un monoïde.)

Remarque :
L'opération $\cdot$ n'est pas commutative.

Définition : Soit x et y deux mots sur l'alphabet Σ. On dit que
— x est un *préfixe* de y si $\exists v \in \Sigma^\star,\ y = x \cdot v$;
— x est un *suffixe* de y si $\exists v \in \Sigma^\star,\ y = v \cdot x$;
— x est un *facteur* de y si $\exists (v,w) \in \left(\Sigma^\star\right)^2,\ y = v \cdot x \cdot w.$

Exemple : — a est facteur de aa ;
— ε est un facteur de a.

Définition : On dit que x est un *sous-mot* de y si x est une suite extraite de y. Par exemple

$$a \not b\, a\, a \not b\, a \qquad \longrightarrow \qquad a\, a\, a\, a.$$

Définition : Un *langage* est un ensemble de mots. C'est donc un élément de $\wp(\Sigma^\star)$.

Remarque (B) :
$\neq \{\varepsilon\}$.

IV.3 Langage régulier

IV.3.1 Opérations sur les langages

Remarque :
Les langages sont des ensembles. On peut donc leurs appliquer des opérations ensemblistes.

Définition : Soient $L_1, L_2 \in \wp(\Sigma^\star)$ deux langages. On définit la *concaténation* de deux langages, notée $L_1 \cdot L_2$:

$$L_1 \cdot L_2 = \{u \cdot v \mid u \in L_1,\, v \in L_2\}.$$

Remarque : — L'opération $\cdot$ (langages) a $\{\varepsilon\}$ pour neutre.
— L'opération $\cdot$ (langages) a pour élément absorbant :

$$\forall L \in \wp(\Sigma^\star),\ L \cdot = \cdot L = .$$

— L'opération $\cdot$ est distributive : soient K, L, M trois langages ; on a

$$K \cdot (L \cup M) = (K \cdot L) \cup (K \cdot M);$$
$$(L \cup M) \cdot K = (L \cdot K) \cup (M \cdot K).$$

Définition : Étant donné un langage L, on définit par récurrence :
— $L^0 = \{\varepsilon\}$;
— $L^{n+1} = L^n \cdot L = L \cdot L^n$. [1]
On note alors

$$L^\star = \bigcup_{n \in \mathbb{N}} L^n \qquad \text{et} \qquad L^+ = \bigcup_{n \in \mathbb{N}} L^n.$$

Remarque :
On a $\Sigma^\star = \Sigma^*$. On notera donc $\Sigma^\star$ dans tous les cas.

Remarque :
Si $\varepsilon \in L$, alors $L^\star = L^+$. En effet, $L^\star = L^+ \cup \{\varepsilon\}$.

Remarque :
On nomme l'application $L \mapsto L^\star$ l'*étoile de Kleene*.

Remarque :
Avec L et K deux alphabets, on a

$$|L \cdot K| \leqslant |L|\,|K|.$$

En effet, avec $K = \{a, aa\}$, on a $K^2 = \{aa, aaa, aaaa\}$.

1. La deuxième égalité est assurée par l'associativité de l'opération $\cdot$.

Exemple :
Avec $L = \{a, ab\}$, on a
- $L^1 = L$;
- $L^2 = \{aa,\ aab,\ aba\,abab\}$;
- $L^\star \supseteq \{\varepsilon,\ a,\ ab,\ aa, \ldots, aaaaaaa\ldots\}$.

Définition : Soit Σ un alphabet. On appelle *ensemble des langages réguliers*, noté LR. Le plus petit ensemble tel que
- $\subset \mathrm{LR}$;
- Si $a \in \Sigma$, alors $a \in \mathrm{LR}$;
- Si $L_1 \in \mathrm{LR}$ et $L_2 \in \mathrm{LR}$, on a $L_1 \cup L_2 \in \mathrm{LR}$;
- Si $L_1 \in \mathrm{LR}$ et $L_2 \in \mathrm{LR}$, on a $L_1 \cdot L_2 \in \mathrm{LR}$;
- Si $L \in \mathrm{LR}$, alors $L^\star \in \mathrm{LR}$.

Exemple : — Soit $\Sigma = \{t, o\}$. Est-ce que $\{toto\} \in \mathrm{LR}$? On sait déjà que $\{t\}$ et $\{o\}$ sont déjà des langages réguliers. Or,

$$\{toto\} = \{t\} \cdot \{o\} \cdot \{t\} \cdot \{o\}.$$

Et donc $\{toto\} \in \mathrm{LR}$.
- On a $\{\varepsilon\} = {}^\star \in \mathrm{LR}$.
- On a
$$\left\{ \begin{array}{cccc} x_{11} & x_{12} & \ldots & x_{1,n_1} \\ x_{21} & x_{22} & \ldots & x_{2,n_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m,1} & x_{m,2} & \ldots & x_{m,n_m} \end{array} \right\} \in \mathrm{LR}$$
car $\{x_{i,1}, x_{i,2}, \ldots, x_{i,n_i}\} \in \mathrm{LR}$ et c'est stable par union finie.
- Avec $\Sigma = \{a, b\}$, on a
$$L = \{\varepsilon,\ a,\ aa,\ aaa, \ldots\} = \underbrace{\Big(\overbrace{\{a\}}^{\in \mathrm{LR}}\Big)^\star}_{\in \mathrm{LR}}.$$
- $\Sigma^\star \in \mathrm{LR}$.
- Contre-exemple : $\{a^n \mid a \text{ premier}\} \notin \mathrm{LR}$.

IV.3.2 Expressions régulières

On représente l'ensemble vide, _|_ l'union de deux expressions régulières, _·_ la concaténation de deux expression régulières, et, _* l'étoile de Klein pour les expressions régulières.

On cherche à représenter informatiquement ces expressions à l'aide d'une règle de construction nommée.

Définition : Étant donné un alphabet Σ, on définit $\mathrm{Reg}(\Sigma)$ défini par induction nommée à partir des règles :

- $\Big|^0$;
- $\star\Big|^1$;
- $|\Big|^2$;
- $L\Big|^1_\Sigma$;
- $\cdot\Big|^2$;
- $\varepsilon\Big|^0$.

Ces règles peuvent être définies en OCamL (douteux) de la façon suivante :

```
type regex =
  |
  | |  of regex * regex
  | ·  of regex * regex
  | *  of regex
  | L of char
  | ε
```

Code 1.2 – Règles des expressions régulières en OCamL

On peut donc écrire

$$\big((^\star) \mid (a \cdot b)\big) \quad \longrightarrow \quad |(\star(()), \cdot(L(a), L(b))).$$

A-t-on $|(L(a), L(b)) \stackrel{?}{=} |(L(b), L(a))$? Non, sinon on risque d'avoir une boucle infinie au moment de l'évaluation de cette expression.

On peut simplifier la notation : au lieu d'écrire $|(\star(()), \cdot(L(a), L(b)))$, on note $^\star \mid (a \cdot b)$.

Définition : On définit

$$\begin{aligned}
\mathscr{L} : \mathrm{Reg}(\Sigma) &\longrightarrow \wp(\Sigma^\star) \\
&\longmapsto \\
a &\longmapsto \{a\} \\
\varepsilon &\longmapsto \{\varepsilon\} \\
e_1 \cdot e_2 &\longmapsto \mathscr{L}(e_1) \cdot \mathscr{L}(e_2) \\
e_1 \mid e_2 &\longmapsto \mathscr{L}(e_1) \cup \mathscr{L}(e_2) \\
e^\star &\longmapsto \mathscr{L}(e)^\star
\end{aligned}$$

Exemple :
Deux expressions régulières peuvent donner le même langage : on a $\mathscr{L}() =$ mais également $\mathscr{L}(\mid) = \mathscr{L}() \cup \mathscr{L}() = \cup = .$ De même, $\mathscr{L}\big(a \mid (b \cdot b^\star)\big) = \{a, b, bb, bbb, \ldots\} = \mathscr{L}\big((bb^\star) \mid a\big)$.

Définition : On définit sur $\mathrm{Reg}(\Sigma)$ la fonction "vars" définie comme

$$\begin{aligned}
\mathrm{vars} : \mathrm{Reg}(\Sigma) &\longrightarrow \wp(\Sigma) \\
&\longmapsto \\
\varepsilon &\longmapsto \\
a \in \Sigma &\longmapsto \{a\} \\
e_1 \cdot e_2 &\longmapsto \mathrm{vars}(e_1) \cup \mathrm{vars}(e_2) \\
e_1 \mid e_2 &\longmapsto \mathrm{vars}(e_1) \cup \mathrm{vars}(e_2) \\
e^\star &\longmapsto \mathrm{vars}(e).
\end{aligned}$$

Proposition : Un langage L est régulier si et seulement s'il existe $e \in \mathrm{Reg}(\Sigma)$ telle que $\mathscr{L}(e) = L$.

Preuve " $\Longleftarrow$ " Montrons que, pour toute expression régulière $e \in \mathrm{Reg}(\Sigma)$, P_e : "le langage $\mathscr{L}(e)$ est régulier." On procède par induction.

- $P : \mathscr{L}() = \ \in \mathrm{LR}$;
- $P_\varepsilon : \mathscr{L}(\varepsilon) = \{\varepsilon\} = {}^\star \in \mathrm{LR}$;
- Soit $a \in \Sigma$. Montrons $P_a : \mathscr{L}(a) = \{a\} \in \mathrm{LR}$;
- Soient e_1 et e_2 deux expressions régulières telles que P_{e_1} et P_{e_2} soient vrais. Montrons $P_{e_1 \cdot e_2} : \mathscr{L}(e_1 \cdot e_2) = \underset{\in \mathrm{LR}}{\mathscr{L}(e_1)} \cdot \underset{\in \mathrm{LR}}{\mathscr{L}(e_2)} \in \mathrm{LR}$
- Soient e_1 et e_2 deux expressions régulières telles que P_{e_1} et P_{e_2} soient vrais. Montrons $P_{e_1 \mid e_2} : \mathscr{L}(e_1 \mid e_2) = \underset{\in \mathrm{LR}}{\mathscr{L}(e_1)} \cup \underset{\in \mathrm{LR}}{\mathscr{L}(e_2)} \in \mathrm{LR}$

" $\Longrightarrow$ " Montrons que, pour tout langage régulier L, il existe une expression régulière e de l'alphabet Σ telle que $\mathscr{L}(e) = L$. Soit X l'ensemble des langages L tels qu'il existent une expression régulière e de l'alphabet Σ telle que $\mathscr{L}(e) = L$. On a

$$X \supseteq \underset{\mathscr{L}()}{\{\}} \cup \Big\{ \underset{\mathscr{L}(a)}{\{a\}} \;\Big|\; a \in \Sigma \Big\}.$$

De plus, si deux langages L_1 et L_2 sont dans X, alors il existent e_1 et e_2 deux expressions régulières de Σ telle que $\mathscr{L}(e_1) = L_1$ et $\mathscr{L}(e_2) = L_2$. Or, $\mathscr{L}(e_1 \mid e_2) = \mathscr{L}(e_1) \cup \mathscr{L}(e_2) = L_1 \cup L_2$ et donc $L_1 \cup L_2$.

De même pour $L_1 \cdot L_2$.

Si un langage L est dans X, alors il existe une expression régulière e d'un alphabet Σ telle que $\mathscr{L}(e) = L$, alors $\mathscr{L}(e^\star) = L^\star \in X$.

X contient les langages et $\{a\}$ (avec $a \in \Sigma$) et X est stable par $\cup$,

· et $\star$. Or, LR est défini comme le plus petit ensemble vérifiant les propriétés et donc LR $\subseteq X$.

□

Remarque (Notation) :
Les notations Reg(Σ) et Regexp(Σ) sont équivalentes.

IV.4 Automates finis (sans ε-transitions)

On considère l'automate représenté par les états suivants. L'entrée est représentée par la flèche sans nœud de départ et la sortie par celle sans nœud d'arrivée.

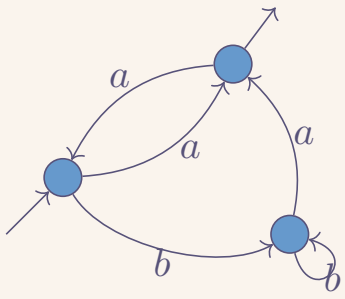


Figure 1.2 – Exemple d'automate

On représente une séquence d'état par un mot comme *aaba* (qui correspond à une séquence valide) ou *bbab* (qui n'est pas valide).

IV.4.1 Définitions

Définition : Un *automate fini* (sans ε-transition) est un quintuplet $(Q, \Sigma, I, F, \delta)$ où

- Q est un ensemble d'états ;
- Σ est son alphabet de travail ;
- $I \subseteq Q$ est l'ensemble des états initiaux ;
- $F \subseteq Q$ est l'ensemble des états finaux.
- $\delta \subseteq Q \times \Sigma \times Q$.

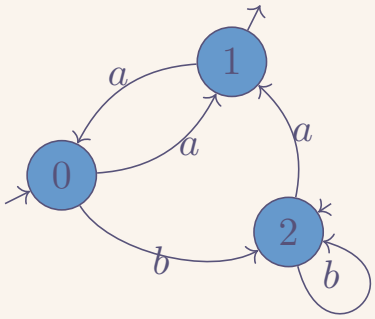


FIGURE 1.3 – Exemple d'automate (2)

EXEMPLE :
L'automate ci-dessus est donc représenté mathématiquement par

$$\Big(\underbrace{\{0,1,2\}}_{Q},\underbrace{\{a,b\}}_{\Sigma},\underbrace{\{0,2\}}_{I},\underbrace{\{1\}}_{F},\underbrace{\big\{(0,a,1),(0,b,2),(1,a,0),(2,a,1),(2,b,2)\big\}}_{\delta}\Big).$$

Définition : On dit d'une suite $(q_0, q_1, q_2, \dots, q_n) \in Q^{n+1}$ qu'elle est *une suite de transitions de l'automate* $\mathscr{A} = (Q, \Sigma, I, F, \delta)$ dès lors qu'il existe $(a_1, a_2, \dots, a_n) \in \Sigma^n$ tels que, pour out $i \in [\![1, n]\!]$, $(q_{i-1}, a_i, q_i) \in \delta$. On note parfois une telle suite de transition par

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \xrightarrow{a_3} q_3 \to \cdots \to q_n - 1 \xrightarrow{a_n} q_n.$$

EXEMPLE :
$1 \xrightarrow{a} 0 \xrightarrow{b} 2 \xrightarrow{b} 2$ est une suite de transitions de l'automate ci-avant.

Définition : On dit qu'une suite $(q_0, q_1, \dots, q_n)$ est une *exécution* dans l'automate $\mathscr{A} = (Q, \Sigma, I, F, \delta)$ si c'est une suite de transition de A telle que $q_0 \in I$. On dit également qu'elle est *acceptante* si $q_n \in F$.

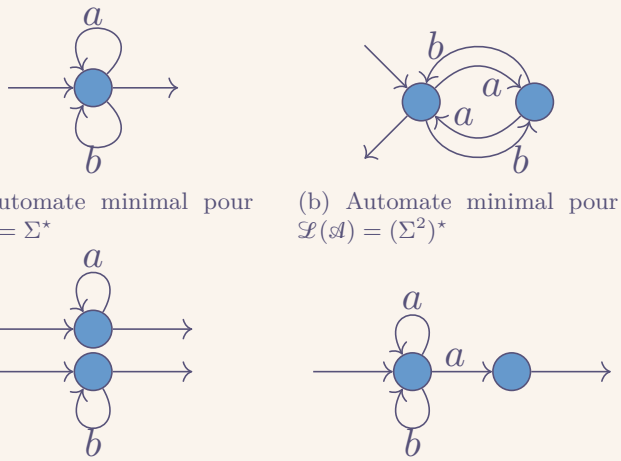
Lorsque $q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \to \cdots \to q_{n-1} \xrightarrow{a_n} q_n$ est une suite de transitions d'un automate $\mathscr{A}$, on dit que le mot $a_1 a_2 \dots a_n$ est l'*étiquette* de cette transition.

Définition (Langage reconnu par un automate) **:** On dit qu'un mot $w \in \Sigma^\star$ est *reconnu* par un automate $\mathscr{A} = (Q, \Sigma, I, F, \delta)$ s'il est l'étiquette d'une exécution acceptante de $\mathscr{A}$. On note alors $\mathscr{L}(\mathscr{A})$ l'ensemble des mots reconnus par l'automate $\mathscr{A}$.

Définition : On dit d'un langage L qu'il est *reconnaissable* s'il existe un automate $\mathscr{A}$ tel que $\mathscr{L}(\mathscr{A}) = L$. On note $\mathrm{Rec}(\Sigma)$ l'ensemble des mots reconnaissables.

Exemple :
Avec $\Sigma = \{a, b\}$, on cherche $\mathscr{A}$ tel que

— $\mathscr{L}(\mathscr{A}) = \Sigma^\star$
— $\mathscr{L}(\mathscr{A}) = (\Sigma^2)^\star$



(a) Automate minimal pour $\mathscr{L}(\mathscr{A}) = \Sigma^\star$

(b) Automate minimal pour $\mathscr{L}(\mathscr{A}) = (\Sigma^2)^\star$

(c) Automate minimal pour $\mathscr{L}(\mathscr{A}) = \{a\}^\star \cup \{b\}^\star$

(d) Automate minimal pour $\mathscr{L}(\mathscr{A}) = \Sigma^\star \cdot \{a\}$

Figure 1.4 – Automates minimaux pour différentes valeurs de $\mathscr{L}(\mathscr{A})$

Définition (Automate déterministe) **:** On dit d'un automate $\mathscr{A} = (Q, \Sigma, I, F, \delta)$ qu'il est *déterministe* si

1. $|I| = 1$;
2. $\forall (q, q_1, q_2) \in Q^3$, $\forall a \in \Sigma$, $(q, a, q_1) \in \delta$ et $(q, a, q_2) \in \delta \implies q_1 = q_2$;

Remarque :
(2) est équivalent à

$$\forall (q, a) \in Q \times \Sigma,\ \big|\{q' \in Q \mid (q, a, q') \in \delta\}\big| \leqslant 1.$$

Définition (Automate complet) **:** On dit d'un automate $\mathscr{A} = (Q, \Sigma, I, F, \delta)$ qu'il est *complet* si

$$\forall (q, a) \in Q \times \Sigma,\ \exists q' \in Q,\ (q, a, q') \in \delta.$$

Exemple :
Les automates ci-avant sont

(a) complet et déterministe ;
(b) complet et déterministe ;
(c) non complet et non déterministe ;
(d) non complet et non déterministe.

IV.4.2 Transformations en automates équivalents

On peut représenter le langage utilisé par l'automate ci-dessous avec une expression régulière : $a^\star \cdot (a \mid bab)$. L'arbre ci-dessous n'est pas déterministe. On cherche à le rendre déterministe : pour cela, on trace un arbre contenant les nœuds accédés en fonctions de l'expression lue.

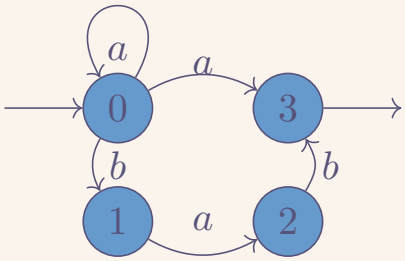


Figure 1.5 – Automate non déterministe ayant pour expression régulière $a^\star \cdot (a \mid bab)$

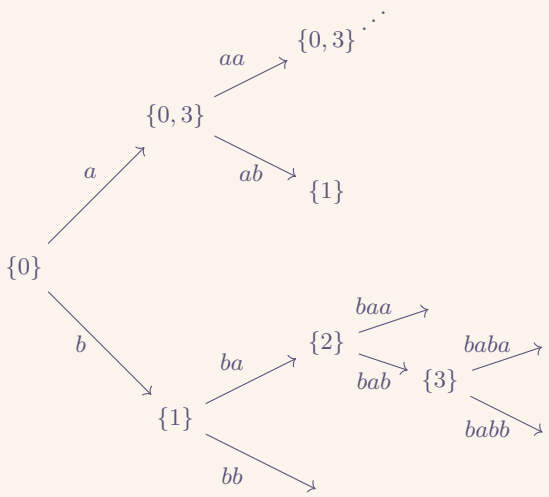


Figure 1.6 – Nœuds possibles par rapport à l'expression lue

À l'aide de cet arbre, on peut trouver un automate déterministe équivalent à l'automate précédent.

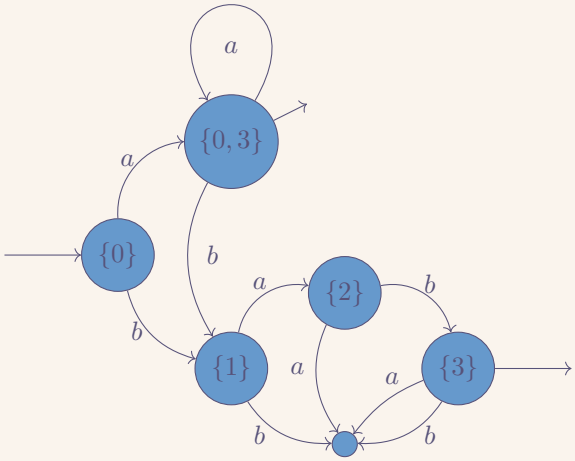


FIGURE 1.7 – Automate déterministe ayant pour expression régulière $a^\star \cdot (a \mid bab)$

Définition : On dit de deux automates $\mathscr{A}$ et $\mathscr{A}'$ qu'ils sont *équivalents* si $\mathscr{L}(\mathscr{A}) = \mathscr{L}(\mathscr{A}')$.

Théorème : Pour tout automate $\mathscr{A}$, il existe un automate déterministe $\mathscr{A}'$ tel que $\mathscr{L}(\mathscr{A}) = \mathscr{L}(\mathscr{A}')$.

Preuve :
Soit $\mathscr{A} = (\mathbb{Q}, \Sigma, I, F, \delta)$ un automate. On pose $\Sigma' = \Sigma$, $\mathbb{Q}' = \wp(\mathbb{Q})$, $I' = \{I\}$, $F = \{Q \in \wp(\mathbb{Q}) \mid Q \cap F \neq \}$ et

$$\delta' = \left\{ (Q, a, Q') \in \mathbb{Q}' \times \Sigma \times \mathbb{Q}' \;\middle|\; Q' = \left\{ q' \in \mathbb{Q} \mid \exists q \in Q,\ (q, a, q') \in \delta \right\} \right\}.$$

On pose alors l'automate $\mathscr{A}' = (\mathbb{Q}', \Sigma', I', F', \delta')$. Montrons que $\mathscr{L}(\mathscr{A}') = \mathscr{L}(\mathscr{A})$. On procède par double-inclusion.

"$\subseteq$" Soit $w \in \mathscr{L}(\mathscr{A})$. Il existe donc une exécution acceptante $I \ni q_0 \xrightarrow{w_1} q_1 \xrightarrow{w_2} q_2 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n \in F$ telle que $w = w_1 w_2 \dots w_n$. On pose $Q_0 = I$, et, pour tout entier $i \in [\![1, n]\!]$,

$$Q_i = \left\{ q' \in \mathbb{Q} \mid \exists q \in Q_{i-1},\ (q, w_i, q') \in \delta \right\}.$$

Remarquons que, pour tout entier $i \in [\![1, n]\!]$, on a $(Q_{i-1}, w_i, Q_i) \in \delta'$. On a donc $I' \ni Q_0 \xrightarrow{w_1} Q_1 \to \cdots \to Q_{n-1} \xrightarrow{w_n} Q_n$ est une exécution de $\mathscr{A}'$. Montrons que, pour tout $i \in [\![0, n]\!]$, on a $q_i \in Q_i$ par récurrence finie.

— $q_0 \in I = Q_0$.
— Soit $p < n$ tel que $q_p \in Q_p$ alors q_{p+1} est tel que $(q_p, w_{p+1}, q_{p+1}) \in \delta$ et q_{p+1} est tel qu'il existe $q \in Q_p$ tel que $(q, w_{p+1}, q_{p+1}) \in \delta$. On en déduit $q_{p+1} \in Q_{p+1}$.

On a donc $q_n \in Q_n$ et $q_n \in F$ donc $Q_n \cap F \neq$ et donc $Q_n \in F'$. L'exécution $Q_0 \xrightarrow{w_1} Q_1 \to \cdots \to Q_{n-1} \xrightarrow{w_n} Q_n$ est donc acceptante dans $\mathscr{A}'$ et donc $w = w_1 \dots w_n \in \mathscr{L}(\mathscr{A}')$.

"$\supseteq$" Soit $w \in \mathscr{L}(\mathscr{A}')$. Soit donc $I' \ni Q_0 \xrightarrow{w_1} Q_1 \to \cdots \to Q_{n-1} \xrightarrow{w_n} Q_n \in F'$ une exécution acceptante de w dans $\mathscr{A}'$. $Q_n \cap F \neq$. Soit donc $q_n \in Q_n \cap F$. Soit $q_{n-1} \in Q_{n-1}$ tel que $(q_{n-1}, w_n, q_n) \in \delta$ (par définition de $(Q_{n-1}, w_n, Q_n) \in \delta'$). " De proche en proche," il existe $q_0, q_1, \dots, q_{n-2}$ tels que, pour tout $i \in [\![1, n]\!]$, $(q_{i-1}, w_i, q_i) \in \delta$ et $q_i \in Q_i$. Or, $q_0 \in Q_0 \in I' = \{I\}$ donc $Q_0 = I$ et donc $q_0 \in I$. On rappelle que $q_n \in F$. On en déduit donc que $q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n$ une exécution acceptante da ns $\mathscr{A}$ et donc $w \in \mathscr{L}(\mathscr{A}')$.

□

Pour comprendre la construction de l'automate dans la preuve, on fait un exemple. On considère l'automate non-déterministe ci-dessous.

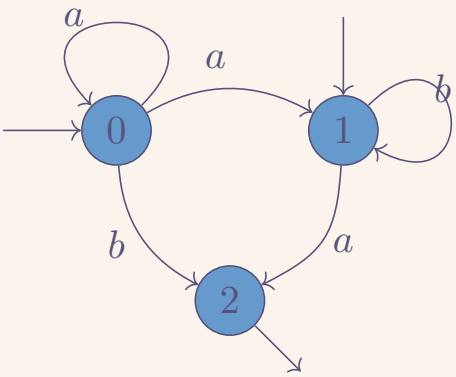


FIGURE 1.8 – Automate non déterministe

On construit la *table de transition* :

	a	b
$\{0\}$	$\{0,1\}$	$\{2\}$
$\{1\}$		

TABLE 1.1 – Table de transition de l'automate ci-avant

À faire : Finir la table de transition

REMARQUE :

L'automate $\mathcal{A}'$ construit dans le théorème précédent est complet mais son nombre de nœud suit une exponentielle.

Proposition : Soit $\mathcal{A}$ un automate fini à n états. Il existe un automate $\mathcal{A}'$ ayant $n+1$ états tel que $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}')$ avec $\mathcal{A}'$ complet.

Preuve :
Soit $\mathcal{A} = (\mathbb{Q}, \Sigma, I, F, \delta)$ un automate à n états. Soit $P \notin \mathbb{Q}$. On pose $\Sigma' = \Sigma$, $\mathbb{Q}' = \mathbb{Q} \cup \{P\}$, $I' = I$, $F' = F$ et

$$\delta' = \delta \cup \left\{ (q, \ell, P) \in \mathbb{Q}' \times \Sigma \times \{P\} \;\middle|\; \forall q' \in \mathbb{Q}',\ (q, \ell, q') \notin \delta \right\}.$$

Montrons que $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}')$. À faire : Preuve à faire

□

Définition : Soit $\mathcal{A} = (\mathbb{Q}, \Sigma, I, F, \delta)$ un automate. On dit d'un état $q \in \mathbb{Q}$ qu'il est

- *accessible* s'il existe une exécution $I \ni q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n = q$.
- *co-accessibles*'il existe une suite de transitions $q \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n \in F$.

Dans l'automate ci-dessous, l'état 0 n'est pas accessible et l'état 2 n'est pas co-accessible.

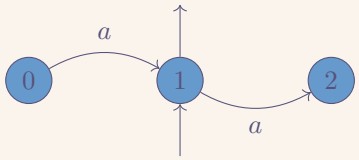


FIGURE 1.9 – Non-exemples d'états accessibles et co-accessibles

Définition : On dit d'un automate $\mathcal{A}$ qu'il est *émondé* dès lors que chaque état est accessible et co-accessible.

Proposition : Soit $\mathcal{A}$ un automate. Il existe $\mathcal{A}'$ un automate émondé tel que $\mathcal{L}(\mathcal{A}') = \mathcal{L}(\mathcal{A})$.

Preuve :
Soit $\mathscr{A} = (\mathbb{Q}, \Sigma, I, F, \delta)$. On pose $\Sigma' = \Sigma, \mathbb{Q}' = \{q \in \mathbb{Q} \mid q \text{ accessible ou co-accessible}\}$, $I' = I \cap R'$, $F' = F \cap R'$ et

$$\delta = \left\{(q, \ell, q') \in \mathbb{Q}' \times \Sigma \times \mathbb{Q}' \;\middle|\; (q, \ell, q') \in \delta\right\} = (\mathbb{Q}', \Sigma, \mathbb{Q}') \cap \delta.$$

Montrons que $\mathscr{L}(\mathscr{A}) = \mathscr{L}(\mathscr{A}')$. On procède par double inclusion. On vérifie aisément que $\mathscr{L}(A') \subseteq \mathscr{L}(\mathscr{A})$. On montre maintenant $\mathscr{L}(\mathscr{A}) \subseteq \mathscr{L}(\mathscr{A}')$. Soit $w \in \mathscr{L}(\mathscr{A}')$. Soit $q_0, \dots, q_n$ tels que $q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n$ est une exécution acceptante. Or, pour tout $i \in [\![0, n]\!]$, q_i est accessible et co-accessible donc $q_i \in \mathbb{Q}'$. De plus, $q_0 \in I'$ et $q_n \in F'$. De plus, pour tout $i \in [\![0, n-1]\!]$, $(q_i, w_{i+1}, q_{i+1}) \in \delta'$. Donc, $q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n$ est une exécution acceptante de $\mathscr{A}'$. □

Parfois, on veut pouvoir "sauter" d'un état à un autre dans un automate. On utilise pour cela des ε-transitions.

IV.5 Automates finis avec ε-transitions

Définition : On dit d'un automate sur l'alphabet $\Sigma \cup \{\varepsilon\}$ que c'est un *automate avec ε-transition.*

Exemple :
L'automate ci-dessous est un automate avec ε-transitions.

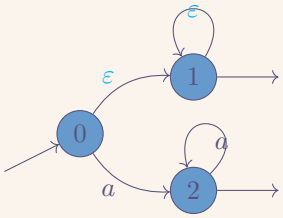


Figure 1.10 – Exemple d'automate avec ε-transition

Définition : Soit $w \in \left(\Sigma \cup \{\varepsilon\}\right)^\star$. On définit alors $\tilde{w}$ le mot obtenu en supprimant les occurrences de ε dans w.

Exemple :
Avec $\Sigma = \{a, b\}$ et $w = ab\varepsilon aa\varepsilon\varepsilon a$, on a $\tilde{w} = abaaa$.

On a également $\tilde{\varepsilon} = \varepsilon$; pour deux mots w_1 et w_2, on a $\widetilde{w_1 \cdot w_2} = \tilde{w}_1 \cdot \tilde{w}_2$; on a également $\tilde{a} = a$ pour $a \in \Sigma$ et $\tilde{\varepsilon} = \varepsilon$.

Définition : Soit $\mathscr{A}$ un automate avec ε-transition. On pose $\tilde{\mathscr{L}}(\mathscr{A})$ est le langage de l'automate sur l'alphabet $\Sigma \uplus \{\varepsilon\}$. On appelle *langage* de $\mathscr{A}$, l'ensemble À faire : retrouver la formule.

Exemple :
On peut trouver un automate reconnaissant la concaténation des langages des deux automates ci-dessous.

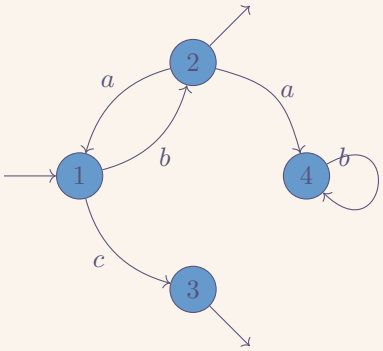


Figure 1.11 – Automate reconnaissant le langage $(ba)^\star \cdot \big(c \mid a(ba)^\star\big)$

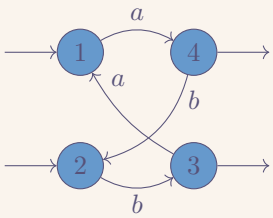


Figure 1.12 – Automate reconnaissant le langage $(a \mid baa)(bbaa)^\star \mid (b \mid abb)(aabb)^\star$

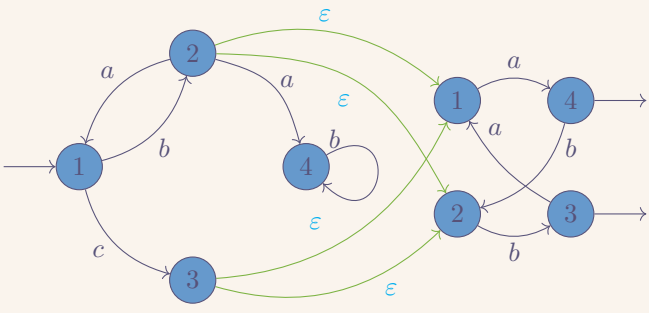


Figure 1.13 – Automate reconnaissant la concaténation des deux précédents

IV.5.1 Cloture par concaténation

Proposition : Soient $\mathscr{A} = (\Sigma, Q, I, F, \delta)$ et $\mathscr{A}' = (\Sigma', Q', I', F', \delta')$ deux automates avec $Q \cap Q' = .$ Alors $\mathscr{L}(\mathscr{A}) \cdot \mathscr{L}(\mathscr{A}')$ est un langage reconnaissable. Il est d'ailleurs reconnu par l'automate $\mathscr{A}^{\cdot} = (\Sigma^{\cdot}, Q^{\cdot}, I^{\cdot}, F^{\cdot}, \delta^{\cdot})$ défini avec $\Sigma^{\cdot} = \Sigma \cup \Sigma'$, $Q^{\cdot} Q \cup Q'$, $I^{\cdot} = I$, $F^{\cdot} = F'$ et

$$\delta^{\cdot} = \{(q, \varepsilon, q) \mid q \in F,\, q' \in I'\}.$$

Preuve :
Montrons que $\mathscr{L}(\mathscr{A}^{\cdot}) = \mathscr{L}(\mathscr{A}) \cdot \mathscr{L}(\mathscr{A}')$. On procède par double inclusion.

"$\subseteq$" Soit $w \in \mathscr{L}(\mathscr{A}^{\cdot})$ et soit

$$Q \supseteq I = I^{\cdot} \ni q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} q_2 \to \cdots \to q_{n-1} \xrightarrow{u_n} q_n \in F^{\cdot} = F' \subseteq Q$$

une exécution acceptante de $\mathscr{A}^{\cdot}$ telle que $\tilde{u} = w$. On pose $i_0 = \min\{i \in [\![1, n]\!] \mid q_i \in Q\}$. On a alors, $\forall i \in [\![1, i_0 - 1]\!]$, $q_i \in Q$. Montrons que $\forall i \in [\![i_0, n]\!]$, $q_i \in Q'$ par récurrence finie. On a $q_{i_0} \in Q'$. De plus, si $q_i \in Q'$ et $(q_i, u_{i+1}, q_{i+1}) \in \delta^{\cdot}$ donc $q_{i+1} \in Q'$. Inspectons $(Q \ni q_{i_0 - 1}, u_{i_0}, q_{i_0} \in Q') \in \delta^{\cdot}$. On sait que $(q_{i_0 - 1}, u_{i_0}, q_{i_0}) \notin \delta$ car $q_{i_0} \in Q'$; de même, $(q_{i_0 - 1}, u_{i_0}, q_{i_0}) \notin \delta'$ car $q_{i_0 - 1} \in Q$ donc $(q_{i_0 - 1}, u_{i_0}, q_{i_0}) \in \{(q, \varepsilon, q') \mid q \in F n q' \in I'\}$. On a donc que $q_{i_0 - 1} \in F$ et $q_{i_0} \in I$. Ainsi

$$I \ni \underbrace{q_0 \xrightarrow{u_1} q_1 \to \cdots \to \overset{F}{\underset{\ni}{q_i}}}_{} \xrightarrow{\varepsilon} \underbrace{\overset{I'}{\underset{\ni}{q_{i_0}}} \xrightarrow{u_{i_0}} \to \cdots \to q_n}_{} \in F$$

est une exécution acceptante de $\mathscr{A}$ d'étiquette $\widetilde{u_1 \dots u_{i_0 - 1}}$.

est une exécution acceptante de $\mathscr{A}'$ d'étiquette $\widetilde{u_{i_0 + 1} \dots u_n}$.

donc $\widetilde{u_{|[\![1, i_0 - 1]\!]}} \in \mathscr{L}(\mathscr{A})$ et $\widetilde{u_{|[\![i_0 + 1, n]\!]}} \in \mathscr{L}(\mathscr{A}')$.

$$\begin{aligned} w = \tilde{u} &= u_{|[\![1, i_0 - 1]\!]} \cdot \widetilde{u_{i_0} \cdot u_{|[\![i_0 + 1, n]\!]}} \\ &= \widetilde{u_{|[\![1, i_0 + 1]\!]}} \cdot \widetilde{u_{|[\![i_0 + 1, n]\!]}} \end{aligned}$$

"$\supseteq$" Montrons que $\mathscr{L}(\mathscr{A}) \cdot \mathscr{L}(\mathscr{A}') \subseteq \mathscr{L}(\mathscr{A}^{\star})$. Soit $w \in \mathscr{L}(\mathscr{A}) \cdot \mathscr{L}(\mathscr{A}^{\cdot})$, il existe donc

$$I \ni q_0 \xrightarrow{u_1} q_1 \to \cdots \to q_n \in F$$

une exécution acceptante dans $\mathscr{A}$ d'étiquette $\widetilde{u_1 \dots u_n}$. Il existe également

$$I' \ni q_{n+1} \xrightarrow{u_{n+2}} q_{n+1} \to \cdots \to q_m \in F$$

une exécution acceptante dans $\mathscr{A}'$ d'étiquette $\widetilde{u_{n+2} \dots u_m}$. Or, $\delta \subseteq \delta^{\cdot}$ et $\delta' \subseteq \delta^{\cdot}$ donc $\forall i \in [\![1, n]\!]$, $(q_{i-1}, u_i, q_i) \in \delta^{\cdot}$ et $\forall i \in [\![n + 2, m]\!]$, $(q_{i-1}, u_i, q_i) \in \delta^{\cdot}$. Or, $q_n \in F$ et $q_{n+1} \in I'$ donc $(q_n, \varepsilon, q_{n+1}) \in \delta^{\cdot}$. Finalement À faire : recopier.

□

IV.5.2 Cloture par étoile

Proposition : Soit $\mathscr{A} = (\Sigma, Q, I, F, \delta)$ un automate fini. Alors $\mathscr{L}(\mathscr{A})^\star$ est un automate reconnaissable, il est de plus reconnu par l'automate $\mathscr{A}_\star = (\Sigma_\star, Q_\star, I_\star, F_\star, \delta_\star)$ défini avec $\Sigma_\star = \Sigma$, $Q_\star = Q \cup \{V\}$ où $V \notin Q$. À faire : recopier ici...

Exemple :

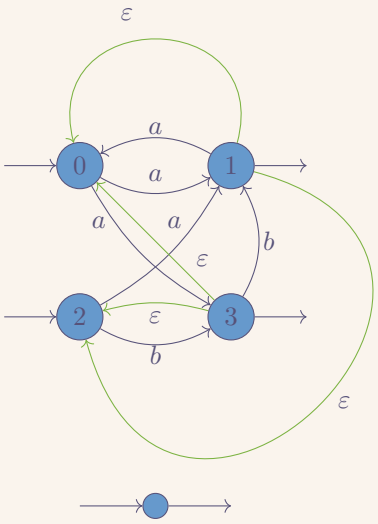


Figure 1.14 – Automate reconnaissant $\mathscr{L}(\mathscr{A})^\star$

IV.5.3 Cloture par union

Proposition : Soit $\mathscr{A} = (\Sigma, Q, I, F, \delta)$ et $\mathscr{A}' = (\Sigma', Q', I', F', \delta')$ deux automates avec $Q \cap Q' = $. Alors, $\mathscr{L}(\mathscr{A}) \cup \mathscr{L}(\mathscr{A}')$ est un langage reconnaissable. Il est, de plus, reconnu par $\mathscr{A}^\cup = (\Sigma^\cup, Q^\cup, I^\cup, F^\cup, \delta^\cup)$ avec $\Sigma^\cup = \Sigma \cup \Sigma'$, $Q^\cup = Q \cup Q'$, $I^\cup = I \cup I'$, $F^\cup = F \cup F'$ et $\delta^\cup = \delta \cup \delta'$.

Preuve :
Montrons que $\mathscr{L}(\mathscr{A}^\cup) \subseteq \mathscr{L}(\mathscr{A}) \cup \mathscr{L}(\mathscr{A}')$. Supposons, sans perte de généralité

que les automates $\mathscr{A}$ et $\mathscr{A}'$ sont sans ε-transitions. Soit $w \in \mathscr{L}(\mathscr{A}^{\cup})$. Il existe une exécution acceptante

$$I^{\cup} \ni q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n \in F^{\cup}$$

avec $w = w_0 \dots w_n$.

Montrons que, en supposant $q_0 \in I$ sans perte de généralité, $\forall i \in [\![1, n]\!]\,, q_i \in Q$ de proche en proche.

On a donc $q_n \in Q \cap F^{\cup} = F$ et on a alors, pour tout $i \in [\![1, n]\!]$, $(q_{i-1}, w_i, q_i) \in \delta^{\cup}$. Or, $q_{i-1} \in Q$ et $(q_{i-1}, w_i, q_i) \in \delta'$ donc $(q_{i-1}, w_i, q_i) \in \delta$.

Finalement, $q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_n$ est un exécution acceptante de $\mathscr{A}$ donc $w \in \mathscr{L}(\mathscr{A})$. □

Remarque :
Pour tout $a \in \Sigma$, $\{a\}$ est reconnaissable : par exemple,

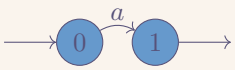


Figure 1.15 – Automate reconnaissant $\{a\}$ avec $a \in \Sigma$

Remarque :
est reconnaissable : par exemple,

Figure 1.16 – Automate reconnaissant

Proposition : De ce qui précède, on en déduit que l'ensemble des langages reconnaissables par automates avec ε-transition est au moins l'ensemble des langages réguliers.

Théorème : Si $\mathscr{A}$ est un automate avec ε-transitions, alors il existe un automate $\mathscr{A}'$ sans ε-transition tel que $\mathscr{L}(\mathscr{A}) = \mathscr{L}(\mathscr{A}')$.

Exemple :

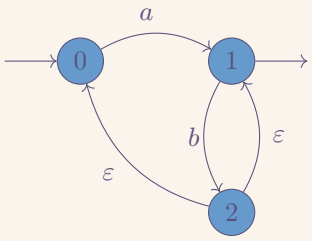


FIGURE 1.17 – Automate avec ε-transition

L'automate avec ε-transition ci-dessus peut être transformé en automate sans ε-transition comme celui ci-dessous.

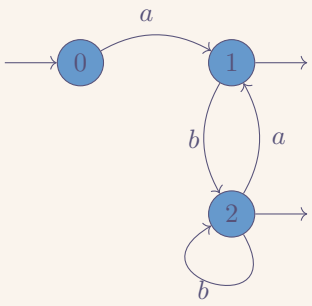


FIGURE 1.18 – Automate sans ε-transition

Proposition : Soit $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ un automate avec ε-transitions. Soit $q_r \in \mathbb{Q}$ un état de l'automate. Alors, l'automate $\mathscr{A}' = (\Sigma', \mathbb{Q}', I', F', \delta')$ défini par $\Sigma' = \Sigma$, $\mathbb{Q}' = \mathbb{Q}$, $I' = I$,

$$F' = F \cup \begin{cases} \{q \in \mathbb{Q} \mid (q, \varepsilon, q_r) \in \delta\} & \text{si } q_r \in F \\ & \text{sinon,} \end{cases}$$

$$\begin{aligned} \delta' = (\delta \setminus \{(q, \varepsilon, q_r) \in \delta \mid q \in \mathbb{Q}\}) \\ \cup \{(q, a, q') \mid (q, \varepsilon, q_r) \in \delta \,\text{et}\, (q_r, a, q') \in \delta \,\text{et}\, a \in \Sigma\} \\ \cup \{(q, \varepsilon, q') \mid (q, \varepsilon, q_r) \in \delta \text{ et } (q_r, \varepsilon, q') \in \delta \text{ et } q_r \neq q' \in \mathbb{Q}\}, \end{aligned}$$

est tel que

- il n'y a pas d'ε-transitions entrant en q_r ;
- $\mathscr{L}(\mathscr{A}') = \mathscr{L}(\mathscr{A})$;
- si $q \in \mathbb{Q}$ n'a pas d'ε-transition entrante dans $\mathscr{A}$, il n'en a pas dans $\mathscr{A}'$.

Algorithme 1.1 Suppression des ε-transitions

Entrée un automate $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$
Sortie un automate équivalent à $\mathscr{A}$ sans ε-transitions
1 : $\delta' \leftarrow \delta$
2 : $F' \leftarrow F$
3 : $\mathbb{Q}' \leftarrow \mathbb{Q}$
4 : **tant que** il existe $q \in \mathbb{Q}'$ avec une ε-transition entrante dans δ' **faire**
5 : $\quad (\Sigma', \mathbb{Q}', I', F', \delta') \leftarrow$ résultat de la proposition précédente avec $q_R = q$
6 : **retourner** $(\Sigma', \mathbb{Q}', I', F', \delta')$

On a donc démontré que tout langage régulier peut être reconnu par un automate.

Exemple :
On veut, par exemple, reconnaître le langage $(a \cdot b)^\star \cdot (a \mid b)$. À faire : Faire les automates

IV.6 Théorème de Kleene

On s'intéresse à un autre ensemble de langages, les *langages locaux*.

IV.6.1 Langages locaux

Définitions, propriétés

Définition (lettre préfixe, lettre suffixe, facteur de taille 2, non facteur) **:** Soit L un langage. On note l'ensemble $P(L)$ des lettres préfixes défini comme

$$\begin{aligned} P(L) &= \{\ell \in \Sigma \mid \exists w \in \ell,\ \exists v \in \Sigma^\star, w = \ell \cdot v\} \\ &= \{\ell \in \Sigma,\ \{\ell\} \cdot \Sigma^\star \cap L = \}. \end{aligned}$$

On note l'ensemble $S(L)$ des lettres suffixes défini comme

$$S(L) = \{w_{|w|} \mid w \in L\} = \{\ell \in \Sigma \mid \Sigma^\star \cdot \{\ell\} \cap L \neq \}.$$

On note l'ensemble $F(L)$ des facteurs de taille 2 défini comme

$$F(L) = \{\ell_1 \cdot \ell_2 \in \Sigma^2 \mid \Sigma^\star \cdot \{\ell_1, \ell_2\} \cdot \Sigma^\star \cap L \neq \}.$$

On note l'ensemble $N(L)$ des non-facteurs défini comme

$$N(L) = \Sigma^2 \setminus F(L).$$

On défini également l'ensemble

$$\Lambda(L) = L \cap \{\varepsilon\}.$$

Définition : Soit L un langage. On définit le *langage local engendré* par L comme étant

$$\rho(L) = \Lambda(L) \cup \Big(P(L) \cdot \Sigma^\star \cap \Sigma^\star \cdot S(L)\Big) \setminus \Sigma^\star N(L) \Sigma^\star.$$

Exemple :
Avec $L = \{aab, \varepsilon\}$, on a $P(L) = \{a\}$, $S(L) = \{b\}$, $F(L) = \{aa, ab\}$, $N(L) = \{ba, bb\}$, $\Lambda(L) = \{\varepsilon\}$. Et donc, on en déduit que

$$\rho(L) = \{\varepsilon\} \cup \{ab\} \cup \{aab\} \cup \cdots \{\varepsilon\} \cup \{a^n \cdot b \mid n \in \mathbb{N}^\star\}.$$

Définition : Un langage est dit *local* s'il est son propre langage engendré i.e. $\rho(L) = L$.

Proposition : Soit L un langage. Alors, $\rho(L) \supseteq L$.

Preuve :
Soit $w \in L$. Montrons que $w \in \rho(L)$.

- Si $w = \varepsilon$, alors $\Lambda(L) = L \cap \{\varepsilon\} = \{\varepsilon\}$ donc $w \in \rho(L)$.
- Sinon, notons $w = w_1 w_2 \dots w_n$. On doit montrer que $w_1 \in P(L)$, $w_n \in S(L)$, et $\forall i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F(L)$. Par définition de ces ensembles, c'est vrai.

□

Proposition : Soit L de la forme

$$\Lambda \cup (P\Sigma^\star \cap \Sigma^\star S) \setminus (\Sigma^\star N \Sigma^\star)$$

avec $\Lambda \subseteq \{\varepsilon\}$, $P \subseteq \Sigma$, $S \subseteq \Sigma$, et $N \subseteq \Sigma^2$. Alors $\rho(L) = L$.

Preuve :
On a $L \subseteq \rho(L)$. Montrons donc $\rho(L) \subseteq L$.

- Montrons que $\Lambda(L) \subseteq L$.
  - Si $\Lambda(L) =$, alors ok.
  - Sinon, $\Lambda(L) = \{\varepsilon\} = L \cap \{\varepsilon\}$ donc $\varepsilon \in L$ et donc $\varepsilon \in \Lambda$ parce que ce n'est possible.
- Montrons que $P(L) \subseteq P$. Soit $\ell \in P(L)$. Soient $v \in \Sigma^\star$, et $w \in L$

tels que $w = \ell v$. On a donc $w \notin \Lambda$, donc $w \in (P\Sigma^\star \cap \Sigma^\star S)$ et donc $\ell v = w \in P\Sigma^\star$ et donc $\ell \in P$.
— De même, $S(L) \subseteq L$
— À faire à la maison : $N \subseteq N(L)$ (ou $F(L) \subseteq F$)

□

Corollaire : On a $\rho^2 = \rho$.

À faire : Figure ensembles langages locaux, réguliers, ...

Preuve :
$\rho() =$ et $\rho(\Sigma^\star) = \Sigma^\star$. □

Remarque :
Un langage L est local si et seulement s'il existe $S \subseteq \Sigma$, $P \subseteq \Sigma$, $N \subseteq \Sigma^2$ tel que

$$L \setminus \{\varepsilon\} = (P\Sigma^\star \cap \Sigma^\star S) \setminus \Sigma^\star N \Sigma^\star.$$

Exemple :
Le langage $L = \{a\}$ est local avec $S = \{a\}$, $P = \{a\}$, $F =$ et $\Lambda = .$

Le langage $L = \{a, ab\}$ est local avec $S = \{b, a\}$, $P = \{a\}$, $F = \{ab\}$ et $\Lambda = .$

Le langage $L = (ab)^\star$ est local avec $S = \{b\}$, $P = \{a\}$, $F = \{ab, ba\}$. Soit $w \in \rho(L)$. Si $w = \varepsilon$, alors ok. Sinon, $w = abw_1$ et $w_1 \in \rho(L)$. Par récurrence, on montre que le langage est local.

Le langage $L = a \cdot (ab)^\star$ n'est pas local.

Stabilité
Intersection

Proposition : Si L_1 et L_2 sont deux langages locaux, alors $L_1 \cap L_2$ est un langage local.

Preuve :
Soit $L_1 = \Lambda_1 \cup \big(P_1\Sigma^\star \cap \Sigma^\star S_1\big) \setminus \big(\Sigma^\star N_1 \Sigma^\star\big)$, et $L_2 = \Lambda_2 \cup \big(P_2\Sigma^\star \cap \Sigma^\star S_2\big) \setminus \big(\Sigma^\star N_2 \Sigma^\star\big)$. On pose $F_1 = \Sigma^2 \setminus N_1$ et $F_2 = \Sigma^2 \setminus N_2$. On pose alors $\Lambda_\cap = \Lambda_1 \cap \Lambda_2$; $P_\cap = P_1 \cap P_2$; $S_\cap = S_1 \cap S_2$; $F_\cap = F_1 \cap F_2$; $N_\cap = \Sigma^2 \setminus F_\cap$. On a

$$L_1 \cap L_2 = \Lambda_\cap \cup \big(P_\cap \Sigma^\star \cap \Sigma^\star S_\cap\big) \setminus \Sigma^\star N_\cap \Sigma^\star.$$

En effet,

$$\begin{aligned} L_1 \cap L_2 &= (\Lambda_1 \cap \Lambda_2) \\ &\quad \cap (\Lambda_1 \cap (P_2\Sigma^\star \cap \Sigma^\star S_2) \setminus \Sigma^\star N_2 \Sigma^\star) \\ &\quad \cap \big(((P_1\Sigma^\star \cap \Sigma^\star S_1) \setminus \Sigma^\star N_1\Sigma^\star) \cap \Lambda_2\big) \\ &\quad \cap \big(((P_1\Sigma^\star \cap \Sigma^\star S_1) \setminus \Sigma^\star N_1\Sigma^\star) \cap (P_2\Sigma^\star \cap (P_2\Sigma^\star \cap \Sigma^\star S_2) \setminus \Sigma^\star N_2\Sigma^\star\big) \\ &= (\Lambda_1 \cap \Lambda_2)\big((P_1 \cap P_2)\Sigma^\star \cap \Sigma^\star(S_1 \cap S_2)\big) \setminus \Sigma^\star(N_1 \cap N_2)\Sigma^\star \end{aligned}$$

□

Union

Contre-exemple :
Avec $L_1 = ab$ et $L_2 = ba$, on a $\Lambda_1 = \Lambda_2 = $, $P_1 = \{a\}$, $P_2 = \{b\}$, $S_1 = \{b\}$, $S_2 = \{b\}$, $F_1 = \{ab\}$ et $F_2 = \{ba\}$. Le langage $L_1 \cup L_2 = \{ab, ba\}$ n'est pas local : en effet, on a $\Lambda = $, $P = \{a, b\}$, $S = \{a, b\}$, et $F = ab, ba$. Le mot aba est donc dans le langage local engendré.

On doit donc ajouter une contrainte afin d'éviter ce type de contre-exemples. L'intersection des alphabets est vide.

Proposition : Soient L_1 un langage local sur un alphabet Σ_1 et L_2 un langage local sur un alphabet Σ_2 avec $\Sigma_1 \cap \Sigma_2 = $. Alors $L_1 \cup L_2$ est local.

Preuve :
Soient Λ_1, S_1, P_1, N_1, F_1 tels que L_1 soit défini par $(\Lambda_1, S_1, P_1, N_1, F_1)$. De même, soient Λ_2, S_2, P_2, N_2, F_2 tels que L_2 soit défini par $(\Lambda_2, S_2, P_2, N_2, F_2)$. Construisons alors $\Lambda_\cup = \Lambda_1 \cup \Lambda_2$, $P_\cup = P_1 \cup P_2$, $S_\cup = S_1 \cup S_2$, $F_\cup = F_1 \cup F_2$ et $N_\cup = (\Sigma_1 \cup \Sigma_2)^2 \setminus F_\cup$. On note $\Sigma = \Sigma_1 \cup \Sigma_2$. Montrons alors que

$$L_1 \cup L_2 = \underbrace{\Lambda_\cup \cup (P_\cup\Sigma^\star \cap \Sigma^\star S_\cup) \setminus (\Sigma^\star N_\cup \Sigma^\star)}_{L_\cup}.$$

On procède par double-inclusion.

"$\subseteq$" Soit $w \in L_1 \cup L_2$.

- Cas 1 $w = \varepsilon$, alors $\Lambda_1 = \{\varepsilon\}$ ou $\Lambda_2 = \{\varepsilon\}$ donc $L_1 \cup L_2 = \{\varepsilon\}$ et donc $w \in L_\cup$.
- Cas 2 $w \neq \varepsilon$. On pose $w = w_1 \dots w_n$. Sans perte de généralité, on suppose $w \in L_1$ et $w \notin L_2$. D'où $w_1 \in P_1$ et $w_n \in S_1$. Et, pour $i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F_1$ donc $w_1 \in P_1 \cup P_2$, $w_n \in S_1 \cup S_2$ et $\forall i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F_1 \cup F_2$. D'où $w \in L_\cup$.

"$\supseteq$" Cas 1 $w = \varepsilon$ alors $w \in \Lambda_\cup = L_1 \cup L_2$ donc $w \in \Lambda_1$ ou $w \in \Lambda_2$ donc $w \in L_1$ ou $w \in L_2$.

Cas 2 $w \neq \varepsilon$. On pose $w = w_1 w_2 \dots w_n$ avec $w_1 \in P_\cup$, $w_n \in S_\cup$ et $\forall i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F_\cup$. Alors, sans perte de généralité, on suppose $w_1 \in \Sigma_1$. Montrons par récurrence que $\forall p \in [\![1, n]\!]$, $w_p \in \Sigma_1$.

- On sait que $w_1 \in \Sigma_1$ par hypothèse.
- On suppose que $w_p \in \Sigma_1$ avec $p < n$. Alors, $w_p w_{p+1} \in F_\cup = F_1 \cup F_2$. Or, $F_2 \subseteq (\Sigma_2)^2$ et $w_p \in \Sigma_1$ avec $\Sigma_1 \cap \Sigma_2 =$ donc $w_{p+1} \in \Sigma_1$.

On conclut par récurrence que $\forall i \in [\![1, n]\!]$, $w_i \in \Sigma_i$. Or, $w_n \in S_1 \cup S_2$ et $S_2 \cap \Sigma_1 =$ donc $w_n \in S_1$. De plus, pour $i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F_1 \cup F_2$ donc $w_i w_{i+1} \in F_1$ et donc $w \in L_1$.

□

Concaténation

Contre-exemple :
Avec $L_1 = \{ab\}$ et $L_2 = \{ab\}$, deux langages locaux, alors $L_1 \cdot L_2 = \{abba\}$ n'est pas local. En effet, $P = \{a\}$, $S = \{a\}$, $F = \{ab, bb, ba\}$; or $aba \notin L_1 \cdot L_2$.

Proposition : Soient L_1 un langage local sur un alphabet Σ_1 et L_2 un langage local sur un alphabet Σ_2, avec $\Sigma_1 \cap \Sigma_2 =$. Alors $L_1 \cdot L_2$ est un langage local.

Preuve :
Soient Λ_1, S_1, P_1, N_1, F_1 définissant L_1 et soient Λ_2, S_2, P_2, N_2, F_2 définissant L_2. Construisons $\Lambda_\bullet = \Lambda_1 \cap \Lambda_2$, $P_\bullet = P_1 \cup \Lambda_1 \cdot P_2$, $S_\bullet = S_2 \cup \Lambda_2 \cdot S_1$, $F_\bullet = F_1 \cup F_2 \cup S_1 \cdot P_2$, $\Sigma = \Sigma_1 \cup \Sigma_2$. Montrons que

$$L_1 \cdot L_2 = \underbrace{\Lambda_\bullet \cup (P_\bullet \Sigma^\star \cap \Sigma^\star S_\bullet) \setminus \Sigma^\star N_\bullet \Sigma^\star}_{L^\bullet}.$$

On procède par double inclusion.

"$\subseteq$" Soit $w \in L_1 \cdot L_2$.

- Si $w = \varepsilon$, alors $\varepsilon \in L_1$ et $\varepsilon \in L_2$ donc $w = \varepsilon \in \Lambda_\bullet \subseteq L^\bullet$.
- Sinon, $w = u \cdot v$ avec $u \in L_1$ et $v \in L_2$. On sait que $|u| > 0$ ou $|v| > 0$.
  - Si $u \neq \varepsilon$, alors $u = u_1 \dots u_p$ avec $p \geqslant 1$. On sait que $u_1 \in P_1$, $u_p \in S_1$ et, pour $i \in [\![1, p-1]\!]$, $u_1 u_{i+1} \in F_1$.

  Sous-cas 1 Si $v = \varepsilon$, alors $\Lambda_2 = \{\varepsilon\}$, et donc $S_1 \subseteq S_\bullet$. Or, $P_1 \subseteq P_\bullet$ et $F_1 \subseteq F_\bullet$. On en déduit que $w = u \in L^\bullet$.

  Sous-cas 2 $v \neq \varepsilon$, alors $v = v_1 \dots v_q$ avec $v_1 \in P_2$, $v_q \in S_2$ et, pour

$i \in [\![1, nq-1]\!]$, $v_i v_{i+1} \in F_2$. Or, $u_p v_1 \in S_1 \cdot P_2$ et donc $w = u \cdot v \in L^\bullet$.

— Si $u = \varepsilon$, on procède de la même manière.

"$\supseteq$" Soit $w \in L^\bullet$.

— Si $w = \varepsilon$, alors $\varepsilon \in \Lambda_\bullet$ et donc $\varepsilon \in L_1$ et $\varepsilon \in L_2$. D'où $\varepsilon \in L_1 \cdot L_2$.

— Sinon, on pose $w = w_1 \dots w_n$.

Sous-cas 1 Si $\{i \in [\![1,n]\!] \mid w_i \in \Sigma_2\} = $, on a donc $\forall i \in [\![1,n]\!]$, $w_i \in \Sigma_1$. De plus, $w_1 \in P_\bullet$, $w_n \in S_\bullet$ et, pour $i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F_\bullet$. Or, $P_\bullet \cap \Sigma_1 = P_1$, $S_\bullet \cap \Sigma_1 = S_1$, $\Lambda_2 = \{\varepsilon\}$ et $\forall i \in [\![1, n-1]\!]$ $w_i w_{i+1} \in F_1$. On en déduit que $w = w_1 \dots w_n \cdot \varepsilon \in L_1 \cdot L_2$.

Sous-cas 2 Si $M = \{i \in [\![1,n]\!] \mid w_i \in \Sigma_2\} \neq $. Soit $i_0 = \min(M)$. D'où

$$w = \underbrace{w_1 \dots w_{i_0-1}}_{\in \Sigma_1} \cdot \underbrace{w_{i_0}}_{\in \Sigma_2} \dots w_n.$$

Si, $\ell_1, \ell_2 \in F_\bullet$, et $\ell_1 \in \Sigma_2$, alors $\ell_2 \in \Sigma_2$. De proche en proche, on en déduit que $\forall i \in [\![i_0, n]\!]$, $w_i \in \Sigma_2$.

— Si $i_0 = 1$, alors $w_1 \in \Sigma_2$, $w_1 \in P_\bullet$, $w_1 \in P_2$, $w_1 \in P_2$, $\Lambda_1 = \{\varepsilon\}$, et $w_n \in S_\bullet \cap \Sigma_2$, et $w_n \in S_2$. De plus, pour $i \in [\![1, n-1]\!]$, $w_i w_{i+1} \in F_\bullet \cap (\Sigma_2)^2$ donc $w_i w_{i+1} \in F_2$. D'où $w = \varepsilon \cdot w_1 \dots w_n \in L_1 \cdot L_2$.

— Si $i_0 > 1$, alors $w_1 \in \Sigma_1 \cap P^\bullet = P_1$, $w_n \in \Sigma_2 \cap S^\bullet = S_2$, et $\forall i \in [\![1, i_0 - 2]\!]$, $w_i w_{i+1} \in F^\bullet \cap (\Sigma_1)^2 = F_1$. D'où $w_{i_0-1} w_{i_0} \in F^\bullet \cap \Sigma_1 \Sigma_2 = S_1 P_2$ donc $w_{i_0-1} \in S_1$ et $w_{i_0} \in P_2$ donc $w_1 \dots w_{i_0-1} \in L_1$. Finalement, $\forall i \in [\![i_0, n-1]\!]$, $w_i w_{i_1 \in F_\bullet \cap (\Sigma)^2}$ donc À faire : Finir la preuve.

□

Étoile

Proposition : Soit L un langage local, alors $L^\star$ est un langage local.

Preuve :
Soient Λ, P, S, F et N définissant L. Alors $\Lambda_\star = \{\varepsilon\}$, $P_\star = P$, $S_\star = S$ et $F_\star = F \cup S \cdot P$. À faire : preuve à faire à la maison. □

Exemple :
Avec $L = \{a, b\}$, un langage local, on a $\Lambda_\star = \{\varepsilon\}$, $P_\star = S_\star = \{a, b\}$ (car $P = \{a, b\} = S$), et $S_\star = \{ab, ba, aa, bb\}$.

IV.6.2 Expressions régulières linéaires

Définition : Un expression régulière est dite *linéaire* si chacune de ses lettres apparaît une fois au plus dans l'expression.

Exemple :

Oui	Non
a	aa
$a\|b$	$a\|ba$

Table 1.2 – Exemples et non-exemples d'expressions régulières linéaires

Exemple :
On définit une fonction booléenne permettant de vérifier si une expression régulière est linéaire :

$$\text{linéaire} : \left(\begin{array}{rcl} & \mapsto & \top \\ \varepsilon & \mapsto & \top \\ a \in \Sigma & \mapsto & \top \\ e_1 \cdot e_2 & \mapsto & (\text{vars}(e_1) \cap \text{vars}(e_2) =) \text{ et linéaire}(e_1) \text{ et linéaire}(e_2) \\ e_1 \mid e_2 & \mapsto & (\text{vars}(e_1) \cap \text{vars}(e_2) =) \text{ et linéaire}(e_1) \text{ et linéaire}(e_2) \\ {e_1}^\star & \mapsto & \text{linéaire}(e_1) \end{array} \right).$$

Proposition : Le langage d'une expression régulière est local.

Preuve :
Il nous suffit de montrer le résultat sur le cas de base.

$\mathscr{L}() :$ qui correspond à $\Lambda = , S = , P = , F = .$

$\mathscr{L}(\varepsilon) = \{\varepsilon\}$ qui correspond à $\Lambda = \{\varepsilon\}$ et $S = P = F = .$

$\mathscr{L}(a) = \{a\}$ qui correspond à $\Lambda = , S = \{a\}, P = \{a\}$ et $F = .$ □

Remarque :
Les grandeurs Λ, P, S et F sont de plus définies individuellement par la table suivante.

e	Λ	P	S	F
ε	$\{\varepsilon\}$			
a		$\{a\}$	$\{a\}$	
${e_1}^\star$	$\{\varepsilon\}$	$P(e_1)$	$S(e_1)$	$F(e_1) \cup S(e_1) \cdot P(e_1)$
$e_1 \cdot e_2$	$\Lambda(e_1) \cap \Lambda(e_1)$	$P(e_1) \cup \Lambda(e_2) \cdot P(e_2)$	$S(e_2) \cup \Lambda(e_2) \cdot S(e_1)$	$F(e_1) \cup F(e_2) \cup S(e_1) \cdot P(e_2)$
$e_1 \mid e_2$	$\Lambda(e_1) \cup \Lambda(e_2)$	$P(e_1) \cup P(e_2)$	$S(e_1) \cup S(e_2)$	$F(e_1) \cup F(e_2)$

TABLE 1.3 – Construction de Λ, P, S et F dans différents cas

REMARQUE (Notation) :
Si Σ_1 et Σ_2 sont deux alphabets et $\varphi : \Sigma_1 \to \Sigma_2$, alors on note $\tilde{\varphi}$ l'extension de φ aux mots de $\Sigma_1^\star$:

$$\tilde{\varphi}(w_1 \dots w_n) = \varphi(w_1) \dots \varphi(w_n)$$

et, de plus, on note

$$\tilde{\varphi}(L) = \{\tilde{\varphi}(w) \mid w \in L\}.$$

REMARQUE :
On a $\tilde{\varphi}(L \cup M) = \tilde{\varphi}(L \cup M) = \tilde{\varphi}L \cup \tilde{\varphi}(M)$.

Proposition :

$$\tilde{\varphi}(L \cdot M) = \tilde{\varphi}(L) \cdot \tilde{\varphi}(M)$$

Preuve :

$$\begin{aligned} w \in \tilde{\varphi}(L \cdot M) &\iff \exists u \in L \cdot M,\ w = \tilde{\varphi}(u) \\ &\iff \exists (v,t) \in L \times M,\ w = \tilde{\varphi}(v \cdot t) \\ &\iff \exists (v,t) \in L \times M,\ w = \tilde{\varphi}(v) \cdot \tilde{\varphi}(t) \\ &\iff w \in \tilde{\varphi}(L) \cdot \tilde{\varphi}(M). \end{aligned}$$

□

Définition : Soient $e \in \mathrm{Reg}(\Sigma_1)$, $\varphi : \Sigma_1 \to \Sigma_2$. On définit alors inductivement e_φ comme étant

$$\begin{array}{ll} \varphi = & a_\varphi = \varphi(a) \text{ si } a \in \Sigma_1 \qquad (e_1 \mid e_2)_\varphi = (e_1)_\varphi \mid (e_2)_\varphi \\ \varepsilon_\varphi = \varepsilon & (e_1 \cdot e_2)_\varphi = (e_1)_\varphi \cdot (e_2)_\varphi \qquad (e_1^\star)_\varphi = ((e_1)_\varphi)^\star. \end{array}$$

Proposition : Si $\varphi : \Sigma_1 \to \Sigma_2$ et $e \in \mathrm{Reg}(\Sigma_1)$, alors

$$\mathscr{L}(e_\varphi) = \tilde{\varphi}(\mathscr{L}(e)).$$

Preuve (par incuction sur $e \in \mathrm{Reg}(\Sigma_1)$) *:* cas $\mathscr{L}(_\varphi) = \mathscr{L}() = \ = \tilde{\varphi}() = \tilde{\varphi}(\mathscr{L}())$
cas ε $\mathscr{L}(\varepsilon_\varphi) = \mathscr{L}(\varepsilon) = \{\varepsilon\} = \tilde{\varphi}($ À faire : recopier ici
cas $e_1 \cdot e_2$ $\mathscr{L}((e_1 \cdot e_2)_\varphi) = \mathscr{L}((e_1)_\varphi \cdot (e_2)_\varphi)) = \mathscr{L}((e_1)_\varphi) \cdot \mathscr{L}((e_2)_\varphi) = \tilde{\varphi}(\mathscr{L}(e_1)) \cdot \tilde{\varphi}(\mathscr{L}(e_2)) = \tilde{\varphi}(\mathscr{L}(e_1) \cdot \mathscr{L}(e_2)) = \tilde{\varphi}(\mathscr{L}(e_1 \cdot e_2))$.
De même pour les autres cas

□

Proposition : Soit $e \in \mathrm{Reg}(\Sigma_1)$. Il existe $f \in \mathrm{Reg}(\Sigma)$ et $\varphi : \Sigma \to \Sigma_1$ tel que f est linéaire et $e = f_\varphi$.

Preuve :
Il suffit de numéroter les lettres (c.f. exemple ci-dessous). □

Exemple :
Avec $e = c^\star((a \cdot a) \mid \varepsilon) \cdot ((a \mid c \mid \varepsilon)^\star))^\star \cdot b \cdot a \cdot a^\star$, on a

$$f = c_1^\star((a_1 \cdot a_2) \mid \varepsilon) \cdot (b_1((a_3 \mid c_2 \mid \varepsilon)^\star))^\star \cdot b_2 \cdot a_4 \cdot a_5$$

et

$$\varphi : \left(\begin{array}{ccc} a_1 & \mapsto & a \\ a_2 & \mapsto & a \\ a_3 & \mapsto & a \\ a_4 & \mapsto & a \\ a_5 & \mapsto & a \\ b_1 & \mapsto & b \\ b_2 & \mapsto & b \\ c_1 & \mapsto & c \\ c_2 & \mapsto & c \end{array} \right).$$

IV.6.3 Automates locaux

Définition (automate local, local standard) **:** Un automate $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ est dit *local* dès lors que pour out $\forall (q_1, q_2, \ell, q_3, q_4) \in \mathbb{Q} \times \mathbb{Q} \times \Sigma \times \mathbb{Q} \times \mathbb{Q}$,

$$(q_1, \ell, q_3) \in \delta \quad \text{et} \quad (q_2, \ell, q_4) \in \delta \qquad \Longrightarrow \qquad q_3 = q_4.$$

L'automate $\mathscr{A}$ est dit, de plus, *standard* lorsque $\mathrm{Card}(I) = 1$ et qu'il n'existe pas de transitions entrante en l'unique état initial q_0.

Proposition : Un langage est local si et seulement s'il est reconnu par un automate local standard.

Exemple :

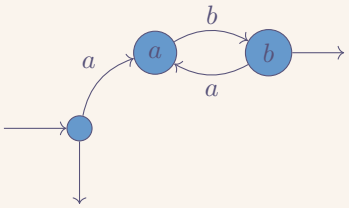


Figure 1.19 – Automate local reconnaissant le langage $(ab)^\star$

Preuve "$\Longrightarrow$" Soit L un langage local. Soit (Λ, S, P, F, N) tels que

$$L = \Lambda \cup (P\Sigma^\star \cap \Sigma^\star) \setminus (\Sigma^\star N \Sigma^\star).$$

Soit alors l'automate $\mathbb{Q} = \Sigma \cup \{\varepsilon\}$, $I = \{\varepsilon\}$, $F_{\mathscr{A}} = S \cup \Lambda$, et

$$\begin{aligned}\delta = \quad & \{(q, \ell, q') \in \mathbb{Q} \times \Sigma \times \mathbb{Q} \mid qq' \in F \text{ et } q' = \ell\} \\ & \cup \{(\varepsilon, \ell, q) \in \mathbb{Q} \times \Sigma \times \mathbb{Q} \mid \ell = q \text{ et } q \in P\}.\end{aligned}$$

On pose $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F_{\mathscr{A}}, \delta)$. Montrons que $\mathscr{L}(\mathscr{A}) = L$.

"$\subseteq$" Soit $w \in \mathscr{L}(\mathscr{A})$. Soit donc

$$q_1 \xrightarrow{w_1} q_2 \to \cdots \to q_{n-1} \xrightarrow{w_n} q_n$$

une exécution acceptante dans $\mathscr{A}$. Montrons que $w_1 \dots w_n \in L$.

Cas 1 $w = \varepsilon$ et $n = 0$. Ainsi $q_0 = q_n = \varepsilon$ et $F \cap I = .$ Or $F_{\mathscr{A}} = S \cup \Lambda$, et donc $\Lambda = \{\varepsilon\}$, d'où $\varepsilon \in L$.

Cas 2 $w \neq \varepsilon$. On sait que $w_1 \in P$; en effet, $(\varepsilon, w_1, q_1) \in \delta$ donc $w_1 = q_1 \in P$. De même, $(q_{n-1}, w_n, q_n) \in \delta$, d'où $S \ni w_n = q_n$. De plus, $\forall i \in [\![1, n-1]\!]$, $(q_{i-1}, w_i, q_i) \in \delta$ et $(q_i, w_{i+1}, q_{i+1}) \in \delta$. Ainsi, $w_i = q_i$ et $w_{i+1} = q_{i+1}$ avec $q_i q_{i+1} \in F$, d'où $w_i w_{i+1} \in F$. Donc $w \in L$.

"$\supseteq$" Soit $w = w_1 \dots w_n \in L$.

Cas 1 $w = \varepsilon$. On a $\Lambda = \{\varepsilon\}$, et donc ε est final (ou initial). On en déduit que $\varepsilon \in \mathscr{L}(\mathscr{A})$.

Cas 2 $w \neq \varepsilon$. Montrons, par récurrence finie sur $p \leqslant n$, qu'il existe une exécution

$$q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_p} q_p$$

dans $\mathscr{A}$.

— Avec $p = 1$, on a $w_1 \in P$ donc $(\varepsilon, w_1, w_1) \in \delta$. Ainsi, $\varepsilon \xrightarrow{w_1} w_1$ est une exécution dans $\mathscr{A}$.

— Supposons construit $\varepsilon \xrightarrow{w_1} q_1 \to \cdots \xrightarrow{w_p} q_p = w_p$ avec $p < n$. Or, $w_p w_{p+1} \in F$ donc $(w_p, w_{p+1}, w_{p+1}) \in \delta$. Ainsi,

$$\varepsilon \xrightarrow{w_1} q_1 \to \cdots \xrightarrow{w_p} q_p \xrightarrow{w_{p+1}} w_{p+1}$$

est une exécution acceptante de $\mathscr{A}$.

De proche en proche, on a

$$\varepsilon \xrightarrow{w_1} q_1 \to \cdots \to q_{n-1} \xrightarrow{w_n} w_n$$

une exécution dans $\mathscr{A}$. Or, $w_n \in S = F_{\mathscr{A}}$ et donc l'exécution est acceptante dans $\mathscr{A}$, et $w \in \mathscr{L}(\mathscr{A})$.

" $\Longleftarrow$ " Soit $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F_{\mathscr{A}}, \delta)$ un automate localement standard. Montrons que $\mathscr{L}(\mathscr{A})$ est local. Il suffit de montrer que $\rho(\mathscr{L}(\mathscr{A})) = \mathscr{L}(\mathscr{A})$. Or $\mathscr{L}(\mathscr{A}) \subseteq \rho(\mathscr{L}(\mathscr{A}))$. On montre donc $\rho(\mathscr{L}(\mathscr{A})) \subseteq \mathscr{L}(\mathscr{A})$.

Soit $w \in \rho(\mathscr{L}(\mathscr{A}))$. Ainsi,

$$w \in \Lambda(\mathscr{L}(\mathscr{A})) \cup \Big(P(\mathscr{L}(\mathscr{A}))\Sigma^\star \cap \Sigma^\star S(\mathscr{L}(\mathscr{A}))\Big) \setminus \Big(\Sigma^\star N(\mathscr{L}(\mathscr{A}))\Sigma^\star\Big).$$

Montrons que $w \in \mathscr{L}(\mathscr{A})$.

— Si $w \in \Lambda(\mathscr{L}(\mathscr{A}))$, alors $w = \varepsilon$. Or, $\Lambda(\mathscr{L}(\mathscr{A})) = \mathscr{L}(\mathscr{A}) \cap \{\varepsilon\}$. Ainsi $w \in \mathscr{L}(\mathscr{A})$.

— Sinon, $w = w_1 \dots w_n$ avec $w_1 \in P(\mathscr{L}(\mathscr{A}))$, donc il existe $u \in \Sigma^\star$ tel que $w_1 \cdot u \in \mathscr{L}(\mathscr{A})$. Il existe donc une exécution acceptante

$$I \ni q_0 \xrightarrow{w_1} q_1 - \overset{u}{-} \to q_s \in F_{\mathscr{A}}.$$

Il existe donc une exécution $q_0 \xrightarrow{w_1} q_1$.

Supposons construit $q_1 \xrightarrow{w_1} q_1 \to \cdots \xrightarrow{w_p} q_p$ avec $p < n$. Or, $w_p w_{p+1} \in F(\mathscr{L}(\mathscr{A}))$, donc il existe $w \in \Sigma^\star$ et $y \in \Sigma^\star$ tels que $x \cdot w_p \cdot w_{p+1} \cdot y \in \mathscr{L}(\mathscr{A})$. Il existe donc une exécution acceptante

$$r_0 - \overset{x}{-} \to r_{p-1} \xrightarrow{w_p} r_p \xrightarrow{w_{p+1}} r_{p+1} - \overset{y}{-} \to r_s.$$

Or, par localité de l'automate, $q_p = r_p$. Il existe donc q_{p+1} $(= r_{p+1})$ tel que $(q_p, w_{p+1}, q_{p+1}) \in \delta$. On a donc une exécution

$$q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_p \xrightarrow{w_{p+1}} q_{p+1}.$$

De proche en proche, il existe une exécution

$$q_0 \xrightarrow{w_1} q_1 \to \cdots \to q_n.$$

Or, $w_n \in S(\mathscr{L}(\mathscr{A}))$, il existe donc $v \in \Sigma^\star$ tel que $v \cdot w_n \in \mathscr{L}(\mathscr{A})$, donc il existe un exécution acceptante

$$I \ni r_0 - \overset{v}{-} \to r_{s-1} \xrightarrow{w_n} r_s \in F_{\mathscr{A}}.$$

Par localité, $r_s = q_n \in F_{\mathscr{A}}$.

Donc $\rho(\mathscr{L}(\mathscr{A})) \subseteq \mathscr{L}(\mathscr{A})$ et donc $\rho(\mathscr{L}(\mathscr{A})) = \mathscr{L}(\mathscr{A})$. On en déduit que $\mathscr{L}(\mathscr{A})$ est local.

□

Exemple :
Dans le langage local $(ab)^\star \mid c^\star$, on a $\Lambda = \{\varepsilon\}$, $S = \{c, b\}$, $P = \{a, c\}$ et $F = \{ab, ba, cc\}$. L'automate local reconnaissant ce langage est celui ci-dessous.

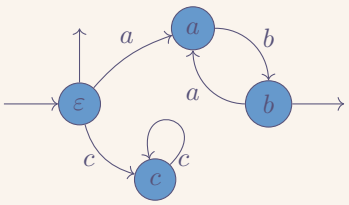


Figure 1.20 – Automate local reconnaissant $(ab)^\star \mid c^\star$

Proposition : Soit $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ un automate et $\varphi : \Sigma \to \Sigma_1$. On pose

$$\delta' = \{(a, \varphi(\ell), q') \mid (q, \ell, q') \in \delta\}.$$

On pose $\mathscr{A}' = (\Sigma, \mathbb{Q}, I, F, \delta')$. On a $\mathscr{L}(\mathscr{A}') = \tilde{\varphi}(\mathscr{L}(\mathscr{A}))$.

Exercice :
Montrons que LR $\subsetneq \wp(\Sigma^\star)$ i.e. il existe des langages non reconnaissables.

$\mathbb{R}$ n'est pas dénombrable. On écrit un nombre réel comme une suite infinie

$$0{,}10110010101\ldots1010110\ldots$$

On pose $\Sigma = \{a\}$, on crée le langage L, associé au nombre ci-dessus comme l'ensemble contenant a, aaa, $aaaa$,...

Remarque (Notation) :
On note A_φ, l'automate $\big(\varphi(E), \mathbb{Q}, I, F, \delta'\big)$ où $\delta' = \{(q, \varphi(\ell), q') \mid (q, \ell, q') \in \delta\}$.

IV.6.4 Algorithme de Berry-Sethi : les langages réguliers sont reconnaissables

Exemple :
On considère l'expression régulière $aab(a \mid b)^\star$. On numérote les lettres : $a_1a_2b_1(a_3 \mid b_2)^\star$, avec

$$\varphi : \begin{pmatrix} a_1 & \mapsto & a \\ a_2 & \mapsto & a \\ a_3 & \mapsto & a \\ b_1 & \mapsto & b \\ b_2 & \mapsto & b \end{pmatrix}.$$

	Λ	S	P	F
a_1		a_1	a_1	
a_2		a_2	a_2	
$a_1 \cdot a_2$		a_2	a_1	a_1a_2
b_1		b_1	b_1	
$a_1a_2b_1$		b_1	a_1	a_1a_2, a_2b_1
a_3		a_3	a_3	
b_2		b_2	b_2	
$a_3 \mid b_2$		a_3, b_2	a_3, b_2	
$(a_3 \mid b_2)^\star$	ε	a_3, b_2	a_3, b_2	$a_3b_2, b_2a_3, a_3a_3, b_2b_2$
$a_1a_2b_1(a_3 \mid b_2)^\star$		a_3, b_2ab_1	a_1	$a_3b_2, b_2a_3, a_3a_3, b_2b_2, a_1a_2, a_2b_1, b_1a_3, b_1b_2$

Table 1.4 – Λ, S, P et F pour les différents mots reconnus

On crée donc l'automate ci-dessous.

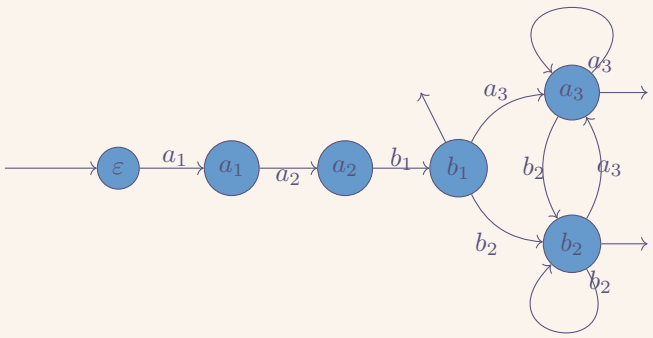


Figure 1.21 – Automate déduit de la table 1.4

On applique la fonction φ a tous les états et transitions pour obtenir l'automate ci-dessous. Cet algorithme reconnaît le langage $aab(a \mid b)^\star$.

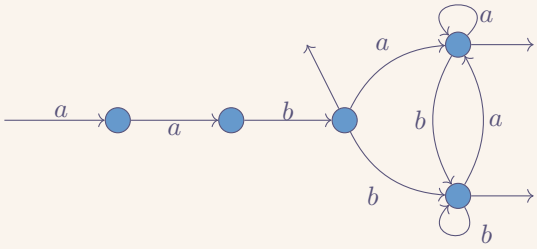


FIGURE 1.22 – Application de φ à l'automate de la figure 1.21

Théorème : Tout langage régulier est reconnaissable. De plus, on a un algorithme qui calcule un automate le reconnaissant, à partir de sa représentation sous forme d'expression régulière.

Algorithme (BERRY-SETHI) **:** Entrée : Une expression régulière e
Sortie : Un automate reconnaissant $\mathscr{L}(e)$

1. On linéarise e en f avec une fonction φ telle que $f_\varphi = e$.
2. On calcule inductivement $\Lambda(f)$, $S(f)$, $P(f)$, et $F(f)$.
3. On fabrique $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ un automate reconnaissant $\mathscr{L}(f)$.
4. On retourne $\mathscr{A}_\varphi$.

À faire : refaire la mise en page pour les algorithmes

IV.6.5 Les langages reconnaissables sont réguliers

On fait le « sens inverse » : à partir d'un automate, comment en déduire le langage reconnu par cet automate ?

L'idée est de supprimer les états un à un. Premièrement, on rassemble les états initiaux en les reliant à un état i, et de même, on relie les états finaux à f. Pour une suite d'états, on concatène les lettres reconnus sur chaque transition :

FIGURE 1.23 – Succession d'états

De même, lors de « branches » en parallèles, on les concatène avec un |. En appliquant cet algorithme à l'automate précédent, on a

$$(aab) \cdot \Big((\varepsilon \mid aa^\star) \mid (b \mid aa^\star b) \cdot (b \mid aa^\star b)^\star (aa^\star \mid \varepsilon) \Big).$$

Définition : Un *automate généralisé* est un quintuplet $(\Sigma, \mathbb{Q}, I, F, \delta)$ où
- Σ est un alphabet ;
- $\mathbb{Q}$ est un ensemble fini ;
- $I \subseteq \mathbb{Q}$;
- $F \subseteq \mathbb{Q}$;
- $\delta \subseteq \mathbb{Q} \times \mathrm{Reg}(\Sigma) \times \mathbb{Q}$, avec

$$\forall r \in \mathrm{Reg}(\Sigma),\ \forall (q, q') \in \mathbb{Q}^2,\ \mathrm{Card}(\{(q, r, q') \in \delta\}) \leqslant 1.$$

Définition (Langage reconnu par un automate généralisé) **:** Soit $(\Sigma, \mathbb{Q}, I, F, \delta)$ un automate généralisé. On dit qu'un mot w est reconnu par l'automate s'il existe une suite

$$q_0 \xrightarrow{r_1} q_1 \xrightarrow{r_2} q_2 \to \cdots \to q_{n-1} \xrightarrow{r_n} q_n$$

et $(u_i)_{i \in [\![1,n]\!]}$ tels que $\forall i \in [\![1, n]\!]$, $u_i \in \mathscr{L}(r_i)$ et $w = u_1 \cdot u_2 \cdot \ldots \cdot u_n$.

Définition : Un automate généralisé $(\Sigma, \mathbb{Q}, I, F, \delta)$ est dit « bien détouré[2] » si $I = \{i\}$ et $F = \{f\}$, avec $i \neq f$, tels que i n'a pas de transitions entrantes et f n'a pas de transitions sortantes.

Lemme : Tout automate généralisé est équivalent à un automate généralisé « bien détouré. » En effet, soit $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ un automate généralisé. Soit $i \notin \mathbb{Q}$ et $f \notin \mathbb{Q}$. On pose $\Sigma' = \Sigma$, $I' = \{i\}$, $F' = \{f\}$, $\mathbb{Q}' = \mathbb{Q} \cup \{i, f\}$ et

$$\delta' = \delta \cup \{(i, \varepsilon, q) \mid q \in I\} \cup \{(q, \varepsilon, f) \mid q \in F\}.$$

Alors, l'automate $\mathscr{A}' = (\Sigma', \mathbb{Q}', I', F', \delta')$ est équivalent à $\mathscr{A}$ et « bien détouré. »

Lemme : Soit $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ un automate généralisé « bien détouré » tel que $|\mathbb{Q}| \geqslant 3$. Alors il existe un automate généralisé « bien détouré » $\mathscr{A}' = (\Sigma, \mathbb{Q}', I, F, \delta')$ avec $\mathbb{Q}' \subsetneq \mathbb{Q}$ et $\mathscr{L}(\mathscr{A}) = \mathscr{L}(\mathscr{A}')$.

Preuve :
Étant donné qu'il existe au plus une transition entre chaque pair d'état $(q, q') \in \mathbb{Q}^2$, il est possible de le représenter au moyen d'une fonction de

2. Cette notation n'est pas officielle.

transition

$$T : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathrm{Reg}(\Sigma).$$

À faire : Recopier la def de T Soit $q \in \mathbb{Q} \setminus \{i, f\}$. Soit alors T' défini, pour $(q_a, q_b) \in \mathbb{Q} \setminus \{q\}$, par

$$T'(q_a, q_b) = T(q_a, q_b) \mid T(q_a, q) \cdot T(q, q)^\star \cdot T(q, q_b).$$

On considère l'automate $\mathbb{Q}' = \mathbb{Q} \setminus \{q\}$ et δ' construit à partir de T'. □

Exemple :
On considère l'automate ci-dessous.

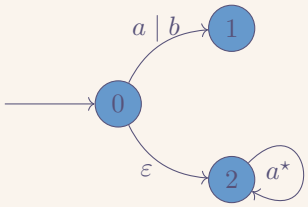


Figure 1.24 – Automate exemple

La fonction T peut être représentée dans la table ci-dessous.

	0	1	2
0		$a \mid b$	ε
1			
2			$a^\star$

Table 1.5 – Fonction T équivalente à l'automate de la figure 1.24

Exemple :
On applique l'algorithme à l'automate suivant.

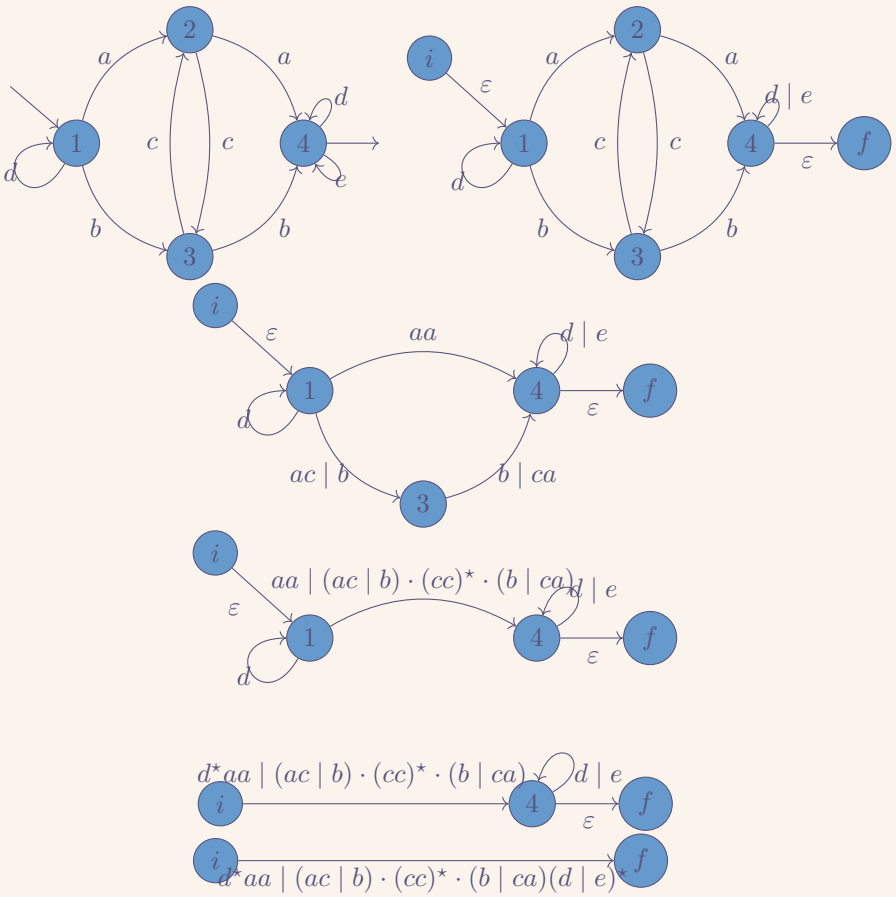


FIGURE 1.25 – Application de l'algorithme à un exemple

On a donc que le langage de l'automate initial est

$$\mathscr{L}(d^\star(aa) \mid (ac \mid b)(cc)^\star(b \mid ca)(d \mid e)^\star).$$

Théorème : Un langage reconnaissable est régulier.

Preuve :
On itère le lemme précédent depuis un automate généralisé $\mathscr{A}$ jusqu'à obtention d'un automate comme celui ci-dessous.

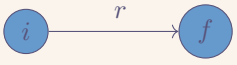


FIGURE 1.26 – Automate résultat de l'application du lemme

On a alors $\mathscr{L}(\mathscr{A}) = \mathscr{L}(r)$. □

Théorème (KLEENE) **:** Un langage est régulier si et seulement s'il est reconnaissable. Et, on a donné un algorithme effectuant ce calcul dans les deux sens.

IV.7 La classe des langages réguliers

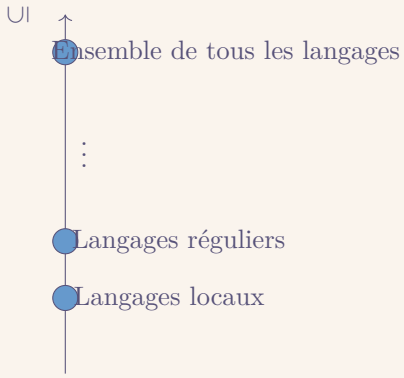


FIGURE 1.27 – Ensembles de langages

Proposition : La classe des langages réguliers/reconnaissables est stable par passage au complémentaire.

Preuve :
Soit $L \in$ LR. Soit $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ un automate reconnaissant le langage L. Soit $\mathscr{A}' = (\Sigma, \mathbb{Q}', I', F', \delta')$ un automate déterministe et complet équivalent à $\mathscr{A}$. Soit $\mathscr{A}'' = (\Sigma, \mathbb{Q}', I', \mathbb{Q}' \setminus F', \delta')$. Alors (à prouver à la maison) $\mathscr{L}(\mathscr{A}'') = \Sigma^\star \setminus \mathscr{L}(\mathscr{A}) = \Sigma^\star \setminus L$ et donc $\Sigma^\star \setminus L$ est reconnaissable/régulier. □

Corollaire : On a la stabilité par intersection. En effet,

$$L \cap L' = \left(L^{\mathrm{c}} \cup (L')^{\mathrm{c}}\right)^{\mathrm{c}}$$

où L^{c} est le complémentaire de L.

Corollaire : Si L et L' sont deux langages réguliers (quelconques), alors $L \setminus L'$ est un langage régulier. En effet,

$$L \setminus L' = L \cap (L')^{\mathrm{c}}.$$

Corollaire : Si L et L' sont deux langages réguliers. Alors $L \triangle L'$ [3] est un langage régulier. En effet

$$L \triangle L' \overset{(\mathrm{def})}{=} (L \cup L') \setminus (L \cap L').$$

IV.7.1 Limite de la classe/Lemme de l'étoile

Théorème (Lemme de l'étoile) **:** Soit L un langage reconnu par un automate à n états. Pour tout mot $u \in L$ de longueur supérieure ou égale à n, il existe trois mots x, y et z tels que

$$u = x \cdot y \cdot z, \qquad |x \cdot y| \leqslant n, \qquad y \neq \varepsilon, \qquad \text{et} \qquad \forall p \in \mathbb{N},\ x \cdot y^p \cdot z \in L.$$

Preuve :
Soit L un langage reconnu par un automate $\mathscr{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ à n états. Soit u un mot d'un alphabet Σ de longueur supérieure ou égale à n ($u \in \Sigma^{\geqslant n}$) tel que $u \in L$. Alors, il existe un exécution acceptante

$$q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} q_2 \to \cdots \to q_{m-1} \xrightarrow{u_m} q_m$$

avec $m \geqslant n$. Par principe des tiroirs, l'ensemble $\{(i,j) \in [\![0,m]\!]^2 \mid i < j \text{ et } q_i = q_j\}$ est non vide. Et donc $A = \{j \in [\![0,m]\!] \mid \exists i \in [\![0, j-1]\!],\ q_i = q_j\}$ est non vide. Soit alors $j_0 = \min A$ bien défini. Alors, par définition de A, il existe $i_0 \in [\![0, j_0 - 1]\!]$ tel que $q_{i_0} = q_{j_0}$ et $j_0 \leqslant n$. On pose donc

$$\underbrace{q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} \cdots \xrightarrow{u_{i_0}}}_{x} q_{i_0} \underbrace{\xrightarrow{u_{i_0+1}} q_{i_0+1} \to \cdots \xrightarrow{u_{j_0}}}_{y} q_{j_0} \underbrace{\xrightarrow{u_{j_0+1}} q_{j_0+1} \to \cdots \xrightarrow{u_m}}_{z} q_m :$$

$x = u_1 u_2 \dots u_{i_0}$, $y = u_{i_0+1} \dots u_{j_0}$ et $z_{j_0+1} \dots u_m$. On a donc $y \neq \varepsilon$: en effet $i_0 < j_0$. Également, on a $|x \cdot y| = j_0 \leqslant n$ et $u = x \cdot y \cdot z$. Montrons alors que $\forall p \in \mathbb{N}$, $x \cdot y^p \cdot z \in L$. La suite de transitions

$$q_0 \xrightarrow{u_1} q_1 \to \cdots \xrightarrow{u_{i_0}} q_{i_0} \xrightarrow{u_{j_0+1}} q_{j_0+1} \to \cdots \xrightarrow{u_m} q_m$$

est une exécution acceptante donc $x \cdot z \in L$. De proche en proche, on en déduit que $x \cdot y^p \cdot z \in L$ pour tout $p \in \mathbb{N}$. □

3. $\triangle$ est la différence symétrique

Corollaire : Il y a des langages non réguliers/reconnaissables.

Preuve :
Soit $L = \{a^n \cdot b^n \mid n \in \mathbb{N}\}$. Montrons que L n'est pas régulier par l'absurde. Supposons L reconnaissable par un automate $\mathscr{A}$ à n états, et soit $u = a^n \cdot b^n$. Alors $|u| \geqslant n$. D'où, d'après le lemme de l'étoile, il existe un triplet $(x, y, z) \in (\Sigma^\star)^3$ tel que $y \neq \varepsilon$, $u = x \cdot y \cdot z$, $|x \cdot y| \leqslant n$ et $x \cdot y^\star \cdot z \subseteq L$ $(\star)$. Il existe donc $p \in [\![1, n]\!]$ tel que $y = a^p$. De même, il existe $q \in [\![0, n-p]\!]$ tel que $x = a^q$ et $z = a^{n-p-q} \cdot b^n$. Donc, d'après $(\star)$, $x \cdot y \cdot y \cdot z \in L$ et donc $a^q \cdot a^p \cdot a^p \cdot a^{n-p-q} \cdot b^n \in L$, d'où $a^{n+p} \cdot b^n \in L$. Or, comme $p \neq 0$, $n+p \neq n$: une contradiction. □

Exercice :
On considère le langage $L_2 = \{w \in \Sigma^\star \mid |w|_a = |w|_b\}$. *Le langage L_2 est-il régulier ?* La même démonstration fonction en remplaçant L par L_2. Mais, nous allons procéder autrement, par l'absurde : on suppose L_2 régulier. Or, on sait que, d'après la preuve précédente, $L = L_2 \cap a^\star \cdot b^\star$, et $a^\star \cdot b^\star$ est régulier. D'où L régulier, ce qui est absurde.

Exercice :
On considère le langage $L = \{w \in \Sigma^\star \mid |w|_a \equiv |w|_b \ [3]\}$. *Le langage L est-il régulier ?* Oui, l'automate de la figure suivante reconnait le langage L (les états représentent la différence $|w|_a - |w|_b \bmod 3$).

Montrons à présent qu'un automate à moins de trois états n'est pas possible : si $\delta^\star(i_0, a^x) = \delta^\star(i_0, a^y)$ avec $[\![0, 2]\!] \ni x < y \in [\![0, 2]\!]$, alors pour tout $z \in \mathbb{N}$, $\delta^\star(i_0, a^{x+z}) = \delta^\star(i_0, a^{y+z})$. On pose $z = 3 - y$. Alors

$$\delta^\star(i_0, a^{\underset{\not\in F}{x+3-y}}) = \delta^\star(i_0, a^{\underset{\in F}{3}}).$$

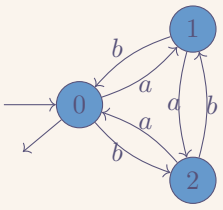


Figure 1.28 – Automate reconnaissant le langage $\{w \in \Sigma^\star \mid |w|_a \equiv |w|_b \ [3]\}$

Exercice :
Soit $\Sigma = \{0, 1, \text{`(`}, \text{`)`}, \text{`\{`}, \text{`\}`}, \text{`,`}\}$. On écrit en OCaml la fonction `to_string` définie telle que si (`affiche` $\mathscr{A}$) et (`affiche` $\mathscr{A}'$) donnent le même affichage, alors $\mathscr{A} = \mathscr{A}'$.

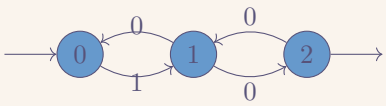


FIGURE 1.29 – Codage d'un automate par une chaîne de caractères

Par exemple, on représente l'automate ci-dessus par

"$\big(\{0,1,10\},\{0\},\{10\},\{(0,0,1),(1,0,10),(10,0,1),(1,1,0)\}\big)$."

```
1 let affiche (Q,I,F,δ) =
```

CODE 1.3 – Fonction `affiche` affichant un automate

À faire : Recopier le code

EXERCICE :
Supposons que tout langage est reconnaissable. Soit $L = \{w \in \Sigma^\star \mid \exists \mathcal{A},\ w \leftarrow \texttt{affiche}\ \mathcal{A} \text{ et } w \notin \mathscr{L}(\mathcal{A})\}$. Soit B un automate tel que $L = \mathscr{L}(B)$. Soit $w \in \texttt{affiche}\ B$. Si $w \in L$, alors il existe un automate tel que $w = \texttt{affiche}\ \mathcal{A}$ et $w \notin \mathscr{L}(\mathcal{A})$. D'où $\mathcal{A} = B$ par injectivité et donc $w \notin \mathscr{L}(B) = L$, ce qui est absurde. Sinon, si $w \notin L$, alors $w = \texttt{affiche}\ B$ avec $w \notin \mathscr{L}(B)$ et $w \in L$, ce qui est absurde.

Annexe 1.A Comment prouver la correction d'un programme ?

Avec $\Sigma = \{a, b\}$. Comment montrer qu'un mot a au moins un a et un nombre pair de b.

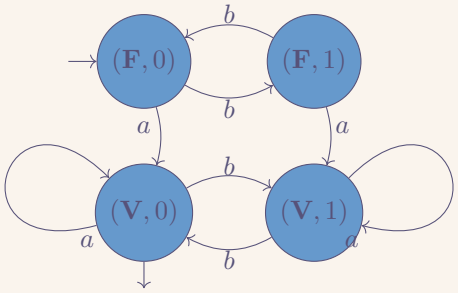


FIGURE 1.30 – Automate reconnaissant les mots valides

On veut montrer que

P_w : « $\forall w \in \Sigma^\star$, $\forall q \in \mathbb{Q}$, (il existe une exécution par w menant à q) $\iff$ w satisfait I_q »

où

$$I_{\underset{\mathbb{B}}{\cap}(v,\ \underset{\{0,1\}}{\cap} r)} \quad : \quad (|w|_a \geqslant 1 \iff v) \text{ et } (r = |w|_b \bmod 2).$$

On le montre par récurrence sur la longueur de w :

“ $\Longrightarrow$ ” — Pour $w = \varepsilon$, alors montrons que $\forall q \in \mathbb{Q}$, il existe un exécution menant à q étiquetée par w (noté $\xrightarrow[\mathcal{A}]{w} q$) si et seulement si w satisfait I_q.

- $\xrightarrow[\mathcal{A}]{\varepsilon} (\mathbf{F}, 0)$ est vrai, de plus ε satisfait $I_{(\mathbf{F},0)}$;
- sinon si $q \neq (\mathbf{F}, 0)$, alors $\xrightarrow[\mathcal{A}]{\varepsilon} q$ est fausse, de plus ε ne satisfait pas I_q.

— Supposons maintenant P_w vrai pour tout mot w de taille n. Soit $w = w_1 \dots w_n w_{n+1}$ un mot de taille $n+1$. Notons $\underline{w} = w_1 \dots w_n$. Montrons que P_w est vrai. Soit $q \in \mathbb{Q}$. Supposons $\xrightarrow[\mathcal{A}]{w} q$.

- Si $q = (\mathbf{F}, 0)$ et $w_{n+1} = b$. On a donc $\xrightarrow[\mathcal{A}]{\underline{w}} (\mathbf{F}, 1)$, et, par hypothèse de récurrence, $\underline{w}$ satisfait. Donc $|\underline{w}|_a = 0$ et $|\underline{w}|_b \equiv 1$ [2] donc $|w|_a = 0$ et $|w|_b \equiv 0$ [2] donc w satisfait $I_{(\mathbf{F},0)}$.
- De même pour les autres cas.

“ $\Longleftarrow$ ” Réciproquement, supposons que w satisfait I_q.

— Si $w = (\mathbf{V}, 0)$ et $w_{n+1} = a$. Alors,

- si $|\underline{w}|_a = 0$, alors $\underline{w}$ satisfait $I_{(\mathbf{F},0)}$. Par hypothèse de récurrence, on a donc $\xrightarrow[\mathcal{A}]{\underline{w}} (\mathbf{F}, 0)$ et donc $\xrightarrow[\mathcal{A}]{w} (\mathbf{V}, 0)$.

— si $|\underline{w}|_b \geqslant 1$, alors $\underline{w}$ satisfait $I_{(\mathbf{V},0)}$ donc $\xrightarrow[\mathcal{A}]{\underline{w}} (\mathbf{V},0)$ et donc $\xrightarrow[\mathcal{A}]{\underline{w}} (\mathbf{V},0)$.

— De même pour les autres cas.

On a donc bien

$$\forall w \in \Sigma^\star, \forall q \in \mathbb{Q},\ \xrightarrow[\mathcal{A}]{w} q \iff w \text{ satisfait } I_q.$$

Finalement,

$$\begin{aligned}\mathscr{L}(\mathcal{A}) &= \{w \in \Sigma^\star \mid \exists f \in F,\ \xrightarrow[\mathcal{A}]{w} f\}\\ &= \{w \in \Sigma^\star \mid \xrightarrow[\mathcal{A}]{w} (\mathbf{V},0)\}\\ &= \{w \in \Sigma^\star \mid w \text{ satisfait } I_{(\mathbf{V},0)}\}\\ &= \{w \in \Sigma^\star \mid |w|_a \geqslant 1 \text{ et } |w|_b \equiv 0\ [2]\}\end{aligned}$$

Annexe 1.B Hors-programme

Définition : On appelle monoïde un ensemble M muni d'une loi "$\cdot$" interne associative admettant un élément neutre 1_M.

Définition : Étant donné deux monoïdes M et N, on appelle morphisme de monoïdes une fonction $\mu : M \to N$ telle que

1. $\mu(1_M) = 1_N$;
2. $\mu(x \cdot_M y) = \mu(x) \cdot_N \mu(y)$.

Exemple :
$|\cdot| : (\Sigma^\star, \cdot) \to (\mathbb{N}, +)$ est un morphisme de monoïdes.

Définition : Un langage L est dit reconnu par un monoïde M, un morphisme $\mu : \Sigma^\star \to M$ et un ensemble $P \subseteq M$ si $L = \mu^{-1}(P)$.

Exemple :
L'ensemble $\{a^{n^3} \mid n \in \mathbb{N}\}$ est reconnu par le morphisme $|\cdot|$ et l'ensemble $P = \{n^3 \mid n \in \mathbb{N}\}$.

Théorème : Un langage est régulier si et seulement s'il est reconnu par un monoïde fini.

Exemple :
L'ensemble $\{a^{2n} \mid n \in \mathbb{N}\}$ est un langage régulier. En effet, on a $M = \mathbb{Z}/2\mathbb{Z}$,

$P = \{0\}$ et

$$\begin{aligned} \mu : \Sigma^\star &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\ w &\longmapsto |w| \bmod 2. \end{aligned}$$

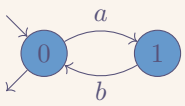


FIGURE 1.31 – Automate reconnaissant $\mu^{-1}(P) = L$

Preuve $\Longleftarrow$ " Soit $L \in \wp(\Sigma^\star)$ reconnu par un monoïde M fini, un morphisme μ et un ensemble $P : L = \mu^{-1}(P)$. Posons $\mathcal{A} = (\Sigma', \mathbb{Q}, I, F, \delta)$ avec

$$\Sigma' = \Sigma \qquad \mathbb{Q} = M \qquad I = \{1_M\} \qquad F = P$$

$$\delta = \{(q, \ell, q') \in \mathbb{Q} \times \Sigma \times \mathbb{Q} \mid q \cdot \mu(\ell) = q'\}.$$

Montrons que $\mathscr{L}(\mathcal{A}) = L$. Soit $w \in \mathscr{L}(\mathcal{A})$. Il existe une exécution acceptante

$$1_M = q_0 \xrightarrow{w_1} q_1 \to \cdots \xrightarrow{w_n} q_n \in P.$$

Or, $\mu(w_1 \dots w_n) = \prod_{i=1}^n \mu(w_i) = q_0 \prod_{i=1}^n \mu(w_i) = q_0 \mu(w_1) \cdot \prod_{i=1}^n \mu(w_i) = q_1 \prod_{i=1}^n \mu(w_i) = q_n \in P$.

□

Chapitre 2

Algorithmes probabilistes

IV.1 Introduction

Dans ce chapitre, on s'intéresse aux algorithmes probabilistes de deux types : Monte-Carlo et Las-Vegas. L'idée est de donner une définition plus mathématique d'un « algorithme probabiliste » et de l'influence de l'aléatoire.

> **Définition :** Un algorithme *déterministe* est un algorithme tel que pour chaque entrée I de l'algorithme, l'exécution de l'algorithme produit toujours exactement la même suite d'états.

Remarque :
Un algorithme déterministe produit donc toujours les même sorties sur les mêmes entrées.

> **Définition :** Un algorithme *probabiliste* est un algorithme opérant sur un ensemble $\mathscr{E}$, tel que la suite d'états obtenus par exécution de l'algorithme sur une entrée $e \in \mathscr{E}$ est une variable aléatoire.

Remarque :
Avec cette définition, un algorithme déterministe est un algorithme probabiliste.

Exemple :
On considère le problème suivant :

$$\text{Problème Tri} : \begin{cases} \text{Entrée} & : \text{ un tableau } T \text{ de taille } n \\ \text{Sortie} & : T \text{ trié.} \end{cases}$$

Une réponse à ce problème est l'algorithme nommé Bozosort décrit ci-dessous. On le nomme aussi « tri aléatoire. »

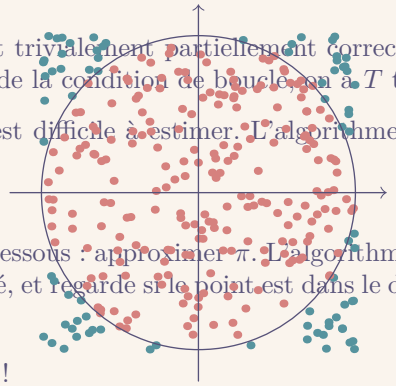
Algorithme 2.1 BOZOSORT

Entrée T un tableau
1 : **tant que** T non trié **faire**
2 : $\quad i \leftarrow \mathcal{U}(\llbracket 1, n-1 \rrbracket)$
3 : $\quad j \leftarrow \mathcal{U}(\llbracket 1, n-1 \rrbracket)$
4 : $\quad$ Échanger i et j dans le tableau T

On étudie l'algorithme ci-dessus : il est trivialement partiellement correct (i.e. s'il est correct). En effet, par négation de la condition de boucle, on a T trié.

Le temps d'exécution de l'algorithme est difficile à estimer. L'algorithme peut ne pas terminer.

EXEMPLE :
On considère à présent le problème ci-dessous : approximer π. L'algorithme tire des points au hasard dans un carré unité, et regarde si le point est dans le disque unité.



!

FIGURE 2.1 – Algorithme de MONTE-CARLO pour approximer π

On compte le nombre de points dans le disque, et ceux en dehors. Avec un grand nombre de points, on approxime le ratio de l'aire du disque et de l'aire du carré. Puis, on calcule

$$4 \times \left(\frac{\#\bullet}{\#\bullet + \#\bullet} \right) \approx \pi.$$

Le temps d'exécution dépend uniquement des paramètres de précision de l'algorithme, pas des tirages. Par contre, la qualité de la réponse dépend des choix aléatoires.

Définition (Algorithme de type LAS VEGAS) **:** Étant donné un problème P, un algorithme probabiliste répondant au problème P est dit de type LAS VEGAS dès lors que, s'il se termine, c'est en donnant une réponse correcte.

Définition (Algorithme de type MONTE-CARLO) **:** Étant donné un problème P, un algorithme probabiliste répondant au problème P est dit de type MONTE-CARLO dès lors que son temps d'exécution dépend uniquement de son entrée. L'algorithme peut cependant répondre de manière erronée au problème P avec une « certaine » probabilité.

REMARQUE :
Dans le cas d'un problème de décision (la réponse de l'algorithme est OUI ou NON), un algorithme de type MONTE-CARLO est dit

— « à erreur unilatérale » s'il existe une des réponses (OUI ou NON) r telle que, si l'algorithme répond r, alors il a raison (r est la réponse au problème) ;
— « à erreur bilatérale » si pour chaque réponse l'algorithme se trompe avec une probabilité non nulle.

EXEMPLE :
On considère le problème : étant donné un tableau $T \in \{0,1\}^n$ tel que T contient p fois la valeur '0', avec $0 < p < n$, on cherche si, pour $i \in [\![1, n-1]\!]$, $T[i] = 1$.

Une réponse à ce problème est un algorithme de type MONTE-CARLO, comme celui ci-dessous.

Algorithme 2.2 Algorithme de MONTE-CARLO pour répondre au problème

Entrée $k \in \mathbb{N}$ et T un tableau
1 : $i \leftarrow 0$
2 : **pour** $j \in [\![1, k]\!]$ **faire**
3 : $\quad i \leftarrow \mathcal{U}([\![1, n-1]\!])$
4 : $\quad$ **si** $T[i] = 1$ **alors**
5 : $\quad\quad$ **retourner** i
6 : **retourner** i

Mais, on peut également donner un algorithme de LAS-VEGAS répondant aussi au même problème.

Algorithme 2.3 Algorithme de LAS-VEGAS pour répondre au problème

Entrée T un tableau
1 : $i \leftarrow \mathcal{U}([\![1, n-1]\!])$
2 : **tant que** $T[i] \neq 1$ **faire**
3 : $\quad i \leftarrow \mathcal{U}([\![0, n-1]\!])$
4 : **retourner** i

Étudions l'algorithme de LAS-VEGAS : la correction partielle est validée. Étudions la terminaison : fixons T un tableau de taille n contenant p occurrences de '0' avec $0 < p < n$. Notons $(X_\ell)_{\ell \in \mathcal{D}}$ la suite des variables aléatoires donnant la valeur produite par le ℓième appel à $\mathcal{U}([\![0, 1]\!])$. Remarquons que $\mathcal{D}$ est une variable aléatoire : en effet c'est $[\![0, N]\!]$ pour un certain $N \in \mathbb{N}$ si l'algorithme se termine ; sinon, on a $\mathcal{D} = \mathbb{N}$. Notons A_q l'événement « l'algorithme s'arrête après q appels au générateur $\mathcal{U}([\![0, n-1]\!])$. On a donc

$$A_q = \text{“}T[X_0] = 0 \wedge T[X_1] = 0 \wedge \cdots \wedge T[X_{q-2}] = 0 \wedge T[X_{q-1}] = 1\text{”}.$$

D'où en passant aux probabilités, on a

$$P(A_q) = P(\text{“}T[X_0] = 0 \wedge T[X_1] = 0 \wedge \cdots \wedge T[X_{q-2}] = 0 \wedge T[X_{q-1}] = 1\text{”})$$

et, par indépendance, on a donc

$$P(A_q) = P(T[X_{q-1} = 1) \times \Big(\prod_{j=0}^{q-2} P(T[X_j] = 0) \Big).$$

Or, $\forall j \in [\![0, q-2]\!]$, $P(T[X_j] = 0) = \frac{p}{n}$ par uniformité, et, de plus, $P(T[X_{q-1}] = 1) = \frac{n-p}{n}$ par uniformité. On pose $\rho = \frac{p}{n}$, et donc $P(A_q) = \rho^{q-1}(1-\rho)$. Notons N l'événement « l'algorithme ne se termine pas » et calculons

$$\begin{aligned} P(N) &= 1 - P(\bar{N}) \\ &= 1 - P\Big(\bigvee_{q \in \mathbb{N}^\star} A_q\Big) \\ &= 1 - \sum_{q \in \mathbb{N}^\star} P(A_q) \\ &= 1 - \sum_{q \in \mathbb{N}^\star} \rho^{q-1}(1-\rho) \\ &= 1 - \frac{1-\rho}{1-\rho} \\ &= 0 \end{aligned}$$

Soit $\mathcal{T}$ la variable aléatoire indiquant le temps d'arrêt de l'algorithme (en nombre d'itérations). On calcule l'espérance de $\mathcal{T}$:

$$\begin{aligned} \mathrm{E}(\mathcal{T}) &= \sum_{t=1}^{+\infty} t \times P(\mathcal{T} = t) \\ &= \sum_{t=1}^{+\infty} t \times \rho^{t-1}(1-\rho) \\ &= (1-\rho) \sum_{t=1}^{+\infty} t \times \rho^{t-1} \\ &= (1-\rho) \sum_{t=1}^{+\infty} \sum_{k=0}^{t-1} \rho^t \\ &= (1-\rho) \sum_{k=0}^{+\infty} \sum_{t=k+1}^{+\infty} \rho^{t-1} \\ &= \cdots\cdots \text{ [1]} \\ &= \frac{1}{1-\rho} \end{aligned}$$

Étudions maintenant l'algorithme de Monte-Carlo. Il se termine trivialement, et la probabilité d'erreur est $\underbrace{\rho \times \cdots \times \rho}_{k}$. Par exemple, pour $\rho = \frac{1}{2}$, et $k = 80$, la probabilité d'erreur est de $\frac{1}{2^{80}}$.

IV.2 Algorithme de Monte-Carlo

On considère le problème : « étant donné trois matrices A, B, C de $\mathscr{M}_n(\mathbb{Z}/2\mathbb{Z})$, a-t-on $A \cdot B = C$? »

1. à faire

Un algorithme trivial serait de calculer $A \cdot B$ et on vérifie, point à point, que $A \cdot B = C$. La complexité cet algorithme est en $\Theta(n^3)$ à cause du produit matriciel.

Un algorithme de Monte-Carlo serait le suivant.

Algorithme 2.4 Algorithme de Monte-Carlo répondant au problème

Entrée A, B, C trois matrices et $k \in \mathbb{N}$

```
pour j ∈ ⟦1, k⟧ faire
    r ← 𝒰((ℤ/2ℤ)^n)        ▷ n
    r_1 ← B · r            ▷ n^2
    r_2 ← A · r_1          ▷ n^2
    r_3 ← C · r            ▷ n^2
    si r_3 ≠ r_2 alors
        retourner Non
retourner Oui
```

Dans le pire cas, la complexité est en $k \times n^2$. On cherche la probabilité d'erreur de cet algorithme. Pour cela, on utilise le lemme suivant.

Lemme : Si $D \neq 0$, et $r \sim \mathcal{U}\big((\mathbb{Z}/2\mathbb{Z})^n\big)$, alors $P(D \cdot r = 0) \leqslant \frac{1}{2}$.

Preuve :
Si $D \in \mathcal{M}_n(\mathbb{Z}/2\mathbb{Z}) \setminus \{0\}$, alors il existe i et j tels que $D_{i,j} \neq 0$. Si $D \cdot r = 0$, on a

$$\sum_{k=1}^{n} D_{i,k} r_k = 0 \quad \text{et donc} \quad r_k = -\sum_{\substack{k=1 \\ k \neq j}}^{n} D_{i,k} r_k.$$

Donc, si $r_j \neq \sum_{\substack{k=1 \\ k \neq j}}^{n} D_{ik} r_k$, alors $P(D \cdot r \neq 0) \geqslant P\Big(r_j \neq \sum_{\substack{k=1 \\ k \neq j}}^{n} D_{i,k} r_k\Big)$.
On note E_0 l'événement « $r_j = 0$ et $\sum_{\substack{k=1 \\ j \neq j}}^{n} D_{i,k} r_k = 1$ » et E_1 l'événement « $r_j = 1$ et $\sum_{\substack{k=1 \\ j \neq j}}^{n} D_{i,k} r_k = 0$. » D'où

$$P\Big(r_j \neq \sum_{\substack{k=1 \\ j \neq j}}^{n} D_{i,k} r_k\Big) = P(E_0 \vee E_1).$$

Par incompatibilité, on a $P(E_0 \vee E_1) = P(E_0) + P(E_1)$, d'où

$$\forall a \in \{0,1\}, \quad P(E_a) = P\Big(r_j = a \wedge \sum_{\substack{k=1 \\ j \neq j}}^{n} D_{i,k} r_k = 1 - a\Big)$$

et, par indépendance,

$$\forall a \in \{0,1\} \quad P(E_a) = P(r_j = a) \cdot P\Big(\sum_{\substack{k=1\\ j\neq j}}^{n} D_{i,k} r_k = 1 - a\Big) = \frac{1}{2} P(\ldots).$$

D'où

$$P\Big(r_j \neq \sum_{\substack{k=1\\ j\neq j}} D_{i,k} r_k\Big) = \frac{1}{2}\Big[P\Big(\sum_{\substack{k=1\\ j\neq j}}^{n} D_{i,k} r_k = 1\Big) + P\Big(\sum_{\substack{k=1\\ j\neq j}}^{n} D_{i,k} r_k = 0\Big)\Big]$$

et, par incompatibilité,

$$P\Big(r_j \neq \sum_{\substack{k=1\\ j\neq j}} D_{i,k} r_k\Big) = \frac{1}{2}\frac{1}{2} P\Big(\sum_{\substack{k=1\\ j\neq j}} D_{i,k} r_k \in \{0,1\}\Big) = \frac{1}{2}.$$

□

D'où, l'algorithme ci-dessous est tel que sa probabilité d'échec est de $\frac{1}{2^k}$. Or, l'algorithme a une complexité de $\mathcal{O}(k\,n^2)$.

IV.3 Algorithme de type Las-Vegas

On étudie le tri rapide. On considère les fonctions " Partitionner," puis " Tri Rapide."

Algorithme 2.5 Fonction "Partitionner" utilisée dans le tri rapide

Entrée T le tableau à trier, g, d et p trois entiers (bornes du tableau)
Sortie un entier J et le sous-tableau $T[g..d]$ est modifié en $\bar{T}$ de sorte que $\bar{T}$[2]$[J] = \underline{T}[p]$, et $\forall i \in [\![g, J-1]\!]$, $\bar{T}[i] \leqslant \bar{T}[J]$, et $\forall i \in [\![J+1, d]\!]$, $\bar{T}[i] \geqslant \bar{T}[J]$, et $\forall i \in [\![0, n-1]\!] \setminus [\![g, d]\!]$, $\bar{T}[i] = \underline{T}[i]$, et $\bar{T}$ est une permutation de $\underline{T}$.

```
1 : ÉCHANGER(T, J, d)
2 : J ← g
3 : I ← g
4 : tant que I < d faire
5 :     si T[I] > T[d] alors        ▷ Cas "T[I] > pivot"
6 :         I ← I + 1
7 :     sinon                       ▷ Cas "T[I] ⩽ pivot"
8 :         ÉCHANGER(T, I, J)
9 :         J ← J + 1
10 :        I ← I + 1
11 : ÉCHANGER(T, J, d)
12 : retourner J
```

2. La notation $\bar{T}$ représente le tableau T après l'algorithme, et la notation $\underline{T}$ représente le tableau T avant l'algorithme.

Remarque :
On admet que $\bar{T}$ est une permutation de $\underline{T}$. On admet également que, $\forall i \in [\![0, n-1]\!] \setminus [\![g, d]\!]$, $\bar{T}[i] = \underline{T}[i]$.

Lemme : "Partitionner" est correct.

Preuve :
On considère

$$(\mathcal{I}) : \begin{cases} \forall k \in [\![g, I]\!]\,,\ T[k] \leqslant T[d] & (1) \\ \forall k \in [\![J, I-1]\!]\,,\ T[k] > T[d] & (2)\ . \\ g \leqslant J \leqslant I \leqslant d & (3) \end{cases}$$

— Montrons que $\mathcal{I}$ est vrai initialement : à l'initialisation, $I = g$ et $J = g$, donc les trois propriétés $(\mathcal{I})$ sont trivialement vraies.
— Montrons que l'invariant $(\mathcal{I})$ se propage. Notons $\underline{I}$, $\underline{J}$, et $\underline{T}$ les valeurs de I, J et T avant itération de boucle. Notons également $\bar{I}$, $\bar{J}$ et $\bar{T}$ les valeurs de I, J et T après cette même itération de boucle. Supposons que $\underline{I}$, $\underline{J}$ et $\underline{T}$ vérifient $(\mathcal{I})$, et la condition de boucle. Montrons que $\bar{I}$, $\bar{J}$ et $\bar{T}$ vérifient $(\mathcal{I})$. On a donc, d'après $(\mathcal{I})$,

$$\begin{cases} \forall k \in [\![g, \underline{J}-1]\!]\,,\ \underline{T}[k] \leqslant \underline{T}[d] \\ \forall k \in [\![\underline{T}, \underline{I}-1]\!]\,,\ \underline{T}[k] > \underline{T}[d] \\ g \leqslant \underline{J} \leqslant \underline{I} \leqslant d. \end{cases}$$

Mais aussi, d'après la condition de boucle, $\underline{I} \leqslant d$. Mais également, d'après le programme,
— si $\underline{T}[\underline{I}] > \underline{T}[d]$, alors $\bar{I} = \underline{I} + 1$, $\bar{T} = \underline{T}$, et $\bar{J} = \underline{J}$;
— sinon si $\underline{T}[\underline{I}] \leqslant \underline{T}[d]$, et donc $\bar{J} = \underline{J} + 1$, $\bar{I} = \underline{I} + 1$, $\forall k \in [\![0n, -1]\!] \setminus \{\underline{I}, \underline{J}\}$, $\bar{T}[k] = \underline{T}[k]$, et $\bar{T}[\bar{I}] = \underline{T}[J]$, et $\bar{T}[J] = \underline{T}[\underline{I}]$.

Cas 1 $\underline{T}[\underline{I}] > \underline{T}[d]$, alors
(3) $g \leqslant \underline{J} = \bar{J} \leqslant \underline{I} < \bar{I} \leqslant d$.
(1) Soit $k \in [\![g, \bar{J}-1]\!]$, on a donc $k \in [\![g, \underline{J}-1]\!]$, et donc $\bar{T}[k] = \underline{T}[k] \leqslant \underline{T}[d] = \bar{T}[d]$.
(2) Soit $k \in [\![\bar{J}, \bar{I}-1]\!]$,
— si $k \in [\![\underline{J}, \underline{I}-1]\!]$, alors $\bar{T}[k]$ă $= \underline{T}[k] > \underline{T}[d] = \bar{T}[d]$.
— si $k = \bar{I} - 1 = \underline{I}$, par condition `if`, alors $\bar{T}[\underline{I}] = \underline{T}[\underline{I}] > \underline{T}[d] = \bar{T}[d]$.

Cas 2 $\underline{T}[\underline{I}] \leqslant \underline{T}[d]$
(3) On a $\underline{J} \leqslant \underline{I}$, donc $\underline{J}+1 \leqslant \underline{I}+1$, d'où $g \leqslant \underline{J}+1 = \bar{J} \leqslant \bar{I} \leqslant d$.
(1) Soit $k \in [\![g, \bar{J}-1]\!]$, donc
— si $k \in [\![g, \underline{J}-1]\!]$, alors $\bar{T}[k] = \underline{T}[k] \leqslant \underline{T}[d] = \bar{T}[d]$.

— si $k = \bar{J} - 1 = \underline{J}$, alors $\bar{T}[k] = \bar{T}[\underline{J}] = \underline{T}[\underline{I}] \leqslant \underline{T}[d] = \bar{T}[d]$.

(2) Soit $k \in [\![\bar{J}, \bar{I} - 1]\!]$, alors

— si $k \in [\![\bar{J}, \underline{J} - 1]\!]$, alors, comme $\bar{J} \geqslant \underline{J}$, et donc $\bar{T}[k] = \underline{T}[k] > \underline{T}[d] = \bar{T}[d]$.

— si $k = \bar{I} - 1 = \underline{I}$, et donc $\bar{T}[k] = \bar{T}[\underline{I}] = \bar{T}[\underline{J}] > \underline{T}[d] = \bar{T}[d]$.

Ainsi, $(\mathcal{I})$ est un invariant, et donc, en sortie de boucle, I, J et T sont tels que

$$\left.\begin{array}{l} \forall k \in [\![g, J-1]\!]\,,\ T[k] \leqslant T[d] \\ \forall k \in [\![J, I-1]\!]\,,\ T[k] > T[d] \\ g \leqslant J \leqslant I \leqslant d \end{array}\right\} \quad \text{et} \quad I \geqslant d,$$

la négation de la condition de boucle. On a donc $I = d$, et donc en fin de programme,

$$\forall k \in [\![g, J-1]\!]\,,\ T[k] \leqslant T[J] \quad \text{et} \quad \forall k \in [\![J+1, I]\!]\,,\ T[k] > T[J].$$

□

Algorithme 2.6 Tri rapide

Entrée T un tableau, g et d les bornes de ce tableau

```
1 : si d > g alors
2 :     p ← ChoixPivot(T, g, d)
3 :     J ← Partition(T, g, d, p)
4 :     TriRapide(T, g, J − 1)
5 :     TriRapide(T, J + 1, d)
```

La fonction "Tri(T)" est donc définie comme TriRapide($T, 0, n-1$) si T est un tableau de taille n.

Étudions rapidement l'influence du choix du pivot.

Cas 1 On définit "ChoixPivot$(T, g, d) = g$." Ainsi

À faire : Figure

Figure 2.2 – Arbre des appels récursifs de "TriRapide" avec le pivot à gauche

Ainsi, la complexité de cet algorithme, avec ce choix de pivot, est en $(n-1) + (n-2) + (n-3) + \cdots + 2 = \Theta(n^2)$.

Cas 2 On définit maintenant le choix du pivot comme l'indice de la médiane.

À faire : Figure

Figure 2.3 – Arbre des appels récursifs de "TriRapide" avec le pivot à la médiane

Rédigeons-le rigoureusement : soit $C_n = \max_{T \text{ tableau de taille } n} C(T)$. Posons $(u_p)_{p\in\mathbb{N}} = (C_{2^p})_{p\in\mathbb{N}}$. D'après l'algorithme de "TriRapide," on a

$$\begin{aligned} u_{p+1} &= 2^{p+1} - 1 + u_p + u_p \\ &= 2^{p+1} - 1 + 2u_p \\ &= (2^{p+1} - 1) + 2(2^p - 1) + 2^2 u_{p-1} \\ &= 2^{p+1} - 1 + 2^{p+1} - 2 + 2^2 u_{p-1} \\ &= 2^{p+1} - 1 + 2^{p+1} - 2 + 2^2(2^{p-1} - 1 + 2u_{p-2}) \\ &= 2^{p+1} - 1 + 2^{p+1} - 2 + 2^{p+1} - 2^2 + 2^3 u_{p-2}. \end{aligned}$$

On a donc $u_0 = 1$ et $u_p = p \times 2^p - (2^p - 1)$. Or, la suite $(c_n)_{n\in\mathbb{N}}$ est croissante. Or,

$$\forall n \in \mathbb{N},\ 2^{\lfloor \log_2 n \rfloor} \leqslant n \leqslant 2^{\lfloor \log_2 n \rfloor + 1}$$

donc

$$u_{\lfloor \log_2 n \rfloor} \leqslant C_n \leqslant u_{\lfloor \log_2 n \rfloor + 1}.$$

D'où

$$c_n \leqslant (\lfloor \log_2 n \rfloor + 1) \times 2^{\lfloor \log_2 n \rfloor + 1} - 2^{\lfloor \log_2 n \rfloor - 1}.$$

Et donc, on en déduit que $c_n = \Theta\big(n \log_2(n)\big)$.

Remarque (Notations) :
On fixe un tableau T de taille n. De plus, on suppose dans toute la suite, que $T \in \mathfrak{S}_n$.[3] On note alors $X_g^d[T]$ la variable aléatoire indiquant le nombres de comparaisons effectuées par l'algorithme TriRapide(T, g, d), dès lors que $T(\llbracket g, d \rrbracket) \subseteq \llbracket g, d \rrbracket$.

On note de plus, $\mathrm{E}\big[X_g^d[T]\big]$ l'espérance de cette variable aléatoire.

Théorème : Le nombre moyen de comparaisons effectuées par l'algorithme de tri rapide pour une entrée T de taille n est équivalent à $2n \ln n$. Autrement dit,

$$\mathrm{E}\big[X_0^{n-1}[T]\big] \sim 2n \ln n.$$

Preuve :
— Lorsque $d \leqslant g$, alors $X_g^d[T] = 0$.
— Lorsque $g < d$,
  — dans l'éventualité d'un choix de pivot d'indice $p \in \llbracket g, d \rrbracket$, le

3. T est une permutation de n éléments. Ici, $\mathfrak{S}_n$ représente l'ensemble des permutations de $\llbracket 1, n \rrbracket$.

nombre de comparaisons est alors

$$\underbrace{d-g-1}_{\text{coût de } \textsc{Partition}(T,g,d,p)} + \overbrace{X_g^{T[p]-1}\left[T^{g,d,p}\right]}^{\text{coût du } 1^{\text{er}} \text{ appel récursif}} + \underbrace{X_{T[p]+1}^{d}\left[T^{g,d,p}\right]}_{\text{coût du } 2^{\text{nd}} \text{ appel récursif}}$$

où $T^{g,d,p}$ est le tableau T après appel à $\textsc{Partition}(T,g,d,p)$. D'où

$$\begin{aligned}
\mathrm{E}\left[X_g^d[T]\right] &= \sum_{j=g}^{d} \mathrm{E}\Big[X_g^d[T]\Big|_{p=j}\Big] \cdot P(p=j) \\
&= \frac{1}{d-g+1}\sum_{j=g}^{d} \mathrm{E}\Big[X_g^d[T]\Big|_{p=j}\Big] \\
&= \frac{1}{d-g+1}\sum_{j=g}^{d} \Big(d-g-1+\mathrm{E}\Big[X_g^{T[j]-1}\Big[T^{g,d,j}\Big]\Big] \\
&\qquad\qquad + \mathrm{E}\Big[X_{T[j]+1}^{d}\Big[T^{g,d,j}\Big]\Big]\Big) \\
&= (d-g-1) + \frac{1}{d-g+1}\sum_{k=g}^{d} \Big(\mathrm{E}\Big[X_g^{k-1}\Big[T^{g,d,T^{-1}[k]}\Big]\Big] \\
&\qquad\qquad + \mathrm{E}\Big[X_{k+1}^{d}\Big[T^{g,d,T^{-1}[k]}\Big]\Big]\Big)
\end{aligned}$$

car $T : [\![g,d]\!] \to [\![g,d]\!]$ est une bijection.

Soit donc la suite $(c_\ell)_{\ell\in\mathbb{Z}}$ définie par

$$\begin{cases} \forall \ell \in \mathbb{Z}^-, & c_\ell = 0 \\ \forall \ell \in \mathbb{N}^\star, & c_\ell = \mathrm{E}\big[X_0^\ell[\mathrm{id}]\big]. \end{cases}$$

On a alors

$$\begin{aligned}
\forall \ell \in \mathbb{N}^\star, \quad c_\ell &= (\ell-1) + \frac{1}{\ell-1}\sum_{k=0}^{\ell}(c_{k-1} - c_{\ell-k-1}) \\
c_\ell &= (\ell-1) + \frac{2}{\ell+1}\sum_{k=1}^{\ell-1} c_k \\
(\ell+1)c_\ell &= (\ell+1)(\ell-1) + 2\sum_{k=1}^{\ell-1} c_k
\end{aligned}$$

D'où, $\ell c_\ell = \ell(\ell-2) + 2\sum_{k=1}^{\ell-2} c_k$, et donc

$$(\ell+1)c_\ell - \ell c_{\ell-1} = \ell^2 - 1 - \ell^2 + 2\ell + 2c_{\ell-1}.$$

On en déduit donc que

$$(\ell+1)c_\ell - (\ell+2)c_{\ell-1} = 2\ell - 1$$

et donc

$$\frac{c_\ell}{\ell+2} - \frac{c_{\ell-1}}{\ell+1} = \frac{2\ell-1}{(\ell+1)(\ell+2)}.$$

Soit alors $(u_\ell)_{\ell\in\mathbb{N}} = \big(c_\ell/(\ell+2)\big)_{\ell\in\mathbb{N}}$, et $u_0 = 0$. Alors

$$u_\ell = \sum_{k=1}^{n}(u_k - u_{k-1}) = \sum_{k=1}^{n}\frac{2k-1}{(k+1)(k+2)}$$

or $\frac{2k-1}{(k+1)(k+2)} \sim \frac{2}{k}$, et $\sum_{k\geqslant 1}\frac{2}{k}$ diverge donc $u_\ell \sim \sum_{k=1}^{\ell}\frac{2}{k} \sim 2\ln\ell$. On en déduit donc que $c_\ell \sim 2\ell\ln\ell$.

□

Dans la preuve précédente, on a utilisé le lemme suivant.

Lemme : Soit $(g,d) \in \mathbb{N}^2$ et soit $T \in \mathfrak{S}_n$ une permutation telle que $T(\llbracket g,d \rrbracket) \subseteq \llbracket g,d \rrbracket$.

$$\mathrm{E}\Big[X_g^d[T]\Big] = \mathrm{E}\Big[X_0^{d-g}[\mathrm{id}]\Big].$$

Preuve (par récurrence forte sur $d-g=\ell \in \mathbb{N}$) *:* — Soient $(g,d) \in \mathbb{N}^2$ tel que $d-g=0$. Soit $T \in \mathfrak{S}_n$ telle que $T(\llbracket g,d \rrbracket) \subseteq \llbracket g,d \rrbracket$. On a bien $X_g^d[T]=0=X_0^{d-g}[\mathrm{id}]$.

— On remarque, par hypothèse de récurrence,

$$\mathrm{E}\Big[X_g^{k-1}\Big[\overbrace{T^{g,d,T^{-1}[k]}}^{k-1-g<d-g}\Big]\Big] = \mathrm{E}\Big[X_0^{k-1-g}[\mathrm{id}]\Big]$$

et

$$\mathrm{E}\Big[X_{k-1}^{d}\Big[T^{g,d,T^{-1}[k]}\Big]\Big] = \mathrm{E}\Big[X_0^{d-k-1}[\mathrm{id}]\Big].$$

On a alors

$$\begin{aligned}
&\mathrm{E}\Big[X_g^d[T]\Big] \\
&= (d-g-1) + \frac{1}{d-g+1}\sum_{k=g}^{d}\left(\mathrm{E}\Big[X_g^{k-1}\Big[T^{g,d,T^{-1}[k]}\Big]\Big] + \mathrm{E}\Big[X_{k-1}^{d}\Big[T^{g,d,T^{-1}[k]}\Big]\Big]\right) \\
&= (d-g-1) + \frac{1}{d-g-1}\sum_{k=g}\left(\mathrm{E}\Big[X_0^{k-1-g}[\mathrm{id}]\Big] + \mathrm{E}\Big[X_0^{d-k-1}[\mathrm{id}]\Big]\right).
\end{aligned}$$

Ceci est vrai pour tout $T \in \mathfrak{S}_n$ telle que $T(\llbracket g,d \rrbracket) \subseteq \llbracket g,d \rrbracket$, donc

$$\begin{aligned}
\mathrm{E}\big[X_g^d[\mathrm{id}]\big] &= (d-g-1) + \frac{1}{d-g-1}\sum_{k=g}\left(\mathrm{E}\Big[X_0^{k-1-g}[\mathrm{id}]\Big] + \mathrm{E}\Big[X_0^{d-k-1}[\mathrm{id}]\Big]\right) \\
&= \mathrm{E}\big[X_g^d[T]\big]
\end{aligned}$$

□

Annexe 2.A Hors-programme

Chapitre 3

Apprentissage

IV.1 Motivation

L'INTELLIGENCE ARTIFICIELLE est vue comme un « objet magique » mais ce n'est pas le cas : c'est ce que nous allons étudier dans ce chapitre. Il existe plusieurs méthodes permettant l'apprentissage : descente de gradient, k-plus proches voisins, ...

La base de donnée la plus utilisée est MNIST : elle contient 60 000 images de 28×28 pixels représentant un chiffre, et le chiffre correspondant. L'idée de l'apprentissage est de « deviner » le chiffre dessiné en connaissant l'image.

IV.2 Vocabulaire

Définition : On appelle *signature de données* un n-uplet de paires nom, ensemble ; on le typographie

$$\big(\text{nom}_1 : S_1, \text{nom}_2 : S_2, \dots, \text{nom}_n : S_n\big).$$

EXEMPLE : 1. $\mathbb{S}_1 = \big(\text{titre} : \text{string}, \text{longueur} : \mathbb{N}, \text{date} : \mathbb{N}\big)$,
2. $\mathbb{S}_2 = \big(x : \mathbb{R}, y : \mathbb{R}\big)$,
3. $\mathbb{S}_3 = \big(R : [\![0, 255]\!], G : [\![0, 255]\!], B : [\![0, 255]\!]\big)$.

Définition : Étant donné une signature de données $\mathbb{S} = \big(\text{nom}_1 : S_1, \dots, \text{nom}_n : S_n\big)$, on appelle *donnée* un vecteur

$$\bar{v} = (v_1, v_2, \dots, v_n) \in S_1 \times S_2 \times \cdots \times S_n.$$

EXEMPLE : 1. $\big(\text{“2001, a space odyssey”}, 139, 1968\big)$ est une donnée/un vecteur de signature $\mathbb{S}_1$.

2. $(\pi, \sqrt{2})$ est une donnée/un vecteur de signature $\mathbb{S}_2$.

Définition : Étant donné une signature de données $\mathbb{S}$, on appelle *jeu de données* un ensemble fini de vecteurs de signature $\mathbb{S}$.

Définition : Étant donnée une signature de données $\mathbb{S}$ et un ensemble de classes $\mathscr{C}$, on appelle *jeu de données classifié* la donnée
— d'un jeu de données S,
— d'une fonction $f : S \to \mathscr{C}$ de classification.

IV.3 Apprentissage supervisé

L'objectif de cette section est de construire des fonctions de classification, à partir d'un jeu de données classifié.

Définition : Étant donné une signature de données $\mathbb{S}$, et un ensemble de classes $\mathscr{C}$, on appelle *fonction de classification* une fonction des données de signature $\mathbb{S}$ dans $\mathscr{C}$.

Remarque :
On discutera de la « qualité » d'une fonction de classification en fonction de ses résultats sur les données d'un jeu de données et sur des exemples de tests.

IV.3.1 k plus proches voisins

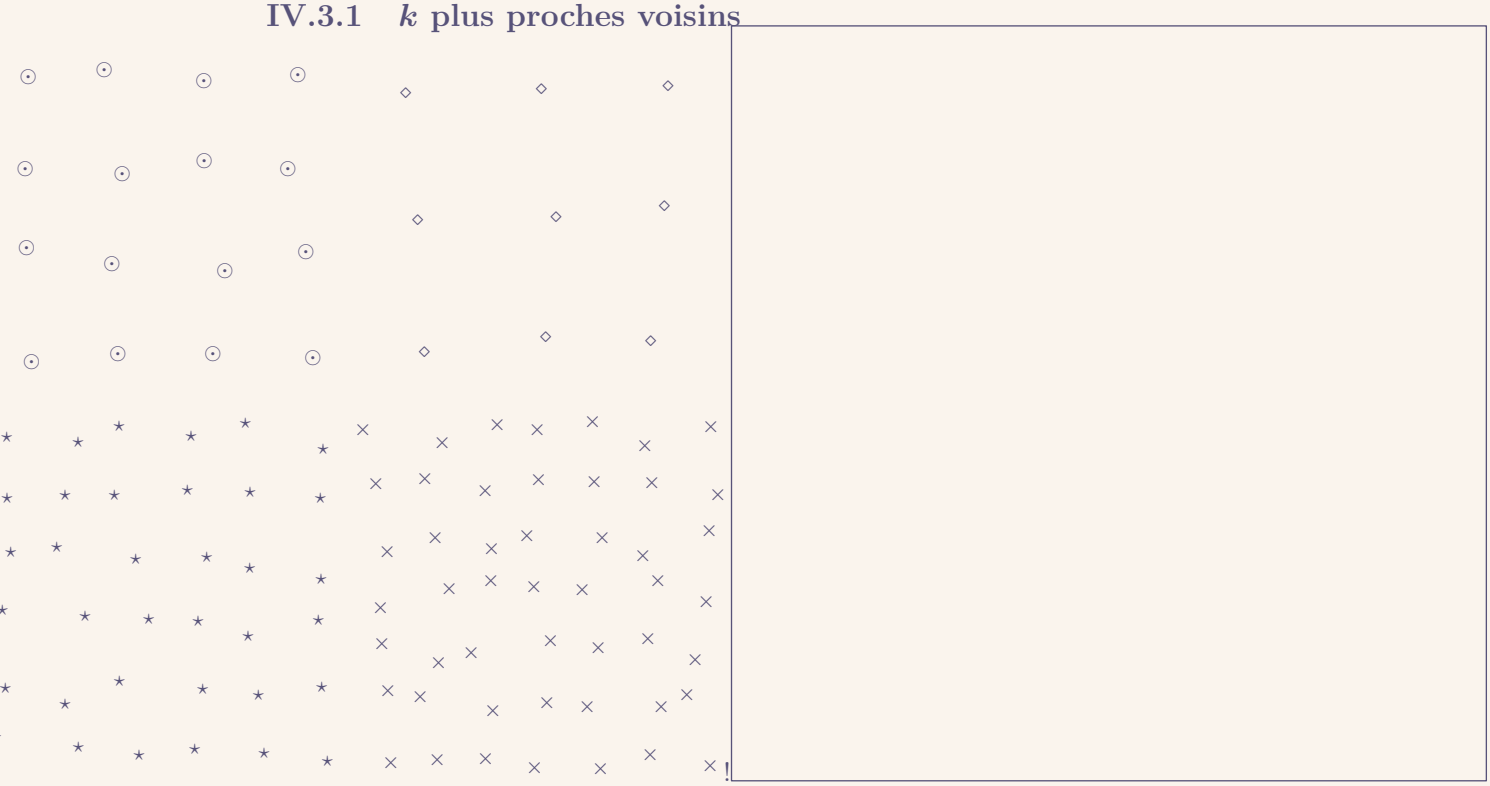


FIGURE 3.1 – Représentation de l'algorithme des k plus proches voisins

Algorithme 3.1 k-NN (k *nearest neighbors*)

Entrée Un jeu de données classifié (S, c), un vecteur d'entrée $\bar{v}$

On trie S par distance croissante de v en d_1, d_2, …, d_k, d_{k+1}, …
Soit D un dictionnaire de $\mathscr{C}$ vers $\mathbb{N}$ initialisé à 0 [1]
pour $j \in [\![1, k]\!]$ **faire**
    $D\big[c(d_j)\big] \leftarrow D\big[c(d_j)\big] + 1$
retourner $\operatorname{argmax}_{d \in \mathscr{C}} D[d]$

REMARQUE :
On doit avoir $k \leqslant n$, et l'espace doit être muni d'une distance. Les résultats de l'algorithme dépendent fortement du jeu de données, du paramètre k et de la distance choisie.

Matrice de confusion

Définition : On appelle *matrice de confusion* d'un algorithme de

1. où toutes les valeurs sont initialisées à 0, pas un dictionnaire vide

prédiction $\mathscr{A}$ sur un jeu de données classifié (T, c), la matrice

$$\Big(\operatorname{Card}\{t \in T \mid \mathscr{A}(t) = i \text{ et } c(t) = j\}\Big)_{(i,j)\in\mathscr{C}^2}.$$

Dans le cas particulier d'une classification $(\mathbf{V}, \mathbf{F})$, on nomme

$\mathscr{A}$ \ vrai	**F**	**V**
F	vrai négatif	faux négatif
V	faux positif	vrai positif

.

TABLE 3.1 – Matrice de confusion dans le cas d'une classification en **V** et **F**

Comment améliorer la performance de l'algorithme des k plus proches voisins ? En dimension 1, on peut utiliser une dichotomie. Mais, dans des dimensions plus grandes, l'ordre lexicographique, et l'ordre produit ne fonctionnent pas. Mais, on peut appliquer une "dichotomie" en changeant de dimension. Par exemple, en deux dimension, on obtient la dichotomie ci-dessous.

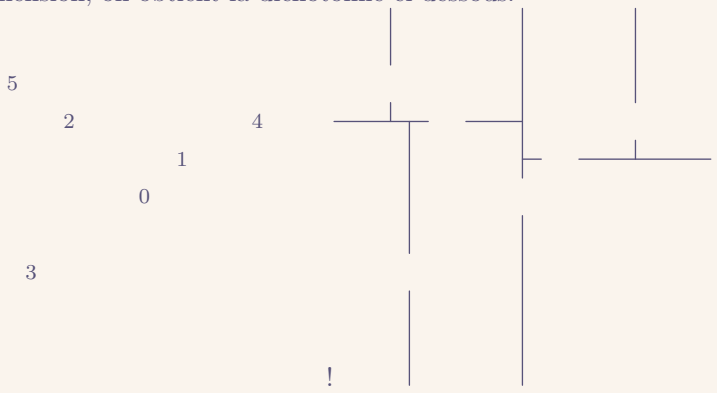


FIGURE 3.2 – Représentation de la "dichotomie" en dimension 2

Pour représenter cette structure de données, on utilise un arbre binaire comme montré ci-dessous. Cet arbre est appelé un arbre k-dimensionnels.

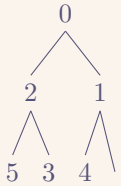


FIGURE 3.3 – Arbre 2-dimensionnel représentant la "dichotomie" précédente

IV.3.2 Arbres k-dimensionnels

Remarque (Notations) :
Étant donné un jeu de données S, on note pour $v \in S$,

$$S^{\leqslant_i v} = \{u \in S \mid u_i \leqslant v_i\} \qquad \text{et} \qquad S^{>_i v} = \{u \in S \mid u_i > v_i\}.$$

Algorithme 3.2 "F" : Fabrication d'un arbre k-dimensionnel

Entrée $\mathcal{V}$ un jeu de données et $i \in [\![0, n-1]\!]$, où n est la dimension des données

```
si V = ∅ alors
    retourner Vide
sinon
    On cherche v ∈ V tel que v_i est la médiane de {u_i | u ∈ V}
    retourner Nœud((v, i), F((V \ {v})^{≤_i v}, i+1 mod n), F((V \ {v})^{>_i v}, i+1 mod n))
```

Algorithme 3.3 "R" : Recherche du point le plus proche

Entrée Un arbre k-dimensionnel et un vecteur v

```
si T est vide alors
    retourner None
sinon
    Nœud((u, i), G, D) ← T
    si u_i ⩽ v_i alors
        W ← R(D, v)
        si W = None alors
            W' ← R(G, v)
            si W' = ∅ alors
                retourner Some(u)
            sinon
                Some(z) ← W'
                retourner le plus proche de v entre u et z
        sinon
            Some(w) ← W
            si v_i − u_i ⩽ d(w, v) alors        ▷ d(w, v) représente la distance entre w et v
                W' ← R(G, v)
                si W' = None alors
                    retourner Some(plus proche de v entre u et w)
                sinon
                    Some(z) ← w
                    retourner Some(plus proche de v entre u, z, et w)
            sinon
                retourner W
    sinon
        ⟨comme le cas précédent⟩
```

IV.3.3 Algorithme id3

L'algorithme des k plus proches voisins (sans arbres k-dimensionnels) n'a pas de *phase d'apprentissage* : en effet, les données ne sont pas réorganisées. Mais, par exemple, pour l'utilisation des arbres k-dimensionnels, les données sont réorganisées dans un arbre.

Ce qu'on aimerai avoir, c'est des *bordures* entre les différentes classes. Par exemple, dans l'exemple précédent, on aimerai avoir les différentes zones ci-dessous.

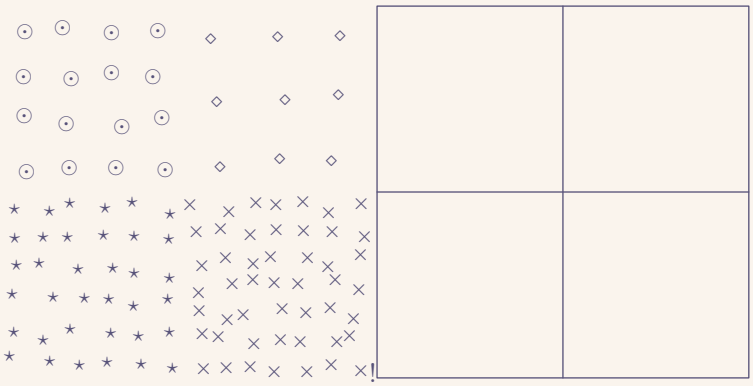


FIGURE 3.4 – Représentation de *bordures* entre les différentes classes

De ces zones, on peut construire un algorithme qui classifie les données, que l'on représente sous forme d'arbre. Ce type d'arbre est un *arbre de décision*. Dans l'exemple précédent, on peut donc créer l'arbre ci-dessous. [2]

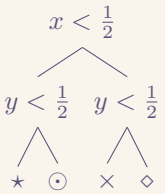


FIGURE 3.5 – Arbre de décision pour la classification

Dans le reste de cette section, on s'intéresse uniquement à des données de $\mathbb{B}^n$ (une liste de n booléens) pour un certain $n \in \mathbb{N}$.

On considère l'exemple dont les données ci-dessous.

2. Dans cet arbre, si un nœud représente une condition, son fils gauche représente si cette condition est vraie, et le fils droit sinon.

Transport	Moteur	Rails	Sous-terre	$\geqslant 320$ km/h	Train ?
A380	✓	✗	✗	✓	✗
TGV	✓	✓	✗	✓	✓
Métro	✓	✓	✓	✗	✓
Wagonnet	✗	✓	✓	✗	✗
Draisine	✗	✓	✗	✗	✗
Tram	✓	✓	✗	✗	✓

TABLE 3.2 – Exemple de données

Entropie

Définition : Étant donné un variable aléatoire finie X à valeurs dans E. On note $p_X : E \to [0,1]$ sa loi de probabilité :

$$\forall x \in E, \quad p_X(x) = P(X = x).$$

On définit l'*entropie* $\mathrm{H}(X)$ de cette variable aléatoire comme

$$\mathrm{H}(X) = -\sum_{x \in E} p_X(x)\ \ln\big(p_X(x)\big).$$

On prolonge $p_X(x)\ln(p_X(x))$ par continuité à la valeur 0 lorsque $p_X(x) = 0$.

EXEMPLE :
On considère la variable aléatoire X à valeur dans $\{\bullet, \bullet\}$ telle que $P(X = \bullet) = 1$ et $P(X = \bullet) = 0$. On a

$$\mathrm{H}(X) = -0\ln 0 - 1\ln 1 = 0.$$

EXEMPLE :
On considère la variable aléatoire X à valeur dans $\{\bullet, \bullet\}$ telle que $P(X = \bullet) = p$ et $P(X = \bullet) = 1 - p$, avec $p \in [0,1]$. On a alors

$$\mathrm{H}(X) = -p\ln p - (1-p)\ln(1+p)$$

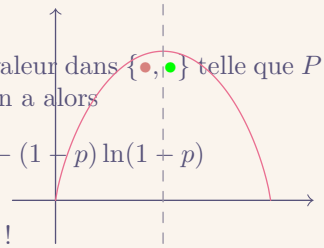


FIGURE 3.6 – Représentation graphique de $\mathrm{H}(X)$ en fonction de p

Lemme : Si $(p_i)_{i \in [\![1,n]\!]} \in]0,1]^n$ sont tels que $\sum_{i=1}^n p_i = 1$. Soit $(q_i)_{i \in [\![1,n]\!]}$ tels que $\forall i$, $q_i = \frac{1}{n}$. On a alors

$$-\sum_{i=1}^{n} p_i \ln p_i \leqslant -\sum_{i=1}^{n} p_i \ln(q_i).$$

Preuve :
On a

$$\sum_{i=1}^{n} p_i \ln(q_i) - \sum_{i=1}^{n} p_i \ln(p_i) = \sum_{i=1}^{n} p_i \ln\left(\frac{q_i}{p_i}\right) \leqslant \ln\left(\sum_{i=1}^{n} p_i \frac{q_i}{p_i}\right) = 0.$$

□

Proposition : Soit $n = |E|$. L'entropie d'une variable aléatoire à valeurs dans E est maximale lorsque

$$\forall e \in E,\ P(X = e) = \frac{1}{n}.$$

Preuve :
On conclut, d'après le lemme précédent. □

Définition : Étant donné un jeu de données classifiés (S, c) où $c : \mathbb{S} \to E$, on appelle *entropie* de ce jeu de données l'entropie de la variable aléatoire $c(Y)$ où $Y \sim \mathcal{U}(S)$. On a donc

$$\mathrm{H}\big((S, c)\big) = -\sum_{e \in E} \frac{\mathrm{Card}\ c^{-1}\big(\{e\}\big)}{\mathrm{Card}\, S} \ln\left(\frac{\mathrm{Card}\ c^{-1}\big(\{e\}\big)}{\mathrm{Card}\, S}\right).$$

Définition : Étant donné un jeu de données une partition $\{S_1, S_2, \ldots, S_p\}$ d'un jeu de données classifié (S, c), l'*entropie* de cette partition est la moyenne (pondérée par les cardinaux et renormalisée) :

$$\mathrm{H}\big(\big(\{S_1, \ldots, S_p\}, c\big)\big) = \sum_{i=1}^{p} \frac{\mathrm{Card}\, S_i}{\mathrm{Card}\, S}\, \mathrm{H}\big((S_i, c)\big).$$

L'entropie de $\{w, a, t, d, r, m\}$ est $\mathrm{H} = -\frac{3}{6}\ln\left(\frac{3}{6}\right) - \frac{3}{6}\ln\left(\frac{3}{6}\right) = \ln 2 \simeq 0{,}69$. Mais, avec le découpage de l'arbre de décision ci-dessous, on obtient l'entropie

$$\begin{aligned}
\mathrm{H} &= \frac{2}{6}\mathrm{H}(\{w; d\}) + \frac{4}{6}\mathrm{H}(\{a, t, r, m\}) \\
&= \frac{2}{6} \times 0 + \frac{4}{6} \times \left(-\frac{1}{4}\ln\left(\frac{1}{4}\right) - \frac{3}{4}\ln\left(\frac{3}{4}\right)\right) \\
&\simeq 0{,}37.
\end{aligned}$$

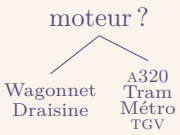


FIGURE 3.7 – Arbre de décision possible se basant sur le moteur

Avec un autre arbre (comme celui ci-dessous), on obtient une entropie différente :

$$\begin{aligned} \mathrm{H} &= \frac{1}{6}\mathrm{H}(\{a\}) + \frac{5}{6}\mathrm{H}(\{w,d,t,r,m\}) \\ &= \frac{5}{6}\left(-\frac{2}{5}\ln\left(\frac{2}{5}\right) - \frac{3}{5}\ln\left(\frac{3}{5}\right)\right) \\ &\simeq 0{,}56. \end{aligned}$$

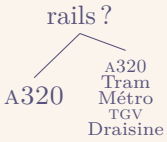


FIGURE 3.8 – Arbre de décision possible se basant sur les rails

Pour le sous-terrain, on a $\mathrm{H} = \ln 2$.

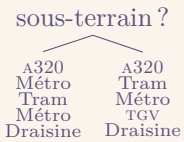


FIGURE 3.9 – Arbre de décision possible se basant sur sous-terrain
À faire : Vérifier

À faire : Autre cas

Ainsi, on choisit de commencer avec la condition “moteur” car l’entropie est la plus faible avec cette condition. Ainsi, l’arbre de décision ressemble à celui ci-dessous.

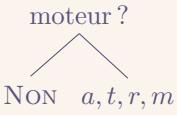


FIGURE 3.10 – Arbre de décision partiel

On réitère avec les autres conditions. L’entropie en se basant sur la vitesse est $\frac{1}{2}\ln 2 \simeq 0{,}34$. En effet, l’arbre de décision possible ressemble à celui ci-dessous.

FIGURE 3.11 – Arbre de décision possible se basant sur le moteur puis la vitesse

Mais, en se basant sur sous-terrain, on obtient une entropie de $\frac{3}{4}\left(-\frac{2}{3}\ln\left(\frac{2}{3}\right)-\frac{1}{3}\ln\left(\frac{1}{3}\right)\right) \simeq 0{,}48$.

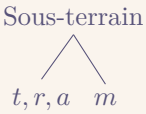


FIGURE 3.12 – Arbre de décision possible se basant sur le moteur puis sous-terrain

Et, en se basant sur les rails, on obtient une entropie de 0.

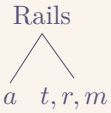


FIGURE 3.13 – Arbre de décision possible se basant sur le moteur puis les rails

On en déduit que l'arbre final de décision est celui ci-dessous.

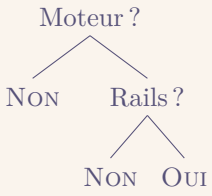


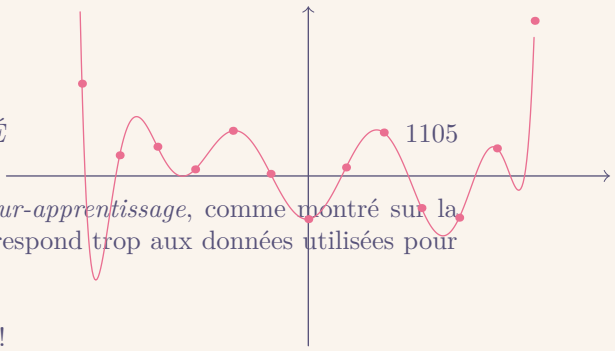
FIGURE 3.14 – Arbre de décision final pour la classification de trains

Les données que l'on a utilisées sont pour l'apprentissage. On teste notre arbre de décision sur les données ci-dessous.

Nom	Moteur	Rail	Sous-terre	Vitesse	Résultat de l'algorithme
Bus	✓	✗	✗	✗	✗
TER	✓	✓	✗	✗	✓
Cheval	✗	✗	✗	✗	✗
Ascenseur spatial	✓	✓	✗	✗	✓

TABLE 3.3 – Test de l'arbre de décision créé

ATTENTION : il ne faut pas faire du *sur-apprentissage*, comme montré sur la figure ci-dessus, où la modélisation correspond trop aux données utilisées pour la classification.



!

FIGURE 3.15 – Représentation graphique du problème de *sur-apprentissage*

Aussi, il faut faire attention aux critères : par exemple, lors de la classification de photos de chats et de chiens, les photos de chiens sont en général prises en extérieur et l'algorithme ID3 aurait donc pu choisir de baser sa décision sur l'emplacement de la photo, même si elle n'importe pas dans la différenciation chat/chiens.

Autre exemple : on considère la table de données ci-dessous. Utilisons l'algorithme ID3 sur ces données, et trouvons l'arbre de décision.

A	B	C	D	Classification
✓	✗	✗	✓	•
✓	✓	✗	✓	•
✓	✗	✓	✓	•
✓	✓	✓	✓	•
✗	✗	✓	✓	•
✗	✓	✓	✗	•
✗	✗	✗	✗	•
✗	✓	✗	✓	•

TABLE 3.4 – Table de données d'exemple

Pour les conditions A, B et C, on a $\mathrm{H} \simeq 0{,}63$ et, pour D, on a $\mathrm{H} = 0{,}65$. Comme on prend le $1^{\underline{\text{er}}}$ dans l'ordre lexicographique, on choisit la condition A. De même, on construit l'arbre ci-dessous.

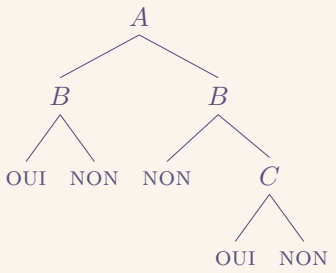


FIGURE 3.16 – Arbre de décision pour la table de données précédente

Le nom de ID3 vient de *iterative dichotomizer*.

IV.4 Apprentissage non supervisé

On rappelle que l'*apprentissage non supervisé* utilise des données non classifiées. L'objectif est de les classifier. Plus rigoureusement, étant donné un jeu de données $\mathcal{D}$, on veut partitionner $\mathcal{D}$ en $\{S_1, S_2, \ldots, S_n\}$ où les S_i sont regroupés par « similitude. »

Remarque :
Dans le reste de cette section, $\mathcal{D} \subseteq \mathbb{R}^p$, avec $p \in \mathbb{N}^\star$, et la notion de similitude est donnée par la distance euclidienne.

IV.4.1 Algorithme hac, classification hiérarchique ascendant

Définition : Étant donné deux sous-ensembles A et B de $\mathcal{D}$ disjoints et non-vides, on définit différentes *mesures de dissimilarité* :

- $D(A,B) = \min\{d(a,b) \mid a \in A, b \in B\}$;
- $D(A,B) = \max\{d(a,b) \mid a \in A, b \in B\}$;
- $D(A,B) = \frac{1}{|A|\,|B|} \times \sum_{(a,b)\in A\times B} d(a,b)$,

où $d(a,b)$ représente la distance entre a et b.

Algorithme 3.4 Algorithme hac

```
P ← {{x} | x ∈ 𝒟}
tant que |P| ⩾ 2 et ?[3] faire
    Soit A, B ∈ P minimisant D(A,B) avec A ≠ B
    P ← (P \ {A,B}) ∪ {A ∪ B}
retourner P
```

IV.4.2 *k*-moyenne

Au préalable, on fixe le nombre de classes k que l'on souhaite obtenir après exécution de l'algorithme.

Proposition : On considère la fonction

$$\begin{aligned} f : \mathbb{R}^p &\longrightarrow \mathbb{R} \\ H &\longmapsto \sum_{v\in\mathcal{D}} \|H - v\|_2^2. \end{aligned}$$

Cette fonction atteint son minimum en le barycentre G.

3. où, pour ?, on peut choisir (1) un critère sur le nombre de classes (2) un critère sur la valeur de la plus petite dissimilarité

Preuve :
Soit G le barycentre de $\mathscr{D}$. Soit $H \in \mathbb{R}^p$. Montrons que $f(H) > f(G)$. On calcule

$$\begin{aligned} f(H) &= f(H-G+G) \\ &= \sum_{v\in\mathscr{D}} \Big\langle (H-G+G)-v \,\Big|\, (H-G+G)-v \Big\rangle \\ &= \sum_{v\in\mathscr{D}} \Big(\langle G-v \mid G-v\rangle + 2\langle H-G \mid H-v\rangle + \langle H-G \mid H-G\rangle \Big) \\ &= f(G) + \underbrace{|\mathscr{D}|\cdot\|H-G\|_2^2}_{\geqslant 0} + \underbrace{2\Big\langle H-G \,\Big|\, \sum_{v\in\mathscr{D}}(G-v)\Big\rangle}_{\substack{=0 \\ \text{par définition du barycentre}}} \end{aligned}$$

Donc, si $H \neq G$, on a bien $f(H) > f(G)$. □

Dans la suite de cette sous-section, on s'intéresse à des partitionnement particuliers : étant donné une famille $(m_i)_{i\in[\![1,k]\!]}$ de vecteurs de $\mathbb{R}^p$, et un entier $j \in [\![1,k]\!]$, on définit

$$\mathscr{C}_j^m = \Big\{ v \in \mathscr{D} \,\Big|\, \operatorname{argmin}_{i\in[\![1,k]\!]} \|v-m_i\|_2 = j \Big\}.$$

Remarque :
En cas d'égalité ($\|v-m_{i_1}\|_2 = \|v-m_{i_2}\|_2$), le "argmin" retourne le plus petit indice : $\min(i_1,i_2)$.

Étant donné une famille $(m_i)_{i\in[\![1,k]\!]}$ de vecteurs de $\mathbb{R}^p$, on a donc un partitionnement $\{\mathscr{C}_j^m \mid j \in [\![1,k]\!]\}$.

Définition : Étant donné une famille $(m_i)_{i\in[\![1,k]\!]}$ de vecteurs de $\mathbb{R}^p$, on définit

$$L(m) = \sum_{k=1}^{n} \Big(\sum_{v\in\mathscr{C}_i^m} \|v-m_i\|_2^2 \Big).$$

Pour minimiser localement la fonction L, on aimerait que les $(m_i)_{i\in[\![1,k]\!]}$ soient les barycentres des $(\mathscr{C}_i^m)_{i\in[\![1,k]\!]}$. Mais, la définition des $(\mathscr{C}_i^m)$ dépend de la position des (m_i). Ainsi, en itérant ce procédé, en modifiant les (m_i) pour être les barycentres des $(\mathscr{C}_i^m)$ respectifs, puis en modifiant les $(\mathscr{C}_i^m)$, la famille $(m_i)_{i\in[\![1,k]\!]}$ converge vers les barycentres des classes.

Algorithme 3.5 k-moyenne

Entrée $\mathcal{D}$ et k

1 : $(m_i)_{i\in[\![1,k]\!]} \leftarrow k$ vecteurs de $\mathcal{D}$
2 : stable $\leftarrow$ **F**
3 : **tant que** $\neg$stable **faire**
4 : $\quad C \leftarrow (\mathcal{C}_i^m)_{i\in[\![1,k]\!]}$
5 : $\quad m' \leftarrow \big(\text{barycentre}(\mathcal{C}_i)\big)_{i\in[\![1,k]\!]}$
6 : $\quad$ stable $\leftarrow m \stackrel{?}{=} m'$
7 : $\quad m \leftarrow m'$
8 : **retourner** C

Chapitre 4

Calculabilité, Décidabilité, Complexité

Au chapitre 1, on s'est intéressé aux langages réguliers, et aux automates qui est un modèle de calcul relativement simple. Dans ce chapitre, on s'intéresse à un modèle plus puissant : un *ordinateur*, on va notamment redéfinir la notion de *problème*. Le choix classique de définition d'un ordinateur n'est pas celui qui a été choisi au programme : un programme OCaml.

IV.1 Remarques mathématiques

Définition : Étant donné une relation $\mathscr{R}$ sur $\mathscr{E} \times \mathscr{F}$, on dit que $\mathscr{R}$ est
- *totale à gauche* dès lors que $\forall e \in \mathscr{E}$, $\exists f \in \mathscr{F}$, $(e, f) \in \mathscr{R}$;
- *déterministe* dès lors que $\forall e \in \mathscr{E}$, $\forall (f, f') \in \mathscr{F}^2$, si $(e, f) \in \mathscr{R}$ et $(e, f') \in \mathscr{R}$, alors $f = f'$.

Définition : On appelle *fonction totale* de $\mathscr{E}$ dans $\mathscr{F}$ une relation sur $\mathscr{E} \times \mathscr{F}$ déterministe et totale à gauche.

Définition : On appelle *fonction partielle* de $\mathscr{E}$ dans $\mathscr{F}$ une relation sur $\mathscr{E} \times \mathscr{F}$ déterministe. On note alors

$$\mathrm{def}(f) = \{x \in \mathscr{E} \mid \exists y \in \mathscr{F},\ (x, y) \in f\}.$$

Remarque :
Soit f une fonction partielle de $\mathscr{E}$ dans $\mathscr{F}$ tel que $\square \notin \mathscr{F}$, alors on peut completer

f en une fonction totale de $\mathscr{E}$ dans $\mathscr{F} \cup \{\square\}$ de la manière suivante :

$$f : \mathscr{E} \longrightarrow \mathscr{F} \cup \{\square\}$$
$$x \longmapsto \begin{cases} f(x) & \text{si } x \in \text{def}(f) \\ \square & \text{sinon.} \end{cases}$$

IV.2 Problèmes

Définition : Étant donnés un ensemble d'entrée $\mathscr{E}$, un ensemble de sortie $\mathcal{S}$, on appelle *problème* sur $\mathscr{E} \times \mathcal{S}$ une relation $\mathscr{R}$ [1] sur $\mathscr{E} \times \mathcal{S}$ totale à gauche.

Exemple :
Le problème

$$\textsc{Prime} : \begin{cases} \textbf{Entrée} & : n \in \mathbb{N} \\ \textbf{Sortie} & : n \text{ est-il premier ?} \end{cases}$$

est donc défini comme

$$\textsc{Prime} = \{(0, \mathbf{F}), (1, \mathbf{F}), (2, \mathbf{V}), (3, \mathbf{V}), (4, \mathbf{F}), (5, \mathbf{V}), \dots\} \subseteq \mathbb{N} \times \mathbb{B}.$$

Exemple :
Le problème

$$\textsc{Find}_0 : \begin{cases} \textbf{Entrée} & : \text{un tableau } T \text{ contenant au moins un } 0 \\ \textbf{Sortie} & : i \in \mathbb{N} \text{ tel que } T[i] = 0 \end{cases}$$

est donc défini comme

$$\textsc{Find}_0 = \Big\{ \big([|0,1,1|], 0\big), \big([|0,1,0|], 0\big), \big([|0,1,0|], 2\big), \dots \Big\}.$$

Remarque :
De la même manière qu'en mathématiques, on n'écrit pas $\{(0,1),(1,2),(2,3),\dots\}$ mais $x \mapsto x+1$, en informatique, on préfère la notation sous forme de problème.

Remarque :
On précisera, en cas d'ambigüité la représentation choisie pour les entrées.

Exemple :
Les deux problèmes

$$\begin{cases} \textbf{Entrée} & : n \text{ sous forme décomposée en facteurs premiers} \\ \textbf{Sortie} & : n \text{ est-il premier ?} \end{cases}$$

et

$$\begin{cases} \textbf{Entrée} & : n \text{ en base 2} \\ \textbf{Sortie} & : n \text{ est-il premier ?} \end{cases}$$

sont différents.

1. C'est l'ensemble des liens entrées/sorties

Remarque :
Lorsque ce n'est pas précisé, dans la suite du cours, les entiers sont représentés en base 2.

Exemple :
Dans le problème

$$\begin{cases}\textbf{Entrée} & : L_1 \text{ et } L_2 \text{ deux langages réguliers} \\ \textbf{Sortie} & : L_1 = L_2,\end{cases}$$

on doit préciser la représentation de L_1 et L_2.

Définition : On appelle *problème de décision* un problème à valeurs dans $\mathbb{B}$ déterministe.

Exemple :
Par exemple, le problème Prime est un problème de décision.

Remarque (Notation) :
Lorsque Q est un problème, on note $\mathscr{E}_Q$ son espace d'entrée, et $\mathscr{S}_Q$ son espace de sortie. De plus, si Q est un problème de décision, on note $Q^+ = \{e \in \mathscr{E}_Q \mid (e, \mathbf{V}) \in Q\}$ et $Q^- = \{e \in \mathscr{E}_Q \mid (e, \mathbf{F}) \in Q\}$. $\{Q^+, Q^-\}$ est une partition de $\mathscr{E}_Q$.

IV.3 Décidabilité

La définition d'un algorithme comme une suite finie d'instruction élémentaire, nous montre que l'ensemble d'algorithmes est dénombrable.[2] Mais, l'ensemble de problèmes est indénombrable. En effet, pour $x \in [0, 1[$, on définit le problème

$$\text{Bit}_x : \begin{cases}\textbf{Entrée} & : n \in \mathbb{N} \\ \textbf{Sortie} & : \text{le } n\text{-ième bit de } x.\end{cases}$$

Et, comme $[0, 1[$ n'est pas dénombrable, l'ensemble des problèmes ne l'est pas non plus.

IV.3.1 Modèles de calcul

Définition : On appellera *modèle de calcul* la donnée d'un ensemble de machines
- qu'il est possible d'exécuter sur des entrées ;
- qui peuvent ou pas retourner une réponse.

Exemple :
Les automates déterministes qu'il est possible d'exécution sur une entrée $w \in \Sigma^\star$, obtenant ainsi un booléen $b \in \mathbb{B}$, est un modèle de calcul.

2. en bijection avec $\mathbb{N}$

Dans ce chapitre, notre modèle de calcul sera l'ensemble des fonction OCaml ayant pour type `string` $\to$ `string` qu'il est possible d'exécuter, qui peuvent donner un réponse ou non (boucle infinie, erreur).

Remarque :
On se place dans un monde d'exécution idéal : *mémoire infinie*.

Exemple :
On reprend le problème Prime. On code, sous forme de fonction OCaml, la machine ci-dessous. Elle répond au problème Prime.

```
let est_premier (s: string) : string =
  let n = int_of_string s in
  if n <= 1 then "false"
  else
    let i = ref 2 in
    let i_sq = ref 4 in
    let compose = ref false in
    while not !compose && !i_sq <= n do
      if n mod !i = 0 then compose := true
      else i_sq := !i_sq + 2 * !i + 1;
        i := !i + 1;
    done;
    string_of_bool(not !compose)
```

Code 4.1 – Machine décidant le problème Prime

Remarque (Notation) :
Dans la suite, lorsque $\mathscr{M}$ est une machine, et $w \in$ `string`, on notera

— $w \xrightarrow[\mathscr{M}]{} w'$ si l'exécution de $\mathscr{M}$ sur w conduit à $w' \in$ `string`.
— $w \xrightarrow[\mathscr{M}]{} \circlearrowleft$ si l'exécution de $\mathscr{M}$ sur w conduit à une erreur.

Dans la suite de ce chapitre, on fixe $\Sigma =$ `char` et donc $\Sigma^\star =$ `string`.

Remarque :
On pourra, dans la suite, généraliser la signature de nos machines à un type $\mathscr{E} \to \mathscr{F}$ dès lors qu'on exhibe une fonction de sérialisation $\varphi : \mathscr{E} \to \Sigma^\star$ inversible (sur son espace image) injective : avec $\varphi_{\mathscr{E}} : \mathscr{E} \to \Sigma^\star$ et $\varphi_{\mathscr{F}} : \mathscr{F} \to \Sigma^\star$, on a

```
let ma_super_fonction (e: 𝓔) : 𝓕 = ...

let ma_fonction (s: string) : string =
  φ_𝓕(ma_super_fonction(φ_𝓔^-1(s)))
```

Code 4.2 – Généralisation des machines ayant pour entrée un ensemble $\mathscr{E}$ et sortie $\mathscr{F}$

IV.3.2 Décidabilité

Définition : Une fonction partielle $f : \mathscr{E} \to \mathcal{S}$ est dite *calculée* par une machine $\mathscr{M}$ dès lors que

$$\forall e \in \mathrm{def}(f), \quad e \xrightarrow[\mathscr{M}]{} f(e).$$

On dit alors d'une telle fonction qu'elle est *calculable*.

Remarque :
Cette définition ne spécifie aucunement le comportement de $\mathscr{M}$ sur une entrée $e \notin \mathrm{def}(f)$.

Exemple :
Considérons la fonction partielle $\sqrt{\ } : \mathbb{Z} \to \mathbb{Z}$ telle que $\mathrm{def}(\sqrt{\ }) = \{p^2 \mid p \in \mathbb{N}\}$, et $\sqrt{x}$ est l'unique $y \in \mathbb{N}$ tel que $y^2 = x$.

```
let sqrt (n: int): int =
  if m < 0 then -1
  else
    begin
      let i = ref 0 in
      let i_sq = ref 0 in
      while !i_sq <> n do
        i_sq := !i_sq + 2 * !i + 1;
        i := !i + 1;
      done;
      !i
    end
```

Code 4.3 – Machine calculant la fonction $\sqrt{\ }$

— Pour $\mathtt{n} < 0$, on a $\mathtt{n} \underset{\mathscr{M}}{\longrightarrow} -1$.
— Pour $\mathtt{n} \geqslant 0$ qui n'est pas un carré, $\mathtt{n} \underset{\mathscr{M}}{\longrightarrow} \circlearrowleft$.
— Pour $\mathtt{n} \geqslant 0$ qui est un carré, $\mathtt{n} \underset{\mathscr{M}}{\longrightarrow} \sqrt{\mathtt{n}}$.

Ainsi, $\sqrt{\ }$ est calculable.

Définition : Étant donné qu'un problème de décision Q est un cas particulier de fonction totale $\mathscr{E}_Q \to \mathbb{B}$, on dit que Q est *décidé* par une machine $\mathscr{M}$ dès lors que

$$\forall e \in \mathscr{E}_Q, \qquad \Big(e \in Q^+ \iff e \underset{\mathscr{M}}{\longrightarrow} \mathbf{V} \quad \text{et} \quad e \in Q^- \iff e \underset{\mathscr{M}}{\longrightarrow} \mathbf{F}\Big).$$

On dit alors que ce problème Q est *décidable*.

Exemple :
On considère le problème

$$\textsc{Existe}_0 : \begin{cases} \textbf{Entrée} & : \text{un tableau } T \\ \textbf{Sortie} & : \exists i \in \mathbb{N},\ T[i] = 0 ? \end{cases}$$

La machine ci-dessous décide le problème $\textsc{Existe}_0$.

```
exception OK

```

```
let existe (t: int array) : bool =
  try
    for i = 0 to (Array.length t) - 1 do
      if t.(i) = 0 then
        raise OK
    done;
    false
  with
  | OK -> true
```

CODE 4.4 – Machine décide le problème EXISTE$_0$

IV.3.3 Langages et problèmes de décision

Les notions de langages et problèmes de décision d'entrée $\Sigma^\star$ coïncident. En effet, à un langage $L \subseteq \Sigma^\star$, on associe le problème de décision

$$\text{APPARTIENT}_L : \begin{cases} \textbf{Entrée} & : w \in \Sigma^\star \\ \textbf{Sortie} & : w \in L \ ?. \end{cases}$$

On a alors $(\text{APPARTIENT}_L)^+ = L$. Réciproquement, à un problème de décision Q d'entrées $\Sigma^\star$, on associe le langage Q^+.

Définition : Un langage L est dit *décidable* lorsque le problème APPARTIENT_L est décidable.

Définition : Étant donné une machine $\mathscr{M}$ de type `string` $\to$ `bool`, on appelle *langage* de $\mathscr{M}$, que l'on note $\mathscr{L}(\mathscr{M})$, l'ensemble

$$\left\{w \in \Sigma^\star \mid w \underset{\mathscr{M}}{\longrightarrow} \mathbf{V}\right\}.$$

REMARQUE :
$\mathscr{L}(\mathscr{M})$ n'est pas le complémentaire de $\left\{w \in \Sigma^\star \mid w \underset{\mathscr{M}}{\longrightarrow} \mathbf{F}\right\}$. En effet, il peut exister $w \in \Sigma^\star$ tel que $w \underset{\mathscr{M}}{\longrightarrow} \circlearrowleft$.

Proposition : Un langage L est décidable si, et seulement si L est le langage d'une machine $\mathscr{M}$ telle que $\forall w \in \Sigma^\star$, $w \underset{\mathscr{M}}{\longrightarrow} \mathbf{V}$ ou $w \underset{\mathscr{M}}{\longrightarrow} \mathbf{F}$.

Proposition : Tout langage régulier est décidable.

Preuve :
Soit L un langage régulier. Montrons que L est décidable. On utilise alors

la fonction OCaml suivante de reconnaissance d'un mot dans un automate (que l'on a déjà codé en TP). □

Proposition (stabilité des langages décidables) **:** Un langage décidable est stable par

1. union ;
2. intersection ;
3. complémentaire.

Preuve : 1. Soient L_1 et L_2 deux langages décidables. Montrons que $L_1 \cup L_2$ est décidable. Soit $\texttt{decide}_1 : \texttt{string} \to \texttt{bool}$ la fonction décidant le langage L_1.[3] Soit $\texttt{decide}_2 : \texttt{string} \to \texttt{bool}$ la fonction décidant du langage L_2. On construit alors la fonction

```
let decide (w : string) : bool =
  (decide₁ w) || (decide₂ w)
```

Code 4.5 – Fonction OCamlreconnaissant l'union de deux langages décidables

□

Remarque :
est décidable (par `fun s -> false`) ; $\Sigma^\star$ est décidable (par `fun s -> true`).

IV.3.4 Sérialisation

Définition : Étant donné un type OCaml `t`, on appelle *sérialisation calculable* de ce type `t`, la donnée d'une fonction `f` OCaml de type `t -> string` qui soit telle que

- pour tout e : `t`, (`f` e) est bien parenthésée ;
- `f` est injective ;
- la réciproque de `f` (définie sur Im(`f`)) est définissable en OCaml.

Exemple :
Le type `int` est sérialisable par la fonction `string_of_int`.

Proposition : Soit $\texttt{t}_\texttt{a}$ et $\texttt{t}_\texttt{b}$ deux types OCaml sérialisables, alors le type $\texttt{t}_\texttt{a} \star \texttt{t}_\texttt{b}$ est sérialisable.

3. *i.e.* $\forall w \in \Sigma^\star,\ w \in L_1 \iff \texttt{decide}_1(w) = \texttt{true}$

Preuve :
Soit φ_a et φ_b les fonctions de sérialisation des types t_a et t_b. On définit alors la fonction

```
let φ ((a,b): t_a * t_b) =
  "(" ^ (φ_a a) ^ "),(" ^ (φ_b b) ^ ")"
```

CODE 4.6 – Fonction OCAML sérialisant le produit cartésien de deux types sérialisables

On remarque que

- φ est à valeur dans les chaînes de caractères bien parenthésées ;
- φ est injective (par identification de parenthèses et injectivité de φ_a et φ_b) ;
- la réciproque de φ est décidable en OCAML (preuve à faire en OCAML).

□

REMARQUE :
Une programme OCAML est trivialement sérialisable : c'est déjà une chaîne de caractères.

EXEMPLE :
La sérialisation de la fonction

```
let rec fact (n : int) : int =
  if n = 0 then 1
  else n * (fact (n-1))
```

CODE 4.7 – Fonction factorielle en OCAML

est la chaîne de caractère

```
"let␣rec␣fact␣(n␣:␣int)␣:␣int␣=
␣␣if␣n␣=␣0␣then␣1
␣␣else␣n␣*␣(fact␣(n-1))".
```

IV.3.5 Machine universelle

Soit l'ensemble $\mathcal{O}$ des chaînes de caractères qui sont des sérialisations de programme OCAML valide.

EXEMPLE :
La sérialisation de la fonction `fact` trouvée précédemment est un élément de $\mathcal{O}$. Mais, "`let`" $\notin \mathcal{O}$.

Définition : Soit la fonction `interprète` : $\mathfrak{G} \times \Sigma^\star \to \Sigma^\star$ définie par

$$\texttt{interprète}(\mathscr{M}, w) = \begin{cases} w' \text{ tel que } w \underset{\mathscr{M}}{\longrightarrow} w' \\ \text{non défini sinon.} \end{cases}$$

Théorème : La fonction `interprète` est calculable. On appelle *machine universelle* un programme OCaml la calculant.

Preuve :
On considère `utop` ou `WinCaml`. □

De même, considérons le problème suivant

$$\begin{cases} \textbf{Entrée} & : M \in \mathfrak{G}, w \in \Sigma^\star, n \in \mathbb{N} \\ \textbf{Sortie} & : M \text{ se termine-t-elle sur } w \text{ en moins de } n \text{ étapes élémentaires ?} \end{cases}$$

Ce problème est décidable.

IV.3.6 Théorème de l'Arrêt

Dans cette sous-section, on considère le problème

$$\text{Arrêt} : \begin{cases} \textbf{Entrée} & : M \in \mathfrak{G}, w \in \Sigma^\star \\ \textbf{Sortie} & : M \text{ s'arrête-t-elle sur } w.\ ^4 \end{cases}$$

Théorème : Le problème Arrêt est indécidable.

Preuve :
Par l'absurde : supposons Arrêt décidable. Soit `arret` : `string` → `bool` prenant en argument une chaîne de caractères qui est la sérialisation d'un couple M code d'une machine ($M \subseteq \Sigma^\star$), et $w \in \Sigma^\star$, et retournant `true` si et seulement si M s'arrête sur l'entrée w. Si l'entrée n'est pas une sérialisation convenable, on retourne `false`. On crée le programme suivant

```
let paradoxe (w : string) : bool =
  if arret (serialise_couple w w) then
    (while true do () done; true)
  else false
```

Code 4.8 – Programme paradoxe prouvant que le problème Arrêt est indécidable

4. *i.e.* $\exists ? w' \in \Sigma^\star,\ w \underset{M}{\longrightarrow} w'$

où `serialise_couple` est une fonction sérialisant un couple avec l'algorithme trouvé précédemment. Soit $S_{\texttt{paradoxe}}$ la sérialisation de la fonction `paradoxe`.

Quid de (`paradoxe` $S_{\texttt{paradoxe}}$) : soit $c = (\texttt{serialise\_couple}\ S_{\texttt{paradoxe}}\ S_{\texttt{paradoxe}})$. La chaîne c est donc la sérialisation d'un couple dont la première composante est le code de la fonction `paradoxe`. De plus, `arret` se termine sur toute entrée.

- Si (`arret` c) = `false`, alors on va dans la branche `else` et l'exécution de `paradoxe` sur $S_{\texttt{paradoxe}}$ termine. Mais, comme (`arret` c) = `false`, `paradoxe` ne se termine pas sur $S_{\texttt{paradoxe}}$.
- Si (`arret` c) = `true`, alors on va dans la branche `then`, et donc (`paradoxe` $S_{\texttt{paradoxe}}$) ne se termine pas. Mais, comme (`arret` c) = `true`, alors (`paradoxe` $S_{\texttt{paradoxe}}$) se termine.

On en conclut que le problème Arrêt est indécidable. □

Corollaire : Il existe des problèmes indécidables.

IV.3.7 Réduction

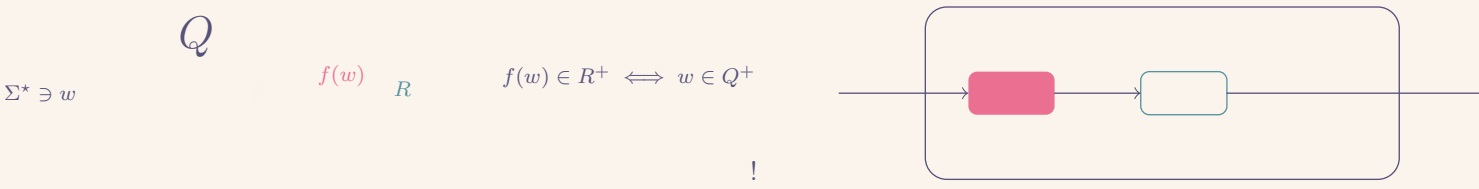


Figure 4.1 – Structure d'un sous-problème

Définition : Soit Q et R deux problèmes de décision. On dit que Q *se réduit au problème* R s'il existe $f : \mathscr{C}_Q \to \mathscr{C}_R$ totale et calculable, telle que

$$w \in Q^+ \iff f(w) \in R^+.$$

On note alors $Q \preccurlyeq R$.

Proposition : Si $Q \preccurlyeq R$, et que R est décidable, alors Q est décidable.

Preuve :
Soit $\texttt{decide}_R : \texttt{string} \to \texttt{bool}$ décidant R *i.e.* $(\texttt{decide}_R\ w) = \texttt{true} \iff w \in R^+$. Soit $f : \mathscr{C}_Q \to \mathscr{C}_R$ totale calculable, telle que $w \in Q^+ \iff f(w) \in R^+$. On doit coder la fonction suivante.

```
let decide_Q (w: string) : bool =
  (decide_R (f w))
```

CODE 4.9 – Fonction décidant un sous-problème

La fonction $\texttt{decide}_Q$ décide bien le problème Q. En effet,

$$\begin{aligned}(\texttt{decide}_Q\ \texttt{w}) = \texttt{true} &\iff (\texttt{decide}_R\ (f\ \texttt{w})) \\ &\iff (f\ \texttt{w}) \in R^+ \\ &\iff w \in Q^+.\end{aligned}$$

□

Corollaire : Si $Q \preccurlyeq R$, et Q non décidable, alors R non décidable.

EXEMPLE :
On considère le problème

$$\text{NONVIDE} : \begin{cases}\textbf{Entrée} & : M \in \mathbb{O} \\ \textbf{Sortie} & : \mathscr{L}(M) \neq\ ?\ .\end{cases}$$

Le problème NONVIDE est indécidable.

EXEMPLE :
Les problèmes

$$\begin{cases}\textbf{Entrée} & : M_1 \text{ et } M_2 \text{ deux machines} \\ \textbf{Sortie} & : \mathscr{L}(M_1) \cup \mathscr{L}(M_2) = \Sigma^\star\end{cases}$$

et

$$\begin{cases}\textbf{Entrée} & : M_1 \text{ et } M_2 \text{ deux machines} \\ \textbf{Sortie} & : \mathscr{L}(M_1) \cap \mathscr{L}(M_2) =\end{cases}$$

sont indécidables.

Proposition : La relation $\preccurlyeq$ est un *pré-ordre* :
- $\preccurlyeq$ est réflective ;
- $\preccurlyeq$ est transitive.

Preuve :
Soit Q un problème de décision.
- $Q \preccurlyeq Q$ par la fonction identité, qui est totale et calculable.
- Soient Q, R et S trois problèmes de décision tels que $Q \preccurlyeq R$ et $R \preccurlyeq S$. Soit donc f_1 la réduction de Q à R, et f_2 la réduction de R à S. Soit $f = f_2 \circ f_1 : \mathscr{C}_Q \to \mathscr{C}_S$. La fonction f est totale comme composée de fonctions totales, f est calculable comme composée de fonctions

calculables. De plus,

$$\begin{aligned} \forall e \in \mathscr{C}_Q, \qquad f(e) \in S^+ &\iff f_2(f_1(e)) \in S^+ \\ &\iff f_1(e) \in R^+ \\ &\iff e \in Q^+ \end{aligned}$$

□

IV.4 Classe P et NP

Pour répondre à un problème, on peut le résoudre par des algorithmes plus ou moins rapides. Mais, l'objectif de cette section est de montrer que certains problèmes ne peuvent se résoudre que par des algorithmes lents, et que l'on ne peut pas faire mieux.

Définition : Le modèle de calcul impose une représentation des entrées par chaînes de caractères. Cela induit donc une notion de *taille d'entrée*, qui est la longueur de la chaîne de caractères.

IV.4.1 Complexité d'une machine

Définition : Étant donné une machine $\mathscr{M}$ et une entrée $w \in \Sigma^\star$, on note $C^{\mathscr{M}}(w)$ le nombre d'opérations élémentaires effectuées lors de l'appel de $\mathscr{M}$ sur w. Lorsque $w \underset{\mathscr{M}}{\longrightarrow} \circlearrowleft$, on définit $C^{\mathscr{M}} = +\infty$.

Pour $n \in \mathbb{N}$, on définit alors

$$C_n^{\mathscr{M}} = \max\{C^{\mathscr{M}}(w) \mid w \in \Sigma^n\}.$$

Remarque :
On a, $\forall n \in \mathbb{N}$, $C_n^{\mathscr{M}} \in \bar{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$.

Définition : Soit $f : \mathbb{N} \to \mathbb{N}$ une fonction totale et calculable. On note $\textsc{Time}(f)$ l'ensemble des machines $\mathscr{M}$ telles que

- $\mathscr{M}$ s'arrête sur toute entrée ;
- $\big(C_n^{\mathscr{M}}\big)_{n\in\mathbb{N}} = \mathcal{O}\big(\big(f(n)\big)_{n\in\mathbb{N}}\big)$.

IV.4.2 Classe P

Définition : On dit d'une machine $\mathscr{M}$ qu'elle est de *complexité polynômiale* dès lors qu'il existe $k \in \mathbb{N}$ tel que $\mathscr{M} \in \textsc{Time}(n^k)$.

Définition : On dit d'une fonction (partielle ou non), qu'elle est *calculable en temps polynômial* dès lors qu'il existe une machine $\mathscr{M}$ de complexité polynômiale la calculant.

Exemple : — l'identité $(n \mapsto n)$

— la fonction successeur $(n \mapsto n+1)$

Proposition : La composée de deux fonctions totales calculables en temps polynômial est une fonction totale calculable en temps polynômial.

Preuve :
Soient f_1 et f_2 deux telles fonctions. Soit donc $\texttt{calcule}_1$: `string` $\to$ `string` et $\texttt{calcule}_2$: `string` $\to$ `string` calculant respectivement f_1 et f_2. On pose la fonction ci-dessous

```
1 let calcul s = calcule1 (calcule2 s)
```

Code 4.10 – Machine calculant la composée en temps polynômial

dont le nombre d'opérations élémentaires est

$$C(\mathtt{s}) = \underbrace{C^2(\mathtt{s})}_{\text{calcul de } f_2(\mathtt{s})} + \overbrace{C^1(f_2(\mathtt{s}))}^{\text{calcul de } f_1(\mathtt{s})} + \underbrace{1}_{\text{composée}}.$$

Or, la fabrication d'une chaîne de caractères de taille n nécessite au moins n opérations élémentaires. Soit $p_1 \in \mathbb{N}$ et $p_2 \in \mathbb{N}$ tels que la complexité de $\texttt{calcule}_1$ est $\mathcal{O}(n^{p_1})$ et la complexité de $\texttt{calcule}_2$ est $\mathcal{O}(n^{p_2})$. On a donc, pour tout $w \in \Sigma^\star$ avec $|w| = n$, que $|f_2(w)| = \mathcal{O}(n^{p_2})$ Par composition des $\mathcal{O}$, on a que

$$C(\mathtt{s}) = \mathcal{O}(|\mathtt{s}|^{p_1 \cdot p_2}).$$

□

Remarque :
Dans la preuve précédente, l'ordre du polynôme change. En effet, la composée de deux programmes en $\mathcal{O}(n^2)$ est un $\mathcal{O}(n^4)$. L'espace des fonctions calculables en $\mathcal{O}(n^p)$, pour un p fixé, n'est pas stable par composition.

Définition (Classe **P**) **:** On dit qu'un problème est dans **P** dès lors qu'il est décidable en temps polynômial.

Proposition (Stabilité de la classe **P**) **:** La classe **P** est stable par
— union ; — intersection ; — complémentaire.

Preuve :
à faire □

IV.4.3 Classe NP

Définition (Classe **NP**) **:** On dit qu'un problème de décision Q est dans **NP** si et seulement si
— il existe un polynôme A ;
— un problème $\textsc{Verif} \in \mathbf{P}$;
— un ensemble $\mathscr{C}$ (certificats),
tels que

$$\forall w \in \Sigma^\star, \quad \Big(w \in Q^+ \iff \exists u \in \mathscr{C},\ |u| \leqslant A(|w|) \text{ et } (w,u) \in \textsc{Verif}^+ \Big).$$

La classe **NP** est la classe de problèmes tels qu'ils sont vérifiables en temps polynômial. Par exemple, si on a une formule logique, trouver un environnement propositionnel est coûteux en temps, MAIS vérifier la solution est très simple. Nous verrons ce résultat plus tard dans cette sous-section.

Le "**NP**" ne vient pas de **N**on **P**olynômial, mais vient de **N**on-déterministe **P**olynômial.

Proposition :

$$\mathbf{P} \subseteq \mathbf{NP}.$$

Preuve :
À faire : Modifier la définition de VERIF avec la nouvelle définition d'un problème **NP** Soit Q un problème de décision dans **P**. On pose $\mathscr{C} = \mathscr{C}_Q$, $A(X) = X$, et $\textsc{Verif} = Q$. En effet, pour tout $w \in \Sigma^\star$,

$$w \in Q^+ \iff \exists u = w,\ |u| \leqslant A(|w|) \text{ et } u \in \textsc{Verif}^+.$$

□

Proposition :

$$\textsc{Sat} \in \mathbf{NP}.$$

RAPPEL :

On rappelle la définition du problème Sat.

$$\textsc{Sat} : \begin{cases} \textbf{Entrée} & : \text{Une formule } G \\ \textbf{Sortie} & : \text{Existe-t-il } \rho \in \mathbb{B}^{\text{vars}(G)} \text{ tel que } [\![G]\!]^\rho = \mathbf{V} \,? \end{cases}$$

Preuve :
Soit alors le problème suivant.

$$\textsc{VerifSat} : \begin{cases} \textbf{Entrée} & : \begin{pmatrix} \text{Une formule } G, \\ \text{un environnement propositionnel } \rho \in \mathbb{B}^{\text{vars}(G)}, \end{pmatrix} \\ \textbf{Sortie} & : [\![G]\!]^\rho =^? \mathbf{V} \end{cases}$$

En TP, on a codé une solution polynômial à VerifSat donc VerifSat $\in \mathbf{P}$.
On définit l'ensemble $\mathscr{C}$ des certificats comme

$$\mathscr{C} = \left\{ (G, \rho) \;\middle|\; G \in \mathscr{F} \text{ et } \rho \in \mathbb{B}^{\text{vars}(G)} \right\}.$$

On a alors

$$G \in \textsc{Sat}^+ \iff \exists \rho \in \mathbb{B}^{\text{vars}(G)},\ [\![G]\!]^\rho = \mathbf{V}.$$

Il suffit alors de choisir $A(X) = 2X$. □

IV.4.4 NP-difficile

Figure 4.2 – Structure d'un sous-problème

Définition (Réduction polynômiale) **:** Soit Q et R deux problèmes de décision, on appelle *réduction polynômiale* de Q à R la donnée d'une fonction f totale, calculable en temps polynômial de $\mathscr{C}_Q$ dans $\mathscr{C}_R$ telle que

$$\forall w \in \mathscr{C}_Q, \quad w \in Q^+ \iff f(w) \in R^+.$$

On note alors $Q \preccurlyeq_{\text{p}} R$.

Proposition : La relation $\preccurlyeq_{\text{p}}$ est transitive et reflective : c'est un pré-ordre.

Preuve :
La réflectivité est assurée car id est totale et calculable en temps polynômial. La transitivité est assurée par les propriétés précédentes (composée de deux fonctions polynômiales ?). □

Proposition : Si $R \preccurlyeq_{\mathrm{p}} Q$, et $R \in \mathbf{P}$, alors $Q \in \mathbf{P}$. □

Définition (**NP**-difficile) **:** Un problème Q est **NP**-difficile si

$$\forall R \in \mathbf{NP},\ R \preccurlyeq_{\mathrm{p}} Q.$$

Proposition : Si Q est **NP**-difficile, et $Q \preccurlyeq_{\mathrm{p}} R$, alors R est **NP**-difficile.

Preuve :
Soit $S \in \mathbf{NP}$, donc $S \preccurlyeq_{\mathrm{p}} Q$. De plus, $Q \preccurlyeq_{\mathrm{p}} R$, donc $S \preccurlyeq_{\mathrm{p}} R$, par transitivité. Ceci étant vrai pour tout $S \in \mathbf{NP}$, on en déduit que R est **NP**-difficile. □

On admet le théorème suivant.

Théorème (Cook-Levin) **:** Le problème Sat est **NP**-difficile.

Preuve :
Admis □

Définition (***n*-FNC**) **:** Soit $n \in \mathbb{N}$. Une formule G est sous forme n-FNC dès lors que G est sous forme FNC et chaque clause de G contient au plus n littéraux.

On parle aussi de forme CNF traduction anglaise de FNC. De même, on parle de forme n-CNF au lieu de n-FNC.

Exemple :
La formule $(p \vee q) \wedge r$ est une 2-CNF. La formule $(p \vee q \vee p) \wedge (r \vee p \vee q \vee q)$ est une 4-CNF.

Définition : On définit le problème ci-dessous.

$$n\text{-CNF-SAT} : \begin{cases} \textbf{Entrée} & : G \text{ une } n\text{-CNF} \\ \textbf{Sortie} & : \text{Existe-t-il } \rho \text{ tel que } [\![G]\!]^\rho = \mathbf{V} \,? \end{cases}$$

Proposition : Soit 3SAT = 3-CNF-SAT. Le problème 3SAT est **NP**-difficile.

Preuve (par réduction de SAT à 3SAT) *:*
Soit G une formule sur $\mathbb{Q}$, un ensemble de variables propositionnelles. Pour toute sous-formule H, on note

- x_H une variable propositionnelle,
- K_H une formule définie par
  - si $H = \top$, $H = \bot$ ou $H = p \in \mathbb{Q}$, alors $K_H = H$,
  - si $H = \neg H_1$, alors $K_H = \neg x_{H_1}$,
  - si $H = H_1 \odot H_2$, avec $\odot \in \{\to, \vee, \wedge, \leftrightarrow\}$, alors $K_H = x_{H_1} \odot x_{H_2}$.

Définissons alors la formule

$$K = \bigwedge_{H \text{ sous-formule de } G} (x_H \leftrightarrow K_H).$$

On note aussi, si $\mathbb{Q} \subseteq \mathbb{Q}'$ deux ensembles de variables propositionnelles, et $\rho \in \mathbb{B}^{\mathbb{Q}}$, on note $\rho' \sqsupseteq \rho$ dès lors que $\mathrm{def}(\rho') = \mathbb{Q}'$ et $\forall x \in \mathbb{Q}$, $\rho(x) = \rho'(x)$. On pose $\mathbb{Q}' = \mathbb{Q} \cup \{x_H \mid H \text{ sous-formule de } G\}$. On considère à présent le lemme suivant.

Lemme : Soit $\rho \in \mathbb{B}^{\mathbb{Q}}$. Il existe $\rho' \in \mathbb{B}^{\mathbb{Q}'}$ tel que $\rho' \sqsupseteq \rho$ et $[\![K]\!]^\rho = \mathbf{V}$.

Prouvons ce lemme.

Preuve :
On définit

$$\rho'(x) = \begin{cases} \rho(x) & \text{si } x \in \mathbb{Q} \\ [\![H]\!]^{\rho} & \text{si } x = x_H. \end{cases}$$

Soit alors H une sous-formule de G.

— Si $H = \top$, alors $\rho'(x_H) = [\![H]\!]^{\rho} = [\![x_H]\!]^{\rho'}$, et $[\![K_H]\!]^{\rho'} = [\![H]\!]^{\rho'} = [\![\top]\!]^{\rho'} = [\![H]\!]^{\rho}$. Ainsi, $[\![x_H \leftrightarrow K_H]\!]^{\rho'} = \mathbf{V}$.

— Si $H = \neg H_1$, alors $[\![x_H]\!]^{\rho'} = [\![H]\!]^{\rho}$, et

$$[\![K_H]\!]^{\rho'} = [\![\neg x_{H_1}]\!]^{\rho'} = \overline{[\![x_{H_1}]\!]^{\rho'}} = \overline{[\![H_1]\!]^{\rho}} = [\![H]\!]^{\rho}.$$

On en déduit que $[\![x_H \leftrightarrow K_H]\!]^{\rho'} = \mathbf{V}$.

— Si $H = H_1 \wedge H_2$, alors $[\![x_H]\!]^{\rho'} = [\![H]\!]^{\rho}$, et

$$\begin{aligned} [\![K_H]\!]^{\rho'} &= [\![x_{H_1} \wedge x_{H_2}]\!]^{\rho'} \\ &= [\![x_{H_1}]\!]^{\rho'} \cdot [\![x_{H_2}]\!]^{\rho'} \\ &= [\![H_1]\!]^{\rho} \cdot [\![H_2]\!]^{\rho} \\ &= [\![H_1 \wedge H_2]\!]^{\rho} \\ &= [\![H]\!]^{\rho} \end{aligned}$$

— De même pour les autres cas...

On a donc

$$\left[\!\!\left[\bigwedge_{H \text{ sous-formule de } G} x_H \leftrightarrow K_H \right]\!\!\right]^{\rho'} = \bigbullet_{H \text{ sous-formule de } G} [\![x_H \leftrightarrow K_H]\!]^{\rho'} = \mathbf{V}$$

et donc $[\![K]\!]^{\rho'} = \mathbf{V}$. □

Lemme : Pour tout environnement propositionnel $\rho \in \mathbb{B}^{\mathbb{Q}}$, et pour tout $\rho' \in \mathbb{B}^{\mathbb{Q}'}$. Si $[\![K]\!]^{\rho'} = \mathbf{V}$, alors $\rho(x_G) = [\![G]\!]^{\rho}$.

Preuve :
Soient $\rho \in \mathbb{B}^{\mathbb{Q}}$ et $\rho' \in \mathbb{B}^{\mathbb{Q}'}$ deux environnements propositionnels. *Montrons, par induction sur les sous-formules de G, pour toute sous-formule H de G, que $\rho'(x_H) = [\![H]\!]^{\rho}$.*

— Si $H = \top$, alors, comme $[\![K]\!]^{\rho'} = \mathbf{V}$, on a $[\![x_H \leftrightarrow K_H]\!]^{\rho'} = \mathbf{V}$, donc $\rho'(x_H) = [\![H]\!]^{\rho'} = [\![H]\!]^{\rho}$.

— Si $H = \neg H_1$, avec $\rho'(x_{H_1}) = [\![H_1]\!]^{\rho}$ par hypothèse d'induction, alors $[\![K]\!]^{\rho'} = \mathbf{V}$ donc $[\![x_H \leftrightarrow K_H]\!]^{\rho'} = \mathbf{V}$, d'où

$$\begin{aligned}\rho'(x_H) &= [\![K_H]\!]^{\rho'}\\ &= [\![\neg x_{H_1}]\!]^{\rho'}\\ &= \overline{[\![x_{H_1}]\!]^{\rho'}}\\ &= \overline{[\![H_1]\!]^{\rho}}\\ &= [\![\neg H_1]\!]^{\rho}\\ &= [\![H]\!]^{\rho}\end{aligned}$$

— Si $H = H_1 \wedge H_2$, avec $\rho'(x_{H_1}) = [\![H_1]\!]^{\rho}$, et $\rho'(x_{H_2}) = [\![H_2]\!]^{\rho}$ par hypothèse d'induction, alors $[\![K]\!]^{\rho} = \mathbf{V}$ donc $[\![x_H \leftrightarrow K_H]\!]^{\rho'} = \mathbf{V}$ d'où

$$\begin{aligned}\rho'(x_H) &= [\![K_H]\!]^{\rho'}\\ &= [\![x_{H_1} \wedge x_{H_2}]\!]^{\rho'}\\ &= [\![x_{H_1}]\!]^{\rho'} \cdot [\![x_{H_2}]\!]^{\rho'}\\ &= [\![H_1]\!]^{\rho} \cdot [\![H_2]\!]^{\rho}\\ &= [\![H_1 \wedge H_2]\!]^{\rho}\\ &= [\![H]\!]^{\rho}\end{aligned}$$

— De même pour les autres cas...

□

À l'instance G du problème SAT, on associe donc la formule $K \wedge x_G$.

" $\Longrightarrow$ " Soit $G \in \text{SAT}^+$, soit alors ρ tel que $[\![G]\!]^{\rho} = \mathbf{V}$, alors il existe, d'après le premier lemme, un environnement ρ' tel que $[\![K]\!]^{\rho'} = \mathbf{V}$. Le second lemme nous donne alors $[\![x_G]\!]^{\rho'} = [\![G]\!]^{\rho} = \mathbf{V}$ donc $[\![K \wedge x_G]\!]^{\rho'}$ d'où $[\![K \wedge x_G]\!] \in \text{SAT}^+$.

" $\Longleftarrow$ " Si $K \wedge x_G \in \text{SAT}^+$, il existe donc ρ' tel que $[\![K \wedge x_G]\!]^{\rho'} = \mathbf{V}$ donc $[\![K]\!]^{\rho'} = \mathbf{V}$ et $\rho'(x_G) = \mathbf{V}$. Soit alors ρ la restriction de ρ' à $\mathbb{Q}$. Ainsi, d'après le second lemme, $[\![G]\!]^{\rho} = \rho'(x_G) = \mathbf{V}$.

□

Remarque :
Pour tout $n \geqslant 3$, le problème n-CNF-SAT est **NP**-difficile. Ceci peut être prouvé par réduction avec la fonction identité à 3SAT.

Définition : On dit qu'un problème est **NP**-complet s'il est dans la classe **NP** et dans la classe **NP**-difficile :

$$\textbf{NP}\text{-complet} = \textbf{NP}\text{-difficile} \cap \textbf{NP}.$$

Remarque :
Le problème SAT est **NP**-complet.

Chapitre 5

Trois exemples d'algorithmes de graphes

Dans ce chapitre, on s'intéresse aux graphes. Nous rappellerons les notions et algorithmes de graphes vus l'année dernière. On considère 3 exemples d'algorithmes de graphes.

Par exemple, l'année dernière, nous avons vu comment décomposer un graphe non-orienté en composantes connexes : on choisit un sommet au hasard, puis on parcours les voisins de ce sommets, et on répète. Mais, dans un graphe orienté, la notion de « composante connexe » n'est plus la même dans un graphe orienté. C'est l'algorithme décrit dans la section 1.

IV.1 Composantes fortement connexes (cfc)

Dans la suite de cette section, $G = (S, A)$ est un graphe orienté.

Définition : On dit que $v \in S$ est *accessible* depuis $u \in S$ s'il existe un chemin de u à v, que l'on note $u \xrightarrow{\star} v$. De même, on dit que $v \in S$ est *co-accessible* depuis $u \in S$ s'il existe un chemin de v à u, que l'on note $v \xrightarrow{\star} u$.

Définition ($u \sim_G v$) : On note $u \sim_G v$ si $u \xrightarrow{\star} v$ et $v \xrightarrow{\star} u$.

Remarque :
La relation $\sim_G$ est une relation d'équivalence.

Digression L'année dernière, dans un graphe non orienté, on peut noter $\sim$ la relation d'équivalence induite par, si $\{u, v\} \in A$, alors $u \sim v$. Dans ce cas, le même chemin permet d'aller de u à v, puis de v à u, et ce chemin est le même.

Mais, dans un graphe orienté, si $u \sim_G v$, les chemins de u à v puis de v à u ne sont pas forcément les mêmes.

Définition (CFC) **:** On appelle *composantes fortement connexes* (CFC) d'un graphe G, les classes d'équivalences de la relation $\sim_G$.

Définition : On dit d'un graphe ayant une unique composante fortement connexe qu'il est *fortement connexe*.

EXEMPLE :
Le graphe ci-dessous a deux composantes fortement connexes, il n'est donc pas fortement connexe.

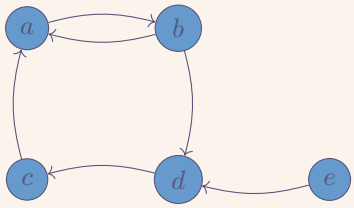


FIGURE 5.1 – Graphe non fortement connexe

Définition : On appelle *ensemble fortement connexe* un ensemble $V \subseteq S$ tel que G_V est fortement connexe où G_V est le *graphe induit* par V : $G_V = (V, A \cap V^2)$.

EXEMPLE :
Avec le graphe précédent, l'ensemble $\{a, b\}$ est un ensemble fortement connexe.

Lemme : Si W est une composante fortement connexe de G, alors W est un ensemble fortement connexe.

Preuve :
Soit W une composante fortement connexe. On doit montrer que W est un ensemble fortement connexe, *i.e.* le graphe G_W est fortement connexe, *i.e.* pour tout couple de sommets $(u, v) \in W^2$, $u \sim_{G_W} v$. Étant donné que W est une composante connexe, $u \sim_G v$, donc il existe $(n, m) \in \mathbb{N}^2$ et deux chemins

$$u \to v_1 \to v_2 \to \cdots \to v_n = v \quad \text{et} \quad v \to u_1 \to u_2 \to \cdots \to u_m = u.$$

Soit alors $i \in [\![1, n]\!]$. On a donc deux chemins

$$v \to u_1 \to u_2 \to \cdots \to u_m = u \to v_1 \to \cdots \to v_i$$

et

$$v_i \to v_{i+1} \to \cdots \to v_n = v.$$

Ainsi, $v \sim_G v_i$ et $v_i \in W$. De même, pour tout $j \in [\![1, m]\!]$, $u_j \in W$. Ainsi, $u \sim_{G_w} v$ (en utilisant les mêmes chemins). Donc, G_W est fortement connexe puisque toute paire de sommets est équivalent) □

Proposition : Les composantes fortement connexes sont les ensembles fortement connexes qui sont maximaux pour l'inclusion.

Preuve " $\Longleftarrow$ " Soit V un ensemble fortement connexe maximal pour l'inclusion.
Remarque : on a $V \neq$. En effet, un singleton est un ensemble fortement connexe, et donc V ne sera pas maximal pour l'inclusion.
Soit $(u, v) \in V^2$. Par définition de fortement connexe, $u \sim_{G_V} v$ donc $u \sim_G v$. Soit alors W la classe des éléments de $V \subseteq W$. L'ensemble W est fortement connexe (d'après le lemme précédent). Ainsi, $W = V$, W est donc une composante fortement connexe.

" $\Longrightarrow$ " Soit V une composante fortement connexe. L'ensemble V est fortement connexe, d'après le lemme précédent. Soit $W \supseteq V$ tel que W est fortement connexe. Montrons que $V = W$.

- Si $W \setminus V =$, alors OK.
- Si $W \setminus V \neq$, alors soit $z \in W \setminus V$. L'ensemble W est fortement connexe. Soit $u \in V$. On a $u \sim_{G_W} z$, donc $u \sim_G z$, donc $z \in V$ ce qui est absurde.

□

Définition : On appelle *graphe réduit* de G le graphe orienté $\hat{G} = (\hat{S}, \hat{A})$ où

$$\hat{S} = \{\bar{x} \mid x \in S\} \quad \text{et} \quad \hat{A} = \big\{(\bar{x}, \bar{y}) \mid (x, y) \in A \text{ et } \bar{x} \neq \bar{y}\big\}.$$

Exemple :
À faire : Figure

Remarque : — $\hat{G}$ est acyclique.
— Pour tout couple $(\bar{x}, \bar{y}) \in \hat{S}^2$, si $\bar{x} \xrightarrow{\star}_{\hat{G}} \bar{y}$, alors $\forall u \in \bar{x}$, $\forall v \in \bar{y}$, $x \xrightarrow{\star}_G v$.

IV.1.1 Rappels

Définition : La *bordure* d'un ensemble de sommets $V \subseteq S$, noté $\mathscr{B}(V)$, est l'ensemble des successeurs de V non dans V :

$$\mathscr{B}(V) = \{s \in S \setminus V \mid \exists u \in V,\ (u, s) \in A\}.$$

Définition (parcours) **:** Un *parcours* est une permutation des sommets $(L_1, L_2, \ldots, L_n)$ telle que, pour $i \in [\![1, n-1]\!]$,

$$L_i \in \mathscr{B}(\{L_1, \ldots, L_{i-1}\}) \quad \text{ou} \quad \mathscr{B}(\{L_1, \ldots, L_{i-1}\}) = .$$

On dit d'un L_i avec $i \in [\![1, n]\!]$ tel que $\mathscr{B}(\{L_1, \ldots, L_{i-1}\}) = $, que c'est un *point de régénération* du parcours.

Lemme : Si $V \subseteq S$ est tel que $\mathscr{B}(V) = $, il n'existe aucun chemin d'un sommet de V à un chemin de $S \setminus V$.

Preuve (par l'absurde) *:*
Soit un chemin $V \ni u_0 \to u_1 \to \cdots \to u_k \in S \setminus V$ avec $k \in \mathbb{N}$. Soit $I = \{i \in [\![0, k]\!] \mid u_i \in S \setminus V\}$. L'ensemble I est non vide, car $u_k \in S \setminus V$, et $I \subseteq N$. Il admet donc un plus petit élément ; nommons le $i_0 \in [\![0, k]\!]$. On a $i_0 \neq 0$ car $u_0 \in V$. Ainsi, $u_{i_0-1} \in V$, $u_{i_0} \in S \setminus V$, et $(u_{i_0-1}, u_{i_0}) \in A$. Donc, $u_{i_0} \in \mathscr{B}(V)$, ce qui est absurde. □

Définition : Soit $(L_1, L_2, \ldots, L_n)$ un parcours de G. On note K le nombre de ses points de régénération. On note $(r_k)_{k \in [\![1,k]\!]}$ l'extractrice des points de régénération. En notant de plus $r_{K+1} = n+1$. Le *partitionnement associé au parcours* est alors

$$\Big\{\{L_{r_i}, L_{r_i+1}, \ldots, L_{r_{i+1}-1}\} \,\Big|\, i \in [\![1, K]\!]\Big\}..$$

Exemple :
Si $n = 10$ et les points de régénération sont d'indices 1, 4, 7 et 8, alors le partitionnement associé est donc

$$\Big\{\{1, 2, 3\}, \{4, 5, 6\}, \{7\}, \{8, 9, 10\}\Big\}.$$

Définition : Un partitionnement P_1 est un *raffinement* d'un

partitionnement P_2 dès lors que

$$\forall C_1 \in P_1,\ \exists C_2 \in P_2,\ C_1 \subseteq C_2.$$

Proposition : Les composantes fortement connexes sont un raffinement des partitionnement des parcours.

Preuve :
Soient u et v deux sommets de la même composante fortement connexes. Supposons que u et v ne sont pas dans la même partie du partitionnement pour un parcours $(L_1, \dots, L_n)$ du graphe. Soit i_u et i_v tels que $u = L_{i_u}$ et $v = L_{i_v}$. Sans perdre en généralité, on peut supposer $i_u \leqslant i_v$. Il existe alors $i_0 \in [\![i_u, i_v]\!]$ tels que L_{i_0} est un point de régénération. Alors,

$$\mathscr{B}\big(\{L_1, L_2, \dots, L_{i_0-1}\}\big) = .$$

D'après le lemme précédent, il n'existe pas de chemin de u à v, ce qui est absurde car u et v sont dans la même composante fortement connexe. □

IV.1.2 Rangement particulier de graphe

Définition (Sommet ouvert) **:** Soit $(L_1, \dots, L_n)$ un parcours de G. Pour $k \in [\![1, n]\!]$ et $i \in [\![1, k[\![$, on dit que L_i est *ouvert* à l'étape k si

$$\mathrm{Succ}(L_i) \not\subseteq \{L_j \mid j \in [\![1, k[\![\}$$

où $\mathrm{Succ}(L_i)$ est l'ensemble des successeurs de L_i.

Cette définition nous permet de définir les parcours en largeur et en profondeur.

Définition (parcours en largeur) **:** Soit $(L_1, \dots, L_n)$ un parcours. Il est dit *en largeur* si chaque sommet du parcours qui n'est pas un point de régénération est un successeur du premier sommet ouvert à cette étape :

$$\forall k \in [\![2, n]\!], \qquad \mathscr{B}(\{L_j \mid j \in [\![1, k[\![\} = \quad \text{ou} \quad L_k \in \mathrm{Succ}(L_{i_0})$$

avec $i_0 = \min\{i \in [\![1, k[\![\mid L_i \text{ ouvert à l'étape } k\}$.

Définition (parcours en profondeur) **:** Soit $(L_1, \dots, L_n)$ un parcours. Il est dit *en largeur* si chaque sommet du parcours qui n'est pas un point de

régénération est un successeur du dernier sommet ouvert à cette étape :

$$\forall k \in [\![2, n]\!], \qquad \mathscr{B}(\{L_j \mid j \in [\![1, k[\![\}) = \qquad \text{ou} \qquad L_k \in \mathrm{Succ}(L_{i_0})$$

avec $i_0 = \max\{i \in [\![1, k[\![\mid L_i \text{ ouvert à l'étape } k\}$.

Exemple :
Dans le graphe ci-dessous, un parcours en largeur est

$$\underline{a} \to c \to b \to d \to f \rightsquigarrow \underline{e}.$$

Les sommets soulignées sont les points de régénération. On peut remarquer qu'il n'y a pas unicité du parcours en largeur, on aurait pu commencer le parcours par $\underline{a} \to b \to c \to \cdots$, et ce parcours est aussi un parcours en largeur.

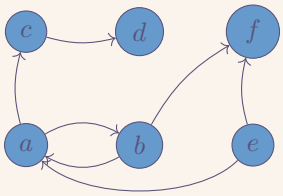


Figure 5.2 – Exemple de graphe orienté – parcours en largeur

Sur le même graphe, un parcours en profondeur est

$$\underline{a} \to b \to f \to c \to d \rightsquigarrow \underline{e}.$$

De même, il n'y a pas unicité du parcours en profondeur.

Définition (tri topologique) **:** Soit $(T_i)_{i \in [\![1,n]\!]}$ une permutation des sommets. On dit que T est un *tri topologique* si

$$\forall (i, j) \in [\![1, n]\!]^2, \qquad \text{si } (T_i, T_j) \in A \text{ alors } i \leqslant j.$$

Exemple :
Un tri topologique du graphe ci-dessous est la permutation indiquée dans le graphe.

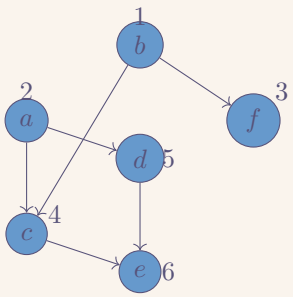


FIGURE 5.3 – Tri topologique d'un graphe

Définition : Soit une permutation de sommets $(T_i)_{i\in[\![1,n]\!]}$. On appelle *rang* de $u \in S$ dans T le plus petit indice dans T d'un élément accessible $(u \xrightarrow{\star} v)$ et co-accessible $(v \xrightarrow{\star} u)$ depuis u. On définit

$$\mathrm{rang}_T(u) = \min\{i \in [\![1,n]\!] \mid T_i \sim_G u\}.$$

Définition : Étant donné une permutation $(T_i)_{i\in[\![1,n]\!]}$ des sommets de G, on définit la relation

$$\preccurlyeq_T = \{(u,v) \in S^2 \mid \mathrm{rang}(u) \leqslant \mathrm{rang}(v)\}.$$

On dit alors que T est un *tri préfixe* dès lors que, pour tout $(u,v) \in S^2$, si $u \xrightarrow{\star} v$ alors $u \preccurlyeq_T v$.

REMARQUE :
Étant donné une permutation T, pour tout couple de sommets (u,v),

$$u \sim_G v \iff (u \preccurlyeq_T v \text{ et } v \preccurlyeq_T u).$$

IV.1.3 Graphe transposé et cfc

Définition : Étant donné un graphe $G = (S,A)$, on appelle *graphe transposé* de G, que l'on note $G^\top$, le graphe

$$G^\top = \Big(S, \big\{(y,x) \in S^2 \,\big|\, (x,y) \in A\big\}\Big).$$

Proposition : Soit T un tri préfixe de G. Soit L un parcours de $G^\top$ utilisant l'ordre des points de régénération induit par T. Alors, la partition associée à L est la décomposition en composantes forment connexes.

Preuve :
Soit T un tri préfixe du graphe G. Soit L un parcours de $G^\top$. Montrons que le partitionnement associé à L est la décomposition en composantes fortement connexes. Il suffit de montrer que, si u et v sont dans la même partition du parcours L de $G^\top$: $u \sim_G v$.

Remarque : les composantes fortement connexes de G et $G^\top$ sont les mêmes.

Soient u et v deux sommets dans la même partition de L. C'est donc qu'il existe un point de régénération L_{r_k} tel que $L_{r_k} \xrightarrow{\star}_{G^\top} u$ et $L_{r_k} \xrightarrow{\star}_{G^\top} v$. Ainsi, $L_{r_k} \xleftarrow{\star}_G u$ et $L_{r_k} \xleftarrow{\star}_G v$. Alors, $\text{rang}_T(u) \leqslant \text{rang}_T(L_{r_k})$.

Supposons que $L_{r_k} \not\xrightarrow{\star}_G u$. Alors, $\text{rang}_T(u) \neq \text{rang}_T(L_{r_k})$. D'où, il existe $w \sim_G u$ apparaissant avant (strictement) L_{r_k} dans T. Ce qui est absurde car on aurait dû visiter w avant.

On en déduit que $L_{r_k} \xrightarrow{\star}_G u$, et $v \xrightarrow{\star}_G u$, De même pour v, on a $L_{r_k} \xrightarrow{\star}_G v$ et $u \xrightarrow{\star}_G v$. Finalement, on a

$$u \sim_G v.$$

□

Exemple :

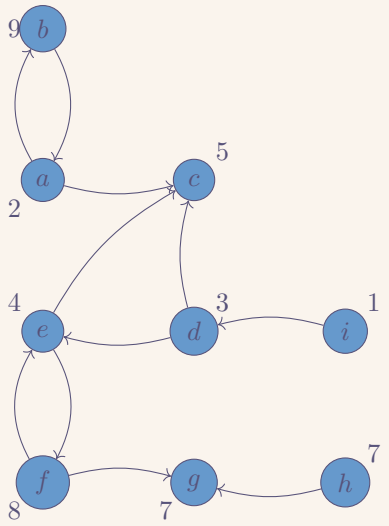


Figure 5.4 – Exemple de tri préfixe

Un tri préfixe dans le graphe ci-dessous est $g \leftarrow f \leftarrow c \leftarrow e \leftarrow d \rightsquigarrow i \rightsquigarrow b \leftarrow a \rightsquigarrow h$. Il s'agit d'un parcours en profondeur.

IV.1.4 Calcul de tri préfixe

On peut donc donner un algorithme calculant un tri préfixe. On donne cet algorithme en impératif, même si la version récursive est plus simple.

Algorithme 5.1 Calcul d'un tri préfixe

Entrée Un graphe $G = (S, A)$.
Sortie Un tri préfixe des sommets de G.

```
1 : Procédure ExploreDescendants(s, Visités, Res)
2 :     Entrée Un graphe G = (S, A), Res, Visités, s ∈ S.
3 :     Sortie Modifie Res et Visités de sorte que Res soit un parcours préfixe
        de Visités et des sommets accessibles depuis s.
4 :     todo ← pileVide
5 :     empiler((s, Succ(s)), todo)
6 :     Visités ← {s} ∪ Visités
7 :     tant que todo ≠ pileVide faire
8 :         (x, ℓ) ← depiler(todo)
9 :         si ℓ = ( ) alors
10 :            Res ← x · Res
11 :        sinon
12 :            t · ℓ' ← ℓ        ▷ on sépare la tête t du reste ℓ' de la pile ℓ.
13 :            empiler((x, ℓ'), todo)
14 :            si t ∉ Visités alors
15 :                Visités ← {t} ∪ Visités
16 :                empiler((t, Succ(t)), todo)

17 : Visités ←
18 : Res ← ( )
19 : tant que S \ Visités ≠ faire
20 :     s ← un sommet de S \ Visités
21 :     ExploreDescendants(s, Visités, Res)
22 : retourner Res
```

On montre la correction de cet algorithme. On cherche des invariants *intéressants*, que l'on ne prouvera pas. Pour la boucle "tant que," dans la procédure ExploreDescendants, on choisit les invariants

1. pour tout couple de sommets $(u, v) \in S^2$, si $\mathscr{C}\ell(u) \subseteq$ Res et que $u \xrightarrow{\star} v$, alors $\mathscr{C}\ell(v) \subseteq$ Res et $\mathrm{rand}_{\mathrm{Res}}(u) \leqslant \mathrm{rang}_{\mathrm{Res}}(v)$,
2. $K(\mathrm{todo}) \cup \mathrm{Res} = \mathrm{Visités}$, où où $K(\mathrm{todo})$ est l'ensemble des premières composantes des couples de todo,
3. les clés de todo, du fond de la pile au sommet forment un chemin,
4. si u est un élément de Visités, et v est un descendant de u,
   - ou bien $v \in$ Res,
   - ou bien $v \in K(\mathrm{todo})$
   - ou bien v est un descendant d'un élément d'une liste adjointe à un élément $w \in K(\mathrm{todo})$ tel que $u \xrightarrow{\star} w$.

On admet que ces 4 propriétés sont invariantes. À la fin, $\forall x \in$ Res, $\mathscr{C}\ell(x) \subseteq$ Res, et dnc l'invariant 1 assure alors que nous avons un tri préfixe.

IV.1.5 Algorithme de Kosaraju

Algorithme 5.2 Algorithme de Kosaraju

Entrée Un graphe $G = (S, A)$
Sortie Les composantes fortement connexes de G
1 : On calcule un tri préfixe de G.
2 : On parcours $G^\top$ en utilisant l'ordre T comme points de régénération.
3 : On retourne le plus petit partitionnement associé au parcours.

IV.1.6 Applications

Théorème : 2-CNF-SAT $\in$ **P**.

EXEMPLE :
On considère la formule $H = (x \vee \neg y) \wedge (\neg y \vee z) \wedge (y \vee \neg z) \wedge (y \vee z)$. Elle est équivalente à

$$\begin{aligned} H' = \quad & (\neg x \to \neg y) \\ & \wedge (y \to x) \\ & \wedge (y \to z) \\ & \wedge (\neg z \to \neg y) \\ & \wedge (z \to y) \\ & \wedge (\neg y \to \neg z) \\ & \wedge (\neg y \to z) \\ & \wedge (\neg z \to y) \end{aligned}$$

En replaçant les $\to$ par des arrêtes dans un un graphe, on obtient celui représenté ci-dessous.

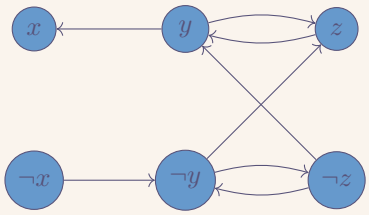


FIGURE 5.5 – Représentation d'une formule 2-CNF-SAT par un graphe

Preuve :
Soit $H \in$ 2CNF. On pose

$$H = (\ell_{1,1} \vee \ell_{1,2}) \wedge \ldots \wedge (\ell_{n,1} \vee \ell_{n,2}).$$

Dans la suite, on note $\ell^{\mathrm{c}}_{i,j}$ le littéral opposé à $\ell_{i,j}$. À la formule H, nous

associons le graphe G_H défini comme suit :

$$S_H = \big\{(\ell_{i,j}) \mid i \in [\![1,n]\!], j \in \{1,2\}\big\} \cup \big\{(\ell^{\mathrm{c}}_{i,j}) \mid i \in [\![1,n]\!], j \in \{1,2\}\big\},$$
$$A_H = \big\{(\ell^{\mathrm{c}}_{i,1}, \ell_{i,2} \mid i \in [\![1,n]\!]\big\} \cup \big\{(\ell^{\mathrm{c}}_{i,2}, \ell_{i,1}) \mid i \in [\![1,n]\!]\big\}.$$

Lemme : Si ρ est un modèle de H et $u \xrightarrow{\star} v$ tel que $[\![u]\!]^\rho = \mathbf{V}$, alors $[\![v]\!]^\rho = \mathbf{V}$.

Preuve :
Soit ρ un modèle de H. Montrons par récurrence P_n : "si $u \xrightarrow{\star} v$ par un chemin de longueur n et $[\![u]\!]^\rho = \mathbf{V}$, alors $[\![v]\!]^\rho = \mathbf{V}$."

— P_0 : $u = v$, donc OK.

— P_{n+1} : supposons P_n vraie pour $n \in \mathbb{N}$. Soient u et v tels que

$$u \to u_1 \to u_2 \to \cdots \to u_n \to u_{n+1} = v$$

et $[\![u_n]\!]^\rho = \mathbf{V}$. D'après P_n, $[\![u_n]\!]^\rho = \mathbf{V}$. Or, $(u_n, u_{n+1}) \in A_H$. C'est donc que $u_n^{\mathrm{c}} \vee u_{n+1} \in H$. Or, $[\![u_n]\!]^\rho = \mathbf{V}$, donc $[\![u_n^{\mathrm{c}}]\!]^\rho = \mathbf{F}$. Or, $[\![u_n \vee v]\!]^\rho = \mathbf{V}$ et donc $[\![v]\!]^\rho = \mathbf{V}$.

On conclut par récurrence. □

Proposition : H est satisfiable si, et seulement si aucune variable et sa négation ne se trouvent dans la même CFC de G_H.

Preuve $\Longrightarrow$ " Par contraposée, soit x et $\neg x$ se trouvant dans la même CFC de G_H. On procède par l'absurde. Soit ρ un environnement propositionnel tel que $[\![H]\!]^\rho = \mathbf{V}$.

— Si $\rho(x) = \mathbf{V}$, alors $[\![x]\!]^\rho = \mathbf{V}$. Or, $x \xrightarrow{\star} \neg x$. Alors, d'après le lemme, $[\![\neg x]\!]^\rho = \mathbf{V}$ et donc $\rho(x) = \mathbf{F}$, absurde.

— Si $\rho(x) = \mathbf{F}$, alors $[\![\neg x]\!]^\rho$. Or, $\neg x \xrightarrow{\star} x$ et donc, d'après le lemme, $[\![x]\!]^\rho = \mathbf{V}$ d'où $\rho(x) = \mathbf{V}$, absurde.

Il n'existe donc pas un tel ρ.

" $\Longleftarrow$ " Si G_H est telle qu'aucune variable et sa négation soient dans la même CFC. Soit $x \in \mathbb{Q}$ une variable propositionnelle. Soit $C_1, \ldots, C_p$ les composantes fortement connexes du graphe, triées par ordre topologique *i.e.* pour $(i,j) \in [\![1,p]\!]^2$, si $j > i$, alors il n'y a pas de chemin d'un élément de C_j vers un élément de C_i. Regardons alors où sont rangés x et $\neg x$. Si $x \in C_i$ et $\neg x \in C_j$ avec $i < j$, on définit alors $\rho(x) = \mathbf{F}$. Sinon, on définit $\rho(x) = \mathbf{V}$. Montrons alors que ρ est un modèle de H : $[\![H]\!]^\rho = \mathbf{V}$. Par l'absurde, soit $\ell_{i,1} \vee \ell_{i,2}$ une 2-clause de H telle que $[\![\ell_{i,1} \vee \ell_{i,2}]\!]^\rho = \mathbf{F}$, donc $[\![\ell_{i,1}]\!]^\rho = \mathbf{F}$ et $[\![\ell_{i,2}]\!]^\rho = \mathbf{F}$. Alors, $(\ell^{\mathrm{c}}_{i,2}, \ell_{i,1})$ est une arrête de G_H et, $(\ell^{\mathrm{c}}_{i,1}, \ell_{i,2})$ est une arrête de G_H. Ainsi, en notant a l'indice de la composante $\ell^{\mathrm{c}}_{i,2}$, b l'indice de $\ell_{i,1}$, c l'indice de $\ell^{\mathrm{c}}_{i,1}$ et d l'indice de $\ell_{i,2}$, on a $a \leqslant b$, $b < c$ par définition de ρ, $c \leqslant d$ et $d < a$ par définition de ρ, d'où

$$a \leqslant b < c \leqslant d < a,$$

ce qui est absurde. On a donc pour toute 2-clause $\ell_{i,1} \vee \ell_{i,2}$ de H, $[\![\ell_{i,1} \vee \ell_{i,2}]\!]^\rho = \mathbf{V}$ et donc $[\![H]\!]^\rho = \mathbf{V}$.

□

Algorithme 5.3 Solution au problème 2CNFSAT

Entrée H une 2-CNF
Sortie ρ un modèle de H ou None si H n'est pas satisfiable

1 : On construit G_H
2 : On construit les CFC $C_1, \ldots, C_p$ de G_H (dans un ordre topologique)
3 : **si** il existe x et $i \in [\![1,p]\!]$ tel que $x \in C_i$ et $\neg x \in C_i$ **alors**
4 : | **retourner** None
5 : **sinon**
6 : | **retourner** ρ défini comme

$$\rho : \mathbb{Q} \longrightarrow \mathbb{B}$$
$$x \longmapsto \begin{cases} \mathbf{F} & \text{si } i < j \\ \mathbf{V} & \text{sinon} \end{cases}$$

| où $x \in C_i$ et $\neg x \in C_j$.

□

IV.2 Arbres couvrants de poids minimum

Exemple :
On considère le graphe ci-dessous.

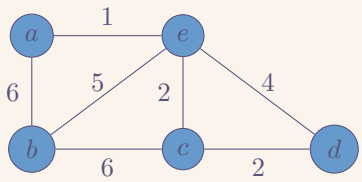


Figure 5.6 – Arbre pondéré

On cherche à « supprimer » des arrêtes de ce graphe afin d'avoir un poids total minimum, tout en conservant la connexité du graphe. Une structure assurant cette condition est un arbre.

Pour résoudre ce problème, on part du graphe vide, et on ajoute les arrêtes les moins coûteuses en premier.

Définition (Arbre) **:** Soit $G = (S, A)$ un graphe non-orienté. On dit que G est un *arbre* si G est connexe et acyclique.

Définition (Arbre couvrant) **:** Étant donné un graphe non orienté pondéré par poids positifs $G = (S, A, c)$, [1] on dit de $G' = (S', A')$ que c'est un *arbre couvrant* de G si $S' = S$ et $A' \subseteq A$, et G' est un arbre.

Définition (Arbre couvrant de poids minimum) **:** Étant donné un graphe non orienté pondéré $G = (S, A, c)$ et un arbre couvrant $T = (S', A')$, on appelle *poids* de l'arbre T la valeur $\sum_{a \in A'} c(a)$.

Si G est connexe, il admet au moins un arbre couvrant, on peut définir l'*arbre couvrant de poids minimum* (ACPM).

On définir alors le problème

ACPM [2] $\begin{cases} \textbf{Entrée} & : G = (S, A, c) \text{ connexe} \\ \textbf{Sortie} & : \text{ le poids de l'arbre couvrant de poids minimum.} \end{cases}$

1. on dit que c est la fonction de pondération de ce graphe
2. Arbre Couvrant de Poids Minimum

Algorithme 5.4 Algorithme de KRUSKAL

Entrée $G = (S, A, c)$ un graphe connexe
Sortie Un arbre couvrant de poids minimum

$B \leftarrow$
$U \leftarrow$
tant que il existe u et v tels que $u \not\sim_B v$ **faire**
  Soit $\{x, y\} \in A \setminus U$ de poids minimal
  si $x \sim_B y$ **alors**
    $U \leftarrow \{\{x, y\}\} \cup U$
  sinon
    $U \leftarrow \{\{x, y\}\} \cup U$
    $B \leftarrow \{\{x, y\}\} \cup B$
retourner $T = (S, B)$

Proposition : L'algorithme de KRUSKAL est correct.

Preuve : 1. Il existe un arbre couvrant de poids minimum utilisant les arrêtes de B ;
2. $B \subseteq U \subseteq A$;
3. $\forall \{u, v\} \in U$, $u \sim_B v$.

Ces trois propriétés sont invariantes.

Initialement $B = \ = U$, donc OK.

Propagation Soient $\underline{B}$ et $\underline{U}$ (resp. $\bar{B}, \bar{U}$) les valeurs de B et U avant (resp. après) une itération de boucle. Supposons que $\underline{B}$ et $\underline{U}$ satisfont les propriétés 1, 2 et 3. Montrons que $\bar{B}$ et $\bar{U}$ les satisfont aussi.

2. On a $\{x, y\} \in A$ et $\underline{B} \subseteq \underline{U} \subseteq A$, donc
$$\bar{B} \subseteq \underline{B} \cup \{\{x, y\}\} \subseteq \underline{U} \cup \{\{x, y\}\} \subseteq A.$$
3. Soit $\{u, v\} \in \bar{U}$.
   — Si $\{u, v\} \in \underline{U}$, alors de 3, $u \sim_{\underline{B}} v$. Or, $\underline{B} \subseteq \bar{B}$ et donc $u \sim_{\bar{B}} v$.
   — Sinon, $\{u, v\} = \{x, y\}$, alors $x = u$ et $v = y$.
      — Sous-cas 1 : $\bar{B} = \underline{B} \cup \{\{x, y\}\}$, alors $x \sim_{\bar{B}} y$.
      — Sous-cas 2 : $\bar{B} = \underline{B}$, alors par condition du **si**, $x \sim_{\underline{B}} y$ et donc $x \sim_{\bar{B}} y$.
1. Soit $\mathcal{T}$ un ACPM contenant $\underline{B}$.
   — Cas 1 : $\bar{B} = \underline{B}$, OK
   — Cas 2 : $\bar{B} = \underline{B} \cup \{\{x, y\}\}$.
      — Sous-cas 1 : $\{x, y\} \in \mathcal{T}$, alors $\mathcal{T}$ est un ACPM qui contient $\bar{B}$.

— Sous-cas 2 : $\{x,y\} \notin \mathcal{T}$, $\mathcal{T}$ est un arbre couvrant, donc il contient une chaîne de x à y :

$$\{\overset{x}{\overset{\|}{x_0}}, x_1\}, \{x_1, x_2\}, \ldots, \{x_{n-1}, \underset{\|}{x_n}\}.$$
$$y$$

Or, $\forall i \in [\![1, n-1]\!]$, $x_i \sim_{\underline{B}} x_{i+1}$. Par transitivité, on a donc $x = x_0 \sim_{\underline{B}} x_n = y$, ce qui n'est pas le cas. Il existe donc $i_0 \in [\![0, n-1]\!]$, tel que $x_{i_0} \nsim_{\underline{B}} x_{i_0+1}$ et donc $\{x_{i_0}, x_{i_0+1}\} \notin \underline{U}$. D'où, d'après 3, on a $\{x_{i_0}, x_{i_0+1}\} \notin \underline{B}$ Considérons alors $\mathcal{T}' = \big(\mathcal{T} \setminus \{\{x_{i_0}, x_{i_0+1}\}\}\big) \cup \{\{x, y\}\}$. Montrons que $\mathcal{T}'$ est un ACPM contenant B, en commençant par montrer que c'est un arbre couvrant. L'arbre $\mathcal{T}'$ a $n-1$ arrêtes (autant que $\mathcal{T}$). Montrons que $\mathcal{T}'$ est connexe. Soit $(a,b) \in S^2$. $\mathcal{T}$ est connexe, soit donc une chaîne

$$C : \quad a = u_0, u_1, \ldots, u_n = b$$

de $\mathcal{T}$. Si la chaîne C n'utilise pas l'arrête $\{x_{i_0}, x_{i_0+1}\}$, alors C est une chaîne de $\mathcal{T}'$. Sinon, on pose μ et τ tels que

$$\underbrace{a, \ldots, x_{i_0}}_{\mu}, \underbrace{x_{i_0+1}, \ldots, b}_{\tau}.$$

Soit alors la chaîne

$$\overbrace{a, \ldots, x_{i_0}}^{\mu}, x_{i_0-1}, x_{i_0-2}, \ldots, x_0 = x,$$
$$\underbrace{b, \ldots, x_{i_0+1}}_{\tau}, x_{i_0+2}, \ldots, x_{n-1}, x_n = y$$

qui est dans $\mathcal{T}'$. Montrons que le poids est minimum. Notons $P(\mathcal{T})$ le poids de l'arbre. On a donc

$$P(\mathcal{T}') = P(\mathcal{T}) + c(\{x,y\}) - c(\{x_{i_0}, x_{i_0+1}\}).$$

Par choix glouton, $(\{x_{i_0}, x_{i_0+1} \notin \underline{U}\})$, $c(\{x,y\}) \leqslant c(\{x_{i_0}, x_{i_0+1}\})$ donc $P(\mathcal{T}') \leqslant P(\mathcal{T})$, et $\mathcal{T}$ étant de poids min, $P(\mathcal{T}') = P(\mathcal{T})$ et $\mathcal{T}'$ est un ACPM contenant $\bar{B}$.

Les invariants le sont. □

À la fin, B induit un graphe connexe et B est contenu dans un ACPM, c'en est donc un.

Une structure pour la gestion des partitions : UnionFind.

Définition (Type de données abstrait UnionFind) **:** On définit le type de données abstrait UnionFind comme contenant

- un type `t` de partitions ;
- un type `elem` des éléments manipulés par les partitions ;
- `initialise_partition` : `elem list` $\to$ `t` retournant le partitionnement dans lequel chaque élément est seul dans sa classe ;
- `find` : (`t * elem`) $\to$ `elem` retournant un représentant de la classe de l'élément. Si deux éléments x et y sont dans la même classe, dans le partitionnement p, alors $\texttt{find}(p, x) = \texttt{find}(p, y)$;
- `union` : (`t*elem*elem`) $\to$ `t` retourne le partitionnement dans lequel on a fusionné les classes des arguments.

Exemple :
On réalise le *pseudo-code* ci-dessous.

- $p \leftarrow \texttt{initialise\_partition}([1, 2, 3, 4, 5]) \rightsquigarrow \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$
- $\texttt{find}(p, 1) = 1$
- $\texttt{union}(p, 1, 3) \rightsquigarrow \{\{1, 3\}, \{2\}, \{4\}, \{5\}\}$
- $\texttt{find}(p, 1) = \texttt{find}(p, 3)$

On implémente ce type abstrait en OCaml.

Remarque (Niveau zéro – listes de liste) :

```
type 'a t = 'a list list

let initialise_partition (l: 'a list): 'a t =
  List.map (fun x -> [ x ] ) l

let rec find (p: 'a t) (x: 'a): 'a =
  match p with
  | classe :: classes ->
      if List.mem x classe then List.hd classe
      else find classes x
  | [] -> raise Not_Found

let est_equiv (p: 'a t) (x: 'a) (y: 'a): bool =
  (find p x) = (find p y)

let rec extrait_liste (x: 'a) (p: 'a t): 'a list * 'a
    ↪ p =
  match p with
  | classe :: classes ->
      if List.mem x classe then (classe, classes)
      else
        let cl, cls' = extrait_liste x classes in
        (cl, classe :: cls')
  | [] -> raise Not_Found

let union (p: 'a t) (x: 'a) (y: 'a): 'a t =
  if est_equiv p x y then p
  else
    let cx, p' = extrait_liste x p in
    let cy, p'' = extrait_liste y p' in
    (cx @ cy) :: p''
```

Code 5.1 – Implémentation du type UnionFind en OCaml

Remarque (Niveau un – tableau de classes) :
Dans la case du tableau, on inscrit le numéro de sa classe. Pour `find`, on prend le premier ayant la même classe. Pour `union`, on re-numérote vers un numéro commun. Par exemple,

0	1	0	0	1	2
0	1	2	3	4	5

$\longleftrightarrow \qquad \{\{0,2,3\},\{1,4\},\{5\}\}.$

Remarque (Niveau deux – tableau de représentants) :
Dans les cases du tableau, on écrit le représentant de la classe de i. Pour `find`, on lit la case. Pour `union`, on re-numérote vers un numéro commun. Par exemple,

2	4	2	2	4	5
0	1	2	3	4	5

$\longleftrightarrow \qquad \{\{0,2,3\},\{1,4\},\{5\}\}.$

Remarque (Niveau trois – arbres) :
Pour `union`$(0,1)$, on cherche le représentant de 0 (2) puis celui de 1 (4). On fait pointer 4 vers 2. Pour la suite de l'implémentation, *c.f.* DM$_3$.

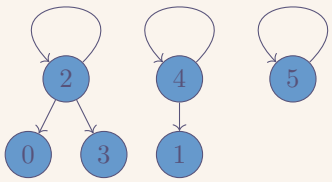


Figure 5.7 – Représentation par des arbres

Avec cette nouvelle structure, on peut maintenant revenir sur l'algorithme de Kruskal.

Algorithme 5.5 Algorithme de Kruskal – version 2

Entrée Un graphe $G = (S, A, c)$ un graphe non orienté, pondéré
Sortie Un acpm

```
Soit (e_i)_{i∈⟦1,m⟧} un tri des arrêtes par coût croissant
f ← 0          ▷ Nombre d'union effectuées
p ← initialise_partition(S)
I ← 0
B ←
tant que f < n − 1 faire
    {x, y} ← e_I
    si find(p, x) ≠ find(p, y) alors
        p ← union(p, x, y)
        B ← B ∪ {{x, y}}
        f ← f + 1
    I ← I + 1
retourner (S, B)
```

Étude de complexité. Notons $C^n_{\texttt{find}}$ un majorant du coût de `find` sur une structure contenant n éléments, notons $C^n_{\texttt{union}}$ un majorant du coût de `union` sur une structure contenant n éléments, et notons $C^n_{\texttt{init}}$ un majorant du coût de `init` sur une structure contenant n éléments. La complexité de cet algorithme est de

$$\mathcal{O}\big(C^n_{\texttt{init}} + 2m\, C^n_{\texttt{find}} + n\, C^n_{\texttt{union}} + m \log_2 m\big).$$

IV.3 Couplage dans un graphe biparti

Définition (Couplage) **:** On appelle *couplage* d'un graphe non orienté $G = (S, A)$, la donnée d'un sous-ensemble $C \subseteq A$ tel que

$$\forall \{x, y\}, \{x', y'\} \in C, \qquad \{x, y\} \cap \{x', y'\} \neq \varnothing \implies \{x, y\} = \{x', y'\}.$$

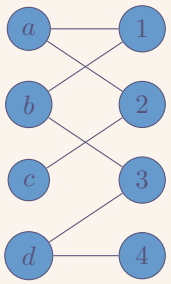


FIGURE 5.8 – Exemple de couplage

EXEMPLE :
On réutilise l'exemple ci-dessous dans toute la section. L'ensemble $C = \{\{a, 2\}, \{b, 3\}\}$ est un couplage. Mais, l'ensemble $C' = \{\{a, 1\}, \{a, 2\}\}$ n'en est pas un.

Définition : Un couplage est dit *maximal* s'il est maximal pour l'inclusion ($\subseteq$). Un couplage est dit *maximum* si son cardinal est maximal.

EXEMPLE :
Dans l'exemple précédent,

- le couplage $C = \{\{a, 2\}, \{b, 3\}\}$ n'est ni maximal, ni maximum ;
- le couplage $C' = \{\{a, 2\}, \{b, 3\}, \{d, 4\}\}$ est maximal mais pas maximum ;
- le couplage $C'' = \{\{a, 1\}, \{b, 3\}, \{c, 2\}, \{d, 4\}\}$ est maximum.

REMARQUE :
Dans toute la suite, on ne considère que des graphes bipartis.

Définition : Étant donné un graphe biparti $G = (S, A)$ et un couplage C, un sommet x est dit *libre* dès lors que

$$\forall \{y, z\} \in C,\ x \notin \{y, z\}.$$

Une chaîne élémentaire [3] $(c_0, c_1, \ldots, c_{2p+1})$ est dit *augmentante* si

- c_0 et c_{2n+1} sont libres ;
- $\forall i \in [\![0, p]\!]$, $\{c_{2i}, c_{2i+1}\} \in A \setminus C$;
- $\forall i \in [\![0, p-1]\!]$, $\{c_{2i+1}, c_{2i+2}\} \in C$.

Exemple :

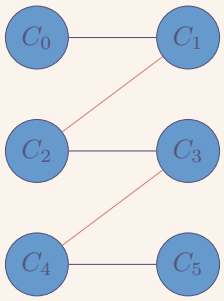


Figure 5.9 – Chaîne augmentante

Exemple :
Dans l'exemple de cette section, $(d, 4)$ et $(c, 2, a, 1)$ sont deux chaînes augmentantes.

Proposition : Étant donné un graphe biparti $G = (S, A)$ avec $S = S_1 \cup S_2$ (partitionnement du graphe biparti), un couplage C est maximum si, et seulement s'il n'admet pas de chaînes augmentantes.

Preuve " $\Longrightarrow$ " Soit C un couplage admettant une chaîne augmentante. Montrons que C n'est pas maximum. Soit la chaîne augmentante [4]

$$c_0 \to c_1 \Rightarrow c_2 \to c_3 \Rightarrow c_4 \to \cdots \to c_{2p-1} \Rightarrow c_{2p} \to c_{2p+1}.$$

On considère alors le couplage

$$C' = \Big(C \setminus \big\{\{c_{2i+1}, c_{2i+2}\} \mid i \in [\![0, p-1]\!]\big\}\Big) \cup \big\{\{c_{2i}, c_{2i+1}\} \mid i \in [\![0, p]\!]\big\}.$$

3. *i.e.* une chaîne sans boucles.

On transforme donc la chaîne en

$$c_0 \Rightarrow c_1 \to c_2 \Rightarrow c_3 \to \cdots \to c_{2p-1} \to c_{2p} \Rightarrow c_{2p+1}.$$

C'est bien un couplage, et $\mathrm{Card}(C') = \mathrm{Card}\, C + 1$. C n'est donc pas un couplage maximum.

" $\Longleftarrow$ " Soit C un couplage non maximum. Montrons que C admet une chaîne augmentante. Soit M un couplage maximum, et $D = C \triangle M = (C \setminus M) \cup (M \setminus C)$. On a $\mathrm{Card}\, C < \mathrm{Card}\, M$ et $\mathrm{Card}(C \setminus M) < \mathrm{Card}(M \setminus C)$. On remarque que, si $c_0 \to c_1 \to c_2 \to \cdots \to c_{p-1} \to c_p$ est une chaîne de D, (si $c_0 \to c_1 \in C \setminus M$ et $c_1 \to c_2 \in C \setminus M$ donc c_1 est dans deux arrêtes distinctes d'un couplage C, ce qui est absurde ; de même pour les autres arrêtes). Ainsi, 2 arrêtes consécutives ne sont pas dans la même composante de l'union $(C \setminus M) \cup (M \setminus C)$. Considérons la relation d'équivalence $\sim$ sur D définie par $\{x, y\} \sim \{z, t\} \overset{\text{def.}}{\Longleftrightarrow}$ il existe une chaîne de D utilisant l'arrête $\{x, y\}$ et l'arrête $\{z, t\}$. Soit le partitionnement $D_1, \ldots, D_q$ de D par $\sim$. Par inégalité de cardinal, il existe un D_i tel que

$$\mathrm{Card}\{e \in D_i \mid e \in C\} < \mathrm{Card}\{e \in D_i \mid e \in M\}.$$

L'ensemble D_i contient alors une chaîne augmentante.

□

Algorithme 5.6 ChaîneAugmentante : Trouver une chaîne augmentante dans un graphe biparti $G = (S, A)$ muni d'un couplage C partant d'un sommet $s \in S$

```
1 : Procédure Augmente(x, chaîne)
2 :     pour y ∈ Succ(x) \ chaîne faire
3 :         si y est libre dans C alors
4 :             retourner Some(chaîne ⊎ (y))
5 :         sinon
6 :             Soit z tel que {y, z} ∈ C.
7 :             r ← Augmente(z, chaîne ⊎ (y, z))
8 :             si r ≠ None alors
9 :                 retourner r
10 :            retourner None
11 : si s est libre dans C alors
12 :     retourner Augmente(s, (s))
13 : sinon
14 :     retourner None
```

Remarque :
Si un sommet n'est pas libre dans le couplage C, il n'est pas libre dans les couplage obtenus par inversion de chaîne depuis C.

4. On représente $\Rightarrow$ pour les arrêtes dans le couplage C.

Algorithme 5.7 Calcul d'un couplage maximum

Entrée $G = (S, A)$ un graphe biparti, avec $S = S_1 \uplus S_2$

```
1 : C ←
2 : Done ←
3 : tant que ∃x ∈ S_1 \ Done faire
4 :     Soit un tel x.
5 :     r ← ChaîneAugmentante(G, C, x)
6 :     si r ≠ None alors
7 :         Some(a) ← r
8 :         On inverse la chaîne a dans C.
9 :     Done ← {x} ∪ Done
10 : retourner C
```

Annexe 5.A Remarques supplémentaires

Le parcours d'un graphe $G = (S, A)$ a une complexité en $\mathcal{O}(|S| + |A|)$.

Chapitre 6

Preuves

L'objectif de ce chapitre, sera de "critiquer" le travail en logique fait précédement, puis d'apporter une solution à ce problème ; on finira par un peu de Hors-Programme.

IV.0 Motivation

IV.0.1 Tables de vérité

Pour l'instant, pour montrer $\Gamma \models G$ ou $G \equiv H$, nous devons encore utiliser une table de vérité. Par exemple, montrons

$$\underbrace{(p \to q) \wedge (q \to r)}_{G} \models \overbrace{p \to r}^{H}.$$

On réalise la table de vérité ci-dessous.

p	q	r	$p \to q$	$q \to r$	G	H	
F	**F**	**F**	**V**	**V**	**V**	**V**	✓
F	**F**	**V**	**V**	**V**	**V**	**V**	✓
F	**V**	**F**	**V**	**F**	**F**	**V**	✓

À faire : Finir table de vérité

Table 6.1 – Table de vérité pour montrer $(p \to q) \wedge (q \to r) \models p \to r$

IV.0.2 Équations

Supposons $[\![G]\!]^\rho = \mathbf{V}$. Montrons que $[\![H]\!]^\rho = \mathbf{V}$. On a

$$\begin{aligned}\mathbf{V} &= [\![G]\!]^\rho \\ &= [\![(p \to q) \wedge (q \to r)]\!]^\rho \\ &\vdots \\ &= \overline{[\![p]\!]^\rho} \cdot \overline{[\![q]\!]^\rho} + \overline{[\![p]\!]^\rho} \cdot \overline{[\![q]\!]^\rho} \cdot [\![r]\!]^\rho + [\![q]\!]^\rho \cdot [\![r]\!]^\rho\end{aligned}$$

et

$$\begin{aligned}[\![H]\!]^\rho &= [\![p \to r]\!]^\rho \\ &\vdots \\ &= \overline{[\![p]\!]^\rho} \cdot \overline{[\![q]\!]^\rho} + \overline{[\![p]\!]^\rho} \cdot \overline{[\![q]\!]^\rho} \\ &\quad + [\![r]\!]^\rho \cdot \overline{[\![q]\!]^\rho} \cdot \left([\![p]\!]^\rho + \overline{[\![p]\!]^\rho}\right) \\ &\quad + [\![r]\!]^\rho + ?\end{aligned}$$

À faire : finir le calcul

IV.0.3 Raisonnement mathématiques

Supposons $(p \to q) \wedge (q \to r)$. Montrons que $p \to r$.

↪ Supposons donc p. Montrons r
  ↪ Montrons q.
    ↪ Montrons p, qui est une hypothèse.
    ↪ Montrons $p \to q$, qui est aussi une hypothèse.
  — Montrons $q \to r$, ce qui est vrai par hypothèse.

On reconnaît un arbre.

IV.1 La déduction naturelle en logique propositionnelle

IV.1.1 Séquents

Objectifs de preuves.

Exemple :
Montrons $P \wedge Q$ est vrai.
↪ Montrons P.
↪ Montrons Q.

Hypothèses courantes.

Exemple :
Montrons que $(n \in 4\mathbb{N} \to n \in 2\mathbb{N}) \wedge (n \in 4\mathbb{N}+3 \to n \in 2\mathbb{N}+1)$.

$\hookrightarrow$ Montrons $n \in 4\mathbb{N} \to 2\mathbb{N}$.

$\hookrightarrow$ Supposons $n \in 4\mathbb{N}$. Montrons $n \in 2\mathbb{N}$.
(local)

$\hookrightarrow$ Montrons $n \in 4\mathbb{N}+3 \to n \in 2\mathbb{N}+1$.

$\hookrightarrow$ Supposons $n \in 4\mathbb{N}+3$. Montrons $n \in 2\mathbb{N}+1$.

Définition (Séquent) **:** Un *séquent* est la donnée
— d'un ensemble d'hypothèses Γ ;
— d'un objectif G.
On le typographie $\Gamma \vdash G$.

Exemple :
Montrons $\vdash (n \in 4\mathbb{N} \to n \in 2\mathbb{N}) \wedge (n \in 4\mathbb{N}+3 \to n \in 2\mathbb{N}+1)$

$\hookrightarrow$ $\vdash (n \in 4\mathbb{N} \to n \in 2\mathbb{N})$

$\hookrightarrow$ $\{n \in 4\mathbb{N}\} \vdash n \in 2\mathbb{N}$

$\hookrightarrow$ $\vdash (n \in 4\mathbb{N}+3 \to n \in 2\mathbb{N}+1)$

$\hookrightarrow$ $\{n \in 4\mathbb{N}+3\} \to n \in 2\mathbb{N}+1$

On typographie cette preuve sous forme d'un arbre.ăÀ faire : Arbre à faire

IV.1.2 Preuves

Définition : On appelle *règle de construction de preuves* une règle de la forme :

$$\frac{\Gamma_1 \vdash \varphi_1 \quad \Gamma_2 \vdash \varphi_2 \quad \Gamma_3 \vdash \varphi_3 \quad \cdots \quad \Gamma_n \vdash \varphi_n}{\Gamma \vdash \varphi}\ \text{nom.}$$

On appelle $\Gamma_1 \vdash \varphi_1$, $\Gamma_2 \vdash \varphi_2$, $\Gamma_3 \vdash \varphi_3$, …, $\Gamma_n \vdash \varphi_n$ les *prémisses*, et $\Gamma \vdash \varphi$ la *conclusion*.

Si $n = 0$, on dit que c'est une *règle de base*.

Remarque (Notation) :
Γ est un ensemble. Alors, l'ensemble $\Gamma \cup \{\psi\}$ est noté Γ, ψ.

Exemple :
Un *axiome* est de la forme

$$\frac{}{\Gamma, \varphi \vdash \varphi}\ \text{Ax}.$$

Une preuve de la forme, appelée *introduction du* ET,

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi} \wedge\text{i}$$

permet de prouver un ET. Il correspond au raisonnement mathématique suivant : supposons Γ ; montrons $\varphi \wedge \psi$;

- $\hookrightarrow$ montrons φ ;
- $\hookrightarrow$ montrons ψ.

Définition (Arbre de preuve) **:** On appelle *arbre de preuve* un arbre étiqueté par des séquents, et dont les liens père–fils sont des liens autorisés par les règles du système de preuves. Un *système de preuves* étant un ensemble de règles.

EXEMPLE (Système Jouet) :

$$\frac{}{\Gamma, \varphi \vdash \varphi}\ \text{Ax} \qquad \frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ \wedge\text{i} \qquad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ \vee\text{i,g} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ \vee\text{i,d}.$$

EXEMPLE :
Avec le système précédent,

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{P,Q,R\} \vdash P}\ \text{Ax}}{\{P,Q,R\} \vdash P \vee Q}\ \vee\text{i,g} \qquad \dfrac{\dfrac{}{\{P,Q,R\} \vdash Q}\ \text{Ax}}{\{P,Q,R\} \vdash Q \vee \neg R}\ \vee\text{i,g}}{\{P,Q,R\} \vdash (P \vee Q) \wedge (Q \vee \neg R)}\ \wedge\text{i}}{\{P,Q,R\} \vdash (P \wedge X) \vee \big((P \vee Q) \wedge (Q \vee \neg R)\big)}\ \vee\text{i,d} \quad .$$

Définition (Être prouvable) **:** On dit d'un séquent $\Gamma \vdash G$ qu'il est *prouvable* dans un système de preuve dès lors qu'il existe une preuve dont la racine est étiquetée par $\Gamma \vdash G$.

RAPPEL (objectifs) :
On veut trouver d'autres moyens de montrer $F \models G$. On veut que, si $F \vdash G$, alors $F \models G$ (correction). Mais, on veut aussi que, si $F \models G$, alors $G \vdash F$ (complétude). On veut aussi qu'il existe un algorithme qui vérifie $F \models G$ (décidabilité).

Définition (Correction) **:** On dit d'un système de preuve qu'il est *correct* dès lors que : pour tout Γ, pour tout G, si $\Gamma \vdash G$ admet une preuve, alors $\Gamma \models G$.

Exemple : 1. On pose la règle “Menteur” définie comme

$$\frac{}{\Gamma \vdash \bot}\ \text{Menteur}.$$

Ce système de preuve n'est pas correct car $\{\top\} \not\models \bot$. Or,

$$\frac{}{\{\top\} \vdash \bot}\ \text{Menteur}.$$

2. Le système jouet est correct. Montrons cela par induction sur la preuve de $\Gamma \vdash G$.
   - Si la preuve de $\Gamma \vdash G$ est de la forme

$$\frac{}{\Gamma', G \vdash G}\ \text{Ax}.$$

     Montrons que $\Gamma' \cup \{G\} \models \{G\}$. Soit donc ρ un modèle de $\Gamma \cup \{G\}$. Alors $\forall \varphi \in \Gamma \cup \{G\}$, $[\![\varphi]\!]^\rho = \mathbf{V}$. Montrons que ρ est un modèle de G. On pose $\varphi = G$; on a donc $[\![G]\!]^\rho = \mathbf{V}$.
   - Si la preuve de $\Gamma \vdash G$ est de la forme

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ \wedge\text{i}.$$

     On appelle π_1 la branche gauche de l'arbre, et π_2 la branche de droite. Par hypothèse d'induction sur π_1, $\Gamma \vdash \varphi$ admet une preuve (qui est une sous-preuve), donc $\Gamma \models \varphi$. De même, $\Gamma \models \psi$ avec la branche π_2. On en déduit que $\Gamma \models \varphi \wedge \psi$ d'après les résultats du chapitre 0.
   - De même pour les autres cas.

Définition (Complétude) **:** Un système de preuves est *complet* dès lors que, si $\Gamma \models G$, alors il existe un preuve de $\Gamma \vdash G$.

Exemple :
Le système de preuve ayant pour règle, pour tout Γ, et tout G,

$$\frac{}{\Gamma \vdash G}\ \text{OP}$$

est complet mais pas correct.

Exemple :
Le système de preuve ayant pour règle, pour tout Γ, et tout G tel que $\Gamma \models G$,

$$\frac{}{\Gamma \vdash G}$$

est complet et correct.

IV.1.3 Déduction naturelle

On définit les différentes règles d'introduction et d'élimination suivantes.

Symbole	Règle d'introduction	Règle d'élimination
$\top$	$\dfrac{}{\Gamma \vdash \top}\ \top\text{i}$	
$\bot$		$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash G}\ \bot\text{e}$
$\neg$	$\dfrac{\Gamma, G \vdash \bot}{\Gamma \vdash \neg G}\ \neg\text{i}$	$\dfrac{\Gamma \vdash G \quad \Gamma \vdash \neg G}{\Gamma \vdash \bot}\ \neg\text{e}$
$\to$	$\dfrac{\Gamma, G \vdash H}{\Gamma \vdash G \to H}\ \to\text{i}$	$\dfrac{\Gamma \vdash H \to G \quad \Gamma \vdash H}{\Gamma \vdash G}\ \to\text{e}$
$\wedge$	$\dfrac{\Gamma \vdash G \quad \Gamma \vdash H}{\Gamma \vdash G \wedge H}\ \wedge\text{i}$	$\dfrac{\Gamma \vdash G \wedge H}{\Gamma \vdash G}\ \wedge\text{e,g} \qquad \dfrac{\Gamma \vdash G \wedge H}{\Gamma \vdash H}\ \wedge\text{e,d}$
$\vee$	$\dfrac{\Gamma \vdash G}{\Gamma \vdash G \vee H}\ \vee\text{i,g} \qquad \dfrac{\Gamma \vdash H}{\Gamma \vdash G \vee H}\ \vee\text{i,d}$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash G \quad \Gamma, B \vdash G}{\Gamma \vdash G}\ \vee\text{e}$
	$\dfrac{}{\Gamma, \varphi \vdash \varphi}\ \text{Ax}$	

Table 6.2 – Règles d'introduction et d'élimination

À ce stade, nous avons définis le système de preuves que l'on appellera *déduction naturelle intuitionniste*. Dans le chapitre 0, on a donné une notion de vérité. On a maintenant donné une notion de preuve. On souhaite maintenant montrer le séquent $\vdash p \vee \neg p$, nommé *tiers exclu* : la variable p est, soit vrai, soit fausse. Avec le système de preuve actuel, on ne peut pas le montrer. Mais, on a bien $\models p \vee \neg p$, car pour tout environment propositionnel ρ, $[\![p \vee \neg p]\!]^\rho = \mathbf{V}$. D'où la remarque suivante.

Remarque :
Ce système de preuve n'est pas complet vis à vis de la sémantique de la logique propositionnelle : on ne peut pas prouver le séquent $\vdash p \vee \neg p$ malgré son caractère tautologique.

Exemple :
De plus, montrons le résultat : il existe deux irrationnels x et y tels que x^y soit rationnel. On considère le réel $\sqrt{2}^{\sqrt{2}}$. S'il est rationnel, la preuve est terminée. S'il ne l'est pas, notons $x = \sqrt{2}^{\sqrt{2}}$, et on remarque que $x^{\sqrt{2}} = 2$. Dans cette preuve, on utilise le tiers exclu : x est soit rationnel, soit irrationnel.

Ainsi, la *déduction naturelle classique* est le système de preuve obtenue en ajoutant la règle suivante :

$$\frac{}{\Gamma \vdash G \vee \neg G}\ \text{TE}.$$

La déduction naturelle classique est un système de preuve complet.

Exemple (preuve en déduction naturelle classique) :
Montrons le séquent $\vdash \neg\neg p \to p$. Une preuve de ce séquent n'était pas possible

en déduction naturelle intuitionniste, mais elle est possible en déduction naturelle classique à l'aide de la règle du tiers exclu TE.

$$\dfrac{\dfrac{}{\neg p \vee \neg\neg p}\ \text{TE} \qquad \dfrac{\dfrac{\dfrac{}{\neg\neg p, \neg p \vdash \neg p}\ \text{Ax} \qquad \dfrac{}{\neg\neg p, \neg p \vdash p}\ \text{Ax}}{\neg\neg p, \neg p \vdash \bot}\ \neg\text{e}}{\neg\neg p, \neg p \vdash p}\ \bot\text{e} \qquad \dfrac{}{\neg\neg p, p \vdash p}\ \text{Ax}}{\neg\neg p \vdash p}\ \vee\text{e}}{\vdash \neg\neg p \to p}\ \to\text{i}$$

Exemple (preuve en dédution naturelle intuitionniste) :
On montre maintenant l'implication inverse. S'il existe une preuve en déduction naturelle intuitionniste, elle reste valide dans le système de preuve de la déduction naturelle classique.

$$\dfrac{\dfrac{\dfrac{}{p, \neg p \vdash p}\ \text{Ax} \qquad \dfrac{}{p, \neg p \vdash \neg p}\ \text{Ax}}{p, \neg p \vdash \bot}\ \neg\text{e}}{p \vdash \neg\neg p}\ \neg\text{i}}{\vdash p \to (\neg\neg p)}\ \to\text{i}$$

Exemple :
On prouve le séquent introductif $\vdash \big((p \to q) \wedge (q \to r)\big) \to (p \to r)$, à l'aide le la déduction naturelle intuitionniste. On nomme Γ l'ensemble $p, (p \to q) \wedge (q \to r)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash (p \to q) \wedge (q \to r)}\ \text{Ax}}{\Gamma \vdash q \to r}\ \wedge\text{e,d} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash (p \to q) \wedge (q \to r)}\ \text{Ax}}{\Gamma \vdash p \to q}\ \wedge\text{e,g} \qquad \dfrac{}{\Gamma \vdash p}\ \text{Ax}}{\Gamma \vdash q}\ \to\text{e}}{p, (p \to q) \wedge (q \to r) \vdash r}\ \to\text{e}}{(p \to q) \wedge (q \to r) \vdash p \to r}\ \to\text{i}}{\vdash \big((p \to q) \wedge (q \to r)\big) \to (p \to r)}\ \to\text{i}\ .$$

Exemple :
Toujours en déduction naturelle intuitionniste, on prouve le séquent

$$\vdash (p \to q) \to (\neg q \to \neg p).$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p, \neg q, p \to q \vdash \neg q}\ \text{Ax} \qquad \dfrac{\dfrac{}{p, \neg q, p \to q \vdash p \to q}\ \text{Ax} \qquad \dfrac{}{p, \neg q, p \to q \vdash p}\ \text{Ax}}{p, \neg q, p \to q \vdash q}\ \to\text{e}}{p, \neg q, p \to q \vdash \bot}\ \neg\text{e}}{\neg q, p \to q \vdash \neg p}\ \neg\text{i}}{p \to q \vdash \neg q \to \neg p}\ \to\text{i}}{\vdash (p \to q) \to (\neg q \to \neg p)}\ \to\text{i}\ .$$

Théorème : La déduction naturelle classique (respectivement intuitionniste) est correcte.

Preuve :
Par induction (longue) sur l'arbre de preuves (*c.f.* plus haut). □

Corollaire : Pour prouver $\Gamma \models G$, il suffit de construire un arbre de preuve de $\Gamma \vdash G$.

Remarque :
On aurait pu définir la déduction naturelle classique en ajoutant une des deux règles suivantes plutôt que le tiers exclus :

$$\frac{\Gamma \vdash \neg\neg G}{\Gamma \vdash G}\ \neg\neg\text{e} \qquad \frac{\Gamma, \neg G \vdash \bot}{\Gamma \vdash G}\ \text{Abs}^{1}.$$

Exercice :
Refaire les preuves du séquent $\vdash \neg\neg p \to p$ avec les règles $\neg\neg$e, et Abs.

IV.2 La logique du premier ordre

On veut rajouter à la déduction naturelle des quantificateurs, tels que $\forall$ ou $\exists$. On considère la formule

$$G = \forall x,\ \Big(\big((x > 0) \wedge (\exists y,\ x = y + 1)\big) \vee (x = 0)\Big).$$

Cette formule peut être représentée sous forme d'arbre syntaxique, comme celui ci-dessous.

1. Abs correspond à absurde

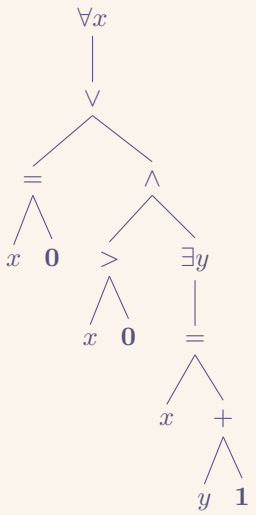


FIGURE 6.1 – Arbre syntaxique de la formule $G = \forall x, \Big(\big((x > 0) \wedge (\exists y,\ x = y + 1)\big) \vee (x = 0)\Big)$

IV.2.1 Syntaxe de la logique du premier ordre

Définition : On appelle *signature du premier ordre* la donnée de deux ensembles $\mathcal{S}$ et $\mathcal{P}$.[2] Ces symboles viennent avec une notion d'arité

$$\mathfrak{a} : \mathcal{S} \cup \mathcal{P} \longrightarrow \mathbb{N}.$$

On appelle l'ensemble des *constantes* la sous-partie des éléments c de $\mathcal{S}$ telle que $\mathfrak{a}(c) = 0$. Les autres symboles, non constantes, sont appelés *fonctions*. On appelle $\mathcal{P}$ l'ensemble des prédicats. On a toujours $\mathcal{S} \cap \mathcal{P} = .$

Définition : Étant donné un ensemble $\mathcal{S}$ de symboles de fonctions et de constantes, et un ensemble $\mathcal{V}$ de variables, on définit inductivement l'ensemble des *termes* sur $\mathcal{S}$ et $\mathcal{V}$, typographié $\mathcal{T}(\mathcal{S}, \mathcal{V})$, par

— $\mathcal{V} \subseteq \mathcal{T}(\mathcal{S}, \mathcal{V})$;

— si $f \in \mathcal{S}$, et $t_1, t_2, \ldots, t_{\mathfrak{a}(f)} \in \big(\mathcal{T}(\mathcal{S}, \mathcal{V})\big)^{\mathfrak{a}(f)}$, alors $f\big(t_1, t_2, \ldots, f_{\mathfrak{a}(f)}\big) \in \mathcal{T}(\mathcal{S}, \mathcal{V})$.

EXEMPLE :
Si $\mathcal{S} = \{+, -, \mathbf{0}\}$, avec $\mathfrak{a}(+) = 2$, $\mathfrak{a}(-) = 1$[3] et $\mathfrak{a}(\mathbf{0}) = 0$; si $\mathcal{V} \supseteq \{x, y, z\}$, alors

— $+(x, y)$

— $-(x)$

2. $\mathcal{S}$ est l'ensemble des symboles utilisés pour construire des termes ; $\mathcal{P}$ est l'ensemble des symboles utilisés pour passer du monde des termes pour passer au monde des formules.

— $\mathbf{0}$
— $+\Big(x, -\big(+(z, \mathbf{0})\big)\Big)$
sont des termes.

Définition (Logique du premier ordre) **:** Étant donné une signature du premier ordre $(\mathcal{S}, \mathcal{P})$, et un ensemble $\mathcal{V}$ de variables, on définit l'ensemble des formules des *formules de la logique du premier ordre* typographié $\mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V})$, par induction

— si $P \in \mathcal{P}$, et $t_1, \ldots, t_{\mathfrak{a}(P)} \in \big(\mathcal{T}(\mathcal{S}, \mathcal{V})\big)^{\mathfrak{a}(P)}$, alors $P\big(t_1, \ldots, t_{\mathfrak{a}(P)}\big) \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V})$;
— $\bot, \top \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V})$;
— si $(G, H) \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V})^2$, alors

$$G \wedge H \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}), \quad \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}), \qquad \neg G \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}) ;$$
$$G \vee H \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}), \quad G \leftrightarrow H \in$$
$$G \to H \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}),$$

— Si $x \in \mathcal{V}$ et $G \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V})$, alors

$$(\forall x,\ G) \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}) \qquad (\exists x,\ G) \in \mathcal{F}(\mathcal{S}, \mathcal{P}, \mathcal{V}).$$

On note un symbole $+$ avec son arité $\mathfrak{a}(+) = 2$ comme $+(2)$.

Exemple :
En choisissant $\mathcal{P} = \{>(2), =(2)\}$, $\mathcal{S} = \{+(2), \mathbf{0}(0), \mathbf{1}(0)\}$ et $\mathcal{V} \supseteq \{x, y\}$, on peut alors construire la formule de l'exemple précédent :

$$G = \forall x,\ \Big(\big((x > 0) \wedge (\exists y,\ x = y + 1)\big) \vee (x = 0)\Big).$$

Codons le en OCaml, comme montré ci-dessous.

```
type symbole_arite = string * int

type signature = {
  symbole_terme: symbole_arite list;
  symbole_predicat: symbole_arite list
}

type var = string

type terme =
  | V of var
  | T of symbole_arite * (terme list)

(* Quelques exemples *)

let ex0 = T(("0", 0), []);
let ex1 = T(("1", 0), []);
```

3. il s'agit du '−' dans l'expression $-x$.

```
let ex2 =
  T(("+", 2), [
    V("x"),
    T(("-", 1), [
      T(("+", 2), [
        V("z"),
        T(("0", 0), [])
      ])
    ])
  ])

(* Definissons la logique du 1er ordre *)

type po_logique =
  | Pred    of symbole_arite * (terme list)
  | Top | Bottom
  | And     of po_logique * po_logique
  | Or      of po_logique * po_logique
  | Imp     of po_logique * po_logique
  | Equiv   of po_logique * po_logique
  | Not     of po_logique
  | Forall  of var * po_logique
  | Exists  of var * po_logique
```

CODE 6.1 – Définition des formules de premier ordre en OCAML

On définit, dans la suite de cette section, l'introduction et l'élimination de $\forall$ et $\exists$. Mais, nous devons réaliser des *substitutions*, et c'est ce que nous allons faire dans le reste de cette sous-section.

Définition : On définit vars inductivement sur $\mathcal{T}(\mathcal{S},\mathcal{V})$ par :

— si $x \in \mathcal{V}$, $\text{vars}(x) = \{x\}$;

— $\text{vars}\big(f(t_1,\dots,t_n)\big) = \bigcup_{i=1}^{n} \text{vars}(t_i)$.

Définition : On définit inductivement deux fonctions

$$\mathsf{FV} : \mathcal{F}(\mathcal{S},\mathcal{P},\mathcal{V}) \longrightarrow \wp(\mathcal{V})^{\,4} \qquad \mathsf{BV} : \mathcal{F}(\mathcal{S},\mathcal{P},\mathcal{V}) \longrightarrow \wp(\mathcal{V})^{\,5}$$

par

— $\mathsf{FV}(\top) =$,
— $\mathsf{FV}(\bot) =$,
— $\mathsf{FV}(G \odot H) = \mathsf{FV}(G) \cup \mathsf{FV}(H)$ avec $\odot \in \{\wedge, \vee, \to, \leftrightarrow\}$,
— $\mathsf{FV}\big(P(t_1,\dots,t_n)\big) = \bigcup_{i=1}^{n} \text{vars}(t_i)$,
— $\mathsf{FV}(\neg G) = \mathsf{FV}(G)$,
— $\mathsf{FV}(\forall x,\, G) = \mathsf{FV}(G) \setminus \{x\}$,
— $\mathsf{FV}(\exists x,\, G) = \mathsf{FV}(G) \setminus \{x\}$,

et

- $\mathsf{BV}(\top) = ,$
- $\mathsf{BV}(\bot) = ,$
- $\mathsf{BV}\big(P(t_1, \ldots, t_n)\big) = ,$
- $\mathsf{BV}(\neg G) = \mathsf{BV}(G),$
- $\mathsf{BV}(G \odot H) = \mathsf{BV}(G) \cup \mathsf{BV}(H)$ avec $\odot \in \{\wedge, \vee, \to, \leftrightarrow\},$
- $\mathsf{BV}(\forall x,\, G) = \mathsf{BV}(G) \cup \{x\},$
- $\mathsf{BV}(\exists x,\, G) = \mathsf{BV}(G) \cup \{x\},$

Exemple :
À faire : Inclure exemple. $\mathsf{BV}(F) = \{x, y\}$ et $\mathsf{FV}(F) = \{y, z\}$.

Définition (α-renommage) **:** On appelle *α-renommage* l'opération consistant à renommer les occurrences liées des variables dans une formule.

Exemple :
On considère la formule

$$\big(\forall x,\, P(X)\big) \wedge \big(\forall x,\, \forall y,\, Q(x, x{+}y)\big).$$

Elle a pour α-renommage les formules

- $\big(\forall x,\, P(x)\big) \wedge \big(\forall x,\, \forall y,\, Q(x, x{+}y)\big)$;
- $\big(\forall z,\, P(z)\big) \wedge \big(\forall x,\, \forall y,\, Q(x, x{+}y)\big)$;
- $\big(\forall z,\, P(z)\big) \wedge \big(\forall z,\, \forall y,\, Q(z, z{+}y)\big)$;
- $\big(\forall z,\, P(z)\big) \wedge \big(\forall x,\, \forall z,\, Q(x, x{+}z)\big)$;
- ~~$\big(\forall z,\, P(z)\big) \wedge \big(\forall y,\, \forall y,\, Q(y, y{+}y)\big)$~~.

IV.2.2 Substitution

Définition (Substitution) **:** Une *substitution* est une fonction de $\mathscr{V} \longrightarrow \mathscr{T}(\mathcal{S}, \mathscr{V})$ qui est l'identité partout, sauf sur un nombre fini de variables que l'on appelle *clé* de cette substitution.

Exemple :
On considère la substitution

$$\begin{aligned} \sigma : \mathscr{V} &\longrightarrow \mathscr{T}(\mathcal{S}, \mathscr{V}) \\ x &\longmapsto \begin{cases} y{+}y & \text{si } x = y \\ x & \text{sinon.} \end{cases} \end{aligned}$$

L'ensemble des clés de cette substitution sont $\{y\}$; en effet, $\sigma(y) = y{+}y$, et $\sigma(z) = z$.

Définition (Application d'une substitution à un terme) **:** Étant donné

5. FV : *free variable*, variable libre
5. BV : *bound variable*, variable liée

une substitution σ, on définit inductivement la fonction

$$\begin{aligned} \cdot[\sigma] : \mathcal{T}(\Sigma, \mathcal{V}) &\longrightarrow \mathcal{T}(\mathcal{S}, \mathcal{V}) \\ t &\longmapsto t[\sigma] \end{aligned}$$

par

— $x[\sigma] = \sigma(x)$ avec $x \in \mathcal{V}$;
— $\big(f(t_1, \ldots, t_n)\big)[\sigma] = f\big(t_1[\sigma], \ldots, t_n[\sigma]\big)$.

Définition (Application d'une substitution à une formule) **:** Étant donné une substitution σ, on définit inductivement l'application de la substitution σ à une formule par

— $\top[\sigma] = \top$;
— $\bot[\sigma] = \bot$;
— $P(t_1, \ldots, t_n)[\sigma] = P\big(t_1[\sigma], \ldots, t_n[\sigma]\big)$;
— $(G \odot H)[\sigma] = G[\sigma] \odot H[\sigma]$ avec $\odot \in \{\vee, \wedge, \to, \leftrightarrow\}$;
— $(\neg G)[\sigma] = \neg\big(G[\sigma]\big)$;
— $(\forall x,\ G)[\sigma] = \forall x,\ G\big[\sigma[x \mapsto x]\big]$
— $(\exists x,\ G)[\sigma] = \exists x,\ G\big[\sigma[x \mapsto x]\big]$

B On s'assurera que les variables apparaissent dans l'espace image de la substitution σ n'intersecte pas avec les variables liées de G lors du calcul de $G[\sigma]$. Ce peut-être assuré au moyen du α-renommage.

Exemple :
On considère la formule $P(x, y) \wedge \big(\forall x,\ Q(x, y)\big)$. On applique la substitution $\sigma : (x \mapsto x{+}y,\ y \mapsto 0)$.

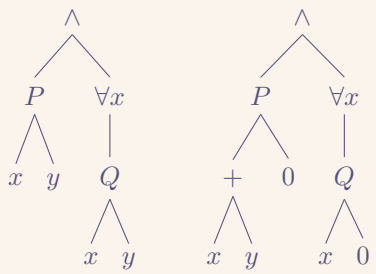
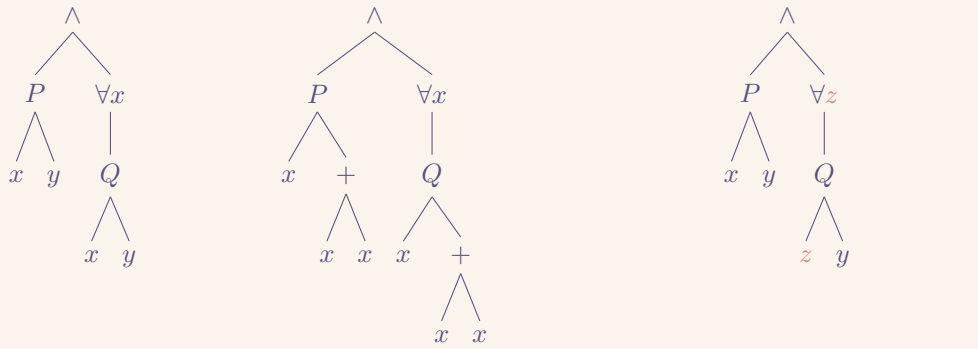


Figure 6.2 – Arbre de syntaxe de la formule $P(x, y) \wedge \big(\forall x, Q(x, y)\big)$, application de la substitution $\sigma = (x \mapsto x{+}y,\ y \mapsto 0)$

Exemple :
On considère la même formule, et la substitution $\sigma : (y \mapsto x{+}x)$.



formule originale substitution sans α-renommage substitution après α-renommage

FIGURE 6.3 – Arbre de syntaxe de la formule $P(x,y) \wedge \big(\forall x, Q(x,y)\big)$, application de la substitution $\sigma = (y \mapsto x{+}x)$ directement et avec α-renommage

IV.2.3 Extension au premier ordre de la déduction naturelle

On ajoute les règles suivantes.

SYMBOLE	RÈGLE D'INTRODUCTION	RÈGLE D'ÉLIMINATION
$\forall$	$\dfrac{\Gamma \vdash G}{\Gamma \vdash \forall x,\ G}\ \forall\text{i}$ $x \notin \mathsf{FV}(\Gamma)$	$\dfrac{\Gamma \vdash \forall x,\ G}{\Gamma \vdash G\big[(x \mapsto t)\big]}\ \forall\text{e}$ $\mathrm{vars}(t) \cap \mathsf{BV}(G) =$
$\exists$	$\dfrac{\Gamma \vdash G\big[(x \mapsto t)\big]}{\Gamma \vdash \exists x,\ G}\ \exists\text{i}$	$\dfrac{\Gamma \vdash \exists x,\ H \qquad \Gamma, H \vdash G}{\Gamma \vdash G}\ \exists\text{e}$ $x \notin \mathsf{FV}(\Gamma) \cup \mathsf{FV}(G)$

TABLE 6.3 – Extension au premier ordre de la déduction naturelle

EXEMPLE :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x,\ P(\mathbf{0},x) \vdash \forall x,\ P(\mathbf{0},x)}\ \text{Ax}}{\forall x,\ P(\mathbf{0},x) \vdash P(\mathbf{0},\mathbf{1})}\ \forall\text{e}}{\forall x,\ P(\mathbf{0},x) \vdash \exists y,\ P(y,\mathbf{1})}\ \exists\text{i}}{\vdash \big(\forall x,\ P(\mathbf{0},x)\big) \to \big(\exists y,\ P(y,\mathbf{1})\big)}\ \to\text{i}$$

EXEMPLE :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x,\ P(x) \vdash \forall x,\ P(x)}\ \mathrm{Ax}}{\forall x,\ P(x) \vdash P(x)}\ \forall\mathrm{e}}{\forall x,\ P(x) \vdash \exists x,\ P(x)}\ \exists\mathrm{i}}{\vdash \big(\forall x,\ P(x)\big) \to \big(\exists x,\ P(x)\big)}\ \to\mathrm{i}$$

Exemple :
On pose $F_1 = \exists x,\ P(x)$ et $F_2 = \forall x,\ \forall y,\ \big(P(x) \to Q(y)\big)$.

$$\dfrac{\dfrac{}{F_1, F_2 \vdash \exists x,\ P(x)}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{F_1, F_2, P(x) \vdash \exists y,\ P(x) \to Q(y) \vdash \exists y,\ P(x) \to Q(y)}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma, P(x) \to Q(y), P(x) \vdash P(x) \to Q(y)}\ \text{Ax} \qquad \dfrac{}{\Gamma, P(x) \vdash P(x)}\ \text{Ax}}{F_1, F_2, P(x), \big(\exists y\ P(x) \to Q(y)\big), P(x) \to Q(y) \vdash Q(y)}\ \to\text{e}}{F_1, F_2, P(x), \big(\exists y\ P(x) \to Q(y)\big), P(x) \to Q(y) \vdash \exists y,\ Q(y)}\ \exists\text{i}}{F_1, F_2, P(x), \big(\exists y\ P(x) \to Q(y)\big) \vdash \exists z,\ Q(z)}\ \exists\text{e}}{F_1, F_2, P(x) \vdash \big(\exists y\ P(x) \to Q(y)\big) \to (\exists z,\ Q(z))}\ \to\text{i} \qquad \dfrac{\dfrac{}{F_1, F_2, P(x) \vdash \forall x,\ \exists y,\ P(x) \to Q(y)}\ \text{Ax}}{F_1, F_2, P(x) \vdash \exists y,\ P(x) \to Q(y)}\ \forall\text{e}}{F_1, F_2, P(x) \vdash \exists z,\ Q(z)}\ \to\text{e}}{\exists x,\ P(x); \forall x,\ \exists y,\ \big(P(x) \to Q(y)\big) \vdash \exists z,\ Q(z)}\ \exists\text{e}$$

Exemple (Paradoxe du buveur) :
On pose $\varphi = \exists x,\ \neg B(x)$.

$$\dfrac{\dfrac{}{\vdash \varphi \vee \neg\varphi}\ \text{TE} \qquad \dfrac{\dfrac{}{\varphi \vdash \varphi}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi, \neg B(x), B(x) \vdash B(x)}\ \text{Ax} \qquad \dfrac{}{\varphi, \neg B(x), B(x) \vdash \neg B(x)}\ \text{Ax}}{\varphi, \neg B(x), B(x) \vdash \bot}\ \bot\text{e}}{\varphi, \neg B(x), B(x) \vdash \forall y,\ B(y)}\ \to\text{i}}{\varphi, \neg B(x) \vdash B(x) \to \forall y,\ B(y)}\ \exists\text{i}}{\varphi, \neg B(x) \vdash \exists x,\ \big(B(x) \to \forall y,\ B(y)\big)}\ \exists\text{e}}{\varphi \vdash \exists x,\ \big(B(x) \to \forall y,\ B(y)\big)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\big(\exists x,\ \neg B(x)\big), B(x), \neg B(y) \vdash \neg\big(\exists x,\ \neg B(x)\big)}\ \text{Ax} \qquad \dfrac{}{\neg\big(\exists x,\ \neg B(x)\big), B(x), \neg B(y) \vdash \neg B(y)}\ \text{A}}{\neg\big(\exists x,\ \neg B(x)\big), B(x), \neg B(y) \vdash \exists x,\ \neg B(x)}}{\neg\big(\exists x,\ \neg B(x)\big), B(x), \neg B(y) \vdash \bot}\ \text{Abs}}{\neg\big(\exists x,\ \neg B(x)\big), B(x) \vdash B(y)}\ \forall\text{i}}{\neg\varphi, B(x) \vdash \forall y,\ B(y)}\ \to\text{i}}{\neg\varphi \vdash B(x) \vdash \forall y,\ B(y)}\ \exists\text{i}}{\neg\varphi \vdash \exists x,\ \big(B(x) \to \forall y,\ B(y)\big)}\ \vee\text{e}}{\vdash \exists x,\ \big(B(x) \to \forall y,\ B(y)\big)}$$

Théorème : L'ajout des quatre règles précédentes à la déduction naturelle, intuitionniste ou classique, maintient sa correction. □

Remarque (Hors-Programme) :
L'ajout de ces règles maintient également sa complétude vis-à-vis de la logique classique.

IV.2.4 Règles dérivées

On définit de manière informelle la notion de *règle dérivée* comme des règles que l'on peut obtenir comme combinaison des règles déjà existantes.

Exemple :
On considère la règle nommée TE′ définie comme

$$\frac{\Gamma, H \vdash G \qquad \Gamma, \neg H \vdash G}{\Gamma \vdash G}\ \text{TE}'.$$

Elle se dérive des règles TE et $\vee$e :

$$\frac{\dfrac{}{\Gamma \vdash H \vee \neg H}\ \text{Ax} \qquad \Gamma, H \vdash G \qquad \Gamma, \neg H \vdash G}{\Gamma \vdash G}\ \vee\text{e}.$$

Remarque :
Si $\Gamma \vdash G$ est prouvable, et si $\Gamma \subseteq \Gamma'$, alors $\Gamma' \vdash G$ est prouvable. On ajoute donc parfois une règle dit d'*affaiblissement*, définie comme

$$\frac{\Gamma' \vdash G}{\Gamma \vdash G}\ \text{Aff} \qquad \Gamma' \subseteq \Gamma.$$

IV.2.5 Sémantique

On considère la formule défini par l'arbre de syntaxe suivant. On a $\mathscr{P} = \{P(1), Q(1)\}$, $\mathscr{S} = \{\oplus(2), \tilde{0}(0), \tilde{1}(0), \ominus(3)\}$ et $\mathscr{V} \supseteq \{x, y, z\}$.

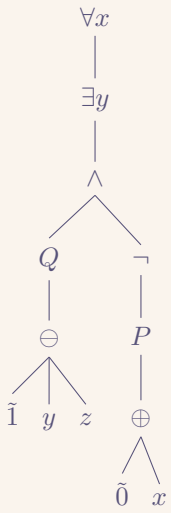


FIGURE 6.4 – Arbre de syntaxe exemple

Pour interpréter une formule de la logique du premier ordre, on doit définir le "monde" des variables, leur valeur, la valeur d'une constante et d'une fonction, la valeur des prédicats, et le sens des quantificateurs.

Définition (Domaine) **:** On appelle *domaine d'interprétation* des termes un ensemble non vide M.

EXEMPLE :
On peut choisir $\mathrm{M} = \mathbb{R}$, ou $\mathrm{M} = \mathbb{N}$, $\mathrm{M} = \mathbb{Z}$, $\mathrm{M} = \mathbb{B}$ ou $\mathrm{M} = \mathcal{T}(\mathcal{S}, \mathcal{V})$.

Dans toute la suite de cette section, on fixe les ensembles $\mathcal{S}$, $\mathcal{V}$ et $\mathcal{P}$.

Définition (Environnement de variables) **:** On appelle *environnement de variable* sur $V \subseteq \mathcal{V}$ une fonction

$$\mu : V \longrightarrow \mathrm{M}.$$

EXEMPLE :
On a par exemple $\mu = (x \mapsto 3)$.

Définition (Structure d'interprétation) **:** On appelle *structure d'interprétation* la donnée de

- un domaine M ;
- une fonction $f^M : \mathrm{M}^{\mathfrak{a}(f)} \longrightarrow \mathrm{M}$ pour chaque symbole $f \in \mathcal{S}$;
- une fonction $P^M : \mathrm{M}^{\mathfrak{a}(P)} \longrightarrow \mathbb{B}$ pour chaque symbole $P \in \mathcal{P}$.

On typographie une telle structure M.

Exemple :
Si $\mathcal{S} = \{\oplus(2), \ominus(2)\}$, $\mathcal{P} = \{\lessdot(2), \ominus\!\!\!\!-(2)\}$, et M $= \mathbb{N}$, alors on définit les fonctions

$$\oplus^M : \mathbb{N}^2 \longrightarrow \mathbb{N} \qquad (m,n) \longmapsto m+n,$$

$$\lessdot^M : \mathbb{N}^2 \longrightarrow \mathbb{B} \qquad (n,m) \longmapsto \begin{cases} \mathbf{V} & \text{si } n < m \\ \mathbf{F} & \text{sinon,} \end{cases}$$

et

$$\ominus^M : \mathbb{N}^2 \longrightarrow \mathbb{N} \qquad (n,m) \longmapsto \begin{cases} n-m & \text{si } n \geqslant m \\ 0 & \text{sinon,} \end{cases}$$

$$\ominus\!\!\!\!-^M : \mathbb{N}^2 \longrightarrow \mathbb{B} \qquad (n,m) \longmapsto \begin{cases} \mathbf{V} & \text{si } n = m \\ \mathbf{F} & \text{sinon.} \end{cases}$$

Définition : On définit la fonction `eval` prenant en argument
- un terme t,
- une structure d'interprétation,
- un environnement sur au moins les variables de t,

et s'évaluant dans M, telle que $\texttt{eval}(x, M, \mu) = \mu(x)$ avec $x \in \mathcal{V}$, et que

$$\begin{aligned} &\texttt{eval}\big(f(t_1, t_2, \ldots, t_{\texttt{a}(f)}), M, \mu\big) \\ =&f^M\big(\texttt{eval}(t_1, M, \mu), \texttt{eval}(t_2, M, \mu), \ldots, \texttt{eval}(t_{\texttt{a}(f)}, M, \mu)\big) \end{aligned}$$

Exemple :
Avec la structure précédente, on a

$$\begin{aligned} \texttt{eval}\Big(\oplus\big(x, \ominus(x,y)\big), M, (x \mapsto 1, y \mapsto 2)\Big) &= \oplus^M\Big(\mu(x), \ominus^M\big(\mu(x), \mu(y)\big)\Big) \\ &= 1 + \ominus^M(1,2) \\ &= 1 + 0 = 1 \end{aligned}$$

Définition (Interprétation des formules) **:** On définit inductivement $[\![\cdot]\!]^{M,\mu}$ comme
- $[\![\top]\!]^{M,\mu} = \mathbf{V}$;
- $[\![\bot]\!]^{M,\mu} = \mathbf{F}$;
- $[\![\neg G]\!]^{M,\mu} = \overline{[\![G]\!]^{M,\mu}}$;
- $[\![G \wedge H]\!]^{M,\mu} = [\![G]\!]^{M,\mu} \cdot [\![H]\!]^{M,\mu}$;
- $[\![G \vee H]\!]^{M,\mu} = [\![G]\!]^{M,\mu} + [\![H]\!]^{M,\mu}$;
- $[\![G \to H]\!]^{M,\mu} = \overline{[\![G]\!]^{M,\mu}} + [\![H]\!]^{M,\mu}$;

— $[\![G \leftrightarrow H]\!]^{M,\mu} = \left(\overline{[\![G]\!]^{M,\mu}} + [\![H]\!]^{M,\mu}\right) \cdot \left(\overline{[\![H]\!]^{M,\mu}} + [\![G]\!]^{M,\mu}\right)$;
— $\left[\!\left[P(t_1, \ldots, t_{\mathfrak{a}(P)})\right]\!\right]^{M,\mu} = P^M\left(\texttt{eval}(t_1, M, \mu), \ldots, \texttt{eval}(t_{\mathfrak{a}(P)}, M, \mu)\right)$;
— $[\![\exists x,\, G]\!]^{M,\mu} = \underset{v_x \in \mathrm{M}}{+} [\![G]\!]^{M,\mu[x \mapsto v_x]}$;
— $[\![\forall x,\, G]\!]^{M,\mu} = \underset{v_x \in \mathrm{M}}{\bullet} [\![G]\!]^{M,\mu[x \mapsto v_x]}$,

où on définit $+\mathscr{B} = \mathbf{V} \iff \mathbf{V} \in \mathscr{B}$, et $\bullet\, \mathscr{B} = \mathbf{F} \iff \mathbf{F} \in \mathscr{B}$ avec $\mathscr{B} \subseteq \{\mathbf{V}, \mathbf{F}\}$.

Exemple :
On pose $\mathcal{S} = \{\oplus(2), Z(0)\}$, $\mathcal{P} = \{\circledleq(2), \ominus(2)\}$, et

$$G = \forall x,\, \Big(\exists y,\, \Big(\exists z, \ominus\big(x, \oplus(y, z)\big) \wedge \neg\ominus\big(z, Z\big)\Big)\Big).$$

On considère la structure M définie comme donnée de $\mathrm{M} = \mathbb{N}$, $\oplus^M = +$, $Z^M = 0$, $\ominus^M = \leqslant$, et $\ominus^M =$ " = ". Ainsi,

$$[\![G]\!]^{M,(\,)} = \underset{v_x \in \mathbb{N}}{\bullet} \Big(\underset{v_y \in \mathbb{N}}{+} \Big(\underset{v_z \in \mathbb{N}}{+} \mathbb{1}_{v_x = v_y + v_z} \cdot \overline{\mathbb{1}_{v_z = 0}} \Big) \Big),$$

où l'on définit $\mathbb{1}_G$ comme $\mathbf{V}$ si G est vrai, et $\mathbf{F}$ sinon. Pour $v_x = 0$, alors, pour tous $v_y \in \mathbb{N}$ et $v_z \in \mathbb{N}$, on a $\mathbb{1}_{v_x = v_y + v_z} \cdot \overline{\mathbb{1}_{v_z = 0}} = \mathbf{F}$. Ainsi, $[\![G]\!]^{M,\mu} = \mathbf{F}$. À faire : cas où $\mathrm{M} = \mathbb{Z}$

Définition : Une formule G de la logique du premier ordre est dite *satisfiable* dès lors qu'il existe une structure M, et un environnement de variables μ tel que $[\![G]\!]^{M,\mu} = \mathbf{V}$.

Une structure M est dit *modèle* de G dès lors que, pour tout environnement de variables μ, on a $[\![G]\!]^{M,\mu} = \mathbf{V}$.

Une formule G de la logique du premier ordre est dite *valide* dès lors que pour toute structure M, et tout environnement de variables μ, on a $[\![G]\!]^{M,\mu} = \mathbf{V}$.

Étant donné deux formules G et H, on dit que H est *conséquence sémantique* de G dès lors que, pour toute structure M et environnement de variables μ, si $[\![G]\!]^{M,\mu} = \mathbf{V}$, alors $[\![H]\!]^{M,\mu} = \mathbf{V}$. On le note $G \models H$.

On dit que deux formules G et H sont *équivalentes* dès lors que, $G \models H$ et $H \models G$. On le note $G \equiv H$.

Remarque : — Une formule est dit *close* dès lors que $\mathsf{FV}(H) = .$
— Une formule de ma forme $P(t_1, t_2, \ldots, t_{\mathfrak{a}(P)})$ est appelée *formule atomique* ou *prédicat atomique.*
— Si $\mathsf{FV}(G) = \{x_1, \ldots, x_n\}$, la formule $\forall x_1, \ldots, \forall x_n,\, G$ est appelée *cloture universelle* de G. La formule $\exists x_1, \ldots, \exists x_n,\, G$ est appelée *cloture existentielle* de G.

IV.3 Synthèse du chapitre

Symbole	Règle d'introduction	Règle d'élimination
$\top$	$\dfrac{}{\Gamma \vdash \top}\ \top\text{i}$	
$\bot$		$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash G}\ \bot\text{e}$
$\neg$	$\dfrac{\Gamma, G \vdash \bot}{\Gamma \vdash \neg G}\ \neg\text{i}$	$\dfrac{\Gamma \vdash G \quad \Gamma \vdash \neg G}{\Gamma \vdash \bot}\ \neg\text{e}$
$\to$	$\dfrac{\Gamma, G \vdash H}{\Gamma \vdash G \to H}\ \to\text{i}$	$\dfrac{\Gamma \vdash H \to G \quad \Gamma \vdash H}{\Gamma \vdash G}\ \to\text{e}$
$\wedge$	$\dfrac{\Gamma \vdash G \quad \Gamma \vdash H}{\Gamma \vdash G \wedge H}\ \wedge\text{i}$	$\dfrac{\Gamma \vdash G \wedge H}{\Gamma \vdash G}\ \wedge\text{e,g} \qquad \dfrac{\Gamma \vdash G \wedge H}{\Gamma \vdash H}\ \wedge\text{e,d}$
$\vee$	$\dfrac{\Gamma \vdash G}{\Gamma \vdash G \vee H}\ \vee\text{i,g} \qquad \dfrac{\Gamma \vdash H}{\Gamma \vdash G \vee H}\ \vee\text{i,d}$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash G \quad \Gamma, B \vdash G}{\Gamma \vdash G}\ \vee\text{e}$
	$\dfrac{}{\Gamma, \varphi \vdash \varphi}\ \text{Ax}$	

Table 6.4 – Règles d'introduction et d'élimination

$\dfrac{}{\Gamma \vdash G \vee \neg G}\ \text{TE}$	$\dfrac{\Gamma \vdash \neg\neg G}{\Gamma \vdash G}\ \neg\neg\text{e}$	$\dfrac{\Gamma, \neg G \vdash \bot}{\Gamma \vdash G}\ \text{Abs}$

Table 6.5 – Déduction naturelle classique

Symbole	Règle d'introduction	Règle d'élimination
$\forall$	$\dfrac{\Gamma \vdash G}{\Gamma \vdash \forall x,\, G}\ \forall\text{i}$ $x \notin \mathsf{FV}(\Gamma)$	$\dfrac{\Gamma \vdash \forall x,\, G}{\Gamma \vdash G\big[(x \mapsto t)\big]}\ \forall\text{e}$ $\text{vars}(t) \cap \mathsf{BV}(G) =$
$\exists$	$\dfrac{\Gamma \vdash G\big[(x \mapsto t)\big]}{\Gamma \vdash \exists x,\, G}\ \exists\text{i}$	$\dfrac{\Gamma \vdash \exists x,\, H \quad \Gamma, H \vdash G}{\Gamma \vdash G}\ \exists\text{e}$ $x \notin \mathsf{FV}(\Gamma) \cup \mathsf{FV}(G)$

Table 6.6 – Extension au premier ordre de la déduction naturelle

Chapitre 7

Tentative de réponse à la NP-complétude

IV.0 Motivation

On considère le problème **NP**-complet du *voyageur de commerce* : étant donné un graphe pondéré G quel est le tour de longueur[1] minimale *i.e.* quelle est la permutation de sommets telle que la longueur totale est minimale.

On se ramène à un problème de décision : étant donné une constante $K \in \mathbb{R}$, existe-t-il un chemin de longueur inférieure à K.

Un algorithme glouton, allant d'un sommet à son voisin le plus proche, ne permet pas de résoudre ce problème en complexité polynômiale.

On ne cherche plus le « tour optimal » mais on cherche une solution proche : on veut trouver une constante ρ telle que, quelque soit l'entrée, le chemin obtenu est de longueur inférieure à ρ fois la longueur optimale.

IV.1 Problèmes d'optimisation

Dans un premier temps, on s'intéresse à un problème où l'on cherche à minimiser quelque chose. On réalise la transformation réalisée dans la partie précédente : étant donné un seuil K, on est ce que la valeur est inférieure à K. On se ramène donc à un problème de décision.

Définition : Soit $Q \subseteq \mathcal{E} \times \mathcal{S}$ un problème. Soit opt $\in \{\min, \max\}$. On dit que Q est un *problème d'*opt*imisation* (*i.e.* problème de minimisation, maximisation), si pour toute entrée $e \in \mathcal{E}$, il existe

— un ensemble sol(e) de solutions,

1. poids des arrêtes total

— une fonction $c_e : \mathrm{sol}(e) \to \mathbb{R}^+$,

tels que $c_e^\star = \mathrm{opt}\{c_e(s) \mid s \in \mathrm{sol}(e)\}$ est bien défini, et

$$\forall s \in \mathrm{sol}(e), \qquad (e, s) \in Q \implies c_e(s) = c_e^\star.$$

On nomme :

— $\mathrm{sol}(e)$ l'*ensemble des solutions pour l'entrée* e,
— c_e *la fonction objectif*,
— $c_e^\star$ la *valeur* opt*imale* (minimale ou maximale),
— pour une solution $s \in \mathrm{sol}(e)$, $c_e(s)$ est appelée la *valeur de la solution*.

On appelle *solution* opt*imale* une solution de valeur optimale.

Exemple :
On considère le problème

$$\begin{cases} \textbf{Entrée} & : G = (S, A) \text{ un graphe orienté fortement connexe, } s \in S, \text{ et } p \in S \\ \textbf{Sortie} & : \text{un plus court chemin (en nombre d'arcs) de } s \text{ à } p \text{ dans } G. \end{cases}$$

Soit l'entrée ci-dessous.

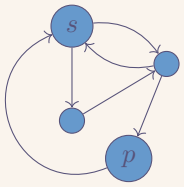


Figure 7.1 – Entrée du problème du plus court chemin

L'ensemble $\mathrm{sol}(e)$ est l'ensemble (infini) des chemins de s à p, et $c_e(\gamma) = |\gamma|$ (la longueur du chemin γ). On vérifie qu'il existe un chemin de s à p, donc $\{c_e(s) \mid s \in \mathrm{sol}(e)\}$ est une partie de $\mathbb{N}$ non vide, elle admet donc un minimum.

Définition : Le *problème de décision associé* à un problème d'optimisation est le problème obtenu en ajoutant une constante aux entrées et en demandant en sortie s'il est possible de dépasser cette constante.

Exemple :
Étant donné le problème d'optimisation

$$Q_{\mathrm{O}} : \begin{cases} \textbf{Entrée} & : e \in \mathscr{E}_{Q_{\mathrm{O}}} \\ \textbf{Sortie} & : \arg\mathrm{opt}_{s \in \mathrm{sol}(e)} c_e(s), \end{cases}$$

on définit le problème de décision associé

$$Q : \begin{cases} \textbf{Entrée} & : e \in \mathscr{E}_{Q_{\mathrm{O}}},\ K \in \mathbb{R}^+ \\ \textbf{Sortie} & : \text{existe-t-il } s \in \mathrm{sol}(e) \text{ tel que } c_e(s) \bowtie K \end{cases}$$

avec $\bowtie = \leqslant$ si opt = min et $\bowtie = \geqslant$ si opt = max.

Exemple :
Avec l'exemple précédent (plus court chemin), le problème de décision associé est

$$\begin{cases} \textbf{Entrée} & : G = (S, A) \text{ un graphe orienté fortement connexe, } (p, s) \in S^2, \text{ et } K \in \mathbb{R}^+ \\ \textbf{Sortie} & : \text{Existe-t-il un chemin de } s \text{ à } p \text{ dans } G \text{ de longueur inférieure ou égale à } K \,? \end{cases}$$

Exemple :
On considère le problème Knapsack de décision défini comme

$$\begin{cases} \textbf{Entrée} & : \text{Un entier } n \in \mathbb{N},\ (p_1, \dots, p_n) \in (\mathbb{N}^\star)^n,\ (v_1, \dots, v_n) \in (\mathbb{N}^\star)^n,\ P \in \mathbb{N} \text{ et } K \in \mathbb{N} \\ \textbf{Sortie} & : \text{Existe-t-il } I \subseteq [\![1, n]\!] \text{ telle que } \sum_{i \in I} p_i \leqslant P \text{ et } \sum_{i \in I} v_i \geqslant K \,? \end{cases}$$

Le problème d'optimisation associé est Knapsack_O défini comme

$$\begin{cases} \textbf{Entrée} & : \text{Un entier } n \in \mathbb{N},\ (p_1, \dots, p_n) \in (\mathbb{N}^\star)^n,\ (v_1, \dots, v_n) \in (\mathbb{N}^\star)^n, \text{ et } P \in \mathbb{N} \\ \textbf{Sortie} & : I \subseteq [\![1, n]\!] \text{ tel que } \sum_{i \in I} p_i \leqslant P \text{ et maximisant } \sum_{i \in I} v_i. \end{cases}$$

Remarque :
Soit Q_O un problème d'optimisation et Q le problème de décision associé. Étant donné un algorithme $\mathscr{A}_\text{O}$ pour Q_O, on fabrique l'algorithme $\mathscr{A}$ suivant résolvant Q.

Algorithme 7.1 Solution à un problème de seuil

Entrée e une entrée de Q_O et K un seuil

1 : **retourner** $c_e(\mathscr{A}_\text{O}) \overset{?}{\bowtie} K$ ▷ *où* $\bowtie$ *est* $\geqslant$ *pour si* opt *est* max, *et* $\leqslant$ *si* opt *est* min

Ainsi, le problème Q_O est plus difficile à résoudre que le problème Q de décision associé. Alors, lorsque le problème de décision Q associé à un problème d'optimisation S_O est **NP**-difficile, c'est mal engagé.

IV.2 Algorithmes d'approximations

Remarque (Vocabulaire) :
On fixe dans la suite un problème d'optimisation Q, on note $\text{OPT}(e)$ la valeur optimale pour une entrée e.

Définition (Algorithme d'approximation pour un problème de maximisation) **:** On dit d'un algorithme $\mathscr{A} : \mathscr{E}_Q \to \mathbb{R}^+$ qu'il approxime un problème Q de maximisation avec un ratio d'approximation $\rho < 1$ dès lors que

$$\forall e \in \mathscr{E}_Q, \quad \mathscr{A}(e) \geqslant \rho \cdot \text{OPT}(e).$$

On dit alors que l'algorithme $\mathscr{A}$ est une *ρ-approximation* (standard).

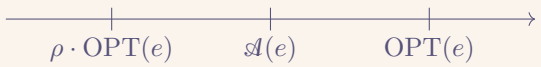


FIGURE 7.2 – Algorithme d'approximation pour un problème de maximisation

Définition (Algorithme d'approximation pour un problème de minimisation) **:** On dit d'un algorithme $\mathscr{A} : \mathscr{C}_Q \to \mathbb{R}^+$ qu'il approxime un problème Q de minimisation avec un ratio d'approximation $\rho > 1$ dès lors que

$$\forall e \in \mathscr{C}_Q, \quad \mathscr{A}(e) \leqslant \rho \cdot \mathrm{OPT}(e).$$

On dit alors que l'algorithme $\mathscr{A}$ est une *ρ-approximation* (standard).

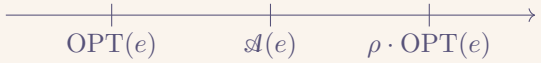


FIGURE 7.3 – Algorithme d'approximation pour un problème de minimisation

Dans la définition suivante, on suppose connu une fonction $\mathrm{Pire}(e)$ donnant la pire valeur de solution pour une entrée e.

Définition : On dit qu'un algorithme $\mathscr{A} : \mathscr{C}_Q \to \mathbb{R}$ est une *ρ-approximation différentielle* dès lors que

$$\frac{\big|\mathscr{A}(e) - \mathrm{Pire}(e)\big|}{\big|\mathrm{Pire}(e) - \mathrm{OPT}(e)\big|} \geqslant \rho.$$

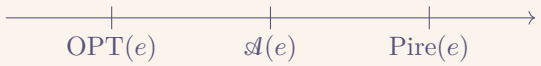


FIGURE 7.4 – ρ-approximation différentielle

REMARQUE :
Dans le cadre d'un problème de minimisation, on ne calcule pas $\mathrm{OPT}(e)$ en général. On minore $\mathrm{OPT}(e)$, et alors

$$\frac{\mathscr{A}(e)}{\mathrm{OPT}(e)} \leqslant \underbrace{\frac{\mathscr{A}(e)}{B}}_{\rho}.$$

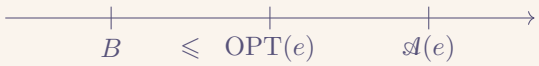


FIGURE 7.5 – Calcul de OPT(e)

EXEMPLE :
Soit $C \in \mathbb{N}^\star$. On rappelle le problème STABLE, restreint à un graphe de degré maximal C :

$$\text{STABLE} : \begin{cases} \textbf{Entrée} & : G = (S, A) \text{ une graphe tel que } 0 \neq \Delta(G) \leqslant C \\ \textbf{Sortie} & : \text{ un stable de } G \text{ de cardinal maximal} \end{cases}$$

où $X \subseteq S$ est un stable si pour tout $(u, v) \in X^2$, $\{u, v\} \notin A$, et $\Delta(G) = \max_{v \in S} \deg_G(v)$ est le degré du graphe.

Algorithme 7.2 Algorithme glouton de recherche de stables

Entrée $G = (S, A)$ un graphe
1 : $S' \leftarrow$
2 : **tant que** $S \neq$ **faire**
3 : $\quad v^\star = \text{argmin}_{v \in S} \deg_G(v)$ ▷ *les degrés sont modifiés à chaque itération*
4 : $\quad S' \leftarrow S' \cup \{v^\star\}$
5 : $\quad S \leftarrow S \setminus \big(\{v^\star\} \cup \text{voisins}(v^\star)\big)$
6 : $\quad A \leftarrow$ restriction de A à S
7 : **retourner** S'

Cet algorithme n'est pas correct, la figure ci-après en est un contre-exemple.

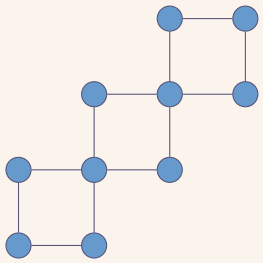


FIGURE 7.6 – Contre-exemple à l'algorithme 7.2

Proposition : L'algorithme 7.2 est une $\frac{1}{\Delta(G)}$-approximation.

Preuve :
Soit S' la réponse de l'algorithme. Soit $S^\star$ la solution optimale. On a, par

terminaison de l'algorithme

$$\forall v \in S \setminus S, \exists v' \in S',\ \{v, v'\} \in A$$

car l'algorithme s'arrête. En particulier, $\forall v^\star \in S^\star \setminus S', \exists v' \in S', \{v, v'\} \in A$. Or, $S^\star$ est stable donc, si $v^\star \in S^\star$ et $v' \in S'$ tels que $\{v^\star, v' \in A\}$, alors $v' \notin S^\star$. D'où,

$$\forall v^\star \in S^\star \setminus S',\ \exists v' \in S' \setminus S^\star,\ \{v^\star, v'\} \in A.$$

Par définition de degré d'un graphe, on a $|S^\star \setminus S'| \leqslant \Delta(G)\,|S' \setminus S^\star|$ donc

$$\begin{aligned} |S^\star| &= |S^\star \cap S'| + |S^\star \setminus S'| \\ &\leqslant |S^\star \cap S'| + \Delta(G)\,|S' \setminus S^\star| \\ &\leqslant \Delta(G)\,|S^\star \cap S'| + \Delta(G)\,|S' \setminus S^\star| \\ &\leqslant \Delta(G)\,|S'|. \end{aligned}$$

□

Remarque :
Cette preuve ne fait pas d'hypothèses sur le résultat de l'algorithme. Tout algorithme répondant au problème est une $\frac{1}{\Delta(G)}$-approximation.

Exemple :
On appelle *couverture par sommets* d'un graphe $G = (S, A)$ la donnée d'un ensemble $X \subseteq S$ tel que

$$\forall \{u, v\} \in A, \quad u \in X \text{ ou } v \in X.$$

Exemple :
L'ensemble ● est une couverture par sommets du graphe ci-dessous.

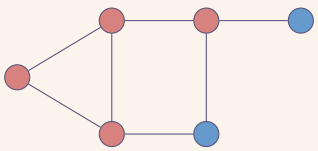


Figure 7.7 – Exemple de couverture par sommets

On considère le problème

$$\begin{cases} \textbf{Entrée} & : G = (S, A) \text{ un graphe} \\ \textbf{Sortie} & : \text{une couverture de cardinal maximal.} \end{cases}$$

Ce problème peut-être résolu à l'aide du calcul de couplages maximal.

Algorithme 7.3 Calcul d'un couplage maximal (CouplageMaximal)

Entrée $G = (S, A)$ un graphe
Sortie C un couplage maximal, *non nécessairement maximum*
1 : $C \leftarrow$
2 : **tant que** $\exists \{u, v\} \in A$, u libre dans C et v libre dans C **faire**
3 : Soit $\{u, v\}$ une telle arrête.
4 : $C \leftarrow C \cup \{\{u, v\}\}$
5 : **retourner** C

L'algorithme retourne un couplage maximal d'après la négation de la condition de boucle. On répond donc au problème avec l'algorithme ci-dessous.

Algorithme 7.4 Approximation de couverture par sommets

Entrée $G = (S, A)$ un graphe
Sortie Une couverture par sommets
1 : $C \leftarrow$ CouplaxeMaximal(G)
2 : **retourner** $\{u \in S \mid \exists v \in S, \{u, v\} \in C\}$.

L'algorithme retourne une couverture : soit X la valeur retournée pour une entrée $G = (S, A)$. Soit $\{u, v\} \in A$. Si $u \notin X$ et $v \notin X$, alors le couplage C calculé pour l'algorithme n'est pas maximal, on peut y ajouter $\{u, v\}$. Montrons que l'algorithme $\mathscr{A}$ est une 2-approximation du problème « couverture par sommets. »

$$\forall G \in \mathscr{C}, \quad \mathscr{A}(G) \leqslant 2\,\mathrm{OPT}(G).$$

Soit $G \in \mathscr{C}$. Soit X la couverture par sommets calculé par $\mathscr{A}$ sur G, et C le couplage calculé par cet algorithme. Soit $X^\star$ la couverture par sommets optimale. Soit donc

$$\varphi : \quad C \longrightarrow X^\star$$
$$\{u, v\} \longmapsto \begin{cases} u & \text{si } u \in X^\star \\ v & \text{si } v \in X^\star \end{cases}$$

Soit $(c_1, c_2) \in C^2$, tels que $\varphi(c_1) = \varphi(c_2)$, alors c_1 et c_2 partagent un sommet, ce qui est absurde (*c.f.* définition de couplage). Donc φ est injective, d'où $|C| \leqslant |X^\star|$. Or, $\mathscr{A}(X) = |X| = 2|C| \leqslant 2\,|X^\star| \leqslant 2\,\mathrm{OPT}(X)$.

IV.3 *Branch and Bound* — Séparation et évaluation

Branch and Bound n'est pas un algorithme, mais une famille d'algorithmes, similairement au algorithmes diviser pour régner. Ces algorithmes répondent à des problèmes de maximisation. Les algorithmes *Branch and Bound* sont des algorithmes enrichit de trois fonctions :

— une fonction `branch` de branchement, *i.e.* découpage en sous-problèmes,

— une fonction `valeur` donnant un résultat, pas forcément optimal, *i.e.* elle associe une solution partielle à une solution,

— une fonction `bound` donnant un majorant de la solution optimale, complétant cette solution partielle.

Avec les deux dernières fonctions, on borne la valeur de la solution optimale.

EXEMPLE (PL et PLNE) :
c.f. DM4.

EXEMPLE :
On considère le problème KNAPSACK :

$$\begin{cases}\textbf{Entrée} & : n \in \mathbb{N},\ (v_i)_{i\in[\![1,n]\!]} \in (\mathbb{N}^\star)^n,\ (w_i)_{i\in[\![1,n]\!]} \in (\mathbb{N}^\star)^n,\ \text{et } P \in \mathbb{N}^\star \\ \textbf{Sortie} & : \text{une allocation } I \text{ maximale d'objets de somme de poids } (w_i)_{i\in I} \text{ inférieure ou égale à } P.\end{cases}$$

Dans toute la suite de l'exemple, les $(v_i)_{i\in[\![1,n]\!]}$ et $(w_i)_{i\in[\![1,n]\!]}$ sont triés par v_i/w_i décroissants.

Tentative 1. Algorithme glouton.

Algorithme 7.5 Algorithme glouton $\mathcal{G}^{\mathbb{N}}$ répondant au problème KNAPSACK

```
1 : I ←
2 : S ← 0
3 : pour i ∈ ⟦1, n⟧ faire
4 :     si S + w_i ⩽ P alors
5 :         I ← I ∪ {i}
6 :         S ← S + w_i
7 : retourner I
```

Cet algorithme ne donne pas toujours une solution optimale, voici un contre-exemple : $P = 3$, $(v_i) = (1, 2)$ et $(w_i) = (1, 3)$. L'algorithme renvoie $\mathcal{G}^{\mathbb{N}}(E_1) = 1$ mais la solution optimale $\mathrm{OPT}(E_1) = 2$, pour l'entrée E_1. On peut compléter une solution partielle à l'aide de cet algorithme, on a donc défini la fonction `valeur`.

Tentative 2. On résout le problème associé dans $\mathbb{R}$, définit ci-dessous :

$$\text{KNAPSACK}_{\mathbb{R}} \begin{cases}\textbf{Entrée} & : n \in \mathbb{N},\ (v_i)_{i\in[\![1,n]\!]} \in (\mathbb{N}^\star)^n,\ (w_i)_{i\in[\![1,n]\!]} \in (\mathbb{N}^\star)^n,\ \text{et } P \in \mathbb{N}^\star \\ \textbf{Sortie} & : \operatorname{argmax}_{x\in S} \sum_{i=1}^n x_i v_i\end{cases}$$

où $S = \left\{(x_i)_{i\in[\![1,n]\!]} \in [0,1]^n \;\middle|\; \sum_{i=1}^n x_i w_i \leqslant P\right\}$. On résout ce problème à l'aide d'un algorithme glouton.

Algorithme 7.6 Algorithme glouton $\mathscr{G}^{\mathbb{R}}$ répondant au problème $\textsc{Knapsack}_{\mathbb{R}}$

```
1 : S ← 0
2 : i ← 1
3 : x ← (0)_{i∈⟦1,n⟧}
4 : tant que i ⩽ n et S + w_i < P faire
5 :     S ← S + w_i
6 :     x_i ← 1
7 :     i ← i + 1
8 : si i ⩽ n alors
9 :     x_i ← (P − S)/2
10 :    S ← P
11 : retourner x
```

En notant $\mathrm{OPT}(e)$ une solution optimale à Knapsack, et $\mathrm{OPT}^{\mathbb{R}}(e)$ une solution optimale à $\textsc{Knapsack}_{\mathbb{R}}$, on a $\forall e \in \mathscr{C}, \quad \mathrm{OPT}(e) \leqslant \mathrm{OPT}^{\mathbb{R}}(e)$. De plus, à faire à la maison, le glouton $\mathscr{G}^{\mathbb{R}}$ donne la solution optimale : on a $\mathrm{OPT}^{\mathbb{R}}(e) = \mathscr{G}^{\mathbb{R}}(e)$.

On branche sur la partie fractionnaire. On considère l'entrée définie dans la table ci-après, avec $P = 20$.

i	1	2	3	4	5	6
v_i	13	16	19	24	3	5
w_i	6	8	10	14	2	5
$\approx v_i/w_i$	2,2	2	1,9	1,7	1,5	1

Table 7.1 – Entrée du problème Knapsack

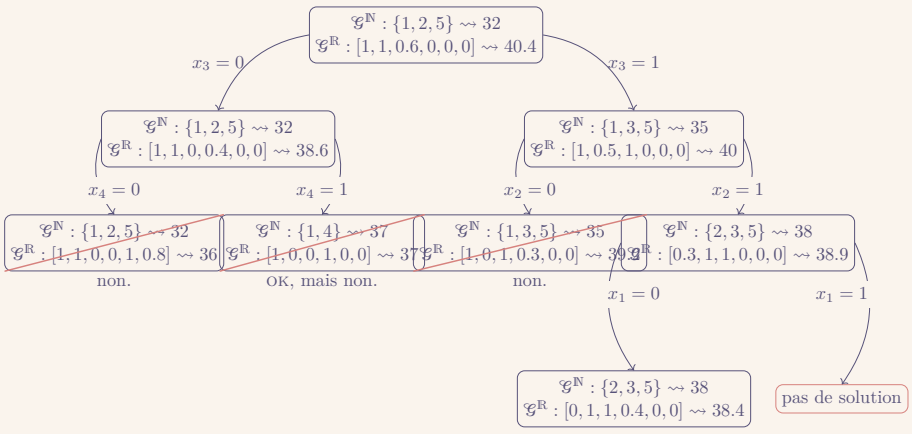


Figure 7.8 – Stratégie *branch and bound* appliquée au problème Knapsack

Annexe 7.A Programmation dynamique

On rappelle le problème KNAPSACK :

$$\begin{cases}\textbf{Entrée} & : n \in \mathbb{N},\ w \in (\mathbb{N}^\star)^n,\ v \in (\mathbb{N}^\star)^n,\ P \in \mathbb{N} \\ \textbf{Sortie} & : \max_{x\in\{0,1\}^n} \big\{ \langle x, v\rangle \ \big|\ \langle x, w\rangle \leqslant P\big\}.\end{cases}$$

On pose

$$\text{SAD}(n, w, v, P) = \max_{x\in\{0,1\}^n} \big\{ \langle x, v\rangle \ \big|\ \langle x, w\rangle \leqslant P\big\},$$

et

$$\text{sol}(n, w, v, P) = \{\langle x, v\rangle \mid \langle x, w\rangle \leqslant P,\ x \in \{0, 1\}^n\}.$$

Lorsque $y \in \mathbb{R}^n$, avec $y = (y_1, \dots, y_n)$, on note $\mathbb{R}^{n-1} \ni \tilde{y} = (y_2, y_3, \dots, 0)$. Ainsi, si $n > 0$,

$$\begin{aligned}\text{sol}(n, w, v, P) &= \{\langle x, v\rangle \mid \langle x, w\rangle \leqslant P,\ x \in \{0, 1\}^n \text{ et } x_1 = 0\} \\ &\quad \cup \{\langle x, v\rangle \mid \langle x, w\rangle \leqslant P,\ x \in \{0, 1\}^n \text{ et } x_1 = 1\} \\ &= \{\langle \tilde{x}, \tilde{v}\rangle \mid \langle \tilde{x}, \tilde{w}\rangle \leqslant P,\ xu \in \{0, 1\}^n \text{ et } x_1 = 0\} \\ &\quad \cup \{v_1 + \langle \tilde{x}, \tilde{v}\rangle \mid \langle \tilde{x}, \tilde{w}\rangle \leqslant P - w_1,\ x \in \{0, 1\}^n \text{ et } x_1 = 1\} \\ &= \{\langle y, \tilde{v}\rangle \mid \langle y, \tilde{w}\rangle \leqslant P \text{ et } y \in \{0, 1\}^{n-1}\} \\ &\quad \cup \{v_1 + \langle y, \tilde{v}\rangle \mid \langle y, \tilde{w}\rangle \leqslant P - w_1 \text{ et } y \in \{0, 1\}^{n-1}\}\end{aligned}$$

D'où, par passage au max, si $n > 0$,

$$\begin{aligned}\text{SAD}(n, w, v, P) = \max(&\\ &\max\{\langle y \mid \tilde{v}\rangle \mid \langle y, \tilde{w}\rangle \leqslant P \text{ et } y \in \{0, 1\}^{n-1}\} \\ &v_1 + \max\{\langle y \mid \tilde{v}\rangle \mid \langle y, \tilde{w}\rangle \leqslant P - w_1 \text{ et } y \in \{0, 1\}^{n-1}\} \\ ) = \max\big(&\text{SAD}(n-1, \tilde{w}, \tilde{v}, P), v_1 + \text{SAD}(n-1, \tilde{w}, \tilde{v}, P - w_1)\big).\end{aligned}$$

Si $n = 0$, alors $\text{SAD}(0, v, w, P) = 0$.

REMARQUE :
Si on le code *tel quel*, il y aura $\mathcal{O}(2^n)$ appels récursifs. Mais, on a $(n+1)(P+1)$ sous-problèmes.

Notons alors, pour n, v, w, P fixés, $(s_{i,j})_{\substack{i\in[\![1,n]\!]\\ j\in[\![0,P]\!]}}$ tel que

$$s_{i,j} = \text{SAD}\Big(n - i, v_{\big|[\![i+1,n]\!]}, w_{\big|[\![i+1,n]\!]}, j\Big).$$

On a alors $\text{SAD}(n, v, w, P) = s_{0,P}$. Ainsi, pour $j \in [\![0, P]\!]$, $s_{n,j} = 0$; pour $i \in [\![0, n]\!]$, $s_{i,0} = 0$;

$$s_{i,j} = \max(s_{i+1,j}, v_{i+1} + s_{i+1,j-w_{i+1}});$$

et, si $w_{i+1} > j$, alors $s_{i,j} = s_{i+1,j}$.

La complexité de remplissage de la matrice est en $\mathcal{O}(n\,P)$ en temps et en espace. On n'a pas prouvé $\mathbf{P} = \mathbf{NP}$, la taille de l'entrée est

— pour un entier n : $\log_2(n)$,
— pour un tableau de n entiers : $n \log_2(n)$,
— pour un tableau de n entiers : $n \log_2(n)$,
— pour un entier P : $\log_2(P)$.

Vis à vis de la taille de l'entrée, la complexité de remplissage est exponentielle.

Chapitre 8

Jeux

Dans ce chapitre, on s'intéresse à la théorie des jeux. L'objectifs est de modéliser des interactions (économie, coopération, ...). On s'intéressera, par contre, à une petite partie de la théorie des jeux : les jeux d'accessibilité. Par exemple, les échecs et le go sont deux jeux d'accessibilité, mais on s'intéressera à des jeux beaucoup plus simples. On cherchera les stratégies gagnantes pour ces jeux, des heuristiques. On raccrochera ce chapitre avec la théorème des graphes.

Par exemple, on peut coder un programme répondant, *plus ou moins correctement*, au jeu puissance 4. [Démonstration d'un jeu de puissance 4.]

Dans un premier temps, on s'intéresse à un jeu simple. On a 13 allumettes :

| | | | | | | | | | | | | |.

On peut retirer une, deux ou trois allumettes. Le joueur retirant la dernière allumette perd. On peut représenter le jeu par un graphe, et *jouer* au jeu est se déplacer dans ce graphe. Ce graphe est *biparti*.

IV.1 Jeux sur un graphe

Définition : On appelle *arène* la donnée
- d'un graphe biparti orienté $G = (V, E)$, avec $V = V_A \uplus V_B$ la séparation en deux sommets de ce graphes bipartis ;
- d'un sommet initial s.

Définition : Un état du jeu (un sommet de l'arène) est dit *terminal* lorsqu'il n'a pas de successeurs. On note, dans la suite, $V_A^\star$ et $V_B^\star$ les états non terminaux (notation non officielle).

Remarque :
Les états V_A sont les états où c'est à Alice de jouer. Les états V_B sont les états

où c'est à Bob de jouer.

Exemple :
On reprend l'exemple du jeu des allumettes. La figure ci-dessus représente les états du jeu. Les états (i) représentent les états de Alice (*i.e.* des éléments de V_A), les états $\boxed{j}$ représentent les états de Bob (*i.e.* des éléments de V_B). Les états doublement encadrés sont terminaux, les autres sont non terminaux.

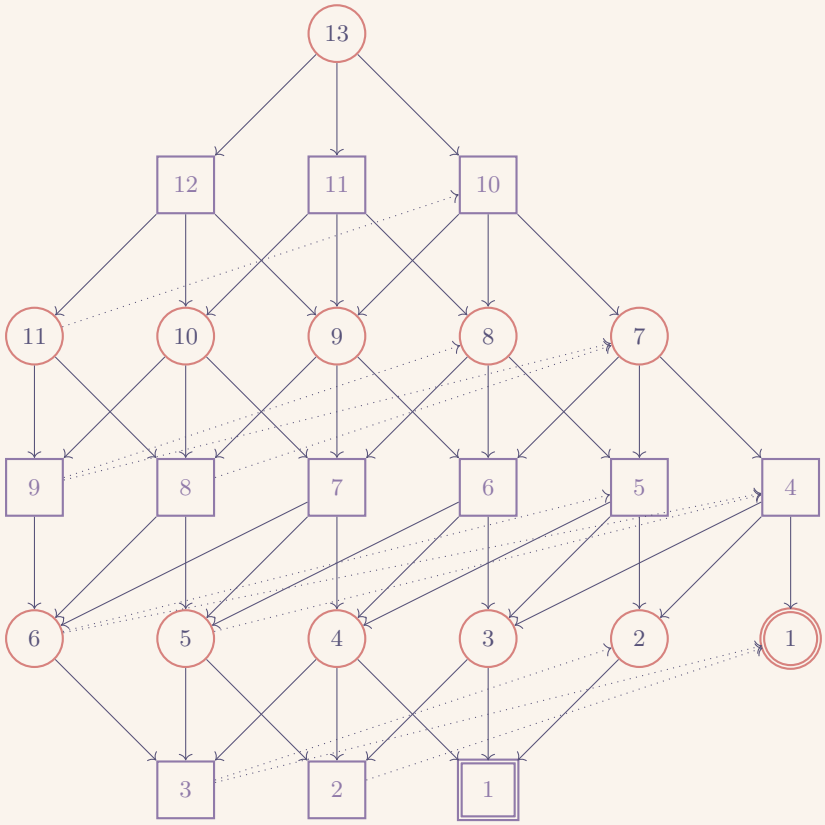


Figure 8.1 – États du jeu des allumettes

Définition : Un *jeu d'accessibilité* est déterminé par une arène $G = (V_A \uplus V_B, E)$ de sommet initial s, et deux ensembles $\mathcal{O}_A$ et $\mathcal{O}_B$ de sommets terminaux tels que

- $\mathcal{O}_A \cap \mathcal{O}_B = ,$
- $\mathcal{O}_A \subseteq V_A \uplus V_B,$
- et $\mathcal{O}_B \subseteq V_A \uplus V_B.$

L'ensemble $\mathcal{O}_A$ représente les sommets « *gagnants* » pour Alice. L'ensemble $\mathcal{O}_B$ représente les sommets « *gagnants* » pour Bob.

Remarque :

Ils ne forment pas nécessairement une partition des sommets terminaux.

Exemple :
Dans la figure 8.1, l'état gagnant pour Alice est ⓵ ; celui de Bob est 1.

Définition : Une *partie depuis un sommet* s dans un jeu d'accessibilité est une suite (finie ou infinie) de sommets formant un chemin dans l'arène, partant de s, telle que, si la partie est finie, le dernier sommet est terminal.

On dit d'une partie

- qu'elle est *gagnée par Alice* si elle est finie et le dernier sommet est dans $\mathcal{O}_A$;
- qu'elle est *gagnée par Bob* si elle est finie et le dernier sommet est dans $\mathcal{O}_B$;
- qu'elle est nulle sinon.

Exemple :
À faire : Ajouter exemple ?

Définition : On appelle *stratégie pour Alice* une fonction $f : V_A^\star \to V_B$ telle que, pour tout état $s_A \in V_A^\star$, on a $\big(s_A, f(s_A)\big) \in E$.

Soit $N \in \mathbb{N} \cup \{+\infty\}$ la longueur d'une partie $(s_1, s_2, \dots, s_n, \dots, s_N ?)$, cette partie est dite *jouée selon une stratégie* f si

$$\forall i \in [\![1, N+1[\![, \quad s_i \in V_A^\star \implies s_{i+1} = f(s_i).$$

Une stratégie pour Alice est dit *gagnante depuis un état* s dès lors que toute partie depuis s jouée selon f est gagnée par Alice. Plus généralement, une stratégie est dit *gagnante* si elle est gagnante depuis l'état initial.

On appelle *stratégie pour Bob* une fonction $f : V_B^\star \to V_B$ telle que, pour tout état $s_B \in V_B^\star$, on a $\big(s_B, f(s_B)\big) \in E$.

Soit $N \in \mathbb{N} \cup \{+\infty\}$ la longueur d'une partie $(s_1, s_2, \dots, s_n, \dots, s_N ?)$, cette partie est dite *jouée selon une stratégie* f si

$$\forall i \in [\![1, N+1[\![, \quad s_i \in V_B^\star \implies s_{i+1} = f(s_i).$$

Une stratégie pour Bob est dit *gagnante depuis un état* s dès lors que toute partie depuis s jouée selon f est gagnée par Bob.

Exemple :
La stratégie $\Rightarrow$ est gagnante pour Bob.

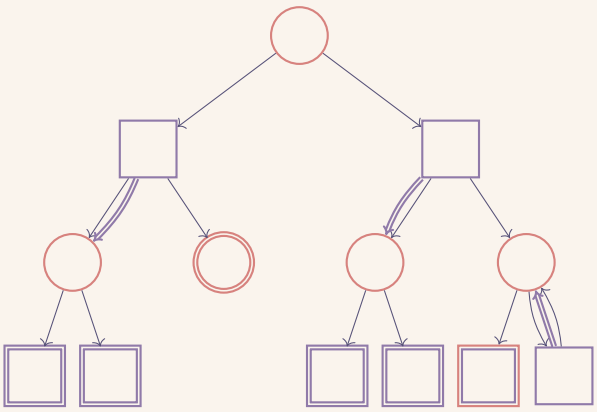


FIGURE 8.2 – Stratégie gagnante pour Bob

Interlude : représentation machine des jeux. On représente le graphe de manière implicite.

```
type joueur
type etat

val joueur : etat -> move
val possibilite_moves : etat -> etat list
val init : etat
val est_gagant : etat -> joueur option
```

CODE 8.1 – Représentation machine des jeux, types

```
type joueur = Alice | Bob
type etat = { allu : int; joueur : joueur }

let autre = function
| Alice -> Bob
| Bob -> Alice

let joueur (e: etat) = e.joueur
let init = { allu = 13; joueur = Alice }
let est_gagnant (e: etat) =
  if e.allu = 1 then Some(autre e.joueur)
  else None
let possible_moves (e: etat) =
  (if e.allu > 3 then
    [{ allu = e.allu - 3; joueur = autre e.joueur }]
      ↪ else [])
  @ (if e.allu > 2 then
    [{ allu = e.allu - 2; joueur = autre e.joueur }]
      ↪ else [])
  @ (if e.allu > 1 then
    [{ allu = e.allu - 1; joueur = autre e.joueur }]
      ↪ else [])
```

CODE 8.2 – Représentation machine du jeux des allumettes

Avec une représentation implicite du graphe, on ne stocke pas l'entièreté du graphe directement mais on ne récupère que les successeurs d'un sommet en particulier.

Par exemple, pour écrire un moteur de recherche, on utilise aussi une représentation implicite pour le graphe *internet* ; on ne peut pas *juste* télécharger l'entièreté du graphe.

Attracteur.

Remarque :
On suppose que les deux joueurs (Alice et Bob) jouent intelligemment. On se met à la place d'Alice. Bob joue le "mieux" pour lui, et le "pire" pour nous. Nous jouerons le "mieux" pour nous. Ainsi, Bob jouera vers un état de valeur minimale, nous jouerons vers un état de valeur maximale.

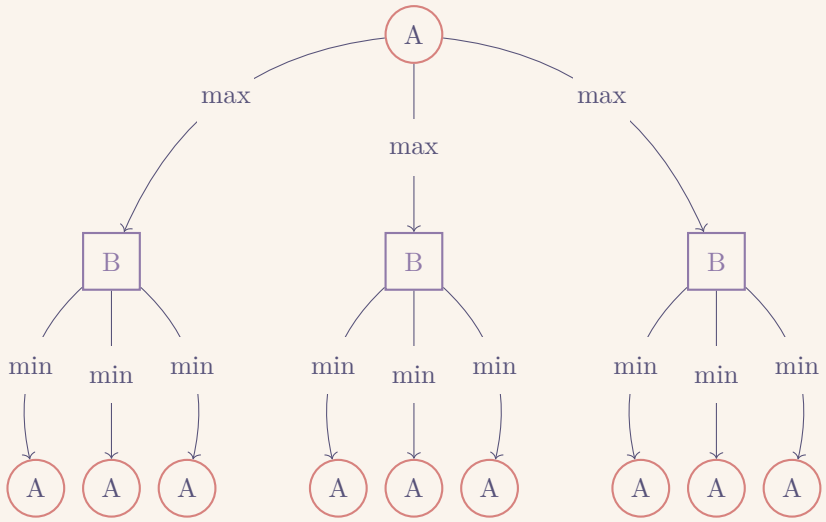


Figure 8.3 – Stratégie de minimisation pour Bob, et de maximisation pour Alice

Définition : On définit la suite d'ensembles $(\mathscr{A}_i)_{i\in\mathbb{N}}$ par $\mathscr{A}_0 = \mathcal{O}_\mathrm{A}$, et, pour tout $n \in \mathbb{N}$,

$$\begin{aligned}\mathscr{A}_{n+1} = \mathscr{A}_n \cup \{s_\mathrm{B} \in V_\mathrm{B}^\star \mid \forall s_\mathrm{A} \in \mathrm{succ}(s_\mathrm{B}),\ s_\mathrm{A} \in \mathscr{A}_n\} \\ \cup \{s_\mathrm{A} \in V_\mathrm{A}^\star \mid \exists s_\mathrm{B} \in \mathrm{succ}(s_\mathrm{A}),\ s_\mathrm{B} \in \mathscr{A}_n\}.\end{aligned}$$

On a appelle alors *attracteur d'Alice* les états $\mathscr{A} = \bigcup_{n\in\mathbb{N}} \mathscr{A}_n$.

Remarque :
La suite des $(\mathscr{A}_n)_{n\in\mathbb{N}}$ est croissante pour l'inclusion $\subseteq$, et ultimement stationnaire car le graphe est fini :

$$\exists N \in \mathbb{N},\ \forall n \geqslant N, \qquad \mathscr{A}_n = \mathscr{A}_N.$$

De même, on définit la suite d'ensembles $(\mathscr{B}_n)_{n\in\mathbb{N}}$ et l'ensemble $\mathscr{B}$ des attracteurs de Bob, en permutant les deux joueurs dans la définition précédente.

Exemple :
À faire : Ajouter exemple, *c.f. cahier de prépa* Si Bob joue intelligemment, il est garanti de gagner.

Remarque :
On remarque que les ensembles $\bigcup_{n\in\mathbb{N}}\mathscr{A}_n$ et $\bigcup_{n\in\mathbb{N}}\mathscr{B}_n$ ne forment pas une partition de l'ensemble des états : l'intersection est bien vide, mais l'union de ces deux ensembles ne couvre pas l'ensemble des états.

Définition (Stratégie induite par les attracteurs) **:** Soit $\mathscr{A}$ l'ensemble des attracteurs d'Alice. On définit la stratégie suivante

$$f : V_{\mathrm{A}}^{\star} \longrightarrow V_{\mathrm{B}}$$
$$s_{\mathrm{A}} \longmapsto \begin{cases} s_{\mathrm{B}} \in \mathrm{succ}(s_{\mathrm{A}}) \cap \mathscr{A} & \text{si } s_{\mathrm{A}} \in \mathscr{A} \\ s_{\mathrm{B}} \in \mathrm{succ}(s_{\mathrm{A}}) \text{ quelconque} & \text{sinon.} \end{cases}$$

Cette stratégie est nommée *stratégie induite par les attracteurs.*

Définition : Soit $s \in \mathscr{A}$ un attracteur. On appelle *rang* de s, notée $\mathrm{rg}(s)$ l'entier

$$\mathrm{rg}(s) = \min\{n \in \mathbb{N} \mid s \in \mathscr{A}_n\}.$$

Lemme : Pour tout entier n, pour tout état $s \in \mathscr{A}_n$, un des trois cas est vrai :

- $s \in \mathcal{O}_{\mathrm{A}}$;
- $n > 0$, $s \in V_{\mathrm{A}}^{\star}$ et il existe $s_{\mathrm{B}} \in \mathrm{succ}(s)$ tel que $s_{\mathrm{B}} \in \mathscr{A}_{n-1}$;
- $n > 0$, $s \in V_{\mathrm{B}}^{\star}$ et pour tout $s_{\mathrm{A}} \in \mathrm{succ}(s)$, $s_{\mathrm{A}} \in \mathscr{A}_{n-1}$.

Preuve :
Par récurrence.

- Si $n = 0$, alors $\mathscr{A}_0 = \mathcal{O}_{\mathrm{A}}$.
- Supposons la propriété vraie au rang n. Soit $s \in \mathscr{A}_{n+1}$. Alors,
  - ou bien $s \in \mathscr{A}_n$, et on conclut par hypothèse de récurrence.
  - ou bien $s \in V_{\mathrm{A}}^{\star}$, et il existe $s_{\mathrm{B}} \in \mathrm{succ}(s)$ tel que $s_{\mathrm{B}} \in \mathscr{A}_n$, alors OK ;
  - ou bien $s \in B_{\mathrm{B}}^{\star}$, et pour tout $s_{\mathrm{A}} \in \mathrm{succ}(s)$, $s_{\mathrm{A}} \in \mathscr{A}_n$, alors OK.

□

Proposition : On a $\mathscr{A} \cap \mathscr{B} = .$

Preuve :
Montrons par récurrence que, pour tout entier n, $\mathscr{A}_n \cap \mathscr{B}_n = .$ À faire : finir cette partie de la preuve. Soit $N \in \mathbb{N}$ tel que $\mathscr{A}_n = \mathscr{A}_N$, pour tout $n \geqslant N$. Soit $M \in \mathbb{N}$ tel que $\mathscr{B}_n = \mathscr{B}_M$, pour tout $n \geqslant M$. Ainsi, $\mathscr{A} = \mathscr{A}_N$ et $\mathscr{B} = \mathscr{B}_M$. On pose $K = \max(M, N)$, et on a donc

$$\mathscr{A} \cap \mathscr{B} = \mathscr{A}_K \cap \mathscr{B}_K = .$$

□

Proposition : Si f est une stratégie induite par les attracteurs d'Alice $\mathscr{A}$, et que $s \in \mathscr{A}$, alors toute partie jouée selon f depuis s est gagnante pour Alice.

Preuve :
Soit $(s_n)_{n \in [\![1, N+1[\![}$, avec $N \in \mathbb{N} \cup \{+\infty\}$, une partie jouée selon f depuis s.

- Montrons $\forall n \in [\![1, N+1[\![$, $s_n \in \mathscr{A}$. Par récurrence. On a $s_1 = s \in \mathscr{A}$, d'où l'initialisation. Si la propriété est vraie au rang $n \in [\![1, N[\![$ (ainsi s_{n+1} existe),
  - si $s_n \in V_{\mathrm{A}}^\star$, alors $s_{n+1} = f(s_n) \in \mathrm{succ}(s_n) \cap \mathscr{A}$ donc $s_{n+1} \in \mathscr{A}$,
  - si $s_n \in V_{\mathrm{B}}^\star$, on a $s_n \in \mathscr{A}$ et $s_{n+1} \in \mathrm{succ}(s_n)$, d'où $s_{n+1} \in \mathscr{A}$.

  Concluant ainsi la récurrence.
- Montrons que $N \neq +\infty$. En effet, montrons que, $\forall n \in [\![1, N[\![$, $\mathrm{rg}(s_{n+1}) < \mathrm{rg}(s_n)$. L'état $s_n \in \mathscr{A}$, son rang est bien défini. De plus, $s_n \in \mathscr{A}_r$, où $r = \mathrm{rg}(s_n)$. Or, $s_n \notin \mathcal{O}_{\mathrm{A}}$. D'après le lemme, $s_{n+1} \in \mathscr{A}_{r-1}$, donc $\mathrm{rg}(s_{n+1}) \leqslant r - 1 < r$. Ainsi, $N \neq +\infty$ par existence du variant, comme l'ensemble ordonné $(\mathbb{N}, \leqslant)$ est bien fondé.

Ainsi, $(s_n)_{n \in [\![1, N+1[\![}$ est une partie finie, et $\forall n \in [\![1, N]\!]$, $s_n \in \mathscr{A}$. L'état s_N est terminal, et donc $s_N \in \mathcal{O}_{\mathrm{A}}$, d'où le résultat. □

Proposition : Soit s un sommet admettant une stratégie gagnante pour Alice. Alors, s est un attracteur : $s \in \mathscr{A}$.

Preuve :
Montrons par récurrence forte : « si s est un sommet admettant une stratégie gagnante f et que toute partie jouée depuis s selon f est de longueur au plus n, alors $s \in \mathscr{A}_n$. »

— Si le sommet s admet une stratégie gagnante, et toute partie depuis s est de longueur 0, alors $s \in \mathcal{O}_A = \mathcal{A}_0$.
— Supposons, pour tout $k \in [\![1, n]\!]$, l'hypothèse de récurrence. Montrons la propriété pour $n+1$. Soit s admettant une stratégie gagnante f et tel que toute partie jouée depuis s selon f est de longueur au plus $n+1$.
  — Si $s \in V_B$, alors
    — si s est terminal, $s \in \mathcal{O}_A \subseteq \mathcal{A}$.
    — sinon, soit $s_1 \in \text{succ}(s)$. Soit γ une partie jouée selon f depuis s_1. γ est une partie jouée selon f depuis s, elle est donc gagnante et de longueur au plus $n+1$. Alors γ est gagnante et de longueur au plus n donc s_1 vérifie les prémisses de l'hypothèse de récurrence, et donc $s_1 \in \mathcal{A}_n$. Ceci étant vrai pour tout $s_1 \in \text{succ}(s)$, on a $s \in \mathcal{A}_{n+1}$.
  — Si $s \in V_A$, alors
    — si s est terminal, alors $s \in \mathcal{O}_A \subseteq \mathcal{A}$.
    — sinon, soit $s_1 = f(s)$, alors s_1 admet une stratégie gagnante (f), et toute partie jouée depuis s_1 est de longueur, au plus, n. L'état s_1 vérifie donc les prémisses l'hypothèse de récurrence. Ainsi $s_1 \in \mathcal{A}_n$, et donc s a un successeur dans $\mathcal{A}_n$. On en déduit $s \in \mathcal{A}_{n+1}$.

Soit alors s admettant une stratégie gagnante f. Ainsi, toute partie jouée depuis s selon f est finie. On peut donc conclure grâce à la démonstration par récurrence ci-avant. □

En pratique, la détermination des attracteurs nécessite une quantité bien trop importante de calculs. On souhaite revenir à une idée développée précédemment : réaliser un min-max. Mais, pour cela, il est nécessaire de donner une notion de « valeur » a chaque état du jeu. On définit donc une *fonction d'heuristique* qui, à un état, associé sa valeur. Le choix de cette fonction reste, cependant, très subjectif.

IV.2 Résolution par heuristique

On suppose définie une *fonction d'heuristique* h de la forme :

$$h : \underset{\text{joueur}}{\{A, B\}} \times \underset{\text{états}}{V} \to \overbrace{\mathbb{Z} \cup \{+\infty, -\infty\}}^{\bar{\mathbb{Z}}}.$$

On représente informatiquement l'ensemble $\bar{\mathbb{Z}}$ par le type OCaml `int_bar` défini ci-dessous

```
type int_bar =
  | PInt
  | NInt
  | F of int
```

CODE 8.3 – Type `int_bar` représentant un élément l'ensemble $\bar{\mathbb{Z}}$

On peut donc définir l'algorithme MINMAX.

Algorithme 8.1 Algorithme MINMAX

Entrée Un état e, un seuil de profondeur d, le joueur j
Sortie Un score

```
si succ(e) = ∅ alors
    si e ∈ 𝒪_j alors
        retourner +∞
    sinon si e ∈ 𝒪_autre(j) alors
        retourner −∞
    sinon
        retourner 0
sinon si d = 0 alors
    retourner h(j, e)
sinon
    si j = joueur(e) alors
        retourner max{MinMax(e', d − 1, j) | e' ∈ succ(e)}
    sinon
        retourner min{MinMax(e', d − 1, j) | e' ∈ succ(e)}
```

EXEMPLE :
c.f. cahier-de-prépa On applique l'algorithme MINMAX pour Alice.

EXEMPLE (TD 13. Exercice 4) :

On peut améliorer l'algorithme MINMAX avec « l'élagage α, β. »

Algorithme 8.2 Algorithme MinMax avec élagage α, β

Entrée Un état e, un seuil de profondeur d, le joueur j, et $\alpha, \beta \in \bar{\mathbb{Z}}$
Sortie Un score dans $[\alpha, \beta]$

```
si succ(e) = alors
    si e ∈ 𝒪_j alors
        retourner β
    sinon si e ∈ 𝒪_autre(j) alors
        retourner α
    sinon
        si β ⩽ 0 alors retourner β
        sinon si α ⩾ 0 alors retourner α
        sinon retourner 0
sinon si d = 0 alors
    si h(j, e) ⩾ β alors retourner β
    sinon si h(j, e) ⩽ α alors retourner α
    sinon retourner h(j, e)
sinon
    si joueur(e) = j alors
        v ← α
        pour e' ∈ succ(e) faire
            v ← max(v, MinMaxÉlagué(e', d − 1, j, v, β))
            si v ⩾ β alors
                retourner β
        retourner v
    sinon
        u ← β
        pour e' ∈ succ(e) faire
            u ← min(u, MinMaxÉlagué(e', d − 1, j, α, u))
            si u ⩽ α alors
                retourner α
        retourner u
```

Chapitre 9

Grammaires non contextuelles

Ce chapitre se rattache à la branche de l'informatique des langages formels. On l'a étudié au chapitre 1 avec les automates, et au chapitre 4 avec les machines. Pour le moment, nous avons 5 classes de langages : (1) les langages finis, (2) les langages locaux, (3) les langages réguliers, (4) les langages décidables en temps polynomial, (5) les langages décidables. L'objectif de ce chapitre se situe entre les points (3) et (4).

Intéressons-nous à un langage particulier, le langage des programmes OCaml avec une syntaxe valide. Ce langage est il régulier ? Non. On peut considérer l'expression

$$e_n = \text{« } \underbrace{((\cdots(}_{n}0\underbrace{)\cdots))}_{n} \text{ »}$$

qui est une expression OCaml valide. Par application du lemme de l'étoile, il n'est pas reconnaissable par un automate à N états en considérant e_{N+1}.

L'ensemble $\mathscr{B}$ des mots bien parenthésés est le plus petit ensemble tel que

— $\varepsilon \in \mathscr{B}$
— si $u \in \mathscr{B}$ et $v \in \mathscr{B}$, alors $u \cdot v \in \mathscr{B}$
— si $u \in \mathscr{B}$, alors $(\cdot u \cdot) \in \mathscr{B}$.

Une telle définition de langage est appelée une grammaire. Un autre exemple de langage est la grammaire de la langue française :

— phrase : sujet + verbe + complément,
— complément : COD + complément,
— complément : CCL + complément,
— complément : ε.

Avec cette définition [1], on peut reconnaître des phrases simples comme

$$\text{« } \underbrace{\text{Matthieu}}_{\text{sujet}}\ \underbrace{\text{aime}}_{\text{verbe}}\ \underbrace{\text{les trains}}_{\text{complément}}\ \text{. »}$$

1. On néglige les règles manquantes à cette définition de la grammaire française.

IV.1 Définition, vocabulaire, propriétés

IV.1.1 Grammaires non contextuelles

Définition : On se munit d'un alphabet Σ qu'on appelle *terminaux*. On se munit d'un ensemble de symboles $\mathscr{V}$ qu'on appelle *non-terminaux*. On suppose $\mathscr{V} \cap \Sigma$.

Exemple :
Dans la suite, on pose $\Sigma = \{(,)\}$ et $\mathscr{V} = \{\mathrm{B}\}$.

Définition : On appelle *règle de production* la donnée
- d'un symbole $V \in \mathscr{V}$,
- d'un mot $w_1 w_2 \dots w_n$ sur l'alphabet $\mathscr{V} \cup \Sigma$,

que l'on note $V \to w_1 w_2 \dots w_n$.

Exemple :
L'ensemble $\mathscr{B}$ est décrit par les règles
- $\mathrm{B} \to \varepsilon$,
- $\mathrm{B} \to \mathrm{BB}$,
- $\mathrm{B} \to (\mathrm{B})$.

Définition (Grammaire non contextuelle) **:** Une *grammaire non contextuelle* est la donnée de
- un alphabet de non-terminaux $\mathscr{V}$,
- un alphabet de terminaux Σ,[2]
- un ensemble fini de règles de production P,
- un symbole initial $S \in \mathscr{V}$,

que l'on note $(\mathscr{V}, \Sigma, P, S)$.

Exemple :
On note dans la suite

$$\mathscr{G} = \big(\{\mathrm{B}\}, \{(,)\}, \{\mathrm{B} \to \varepsilon, \mathrm{B} \to \mathrm{BB}, \mathrm{B} \to (\mathrm{B})\}, \mathrm{B}\big).$$

Interlude. Avec cette définition, on espère pouvoir appliquer ces règles pour définir des mots valides. Par exemple,

$$\mathrm{B} \overset{?}{\rightsquigarrow} \mathrm{BB} \overset{?}{\rightsquigarrow} (\mathrm{B})\mathrm{B} \overset{?}{\rightsquigarrow} (\mathrm{B})(\mathrm{B}) \overset{?}{\rightsquigarrow} (\mathrm{BB})(\mathrm{B}) \overset{?}{\rightsquigarrow} (\mathrm{BB})() \overset{?}{\rightsquigarrow} (\mathrm{B})() \overset{?}{\rightsquigarrow} ((\mathrm{B}))() \overset{?}{\rightsquigarrow} (())().$$

C'est l'objectif de la sous-section suivante.

2. avec "terminaux/non-terminaux" vient l'implication que $\mathscr{V} \cap \Sigma =$

IV.1.2 Dérivation

Définition (Dérivation immédiate) **:** Soit $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$ une grammaire. Soient u et v deux mots de $(\Sigma \cup \mathcal{V})^\star$. On dit que v *dérive immédiatement* de u dans la grammaire $\mathcal{G}$, que l'on note $u \Rightarrow v$, si

— il existe x et y deux mots de $(\Sigma \cup \mathcal{V})^\star$

— il existe $(V \to w_1 w_2 \dots w_n) \in P$

tels que $u = x \cdot V \cdot y$ et $v = x \cdot w_1 w_2 \dots w_n \cdot y$.

Exemple :
Ainsi, $u \Rightarrow v$.

Lemme (de composition) **:** Soit $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$ une grammaire. Soient $u, v \in (\Sigma \cup \mathcal{V})^\star$ tels que $u \Rightarrow v$. Soit $w \in (\Sigma \cup \mathcal{V})^\star$. On a $u \cdot w \Rightarrow v \cdot w$ et $w \cdot u \Rightarrow w \cdot v$.

Preuve :
À faire à la maison. □

On propose trois définitions différentes mais équivalentes pour la dérivation $\overset{\star}{\Rightarrow}$.

Définition : Étant donné une grammaire $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$, on étend $\Rightarrow$ en sa cloture réflexive et transitive, que l'on note $\overset{\star}{\Rightarrow}$, appelé *dérivation.*

Définition : On définit $\overset{\star}{\Rightarrow}$ comme $u \overset{\star}{\Rightarrow} v \overset{\text{def.}}{\iff} \exists n \in \mathbb{N}, \exists (u_0, u_1, \dots, u_n) \in \big((\mathcal{V} \cup \Sigma)^\star\big)^{n+1}$ tels que $u_0 = u$, $u_n = v$ et $\forall i \in [\![0, n-1]\!]$, $u_i \Rightarrow u_{i+1}$.

Définition : Soit la suite $(\Rightarrow^n)_{n \in \mathbb{N}}$ définie inductivement par

— $u \Rightarrow^0 v \overset{\text{def.}}{\iff} u = v$,

— $u \Rightarrow^{n+1} v \overset{\text{def.}}{\iff} u \Rightarrow^n v$ ou $\exists w \in (\Sigma \cup \mathcal{V})^\star$, $u \Rightarrow w$ et $w \Rightarrow^n v$.

On pose alors $\overset{\star}{\Rightarrow} = \bigcup_{n \in \mathbb{N}} \Rightarrow^n$.

Lemme (de composition*) **:** Soit $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$ une grammaire, et soient $u, v \in (\Sigma \cup \mathcal{V})^\star$ tels que $u \Rightarrow^p v$, pour $p \in \mathbb{N}$. Et, soient $(w, t) \in (\Sigma \cup \mathcal{V})^2$ tels que $w \Rightarrow^q t$, pour $q \in \mathbb{N}$. Alors, $uw \Rightarrow^{p+q} vt$.

Preuve :
Soit $u_0u_1\dots u_p$ tels que $u_0 = u$, $u_p = v$ et $\forall i \in [\![0, p-1]\!]$, $u_i \Rightarrow u_{i+1}$. Soit $w_0w_1\dots w_n$ tels que $w_0 = w$, $w_q = t$ et $\forall i \in [\![0, q-1]\!]$, $w_i \Rightarrow w_{i+1}$. Soit alors la dérivation

$$uw = u_0w \Rightarrow u_1w \Rightarrow u_2w \Rightarrow \cdots \Rightarrow u_pw \Rightarrow u_pw_1 \Rightarrow u_pw_2 \Rightarrow \cdots \Rightarrow u_pw_q = vt.$$

On a donc $uw \Rightarrow^{p+q} vt$. □

Définition : Soit $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$ une grammaire. Son langage est défini par

$$\mathcal{L}(\mathcal{G}) = \{u \in \Sigma^\star \mid S \overset{\star}{\Rightarrow} u\}.$$

Exemple :
Dans l'exemple précédent, on a

$$\mathcal{L}(\mathcal{G}) = \mathcal{B}.$$

Interlude : grammaires contextuelles. Dans une grammaire contextuelle, une règle de production peut-être de la forme $b\mathrm{B} \to a\mathrm{B}a\mathrm{B}$, où $\Sigma = \{a, b\}$. Ces règles dépendent du contexte, et non juste des symboles.

Lemme (de décomposition) **:** Étant donnée une grammaire non contextuelle $(\mathcal{V}, \Sigma, P, S)$, soit $w = w_1\dots w_n$ un mot de n lettres tel qu'il existe $p \in \mathbb{N}$ et $v \in (\Sigma \cup \mathcal{V})^\star$ tel que $w \Rightarrow^p v$ alors il existe $\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_n \in (\Sigma \cup \mathcal{V})^\star$ et $p_1, \dots, p_n \in \mathbb{N}$ tels que $w_1 \Rightarrow^{p_1} \tilde{v}_1$, $w_2 \Rightarrow^{p_2} \tilde{v}_2$, $\dots$, $w_n \Rightarrow^{p_n} \tilde{v}_n$, et $v = \tilde{v}_1 \cdots \tilde{v}_n$, et $\sum_{i=1}^n p_i = p$.

Preuve :
On procède par récurrence sur $p \in \mathbb{N}$.

- **cas de base ($p = 0$).** On a $w_1w_2\dots w_n \Rightarrow^0 v$, d'où $v = w_1w_2\dots w_n$. On choisit donc $\tilde{v}_i = w_i$ et $p_i = 0$ pour tout $i \in [\![1, n]\!]$. On a alors, pour tout $i \in [\![1, n]\!]$, $w_i \Rightarrow^0 \tilde{v}_i$, et $v = \tilde{v}_1\dots\tilde{v}_n$ et $\sum_{i=1}^n p_i = 0 = p$.
- **hérédité.** Soit $w \Rightarrow w_1\dots w_{q-1}u_1u_2\dots u_rw_{q+1}\dots w_n \Rightarrow^{p-1} v$, où $(w_q \to u_1\dots u_r) \in P$. Soit donc, par hypothèse de récurrence, $\hat{v}_1, \hat{v}_2, \dots, \hat{v}_{n-1+r}$ tels que
  - $\forall i \in [\![1, q_1]\!]$, $w_i \Rightarrow^{s_i} \hat{v}_i$,
  - $\forall i \in [\![1, r]\!]$, $u_i \Rightarrow^{s_{i+q-1}} \hat{v}_{i+q-1}$,
  - $\forall i \in [\![q+1, n]\!]$, $w_i \Rightarrow^{s_{i+r-1}} \hat{v}_{i+r-1}$,
  - et $\sum_{i=1}^{n-1+r} s_i = p - 1$.

  On pose alors, pour tout $i \in [\![1, q-1]\!]$, $\tilde{v}_i = \hat{v}_i$, $\tilde{v}_q = \hat{v}_q\hat{v}_{q+1}\cdots\hat{v}_{q+r-1}$,

et pour tout $i \in [\![q+1, n]\!]$, $\tilde{v}_i = \hat{v}_{i+r-1}$. On pose aussi, pour $i \in [\![1, q-1]\!]$, $p_i = s_i$, puis $p_q = 1 + \sum_{i=1}^{r} s_{i+q-1}$, et, pour $i \in [\![q+1, n]\!]$, $p_i = s_{i+r-1}$.

On a clairement $v = \tilde{v}_1\tilde{v}_2\cdots\tilde{v}_n$. De plus, $\sum_{i=1}^{n} p_i = \left(\sum_{i=1}^{n+r-1} s_i\right) + 1 = (p-1)+1 = p$. Et surtout, pour $i \in [\![1, q-1]\!]$, $w_i \Rightarrow^{s_i} \hat{v}_i$ donc $w_i \Rightarrow^{p_i} \tilde{v}_i$. Ainsi,

$$w_q \Rightarrow u_1 \dots u_r \Rightarrow^{\sum_{i=1}^{r} s_{i+q-1}} \underbrace{\hat{v}_q \dots \hat{v}_{q+r-1}}_{\tilde{v}_q},$$

donc $w_q \Rightarrow^{p_q} \tilde{v}_q$ et, pour $i \in [\![q+1, n]\!]$, $w_i \Rightarrow^{s_{i+r-1}} \hat{v}_{r+r-1}$ et $w_i \Rightarrow^{p_i} \tilde{v}_i$.

□

IV.1.3 Preuves par induction

Proposition (principe d'induction) **:** Étant donnée une grammaire $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$, et un non-terminal $V \in \mathcal{V}$, on note localement $V_\downarrow = \{w \in \Sigma^\star \mid V \overset{\star}{\Rightarrow} w\}$.[3] Soit alors un ensemble de propriétés $\mathcal{P}_V$ pour $V \in \mathcal{V}$, tel que, $\forall (V \to w_1 w_2 \dots w_n) \in P$, $\forall (\hat{w}_1, \hat{w}_2, \dots, \hat{w}_m) \in (\Sigma^\star)^m$

$$\left(\forall i \in [\![1, m]\!], \begin{cases} w_i \in \Sigma \implies \hat{w}_i = w_i \\ w_i \in \mathcal{V} \implies \hat{w}_i \text{ vérifie } \mathcal{P}_{w_i} \end{cases}\right) \implies \hat{w}_i \dots \hat{w}_n \text{ vérifie } \mathcal{P}_V,$$

alors pour tout $V \in \mathcal{V}$, $V_\downarrow$ vérifie $\mathcal{P}_V$.

Exemple :
On considère $\mathcal{G}$ la grammaire

$$\mathcal{G} = \big(\{\mathrm{P}, \mathrm{I}, \mathrm{X}\}, \{a\}, \{\mathrm{P} \to \varepsilon, \mathrm{I} \to a, \mathrm{P} \to a\mathrm{P}a, \mathrm{I} \to a\mathrm{I}a, \mathrm{X} \to \mathrm{IPI}\}, \mathrm{X}\big).$$

On pose les propriétés $\mathcal{P}_\mathrm{P}(w)$: « $|w|$ est pair » ; $\mathcal{P}_\mathrm{I}(w)$: « $|w|$ est impair » ; et, $\mathcal{P}_\mathrm{X}(w)$: « $|w|$ est pair. »

- **cas P $\to \varepsilon$.** Le mot ε est de taille pair donc $\mathcal{P}_\mathrm{P}(\varepsilon)$ est vrai.
- **cas I $\to a$.** $|a|$ est impair donc $\mathcal{P}_\mathrm{I}(a)$ est vrai.
- **cas P $\to a$Pa.** Soit donc $w = aw'a$ avec w' vérifiant $\mathcal{P}_\mathrm{P}$. Alors, $|w| = 2 + |w'|$ qui est pair.
- **cas I $\to a$Ia.** Soit donc $w = aw'a$ avec w' vérifiant $\mathcal{P}_\mathrm{I}$. Alors, $|w| = 2+|w'|$ qui est impair.
- **cas X $\to$ IPI.** Soit donc $w = xyz$, avec x et z vérifiant $\mathcal{P}_\mathrm{I}$, et y vérifiant $\mathcal{P}_\mathrm{P}$. Alors, $|w| = |x| + |y| + |z|$, qui est pair.

3. Avec cette définition, $\mathscr{L}(\mathcal{G}) = S_\downarrow$.

IV.1.4 Définitions équivalentes

Comment représenter une dérivation en machine ? On considère les règles de production $\mathrm{X} \to \mathrm{XX}$ et $\mathrm{X} \to a$. On peut, par exemple, représenter une dérivation par un ensemble de possibilités :

$$\mathrm{X} \Rightarrow \mathrm{XX} \Rightarrow \{a\mathrm{X}, \mathrm{X}a, \mathrm{XXX}\} \Rightarrow \cdots .$$

Mais, avec une telle définition, il y a explosions du nombre de possibilités.

Définition (Dérivation immédiatement gauche (resp. droite)) **:** Étant donnée une grammaire $\mathcal{G} = (\mathcal{V}, \Sigma, P, I)$, et étant donnés deux mots u et v de $(\Sigma \cup \mathcal{V})^\star$, on dit que u *dérive immédiatement à gauche* (resp. droite) de u dès lors qu'il existe $x \in \Sigma^\star$, $y \in (\Sigma \cup \mathcal{V})^\star$ (resp. $x \in (\Sigma \cup \mathcal{V})^\star$ et $y \in \Sigma^\star$), et $(V \to w_1 \dots w_n) \in P$ tels que $u = xVy$ et $v = x \cdot w_1 w_2 \dots w_n \cdot y$. On note alors $u \Rightarrow_{\mathrm{g}} v$ (resp. $u \Rightarrow_{\mathrm{d}} v$). On définit, de la même manière que pour la dérivation simple, $\overset{\star}{\Rightarrow}_{\mathrm{g}}$ et $\overset{\star}{\Rightarrow}_{\mathrm{d}}$.

Exemple :
On considère une grammaire ayant pour règles de production $\mathrm{X} \to \mathrm{XX}$ et $\mathrm{X} \to a$. A-t-on

— $\mathrm{X} \overset{\star}{\Rightarrow}_{\mathrm{g}} a\mathrm{X}$? ✓ $(\mathrm{X} \Rightarrow_{\mathrm{g}} \mathrm{XX} \Rightarrow_{\mathrm{g}} a\mathrm{X})$

— $\mathrm{X} \overset{\star}{\Rightarrow}_{\mathrm{g}} \mathrm{X}a$? ✗

Définition (Arbre de dérivation) **:** Étant donnée une grammaire $\mathcal{G} = (\mathcal{V}, \Sigma, P, S)$, on appelle *arbre de dérivation* un arbre dont les nœuds sont étiquetés par des éléments de $\{\varepsilon\} \cup \mathcal{V} \cup \Sigma$ et tel que

- tout nœud interne (ayant des fils) est étiquetés par un élément de $\mathcal{V}$,
- la racine est étiquetée par S,
- tout nœud interne ayant une étiquette V et ayant des fils $T_1, \dots, T_n$ où $n \neq 0$ dont les racines sont étiquetées par $w_1, \dots, w_n$ avec $(V \to w_1 \dots w_n) \in P$.
- tout nœud interne d'étiquette V ayant pour unique fils l'arbre feuille réduit à ε et tel que $(V \to \varepsilon) \in P$.

Dans la suite du chapitre, on fixe $\mathcal{G} = (\mathcal{V}, \Sigma, I, P)$ une grammaire.

Exemple :

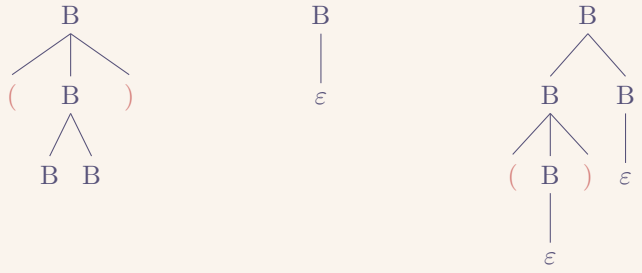


FIGURE 9.1 – Exemple d'arbres de dérivation

Définition (« production » d'un arbre) **:** On définit inductivement la fonction prod de l'ensemble des arbres de la grammaire $\mathcal{G}$ vers $(\Sigma \cup \mathcal{V})^\star$, comme

— $\text{prod}\big(\text{Leaf}(x)\big) = x$,
— $\text{prod}\big(\text{Node}(\_, [T_1, \dots, T_n])\big) = \text{prod}(T_1) \cdot \text{prod}(T_2) \cdot \ldots \cdot \text{prod}(T_n)$.

EXEMPLE :
Dans les arbres de dérivation exemples précédents, la fonction prod retourne (BB), ε et ( ).

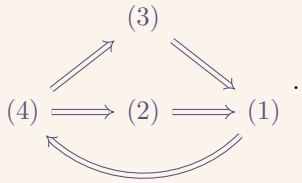
REMARQUE (Notation) :
On dit qu'un arbre de dérivation T est « *clos* » lorsque $\text{prod}(T) \in \Sigma^\star$.

EXEMPLE :
Dans les exemples précédents, le premier arbre n'est pas « clos » mais les deux suivants le sont.

Proposition : Étant donné $w \in \Sigma^\star$, il est équivalent de dire que
(1) $w \in \mathscr{L}(\mathcal{G})$,
(2) $S \overset{\star}{\Rightarrow}_{\text{g}} w$
(3) $S \overset{\star}{\Rightarrow}_{\text{d}} w$
(4) il existe un arbre de dérivation T dont w est le produit.

Preuve :

On procède la démonstration dans l'ordre suivant.



— **(4) $\implies$ (2).** Soit la propriété $\mathscr{P}(T)$: « si $w \in \Sigma^\star$ admet T comme arbre de dérivation (w est le produit de T) avec T un arbre de dérivation généralisé, enraciné en $V \in \mathscr{V}$, alors $V \overset{\star}{\Rightarrow}_{\mathrm{g}} w$. » Montrons cette propriété par induction.
  — Si $T = \mathrm{Leaf}(x)$ avec $x \in \Sigma \cup \{\varepsilon\}$, alors OK par un arbre de dérivation.
  — Si T = $\mathrm{Node}(V, [T_1, \dots, T_n])$, alors, pout $i \in [\![1, n]\!]$, raisonnons par disjonction.
    — Si T_i a une racine d'étiquette $w_i \in \Sigma$, alors $\mathrm{prod}(T_i) = w_i$, donc $w_i \overset{\star}{\Rightarrow}_{\mathrm{g}} \mathrm{prod}(T_i)$
    — Si T_i a une racine d'étiquette $w_i \in \mathscr{V}$, alors, par hypothèse d'induction sur T_i, on a $w_i \overset{\star}{\Rightarrow}_{\mathrm{g}} \mathrm{prod}(T_i)$.

  Ainsi, par concaténation, $\mathrm{prod}(T) = \mathrm{prod}(T_1) \cdot \ldots \cdot \mathrm{prod}(T_n)$. Or, $(V \to w_1 \dots w_n) \in P$. Alors, considérons la dérivation

$$\begin{aligned} V &\Rightarrow_{\mathrm{g}} w_1 w_2 \dots w_n \\ &\overset{\star}{\Rightarrow}_{\mathrm{g}} \mathrm{prod}(T_1) \cdot w_2 \dots w_n \\ &\overset{\star}{\Rightarrow}_{\mathrm{g}} \mathrm{prod}(T_1) \cdot \mathrm{prod}(T_2) \\ &\overset{\star}{\Rightarrow}_{\mathrm{g}} \cdots \overset{\star}{\Rightarrow}_{\mathrm{g}} \mathrm{prod}(T_1) \cdot \mathrm{prod}(T_2) \cdot \ldots \cdot \mathrm{prod}(T_n) \end{aligned}$$

— **(2) $\implies$ (1).** Vrai car $\Rightarrow_{\mathrm{g}}$ est « inclus dans » $\Rightarrow$ (c'est un cas particulier).

— **(1) $\implies$ (4).** Soit la propriété $\mathscr{P}_n$ « $\forall V \in \mathscr{V}$, $\forall w \in \Sigma^\star$, si $V \Rightarrow^n w$, alors w admet un arbre de dérivation généralisé enraciné en V. » Montrons le par induction.
  — Si $n = 0$, absurde.
  — Si $V \Rightarrow^n w$ avec $n \geqslant 1$, donc $V \Rightarrow w_1 w_2 \dots w \Rightarrow^{n-1} w$ donc $(V \to w_1 w_2 \dots w_n) \in P$, alors, par lemme de décompositions, il existe $\tilde{w}_1, \dots, \tilde{w}_p$ tels que $w = \tilde{w}_1 \cdot \ldots \cdot \tilde{w}_p$ et $\forall i \in [\![1, p]\!]$, $w_i \Rightarrow^{p_i} \tilde{w}_i$ avec $\sum_{i=1}^{p} p_i = n - 1$. D'où, $\forall i \in [\![1, p]\!]$, $p_i < n$. Par hypothèse d'induction, il existe, pour tout $i \in [\![1, p]\!]$, un arbre T_i produisant $\tilde{w}_i$ enraciné en w_i. Soit alors $T = \mathrm{Node}(w, [T_1, \dots, T_p])$. Ainsi, $\mathrm{prod}(T) = \tilde{w}_1 \cdot \ldots \cdot \tilde{w}_p = w$. Dans l'éventualité où l'un des p_i aurait le mauvais goût d'être nul, on fabrique, à la place, l'arbre $T_i = \mathrm{Leaf}(w_i)$.

□

Définition : Une grammaire est dite *ambigüe* s'il existe un mot w de son langage admettant au moins deux arbres de dérivations.

Exemple :
On considère la grammaire de non-terminal initial B ayant pour règles de production $\mathrm{F} \to 0 \mid 1 \mid \cdots \mid 9$ et $\mathrm{B} \to \mathrm{B}+\mathrm{B} \mid \mathrm{B}-\mathrm{B} \mid \mathrm{F}$. Le mot « $1-1+9$ » admet les deux arbres de dérivations ci-dessous.

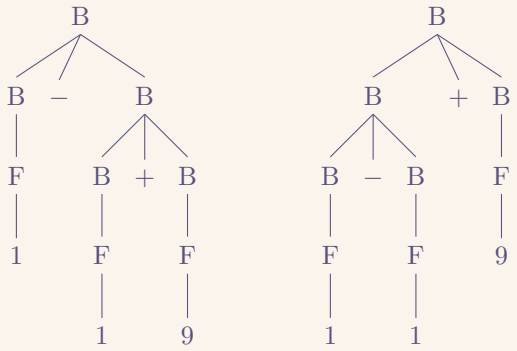


Figure 9.2 – Arbres de dérivations de « $1-1+9$ »

Interlude : langages algébriques. Les langages reconnus par des grammaires non-contextuelles sont des solutions d'équations polynômiales, où la multiplication correspond à la concaténation et l'addition correspond à l'union. D'où le terme langage *algébrique*.

Définition : Deux grammaires $\mathcal{G}_1$ et $\mathcal{G}_2$ sont dites *faiblement équivalentes* dès lors que $\mathcal{L}(\mathcal{G}_1) = \mathcal{L}(\mathcal{G}_2)$.

Exemple :
On considère la grammaire $\mathcal{G}_1$ de règle de production $\mathrm{S} \to a\mathrm{S} \mid \varepsilon$, et la grammaire $\mathcal{G}_2$ de règle de production $\mathrm{S} \to \mathrm{SS} \mid a \mid \varepsilon$. Les deux grammaires $\mathcal{G}_1$ et $\mathcal{G}_2$ sont faiblement équivalentes. En effet, $\mathcal{L}(\mathcal{G}_1) = \mathcal{L}(a^\star) = \mathcal{L}(\mathcal{G}_2)$. Mais, elles ne sont pas fortement équivalentes. [4]

IV.2 La hiérarchie de Chomsky

Le terme « *hiérarchie de Chomsky* » n'est pas au programme. Dans cette partie, on traite des inclusions avec les autres familles des langages au programme.

IV.2.1 Avec les langages réguliers

4. Deux grammaires sont fortement équivalentes si elles produisent les mêmes arbres de dérivation.

Proposition : Soient $\mathcal{G}_1$ et $\mathcal{G}_2$ des grammaires non contextuelles. Alors,

1. $\mathcal{L}(\mathcal{G}_1) \cup \mathcal{L}(\mathcal{G}_2)$ est reconnu par une grammaire non-contextuelle ;
2. $\mathcal{L}(\mathcal{G}_1) \cdot \mathcal{L}(\mathcal{G}_2)$ est reconnu par une grammaire non-contextuelle ;
3. $\big(\mathcal{L}(\mathcal{G}_1)\big)^\star$ est reconnu par une grammaire non-contextuelle.

Preuve :
Soient $\mathcal{G}_1 = (\mathcal{V}_1, \Sigma, P_1, S_1)$ et $\mathcal{G}_2 = (\mathcal{V}_2, \Sigma, P_2, S_2)$. On peut supposer, quitte à renommer les non-terminaux, que $\mathcal{V}_1 \cap \mathcal{V}_2 = .$

1. Soit alors $S \notin \mathcal{V}_1 \cup \mathcal{V}_2$. On pose $\mathcal{G} = (\mathcal{V}_1 \cup \mathcal{V}_2 \cup \{S\}, \Sigma, P_1 \cup P_2 \cup \{S \to S_1 \mid S_2\}, S)$. Soit $w \in \Sigma^\star$.

$$\begin{aligned} w \in \mathcal{L}(\mathcal{G}) &\iff S \overset{\star}{\Rightarrow}_{\mathcal{G}} w \\ &\iff \big(S \Rightarrow_{\mathcal{G}} S_1 \overset{\star}{\Rightarrow}_{\mathcal{G}} w\big) \text{ ou } \big(S \Rightarrow_{\mathcal{G}} S_2 \overset{\star}{\Rightarrow}_{\mathcal{G}} w\big) \\ &\iff (S_1 \overset{\star}{\Rightarrow}_{\mathcal{G}} w) \text{ ou } (S_2 \overset{\star}{\Rightarrow}_{\mathcal{G}} w) \\ &\iff (S_1 \overset{\star}{\Rightarrow}_{\mathcal{G}_1} w) \text{ ou } (S_2 \overset{\star}{\Rightarrow}_{\mathcal{G}_2} w) \\ &\iff w \in \mathcal{L}(\mathcal{G}_1) \cup \mathcal{L}(\mathcal{G}_2) \end{aligned}$$

2. Soit alors $S \notin \mathcal{V}_1 \cup \mathcal{V}_2$. On pose $\mathcal{G} = (\mathcal{V}_1 \cup \mathcal{V}_2 \cup \{S\}, \Sigma, P_1 \cup P_2 \cup \{S \to S_1 \cdot S_2\}, S)$. Soit $w \in \Sigma^\star$.

$$\begin{aligned} w \in \mathcal{L}(\mathcal{G}) &\iff S \overset{\star}{\Rightarrow}_{\mathcal{G}} w \\ &\iff S \Rightarrow S_1 \cdot S_2 \overset{\star}{\Rightarrow}_{\mathcal{G}} w \\ &\iff \exists (u,v) \in (\Sigma^\star)^2,\ S_1 \overset{\star}{\Rightarrow}_{\mathcal{G}} u \text{ et } S_2 \overset{\star}{\Rightarrow}_{\mathcal{G}} v \text{ et } w = u \cdot v \\ &\iff \exists (u,v) \in (\Sigma^\star)^2,\ S_1 \overset{\star}{\Rightarrow}_{\mathcal{G}_1} u \text{ et } S_2 \overset{\star}{\Rightarrow}_{\mathcal{G}_2} v \text{ et } w = u \cdot v \\ &\iff \exists (u,v) \in (\Sigma^\star)^2,\ u \in \mathcal{L}(\mathcal{G}_1) \text{ et } v \in \mathcal{L}(\mathcal{G}_2) \text{ et } w = u \cdot v \\ &\iff w \in \mathcal{L}(\mathcal{G}_1) \cdot \mathcal{L}(\mathcal{G}_2) \end{aligned}$$

3. Soit alors $S \notin \mathcal{V}_1 \cup \mathcal{V}_2$. On pose $\mathcal{G} = (\mathcal{V}_1 \cup \{S\}, \Sigma, P_1 \cup \{S \to S \cdot S_1 \mid$

$\varepsilon\}, S)$. Soit $w \in \Sigma^\star$.

$$
\begin{aligned}
w \in \mathscr{L}(\mathscr{G}) &\iff S \overset{\star}{\Rightarrow}_{\mathscr{G}} w \\
&\iff S \overset{\star}{\Rightarrow}_{\mathscr{G},\mathrm{g}w} \\
&\iff S \Rightarrow \overbrace{S \cdot S_1 \Rightarrow SS_1S_1 \Rightarrow \cdots \Rightarrow \underbrace{S_1S_1\cdots S_1}_{n}}^{n} \overset{\star}{\Rightarrow}_{\mathscr{G}} w^\star \\
&\iff \exists n \in \mathbb{N},\ \exists(\tilde{w}_1,\ldots,\tilde{w}_n),\ (\forall i \in [\![1,n]\!],\ S_1 \overset{\star}{\Rightarrow}_{\mathscr{G}} \tilde{w}_i) \text{ et } w = \tilde{w}_1\cdots\tilde{w}_n \\
&\iff \exists n \in \mathbb{N},\ \exists(\tilde{w}_1,\ldots,\tilde{w}_n),\ (\forall i \in [\![1,n]\!],\ S_1 \overset{\star}{\Rightarrow}_{\mathscr{G}_1} \tilde{w}_i) \text{ et } w = \tilde{w}_1\cdots\tilde{w}_n \\
&\iff \exists n \in \mathbb{N},\ \exists(\tilde{w}_1,\ldots,\tilde{w}_n),\ \big(\forall i \in [\![1,n]\!],\ \tilde{w}_i \in \mathscr{L}(\mathscr{G}_1)\big) \text{ et } w = \tilde{w}_1\cdots\tilde{w}_n \\
&\iff w \in \big(\mathscr{L}(\mathscr{G}_1)\big)^\star
\end{aligned}
$$

□

Théorème : Tout langage régulier est reconnu par une grammaire non contextuelle.

Preuve :
On a déjà montré que les grammaires non-contextuelles sont stables par union, concaténation et passage à l'étoile. Il ne reste qu'à montrer le résultat sur les cas de base. On a

- $\{\varepsilon\} = \mathscr{L}\big((\{S\}, \Sigma, \{S \to \varepsilon\}, S)\big)$,
- $\varnothing = \mathscr{L}\big((\{S\}, \Sigma, , S)\big)$, (▷ voir TD 14.)
- $\{\ell\} = \mathscr{L}\big((\{S\}, \Sigma, \{S \to \ell\}, S)\big)$.

Il suffit alors de conclure par induction. □

REMARQUE :
L'inclusion précédente est stricte. En effet le langage $\{a^n \cdot b^n \mid n \in \mathbb{N}\}$ est reconnu par une grammaire non contextuelle mais n'est pas un langage régulier.

REMARQUE (Digression) :

« *Tout langage est-il le langage d'une grammaire non contextuelle ?* »

On procède par un argument de taille d'ensembles. Soit $\mathscr{G} = (\mathscr{V}, \Sigma, P, I)$ une grammaire. On considère $\Sigma = \{0,1\}$. On pose $|\mathscr{G}| = |\Sigma| + |\mathscr{V}| + \sum_{(V \to w_1 \ldots w_n) \in P}(n+1) + 1$. On considère $\mathbb{G}_n = \{\mathscr{G} \mid |\mathscr{G}| = n\}$. L'ensemble $\mathbb{G} = \bigcup_{n\in\mathbb{N}} \mathbb{G}_n$ est dénombrable comme union dénombrable d'ensembles finis. Montrons qu'il existe une bijection entre $\wp(\{0,1\}^\star)$ et $[0,1[$. À tout $x \in [0,1[$,

on peut poser $x = 0, x_1 x_2 \dots x_n \dots$. D'où,

$$[0,1[\xleftarrow[\text{encodage binaire}]{\text{bijection}} (\mathbb{N} \to \{0,1\}) \xleftarrow[\mathbb{1}]{\text{bijection}} \wp(\mathbb{N}) \xleftarrow[\text{encodage binaire}]{\text{bijection}} \wp(\{0,1\}^\star).$$

IV.2.2 Lien avec les langages décidables

Proposition : Les langages des grammaires non contextuelles sont des langages décidables. □

La preuve de cette propriété est dans le TD 15. (On peut montrer, par programmation dynamique, que l'appartenance d'un mot à une grammaire non contextuelle est calculable en temps polynômial, en $\mathcal{O}(n^3)$.)

EXEMPLE :
▷ TD 15, exercice 1.

EXEMPLE :
On considère l'alphabet $\Sigma = \{C, LP, RP\}$ et les règles de production $\mathrm{S} \to \mathrm{TS} \mid C$ et $\mathrm{T} \to LP \cdot \mathrm{S} \cdot RP$. Codons un programme reconnaissant la grammaire définie par ces règles. On représente Σ par le type `token` où C correspond à `C`, LP à `LP` et RP à `RP`.

```
type token = C | LP | RP
type word = token list

type non_term = S | T

(* closed derivation tree *)
type cdt =
  | Node of non_term * cdt list
  | Leaf of token option


exception Non

let rec parse_s (w: word): cdt * word =
  match w with
  | C ::  w' -> (Node(S, [Leaf(Some C)]), w')
  | _        ->
      let (g, w')  = parse_t w  in
      let (d, w'') = parse_s w' in
      (Node (S, [g; d]), w'')
and parse_t (w: word): cdt * word =
  match w with
  | LP :: w' -> begin
      let (u, w'') = parse_s w' in
      match w'' with
      | RP :: w''' -> (Node (T,
          [Leaf (Some LP); u; Leaf (Some RP)]), w''')
      | _          -> raise Non
    end
  | _ -> raise Non
```

CODE 9.1 – Programme reconnaissant une grammaire $\mathcal{G}$

Chapitre 10

Concurrence

IV.1 Motivation

On place au centre de la classe 40 bonbons. On en distribue un chacun. Si, par exemple, chacun choisit un bonbon et, au *top* départ, prennent celui choisi. Il est probable que plusieurs choisissent le même. Comme gérer lorsque plusieurs essaient d'accéder à la mémoire ?

Deuxièmement, sur l'ordinateur, plusieurs applications tournent en même temps. Pour le moment, on considérait qu'un seul programme était exécuté, mais, le PC ne s'arrête pas pendant l'exécution du programme.

On s'intéresse à la notion de « processus » qui représente une tâche à réaliser. On ne peut pas assigner un processus à une unité de calcul, mais on peut « allumer » et « éteindre » un processus. Le programme allumant et éteignant les processus est « l'ordonnanceur. » Il doit aussi s'occuper de la mémoire du processus (chaque processus à sa mémoire séparée).

On s'intéresse, dans ce chapitre, à des programmes qui « partent du même » : un programme peut créer un « fil d'exécution » (en anglais, *thread*). Le programme peut gérer les fils d'exécution qu'il a créé, et éventuellement les arrêter. Les fils d'exécutions partagent la mémoire du programme qui les a créé.

En C, une tâche est représenté par une fonction de type `void* tache(void* arg)`. Le type `void*` est l'équivalent du type `'a` : on peut le *cast* à un autre type (comme `char*`).

```
1  void* tache(void* arg) {
2    printf("%s\n", (char*) arg);
3    return NULL;
4  }
5
6  int main() {
7    pthread_t p1, p2;
8
9    printf("main: begin\n");
10
11   pthread_create(&p1, NULL, tache, "A");
```

```
12    pthread_create(&p2, NULL, tache, "B");
13
14    pthread_join(p1, NULL);
15    pthread_join(p2, NULL);
16
17    printf("main: end\n");
18
19    return 0;
20  }
```

CODE 10.1 – Création de *threads* en C

```
1   int max = 10;
2   volatile int counter = 0;
3
4   void* tache(void* arg) {
5     char* letter = arg;
6     int i;
7
8     printf("%s begin [addr of i: %p] \n", letter, &i);
9
10    for(i = 0; i < max; i++) {
11      counter = counter + 1;
12    }
13
14    printf("%s: done\n", letter);
15    return NULL;
16  }
17
18  int main() {
19    pthread_t p1, p2;
20
21    printf("main: begin\n");
22
23    pthread_create(&p1, NULL, tache, "A");
24    pthread_create(&p2, NULL, tache, "B");
25
26    pthread_join(p1, NULL);
27    pthread_join(p2, NULL);
28
29    printf("main: end\n");
30
31    return 0;
32  }
```

CODE 10.2 – Mémoire dans les *threads* en C

Dans les *threads*, les variables locales (comme `i`) sont séparées en mémoire. Mais, la variable `counter` est modifiée, mais elle ne correspond pas forcément à $2 \times$ `max`. En effet, si `p1` et `p2` essaient d'exécuter au même moment de réaliser l'opération `counter = counter + 1`, ils peuvent récupérer deux valeurs identiques de `counter`, ajouter 1, puis réassigner `counter`. Ils « se marchent sur les pieds. »

Parmi les opérations, on distingue certaines dénommées « atomiques » qui ne peuvent pas être séparées. L'opération `i++` n'est pas atomique, mais la lecture et l'écriture mémoire le sont.

Définition : On dit d'une variable qu'elle est *atomique* lorsque l'ordonnanceur ne l'interrompt pas.

Exemple :
L'opération `counter = counter + 1` exécutée en série peut être représentée comme ci-dessous. Avec `counter` valant 40, cette exécution donne 42.

Exécution du fil A	Exécution du fil B
(1) $\text{reg}_1 \leftarrow$ `counter`	(4) $\text{reg}_2 \leftarrow$ `counter`
(2) reg_1++	(5) reg_2++
(3) `counter` $\leftarrow \text{reg}_1$	(6) `counter` $\leftarrow \text{reg}_2$

Mais, avec l'exécution en simultanée, la valeur de `counter` sera 41.

Exécution du fil A	Exécution du fil B
(1) $\text{reg}_1 \leftarrow$ `counter`	(2) $\text{reg}_2 \leftarrow$ `counter`
(3) reg_1++	(5) reg_2++
(4) `counter` $\leftarrow \text{reg}_1$	(6) `counter` $\leftarrow \text{reg}_2$

Il y a *entrelacement* des deux fils d'exécution.

Remarque (Problèmes de la programmation concurrentielle) :
- Problème d'accès en mémoire,
- Problème du rendez-vous, [1]
- Problème du producteur-consommateur, [2]
- Problème de l'entreblocage, [3]
- Problème famine, du dîner des philosophes. [4]

Exemple (Problème de l'entreblocage) :

Fil A	Fil B	Fil C
RDV(C)	RDV(A)	RDV(B)
RDV(B)	RDV(C)	RDV(A)

Table 10.1 – Problème de l'entreblocage

Comment résoudre le problème des deux incrementations ? Il suffit de « mettre un verrou. » Le premier fil d'exécution « s'enferme » avec l'expression `count++`, le second fil d'exécution attend que l'autre sorte pour pouvoir entrer et s'enfermer à son tour.

1. Lorsque deux programmes terminent, ils doivent s'attendre pour donner leurs valeurs.
2. Certains programmes doivent ralentir ou accélérer.
3. *c.f.* exemple ci-après.
4. Les philosophes mangent autour d'une table, et mangent du riz avec des baguettes. Ils décident de n'acheter qu'une seule baguette par personne. Un philosophe peut, ou penser, ou manger. Mais, pour manger, ils ont besoin de deux baguettes. S'ils ne mangent pas, ils meurent.

IV.2 *Mutex*

Le mot *mutex* vient de *mutual exception* (exclusion mutuelle).

Définition :
Le type de données abstrait verrou fournit

- un type `t` : le type des verrous,
- une fonction `lock : t → unit` qui ferme le verrou,
- une fonction `unlock : t → unit` qui ouvre le verrou,
- une fonction `create : ( ) → t` qui crée un verrou,

de sorte que, lorsque plusieurs fils d'exécution exécutent de manière concurrent l'algorithme ci-dessous, on ait

```
1  lock(v);
2  /* section critique */
3  unlock(v);
```

1. au plus un seul fil d'exécution dans la section critique (exclusion mutuelle) ;
2. un fil d'exécution en attente (ayant appelé la fonction `lock`) n'empêche pas d'autres fils d'exécutions d'accéder à la section critique ;
3. un fil d'exécution ayant fini `lock` aura accès à un moment à la section critique.

IV.2.1 À deux fils d'exécutions

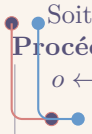
On se restreint, pour simplifier, dans le cas où l'on n'a que deux fils d'exécutions.

Algorithme 10.1 Tentative 1 d'implémentation du type verrou

```
1 : Soit Dedans un tableau de taille 2 initialisé à F.
2 : Procédure Lock(i)        ▷ i ∈ {0,1} est l'identifiant du fil
3 :     o ← 1 − i            ▷ identifiant de l'autre fil d'exécution
4 :     tant que Dedans[o] faire
5 :         rien
6 :     Dedans[i] ← V
7 : Procédure Unlock(i)
8 :     Dedans[i] ← F
```

Mais, cet tentative ne résout pas le problème. En effet, l'exécution où l'ordonnanceur exécute l'algorithme jusqu'à la fin de tant que pour le fil 1, puis passe au fil 2, est un contre-exemple à la tentative 1 d'implémentation du type verrou. ▷ propriété d'exclusion mutuelle

Algorithme 10.2 Tentative 2 d'implémentation du type verrou



```
1 : Soit Want un tableau de taille 2 initialisé à F.
2 : Procédure Lock(i)        ▷ i ∈ {0,1} est l'identifiant du fil
3 :     o ← 1 − i            ▷ identifiant de l'autre fil d'exécution
4 :     Want[i] ← V
5 :     tant que Want[o] faire
6 :         rien
7 : Procédure Unlock(i)
8 :     Want[i] ← F
```

Cette tentative ne résout pas non plus le programme : si l'ordonnanceur exécute le fil 1 jusqu'à avant la boucle tant que, puis passe au fil 2, les deux fils sont bloqués. ▷ propriété de non-entreblocage

Algorithme 10.3 Tentative 3 d'implémentation du type verrou

```
1 : turn ← 0          ▷ premier fil d'exécution
2 : Procédure Lock(i)
3 :     o ← 1 − i
4 :     tant que turn = o faire
5 :         rien
6 : Procédure Unlock(i)
7 :     o ← 1 − i
8 :     turn ← o
```

Cette tentative impose une alternance 0 puis 1 puis 0… Mais, si l'un des deux fils termine, alors l'autre est bloqué.

Dans la suite, on suppose qu'un fil ne meure pas dans la section critique, ou lors de l'appel de Lock(i), ou lors de l'appel de Unlock(i).

On donne donc la tentative finale, ci-dessous, qui réussi à combler toutes les hypothèses du type verrou.

Algorithme 10.4 Tentative 4 d'implémentation du type verrou – Algorithme de Peterson

```
1 : turn ← 0          ▷ premier fil d'exécution
2 : Soit Want un tableau de taille 2 initialisé à F.
3 : Procédure Lock(i)
4 :     o ← 1 − i
5 :     Want[i] ← V
6 :     turn ← o
7 :     tant que turn = o et Want[o] faire
8 :         rien
9 : Procédure Unlock(i)
10 :    Want[i] ← F
```

On vérifie que les trois propriétés du type verrou sont vérifiées.

1. **Exclusion mutuelle.** Par l'absurde, supposons que les deux fils d'exécutions sont dans la section critique. Ainsi, Want[0] = Want[1] = **V**. Le fil d'exécution 0 nous donne que Want[1] = **F** ou turn $\neq$ 1. Le fil d'exécution 1 nous donne que Want[0] = **F** ou turn $\neq$ 0. On en déduit que turm $\neq$ 0 et turn $\neq$ 1. Or, turn $\in \{0, 1\}$ (on peut le montrer par un rapide invariant). D'où l'absurdité.

2. **Non-interblocage.** Si les deux conditions de boucles sont vraies, alors turn = 0 et turn = 1, ce qui est absurde.

3. **Résilience à la mort de l'autre fil d'exécution.** [5] Supposons que le fil d'exécution n'exécute plus Lock(1) (mais il a exécuté Unlock(1) avant de partir). Alors, Want[1] = **F**, et ce pour toujours. Donc, le fil 0 n'est pas bloqué.

IV.2.2 À *N* fils d'exécutions

On propose de l'algorithme de la boulangerie. On se donne un « ticket » qui donne l'ordre de passage. En voulant accéder à la boulangerie, on prend un ticket (1 plus la valeur maximale des tickets), et on attend son tour Pour attendre son tour, on attend que chacune des personnes n'ai un ticket inférieur au sien. Ceci donne l'algorithme suivant.

Algorithme 10.5 Tentative 1 d'implémentation du type verrou à N fils

```
1 : Ticket est un tableau de n entiers initialisés à 0.
2 : Procédure Lock(Ticket, i)
3 :     Ticket[i] ← 1 + max{Ticket[j] | j ∈ ⟦0, n − 1⟧}
4 :     pour j ∈ ⟦0, n − 1⟧ faire
5 :         tant que Ticket[i] ≠ 0 et Ticket[j] < Ticket[i] faire
6 :             rien
7 : Procédure Unlock(Ticket, i)
8 :     Ticket[i] ← 0
```

Mais, cet algorithme peuvent prendre un ticket pendant le calcul du max. On utilise une variable EnCalcul qui dit lorsque le calcul du max est en cours.

5. *i.e.* accès peu importe si l'autre est encore en vie ou non.

Algorithme 10.6 Tentative 2 d'implémentation du type verrou à N fils

```
1 : Ticket est un tableau de n entiers initialisés à 0.
2 : EnCalcul est un tableau de n booléens initialisés à F.
3 : Procédure Lock(Ticket, i)
4 :     EnCalcul[i] ← V
5 :     Ticket[i] ← 1 + max{Ticket[j] | j ∈ ⟦0, n − 1⟧}
6 :     EnCalcul[i] ← F
7 :     pour j ∈ ⟦0, n − 1⟧ faire
8 :         tant que EnCalcul[j] faire
9 :             rien
10 :        tant que Ticket[i] ≠ 0 et Ticket[j] < Ticket[i] faire
11 :            rien
12 : Procédure Unlock(Ticket, i)
13 :    Ticket[i] ← 0
```

Mais, cet algorithme laisse avoir deux personnes ayant un ticket de même valeur. On peut départager les deux personnes avec les identifiants.

Algorithme 10.7 Tentative 3 d'implémentation du type verrou à N fils – algorithme de la boulangerie

```
1 : Ticket est un tableau de n entiers initialisés à 0.
2 : EnCalcul est un tableau de n booléens initialisés à F.
3 : Procédure Lock(Ticket, i)
4 :     EnCalcul[i] ← V
5 :     Ticket[i] ← 1 + max{Ticket[j] | j ∈ ⟦0, n − 1⟧}
6 :     EnCalcul[i] ← F
7 :     pour j ∈ ⟦0, n − 1⟧ faire
8 :         tant que EnCalcul[j] faire
9 :             rien
10 :        tant que Ticket[j] ≠ 0 et [Ticket[j] < Ticket[i] ou (Ticket[j] = Ticket[i] et j < i)]
            faire                    (ordre lexicographique)
11 :            rien
12 : Procédure Unlock(Ticket, i)
13 :    Ticket[i] ← 0
```

Cet algorithme assure l'exclusion mutuelle. On peut penser que ce problème peut créer le problème de famine. Mais, non, la comparaison entre identifiants n'a lieu qu'en cas d'égalité de ticket, donc lorsque deux personnes arrivent en même temps à la boulangerie.

IV.3 Sémaphore

Un sémaphore est utilisé pour assurer une propriété moins forte que le *mutex* : on assure qu'il n'y a pas « trop » de personnes dans la zone critique. On fixe un nombre maximal de fils qui sont dans la zone critique et on évite un « flot » de personnes ininterrompu dans la zone critique. Par exemple, en TP, on n'a

qu'un nombre limité d'ordinateurs. À l'entrée de la salle, on met à disposition les ordinateurs et chacun dépose le sien lorsqu'il a fini de l'utiliser.

Définition : Le type de données abstrait sémaphore fournit
- le type `t` des sémaphores,
- une fonction d'acquisition du sémaphore `acquire` : `t` $\to$ ( ),
- une fonction de libération du sémaphore `release` : `t` $\to$ ( ),
- une fonction de création/d'initialisation du sémaphore `make` : $\mathbb{N} \to$ `t`,

tels que
- lors d'une tentative d'acquisition du sémaphore : si le compteur du sémaphore est nul, alors le fil d'exécution courant est mis en attente ; sinon, le compteur est décrémenté et le fil d'exécution peut continuer ;
- lors de la libération du sémaphore : si un fil d'exécution est en attente, on le laisse continuer son exécution ; sinon, on incrémente le compteur.

Exemple :
On considère deux « types » de personnes. Les *producteurs* qui peuvent écrire une donnée. Les *consommateurs* qui récupère une donnée (qui consomme une donnée). En tant que métaphore, on considère que les données sont des pommes. Le producteur ne doit pas produire trop de pommes, le consommateur doit avoir des pommes à consommer. On considère, à présent, l'algorithme ci-dessous.

Algorithme 10.8 Utilisation de la structure sémaphore dans une problématique producteur/consommateur

```
1 : Procédure Producteur
2 :     acquire plein
3 :     lock()
4 :     Produit une pomme.
5 :     unlock()
6 :     release vide

7 : Procédure Consommateur
8 :     acquire vide
9 :     lock()
10 :    Mange une pomme.
11 :    unlock()
12 :    release plein

13 : vide ← make 0
14 : plein ← make nb_pommes
15 : pour i ∈ ⟦1, n⟧ faire
16 :     Soit un nouveau consommateur.      ▷ i.e. un fil d'exécution qui exécute
         la procédure Consommateur
17 : pour j ∈ ⟦1, m⟧ faire
18 :     Soit un nouveau producteur.        ▷ i.e. un fil d'exécution qui exécute la
         procédure Producteur
```

Partie V

MPI – Informatique – TDs

Chapitre 1

Ordre & Induction

V.1 Listes, listes, listes !

1. On a $\forall \ell \in \mathscr{L}$, $@([\,], \ell) = \ell$; $\forall \ell_1, \ell \in \mathscr{L}$, $@\big(::(x, \ell_1), \ell\big) = ::\big(x, @(\ell_1, \ell)\big)$.
2. On fait une induction. Comme dans l'énoncé, on passe le '@' en infixe. Notons P_ℓ : "$\ell \mathbin{@} [\,] = \ell$".

   Montrons $P_{[\,]}$: on sait que $[\,] \mathbin{@} [\,] = [\,]$ par définition de @.

   On suppose P_ℓ est vraie pour une certaine liste $\ell \in \mathscr{L}$. Montrons que, $\forall x \in \mathbb{N}$, $P_{::(x,\ell)}$ vrai. Soit $x \in \mathbb{N}$.

$$\begin{aligned}\big(::(x, \ell)\big) \mathbin{@} [\,] &\overset{(\text{def})}{=} ::(x, \ell \mathbin{@} [\,]) \\ &\overset{(P_\ell)}{=} ::(x, \ell).\end{aligned}$$

3. Notons P_{ℓ_1} : "$\forall \ell_2, \ell_3 \in \mathscr{L}$, $(\ell_1 \mathbin{@} \ell_2) \mathbin{@} \ell_3 = \ell_1 \mathbin{@} (\ell_2 \mathbin{@} \ell_3)$", où $\ell_1 \in \mathscr{L}$ est une liste.

   Soient $\ell_2, \ell_3 \in \mathscr{L}$ deux listes. On a, par définition de @, $([\,] \mathbin{@} \ell_2) \mathbin{@} \ell_3 = \ell_2 \mathbin{@} \ell_3$ et $[\,] \mathbin{@} (\ell_2 \mathbin{@} \ell_3) = \ell_2 \mathbin{@} \ell_3$.

   Soit $\ell_1 \in \mathscr{L}$ une liste telle que P_{ℓ_1}. Soient $\ell_2, \ell_2 \in \mathscr{L}$ deux listes. Soit $x \in \mathbb{N}$. Montrons que $P\big(::(x, \ell_1)\big)$:

$$\begin{aligned}\big(::(x, \ell_1) \mathbin{@} \ell_2\big) \mathbin{@} \ell_3 &= ::(x, \ell_1 \mathbin{@} \ell_2) \mathbin{@} \ell_3 \\ &= ::\big(x, (\ell_1 \mathbin{@} \ell_2) \mathbin{@} \ell_3\big) \\ &\overset{(H)}{=} ::\big(x, \ell_1 \mathbin{@} (\ell_2 \mathbin{@} \ell_3)\big) \\ &= ::(x, \ell_1) \mathbin{@} (\ell_2 \mathbin{@} \ell_3).\end{aligned}$$

4. Notons P_{ℓ_1} : "$\forall \ell_2 \in \mathscr{L}$, $\texttt{rev}(\ell_1 \mathbin{@} \ell_2) = \texttt{rev}(\ell_2) \mathbin{@} \texttt{rev}(\ell_1)$. Soit $\ell_2 \in \mathscr{L}$.

   On a $\texttt{rev}([\,] \mathbin{@} \ell_2) = \texttt{rev}(\ell_2) = \texttt{rev}(\ell_2) \mathbin{@} \texttt{rev}([\,])$.

On suppose P_{ℓ_1} vraie pour une certaine liste $\ell_1 \in \mathscr{L}$. Soit $x \in \mathbb{N}$.

$$\begin{aligned}
\texttt{rev}(::x, \ell_1) \mathbin{@} \ell_2) &= \texttt{rev}(::(x, \ell_1 \mathbin{@} \ell_2) \\
&= \texttt{rev}(\ell_1 \mathbin{@} \ell_2) \mathbin{@} ::(x, [\,]) \\
&= \big(\texttt{rev}(\ell_2) \mathbin{@} \texttt{rev}(\ell_1)\big) \mathbin{@} ::(x, [\,]) \\
&= \texttt{rev}(\ell_2) \mathbin{@} \big(\texttt{rev}(\ell_1) \mathbin{@} ::(x, [\,])\big) \\
&= \texttt{rev}(\ell_2) \mathbin{@} \texttt{rev}\big(::(x, \ell_1)\big)
\end{aligned}$$

5. Notons, pour toute liste $\ell \in \mathscr{L}$, P_ℓ : "$\texttt{rev}\big(\texttt{rev}(\ell)\big) = \ell$".

   Montrons que $P_{[\,]}$ est vraie : $\texttt{rev}(\texttt{rev}([\,])) = \texttt{rev}([\,]) = [\,]$.

   Soit une liste $\ell \in \mathscr{L}$ telle que P_ℓ soit vraie. Soit $n \in \mathbb{N}$. Montrons que $P_{::(x,\ell)}$ vraie :

$$\begin{aligned}
\texttt{rev}(\texttt{rev}(::(x, \ell))) &= \texttt{rev}(\texttt{rev}(\ell) \mathbin{@} ::(x, [\,])) \\
&= \texttt{rev}(::(x, [\,])) \mathbin{@} ::(x, \ell) \mathbin{@} \ell \\
&= [\,] \mathbin{@} ::(x, [\,]) \mathbin{@} \ell \\
&= ::(x, [\,]) \mathbin{@} \ell \\
&= ::(x, \ell).
\end{aligned}$$

V.2 Ensembles définis inductivement

La correction est disponible sur *cahier-de-prepa*.

V.3 Arbres, Arbres, Arbres !

1. On pose $R = \left\{V\big|^0,\ N\big|^2_{\mathbb{N}}\right\}$. Ainsi, par induction nommée, on crée l'ensemble $\mathscr{A}$ des arbres.
2. On pose

$$\begin{aligned}
h : \mathscr{A} &\longrightarrow \mathbb{N} \cup \{-1\} \\
V &\longmapsto -1 \\
N(x, f_1, f_2) &\longmapsto 1 + \max\big(h(f_1), h(f_2)\big)
\end{aligned}$$

   et

$$\begin{aligned}
t : \mathscr{A} &\longrightarrow \mathbb{N} \\
V &\longmapsto 0 \\
N(x, f_1, f_2) &\longmapsto 1 + t(f_1) + t(f_2)
\end{aligned}$$

3. On rappelle les relations taille/hauteur (vues l'année dernière) :

$$h(a)+1 \leqslant t(a) \leqslant 2^{h(a)+1}-1.$$

Soit, pour tout arbre $a \in \mathcal{A}$, P_a la propriété ci-dessus. Montrons que P_a est vraie pour tout arbre $a \in \mathcal{A}$ par induction.

Montrons que P_V vraie : on a $h(V)+1 = 1-1 = 0$, $t(V) = 0$ et $2^{h(V)+1} - 1 = 1-1 = 0$ d'où $h(V)+1 \leqslant t(V) \leqslant 2^{h(V)+1}-1$.

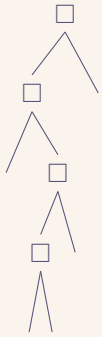
Supposons P_g vraie et P_d vraie pour deux arbres $g, d \in \mathcal{A}$. Soit $x \in \mathbb{N}$. Montrons que $P_{N(x,g,d)}$ est vraie :

$$\begin{aligned} h\big(N(x,g,d)\big) - 1 &= 1 + \max\big(h(g),h(d)\big) + 1 \\ &\leqslant \max(t(g)-1, t(d)-1) + 2 \\ &\leqslant \max\big(t(g),t(d)\big) + 1 \\ &\leqslant t(g) + t(d) + 1 \\ &= t\big(N(x,g,d)\big) \end{aligned}$$

et

$$\begin{aligned} t\big(N(x,g,d)\big) &= t(g) + t(d) + 1 \\ &\leqslant 2^{h(g)+1} + 2^{h(d)+1} - 1 \\ &\leqslant 2 \times 2^{\max(h(g),h(d))+1} - 1 \\ &\leqslant 2^{\max(h(g),h(d))+2} - 1 \\ &\leqslant 2^{h(N(x,g,d))+1} - 1. \end{aligned}$$

4. Je pense qu'il y a une erreur d'énoncé : les arbres crées sont de la forme



où □ représente un nœud. Il ne sont pas de la forme "peigne."

V.4 Ordre sur *powerset*

1. Soient A et B deux parties d'un ensemble ordonné $(S, \preccurlyeq)$. Si $A = B$, alors $A \dot{\preccurlyeq} B$ et donc A et B sont comparables. Si $A \neq B$, alors $A \triangle B \neq$, et donc $A \triangle B$ admet un plus petit élément m. Par définition de $\triangle$, on a

$m \in A$ (et donc $A \dot{\succcurlyeq} B$) ou $m \in B$ (et donc $A \dot{\preccurlyeq} B$). On en déduit que A et B sont comparables. La relation $\dot{\preccurlyeq}$ est donc totale.

2. On a
$$\dot{\preccurlyeq}\{2\} \dot{\preccurlyeq} \{1\} \dot{\preccurlyeq} \{1,2\} \dot{\preccurlyeq} \{0\} \dot{\preccurlyeq} \{0,2\} \dot{\preccurlyeq} \{0,1\} \dot{\preccurlyeq} \{0,1,2\}.$$
3. Non, l'ordre $(\wp(S), \dot{\preccurlyeq})$ n'est pas forcément bien fondé. Par exemple, on pose $(S, \preccurlyeq) = (\mathbb{N}, \leqslant)$. Toute partie non vide de $\mathbb{N}$ admet bien un plus petit élément. Mais, la suite $(u_n)_{n\in\mathbb{N}} = (\{n\})_{n\in\mathbb{N}}$ est strictement décroissante : en effet, pour $n \in \mathbb{N}$, on a $u_n \triangle u_{n+1} = \{n, n+1\}$ qui admet pour élément minimal $n \in A$, d'où $u_n \dot{\succcurlyeq} u_{n+1}$.

V.5 Ordres bien fondés en vrac

1. Non, l'ensemble $(\mathbb{N}, \sqsubseteq)$ n'est pas un ensemble ordonné. En effet, en posant $n = 4$ et $m = 8$, on a $\forall i \in \mathbb{N}$, $\frac{n}{2^i} \pmod 2 = 0$, et $\forall i \in \mathbb{N}$, $\frac{m}{2^i} \pmod 2 = 0$. Ainsi, on a $n \sqsubseteq m$, et $m \sqsubseteq n$, mais comme $n \neq m$, la relation "$\sqsubseteq$" n'est pas anti-symétrique, ce n'est donc pas une relation d'ordre (et donc encore moins un ordre bien fondé).
2. Non, l'ensemble $(\Sigma^\star, \sqsubseteq)$ n'est pas un ensemble ordonné. En effet, en posant $\Sigma = \{a, b\}$, et $u = aa$ et $v = ab$ deux mots de Σ, on a $|u| = |v|$ et donc $u \sqsubseteq v$ et $u \sqsupseteq v$ mais comme $u \neq v$, la relation "$\sqsubseteq$" n'est pas anti-symétrique, ce n'est donc pas une relation d'ordre (et donc encore moins un ordre bien fondé).
3. Oui, l'ensemble $(\Sigma^\star, \sqsubseteq)$ est un ensemble ordonné, et cet ordre est total. En effet, soit u, v et w trois mots. On a bien $u \sqsubseteq u$ (avec $\phi = \mathrm{id}_{[\![0,|u|-1]\!]}$). Également, si $u \sqsubseteq v$ et $v \sqsubseteq u$, alors $|u| = |v|$, et par stricte croissance de ϕ, on a bien $u = v$. Aussi, si $u \sqsubseteq v$ et $v \sqsubseteq w$, alors soit ϕ l'extractrice de la suite v de u, et soit φ l'extractrice de la suite w de v. Alors, la fonction $\phi \circ \varphi$ est strictement croissante, et $\forall i \in [\![|u| - 1]\!]$, $u_i = v_{\phi(i)} = w_{\phi(\varphi(i))}$, et donc $u \sqsubseteq w$. Ainsi, la relation "$\sqsubseteq$" est une relation d'ordre.

   Montrons à présent que l'ordre est bien fondé. Soit L une partie non vide de $\Sigma^\star$. Soit $x \in L$. Si $\varepsilon \in L$, alors $x \sqsupseteq \varepsilon$.
4. Non, l'ensemble $(\wp(E), \sqsubseteq)$ n'est pas un ensemble ordonné. En effet, on pose $E = \mathbb{N}$. Soit A une partie finie de E. On sait que son plus grand élément existe, et on le note m. Par définition du maximum, $\forall y \in A$, $y \preccurlyeq m$. Et donc $A \not\sqsubseteq A$. La relation "$\sqsubseteq$" n'est donc pas une relation d'ordre (et donc encore moins un ordre bien fondé).

V.6 Définition inductive des mots et ordre préfixe

1. On pose $X_0 = \{\varepsilon\}$, et pour $n \in \mathbb{N}$,
$$X_{n+1} = X_n \cup \Big(\bigcup_{a\in\Sigma} \{a \cdot w \mid w \in X_n\} \Big).$$
   Ainsi, on définit par induction l'ensemble des mots $\Sigma^\star$.

2. Soient u et v deux mots. Montrons $u \preccurlyeq_1 v \iff u \preccurlyeq_2 v$.

" $\Longrightarrow$ " Supposons $u \preccurlyeq_1 v$. Soit $w \in \Sigma^\star$ tel que $v = uw$. Par définition de $\preccurlyeq_2$, on a bien $\varepsilon \preccurlyeq_2 w$. On décompose u en $u = u_1 \cdot u_2 \cdot \ldots \cdot u_n \cdot \varepsilon$ (avec la définition de mot de la question précédente). D'où, toujours par définition de $\preccurlyeq_2$, on a $u_n \cdot \varepsilon \preccurlyeq_2 u_n \cdot w$, puis $u_{n-1} \cdot u_n \cdot \varepsilon \preccurlyeq_2 u_{n-1} \cdot u_n \cdot w$. En itérant ce procédé, on obtient

$$\underbrace{u_1 \cdot u_2 \cdot \ldots \cdot u_n \cdot \varepsilon}_{u} \preccurlyeq_2 \overbrace{\underbrace{u_1 \cdot u_2 \cdot \ldots \cdot u_n}_{u} \cdot w}^{v}.$$

Et donc $u \preccurlyeq_2 v$.

" $\Longleftarrow$ " Supposons à présent que $u \preccurlyeq_2 v$. On pose $u = u_1 u_2 \ldots u_n$, et $v = v_1 v_2 \ldots v_m$. Par définition de $\preccurlyeq_2$, on a $u_1 \cdot (u_2 \ldots u_n) \preccurlyeq_2 u_1 \cdot (v_2 \ldots v_m)$. Puis, toujours par définition de $\preccurlyeq_2$, on a $u_1 \cdot u_2 \cdot (u_3 \ldots u_n) \preccurlyeq u_1 \cdot u_2 \cdot (v_3 \ldots v_n)$. En itérant ce procédé, on a $u \cdot \varepsilon \preccurlyeq u \cdot (v_n \ldots v_m)$. On pose $w = v_n \ldots v_m$, et on a bien $v = uw$. D'où $v \succcurlyeq_1 u$.

V.7 $\mathcal{N}$

1. On définit par induction la fonction suivante

$$\begin{aligned} \oplus : \mathcal{N}^2 &\longrightarrow \mathcal{N} \\ (\mathbf{S}(x), y) &\longmapsto \oplus(x, \mathbf{S}(y)) \\ (\mathbf{0}, x) &\longmapsto x. \end{aligned}$$

2. Soit $(x, y) \in \mathcal{N}^2$.
   - Si $f(x) = 0$, alors $\oplus(x, y) = y$ et donc $f(\oplus(x, y)) = f(y) = f(x) + f(y)$.
   - Si $f(x) \geqslant 1$, alors $x = \mathbf{S}(z)$ avec $z \in \mathcal{N}$. Ainsi, $\oplus(x, y) = \oplus(z, \mathbf{S}(y))$. Or, $f(z) = f(x) - 1 \leqslant f(x)$. Et donc, par définition de $\oplus$ puis par hypothèse d'induction, on a $f(\oplus(x, y)) = f(\oplus(z, \mathbf{S}(y)) = f(z) + f(\mathbf{S}(y))$. On en déduit que $f(\oplus(x, y)) = f(x) - 1 + f(y) + 1 = f(x) + f(y)$.

   Par induction, on a bien $\forall (x, y) \in \mathcal{N}^2,\ f\big(\oplus(x, y)\big) = f(x) + f(y)$.
3. On définit par induction la fonction suivante

$$\begin{aligned} \otimes : \mathcal{N}^2 &\longrightarrow \mathcal{N} \\ (\mathbf{S}(x), y) &\longmapsto \oplus\big(y, \otimes(x, y)\big) \\ (\mathbf{0}, y) &\longmapsto \mathbf{0}. \end{aligned}$$

4. Soit $(x, y) \in \mathcal{N}^2$.
   - Si $f(x) = 0$, alors $\otimes(x, y) = \mathbf{0}$, et donc $f(\otimes(x, y)) = 0 = f(x) \times f(y)$.
   - Si $f(x) \geqslant 1$, alors $x = \mathbf{S}(z)$ avec $z \in \mathcal{N}$. Ainsi, par définition de $\otimes$, on a $\otimes(x, y) = \oplus(y, \otimes(z, y))$. Or, par hypothèse d'induction, $f(\otimes(z, y)) = f(z) \times f(y)$ (car $f(z) < f(x)$), et donc $f(\otimes(x, y)) = f(y) + f(\otimes(z, y)) = f(y) + f(z) \times f(y) = f(y) \times (1 + f(z)) = f(y) \times f(x)$.

Par induction, on a bien $\forall (x,y) \in \mathcal{N}^2,\ f\big(\otimes(x,y)\big) = f(x) \times f(y)$.

5. On définit par induction la fonction suivante

$$\begin{aligned} ① : \mathcal{N} &\longrightarrow \mathcal{N} \\ \mathbf{0} &\longmapsto \mathbf{S}(\mathbf{0}) \\ \mathbf{S}(x) &\longmapsto \otimes\big(\mathbf{S}(x), ①(x)\big). \end{aligned}$$

6. Soit $x \in \mathcal{N}$.
   - Si $f(x) = 0$, alors $①(x) = \mathbf{S}(\mathbf{0})$ par définition, et donc $f(①(x)) = 1 = 0! = f(x)!$.
   - Si $f(x) \geqslant 1$, alors $x = \mathbf{S}(z)$ avec $z \in \mathcal{N}$. Ainsi, par définition de ①, on a $①(x) = \otimes(x, ①(z))$, et donc, par hypothèse de récurrence, $f(①(x)) = f(x) \times f(①(z)) = f(x) \times \big(f(z)!\big)$. Or, comme $f(z) = f(x) - 1$, on a donc $f(①(x)) = f(x) \times \big(f(x) - 1\big)! = f(x)!$.

   Par induction, on a bien $\forall x \in \mathcal{N},\ f\big(①(x)\big) = f(x)!$.

V.8 Résultats manquants du cours

Chapitre 2

Logique propositionnelle

V.1 Logique avec `If`

V.1.1 Représentatibilité des fonctions booléennes par formules de $\mathscr{F}_{\texttt{if}}$

1. On pose $G = \texttt{if } p \texttt{ then } \top \texttt{ else } (\underbrace{\texttt{if } q \texttt{ then } \top \texttt{ else } r}_{A})$, et on a

$$\begin{aligned}
[\![G]\!]^\rho &= [\![p]\!]^\rho \cdot [\![\top]\!]^\rho + \overline{[\![p]\!]^\rho} \cdot [\![A]\!]^\rho \\
&= \rho(p) + \overline{\rho(p)} \cdot \left([\![q]\!]^\rho \cdot [\![\top]\!]^\rho + \overline{[\![q]\!]^\rho} \cdot [\![r]\!]^\rho \right) \\
&= \rho(p) + \overline{\rho(p)} \cdot \left(\rho(q) + \overline{\rho(q)} \cdot \rho(r) \right) \\
&= \rho(p) + \overline{\rho(p)} \cdot \rho(q) + \overline{\rho(p)} \cdot \overline{\rho(q)} \cdot \rho(r) \\
&= \rho(p) + \rho(q) + \rho(r).
\end{aligned}$$

2. $$[\![\texttt{if } C \texttt{ then } G \texttt{ else } H]\!]^\rho = \begin{cases} [\![G]\!]^\rho & \text{si } [\![C]\!]^\rho = \mathbf{V} \\ [\![H]\!]^\rho & \text{if } [\![C]\!]^\rho = \mathbf{F} \end{cases}.$$

3. Soit $G \in \mathbb{F}$.

   Cas 1 Soit $\mathscr{P} = \{p\}$

   — Sous-cas 1 : $f : \rho \mapsto \mathbf{V}$ est associée à $\top$.

   — Sous-cas 2 : la fonction dont la table de vérité est ci-dessous est associée à p.

p	f
F	**F**
V	**V**

   — Sous-cas 3 : la fonction dont la table de vérité est ci-dessous est associée à $\bar{p}$.

p	f
F	**V**
V	**F**

— Sous-cas 4 : $f : \rho \mapsto \mathbf{F}$ est associée à $\bot$.

Cas 2 Soit $\mathscr{P} = \{p_1, \ldots, p_n\}$ et on pose

$$P_r : \text{“}\forall f : \mathbb{B}^{\{p_1,\ldots,p_r\}} \to \mathbb{B}, \exists G \in \mathscr{F}_{\texttt{if}}, [\![G]\!] = f.\text{”}$$

Soit $r \in [\![2, n]\!]$ et f une fonction booléenne définie sur $\mathbb{B}^{\{p_1,\ldots,p_r\}}$ à valeurs dans $\mathbb{B}$. Soit

$$\begin{aligned} g : \mathbb{B}^{\{p_1,\ldots,p_{r-1}\}} &\longrightarrow \mathbb{B} \\ \rho' &\longmapsto f\big(\rho' \uplus (p_r \mapsto \mathbf{V})\big). \end{aligned}$$

où $\uplus$ est défini comme dans l'exemple $(p \mapsto \mathbf{V}, q \mapsto \mathbf{F}) \uplus (r \mapsto \mathbf{V}) = (p \mapsto \mathbf{V}, q \mapsto \mathbf{F}, r \mapsto \mathbf{V})$. Soit alors G par hypothèse de récurrence tel que $[\![G]\!] = g$. Soit

$$\begin{aligned} h : \mathbb{B}^{\{p_1,\ldots,p_{r-1}\}} &\longrightarrow \mathbb{B} \\ \rho' &\longmapsto f\big(\rho' \uplus (p_r \mapsto \mathbf{F})\big). \end{aligned}$$

Soit alors H par hypothèse de récurrence tel que $[\![H]\!] = h$.

On pose alors $A = \texttt{if } p_r \texttt{ then } G \texttt{ else } H$. Montrons que $[\![A]\!] = f$. Soit $\rho \in \mathbb{B}^{\{p_1,\ldots,p_r\}}$.

— Si $\rho(p_r) = \mathbf{V}$ alors

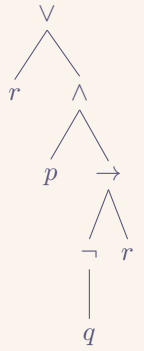
$$\begin{aligned} [\![A]\!]^\rho &= [\![G]\!]^\rho \\ &= [\![G]\!]^{\rho_{|\{p_1,\ldots,p_{r-1}\}}} \\ &= g\left(\rho_{|\{p_1,\ldots,p_{r-1}\}}\right) \\ &= f\left(\rho_{|\{p_1,\ldots,p_{r-1}\}} \uplus (p_r \mapsto \mathbf{V})\right) \\ &= f(\rho) \end{aligned}$$

— Si $\rho(p_r) = \mathbf{F}$, alors

$$\begin{aligned} [\![A]\!]^\rho &= [\![H]\!]^\rho \\ &= [\![H]\!]^{\rho_{|\{p_1,\ldots,p_{r-1}\}}} \\ &= h\left(\rho_{|\{p_1,\ldots,p_{r-1}\}}\right) \\ &= f\left(\rho_{|\{p_1,\ldots,p_{r-1}\}} \uplus (p_r \mapsto \mathbf{F})\right) \\ &= f(\rho) \end{aligned}$$

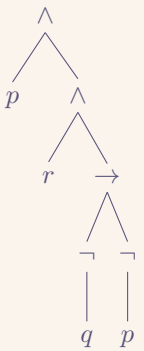
V.2 Définitions de cours : syntaxe

1. On considère la formule $H_1 = r \vee (p \wedge (\neg q \to r))$. Son arbre syntaxique est



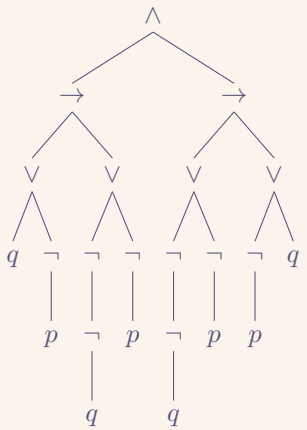
Ses sous-formules sont $r \vee (p \wedge (\neg q \to r))$, r, $p \wedge (\neg q \to r)$, p, $\neg q \to r$, $\neg q$, et q. Ses variables sont p, q et r.

2. On considère la formule $H_2 = p \wedge (r \wedge (\neg q \to \neg p))$. Son arbre syntaxique est



Ses sous-formules sont $p \wedge (r \wedge (\neg q \to \neg p))$, p, $r \wedge (\neg q \to \neg p)$, r, $\neg q \to \neg p$, $\neg q$, q, et $\neg p$. Ses variables sont p, q et r.

3. On considère la formule $H_3 = ((q \vee \neg p) \to (\neg\neg q \vee \neg p)) \wedge ((\neg\neg q \vee \neg p) \to (\neg p \vee q))$. Son arbre syntaxique est



Ses sous-formules sont $((q \vee \neg p) \to (\neg\neg q \vee \neg p)) \wedge ((\neg\neg q \vee \neg p) \to (\neg p \vee q))$, $(q \vee \neg p) \to (\neg\neg q \vee \neg p)$, $(\neg\neg q \vee \neg p) \to (\neg p \vee q)$, $q \vee \neg p$, $\neg\neg q \vee \neg p$, $\neg p \vee q$,

q, $\neg p$, $\neg\neg q$, p, et $\neg q$. Ses variables sont p et q.

V.3 Formules duales

1. On définit par induction $(\cdot)^\star$ comme

   — $\top^\star = \bot$;
   — $\bot^\star = \top$;
   — $(G \vee H)^\star = G^\star \wedge H^\star$;
   — $(G \wedge H)^\star = G^\star \vee H^\star$;
   — $(\neg G)^\star = \neg G^\star$;
   — $p^\star = p$.

2. Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. Montrons, par induction, $P(H)$: " $[\![H^\star]\!]^\rho = [\![\neg H]\!]^{\bar\rho}$ " où $\bar\rho : p \mapsto \overline{\rho(p)}$.
   — On a $[\![\bot^\star]\!]^\rho = [\![\top]\!]^\rho = \mathbf{V}$, et $[\![\neg\bot]\!]^{\bar\rho} = [\![\top]\!]^{\bar\rho} = \mathbf{V}$, d'où $P(\bot)$.
   — On a $[\![\top^\star]\!]^\rho = [\![\bot]\!]^\rho = \mathbf{F}$, et $[\![\neg\top]\!]^{\bar\rho} = [\![\bot]\!]^{\bar\rho} = \mathbf{F}$, d'où $P(\top)$.
   — Soit $p \in \mathscr{P}$. On a $[\![p^\star]\!]^\rho = [\![p]\!]^\rho = \rho(p)$, et $[\![\neg p]\!]^{\bar\rho} = \overline{[\![p]\!]^{\bar\rho}} = \overline{\bar\rho(p)} = \overline{\overline{\rho(p)}} = \rho(p)$, d'où $P(p)$.

   Soient F et G deux formules.
   — On a

$$\begin{aligned}[\![(F \wedge G)^\star]\!]^\rho &= [\![F^\star \vee G^\star]\!]^\rho \\ &= [\![F^\star]\!]^\rho + [\![G^\star]\!]^\rho \\ &= [\![\neg F]\!]^{\bar\rho} + [\![\neg G]\!]^{\bar\rho} \\ &= [\![\neg F \vee \neg G]\!]^{\bar\rho} \\ &= [\![\neg(F \wedge G)]\!]^{\bar\rho}\end{aligned}$$

   d'où $P(F \wedge G)$.
   — On a

$$\begin{aligned}[\![(F \vee G)^\star]\!]^\rho &= [\![F^\star \wedge G^\star]\!]^\rho \\ &= [\![F^\star]\!]^\rho \cdot [\![G^\star]\!]^\rho \\ &= [\![\neg F]\!]^{\bar\rho} \cdot [\![\neg G]\!]^{\bar\rho} \\ &= [\![\neg F \wedge \neg G]\!]^{\bar\rho} \\ &= [\![\neg(F \vee G)]\!]^{\bar\rho}\end{aligned}$$

   d'où $P(F \vee G)$.
   — On a

$$[\![(\neg F)^\star]\!]^\rho = [\![\neg(F^\star)]\!]^\rho = \overline{[\![F^\star]\!]^\rho} = \overline{[\![\neg F]\!]^{\bar\rho}} = [\![\neg(\neg F)]\!]^{\bar\rho}.$$

   d'où $P(\neg F)$.

   Par induction, on en conclut que $P(F)$ est vraie pour toute formule F.
3. Soit G une formule valide. Alors, par définition, $G \equiv \top$. Or, d'après la question précédente, $G^\star \equiv (\top)^\star = \bot$. Ainsi, $G^\star$ n'est pas satisfiable.

V.4 Conséquence sémantique

1. Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. On suppose $[\![A \vee B]\!]^\rho = \mathbf{V}$, $[\![A \to C]\!]^\rho = \mathbf{V}$ et $[\![B \to C]\!]^\rho = \mathbf{V}$.
   - Si $[\![A]\!]^\rho = \mathbf{V}$, alors, comme $[\![A \to C]\!]^\rho = \mathbf{V}$, $[\![C]\!]^\rho = \mathbf{V}$.
   - Si $[\![B]\!]^\rho = \mathbf{V}$, alors, comme $[\![B \to C]\!]^\rho = \mathbf{V}$, $[\![C]\!]^\rho = \mathbf{V}$.

   D'où $\{A \vee B, A \to C, B \to C\} \models C$.
2. Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. On suppose $[\![A \to B]\!]^\rho = \mathbf{V}$. Si $[\![B]\!]^\rho = \mathbf{F}$ (i.e. $[\![\neg B]\!]^\rho = \mathbf{V}$), alors $[\![A]\!]^\rho = \mathbf{F}$, par implication. Et donc, $[\![\neg A]\!]^\rho = \mathbf{V}$. On a donc bien $[\![\neg B \to \neg A]\!]^\rho$. On en déduit que $A \to B \models \neg B \to \neg A$.
3. oui
4. non
5. oui
6. non
7. oui
8. non
9. oui
10. non

V.5 Axiomatisation algèbre de Boole

1. On pose, pour $t \in \mathbb{T}$, $P(t)$: "$t \simeq 0$ ou $t \simeq 1$," et on démontre cette propriété par induction.
   - On a bien $P(\mathbf{0})$ et $P(\mathbf{1})$.
   - Soient $t_1, t_2 \in \mathbb{T}$.
     (a) Si $t_1 \simeq \mathbf{1}$, alors $\bar{t}_1 \simeq \bar{\mathbf{1}} \simeq \bar{\bar{\mathbf{0}}} \simeq \mathbf{0}$; si $t_1 \simeq \mathbf{0}$, alors $\bar{t}_1 \simeq \bar{\mathbf{0}} \simeq \mathbf{1}$.
     (b) Si $t_1 \simeq \mathbf{0}$, alors $t_1 \cdot t_2 \simeq \mathbf{0} \cdot t_2 \simeq \mathbf{0}$; si $t_1 \simeq \mathbf{1}$, alors $t_1 \cdot t_2 \simeq \mathbf{1} \cdot t_2 \simeq t_2$ (qui est équivalent à $\mathbf{0}$ ou $\mathbf{1}$).
     (c) Si $t_1 \simeq \mathbf{1}$, alors $t_1 + t_2 \simeq \mathbf{1} + t_2 \simeq \mathbf{1}$; si $t_1 \simeq \mathbf{0}$, alors $t_1 + t_2 \simeq \mathbf{0} + t_2 \simeq t_2$ (qui est équivalent à $\mathbf{0}$ ou $\mathbf{1}$)
2. En reprenant les relations trouvées dans la question précédente, on construit les tables ci-dessous.

t_1	t_2	$t_1 \cdot t_2$
0	**0**	**0**
0	**1**	**0**
1	**0**	**0**
1	**1**	**1**

t_1	t_2	$t_1 + t_2$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**1**

t_1	$\bar{t}_1$
0	**1**
1	**0**

V.6 Exercice 6 : Barre de Scheffer

1. — $\neg H_1 \equiv H_1$ nand H_1 ;
   — $H_1 \wedge H_2 \equiv \neg(H_1 \text{ nand } H_2) \equiv (H_1 \text{ nand } H_1) \text{ nand } (H_2 \text{ nand } H_2)$;
   — $H_1 \vee H_2 \equiv \neg H_1 \text{ nand } \neg H_2 \equiv (H_1 \text{ nand } H_1) \text{ nand } (H_2 \text{ nand } H_2)$;
   — $H_1 \to H_2 \equiv H_1 \vee (\neg H_2) \equiv (H_1 \text{ nand } H_1) \text{ nand } H_2$;
   — $H_1 \leftrightarrow H_2 \equiv (H_1 \to H_2) \wedge (H_2 \to H_1)$.
2. — $\neg H_1 \equiv H_1$ nor H_1 ;
   — $H_1 \vee H_2 \equiv \neg(H_1 \text{ nor } H_2) \equiv (H_1 \text{ nor } H_2) \text{ nor } (H_1 \text{ nor } H_2)$;
   — $H_1 \wedge H_2 \equiv (\neg H_1) \text{ nor } (\neg H_2) \equiv (H_1 \text{ nor } H_1) \text{ nor } (H_2 \text{ nor } H_2)$;
   — $H_1 \to H_2 \equiv H_1 \vee (\neg H_2) \equiv \neg(H_1 \text{ nor } (\neg H_2)) \equiv (H_1 \text{ nor } (H_2 \text{ nor } H_2)) \text{ nor } (H_1 \text{ nor } (H_2 \text{ nor } H_2))$;
   — $H_1 \leftrightarrow H_2 \equiv (H_1 \to H_2) \wedge (H_2 \to H_1)$.

V.7 Énigmes en logique propositionnelle

V.7.1 Fraternité

1. Ou les deux mentent, ou les deux disent la vérité. D'où $(A_1 \wedge C_1) \vee (\neg A_1 \wedge \neg C_1)$.
2. On a $A_1 = G \vee R$, et $C_1 = \neg G$.
3. On développe l'expression trouvée dans la question 1. :

$$\begin{aligned}(A_1 \wedge C_1) \vee (\neg A_1 \wedge \neg C_1) \equiv & \big((G \vee R) \wedge \neg G\big) \vee \big(\neg(G \vee R) \wedge \neg\neg G\big) \\ \equiv & (G \wedge \neg G \vee R \wedge \neg G) \vee \big((\neg G \wedge \neg R) \wedge G\big) \\ \equiv & (\bot \vee R \wedge \neg G) \vee (\neg G \wedge G \wedge \neg R) \\ \equiv & (R \wedge \neg G) \vee (\bot \wedge \neg R) \\ \equiv & (R \wedge \neg G) \vee \bot \\ \equiv & R \wedge \neg G.\end{aligned}$$

   La cérémonie se tiendra donc dans le réfectoire et non dans le gymnase.
4. $H = (A_2 \wedge B_2 \wedge C_2) \vee (\neg A_2 \wedge \neg B_2 \wedge \neg C_2)$.
5. $A_2 = E_1 \vee E_3$, $B_2 = E_2 \to \neg E_3$, $C_2 = E_1 \wedge \neg E_2$.
6.

E_1	E_2	E_3	A_2	B_2	C_2	H
F	**F**	**F**	**F**	**V**	**F**	**F**
F	**F**	**V**	**F**	**V**	**F**	**F**
F	**V**	**F**	**F**	**V**	**F**	**F**
F	**V**	**V**	**F**	**F**	**F**	**V**
V	**F**	**F**	**F**	**V**	**V**	**F**
V	**F**	**V**	**V**	**V**	**V**	**V**
V	**V**	**F**	**F**	**V**	**F**	**F**
V	**V**	**V**	**V**	**F**	**F**	**F**

   L'escalier 3 conduit bien à l'intronisation.
7. Si les trois mentent, alors on peut aussi prendre l'escalier 2.

V.7.2 Alice au pays des merveilles

1. $I_R = \bar{J} \wedge B$, $I_J = \bar{R} \to \bar{B}$, et $I_B = B \wedge (\bar{R} \vee \bar{J})$.
2. Oui, la situation où le flacon jaune contient le poison ($\bar{J}$) satisfait ces formules.
3. Oui, on a $I_B \models I_R$.
4. Oui, les instructions sur le flacon rouge et le bleu sont fausses. En effet, le flacon jaune ne contient pas de poison, et il n'y a pas "au moins l'un des deux autres flacons contenant du poison."
5. Oui, comme vu précédemment, la configuration où le poison est seulement dans le flacon jaune est valide. Si le flacon rouge contient du poison ou le flacon bleu contient du poison, on a une contradiction avec l'une des instructions. La configuration trouvée précédemment est la seule valide.
6. À cette condition, deux autres configurations sont possibles : le poison est dans les flacons jaune et rouge, ou le poison est dans les flacons rouge et bleu.

V.7.3 Socrate et Cerbère

1. On a $H = (I_1 \wedge I_2 \wedge I_3) \vee (\neg I_1 \wedge \neg I_2 \wedge \neg I_3)$.
2. On a $I_1 = C_1 \wedge C_3$, $I_2 = C_2 \to \bar{C}_3$, et $I_3 = C_1 \wedge \bar{C}_2$.
3.

C_1	C_2	C_3	I_1	I_2	I_3	H
F	**F**	**F**	**F**	**V**	**F**	**F**
V	**F**	**F**	**F**	**V**	**V**	**F**
F	**V**	**F**	**F**	**V**	**F**	**F**
V	**V**	**F**	**F**	**V**	**F**	**F**
F	**F**	**V**	**F**	**V**	**F**	**F**
V	**F**	**V**	**V**	**V**	**V**	**V**
F	**V**	**V**	**F**	**F**	**F**	**V**
V	**V**	**V**	**V**	**F**	**F**	**F**

   Socrate doit suivre le couloir 3.
4. En supposant que Cerbère ait menti, on suppose que les trois têtes ont menti, et donc que I_1, I_2 et I_3 sont fausses. On aurait aussi pu choisir le couloir 2.

V.8 Compléments de cours, en vrac

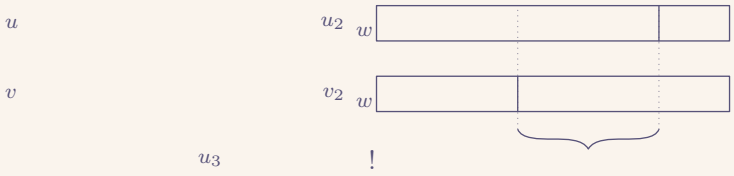
1. *Montrer que $\models$ est une relation d'ordre sur $\mathscr{F}$.*
   - Soit F une formule. On sait que $F \models F$. En effet, pour tout $\rho \in \mathbb{B}^{\mathscr{P}}$, si $[\![F]\!]^\rho = \mathbf{V}$, alors $[\![F]\!]^\rho = \mathbf{V}$. La relation $\models$ est donc reflective.
   - Soient F et G deux formules. On suppose $F \models G$ et $G \models H$. Montrons que $F \equiv G$. On reprend la démonstration du cours : soit $\rho \in \mathbb{B}^{\mathscr{P}}$. On suppose $[\![G]\!]^\rho = \mathbf{V}$, alors $[\![F]\!] = \mathbf{V}$ car $G \models H$; et donc $[\![G]\!]^\rho = [\![F]\!]^\rho$. On suppose à présent que $[\![G]\!]^\rho = \mathbf{F}$, alors, par contraposée, $[\![F]\!]^\rho = \mathbf{F}$; on a donc $[\![G]\!]^\rho = [\![F]\!]^\rho$. On en déduit que $[\![G]\!] = [\![F]\!]$, i.e. $G \equiv F$. La relation est donc *quasi*–anti-symétrique.
   - Soient F, G et H trois formules. On suppose $F \models G$ et $G \models H$. Soit $\rho \in \mathbb{B}^{\mathscr{P}}$. Si $[\![F]\!]^\rho = \mathbf{V}$, alors $[\![G]\!]^\rho = \mathbf{V}$. Or, comme $G \models H$, si $[\![G]\!]^\rho = \mathbf{V}$, alors $[\![H]\!]^\rho = \mathbf{V}$. D'où $[\![F]\!]^\rho = \mathbf{V} \implies [\![H]\!]^\rho = \mathbf{V}$. On a donc $F \models H$. La relation $\models$ est donc transitive.
2. Soit $A \in \mathscr{F}$, soit $\rho \in \mathbb{B}^{\mathscr{P}}$, et soit $\sigma \in \mathscr{P}^{\mathscr{F}}$. On pose, pour $p \in \mathscr{P}$, $\tau(p) = [\![\sigma(p)]\!]^\rho$. *Montrons que* $[\![A[\sigma]]\!]^\rho = [\![A]\!]^\tau$.

Chapitre 3

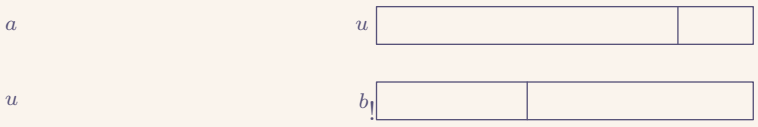
Langages et expressions régulières

V.1 Propriétés sur les mots

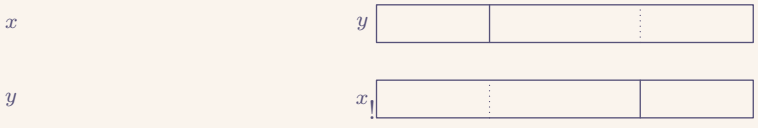
1. Soit $u_2, v_2 \in \Sigma^\star$ tels que $w = uu_2$ et $w = vv_2$. Si $|u_2| = |v_2|$, alors $u = v = v\varepsilon$ donc v est préfixe de u. Si $|u_2| < |v_2|$, u_2 est suffixe de v_2. Soit $u_3 \in \Sigma^\star$ tel que $v_2 = u_2u_3$. Ainsi, $w = vu_3u_2 = uu_2$, d'où $u = vu_3$. On en déduit que v est un préfixe de u. Similairement, si $|u_2| > |v_2|$, par symétrie du problème, en inversant u et v, puis u_2 et v_2, on se trouve bien dans le cas précédent. Ainsi, on a bien u est un préfixe de v.



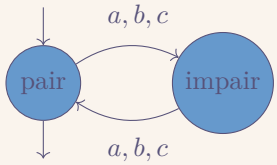
2. Soit $u = u_1 \dots u_n$ avec, pour tout $i \in [\![1, n]\!]$, $u_i \in \Sigma$. Or, $au = ub$ donc $au_1 \dots u_n = u_1 \dots u_n b$ donc, pour tout $i \in [\![1, n-1]\!]$, $u_i = u_{i+1}$. Or, $u_1 = a$. De proche en proche, on a $\forall i \in [\![1, n]\!]$, $u_i = a$. Or, $u_n = b$ et donc $a = b$. On en déduit également que $u \in a^\star$.

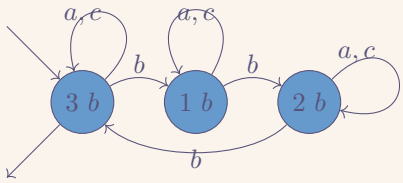


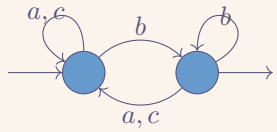
3. La suite de la correction de cet exercice est disponible sur *cahier-de-prepa*.

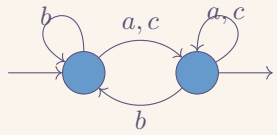


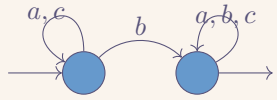
V.2 Construction d'automates

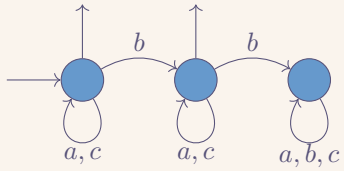
1.


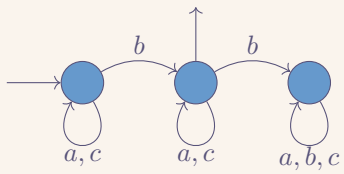
2.


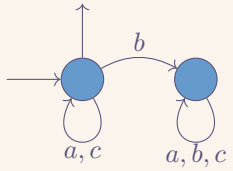
3.


4.


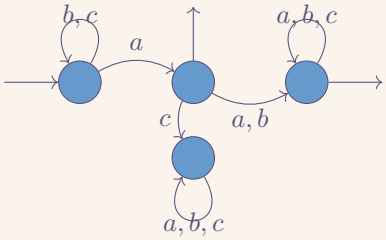
5.


6.


7.


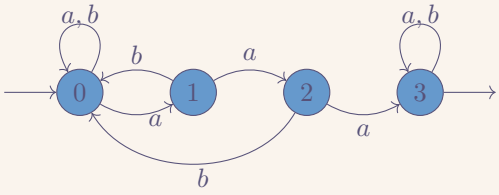
8.


9.

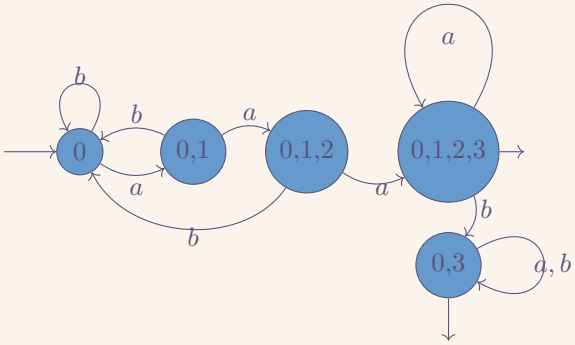


V.3 Déterminisation 1

1.

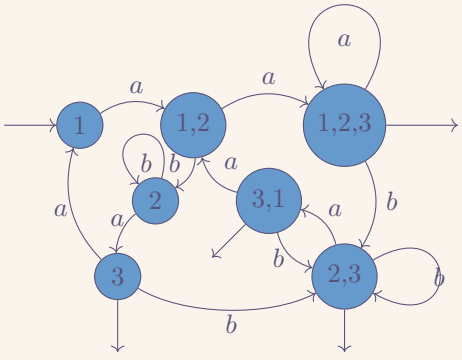


2.

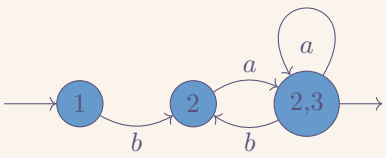


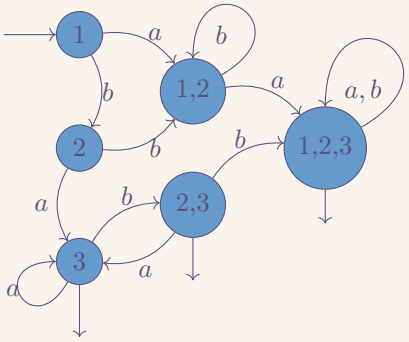
V.4 Déterminisation 2

1.



2.



3. 

V.5 Une équivalence sur les mots

La correction de cet exercice est disponible sur *cahier-de-prepa*.

V.6 Langages

La correction de cet exercice est disponible sur *cahier-de-prepa*.

V.7 Propriétés sur les opérations régulières

1. On a
$$\star = \{\varepsilon\}\ ; \qquad \cdot A = \ ; \qquad \{\varepsilon\} \cdot A = A.$$

2. *(1)* On procède par double-inclusion.
   - "$\subseteq$" Soit $w \in (A \cdot B) \cdot C$. On pose $w = u \cdot v$ avec $u \in A \cdot B$ et $v \in C$. On pose ensuite $u = x \cdot y$ avec $x \in A$ et $y \in B$. Or, comme l'opération "$\cdot$," pour les mots, est associative, on a bien $w = (x \cdot y) \cdot v = x \cdot (y \cdot v)$, et donc $w \in A \cdot (B \cdot C)$.
   - "$\supseteq$" Soit $w \in A \cdot (B \cdot C)$. On pose $w = u \cdot v$ avec $u \in A$ et $v \in B \cdot C$. On pose ensuite $v = x \cdot y$ avec $x \in B$ et $y \in C$. Or, comme l'opération "$\cdot$," pour les mots, est associative, alors $w = u \cdot (x \cdot y) = (u \cdot x) \cdot y$ et donc $w \in A \cdot (B \cdot C)$.

   (2) On suppose $A \subseteq B$. On a donc $B = A \cup (B \setminus A)$, et par définition $A^\star = \bigcup_{n\in\mathbb{N}} A^n$, et $B^\star = \bigcup_{n\in\mathbb{N}} B^n$. Montrons par récurrence, pour $n \in \mathbb{N}$, $P(n)$: "$A^n \subseteq B^n$."
   - On a $A^0 = \{\varepsilon\} \subseteq B^0 = \{\varepsilon\}$ d'où $P(0)$.
   - Soit $n \in \mathbb{N}$ tel que $A^n \subseteq B^n$. On a $A^{n+1} = A^n \cdot A$ et $B^{n+1} = B^n \cdot B$. Or, comme $A^n \subseteq B^n$ et $A \subseteq B$, et que "$\cdot$"est croissant (dans l'inclusion), on en déduit que $A^{n+1} \subseteq B^{n+1}$. D'où $P(n+1)$.

   (3) On procède par double-inclusion.
   - "$\supseteq$" On a $A^\star = (A^\star)^1 \subseteq \bigcup_{n\in\mathbb{N}} (A^\star)^n = (A^\star)^\star$.
   - "$\subseteq$" Soit $w \in (A^\star)^\star$. On pose donc $w = u_1 \dots u_n$ avec, pour tout $i \in [\![1, n]\!]$, $u_i \in A^\star$. On pose également, pour tout $i \in [\![1, n]\!]$,

$u_i = v_{i,1} \dots v_{i,m_i}$ où, pour tout $j \in [\![1, m_i]\!]$, $v_{i,j} \in A$. D'où, $w = v_{11} \dots v_{1,m_1} v_{21} \dots v_{2,m_2} \dots v_{n,m_n} \in A^\star$. On en déduit que $(A^\star)^\star \subseteq A^\star$.

(4) On procède par double-inclusion.

"$\subseteq$" On a $\{\varepsilon\} \subseteq A^\star$ et donc $A^\star = A^\star \cdot \{\varepsilon\} \subseteq A^\star \cdot A^\star$. D'où $A^\star \subseteq A^\star \cdot A^\star$.

"$\supseteq$" Soit $w \in A^\star \cdot A^\star$. On décompose ce mot : soient $u_1, u_2 \in A^\star$ tels que $w = u_1 \cdot u_2$. On pose $n = |u_1|$, et $m = |u_2|$. On décompose également ces deux mots : soient $(w_1, w_2, \dots, w_n) \in A^n$ et $(w_{n+1}, w_{n+2}, \dots, w_{n+m}) \in A^m$ tels que $u_1 = w_1 \cdot w_2 \cdot \dots \cdot w_n$ et $u_2 = w_{n+1} \cdot w_{n+2} \cdot \dots \cdot w_{n+m}$. Ainsi,

$$w = w_1 \cdot w_2 \cdot \dots \cdot w_n \cdot w_{n+1} \cdot \dots \cdot w_{n+m} \in A^\star.$$

D'où $A^\star \cdot A^\star \subseteq A^\star$.

(5) On procède par double-inclusion.

"$\subseteq$" Soit $w \in A \cup B$.

— Si $w \in A$, alors $w \in A^\star$, et donc $w = w \cdot \varepsilon \in A^\star \cdot B^\star$.

— Si $w \in B$, alors $w \in B^\star$, et donc $w = \varepsilon \cdot w \in A^\star \cdot B^\star$.

On a donc bien $A \cup B \subseteq A^\star \cdot B^\star$, et par croissance de l'étoile, on a bien $(A \cup B)^\star \subseteq (A^\star \cdot B^\star)^\star$.

"$\supseteq$" Soit $w \in (A^\star \cdot B^\star)^\star$. On pose

$$\begin{aligned} w = \; & u_{11} \dots u_{1,n_1} v_{11} \dots v_{1,m_1} \\ & \cdot u_{21} \dots u_{2,n_2} v_{21} \dots v_{2,n_2} \\ & \vdots \\ & \cdot u_{p,1} \dots u_{p,n_p} v_{p,1} \dots v_{p,m_p} \end{aligned}$$

où, $u_{i,j} \in A$ et $v_{i,j} \in B$. On a donc $w \in (A \cup B)^\star$.

(6) On procède par double-inclusion.

"$\subseteq$" Soit $w \in A \cdot (B \cup C)$. On pose $w = u \cdot v$ avec $u \in A$ et $v \in B \cup C$.

— Si $v \in B$, alors $w = u \cdot v \in A \cdot B$ et donc $w \in (A \cdot B) \cup (A \cdot C)$.

— Si $v \in C$, alors $w = u \cdot v \in A \cdot C$ et donc $w \in (A \cdot B) \cup (A \cdot C)$.

On a bien montré $A \cdot (B \cup C) \subseteq (A \cdot B) \cup (A \cdot C)$.

"$\supseteq$" Soit $w \in (A \cdot B) \cup (A \cdot C)$.

— Si $w \in A \cdot B$, on pose alors $w = u \cdot v$ avec $u \in A$ et $v \in B \subseteq B \cup C$. Ainsi, on a bien $w = u \cdot v \in A \cdot (B \cup C)$.

— Si $w \in A \cdot C$, on pose alors $w = u \cdot v$ avec $u \in A$ et $v \in C \subseteq B \cup C$. Ainsi, on a bien $w = u \cdot v \in A \cdot (B \cup C)$.

On a bien montré $A \cdot (B \cup C) \supseteq (A \cdot B) \cup (A \cdot C)$.

3. *(1)* Soit $A = \{a\}$ et $B = \{b\}$ avec $a \neq b$. On sait que $abab \in (A \cdot B)^\star$. Or, $abab \notin A^\star \cdot B^\star$ donc $L_1 \not\subseteq L_2$. De plus, $a \in A^\star \cdot B^\star$ et $a \notin (A \cdot B)^\star$ donc $L_2 \not\subseteq L_1$. Il n'y a aucune relation entre L_1 et L_2.

(2) On sait que $(A \cdot B)^\star \subseteq (A^\star \cdot B^\star)^\star$ (car $A \cdot B \subseteq A^\star \cdot B^\star$ et par croissance de l'étoile). Mais, $(A \cdot B)^\star \not\supseteq (A^\star \cdot B^\star)^\star$. En effet, avec $A = \{a\}$ et $B = \{b\}$ où $a \neq b$, on a $ba \in (A^\star \cdot B^\star)^\star$ (d'après la question précédente) mais $ba \notin (A \cdot B)^\star$. On a donc seulement $L_1 \subseteq L_2$.

(3) On a $L_1 \subseteq L_2$. En effet, $A \cap B \subseteq B$ donc $(A \cap B)^\star \subseteq B^\star$ par croissance l'étoile. De même, $A \cap B \subseteq A$ donc $(A \cap B)^\star \subseteq A^\star$. D'où $(A \cap B)^\star \subseteq A^\star \cap B^\star$. Mais, $L_1 \not\supseteq L_2$. En effet, avec $A = \{a\}$ et $B = \{aa\}$, on a $A \cap B =$ et donc $L_1 = (A \cap B)^\star = \{\varepsilon\}$, mais, $L_2 = A^\star \cap B^\star = B^\star$ (car $A^\star \subseteq B^\star$), et donc $L_2 \not\subseteq L_1$.

(4) Comme $A^\star \subseteq (A \cup B^\star)$ et $B^\star \subseteq (A \cup B)^\star$, alors $A^\star \cup B^\star \subseteq (A \cup B)^\star$. Mais, $A^\star \cup B^\star \not\supseteq (A \cup B)^\star$. En effet, si $A = \{a\}$ et $B = \{b\}$ où $a \neq b$, alors on a $ba \in (A \cup B)^\star$ mais $ba \notin A^\star \cup B^\star$. On a donc seulement $L_1 \subseteq L_2$.

(5) On a $L_1 \subseteq L_2$. En effet, soit $w \in A \cdot (B \cap C)$. On pose $w = u \cdot v$ avec $u \in A$ et $v \in B \cap C$. Comme $v \in B$, alors $w = u \cdot v \in A \cdot B$. De même, comme $v \in C$, alors $w = u \cdot v \in A \cdot C$. On a donc bien $w \in (A \cdot B) \cap (A \cdot C)$. D'où $L_1 \subseteq L_2$. Mais, $L_1 \not\supseteq L_2$. En effet, avec $A = \{a, aa\}$, $B = \{b\}$ et $C = \{ab\}$ où $a \neq b$, on a $aab \notin B \cap C =$ mais, $aab \in A \cdot B$ et $aab \in A \cdot C$, donc $aab \in L_2$. On a donc seulement $L_1 \subseteq L_2$.

(6) On a, d'après la question 2.

$$L_1 = (A^\star \cup B)^\star = \big((A^\star)^\star \cdot B^\star\big)^\star = (A^\star \cdot B^\star)^\star = (A \cup B)^\star = L_2.$$

V.8 Habitants d'expressions régulières

1. *(1)* Les mots de taille 1, 2, 3 et 4 de $\big((ab)^\star \mid a\big)^\star$ sont a, aa, ab, aaa, $aaaa$, $abab$, aba, $abaa$, aab, $aaab$ et $aaba$.

   (2) On sait, tout d'abord, que l'expression régulière $\big(a \cdot \big((b \cdot b)^\star \mid (a \cdot)\big) \cdot b\big) \big| \varepsilon$ est équivalente à $\big(a \cdot (bb)^\star \cdot b\big)$. Les mots de taille 1, 2, 3 et 4 sont donc $abbb$ et ab.

2. *(1)* Les mots de taille 1, 2 et 3 de $(a \mid b)^\star \cdot (a \mid c)^\star$ sont a, b, c, aa, bb, cc, ab, ac, bc, ba, ca, aaa, bbb, ccc, aac, aab, bbc, bba, cca, aba, abc, baa, aca, acc, abb, bca, bcc, cac, bab et caa.

   (2) Les mots de taille 1, 2 et 3 de $(a \cdot b)^\star \mid (a \cdot c)^\star$ sont ab et ac.

V.9 Regexp Crossword

`https://regexcrossword.com/`

V.10 Description d'automates au moyen d'expression régulières

1. $(a \mid b)^\star \cdot a \cdot b \cdot b \cdot a \cdot (a \mid b)^\star$;
2. $a^\star \cdot a \cdot b^\star$;
3. $\big(a \cdot (ab)^\star\big) \mid \big(a \cdot a \cdot (ba)^\star\big)$;
4. $(aa) \cdot (aa)^\star$.

V.11 Vocabulaire des automates

On représente, ci-dessous, l'automate $\mathscr{A}$ décrit dans l'énoncé.

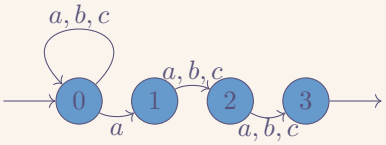


FIGURE 3.1 – Automate décrit dans l'énoncé de l'exercice 8

1. Cet automate n'est pas complet : à l'état 0, la lecture d'un a peut conduire à l'état 0 ou bien à l'état 1.
2. Le mot *baba* est reconnu par $\mathcal{A}$ mais pas le mot *cabcb*.
3. L'automate reconnaît les mots dont la $3^{\underline{\text{ème}}}$ lettre du mot, en partant de la fin, est un a.

V.12 Complétion d'automate

1. Non, cet automate n'est pas complet. Par exemple, la lecture d'un b à l'état 1 est impossible.
2. Cet automate reconnaît le langage $L = \mathscr{L}\big(a \cdot b \cdot (a \mid b)^\star\big)$.
3.

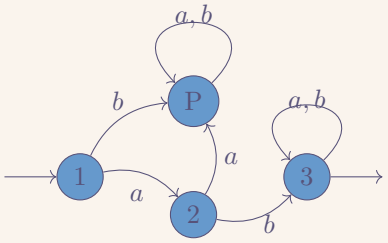


FIGURE 3.2 – Automate complet équivalent à $\mathcal{A}$

V.13 Exercice supplémentaire 1

1. *Montrer que l'ensemble des langages reconnaissables est stable par complémentaire.*
2. *Montrer que l'ensemble des langages reconnaissables est stable par intersection.*

1. Soient $\mathcal{A} = (\Sigma, \mathbb{Q}, I, F, \delta)$ et $\mathcal{A}' = (\Sigma, \mathbb{Q}', I', F', \delta')$ deux automates déterministes complets, tels que $\mathscr{L}(\mathcal{A}) = \mathscr{L}(\mathcal{A}')$. Alors

$$\mathscr{L}\big(\Sigma, \mathbb{Q}', I', \mathbb{Q}' \setminus F', \delta'\big) = \Sigma^\star \setminus \mathscr{L}(\mathcal{A}).$$

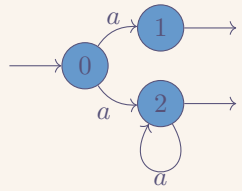
2. On utilise les lois de DE MORGAN en passant au complémentaire les deux automates, puis l'union (que l'on a vu en cours), et on repasse au complémentaire.

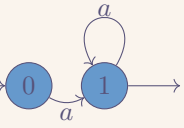
Chapitre 4

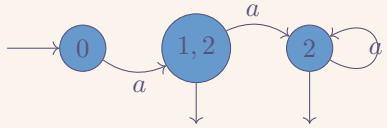
Langages et expressions régulières (2)

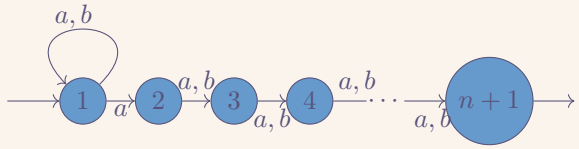
V.1 Déterminisation de taille exponentielle

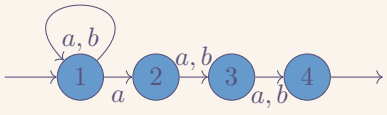
1. En notant n le nombre d'états de $\mathscr{A}$, alors le nombre d'états de $\det(\mathscr{A})$ est, au plus, 2^n. En effet, les états sont des éléments de $\wp(Q)$ et $|\wp(Q)| = 2^n$.

2. $\mathscr{A}$: 

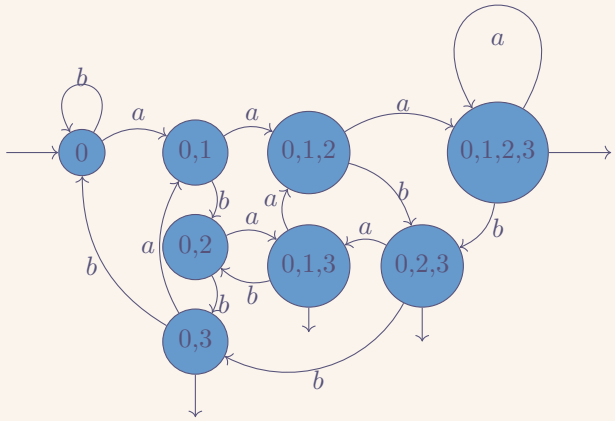
$\mathscr{B}$: 

mais $\det(\mathscr{A})$: 

3. $\mathscr{A}_n$: 

4. $\mathscr{A}_3$: 

et, $\det(\mathscr{A}_3)$:

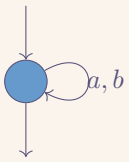


5. Soit $i_0 = \max\{k \in [\![1, n]\!] \mid u_k \neq v_k\}$. Soit $m \in \Sigma^{i_0}$ tel que $u \cdot m \in L_n$ mais $v \cdot m \notin L_n$. Or, $\delta^\star(i, u \cdot m) = \delta^\star(\delta^\star(i, u), m)$ et $\delta^\star(i, v \cdot m) = \delta^\star(\delta^\star(i, v), m)$. D'où $\delta^\star(i, u \cdot m) \in F$ et $\delta^\star(i, v \cdot m) \notin F$. Ce qui est absurde.
6. Ainsi, l'application

$$\begin{aligned} f : \Sigma^\star &\longrightarrow Q \\ u &\longmapsto \delta^\star(i, u) \end{aligned}$$

est injective. D'où, $\mathscr{D}_n = |Q| \geqslant |\Sigma^\star| = 2^n$.
7. D'où, d'après les questions 1 et 6, on en déduit que le nombre d'états utilisés pour la déterminisation de $\mathscr{A}_n$ est de $\mathscr{D}_n \geqslant 2^n$.

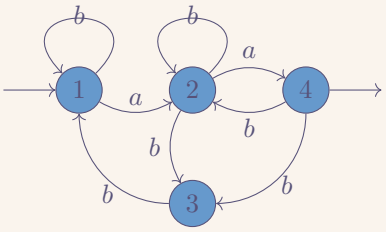
V.2 Suppression des ε-transitions



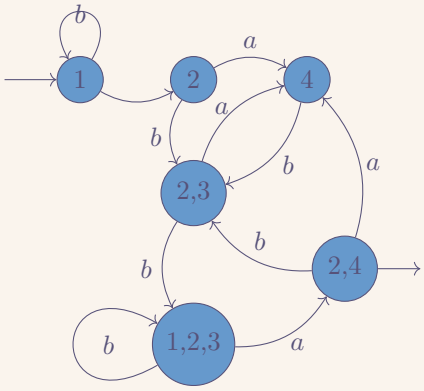
V.3 Déterminisation d'automates avec ε-transitions

Pour les deux automates, on commence par supprimer les ε-transitions, puis on le déterminise.

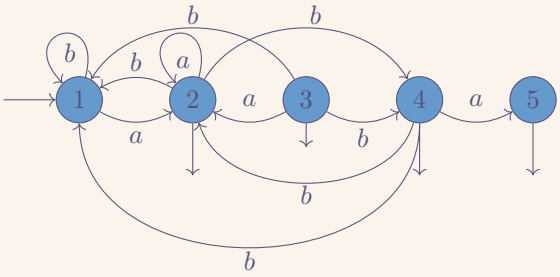
1. L'automate équivalent sans ε-transitions est le suivant.



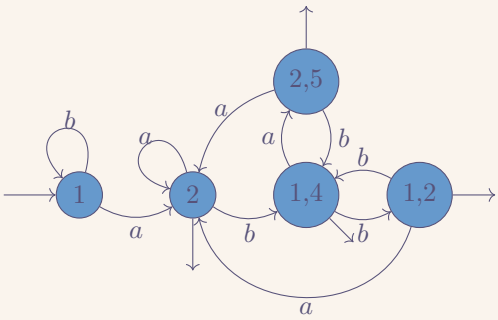
Une fois déterminisé, on obtient l'automate ci-dessous.



2. L'automate équivalent, sans ε-transitions, est le suivant.



Une fois déterminisé, on obtient l'automate ci-dessous.

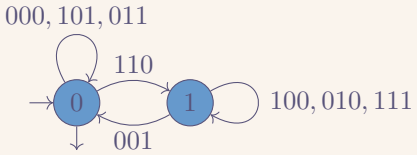


V.4 Automates pour le calcul de modulo

V.5 Automates pour le calcul de l'addition en binaire

V.5.1 Nombres de même tailles

Q. 1



Q. 2 Pour $r \in \{0,1\}$, il existe une exécution dans $\mathscr{A}$ étiquetée par

$$(u_0,v_0,w_0)(u_1,v_1,w_1)\dots(u_{n-1},v_{n-1},w_{n-1})$$

menant à r si et seulement si

$$\overline{u_0\dots u_{n-1}}^2+\overline{v_0\dots v_{n-1}}^2=\overline{w_0\dots w_{n-1}}^2+r\,2^n,$$

ce qui est équivalent à si et seulement si

$$\overline{u_0\dots u_{n-1}0}^2+\overline{v_0\dots v_{n-1}0}^2=\overline{w_0\dots w_{n-1}r}^2.$$

Q. 3 Prouvons-le par récurrence.

— Pour $n=0$, il existe une exécution dans $\mathscr{A}$ étiquetée par ε menant à $r=0$ si et seulement si $\overline{\varepsilon}^2+\overline{\varepsilon}^2=0=\overline{\varepsilon}^2+0\times 2^0$. De même, il existe une exécution dans $\mathscr{A}$ étiquetée par ε menant à $r=1$ si et seulement si $\overline{\varepsilon}^2+\overline{\varepsilon}^2=0=1=\overline{\varepsilon}^2+1\times 2^0$.

Chapitre 5

Langages et expressions régulières (3)

V.1 Exercice 4

Q. 1

Algorithme : *Entrée* : Un automate $\mathscr{A}$;
Sortie : $\mathscr{L}(\mathscr{A}) =$;
On fait un parcours en largeur depuis les états initiaux et on regarde si on atteint un état final.

Algorithme (Nathan F.) **:** *Entrée* : Deux automates $\mathscr{A}$ et $\mathscr{B}$
Sortie : $\mathscr{L}(\mathscr{A}) = \mathscr{L}(\mathscr{B})$; Soit $\mathscr{C}$ l'automate reconnaissant $\mathscr{L}(\mathscr{A}) \triangle \mathscr{L}(\mathscr{B})$.
On retourne $\mathscr{L}(\mathscr{C}) \stackrel{?}{=}$ à l'aide de l'algorithme précédent.

Autre possibilité, on procède par double inclusion :

Algorithme ($\subseteq$) **:** *Entrée* : Deux automates $\mathscr{A}$ et $\mathscr{B}$
Sortie : $\mathscr{L}(\mathscr{A}) \subseteq \mathscr{L}(\mathscr{B})$; On retourne $\mathscr{A} \setminus \mathscr{B} \stackrel{?}{=}$.

Q. 2 L'algorithme reconnaissant $\mathscr{L}(\mathscr{A}) \triangle \mathscr{L}(\mathscr{B})$ doit être déterminisé, sa complexité est donc au moins de 2^n.

V.2 Exercice 5

1. On a $e = a(ab \mid b^\star) \mid a$, $f = a_1(a_2b_1 \mid b_2^\star) \mid a_3$et $f_\varphi = e$ où

$$\varphi : \left(\begin{array}{lcl} \forall i,\ a_i & \longmapsto & a \\ \forall i,\ b_i & \longmapsto & b \end{array} \right).$$

D'où

	Λ	P	S	F
a_1		a_1	a_1	
a_2		a_2	a_2	
$b_2^\star$	ε	b_2	b_2	b_1b_2
$a_2b_1 \mid b_2^\star$	ε	a_2, b_2	b_1, b_2	a_2b_1, b_2b_2
a_3		a_3	a_3	
$a_1(a_2b_1 \mid b_2^\star)$		a_1	b_1, b_2, a_1	$a_1a_2, a_1b_2, a_2b_1, b_2b_2$
f		a_1, a_3	b_1, b_2, a_3, a_1	$a_1a_2, a_1b_2, a_3b_1, b_2b_2$

.

Automate à faire...

2. On pose $e = (\varepsilon \mid a)^\star \cdot ab \cdot (a \mid b)^\star$ et $f = (\varepsilon \mid a_1)^\star \cdot a_2b_1 \cdot (a_3 \mid b_2)^\star$ et

$$\varphi : \left(\begin{array}{lcl} \forall i,\ a_i & \longmapsto & a \\ \forall i,\ b_i & \longmapsto & b \end{array} \right)$$

d'où $f_\varphi = e$.

V.3 Exercice 6 : Langages reconnaissables ou non

Q. 7 *Le carré d'un langage est le langage $L_2 = \{u \cdot u \mid u \in L\}$. Si L est reconnaissable, L_2 est-il nécessairement reconnaissable ?*

Avec $\Sigma = \{a, b\}$, soit $L = \mathscr{L}(a^\star \cdot b^\star)$. On a donc $L_2 = \{a^n \cdot b^m \cdot a^n \cdot b^m \mid (n, m) \in \mathbb{N}^2\}$. Supposons L_2 reconnaissable. Soit $\mathscr{A}$ un automate à n états reconnaissant L_2. On pose $u = a^{2n} \cdot b^n \cdot a^{2n} \cdot b^n \in L_2$. D'après le lemme de l'étoile, il existe $(x, y, z) \in (\Sigma^\star)^3$ tel que $u = x \cdot y \cdot z$, $|xy| \leqslant n$, $\mathscr{L}(x \cdot y^\star \cdot z) \subseteq L_2$, et $y \neq \varepsilon$. Ainsi, il existe $m \in [\![1, n]\!]$ et $p \in [\![1, n]\!]$ tels que $y = a^m$, $x = a^p$ et $z = a^{2n-m-p} \cdot b^n \cdot a^{2n} \cdot b^n$. Et alors, $x \cdot y^2 \cdot z = a^p \cdot a^{2m} \cdot a^{n-m-p} \cdot b^n \cdot a^{2n} \cdot b^n = a^{2n+m} \cdot b^n \cdot a^{2n} \cdot b^n \notin L_2$.

Q. 5 *Le langage $L_5 = \{a^{n^3} \mid n \in \mathbb{N}\}$ est-il reconnaissable ?* Soit $\mathscr{A}$ un automate à N états, et soit $u = a^{N^3}$. D'après le lemme de l'étoile, il existe $(x, y, z) \in (\Sigma^\star)^3$ tel que $u = x \cdot y \cdot z$, $|xy| \leqslant N$, $\mathscr{L}(x \cdot y^\star \cdot z) \subseteq L_5$ et $y \neq \varepsilon$. D'où $x \cdot y^0 \cdot z \in L$, et donc $a^{N^3-i} \in L$, avec $i \leqslant N$. Or, $\forall k \in \mathbb{N}$, $N^3 - i \neq k^3$, ce qui est absurde.

Chapitre 6

Algorithmes probabilistes

V.1 Exercice 1 : Vérification d'égalité polynomiale

1. Étant donnés deux tableaux représentant deux polynômes, on peut calculer leurs produit en concaténant ce tableau. La complexité du produit de polynômes avec cet algorithme est en $\mathcal{O}(nm)$ où n est le degré du 1er polynôme, et m est le degré du second. En effet, *dans le pire des cas*, tous les polynômes représentant les deux polynômes sont des monômes, or, la concaténation étant en $\mathcal{O}(nm)$ (pour un tableau de taille n et un de taille m). D'où la complexité en $\mathcal{O}(nm)$.
2. Afin d'évaluer ces polynômes, on utilise l'algorithme de Horner, qui est en $\mathcal{O}(n)$, donc en temps linéaire.
3. En développant ces polynômes, la complexité serait en $\mathcal{O}(n^3)$. En effet, la multiplication de deux polynômes de degrés n a une complexité en $\mathcal{O}(n^2)$. D'où la complexité en $\mathcal{O}(n^3)$ pour la multiplication de deux polynômes ayant chacun un degré n.
4. Un polynôme de degré n a, au plus, n racines. D'où, le polynôme $P - Q$, a au plus n racines (où $n = \max(\deg P, \deg Q)$). Ainsi, s'il a $n+1$ racines, c'est alors le polynôme nul, et donc $P = Q$.

Algorithme 6.1 Algorithme déterministe pout tester l'égalité polynomiale en $\mathcal{O}(n^2)$

Entrée : $P = (P_i)_{i \in [\![1,m]\!]}$ et $Q = (Q_j)_{j \in [\![1,p]\!]}$ deux polynômes
$n \leftarrow \deg P$
pour $i \in [\![0, n]\!]$ **faire**
  si $P(i) \neq Q(i)$ **alors** ▷ *Avec l'algorithme de Horner, évaluation en $\mathcal{O}(n)$*
    retourner Non
retourner Oui

5.

Algorithme 6.2 Algorithme probabiliste pout tester l'égalité polynomiale en $\mathcal{O}(n)$

Entrée $P = (P_i)_{i\in[\![1,n]\!]}$ et $Q = (Q_j)_{j\in[\![1,n]\!]}$ deux polynômes, et $k \in \mathbb{N}$ un entier

```
1 : x ← 𝒰([[1, k × n]])
2 : si P(x) ≠ Q(x) alors
3 :     retourner Non
4 : retourner Oui
```

Soit X la variable aléatoire de $\mathcal{U}([\![1, k \times n]\!])$. L'événement "$P \neq Q$ mais l'algorithme retourne Oui" arrive si $X \in \{j \in [\![1, kn]\!] \mid P(j) = Q(j)\} = A$. Or $|A| \leqslant n$, et $A \subseteq [\![1, kn]\!]$. Ainsi, l'événement a une probabilité de $\frac{1}{k}$.

V.2 Test de primalité probabiliste

V.2.1 Résultats mathématiques

1. — Élément neutre : soit $x \in G_n$, d'où $x \cdot 1 = 1 \times x \bmod n = x \bmod n$, et donc $1 \in G_n$ est l'élément neutre de G_n.
   — Associativité : par associativité de $\times$, et par le fait que "mod" soit une congruence, on en conclut que $\cdot$ est associative.
   — Soient $x, y \in G_n$. Ainsi, $x \cdot y = x \times y \bmod n$. Or, $x \times y \wedge n = 1$, et donc $x \cdot y \wedge n = 1$.
   — Soit $x \in G_n$, donc $x \wedge n = 1$. D'où, d'après le théorème de Bézout, il existe u et $v \in \mathbb{Z}$ deux entiers tels que $u \times x + v \times n = 1$. D'où $1 \bmod n = u \times x + v \times n \bmod n$ et donc $1 = u \times x \bmod n$. Ainsi $x^{-1} = u \in G_n$, car $u \neq 0$.
2. On sait que $1 \in E_n$. Soit $y \in E_n$, d'où $y^{n-1} \equiv 1\ [n]$, i.e. $y \times (y^{n-2}) \equiv 1\ [n]$, donc $y^{n-2} \in E_n$ est l'inverse de y. Soient x et $y \in E_n$. On a $(x \cdot y^{-1})^{n-1} \equiv x^{n-1} \cdot y^{n-1}\ [n] \equiv 1\ [n]$. D'où $x \cdot y^{-1} \in E_n$. Ainsi, E_n est un sous-groupe de $(G_n, \cdot)$.
3. Soit n composé. Il existe $a \in [\![1, n-1]\!]$ tel que $a^{n-1} \not\equiv 1\ [n]$, et donc $E_n \subsetneq G_n$. Or, *le cardinal d'un sous-groupe divise le cardinal du groupe*, et donc $|E_n| \mid |G_n| \leqslant n - 1$, donc $|E_n| \leqslant \frac{n-1}{2}$.

V.2.2 Algorithme

4.

Algorithme 6.3 Algorithme Monte-Carlo testant la primalité d'un nombre en $\mathcal{O}(k\,(\ln k)^3$

Entrée $n \in \mathbb{N}$ et $k \in \mathbb{N}$ deux entiers.

```
1 : pour j ∈ [[1, k]] faire
2 :     a ← 𝒰([[1, n − 1]])
3 :     si a^{n−1} mod n ≠ 1 alors
4 :         retourner Non
5 : retourner Oui
```

En effet, si $|E_n| \leqslant \frac{n-1}{2}$, donc si $a \sim \mathcal{U}(\llbracket 1, n-1 \rrbracket)$, d'où $P(a \in E_n) \leqslant \frac{1}{2}$. La probabilité que l'algorithme échoue est inférieure à $\frac{1}{2^k}$.

V.2.3 Implémentation

Indications Pour calculer $a^b \bmod c$, on décompose b en base 2 : $b = \sum_{i=1}^{p} b_i 2^i$, et donc

$$a^b \bmod c = \left(\prod_{i=1}^{p} a^{b_i 2^i}\right) \bmod c = \prod_{i=0}^{p} \left(a^{b_i 2^i} \bmod c\right).$$

Et, $p \sim \log_2(n)$.

V.3 Exercice 3 : Échantillonnage

Q. 1

Algorithme 6.4 Échantillonnage naïf

Entrée T un tableau à n éléments, et $k \in \mathbb{N}$ avec $k \leqslant n$

1 : $T \leftarrow$ Mélanger(T)
2 : $R \leftarrow T[0..k]$
3 : **retourner** R

Q. 2 Un invariant de boucle est « $\forall p \in \llbracket 0, I-1 \rrbracket$, $P(T[p] \in \mathsf{Res}) = \frac{k}{I}$ et $\forall p \in \llbracket I, n \rrbracket$, $T[p] \notin \mathsf{Res}$ »

Q. 3 Notons $\underline{I}$ et $\underline{\mathsf{Res}}$ l'état des variables avant un tour de boucle ; et, $\bar{I}$ et $\overline{\mathsf{Res}}$ l'état des variables après un tour de boucle.

— Pour $k = I$, on a

1. $\forall p \in \llbracket 0, k-1 \rrbracket$, $P(T[p] \in \mathsf{Res}) = 1$,
2. $\forall p \in \llbracket k, n-1 \rrbracket$, $T[p] \notin \mathsf{Res}$,
3. $I \leqslant n$.

— Supposons $\underline{I}$, et $\underline{\mathsf{Res}}$ vérifiant l'invariant et la condition de boucle. Alors, on a

1. $\forall p \in \llbracket 0, \underline{I}-1 \rrbracket$, $P(T[p] \in \underline{\mathsf{Res}}) = \frac{k}{\underline{I}}$,
2. $\forall p \in \llbracket \underline{I}, n-1 \rrbracket$, $T[p] \notin \underline{\mathsf{Res}}$,
3. $\underline{I} < n$, la condition de boucle.

Soit $j \in \llbracket 0, \underline{I} \rrbracket$. On a $\bar{I} = \underline{I} + 1$.

Cas 1 $j < k$, et donc $\overline{\mathsf{Res}}(j) = T[\underline{I}]$, et $\forall \ell \neq j$, $\overline{\mathsf{Res}}[\ell] = \underline{\mathsf{Res}}[\ell]$.

Cas 2 $j \geqslant k$, et donc $\forall \ell$, $\overline{\mathsf{Res}}[\ell] = \underline{\mathsf{Res}}[\ell]$.

1. Soit $p \in [\![0, \underline{I}]\!]$. Montrons $P(T[p] \notin \overline{\mathsf{Res}}) = \frac{k}{I}$. Si $p < \underline{I}$, alors

$$\begin{aligned} P(T[p] \in \overline{\mathsf{Res}}) &= P\big(T[p] \in \underline{\mathsf{Res}} \cap j \neq p\big) \\ &= \frac{k}{\underline{I}} \times \frac{\underline{I}}{\underline{I}+1} \\ &= \frac{k}{\underline{I}}. \end{aligned}$$

Si $P = \underline{I}$, alors d'après 2. $T[p] \notin \underline{\mathsf{Res}}$, donc $P(T[p] \in \overline{\mathsf{Res}}) = P(j < k) = \frac{k}{I+1}$.

Chapitre 7

Décidabilité, Calculabilité

V.1 Quelques problèmes décidables

1. Soit $f : \mathbb{R} \to \mathbb{R}$.
   - Si f admet un zéro, on pose $\mathscr{M} =$ `fun s` $\to$ `true`.
   - Si f n'admet pas un zéro, on pose $\mathscr{M} =$ `fun s` $\to$ `false`.

   Alors, $\mathscr{M}$ décide $\textsc{Zero}_f$.
2. Soit $\mathscr{M}$ une machine, et soit $w \in \Sigma^\star$.
   - Si $\mathscr{M}$ se termine sur l'entrée w, alors on pose $\mathscr{M}' =$ `fun s` $\to$ `true`.
   - Si $\mathscr{M}$ ne se termine pas sur l'entrée w, alors on pose $\mathscr{M}' =$ `fun s` $\to$ `false`.

   Alors, $\mathscr{M}'$ décide $\textsc{Arrêt}_{\mathscr{M},w}$.
3. Le problème est trivialement vrai. En effet, soit $M \in \mathbb{6}$, de la forme

   ```
   let m (s: string): string =
     ⟨code⟩
   ```

   On crée la machine $\mathscr{N}$ ci-dessous.

   ```
   let n (s: string): string =
     if true then
       ⟨code⟩
     else
       ⟨code⟩
   ```

   On a $\mathtt{m} \neq \mathtt{n}$, mais $\mathscr{L}(\mathtt{m}) = \mathscr{L}(\mathtt{n})$, donc le problème est vrai sur toute entrée et la fonction `fun s` $\to$ `true` répond au problème.

V.2 Sérialisation de types énumérés

1. Pour sérialiser une liste, on utilise la fonction `serialise_couple` définie dans le cours.

```
let rec serialise_liste (t: 'a list) (serialise:
    ↪ 'a -> string): string =
  match s with
  | [] -> ""
  | x :: q -> serialise_couple (serialise x) (
      ↪ serialise_liste t serialise)
```

CODE 7.1 – Sérialisation de listes

2. Soit $(\varphi_{i,j})_{\substack{i\in[\![1,m]\!]\\ j\in[\![1,n_i]\!]}}$ sérialisant le type $\mathtt{t}_{i,j}$. Soit

$$\varphi_i : (x_1, \dots, x_{n_i}) \longmapsto \text{“(”} \hat{} \ \varphi_{i,1}(x_1) \hat{} \text{“),(”} \hat{} \dots \hat{} \ \varphi_{i,n_i}(x_{n_i}) \hat{} \text{“)”}.$$

```
let rec serialise_enum (e : enumeration) : string
    ↪  =
  let rec aux (i: int) (j: int)
  match e with
  | C1(e1,1,...,e1,n1) ->
    serialise_couple (1, φ1(e1,...,en1))
  | ...
  | Cm(em,1,...,em,nm) ->
    serialise_couple (m, φm(e1,...,enm))
```

CODE 7.2 – Serialisation de types énumérés

V.3 Stabilité de la classe des langages décidables

1. Soit L un langage fini. On pose donc $L = \{w_1, \dots, w_n\}$. On code donc la fonction ci-dessous.

```
let decide_L (w: string): bool =
  match w with
  | w1 -> true
  | ...
  | wn -> true
  | _ -> false
```

CODE 7.3 – Fonction décidant d'un langage fini

Autre preuve : tout langage fini est régulier, et tout langage régulier est reconnaissable, et est donc décidable.

2. Soient L_1 et L_2 deux langages décidables. Soit $\texttt{decide}_{L_1}$ et $\texttt{decide}_{L_2}$ décidant respectivement L_1 et L_2. On code la fonction $\texttt{decide}_{L_1 \cdot L_2}$:

```
let decide_{L1·L2} (w: string) : bool =
  let m = String.length w in
  let rep = ref false in
  for i = 0 to n - 1 do
    if decide_{L1} w|_{[0,i]} && decide_{L2} w|_{[i+1,n-1]} then
      rep := true
  done;
  !rep
```

CODE 7.4 – Fonction décidant d'une concaténation de langages décidables

3.
4. Tout langage singleton est décidable. Soit $L_{\text{ArrêT}}$ l'ensemble

$$L_{\text{ArrêT}} = \{\texttt{serialise\_couple}\ M\ w \mid M \text{ s'arrête sur } w\}.$$

Le langage $L_{\text{ArrêT}}$ est indécidable. Mais, $L_{\text{ArrêT}} = \bigcup_{x \in L_{\text{ArrêT}}} \{x\}$, est une union dénombrable.

V.4 Non monotonie du caractère décidable des langages

1. *Montrer qu'il existe trois langages A, B et C tels que $A \subseteq B \subseteq C$, que A soit décidable, B indécidable et C décidable.*
2. *Montrer qu'il existe A, B et C trois langages tels que $A \subseteq B \subseteq C$, que A soit indécidable, B décidable, et C indécidable.*

1. On pose $A = $, et $C = \Sigma^\star$, et $B = \{(M, w) \mid M \text{ s'arrête sur } w\}$.
2. Soit $w \in \Sigma^\star$. On pose

$$L_0 = \{\texttt{serialise\_couple}(w, M) \mid M \in L_{\text{ArrêtUniv}}{}^{1}\}.$$

Montrons que le langage L_0 est indécidable. Soit $M \in \mathcal{O}$ une entrée du problème ArrêtUniv.

$$\begin{aligned}\texttt{serialise\_couple}(w, M) \in L_0 &\iff M \text{ s'arrête sur toutes ses entrées} \\ &\iff M \in \text{ArrêtUniv}^+.\end{aligned}$$

En effet, la fonction f de cette réduction est définie comme ci-dessous.

```
let f (M : string) : string =
  serialise_couple w M
```

Par réduction de ArrêtUniv à Appartient_{L_0}, le problème Appartient_{L_0} est indécidable.

On pose ensuite

$$L_1 = \{\texttt{serialise\_couple}(M, w) \mid w \in \Sigma^\star, M \in L_{\text{ArrêtUniv}}\}.$$

Soit $M \in \mathcal{O}$ une entrée du problème ArrêtUniv. La fonction g de cette réduction est définie comme ci-dessous.

```
let g (M: string) : string =
  serialise_couple M "a"
```

$$\begin{aligned}g(M) \in L_1 &\iff \begin{cases}\texttt{"a"} \in \Sigma^\star \\ M \in \text{ArrêtUniv}^+\end{cases} \\ &\iff M \in \text{ArrêtUniv}^+\end{aligned}$$

On pose $w =$ "`fun` $s \to$ `true`." On a $L_0 \subseteq L \subseteq L_2$ où

$$L = \{\texttt{serialise\_couple}(\text{“}\texttt{fun}\ s \to \texttt{true}\text{”}, w) \mid w \in \Sigma^\star\}.$$

Le langage L est décidable. En effet, le code ci-dessous décide du problème $\textsc{Appartient}_L$.

```
let decide_L (w: string) : bool =
  let m = String.length w in
  w.[n - 1] = ')' && w_|[0,15]| = "(fun␣s␣->␣true)("
```

V.5 Réduction

1. Soit $\texttt{m}, w$ les entrées du problème de l'Arrêt. On fabrique la sérialisation de machine

   "`fun s` $\to$ `execute` $\{\{\texttt{m}\}\}$ $\{\{w\}\}$."

   Notons $M'_{\texttt{m},w}$ cette machine. On a

   $$\begin{aligned} M'_{\texttt{m},w} \in \textsc{ArrêtUniv}^+ &\iff \forall x \in \Sigma^\star, \texttt{execute m}\ w \text{ se termine} \\ &\iff \texttt{execute m}\ w \text{ se termine} \\ &\iff (\texttt{m}, w) \in \textsc{Arrêt}^+ \end{aligned}$$

   Ainsi, on crée la réduction.

   ```
   let reduction (s: string): string =
     let (m, w) = deserialise_couple s in
     "fun␣x␣->␣execute␣" ^ m ^ "␣" ^ w
   ```

   Code 7.5 – Réduction de ArrêtUniv au problème de l'Arrêt

   Ainsi, ArrêtUniv est indécidable par réduction.
2. Réduisons le problème Arrêt à ArrêtSimult. Soit $\texttt{m}, w$ les données du problème de l'Arrêt. Posons les machines $M_{\texttt{m},w} =$ "`fun` $x \to$ `execute` $\{\{\texttt{m}\}\}$ $\{\{w\}\}$", et N : "`fun` $x \to 3$." On a

   $$\begin{aligned} &\texttt{serialise\_couple}(M_{\texttt{m},w}, N) \in \textsc{Arrêt}^+ \\ \iff &\big(\forall x \in \Sigma^\star, \quad \texttt{execute}\ M_{\texttt{m},w}\ x \text{ termine} \iff \texttt{execute}\ N\ x \text{ termine}\big) \\ \iff &\big(\texttt{execute}\ \{\{\texttt{m}\}\}\ \{\{w\}\} \text{ termine} \iff \mathbf{V}\big) \\ \iff &\texttt{execute}\ \{\{\texttt{m}\}\}\ \{\{w\}\} \text{ termine} \\ \iff &(\texttt{m}, w) \in \textsc{Arrêt}^+. \end{aligned}$$

   Autre possibilité : réduisons ArrêtUniv à ArrêtSimult. On pose N : "`fun` $x \to 2$," et on a

   $$\begin{aligned} &\texttt{serialise\_couple}(M, N) \in \textsc{ArrêtSimult}^+ \\ \iff &\big(\forall x \in \Sigma^\star, \quad \texttt{execute}\ M\ x \text{ termine} \iff \texttt{execute}\ N\ x \text{ termine}\big) \\ \iff &\forall x \in \Sigma^\star, \texttt{execute}\ M\ x \text{ termine} \\ \iff &M \in \textsc{ArrêtUniv}^+. \end{aligned}$$

3. Réduisons ARRÊT à RÉGULIER. Soit $(\mathtt{m}, w)$ une entrée du problème de l'ARRÊT.

```
let reconnait_an_bn (w: string): bool =
  let n = String.length w in
  if n mod 2 = 1 then false
  else begin
      let ok = ref true in
      for i = 1 to n / 2 do
        if w.[i] = 'a' then ok := false
      done;
      for i = (n / 2) + 1 to n do
        if w.[i] = 'b' then ok := false
      done;
      !ok
    end
```

CODE 7.6 – Machine reconnaissant le langage $\{a^n \cdot b^n \mid n \in \mathbb{N}\}$

On considère la fonction de réduction ci-dessous.

```
let f (e: string): string =
  let (m, w) = deserialise_couple e in
  "fun␣s -> execute {{m}} {{w}}; reconnait_an_bn
      ↪ {{w}}"
```

En notant $(\mathtt{m}, \mathtt{w}) = \mathtt{deserialise\_couple(e)}$,

$$(f\ \mathtt{e}) \in \text{RÉGULIER}^+ \iff \text{“}\mathtt{fun}\ s \to \mathtt{execute}\{\{\mathtt{m}\}\}\{\{\mathtt{w}\}\}\text{”}.$$

Or,

— si $w \underset{\mathtt{m}}{\to} \circlearrowleft$, alors $\forall s \in \Sigma^\star$, $s \underset{\mathtt{m}}{\to} \circlearrowleft$, donc $\mathscr{L}(\mathtt{m}) = .$

— si $w \underset{\mathtt{m}}{\to} w'$, avec $w' \in \Sigma^\star$, alors

  — si $s \underset{\mathtt{m}}{\to} \mathtt{true} \iff s \in \{a^n \cdot b^n \mid n \in \mathbb{N}\}$,

  — si $s \underset{\mathtt{m}}{\to} \mathtt{false} \iff s \notin \{a^n \cdot b^n \mid n \in \mathbb{N}\}$,

  Et donc, $\mathscr{L}(\mathtt{m}) = \{a^n \cdot b^n \mid n \in \mathbb{N}\}$.

On a donc

$$\begin{aligned}(f\ \mathtt{e}) \in \text{RÉGULIER}^+ &\iff w \underset{\mathtt{m}}{\to} \circlearrowleft \\ &\iff (\mathtt{m}, w) \in \text{ARRÊT}^- \\ &\iff (\mathtt{m}, w) \in \text{COARRÊT}^+\end{aligned}$$

où le problème COARRÊT est défini comme

$$\text{COARRÊT} : \begin{cases} \textbf{Entrée} & : (\mathtt{m}, w) \\ \textbf{Sortie} & : \text{A-t-on } w \underset{\mathtt{m}}{\to} \circlearrowleft \end{cases}.$$

On a $\text{COARRÊT}^- = \text{ARRÊT}^+$, et $\text{COARRÊT}^+ = \text{ARRÊT}^-$. Le problème COARRÊT est indécidable par stabilité des problèmes décidables par complémentaire. On conclut par réduction de COARRÊT à RÉGULIER.

4. Réduisons ArrêtUniv à ArrêtExiste. Soit M une entrée du problème ArrêtExiste.

V.6 Amélioration de code

1.

```
let mort (s: string): string =
  let f (a: int) = a in
  "sortie"
```

Code 7.7 – Fonction morte

2. On réalise une réduction du problème ArrêtUniv au problème CodeMort. Soit $\mathscr{M}$ une entrée du problème ArrêtUniv. Fabriquons l'entrée M du problème CodeMort, comme montré ci-dessous.

```
let M (s: string): string =
  execute 𝓜 s;
  let f (a: string) = a in
  f x
```

Code 7.8 – Réduction de ArrêtUniv à CodeMort

Ainsi, avec cette construction de la machine M, on définition u comme `execute` $\mathscr{M}$ `s`, on définit d comme `let f (a: string) = a in`, et on définit v comme `f x`. Alors,

$$\begin{aligned} M \in \text{CodeMort}^+ &\iff \mathscr{L}(u \cdot d \cdot v) = \mathscr{L}(u \cdot v) \\ &\iff \forall \texttt{s} \in \Sigma^\star, \text{ la ligne 4 est atteinte} \\ &\iff \forall \texttt{s} \in \Sigma^\star, \texttt{execute } \mathscr{M} \texttt{ s se termine} \\ &\iff \forall \texttt{s} \in \Sigma^\star, \mathscr{M} \text{ se termine sur l'entrée } \texttt{s} \\ &\iff \mathscr{M} \in \text{ArrêtUniv}^+. \end{aligned}$$

Or, comme ArrêtUniv est indécidable, CodeMort aussi.

3.

```
let f (s: string): string =
  let x = ref 3 in
  let y = int_of_string s in
  string_of_int (!x + y)

let f (s: string): string =
  let y = int_of_string s in
```

```
8 |   string_of_int (3 + y)
```

CODE 7.9 – Variable constante

4. Soit M une entrée du problème CODEMORT. Fabriquons l'entrée $(M', \mathscr{V})$ du problème P de détection de variables constantes. Soit F l'ensemble des "fonctions locales" de M.[2] Au début de la machine M', on définit, pour chaque fonction locale $\texttt{f} \in F$, la variable $\texttt{x}_\texttt{f}$ comme `let` $\texttt{x}_\texttt{f}$ `= ref 0 in`. On pose $\mathscr{V}$ l'ensemble de ces nouvelles variables :

$$\mathscr{V} = \{\texttt{x}_\texttt{f} \mid \texttt{f} \in F\}.$$

Puis, on transforme chaque définition de fonction locale $\texttt{f} \in F$ en

```
1 | let f ⟨arguments de f⟩ =
2 |   incr x_f;
3 |   ⟨code original de f⟩
```

Ainsi,

$$\begin{aligned}(M', \mathscr{V}) \in P^+ &\iff \exists \texttt{x}_\texttt{f} \in \mathscr{V}, \text{ la variable } \texttt{x}_\texttt{f} \text{ n'est pas modifiée} \\ &\iff \exists \texttt{f} \in F, \text{ la fonction } \texttt{f} \text{ n'est pas appelée} \\ &\iff \exists \texttt{f} \in F, \texttt{f} \text{ est une fonction morte} \\ &\iff M \in \text{CODEMORT}^+.\end{aligned}$$

Or, comme le problème CODEMORT est indécidable, le problème de détection de variables constantes l'est aussi.

V.7 Théorème de Rice

V.8 Un changement de modèle de calcul

1. Pour toute machine M, on considère la *super-machine* $\mathscr{M}_M$ suivante :

```
1 | let arret (n_V: int) (x: string): bool =
2 |   let (M,w) = deserialise_couple x in
3 |   decide_ArrêtÉtapes M w n_V
```

CODE 7.10 – *Super-machine* résolvant le problème de l'ARRÊT sur une machine classique

où la fonction $\texttt{decide}_{\text{ARRÊTÉTAPES}}$ décide du problème

$$\text{ARRÊTÉTAPES} : \begin{cases} \textbf{Entrée} & : M \in \mathbb{O},\ w \in \Sigma^\star,\ n \in \mathbb{N} \\ \textbf{Sortie} & : M \text{ se termine-t-elle sur } w \text{ en moins de } n \text{ étapes élémentaires ?} \end{cases}.$$

2. S'il y a plusieurs fonctions ayant le même nom, on les numérote de telle sorte que leurs noms soient différents.

D'après le cours, ce problème est décidable. Ainsi, pour tout mot $w \in \Sigma^\star$ et toute machine M,

$$\begin{aligned} w \xrightarrow[\mathcal{M}_M]{} \mathbf{V} &\iff \exists n \in \mathbb{N},\ \texttt{arret}\ n\ (\texttt{serialise\_couple}\ M\ w) = \texttt{true} \\ &\iff \exists n \in \mathbb{N},\ M \text{ s'arrête en moins de } n \text{ étapes sur } w \\ &\iff M \text{ s'arrête sur l'entrée } w \\ &\iff (M, w) \in \textsc{Arrêt}^+. \end{aligned}$$

2. Par l'absurde, supposons le problème de l'arrêt pour les *super-machines* décidable. Soit `arret` une fonction décidant de ce problème. On considère la machine suivante.

```
let paradoxe (n: int) (w: string): bool =
  if arret n (serialise_couple w w) then
    (while true do () done; true)
  else false
```

CODE 7.11 – Programme paradoxe proubant que le problème de l'arrêt des *super-machines* est indécidable

Soit $S_{\texttt{paradoxe}}$ la sérialisation de la fonction `paradoxe` ci-dessous. Analysons l'exécution de (`paradoxe` n $S_{\texttt{paradoxe}}$). Soit $c =$ (`serialise_couple` $S_{\texttt{paradoxe}}$ $S_{\texttt{paradoxe}}$).

Chapitre 8

Classe P, classe NP

V.1 Problèmes de partitions

1. On définit les quatre problèmes comme

   SubsetSum : $\begin{cases} \textbf{Entrée} & : n \in \mathbb{N},\ (w_1, \dots, w_n) \in \mathbb{N}^n \text{ et } W \in \mathbb{N} \\ \textbf{Sortie} & : \text{Existe-t-il une partie } I \in \wp(\llbracket 1, n \rrbracket) \text{ telle que } \sum_{i \in I} w_i = W \,? \end{cases}$

   Partition : $\begin{cases} \textbf{Entrée} & : n \in \mathbb{N} \text{ et } (w_1, \dots, w_n) \in \mathbb{N}^n \\ \textbf{Sortie} & : \text{Existe-t-il } I \in \wp(\llbracket 1, n \rrbracket) \text{ telle que } \sum_{i \in I} w_i = \sum_{i \in \llbracket 1,n \rrbracket \setminus I} w_i \,? \end{cases}$

   Knapsack : $\begin{cases} \textbf{Entrée} & : n \in \mathbb{N},\ (x_1, \dots, x_n) \in \mathbb{N}^n,\ (v_1, v_2, \dots, v_n) \in \mathbb{N}^n,\ P \in \mathbb{N} \text{ et } K \in \mathbb{N} \\ \textbf{Sortie} & : \text{Existe-t-il } I \in \wp(\llbracket 1, n \rrbracket) \text{ telle que } \sum_{i \in I} x_i \leqslant P \text{ et } \sum_{i \in I} v_i \geqslant K \,? \end{cases}$

   BinPacking : $\begin{cases} \textbf{Entrée} & : n \in \mathbb{N},\ (t_1, \dots, t_n) \in \mathbb{N}^n,\ C \in \mathbb{N} \text{ et } K \in \mathbb{N} \\ \textbf{Sortie} & : \text{Existe-t-il } k \in \mathbb{N} \text{ et } (I_1, \dots, I_k) \in \wp(\llbracket 1, n \rrbracket)^k \ k \text{ parties de } \llbracket 1, n \rrbracket \\ & \quad \text{telles que } \bigcup_{i \in \llbracket 1,k \rrbracket} I_i = \llbracket 1, n \rrbracket,\ \forall i \neq j,\ I_i \cap I_j = ,\ k \leqslant K \text{ et} \\ & \quad \forall i \in \llbracket 1, k \rrbracket,\ \sum_{j \in I_i} t_j \leqslant C \,? \end{cases}$

2. (a) Soit (Ω, W) une entrée de SubsetSum. On fabrique l'entrée (Ω, Ω, W, W) du problème Knapsack. On pose $\Omega = (w_1, \dots, w_n)$ et on a

$$\begin{aligned} (\Omega, W) \in \text{SubsetSum}^+ &\iff \exists A \in \wp(\Omega),\ \sum_{w \in A} w = W \\ &\iff \exists A \in \wp(\Omega),\ \sum_{w \in A} w \geqslant W \text{ et } \sum_{w \in A} w \leqslant W \\ &\iff (\Omega, \Omega, W, W) \in \text{Knapsack}^+. \end{aligned}$$

   Cette réduction est polynômiale.

   (b) Soit Ω une entrée de Partition. On pose $\Omega = (w_1, \dots, w_n)$. Fabriquons l'entrée $(\Omega, S/2)$ du problème SubsetSum, où

$S = \sum_{i=1}^{n} w_i$. On suppose $S \equiv 0$ [2]. On a

$$\begin{aligned}\Omega \in \textsc{Partition} &\iff \exists I \subseteq [\![1,n]\!]\,,\ \sum_{i\in I} w_i = \sum_{i\in[\![1,n]\!]\setminus I} w_i \\ &\iff \exists I \subseteq [\![1,n]\!],\ \sum_{i\in I} w_i = \frac{S}{2} \\ &\iff (\Omega, S/2) \in \textsc{SubsetSum}^+\end{aligned}$$

V.2 Optimisation linéaire en nombres entiers

1. Montrons $\textsc{SysLin} \preccurlyeq_{\mathrm{p}} \textsc{SysLinIneg}$. Soient n, m, A et b les entrées du problème SysLin. Fabriquons, en temps polynômial, les entrées n', m', A', b' du problème SysLinIneg : on choisit $n' = 2n$, $m' = m$, $A' = \binom{A}{-A}$ et $b' = \binom{b}{-b}$. Ainsi,

$$\begin{aligned}(n', m', A', b') \in \textsc{SysLinIneg}^+ &\iff \exists X,\ A'X \leqslant b' \\ &\iff \exists X,\ AX \leqslant b \text{ et } -AX \leqslant -b \\ &\iff \exists X,\ AX = b \\ &\iff (n, m, A, b) \in \textsc{SysLin}^+\end{aligned}$$

V.3 Clique, Stable et Couv.Sommets

1. Soit $G = (S, A)$ un graphe. On pose $G' = (S, A')$ où $A' = \big\{\{x, y\} \in \mathscr{C}_2(S) \;\big|\; \{x, y\} \notin A\big\}$. [1]

   Prouvons la réduction de Clique à Stable. Soit (G, K) une entrée du problème Clique. Fabriquons l'entrée (G', K) de Stable, comme défini précédemment. Montrons que $(G, K) \in \textsc{Clique}^+ \iff (G', K) \in \textsc{Stable}^+$. On a

$$\begin{aligned}(G, K) \in \textsc{Clique}^+ &\iff \exists S_1 \subseteq S_2 \text{ avec } |S_1| \geqslant K,\ \forall x \neq y \in S_1,\ \{x, y\} \in A \\ &\iff \exists S_1 \subseteq S_2 \text{ avec } |S_1| \geqslant K,\ \forall x \neq y,\ \{x, y\} \notin A' \\ &\iff (G', K) \in \textsc{Stable}^+.\end{aligned}$$

   La réduction est calculable en temps polynômiale. On a donc $\textsc{Clique} \preccurlyeq_{\mathrm{p}} \textsc{Stable}$.

   La réduction de Stable à Clique est la même. Elle est également en temps polynômiale.

2. Montrons la réduction de CouvSommets à Clique. Soit (G, K) une entrée du problème CouvSommets. Fabriquons $(G', n-K)$ une entrée du problème Stable, où $G' = (S, A')$ comme défini à la question précédente,

1. On note $\mathscr{C}_p(E)$ l'ensemble des parties de E de cardinal p.

et $n = |S|$. On a

$$\begin{aligned}
&(G, K) \in \textsc{CouvSommets}^+ \\
\iff &\exists S_1 \subseteq S \text{ avec } |S_1| \leqslant K,\ \forall \{x, y\} \in A,\ x \in S_1 \text{ ou } x \in S_2 \\
\iff &\exists S_1 \subseteq S \text{ avec } |S_1| \leqslant K,\ \forall x \neq y \in S \setminus S_1,\ \{x, y\} \notin A \\
\iff &\exists S_1 \subseteq S \text{ avec } |S \setminus S_1| \leqslant |S| - K,\ \forall x \neq y \in S \setminus S_1,\ \{x, y\} \in A' \\
\iff &\exists S_2 \subseteq S \text{ avec } |S_2| \geqslant |S| - K,\ \forall x \neq y \in S_2,\ \{x, y\} \in A' \\
\iff &(G', |S| - K) \in \textsc{Stable}^+.
\end{aligned}$$

3. On représente le graphe G pour l'entrée $\{x \vee x \vee y, \neg x \vee \neg y \vee \neg y, x \vee y \vee y\}$.

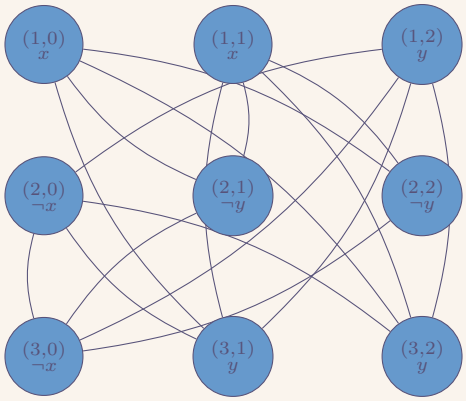


FIGURE 8.1 – Représentation du graphe G pour l'entrée $\{x \vee x \vee y, \neg x \vee \neg y \vee \neg y, x \vee y \vee y\}$

4. Montrons la réduction de 3SAT à CLIQUE. Soit $H = \{c_1, \ldots, c_m\}$ une instance de 3SAT. Construisons le graphe G comme proposé dans l'énoncé. On construit alors l'entrée de CLIQUE (G, m). Soit $(G, m) \in \textsc{Clique}^+$. C'est donc qu'il existe une clique de G de taille m ; nommons la C. Deux sommets $(i, \_)$ et $(j, \_)$ ne sont pas reliés dans G si $i = j$. Ainsi,

$$\forall i \in [\![1, m]\!]\,,\ \exists! j \in [\![0, 2]\!]\,,\ (i, j) \in C.$$

Soient p et $\neg p$ deux littéraux. Si $p \in C$, alors $\neg p \notin C$. Si $\neg p \in C$, alors $p \notin C$. On construit alors l'environnement propositionnel

$$\rho : \mathbb{Q} \longrightarrow \mathbb{B}$$
$$p \longmapsto \begin{cases} \mathbf{V} & \text{si } p \in C \\ \mathbf{F} & \text{sinon.} \end{cases}$$

Pour $i \in [\![1, m]\!]$, soit $j \in [\![0, 2]\!]$, tel que $(i, j) \in C$, on a donc $[\![\ell_{i,j}]\!]^\rho = \mathbf{V}$. On en déduit que $\forall i \in [\![1, m]\!]\,,\ [\![c_i]\!]^\rho = \mathbf{V}$. On en déduit que $[\![H]\!]^\rho = \mathbf{V}$, *i.e.* $H \in 3\textsc{sat}^+$.

Réciproquement, supposons $H \in 3\textsc{sat}^+$. Alors, soit $\rho \in \mathbb{B}^{\mathbb{Q}}$ tel que $[\![H]\!]^\rho = \mathbf{V}$. On a

$$\forall i \in [\![1, m]\!]\,,\ \exists j \in [\![0, 2]\!]\,,\ [\![\ell_{i,j}]\!]^\rho = \mathbf{V}.$$

Notons $\varphi(i)$ un tel j. On fabrique alors l'ensemble de m sommets $C = \{(i, \varphi(i)) \mid i \in [\![1, m]\!]\}$. Soient $(i, \varphi(i))$ et $(j, \varphi(j))$ deux éléments de C. Si $i \neq j$, alors $\{(i, \varphi(i)), (j, \varphi(j))\} \in A$, car $[\![\ell_{i,\varphi(i)}]\!]^\rho = \mathbf{V}$ et $[\![\ell_{j,\varphi(j)}]\!]^\rho = \mathbf{V}$. On en déduit que C est une clique de taille m. Ainsi, $(G, m) \in \textsc{Clique}^+$.

5. Comme Clique est **NP**-difficile, alors Stable et CouvSommets sont **NP**-difficile. Montrons que Clique est un problème **NP**. Le programme Clique est vérifiable en temps polynômiale : ...

V.4

Chapitre 9

Algorithmique des graphes

V.1 Arbres et forêts

V.2 Tri topologique

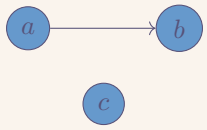


FIGURE 9.1 – Exemple de graphe

1. Dans le graphe ci-dessus, $a \to c \to b$ est un tri topologique mais pas un parcours.
2. Dans le même graphe, $b \to a \to c$ est un parcours mais pas un tri topologique.
3. Supposons que L_1 possède un prédécesseur, on le note L_i où $i > 1$. Ainsi, $(L_i, L_1) \in A$ et donc $i < 1$, ce qui est absurde. De même pour le dernier.
4. Il existe un tri topologique si, et seulement si le graphe est acyclique.

" $\Longrightarrow$ " Soit $L_1, \ldots, L_n$ un tri topologique. Montrons que le graphe est acyclique. Par l'absurde, on suppose le graphe non acyclique : il existe $(i, j) \in [\![1, n]\!]^2$ avec $i \neq j$ tels que $T_i \to \cdots \to T_j$ et $T_j \to \cdots \to T_i$ soient deux chemins valides. Ainsi, comme le tri est topologique et par récurrence, $i \leqslant j$ et $j \leqslant i$ et donc $i = j$, ce qui est absurde car i et j sont supposés différents. Le graphe est donc acyclique.

" $\Longleftarrow$ " Soit G un graphe tel que tous les sommets possèdent une arrête entrante. On suppose par l'absurde ce graphe acyclique. Soit x_0 un sommet du graphe. On construit par récurrence $x_0, x_1, \ldots, x_n, x_{n+1}, \ldots$ les successeurs successifs. Il y a un nombre fini de sommets donc deux sommets sont identiques. Donc, il y a nécessairement un cycle, ce qui est absurde.

Algorithme 9.1 Génération d'un tri topologique d'un graphe acyclique

Entrée $G = (S, A)$ un graphe acyclique
Sortie Res un tri topologique.

```
1 : Res ← [ ]
2 : tant que G ≠ ∅ faire
3 :     Soit x un sommet de G sans prédécesseur
4 :     G ← (S \ {x}, A ∩ (S \ {x})²)
5 :     Res ← Res · [x]
6 : retourner Res
```

5.

Algorithme 9.2 Génération d'un tri topologique d'un graphe

Entrée $G = (S, A)$ un graphe
Sortie Res un tri topologique, ou un cycle

```
1 : Res ← [ ]
2 : tant que G ≠ ∅ faire
3 :     si il existe x sans prédécesseurs alors
4 :         Soit x un sommet de G sans prédécesseur
5 :         G ← (S \ {x}, A ∩ (S \ {x})²)
6 :         Res ← Res · [x]
7 :     sinon
8 :         Soit x ∈ S
9 :         Soit x ← x_1 ← x_2 ← ··· ← x_i la suite des prédécesseurs
10 :        retourner x_i, x_{i+1}, ..., x_i, un cycle
11 : retourner Res
```

6. On utilise la représentation par liste d'adjacence, et on stocke le nombre de prédécesseurs que l'on décroit à chaque choix de sommet.
7. On essaie de trouver un tri topologique, et on voit si l'on trouve un cycle.

V.3 Détection de graphe biparti

V.4 Exploration du graphe $\mathfrak{S}_n$

V.5 Parcours selon le miroir d'un tri préfixe

Chapitre 10

Preuves en logique propositionnelle

V.1 Premiers arbres de preuves

1.
$$\dfrac{\dfrac{}{p \vdash p}\,\text{Ax}}{\vdash p \to p}\,{\to}\text{i}.$$

2.
$$\dfrac{\dfrac{}{p, \neg p \vdash p}\,\text{Ax} \qquad \dfrac{}{p, \neg p \vdash \neg p}\,\text{Ax}}{p, \neg p \vdash \bot}\,\neg\text{e}.$$

3.
$$\dfrac{\dfrac{}{p, q \vdash p}\,\text{Ax} \qquad \dfrac{}{p, q \vdash q}\,\text{Ax}}{p, q \vdash p \wedge q}\,\wedge\text{i}.$$

4.
$$\dfrac{\dfrac{\dfrac{}{p \wedge q \vdash p \wedge q}\,\text{Ax}}{p \wedge q \vdash q}\,\wedge\text{e,g} \qquad \dfrac{\dfrac{}{p \wedge q \vdash p \wedge q}\,\text{Ax}}{p \wedge q \vdash p}\,\wedge\text{e,d}}{p \wedge q \vdash q \wedge p}\,\wedge\text{i}.$$

5.
$$\dfrac{\dfrac{}{p \vee q \vdash p \vee q}\,\text{Ax} \qquad \dfrac{\dfrac{}{p \vee q, p \vdash p}\,\text{Ax}}{p \vee q, p \vdash q \vee p}\,\vee\text{i,d} \qquad \dfrac{\dfrac{}{p \vee q, q \vdash q}\,\text{Ax}}{p \vee q, q \vdash q \vee p}\,\vee\text{i,g}}{p \vee q \vdash q \vee p}\,\vee\text{e}.$$

6.
$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \wedge \neg p \vdash p \wedge \neg p}\,\text{Ax}}{p \wedge \neg p \vdash p}\,\wedge\text{e,g} \qquad \dfrac{\dfrac{}{p \wedge \neg p \vdash p \wedge \neg p}\,\text{Ax}}{p \wedge \neg p \vdash \neg p}\,\wedge\text{e,d}}{p \wedge q \vdash \bot}\,\neg\text{e}}{\vdash \neg(p \wedge \neg p)}\,\neg\text{i}.$$

V.2 Divers arbres de preuves

1.
$$\dfrac{\dfrac{}{p \vee (p \wedge q) \vdash p \vee (p \wedge q)}\,\text{Ax} \qquad \dfrac{}{p \vee (p \wedge q), p \vdash p}\,\text{Ax} \qquad \dfrac{\dfrac{}{p \vee (p \wedge q), p \vee q \vdash p \vee q}\,\text{Ax}}{p \vee (p \wedge q), p \vee q \vdash p}\,\wedge\text{e,g}}{p \vee (p \wedge q) \vdash p}\,\vee\text{e}.$$

2.
$$\dfrac{\dfrac{\dfrac{}{p \wedge q, r \wedge s \vdash p \wedge q}\,\text{Ax}}{p \wedge q, r \wedge s \vdash p}\,\wedge\text{e,g} \qquad \dfrac{\dfrac{}{p \wedge q, r \wedge s \vdash r \wedge s}\,\text{Ax}}{p \wedge q, r \wedge s \vdash r}\,\wedge\text{e,d}}{p \wedge q, r \wedge s \vdash p \wedge r}\,\wedge\text{i}.$$

3.
$$\dfrac{\dfrac{}{p, q \wedge r \vdash p}\,\text{Ax} \qquad \dfrac{\dfrac{}{p, q \wedge r \vdash q \wedge r}\,\text{Ax}}{p, q \wedge r \vdash q}\,\wedge\text{e,g}}{p, q \wedge r \vdash p \wedge q}\,\wedge\text{i}.$$

4.
$$\dfrac{\dfrac{\dfrac{}{p, \neg p \vdash p}\,\text{Ax} \qquad \dfrac{}{p, \neg p \vdash \neg p}\,\text{Ax}}{p, \neg p \vdash \bot}\,\neg\text{e}}{p \vdash \neg\neg p}\,\neg\text{i}.$$

5.
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p, \neg\neg\neg p, \neg p \vdash p}\,\text{Ax} \qquad \dfrac{}{p, \neg\neg\neg p, \neg p \vdash \neg p}\,\text{Ax}}{\neg\neg\neg p, p, \neg p \vdash \bot}\,\neg\text{e}}{\neg\neg\neg p, p \vdash \neg\neg p}\,\neg\text{i} \qquad \dfrac{}{\neg\neg\neg p, p \vdash \neg\neg\neg p}\,\text{Ax}}{\neg\neg\neg p \vdash \bot}\,\neg\text{e}}{\neg\neg\neg p \vdash \neg p}\,\neg\text{i}.$$

V.3 Lois de de Morgan

1.
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(p\vee q),p\vdash p}\,\mathrm{Ax}}{\neg(p\vee q),p\vdash p\vee q}\,\vee\mathrm{i,g} \quad \dfrac{}{\neg(p\vee q),p\vdash\neg(p\vee q)}\,\mathrm{Ax}}{\neg(p\vee q),p\vdash\bot}\,\neg\mathrm{e}}{\neg(p\vee q)\vdash\neg p}\,\neg\mathrm{i} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg(p\vee q),q\vdash q}\,\mathrm{Ax}}{\neg(p\vee q),q\vdash p\vee q}\,\vee\mathrm{i,d} \quad \dfrac{}{\neg(p\vee q),q\vdash\neg(p\vee q)}\,\mathrm{Ax}}{\neg(p\vee q),q\vdash\bot}\,\neg\mathrm{e}}{\neg(p\vee q)\vdash\neg q}\,\neg\mathrm{i}}{\neg(p\vee q)\vdash\neg p\wedge\neg q}\,\wedge\mathrm{i}.$$

2.
$$\dfrac{\dfrac{\dfrac{}{\neg p\vee\neg q,p\vee q\vdash p\vee q}\,\mathrm{Ax} \quad \dfrac{\dfrac{}{\neg p\wedge\neg q,p\vee q,p\vdash p}\,\mathrm{Ax} \quad \dfrac{}{\neg p\wedge\neg q,p\vee q,p\vdash\neg p\wedge\neg q}\,\mathrm{Ax}}{\neg p\wedge\neg q,p\vee q,p\vdash\neg p}\,\wedge\mathrm{e,d}}{\neg p\wedge\neg q,p\vee q,p\vdash\bot}\,\neg\mathrm{e} \quad \dfrac{\dfrac{}{\neg p\wedge\neg q,p\vee q,q\vdash q}\,\mathrm{Ax} \quad \dfrac{}{\neg p\wedge\neg q,p\vee q,q\vdash\neg p\wedge\neg q}\,\mathrm{Ax}}{\neg p\wedge\neg q,p\vee q,q\vdash\neg q}\,\wedge\mathrm{e,d}}{\neg p\wedge\neg q,p\vee q,q\vdash\bot}\,\neg\mathrm{e}}{\neg p\wedge\neg q\vdash\bot}\,\vee\mathrm{e}}{\neg p\wedge\neg q\vdash\neg(p\vee q)}\,\neg\mathrm{i}.$$

V.4 Distributivités entre $\wedge$ et $\vee$

1.
$$\dfrac{\dfrac{\dfrac{}{p\wedge(q\vee r)\vdash p\wedge(q\vee r)}\,\mathrm{Ax}}{p\wedge(q\vee r)\vdash q\vee r}\,\wedge\mathrm{e,d} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{q,p\wedge(q\vee r)\vdash p\wedge(q\vee r)}\,\mathrm{Ax}}{q,p\wedge(q\vee r)\vdash p}\,\wedge\mathrm{e,g} \quad \dfrac{}{p,q\wedge(q\vee r)\vdash q}\,\mathrm{Ax}}{q,p\wedge(q\vee r)\vdash p\vee q}\,\wedge\mathrm{i}}{q,p\wedge(q\vee r)\vdash(q\vee r)\wedge(p\wedge r)}\,\vee\mathrm{i,g} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{r,p\wedge(q\vee r)\vdash p\wedge(q\vee r)}\,\mathrm{Ax}}{r,p\wedge(q\vee r)\vdash p}\,\wedge\mathrm{e,g} \quad \dfrac{}{r,q\wedge(q\vee r)\vdash r}\,\mathrm{Ax}}{r,p\wedge(q\vee r)\vdash p\wedge r}\,\wedge\mathrm{i}}{r,p\wedge(q\vee r)\vdash(p\wedge q)\vee(p\wedge r)}\,\vee\mathrm{i,d}}{p\wedge(q\vee r)\vdash(p\wedge q)\vee(p\wedge r)}\,\vee\mathrm{e}.$$

2. On nomme $\varphi = (p \wedge q) \vee (p \wedge r)$.

$$\dfrac{\dfrac{\dfrac{}{\varphi \vdash (p \wedge q) \vee (p \wedge r)}\,\text{Ax} \quad \dfrac{\dfrac{}{\varphi, p \wedge q \vdash p \wedge q}\,\text{Ax}}{\varphi, p \wedge q \vdash p}\,\wedge\text{e,g} \quad \dfrac{\dfrac{}{\varphi, p \wedge r \vdash p \wedge r}\,\text{Ax}}{\varphi, p \wedge r \vdash p}\,\wedge\text{e,g}}{\varphi \vdash p}\,\vee\text{e} \quad \dfrac{\dfrac{}{\varphi \vdash (p \wedge q) \vee (p \wedge r)}\,\text{Ax} \quad \dfrac{\dfrac{}{\varphi, p \wedge q \vdash p \wedge q}\,\text{Ax}}{\varphi, p \wedge q \vdash q}\,\wedge\text{e,d} \quad \dfrac{\dfrac{}{\varphi, p \wedge r \vdash p \wedge r}\,\text{Ax}}{\varphi, p \wedge r \vdash r}\,\wedge\text{e,d}}{\varphi \vdash q \vee r}\,\vee\text{i,g} \quad \dfrac{}{\varphi, p \wedge r \vdash q \vee r}\,\vee\text{i,d}}{(p \wedge q) \vee (p \wedge r) \vdash p \wedge (q \vee r)}\,\wedge\text{i}\,\vee\text{e}.$$

V.5 Implications

1.

$$\dfrac{\dfrac{}{p, q \vdash q}\,\text{Ax}}{q \vdash p \to q}\,\to\text{i}$$

2.

$$\dfrac{\dfrac{\dfrac{}{p, p \wedge q \vdash p \wedge q}\,\text{Ax}}{p, p \wedge q \vdash q}\,\wedge\text{e,d}}{p \wedge q \vdash p \to q}\,\to\text{i}$$

3.

$$\dfrac{\dfrac{\dfrac{}{p, p \to q \vdash p}\,\text{Ax} \quad \dfrac{\dfrac{}{p, p \to q \vdash p \to q}\,\text{Ax} \quad \dfrac{}{p, p \to q \vdash p}\,\text{Ax}}{p, p \to q \vdash q}\,\to\text{e}}{p, p \to q \vdash p \wedge q}\,\wedge\text{i}}{p \to q \vdash p \to (p \wedge q)}\,\to\text{i}$$

4.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg q, p \to q, p \vdash p \to q}\,\text{Ax} \quad \dfrac{}{\neg q, p \to q, p \vdash p}\,\text{Ax}}{\neg q, p \to q, p \vdash q}\,\to\text{e} \quad \dfrac{}{\neg q, p \to q, p \vdash \neg q}\,\text{Ax}}{\neg q, p \to q, p \vdash \bot}\,\neg\text{e}}{\neg q, p \to q \vdash \neg p}\,\neg\text{i}}{p \to q \vdash \neg q \to \neg p}\,\to\text{i}$$

5.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \wedge q, p \to r \vdash p \wedge q}\,\text{Ax}}{p \wedge q, p \to r \vdash p}\,\wedge\text{e,g} \quad \dfrac{}{p \wedge q, p \to r \vdash p \to r}\,\text{Ax}}{p \wedge q, p \to r \vdash r}\,\to\text{e}}{p \to r \vdash (p \wedge q) \to r}\,\to\text{i}$$

6.

$$\dfrac{\dfrac{\dfrac{}{p, q \vdash p}\,\mathrm{Ax}}{p \vdash q \to p}\,{\to}\mathrm{i}}{\vdash p \to (q \to p)}\,{\to}\mathrm{i}$$

7.

$$\dfrac{\dfrac{\dfrac{}{p \to q, p \vdash p \to q}\,\mathrm{Ax} \quad \dfrac{}{p \to q, p \vdash p}\,\mathrm{Ax}}{p, p \to q \vdash q}\,{\to}\mathrm{e}}{p \vdash (p \to q) \to q}\,{\to}\mathrm{i}$$

V.6 Implications (partie 1 : simplifications)

1.

$$\dfrac{\dfrac{\dfrac{}{p, p \to \neg p \vdash p}\,\mathrm{Ax} \quad \dfrac{\dfrac{}{p, p \to \neg p \vdash p \to \neg p}\,\mathrm{Ax} \quad \dfrac{}{p, p \to \neg p \vdash p}\,\mathrm{Ax}}{p, p \to \neg p \vdash \neg p}\,{\to}\mathrm{e}}{p, p \to \neg p \vdash \bot}\,\neg\mathrm{e}}{p \to \neg p \vdash \neg p}\,\neg\mathrm{i}$$

2.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p, p \to q, \neg q \vdash p \to q}\,\mathrm{Ax} \quad \dfrac{}{p, p \to q, \neg q \vdash p}\,\mathrm{Ax}}{p, p \to q, \neg q \vdash q}\,{\to}\mathrm{e} \quad \dfrac{}{p, p \to q, \neg q \vdash \neg q}\,\mathrm{Ax}}{p, p \to q, \neg q \vdash \bot}\,\neg\mathrm{e}}{p \to q, \neg q \vdash \neg p}\,\neg\mathrm{i}$$

3.

$$\dfrac{\dfrac{}{p \to q, p \vee q}\,\mathrm{Ax} \quad \dfrac{\dfrac{\dfrac{}{p \to q, p \vee q, p \vdash p \to q}\,\mathrm{Ax} \quad \dfrac{}{p \to q, p \vee q, p \vdash p}\,\mathrm{Ax}}{p \to q, p \vee q, p \vdash q}\,{\to}\mathrm{e} \quad \dfrac{}{p \to q, p \vee q, q \vdash q}\,\mathrm{Ax}}{p \to q, p \vee q \vdash q}\,\vee\mathrm{e}$$

4.

$$\dfrac{\dfrac{\dfrac{}{p, p \to q, p \to \neg q \vdash p \to}\,\text{Ax} \quad \dfrac{}{p, p \to q, p \to \neg q \vdash p}\,\text{Ax}}{p, p \to q, p \to \neg q \vdash q}\,\to\text{e} \quad \dfrac{\dfrac{}{p, p \to q, p \to \neg q \vdash p \to \neg q}\,\text{Ax} \quad \dfrac{}{p, p \to q, p \to \neg q \vdash p}\,\to\text{e}}{p, p \to q, p \to \neg q \vdash \neg q}\,\neg\text{e}}{\dfrac{p, p \to q, p \to \neg q \vdash \bot}{p \to q, p \to \neg q \vdash \neg p}\,\neg\text{i}}$$

5. On pose $\Gamma = p, p \to (q \vee r), \neg q, \neg r, q \vee r$.

$$\dfrac{\dfrac{\dfrac{}{p, p \to (q \vee r), \neg q, \neg r \vdash p \to (q \vee r)}\,\text{Ax} \quad \dfrac{}{p, p \to (q \vee r), \neg q, \neg r \vdash p}\,\text{Ax}}{p, p \to (q \vee r), \neg q, \neg r \vdash q \vee r}\,\to\text{e} \quad \dfrac{\dfrac{}{\Gamma \vdash q \vee r}\,\text{Ax} \quad \dfrac{\dfrac{}{\Gamma, q \vdash q}\,\text{Ax} \quad \dfrac{}{\Gamma, q \vdash \neg q}\,\text{Ax}}{\Gamma, q \vdash \bot}\,\neg\text{e} \quad \dfrac{\dfrac{}{\Gamma, r \vdash r}\,\text{Ax} \quad \dfrac{}{\Gamma, r \vdash \neg r}\,\text{Ax}}{\Gamma, r \vdash \bot}\,\neg\text{e}}{p, p \to (q \vee r), \neg q, \neg r, q \vee r \vdash \bot}\,\vee\text{e}}{p, p \to (q \vee r), \neg q, \neg r \vdash \neg(q \vee r)}\,\neg\text{i}}{\dfrac{p, p \to (q \vee r), \neg q, \neg r \vdash \bot}{p \to (q \vee r), \neg q, \neg r \vdash \neg p}\,\neg\text{i}}\,\neg\text{e}$$

6. On pose $\Gamma = p \to (q \to r), p, \neg r, q$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash p \to (q \to r)}\,\text{Ax} \quad \dfrac{}{\Gamma \vdash p}\,\text{Ax}}{\Gamma \vdash q \to r}\,\to\text{e} \quad \dfrac{}{\Gamma \vdash q}\,\text{Ax}}{\Gamma \vdash r}\,\to\text{e} \quad \dfrac{}{\Gamma \vdash \neg r}\,\text{Ax}}{\dfrac{\Gamma \vdash \bot}{p \to (q \to r), p \neg r \vdash \neg q}\,\neg\text{i}}\,\neg\text{e}$$

7. On pose $\Gamma = p \to (q \to r), p, \neg r, q$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash p \to (q \to r)}\,\text{Ax} \quad \dfrac{}{\Gamma \vdash p}\,\text{Ax}}{\Gamma \vdash q \to r}\,{\to}\text{e} \quad \dfrac{}{\Gamma \vdash q}\,\text{Ax}}{\Gamma \vdash r}\,{\to}\text{e} \quad \dfrac{}{\Gamma \vdash \neg r}\,\text{Ax}}{\Gamma \vdash \bot}\,\neg\text{e}}{p \to (q \to r), p, \neg r \vdash \neg q}\,{\to}\text{i}$$

8. On pose $\Gamma = q, p \to (q \to r), q \to p$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash p \to (q \to r)}\,\text{Ax} \quad \dfrac{\dfrac{}{\Gamma \vdash q \to p}\,\text{Ax} \quad \dfrac{}{\Gamma \vdash q}\,\text{Ax}}{\Gamma \vdash p}\,{\to}\text{e}}{\Gamma \vdash q \to r}\,{\to}\text{e} \quad \dfrac{}{\Gamma \vdash q}\,\text{Ax}}{\Gamma \vdash r}\,{\to}\text{e}}{p \to (q \to r), q \to p, \vdash q \to r}\,{\to}\text{i}$$

9.

$$\dfrac{\dfrac{\dfrac{}{p \to (p \to q), p \vdash p \to (p \to q)}\,\text{Ax} \quad \dfrac{}{p \to (p \to q), p \vdash p}\,\text{Ax}}{p \to (p \to q), p \vdash p \to q}\,{\to}\text{e} \quad \dfrac{}{p \to (p \to q), p \vdash p}\,\text{Ax}}{p \to (p \to q), p \vdash q}\,{\to}\text{e}.$$

V.7 Implications (partie 2 : transformations)

1. *c.f.* Exercice 5, question 4.

2.

$$\dfrac{\dfrac{\dfrac{}{p \to q, p \wedge r \vdash p \to q}\,\text{Ax} \quad \dfrac{\dfrac{}{p \to q, p \wedge r \vdash p \wedge r}\,\text{Ax}}{p \to q, p \wedge r \vdash p}\,\wedge\text{e,g}}{p \to q, p \wedge r \vdash q}\,\to\text{e} \quad \dfrac{\dfrac{}{p \to q, p \wedge r \vdash p \wedge r}\,\text{Ax}}{p \to q, p \wedge r \vdash r}\,\wedge\text{e,g}}{\dfrac{p \to q, p \wedge r \vdash q \wedge r}{p \to q \vdash (p \wedge q) \to (q \wedge r)}\,\to\text{i}}\,\wedge\text{i}$$

3.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(p \wedge r) \to (q \wedge r), r, p \vdash (p \wedge r) \to (q \wedge r)}\,\text{Ax} \quad \dfrac{\dfrac{}{(p \wedge r) \to (q \wedge r), r, p \vdash p}\,\text{Ax} \quad \dfrac{}{(p \wedge r) \to (q \wedge r), r, p \vdash r}\,\text{Ax}}{(p \wedge r) \to (q \wedge r), r, p \vdash p \wedge r}\,\wedge\text{i}}{(p \wedge r) \to (q \wedge r), r, p \vdash q \wedge r}\,\to\text{e}}{(p \wedge r) \to (q \wedge r), r, p \vdash q}\,\vee\text{e,g}}{(p \wedge r) \to (q \wedge r), r \vdash p \wedge q}\,\to\text{i}$$

.

4.

$$\dfrac{\dfrac{}{p \to q, p \vee r \vdash p \vee r}\,\text{Ax} \quad \dfrac{\dfrac{\dfrac{}{p \to q, p \vee r, p \vdash p \to q}\,\text{Ax} \quad \dfrac{}{p \to q, p \vee r, p \vdash p}\,\text{Ax}}{p \to q, p \vee r, p \vdash q}\,\to\text{e}}{p \to q, p \vee r, p \vdash q \vee r}\,\vee\text{i,g} \quad \dfrac{\dfrac{}{p \to q, p \vee r, r \vdash r}\,\text{Ax}}{p \to q, p \vee r, r \vdash q \vee r}\,\vee\text{i,d}}{\dfrac{p \to q, p \vee r \vdash q \vee r}{p \to q \vdash (p \vee r) \to (q \vee r)}\,\to\text{i}}\,\vee\text{e}$$

5. On pose $\Gamma = p, q, (p \wedge q) \to r, \neg r$.

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash (p \wedge q) \to r}\,\text{Ax} \quad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash p}\,\text{Ax} \quad \dfrac{}{\Gamma \vdash q}\,\text{Ax}}{\Gamma \vdash p \wedge q}\,\wedge\text{i}}{\Gamma \vdash r}\,\to\text{e} \quad \dfrac{}{\Gamma \vdash \neg r}\,\text{Ax}}{\Gamma \vdash \bot}\,\neg\text{e}}{\neg r, p, (p \wedge q) \to r \vdash \neg q}\,\neg\text{i}}{(p \wedge q) \to r, \neg r, \vdash p \to \neg q}\,\to\text{i}$$

6. On pose $\Gamma =$

Chapitre 11

Preuves

V.1 Formalisation

1. (1) $\forall e,\ \big(\mathsf{etudiant}(e) \to \mathsf{raison}(e)\big)$;
   (2) $\forall e,\ \big(\mathsf{raison}(e) \to \mathsf{humain}(e)\big)$;
   (3) $\forall e,\ \mathsf{raison}(e) \to \neg\mathsf{elephant}(e)$;
   (4) $\forall e, \big((\mathsf{animal}(e) \wedge \neg\mathsf{chien}(e)\big) \to \forall \ell, \big(\mathsf{logicien}(\ell) \to \mathsf{gentil\_avec}(e, \ell)\big)$
   (5) $\forall h,\ \exists e,\ \mathsf{elephant}(e) \to \mathsf{cherche}(h, e)$;
   (6) $\forall e,\ \big[\big(\exists a,\ \mathsf{aime}(x, y)\big) \wedge \big(\exists a,\ \neg\mathsf{aime}(e, a)\big)\big]$;
2. $\forall x, \mathsf{entier}(x) \to \big[\exists y, \mathsf{entier}(y) \to \big(\mathsf{successeur}(x, y) \to (\forall z, \mathsf{entier}(z) \to \neg\mathsf{inf}(z, x) \to \mathsf{inf}(y, z))\big)\big]$.

V.2 Variables libres et liées, clôture universelle

1.

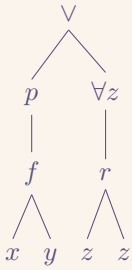


FIGURE 11.1 – Arbre de syntaxe de la formule $p\big(f(x, y)\big) \vee \forall z,\ r(z, z)$

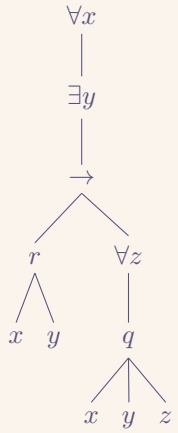


FIGURE 11.2 – Arbre de syntaxe de la formule $\forall x,\ \exists y,\ \big(r(x,y) \to \forall z,\ q(x,y,z)\big)$

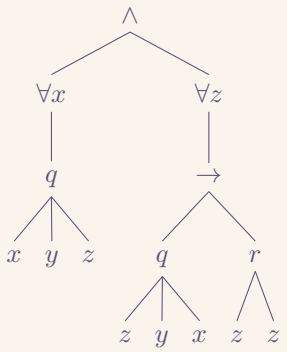


FIGURE 11.3 – Arbre de syntaxe de la formule $\forall x,\ (x,y,z) \wedge \forall z,\ \big(q(z,y,x) \to r(z,z)\big)$

2. Pour la formule (F_1), l'ensemble des constantes est $\mathcal{S}_0 =$, l'ensemble des fonctions est $\mathcal{S} = \big\{f(2)\big\}$. Pour la formule (F_2), l'ensemble des constantes est $\mathcal{S}_0 =$, l'ensemble des fonctions est $\mathcal{S} =$. Pour la formule (F_3), l'ensemble des constantes est $\mathcal{S}_0 =$, l'ensemble des fonctions est $\mathcal{S} =$.
3. Pour la formule (F_1), l'ensemble des symboles de prédicats est $\mathcal{P} = \big\{p(1), r(2)\big\}$. Pour la formule (F_2), l'ensemble des symboles de prédicats est $\mathcal{P} = \big\{r(2), q(3)\big\}$. Pour la formule (F_3), l'ensemble des symboles de prédicats est $\mathcal{P} = \big\{q(3), r(2)\big\}$.
4. Pour la formule (F_1), $\mathsf{FV} = \{x, y\}$ et $\mathsf{BF} = \{z\}$. Pour la formule (F_2), $\mathsf{FV} =$ et $\mathsf{BF} = \{x, y, z\}$. Pour la formule (F_3), $\mathsf{FV} = \{x, y, z\}$ et $\mathsf{BF} = \{x, z\}$.

V.3 Substitution

1.

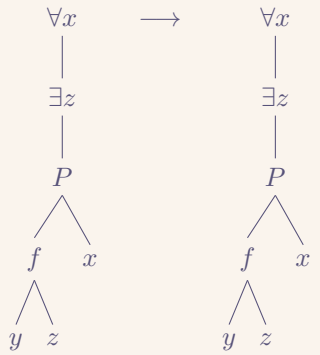


FIGURE 11.4 – Calcul de la substitution $F\big[x \mapsto f(y,z)\big]$, pour la formule 1

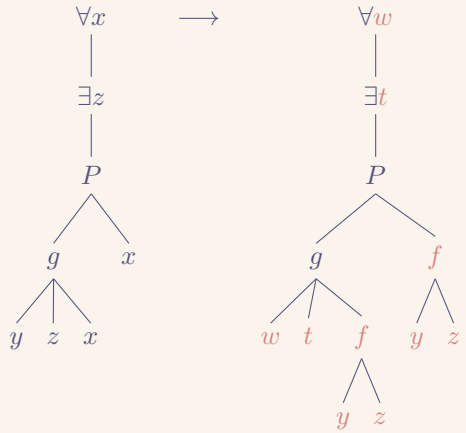


FIGURE 11.5 – Calcul de la substitution $F\big[x \mapsto f(y,z)\big]$, pour la formule 2

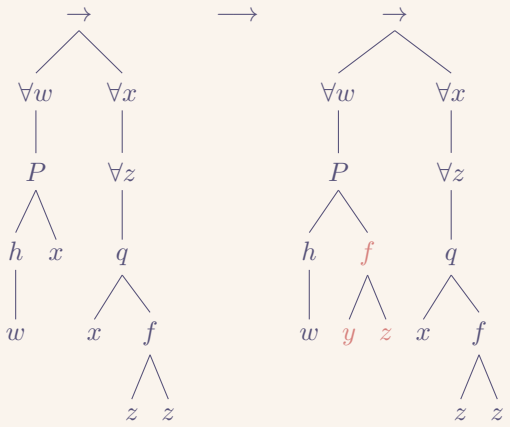


FIGURE 11.6 – Calcul de la substitution $F\big[x \mapsto f(y,z)\big]$, pour la formule 3

V.4 Quelques arbres de preuves

1. *c.f.* exemple chapitre 6.
2. $$\dfrac{\dfrac{}{\exists t,\ \forall x,\ \varphi(t,x) \vdash \exists t,\ \forall x,\ \varphi(t,x)}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{}{\exists t,\ \forall x,\ \varphi(t,x); \forall x,\ \varphi(t,x) \vdash \forall x,\ \varphi(t,x)}\ \text{Ax}}{\exists t,\ \forall x,\ \varphi(t,x); \forall x,\ \varphi(t,x) \vdash \varphi(t,x)}\ \forall\text{e}}{\exists t,\ \forall x,\ \varphi(t,x); \forall x,\ \varphi(t,x) \vdash \forall y,\ \exists x,\ \varphi(x,y)}\ \exists\text{i}}{\exists t,\ \forall x,\ \varphi(t,x) \vdash \forall y,\ \exists x,\ \varphi(x,y)}\ \exists\text{e}.$$
3. $$\dfrac{\dfrac{\dfrac{}{\forall x,\ \varphi; \exists x,\ \neg\varphi \vdash \exists x,\ \neg\varphi}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{}{\forall x,\ \varphi; \exists x,\ \neg\varphi; \neg\varphi \vdash \forall x,\ \varphi}\ \text{Ax}}{\forall x,\ \varphi; \exists x,\ \neg\varphi; \neg\varphi \vdash \varphi}\ \forall\text{e} \qquad \dfrac{}{\forall x,\ \varphi; \exists x,\ \neg\varphi; \neg\varphi \vdash \neg\varphi}\ \text{Ax}}{\forall x,\ \varphi; \exists x,\ \neg\varphi; \neg\varphi \vdash \bot}\ \neg\text{e}}{\forall x,\ \varphi; \exists x,\ \neg\varphi \vdash \bot}\ \exists\text{e}}{\forall x,\ \varphi \vdash \neg(\exists x,\ \neg\varphi)}\ \neg\text{i}.$$
4. $$\dfrac{\dfrac{\dfrac{}{\exists x,\ \neg\varphi; \forall x,\ \varphi \vdash \exists x,\ \neg\varphi}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{}{\exists x,\ \neg\varphi; \forall x,\ \varphi; \neg\varphi \vdash \neg\varphi}\ \text{Ax} \qquad \dfrac{\dfrac{\dfrac{}{\exists x,\ \neg\varphi; \forall x,\ \varphi; \neg\varphi \vdash \forall x,\ \varphi}\ \text{Ax}}{\exists x,\ \neg\varphi; \forall x,\ \varphi; \neg\varphi \vdash \varphi}\ \forall\text{e}}{\exists x,\ \neg\varphi; \forall x,\ \varphi; \neg\varphi \vdash \bot}\ \neg\text{e}}{\exists x,\ \neg\varphi; \forall x,\ \varphi \vdash \bot}\ \exists\text{e}}{\exists x,\ \neg\varphi \vdash \neg(\forall x,\ \varphi)}\ \neg\text{i}}.$$

V.5 Distributivité des quantificateurs

1. $$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x,\ (\varphi \wedge \psi) \vdash \forall x,\ (\varphi \wedge \psi)}\ \text{Ax}}{\forall x,\ (\varphi \wedge \psi) \vdash \varphi \wedge \psi}\ \forall\text{e}}{\forall x,\ (\varphi \wedge \psi) \vdash \varphi}\ \wedge\text{e,g}}{\forall x,\ (\varphi \wedge \psi) \vdash \forall x,\ \varphi}\ \forall\text{i} \qquad \dfrac{\vdots}{\forall x,\ (\varphi \wedge \psi) \vdash \forall x,\ \psi}}{\forall x,\ (\varphi \wedge \psi) \vdash (\forall x,\ \varphi) \wedge (\forall x,\ \psi)}\ \wedge\text{i}.$$

V.6 Semi-distributivité des quantificateurs

V.7 Logique classique du premier ordre

1.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(\exists x,\ \neg\varphi),\neg\varphi\vdash\neg(\exists x,\ \neg\varphi)}\ \mathrm{Ax}\qquad\dfrac{\dfrac{}{\neg(\exists x,\ \neg\varphi),\neg\varphi\vdash\neg\varphi}\ \mathrm{Ax}}{\neg(\exists x,\ \neg\varphi),\neg\varphi\vdash\exists x,\ \neg\varphi}\ \exists\mathrm{i}}{\neg(\exists x,\ \neg\varphi),\neg\varphi\vdash\bot}\ \neg\mathrm{e}}{\neg(\exists x,\ \neg\varphi)\vdash\varphi}\ \mathrm{Abs}}{\neg(\exists x,\ \neg\varphi)\vdash\forall x,\ \varphi}\ \forall\mathrm{i}.$$

Chapitre 12

Algorithmes d'approximation

V.1 Un problème proche de Knapsack

1.

$$\textsc{SommeMax} : \begin{cases} \textbf{Entrée} & : \text{Un entier } n \in \mathbb{N}, \text{ une suite finie } (a_i)_{i\in[\![1,n]\!]} \in \mathbb{N}^n, \\ & \quad \text{un entier } B \in \mathbb{N} \text{ et un seuil } K \in \mathbb{N}, \\ \textbf{Sortie} & : \text{Existe-t-il } I \subseteq [\![1,n]\!] \text{ avec } K \geqslant \sum_{i\in I} a_i \geqslant B \,? \end{cases}$$

2. On a $\textsc{SommeMax} \preccurlyeq_{\text{p}} \textsc{Knapsack}$, mais on ne peut pas faire une réduction.
3. Soit $(w_1, \dots, w_n)$ les entrées du problème Partition. On pose $K = B = \sum_{i=1}^{n} a_i$. On construit l'entrée $(n, (2w_i)_{i\in[\![1,n]\!]}, B, K)$ de SommeMax.

$$\begin{aligned} (n, (2w_i)_{i\in[\![1,n]\!]}, K, B) \in \textsc{SommeMax}^+ &\iff \exists I \subseteq [\![1,n]\!],\ B \leqslant \textstyle\sum_{i\in I} 2a_i \leqslant K \\ &\iff \exists I \subseteq [\![1,n]\!],\ \textstyle\sum_{i=1}^{n} a_i \leqslant \sum_{i\in I} 2a_i \leqslant \sum_{i=1}^{n} a_i \\ &\iff \exists I \subseteq [\![1,n]\!],\ \textstyle\sum_{i\in I} 2a_i = \sum_{i=1}^{n} a_i \\ &\iff \exists I \subseteq [\![1,n]\!],\ \textstyle\sum_{i\in I} a_i = \sum_{i\in[\![1,n]\!]\setminus I} a_i \\ &\iff (w_1, \dots, w_n) \in \textsc{Partition}^+ \end{aligned}$$

Or, comme Partition est **NP**-difficile (*c.f.* TD 8), on en déduit que SommeMax est **NP**-difficile.

4.

Algorithme 12.1 Algorithme glouton pour résoudre le problème $\textsc{SommeMax}_{\text{O}}$ en $\mathcal{O}(n)$

```
1 : somme ← 0
2 : pour i ∈ [[1, n]] faire
3 :     si somme + a_i ⩽ B alors
4 :         somme ← somme + a_i
5 : retourner somme
```

5. L'algorithme n'est pas optimal : avec l'entrée $(1, B)$, l'algorithme renvoie 1, mais la valeur optimale est B. Cet algorithme n'est pas une ρ-approximation, pour $\rho \in \mathbb{R}$.

6.

Algorithme 12.2 Algorithme glouton pour résoudre le problème SommeMax$_O$ en $\mathcal{O}(n \ln n)$

```
1 : On trie, par ordre décroissant, les entrées (a_1, ..., a_n) avec un tri rapide.
2 : somme ← 0
3 : pour i ∈ [[1, n]] faire
4 :     si somme + a_i ⩽ B alors
5 :         somme ← somme + a_i
6 : retourner somme
```

7. Soit e une entrée. Soit S la solution, *non nécessairement optimale*, de l'algorithme. Soit $S^\star$ la solution optimale. On a $S^\star \leqslant B$.

   — Si $S \geqslant \frac{B}{2}$, alors $\frac{S}{S^\star} \geqslant \frac{B/2}{B} = \frac{1}{2}$.

   — Si $S < \frac{B}{2}$, alors, en supposant que $(a_1, \dots, a_n)$ est trié par ordre décroissant, on a, pour $i \in [\![1, n]\!]$, $a_i > B$ ou $a_i < \frac{B}{2}$.

      — Si $\forall i \in [\![1, n]\!]$, $a_i > B$, alors $S = 0 = S^\star$.

      — Soit $i = \text{argmin}_{i \in [\![1,n]\!]}(a_i < B/2)$. On pose I_{algo} les valeurs de i telles que a_i ait été ajoutée à somme. On pose $i' = \max I_{\text{algo}}$.

      Si $i' < n$, alors par l'algorithme, l'objet d'indice n ne rentre pas dans le sac. Or, la valeur du sac est inférieure stricte à $B/2$, et $a_n < B/2$, ce qui est absurde (l'objet rentre dans le sac).

      Ainsi, $i' = n$, et l'algorithme a mis dans le sac tous les objets de poids inférieurs ou égal à $B/2$, donc tous les objets ont un poids inférieur ou égal à B. Donc $S^\star = S$.

8.

Algorithme 12.3 Algorithme glouton pour résoudre le problème SommeMax$_O$ en $\mathcal{O}(n)$

```
Entrée (a_i)_{i ∈ [[1,n]]} une suite finie
1 : somme ← 0
2 : maxi ← 0
3 : pour i ∈ [[1, n]] faire
4 :     si a_i ⩾ B/2 et a_i ⩽ B alors
5 :         maxi ← a_i
6 :     sinon si a_i + somme ⩽ B alors
7 :         somme ← somme + a_i
8 : retourner max(somme, a_i)
```

V.2 Le problème BinPacking

1.

$$\textsc{BinPacking}_O : \begin{cases} \textbf{Entrée} & : \text{un entier } n \in \mathbb{N}, \text{ une suite finie } (t_i)_{i\in[\![1,n]\!]} \in \mathbb{N}^n \text{ et } C \in \mathbb{N}^\star \\ \textbf{Sortie} & : \max\left\{K \in \mathbb{N} \mid \exists \varphi : [\![1,n]\!] \to [\![1,K]\!],\ \forall i \in [\![1,K]\!],\ \sum_{j\in\varphi^{-1}(\{i\})} t_k \leqslant C\right\} \end{cases}$$

2. On réduit Partition à BinPacking. On construit les entrées à l'aide de l'algorithme ci-dessous.

Algorithme 12.4 Réduction polynômiale de Partition à BinPacking

```
1 : B ← Σ_{i=1}^{n} t_i
2 : si B ≡ 0 [2] et B ≠ 0 alors
3 :     retourner (n, T, B/2, 2)
4 : sinon
5 :     retourner (3, (1, 1, 1), 2, 1)
```

Montrons que BinPacking $\in$ **NP**. On choisit pour ensemble de certificats l'ensemble des fonctions $\varphi : [\![1,n]\!] \to [\![1,K]\!]$, pour $(n,K) \in \mathbb{N}^2$. On devine un certificat φ, on vérifie que $\forall i \in [\![1,K]\!]$, $\sum_{j\in\varphi^{-1}(\{i\})} t_j \leqslant C$ en temps polynômiale.

3.

4. On considère l'entrée $(3,(3,3,3),3)$ de l'algorithme. La solution optimale est 3, et c'est la réponse donnée par l'algorithme. On considère l'entrée $(3,(2,3,1),3)$ de l'algorithme. La solution optimale est 2, mais l'algorithme renvoie 3.
5. Pour une instance (n,t,C), un minorant est $\left\lceil \frac{V}{C} \right\rceil$ avec $V = \sum_{i=1}^{n} t_i$, un majorant est n.

V.3 Le problème VoyageurCommerce

1. Soit $\mathscr{C} = \{a_1,a_2\} - \cdots - \{a_n,a_{n+1}\}$ et $a_{n+1} = a_1$, un tour où $\bigcup_{i\in[\![1,n]\!]}\{a_i\} = S$. Soit $\{a,b\}$ une arrête. Posons $\mathscr{C}' = \mathscr{C} \setminus \big\{\{a,b\}\big\}$, et $H = (S',\mathscr{C}')$, où $S' = S$. Montrons que H est un arbre couvrant.
   - Montrons que H est connexe. Soit un couple sommets $(x,y) \in S^2$ tel que $x \neq y$. $\mathscr{C}$ est un tour, donc en re-numérotant
   $$x - b_1 - b_2 - \cdots - b_{n-1} - x.$$
   Soit $i \in [\![1,n-1]\!]$ tel que $b_i = y$. Soit $j \in [\![1,n]\!]$ tel que $\{b_j,b_{j+1}\} = \{a,b\}$.
   Cas 1 Si $j < i$, alors $y - b_{i+1} - \cdots - b_{n-1} - x$ est un chemin.
   Cas 2 Si $j > i$, alors $x - b_1 - \cdots - b_{i-1} - y$ est un chemin.
   Donc H est connexe.
   - On a $\#\mathscr{C}' = n-1$ et H est connexe, donc acyclique.
   - Enfin $S' = S$, donc H est couvrant.

2. Soit $T^\star$ le tour de coût minimal. On note $c(T)$ le coût d'un tour T. On a $c(T^\star) \geqslant c(H)$ où H est l'arbre défini dans la question précédente (par suppression d'arête), d'où $c(T^\star) = c(H^\star)$ où $H^\star$ est un arbre couvrant de poids minimal (par définition de poids minimal).
3. Non, avec le graphe ci-dessous est un contre-exemple.

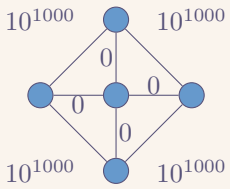


FIGURE 12.1 – Contre exemple

4. On obtient l'arbre couvrant de poids minimal suivant.

FIGURE 12.2 – Arbre couvrant de poids minimal

Un parcours en profondeur est

$$a \to e \to c \to d \to h \rightsquigarrow g \to b \to f.$$

Chapitre 13

Jeux

V.1 Attracteurs pour le jeu de la soustraction généralisé

1. On considère une partie nulle.

   — Le nombre d'allumettes, à chaque tours, décroît strictement dans $(\mathbb{N}, \leqslant)$. Or, $(\mathbb{N}, \leqslant)$ est bien fondé, donc la partie se termine.

   — Il existe donc un joueur j qui prend la dernière allumette. Ce joueur perd et l'autre gagne, donc la partie est non nulle.

2. Montrons que

$$\mathscr{A} = \{(\mathrm{A}, i) \mid i \in [\![1, n]\!],\ i \not\equiv 1 \ \ [k+1]\} \cup \{(\mathrm{B}, i) \mid i \in [\![1, n]\!],\ i \equiv 1 \ \ [k+1]\}$$
$$\mathscr{B} = \{(\mathrm{B}, i) \mid i \in [\![1, n]\!],\ i \not\equiv 1 \ \ [k+1]\} \cup \{(\mathrm{A}, i) \mid i \in [\![1, n]\!],\ i \equiv 1 \ \ [k+1]\}$$

On pose, pour tout $p \in \mathbb{N}$,

V.2 Chomp

V.3 Hex

V.4 Calcul de MinMax

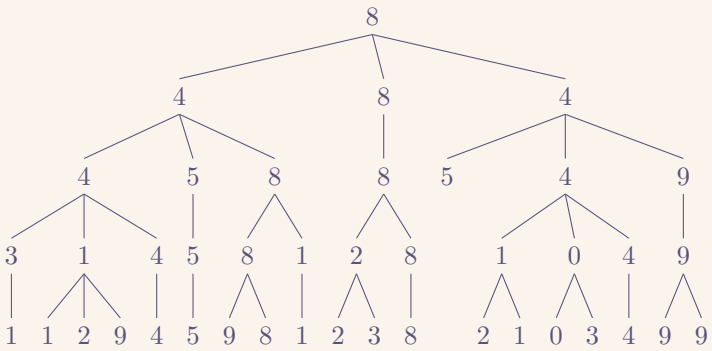


FIGURE 13.1 – Arbre remplit avec l'algorithme MINMAX

1.

V.5 Calcul de MinMax avec mémoïsation

Chapitre 14

Grammaires non contextuelles (1)

V.1 Exemples de dérivations

1. Les dérivations (b), et (d) sont vraies.
2. Les dérivations (a), (c), et (d).
3. On a $\{ab, ba, aab\} \subseteq \mathscr{L}(\mathscr{G})$. En effet,
   — $\mathrm{S} \Rightarrow \mathrm{D} \Rightarrow a\mathrm{T}b \Rightarrow ab$,
   — $\mathrm{S} \Rightarrow \mathrm{D} \Rightarrow b\mathrm{T}a \Rightarrow ba$,
   — $\mathrm{S} \Rightarrow \mathrm{D} \Rightarrow a\mathrm{T}b \Rightarrow a\mathrm{X}b \Rightarrow aab$.
4. On a $\varepsilon \notin \mathscr{L}(\mathscr{G})$, $aa \notin \mathscr{L}(\mathscr{G})$ et $bb \notin \mathscr{L}(\mathscr{G})$.
5. Le langage $\mathscr{L}(\mathscr{G})$ est l'ensemble des mots non palindromes.

V.2 Arbres de dérivations

1.

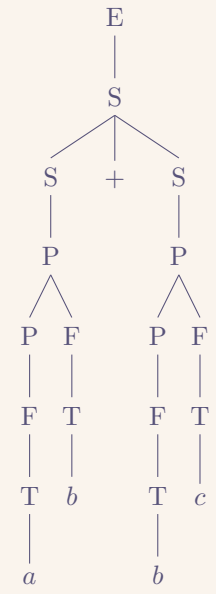


FIGURE 14.1 – Arbre de dérivation de $ab + bc$ dans la grammaire $\mathscr{G}$

2.

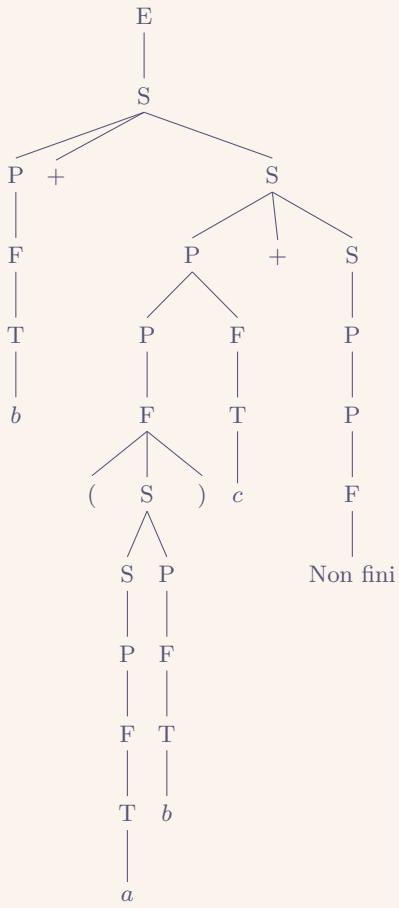


FIGURE 14.2

V.3 Construction de grammaires

1. — $\mathcal{G}_0 = (\Sigma, \{\mathrm{L}, \mathrm{A}, \mathrm{S}\}, \{\mathrm{S} \to \mathrm{LLLA}, \mathrm{L} \to a \mid b, \mathrm{A} \to \mathrm{LA} \mid \varepsilon\}, \mathrm{S})$,
   — $\mathcal{G}_1 = (\Sigma, \{\mathrm{L}, \mathrm{A}, \mathrm{S}\}, \{\mathrm{S} \to \mathrm{A}a\mathrm{A}a\mathrm{A}a\mathrm{A}, \mathrm{A} \to \mathrm{LA} \mid \varepsilon, \mathrm{L} \to a \mid b\}, \mathrm{S})$,
   — $\mathcal{G}_2 = (\Sigma, \{\mathrm{S}, \mathrm{V}\}, \{\mathrm{S} \to a\mathrm{X}a \mid b\mathrm{X}b, \mathrm{X} \to a\mathrm{X} \mid b\mathrm{X} \mid \varepsilon\}, \mathrm{S})$,
   — $\mathcal{G}_3(\Sigma, \{\mathrm{S}, \mathrm{X}\}, \{\mathrm{S} \to \mathrm{X}, \mathrm{X} \to \mathrm{S}\}, \mathrm{S})$.
2. — $\mathcal{G}_4 = (\Sigma, \{\mathrm{L}, \mathrm{S}, \mathrm{X}\}, \{\mathrm{S} \to \mathrm{LX}, \mathrm{L} \to a \mid b, \mathrm{X} \to \mathrm{LLX} \mid \varepsilon\}, \mathrm{S})$,
   — $\mathcal{G}_5 = (\Sigma, \{\mathrm{S}, \mathrm{X}\}, \{\mathrm{S} \to \mathrm{X}a\mathrm{X}, \mathrm{X} \to a\mathrm{X} \mid b\mathrm{X} \mid \varepsilon\}, \mathrm{S})$,
   — $\mathcal{G}_6 = (\Sigma, \{\mathrm{S}, \mathrm{X}\}, \{\mathrm{S} \to a\mathrm{S}a \mid b\mathrm{S}b \mid \mathrm{X}, \mathrm{X} \to \varepsilon \mid a \mid b\}, \mathrm{S})$,
   — *c.f.* exercice 1.
3. — $\mathcal{G}_8 = (\Sigma, \{\mathrm{S}\}, \{\mathrm{S} \to \varepsilon \mid a\mathrm{S}b\}, \mathrm{S})$,
   — $\mathcal{G}_9 = (\Sigma, \{\mathrm{S}, \mathrm{X}\}, \{\mathrm{S} \to a\mathrm{S}b \mid \mathrm{SX}, \mathrm{X} \to b\mathrm{X} \mid \varepsilon\}, \mathrm{S})$,
   — $\mathcal{G}_{10} = (\Sigma, \{\mathrm{S}\}, \{\mathrm{S} \to a\mathrm{S}bb \mid \mathrm{S}b \mid \varepsilon\}, \mathrm{S})$
4. — $\mathcal{G}_{11} = (\Sigma, \{\mathrm{S} \to a\mathrm{S}b \mid b\mathrm{S}a \mid a\mathrm{S} \mid \mathrm{SS} \mid \varepsilon\}, \mathrm{S})$,

V.4 Raisonner par induction sur une grammaire

1. Montrons le par induction.
   - **Cas $\mathrm{S} \to a\mathrm{S}$.** Soit $w = aw'$ un mot, où ba n'est pas un sous-mot de w'. Alors, ba n'est pas un sous-mot de $w = aw'$.
   - **Cas $\mathrm{S} \to \mathrm{S}b$.** Soit $w = w'b$ un mot, où ba n'est pas un sous-mot de w'. Alors, ba n'est pas un sous-mot de $w = w'b$.
   - **Cas $S \to \varepsilon \mid a \mid b$.** Le mot ba n'est pas un sous-mot de a, ni de b, ni de ε.
2. Montrons, par double-inclusion, que $\mathscr{L}(\mathscr{G}) = \mathscr{L}(a^\star b^\star)$.

   "$\supseteq$" Soit $w \in \mathscr{L}(a^\star b^\star)$. Il existe m et n deux entiers tels que $w = a^n b^m$. On applique la dérivation

   $$\underbrace{\mathrm{S} \Rightarrow a\mathrm{S} \Rightarrow aa\mathrm{S} \Rightarrow \cdots \Rightarrow a^n\mathrm{S}}_{n \text{ fois}} \Rightarrow \underbrace{a^n\mathrm{S}b \Rightarrow a^n\mathrm{S}bb \Rightarrow \cdots \Rightarrow a^n\mathrm{S}b^m}_{m \text{ fois}} \Rightarrow a^n b^m.$$

   "$\subseteq$" D'après la question 1, on a ce sens de l'inclusion.

V.5 Ambigüité

V.6 Langage de Dyck

1. On suppose ce langage reconnaissable par un automate à n états. On considère le mot $w = ({}^n \cdot)^n$, donc $|w| \geqslant n$. Ainsi, il existe x, y et z trois mots tels que $w = xyz$, $|xy| \leqslant n$, $y \neq \varepsilon$ et $\forall p \in \mathbb{N}$, $xy^p z \in \mathscr{L}(\mathscr{G})$. Soit alors $p \in [\![1, n-1]\!]$ et $q \in [\![1, n-p]\!]$ tels que $x = ({}^p$, $y = ({}^q$ et $z = ({}^{n-q-p} \cdot)^n$. Ainsi, $xy \in \mathscr{L}(\mathscr{G})$, ce qui est absurde. On en déduit que $\mathscr{L}(\mathscr{G})$ n'est pas reconnaissable, il n'est donc pas régulier.
2. On pose $\mathscr{G} = (\Sigma, \{\mathrm{S}\}, \{\mathrm{S} \to (\mathrm{S}) \mid \mathrm{SS} \mid \varepsilon\}, \mathrm{S})$.
3. — On le montre par induction.
   - **Cas $\mathrm{S} \to \varepsilon$.** On a $|\varepsilon|_(= 0 = |\varepsilon|_)$.
   - **Cas $\mathrm{S} \to (\mathrm{S})$.** Soit $u \in \mathscr{L}(\mathscr{G})$ avec $|u|_(= |u|_) = n$. Ainsi, $|(u)|_(= |(u)|_) = n + 1$.
   - **Cas $\mathrm{S} \to \mathrm{SS}$.** Soient u et v deux mots de $\mathscr{L}(\mathscr{G})$ tels que $|u|_(= |u|_) = n$ et $|v|_(= |v|_) = m$. Alors, $|u \cdot v|_(= |v \cdot u|_) = n + m$.

   — Montrons par induction $\mathscr{P}_u$: « pour tout v préfixe de u, $|v|_(\geqslant |v|_)$. »
   - **Cas $\mathrm{S} \to \varepsilon$.** Le seul préfixe de ε est ε, et on a bien $|\varepsilon|_(= 0 \geqslant 0 = |\varepsilon|_)$.
   - **Cas $\mathrm{S} \to (\mathrm{S})$.** Soit u un mot de $\mathscr{L}(\mathscr{G})$ vérifiant $\mathscr{P}_u$. Soit v un préfixe de (u). On procède par induction sur v.
     - **Cas $v = \varepsilon$ ou $($.** OK.
     - **Cas $(\tilde{u}$,** où $\tilde{u}$ est un préfixe de u. Par hypothèse d'induction, $|\tilde{u}|_(\geqslant |\tilde{u}|_)$ donc $|(\tilde{u}|_(= |(\tilde{u}|_)$.
     - **Cas (u).** Par hypothèse d'induction, $|u|_(\geqslant |u|_)$ donc $|(u)|_(\geqslant |(u)|_)$.
4. On note $\overline{w}^j = \left|w_{[\![0,j]\!]}\right|_(- \left|w_{[\![0,j]\!]}\right|_)$. Alors les deux conditions se traduisent par $\overline{w}^{|w|} = 0$ et $\forall i \in [\![0, |w|-1]\!]$, $\overline{w}^i \geqslant 0$.

V.7 Listes OCaml

On pose $\mathscr{G} = (\Sigma, \{\mathrm{S}, \mathrm{L}, \mathrm{B}\}, \{\mathrm{S} \to \texttt{[L]} \mid \texttt{[]}, \mathrm{L} \to \mathrm{B}\,\texttt{;}\,\mathrm{L} \mid \mathrm{B}, \mathrm{B} \to \texttt{true} \mid \texttt{false}\}, \mathrm{S})$.

V.8 Mots de Łukasiewicz

1. On a $\Sigma \cap \mathscr{L} = \{\square\}$, $\Sigma^2 \cap \mathscr{L} =$ et $\Sigma^3 \cap \mathscr{L} = \{\bigcirc\square\square\}$.
2. Montrons que $\Sigma^{2N} \cap \mathscr{L} =$, pour tout $N \in \mathbb{N}^\star$. (Dans le cas $N = 0$, le seul mot est ε, et il n'est pas dans $\mathscr{L}$.) Soit $w \in \Sigma^{2N} \cap \mathscr{L}$. On sait que $-1 = \overline{w}^{|w|} = \overline{w}^{|w|-1} + \mathsf{va}(w_{|w|}) \geqslant \mathsf{va}(w_{|w|})$, d'où $w_{|w|} = \square$, et $\overline{w}^{|w|-1} = 0$. On pose $w = u \cdot \square$, le mot u est donc de longueur impaire. Or, la somme $\sum_{k=1}^{|u|} \mathsf{va}(w_i)$ est une somme d'un nombre impaire de termes valant -1 ou 1, elle ne peut pas être nulle. Mais, comme $\overline{w}^{|w|-1} = 0$, donc elle est nulle, une contradiction. On en déduit que $\mathscr{L} \cap \Sigma^{2N} =$. Par suite, on conclut que $\mathscr{L}$ ne contient pas de mots pairs.
3. On suppose $\mathscr{L}$ reconnaissable par un automate $\mathscr{A}$ à n états. On considère le mot $w = \bigcirc^n \cdot \square^n \cdot \square \in \mathscr{L}$. Alors, par application du lemme de l'étoile à l'automate $\mathscr{A}$ avec ce mot w, il existe donc x, y et z trois mots de $\Sigma^\star$ tels que $w = xyz$, $|xy| \leqslant n$, $y \neq \varepsilon$ et, pour tout $p \in \mathbb{N}$, $xy^pz \in \mathscr{L}$. D'où, $x = \bigcirc^k$, $y = \bigcirc^j$ et $z = \bigcirc^{n-k-j} \cdot \square^{n+1}$, où k et j sont des entiers. De plus, $j \neq 0$ car, sinon, $y = \varepsilon$. Alors, $xy^pz \in \mathscr{L}$, pour tout $p \in \mathbb{N}$. En particulier, pour $p = 0$, $xz \in \mathscr{L}$. Or, $xz = \bigcirc^{n-j} \cdot \square^{n+1} \notin \mathscr{L}$ car $\overline{xz}^{|xz|} = (n-j) - (n+1) = -j - 1 \neq -1$ car $j \neq 0$. On en déduit donc que que $\mathscr{L}$ n'est pas reconnaissable par un automate à n états. Ceci étant vrai pour tout n, alors $\mathscr{L}$ n'est pas un langage régulier.
4.

```
let est_luka (w: word): bool =
  let l = List.map va w in
  let rec aux (l: int list) (s: int): bool =
    match l with
    | []     -> s = -1
    | x :: q -> s >= 0 && aux q (s + x)
  in aux l 0
```

Code 14.1 – Fonction `est_luka` testant si w est un mot de Łukasiewicz

5. Soit $w = u \cdot v \in \mathscr{L}$, où $u \neq \varepsilon$ est un préfixe strict de w. Alors, $0 \leqslant \overline{w}^{|u|} = \overline{u}^{|u|} \neq -1$ donc $u \notin \mathscr{L}$.
6. Soient u et v deux mots de $\mathscr{L}$. On pose $w = \bigcirc \cdot u \cdot v$. Montrons que $w \in \mathscr{L}$. On pose $n = |u|$, et $m = |v|$.
   — On a $\overline{w}^0 = 0 \geqslant 0$,
   — et $\overline{w}^1 = \mathsf{va}(\bigcirc) = 1 \geqslant 0$,
   — et, pour tout $i \in [\![1, n[\![$, $\overline{w}^{i+1} = \overline{u}^i + \mathsf{va}(\bigcirc) \geqslant \mathsf{va}(\bigcirc) \geqslant 0$,
   — et, pour tout $i \in [\![1, m[\![$, $\overline{w}^{i+n+1} = \overline{u}^n + \overline{v}^i + \mathsf{va}(\bigcirc) = \overline{v}^i \geqslant 0$,
   — et finalement, $\overline{w}^{n+m+1} = \overline{u}^n + \overline{v}^m + \mathsf{va}(\bigcirc) = -1 - 1 + 1 = -1$.

   On en conclut que $w \in \mathscr{L}$.
7. Soit $w \in \mathscr{L}$, un mot de taille n. Comme montré précédemment, $\overline{w}^{n-1} = 0$. Ainsi, l'ensemble $\{k \in [\![1, n]\!] \mid \overline{w}^i = 0\}$ est une partie de $\mathbb{N}$ non vide, elle

admet donc un minimum que l'on notera k. De plus, on a montré que $w_0 = \bigcirc$. On en déduit que w peut être décomposé en

$$w = \bigcirc \cdot \underbrace{w_2 w_3 \dots w_k}_{u} \cdot \underbrace{w_{k+1} w_{k+2} \dots w_n}_{v} \cdot$$

Montrons que u et v sont des mots de $\mathscr{L}$. D'une part, pour $i \in [\![1, k-2]\!]$, $0 < \overline{w}^{i+1} = \overline{u}^i + \mathsf{va}(\bigcirc)$, d'où $\overline{u}^i \geqslant 0$. De plus, $0 = \overline{w}^k = \overline{u}^{k-1} + \mathsf{va}(\bigcirc)$, d'où $\overline{u}^{k-1} = \overline{u}^{|u|} = -1$. Également, pour $i \in [\![1, n-k-1]\!]$, $0 \leqslant \overline{w}^{k+i} = \overline{w}^k + \overline{v}^i = \overline{v}^i$. Finalement, $-1 = \overline{w}^n = \overline{w}^k + \overline{v}^{n-k} = \overline{v}^{|v|}$. On en conclut que u et v sont bien des mots de $\mathscr{L}$.

Montrons, à présent, l'unicité de la décomposition. On suppose qu'il existe u' et v' deux mots de $\mathscr{L}$ tels que $w = \bigcirc \cdot u' \cdot v'$. Nous savons, en particulier, que $\overline{w}^{1+|u'|} = 0$, afin de maintenir la condition $u \in \mathscr{L}$. Alors, $1 + |u'| \leqslant p$, et donc $|u'| \geqslant |u|$. Le mot u' est donc un préfixe de u. Au vu de la question 5., afin que u' soit un mot de $\mathscr{L}$, il est nécessaire que u' ne soit pas un préfixe strict de u. On en déduit que $u' = u$.

8. On utilise habilement la question précédente, et on pose

$$\mathscr{G} = (\{\mathrm{L}\}, \Sigma, \{\mathrm{L} \to \bigcirc \mathrm{LL} \mid \bigcirc\}, \mathrm{L}).$$

La question précédente montre la non-ambigüité de la grammaire, et que $\mathscr{L}(\mathscr{G}) = \mathscr{L}$.

9.

Chapitre 15

Grammaires non contextuelles (2)

V.1 Forme normale conjonctive

1. On pose la grammaire $\mathcal{G}$ de symbole initial U et ayant pour règles de production

$$\begin{gathered} \mathrm{U} \to \mathrm{S} \mid \varepsilon, \\ \mathrm{S} \to \mathrm{S\&X} \mid \mathrm{X}, \\ \mathrm{X} \to \mathrm{-V} \mid \mathrm{V} \mid \mathrm{V|X} \mid \mathrm{-V|X}, \\ \mathrm{V} \to \mathtt{p} \mid \mathtt{q} \mid \cdots . \end{gathered}$$

2.

```
'p' ⇝ la variable p
('p', true) ⇝ le littéral p
('p', false) ⇝ le littéral ¬p
[ ('p', true); ('q', true) ] ⇝ la clause p ∨ q
[[ ('p', true); ('q', true) ]] ⇝ la formule p ∨ q
[[('p', true)]; [('q', true)]]] ⇝ la formule p ∧ q
[[('p', true)]; [('q', true); ('p', false)]]] ⇝ la
    formule p ∧ (q ∨ ¬p)
```

Code 15.1 – Expressions OCaml

3.

```
let rec parse_f (s: string) (start: int) (len:
    ↪ int): fnc =
  if String.length s = 0 then []
  else parse_d s start len
and parse_d (s: string) (start: int) (len: int):
    ↪ fnc =
  let i = ref start in
```

```
6   while s.[!i] != '&' && !i < len do incr i; done ;
7   if !i = len then [parse_c s start len]
8   else (parse_c s start (!i - 1)) :: (parse_d s (!i+1) len)
9 and parse_c (s: string) (start: int) (len: int): cls =
10  let i = ref start in
11  while s.[!i] != '|' && !i < len do incr i; done ;
12  if !i = len then [parse_l s start len]
13  else (parse_l s start (!i - 1)) :: (parse_c s (!i+1) len)
14 and parse_l (s: string) (start: int) (len: int): lit =
15  if s.[start] = '-' then (parse_v s (start + 1) len, false)
16  else (parse_v s start len, true)
17 and parse_v (s: string) (start: int) (len: int): char =
18  let x = s.[start] in
19  assert(Char.code x >= 97 && Char.code x <= 122) ;
20  assert(len - start = 1);
21  x
```

CODE 15.2 – Parsing des fonctions OCAML

V.2 Réduction de grammaire et systèmes de conséquences

V.2.1 Digression OCaml

V.3 Grammaires propres

V.4 Un lemme d'itération

V.5 Les langages réguliers sont non contextuels

V.5.1 Avec des automates

1. On pose P l'ensemble des règles de productions définies comme

$$\{X_q \to \ell X_{q'} \mid (q, \ell, q') \in \delta\} \cup \{X_q \to \varepsilon \mid q \in F\}.$$

Montrons par récurrence $\mathscr{P}(n)$:

« $\forall q \in \mathbb{Q}$, $\mathscr{L}_n(\mathscr{A}_q) = \{w \in \mathscr{L} \mid |w| = n\} = \{w \in \Sigma^n \mid X_q \overset{\star}{\Rightarrow} w\} = G_n(q)$. »

— Pour $n = 0$, soit $q \in Q$ et soit $w \in \Sigma^\star$. Si $w \in \mathscr{L}_n(\mathscr{A}_q)$, alors $w = \varepsilon$ et $q \in F$, d'où $(X_q \to \varepsilon) \in P$ donc $X_q \overset{\star}{\Rightarrow} w$ donc $w \in G_n(q)$. Réciproquement, si $w \in G_n(q)$, alors $X_q \overset{\star}{\Rightarrow} \varepsilon$ car il n'y a pas d'ε-transitions, donc $q \in F$ et donc $w = \varepsilon \in \mathscr{L}_n(\mathscr{A}_q)$.

— Soit $n \in \mathbb{N}$. On suppose $\mathscr{P}(n)$ vraie. Soit $q \in Q$ et soit $w \in \Sigma^{n+1}$. Si $w \in \mathscr{L}_{n+1}(\mathscr{A}_q)$, alors il existe une exécution acceptante

$$q \xrightarrow{w_1} q_1 \to \cdots \to q_n \xrightarrow{w_{n+1}} q_{n+1} \in F.$$

D'où, $w_2 \dots w_{n+1} \in \mathscr{L}_n(\mathscr{A}_{q_1}) = G_n(q_1)$ par hypothèse donc $X_{q_1} \overset{\star}{\Rightarrow} w_2 \dots w_{n+1}$. Or, $(q, w_1, q_1) \in \delta$ donc $(X_q \to w_n X_{q_1}) \in P$ et donc $X_q \Rightarrow w_1 X_{q_1} \overset{\star}{\Rightarrow} w$. D'où, $X_q \overset{\star}{\Rightarrow} w$ et donc $w \in G_{n+1}(q)$.

Réciproquement, si $w \in G_{n+1}(q)$ alors $X_q \overset{\star}{\Rightarrow} w$. Soit $w' \in Q$ tel que $X_q \Rightarrow w_1 X_{q'}$. Alors, $(q, w_1, q') \in \delta$. De plus, $|w_2 \dots w_n| = n$ et $X_{q'} \overset{\star}{\Rightarrow} w_2 \dots w_{n+1}$ donc $w_2 \dots w_{n+1} \in G_n(q') = \mathscr{L}_n(\mathscr{A}_{q'})$. Il existe donc une exécution acceptante

$$q' \xrightarrow{w_2} q_2 \to \cdots \to q_n \xrightarrow{w_{n+1}} q_{n+1} \in F.$$

Or, $(q, w_1, q') \in \delta$ d'où

$$q \xrightarrow{w_1} q' \xrightarrow{w_2} q_2 \to \cdots \to q_n \xrightarrow{w_{n+1}} q_{n+1} \in F$$

est une exécution acceptante de $\mathscr{A}_q$. On en déduit que $w \in \mathscr{L}_{n+1}(\mathscr{A}_q)$.

2. On en conclut que tout langage régulier est représentable par une grammaire non-contextuelle.

V.5.2 Avec des expressions régulières

3. On pose P l'ensemble de règles de productions défini comme

$$\begin{aligned} P = \quad & \{X_r \to X_r X_{r'} \mid \varepsilon \text{ tel que } r = (r')^\star\} \\ & \cup \{X_r \to X_{r_1} \mid X_{r_2} \text{ tel que } r = r_1 \mid r_2\} \\ & \cup \{X_r \to X_{r_1} X_{r_2} \text{ tel que } r = r_1 \cdot r_2\} \\ & \cup \{X_r \to r \text{ tel que } r \in \Sigma\} \\ & \cup \{X_r \to \varepsilon \text{ tel que } r = \varepsilon\} \end{aligned}$$

Chapitre 16

Concurrence

V.1 Entrelacements

V.2 Généralisation de l'algorithme de Peterson à N fils

1. *c.f.* cours

2. Les algorithmes 1 et 2 ne sont pas corrects. On donne deux exécutions posant problème.

Algorithme 16.1 Proposition 1

```
1 :  Turn ← 0
2 :  Want est un tableau de N booléens initialisé à F.
3 :  Procédure Lock(i)
4 :      Want[i] ← V
5 :      Turn ← i + 1 mod N
6 :      tant que Turn ≠ i et Want[Turn] faire
7 :          rien
8 :
9 :  Procédure Unlock(i)
10 :     Want ← F
```

Algorithme 16.2 Proposition 2

```
1 :  Turn ← 0
2 :  Want est un tableau de N booléens initialisé à F.
3 :  Procédure Lock(i)
4 :      Want[i] ← V
5 :      Turn ← i + 1 mod N
6 :      tant que Turn ≠ i faire
7 :          si Want[Turn] alors
8 :
9 :              Turn ← Turn + 1 mod N
10 :  Procédure Unlock(i)
11 :     Want ← F
```

V.3 Parallélisation pour le produit de deux matrices

V.4 Calcul du maximum par “diviser pour régner”

V.5 Un très mauvais algorithme de tri

Chapitre 17

Concurrence

V.1 Addition binaire en parallèle

V.2 Producteurs–consommateurs en mémoire non bornée

V.2.1 Version allégée de la solution vue en cours

1. C'est le sémaphore Plein qui a pour rôle d'éviter les problèmes de dépassement. Avec l'hypothèse d'une mémoire non bornée, on retire l'appel `acquire` Plein de la procédure PRODUCTION, l'appel `release` Plein de la procédure CONSOMMATION, et la création du sémaphore Plein de l'algorithme 1.
2. L'utilisation d'une telle variable sur plusieurs fils d'exécution nécessite un *mutex* afin que l'écriture en mémoire ne soit faite qu'un fil à la fois.
3.

V.3 Rendez-vous à l'aide de sémaphores

V.3.1 Deux fils d'exécutions se rencontrent une fois

1. On considère les fils P_1 et P_2. Dans le programme principal, on crée deux sémaphores $\mathcal{S}_1$ et $\mathcal{S}_2$, initialisés à 0.

Algorithme 17.1 Fil d'exécution P_1

```
1 : A_1
2 : release S_2
3 : acquire S_1
4 : B_1
```

Algorithme 17.2 Fil d'exécution P_2

```
1 : A_2
2 : release S_1
3 : acquire S_2
4 : B_2
```

Pour généraliser, on considère 3 sémaphores $\mathcal{S}_1$, $\mathcal{S}_2$ et $\mathcal{S}_3$ initialement à 0.

On définit donc les fils P_1, P_2 et P_3 définis ci-dessous.

Algorithme 17.3 Fil d'exécution P_1

```
1 : A_1
2 : release S_2
3 : release S_3
4 : acquire S_1
5 : acquire S_1
6 : B_1
```

Algorithme 17.4 Fil d'exécution P_2

```
1 : A_2
2 : release S_1
3 : release S_3
4 : acquire S_2
5 : acquire S_2
6 : B_2
```

Algorithme 17.5 Fil d'exécution P_3

```
1 : A_3
2 : release S_1
3 : release S_2
4 : acquire S_3
5 : acquire S_3
6 : B_3
```

2. On perds l'indépendance des fils P_1 et P_2. Pour généraliser la solution, on considère les algorithmes ci-dessous.

Algorithme 17.6 Fil P_1

```
1 : A_1
```

Algorithme 17.8 Fil P_2

```
1 : A_2
```

Algorithme 17.10 Fil P_3

```
1 : A_3
```

Algorithme 17.7 Fil P'_1

```
1 : B_1
```

Algorithme 17.9 Fil P'_2

```
1 : B_2
```

Algorithme 17.11 Fil P'_3

```
1 : B_3
```

Algorithme 17.12 Programme principal

```
1 : lancer P_1, P_2 et P_3 en parallèle
2 : attendre la fin de P_1, P_2 et P_3
3 : lancer P'_1, P'_2 et P'_3 en parallèle
```

3. Non, les instructions B_2 et A_1 pourraient être exécutées en parallèle, mais ce n'est pas possible avec la subdivision des fils.

V.3.2 Plusieurs fils se rencontrent une fois

4. On considère l'algorithme ci-dessous.

Algorithme 17.13 Implémentation de la structure barrière $\mathscr{b}$

```
1 : Procédure CréeBarrière
2 :     Soit un verrou 𝒱.
3 :     Soit i = 0.
4 :     Soit un sémaphore 𝒮 initialisé à 0.
5 :     retourner 𝒷 = (𝒱, 𝒮, i).
6 : Procédure AppelBarrière(b)
7 :     (𝒱, 𝒮, i) ← 𝒷
8 :     lock(𝒱)
9 :     i ← i + 1
10 :    si i = n alors
11 :        pour k ∈ ⟦1, n⟧ faire
12 :            release 𝒮
13 :    unlock(𝒱)
14 :    acquire 𝒮
```

V.3.3 Plusieurs fils d'exécution se rencontrent plusieurs fois

5.

6. On considère l'algorithme suivant.

Algorithme 17.14 Implémentation de la structure barrière robuste $\mathscr{b}$

```
1 : Procédure CréeBarrière(n)
2 :     Soit un verrou 𝒱.
3 :     Soit i = 0, et soit nb = i.
4 :     Soit un sémaphore 𝒮 initialisé à 0.
5 :     retourner 𝒷 = (𝒱, 𝒮, i, nb).
6 : Procédure AppelBarrière(b)
7 :     (𝒱, 𝒮, i) ← 𝒷
8 :     lock(𝒱)
9 :     i ← i + 1
10 :    si i = n alors
11 :        pour k ∈ ⟦1, n⟧ faire
12 :            release 𝒮
13 :    unlock(𝒱)
14 :    acquire 𝒮
15 : Procédure JeNeViendraisPlus(𝒷)
16 :    (𝒱, 𝒮, i, nb) ← 𝒷
17 :    lock(𝒱)
18 :    nb ← nb − 1
19 :    si i = nb alors
20 :        pour k ∈ ⟦1, nb⟧ faire
21 :            release 𝒮
22 :        i ← 0
23 :    unlock(𝒱)
```

Chapitre 18

Complexité amortie

V.1 Complexité amortie

1. (a) Soit $n \in \mathbb{N}$.

— Si n est pair, $\displaystyle\sum_{i=0}^{n-1} c_i = \sum_{i=1}^{n/2} 1 + \sum_{i=1}^{n/2} 3 = 2n.$

— Si n est impair,

$$\begin{aligned}\sum_{i=0}^{n-1} c_i &= \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor + 1} 1 + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} 3 \\ &= \left\lfloor \frac{n}{2} \right\rfloor + 1 + 3 \left\lfloor \frac{n}{2} \right\rfloor \text{ car } n = 2 \left\lfloor \frac{n}{2} \right\rfloor + 1 \\ &= 4 \left\lfloor \frac{n}{2} \right\rfloor + 1 \\ &= n + 2 \left\lfloor \frac{n}{2} \right\rfloor \\ &= n + n - 1 \\ &= 2n - 1\end{aligned}$$

(b) On pose h la fonction de potentiel définie comme

$$\begin{aligned} h : \mathbb{N} &\longrightarrow \mathbb{R}^+ \\ n &\longmapsto \begin{cases} 0 & \text{si } n \text{ est pair,} \\ 1 & \text{si } n \text{ est pair.} \end{cases}\end{aligned}$$

— Si n est pair, $\quad \underline{C}_o(n) = C_o(n) + h(n+1) - h(n) = 1 + 1 = 2.$

— Si n est impair, $\underline{C}_o(n) = C_o(n) + h(n+1) - h(n) = 3 + 0 - 1 = 2.$

V.2 Incrementation compteur binaire

V.3 Tableaux dynamiques

3. On trouve une complexité amortie en n^2. À rédiger.
4. Au lieu de diviser quand $r < n/2$, mais quand $r < n/4$.

V.4 Tableaux dynamiques, 2

Chapitre 19

Diviser pour régner

V.1 Suites récurrentes de complexité

(*a*) On considère la suite $u_0 = 1$ et $u_n = u_{n-1} + a$ pour $a > 0$. Montrons que $u_n = \Theta(n)$.

(*b*) On considère la suite $u_0 = 1$ et $u_n = u_{n-1} + an$ pour $a > 0$.

(*c*) On considère la suite $u_0 = 1$ et $u_n = au_{n-1} + b$ pour $a > 2$ et $b \in \mathbb{R}_+^\star$.

$$\begin{aligned} u_n &= au_{n-1} + b \\ &= a(au_{n-2} + b) + b \\ &= a^2 u_{n-2} + ab + b \\ &= a^3 u_{n-3} + a^2 b + ab + b \\ &\vdots \\ &= a_n + \sum_{k=0}^{n-1} a^k b \\ &= a^n + b\frac{1-a^n}{1-a} \\ &= a^n \cdot \left(1 - \frac{b}{1-a}\right) + \frac{b}{1-a} \\ &= \Theta(a^n) \end{aligned}$$

(*d*) On considère la suite $u_0 = 1$ et $u_n = u_{n/2} + b$ avec $b > 0$. Soit $(v_p)_{p\in\mathbb{N}}$ la suite définie par $v_p = u_{2^p}$. Donc

$$v_p = u_{2^p} = u_{2^p/2} + b = u_{2^{p-1}/2} + 2b = \cdots = v_0 + bp = 1 + (p+1)b.$$

La suite $(u_n)_{n\in\mathbb{N}}$ est croissante donc, pour $n \in \mathbb{N}$, Alors,

$$v_{\lfloor \log_2 n \rfloor} \leqslant u_n \leqslant v_{\lceil \log_2 n \rceil} \text{ d'où } b(\lfloor \log_2 n \rfloor + 1) + 1 \leqslant u_n \leqslant b$$
$$\text{d'où } b\log_2 n + 1 \leqslant u_n \leqslant b(\log_2 n + 2) + 1$$

On en déduit que $u_n = \Theta(\log_2 n)$.

(*e*) On considère la suite $u_0 = 1$ et $u_n = u_{n/2} + bn$ avec $b > 0$. On pose $(v_p)_{p\in\mathbb{N}}$ la suite définie par $v_p = u_{2^p}$.

$$\begin{aligned} v_p &= v_{p-1} + 2^p b \\ &= v_{p-2} + 2^{p-1} b + 2^p b \\ &= b\sum_{k=1}^{p} 2^k + v_0 \\ &= b\sum_{k=0}^{p} 2^k + u_1 \\ &= b\sum_{k=0}^{p} 2^k + 1 + b \\ &= b\sum_{k=0}^{p} 2^k + 1 \\ &= b(2^{p+1} - 1) + 1. \end{aligned}$$

D'où, par croissance de la suite $(u_n)_{n\in\mathbb{N}}$,

$b(2^{\log_2 n}-1)+1 \leqslant u_n \leqslant b(2^{\log_2 n+2}-1)+1$ d'où $bn-b+1 \leqslant u_n \leqslant 4bn-b+1$.

Ainsi, $u_n = \Theta(n)$.

V.2 Multiplication d'entiers par algorithme de Karatsuba

1. On peut éventuellement rajouter des zéros à gauche jusqu'à avoir la même taille pour les deux nombres.
2. L'algorithme a une complexité en $\mathcal{O}(n^2)$.
3. On a $u = u_\mathrm{a} + 2^p \cdot u_\mathrm{b}$, où $p = |u|/2$. De même, $v = v_\mathrm{a} + 2^p \cdot v_\mathrm{b}$. On remarque que

   $$\mathrm{prod}(u,b) = \mathrm{prod}(u_\mathrm{a}, v_\mathrm{a}) + 2^p\big(\mathrm{prod}(u_\mathrm{a}, v_\mathrm{b}) + \mathrm{prod}(u_\mathrm{b}, v_\mathrm{a})\big) + 2^{2p}\cdot\mathrm{prod}(u_\mathrm{b}, v_\mathrm{b}).$$

   Avec $|u| = 2^p$, on note la complexité C_p. On a $C_p = 4C_{p-1} + K = 4(4C_{p-2} + K) + K = 4^p C_0 + K\sum_{i=0}^{p-1} 4^i$. On en déduit que $C_o = \Theta(4^p)$. Or, $p = \log_2 |u|$, d'où $4^{\log_2 |u|} = n^2$. L'algorithme est en $\mathcal{O}(n^2)$.
4. On remarque que $u_\mathrm{a}v_\mathrm{a} + u_\mathrm{b}v_\mathrm{b} - (u_\mathrm{a} - u_\mathrm{b})(v_\mathrm{a} - v_\mathrm{b}) = u_\mathrm{a}v_\mathrm{a} + u_\mathrm{b}v_\mathrm{b}$. Ainsi, $C_p = 3C_{p-1} + K$, d'où $C_p = \Theta(3^p)$. On en déduit que l'algorithme est en $\mathcal{O}(n^{\log_2 3})$.

Partie VI

MPI – Informatique – Annexes

Chapitre 1

Complexité amortie

Avec une fonction PA(n) ayant une complexité en $\mathcal{O}(f(n))$, on considère le problème ci-dessous.

```
for i = 0 to n - 1 do
  PA(i)
done
```

Cet algorithme a une complexité en $\mathcal{O}(nf(n))$. Mais, parfois, cette complexité est trop approximative : parfois, des sommes mathématiques se compensent :

$$\sum_{i=0}^{n-1} 2^i = 2^n \neq \not{\mathcal{O}}(n2^n).$$

On considère le problème ci-dessous.

```
for (int i = 0; i < n; i = i + 1) (
  // calcul qui ne coute pas cher
}
```

Le calcul `i = i + 1` est parfois plus coûteux que le calcul dans la boucle. Par exemple, un algorithme permettant de faire ce calcul est celui ci-dessous.

Algorithme 1.1 Calcul de $n+1$ avec un tableau de *bit*s

Entrée un entier n, représenté sous la forme d'un tableau de *bit* T (où les *bit*s de poids forts sont à droite

1 : $I \leftarrow \text{len}(T) - 1$
2 : **tant que** $T[I] = 1$ **faire**
3 : $\quad T[I] \leftarrow 0$
4 : $\quad I \leftarrow I - 1$
5 : $T[I] \leftarrow 1$

Avec un tel algorithme, on a une complexité, dans le pire des cas, en $\Theta(\log_2 n)$. Ainsi, en modifiant le code, on peut avoir une complexité importante.

```
1       // n est une valeur donnee par l'utilisateur
2       for (int i = 0; i < 2^n; i = i + 1) (
3         // calcul qui ne coute pas cher
4       }
```

La complexité de cet algorithme, que l'on nommera $\mathcal{A}$ dans la suite, est en $\mathcal{O}(\mathtt{n}\,2^{\mathtt{n}})$, car le `i = i + 1` coûte, au pire des cas, `n`. En réalisant des mesures, et en graphant le temps de cet algorithme divisé par $2^{\mathtt{n}}$, on remarque que ce le ratio n'est pas une droite de coefficient directeur `n`, mais une constante (à partir d'un certain rang). On doit donc faire une étude plus précise de la complexité, et faire le calcul de la somme plus proprement. Une étude plus fine nous montre que l'algorithme est beaucoup plus long pour les entiers en plaisances de deux, mais les autres nombres, on n'a pas besoin d'autant de calcul. Faisons cette étude plus fine.

On nomme $\mathcal{T}$ l'ensemble des tableaux de taille n contenant des valeurs dans $\{0,1\}$. On a,

$$\text{Coût}_{\mathcal{A}}(n) = \sum_{t\in\mathcal{T}} \text{Coût}_{\text{Incr}}(t).$$

Partitionnons $\mathcal{T}$:

$$\mathcal{T}_i = \left\{ \begin{array}{|c|c|c|c|c|c|} \hline \ldots & i+1 & i & i-1 & \ldots & 0 \\ \hline \ldots & \mathbf{0} & \mathbf{1} & \mathbf{1} & \ldots & \mathbf{1} \\ \hline \end{array} \in \mathcal{T} \right\}.$$

Si $t \in \mathcal{T}_i$, on sait que $\text{Coût}_{\text{Incr}}(t) = i+1$. Ainsi,

$$\begin{aligned}
\sum_{t\in\mathcal{T}} \text{Coût}_{\text{Incr}}(t) &= \sum_{i=0}^{n-1} \sum_{t\in\mathcal{T}_i} \text{Coût}_{\text{Incr}}(t) \\
&= \sum_{i=0}^{n-1} |\mathcal{T}_i| \cdot (i+1) \\
&= \sum_{i=0}^{n-1} 2^{n-1-i}\,(i+1) \\
&= 2^n \sum_{i=1}^{n} \frac{i}{2^i} \\
&= 2^n \times \mathcal{O}(1) \\
&= \mathcal{O}(2^n)
\end{aligned}$$

ce qui explique les résultats trouvés précédemment. L'incrementation `i = i + 1` est donc en $\mathcal{O}(1)$, et non en $\mathcal{O}(\log_2 \mathtt{i})$.

Définition : Étant donnée une structure (des éléments d'un type de données abstrait, TDA), $\mathbb{F}$, munie d'opérations $\mathbb{O}$ opérant sur $\mathbb{F}$ munis de fonctions de coût

$$\forall o \in \mathbb{O}, \quad C_o : \mathbb{F} \to \mathbb{R}^+.$$

Étant donné un élément initial $f_0 \in \mathbb{F}$ et une suite d'opérations $(o_1, \dots, o_n) \in \mathbb{O}^n$, cela conduit donc à une suite d'éléments

$$f_0 \overset{o_1}{\rightsquigarrow} f_1 \overset{o_2}{\rightsquigarrow} f_2 \rightsquigarrow \cdots \rightsquigarrow f_n.$$

On appelle *complexité* de cette séquence, notée $\tilde{c}$,

$$\tilde{C}\big((o_1, \dots, o_n), f_0\big) = \sum_{i=0}^{n} C_{o_i}(f_{i-1}).$$

On appelle alors *complexité amortie* depuis $f_0 \in \mathbb{F}$ la suite

$$C_{\mathrm{A}}(f_0, n) = \frac{1}{n} \sup_{(o_1,\dots,o_n)\in\mathbb{O}^n} \tilde{C}\big((o_1, \dots, o_n), f_0\big).$$

Exemple (Tableaux dynamiques) :
On s'intéresse aux tableaux à longueur variable : on alloue un tableau de petite taille, et on alloue plus de mémoire au besoin. On a une structure de tableau dynamique :

Algorithme 1.2 Agrandit(T), fonction agrandissant le tableau t

```
1 : Soit taille' = f(len(T))        ▷ f reste à déterminer
2 : On alloue T' de taille taille'
3 : On recopie T dans T'
4 : T ← T'
```

Cet algorithme a une complexité $\text{Coût}_{\text{Agrandit}}(n) = n + f(n)$. On suppose que le tableau T est rempli jusqu'à la r-ième case.

Algorithme 1.3 Ajout(T, x), ajout d'un élément dans le tableau

```
1 : si len(T) = r alors
2 :     Agrandit(T)
3 : T[r] ← x
4 : r ← r + 1
```

On choisit la fonction f.

Cas 1 On choisit $f(n) = n + 1$. Soit une suite de n opérations Ajout depuis un tableau de taille 1, où $r = 0$. Ainsi,

$$f_0 \overset{\text{Ajout}}{\rightsquigarrow} f_1 \overset{\text{Ajout}}{\rightsquigarrow} \cdots \rightsquigarrow f_i \rightsquigarrow \cdots \rightsquigarrow f_{n-1} \overset{\text{Ajout}}{\rightsquigarrow} f_n.$$

La complexité de cette suite d'opérations est

$$\tilde{C}\big((o_1, \dots, o_n), f_0\big) = n + 2 \cdot \frac{n(n+1)}{2},$$

d'où la complexité amortie est de $C_{\mathrm{A}}(f_0, n) = \Theta(n)$.

Cas 2 On choisit $f(n) = 2n$. On somme les complexités : $2n$ (clairement par dessin). Ainsi, $C_{\mathrm{A}}(f_0, n) = \Theta(1)$.

Méthode (du potentiel) :
Considérons une fonction $h : \mathbb{F} \to \mathbb{R}^+$ dite *de potentiel* telle que $h(f_0) = 0$. Intéressons nous alors à $\underline{C}_o(f) = C_o(f) + h(\bar{f}) - h(f)$, où $f \overset{o}{\rightsquigarrow} \bar{f}$. Soit alors

$$f_0 \overset{o_1}{\rightsquigarrow} f_1 \overset{o_1}{\rightsquigarrow} f_2 \rightsquigarrow \cdots \rightsquigarrow f_n$$

une suite d'opérations. Alors,

$$\begin{aligned}\sum_{i=1}^{n} \underline{C}_{o_i}(f_{i-1}) &= \sum_{i=1}^{n} \Big(C_{o_i}(f_{i-1}) + h(f_i) - h(f_{i-1}) \Big) \\ &= \Big(\sum_{i=1}^{n} C_{o_i}(f_{i-1}) \Big) + \underbrace{h(f_n) - h(f_0)}_{\geqslant 0}\end{aligned}$$

par télescopage. Ainsi,

$$\sum_{i=1}^{n} C_{o_i}(f_{i-1}) \leqslant \sum_{i=1}^{n} \underline{C}_{o_i}(f_{i-1}).$$

Exemple :
On applique la méthode du potentiel au cas 2 de l'exemple ci-avant. On rappelle que $\mathbb{F}$ est l'ensemble des tableaux. On pose la fonction

$$\begin{aligned} h : \mathbb{F} &\longrightarrow \mathbb{R}^+ \\ (T, r) &\longmapsto 6 \left(r - \frac{\mathrm{len}(T)}{2} \right)\end{aligned}$$

Inspectons alors

$$\underline{C}_{\textsc{Ajout}}(T, r) = C_{\textsc{Ajout}}(\underline{T}, \underline{r}) + 6\bar{r} - 3\,\mathrm{len}(\bar{T}) - 3\underline{r} + 3\,\mathrm{len}(\underline{T}).$$

Si $\mathrm{len}(\underline{T}) = \underline{r}$, alors $C_{\textsc{Ajout}}(\underline{T}, \underline{r}) = 3\,\mathrm{len}(\underline{T})$ et $\mathrm{len}(\bar{T}) = 2\,\mathrm{len}(\underline{T})$ et $\bar{r} = \underline{r} + 1$. D'où,

$$\underline{C}_{\textsc{Ajout}}(\underline{T}, \underline{r}) = 3\,\mathrm{len}(\underline{T}) + 6\underline{r} + 6 - 6\,\mathrm{len}(\underline{T}) - 6\underline{r} + 3\,\mathrm{len}(\underline{T}) = 6.$$

Sinon, $\mathrm{len}(\underline{T}) > \underline{r}$, alors $\mathrm{len}(\bar{T}) = \mathrm{len}(\underline{T})$ et $\bar{r} = \underline{r} + 1$. Ainsi,

$$\underline{C}_{\textsc{Ajout}}(\underline{T}, \underline{r}) = 1 + 6(\underline{r} + 1) - 6\,\mathrm{len}(\bar{T}) - 6\underline{r} + 6\,\mathrm{len}(\underline{T}) = 7$$

D'où

$$\sum_{i=1}^{n} C_{o_i}(f_{i-1}) \leqslant \sum_{i=1}^{n} \underline{C}_{o_i}(f_{i-1}) \leqslant 7n.$$

Le coût amorti est en $\mathcal{O}(1)$.

Exemple (Méthode du Banquier) :
On encode une file avec deux piles. Au moment de défiler, on doit potentiellement transvaser une pile dans une autre. Avec la méthode du Banquier, on a l'*intuition* que le coût amorti est constant.

On pose $\mathbb{F}$ l'ensemble des couples de piles (p_1, p_2). On a

$$C_{\text{défiler}}\big((p_1,p_2)\big) = \begin{cases} \text{taille } p_1 + 1 & \text{si } p_2 \text{ est vide} \\ 1 & \text{sinon} \end{cases}, \text{ et } C_{\text{enfiler}}\big((p_1,p_2)\big) = 1.$$

Soit h la fonction de potentiel définie comme

$$\begin{aligned} h : \mathbb{F} &\longrightarrow \mathbb{R}^+ \\ (p_1,p_2) &\longmapsto \text{taille } p_1 \end{aligned}$$

Étudions alors $\mathcal{C}_{\text{défiler}}\big((p_1,p_2)\big)$.

— Si p_2 est vide, alors

$$\begin{aligned} \mathcal{C}_{\text{défiler}}\big((p_1,p_2)\big) &= C_{\text{défiler}}\big((p_1,p_2)\big) + h\big((\bar{p}_1,\bar{p}_2)\big) - h\big((p_1,p_2)\big) \\ &= \text{taille } p_1 + 1 + \overbrace{\text{taille } \bar{p}_1}^{=0} - \text{taille } p_1 \\ &= 1. \end{aligned}$$

— Si p_2 n'est pas vide, alors

$$\mathcal{C}_{\text{défiler}}\big((p_1,p_2)\big) = 1 + \underbrace{\text{taille } \bar{p}_1}_{=\text{taille } p_1} - \text{taille } p_1.$$

D'où, pour $(p_1,p_2) \in \mathbb{F}$, $\mathcal{C}_{\text{défiler}}\big((p_1,p_2)\big) \leqslant 1$. De plus,

$$\begin{aligned} \mathcal{C}_{\text{ enfiler}}\big((p_1,p_2)\big) &= C_{\text{enfiler}}\big((p_1,p_2)\big) + h\big((\bar{p}_1,\bar{p}_2)\big) - h\big((p_1,p_2)\big) \\ &= 1 + \text{taille } \bar{p}_1 - \text{taille } p_1 \\ &= 2 \end{aligned}$$

Finalement, pour toute séquence d'opérations $o_1, \ldots, o_n$ initialisée à la file vide f_0, on a

$$\begin{aligned} \frac{1}{n}\tilde{C}\big((o_1,\ldots,o_n), f_0\big) &= \frac{1}{n}\sum_{i=0}^{n} C_{o_i}(f_{i-1}) \\ &\leqslant \frac{1}{n}\sum_{i=1}^{n} \mathcal{C}_{o_i}(f_{i-1}) \\ &\leqslant 2 \end{aligned}$$

D'où, un coût amorti constant.

Chapitre 2

Algorithmes Dijkstra et $A^\star$

On s'intéresse, dans cette annexe, à l'algorithme $A^\star$. Cette annexe se situe à l'intersection des chapitres sur les graphes, et sur les jeux. L'algorithme $A^\star$ est une modification de l'algorithme de Dijkstra. Dans cette annexe, on prouvera la correction de l'algorithme $A^\star$.

On se place dans le contexte d'exécution d'un algorithme de calcul de plus cours chemin utilisant un tableau de distances μ, et le manipulant en n'effectuant que des opérations Relâcher. Notons le graphe $G = (V, E)$, le sommet source s. Notons également $d(\cdot, \cdot)$ la distance induite par les arêtes du graphe G. De plus, on notera $c(\cdot, \cdot)$ les coûts (positifs, non nuls) d'une arête de G. Notons $\ell(\cdot)$ les rongeurs des chemins.

Lemme 1 :

$$\forall (u, v) \in E, \quad d(s, v) \leqslant d(s, u) + c(u, v).$$

Preuve :
Soit $(u, v) \in E$. Soit γ_u un plus court chemin de s à u. Alors, $\gamma_u \cdot v$ est un chemin de s à v :

$$\ell(\gamma_u \cdot v) = \ell(\gamma_u) + c(u, v) = d(s, u) + c(u, v) \geqslant d(s, v).$$

□

Lemme 2 : Pour tout sommet u, la valeur de $\mu[u]$ est décroissant à mesure que l'algorithme s'exécute.

Preuve :

Soit $\underline{\mu}$ et $\bar{\mu}$ les valeurs de μ avant et après une opération RELÂCHER(x, y). Pour tout sommet $v \neq y$, $\bar{\mu}[v] = \underline{\mu}[v]$. De plus, par disjonction de cas,

— ou bien $\bar{\mu}[y] = \underline{\mu}[y]$, OK.

— ou bien $\bar{\mu}[y] = \underline{\mu}[x] + c(x, y)$ lorsque $\underline{\mu}[x] + c(x, y) \leqslant \underline{\mu}[y]$, donc $\bar{\mu}[y] \leqslant \underline{\mu}[y]$, OK.

□

Lemme 3 : Supposons que l'algorithme ait initialisé μ de la manière suivante :

$$\forall u \in V, \qquad \mu[u] = \begin{cases} +\infty & \text{si } u \neq s \\ 0 & \text{sinon.} \end{cases}$$

Alors, tout au long de l'exécution de l'algorithme, pour tout sommet u, $\mu[u] \geqslant d(s, u)$.

*Preuve :***Initialement** La propriété est vraie par hypothèse.

Hérédité ăSupposons vrai jusqu'à un certain état $\underline{\mu}$, pour une opération RELÂCHER(x, y). Pour tout sommet $v \neq y$, $\underline{\mu}[v] = \bar{\mu}[v] \geqslant d(s, v)$. De plus, par disjonction de cas,

— si $\bar{\mu}[y] = \underline{\mu}[y] \geqslant d(s, y)$;

— sinon si $\underline{\mu}[y] = \underline{\mu}[x] + c(x, y) \geqslant d(s, x) + c(x, y) \geqslant d(s, y)$ par hypothèse de récurrence, puis par lemme 1.

□

Corollaire : Si « à un moment » $\mu[u] = d(s, u)$, alors « pour toujours après » $\mu[u] = d(s, u)$. □

Lemme 4 : Si $(s, \ldots, u, v)$ est un plus court chemin de s à v tel que $\underline{\mu}[u] = d(s, u)$ « à un certain moment de l'exécution de l'algorithme. » Notons $\bar{\mu}$ obtenu par RELÂCHER(u, v).

Preuve :
On a

$$\bar{\mu} = \begin{cases} \underline{\mu}[v] & \text{si } \underline{\mu}[v] \text{ă} < \underline{\mu}[u] + c(u, v) \\ \underline{\mu}[u] + c(u, v) & \text{sinon.} \end{cases}$$

Par disjonction de cas,

— si $\underline{\mu}[v] < \underline{\mu}[u] + c(u, v) = d(s, u) + c(u, v) = d(s, v)$, et donc, en utilisant le lemme 3, $\bar{\mu}[v] = \underline{\mu}[v] = d(s, v)$.

— sinon, $\bar{\mu}[v] = \underline{\mu}[u] + c(u,v) = d(u,v) + c(u,v) = d(s,v)$.

□

Lemme 5 : Soit $(s = x_0, x_1, x_2, \ldots, x_n)$ un plus court chemin. Si on effectue des opérations RELÂCHER(x_i, x_{i+1}) dans l'ordre $0 \to n-1$, possiblement entremêlés avec d'autres opérations RELÂCHER, alors pour tout $i \in [\![0, n]\!]$, $\mu_{\text{final}}[x_i] = d(s, x_i)$.

Preuve (par récurrence) *:* — Initialement, $\mu[x_0] = d(s, x_0) = d(s,s)$.
— Et, pour tout les i inférieurs stricts, $\mu[x_i] = d(s, x_i)$, on conclut par le lemme 4.

□

(De ce lemme découle l'algorithme de BELLMAN-FORD.)

Corollaire : L'algorithme DIJKSTRA est correct.

Preuve :
Soit $t \in V$, un sommet du graphe. Soit $(s = x_0, x_1, \ldots, x_{p-1}, x_p = t)$ un plus court chemin de s à t. Montrons que $\mu_{\text{final}}[t] = d(s,t)$. En utilisant le lemme 5, il suffit de montrer que DIJKSTRA relâche les arêtes dans cet ordre. Supposons les sommets extraits todo dans l'ordre $x_0, \ldots, x_i$, pour $i \in [\![0, p-1]\!]$. Par l'absurde, supposons que DIJKSTRA sorte x_k de todo pour $k \in [\![i+2, p]\!]$. « À ce moment là, » on a

$$d(s, x_k) \leqslant \mu[x_k] \leqslant \mu[x_{i+1}] \leqslant d(s, x_{i+1}),$$

d'après le lemme 5, ce qui est absurde ($k > i+1$). □

Corollaire : L'algorithme $A^\star$ est correct.

Algorithme 2.1 Algorithme $A^\star$ (partiel)

```
1 : Procédure RELÂCHER(u, v)
2 :     si μ[v] > μ[u] + c(u, v) alors
3 :         μ[v] ← μ[u] + c(u, v)
4 :         π[v] ← u
5 :         η[v] ← μ[v] + h(v)
```

Preuve :
Par l'absurde, supposons que non. Soit $t \in V$, un sommet du graphe, tel que $\mu_{\text{final}}[t] \neq d(s,t)$. Donc $d = \mu_{\text{final}}[t] > d(s,t) = d^\star$. Soit $(s = x_0, x_1, \ldots, x_{p-1}, x_p = t)$ un plus court chemin de s à t de longueur $d^\star$. L'algorithme commence par visiter $x_0 = s$ et on relâche les arêtes sortantes. Alors, $\mu[x_i] = d(s,x_1)$ et $\eta[x_1] = \mu[x_1] + \mu[x_1] + h(x_1) \leqslant d(s,x_1) + d(x_1,t) = d(s,t) = d^\star < d$ par hypothèse. « À ce state, » $\eta[t] = \mu[t] + h(t) \geqslant d + 0$. Ainsi, x_1 devrait être choisi avant t. À un tel moment, $\mu[x_1] = d(s,x_1)$, on relâche alors ses arêtes sortantes ; en particulier x_1 et x_2. Ceci assure alors que $\mu[x_2] = d(s,x_2)$, et $\eta[x_2] = \mu[x_2] + h(x_2) \leqslant d(snx_2) + d(x_2,t) \leqslant d(s,t) = d^\star < d$. « De proche en proche, » alors que l'on choisit x_{p-1} dans todo, on a $\mu[x_{p-1}] = d(s,x_{p-1})$. On relâche alors $\mu[x_p] = d(s,x_p) = d^\star$. Or, $d = \mu_{\text{final}}[t] \leqslant \mu_{\text{à ce moment}}[t]$. Absurde. □

Exemple (ré-entrée dans todo) :
Exécution de l'algorithme $A^\star$ sur l'entrée ci-dessus. La pile todo est vaut donc $\not{s}, \not{a}, \not{b}, \not{t}, \not{a}$.

Chapitre 3

Diviser pour régner

On se place dans un contexte dans l'idée de coder des algorithmes avec la stratégie « diviser pour régner. » Par exemple, on considère un algorithme de calcul de maximum divisant le tableau en deux à chaque itération. [1] Le calcul usuel de maximum est en $\mathcal{O}(n)$. On peut espérer que cet algorithme divisant le tableau ait une complexité logarithmique. Calculons cette complexité.

Soit $(C_n)_{n\in\mathbb{N}}$ la suite donnant le nombre de comparaisons entre éléments du tableau [2] effectuées par l'algorithme `aux_max` sur un intervalle de taille $|j-i+1| = n$. On a $C_0 = 0$, $C_1 = 0$, et pour tout $n \geqslant 2$, $C_n = C_{\lfloor \frac{n}{2} \rfloor} + C_{\lceil \frac{n}{2} \rceil} + 1$.

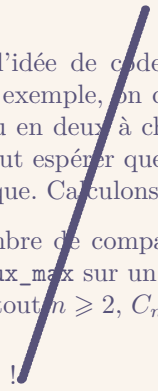


FIGURE 3.1

Soit $(v_p)_{p\in\mathbb{N}}$ la suite définie par $v_p = C_{2^p}$. Ainsi, $v_0 = 0$ et

$$v_{p+1} = C_{2^{p+1}} = C_{\lfloor \frac{2^{p+1}}{2} \rfloor} + C_{\lceil \frac{2^{p+1}}{2} \rceil} + 1 = 2v_p + 1.$$

Calculons v_p :

$$\begin{aligned} v_p &= 2v_{p-1} + 1 \\ &= 2(2v_{p-2} + 1) + 1 \\ &= 2^2 v_{p-2} + 2^1 + 2^0 \\ &\vdots \\ &= 2^p v_0 + \sum_{i=1}^{p-1} 2^i \\ &= 2^p - 1 \end{aligned}$$

1. C'est le principe des tournois sportifs.
2. *i.e.* le nombre d'appels à la fonction `max`.

Ce résultat ne s'applique que pour les puissances de 2, mais, par un argument de croissance, on peut en déduire un résultat pour tout entier n. Montrons que la suite $(C_n)_{n\in\mathbb{N}}$ est croissante. En effet, par récurrence forte, soit $n \geqslant 2$.

— Si n est pair, alors $C_n = 2\times C_{\frac{n}{2}}+1$ et $C_{n-1} = C_{\frac{n-2}{2}}+C_{\frac{n-2}{2}+1}+1 = C_{\frac{n}{2}-1}+C_{\frac{n}{2}}+1$. Et, $C_{\frac{n}{2}-1}\leqslant C_{\frac{n}{2}}$ par hypothèse de récurrence. D'où, $C_n \geqslant C_{n+1}$.

— De même si n est impair.

Ainsi, soit $n \in \mathbb{N}^\star$. On pose alors $p = \lfloor \log_2 n \rfloor$ donc $p \leqslant \log_2 n$. Par croissance de C, on a $C_{2^p} \leqslant C_n \leqslant C_{2^{p+1}}$ donc $v_p \leqslant c_n \leqslant v_{p+1}$. Ainsi,

$$\begin{gathered}
2^p - 1 \leqslant C_n \leqslant 2^{p+1} - 1 \\
2^{\lfloor \log_2 n \rfloor} - 1 \leqslant C_n \leqslant 2^{\lfloor \log_2 n \rfloor + 1} - 1 \\
2^{\log_2(n)-1} - 1 \leqslant C_n \leqslant 2^{\log_2(n)+1} \\
\frac{1}{2}n - 1 \leqslant C_n \leqslant 2n - 1
\end{gathered}$$

Ceci étant vrai pour tout $n \in \mathbb{N}^\star$, on a $C_n = \Theta(n)$. On peut remarquer que cet algorithme a une complexité équivalente à un algorithme itératif. Mais, [3] la complexité de cet algorithme s'améliore si les calculs se font en parallèles.

Autre exemple, le tri fusion a une complexité en $C_n = C_{\lfloor \frac{n}{2} \rfloor} + C_{\lceil \frac{n}{2} \rceil} + n$, ce qui donne une complexité en $\mathcal{O}(n \log n)$.

3. et c'est tout l'intérêt pour les tournois sportifs

Chapitre 4

Lemme d'Arden et retour sur le théorème de Kleene

Exemple (Lemme d'Arden) :
Soient K et L deux langages. Résoudre $X = K \cdot X \cup L$ pour X un langage. (On trouve $X = K^\star \cdot L$.) On suppose que $\varepsilon \notin K$. On procède par double-inclusion.

"$\supseteq$" Soit X un langage tel que $X = K \cdot X \cup L$. Montrons par récurrence « si w est un mot de X de taille n, alors $w \in K^\star \cdot L$.

- Si $n = 0$, alors $w \in L$ car $\varepsilon \notin K$. Ainsi, $w = \varepsilon \cdot w$ et $\varepsilon \in K^\star$. On en déduit que $w \in K^\star \cdot L$.
- Si $|w| = n$, alors
  - si $w \in L$, alors $w = \varepsilon \cdot w$ et donc $w \in K^\star L$.
  - si $w = v \cdot w'$ où $v \in K$ et $w' \in X$, alors $|w'| < |w|$. Ainsi, par hypothèse de récurrence, $w' \in K^\star \cdot L$. Ainsi, $v \cdot w' \in K^\star \cdot L$.

Ainsi, $X \subseteq K^\star \cdot L$.

"$\subseteq$" Soit $w \in K^\star \cdot L$. Il existe donc $n \in \mathbb{N}$, $(v_1, \ldots, v_n) \in K^n$ et $w' \in L$ tels que $w = v_1 \cdot \ldots \cdot v_n \cdot w'$. Alors, $w' \in X$ donc $v_n \cdot w' \in X$ donc $\ldots$ donc $v_1 v_2 \ldots v_n w' \in X$. Ainsi, $w \in X$.

Exemple :
On considère l'automate ci-dessous.

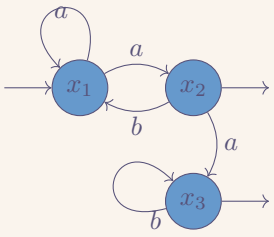


Figure 4.1 – Automate exemple ($\mathcal{A}$)

On pose $X_i = \mathscr{L}\big((\Sigma, \mathbb{Q}, \{i\}, F, \delta)\big)$, où x_i est l'unique point de départ. Ainsi, $\mathscr{L}(\mathscr{A}) = \bigcup_{i\in I} X_i$. Déterminons les valeurs de X_1, X_2 et X_3. On applique un algorithme similaire au « pivot de Gauß. »

$$\left.\begin{array}{ll} X_1 & = \{a\} \cdot X_2 \cup \{a\} X_1 \\ X_2 & = \{b\} \cdot X_1 \cup \{a\} \cdot X_3 \cup \{\varepsilon\} \\ X_3 & = \{b\} X_3 \cup \{\varepsilon\} \end{array}\right\} \iff \begin{cases} X_1 & = \{a\}^\star \cdot \{a\} \cdot X_2 \\ X_2 & = \mathscr{L}(ba^\star \cdot a) X_2 \cup \{a\} X_3 \cup \{\varepsilon\} \\ X_3 & = \{b\} \cdot X_3 \cup \{\varepsilon\} \end{cases}$$

$$\iff \begin{cases} X_1 & = \mathscr{L}(a^\star \cdot a) X_2 \\ X_2 & = \mathscr{L}\big((b \cdot a^\star \cdot a)^\star\big) \cdot \big(\{a\} X_3 \cup \{\varepsilon\}\big) \\ X_3 & = \{b\} X_3 \cup \{\varepsilon\} \end{cases}$$

$$\iff \begin{cases} X_1 & = \mathscr{L}(a^\star \cdot a) X_2 \\ X_2 & = \mathscr{L}\big((b \cdot a^\star \cdot a)^\star\big) \cdot \big(\{a\} X_3 \cup \{\varepsilon\}\big) \\ X_3 & = \mathscr{L}(b^\star) \end{cases}$$

$$\iff \begin{cases} X_1 & = \mathscr{L}(a^\star \cdot a) X_2 \\ X_2 & = \mathscr{L}\big((ba^\star a)^\star \cdot (ab^\star \mid \varepsilon)\big) \\ X_3 & = \mathscr{L}(b^\star) \end{cases}$$

$$\iff \begin{cases} X_1 & = \mathscr{L}\big(a^\star \cdot a \cdot (ba^\star a)^\star \cdot (ab^\star \mid \varepsilon)\big) \\ X_2 & = \mathscr{L}\big((ba^\star a)^\star \cdot (ab^\star \mid \varepsilon)\big) \\ X_3 & = \mathscr{L}(b^\star) \end{cases}$$

On peut généraliser la méthode employée dans l'exemple précédent pour montrer que tout langage reconnaissable est régulier.

Chapitre 5

Tas et files de priorités

L'objectif d'une file de priorité est de récupérer l'élément de priorité minimale. On organise cette structure de données sous forme d'un arbre tournois.[1] Un arbre tournois est un arbre dont la priorité d'un nœud est supérieur à celle de ses fils. On impose une structure supplémentaire, l'arbre doit être parfait : l'arbre est complet jusqu'à l'avant dernier niveau, où il est replis à gauche. On définit plusieurs opérations sur cette file de priorité (de type `fp`, où les éléments sont de type `elem`) :

- `insérer` : `fp` → `elem` → `fp` qui insère un élément,
- `lire_min` : `fp` → `elem` qui récupère l'élément de priorité minimale,
- `supprimer_min` : `fp` → `fp` qui supprime l'élément de priorité minimale,
- (`diminuer_priorité` : `fp` → `elem` → `fp`),[2]
- `créer` : ( ) → `fp`.

On définit un type `btree`, représentant un arbre binaire, et on implémente les opérations ci-dessous en OCaml.

```
type 'a btree =
| Node of 'a * 'a btree * 'a btree
| Empty
```

Code 5.1 – Définition du type `btree`

Pour l'opération `créer`, on retourne `Empty` (cela donne une complexité en $\Theta(1)$). Pour l'opération `insérer`, on insère l'élément comme feuille (de manière à conserver la propriété de l'arbre parfait), et on inverse le nœud avec son parent jusqu'à ce que la propriété soit vérifiée ($\Theta(\log_2 n)$). Pour l'opération `lire_min`, on lit la racine ($\Theta(1)$). Pour l'opération `supprimer_min`, on permute la racine et le dernier nœud (*i.e.* le nœud le plus à droite de hauteur maximale), et on restore la structure d'arbre tournois en permutant un nœud et son fils de valeur minimale, et en répétant ($\Theta(\log_2 n)$). Pour trouver le dernier nœud, on garde en mémoire cet emplacement. On peut aussi implémenter cet algorithme avec un tableau (▷ TP), ou avec une liste triée (mais la complexité est moins bien).

1. Un arbre tournois n'est pas un arbre binaire de recherche.
2. Cette opération est parfois omise car trop compliquée à implémenter.

Chapitre 6

Arithmétique

Un des premiers algorithmes codé est l'algorithme d'Euclide pour calculer le PGCD. Pour $a \neq 0$, on a $a \wedge 0 = a$ et $a \wedge b = b \wedge (a \bmod b)$. On peut le coder en OCaml avec la fonction `euclid` suivante.

```
let rec euclid (a: int) (b: int): int =
  (* Hyp: a >= b et a != 0 *)
  if b = 0 then a
  else euclide b (a mod b)
```

Code 6.1 – Algorithme d'Euclide calculant le PGCD

Quelle est la complexité de cet algorithme ? On représente le nombre d'appels récursifs à `euclid`, et on devine une courbe logarithmique. En notant (u_n) les divisions euclidiennes réalisées et (q_n) les quotients, ainsi, on $u_n = q_{n-1} \cdot u_{n-1} + u_{n-2}$. Alors, $\texttt{euclid}(u_n, u_{n-1}) = \cdots = \texttt{euclid}(u_3, u_2) = \texttt{euclid}(u_2, u_1) = \texttt{euclid}(u_1, u_0)$.

En fixant la complexité, on cherche les valeurs de (u_n) maximisant les appels récursifs. On peut montrer par récurrence que si $\texttt{euclid}(a, b)$ conduit à n appels récursifs de `euclid`, alors $a \geqslant F_n$ et $b \geqslant F_{n-1}$, où $(F_n)_{n\in\mathbb{N}}$ est la suite de Fibonacci.

En effet, soit un tel couple (a, b). Alors, $(b, a \bmod b)$ conduit à $n-1$ appels récursifs donc $b \geqslant F_{n-1}$ et $a \bmod b \geqslant F_{n-2}$ par hypothèse de recurrence. Et, $a = bq + (a \bmod b)$ et donc $a \geqslant F_{n-1} + F_{n-2} = F_n$.

De plus, pour tout $n \in \mathbb{N} \setminus \{0, 1\}$, $F_n \geqslant \varphi^{n-2}$ où φ est le nombre d'or. [1] En effet, $F_2 = 1 \geqslant \varphi^0 = 1$ et $F_3 = 2 \geqslant \varphi^1 = \varphi = (1 + \sqrt{5})/2$. Et, $F_n = F_{n-1} + F_{n-2} \geqslant \varphi^{n-3} + \varphi^{n-4} \geqslant \varphi^{n-4}(1 + \varphi) \geqslant \varphi^{n-2}$.

Soient (p, q), où $p \geqslant q$, une entrée de l'algorithme d'Euclide. Si l'appel $\texttt{euclid}(p, q)$ conduit à plus de $\lceil \log_\varphi p \rceil + 4$ appels, alors $p \geqslant F_{\lceil \log_\varphi p \rceil + 4} \geqslant \varphi^{\lceil \log_\varphi p \rceil + 4 - 2} > \varphi^{\log_\varphi p} = p$, ce qui est absurde.

Ceci conduit à une complexité en $\mathcal{O}(\log p)$.

1. C'est la solution positive de $X^2 - X - 1 = 0$.

Soit n un entier premier. Pour l'algorithme RSA, on cherche un inverse de $a \in \mathbb{Z}/n\mathbb{Z}$: on cherche $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab \equiv 1$ [1]. D'après le théorème de Bézout, on a $au + nv = 1$ car $a \wedge n = 1$. L'inverse est v. D'où l'importance des coefficients de Bézout.

Comment calculer les coefficients de Bézout ? On peut utiliser l'algorithme d'Euclide. On pose r_n la valeur de `a` après n appels récursifs.

r_i	u_i		v_i	
$r_0 = a$	1	a	0	b
$r_1 = b$	0	b	1	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{i-2}	u_{i-2}	a	v_{i-2}	b
r_{i-1}	u_{i-1}	a	v_{i-1}	b

TABLE 6.1 – Valeurs de r_i avec invariant $r_i = au_i + bv_i$

Alors,

$$\begin{aligned} r_i &= u_{i-2}a + v_{i-2}b - (r_{i-2}/r_{i-1})(u_{i-1}a + v_{i-1}b) \\ &= \big(u_{i-2} - (r_{i-2}/r_{i-1})u_{i-1}\big)a + \big(v_{i-2} - (r_{i-2}/r_{i-1})v_{i-1}\big)b \end{aligned}$$

Ainsi, on a bien $\text{pgcd}(a, b) = u_{n-1}a + v_{n-1}b$.

Chapitre 7

Arbres rouges-noirs

Un arbre rouge-noir est un cas particulier des arbres binaires de recherches. On l'utilise notamment pour représenter des ensembles, on veut donc réaliser deux opérations simples : l'insertion et le test d'appartenance. Initialement, on pense représenter un ensemble par une liste triée. Mais, on utilise plutôt un arbre binaire pour représenter des données avec une hauteur logarithmique, contrairement à une hauteur linéaire. Les arbres binaires de recherches sont des arbres dans lesquels ont peut réaliser une dichotomie.

```
1  type 'a btree = E | N of 'a * 'a btree * 'a btree
2
3  let rec mem (x: 'a) (t: 'a btree): bool =
4    match t with
5    | E -> false
6    | N(y, g, d) ->
7        if x < y      then mem x g
8        else if x = y then true
9        else               mem x d
10
11 let rec insere (x: 'a) (t: 'a btree): 'a btree =
12   match t with
13   | E -> false
14   | N(y, g, d) ->
15       if x < y      then N(y, insere x g, d)
16       else if x = y then t
17       else               N(y, g, insere x d)
```

Code 7.1 – Arbre binaire de recherche

La fonction `mem` permet de réaliser ce test d'appartenance et la fonction `insere` insère l'insertion dans l'arbre. Ainsi, on peut représenter un ensemble avec le type `'a btree`.

Mais, cet arbre peut être déséquilibré, et l'utilisation de la dichotomie ne donne pas de résultats très avantageux. On utilise donc un arbre *auto-équilibrant*, comme les AVL du 1er DM. Pour les AVL, la différence de hauteur est -1, 0 ou 1.

On introduit donc le concept d'arbre rouge-noir. Un arbre rouge-noir est un

arbre parfait, qui a une certaine « élasticité. » On colorie chaque nœuds pour imposer des contraintes sur cette élasticité. Les branches de l'arbre a une longueur de rupture. Un arbre contenant uniquement des nœuds noirs est un arbre parfait. Et, entre deux nœuds noirs, on peut insérer un nœud rouge. Un arbre rouge-noir vérifie donc les trois propriétés suivantes :

(*a*) la racine est noire,

(*b*) le père d'un nœud rouge est noir,

(*c*) la hauteur noir de chaque feuille externe est constante. [important]

Une *feuille externe* est, dans le code OCaml, l'expression `E` ; et, la *hauteur noir* d'une feuille externe est le nombre de nœuds noirs depuis la racine. On définit la *hauteur noir* d'un arbre comme la hauteur noir de chaque feuille externe (qui est constante).

Le problème est l'insertion d'un nœud. Insérer un nœud noir est, en général, plus dangereux car il modifie la hauteur noir de tout l'arbre. On préfère donc insérer un nœud rouge, sauf dans le cas de la racine.

On considère donc la propriété (*c*) comme invariante. En effet, corriger un arbre pour valider la propriété (*a*) ou la propriété (*b*) est bien plus simple.

On traite tous les cas dans le diaporama sur *cahier-de-prépa*, et on réalise l'exemple sur les lettres A, L, G, O, R, I, T, H, M, E.

Pour supprimer un nœud dans un arbre binaire classique, on peut le remplacer par le maximal de son sous-arbre droit, ou le minimum de son sous-arbre gauche. Si on supprime un nœud ayant un seul fils, on n'a qu'à re-brancher le sous-arbre. Pour les arbres rouges-noirs, c'est supprimer un nœud noir qui pose problème. Pour cela, on introduit les nœuds doublement noirs, qui comptent pour deux dans la hauteur noir. Ainsi, on supprime le nœud noir et on remplace les autres nœuds par des nœuds doublement noirs. L'algorithme n'a donc qu'à faire remonter le nœud doublement noir, jusqu'à la racine, où il sera transformé en nœud simplement noir.

Un arbre de hauteur h a une hauteur noir $\mathrm{bh} \geqslant h/2$. Et, la taille, *i.e.* le nombre de nœuds, est supérieure à $2^{\mathrm{bh}} - 1$. On conclut que $h \leqslant 2\log_2(\text{taille} + 1)$. De même par la propriété (*c*) permet de conclure que $h = \Theta(\log_2 \text{taille})$.

Chapitre 8

Complexité moyenne

Dans les annexes et cours précédents, on a vu la complexité « pire cas » et la complexité amortie. On considère les nombres d'opérations possibles pour toute entrée de taille n. La complexité « pire cas » est la complexité obtenue en prenant le max d'opération possibilité. Pour la complexité moyenne, on suppose que chaque ensemble d'entrée de taille n est munit d'une probabilité P_n. Par exemple, on considère qu'une entrée est une permutation de n éléments, *i.e.* un élément de $\mathfrak{S}_n$. On suppose que chaque entrée arrive avec équiprobabilité. Ainsi, $\forall \sigma \in \mathfrak{S}_n$, $P_n(\sigma) = 1/n!$. Ainsi, on a

$$C_{\max}(n) = \max_{\sigma \in \mathfrak{S}_n} C(s) \text{ et } C_{\text{moy}} = \sum_{\sigma \in \mathfrak{S}_n} P(\sigma) \cdot C(\sigma).$$

La complexité moyenne est la moyenne des complexité pondérées par les probabilités.

Exemple :
On considère l'algorithme ci-dessous.

Algorithme 8.1 Calcul d'inverse d'une permutation

Entrée $\sigma \in \mathfrak{S}_n$ et $i \in [\![1, n]\!]$
Sortie $j \in [\![1, n]\!]$ tel que $\sigma(j) = i$.
1 : **pour** $j \in [\![1, n]\!]$ **faire**
2 : ⌊ **si** $\sigma(j) = i$ **alors retourner** j

On munit $\mathfrak{S}_n$ de la probabilité uniforme. Soit $i \in [\![1, n]\!]$. Notons, pour tout

$j \in [\![1, n]\!]$, $\mathfrak{S}_n^j = \{\sigma \in \mathfrak{S}_n \mid \sigma(j) = i\}$. Remarquons que $\mathfrak{S}_n = \bigcup_{j=1}^n \mathfrak{S}_n^j$. Ainsi,

$$\begin{aligned} C_{\text{moy}} &= \sum_{j=1}^{n} \sum_{\sigma \in \mathfrak{S}_n^j} P_n(\sigma) C(\sigma) \\ &= \sum_{j=1}^{n} j \times \frac{|\mathfrak{S}_n^j|}{n!} \\ &= \sum_{j=1}^{n} j \times \frac{(n+1)!}{n!} \\ &= \frac{1}{n} \cdot \frac{n(n+1)}{2} \\ &= \frac{n+1}{2} \end{aligned}$$

Chapitre 9

Preuves de correction pour les fonctions récursives

On considère l'insertion dans un arbre binaire de recherche. Démontrons qu'elle est correcte. On adopte les notations de l'annexe G sur les arbres rouges-noirs. Montrons que, pour tout ABR t, et pour tout étiquette $e \in \mathbb{E}$,

$$\text{étiquettes}(\texttt{insertion}(t, x)) = \text{étiquettes}(t) \cup \{x\}.$$

Montrons le par induction.

1. Si $t = \texttt{E}$. Soit $x \in \mathbb{E}$:

$$\text{étiquettes}(\texttt{insertion}(\texttt{E}, x)) = \text{étiquettes}(N(x, \texttt{E}, \texttt{E})) = \{x\} = \underbrace{\text{étiquettes}(\texttt{E})}\cup\{x\}.$$

2. Si $t = \texttt{N}(y, g, d)$. Soit $x \in \mathbb{E}$.
   — si $x < y$, alors

$$\begin{aligned}\text{étiquettes}(\texttt{insertion}(t, x)) &= \text{étiquettes}(\texttt{N}(y, \texttt{insertion}(g, x), d)) \\ &= \{x\} \cup \text{étiquettes}(\texttt{insertion}(g, x)) \cup \text{étiquettes}(d) \\ &= \{y\} \cup \text{étiquettes}(g) \cup \{x\} \cup \text{étiquettes}(d) \\ &= \text{étiquettes}(\texttt{N}(y, g, d)) \cup \{x\} \\ &= \text{étiquettes}(t) \cup \{x\}\end{aligned}$$

   — on procède de même pour les autres cas.

On procède de même pour les autres propriétés.

Partie VII

MPI – Mathématiques – Cours

Chapitre 1

Séries numériques

VII.1 La nature d'une suite ou d'une série

Méthode :
Une suite $(u_n)_{n\in\mathbb{N}}$ peut

1. avoir une limite $\ell \in \mathbb{R}$;
2. avoir pour limite $\pm\infty$;
3. ne pas avoir de limite.

Converger concerne le premier point ; *avoir une limite* correspond aux deux premiers points et *diverger* correspond aux deux derniers.

Théorème de la limite monotone : toute suite croissante majorée a une limite.

Une série est notée $\sum u_n$. On dit qu'elle *converge* si la suite des sommes partielles S_n converge

$$S_n = \sum_{k=0}^{n} u_n.$$

La série "$\sum u_n$" n'a pas de valeurs mais une nature ; contrairement à la somme partielle "$\sum_{k=0}^{n} u_n$ a une valeur, on peut la calculer (elle existe toujours) ; et $\sum_{k=0}^{\infty} u_k$ qui est la limite de la somme partielle (elle existe si la série converge).

Si la suite (u_n) ne tends pas vers 0, la série $\sum u_n$ diverge mais la réciproque est fausse : par exemple, la somme des "$\frac{1}{n}$" tends vers 0 mais la série diverge.

Rappel :

Notation en “grand O” : soient u et v deux suites réelles (ou complexes).

$$\begin{aligned} v_n = O(u_n) &\overset{\text{def}}{\iff} v_n = b_n \times u_n, \text{ où } b_n \text{ est bornée,} \\ v_n = o(u_n) &\overset{\text{def}}{\iff} v_n = \varepsilon_n \times u_n, \text{ où } \varepsilon_n \xrightarrow[n\to+\infty]{} 0, \\ v_n \sim u_n &\overset{\text{def}}{\iff} v_n = \underbrace{(1+\varepsilon_n)}_{\xrightarrow[n\to+\infty]{}1} \times u_n, \text{ où } \varepsilon_n \xrightarrow[n\to+\infty]{} 0. \end{aligned}$$

Si on peut diviser par u_n, on peut vérifier

$$\begin{aligned} v_n = O(u_n) &\iff \frac{v_n}{u_n} \in [m, M], \\ v_n = o(u_n) &\iff \frac{v_n}{u_n} \xrightarrow[n\to+\infty]{} 0, \\ v_n \sim u_n &\iff \frac{v_n}{u_n} \xrightarrow[n\to+\infty]{} 1. \end{aligned}$$

Si la série $\sum u_n$ oscille entre des valeurs positives et négatives, on peut analyser $\sum |u_n|$ car si cette série converge, alors $\sum u_n$ aussi.

Exercice : 1. Quelle est la nature de la série $\sum \frac{1}{n^2+\sqrt{n}}$?

$$0 \leqslant \frac{1}{n^2+\sqrt{n}} \leqslant \frac{1}{n^2}$$

On sait déjà que $\sum \frac{1}{n^2}$ converge (vers $\frac{\pi^2}{6}$) mais ce résultat sera redonné dans la proposition 6 : Critère de Riemann. On en déduit que $\sum \frac{1}{n^2+\sqrt{n}}$ converge aussi (par comparaison).

Autre méthode : on a

$$0 \leqslant \frac{1}{n^2+\sqrt{n}} \sim \frac{1}{n^2}$$

(à démontrer) ; et comme $\sum \frac{1}{n^2}$ converge alors $\sum \frac{1}{n^2+\sqrt{n}}$ aussi.

2. On a, comme dans le 1.,

$$\frac{1}{n^2+\sqrt{n}} \sim \frac{1}{n^2}$$

et, comme $\sum \frac{1}{n^2}$ converge alors $\sum \frac{1}{n^2+\sqrt{n}}$ converge aussi.

3. On a

$$\frac{1}{n\cos^2 n} \geqslant \frac{1}{n},$$

or, $\sum \frac{1}{n}$ diverge (d'après le critère de Riemann) et donc $\sum \frac{1}{n\cos^2 n}$ aussi.

4. On a

$$\frac{\ln n}{n^2} = \underbrace{\boxed{\frac{\ln n}{n^{0,7}}}}_{n\to+\infty} \times \frac{1}{n^{1,3}} = \underset{n\to+\infty}{o}\left(\frac{1}{n^{1,3}}\right).$$

Or, $\sum \frac{1}{n^{1,3}}$ converge (d'après le critère de Riemann) donc $\sum \frac{\ln n}{n^2}$ converge.

5. Dans cet exemple, on ne peut pas utiliser une minoration $\frac{\sin n}{n^2}$ par $\frac{1}{n^2}$ car la première suite change de signe.

   On a
   $$0 \leqslant \left|\frac{\sin n}{n^2}\right| \leqslant \frac{1}{n^2}$$
   or, $\sum \frac{1}{n^2}$ converge d'où $\sum \left|\frac{\sin n}{n^2}\right|$ converge et donc $\sum \frac{\sin n}{n^2}$ converge (absolument).

VII.2 Comparer série et intégrale

Méthode :

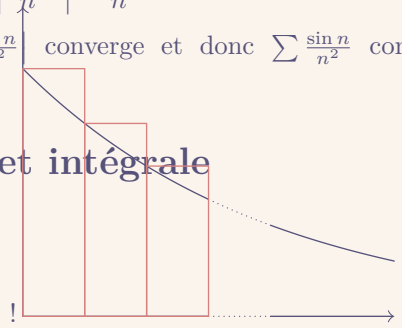


Figure 1.1 – Comparaison série intégrale

À faire : Refaire les deux graphiques

Des deux dessins ci-dessus, on en déduit les deux inégalités suivantes :
$$\int_1^{n+1} f(x)\,\mathrm{d}x \leqslant \sum_{k=1}^{n} u_k \qquad \text{et} \qquad \sum_{k=2}^{n} u_k \leqslant \int_1^{n} f(x)\,\mathrm{d}x.$$

Ainsi,
$$\int_1^{n+1} f(x)\,\mathrm{d}x \leqslant \sum_{k=1}^{n} u_k \leqslant u_1 + \int_1^{n} f(x)\,\mathrm{d}x.$$

Cette méthode permet de calculer une série en calculant une intégrale. On dispose, en effet, de bien plus d'outils pour calculer des intégrales que des séries.

Exercice :
On utilise le résultat trouvé dans la méthode précédente : on pose
$$H_n = \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}.$$

On a donc
$$\begin{aligned} &\int_1^{n+1} \frac{1}{x}\,\mathrm{d}x \leqslant \sum_{k=1}^{n} \frac{1}{k} \leqslant 1 + \int_1^{n} \frac{1}{x}\,\mathrm{d}x \\ \iff &\ln(n+1) - \ln 1 \leqslant H_n \leqslant 1 + \ln n - \ln 1 \\ \iff &\boxed{\ln(n+1) \leqslant H_n \leqslant 1 + \ln n.} \end{aligned}$$

On ne peut pas appliquer le théorème des gendarmes mais comme $\ln(n+1) \xrightarrow[n\to+\infty]{} +\infty$, on en déduit que $H_n \xrightarrow[n\to+\infty]{} +\infty$ et donc la suite (H_n) diverge.
On en déduit que la série $\sum \frac{1}{k}$ diverge.

Pour montrer que $H_n \sim \ln n$, on ne peut pas le faire *à l'intuition* mais il faut procéder comme il suit :

$$\frac{\ln(n+1)}{\ln n} \leqslant \frac{H_n}{\ln n} \leqslant \frac{1+\ln n}{\ln n} = \frac{1}{\ln n} + 1 \xrightarrow[n\to+\infty]{} 1$$

et

$$\begin{aligned}\frac{\ln(n+1)}{\ln n} &= \frac{\ln\left(n\left(1+\frac{1}{n}\right)\right)}{\ln n}\\ &= \frac{\ln n + \ln\left(1+\frac{1}{n}\right)}{\ln n}\\ &= 1 + \frac{\ln\left(1+\frac{1}{n}\right)}{\ln n}.\end{aligned}$$

Or, d'après le théorème des gendarmes, $\frac{H_n}{\ln n} \xrightarrow[n\to+\infty]{} 1$ et donc

$$\boxed{H_n \sim \ln n.}$$

Par suite, on a

$$\begin{aligned}H_n &= \ln(n) \times (1+\varepsilon_n)\\ &= \ln(n) + \varepsilon_n \ln n\\ &= \ln n + \text{o}(\ln n).\end{aligned}$$

On veut montrer que $H_n - \ln n \xrightarrow[n\to+\infty]{} \gamma$ i.e. $H_n - \ln n = \gamma + \varepsilon_n$ i.e. on veut montrer que

$$H_n = \ln n + \gamma + \varepsilon_n.$$

La forme ci-dessus est plus précise que le résultat que l'on a trouvé précédemment. Pourquoi ? On sait que le reste entre H_n et $\ln n$ est constant et ne tends pas vers $+\infty$ (ce qui n'est pas le case de $\text{o}(\ln n)$).

On étudie la suite $(H_n - \ln n)$ et on montre qu'elle est convergente et que ça limite est γ. On sait déjà que l'on ne peut pas calculer γ numériquement, on utilise un théorème qui assure l'existence de la limite sans le calculer ; dans ce cas ci, on utilise le théorème de la limite monotone.

Soit $u_n = H_n - \ln n$ pour tout $n \in \mathbb{N}^\star$. On calcule $u_{n+1} - u_n$ et on pressent un télescopage :

$$\begin{aligned}u_{n+1} - u_n &= \big[H_{n+1} - \ln(n+1)\big] - \big[H_n - \ln(n)\big]\\ &= [H_{n+1} - H_n] - \big[\ln(n+1) - \ln n\big]\\ &= \frac{1}{n+1} - \big[\ln(n+1) - \ln n\big]\end{aligned}$$

car

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n-1} + \frac{1}{n}$$
$$H_{n+1} = 1 + \frac{1}{2} + \cdots + \frac{1}{n-1} + \frac{1}{n}$$

Calculer le signe de

$$\frac{1}{n+1} - \big[\ln(n+1) - \ln n\big].$$

MÉTHODE 1 Graphiquement : À faire : dessin à faire

MÉTHODE 2 Théorème des accroissements finis :

RAPPEL :
Si f est continue sur $[a,b]$ et dérivable sur $]a,b[$, alors

$$\exists c \in]a,b[,\ f(b) - f(a) = f'(c)\,(b-a).$$

On sait déjà que ln est continue sur $[n, n+1]$, et dérivable sur $]n, n+1[$ d'où, il existe $c \in]n, n+1[$ telle que

$$\ln(n+1) - \ln n = \frac{1}{c}\big((n+1) - n\big).$$

Dans les deux cas, on a montré que la suite $(u_n)_{n\in\mathbb{N}^*}$ est décroissante. Or,

$$\ln(n+1) \leqslant H_n \leqslant 1 + \ln n$$
$$\text{d'où} \quad \ln(n+1) - \ln \leqslant H_n - \ln n$$

et, en passant à la limite, on a $0 \leqslant H_n - \ln n$.

On en déduit que la suite de $(u_n)_{n\in\mathbb{N}^*}$ est décroissante et minorée par 0 donc elle converge et on note γ sa limite.

EXERCICE :

$$\begin{aligned}\ln(n!) &= \ln\big(1 \times 2 \times 3 \times \cdots \times (n-1) \times n\big)\\ &= \cancel{\ln(1)} + \ln(2) + \ln(3) + \cdots + \ln(n-1) + \ln n\end{aligned}$$

Pour calculer cette somme, on utilise la méthode des rectangles. Avec des rectangles à droite on obtient l'inégalité

$$\ln(n!) \leqslant \int_2^{n+1} \ln(x)\ \mathrm{d}x.$$

Avec les rectangles à gauche, on obtient

$$\int_1^n \ln x\ \mathrm{d}x \leqslant \ln(n!).$$

D'où

$$\begin{aligned} &\left[x\ln x - x\right]_1^n \leqslant \ln(n!) \leqslant \left[x\ln x - x\right]_2^{n+1} \\ \iff &\frac{\ln n - n + 1}{n\ln n} \leqslant \frac{\ln(n!)}{n\ln n} \leqslant \frac{(n+1)\ln(n+1) - (n+1) - 2\ln 2 + 2}{n\ln n} \end{aligned}$$

Or, les deux "gendarmes" tendent vers 1, par le théorème des gendarmes, on en déduit que

$$\frac{\ln(n!)}{n\ln n} \xrightarrow[n\to+\infty]{} 1 \quad \text{i.e.} \quad \ln(n!) \sim n\ln n.$$

Proposition : La série $\sum \frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

I.3 Le reste d'une série convergente

$$\sum_{k=0}^{n} u_k = S_n \to \text{ somme partielle } \underbrace{u_0 + u_1 + u_2 + \cdots + u_n}_{} \quad + \quad \underbrace{u_{n+1} + u_{n+2} + \cdots}_{} \quad . \quad \sum_{k=n+1}^{\infty} u_k = R_n \to \text{ reste}$$

Le reste est défini si et seulement si la série $\sum u_n$ converge. La somme $S_n + R_n = \sum_{k=0}^{\infty} u_k$ est définie si et seulement si la série $\sum u_n$ converge. On pose $\mathbb{R} \ni \ell = S_n + R_n$. Ainsi, on a

$$\begin{aligned} S_n &\xrightarrow[n\to+\infty]{} \ell \\ \ell - S_n = R_n &\xrightarrow[n\to+\infty]{} \ell - \ell = 0 \end{aligned}$$

Exercice :
La série $\sum \frac{1}{n^2}$ converge d'après le critère de Riemann. D'où le reste $R_n = \sum_{k=n+1}^{\infty} \frac{1}{k^2}$ est bien défini.

On utilise, encore une fois, la méthode des rectangles : en effet, on a

$$\begin{aligned} &\int_{n+1}^{N+1} \frac{1}{x^2}\,\mathrm{d}x \leqslant \sum_{k=n+1}^{N} \frac{1}{k^2} \leqslant \int_n^N \frac{1}{x^2}\,\mathrm{d}x \\ \iff &\left[-\frac{1}{x}\right]_{n+1}^{N+1} \leqslant \sum_{k=n+1}^{N} \frac{1}{k^2} \leqslant \left[-\frac{1}{x}\right]_n^N \\ \iff &\frac{1}{n+1} - \frac{1}{N+1} \leqslant \sum_{k=n+1}^{N} \frac{1}{k^2} \leqslant \frac{1}{n} - \frac{1}{N}. \end{aligned}$$

On n'a pas besoin du théorème des gendarmes ; on utilise le fait que les inégalités larges "passent à la limite."

$$\begin{array}{ccccc} \frac{1}{n+1}-\frac{1}{N+1} & \leqslant & \sum_{k=n+1}^{N} & \leqslant & \frac{1}{n}-\frac{1}{N} \\ \downarrow_{N\to+\infty} & & \downarrow_{N\to+\infty} & & \downarrow_{N\to+\infty} \\ \frac{1}{n+1} & \leqslant & R_n & \leqslant & \frac{1}{n}. \end{array}$$

I.4 Les séries alternées

Théorème (Séries alternées) **:** La série $\sum(-1)^k u_k$ (où u_k tends vers 0 en décroissant, d'où $u_k \geqslant 0$) converge. Et, ℓ a le même signe que le premier terme.

$$\begin{aligned} S_0 &= u_0 \\ S_1 &= u_0 - u_1 \\ S_2 &= u_0 - u_1 + u_2 \\ &\vdots \quad \vdots \\ S_n &= u_0 - u_1 + \cdots + (-1)^n u_n \end{aligned}$$

À faire : Faire figure (fig. 4)

Figure 1.2 – Série alternée

Le reste $R_n = \ell - S_n$ change de signe une fois sur deux i.e. il est alterné. De plus, on a

$$|R_n| \leqslant u_{n+1}.$$

Exercice (Mines-Ponts) :
On pose, pour tout $n \in \mathbb{N}^\star$,

$$S_n = \sum_{k=0}^{n} \frac{(-1)^{k-1}}{k} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{(-1)^{n-1}}{n}.$$

(Ça ne sert à rien mais…) comme $\frac{1}{k}$ tends vers 0 en décroissant, d'où, d'après le théorème des séries alternées, la suite (S_n) converge.

Montrons que

$$(1) \qquad \ln 2 - S_n = \int_0^1 \frac{(-t)^n}{1+t}\,\mathrm{d}t$$

et (2) en déduire que S_n tends vers $\ln 2$.

1. On remarque que

$$\int_0^1 \frac{1}{1+t}\,\mathrm{d}t = \big[\ln|1+t|\big]_0^1 = \ln 2 \quad \text{et} \quad \frac{1}{k} = \int_0^1 t^{k-1}\,\mathrm{d}t = \left[\frac{t^k}{k}\right]_0^1.$$

D'où,

$$\sum_{k=1}^{n}(-1)^{k-1}\int_0^1 t^{k-1}\,\mathrm{d}t.$$

Or, par linéarité de l'intégrale, on a

$$S_n = \int_0^1 \left(\sum_{k=1}^{n}(-1)^{k-1}t^{k-1}\right)\mathrm{d}t.$$

2.

$$\begin{aligned}
|\ln 2 - S_n| &= \left|\int_0^1 \frac{(-1)^n}{1+t}\,\mathrm{d}t\right| \\
&\leqslant \int_0^1 \left|\frac{(-t)^n}{1+t}\right|\,\mathrm{d}t \\
&\leqslant \int_0^1 t^n\,\mathrm{d}t \\
&= \left[\frac{t^{n+1}}{n+1}\right]_0^1 = \frac{1}{n+1}
\end{aligned}$$

par croissance de l'intégrale. D'où, $|\ln 2 - S_n| \xrightarrow[n\to+\infty]{} 0$ d'après le théorème des gendarmes. On en conclut que

$$\boxed{S_n \xrightarrow[n\to+\infty]{} \ln 2.}$$

Or,

$$\begin{aligned}
\sum_{k=1}^{n}(-t)^{k-1} &= (-t)^0 + (-t)^1 + \cdots + (-t)^{n-1} \\
&= \frac{1-(-t)^n}{1-(-t)}
\end{aligned}$$

car

$$\sum_{k=0}^{N} q^k = q^0 + q^1 + \cdots + q^N = \frac{1-q^{N+1}}{1-q} \quad \text{si} q \neq 1.$$

D'où

$$\begin{aligned} S_n &= \int_0^1 \frac{1-(-t)^n}{1+t}\,\mathrm{d}t \\ &= \int_0^1 \frac{1}{1+t}\,\mathrm{d}t - \int_0^1 \frac{(-t)^n}{1+t}\,\mathrm{d}t \\ &= \boxed{\ln 2 - \int_0^1 \frac{(-t)^n}{1+t}\,\mathrm{d}t.} \end{aligned}$$

On sait que R_n est existe car la suite S_n converge.

La série $\sum R_n$ converge-t-elle ou diverge-t-elle ? On sait que $R_n = (-1)^n\,|R_n|$ au signe près. On veut montrer que $|R_n|$ tend vers 0 en décroissant.

$$\begin{aligned} |R_n| = \int_0^1 \frac{t^n}{1+t}\,\mathrm{d}t &\leqslant \int_0^1 t^n\,\mathrm{d}t \text{ car } \frac{t^n}{1+t} \leqslant t^n \forall t \in [0,1] \\ &\leqslant \left[\frac{t^{n+1}}{n+1}\right]_0^1 = \frac{1}{n+1}. \end{aligned}$$

D'où $|R_n|$ tend vers 0 d'après le théorème des gendarmes.

$$\begin{aligned} |R_{n+1}| - |R_n| &= \int_0^1 \frac{t^{n+1}}{n+1}\,\mathrm{d}t - \int_0^1 \frac{t^n}{1+t}\,\mathrm{d}t \\ &= \int_0^1 \frac{t^{n+1}-t^n}{1+t}\,\mathrm{d}t \\ &= \int_0^1 \frac{(t-1)t^n}{1+t}\,\mathrm{d}t \\ &\leqslant 0 \end{aligned}$$

On aurait aussi très bien pu utiliser le théorème des séries alternées : $|R_n| \leqslant u_{n+1}$.

Cadeau du *06/09/2022* : calculer les trois limites suivantes (avec un développement limité)

1. $\lim\limits_{x\to 0} \dfrac{\sqrt[3]{8+x} - 2\sqrt{1+x}}{x}$ (corrigé) ;
2. $\lim\limits_{x\to 0} \dfrac{\tan x - x}{\sin^3 x}$ (non corrigé) ;
3. $\lim\limits_{x\to 0} \dfrac{\ln(\cos x)}{x^2}$ (corrigé).

La limite $\ln(\cos x)/x^2$ existe-t-elle pour $x \to 0$? Si oui, quelle est sa valeurs.

On utilise un développement limité pour $\ln(\cos x)$ et on obtient $\ln(\cos x) = \ln\left(1 - \frac{x^2}{2} + o(x^2)\right) = -\frac{x^2}{2} + o(x^2)$. Et donc, en divisant ce développement limité par x^2, on obtient

$$\frac{\ln(\cos x)}{x^2} = \frac{-\frac{x^2}{2} + o(x^2)}{x^2} = -\frac{1}{2} + o(1) \xrightarrow[x\to 0]{} -\frac{1}{2}.$$

Même question avec $\left(\sqrt[3]{8+x} - 2\sqrt{1+x}\right)/x$.

On a $\sqrt[3]{8+x} = (8+x)^{1/3} = 2\left(1+\frac{x}{8}\right)^{1/3} = 2 \times (1+u)$ où $u = \frac{x}{8}$ tends vers 0. On en déduit que

$$\begin{cases} \sqrt{1+x} &= 1 + \frac{1}{2}x + o(x) \\ \sqrt[3]{8+x} &= 2 + \frac{2}{3}\frac{x}{8} + o(x). \end{cases}$$

D'où,

$$\sqrt[3]{8+x} - 2\sqrt{1+x} = 2 + \frac{1}{12}x + o(x) - 2 + x + o(x) = -\frac{11}{12} + o(x).$$

On en conclut donc que

$$\frac{\sqrt[3]{8+x-2\sqrt{1+x}}}{x} = -\frac{11}{12} + o(1) \xrightarrow[x\to 0]{} -\frac{11}{12}.$$

Cadeau de plus : $(n-\frac{1}{2})\ln\left(1-\frac{1}{n}\right)+1 \sim_{n\to+\infty}$?

I.5 Le critère de d'Alembert

Théorème (Critère de d'Alembert) **:** Soit $(u_n)_{n\in\mathbb{N}}$ une suite strictement positive telle que

$$\lim_{n\to+\infty} \frac{u_{n+1}}{u_n} = \ell.$$

1. Si $\ell < 1$, alors la série $\sum u_n$ converge.
2. Si $\ell > 1$, alors la série $\sum u_n$ diverge.
3. Si $\ell = 1$, on ne sait pas (BOF).

Preuve :
On suppose $u_n > 0$ et $\frac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} \ell < 1$. u_{n+1}/u_n tends vers un réel ℓ inférieur à 1 d'où, il existe un certain λ inférieur à 1 tel qu'à partir d'un certain rang n_0

$$\frac{u_{n+1}}{u_n} \leqslant \lambda.$$

Soit $n \geqslant n_0$. On a

$$u_n = \overbrace{\frac{u_n}{\cancel{u_{n-1}}}}^{\leqslant\lambda} \times \underbrace{\frac{\cancel{u_{n-1}}}{\cancel{u_{n-2}}}}_{\leqslant\lambda} \times \cdots \times \overbrace{\frac{u_{n_0+1}}{\cancel{u_{n_0}}}}^{\leqslant\lambda} \times u_{n_0}.$$

D'où, $u_n \leqslant \lambda^{n-n_0} \times u_{n_0}$ i.e.

$$u_n \leqslant \lambda^n \times \underbrace{\boxed{\frac{u_{n_0}}{\lambda^{n_0}}}}_{=\text{const}} \quad \text{donc} \quad 0 < u_n \leqslant \text{const} \times \lambda^n.$$

Or, $\sum \text{const} \times \lambda^n = \text{const} \times \sum \lambda^n$ la série de droite est une série géométrique de raison $\lambda < 1$.

Rappel (séries géométriques) :

$$\underbrace{\lambda^0 + \lambda^1 + \cdots + \lambda^n}_{=S_n} = \frac{1-\lambda^{n+1}}{1-\lambda} \text{ si } \lambda \neq 1$$
$$\xrightarrow[n\to+\infty]{} \frac{1}{1-\lambda}.$$

Fin du Rappel.

Or, $\sum \lambda^n$ converge car $\lambda < 1$ et donc $\sum u_n$ converge. □

Remarque :

Exercice :
La série $\sum a^n/n$ converge-t-elle ?

Comme on n'a pas d'information sur le signe de a, on s'interesse à la convergence de la série $\sum |a^n/n|$. Or, $|a^n/n| = |a|^n/n$. On étudie plusieurs cas.

- Si $|a| < 1$, alors $|a|^n/n \leqslant |a|^n$ et, comme $\sum |a|^n$ converge (série géométrique), la série $|a|^n/n$ converge et donc a^n/n également.
- Si $|a| = 1$, alors
  - si $a = 1$, alors la série $\sum \frac{1}{n}$ converge.
  - si $a = -1$, alors série $\sum (-1)^n/n$ converge.
- Si $|a| > 1$, alors $|a|^n \xrightarrow[n\to+\infty]{\not\longrightarrow} 0$ car

$$\left.\begin{array}{l} |a|^n = \mathrm{e}^{n\ln|a|} \\ n = \mathrm{e}^{\ln n} \end{array}\right\} \implies \frac{|a|^n}{n} = \frac{\mathrm{e}^{n\ln|a|}}{\mathrm{e}^{\ln n}} = \mathrm{e}^{n\ln|a| - \ln n} \text{ or } n\ln|a| - \ln n \xrightarrow[n\to+\infty]{} +\infty.$$

D'où, $a^n/n \xrightarrow[n\to\infty]{\not\longrightarrow} 0$ donc $\sum a^n/n$ diverge.

La série $\sum a^n/n!$ converge-t-elle ?

Comme pour la 1ère série, on n'a pas d'information sur le signe de a, on utilise des valeurs absolue : soit $u_n = |a|^n/n!$. On utilise le critère d'ALEMBERT :

$$\frac{u_{n+1}}{u_n} = \frac{\frac{|a|^{n+1}}{(n+1)!}}{\frac{|a|^n}{n!}} = \frac{|a|^{n+1}}{|a|^n} \times \frac{n!}{(n+1)!} \xrightarrow[n\to+\infty]{} 0 = \ell < 1.$$

D'où, $\sum |a|^n/n!$ converge et donc

$$\boxed{\sum \frac{a^n}{n!} \text{ converge } \forall a \in \mathbb{R}}.$$

On remarque que $\displaystyle\sum_{n=0}^{\infty} \frac{a^n}{n!} = \mathrm{e}^a$ d'où $\displaystyle\sum_{n=0}^{\infty} \frac{1}{n!} = \mathrm{e}$.

I.6 SOMMER LES $\sim$, $\wr$, $\mathcal{O}$

Lemme :
1. Si $\sum v_n$ converge et $u_n \sim v_n$, alors le reste $\sum_{k=n+1}^{\infty} v_k$ de $\sum v_n$ existe et il est équivalent au reste de $\sum u_n$.
2. Si $\sum v_n$ diverge et si $u_n \sim v_n$, alors le reste de $\sum v_n$ n'existe pas mais on peut utiliser la somme partielle et elle est équivalente à celle de $\sum u_n$.

Le LEMME ci-dessus est également vrai en remplaçant $\sim$ par $\wr$ ou $\mathcal{O}$.

Théorème :

EXERCICE : 1. On sait que $u_n \sim v_n$ car

$$v_n = \frac{\cancel{n} - (\cancel{n}-1)}{n(n-1)} = \frac{1}{n(n-1)} \sim \frac{1}{n^2}$$

OU

$$v_n = \frac{1}{n} \times \left(\frac{1}{1-\frac{1}{n}} - 1\right) = \frac{1}{n} \times \left(1 + \frac{1}{n} + \wr\left(\frac{1}{n}\right) - 1\right) = \frac{1}{n^2} + \wr\left(\frac{1}{n^2}\right) \sim \frac{1}{n^2}.$$

D'où, $\sum u_n$ et $\sum v_n$ ont la même nature, et comme $\sum u_n$ converge, alors $\sum v_n$ converge.

Soient $U_n = \sum_{k=n+1}^{\infty} u_k$ et $V_n = \sum_{k=n+1}^{\infty} v_k$. D'après le THÉORÈME 14, on a $U_n \sim V_n$. On peut calculer V_n (somme télescopique) :

$$\sum_{k=n+1}^{N} \left(\frac{1}{k-1} - \frac{1}{k}\right) = \frac{1}{n} - \cancel{\frac{1}{n+1}} + \cancel{\frac{1}{n+1}} - \cancel{\frac{1}{n+2}} + \cdots + \cancel{\frac{1}{N-1}} - \frac{1}{N}$$
$$= \frac{1}{n} - \frac{1}{N}$$

Or, quand $N \to \infty$, on a $V_n = \sum_{k=n+1}^{\infty} = \frac{1}{n}$. D'où, $U_n \sim \frac{1}{n}$.

2. On a $u_n = \frac{1}{n}$ et $v_n = \ln n - \ln(n-1)$. On sait que $u_n \sim v_n$ car … D'où les séries $\sum u_n$ et $\sum v_n$ ont la même nature. Or, $\sum \frac{1}{n}$ diverge [1] donc les deux séries divergent. Soient $U_n = \sum_{k=2}^{n} \frac{1}{k}$ et $V_n = \sum_{k=2}^{n} \big(\ln k - \ln(k-1)\big)$. Grace au THÉORÈME 14, on a $U_n \sim V_n$. On peut calculer V_n (somme télescopique) :

$$\begin{aligned} V_n &= \sum_{k=2}^{n} \big(\ln k - \ln(k-1)\big) \\ &= \cancel{\ln 2} - \ln 1 + \cancel{\ln 3} - \cancel{\ln 2} + \cdots + \ln n - \cancel{\ln(n-1)} \\ &= \ln n - \ln 1 \\ &= \ln n. \end{aligned}$$

Cadeau du *07/09/2022* : $\lim\limits_{x\to 0} \dfrac{\tan x - x}{\sin^3 x}$?

Comme $\sin x \sim_{x\to 0} x$, $\sin^3 x \sim_{x\to 0} x^3$. Le développement limité de $\tan x$ n'est pas au programme, il faudra donc normalement le redémontrer au besoin. On a $\tan x = (\sin x)/(\cos x)$. Or, comme $\sin x = x - \frac{x^3}{3!} + \cdots$ et $\cos x = 1 - \frac{x^2}{2!} + \cdots$, on a donc

$$\begin{aligned} \tan x = \frac{\sin x}{\cos x} &= \frac{x - \dfrac{x^3}{6} + o(x^3)}{1 - \dfrac{x^2}{2} + o(x^3)} \\ &= \left(x - \frac{x^3}{6} + o(x^3)\right)\left(1 + \frac{x^2}{2} + o(x^3)\right) \\ &= x + \frac{x^3}{3} + o(x^3) \end{aligned}$$

On en déduit que

$$\frac{\tan x - x}{\sin^3 x} = \frac{\dfrac{x^3}{3} + o(x^3)}{x^3 + o(x^3)} = \frac{1}{3} + o(1) \xrightarrow[x\to 0]{} \frac{1}{3}.$$

On cherche un équivalent pour $n \to \infty$ de

$$\left(n - \frac{1}{2}\right)\ln\left(1 - \frac{1}{n}\right) + 1.$$

1. On peut calculer, comme fait après, une expression de V_n, et en déduire que, comme elle diverge, $\sum \frac{1}{n}$ diverge également.

On cherche un développement limité de $\ln\left(1-\frac{1}{n}\right)$ à l'aide de celui de $\ln(1-x)$: $\ln(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} + \cdots$ et donc

$$\ln\left(1-\frac{1}{n}\right) = -\frac{1}{n} - \frac{1}{2n^2} - \frac{1}{3n^3}\cdots.$$

D'où,

$$\begin{aligned}\left(n-\frac{1}{2}\right)\ln\left(1-\frac{1}{n}\right)+1 &= \left(n-\frac{1}{2}\right)\left(-\frac{1}{n}-\frac{1}{2n^2}-\frac{1}{3n^3}+\cdots\right)+1\\ &= -1+0-\frac{1}{12n^2}+\mathop{\wp}\left(\frac{1}{n^2}\right)+1\\ &= -\frac{1}{12n^2}+\mathop{\wp}\left(\frac{1}{n^2}\right)\\ &\underset{n\to\infty}{\sim} -\frac{1}{12n^2}.\end{aligned}$$

I.7 Développements asymptotiques

On cherche un développement asymptotique de la série harmonique (H_n). Cette méthode pourra être utilisée dans le **DM$_1$**. Les formules à démontrer sont

$$\begin{aligned}H_n &= \ln n + \mathop{\wp}(\ln n) && (1.1)\\ &= \ln n + \gamma + \mathop{\wp}(1) && (1.2)\\ &= \ln n + \gamma + \frac{1}{2n} + \mathop{\wp}\left(\frac{1}{n}\right) && (1.3)\\ &= \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \mathop{\wp}\left(\frac{1}{n^2}\right). && (1.4)\end{aligned}$$

Le développement (1) a déjà été fait de deux méthodes différentes dans les Exercices 4 et 15. Le développement (2) a déjà été fait une fois dans l'Exercice 4, mais nous allons utiliser une autre méthode :

$$\begin{aligned}(2) &\iff H_n - \ln n = \gamma + \mathop{\wp}(1)\\ &\iff \text{la suite } (H_n - \ln n) \text{ converge.}\end{aligned}$$

Le " $\Longrightarrow$ " et " $\Longleftrightarrow$ " ne peut pas remplacer les mots français : on ne peut pas écrire

$$\text{"d'où } \frac{u_n}{v_n} \longrightarrow 1 \iff u_n \sim v_n\text{"}$$

mais on doit écrire

$$\text{"d'où } \frac{u_n}{v_n} \longrightarrow 1 \text{ donc } u_n \sim v_n\text{".}$$

On va montrer que $(H_n - \ln n)$ converge. On nomme cette suite $(u_n)_{n\in\mathbb{N}}$.

Remarque (Séries télescopiques) : ($\star$) On sait que

$$(\cancel{u_1} - u_0) + (\cancel{u_2} - \cancel{u_1}) + \cdots + (u_n - \cancel{u_{n-1}}) = u_n - u_0.$$

Autrement dit,

$$\sum_{k=1}^{n} (u_k - u_{k-1}) = u_n - u_0.$$

($\star\star$) On sait que

$$\sum_{k=n+1}^{N} (u_k - u_{k-1}) = (\cancel{u_{n+1}} - u_n) + (\cancel{u_{n+2}} - \cancel{u_{n+1}}) + \cdots + (u_N - \cancel{u_{N-1}}) = u_N - u_n.$$

Or, si u_N tends vers 0 quand $N \to \infty$, alors, en passant à la limite,

$$\sum_{k=n+1}^{\infty} (u_k - u_{k-1}) = -u_n.$$

Fin de la Remarque.

On a

$$\begin{aligned}
u_n - u_{n-1} &= (H_n - \ln n) - \big(H_{n-1} - \ln(n-1)\big) \\
&= (H_n - H_{n-1}) - \big(\ln n - \ln(n-1)\big) \\
&= \frac{1}{n} - \ln \frac{n}{n-1} \\
&= \frac{1}{n} + \ln \frac{n-1}{n} \\
&= \frac{1}{n} + \ln\left(1 - \frac{1}{n}\right) \\
&= \frac{1}{n} - \frac{1}{n} - \frac{1}{2n^2} + \mathcal{o}\left(\frac{1}{n^2}\right) \\
&= -\frac{1}{2n^2} + \mathcal{o}\left(\frac{1}{n^2}\right). \\
&\sim -\frac{1}{2n^2}.
\end{aligned}$$

Or, $\sum \frac{-1}{2n^2} = -\frac{1}{2} \sum \frac{1}{n^2}$ qui est une suite convergente. La série $\sum(u_n - u_{n-1})$ converge donc. Donc, d'après le Théorème 14, les restes des séries $\sum \frac{-1}{2n^2}$ et $\sum(u_n - u_{n-1})$ sont équivalents.

$$\sum_{k=n+1}^{\infty} (u_k - u_{k-1}) = -u_n \qquad \text{car la suite tend vers } 0$$

$$\sum_{k=n+1}^{\infty} \frac{-1}{2k^2} = -\frac{1}{2} \sum_{k=n+1}^{\infty} \frac{1}{k^2}$$

et, en comparant la série $\sum \frac{1}{n^2}$ et l'intégrale $\int \frac{1}{x^2}\,\mathrm{d}x$, on montre que $\sum_{k=n+1}^{\infty} \frac{1}{k^2} \sim_{n\to\infty} \frac{1}{n}$ (c.f. Exercice 7). On en déduit que

$$\sum_{k=n+1}^{\infty} -\frac{1}{2k^2} \sim -\frac{1}{2n} \qquad \text{et donc } u_n \sim \frac{1}{2n}.$$

Cadeau du *08/09/2022* :

$$\int \cos x \ln(1+\cos x)\,\mathrm{d}x \quad \text{(IPP)} \qquad \int \operatorname{Arctan} x\,\mathrm{d}x \quad \text{(IPP puis CDV)}$$

$$\int \operatorname{Arcsin} x\,\mathrm{d}x \quad \text{(IPP puis CDV)} \qquad \int \frac{1-2x}{1+x^2}\,\mathrm{d}x$$

Le développement limité de Arctan est à connaître : pour le retrouver, on peut utiliser le développement de $1/(1+x^2)$ et en primitivant :

$$\frac{1}{1+x^2} = 1-x^2+x^4-x^6+\cdots \qquad \xrightarrow{\int \cdot \mathrm{d}x} \qquad \operatorname{Arctan} x = x-\frac{x^3}{3}+\frac{x^5}{5}-\frac{x^7}{7}+\cdots .$$

Proposition (Stirling) **:**

$$n! \underset{n\to+\infty}{\sim} \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

Exercice :
L'expérience aléatoire est "on lance $2n$ fois une pièce" et l'évènement nommé A est "on obtient autant de **P** que de **F**." Un résultat est une $2n$-liste de **P** et de **F**. (Ce n'est pas un ensemble : l'ordre dans une liste compte.) Autrement dit, un résultat est un élément de $\{\mathbf{P},\mathbf{F}\}^{2n}$. Par exemple

$$(\underbrace{\mathbf{P},\mathbf{F},\mathbf{F},\ldots,\mathbf{P},\mathbf{F}}_{2n}) \in \{\mathbf{P},\mathbf{F}\}^{2n}$$

est un résultat possible. L'ensemble des résultats possibles est nommé "univers Ω." Dans cet exemple-ci, tous les résultats sont équiprobables. L'énoncé de l'exercice est alors de déterminer $u_n = P(A)$:

$$u_n = P(A) = \frac{\#\text{ résultats favorables à } A}{\#\text{ résultats possibles}} = \frac{\operatorname{Card}(A)}{\operatorname{Card}(\Omega)}.$$

On cherche la limite de la suite $(u_n)_{n\in\mathbb{N}}$ quand n tends vers $+\infty$. Construire un résultat de Ω, c'est choisir **P** ou **F** $2n$ fois, il y a 2^{2n} manières. On en déduit que $\operatorname{Card}(\Omega) = 2^{2n} = 4^n$. Construire un résultat de A, c'est : (1) choisir les n places prises par les **P** dans la $2n$-liste ; (2) y placer les n **P** puis ailleurs les n **F**. Pour le (1), il y a $\binom{2n}{n}$ manières ; pour le (2), il y a une seule manière. On conclut que

$$\operatorname{Card}(A) = \binom{2n}{n} \times 1 = \frac{(2n)!}{n!\,(2n-n)!} = \frac{(2n)!}{(n!)^2}.$$

Par équiprobabilité, la probabilité u_n de l'évènement A est

$$u_n = \frac{(2n)!/(n!)^2}{2^{2n}}.$$

D'après la formule de Stirling, on a $n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$. D'où,

$$\begin{cases} (n!)^2 \sim \left(\frac{n}{e}\right)^{2n} 2\pi\, n \\ (2n)! \sim \left(\frac{2n}{e}\right)^{2n} \sqrt{2\pi \times 2n}. \end{cases}$$

$$u_n \sim \frac{\cancel{2^{2n}}\cancel{\left(\frac{n}{e}\right)^{2n}}\sqrt{4\pi\, n}}{\cancel{2^{2n}}\cancel{\left(\frac{n}{e}\right)^{2n}} 2\pi n} \underset{n\to+\infty}{\sim} \frac{1}{\sqrt{\pi n}}.$$

Chapitre 2

Algèbre linéaire

Rappel :
La *dimension* d'un espace vectoriel est le nombre de vecteurs dans une base de cet espace vectoriel.

Soit E un espace vectoriel de dimension finie, n. On a

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \\ \vec{\varepsilon}_1 & \vec{\varepsilon}_2 & \cdots & \vec{\varepsilon}_n \end{pmatrix} \begin{matrix} \vec{e}_1 \\ \vec{e}_2 \\ \vdots \\ \vec{e}_n \end{matrix}.$$

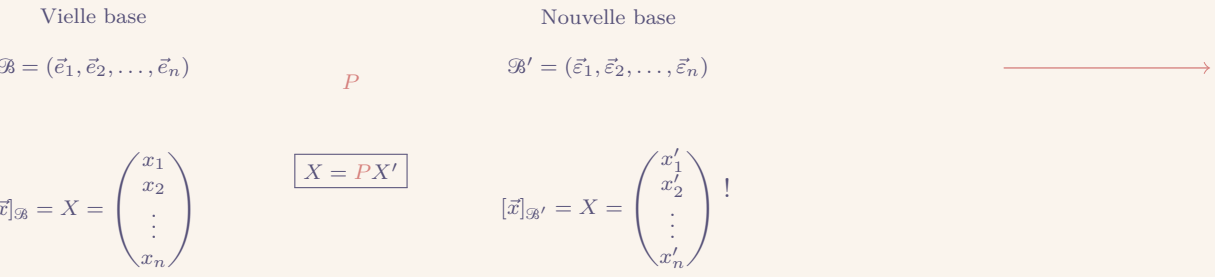


Figure 2.1 – Formule de passage (vecteurs)

On considère maintenant un endomorphisme f.

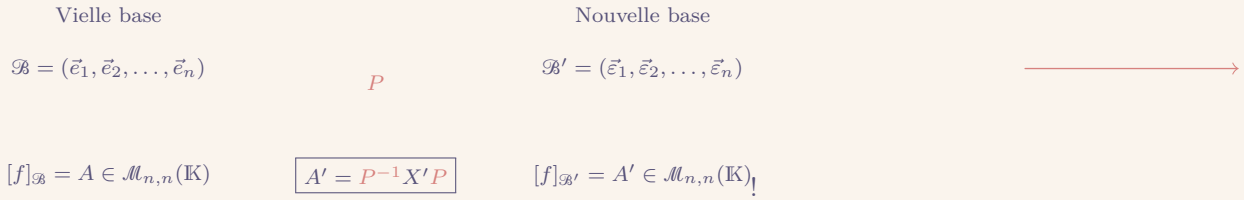


FIGURE 2.2 – Formule de passage (endomorphismes)

On a

$$A = [f]_{\mathscr{B}} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \\ f(\vec{e}_1) & f(\vec{e}_2) & \ldots & f(\vec{e}_n) \end{pmatrix} \begin{matrix} \vec{e}_1 \\ \vec{e}_2 \\ \vdots \\ \vec{e}_n \end{matrix}.$$

EXERCICE :
On doit montrer qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ telle que $A' = P^{-1} \cdot A \cdot P$. On appelle la vielle base $\mathscr{B} = (\vec{\imath}, \vec{\jmath})$ et la nouvelle $\mathscr{B}' = (\vec{\varepsilon}_1, \vec{\varepsilon}_2)$. On a

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \\ f(\vec{\imath}) & f(\vec{\imath}) \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \end{matrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ f(\vec{\varepsilon}_1) & f(\vec{\varepsilon}_2) \end{pmatrix} \begin{matrix} \vec{\varepsilon}_1 \\ \vec{\varepsilon}_2 \end{matrix}$$

La question devient donc de trouver $\vec{\varepsilon}_1$ et $\vec{\varepsilon}_2$.

On a $f(\vec{\varepsilon}_1) = \vec{\varepsilon}_1$ et $f(\vec{\varepsilon}_2) = \vec{\varepsilon}_2$. L'endomorphisme f est la symétrie par rapport à $\mathrm{Vect}(\vec{\varepsilon}_1)$ où $\vec{\varepsilon}_1 = \binom{\cos\theta/2}{\sin\theta/2}$. On représente la situation dans la FIGURE ci-dessous.

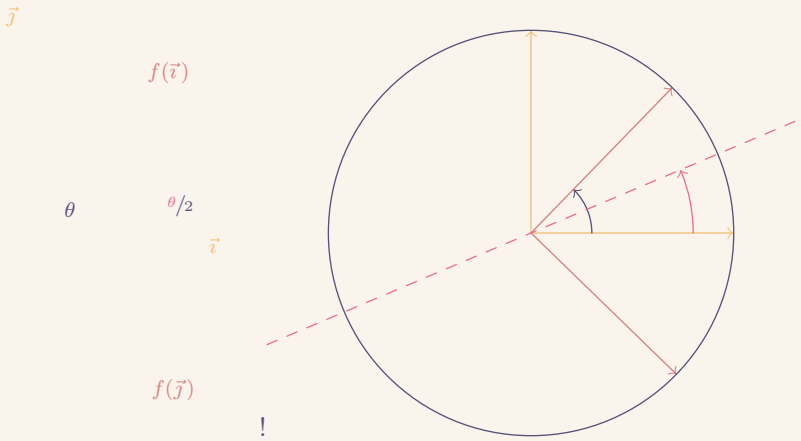


FIGURE 2.3 – Schéma représentant l'EXERCICE 1

On en déduit la matrice P :

$$P = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}.$$

Cette matrice n'est, par contre, pas unique : elle peut être multipliée par un réel non nul sur chacune des colonnes et répondre quand même au problème. Par exemple,

$$\begin{pmatrix} 8\cos\frac{\theta}{2} & -3\sin\frac{\theta}{2} \\ 8\sin\frac{\theta}{2} & 3\cos\frac{\theta}{2} \end{pmatrix}$$

est aussi une matrice valide.

Autre méthode. On "sort les expressions des vecteurs d'un chapeau" : soient $\vec{\varepsilon}_1 = \begin{pmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{pmatrix}$ et $\vec{\varepsilon}_2 = \begin{pmatrix}-\sin(\theta/2)\\ \cos(\theta/2)\end{pmatrix}$. Alors,

$$\begin{aligned} A\begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix} &= \begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix} \\ &= \begin{pmatrix}\cos\theta\,\cos\frac{\theta}{2} + \sin\theta\,\sin\frac{\theta}{2}\\ \sin\theta\cos\frac{\theta}{2} - \cos\theta\,\sin\frac{\theta}{2}\end{pmatrix} \\ &= \begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix} \end{aligned}$$

D'où, $f(\vec{\varepsilon}_1) = \vec{\varepsilon}_1$. De la même manière, on vérifie $f(\vec{\varepsilon}_2) = -\vec{\varepsilon}_2$.

Avant de quitter l'EXERCICE 1 : on vérifie que la matrice P est inversible. On rappelle qu'une matrice est inversible si et seulement si $\det(P) \neq 0$, si et seulement si les colonnes de P forment une base (ou les lignes), si et seulement si le rang de P est le même que la taille de P.

La trace est une opération linéaire : $\operatorname{tr}(\alpha A + \beta B) = \alpha \operatorname{tr} A + \beta \operatorname{tr} B$. Attention, ce n'est pas vrai pour le déterminent : $\det(\alpha A) = \alpha^n \det A \neq \alpha \det A$ où n est la taille de A. Il est cependant linéaire par rapport à chacune de ses colonnes.

$$\operatorname{tr}(AB) = \operatorname{tr}(BA) \neq \operatorname{tr} A \times \operatorname{tr} B \qquad \text{mais} \qquad \det(AB = \det(BA) = \det A \times \det B.$$

Le trace et le déterminant sont invariants par changement de base (par des opérations sur les lignes et les colonnes) : on dit que ces opérations sont invariantes par similitude.

Le noyau de f, noté $\operatorname{Ker} f$ est l'ensemble des x pour lesquels $f(x) = 0_F$. L'image de f, noté $\mathfrak{Im} f$ est l'ensemble des $f(x)$ pour x dans E.

On a

$$\operatorname{Ker} f = \{0_E\} \iff f \text{ injective} \qquad \text{et} \qquad \mathfrak{Im} f = F \iff f \text{ surjective.}$$

On rappelle le théorème du rang :

$$\boxed{\dim E = \dim \operatorname{Ker}(f) + \dim \mathfrak{Im}(f) = \dim \operatorname{Ker}(f) + \operatorname{rg}(f).}$$

Dans le cas particulier où $\dim E = \dim F$, on a

$$\boxed{f \text{ injective} \iff f \text{ surjective} \iff f \text{ bijective.}}$$

Exercice :
Soit E un $\mathbb{K}$-espace vectoriel et soit

$$\begin{aligned} u : E &\overset{\text{linéaire}}{\longrightarrow} E \\ \vec{x} &\longmapsto u(\vec{x}). \end{aligned}$$

On considère S un supplémentaire de $\operatorname{Ker} u$: $\operatorname{Ker} u \oplus S = E$. Ce supplémentaire existe d'après le théorème de la base incomplète. On montre que S est isomorphe à $\mathfrak{Im} u$. On pose

$$\begin{aligned} f : S &\longrightarrow \mathfrak{Im} u \\ \vec{x} &\longmapsto u(\vec{x}) \end{aligned}$$

On montre aisément que f est linéaire car u est, elle-même, linéaire.

Soit $\vec{x} \in S$.

$$\begin{aligned} \vec{x} \in \operatorname{Ker} f &\iff f(\vec{x}) = \vec{0} = u(\vec{x}) \\ &\iff \vec{x} \in \operatorname{Ker}(u) \cap S \\ &\iff \vec{x} = \vec{0} \end{aligned}$$

Donc f est injective.

Soit $\vec{y} \in \mathfrak{Im} u$. Soit $\vec{x} \in E$ tel que $u(\vec{x}) = \vec{y}$. Soient $\vec{a} \in S$ et $\vec{b} \in \operatorname{Ker} u$ tels que $\vec{x} = \vec{a} + \vec{b}$. On a $u(\vec{x}) = u(\vec{a}) = f(\vec{a}) = y$. On en déduit que f est surjective.

On en déduit donc que $\dim(\operatorname{Ker} u) + \dim(\mathfrak{Im} u) = \dim E$: le théorème du rang.

Exercice :
Une forme linéaire φ est une application linéaire d'un $\mathbb{K}$-espace vectoriel dans $\mathbb{K}$.

1. Montrons que φ est, ou bien nulle, ou bien surjective. On vérifie aisément le cas où φ est nulle. Si φ n'est pas nulle, il existe $\vec{x} \in E$ tel que $\varphi(\vec{x}) \neq 0_{\mathbb{K}}$. Alors, on sait que $\varphi(\vec{x}/\varphi(x)) = 1$ par linéarité. Donc, pour tout $\lambda \in \mathbb{K}$, on peut trouver un antécédent $\vec{y} = \frac{\lambda}{\varphi(\vec{x})}\vec{x}$ de λ : $\varphi(\vec{y}) = \lambda$.

   On rappelle également que le noyau d'une forme linéaire non nulle est un *hyperplan* (la dimension vue l'année dernière d'un hyperplan comme un sous-espace vectoriel de dimension $n-1$ n'est pas valable en dimension finie ; cette nouvelle définition est valable en dimension infinie). C'est ce que nous allons montrer dans les deux prochaines questions.
2. Soit H un hyperplan. On sait donc que $H = \operatorname{Ker} \varphi$ où φ est une forme linéaire non nulle (par définition). Ainsi, d'après le théorème du rang, $\dim E = \dim \operatorname{Ker}(\varphi) + \dim \mathfrak{Im}(\varphi)$. Ainsi, d'après la question 1., comme φ est non nulle, elle est surjective et donc $\dim \mathfrak{Im}(\varphi) = 1$. On en conclut que

   $$\dim E = \dim H + 1 \qquad \text{i.e.} \qquad \dim H = n - 1.$$

3. Réciproquement, on suppose $\dim H = n - 1$. Montrons que H est un hyperplan i.e. montrons qu'il existe une forme linéaire φ telle que $H = \operatorname{Ker} \varphi$. Je choisi une base $(\vec{\varepsilon}_1, \vec{\varepsilon}_2, \ldots, \vec{\varepsilon}_{n-1})$ de H. Par le théorème de la

base incomplète, soit $\vec{\varepsilon}_n$ tel que $(\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_n)$ soit une base de E. Soit φ une application linéaire de E dans $\mathbb{K}$ définie comme

$$\begin{array}{rccc} \varphi : & E & \longrightarrow & \mathbb{K} \\ & \vec{x} = x_1\vec{\varepsilon}_1 + x_2\vec{\varepsilon}_2 + \cdots + x_{n-1}\vec{\varepsilon}_{n-1} + x_{n-1}\vec{\varepsilon}_n & \longmapsto & x_n. \end{array}$$

φ n'est pas nulle car $\varphi(\vec{\varepsilon}_n) = 1 \neq 0$. On a donc $\operatorname{Ker}\varphi = H$.

4. L'application tr est une forme linéaire de $\mathscr{M}_{nn}(\mathbb{K})$ dans $\mathbb{K}$. Soit $M \in \mathscr{M}_{nn}(\mathbb{K})$. On pose

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

On sait que $M \in \operatorname{Ker}\varphi$ si et seulement si $a_{11} + a_{22} + \cdots + a_{nn} = 0$ i.e. $a_{nn} = -a_{11} - a_{22} - \cdots - a_{n-1,n-1}$. Il y a donc $n-1$ contraintes (i.e. coordonnées). Ainsi,

$$M \in \operatorname{Ker}\operatorname{tr} \iff M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1,n-1} & a_{1,n} \\ a_{21} & a_{22} & \dots & a_{2,n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{n-1,n-1} & k \end{pmatrix}$$

où $k = -a_{11} - a_{22} - \cdots - a_{n-1,n-1}$. D'où,

$$M \in \operatorname{Ker}\varphi \iff M = a_{11}\begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & \ddots & & \\ & & & 0 & \\ & & & & -1 \end{pmatrix} + a_{22}\begin{pmatrix} 0 & & & & & & \\ & 1 & & & & & \\ & & 0 & & & & \\ & & & \ddots & & & \\ & & & & 0 & & \\ & & & & & -1 & \\ & & & & & & 0 \end{pmatrix} + \cdots.$$

Donc, ces $n^2 - 1$ matrices forment une base de $\operatorname{Ker}\operatorname{tr}$.

Exercice :
Soit $(F_i)_{i\in I}$ une famille de sous-espaces vectoriels d'un espace vectoriel E.

1. On veut montrer que $\bigcap_{i\in I} F_i$ est aussi un sous-espace vectoriel. On sait que $\forall i \in I, 0_E \in F_i$ car F_i est un sous-espace vectoriel de E. Montrons que $\bigcap_{i\in I} F_i$ est stable par combinaisons linéaires (i.e. superpositions). Soient $\alpha, \beta \in \mathbb{K}$ et $\vec{x}, \vec{y} \in \bigcap_{i\in I} F_i$. On veut montrer que $\alpha\vec{x} + \beta\vec{y} \in \bigcap_{i\in I} F_i$. Pour tout $i \in I$, F_i est stable par combinaisons linéaires d'où $\alpha\vec{x} + \beta\vec{y} \in F_i$. Donc, comme ceci est vrai pour tout i, on en déduit que $\alpha\vec{x}+\beta\vec{y} \in \bigcap_{i\in I} F_i$.
2. On donne un contre-exemple. On se place dans le cas $E = \mathbb{R}^2$. On pose $G = \operatorname{Vect}(\vec{\jmath})$ et $H = \operatorname{Vect}(\vec{\imath})$. On a $\vec{\imath}+\vec{\jmath} \notin F \cup G$ car $\vec{\imath}+\vec{\jmath} \notin F$ et $\vec{\imath}+\vec{\jmath} \notin G$.

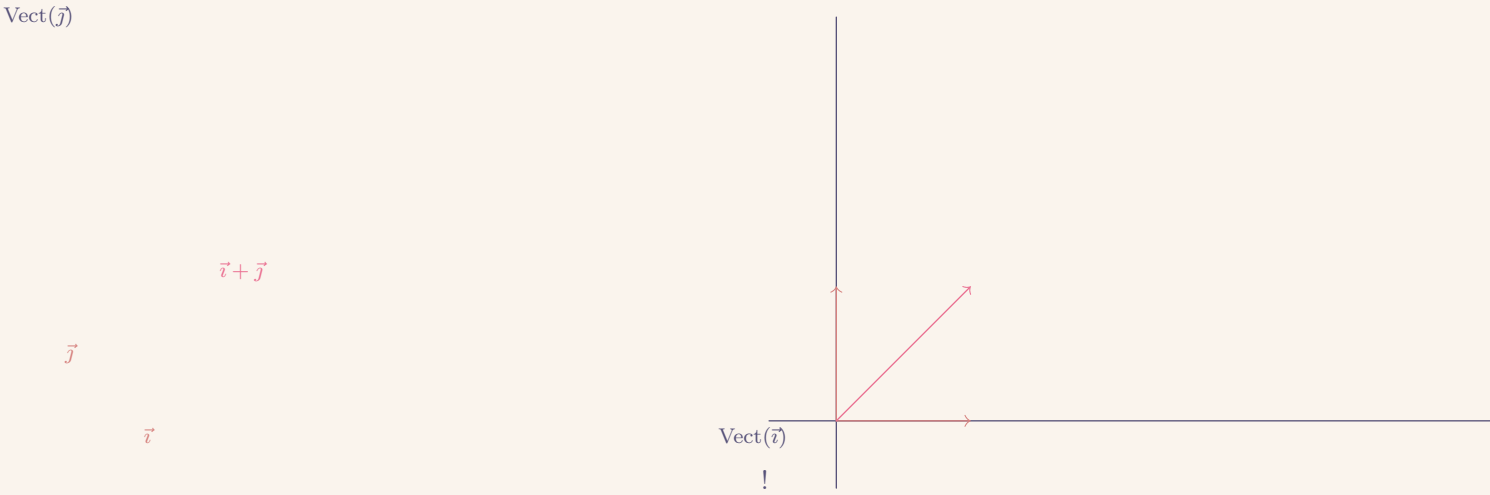


FIGURE 2.4 – Contre-exemple : union de sous-espaces vectoriels n'en est pas un

3. (a) On montre d'abord que si $F \subset G$ ou $G \subset F$, alors $F \cup G$ est un sous-espace vectoriel de E. Si $F \subset G$, alors $F \cup G = G$ qui est un sous-espace vectoriel de E. Si $G \subset F$, alors $F \cup G = F$ qui est un sous-espace vectoriel de E.

   (b) On montre que si $F \not\subset G$ et $G \not\subset F$, alors $F \cup G$ n'est pas un sous-espace vectoriel. On sait donc, par hypothèse, qu'il existe $\vec{g} \in G$ tel que $\vec{g} \notin F$; et, qu'il existe $\vec{f} \in F$ tel que $\vec{f} \notin G$. Or, $\vec{f}+\vec{g} \notin F$ et $\vec{f}+\vec{g} \notin G$ et donc $\vec{f}+\vec{g} \notin F \cup G$. On en déduit que $F \cup G$ n'est pas stable par combinaisons linéaires.

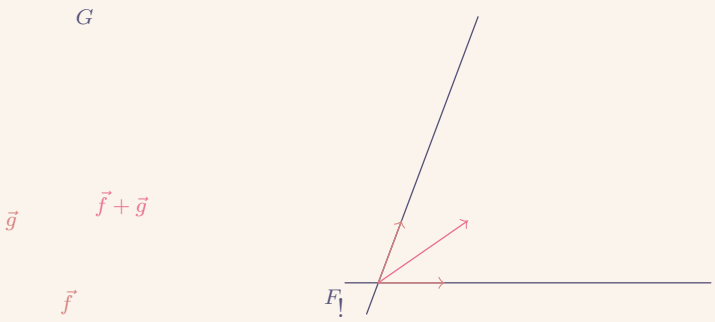


FIGURE 2.5 – L'union de deux sous-espaces vectoriels non inclus n'est pas un sous-espace vectoriel

4. On le fait dans le cas où $r = 2$. On peut ensuite procéder à une récurrence pour le faire pour tout r. Soient F_1 et F_2 deux sous-espaces vectoriels de dimensions finies respectivement d_1 et d_2. Soient $\vec{x}_1 \in F_1$ et $\vec{x}_2 \in F_2$. On sait que $\alpha(\vec{x}_1, \vec{x}_2) + \beta(\vec{y}_1, \vec{y}_2) = (\alpha\vec{x}_1 + \beta\vec{y}_1, \alpha\vec{x}_2 + \beta\vec{y}_2)$. Montrons que $\dim(F_1 \times F_2) = d_1 + d_2 = \dim F_1 + \dim F_2$. Soit $(\vec{e}_1, \ldots, \vec{e}_{d_1})$ une base de

F_1 et $(\vec{f_1}, \dots, \vec{f_{d_2}})$ une base de F_2. On décompose $\vec{x}_1$ et $\vec{x}_2$ dans ces bases :

$$F_1 \ni \vec{x}_1 = \alpha_1\vec{e}_1 + \alpha_2\vec{e}_2 + \cdots + \alpha_{d_1}\vec{e}_{d_1}$$
$$\text{et}$$
$$F_2 \ni \vec{x}_2 = \beta_1\vec{f_1} + \beta_2\vec{f_2} + \cdots + \beta_{d_2}\vec{f}_{d_2}.$$

Ainsi,

$$\begin{aligned} F_1 \times F_2 \ni (\vec{x}_1, \vec{x}_2) &= (\alpha_1\vec{e}_1 + \alpha_2\vec{e}_2 + \cdots, \beta_1\vec{f_1} + \beta_2\vec{f_2} + \cdots) \\ &= \alpha_1(\vec{e}_1, \vec{0}) + \alpha_2(\vec{e}_2, \vec{0}) + \cdots + \beta_1(\vec{0}, \vec{f_1}) + \beta_2(\vec{0}, \vec{f_2}) + \cdots . \end{aligned}$$

Rappel :
Comment montrer que $x \in \bigcap_{i\in I} F_i$? On montre que, pour tout $i \in I$, on a $x \in F_i$.

Comment montrer que $x \in \bigcup_{i\in I} F_i$? On montre qu'il existe $i \in I$, tel que $x \in F_i$.

Définition : Soit $(F_i)_{i\in I}$ une famille de sous-espaces vectoriels de E. La *somme* des sous-espaces vectoriels F_i est S si, pour tout $v \in E$,

$$v \in S \iff \exists (v_1, \dots, v_r) \in F_1 \times \cdots \times F_r,\ v = v_1 + \cdots + v_r.$$

On note alors $S = \sum_{i\in I} F_i$. La somme est *directe* si

$$\forall v \in S,\ \exists! (v_1, \dots, v_r) \in F_1 \times \cdots \times F_r,\ v = v_1 + \cdots + v_r.$$

On note alors $S = \bigoplus_{i\in I} F_i$.

Exercice :
On a $E = \mathbb{R}_3[X]$. On veut d'abord montrer $F + G + H$, puis que cette somme est directe et enfin que F, G et H sont supplémentaires. C'est à dire, on veut montrer que tout vecteur de E (3) peut s'écrire de manière unique (2) comme la somme d'un vecteur de F, d'un vecteur de G et d'un vecteur de H.

Soit $P = a + bX + cX^2 + dX^3 \in \mathbb{R}_3[X]$.

$$P = \underbrace{\alpha X(X-1)(X-2)}_{\in F} + \underbrace{\beta(X-1)(X-2)(X-3)}_{\in G} + \underbrace{\gamma + \delta X^2}_{\in H}$$

$$\iff (\heartsuit) : \begin{cases} -6\beta + \gamma = a \\ 2\alpha + 11\beta = b \\ -3\alpha + 6\beta + \delta = c \\ \alpha + \beta = d \end{cases}$$

Montrons que le système $(\heartsuit)$ a une unique solution.

$1^{\underline{\text{ère}}}$ méthode : on applique la méthode du pivot de Gauß. On a

$$(\heartsuit) \iff \begin{cases} \delta - 6\beta - 3\alpha = c \\ \gamma - 3\beta = a \\ \beta + \alpha = d \\ 11\beta + 2\alpha = b \end{cases}.$$

Le système est triangulaire, il a donc une unique solution.

$2^{\underline{\text{nde}}}$ méthode : on calcule le rang du système $(\heartsuit)$. La matrice A la matrice des coefficients :

$$A = \begin{bmatrix} 0 & -6 & 1 & 0 \\ 2 & 11 & 0 & 0 \\ -3 & -6 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

On peut montrer que $\operatorname{rg} A = 4$ ou montrer que A est inversible i.e. $\det A \neq 0$.

Proposition :
1. La somme des sous-espaces vectoriels F_i est un sous-espace vectoriel de E.
2. Si la dimension des sous-espaces vectoriels F_i est finie, alors $\dim\Big(\sum_{i\in I} F_i\Big) \leqslant \sum_{i\in I} \dim F_i$.
3. La somme est directe si et seulement si $\dim\Big(\sum_{i\in I} F_i\Big) = \sum_{i\in I} \dim F_i$.

Preuve :
Soit φ l'application linéaire définie ci-dessous :

$$\begin{aligned} \varphi : F_1 \times \cdots \times F_r &\longrightarrow E \\ (\vec{x}_1, \ldots, \vec{x}_r) &\longmapsto \vec{x}_1 + \cdots + \vec{x}_r. \end{aligned}$$

1. $\mathfrak{Im}\varphi$ est un sous-espace vectoriel de E car φ est une application linéaire (cf. cours de première année). Or, $\mathfrak{Im}\varphi = F_1 + \cdots + F_r$ d'après la DÉFINITION 5.
2. On applique le théorème du rang à φ :

$$\dim(F_1 \times \cdots \times F_r) = \dim(\operatorname{Ker}\varphi) + \dim(\mathfrak{Im}\varphi).$$

Or, d'après l'EXERCICE 4, $\dim(F_1 \times \cdots F_r) = \dim F_1 + \cdots + \dim F_r$; et, $\dim(\mathfrak{Im}\varphi) = \dim(F_1 + \cdots + F_r)$ d'après la question 1. Comme $\dim(\operatorname{Ker}\varphi) \geqslant 0$, on a donc

$$\sum_{i=1}^{r} \dim F_i \geqslant \dim\Big(\sum_{i=1}^{r} F_i\Big).$$

3. La somme $\sum_{i=1}^{n} F_i = F_1 + \cdots + F_r$ est directe si et seulement si φ est injective si et seulement si $\operatorname{Ker}\varphi = \{0_E\}$ si et seulement si $\dim(\operatorname{Ker}\varphi) = 0$. On en déduit donc, en reprenant l'expression de 2., on a
$$\sum_{i=1}^{r} \dim F_i = \dim\Big(\sum_{i=1}^{r} F_i\Big).$$

□

Exercice (somme de **deux** espaces vectoriels) :
On pose $E = \mathbb{R}^2$, et $n = 3$. Soient F_1, F_2 et F_3 trois sous-espaces vectoriels de $\mathbb{R}^2$.

On a $F_1 \cap F_2 \cap F_3 = \{\vec{0}\}$: $F_1 \cap F_2 = \{\vec{0}\}$, $F_2 \cap F_3 = \{\vec{0}\}$ et $F_1 \cap F_3 = \{\vec{0}\}$. Mais, la somme $F_1 + F_2 + F_3$ n'est pas directe car $\vec{\imath} + \vec{\jmath} = \vec{0} + \vec{0} + (\vec{\imath} + \vec{\jmath}) = \vec{\imath} + \vec{\jmath} + \vec{0}$.

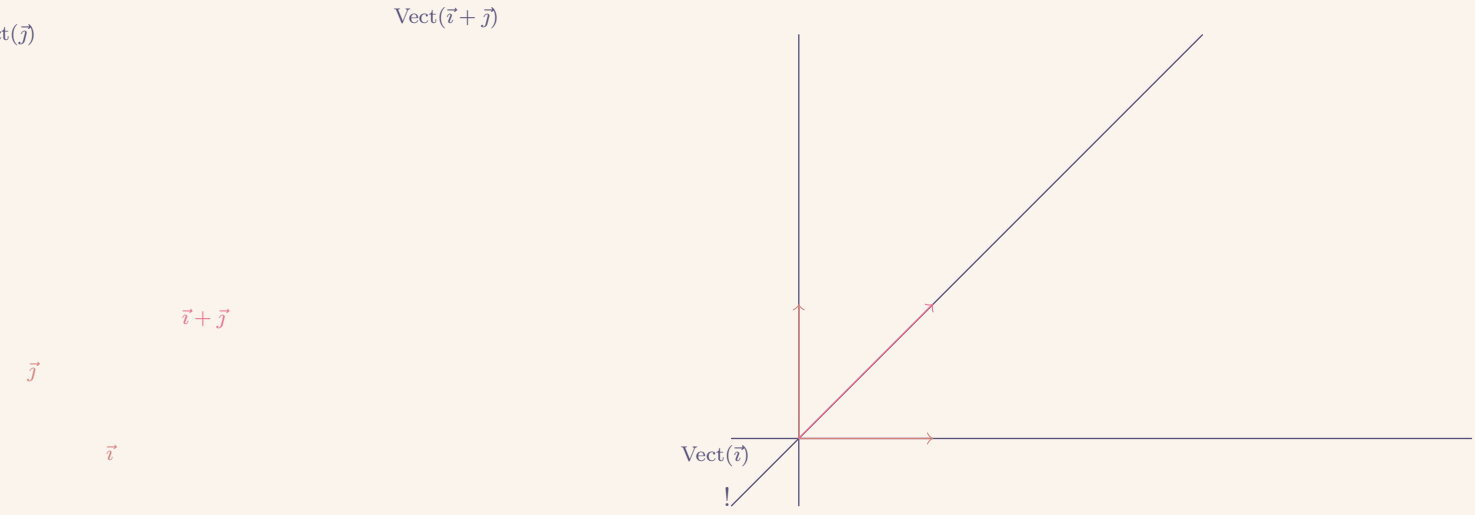


Figure 2.6 – Contre-exemple des propriétés de la somme dans de trois sous-espaces vectoriels

Néanmoins, pour $r = 2$, on a bien la formule de Grassmann :
$$\dim(F + G) = \dim F + \dim G - \dim(F \cap G).$$

On pose l'application linéaire φ comme définie ci-dessous :
$$\begin{aligned} \varphi : F \times G &\longrightarrow E \\ (\vec{x}_1, \vec{x}_2) &\longmapsto \vec{x}_1 + \vec{x}_2. \end{aligned}$$

On a, d'après le théorème du rang,
$$\dim(F \times G) = \dim(\operatorname{Ker}\varphi) + \dim(\mathfrak{Im}\varphi).$$

Or, $\dim(F\times G) = \dim F + \dim G$ d'après l'EXERCICE 4 ; et, comme $\mathfrak{Im}\varphi = F+G$ et donc $\dim(\mathfrak{Im}\varphi) = \dim(F+G)$. Il reste à montrer que $\dim(\operatorname{Ker}\varphi) = \dim(F\cap G)$.

On sait que $\operatorname{Ker}\varphi = \{(\vec{x}_1,\vec{x}_2)\in F\times G \mid \vec{x}_1+\vec{x}_2 = \vec{0}\} = \{(\vec{x},-\vec{x})\in F\times G\}$. Or, on sait que $\forall \vec{x}\in F,\ -\vec{x}\in F$ et on en déduit donc que $\operatorname{Ker}\varphi = \{(\vec{x},-\vec{x})\in (F\cap G)^2\}$. D'où, l'application

$$\begin{aligned} h : F\cap G &\longrightarrow \operatorname{Ker}\varphi \\ \vec{x} &\longmapsto (\vec{x},-\vec{x}) \end{aligned}$$

est un isomorphisme par construction.

La somme est directe si et seulement si $\dim(F+G) = \dim F + \dim G$ donc si et seulement si $\dim(F\cap G) = 0$ et donc si et seulement si $F\cap G = \{\vec{0}\}$.

REMARQUE :
Il est important de vérifier que $E = F\oplus G$. On dit que p est un projecteur et que $p(\vec{x})$ est le projeté de $\vec{x}$ sur F parallèlement à G. Du dessin du polycopié, on en déduit que, pour tout vecteur $\vec{x}$, on a $\vec{x}+\mathcal{s}(\vec{x}) = 2p(\vec{x})$; d'où, $\mathrm{id}_E + \mathcal{s} = 2p$. Un projecteur p projette sur $\mathfrak{Im}p$ parallèlement à $\operatorname{Ker}p$. Une symétrie $\mathcal{s}$ est une symétrie par rapport à $\operatorname{Ker}(\mathcal{s}-\mathrm{id}_E)$ parallèlement à $\operatorname{Ker}(\mathcal{s}+\mathrm{id}_E)$.

EXERCICE :
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soient F et G deux supplémentaires dans E. Soit p un projecteur sur F parallèlement à G. Sans perte de généralité, on peut se placer dans une base particulière, adaptée au problème (à la somme directe $F\oplus G$) car tr et rg sont, ou bien invariants par changement de base, ou bien invariants de similitude. Soit $\mathcal{B} = (\vec{e}_1,\dots,\vec{e}_r,\vec{e}_{r+1},\dots,\vec{e}_n)$ une base de E telle que $(\vec{e}_1,\dots,\vec{e}_r)$ est une base de F et $(\vec{e}_{r+1},\dots,\vec{e}_n)$ est une base de G. Une telle base $\mathcal{B}$ existe car F et G sont supplémentaires.

$$[p]_{\mathcal{B}} = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \begin{matrix} \vec{e}_1 \\ \vdots \\ \vec{e}_r \\ \vec{e}_{r+1} \\ \vdots \\ \vec{e}_n \end{matrix}.$$
$$\begin{matrix} p(\vec{e}_1)\dots p(\vec{e}_r) & p(\vec{e}_{r+1})\dots p(\vec{e}_n) \end{matrix}$$

Définition : Soient E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Soit $f : E\to E$ un endomorphisme. On dit que F est stable par f si $\forall \vec{x}\in F,\ f(\vec{x})\in F$ i.e. $f(F)\subset F$.

Si F est stable par f, alors l'application

$$\begin{aligned} f\big|_F = g : F &\longrightarrow F \\ \vec{x} &\longmapsto f(\vec{x}) \end{aligned}$$

existe et on dit que c'est l'*endomorphisme induit* par f sur F.

Rappel :
On dit que $f(F)$ est l'*image directe* de F par f.

Exemple : 1. $\mathbb{R}_n[X]$ est stable par l'application D définie comme

$$\begin{aligned} D : \mathbb{R}[X] &\longrightarrow \mathbb{R}[X] \\ P(X) &\longmapsto P'(X). \end{aligned}$$

2. Soient F et G deux sous-espaces vectoriels supplémentaires dans un espace vectoriel E. Alors F et G sont stables par le projecteur p sur F parallèlement à G. Et, aussi par la symétrie s par rapport à F parallèlement à G. On a aussi

$$p\big|_F = \mathrm{id}_F\,; \qquad p\big|_G = \tilde{0}\,; \qquad s\big|_F = \mathrm{id}_F\,; \qquad s\big|_G = -\mathrm{id}_G.$$

Exercice :
On pose (i, j, k) une base de $\mathbb{R}^3$. Et, on pose

$$A = \big[f\big]_{(\vec{\imath},\vec{\jmath},\vec{k})} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

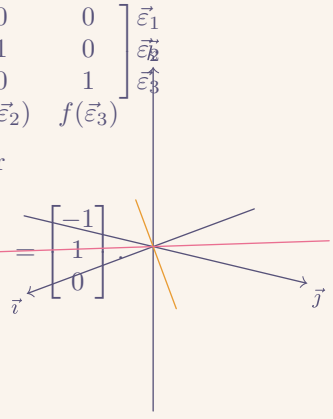
L'application f est la symétrie par rapport à $\mathrm{Vect}(\vec{\imath}+\vec{\jmath},\vec{k})$ parallèlement à $\mathrm{Vect}(\vec{\imath}-\vec{\jmath})$. Les droites vectorielles $\mathrm{Vect}(\vec{\imath}-\vec{\jmath})$, $\mathrm{Vect}(\vec{\imath}+\vec{\jmath})$ et $\mathrm{Vect}(\vec{k})$ sont stables par f.

On cherche maintenant une base $\mathscr{C}$ telle que f soit diagonale. Avec $\mathscr{C} = (\vec{\imath}-\vec{\jmath},\vec{\imath}+\vec{\jmath},\vec{k})$, on a

$$\big[\mathscr{C}\big]_{\mathscr{C}} = \begin{array}{c} \\ \vec{\varepsilon}_1 \\ \vec{\varepsilon}_2 \\ \vec{\varepsilon}_3 \\ \\ f(\vec{\varepsilon}_1) \quad f(\vec{\varepsilon}_2) \quad f(\vec{\varepsilon}_3) \end{array} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

car $f(\vec{\varepsilon}_1) = -\vec{\varepsilon}_1$ car $f(\vec{\imath}-\vec{\jmath}) = -(\vec{\imath}-\vec{\jmath})$ car

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$$



On procède de même pour ε_2 et ε_3.

!

Figure 2.7 – Dessin pour l'application f

Proposition : Soient $u : E \to E$ et $v : E \to E$ deux endomorphismes tels que $u \circ v = v \circ u$, alors le noyau $\mathrm{Ker}\, u$ $(\star)$ et l'image $\mathfrak{Im} u$ $(\star\star)$ sont des sous-espaces vectoriels stables par v.

Preuve :($\star$) : On veut montrer que $\forall \vec{x} \in \operatorname{Ker} u$, $v(\vec{x}) \in \operatorname{Ker} u$. Soit $\vec{x} \in \operatorname{Ker} u$. On a $u(\vec{x}) = \vec{0}$ d'où $v(u(\vec{x})) = v(\vec{0}) = \vec{0}$ i.e. $v \circ u(\vec{x}) = \vec{0}$ d'où $u \circ v(\vec{x}) = \vec{0}$ i.e. $u(v(\vec{x})) = \vec{0}$ d'où $v(\vec{x}) \in \operatorname{Ker} u$.

($\star\star$) : On veut montrer que $\forall \vec{y} \in \mathfrak{Im} u$, $v(\vec{y}) \in \mathfrak{Im} u$. Soit $\vec{y} \in \mathfrak{Im} u$. D'où, il existe $\vec{x} \in E$ tel que $\vec{y} = u(\vec{x})$. Alors, $v(\vec{y}) = v(u(\vec{x})) = v \circ u(\vec{x})$ d'où $v(\vec{y}) = u \circ v(\vec{x}) = u(v(\vec{x}))$.

□

Exercice :
Soient u et v deux endomorphismes tels que $u \circ v = v \circ u$. L'ensemble des vecteurs invariants par u est $\operatorname{Ker}(u - \mathrm{id}_E)$ car

$$u(\vec{x}) = \vec{x} \iff u(\vec{x}) - \vec{x} = \vec{0} \iff (u - \mathrm{id}_E)(\vec{x}) = \vec{0} \iff \vec{x} \in \operatorname{Ker}(u - \mathrm{id}_E).$$

Comme cet ensemble est un noyau, c'est un sous-espace vectoriel de E. Or, $u - \mathrm{id}_E$ et v commutent d'après la démonstration qui suit, d'où $\operatorname{Ker}(u - \mathrm{id}_E)$ est stable par v.

$$\begin{aligned} \forall \vec{x} \in E,\ (u - \mathrm{id}_E) \circ v(\vec{x}) &= (u - \mathrm{id}_E)\big(v(\vec{x})\big) \\ &= u(v(\vec{x})) - v(\vec{x}) \\ &= u \circ v(\vec{x}) - v(\vec{x}) \\ &= v \circ u(\vec{x}) - v(\vec{x}) \end{aligned}$$

car $u \circ v$ commutent par hypothèse. D'où $(u - \mathrm{id}_E) \circ v(\vec{x}) = v \circ (u - \mathrm{id}_E)(\vec{x})$ donc $(u - \mathrm{id}_E) \circ v = v \circ (u - \mathrm{id}_E)$.

Méthode :
c.f. poly

Exercice :
c.f. poly

Définition : Soit $P = \sum_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$ un polynôme.

Avec $P(X) = X^k$, alors $P(A) = A^k = \overbrace{A \times A \times \cdots \times A}^{k \text{ fois}}$, et $P(u) = u^k = \overbrace{u \circ u \circ \cdots \circ u}^{k \text{ fois}}$ pour tout $k \in \mathbb{N}^\star$. Avec $k = 0$, on a $P(X) = X^0$, et donc $P(A) = A^0 = I_n$, et $P(u) = u^0 = \mathrm{id}_E$.

Avec $P(X) = 2 + 8X + 4X^7$, on a donc $P(A) = 2I_n + 8A + 4A^7$ et $P(u) = 2\,\mathrm{id}_E + 8u + 4u^7$.

Si E est de dimension finie, on a $\big[P(u)\big]_{\mathscr{B}} = P\big([u]_{\mathscr{B}}\big)$.

Proposition : Soient $P, Q \in \mathbb{K}[X]$ et $\alpha, \beta \in \mathbb{K}$, on a

$$(\alpha P + \beta Q)(u) = \alpha P(u) + \beta Q(u) \qquad \text{et} \qquad (P \times Q)(u) = P(u) \circ Q(u).$$

De même, on a

$$(\alpha P + \beta Q)(A) = \alpha P(A) + \beta Q(A) \qquad \text{et} \qquad (P \times Q)(A) = P(A) \cdot Q(A).$$

On pose $P(X) = 2 + 3X^4$ et $Q(X) = 7 + 8X^2$, on a $P(X) \times Q(X) = 14 + 16X^2 + 21X^4 + 24X^6$, d'où, d'après la définition 18, on a, d'une part,

$$P \times Q(u) = 14\,\mathrm{id} + 16u^2 + 21u^4 + 24u^6.$$

D'autre part, en évaluant P en u, on a $P(u) = 2\,\mathrm{id} + 3u^4$ et $Q(u) = 7\,\mathrm{id} + 8u^2$, et donc

$$P(u) \circ Q(u) = (2\,\mathrm{id} + 3u^4) \circ (7\,\mathrm{id} + 8u^2) = 14\,\mathrm{id} + 16u^2 + 21u^4 + 24u^6.$$

Exercice :
Soient A et B deux matrices semblables et P un polynôme. Montrer que $P(A)$ et $P(B)$ sont semblables et $P(A^\top) = P(A)^\top$.

Il existe un matrice $Q \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = Q^{-1}AQ$. D'où $B^2 = (Q^{-1}AQ)(Q^{-1}AQ) = Q^{-1}A^2Q$. On peut démontrer que $B^k = Q^{-1}A^kQ$ par récurrence avec cette même méthode pour $k \in \mathbb{N}^\star$. On pose $P = a_0 + a_1X + \cdots + a_dX^d$. On calcule

$$\begin{aligned} Q^{-1}P(B)Q &= Q^{-1}(a_0I_n + a_1B + \cdots + a_dB^d)Q \\ &= Q^{-1}I_nQ + a_1Q^{-1}BQ + a_2Q^{-1}B^2Q + \cdots + a_dQ^{-1}B^dQ \\ &= P(A). \end{aligned}$$

Se rappeler que $(AB)^\top = B^\top \cdot A^\top$. Ainsi, $(A^2)^\top = (A \cdot A)^\top = (A^\top)^2$. D'où $\forall k \in \mathbb{N}^\star$, $(A^k)^\top = (A \times \cdots \times A)^\top = A^\top \cdots A^\top = (A^\top)^k$. De plus, $(A^0)^\top = I_n^\top = I_n = (A^\top)^0$. Et, comme la transposition est linéaire ($\forall \alpha, \beta, \forall A, B$, $(\alpha A + \beta B)^\top = \alpha A^\top + \beta B^\top$), on en déduit que

$$\forall P \in \mathbb{K}[X],\ P(A^\top) = \big(P(A)\big)^\top.$$

Définition : On dit qu'un polynôme P est *annulateur* de A si $P(A) = 0_{\mathcal{M}_{nn}(\mathbb{K})}$.

On dit qu'un polynôme P est *annulateur* de u si $P(u) = 0_{\mathcal{L}(E)}$. Et donc $\forall x \in E$, $P(u)(x) = 0_E$ (attention, ce n'est pas $P\big(u(x)\big)$.

Exemple :
On sait que p un projecteur si et seulement $p \circ p = p$. Autrement dit, si et

seulement si $p \circ p - p = 0_{\mathscr{L}(E)}$, si et seulement si $Q(p) = 0_{\mathscr{L}(E)}$ avec $Q(X) = X^2 - X$.

On sait que s est un symétrie si et seulement si $s \circ s = \mathrm{id}_E$, si et seulement si $s \circ s - \mathrm{id} = 0$, si et seulement si $s^2 - s = 0$ et donc $Q(s) = 0$ où $Q(X) = X^2 - 1$.

Exercice :
On a

$$(I_n + J)^2 = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}^2 = \begin{pmatrix} n & \dots & n \\ \vdots & \ddots & \vdots \\ n & \dots & n \end{pmatrix} = n(I_n + J).$$

On rappelle que $(a+b)^2 = a^2 + 2ab + b^2$ mais pour des matrices A et B, on a $(A+B)^2 = A^2 + AB + BA + B^2$ car la multiplication n'est pas commutative en général. (Mais, c'est le cas dans cet exercice.)

Or, $(I_n+J)^2 = I_n+2J+J^2$ car I_n et J commutent. D'où $I_n+2J+J^2 = nI_n+nJ$. Donc $J^2 - (n-2)J - (n-1)I_n = 0_{\mathscr{M}_{nn}(\mathbb{K})}$ donc le polynôme

$$P(X) = X^2 - (n-2)X - (n-1)$$

est annulateur de la matrice J.

Méthode (Inverser une matrice) :
On applique cette méthode que si le polynôme annulateur n'a pas un terme constant nul. Sinon, on divise par 0.

Exercice :
On a montré que $J^2 - (n-2)J - (n-1)I_n = 0$. D'où $J^2 - (n-2)J = (n-1)I_n$. Donc $\frac{1}{n-1}J^2 - \frac{n-2}{n-1}J = I_n$ car $n - 1 \neq 0$. D'où $J \times \left(\frac{1}{n-1}J - \frac{n-2}{n-1}I_n\right) = I_n$. On en déduit que J est inversible et

$$J^{-1} = \frac{1}{n-1}J - \frac{n-2}{n-1}I_n.$$

Méthode (Calculer les puissances d'une matrice) :
On veut calculer $J^k = P(J)$ où $P = X^k \in \mathbb{K}[X]$. De plus, si on possède un polynôme annulateur de J : $Q(J) = 0$ (où, dans l'exemple $Q = X^2 - (n-2)X - (n-1)$). On réalise la division euclidienne $X^k \div Q$. On obtient un quotient $\mathbb{Q}_k$ et un reste $R_k = \alpha_k + \beta_k X$ car $\deg R_k < 2$. Ainsi, on a $J^k = Q(J) \times \mathbb{Q}_k(J) + R_k(J) = R_k(J)$.

Or, on sait calculer le polynôme R_k sans calculer le quotient (voir Annexe A.) Comment ? On a $X^k = Q(X) \times \mathbb{Q}(X) + R_k(X)$. Or, $Q(-1) = 0 = Q(n-1)$. D'où $(-1)^k = \alpha_k - \beta_k$ et $(n-1)^k = \alpha_k + \beta_k(n-1)$. On résout ce système pour déterminer α_k et β_k ; et donc $R_k(J) = \alpha_k I_n + \beta_k J$.

Exercice :
On sait que $J^2 - (n-2)J - (n-1)I_n = 0$. D'où $J^2 = (n-2)J + (n-1)I_n$. Or, en multipliant par J, et en utilisant l'expression de J^2, on en déduit que $J^3 \in \mathrm{Vect}(I_n, J)$. Et, de "proche en proche," on a $\forall k$, $J^k \in \mathrm{Vect}(I_n, J)$. Mais BOF car on n'a pas la formule pour $J^k = \alpha I_n + \beta_k J$. Pour avoir ces coefficients, on utilise la MÉTHODE 26.

Proposition–Définition : Toute matrice A possède un polynôme annulateur non nul. L'unique polynôme annulateur de A qui est unitaire et de degré minimal est appelé **le** *polynôme minimal* de A et est noté μ_A ou π_A.

Preuve :
On sait que $\dim \mathscr{M}_{nn}(\mathbb{K}) = n^2$. Soit $A \in \mathscr{M}_{nn}(\mathbb{K})$. On considère la famille $(A^0, A^1, A^2, A^3, \ldots, A^{n^2})$ qui contient n^2+1 vecteurs. D'où cette famille est liée : il existe α_0, α_1, $\alpha_2, \ldots, \alpha_{n^2}$ non nuls tels que

$$\alpha_0 A^0 + \alpha_1 A^1 + \cdots + \alpha_{n^2} A^{n^2} = 0.$$

D'où $P(A) = 0$ où $P(X) = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_{n^2} X^{n^2}$.

Ainsi, $\alpha + P(A) + \beta Q(A) = 0$ est un polynôme annulateur de A. D'où, l'ensemble $\mathscr{I}_A$ des polynômes annulateurs de A est un sous-espace vectoriel de $\mathbb{K}[X]$.

D'où $(\mathscr{I}_A, +)$ est un sous-groupe de $(\mathbb{K}[X], +)$. Par ailleurs, si un polynôme $P \in \mathscr{I}_A$ et un autre polynôme $Q \in \mathbb{K}[X]$, alors le produit $P \times Q \in \mathscr{I}_A$ car $(P \times Q)(A) = P(A) \times Q(A) = 0 \times Q(A) = 0$. On en déduit que $\mathscr{I}_A$ est un idéal de $\mathbb{K}[X]$.

Or, tout idéal de l'ensemble des polynôme, d'après l'annexe A, est de la forme $P \cdot \mathbb{K}[X]$ i.e. l'ensemble des multiples d'un polynôme P. Il existe donc un unique polynôme unitaire P tel que $\mathscr{I}_A = P \cdot \mathbb{K}[X]$. □

Exercice : *1. Déterminer le polynôme minimal de la matrice J.*

2. Montrer que la dérivation

$$\begin{aligned} D : \mathscr{C}^\infty(\mathbb{R}) &\longrightarrow \mathscr{C}^\infty(\mathbb{R}) \\ f &\longmapsto f' \end{aligned}$$

ne possède pas de polynôme annulateur non nul.

3. Montrer que deux matrices semblables ont la même polynômes annulateurs et donc le même polynôme minimal.

1. Il n'existe pas de polynôme unitaire annulateur de J
   - de degré n (par l'absurde) : si $Q(J) = 1J + aI_n = 0$ alors $J = -aI_n$ et c'est absurde.
   - de degré 0 (par l'absurde) : si $Q(J) = aI_n = 0$ avec $a \neq 0$, ce qui est absurde.

   Donc $X^2 - (n-2)X - (n-1)$ est déjà le polynôme minimal de J.
2. On sait que D est un endomorphisme de l'espace vectoriel $\mathscr{C}^\infty(\mathbb{R})$ de dimension infinie (en effet, on a $\mathbb{R}[X] \subset \mathscr{C}^\infty(\mathbb{R})$). On procède par l'absurde. Soit $P = a_0 + a_1 X + \cdots + a_n X^n$ (avec $a_n \neq 0$) un polynôme

annulateur non nul de D. Alors, $\forall f \in \mathscr{C}^\infty$, $\big(a_0\,\mathrm{id} + a_1 D + a_2 D^2 + \cdots + a_n D^n\big)(f) = 0$. Or, $\big(a_0\,\mathrm{id} + a_1 D + a_2 D^2 + \cdots + a_n D^n\big)(f) = a_0 f + a_1 f' + a_2 f'' + \cdots + a_n f^{(n)}$. Ce qui est absurde car, avec $f : x \mapsto x^n$, on a $P(D)(f)(0) = a_n \times n! \neq 0$.

3. On démontre que le polynôme minimal est un *invariant de similitude*. Si $P(A) = 0$ et $A' = Q^{-1}AQ$ avec $P \in \mathbb{K}[X]$ et $Q \in \mathrm{GL}_n(\mathbb{K})$, alors $P(A') = P(Q^{-1}AQ) = Q^{-1}P(A)Q = 0$ (c.f. EXERCICE 20). Donc, l'ensemble des polynômes annulateurs de A est aussi celui de A'. *A fortiori*, A et A' ont le même polynôme minimal.

REMARQUE :
Soit $A \in \mathscr{M}_{n,n}(\mathbb{K})$. L'application

$$\begin{aligned} e_A : \mathbb{K}[X] &\longrightarrow \mathscr{M}_{n,n}(\mathbb{K}) \\ P &\longmapsto P(A) \end{aligned}$$

évalue chaque polynôme P en A. C'est un morphisme d'anneaux, d'espaces vectoriels et même d'algèbres.

Définition : On dit qu'un endomorphisme u est *nilpotent* s'il existe $k \in \mathbb{N}^\star$ tel que $u^k = 0$; on dit qu'une matrice carrée A est nilpotente s'il existe $k \in \mathbb{N}^\star$ tel que $A^k = 0$.

EXERCICE :
Soit $A \in \mathscr{M}_{n,n}(\mathbb{K})$ une matrice nilpotente d'indice r : $A^r = 0$ mais $A^{r-1} \neq 0$.

1. Alors $\mu_A = X^r$: $\mu_A(A) = A^r = 0$ d'où μ_A est annulateur. Le polynôme μ_A est unitaire. Il n'existe pas de polynôme annulateur unitaire P de degré strictement inférieur à r car, sinon, $P \mid X^r$ d'où il existe $n < r$, $P = X^k$, or, si $P(A) = A^k = 0$, alors A est nilpotente d'indice $k < r$, ce qui est absurde.
2. (Tarte à la crème) On veut montrer que $r \leqslant n$. On pose $f : E \to E$ telle que $[f]_{\mathscr{B}} = A$ où E est un espace de dimension n, et ayant une base $\mathscr{B}$. On a $A^r = 0$ si et seulement si $f^r = 0$; et, $A^{r-1} \neq 0$ si et seulement si $f^{r-1} \neq 0$. On veut donc montrer que $r \leqslant \dim E$. Or, comme $f^{r-1} \neq 0_{\mathscr{L}(E)}$, il existe $x \in E$ tel que $f^{r-1}(x) \neq 0_E$. Considérons maintenant $\big(x, f(x), f^2(x), \ldots, f^{r-1}(x)\big)$, une famille de r vecteurs, et cette partie est libre car : si (Hyp) : $\alpha_0 + \alpha_1 f(x) + \alpha_2 f^2(x) + \cdots + \alpha_{r-1} f^{r-1}(x) = 0$, alors f^{r-1}(Hyp) donne $\alpha_0 f^{r-1}(x) = 0$ (grâce à la nilpotence de f), or $f^{r-1}(x) \neq 0$ d'où $\alpha_0 = 0$. On applique maintenant f^{r-2}, on a $\alpha_1 = 0$. De proche en proche, on a

   $$\alpha_0 = \alpha_1 = \alpha_2 = \cdots = \alpha_n.$$

   D'où $\mathrm{Vect}\big(x, f(x), \ldots, f^{r-1}(x)\big)$ est un sous-espace vectoriel de dimension r. Or, $\dim E = n$ et donc $r \leqslant n$.
3. On a A^r et $r \leqslant n$ d'où $A^n = A^r \cdot A^{n-r} = 0 \times A^{n-r} = 0$.

Lemme (des noyaux) **:** Soit u un endomorphisme de E. On considère un polynôme P annulateur de u. On factorise ce polynôme en r polynômes : $P(X) = \prod_{k=1}^{r} P_k(X)$. Alors,

$$E = \bigoplus_{k=1}^{r} \operatorname{Ker} P_k(u).$$

Si le polynôme n'est pas annulateur, on remplace E par $\operatorname{Ker} P(u)$ dans l'expression précédente (même si la plupart du temps, en TD, on utilise le cas où P est annulateur).

Preuve (par récurrence) *:*
On initialise avec deux polynômes P_1 et P_2, premiers entre-eux. D'où, d'après le théorème de BÉZOUT, il existe deux polynômes A_1 et A_2 de $\mathbb{K}[X]$ tels que $A_1(X) \times P_1(X) + A_2(X) \times P_2(X) = 1$. En particulier, $A_1(u) \circ P_1(u) + A_2(u) \circ P_2(u) = \mathrm{id}_E$. D'où, pour $x \in E$, $\big(A_1(u) \circ P_1(u)\big)(x) + \big(A_2(u) \circ P_2(u)\big)(x) = x$ $(\star)$. On veut montrer que $\operatorname{Ker}\big((P_1 \times P_2)(u)\big) = \operatorname{Ker}\big(P_1(u)\big) \oplus \operatorname{Ker}\big(P_2(u)\big)$.

— Montrons que $\operatorname{Ker}\big(P_1(u)\big) \cap \operatorname{Ker}\big(P_2(u)\big) = \{0_E\}$. Soit $x \in \operatorname{Ker}\big(P_1(u)\big) \cap \operatorname{Ker}\big(P_2(u)\big)$. Alors $P_1(u)(x) = 0_E$, et, de même, $P_2(u)(x) = 0_E$. Or,

$$\big(A_1(u) \circ \underbrace{P_1(u)\big)(x)}_{0_E} + \big(A_2(u) \circ \underbrace{P_2(u)\big)(x)}_{0_E} = x.$$

D'où $x = 0_E$.

— Montrons que $\operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u) \subset \operatorname{Ker}(P_1P_2)(u)$. Soit $x \in \operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u)$. Alors, il existe $x_1 \in \operatorname{Ker} P_1(u)$ et $x_2 \in \operatorname{Ker} P_2(u)$ tels que $x = x_1 + x_2$. Or, $\big(P_1(u) \circ P_2(u)\big)(x_2) = P_1(u)\big(P_2(u)(x_2)\big) = 0_E$ et $\big(P_2(u) \circ P_1(u)\big)(x_1) = P_2(u)\big(P_1(u)(x_1)\big) = 0_E$. D'où $\big(P_1(u) \circ P_2(u)\big)(x) = 0_E$. D'où $P_1P_2(u)(x) = 0_E$ et donc $x \in \operatorname{Ker}(P_1P_2)(x)$.

— Montrons que $\operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u) \supset \operatorname{Ker}(P_1P_2)(u)$. Soit $x \in \operatorname{Ker}(P_1P_2)(u)$. D'après $(\star)$, $x = x_1 + x_2$ avec $x_1 = \big(A_1(u) \circ P_1(u)\big)(x)$ et $x_2 = \big(A_2(u) \circ P_2(u)\big)(x)$. Alors

$$\begin{aligned} P_2(u)(x_1) &= P_2(u)\Big(\big(A_1(u) \circ P_1(u)\big)(x)\Big) \\ &= P_2(u) \circ A_1(u) \circ P_1(u)(x) = A_1(u) \circ P_1(u) \circ P_2(u)(x) \\ &= A_1(u) \circ \underbrace{P_1(u) \circ P_2(u)(x)}_{0_E} \\ &= 0_E \end{aligned}$$

De même, $P_1(u)(x_2) = 0_E$. D'où $x \in \operatorname{Ker} P_1(u) + \operatorname{Ker} P_2(u)$.

□

Exercice :
Soit $u : E \to E$ un endomorphisme tel que $u^3 = u$. Montrons que $\operatorname{Ker}(u+\mathrm{id}_E) \oplus \operatorname{Ker}(u-\mathrm{id}_E) \oplus \operatorname{Ker} u = E$.

2. De $u^3 = u$, il résulte que le polynôme $P = X^3 - X$ est annulateur de u. Or, $X^3 - X = (X-1)(X+1)$ et ces facteurs sont deux à deux premiers entre-eux. D'où $E = \operatorname{Ker} P(u) = \operatorname{Ker}(u+\mathrm{id}) \oplus \operatorname{Ker}(u-\mathrm{id}) \oplus \operatorname{Ker} u$.
1. On procède, comme demandé dans l'énoncé, à une analyse-synthèse. Soit $x \in E$.

Analyse On suppose que $x = a+b+c$ et que $a \in \operatorname{Ker}(u+\mathrm{id})$, $b \in \operatorname{Ker}(u-\mathrm{id})$ et $c \in \operatorname{Ker} u$. D'où $u(a) = -a$, $u(b) = b$ et $u(c) = 0$. On a $u(x) = u(a)+u(b)+u(c) = b-a$, d'où $b = u(x)-a$ et donc $u(b) = b = u^2(x)+u(a) = u^2(x)-a$ et donc $b = u^2(x) - b + u(x)$. On en déduit que

$$b = \frac{1}{2}\left(u^2(x)+u(x)\right) \qquad a = \frac{1}{2}\left(u^2(x)-u(x)\right) \qquad c = x - u^2(x).$$

— Soient $a = \frac{1}{2}u^2(x) - \frac{1}{2}u(x)$, $b = \frac{1}{2}u^2(x) + \frac{1}{2}u(x)$ et $c = x - u^2(x)$. On remarque que, *a fortiori*, $a+b+c = x$. On a $a \in \operatorname{Ker}(u+\mathrm{id}_E)$; en effet,

$$u(a) = \frac{1}{2}u^3(x) - \frac{1}{2}u^2(x) = \frac{1}{2}u(x) - \frac{1}{2}u^2(x) = -1$$

car $u^3 = u$. De même, on a $b \in \operatorname{Ker}(u-\mathrm{id}_E)$ et $c \in \operatorname{Ker} u$.

On en conclut qu'il existe une unique solution (a,b,c).

Chapitre 3

Intégrer sur un intervalle

VII.1 Intégrer une fonction continue par morceaux sur un segment

Toute fonction $f : \mathbb{R} \to \mathbb{R}$ continue sur un segment $[a, b]$ possède une intégrale $\int_a^b f(t)\,\mathrm{d}t$.

Toute fonction $f : \mathbb{R} \to \mathbb{R}$ continue par morceaux sur un segment $[a, b]$ s'il existe une subdivision $\sigma = (x_0, \dots, x_n) \in \mathfrak{S}_{[a,b]}$ de $[a, b]$ (donc $a = x_0 < \cdots < x_n = b$) et que $f|_{]x_{i-1},x_i[}$ est continue, pour tout i et que les limites de f en x_i et x_{i-1}. On dit que σ est *adaptée* à f. Alors, l'intégrale de f est

$$\int_{[a,b]} f = \sum_{i=1}^{n} \int_{[x_{i-1},x_i]} f_i$$

où $f_i = f|_{[x_{i-1},x_i]}$.

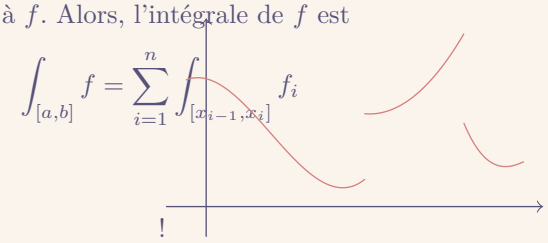


Figure 3.1 – Une fonction continue par morceaux

Remarque (intégrale et primitive) :
On dit que $F : I \to \mathbb{R}$ est une primitive de $f : I \to \mathbb{R}$ si F est dérivable et $F' = f$.

$$F \xrightarrow{\frac{\mathrm{d}}{\mathrm{d}x}(\square)} f \quad . \qquad f \xrightarrow{\int \square\,\mathrm{d}x} F$$

VII.2 Qu'est ce qu'une intégrale généralisée ?

Définition : Une fonction est *continue par morceaux* sur un intervalle I si elle est continue par morceaux sur chacun des segments inclus dans I.

Pour la $1^{\underline{\text{ère}}}$ intégrale, la fonction intégrée n'est pas définie en $t = 1$. On intègre donc jusqu'à x pour $x < 1$ et on prend la limite pour $x \to 1$.

Pour la $2^{\underline{\text{nde}}}$ intégrale, la borne supérieur est $+\infty$. On intègre donc jusqu'à x et on étudie la limite pour $x \to +\infty$ (comme pour les séries).

$$F(x) := \int_a^x f(t)\ \mathrm{d}t \xrightarrow[n\to+\infty]{} \begin{cases} \ell \in \mathbb{R} & \Longrightarrow \text{ l'intégrale } \int_a^{+\infty} f \text{ converge} \\ \text{sinon} & \Longrightarrow \text{ l'intégrale } \int_a^{+\infty} f \text{ diverge.} \end{cases}$$

Définition : Soit f une fonction continue par morceaux sur un intervalle $[a, b[$, où $-\infty < a < b \leqslant +\infty$. Soit, pour $x \in [a, b[$, $F(x) = \int_{[a,x]} f$. On dit que l'intégrale $I = \int_{[a,b[} f$ converge en b si la limite $\lim_{x\to b^-} F(x)$ existe et est finie. Sinon, on dit qu'elle diverge.

Exemple :
Le programme nous permet d'utiliser sans re-démontrer les points 2. et 3.

1. Montrons que $I = \int_0^1 \frac{1}{\sqrt{1-t^2}}\ \mathrm{d}t$ converge.

   L'intégrale I est impropre en 1 (ou est généralisée en 1). On remarque que, pour tout $x \in [0, 1[$,

   $$\int_0^x \frac{1}{\sqrt{1-t^2}}\ \mathrm{d}t = \operatorname{Arcsin} x \xrightarrow[x\to1^-]{} \operatorname{Arcsin} 1$$

   car Arcsin est continue. Or, $\operatorname{Arcsin} 1 = \frac{\pi}{2}$. Donc, l'intégrale I converge et que $I = \frac{\pi}{2}$.

2. *L'intégrale $J = \int_0^1 \ln t\ \mathrm{d}t$ est convergente en 0.*

   L'intégrale J est impropre en 0. On remarque que, pour $x \in]0, 1]$,

   $$\int_x^1 \ln t\ \mathrm{d}t = \big[t \ln t - t\big]_x^1 = -1 - x \ln x + x \xrightarrow[x\to0^+]{} -1$$

   par croissances comparées. On en déduit que l'intégrale J converge et que elle est égale à -1. Même si la borne supérieure est différente, on peut retrouver cette formule avec les relations de Chasles sur les intégrales.

3. *L'intégrale $B = \int_0^{+\infty} \mathrm{e}^{Kt}\ \mathrm{d}t$ (où K est une constante) converge en $+\infty$ si et seulement si $K < 0$.*

   L'intégrale B est impropre en $+\infty$. On remarque que, pour $x \in \mathbb{R}_\star^+$,

   $$\int_0^x \mathrm{e}^{Kt}\ \mathrm{d}t = \begin{cases} \left[\frac{\mathrm{e}^{Kt}}{K}\right]_0^x & \text{si } K \neq 0 \\ x & \text{si } K = 0. \end{cases}$$

Or, $x \xrightarrow[x\to+\infty]{} +\infty$ donc B diverge si $K = 0$; de plus,

$$\frac{\mathrm{e}^{Kx}-1}{K} \xrightarrow[x\to+\infty]{} \begin{cases} -\frac{1}{K} & \text{si } K < 0 \\ +\infty & \text{si } K > 0. \end{cases}$$

On en déduit que l'intégrale B converge si et seulement si $K < 0$ et, si $K < 0$, on a $B = -\frac{1}{K} > 0$.

Remarque :
Si f est continue par morceaux sur $]a, b[$ (où $-\infty \leqslant a < b \leqslant +\infty$), et l'intégrale $\int_{]a,b[} f$ est impropre en a et en b, alors on utilise la relation de Chasles en découpant cette intégrale avec $c \in]a, b[$: l'intégrale $\int_{]a,b[} f$ converge si et seulement si $\int_{]a,c]}$ converge **et** $\int_{[c,b[}$ converge. Si ces deux intégrales convergent, alors

$$\int_{]a,b[} f = \int_{]a,c]} f + \int_{[c,b[} f.$$

Exercice :
Cet exercice, comme indiqué dans le programme, peut être utilisé sans avoir à le re-démontrer. *Soit α un réel. Montrons que*

- *l'intégrale $\int_1^{+\infty} \frac{1}{t^\alpha}\,\mathrm{d}t$ converge si et seulement si $\alpha > 1$ (comme pour les séries) ;*
  [critère de Riemann en $+\infty$]
- *l'intégrale $\int_0^1 \frac{1}{t^\alpha}\,\mathrm{d}t$ converge si et seulement si $\alpha < 1$; [critère de Riemann en 0]*
- *l'intégrale $\int_0^{+\infty} \frac{1}{t^\alpha}\,\mathrm{d}t$ diverge pour tout $\alpha \in \mathbb{R}$.*

1. L'intégrale $\int_1^{+\infty} \frac{1}{t^\alpha}\,\mathrm{d}t$ est impropre en $+\infty$. Soit $x \in [1, +\infty[$.

$$\int_1^x f(t)\,\mathrm{d}t = \begin{cases} \left[\ln t\right]_1^x & \text{si } \alpha = 1 \\ \left[\frac{t^{-\alpha+1}}{-\alpha+1}\right] & \text{si } \alpha \neq 1 \end{cases} = \begin{cases} \frac{x^{-\alpha+1}-1}{-\alpha+1} & \text{si } \alpha \neq 1 \\ \ln x \xrightarrow[x\to+\infty]{} +\infty & \text{si } \alpha = 1 \end{cases}$$

Si $-\alpha + 1 < 0$, alors $\int_1^x \frac{1}{t^\alpha}\,\mathrm{d}t \xrightarrow[x\to+\infty]{} \frac{1}{\alpha-1}$. Si $-\alpha + 1 > 0$, alors $\int_1^x \frac{1}{t^\alpha}\,\mathrm{d}t \xrightarrow[x\to+\infty]{} +\infty$. L'intégrale $\int_1^{+\infty} \frac{1}{t^\alpha}\,\mathrm{d}t$ converge si et seulement si $\alpha > 1$.

Remarque :
Si $f : [a, +\infty[\to \mathbb{R}^+$, l'intégrale $\int_a^{+\infty} f(t)\,\mathrm{d}t$ peut converger même si $f(t) \not\xrightarrow[t\to+\infty]{} 0$. En effet, la fonction décrite sur le poly est un bon exemple : son intégrale converge mais la fonction ne tend pas vers 0.

Proposition (intégrales faussement impropres) **:** Si une fonction $f :]a, b] \to \mathbb{R}$ est continue sur $]a, b]$ et possède une limite finie ℓ en a, alors son intégrale $\int_a^b f(t)\ \mathrm{d}t$est impropre en a mais elle converge en a. On dit donc qu'elle est *faussement* impropre.

Preuve :
Soit $x \in]a, b]$. On considère l'intégrale $\int_x^b f(t)\ \mathrm{d}t = F(b) - F(x)$ où F est une primitive de f sur $]a, b]$. On cherche donc la limite de F quand $x \to a^+$. On prolonge par continuité f en a, en posant $f(a) = \ell$. La fonction f est donc continue sur $[a, b]$. Cette fonction f prolongée possède une primitive F sur $[a, b]$. Donc f est dérivable sur $[a, b]$ et donc continue sur $[a, b]$. On en déduit que $F(x)$ admet une limite finie en a, et donc $\int_a^b f(t)\ \mathrm{d}t$ existe. □

Exemple :
On pose f, le sinus cardinal :

$$f : \mathbb{R}^\star \longrightarrow \mathbb{R}$$
$$t \longmapsto \frac{\sin t}{t}.$$

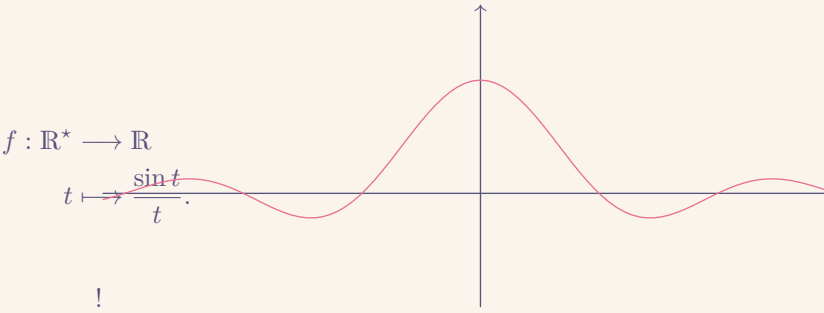


Figure 3.2 – Sinus cardinal

La fonction f est continue sur $]0, 8]$ mais $\lim_{t\to 0} \frac{\sin t}{t} = 1$. D'où $\int_0^8 \frac{\sin t}{t}\ \mathrm{d}t$ est faussement impropre en 0 et donc convergente.

Mais attention ! On ne dit pas « soit $f : t \mapsto \frac{1}{t}$. L'intégrale $\int_8^{+\infty} \frac{1}{t}\ \mathrm{d}t$ est faussement impropre en $+\infty$ car $\lim_{t\to+\infty} \frac{1}{t} = 0$. »

VII.3 Intégrer les $\sim$, $\wr$, et O

Théorème :

Théorème : Le 2. n'est pas la réciproque du 1. mais la contraposée.

Proposition :

Exemple :
On considère l'intégrale $\int_2^{+\infty} \frac{1}{t^2+\cos t}\ \mathrm{d}t$, c'est une intégrale impropre en $+\infty$.

On recherche un équivalent de $\frac{1}{t^2+\cos t}$ en $+\infty$:

$$\frac{1}{t^2+\cos t} \underset{t\to+\infty}{\sim} \frac{1}{t^2}$$

qui ne change pas de signe. Or, $\int_2^{+\infty} \frac{1}{t^2}\,\mathrm{d}t$ converge car c'est une intégrale de RIEMANN avec $\alpha = 2 > 1$. On en déduit que l'intégrale I converge.

On procède autrement :

$$0 \leqslant \frac{1}{t^2+\cos t} \leqslant \frac{1}{t^2-1}.$$

Or, $\int_2^{+\infty} \frac{1}{t^2-1}\,\mathrm{d}t$ converge car

$$\begin{aligned}\int_2^x \frac{1}{t^2-1}\,\mathrm{d}t &= \int_2^x \left(\frac{1/2}{t-1} - \frac{1/2}{t+1}\right)\mathrm{d}t \\ &= \frac{1}{2}\int_2^x \frac{1}{t-1}\,\mathrm{d}t - \frac{1}{2}\int_2^x \frac{1}{t+1}\,\mathrm{d}t \\ &= \frac{1}{2}\Big[\ln|t-1|\Big]_2^x - \frac{1}{2}\Big[\ln|t+1|\Big]_2^x\end{aligned}$$

D'où

$$\int_2^x \frac{1}{t^2-1}\,\mathrm{d}t = \frac{1}{2}\left[\ln\left|\frac{t-1}{t+1}\right|\right]_2^x = \frac{1}{2}\ln\left|\frac{x-1}{x+1}\right| + \frac{1}{2}\ln 3 \xrightarrow[x\to+\infty]{} \frac{1}{2}\ln 3.$$

donc l'intégrale I converge et $I \leqslant \frac{1}{2}\ln_3$.

EXERCICE : 1. L'intégrale $I = \int_0^1 \frac{\sin t}{t^2}\,\mathrm{d}t$ est impropre en 0. On utilise un équivalent : $\sin t \sim_{t\to 0} t$ qui ne change pas de signe. Or, $\int_0^t \frac{1}{t}\,\mathrm{d}t$ diverge (par critère de RIEMANN). Donc I diverge.

L'intégrale $J = \int_1^{+\infty} \sin\frac{1}{t}\,\mathrm{d}t$ est généralisée en $+\infty$. On cherche un équivalent en $+\infty$:

$$\sin\frac{1}{t} \underset{t\to+\infty}{\sim} \frac{1}{t}$$

qui ne change pas de signe. Or, $\int_1^{+\infty} \frac{1}{t}\,\mathrm{d}t$ diverge par critère de RIEMANN. On en déduit que J diverge également.

2. L'intégrale $\int_0^{+\infty} \frac{1}{t^2}\,\mathrm{d}t$ est impropre, **et** en 0, **et** en $+\infty$. Le théorème ne marche donc pas. En effet $t \mapsto \frac{1}{t^2}$ n'est pas continue par morceaux en 0, ce qui était le cas pour $t \mapsto \frac{1}{1+t^2}$.

[Retour sur la REMARQUE 5] L'intégrale $\int_0^{+\infty} \frac{1}{\ln(1+t)}\,\mathrm{d}t$ est impropre en 0 **et** en $+\infty$. $\int_0^{+\infty} \frac{1}{\ln(1+t)}\,\mathrm{d}t$ converge si et seulement si $\int_0^7 \frac{1}{\ln(1+t)}\,\mathrm{d}t$ **et** $\int_7^{+\infty} \frac{1}{\ln(1+t)}\,\mathrm{d}t$ convergent. Et si elles convergent

$$\int_0^{+\infty} \frac{1}{\ln(1+t)}\,\mathrm{d}t = \int_0^7 \frac{1}{\ln(1+t)}\,\mathrm{d}t + \int_7^{+\infty} \frac{1}{\ln(1+t)}\,\mathrm{d}t.$$

On n'utilise pas deux barrières en même temps. Sinon, les intégrales doublement impropres peuvent, et converger, et diverger.

Proposition (avec $\sim$) **:** Si $f(t) \sim_{t\to b} g(t)$ qui ne change pas de signe. Alors,

— ou bien $\int_a^b f(t)\,\mathrm{d}t$ et $\int_a^b g(t)\,\mathrm{d}t$ convergent et $\int_x^b f(t)\,\mathrm{d}t \underset{x\to b}{\sim} \int_x^b g(t)\,\mathrm{d}t$.

— ou bien $\int_a^b f(t)\,\mathrm{d}t$ et $\int_a^b g(t)\,\mathrm{d}t$ divergent et $\int_a^x f(t)\,\mathrm{d}t \underset{x\to b}{\sim} \int_a^x g(t)\,\mathrm{d}t$.

Cette proposition est équivalente à le LEMME 13 sur les séries.

EXERCICE :
Montrons que

$$\int_x^1 \frac{1}{\ln(1+t)}\,\mathrm{d}t \underset{x\to 0^+}{\sim} -\ln x.$$

L'intégrale $\int_x^1 \frac{1}{\ln(1+t)}\,\mathrm{d}t$ est généralisée en 0. *Quelle est sa nature ?* On cherche un équivalent de la fonction intégrée :

$$\frac{1}{\ln(1+t)} \underset{t\to 0^+}{\sim} \frac{1}{t} \text{ qui ne change pas de signe}$$

car $\ln(1+t) = t + \mathop{o}_{t\to 0^+}(t)$, d'où $\ln(1+t) \sim_{t\to 0^+} t$. Or, $\int_0^1 \frac{1}{t}\,\mathrm{d}t$ diverge (par critère de RIEMANN) donc $\int_0^1 \frac{1}{\ln(1+t)}\,\mathrm{d}t$ diverge aussi. D'où, leurs « sommes partielles » sont équivalentes :

$$\int_x^1 \frac{1}{\ln(1+t)}\,\mathrm{d}t \underset{x\to 0^+}{\sim} \int_x^1 \frac{1}{t}\,\mathrm{d}t = \ln 1 - \ln x = -\ln x.$$

VII.4 La convergence absolue

Théorème : Soit $f : [a,b[$ une fonction continue par morceaux. Si l'intégrale $\int_{[a,b[} |f|$ converge, alors $\int_{[a,b[} f$ converge aussi et,

$$\left|\int_{[a,b[} f\right| \leqslant \int_{[a,b[} |f|$$

(inégalité triangulaire).

Preuve :
On a

$$\forall t \in [a,b[, \quad f(t) = \frac{f(t)+|f(t)|}{2} + \frac{f(t)-|f(t)|}{2} = \underbrace{\frac{f(t)+|f(t)|}{2}}_{\geqslant 0} - \underbrace{\frac{|f(t)|-f(t)}{2}}_{\geqslant 0}.$$

L'analogie est, par exemple,

— en analyse, $f(t) = \frac{f(t)+f(-t)}{2} + \frac{f(t)-f(-t)}{2}$, une somme d'une fonction paire et d'une fonction impaire.

— en algèbre, $\mathscr{M}_{n,n}(\mathbb{K}) \ni M = \frac{M+M^\top}{2} + \frac{M-M^\top}{2}$ une somme d'une matrice symétrique $S \in \mathscr{S}_n(\mathbb{K})$ et d'une matrice antisymétrique $A \in \mathscr{A}_n(\mathbb{K})$.

On suppose que l'intégrale $\int_a^b |f(t)|\,\mathrm{d}t$ converge.

— On montre que $\int_a^b \frac{f(t)+|f(t)|}{2}\,\mathrm{d}t$ converge. On sait que

$$0 \leqslant \frac{f(t)-|f(t)|}{2} \leqslant |f(t)|.$$

Or, $\int_a^b |f(t)|\,\mathrm{d}t$ converge et donc $\int_a^b \frac{f(t)+|f(t)|}{2}\,\mathrm{d}t$ converge aussi.

— De même, on montre que $\int_a^b \frac{|f(t)|-f(t)}{2}\,\mathrm{d}t$ converge.

On en déduit que $\int_a^b f(t)\,\mathrm{d}t$ converge.

Montrons à présent l'inégalité triangulaire : on veut montrer que

$$-\int_a^b |f(t)|\,\mathrm{d}t \leqslant \int_a^b f(t)\,\mathrm{d}t \leqslant \int_a^b f(t)\,\mathrm{d}t.$$

Ce qui est vrai car $\forall t \in [a,b[,\ -|f(t)| \leqslant f(t) \leqslant |f(t)|$, et l'intégrale $\int_a^x f(t)\,\mathrm{d}t$ est croissante. D'où, $\forall x \in [a,b[$,

$$\int_a^x |f(t)|\,\mathrm{d}t \leqslant \int_a^x f(t)\,\mathrm{d}t \leqslant \int_a^x |f(t)|\,\mathrm{d}t.$$

Enfin, les inégalités larges passent à la limite quand $x \to b$. □

Exercice : 1. On sait, $\forall t \in [1,+\infty[,\ 0 \leqslant \left|\frac{\sin t}{t^2}\right| \leqslant \frac{1}{t^2}$. Or, l'intégrale $\int_1^{+\infty} \frac{1}{t^2}\,\mathrm{d}t$ converge d'après le critère de Riemann (car $2 > 1$). D'où $\int_1^{+\infty} \left|\frac{\sin t}{t^2}\right|\,\mathrm{d}t$ converge et donc $\int_1^{+\infty} \frac{\sin t}{t^2}\,\mathrm{d}t$ converge aussi.

2. L'intégrale $\int_0^1 \sin\frac{1}{t}\,\mathrm{d}t$ est impropre en 0. Or,

$$0 \leqslant \left|\sin\frac{1}{t}\right| \leqslant 1,$$

et l'intégrale $\int_0^1 1\,\mathrm{d}t$ converge, donc $\int_0^1 \sin\frac{1}{t}\,\mathrm{d}t$ converge absolument.

VII.5 Intégrer par parties et changer de variables

Proposition : L'intégration par parties, pour les intégrales sur un segment, donne, si f et g sont deux fonctions de classes $\mathscr{C}^1$:

$$\int_{[a,b]} fg' = \Big[fg\Big]_a^b - \int_{[a,b]} f'g.$$

Si l'intégrale est généralisé, on « met une barrière » et on utilise l'intégration par parties sur un segment, puis on passe à la limite. On étudie tous les cas :

— si $\left[fg\right]_a^x \xrightarrow[x\to b]{} \ell \in \mathbb{R}$, alors $\int_{[a,b[} fg'$ et $\int_{[a,b[} f'g$ ont la même nature ;

— si $\left[fg\right]_a^x$ diverge quand $x \to b$, alors on ne peut pas conclure.

La « morale » de la proposition 19 est : IPP dans une intégrale généralisée, on « met une barrière. »

EXERCICE (tarte à la crème) :
L'intégrale $\int_0^{+\infty} \frac{\sin t}{t}\,\mathrm{d}t$ est appelée l'intégrale de DIRICHLET. On montre qu'elle converge et, on calculera sa valeur dans le TD n° 3. Elle est impropre en 0 et en $+\infty$. On n'écrit pas

$$\int_0^{+\infty} \frac{\sin t}{t}\,\mathrm{d}t = \int_1^{+\infty} \frac{\sin t}{t}\,\mathrm{d}t + \int_0^1 \frac{\sin t}{t}\,\mathrm{d}t.$$

L'intégrale $\int_0^{+\infty} \frac{\sin t}{t}\,\mathrm{d}t$ converge si et seulement si les deux intégrales

$$I = \int_0^1 \frac{\sin t}{t}\,\mathrm{d}t \qquad \text{et} \qquad J = \int_1^{+\infty} \frac{\sin t}{t}\,\mathrm{d}t$$

convergent.

L'intégrale I converge car elle est faussement impropre ($\sin(t)/t \xrightarrow[t\to 0]{} 1$).

Qu'en est-il de J ? On peut majorer la valeur absolue de la fonction intégrée mais cela ne permet pas de conclure. On fait donc une IPP : on pose, pour $t \in [1,+\infty[$, $f(t) = -\cos t$ et $g(t) = \frac{1}{t}$. Ces deux fonctions sont de classe $\mathscr{C}^1$, d'où

$$\int_1^x f'(t)\times g(t)\,\mathrm{d}t = \Big[fg\Big]_1^x - \int_1^x f(t)\times g'(t)\,\mathrm{d}t = \left[-\frac{\cos t}{t}\right]_1^x - \int_1^x \frac{\cos t}{t^2}\,\mathrm{d}t.$$

On vent montrer que $\int_{[1,x]} f'\cdot g$ a une limite finie quand $x \to +\infty$. D'une part

$$\left[-\frac{\cos t}{t}\right]_1^x = \frac{\cos 1}{1} - \frac{\cos x}{x} \qquad \text{et} \qquad \frac{\cos x}{x} \xrightarrow[x\to+\infty]{} 0$$

car cos est bornée et $\frac{1}{x} \xrightarrow[x\to+\infty]{} 0$.

D'autre par, pour $x \in [1,+\infty[$,

$$0 \leqslant \left|\frac{\cos t}{t^2}\right| \leqslant \frac{1}{t^2}$$

et $\int_1^{+\infty} \frac{1}{t^2}\,\mathrm{d}t$ converge.

Par différence, on en déduit que $\int_0^{+\infty} \frac{\sin t}{t}$ converge.

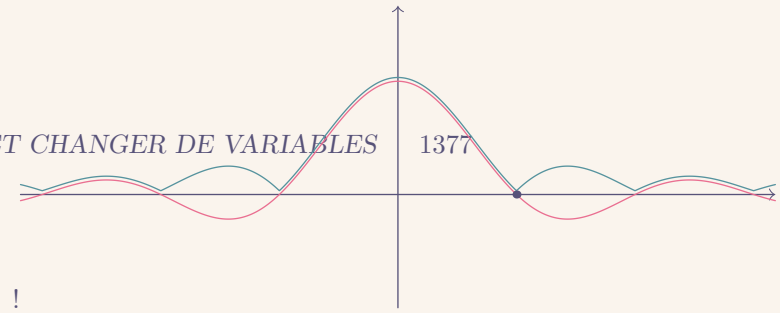


FIGURE 3.3 – Graphe de $\dfrac{\sin t}{t}$ et $\left|\dfrac{\sin t}{t}\right|$

REMARQUE :
Montrons que $\int_{\pi}^{+\infty} \left|\frac{\sin t}{t}\right| \,\mathrm{d}t$ diverge. On va montrer que $\sum_{k\geqslant 1}^{N} \int_{k\pi}^{(k+1)\pi} \underbrace{\left|\frac{\sin t}{t}\right|}_{u_k} \,\mathrm{d}t$ tend vers $+\infty$ quand $N \to +\infty$. On sait que

$$u_k \geqslant \int_{k\pi}^{(k+1)\pi} \frac{|\sin t|}{(k+1)\pi} \,\mathrm{d}t.$$

Or, $\int_{k\pi}^{(k+1)\pi} \frac{|\sin t|}{(k+1)\pi} \,\mathrm{d}t = \frac{1}{(k+1)\pi} \int_{k\pi}^{(k+1)\pi} |\sin t| \,\mathrm{d}t = \frac{1}{(k+1)\pi} \int_{0}^{\pi} |\sin t| \,\mathrm{d}t$ car $|\sin|$ est π-périodique. Or,

$$\int_0^{\pi} |\sin t| \,\mathrm{d}t = \int_0^{\pi} \sin t \,\mathrm{d}t = \Big[-\cos t\Big]_0^{\pi} = 2.$$

D'où

$$\forall k \in \mathbb{N}^{\star}, \quad u_k \geqslant \frac{2}{(k+1)\pi} \geqslant 0.$$

Or, $\sum \frac{2}{(k+1)\pi}$ diverge, d'où $\sum u_k$ diverge et donc

$$\int_0^{+\infty} \left|\frac{\sin t}{t}\right| \,\mathrm{d}t \text{ diverge.}$$

Proposition : Soit φ une fonction de classe $\mathscr{C}^1$ strictement croissante sur $[\alpha, \beta[$. On pose $a = \varphi(\alpha)$ et $b = \lim_{x\to\beta^-} \varphi(x)$. Si f est continue par morceaux sur $[a, b[$, alors

1. les intégrales $\int_a^b f(t) \,\mathrm{d}t$ et $\int_{\alpha}^{\beta} f\big(\varphi(u)\big)\cdot\varphi'(u) \,\mathrm{d}u$ sont de même nature ;
2. si ces intégrales convergent, alors

$$\int_a^b f(t) \,\mathrm{d}t = \int_{\alpha}^{\beta} f\big(\varphi(u)\big) \cdot \varphi'(u) \,\mathrm{d}u.$$

EXERCICE :
On considère l'intégrale $F(x) = \int_0^x \frac{1}{\operatorname{ch} t} \,\mathrm{d}t$, d'où $F(x) = \int_0^x \frac{2}{\mathrm{e}^t + \mathrm{e}^{-t}} \,\mathrm{d}t$. On fait le *changement de variable* suivant : $u(t) = \mathrm{e}^t$, d'où $\mathrm{d}u = \mathrm{e}^t \,\mathrm{d}t = u \,\mathrm{d}t$, et $t \in [0, x] \leftrightarrow u \in [1, \mathrm{e}^x]$. Ainsi

$$F(x) = \int_1^{\mathrm{e}^x} \frac{2}{u + \frac{1}{u}} \times \frac{1}{u} \,\mathrm{d}u = \int_1^{\mathrm{e}^x} \frac{2}{1+u^2} \,\mathrm{d}u = \Big[2 \operatorname{Arctan} u\Big]_1^{\mathrm{e}^x} = 2\operatorname{Arctan}(\mathrm{e}^x) - \frac{\pi}{2}.$$

Si $x \to +\infty$, alors $\mathrm{e}^x \to +\infty$. D'où $\operatorname{Arctan}(\mathrm{e}^x) \longrightarrow \frac{\pi}{2}$. Et donc

$$F(x) \xrightarrow[x\to+\infty]{} \frac{2\pi}{2} - \frac{\pi}{2} = \frac{\pi}{2}.$$

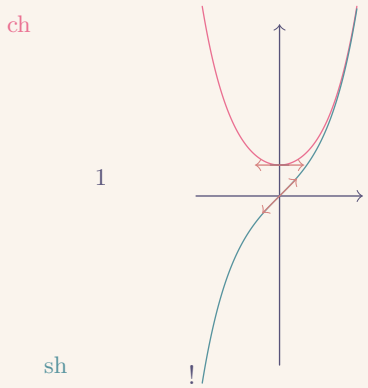


FIGURE 3.4 – Graphe de $\operatorname{ch} t$ et $\operatorname{sh} t$

Chapitre 4

Diagonalisation & trigonalisation

VII.1 (Ne pas) être diagonalisable

Définition : Soit une matrice carrée A. On dit que A est *diagonalisable* s'il existe une matrice inversible $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1} \cdot A \cdot P$ est diagonale.

Exercice : 1. Montrons que la matrice $B = \left(\begin{smallmatrix} 7 & 1 \\ 0 & 7 \end{smallmatrix}\right)$ n'est pas diagonalisable. Par l'absurde : on suppose qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ et $(\lambda_1, \lambda_2) \in \mathbb{R}^2$ tels que

$$P^{-1} \cdot B \cdot P = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

On applique la trace tr et le déterminant det :

$$\mathrm{tr}(B) = \mathrm{tr}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \quad \text{d'où} \quad \lambda_1 + \lambda_2 = 7 + 7 = 14 = \mathscr{s}$$

$$\det(B) = \det\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \quad \text{d'où} \quad \lambda_1 \times \lambda_2 = 7 \times 7 = 49 = p$$

D'où λ_1 et λ_2 sont des solutions de l'équation $X^2 - \mathscr{s}X + p = 0$. Or

$$\begin{aligned} X^2 - \mathscr{s}X + p = 0 &\iff X^2 - 14X + 49 = 0 \\ &\iff (X-7)^2 = 0 \\ &\iff X = 7. \end{aligned}$$

D'où

$$B = PP^{-1}BPP^{-1} = P\begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix}P^{-1} = P \cdot 7I_2 \cdot P^{-1} = 7I_2.$$

La matrice B n'est donc pas diagonalisable.

De même, montrons que la matrice A n'est pas diagonalisable. On remarque que

$$A \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Ainsi,

$$P^{-1} \cdot A \cdot P = \begin{pmatrix} 3 & 0 & 0 \\ 0 & ? & 0 \\ 0 & 0 & ? \end{pmatrix} \qquad \text{où} \qquad P = \begin{pmatrix} 1 & ? & ? \\ 1 & ? & ? \\ 1 & ? & ? \end{pmatrix}.$$

De même, $A \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 1 \times \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$. D'où

$$P^{-1} \cdot A \cdot P = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & ? \end{pmatrix} \qquad \text{où} \qquad P = \begin{pmatrix} 1 & 1 & ? \\ 1 & 1 & ? \\ 1 & 0 & ? \end{pmatrix}.$$

Finalement, on en conclut que

$$P = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad \text{et} \qquad P^{-1} \cdot A \cdot P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix} = D.$$

De plus, la matrice P est inversible car $\det P \neq 0$.

2. Pour calculer A^n, on pourrait chercher un polynôme annulateur Q de A, et on exprime $X^n = Q \times T_n + R_n$, et donc $A^n = R_n(A)$. Mais, on peut également diagonaliser A (si elle est diagonalisable). Ainsi,

$$D^n = (P^{-1} \cdot A \cdot P)^n = P^{-1} \cdot A \cdot \cancel{P} \cdot \cancel{P^{-1}} \cdot \ldots \cdot \cancel{P^{-1}} \cdot A \cdot P = P^{-1} \cdot A^n \cdot P.$$

D'où $A^n = P \cdot D^n \cdot P^{-1}$. Or,

$$D^n = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}^n = \begin{pmatrix} 3^n & 0 & 0 \\ 0 & 1^n & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}.$$

On calcule donc A^n en calculant l'inverse de P :

$$A^n = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3^n & 0 & 0 \\ 0 & 1^n & 0 \\ 0 & 0 & (-1)^n \end{pmatrix} \cdot P^{-1}.$$

3.

$$\left.\begin{aligned} u_{n+1} &= v_n + 2w_n \\ v_{n+1} &= u_n + 2w_n \\ w_{n+1} &= 3w_n \end{aligned}\right\} \iff \begin{pmatrix} u_{n+1} \\ v_{n+1} \\ w_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$$

$$\iff U_{n+1} = A \cdot U_n$$

$$\iff U'_{n+1} = D \cdot U'_n$$

où $D = P^{-1} \cdot A \cdot P$, $U'_{n+1} = P \cdot U_{n+1}$ et $U'_n = P \cdot U_n$.

$$\iff \begin{pmatrix} u'_{n+1} \\ v'_{n+1} \\ w'_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} u'_n \\ v'_n \\ w'_n \end{pmatrix}$$

$$\iff \begin{cases} u'_{n+1} = 3u'_n \\ v'_{n+1} = v'_n \\ w'_{n+1} = -w'_n \end{cases}$$

$$\iff \begin{cases} u'_n = K \times 3^n \\ v'_n = L \\ w'_n = M \times (-1)^n \end{cases}$$

Ainsi,

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix}}_{P} \cdot \begin{pmatrix} K \times 3^n \\ L \\ M \times (-1)^n \end{pmatrix}.$$

D'où $u_n = K \cdot 3^n + L + M \cdot (-1)^n$, $v_n = K \times 3^n + L - M \cdot (-1)^n$ et $w_n = K \cdot 3^n$, où les constantes K, L et M sont des constantes fixées par les conditions initiales.

4.

$$\left.\begin{aligned} x'(t) &= y(t) + 2z(t) \\ y'(t) &= x(t) + 2z(t) \\ z'(t) &= 3z(t) \end{aligned}\right\} \iff \begin{pmatrix} x'(t) \\ y'(t) \\ z'(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix}$$

$$\iff X'(t) = A \cdot X(t)$$

$$\iff U'(t) = D \cdot U(t) \text{ avec } D = P^{-1} \cdot A \cdot P \text{ et } X(t) = P \cdot U(t)$$

$$\iff \begin{pmatrix} u'(t) \\ v'(t) \\ w'(t) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} u(t) \\ v(t) \\ w(t) \end{pmatrix}$$

$$\iff \begin{cases} u'(t) = 3u(t) \\ v'(t) = v(t) \\ w'(t) = -w(t) \end{cases}$$

$$\iff \begin{cases} u(t) = K \cdot \mathrm{e}^{3t} \\ v(t) = L \cdot \mathrm{e}^{t} \\ w(t) = M \cdot \mathrm{e}^{-t} \end{cases}$$

Ainsi

$$\begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix}}_{P} \cdot \begin{pmatrix} K \times \mathrm{e}^{3t} \\ L \cdot \mathrm{e}^{t} \\ M \cdot \mathrm{e}^{-t} \end{pmatrix}.$$

D'où $x(t) = K \cdot \mathrm{e}^{3t} + L \cdot \mathrm{e}^{t} + M \cdot \mathrm{e}^{-t}$, $y(t) = K \cdot \mathrm{e}^{3t} + L \cdot \mathrm{e}^{t} - M \cdot \mathrm{e}^{-t}$ et $z(t) = K \cdot \mathrm{e}^{3t}$. Les constantes K, L et M peuvent être déterminées à partir des conditions initiales.

[équations différentielles] On considère l'équation différentielle $(\star) : x'(t) = \lambda \cdot x(t)$. Les fonctions $x : t \mapsto K \cdot \mathrm{e}^{\lambda t}$ sont des solutions de cette équation. On peut utiliser la méthode de LAGRANGE : la méthode de la « variation de la constante. » On cherche des solutions sous la forme $x(t) = k(t) \cdot \mathrm{e}^{\lambda t}$ (vision du physicien). D'où $k(t) = x(t)/\mathrm{e}^{\lambda t}$ (vision du mathématicien). De plus, $x'(t) = k'(t)\mathrm{e}^{\lambda t} + k(t)\lambda\mathrm{e}^{\lambda t}$. Ainsi, on injecte ce $k(t)$ dans l'équation différentielle :

$$\begin{aligned}(\star) &\iff k'(t)\mathrm{e}^{\lambda t} + k(t)\lambda\mathrm{e}^{\lambda t} = \lambda k(t)\mathrm{e}^{\lambda t}\\ &\iff k'(t)\mathrm{e}^{\lambda t} = 0\\ &\iff k'(t) = 0\\ &\iff \exists K \in \mathbb{R}\ k(t) = K.\end{aligned}$$

Les solutions trouvées dans l'exercice précédent sont donc les uniques solutions du système d'équations différentielles.

De même, pour résoudre une équation différentielle avec $2^{\underline{\text{nd}}}$ membre de la forme

$$(\star\star) : \qquad x'(t) - \lambda \cdot x(t) = b(t).$$

La fonction $t \mapsto x(t)$ est une solution de l'équation SANS $2^{\underline{\text{nd}}}$ membre si et seulement si

$$\exists K \in \mathbb{R},\ \forall t \in \mathbb{R}, \quad x(t) = K \cdot \mathrm{e}^{\lambda t}.$$

Comment résoudre l'équation différentielle AVEC $2^{\underline{\text{nd}}}$ membre si on connaît la solution générale de l'équation SANS $2^{\underline{\text{nd}}}$ membre ?

On utilise la méthode le la variation de la constante. Soit $x(t) = k(t) \cdot \mathrm{e}^{\lambda t}$. Ainsi, en injectant cette expression de x dans l'équation $(\star\star)$, on trouve

$$\begin{aligned}(\star\star) &\iff k'(t)\mathrm{e}^{\lambda t} + k(t) \cdot \lambda\mathrm{e}^{\lambda t} = \lambda k(t)\mathrm{e}^{\lambda t} + b(t)\\ &\iff k'(t)\mathrm{e}^{\lambda t} = b(t)\\ &\iff k'(t) = b(t) \cdot \mathrm{e}^{-\lambda t}\\ &\iff k(t) = \int_0^t b(u) \cdot \mathrm{e}^{-\lambda u}\ \mathrm{d}u + K\\ &\iff x(t) = \left(\int_0^t b(u) \cdot \mathrm{e}^{-\lambda u}\ \mathrm{d}u + K\right)\mathrm{e}^{\lambda t}\\ &\iff x(t) = \underbrace{\int_0^t b(u) \cdot \mathrm{e}^{\lambda(t-u)}\ \mathrm{d}u}_{\text{solution particulière}} + \underbrace{K \cdot \mathrm{e}^{\lambda t}}_{\substack{\text{solution}\\ \text{générale}\\ \text{de } (\star)}}.\end{aligned}$$

VII.2 Valeurs & vecteurs propres

Définition : Soit E un $\mathbb{K}$-espace vectoriel et $u : E \to E$ un endomorphisme.

1. On dit qu'un vecteur $\vec{x} \in E$ est **un** *vecteur propre* de u si $\vec{x}$ n'est pas nul et $u(\vec{x})$ est colinéaire à $\vec{x}$: $\vec{x} \neq \vec{0}$ et $\exists \lambda \in \mathbb{K}$, $u(\vec{x}) = \lambda\vec{x}$.
2. On dit qu'un scalaire $\lambda \in \mathbb{K}$ est **une** *valeur propre* de u s'il existe un

vecteur non nul $\vec{x} \in E$ tel que $u(\vec{x}) = \lambda\vec{x}$.
3. L'ensemble des valeurs propres de u est appelé le *spectre* de u et est noté $\mathrm{Sp}(u)$.

Définition : Soit $n \in \mathbb{N}^\star$ et A une matrice $n \times n$ à coefficients dans $\mathbb{K}$.
1. On dit qu'un vecteur colonne X est **un** *vecteur propre* de A si X n'est pas nul et $A \cdot X$ est colinéaire à X : $X \neq 0$ et $\exists \lambda \in \mathbb{K},\ A \cdot X = \lambda X$.
2. On dit qu'un scalaire $\lambda \in \mathbb{K}$ est **une** *valeur propre* de A s'il existe un vecteur colonne non nul X tel que $A \cdot X = \lambda X$.
3. L'ensemble des valeurs propres de A est appelé le *spectre* de A et est noté $\mathrm{Sp}(A)$.

Définition : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $u : E \to E$ un endomorphisme. On dit que u est *diagonalisable* s'il existe une base $(\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n)$ de E donc chaque vecteur est un vecteur propre de u :

$$\forall i \in [\![1, n]\!], \qquad u(\vec{\varepsilon}_i) = \lambda_i \, \vec{\varepsilon}_i.$$

Proposition–Définition : Soit $A \in \mathcal{M}_{n,n}(\mathbb{K})$ une matrice carrée. La fonction

$$\begin{aligned} \chi_A : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\longmapsto \det(xI_n - A) \end{aligned}$$

est appelé le *polynôme caractéristique de* A. On a

$$\forall x \in \mathbb{K}, \quad \chi_A(x) = \det(xI_n - A) = x^n - (\operatorname{tr} A)x^{n-1} + \cdots + (-1)^n \det A.$$

Preuve :
On a

$$\det(xI_n - A) = \begin{vmatrix} x - a_{11} & a_{12} & \cdots & -a_{1,n} \\ -a_{21} & x - a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & -a_{1,n-1} \\ -a_{n,1} & \cdots & -a_{n,n-1} & x - a_{n,n} \end{vmatrix} \begin{matrix} \\ \\ \\ \downarrow n \end{matrix}$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \longrightarrow n$$

□

Si E est un $\mathbb{K}$-espace vectoriel de dimension finie, alors on peut définir le polynôme caractéristique d'un endomorphisme par

$$\chi_u(x) = \det(x\,\mathrm{id}_E - u).$$

Si $A = [u]_{\mathscr{B}}$, alors $xI_n - A = [x\,\mathrm{id}_E - u]_{\mathscr{B}}$ et donc $\chi_u = \chi_A$.

Preuve :
On pose A une matrice $n \times n$ et A' une matrice semblable à A. On pose $A' = P^{-1} \cdot A \cdot P$. On calcule $\det(xI_n - A')$:

$$\chi_{A'}(x) = \det(xI_n - A') = \det(xI_n - P^{-1} \cdot A \cdot P) = \det(P^{-1}(xI_n - A)P) = \det(xI_n - A) = \chi_A(x).$$

par télescopage. □

Théorème : *Le polynôme caractéristique détecte les valeurs propres.*
Soit A une matrice carrée de taille $n \times n$. Un scalaire $\lambda \in \mathbb{K}$ est une valeur propre de A si et seulement si λ est une racine du polynôme caractéristique $\chi_A \in \mathbb{K}[X]$. Autrement dit,

$$\lambda \in \mathrm{Sp}(A) \iff \det(\lambda I_n - A) = 0.$$

Preuve :
Soit $\lambda \in \mathbb{K}$.

$$\begin{aligned}
\lambda \in \mathrm{Sp}(A) &\iff \exists X \neq 0, \quad A \cdot X = \lambda X \\
&\iff \exists X \neq 0, \quad (A - \lambda I_n) \cdot X = 0 \\
&\iff \exists X \neq 0, \quad -(A - \lambda I_n) \cdot X = 0 \\
&\iff \mathrm{Ker}(\lambda I_n - A) \neq \{0_n\} \\
&\iff \lambda I_n - A \text{ n'est pas inversible} \\
&\iff \det(\lambda I_n - A) = 0 \\
&\iff \chi_A(\lambda) = 0.
\end{aligned}$$

□

[Attention] Parfois, les racines d'un polynôme caractéristique peuvent être complexes et non réelles. Dans ce cas, afin d'éviter toute ambigüité, on écrit $\mathrm{Sp}_{\mathbb{R}}(A)$ pour les racines réelles et $\mathrm{Sp}_{\mathbb{C}}(A)$ pour les racines complexes.

Exercice : 1. On considère la matrice

$$C = \begin{array}{c} \\ \\ \\ \\ f(\vec{\imath}) \quad f(\vec{\jmath}) \quad f(\vec{k}) \end{array} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{array}{l} \vec{\imath} \\ \vec{\jmath} \\ \vec{k} \end{array}$$

On remarque que $f(\vec{\imath}) = \vec{\imath}$ donc $\vec{\imath}$ est un vecteur propre et 1 est une valeur propre. Soit $\lambda \in \mathbb{R}$.

$$\lambda \in \mathrm{Sp}(C) \iff \det(\lambda I_3 - C) = 0.$$

On calcule $\det(\lambda I_3 - C)$:

$$\begin{aligned}\det(\lambda I_3 - C) &= \begin{vmatrix} \lambda - 1 & 0 & 0 \\ 0 & \lambda & 1 \\ 0 & -1 & \lambda \end{vmatrix} \\ &= (\lambda - 1) \begin{vmatrix} \lambda & 1 \\ -1 & \lambda \end{vmatrix} \\ &= (\lambda - 1)(\lambda^2 + 1)\end{aligned}$$

Et donc

$$\lambda \in \mathrm{Sp}_{\mathbb{R}}(C) \iff \lambda = 1.$$

Attention : on ne peut pas en conclure que la matrice C n'est pas diagonalisable (il y a peut-être la même valeur propre 3 fois). On montre que la matrice C n'est pas diagonalisable dans $\mathbb{R}$ par l'absurde : si

$$P^{-1} \cdot C \cdot P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$$

alors, $C = P \cdot I_3 \cdot P^{-1} = I_3$, ce qui est absurde.

On cherche les valeurs propres dans $\mathbb{C}$. Soit $\lambda \in \mathbb{C}$.

$$\lambda \in \mathrm{Sp}_{\mathbb{C}}(C) \iff (\lambda - 1)(\lambda - i)(\lambda + i) = 0$$

et donc

$$\lambda \in \mathrm{Sp}_{\mathbb{C}}(C) \iff \lambda \in \{1, i, -i\} \qquad \text{i.e.} \qquad \mathrm{Sp}_{\mathbb{C}}(C) = \{1, i, -i\}.$$

On peut utiliser la PROPOSITION 18 (mais on la verra plus tard...). On utilise une autre méthode (que l'on doit utiliser à chaque fois que l'on doit

diagonaliser une matrice). Soit $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{M}_{3,1}(\mathbb{C})$.

$$\begin{aligned}
CX = iX &\iff \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = i \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\
&\iff \begin{cases} x = ix \\ -z = iy \\ y = iz \end{cases} \\
&\iff \begin{cases} x = 0 \\ z = -iy \\ y = iz \end{cases} \\
&\iff \begin{cases} x = 0 \\ y = iz \end{cases} \quad \text{car } L_2 = -iL_3 \\
&\iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ iz \\ z \end{pmatrix} = z \cdot \begin{pmatrix} 0 \\ i \\ 1 \end{pmatrix} \\
&\iff X \in \text{Vect} \begin{pmatrix} 0 \\ i \\ 1 \end{pmatrix}
\end{aligned}$$

De même, avec $-i$, on a

$$\begin{aligned}
CX = -iX &\iff \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -i \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\
&\iff \begin{cases} x = -ix \\ -z = -iy \\ y = iz \end{cases} \\
&\iff \begin{cases} x = 0 \\ z = iy \\ y = -iz \end{cases} \\
&\iff \begin{cases} x = 0 \\ y = -iz \end{cases} \\
&\iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ -iz \\ z \end{pmatrix} = z \cdot \begin{pmatrix} 0 \\ -i \\ 1 \end{pmatrix} \\
&\iff X \in \text{Vect} \begin{pmatrix} 0 \\ -i \\ 1 \end{pmatrix}
\end{aligned}$$

On pose $\varepsilon_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\varepsilon_2 = \begin{pmatrix} 0 \\ i \\ 1 \end{pmatrix}$ et $\varepsilon_3 = \begin{pmatrix} 0 \\ -i \\ 1 \end{pmatrix}$. De plus, $\det(\varepsilon_1, \varepsilon_2, \varepsilon_3) \neq 0$. D'où la matrice C est diagonalisable dans $\mathbb{C}$.

2. On considère la matrice

$$M = \begin{pmatrix} 7 & & & \sqrt{2} \\ & 7 & & \\ & & \ddots & \\ & & & 7 \end{pmatrix}.$$

La matrice M a pour polynôme caractéristique $\chi_M(x)$:

$$\chi_M(x) = \begin{vmatrix} x-7 & & & -\sqrt{2} \\ & x-7 & & \\ & & \ddots & \\ & & & x-7 \end{vmatrix} = (x-7)\cdot(x-7)\cdots(x-7) = (x-7)^n.$$

Or, $\lambda \in \mathrm{Sp}(M)$ si et seulement si $\chi_M(\lambda) = 0$ et donc si et seulement si $\lambda = 7$. D'où $\mathrm{Sp}(M) = \{7\}$. On procède par l'absurde : si M est diagonalisable, il existe $P \in \mathrm{GL}_n(\mathbb{K})$, telle que $M = P^{-1} \cdot 7I_n \cdot P = P^{-1} \cdot P \cdot 7I_n = 7I_n$, ce qui est absurde.

Remarque :
Si $A \in \mathscr{M}_{n,n}(\mathbb{R})$ (par exemple $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$), alors $\chi_A(X) \in \mathbb{R}_n[X]$ ($\chi_A(X) = X^2 + 1$, et donc $\mathrm{Sp}_{\mathbb{R}}(A) =$, mais $\mathrm{Sp}_{\mathbb{C}}(A) = \{-i, i\}$). Ainsi,

$$A \in \mathscr{M}_{n,n}(\mathbb{R}) \implies \forall \lambda \in \mathrm{Sp}_{\mathbb{C}}(A),\ \bar{\lambda} \in \mathrm{Sp}_{\mathbb{C}}(A).$$

Autrement dit, le spectre complexe d'une matrice réelle est stable par conjugaison. En effet, si $\lambda \in \mathrm{Sp}_{\mathbb{C}}(A)$, alors il existe $0 \neq X \in \mathscr{M}_{n,1}(\mathbb{C})$, tel $A \cdot X = \lambda X$. D'où

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \lambda \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \quad \text{et donc} \quad \begin{pmatrix} \bar{a}_{1,1} & \cdots & \bar{a}_{1,n} \\ \vdots & \ddots & \vdots \\ \bar{a}_{n,1} & \cdots & \bar{a}_{n,n} \end{pmatrix} \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{pmatrix} = \bar{\lambda} \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{pmatrix}.$$

Autrement dit, $A \cdot \bar{X} = \bar{\lambda}\bar{X}$ où $\bar{X} = \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{pmatrix}$. Or, $\bar{X} \neq 0$, et $A \cdot \bar{X} = \bar{\lambda}\bar{X}$. D'où $\bar{X}$ est un vecteur propre, et il est associé à $\bar{\lambda}$ qui est donc une valeur propre. Et même, $\dim \mathrm{SEP}(\lambda) = \dim \mathrm{SEP}(\bar{\lambda})$.

Proposition : Soit $A \in \mathscr{M}_{n,n}(\mathbb{K})$ une matrice carrée.

1. Le spectre de A continent au plus n valeurs propres distinctes deux à deux.
2. Pour chaque valeur propre $\lambda \in \mathrm{Sp}(A)$, on note m_λ la multiplicité de la racine λ dans le polynôme χ_A. Si le polynôme caractéristique est scindé alors

$$\mathrm{tr}\, A = \sum_{\lambda \in \mathrm{Sp}(A)} m_\lambda \cdot \lambda \qquad \text{et} \qquad \det A = \prod_{\lambda \in \mathrm{Sp}(A)} \lambda^{m_\lambda}.$$

3. La matrice A et sa transposée ont le même polynôme caractéristique : $\chi_{A^\top} = \chi_A$, et donc le même spectre $\mathrm{Sp}(A) = \mathrm{Sp}(A^\top)$.

—

Si la matrice A est diagonalisable, alors il existe un matrice inversible P telle que

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix} = P^{-1} \cdot A \cdot P$$

et donc $\operatorname{tr} A = \operatorname{tr} D = \sum_{i=1}^n \lambda_i$ et $\det A = \det D = \prod_{i=1}^n \lambda_i$. Mais, dans la proposition précédente, on n'a pas l'hypothèse que la matrice est diagonalisable. Ce raisonnement est un cas particulier de la proposition précédente. En effet, si A est diagonalisable alors $\chi_A = \chi_D$:

$$\begin{aligned} \chi_A(X) &= \chi_D(X) \\ \det(XI_n - A) &= \det(XI_n - D) \\ &= \det(XI_n - P^{-1}AP) \\ &= \det\left(P^{-1} \cdot (XI_n - A) \cdot P\right) \\ &= (X - \lambda_1) \cdots (X - \lambda_n) \end{aligned}$$

—

Preuve : 3. On calcule

$$\begin{aligned} \chi_{A^\top}(x) &= \det(xI_n - A^\top) \\ &= \det\left((xI_n - A)^\top\right) \\ &= \det(xI_n - A) \end{aligned}$$

car le déterminant est invariant par passage à la transposée. Or, comme $\chi_{A^\top} = \chi_A$, alors $\mathrm{Sp}(A) = \mathrm{Sp}(A^\top)$.

2. On sait d'après la proposition 6,

$$\chi_A(x) = x^n - \operatorname{tr}(A)\, x^{n-1} + \cdots + (-1)^n \det(A).$$

Or, par hypothèse, χ_A est scindé d'où

$$\chi_A(x) = (x - \lambda_1)(x - \lambda_n) \cdots (x - \lambda_n).$$

Les scalaires $\lambda_1, \dots, \lambda_n$ sont donc les valeurs propres de A. Ainsi, le coefficient devant le x^{n-1} est donc $-(\lambda_1 + \lambda_2 + \cdots + \lambda_n)$ et, le coefficient

devant le x^0 est donc $(-\lambda_1)(-\lambda_2)\cdots(-\lambda_n)$. D'où, par identification

$$\det(A) = \lambda_1 \cdot \lambda_2 \cdots \lambda_n \qquad \text{et} \qquad \mathrm{tr}(A) = \lambda_1 + \cdots + \lambda_n.$$

□

VII.4 Les sous-espaces propres

Définition : Soient E un sous-espace vectoriel et $u : E \to E$ un endomorphisme et λ une valeur propre de u. Le sous-espace vectoriel $\mathrm{Ker}(\lambda\,\mathrm{id}_E - u) = \mathrm{Ker}(u - \lambda\,\mathrm{id}_E)$ est appelé le *sous-espace propre* de u associé à la valeur propre λ. Il est parfois noté E_λ, ou $\mathrm{SEP}(\lambda)$.

Soit $X \in \mathcal{M}_{n,1}(\mathbb{K})$.

$$\begin{aligned} AX = \lambda X &\iff AX - \lambda X = 0 \\ &\iff (A - \lambda I_n)X = 0 \\ &\iff X \in \mathrm{Ker}(A - \lambda I_n) \end{aligned}$$

Attention, on ne dit pas que SEP(λ) est l'ensemble des vecteurs propres associés à la valeur propre λ. En effet, $0 \in \mathrm{SEP}(\lambda)$ mais 0 n'est pas un vecteur propre (par définition).

$\mathrm{SEP}(\lambda)$ est un sous-espace vectoriel de E. En effet, c'est un noyau. Autre méthode : $0 \in \mathrm{SEP}(\lambda)$ car $A \cdot 0 = \lambda 0$ et $\mathrm{SEP}(\lambda)$ est stable par combinaisons linéaires (superposition), car si X_1 et X_2 sont deux éléments de $\mathrm{SEP}(\lambda)$, alors

$$A(\alpha X_1 + \beta X_2) = \alpha\, A\, X_1 + \beta\, A\, X_2 = \alpha\lambda X_1 + \beta\lambda X_2 = \lambda(\alpha X_1 + \beta X_2).$$

Exercice :
On considère la matrice

$$B = \begin{pmatrix} 7 & 1 \\ 0 & 7 \end{pmatrix}.$$

Cherchons les valeurs propres de B :

$$\begin{aligned} \lambda \in \mathrm{Sp}(B) &\iff \det(\lambda I_2 - B) = 0 \\ &\iff \begin{vmatrix} \lambda - 7 & -1 \\ 0 & \lambda - 7 \end{vmatrix} = 0 \\ &\iff (\lambda - 7)^2 = 0. \end{aligned}$$

On en déduit que $\mathrm{Sp}(B) = \{7\}$. Soit $X = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathscr{M}_{2,1}(\mathbb{K})$.

$$\begin{aligned} X \in \mathrm{SEP}(7) &\iff B \cdot X = 7X \\ &\iff \begin{pmatrix} 7 & 1 \\ 0 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 7 \begin{pmatrix} x \\ y \end{pmatrix} \\ &\iff \begin{cases} 7x + y = 7x \\ 7y = 7y \end{cases} \\ &\iff y = 0 \\ &\iff X = \begin{pmatrix} x \\ 0 \end{pmatrix} = x \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

On en déduit que $\mathrm{SEP}(7) = \mathrm{Vect} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

On considère à présent la matrice D :

$$D = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \\ \vec{k} \end{matrix} \\ \begin{matrix} f(\vec{\imath}) & f(\vec{\jmath}) & f(\vec{k}) \end{matrix} \end{array}$$

Soit $\lambda \in \mathbb{K}$.

$$\begin{aligned} \lambda \in \mathrm{Sp}(D) &\iff \begin{vmatrix} \lambda - 1 & 0 & 0 \\ 0 & \lambda & -1 \\ 0 & -1 & \lambda \end{vmatrix} = 0 \\ &\qquad (\lambda - 1)(\lambda^2 - 1) = \\ &\qquad (\lambda - 1)(\lambda - 1)(\lambda + 1) = \\ &\qquad (\lambda - 1)^2(\lambda + 1) = \end{aligned}$$

D'où $\mathrm{Sp}(D) = \{1, -1\}$. Soit $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathscr{M}_{3,1}(\mathbb{K})$.

$$\begin{aligned} X \in \mathrm{SEP}(1) &\iff D \cdot X = 1X \\ &\iff \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\ &\iff \begin{cases} x = x \\ z = y \\ y = z \end{cases} \\ &\iff y = z \\ &\iff X = \begin{pmatrix} x \\ y \\ y \end{pmatrix} \\ &\iff X = x \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}}_{\varepsilon_1} + y \underbrace{\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}}_{\varepsilon_2}. \end{aligned}$$

Donc $\mathrm{SEP}(1) = \mathrm{Vect}(\varepsilon_1, \varepsilon_2)$. C'est un plan car $(\varepsilon_1, \varepsilon_2)$ est une famille libre. De même pour $\mathrm{SEP}(-1)$.

Remarque :
Soit $u : E \to E$ un endomorphisme d'un espace vectoriel E.

1. Si $0 \in \mathrm{Sp}(u)$, alors il existe un vecteur $\vec{x}$ non nul tel que $\vec{x} \in \mathrm{Ker}(u)$ et donc l'endomorphisme u n'est pas injectif.
2. Si $0 \notin \mathrm{Sp}(u)$, alors $\mathrm{Ker}(u) = \mathrm{SEP}(0) = \{0\}$ (car $\mathrm{SEP}(0) = \mathrm{Ker}(0\ \mathrm{id}_E - u) = \mathrm{Ker}\, u$) et donc l'endomorphisme u est injectif.

On en conclut que

$$u \text{ injectif} \iff 0 \notin \mathrm{Sp}(u).$$

En particulier, en dimension finie, une matrice A est inversible si et seulement si $0 \notin \mathrm{Sp}(A)$.

Exercice :
Dans cet exercice, E n'est pas forcément de dimension finie ; on ne passe donc pas par des matrices.

Remarque : l'application u est un *automorphisme*.

On compare les spectre de u et de u^{-1}. Soit $\lambda \in \mathbb{K}$.

$$\begin{aligned}
\lambda \in \mathrm{Sp}(u) &\iff \exists \vec{x} \in E,\ \vec{x} \neq \vec{0} \text{ et } u(\vec{x}) = \lambda \vec{x} \\
&\iff \exists \vec{x} \neq \vec{0},\ u^{-1}(u(\vec{x})) = \vec{x} = \lambda u^{-1}(\vec{x}) \text{ en appliquant } u^{-1} \\
&\iff \exists \vec{x} \neq \vec{0},\ \frac{1}{\lambda}\vec{x} = u^{-1}(\vec{x}) \\
&\iff \frac{1}{\lambda} \in \mathrm{Sp}(u^{-1})
\end{aligned}$$

On peut diviser car $\lambda \neq 0$ car $0 \notin \mathrm{Sp}(u)$ car u est injectif.

De plus,

$$\mathrm{Ker}(\lambda\, \mathrm{id} - u) = \mathrm{Ker}\left(\frac{1}{\lambda}\, \mathrm{id} - u^{-1}\right)$$

car le vecteur $\vec{x}$ ne change pas dans les équivalents précédents.

Proposition : Soit $u : E \to E$ un endomorphisme d'un espace vectoriel E. On a

$$\forall \lambda \in \mathrm{Sp}(u), \qquad 1 \leqslant \dim\ \mathrm{SEP}(\lambda) \leqslant m_\lambda$$

où m_λ est la multiplicité de la racine λ dans le polynôme caractéristique.

Preuve :
Tout d'abord, on sait que $\dim(\mathrm{SEP}(\lambda)) \geqslant 1$ car il existe un vecteur propre, donc un vecteur non nul dans $\mathrm{SEP}(\lambda)$.

De plus, si $\dim(\mathrm{SEP}(\lambda)) = d$, alors il existe $(\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_d)$ soit une base de $\mathrm{SEP}(\lambda)$. On peut compléter cette base de $\mathrm{SEP}(\lambda)$ en une base de E :

$(\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_d, \vec{e}_{d+1}, \dots, \vec{e}_n)$. Ainsi,

$$A \rightsquigarrow A' = \begin{pmatrix} \lambda & 0 & \dots & 0 & & \\ 0 & \ddots & \ddots & \vdots & & \\ \vdots & \ddots & \ddots & 0 & \star & \\ 0 & \dots & 0 & \lambda & & \\ & & & & & \\ & & 0 & & \star & \\ & & & & & \end{pmatrix} \begin{matrix} \vec{\varepsilon}_1 \\ \vec{\varepsilon}_2 \\ \vdots \\ \vec{\varepsilon}_d \\ \vec{e}_{d+1} \\ \vec{e}_{d+2} \\ \vdots \\ \vec{e}_n \end{matrix}$$

et donc

$$\begin{aligned} \chi_{A'}(x) &= \chi_A(x) \\ &= (x-\lambda)^d \times P(x) \\ &= (x-\lambda)^{m_\lambda} \times R(x) \text{ où } R(x) \text{ n'a pas de facteurs en } (x-\lambda) \end{aligned}$$

□

Proposition : Soit $u : E \to E$ un endomorphisme d'un espace vectoriel E. Si des valeurs propres sont distinctes deux à deux, alors les vecteurs propres associés sont libres. Autrement dit, les sous-espaces propres sont en somme directe.

Attention : les sous-espaces propres ne sont pas supplémentaires.

Preuve (méthode 1) *:*
Soit $\vec{x}_1 \in \text{SEP}(\lambda_1)$, $\vec{x}_2 \in \text{SEP}(\lambda_2), \dots, \vec{x}_r \in \text{SEP}(\lambda_r)$ tels que $\vec{x}_1 \neq \vec{0}$, $\vec{x}_2 \neq \vec{0}, \dots, \vec{x}_r \neq \vec{0}$. Ainsi $u(\vec{x}_1) = \lambda_1 \vec{x}_1$, $u(\vec{x}_2) = \lambda_2 \vec{x}_2, \dots$, et $u(\vec{x}_r) = \lambda_r \vec{x}_r$. Soient $\alpha_1, \dots, \alpha_r \in \mathbb{K}$. On suppose $\alpha_1 \vec{x}_1 + \dots + \alpha_r \vec{x}_r = \vec{0}$ (L_1). Alors,

$$u(\alpha_1 \vec{x}_1 + \dots + \alpha_r \vec{x}_r = \vec{0}) = u(\vec{0}) = \vec{0}$$

d'où $\alpha\lambda_1 \vec{x}_1 + \alpha_2 \lambda_2 \vec{x}_2 + \dots + \alpha_r \lambda_r \vec{x}_r = \vec{0}$ (L_2). D'où, en calculant $L_2 - \lambda_r L_1$, on a

$$\alpha_1(\lambda_1 - \lambda_r)\vec{x}_1 + \alpha_2(\lambda_2 - \lambda_r)\vec{x}_2 + \dots + \alpha_{r-1}(\lambda_{r-1} - \lambda_r)\vec{x}_{r-1} = \vec{0}.$$

Par récurrence, pour $r = 1$, c'est vrai : la famille $(\vec{x}_1)$ est libre. On suppose la propriété vraie pour $r-1$ vecteurs. On veut le prouver pour r vecteurs. En utilisant le calcul ci-dessus, comme les valeurs propres sont distinctes deux à deux, on en déduit que $\alpha_1 = \alpha_2 = \dots = \alpha_{r-1} = 0$. Or, d'après L_1, $\alpha_r = 0$. □

Preuve (méthode 2) *:*
On sait que $\mathrm{SEP}(\lambda_1) = \mathrm{Ker}(\lambda_1 \,\mathrm{id} - u)$, $\mathrm{SEP}(\lambda_2) = \mathrm{Ker}(\lambda_2 \,\mathrm{id} - u), \dots$ Or, $\lambda_2 \,\mathrm{id} - u$ est un polynôme $P_1(u)$, et de même pour $P_2(u), P_3(u), \dots$ Les r polynômes sont premiers entre-eux car λ_1, λ_2, …, λ_r sont distinct deux à deux. D'où, d'après le lemme des noyaux,

$$\mathrm{Ker}\Big(P(u)\Big) = \bigoplus_{k=1}^{n} \mathrm{Ker}\left(P_k(u)\right)$$

où $P = P_1 \times P_2 \times \cdots \times P_r$. La somme des sous-espaces propres est donc directe. □

Exercice :
Soient $\lambda_1, \dots, \lambda_r \in \mathbb{R}$ distincts deux à deux. Montrons que, si $\forall x \in \mathbb{R}$, $\alpha_1 \mathrm{e}^{\lambda_1 x} + \cdots + \alpha_r \mathrm{e}^{\lambda_r x} = 0$, alors $\alpha_1 = \cdots = \alpha_r$. On peut procéder de différentes manières : le déterminant de Vandermonde, par analyse-sythèse, ou, en utilisant

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\mathrm{e}^{\lambda_k x}\right) = \lambda_k \mathrm{e}^{\lambda_k x}, \quad \text{d'où} \quad \varphi(f_k) = \lambda_k f_k, \text{ avec } f_k : x \mapsto \mathrm{e}^{\lambda_k x} \quad \text{et} \quad \varphi : f \mapsto f'.$$

On doit vérifier que les f_k sont des vecteurs et l'application φ soit un endomorphisme. On se place donc dans l'espace vectoriel $\mathscr{C}^\infty$. (On ne peut pas se placer dans l'espace $\mathscr{C}^k$, car sinon l'application φ est de l'espace $\mathscr{C}^k$ à $\mathscr{C}^{k-1}$, ce n'est donc pas un endomorphisme ; ce n'est pas le cas pour l'espace $\mathscr{C}^\infty$.) Or, les λ_k sont distincts deux à deux d'où les vecteurs propres f_k sont linéairement indépendants. Et donc si $\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_r f_r = 0$ alors $\alpha_1 = \cdots = \alpha_r = 0$. Mais, comme $\forall x \in \mathbb{R}$, $\alpha_1 f_1(x) + \alpha_2 f_2(x) + \cdots + \alpha_r f_r(x) = 0$, on en déduit que

$$\boxed{\alpha_1 = \cdots = \alpha_r = 0.}$$

VII.5 Critères de diagonalisabilité

Proposition (une condition suffisante pour qu'une matrice soit diagonalisable) **:** Soit A une matrice carrée de taille $n \geqslant 2$. Si A possède n valeurs propres distinctes deux à deux, alors A est diagonalisable.

La réciproque est fausse : par exemple, pour $n > 1$, $7I_n$ est diagonalisable car elle est diagonale. Mais, elle ne possède pas n valeurs propres distinctes deux à deux.

Preuve :
On suppose que la matrice $A \in \mathscr{M}_{n,n}(\mathbb{K})$ possède n valeurs propres distinctes deux à deux (i.e. $\mathrm{Card}\,\mathrm{Sp}(A) = n$). D'où, d'après la proposition 16, les n vecteurs propres associés $\varepsilon_1, \dots, \varepsilon_n$ sont libres. D'où $(\varepsilon_1, \dots, \varepsilon_n)$ est une base formée de vecteurs propres. Donc, d'après la définition 5, la matrice A est diagonalisable. □

Théorème (conditions nécessaires et suffisantes pour qu'une matrice soit diagonalisable) **:** Soient E un espace vectoriel de dimension finie et $u : E \to E$ un endomorphisme. Alors,

$$\begin{aligned}(1)\quad u \text{ diagonalisable} &\iff E = \bigoplus_{\lambda\in \mathrm{Sp}(u)} \mathrm{Ker}(\lambda\,\mathrm{id}_E - u) \quad (2)\\ &\iff \dim E = \sum_{\lambda\in \mathrm{Sp}(u)} \dim(\mathrm{SEP}(\lambda)) \quad (3)\\ &\iff \chi_u \text{ scindé et } \forall \lambda \in \mathrm{Sp}(u),\ \dim(\mathrm{SEP}(\lambda)) = m_\lambda \quad (4)\end{aligned}$$

où m_λ est la multiplicité de la racine λ du polynôme χ_u.

"(1) ~~$\Longrightarrow$~~ (2)" On suppose u diagonalisable. Il existe donc une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de E formée de vecteurs propres de u. On les regroupes par leurs valeurs propres : $(\varepsilon_i, \ldots, \varepsilon_{i+j})$ forme une base de $\mathrm{SEP}(\lambda_k)$. D'où la base $(\varepsilon_1, \ldots, \varepsilon_n)$ de l'espace vectoriel E est une concaténation des bases des sous-espaces propres de u. D'où

$$E = \bigoplus_{\lambda\in \mathrm{Sp}(u)} \mathrm{SEP}(\lambda).$$

"(2) $\Longrightarrow$ (1)" On suppose que $E = \mathrm{SEP}(\lambda_1) \oplus \mathrm{SEP}(\lambda_2) \oplus \cdots \oplus \mathrm{SEP}(\lambda_r)$. Soient $(\varepsilon_1, \ldots, \varepsilon_{d_1})$ une base de $\mathrm{SEP}(\lambda_1)$, $(\varepsilon_{d_1+1}, \ldots, \varepsilon_{d_1+d_2})$ une base de $\mathrm{SEP}(\lambda_2)$, $\ldots$, $(\varepsilon_{d_1+\cdots+d_{r-1}+1}, \ldots, \varepsilon_{d_1+\cdots+d_r})$ une base de $\mathrm{SEP}(\lambda_r)$. En concaténant ces base, on obtient une base de E, d'après l'hypothèse. Dans cette base, tous les vecteurs sont propres donc u est diagonalisable.

"(2) $\Longrightarrow$ (3)" On suppose $E = \mathrm{SEP}(\lambda_1) \oplus \mathrm{SEP}(\lambda_2) \oplus \cdots \oplus \mathrm{SEP}(\lambda_r)$. D'où

$$\dim E = \dim(\mathrm{SEP}(\lambda_1)) + \dim(\mathrm{SEP}(\lambda_2)) + \cdots + \dim(\mathrm{SEP}(\lambda_r))$$

car la dimension d'une somme directe est égale à la somme des dimensions.

"(3) $\Longrightarrow$ (1)" On suppose $\dim E = \dim(\mathrm{SEP}(\lambda_1)) + \dim(\mathrm{SEP}(\lambda_2)) + \cdots + \dim(\mathrm{SEP}(\lambda_r))$. Or, les sous-espaces propres sont en somme directe, d'après la proposition 16. D'où $\dim\left(\sum_{\lambda\in \mathrm{Sp}(u)} \mathrm{SEP}(\lambda)\right) = \sum_{\lambda\in \mathrm{Sp}(u)} \dim(\mathrm{SEP}(\lambda))$. Donc $\sum_{\lambda\in \mathrm{Sp}(u)} \mathrm{SEP}(\lambda) = E$.

"(4) $\Longrightarrow$ (3)" On suppose (a) χ_u scindé et (b) $\dim(\mathrm{SEP}(\lambda)) = m_\lambda$. D'où, d'après (a) :

$$\chi_u(x) = (x-\lambda_1)^{m_{\lambda_1}}(x-\lambda_2)^{m_{\lambda_2}}\cdots(x-\lambda_r)^{m_{\lambda_r}} = x^n + \cdots$$

d'où $m_{\lambda_1} + m_{\lambda_2} + \cdots + m_{\lambda_r} = n$, et d'où

$$\dim(\mathrm{SEP}(\lambda_1)) + \dim(\mathrm{SEP}(\lambda_2)) + \cdots + \dim(\mathrm{SEP}(\lambda_r)) = n$$

d'après l'hypothèse (b).

"(1) $\Longrightarrow$ (4)" On suppose u diagonalisable. D'où, dans une certaine base $\mathscr{B}$, la matrice $[u]_{\mathscr{B}}$ est diagonale. Quitte à changer l'ordre des éléments de $\mathscr{B} = (\varepsilon_1, \dots, \varepsilon_r)$, on peut supposer que $[u]_{\mathscr{B}}$ est de la forme

$$[u]_{\mathscr{B}} = \left[\begin{array}{ccc|ccc|c|ccc|l}
\lambda_1 & & & & & & & & & & \varepsilon_1 \\
& \lambda_1 & & & & & & & & & \varepsilon_2 \\
& & \ddots & & 0 & & 0 & & 0 & & \vdots \\
& & & \lambda_1 & & & & & & & \varepsilon_{d_1} \\
\hline
& & & \lambda_2 & & & & & & & \varepsilon_{d_1+1} \\
& & & & \lambda_2 & & & & & & \varepsilon_{d_1+2} \\
& 0 & & & & \ddots & 0 & & 0 & & \vdots \\
& & & & & & \lambda_2 & & & & \varepsilon_{d_1+d_2} \\
\hline
& & & & & & \ddots & & & & \vdots \\
\hline
& & & & & & & \lambda_r & & & \varepsilon_{d_1+\cdots+d_{r-1}+1} \\
& & & & & & & & \lambda_r & & \varepsilon_{d_1+\cdots+d_{r-1}+2} \\
& 0 & & & 0 & & 0 & 0 & & \ddots & \vdots \\
& & & & & & & & & \lambda_r & \varepsilon_{d_1+\cdots+d_r}
\end{array}\right].$$

D'où $\forall k \in [\![1, r]\!]$, $d_k = \dim(\mathrm{SEP}(\lambda_k))$. En outre, $\chi_u(x) = \det(x\,\mathrm{id} - u) = (x - \lambda_1)^{d_1} \cdot (x - \lambda_2)^{d_2} \cdots (r - \lambda_r)^{d_r}$. D'où $\forall k \in [\![1, r]\!]$, $d_k = m_{\lambda_k}$ et χ_u est scindé.

□

Exercice :
On considère la matrice E ci-dessous

$$E = \begin{pmatrix} 7 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix}.$$

La matrice E ci-dessous est-elle diagonalisable ?

Soit $\lambda \in \mathbb{R}$. On sait que $\lambda \in \mathrm{Sp}(E)$ si et seulement si $\det(\lambda I_3 - E) = 0$. Or

$$\det(\lambda I_3 - E) = \begin{vmatrix} \lambda - 7 & 0 & -1 \\ 0 & \lambda - 3 & 0 \\ 0 & 0 & \lambda - 7 \end{vmatrix} = (\lambda - 7)^2 \cdot (\lambda - 3)^1.$$

Donc $\mathrm{Sp}(E) = \{3, 7\}$, $1 \leqslant \dim\big(\mathrm{SEP}(3)\big) \leqslant 1$, et $1 \leqslant \dim\big(\mathrm{SEP}(7)\big) \leqslant 2$. La matrice E est diagonalisable si et seulement si $\dim(\mathrm{SEP}(3)) + \dim(\mathrm{SEP}(7)) = 3$, donc si et seulement si $\dim(\mathrm{SEP}(7)) = 2$. On cherche donc la dimension de ce

sous-espace propre : soit $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{M}_{3,1}(\mathbb{R})$. On sait que

$$\begin{aligned} X \in \mathrm{SEP}(7) &\iff E \cdot X = 7X \\ &\iff \begin{pmatrix} 7 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 7 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\ &\iff \begin{cases} 7x + 0y + 1z = 7x \\ 3y = 7y \\ 7z = 7z \end{cases} \\ &\iff \begin{cases} z = 0 \\ y = 0 \end{cases} \\ &\iff X = \begin{pmatrix} x \\ 0 \\ y \end{pmatrix} = x \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}}_{\varepsilon_1} \end{aligned}$$

Donc $\mathrm{SEP}(7) = \mathrm{Vect}(\varepsilon_1)$, d'où $\dim(\mathrm{SEP}(7)) = 1$. Donc la matrice E n'est pas diagonalisable.

VII.6 Trigonalisation

Trigonaliser une matrice ne sert que si la matrice n'est pas diagonalisable.

Définition : On dit d'une matrice carrée $A \in \mathcal{M}_{n,n}(\mathbb{K})$ qu'elle est *trigonalisable* s'il existe une matrice inversible P telle que $P^{-1} \cdot A \cdot P$ est triangulaire :

$$P^{-1} \cdot A \cdot P = \begin{pmatrix} \lambda_1 & \ddots & \star \\ & \ddots & \ddots \\ 0 & & \lambda_r \end{pmatrix}.$$

Remarque :

Théorème : Une matrice carrée $A \in \mathcal{M}_{n,n}(\mathbb{K})$ est trigonalisable si et seulement si son polynôme caractéristique $\chi_A \in \mathbb{K}[X]$ est scindé.

Preuve (par récurrence sur n, la largeur de la matrice) *:*
- Si $n = 1$, alors la matrice $A = (a_{11})$ est déjà triangulaire.
- On suppose le polynôme caractéristique χ_A de la matrice scindé dans $\mathbb{K}[X]$, d'où il a au moins une racine dans $\mathbb{K}$. D'où, la matrice A a au moins une valeur propre $\lambda_1 \in \mathbb{K}$. Il existe donc un vecteur non nul $\vec{\varepsilon}_1$ tel que $A \cdot \vec{\varepsilon}_1 = \lambda_1 \vec{\varepsilon}_1$. On complète $(\vec{\varepsilon}_1)$ en une base de $\mathbb{K}^n$:

$(\vec{\varepsilon}_1, \vec{e}_2, \dots, \vec{e}_n)$. En changent de base, il existe une matrice inversible P telle que

$$A' = P^{-1} \cdot A \cdot P = \left(\begin{array}{c|c} \lambda_1 & \star \dots \dots \dots \star \\ \hline 0 \\ \vdots & B \\ 0 \end{array}\right) \begin{matrix} \varepsilon_1 \\ e_1 \\ \vdots \\ e_n \end{matrix}$$
$$\begin{matrix} f(\vec{\varepsilon}_1) & f(\vec{e}_1) & \dots & f(\vec{e}_n) \end{matrix}$$

Comme le polynôme caractéristique est invariant par changement de base, on en déduit que

$$\chi_A(x) = \chi_{A'}(x) = \left|\begin{array}{c|c} x-\lambda_1 & \star \\ \hline 0 & xI_{n-1} - B \end{array}\right| = (x-\lambda_1) \cdot \Pi(x).$$

Or, comme χ_A est scindé, $\Pi(x)$ est aussi scindé. Or, $\Pi(x) = \det(xI_{n-1} - B)$ d'où B est trigonalisable.

□

Corollaire : Toute matrice de $\mathcal{M}_{n,n}(\mathbb{C})$ est trigonalisable.

Exercice :
Soit une matrice carrée $A \in \mathcal{M}_{n,n}(\mathbb{K})$ (où $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$). Montrer que

(1) *la matrice A est nilpotente* $\iff$ *le polynôme caractéristique de A est $\chi_A(X) = X^n$* (2)
$\iff$ *la matrice A est trigonalisable avec des zéros sur sa diagonale* (3)

On montre " (1) $\implies$ (2), " " (2) $\implies$ (3) " puis " (3) $\implies$ (1)."

" (3) $\implies$ (1) " Il existe donc une matrice inversible P telle que $T = P^{-1} \cdot A \cdot P$ et T est une matrice trigonalisable. Or, à chaque produit $A^n \cdot A$, une « sur-diagonalse » de zéros supplémentaires. D'où, à partir d'un certain rang p, on a $A^p = 0$. La matrice A est donc nilpotente.

" (2) $\implies$ (3) " On sait que $\chi_A = X^n = (X-0)^n$ est scindé, d'où A est trigonalisable. Il existe donc une matrice inversible P telle que

$$P^{-1} \cdot A \cdot P = A' = \begin{pmatrix} \lambda_1 & \star & \dots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}.$$

Et donc $\chi_{A'}(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$. Or, le polynôme caractéristique est invariant par changement de base, d'où $\lambda_1 = \lambda_2 = \cdots = \lambda_n$.

" (1) $\Longrightarrow$ (2) " On passe dans $\mathbb{C}$ alors χ_A est scindé dans $\mathbb{C}$. D'où, il existe $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{C}^n$ tels que

$$\chi_A(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n).$$

D'où, chaque λ_i est une valeur propre complexe de la matrice A. Or A est nilpotente, d'où, par définition, il existe $p \in \mathbb{N}$ tel que $A^p = 0$. Les scalaires λ_i sont dans le spectre de A : en effet, il existe un vecteur colonne X non nul tel que $A \cdot X = \lambda_i X$, d'où $A^2 \cdot X = A \cdot AX = A \cdot \lambda_i X = \lambda_i^2 X$. De même, $A^3 \cdot X = A \cdot A^2 \cdot X = A \cdot \lambda_i^2 X = \lambda_i^2 (A \cdot X) = \lambda_i^3 X$. Et, de « proche en proche », on a donc

$$\forall k \in \mathbb{N},\ A^k \cdot X = \lambda_i^k X.$$

En particulier, si $k = p$, on a $0 = 0 \cdot X = A^p \cdot X = \lambda_i^p X$. D'où $\lambda_i^p X = 0$. Or, $X \neq 0$, d'où $\lambda_i^p = 0$ et donc $\lambda_i = 0$. Finalement, $\chi_A(X) = (X - \lambda_1) \cdots (X - \lambda_n) = (X - 0) \cdots (X - 0) = X^n \in \mathbb{C}[X]$. On a donc $\chi_A(X) \in \mathbb{R}[X]$.

VII.7 Le théorème de Cayley & Hamilton et les sous-espaces caractéristiques

Théorème (de Cayley & Hamilton) **:** Le polynôme caractéristique d'une matrice $A \in \mathscr{M}_{n,n}(\mathbb{K})$ est un polynôme annulateur de cette matrice :

$$\chi_A(A) = 0.$$

□

Rappel :
Un polynôme P est annulateur de la matrice A si et seulement si P divise μ_A.

Corollaire : Le polynôme minimal divise le polynôme caractéristique.

Exercice :
Déterminer le polynôme minimal de la matrice E de l'exercice 20 :

$$E = \begin{pmatrix} 7 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix}.$$

On doit donc déterminer le polynôme unitaire de degré minimal annulateur de E. D'après le théorème de Cayley & Hamilton, χ_E est un polynôme annulateur. Or, $\chi_E(X) = (X-7)^2 (X-3)$ car c'est un déterminant triangulaire. D'où $\mu_E(X)$ est égal à $(X - 7)^2 (X - 3)$ ou $(X - 7)(X - 3)$ ou $(X - 7)^2$ ou

$(X-7)$ ou $(X-3)$. Or,

$$(E-7I_3)\cdot(E-3I_3)=\begin{pmatrix}0&0&1\\0&-4&0\\0&0&0\end{pmatrix}\cdot\begin{pmatrix}4&0&1\\0&0&0\\0&0&4\end{pmatrix}$$
$$=\begin{pmatrix}\star&\star&4\\\star&\star&\star\\\star&\star&\star\end{pmatrix}\neq 0_{\mathcal{M}_{3,3}(\mathbb{K})}$$

Ainsi, $\mu_A(X)\neq(X-7)(X-3)$ et $\mu_A(X)\neq(X-7)$. Et,

$$(E-3I_3)^2=\begin{pmatrix}0&0&1\\0&-4&0\\0&0&0\end{pmatrix}^2=\begin{pmatrix}\star&\star&\star\\\star&16&\star\\\star&\star&\star\end{pmatrix}\neq 0_{\mathcal{M}_{3,3}(\mathbb{K})}.$$

Ainsi, $\mu_A(X)\neq(X-3)^2$ et aussi $\mu_A(X)\neq(X-3)$. On en déduit que $\mu_A=\chi_E$.

Définition : Si le polynôme caractéristique d'une matrice $A\in\mathcal{M}_{n,n}(\mathbb{K})$ est scindé, alors le *sous-espace caractéristique* de A associé à chaque valeur propre λ est

$$C_\lambda=\mathrm{Ker}(\lambda I_n-A)^{m_\lambda},$$

où m_λ est la multiplicité de la racine λ dans le polynôme caractéristique.

Proposition : Les sous-espaces caractéristiques sont supplémentaires :

$$E=\bigoplus_{\lambda\in\mathrm{Sp}(A)}C_\lambda$$

et de dimensions $\dim C_\lambda=m_\lambda$.

Preuve :
Comme le polynôme χ_A est scindé, alors

$$\chi_A(X)=(X-\lambda_1)^{m_{\lambda_1}}\times\cdots\times(X-\lambda_r)^{m_{\lambda_r}}$$

et donc, d'après le théorème des noyaux,

$$\mathrm{Ker}\left(\chi_A(M)\right)=\bigoplus_{\lambda\in\mathrm{Sp}(A)}\mathrm{Ker}\left(M-\lambda I_n\right)^{m_\lambda}$$

car les polynômes $(X-\lambda_i)$ sont premiers deux à deux. En particulier, si $M=A$, alors

$$E=\bigoplus_{\lambda\in\mathrm{Sp}(A)}\overbrace{\mathrm{Ker}\left((\lambda I_n-A)^{m_\lambda}\right)}^{\text{sous-espace caractéristique de } A \text{ associé à } \lambda\,:\,C_\lambda}.$$

□

VII.8 Polynômes annulateurs

Si $\vec{x} \in E$ est un vecteur propre de $u \in \mathscr{L}(E)$, associé à la valeur propre $\lambda \in \mathbb{K}$, alors

$$u^2(\vec{x}) = u\big(u(\vec{x})\big) = u(\lambda\vec{x}) = \lambda u(\vec{x}) = \lambda^2\vec{x}.$$

Ainsi, par récurrence,

$$\forall k \in \mathbb{N}^\star, \quad u^k(\vec{x}) = \lambda^k\,\vec{x}.$$

Mais, comme $u^0 = \mathrm{id}_E$, on a donc $u^0(\vec{x}) = \mathrm{id}_E(\vec{x}) = \vec{x} = \lambda^0\,\vec{x}$, et le résultat précédent est également vrai pour $k = 0$. Par linéarité, si $P(X) = a_0 + a_1X + \cdots + a_dX^d$, alors $P(u) = a_0\,\mathrm{id}_E + a_1u + \cdots + a_du^d$, et donc $P(u)(\vec{x}) = a_0\vec{x} + a_1\lambda\vec{x} + \cdots + a_d\lambda^d\vec{x} = P(\lambda)\,\vec{x}$.

Proposition (très souvent utile) **:** Soit $P \in \mathbb{K}[X]$ un polynôme annulateur de $u \in \mathscr{L}(E)$. Si λ est une valeur propre de u (i.e. $P(u) = 0$), alors λ est racine de P :

$$\forall \lambda \in \mathbb{K}, \qquad \lambda \in \mathrm{Sp}(u) \quad \not\Longleftrightarrow \quad P(\lambda) = 0.$$

Autrement dit, le spectre de u est inclus dans l'ensemble des racines d'un polynôme annulateur de u. Mais, en général, il n'y a pas égalité.

La réciproque de la proposition est fausse. Par exemple, $(X-1)(X-7)$ est annulateur de I_n, mais $\mathrm{Sp}(I_n) = \{1\} \subsetneq \{1, 7\}$, qui est l'ensemble des racines de $(X-1)(X-7)$.

Preuve :
Si $\vec{x}$ est un vecteur propre de u associé à la valeur propre λ (i.e. $\vec{x} \neq \vec{0}$ et $u(\vec{x}) = \lambda\vec{x}$), alors $P(\lambda) = 0$ car $\vec{x} \neq \vec{0}$. □

Néanmoins, il y a égalité pour certains polynômes : le polynôme caractéristique (d'après le théorème 7), et le polynôme minimal (dans la proposition 32, suivante).

Proposition : Le spectre de u est égal à l'ensemble des racines du polynôme minimal (qui a donc les même racines que le polynôme caractéristique).

Méthode 1 (à l'aide du théorème de Cayley et Hamilton) On veut montrer que le polynôme caractéristique et le polynôme minimal ont les même racines.

— Tout d'abord, On sait que le polynôme minimal divise le polynôme caractéristique. Ainsi, il existe un polynôme Q, tel que $\chi_A(X) = \mu_A(X) \times Q(X)$. Ainsi, toute racine du polynôme minimal μ_A est aussi racine du polynôme caractéristique χ_A.

— Puis, soit λ une racine de χ_A. D'où λ est une valeur propre de A. D'où $\lambda \in \mathrm{Sp}(A)$. Or, le spectre de A est inclus dans l'ensemble des racines de μ_A car μ_A est polynôme annulateur (d'après la proposition 31). D'où λ est racine de μ_A.

Méthode 2 (sans le théorème de Cayley et Hamilton)

— La démonstration précédente n'utilisant pas, dans ce sens là, le théorème de Cayley et Hamilton. On sait donc que l'ensemble des racines de χ_A est inclus dans l'ensemble des racines de μ_A.

— Reste à montrer l'autre inclusion : l'ensemble des racines de μ_A est inclus dans l'ensemble des racines de χ_A, qui est le spectre de A. Soit λ une racine de μ_A. Alors, il existe un polynôme Q, tel que $\mu_A(X) = (X - \lambda) \times Q(X)$. D'où $0_{\mathcal{M}_{n,n}(\mathbb{K})} = \mu_A(A) = (A - \lambda I_n) \times Q(A)$. Or, $Q(A) \neq 0_{\mathcal{M}_{n,n}(\mathbb{K})}$. En effet, si $Q(A) = 0_{\mathcal{M}_{n,n}(\mathbb{K})}$, alors, comme $\deg Q < \deg \mu_A$, on a donc un polynôme annulateur de A ayant un degré plus petit celui du polynôme minimal : ce qui est absurde. Il existe donc $X \in \mathcal{M}_{n,n}(\mathbb{K})$ tel que $Q(A) \cdot X \neq 0$. Soit U ce vecteur : $U = Q(A) \cdot X$. Alors, comme $(A - \lambda I_n) \times Q(A) = 0_{\mathcal{M}_{n,n}(\mathbb{K})}$, on en déduit que $(A - \lambda I_n) \cdot Q(A) \cdot X = 0 \cdot X$. D'où $(A - \lambda I_n) \cdot U = 0$, et donc $A \cdot U = \lambda U$, et comme $U \neq 0$, on en déduit que $\lambda \in \mathrm{Sp}(A)$.

□

Théorème : Une matrice A est

1. trigonalisable si et seulement si elle possède un polynôme annulateur scindé ;
2. diagonalisable si et seulement si elle possède un polynôme annulateur scindé à racines simples.

Rappel :
Une matrice A est trigonalisable si et seulement si

— χ_A scindé (théorème 3) ;
— elle possède un polynôme annulateur scindé (théorème 33).

Une matrice A est diagonalisable si et seulement si

— $\sum_{\lambda \in \mathrm{Sp}(A)} \dim(\mathrm{SEP}(\lambda))$ est la taille de la matrice A (théorème 19) ;
— les sous-espaces propres sont supplémentaires ;
— χ_A est scindé et $\forall \lambda \in \mathrm{Sp}(A)$, $\dim(\mathrm{SEP}(\lambda)) = m_\lambda$;
— elle possède un polynôme annulateur scindé à racines simples (théorème 33).

Une matrice A est diagonalisable si $\mathrm{Card}(\mathrm{Sp}(A))$ est la taille de la matrice A.

Exercice :
Soit $n \geqslant 2$. Montrer que la matrice

$$J = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & 0 \end{pmatrix} \in \mathscr{M}_{n,n}(\mathbb{K})$$

est diagonalisable, déterminer son spectre et ses sous-espaces propres.

Secret (pour plus tard) la matrice J est symétrique, donc diagonalisable.

On remarque que $J \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = (n-1) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, et $J + I_n = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$, d'où $\operatorname{rg}(J + I_n) = 1$, et donc d'après le théorème du rang, $\dim \operatorname{Ker}(J + I_n) = n - 1 = \dim \operatorname{Ker}(J - \lambda I_n)$, avec $\lambda = -1$. D'où $\dim \operatorname{SEP}_J(-1) + \dim \operatorname{SEP}_j(n-1) = n$ qui est la taille de J donc J est diagonalisable.

Autre méthode : on a déjà fait ça au chapitre II. :

$$(J + I_n)^2 = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}^2 = \begin{pmatrix} n & \dots & n \\ \vdots & \ddots & \vdots \\ n & \dots & n \end{pmatrix} = n(I_n + J).$$

D'où $I_n + 2J + J^2 = nI_n + nJ$. D'où $J^2 - (n-2)J - (n-1)I_n = 0$. Ainsi le polynôme $P(X) = X^2 - (n-2)X - (n-1)$ est annulateur de la matrice J. Or, $P(X) = (X+1)\big(X - (n-1)\big)$ est scindé à racines simples. D'où la matrice J est diagonalisable.

D'où $\operatorname{Sp}(J) \subset \{-1, n-1\}$.

...

VII.9 Stabilité

Rappel :
Un sous-espace vectoriel F de E est stable par un endomorphisme $u : E \to E$ si et seulement si

$$\forall \vec{x} \in E,\ \vec{x} \in F \implies u(\vec{x}) \in F \qquad \text{i.e.} \qquad u(F) \subset F.$$

Alors, $u\big|_F$ est l'endomorphisme induit par u sur F, ceci est parfois noté $u\big|_F^F$: $F \to F$.

Proposition : Soit E un $\mathbb{K}$-espace vectoriel. Soit $\vec{a} \in E$ non nul, et $u : E \to E$ un endomorphisme.

Si la droite $\operatorname{Vect}(\vec{a})$ est stable par l'endomorphisme u alors il existe $\lambda \in \mathbb{K}$ tel que $u(\vec{a}) = \lambda \vec{a}$, et donc $\vec{a}$ est un vecteur propre de u.

Réciproquement, si $\vec{a}$ est un vecteur propre de u, alors il existe $\lambda \in \mathbb{K}$ tel que $u(\vec{a}) = \lambda\vec{a}$.

Preuve :
Soit $\vec{x} \in \text{Vect}(\vec{a})$. Ainsi, il existe $\alpha \in \mathbb{K}$ tel que $\vec{x} = \alpha\vec{a}$. D'où $u(\vec{x}) = u(\alpha\vec{a}) = \alpha u(\vec{a}) = \alpha\lambda\vec{a}$ par hypothèse. D'où $u(\vec{x}) \in \text{Vect}(\vec{a})$ et donc $\text{Vect}(\vec{a})$ est stable par u. □

Exercice (Tarte à la crème) :
Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, et $u : E \to E$ un endomorphisme. Montrons qu'il existe une droite ou un plan stable par u.

On utilise le théorème de Cayley et Hamilton (valable en dimension finie). Soit $A = \left[u\right]_{\mathcal{B}}$, où $\mathcal{B}$ est une base de l'espace vectoriel. Alors, $\chi_A(A) = 0$. On le « casse en petits bouts » :

$$\chi_A(X) = (X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}(X^2+b_1X+c_1)^{n_1} \cdots (X^2+b_\diamond X+c_\diamond)^{n_\diamond}.$$

Le produit $\chi_A(A)$ est un produit de matrices, ce produit est la matrice nulle, d'où ce produit n'est pas inversible, d'où l'un des facteurs n'est pas inversible.

- Ou bien, ce facteur est la forme $(A-\lambda_i I_n)$, et donc il existe $X \in \mathcal{M}_{n,1}(\mathbb{R})$ non nul tel que $(A-\lambda_i I_n)\cdot X = 0$. Alors $A \cdot X = \lambda_i X$ et $X \neq 0$. D'où la droite dirigée par ce vecteur $\text{Vect}(X)$ est stable.
- Ou bien, ce facteur est la forme $(A^2+b_iA+c_iI_n)$, et donc il existe $X \in \mathcal{M}_{n,1}(\mathbb{R})$ non nul tel que $A^2\cdot X + b_iA\cdot X + c_iX = 0$. Autrement dit, il existe un vecteur $\vec{x} \in E$ non nul, tel que $u^2(\vec{x}) + b_iu(\vec{x}) + c_i\vec{x} = \vec{0}$. D'où les vecteurs $\vec{x}$ et $u(\vec{x})$ [1]sont libres, et le plan $\text{Vect}(\vec{x}, u(\vec{x}))$ est stable par u. En effet, $u(\vec{x}) \in \text{Vect}(\vec{x}, u(\vec{x}))$, et $u(u(\vec{x})) = -b_iu(\vec{x}) - c_i\vec{x} \in \text{Vect}(\vec{x}, u(\vec{x}))$.

Rappel :
Au chapitre II. on a montré que, si deux endomorphismes u et v commutent, alors $\text{Ker}\, u$ et $\mathfrak{Im}u$ sont stables par v.

Proposition : Soient u et v deux endomorphisme d'un $\mathbb{K}$-espace vectoriel E. Si u et v commutent ($u \circ v = v \circ u$), alors les sous-espaces propres de u sont stables par v.

Preuve :
Or, $\text{SEP}_u(\lambda) = \text{Ker}(\lambda\,\text{id} - u)$, et, si $u \circ v = v \circ u$, alors $(\lambda\,\text{id} - u) \circ v = v \circ (\lambda\,\text{id} - u)$. D'où $\text{Ker}(\lambda\,\text{id} - u)$ est stable par v. Donc, si deux

1. En effet, si $u(\vec{x})$ et $\vec{x}$ sont liés, alors il existe $k \in \mathbb{R}$ tel que $u(\vec{x}) = k\vec{x}$, et donc le facteur dans l'expression de $\chi_A(X)$ est donc $(X-k)$.

endomorphismes u et v commutent, alors les SEP de l'un sont stables par l'autre. □

RAPPEL (proposition 30) :
Si χ_A est scindé, alors $E = \bigoplus_{\lambda\in \mathrm{Sp}(A)} C_\lambda$ où $C_\lambda = \mathrm{Ker}(\lambda I_n - A)^{m_\lambda}$ et $\forall \lambda \in \mathrm{Sp}(A)$, $\dim C_\lambda = m_\lambda$.

EXERCICE (re-démonstation de la partie jaune (démonstration fausse dans le poly)) :
On choisit une base de E : $\mathscr{B}(\vec{\varepsilon}^1_1, \ldots, \vec{\varepsilon}^1_{d_1}, \vec{\varepsilon}^2_1, \ldots, \vec{\varepsilon}^2_{d_2}, \ldots, \vec{\varepsilon}^r_1, \ldots, \vec{\varepsilon}^r_{d_r})$, telle que $\mathscr{B}_i = (\vec{\varepsilon}^i_1, \ldots, \vec{\varepsilon}^i_{d_i})$ soit une base de C_{λ_i}, où $d_i = \dim C_{\lambda_i}$. Soit u l'endomorphisme représenté par la matrice A dans la base $\mathscr{B}$. Ainsi,

$$[u]_{\mathscr{B}} = \left(\begin{array}{c|c|c|c} B_1 & & & \\ \hline & B_2 & & \\ \hline & & \ddots & \\ \hline & & & B_r \end{array}\right)$$

car chaque sous-espace caractéristique C_{λ_i} est stable par u. Or, A commute avec $(\lambda_i I_n - A)^{m_{\lambda_i}}$. D'où $\mathrm{Ker}(\lambda_i I_n - A)^{m_{\lambda_i}} = C_{\lambda_i}$ est stable par A. De plus, la taille du bloc B_i est égal à la $d_i = \dim C_{\lambda_i}$. On veut montrer que, pour tout i, $d_i = m_{\lambda_i}$. On sait que $B_i = \left[u|_{C_{\lambda_i}}\right]_{\mathscr{B}}$. Or, $C_{\lambda_i} = \mathrm{Ker}\left((\lambda_i \,\mathrm{id} - u)^{m_{\lambda_i}}\right)$, d'où $\forall \vec{x} \in C_{\lambda_i}$, $(\lambda_i \,\mathrm{id} - u|_{C_{\lambda_i}})^{m_{\lambda_i}}(\vec{x}) = \vec{0}$. D'où $\lambda_i \,\mathrm{id} - u|_{C_{\lambda_i}}$ est nilpotent. D'où, le polynôme caractéristique $\chi_{\lambda_i - \mathrm{id} - u|_{C_{\lambda_i}}} = X^{d_i}$. Or, le polynôme caractéristique d'une restriction d'un endomorphisme divise le polynôme caractéristique de cet endomorphisme. D'où $\forall i$, $d_i \leqslant m_{\lambda_i}$. Or, $\sum_{i=1}^r d_i = n$, où $n = \dim E$, et $\sum_{i=1}^r m_{\lambda_i} = n$. D'où, $\forall i$, $d_i = m_{\lambda_i}$. Enfin, $B_i = \left[u\big|_{C_{\lambda_i}}\right]_{\mathscr{B}_i}$. Or, $(u\big|_{C_{\lambda_i}} - \lambda_i \,\mathrm{id})^{m_{\lambda_i}} = 0$. D'où $u\big|_{C_{\lambda_i}} = \lambda_i \,\mathrm{id} + (u\big|_{C_{\lambda_i}} - \lambda_i \,\mathrm{id})$, et donc $B_i = \lambda_i I_{d_i} + N_i$ où N_i est une matrice nilpotente.

Proposition : Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, et $u : E \to E$ un endomorphisme de E. Soit F un sous-espace vectoriel de E stable par u. On définit

$$\begin{aligned} v = u\big|_F : F &\longrightarrow F \\ \vec{x} &\longmapsto u(\vec{x}). \end{aligned}$$

Alors $\chi_v \mid \chi_u$ (i.e. χ_u est un multiple de χ_v).

Preuve :
Soit $A = [u]_{\mathscr{B}}$ où $\mathscr{B}$ est une base de E. Soient F et G deux supplémentaires de E. Soit $(\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_d)$ une base de F. En complétant cette base de F en une base $(\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_d, \vec{\varepsilon}_{d+1}, \ldots, \vec{\varepsilon}_n)$ de E. Il existe une matrice inversible P

telle que

$$P^{-1}\cdot A\cdot P=\left(\begin{array}{c|c} C & \star \\ \hline 0 & D \end{array}\right).$$

Le bloc C est la matrice de v dans la base $(\vec{\varepsilon}_1,\dots,\vec{\varepsilon}_d)$. Or,

$$\chi_A(x)=\det(xI_n-A)=\det\left(\begin{array}{c|c} xI-C & -\star \\ \hline 0 & xI-D \end{array}\right)=\underbrace{\det(xI-C)}_{\chi_C}\times\underbrace{\det(xI-D)}_{\chi_D}$$

car ce déterminant est triangulaire par blocs. D'où $\chi_A=\chi_C\times\chi_D$, et donc $\chi_C\mid\chi_A$ i.e. $\chi_v=\chi_u$. □

Proposition : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, et soit $u:E\to E$ un endomorphisme. Si u est diagonalisable, et F est un sous-espace vectoriel stable par u, alors $u\big|_F$ est aussi diagonalisable.

Preuve :
On suppose u diagonalisable. D'où u possède un polynôme annulateur P scindé à racine simple. Alors $P(u)=0_{\mathscr{L}(E)}$, d'où $\forall\vec{x}\in E$, $P(u)(\vec{x})=\vec{0}_E$, et donc $\forall\vec{x}\in F$, $P\big(u\big|_F\big)(\vec{x})=\vec{0}_E=\vec{0}_F$. Et donc, le polynôme P est annulateur de $u\big|_F$ et il est scindé à racines simples. D'où $u\big|_F$ est diagonalisable. □

Exercice :
Soit A une matrice diagonale par blocs. Montrer que A est diagonalisable si et seulement si chaque bloc est diagonalisable.

$$\left[\begin{array}{c|c|c|c} & & & \\ B_1 & 0 & 0 & 0 \\ & & & \\ \hline & & & \\ 0 & B_2 & 0 & 0 \\ & & & \\ \hline 0 & 0 & \ddots & 0 \\ \hline & & & \\ 0 & 0 & 0 & B_r \\ & & & \end{array}\right]\begin{array}{l}\varepsilon_1\\ \vdots\\ \varepsilon_{d_1}\\ \varepsilon_{d_1+1}\\ \vdots\\ \varepsilon_{d_1+d_2}\\ \vdots\\ \varepsilon_{d_1+\cdots+d_{r-1}+1}\\ \vdots\\ \varepsilon_{d_1+\cdots+d_r}.\end{array}$$

“ $\Longleftarrow$ ” Soit u l'endomorphisme tel que $\big[u\big]_{\mathscr{B}}=A$, où $\mathscr{B}=(\varepsilon_1,\dots,\varepsilon_d,\dots,\varepsilon_{d_1+\cdots+d_{r-1}+1},\dots,\varepsilon_{d_1+\cdots+d_r})$. Chaque sous-espace vectoriel F_i est stable par u car la matrice est diagonale par blocs. Or, chaque bloc est diagonalisable, d'où chaque $u\big|_{F_i}$ est diagonalisable. Il existe donc une base de F_i formée de vecteurs propres de u. En concaténant ces bases, on obtient une base de F formée de vecteurs propres de u.

Autre méthode : Chaque bloc B_i est diagonalisable, d'où $\forall i$, $\exists P_i \in \mathrm{GL}_{d_i}(\mathbb{K})$, $P_i^{-1} \cdot B_i \cdot P_i = D_i$ diagonale. On pose

$$P = \left(\begin{array}{c|c|c|c} P_1 & 0 & \dots & 0 \\ \hline 0 & P_2 & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & 0 \\ \hline 0 & \dots & 0 & P_r \end{array}\right).$$

Et donc

$$P^{-1} \cdot A \cdot P = \left(\begin{array}{c|c|c|c} D_1 & 0 & \dots & 0 \\ \hline 0 & D_2 & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & 0 \\ \hline 0 & \dots & 0 & D_r \end{array}\right).$$

" $\Longrightarrow$ " Réciproquement, pour tout i, on a $B_i = \left[u\big|_{F_i}\right]_{(\varepsilon_{d_1+\cdots+d_{i-1}+1},\dots,\varepsilon_{d_1+\cdots+d_i})}$.
Or u est diagonalisable, donc tout endomorphisme induit par u sur un sous-espace vectoriel stable est diagonalisable. Et donc, chaque bloc est diagonalisable.

Chapitre 5

Suites de fonctions

VII.1 Deux manières de converger

Définition : Soit T une partie de $\mathbb{R}$. Soit, pour $n \in \mathbb{N}$, $f_n : T \to \mathbb{R}$, une fonction. Soit également une fonction $f : T \to \mathbb{R}$. On dit que la suite de fonctions $(f_n)_{n\in\mathbb{N}}$:

1. *converge simplement* sur T vers f, si $\quad \forall t \in T,\ f_n(t) \xrightarrow[n\to+\infty]{} f(t)$;
2. *converge uniformément* sur T vers f, si $\sup_{t\in T} |f_n(t) - f(t)| \xrightarrow[n\to+\infty]{} 0$.

Si une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f, alors la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f. Mais, la réciproque est fausse :

$$\text{convergence uniforme} \quad \Longrightarrow \!\!\!\!\!\!\not\quad \quad \text{convergence simple.}$$

Exercice :
On considère, pour $n \in \mathbb{N}$, la fonction

$$\begin{aligned} f_n : \overbrace{[0,1]}^{T} &\longrightarrow \mathbb{R} \\ t &\longmapsto t^n. \end{aligned}$$

Soit $t \in [0,1]$. Alors,

$$f_n(t) = t^n \xrightarrow[t\to+\infty]{} \begin{cases} 0 & \text{si } t \in [0,1[\\ 1 & \text{si } t = 1. \end{cases}$$

D'où la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction f définie ci-dessous :

$$\begin{aligned} f : [0,1] &\longrightarrow \mathbb{R} \\ t &\longmapsto \begin{cases} 0 & \text{si } t \in [0,1[, \\ 1 & \text{si } t = 1. \end{cases} \end{aligned}$$

Cette convergence n'est pas uniforme car, comme $\sup_{t\in[0,1]} f_n(t) = 1$, d'où $\sup_{t\in[0,1]} |f_n(t) - f(t)| = 1 \xrightarrow[n\to+\infty]{\not\longrightarrow} 0$.

B Méthode

2ème méthode : montrer qu'une suite de fonctions ne converge pas uniformément.
soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels définis, pour $n \in \mathbb{N}^\star$ par $u_n = 1 - \frac{1}{n}$, qui converge vers 1 en $+\infty$. Alors,

$$f_n(u_n) = \left(1 - \frac{1}{n}\right)^n = \mathrm{e}^{n\ln\left(1-\frac{1}{n}\right)} = \mathrm{e}^{n\times\left(-\frac{1}{n}+o\left(\frac{1}{n}\right)\right)} = \mathrm{e}^{-1+o(1)} \xrightarrow[n\to+\infty]{} \mathrm{e}^{-1}.$$

D'où, $f(u_n) - f(u_n) = \left(1 - \frac{1}{n}\right)^n - 0 \xrightarrow[n\to+\infty]{\not\longrightarrow} 0$. Or, $\sup |f_n - f| \geqslant |f_n(u_n) - f(u_n)|$. D'où $\sup |f_n - f| \xrightarrow[n\to+\infty]{\not\longrightarrow} 0$.

Soit $a \in [0, 1[$. Mais, la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément sur $[0, a]$: en effet, montrons que

$$\sup_{t\in[0,a]} |f_n(t) - f(t)| \xrightarrow[n\to+\infty]{} 0 \qquad \text{aussi noté} \qquad \sup_{[0,a]} |f_n - f| \xrightarrow[n\to+\infty]{} 0.$$

Calculons $|f_n(t) - f(t)| = |f_n(t) - 0| = |t^n| \leqslant a^n$. D'où a^n est un majorant. Ainsi, par définition de la borne supérieure, [1] $\sup_{[0,a]} |f_n - f| \leqslant a^n$. Or, $\sup_{[0,a]} |f_n - f| \geqslant 0$, et donc, d'après le théorème d'existence de la limite par encadrement,

$$\sup_{t\in[0,a]} |f_n(t) - f(t)| \xrightarrow[n\to+\infty]{} 0.$$

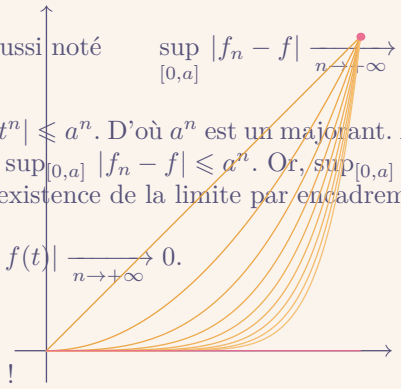


FIGURE 5.1 – Convergence de la suite de fonctions $(t^n)_{n\in\mathbb{N}}$

REMARQUE (sert rarement sauf pour prouver le théorème 6) : 1. $(f_n)_{n\in\mathbb{N}}$ converge simplement sur T vers f si et seulement si

$$\forall t \in T,\ \forall \varepsilon > 0,\ \overbrace{\exists N \in \mathbb{N},\ \forall n \geqslant N,\ |f_n(t) - f(t)| \leqslant \varepsilon}^{\text{« à partir d'un certain rang »}}.$$

Ici, le N dépend de t et de ε.

2. $(f_n)_{n\in\mathbb{N}}$ converge uniformément sur T vers f si et seulement si

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ \forall t \in T,\ |f_n(t) - f(t)| \leqslant \varepsilon.$$

Ici, le N ne dépend que de ε et pas de t : le même N convient pour tous les t.

1. La borne supérieure est définie comme le plus petit majorant.

Exercice :

$(f_n)_{n\in\mathbb{N}}$ converge simplement vers f sur $[0,1] \overset{\text{def.}}{\iff} \forall x \in [0,1], f_n(x) \xrightarrow[n\to+\infty]{} f(x)$.

Or, si $x \in]0,1]$, alors $f_n(x) \xrightarrow[n\to+\infty]{} 0$ car, à partir d'un certain rang N, $\forall n \geqslant N$, $f_n(x) = 0$; et, si $x = 0$, $f_n(x) = f_n(0) = 1 \xrightarrow[n\to+\infty]{} 1$. Soit ainsi

$$\begin{aligned} f : [0,1] &\longrightarrow [0,1] \\ x &\longmapsto \begin{cases} 0 & \text{si } x \in]0,1] \\ 1 & \text{si } x = 0. \end{cases} \end{aligned}$$

Alors, la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge vers la fonction f.

$(f_n)_{n\in\mathbb{N}}$ converge uniformément vers $f \overset{\text{def.}}{\iff} \sup\limits_{x\in[0,1]} |f_n(x) - f(x)| \xrightarrow[n\to+\infty]{} 0$.

Or, $\sup_{x\in[0,1]} |f_n(x) - f(x)| = 1 \not\xrightarrow[n\to+\infty]{} 0$.

Soit $x \in [0,1]$. Si $x = 0$, alors $f_n(x) = f_n(0) = 0 \xrightarrow[n\to+\infty]{} 0$; si $x \in]0,1]$, alors $f_n(x) = 0$ à partir d'un certain rang, et donc $f_n(x) \xrightarrow[n\to+\infty]{} 0$. D'où la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction nulle. Mais, la convergence n'est pas uniforme :

$$\sup_{x\in[0,1]} |f_n(x) - 0| = 2n + 2 \not\xrightarrow[n\to+\infty]{} 0.$$

VII.2 Continuité

Exemple :
Dans l'exercice 2, chaque fonction $f_n : t \mapsto t^n$ est continue sur $[0,1]$ mais la limite f n'est pas continue sur $[0,1]$ (car elle n'est pas continue en 1).

Théorème : Soit a un réel dans un intervalle T de $\mathbb{R}$. Si une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ continues en a converge uniformément sur T vers une fonction f, alors f est aussi continue en a.

Preuve :
On suppose les fonctions f_n continues en a ($f_n(x) \longrightarrow f_n(a)$) et que la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f ($\sup |f_n - f| \longrightarrow 0$).
On veut montrer que f est continue en a : $f(x) \xrightarrow[x\to a]{} f(a)$, i.e.

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in T, \quad |x - a| \leqslant \delta \implies |f(x) - f(a)| \leqslant \varepsilon.$$

Soit $\varepsilon > 0$. On calcule

$$\big|f(x) - f(a)\big| \leqslant \big|f(x) - f_n(x)\big| + \big|f_n(x) - f_n(a)\big| + \big|f_n(a) - f(a)\big|$$

par inégalité triangulaire. Or, par hypothèse, il existe un rang $N \in \mathbb{N}$ (qui ne dépend pas de x ou de a), tel que, $\forall n \geqslant N$, $\big|f(x) - f_n(x)\big| \leqslant \frac{1}{3}\varepsilon$, et $\big|f_n(a) - f(a)\big| \leqslant \frac{1}{3}\varepsilon$. De plus, par hypothèse, il existe $\delta > 0$ tel que si $|x - a| \leqslant \delta$, alors $|f_n(x) - f_n(a)| \leqslant \frac{1}{3}\varepsilon$. [a] On en déduit que $\big|f(x) - f(a)\big| \leqslant \varepsilon$. □

a. C'est là où l'hypothèse de la convergence uniforme est utilisée : on a besoin que le N ne dépende pas de x car on le fait varier.

Corollaire : Soit T un intervalle de $\mathbb{R}$. Si une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ continues sur T converge uniformément sur T vers une fonction continue sur T.

MÉTHODE (Stratégie de la barrière) :

1. La continuité (la dérivabilité aussi) est une propriété *locale*. Pour montrer qu'une fonction est continue sur un intervalle T, il suffit donc de montrer qu'elle est continue sur tout segment inclus dans T.
2. Mais, la convergence uniforme est une propriété *globale*. La convergence sur tout segment inclus dans un intervalle n'implique pas la convergence uniforme sur l'intervalle (voir l'exercice 2).
3. On n'écrit pas

$$\begin{array}{c}\text{convergence uniforme}\\ \text{avec barrière}\end{array} \Longrightarrow \begin{array}{c}\text{convergence uniforme}\\ \text{sans barrière}\end{array} \Longrightarrow \begin{array}{c}\text{continuité}\\ \text{sans barrière}\end{array}$$

   mais plutôt

$$\begin{array}{c}\text{convergence uniforme}\\ \text{avec barrière}\end{array} \Longrightarrow \begin{array}{c}\text{continuité}\\ \text{avec barrière}\end{array} \Longrightarrow \begin{array}{c}\text{continuité}\\ \text{sans barrière}\end{array}.$$

4. Si, pour tous a et b, f est bornée sur $[a, b] \subset T$, mais cela n'implique pas que f est bornée. Contre-exemple : la fonction $f : x \mapsto \frac{1}{x}$ est bornée sur tout intervalle $[a, b]$ avec a, $b \in \mathbb{R}_\star^+$, MAIS f n'est pas bornée sur $]0, +\infty[$.

Théorème (double-limite ou d'interversion des limites) **:** Soit une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ définies sur un intervalle T, et, soit a une extrémité (éventuellement infinie) [a] de cet intervalle. Si la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément sur T vers f et si chaque fonction f_n admet une limite finie b_n en a, alors la suite de réels b_n converge vers un réel b, et $\lim_{t\to a} f(t) = b$. Autrement dit,

$$\lim_{t\to a}\Big(\underbrace{\lim_{n\to+\infty} f_n(t)}_{f(x)}\Big) = \lim_{n\to+\infty}\Big(\underbrace{\lim_{t\to a} f_n(t)}_{b_n}\Big).$$

□

a. autrement dit, $a \in \bar{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$

Le théorème de la double-limite « contient » le théorème 6 (théorème de préservation/transmission de la continuité), c'est un cas particulier. En effet, si les fonctions f_n sont continues, alors

$$\lim_{x\to a} f(x) = \underbrace{\lim_{n\to+\infty} f_n(a)}_{f(a)}.$$

Contre-exemple :
On considère la suite de fonctions $(f_n)_{n\in\mathbb{N}} = (t \mapsto t^n)_{n\in\mathbb{N}}$.

$$1 = \lim_{n\to+\infty} \underbrace{\lim_{t\to 1} f_n(t)}_{1} \neq \lim_{x\to 1} \overbrace{\lim_{n\to+\infty} f_n(t)}^{f(t)} \text{ n'existe pas.}$$

VII.3 Intégrer

Théorème (interversion de la limite et de l'intégrale sur un segment) **:** Si une suite de fonctions continues $(f_n)_{n\in\mathbb{N}}$ sur un segment $[a,b]$ converge uniformément vers f sur $[a,b]$, alors f est continue sur $[a,b]$ (théorème 6) et

$$\int_a^b \Big(\underbrace{\lim_{n\to+\infty} f_n(t)}_{f(t)} \Big)\, \mathrm{d}t = \lim_{n\to+\infty} \underbrace{\Big(\int_a^b f_n(t)\, \mathrm{d}t \Big)}_{I_n}$$

(d'où, pas d'intégrales impropres). Autrement dit, la suite de fonctions $(F_n)_{n\in\mathbb{N}}$ définies comme primitives des fonctions continues f_n :

$$\begin{aligned} F_n : [a,b] &\longrightarrow \mathbb{R} \\ x &\longmapsto \int_a^x f_n(t)\, \mathrm{d}t \end{aligned}$$

converge uniformément vers

$$\begin{aligned} F : [a,b] &\longrightarrow \mathbb{R} \\ x &\longmapsto \int_a^x f(t)\, \mathrm{d}t. \end{aligned}$$

Preuve :
On suppose que la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers

f sur un segment $[a,b]$. On veut monter que

$$\lim_{n\to+\infty}\Big(\int_a^b f_n(t)\ \mathrm{d}t\Big)-\int_a^b f(t)\ \mathrm{d}t=0$$

i.e.

$$\lim_{n\to+\infty}\Big(\int_a^b f_n(t)\ \mathrm{d}t-\int_a^b f(t)\ \mathrm{d}t\Big)=0.$$

Or,

$$0\leqslant\Big|\int_a^b\big(f_n(t)-f(t)\big)\ \mathrm{d}t\Big|\leqslant\int_a^b\big|f_n(t)-f(t)\big|\ \mathrm{d}t$$

d'après l'inégalité triangulaire. Or, $\mathbb{R}\ni M_n=\sup_{t\in[a,b]}|f_n(t)-f(t)|\xrightarrow[n\to+\infty]{}0$. D'où M_n est un majorant donc

$$0\leqslant\Big|\int_a^b\big(f_n(t)-f(t)\big)\ \mathrm{d}t\Big|\leqslant\int_a^b M_n\ \mathrm{d}t=(b-a)\cdot M_n\xrightarrow[n\to+\infty]{}0.$$

D'où, d'après le théorème des gendarmes, [a] on a bien

$$\int_a^b f(t)\ \mathrm{d}t=\lim_{n\to+\infty}\int_a^b f_n(t)\ \mathrm{d}t.$$

La preuve de la seconde partie du théorème est dans le poly. □

a. aussi appelé *théorème d'existence de la limite par encadrement.*

Théorème (convergence dominée) **:** Soit T un intervalle et soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions continues par morceaux sur T. Si

1. la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement sur T vers une fonction f continue par morceaux,
2. il existe une fonction φ continue par morceaux sur T et intégrable [a] sur T telle que

$$\forall n\in\mathbb{N},\ \forall t\in T,\quad\big|f_n(t)\big|\leqslant\varphi(t)$$

alors les fonctions f_n et la fonction f sont intégrables et la suite de réels $\int_T f_n$ converge vers le réel $\int_T f$.

a. i.e. l'intégrale $\int_T|\varphi|$ converge

Exercice :
Montrer que la suite de réels $I_n=\displaystyle\int_0^{+\infty}\frac{\mathrm{e}^{-t/n}}{1+t^2}\,\mathrm{d}t$ *est bien définie, qu'elle converge et déterminer sa limite.*

On doit donc montrer que l'intégrale I_n converge (1) puis étudier la limite de

la suite des réels $(I_n)_{n\in\mathbb{N}}$ (2). Soit

$$\begin{aligned} f_n : [0,+\infty[&\longrightarrow \mathbb{R} \\ t &\longmapsto \frac{\mathrm{e}^{-t/n}}{1+t^2} \end{aligned}$$

1. L'intégrale I_n est impropre en $+\infty$. On a, $\forall t \in [0,1[$, $\forall n \in \mathbb{N}$, $0 \leqslant f_n(t) \leqslant \frac{1}{1+t^2}$. Or, l'intégrale $\int_0^{+\infty} \frac{1}{1+t^2}\,\mathrm{d}t$ converge [2] donc l'intégrale I_n converge.
2. La suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge vers

$$\begin{aligned} f : [0,1] &\longrightarrow \mathbb{R} \\ t &\longmapsto \frac{1}{1+t^2} \end{aligned}$$

car $f_n(t)$ converge vers 1 si $t=0$, et $\frac{\mathrm{e}^{-0}}{1+t^2}$ si $t>0$. De plus, $\forall n, \forall t, |f_n(t)| \leqslant \varphi(t)$ où $\varphi(t) = 1/(1+t^2)$. Or, l'intégrale $\int_0^{+\infty} \frac{1}{1+t^2}\,\mathrm{d}t$ converge. Donc, d'après le théorème de la convergence dominée,

$$\lim_{n\to+\infty} \int_0^{+\infty} \frac{\mathrm{e}^{-\frac{t}{n}}}{1+t^2}\,\mathrm{d}t = \int_0^{+\infty} \lim_{n\to+\infty} \frac{\mathrm{e}^{-\frac{t}{n}}}{1+t^2}\,\mathrm{d}t = \int_0^{+\infty} \frac{1}{1+t^2}\,\mathrm{d}t = \frac{\pi}{2}.$$

Méthode (du discret au continu) :

Rappel (caractérisation séquencielle de la limite) :

$$g(x) \xrightarrow[x\to a\in\bar{\mathbb{R}}]{} \ell \in \bar{\mathbb{R}} \quad \Longleftrightarrow \quad \forall (u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}},\ u_n \xrightarrow[n\to+\infty]{} a \implies f(u_n) \xrightarrow[n\to+\infty]{} \ell.$$

Exercice :
Étudier $\lim_{x\to+\infty} \int_0^{+\infty} \frac{\mathrm{Arctan}(xt)}{1+t^2}\,\mathrm{d}t$.

Méthode 1 sans la caractérisation séquentielle de la limite mais avec le théorème de la limite monotone (croissance de F). On remplace le réel x par un entier n [3] : on veut étudier

$$\lim_{n\to\infty} \int_0^{+\infty} \frac{\mathrm{Arctan}(nt)}{1+t^2}\,\mathrm{d}t.$$

On utilise le théorème de convergence dominée (TCD). Soit, pour $n \in \mathbb{N}$,

$$\begin{aligned} f_n : [0,+\infty[&\longrightarrow \mathbb{R} \\ t &\longmapsto \frac{\mathrm{Arctan}(nt)}{1+t^2}. \end{aligned}$$

Soit $t \in [0,+\infty[$.

$$f_n(t) \xrightarrow[n\to+\infty]{} f(t) = \begin{cases} 0 & \text{si } t=0 \\ \pi/2 \\ \hline 1+t^2 & \text{si } t>0. \end{cases}$$

2. car $\int_0^{+\infty} \frac{1}{1+t^2}\,\mathrm{d}t = [\mathrm{Arctan}\, t]_0^{+}\infty = \frac{\pi}{2} - 0$.
3. i.e. on discrétise le problème

Ainsi, $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f. Et,

$$\forall n \in \mathbb{N},\ \forall t \in [0,+\infty[,\quad |f_n(t)| \leqslant \frac{\pi/2}{1+t^2} = \varphi(t)$$

et $\displaystyle\int_0^{+\infty} \varphi(t)\ \mathrm{d}t$ converge. Ainsi, d'après le théorème de convergence dominée,

$$\lim_{n\to\infty} \int_0^{+\infty} \frac{\operatorname{Arctan}(nt)}{1+t^2}\ \mathrm{d}t = \int_0^{+\infty} f(t)\ \mathrm{d}t = \frac{\pi^2}{4}.$$

Attention, $\lim_{n\to\infty} f(n)$ n'est pas forcément égal à $\lim_{x\to+\infty} f(x)$; par exemple, avec $f(x) = \sin(2\pi x)$. Or, la fonction

$$\begin{aligned} F : [0,+\infty[&\longrightarrow \mathbb{R} \\ x &\longmapsto \int_0^{+\infty} \frac{\operatorname{Arctan}(xt)}{1+t^2}\ \mathrm{d}t \end{aligned}$$

est croissante ; en effet,

$$\begin{aligned} x_1 \leqslant x_2 &\implies x_1 t \leqslant x_2 t \text{ car } t \geqslant 0 \\ &\implies \operatorname{Arctan}(x_1 t) \leqslant \operatorname{Arctan}(x_2 t) \text{ car Arctan est croissante} \\ &\implies \frac{\operatorname{Arctan}(x_1 t)}{1+t^2} \leqslant \frac{\operatorname{Arctan}(x_2 t)}{1+t^2} \\ &\implies F(x_1) \leqslant F(x_2) \text{ par croissance de l'intégrale.} \end{aligned}$$

D'où, d'après le théorème de la limite monotone, $\lim_{x\to+\infty} F(x)$ existe. Or, $F(n) \xrightarrow[n\to\infty]{} \pi^2/4$. Et, par unicité de la limite,

$$\boxed{\lim_{x\to+\infty} \int_0^{+\infty} \frac{\operatorname{Arctan}(xt)}{1+t^2}\ \mathrm{d}t = \frac{\pi^2}{4}.}$$

Ou, autre rédaction :

$$F(\underbrace{\lfloor x \rfloor}_{\in\mathbb{N}}) \leqslant F(x) \leqslant F(\underbrace{\lfloor x \rfloor + 1}_{\in\mathbb{N}})$$

par croissance de F. D'où par théorème des gendarmes, $F(x) \xrightarrow[x\to+\infty]{} \frac{\pi^2}{4}$.

Cas 2 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle qui tend vers $+\infty$. On pose

$$\begin{aligned} f_n(t) : [0,+\infty[&\longrightarrow \mathbb{R} \\ t &\longmapsto \frac{\operatorname{Arctan}(u_n\, t)}{1+t^2}. \end{aligned}$$

On remarque que

$$f_n(t) \xrightarrow[n\to+\infty]{} \begin{cases} 0 & \text{si } t = 0 \\ \frac{\pi/2}{1+t^2} & \text{si } t > 0, \end{cases}$$

on pose donc

$$f : [0,+\infty[\longrightarrow \mathbb{R}$$
$$t \longmapsto \begin{cases} 0 & \text{si } t = 0 \\ \frac{\pi/2}{1+t^2} & \text{si } t > 0. \end{cases}$$

D'où, la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction f. Or,

$$\forall n \in \mathbb{N},\ \forall t \in \mathbb{R}^+, \quad |f_n(t)| \leqslant \frac{\pi/2}{1+t^2}.$$

D'où, d'après le théorème de la convergence dominée,

$$\lim_{n\to\infty} \int_0^{+\infty} f_n(t)\ \mathrm{d}t = \int_0^{+\infty} \lim_{n\to\infty} f_n(t)\ \mathrm{d}t.$$

Or, $\int_0^{+\infty} \lim_{n\to+\infty} f_n(t)\ \mathrm{d}t = \int_0^{+\infty} \frac{\pi/2}{1+t^2}\ \mathrm{d}t = \frac{\pi}{2} \times \frac{\pi}{2}$. D'où, on en déduit que

$$\lim_{n\to\infty} \underbrace{\int_0^{+\infty} f_n(t)\ \mathrm{d}t}_{F(u_n)} = \frac{\pi^2}{4}.$$

On a montré que $F(u_n) \xrightarrow[n\to+\infty]{} \frac{\pi^2}{4}$ pour toute suite $(u_n)_{n\in\mathbb{N}}$ tendant vers $+\infty$. D'où, d'après la caractérisation séquentielle de la limite, on en déduit que

$$F(x) \xrightarrow[x\to+\infty]{} \frac{\pi^2}{4}.$$

VII.4 Dériver

Théorème (interversion limite et dérivée) **:** Soit une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ de classe $\mathscr{C}^1$ sur un segment $[a,b]$. Si,

1. la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement sur $[a,b]$ vers une fonction f,
2. la suite de dérivées $(f_n')_{n\in\mathbb{N}}$ converge uniformément sur $[a,b]$ vers une fonction g ;

alors

1. la fonction f est de classe $\mathscr{C}^1$ sur $[a,b]$, et $\forall x \in [a,b]$, $f'(x) = g(x)$, [a]
2. la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément sur $[a,b]$ vers g.

a. Autrement dit, $\dfrac{\mathrm{d}}{\mathrm{d}x} \lim\limits_{n\to\infty} f_n(x) = \lim\limits_{n\to\infty} \dfrac{\mathrm{d}}{\mathrm{d}x} f_n(x)$.

Preuve :

On utilise le théorème 10 : on a

$$\begin{array}{ccccc} f_n(x) & = & f_n(c) & + & \displaystyle\int_c^x f_n'(t)\,\mathrm{d}t \\ \downarrow & & \downarrow & & \downarrow \\ f(x) & & f(c) & & \displaystyle\lim_{n\to\infty}\int_c^x f_n'(t)\,\mathrm{d}t \\ & & & & \displaystyle=\int_c^x \lim_{n\to\infty} f_n'(t)\,\mathrm{d}t \\ & & & & \displaystyle=\int_c^x g(t)\,\mathrm{d}t \end{array}$$

car $(f_n')_{n\in\mathbb{N}}$ converge uniformément vers g. L'intégrale de f_n' existe car, comme les fonctions f_n sont de classe $\mathscr{C}^1$, alors les fonctions f_n' sont de classe $\mathscr{C}^0$ donc continues. On veut montrer que $g = f'$. On sait que, $\forall x \in [a,b]$, $f(x) = f(c) + \int_c^x g(t)\,\mathrm{d}t$ par unicité de la limite. De plus, la fonction g est continue car $(f_n')_{n\in\mathbb{N}}$ converge uniformément vers g et f_n' est continue (d'après le théorème 6). D'où f est dérivable sur $[a,b]$ et, $\forall x \in [a,b]$, $f'(x) = g(x)$. Mieux : f est de classe $\mathscr{C}^1$. □

4 car (f_n) converge simplement vers f

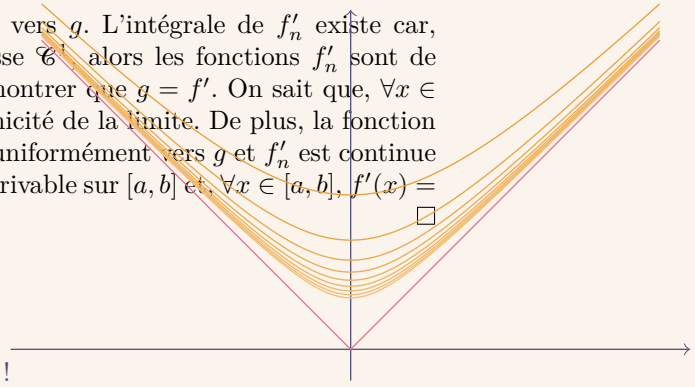


FIGURE 5.2 – Suite de fonctions $\left(\sqrt{x^2+\frac{1}{n}}\right)_{n\in\mathbb{N}^\star}$

EXERCICE :
On pose, pout tout $n \in \mathbb{N}^\star$,

$$\begin{aligned} f_n : [-1,1] &\longrightarrow \mathbb{R} \\ x &\longmapsto \sqrt{x^2+\frac{1}{n}}. \end{aligned}$$

1. *Montrer que la suite de fonctions $(f_n)_{n\in\mathbb{N}^\star}$ converge simplement. Vers quelle fonction f ?*
2. *La convergence est-elle uniforme ?*
3. *Les fonctions f_n sont-elles de classe $\mathscr{C}^1$? Et la fonction f ? Que dit le théorème précédent ?*

1. Soit $x \in [-1,1]$. On a $f_n(x) \xrightarrow[n\to\infty]{} \sqrt{x^2} = |x|$. Ainsi, la suite de fonctions $(f_n)_{n\in\mathbb{N}^\star}$ converge simplement vers

$$\begin{aligned} f : [-1,1] &\longrightarrow \mathbb{R} \\ x &\longmapsto |x|. \end{aligned}$$

On remarque que l'on a perdu la dérivabilité en 0.

2. Soit $n \in \mathbb{N}^\star$. Soit $x \in [-1,1]$. On calcule

$$\begin{aligned}|f_n(x) - f(x)| = \left|\sqrt{x^2+\frac{1}{n}} - |x|\right| &= \sqrt{x^2+\frac{1}{n}} - |x| \\ &= \frac{\sqrt{x^2+\frac{1}{n}} - |x|}{\sqrt{x^2+\frac{1}{n}} + |x|} \times \left(\sqrt{x^2+\frac{1}{n}} + |x|\right) \\ &= \frac{\cancel{x^2} + \frac{1}{n} - \cancel{x^2}}{\sqrt{x^2+\frac{1}{n}} + |x|} \\ &\geqslant \frac{1/n}{\sqrt{0+\frac{1}{n}}+0} = \frac{1}{\sqrt{n}}\end{aligned}$$

qui est un majorant.[5] D'où, $0 \leqslant \sup_{x\in[-1,1]} |f_n(x) - f(x)| = 1/\sqrt{n}$. Donc, d'après le théorème d'existence de la limite par encadrement, $\sup_{x\in[-1,1]} |f_n(x) - f(x)| \xrightarrow[n\to\infty]{} 0$. On déduit donc que la suite de fonctions $(f_n)_{n\in\mathbb{N}^\star}$ converge uniformément vers f qui est la valeur absolue.

3. La fonction f_n est dérivable[6] sur $[-1,1]$, et

$$\forall x \in [-1,1], \quad f_n'(x) = \frac{2x}{2\sqrt{x^2+\frac{1}{n}}}.$$

Or, les fonctions f_n' est continue.[7] Néanmoins, la fonction $f : x \mapsto |x|$ n'est pas dérivable en 0, donc n'est pas $\mathscr{C}^1$. D'où, en utilisant le théorème d'interversion de limite et de dérivée, par l'absurde, la suite de fonctions $(f_n')_{n\in\mathbb{N}^\star}$ ne converge pas uniformément vers f'.

Méthode :

Corollaire :

VII.5 Approximation uniforme par des polynômes

Remarque (Rappel) :
Soit f une fonction d'un intervalle I dans $\mathbb{K}$ (où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$).

La fonction f est continue sur I si et seulement si

$$\forall a \in I, \quad \underbrace{\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in I, \quad |x-a| \leqslant \eta \implies |f(x)-f(a)| \leqslant \varepsilon}_{f \text{ est continue en } a}.$$

La fonction f est uniformément continue sur I si et seulement si

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall a \in I,\ \forall x \in I, \quad |x-a| \leqslant \eta \implies |f(x)-f(a)| \leqslant \varepsilon.$$

5. qui ne dépend pas de x
6. par composée de fonctions dérivables/par les théorèmes généraux
7. car c'est un quotient de fonctions continues dont le dénominateur ne s'annule pas/d'après les théorèmes généraux

L'uniforme continuité implique la continuité. La réciproque est fausse.

Exercice :
Montrer que la fonction $f : x \mapsto x^2$ n'est pas uniformément continue sur $\mathbb{R}$. Soit $\varepsilon > 0$. Par l'absurde, supposons qu'il existe $\eta > 0$ tel que

$$\forall x \in \mathbb{R},\ \forall x \in \mathbb{R}, \quad |x - a| \leqslant \eta \implies |f(x) - f(a)| \leqslant \varepsilon.$$

Or, $|f(x) - f(a)| = |x^2 - a^2|$. Soit $x = a + h$ avec $0 < h \leqslant \eta$, d'où $|x^2 - a^2| = \left|(a+h)^2 - a^2\right| = |2ha + h^2|$. Ce qui est absurde car $|2ah + h^2 \xrightarrow[a \to +\infty]{} +\infty$ comme $h \neq 0$.

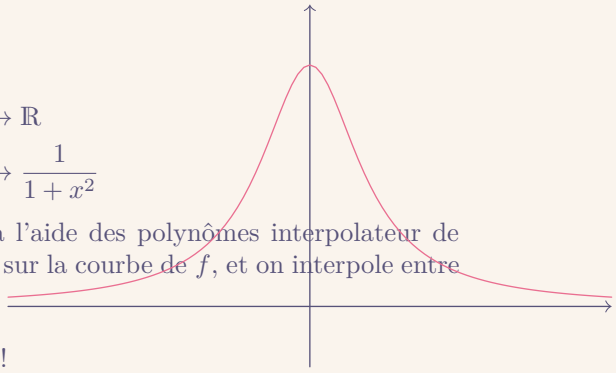
Théorème (Heine) **:** Une fonction continue sur un segment est uniformément continue sur ce même segment.

L'interpolation n'est pas toujours une bonne approximation.

Exemple (phénomène de Runge) :
La fonction

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{1 + x^2} \end{aligned}$$

peut être approché par un polynôme à l'aide des polynômes interpolateur de Lagrange : on choisit plusieurs points sur la courbe de f, et on interpole entre ces points.



!

Figure 5.3 – Graphe de $f : x \mapsto \frac{1}{1+x^2}$

À faire : Interpolation de Lagrange

Théorème (Weierstraß) **:** Si une fonction $f : [a, b] \to \mathbb{R}$ continue sur le segment $[a, b]$, alors il existe une suite de polynômes P_n qui converge uniformément vers f telle que

$$\sup_{[a,b]} |f - P_n| \xrightarrow[n \to \infty]{} 0.$$

Théorème (théorème des moments) **:** Soit f une fonction continue sur un segment $[a, b]$ vers $\mathbb{R}$. Montrer que, si

$$\forall n \in \mathbb{N},\ \int_a^b x^n f(x)\ \mathrm{d}x = 0,$$

alors la fonction f est nulle. Soit $P \in \mathbb{R}[X]$, il existe donc a_0, a_1, ...,

$a_n \in \mathbb{R}^{n+1}$ tels que $P(X) = a_0 + a_1 X + \cdots + a_n X^n$. Alors,

$$\int_a^b P(x) \cdot f(x)\ \mathrm{d}x = \int_a^b \Big(\sum_{k=0}^{n} a_k x^k\Big) \cdot f(x)\ \mathrm{d}x = \sum_{k=1}^{n} a_k \underbrace{\int_a^b x^k f(x)\ \mathrm{d}x}_{0} = 0.$$

Or, d'après le théorème de Weierstrass, il existe une suite de polynômes $(P_n)_{n\in\mathbb{N}}$ qui convergent uniformément vers f. D'où,

$$\forall n \in \mathbb{N},\ \int_a^b P_n(x) \cdot f(x)\ \mathrm{d}x.$$

On va montrer que

$$\int_a^b P_n(x) \cdot f(x)\ \mathrm{d}x \xrightarrow[n\to\infty]{} \int_a^b f(x) \cdot f(x)\ \mathrm{d}x.$$

Or, d'après le théorème de Weierstrass, la suite de polynômes $(P_n)_{n\in\mathbb{N}}$ converge uniformément vers f. D'où,

$$\Big|P_n(x)f(x) - f(x)\cdot f(x)\Big| = \underbrace{\Big|P_n(x) - f(x)\Big|}_{\leqslant \sup_{[a,b]}|f-P_n|} \times \underbrace{\Big|f(x)\Big|}_{\leqslant M}$$

où M est le majorant qui existe car toute fonction continue sur un segment est bornée. D'où,

$$\Big|P_n(x)f(x) - f(x)\cdot f(x)\Big| \leqslant M \times \sup_{[a,b]} |f - P_n|.$$

D'où

$$0 = \lim_{n\to\infty} \int_a^b P_n(x) \cdot f(x)\ \mathrm{d}x = \int_a^b \lim_{n\to\infty} P_n(x) \cdot f(x)\ \mathrm{d}x.$$

On en déduit donc que

$$\int_a^b f^2(x)\ \mathrm{d}x = 0.$$

Or, si l'intégrale d'une fonction positive et continue est nulle, alors la fonction est nulle. Donc

$$\forall x \in [a,b],\quad f(x) = 0.$$

Chapitre 6

Séries de fonctions

VII.1 Trois manières de converger

VII.1.1 Convergence simple et convergence uniforme

Rappel (Suites et séries numériques) :
Les suites (u_n) et les séries $\sum u_n$ ont une nature mais pas de valeurs. Les valeurs u_n et $\sum_{k=0}^{n} u_k$ sont respectivement le n-ième terme de la suite, et la somme partielle de la série. Le reste $\sum_{k=n+1}^{\infty} u_k$ est défini que si la série $\sum u_n$, et il tend vers 0. La somme $\sum_{k=0}^{\infty}$ est définie si la série $\sum u_n$ converge.

Nous avons vu au chapitre précédent les suites de fonctions, et les deux types de convergence : simple et uniforme. Dans ce chapitre, on s'intéresse aux séries de fonctions. Mais, au lieu de deux méthodes de convergence, il y en a trois pour les séries : normale, simple et uniforme. On a

convergence simple $\quad \Longleftarrow \not\Longrightarrow \quad$ convergence uniforme $\quad \Longleftarrow \not\Longrightarrow \quad$ convergence normale.

Attention : les théorèmes sur les séries numériques ne sont pas, en général, vrais pour les séries de fonctions.

Rappel :
La suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction f si, et seulement si

$$\forall x, \qquad f_n(x) \xrightarrow[n\to\infty]{} f(x).$$

Et, elle converge uniformément vers f si, et seulement si

$$\sup_{x\in I} \left|f_n(x) - f(x)\right| \xrightarrow[n\to\infty]{} 0.$$

Définition : La série de fonctions $\sum f_n$ converge simplement vers la

fonction S si

$$\forall x, \quad S_n(x) \xrightarrow[n\to\infty]{} S(x), \quad \text{où} \quad S_n(x) = \sum_{k=0}^{n} f_k(x).$$

De même que pour les suites, la série de fonctions $\sum f_n$ converge uniformément vers la fonction S si

$$\sup_{x\in I} \left|S_n(x) - S(x)\right| \xrightarrow[n\to\infty]{} 0.$$

Remarque :
On pose des notations similaires que pour les séries numériques pour la somme et pour le reste.

Méthode :

la série de fonctions $\sum f_n$ converge uniformément sur I vers la fonction S
$\iff$ le reste R_n (fonction) converge uniformément vers $\tilde{0}$ (fonction nulle)
$\implies$ la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers $\tilde{0}$ (fonction nulle).

Preuve :
On sait que, par définition, la série de fonctions $\sum f_n$ converge uniformément vers S sur I si et seulement si $\sup_{x\in I} \left|S_n(x)-S(x)\right| \xrightarrow[n\to\infty]{} 0$. Or, $\forall x \in I$, $S(x)-S_n(x) = R_n(x)$. D'où, la série de fonctions $\sum f_n$ converge uniformément vers S sur I si et seulement si $\sup_{x\in I} \left|R_n(x)\right| \xrightarrow[n\to\infty]{} 0$, donc si et seulement si (par définition), la suite de fonctions $(R_n)_{n\in\mathbb{N}}$ converge uniformément vers 0. À présent, on veut montrer que $\sup_{x\in I} |f_n(x)| \longrightarrow 0$. Or, $\forall n \in \mathbb{N}^\star$, $\forall x \in I$, $R_n(x) = \sum_{k=n+1}^{\infty} f_k(x)$, et donc $f_n(x) = R_{n-1}(x) - R_n(x)$. D'où $\left|f_n(x)\right| \leqslant \left|R_{n-1}(x)\right| + \left|R_n(x)\right|$. Attention, on ne peut pas passer au sup directement. Or, $\left|R_{n-1}(x) - R_n(x)\right| \leqslant \sup_{x\in I} \left|R_{n-1}(x)\right| + \sup_{x\in I} \left|R_n(x)\right|$, qui est un majorant. D'où, $0 \leqslant \sup_{x\in I} |f_n(x)| \leqslant \sup_{x\in I} |R_{n-1}(x)| + \sup_{x\in I} |R_n(x)| \xrightarrow[n\to\infty]{} 0$. Donc, par théorème d'existence de la limite par encadrement, $\sup_{x\in I} |f_n(x)| \xrightarrow[n\to\infty]{} 0$. □

Exercice :
Soit, pour $n \in \mathbb{N}$, $f_n(x) = x^n$. Montrer que

1. *la série de fonctions $\sum f_n$ converge simplement sur $]-1,1[$ vers la fonction $S : x \mapsto \frac{1}{1-x}$;*
2. *elle ne converge pas uniformément sur $]-1,1[$;*
3. *elle converge uniformément sur tout segment inclus dans $]-1,1[$.*

1. Soit $x \in]-1,1[$. On veut montrer que la série numérique $\sum f_n(x)$

converge vers le réel $\frac{1}{1-x}$. On calcule

$$\sum_{k=0}^{n} x^k = 1 + x + \cdots + x^n = \frac{1-x^{n+1}}{1-x} \text{ car } x \neq 1$$
$$\xrightarrow[n\to\infty]{} \frac{1}{1-x} \text{ car } |x| < 1.$$

1ÈRE MANIÈRE On va montrer que la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ ne converge pas uniformément vers la fonction nulle :

$$\sup_{x\in\,]-1,1[} \big|f_n(x) - 0\big| \not\xrightarrow[n\to\infty]{} 0.$$

On a, pour $x \in\,]-1,1[$, $|f_n(x) - 0| = |x^n|$. Or, $\sup_{x\in\,]-1,1[} |x^n| = 1 \not\xrightarrow[n\to\infty]{} 0$. D'où, la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ ne converge pas uniformément vers la fonction nulle. Ainsi, d'après la méthode 4, la série $\sum f_n$ ne converge pas uniformément sur $]-1,1[$.

2NDE MANIÈRE La série de fonctions $\sum f_n$ converge uniformément vers S sur $]-1,1[$ si, et seulement si la suite de fonctions $(S_n)_{n\in\mathbb{N}}$ converge uniformément vers S, donc si, et seulement si $\sup_{x\in\,]-1,1[} \big|S_n(x) - S(x)\big| \xrightarrow[n\to\infty]{} 0$. On calcule

$$\forall n, \forall x \in\,]-1,1[, \quad \big|S_n(x) - S(x)\big| = \left|\frac{1-x^{n+1}}{1-x} - \frac{1}{1-x}\right| = \left|\frac{x^{n+1}}{1-x}\right| = \frac{|x|^{n+1}}{1-x}.$$

D'où,

$$\sup_{x\in\,]-1,1[} \frac{|x|^{n+1}}{1-x} = +\infty \not\xrightarrow[n\to\infty]{} 0.$$

La série de fonctions $\sum f_n$ ne converge pas uniformément sur $]-1,1[$.

3ÈME MANIÈRE On a $\forall n \in \mathbb{N}$, $\forall x \in\,]-1,1[$, $\big|S_n(x) - S(x)\big| = \frac{|x|^{n+1}}{1-x}$. On pose, pour $n \in \mathbb{N}$, $u_n = 1 - \frac{1}{n+1}$. Montrons que $S_n(u_n) - S(u_n) \not\xrightarrow[n\to\infty]{} 0$. On calcule

$$\left|S_n\left(1-\frac{1}{n}\right) - S\left(1-\frac{1}{n}\right)\right| = \frac{\left(1-\frac{1}{n+1}\right)^{n+1}}{1-\left(1-\frac{1}{n}\right)} = (n+1)\times\left(1-\frac{1}{n+1}\right)^{n+1}.$$

Or, $\left(1-\frac{1}{n+1}\right)^{n+1} = \mathrm{e}^{(n+1)\ln\left(1-\frac{1}{n+1}\right)}$. Et,

$$(n+1)\ln\left(1-\frac{1}{n+1}\right) = (n+1)\left(\frac{-1}{n+1} + \wp\left(\frac{1}{n+1}\right)\right) = -1+\wp(1) \xrightarrow[n\to\infty]{} -1.$$

Ainsi, $\left(1-\frac{1}{n+1}\right)^{n+1} \longrightarrow \mathrm{e}^{-1}$ par continuité de la fonction exponentielle. Et donc, $S_n(u_n) - S(u_n) \xrightarrow[n\to\infty]{} +\infty$ car $n+1 \longrightarrow +\infty$ et $\left(1-\frac{1}{n+1}\right)^{n+1} \longrightarrow \mathrm{e}^{-1}$. Or, $\sup_{x\in\,]-1,1[} \big|S_n(x) - S(x)\big| \geqslant \big|S_n(u_n) - S(u_n)\big|$, et d'où $\sup_{x\in\,]-1,1[} \big|S_n(x) - S(x)\big| \not\xrightarrow[n\to\infty]{} 0$.

3. On considère l'intervalle $[\alpha, \beta] \subset]-1, 1[$. Sans perte de généralité, on choisit un segment $[-a, a]$ avec $0 < a < 1$. On veut montrer que $\sup_{x\in[-a,a]} \left|S_n(x) - S(x)\right| \xrightarrow[n\to\infty]{} 0$. On calcule

$$\forall x \in [-a, a],\ 0 \leqslant \left|S_n(x) - S(x)\right| = \frac{|x|^{n+1}}{1-x} \leqslant \frac{a^{n+1}}{1-a},$$

qui est un majorant. D'où, $0 \leqslant \sup_{x\in[-a,a]} \left|S_n(x) - S(x)\right| \leqslant \frac{a^{n+1}}{1-a} \xrightarrow[n\to\infty]{} 0$ car $|a| < 1$. Donc, d'après le théorème d'existence de la limite par encadrement,

$$\sup_{x\in[-a,a]} \left|S_n(x) - S(x)\right| \xrightarrow[n\to\infty]{} 0.$$

VII.1.2 Convergence normale

Définition : On dit qu'une série de fonctions $\sum f_n$ *converge normalement* sur $I \subset \mathbb{R}$ s'il existe une suite de réels $(u_n)_{n\in\mathbb{N}}$ tels que $\forall n, \forall x, |f_n(x)| \leqslant u_n$, et que la série (numérique) des $\sum u_n$ converge.

Proposition : La série de fonctions $\sum f_n$ converge normalement si, et seulement si la série numérique $\sum \sup |f_n|$ converge.

Preuve " $\Longleftarrow$ " Soit, pour $n \in \mathbb{N}$, $u_n = \sup_{x\in I} |f_n(x)|$. Alors $u_n \geqslant |f_n(x)|$, $\forall x$. D'où, comme la série $\sum u_n$ converge, alors $\sum f_n$ converge normalement.

" $\Longrightarrow$ " $\sup_{x\in I} |f_n(x)|$ est un majorant, et c'est le plus petit. D'où, $\not< \sup_{x\in I} |f_n(x)|$, qui est un majorant. Or, $\sum u_n$ converge, donc $\sum \sup_{x\in I} |f_n(x)|$.

□

Proposition : On a

convergence simple $\underset{\not\Longrightarrow}{\Longleftarrow}$ convergence uniforme $\underset{\not\Longrightarrow}{\Longleftarrow}$ convergence normale..

Preuve :
Montrons convergence normale $\Longrightarrow$ convergence uniforme. Les autres cas ont déjà été traités au chapitre précédent. Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions dont la série $\sum f_n$ converge normalement. Montrons que la série de fonctions converge uniformément, *i.e.*, $\sup_{x\in I} |R_n(x)| \xrightarrow[n\to\infty]{} 0$. Comme la série de fonctions $\sum f_n$ converge normalement, il existe une suite $(u_n)_{n\in\mathbb{N}}$ telle que $\forall n,\ \forall x,\ |f_n(x)| \leqslant u_n$, et la série numérique $\sum u_n$ converge. On

calcule

$$\left|R_n(x)\right| = \Big|\sum_{k=n+1}^{\infty} f_k(x)\Big| \leqslant \sum_{k=n+1}^{\infty} |f_k(x)| \leqslant \sum_{k=n+1}^{\infty} u_n,$$

qui est un majorant. ($R_n(x)$ existe car la série de réels $\sum f_n(x)$ converge car $\sum |f_n(x)|$ converge car $|f_n(x)| \leqslant u_n$, et $\sum u_n$ converge. Également, le reste $\sum_{k=n+1}^{\infty} |f_k(x)|$ existe car la série numérique $\sum |f_k(x)|$ converge.) D'où, $0 \leqslant \sup_{x\in I} |R_n(x)| \leqslant \sum_{k=n+1}^{\infty} u_k$, qui tend vers 0 car tout reste d'une série numérique convergente tend vers 0. D'après le théorème d'existence de la limite par encadrement, $\sup_{x\in I} |R_n(x)| \xrightarrow[n\to\infty]{} 0$. □

Exercice :
Soit, pour $n \in \mathbb{N}^\star$, la fonction

$$\begin{aligned} f_n : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{(-1)^n}{n+x^2}. \end{aligned}$$

Montrer que

1. *la série des fonctions $\sum f_n$ converge simplement sur $\mathbb{R}$*
2. *elle ne converge pas normalement sur $\mathbb{R}$*
3. *elle converge uniformément sur $\mathbb{R}$*

1. Soit $x \in \mathbb{R}$. La série numérique $\sum f_n(x)$ est une série alternée. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par, pour $n \in \mathbb{N}$, $\frac{1}{n+x^2}$. Cette suite tend vers 0 et est décroissante ($u_{n+1} \leqslant u_n$). D'où, d'après le théorème des séries alternées, la série numérique $\sum (-1)^n u_n$ converge. Ainsi, la série de fonctions $\sum f_n$ converge simplement sur $\mathbb{R}$.
2. La convergence n'est pas normal car $|f_n(x)| = \frac{1}{n+x^2}$. Or, $\sum |f_n(x)| = \sum \frac{1}{n+x^2}$ diverge car $\frac{1}{n+x^2} \sim \frac{1}{n}$ qui ne change pas de signe, et $\sum \frac{1}{n}$ par critère de Riemann. Donc, la série $\sum f_n$ ne converge pas normalement.
3. La convergence est uniforme car la suite des restes $\big(R_n(x)\big)_{n\in\mathbb{N}}$ converge uniformément vers 0. On a, pour $n \in \mathbb{N}^\star$, $R_n(x) = \sum_{k=n+1} \frac{(-1)^n}{k+x^2}$. On veut montrer que $\sup_{x\in\mathbb{R}} |R_n(x)| \longrightarrow 0$. On sait que, pour tout $n \in \mathbb{N}^\star$, pour tout $x \in \mathbb{R}$, $|R_n(x)| \leqslant \frac{1}{n+1+x^2} \leqslant \frac{1}{n+1}$, qui est un majorant. D'où, $\sup_{x\in\mathbb{R}} |R_n(x)| \leqslant \frac{1}{n+1}$, qui tend vers 0. D'après le théorème d'existence de la limite par encadrement, $\sup_{x\in\mathbb{R}} |R_n(x)|$ tend vers 0.

VII.2 Continuité

Théorème : Soient I un intervalle de $\mathbb{R}$ et $a \in I$. Soit, pour chaque $n \in \mathbb{N}$, une fonction f_n continue en a. Si la série de fonctions $\sum f_n$ converge uniformément sur I vers une fonction S, alors S est aussi continue en a.

Preuve :
On pose, pour $n \in \mathbb{N}$, la somme partielle $S_n(x) = \sum_{k=0}^{n} f_k(x)$. Comme chaque fonction f_n est continue, alors S_n est continue. Or, comme la série de fonctions converge uniformément, on en déduit que la suite $(S_n)_{n\in\mathbb{N}}$ converge uniformément. Donc, par transmission de la continuité par convergence uniforme, la fonction $S : x \mapsto \sum_{n=0}^{\infty} f_n(x)$ est continue. □

Corollaire : Une série de fonctions continue uniformément convergente, converge vers une fonction continue.

Exercice :
Soit la série de fonctions $\sum x^n(1-x)$. (Soit $\forall n, \forall x,\ f_n(x) = x^n(1-x)$.) *Montrons que* $\sum f_n$ *converge simplement mais pas uniformément.*

Soit $x \in [0,1]$. La série numérique $\sum f_n(x) = \sum x^n(1-x) = (1-x)\sum x^n$ converge car, si $x \in [0,1[$, alors $\sum x^n$ converge, et si $x = 1$, alors $\sum x^n(1-x) = \sum 0$ qui converge. Donc $\sum f_n$ converge simplement sur $[0,1]$.

Mais, chaque fonction $(f_n)_{n\in\mathbb{N}}$ est continue (c'est un polynôme), tandis que la somme ne l'est pas. En effet,

$$\forall x \in [0,1], \quad S(x) = \sum_{n=0}^{\infty} f_n(x) = \sum_{n=0}^{\infty} x^n(1-x).$$

Or, si $x = 1$, alors $S(x) = 0$. Et, si $x \neq 1$, $\sum_{k=0}^{\infty} x^n(1-x) = (1-x)\sum_{k=0}^{\infty} = (1-x)\cdot\frac{1}{1-x} = 1$. La fonction S n'est pas continue. Donc la convergence n'est pas uniforme.

Théorème (double-limite/interversion somme-limite) **:** Soit une suite de fonction $(f_n)_{n\in\mathbb{N}}$ de I et soit $a \in \bar{\mathbb{R}}$, une extrémité de I. Si la série de fonctions $\sum f_n$ converge uniformément sur I, vers une fonction S et si chaque fonction f_n admet une limite finie b_n en a, alors la série numérique $\sum b_n$ converge et $\lim_{x\to a} S(x) = \sum_{n=0}^{\infty} b_n$. Autrement dit,

$$\lim_{x\to a} \sum_{n=0}^{\infty} f_n(x) = \sum_{n=0}^{\infty} \lim_{x\to a} f_n(x).$$

Preuve :
On pose, pour $n \in \mathbb{N}$, $S_n(x) = \sum_{k=0}^{n} f_k(x)$. La suite $(S_n)_{n\in\mathbb{N}}$ converge uniformément sur I. Également, on a $S_n(x) \xrightarrow[x\to a]{} \sum_{k=0}^{n} b_j$, car c'est une somme finie de limites. D'où, d'après le théorème de la double-limite pour

les suites de fonctions (théorème 9 du chapitre précédent), on a

$$\lim_{x\to a} \underbrace{\lim_{n\to\infty} S_n(x)}_{\sum_{k=0}^{\infty} f_k(x)} = \lim_{n\to\infty} \lim_{x\to a} S_n(x).$$

Aussi, $\lim_{n\to\infty} \lim_{x\to a} S_n(x) = \lim_{n\to\infty} \Big(\lim_{x\to a} \sum_{k=0}^{n} f_k(x) \Big)$. Or, comme la somme $\sum_{k=0}^{n} f_k(x)$ est finie, et que *la limite d'une somme finie est la somme des limites*, on a donc

$$\lim_{x\to a} \sum_{n=0}^{\infty} f_n(x) = \lim_{n\to\infty} \Big(\sum_{k=0}^{n} \lim_{x\to a} f_k(x) \Big) = \sum_{k=0}^{\infty} \lim_{x\to a} f_k(x).$$

□

Exercice :
On pose la fonction S définie par

$$\begin{aligned} S : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \sum_{n=1}^{\infty} \frac{(-1)^n}{n+x^2}. \end{aligned}$$

Montrer, de deux manières, que $\lim_{x\to+\infty} S(x) = 0$.

On a déjà montré, dans l'exercice 8, que la série de fonctions $\sum f_n$ converge uniformément en notant $f_n : x \mapsto \frac{(-1)^n}{n+x^2}$. D'une part, la série de fonctions converge uniformément sur $]-\infty, +\infty[$. D'autre part, $\forall n$, $\lim_{x\to+\infty} f_n(x) = 0 \in \mathbb{R}$. D'où, d'après le théorème d'interversion somme-limite,

$$\lim_{x\to+\infty} S(x) = \sum_{n=1}^{\infty} \lim_{x\to+\infty} f_n(x) = \sum_{n=1}^{\infty} 0 = 0.$$

Autre méthode (sans le théorème d'interversion somme-limite, avec le théorème des séries alternées) : on a montré dans l'exercice 8, que $\frac{1}{n+x^2}$ tend vers 0 (quand $n \to \infty$) en décroissant, donc, d'après le théorème des séries alternées, la série numérique $\sum \frac{(-1)^n}{n+x^2}$ converge. De plus, encore d'après le TSA,

$$\forall x \in \mathbb{R}, \quad -\frac{1}{1+x^2} \leqslant S(x) \leqslant -\frac{1}{1+x^2} + \frac{1}{2+x^2}.$$

Or, $-\frac{1}{1+x^2} \xrightarrow[x\to+\infty]{} 0 \xleftarrow[x\to+\infty]{} -\frac{1}{1+x^2} + \frac{1}{2+x^2}$. Donc, d'après le théorème d'existence de la limite par encadrement, $S(x) \xrightarrow[x\to+\infty]{} 0$.

VII.3 Intégrer

Théorème : Soit une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ définies sur un segment $[a, b]$. Si la série de fonctions $\sum f_n$ converge uniformément vers S, alors S

est continue sur $[a,b]$ et

$$\int_a^b S(t)\ \mathrm{d}t = \int_a^b \sum_{n=0}^{\infty} f_n(t)\ \mathrm{d}t = \sum_{n=0}^{\infty} \int_a^b f_n(t)\ \mathrm{d}t.$$

Preuve :
On pose, pour $n \in \mathbb{N}$, $S_n(x) = \sum_{k=1}^{n} f_k(x)$. Comme la série de fonctions $\sum f_n$ converge uniformément sur $[a,b]$, alors la suite de fonctions $(S_n)_{n\in\mathbb{N}}$ converge uniformément sur $[a,b]$. Aussi, chaque fonction S_n est continue (car c'est une somme finie de fonctions continues). D'où, d'après le théorème d'interversion somme-intégrale (pour les suites de fonctions), on a

$$\int_a^b \underbrace{\lim_{n\to\infty} S_n(x)}_{\sum_{n=0}^{\infty} f_n(x)}\ \mathrm{d}x = \lim_{n\to\infty} \int_a^b S_n(x)\ \mathrm{d}x.$$

Or, comme la somme $S_n(x)$ est finie, on peut intervertir somme et intégrale : $\lim_{n\to\infty} \int_a^b \sum_{k=0}^{n} f_k(x)\ \mathrm{d}x = \lim_{n\to\infty} \sum_{k=0}^{n} \int_a^b f_k(x)\ \mathrm{d}x = \sum_{n=0}^{\infty} \int_a^b f_k(x)\ \mathrm{d}x$. □

Ce théorème s'appelle le *théorème d'intégration terme à terme*. Ceci rappelle le théorème d'intégration terme à terme pour les développements limités : si $f(x) = a_0 + a_1 x + \cdots + a_n x^n + \mathrm{o}(x^n)$, alors

$$\begin{aligned}\int_0^x f(t)\ \mathrm{d}t &= \int_0^x \left(a_0 + a_1 x + \cdots + a_n t^n + \mathrm{o}(t^n)\right)\ \mathrm{d}t \\ &= a_0 x + a_1 \frac{x^2}{2} + \cdots a_n \frac{t^{n+1}}{n+1} + \mathrm{o}(x^{n+1}).\end{aligned}$$

Exercice :
Soit $x \in]-1,1[$. On pose, pour tout n, $f_n(t) = t^n$ continue. La série de fonctions $\sum f_n$ converge uniformément sur le segment $[0,x]$ (ou $[x,0]$ si $x<0$), car elle converge normalement sur $[0,x]$. En effet, $\forall n \in \mathbb{N}$, $\forall t \in [0,x]\cup[x,0]$, $|f_n(t)| \leqslant |x|^n$ qui ne dépend pas de t. Et, la série numérique $\sum |x|^n$ converge car c'est une série géométrique de raison $|x| \in]-1,1[$. D'où, on peut intégrer $\frac{1}{1-x} = \sum_{k=0}^{\infty} x^n$ terme à terme :

$$-\ln(1-x) = \sum_{k=0}^{\infty} \frac{x^{n+1}}{n+1}.$$

Théorème (intégration terme-à-terme sur un intervalle quelconque) **:** Soit I un intervalle, et soit une suite de fonctions continues par morceaux et intégrables sur I. Si

1. la série de fonctions $\sum f_n$ converge simplement sur I vers une fonction S continue par morceaux sur I ;

2. la série de réels $\sum \int_I |f_n(t)| \, \mathrm{d}t$ converge,

alors S est intégrable et

$$\sum_{i=1}^{\infty} \int_I f_n(t) \, \mathrm{d}t = \int_I S(t) \, \mathrm{d}t.$$

Ce théorème est admis, et la preuve n'utilise pas le théorème de la convergence dominée.

Exercice :
Montrer que l'intégrale $\int_0^{+\infty} \frac{x}{\mathrm{e}^x - 1} \, \mathrm{d}x$ *est convergente, et qu'elle vaut* $\sum_{i=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$.

L'intégrale $\int_0^{+\infty} \frac{x}{\mathrm{e}^x - 1} \, \mathrm{d}x$ est impropre. Elle converge si et seulement si les deux intégrales $I = \int_0^1 \frac{x}{\mathrm{e}^x - 1} \, \mathrm{d}x$ converge et $J = \int_1^{+\infty} \frac{x}{\mathrm{e}^x - 1} \, \mathrm{d}x$ converge. On a $\frac{x}{\mathrm{e}^x - 1} \sim_{x \to +\infty} \frac{x}{\mathrm{e}^x} = \frac{x}{\mathrm{e}^{x/2}} \times \frac{1}{\mathrm{e}^{x/2}} = \wp(\mathrm{e}^{-x/2})$, et $\mathrm{e}^{-x/2}$ ne change pas de signe. Or, l'intégrale $\int_1^{+\infty} \mathrm{e}^{-x/2} \, \mathrm{d}x$ converge, d'où J aussi. On a $\mathrm{e}^x = 1 + x + \wp_{x \to 0}(x)$, d'où $\mathrm{e}^x - 1 = x + \wp(x) \sim_{x \to o} x$. Donc, $\frac{x}{\mathrm{e}^x - 1} \sim_{x \to 0} 1$ d'où, $\frac{x}{\mathrm{e}^x - 1} \longrightarrow 1$, donc l'intégrale I est faussement impropre en 0, donc convergente.

Calculons sa valeur. On a $x/(\mathrm{e}^x - 1) = x\mathrm{e}^{-x}/(1 - \mathrm{e}^{-x})$, et $\mathrm{e}^{-x}/(1 - \mathrm{e}^{-x}) = \mathrm{e}^{-x} \sum_{k=0}^{\infty} (\mathrm{e}^{-x})^k$ pour tout $x \in]0, +\infty[$, car la série $\sum (\mathrm{e}^{-x})^k$ est une série géométrique dont la raison e^{-x}, en valeur absolue, est strictement inférieure à 1. D'où

$$\int_0^{+\infty} \frac{x}{\mathrm{e}^x - 1} \, \mathrm{d}x = \int_0^{+\infty} \Big(\sum_{k=1}^{\infty} x\mathrm{e}^{-x} \Big) \, \mathrm{d}x.$$

En effet, on calcule l'intégrale suivante à l'aide d'une intégration par parties :

$$\int_0^y x \, \mathrm{e}^{-kx} \, \mathrm{d}x = \left[-\frac{x\mathrm{e}^{-kx}}{k} \right]_0^y - \int_0^y \left(-\frac{1}{k} \mathrm{e}^{-kx} \right) \, \mathrm{d}x \xrightarrow[y \to +\infty]{} -\frac{1}{k^2}.$$

On vérifie à présent les hypothèses d'intégration terme-à-terme sur un intervalle quelconque. Chaque fonction

$$\begin{aligned} f_k :]0, +\infty[&\longrightarrow \mathbb{R} \\ x &\longmapsto x\mathrm{e}^{-kx} \end{aligned}$$

est intégrable sur $]0, +\infty[$ car $\int_0^{+\infty} |f_k(x)| \, \mathrm{d}x = \int_0^{+\infty} x\mathrm{e}^{-kx} \, \mathrm{d}x$ qui converge (en *coupant l'exponentielle en deux*). La série de fonctions $\sum f_k$ converge simplement sur $]0, +\infty[$ car, soit $x > 0$, $\sum f_k(x) = \sum x\mathrm{e}^{-kx}$ converge (en *coupant l'exponentielle en deux*). La série numérique $\sum \int_{\mathbb{R}_\star^+} |f_k(t)| \, \mathrm{d}t$ converge car $\sum \frac{1}{k^2}$ converge.

VII.4 Dériver

Théorème (dérivation terme à terme) **:** Si toute fonction f_n est de classe $\mathscr{C}^1$, que la série de fonctions $\sum f_n$ converge simplement sur $[a,b]$, et que la série de fonctions $\sum f'_n$ converge uniformément sur $[a,b]$, alors

$$\frac{\mathrm{d}}{\mathrm{d}x}\sum_{k=0}^{\infty} f_n(x) = \sum_{k=0}^{\infty} \frac{\mathrm{d}}{\mathrm{d}x} f_n(x).$$

Preuve :
On pose, pour $n \in \mathbb{N}$, $S_n(x) = \sum_{k=0}^{n} f_k(x)$. La suite de fonctions $(S_n)_{n\in\mathbb{N}}$ converge simplement vers une fonction S. Et, la suite de fonctions $(S'_n)_{n\in\mathbb{N}}$ converge uniformément vers S'. Donc, d'après le théorème d'interversion dérivée-limite, on a

$$\frac{\mathrm{d}}{\mathrm{d}x}\underbrace{\lim_{n\to\infty} S_n(x)}_{\sum_{k=0}^{\infty} f_k(x)} = \lim_{n\to\infty} \frac{\mathrm{d}}{\mathrm{d}x} S_n(x).$$

Et, $\frac{\mathrm{d}}{\mathrm{d}x} S_n(x) = \sum_{k=0}^{n} \frac{\mathrm{d}}{\mathrm{d}x} f_n(x)$ car c'est une somme finie. D'où,

$$\frac{\mathrm{d}}{\mathrm{d}x}\sum_{k=0}^{\infty} f_k(x) = \lim_{n\to\infty}\sum_{k=0}^{n} \frac{\mathrm{d}}{\mathrm{d}x} f_n(x) = \sum_{k=0}^{\infty} \frac{\mathrm{d}}{\mathrm{d}x} f_n(x).$$

□

Chapitre 7

Probabilités

VII.0 Dénombrabilité

Remarque :
Un ensemble E est dit *dénombrable* s'il existe une bijection de E dans $\mathbb{N}$. L'ensemble $\mathbb{Z}$ des entiers relatifs, [1] et l'ensemble $\mathbb{N}^2$ des couples d'entiers [2] sont dénombrables.

Par suite, le produit cartésien $E \times F$ de deux ensembles dénombrables E et F est aussi dénombrable. Mieux : une union dénombrable d'ensembles dénombrable est aussi dénombrable.

Ainsi, on peut en conclure que $\mathbb{Q} = \cup_{\substack{p\in\mathbb{Z}\\ q\in\mathbb{N}^\star}} \frac{p}{q}$ est dénombrable car cet union est dénombrable.

Mais, $\mathbb{R}$ n'est pas dénombrable.

Preuve (**une** preuve de Cantor pour la non-dénombrabilité de $\mathbb{R}$) *:*
Par l'absurde, on suppose $\mathbb{R}$ dénombrable. On pose donc $\mathbb{R} = \{u_0, u_1, u_2, \ldots\}$. On construit par récurrence une suite $(a_n)_{n\in\mathbb{N}}$ croissante majorée par 1 et et une suite $(b_n)_{n\in\mathbb{N}}$ décroissante minorée par 0, telles que $u_n \notin [a_{n+1}, b_{n+1}]$. Donc, $(a_n)_{n\in\mathbb{N}}$ converge vers un réel A, et de même $(b_n)_{n\in\mathbb{N}}$ converge vers un réel B. Or, par construction, $\nexists n, A = u_n$.

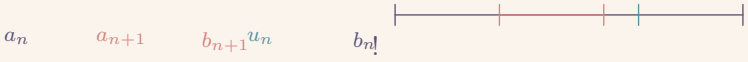


Figure 7.1 – Démonstration de la non-dénombrabilité de $\mathbb{R}$

1. on compte sur chaque côtés simultanément : l'application

$$k \longmapsto \begin{cases} 2k-1 & \text{si } k > 0 \\ -2k & \text{si } k \leqslant 0 \end{cases}$$

est bijective.

2. On place les entiers sur les diagonales : l'application $(x, y) \mapsto \sum_{k=1}^{x+y} k + y$ de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ est bijective.

□

VII.1 Résultats et événements

Exemple :
« On lance un dé » est une expérience aléatoire. Son univers (des résultats possibles) est $\Omega = [\![1, 6]\!]$.

« Le dé est tombé sur un numéro pair » est l'événement $E = \{2, 4, 6\} \subset \wp(\Omega)$. Un événement, c'est l'ensemble des résultats favorables à cet événement. « Le dé est tombé sur 3 » est aussi un événement (c'est l'événement $\{3\}$), et non un résultat 3.

Vocabulaire des probabilités	Notation	Vocabulaire des ensembles
Événement certain	Ω	Univers
Événement impossible		Ensemble vide
Événement contraire	$\Omega \setminus A = \bar{A}$	Complémentaire
Événement élémentaire	$\{\omega\}$	Singleton
A implique B	$A \subset B$	A est une partie de B
Le résultat ω réalise l'événement A	$\omega \in A$	ω appartient à A
ET	$\cap$	Intersection
OU	$\cup$	Réunion (ou union)
Événements incompatibles	$A \cap B =$	Parties disjointes

Table 7.1 – Traduction vocabulaire ensembles-probabilités

Remarque (unions et intersections) :
Par définition,

$$\omega \in \bigcap_{i \in I} A_i \iff \forall i \in I, \omega \in A_i$$

et

$$\omega \in \bigcup_{i \in I} A_i \iff \exists i \in I, \omega \in A_i.$$

On dit que l'union $\bigcup_{i \in I} A_i$ est *disjointe* si les ensembles événements A_i sont disjoints deux à deux : $\forall i \neq j$, $A_i \cap A_j =$ *i.e.* les événements A_i et A_j sont incompatibles ($\neq$ indépendants). On note alors cette union $\bigsqcup_{i \in I} A_i$.

L'opération $\cup$ est distributive par rapport à l'opération $\cap$, et l'opération $\cap$ est distributive par rapport à l'opération$\cup$.

Exercice :
Voici une expérience aléatoire. On lance une pièce indéfiniment. À chaque lancer, la pièce tombe sur Pile *ou* Face. *Quel est lunivers Ω de cette expérience ?*

L'ensemble Ω est l'ensemble des résultats, et un résultat est une suite de Pile ou Face. D'où, $\Omega = \{\text{Pile}, \text{Face}\}^{\mathbb{N}}$.

On pose, pour tout $n \in \mathbb{N}^\star$, les événements A_n : « le premier Face *est au n-ième lancer » et B_n : « les n premiers lancers donnent* Pile. »

1. *Quel est l'événement* $\bigcup_{n\in\mathbb{N}^\star} A_n$ *?* Cet événement correspond à « la pièce est tombée au moins une fois sur FACE. » Cette union est disjointe.
2. *Quel est l'événement* $\bigcap_{n\in\mathbb{N}^\star} B_n$ *?* Cet événement correspond à « on n'obtient que des PILES. »
3. *Exprimer* $\bar{B}_n$ *en fonction des événements* A_k. On a $\bar{B}_n = \bigcup_{k=1}^{n} A_k$.
4. *Quel est l'événement* $B_n \cap \bar{B}_{n+1}$ *?* On a $B_n \cap \bar{B}_{n+1} = A_{n+1}$.

Définition : Soit un ensemble Ω. On dit qu'une partie $\mathcal{A}$ de $\wp(\Omega)$ est une *tribu* sur Ω si :

1. $\Omega \in \mathcal{A}$;
2. si $A \in \mathcal{A}$, alors $\bar{A} \in \mathcal{A}$; (stabilité par passage au complémentaire)
3. si $\forall n \in \mathbb{N}$, $A_n \in \mathcal{A}$, alors $\bigcup_{n\in\mathbb{N}} A_n \in \mathcal{A}$. (stabilité par union dénombrable)

On appelle *événement* tout élément de la tribu.

Proposition : Il en résulte que

1. $\in \mathcal{A}$;
2. si $\forall n \in \mathbb{N}$, $A_n \in \mathcal{A}$, alors $\bigcap_{n\in\mathbb{N}} A_n \in \mathcal{A}$;
3. si $A \in \mathcal{A}$ et $B \in \mathcal{A}$, alors $A \setminus B \in \mathcal{A}$.

Preuve : 1. On a $\bar{\Omega} =$.
2. On a $\overline{\bigcap_{n\in\mathbb{N}} B_n} = \bigcup_{n\in\mathbb{N}} \bar{B}_n$, et $\forall n \in \mathbb{N}$, $\bar{B}_n \in \mathcal{A}$.
3. L'ensemble $A \setminus B$, c'est l'ensemble des éléments qui sont dans A sans être dans B. On a donc $A \setminus B = A \cap \bar{B}$.

□

VII.2 Probabilité

Définition : Le couple $(\Omega, \mathcal{A})$ est appelé *espace probabilisable*. On le munit d'une probabilité P (définie ci-dessous). Ainsi, le triplet $(\Omega, \mathcal{A}, P)$ est dit *espace probabilisable*.

Une *probabilité* P sur $(\Omega, \mathcal{A})$ est une application $P : \mathcal{A} \longrightarrow [0,1]$ telle que

1. $P(\Omega) = 1$;
2. Pour toute suite $(A_n)_{n\in\mathbb{N}}$ d'événements deux-à-deux incompatibles,
$$P\Big(\bigcupdot_{n\in\mathbb{N}} A_n\Big) = \sum_{n\in\mathbb{N}} P(A_n). \qquad (\sigma\text{-additivité}).$$

REMARQUE :
Une union, finie ou dénombrable, est toujours commutative et on peut donc

la notera indifféremment $\bigcup_{n\in\mathbb{N}}$ ou $\bigcup_{n=1}^{\infty}$. Une somme finie de scalaires est commutative, une somme dénombrable aussi si la série est absolument convergente (c'est le cas de la série $\sum P(A_n)$ dans la définition précédente) : on peut noter indifféremment $\sum_{n=0}^{\infty}$ ou $\sum_{n\in\mathbb{N}}$.

Proposition : 1. $P() = 0$.

2. Pour toute suite finie $(A_1, \dots, A_n) \in \mathscr{A}^n$ d'événements deux-à-deux incompatibles,
$$P\Big(\dot{\bigcup_{i=1}^{n}} A_n\Big) = \sum_{i=1}^{n} P(A_n) \qquad \text{(additivité).}$$
3. Pour tout événement $A \in \mathscr{A}$, $P(\bar{A}) = 1 - P(A)$.
4. Pour tout couple $(A, B) \in \mathscr{A}^2$ d'événements,
$$A \subset B \implies P(A) \leqslant P(B). \qquad \text{(croissance de la probabilité)}$$
5. Pour tout couple $(A, B) \in \mathscr{A}^2$ d'événements, $P(A \cup B) = P(A) + P(B) + P(A \cap B)$.
6. Pour toute famille finie d'événements $(A_1, \dots, A_n) \in \mathscr{A}^n$,
$$P\Big(\bigcup_{n=1}^{n} A_n\Big) \leqslant \sum_{n=1}^{n} P(A_n) \qquad \text{(sous-additivité).}$$

Preuve : 1. On utilise le point 3. : $P() = P(\bar{\Omega}) = 1 - P(\Omega) = 0$.

2. *c.f.* poly
3. On utilise le point 5. : $1 = P(A \cup \bar{A}) = P(A) + P(\bar{A}) + P(A \cap \bar{A}) = P(A) + P(\bar{A})$, d'où $P(\bar{A}) = 1 - P(A)$.
4. Si $A \subset B$, on a $B = A \cup (B \setminus A)$, et donc $P(B) = P(A) + P(B \setminus A) \geqslant P(A)$.
5. On a, d'une part $A = (A \cap B) \cup (A \setminus B)$, donc $P(A) = P(A \cap B) + P(A \setminus B)$, et d'autre part, $B = (B \cap A) \cup (B \setminus A)$, d'où $P(B) = P(B \cap A) + P(B \setminus A)$. Or, $(A \setminus B) \cup (B \setminus A) \cup (A \cap B) = A \cup B$, d'où
$$P(A \setminus B) + P(B \setminus A) + P(A \cap B).$$

□

VII.3 La continuité (dé)croissante

Théorème : Soit $(A_n)_{n\in\mathbb{N}}$ une suite d'événements.

1. Si $\forall n$, $A_n \subset A_{n+1}$, alors $P\Big(\bigcup_{n\in\mathbb{N}} A_n\Big) = \lim_{n\to\infty} P(A_n)$. (continuité croissante)
2. Si $\forall n$, $A_n \supset A_{n+1}$, alors $P\Big(\bigcap_{n\in\mathbb{N}} A_n\Big) = \lim_{n\to\infty} P(A_n)$. (continuité décroissante)

Preuve :
On crée une suite d'événements $(B_n)_{n\in\mathbb{N}}$: on pose $B_0 = A_0$, et pour $n \in \mathbb{N}^\star$, on pose $B_n = A_{n+1} \setminus A_n$. L'union $\bigcup_{n\in\mathbb{N}} B_n$ est disjointe. D'où

$$P\Big(\bigcup_{n\in\mathbb{N}}^{\cdot} B_n\Big) = \sum_{n=0}^{\infty} P(B_n) = \lim_{N\to\infty} \sum_{n=0}^{N} P(B_n).$$

De plus, $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in B_n}$, d'où $P\big(\bigcup_{n\in\mathbb{N}} A_n\big) = P\big(\bigcap_{n\in\mathbb{N}} B_n\big)$. Enfin (télescope), comme $A_n = A_{n-1} \cup B_n$ (par construction), d'où

$$P(A_n) = P(A_{n-1}) + P(B_n) \quad \textit{i.e.} \quad P(B_n) = P(A_n) - P(A_{n-1})$$

Ainsi, $\sum_{n=0}^{N} P(B_n) = P(A_N) - P(A_0) + P(B_0) = P(A_N)$. On en déduit que

$$P\Big(\bigcup_{n\in\mathbb{N}} A_n\Big) = \lim_{n\to\infty} P(A_n).$$

Pour la continuité croissante, on passe au complémentaire *c.f.* poly. □

Corollaire : Pour toute suite $(B_n)_{n\in\mathbb{N}}$ d'événements, on a

$$P\Big(\bigcup_{n\in\mathbb{N}} B_n\Big) = \lim_{n\to\infty} P\Big(\bigcup_{k=1}^{n} B_k\Big) \quad \text{et} \quad P\Big(\bigcap_{n\in\mathbb{N}} B_n\Big) = \lim_{n\to\infty} P\Big(\bigcap_{k=1}^{n} B_n\Big).$$

Preuve :
Soit $A_n = \bigcup_{k=1}^{n} B_k$, alors $A_{n+1} = A_n \cup B_{n+1}$, d'où $A_{n+1} \subset A_n$. Et, $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} B_n$. On conclut à l'aide du théorème 10. □

Exercice :
On lance indéfiniment une pièce qui tombe de manière équiprobable sur Pile *ou* Face. *Montrer que la probabilité d'obtenir toujours* Pile *est nulle.*

On pose l'événement A_n : « la pièce est tombée sur Pile aux n premiers lancers. » Ainsi, l'événement « obtenir toujours Pile » vaut $E = \bigcap_{n\in\mathbb{N}^\star} A_n$. On a aussi $A_{n+1} \subset A_n$. D'où, par continuité décroissante, $P(E) = \lim_{n\to\infty} P(A_n)$. Or, il y a équiprobabilité, d'où

$$P(A_n) = \frac{\#\text{ résultats favorables}}{\#\text{ résultats possibles}} = \frac{\mathrm{Card}(A_n)}{\mathrm{Card}(\Omega)} = \frac{1}{2^n}.$$

On en déduit que $P(E) = \lim_{n\to\infty} 2^{-n} = 0$.

L'événement E n'est pas impossible ($E \neq \emptyset$) mais sa probabilité est nulle.

Définition : On dit qu'un événement est :
- *négligeable* ou *presque impossible* si sa probabilité est nulle ;
- *presque certain* si sa probabilité vaut 1.

Proposition (σ-sous-additivé) **:** Soit $(A_n)_{n\in\mathbb{N}}$ une suite d'événements. Si la série $\sum P(A_n)$ converge, alors

$$P\Big(\bigcup_{n\in\mathbb{N}} A_n\Big) \leqslant \sum_{n\in\mathbb{N}} P(A_n).$$

Preuve :
Par récurrence avec $P(A\cup B)\leqslant P(A)+P(B)$, on peut démontrer que

$$P\Big(\bigcup_{n=1}^{N} A_n\Big) \leqslant \sum_{n=1}^{N} P(A_n).$$

Montrons que les limites, quand $N\to\infty$, existent.
- $\lim_{n\to\infty}\sum_{k=0}^{n} P(A_k)$ existe par hypothèse.
- D'après le théorème de la continuité croissante (corolaire 11), on a $\lim_{n\to\infty} P\big(\bigcup_{k=0}^{n} A_k\big) = P\big(\bigcup_{n\in\mathbb{N}} A_n\big)$.

□

Corollaire :
1. Une union finie ou dénombrable d'événements négligeables est un événement négligeable.
2. Une intersection finie ou dénombrable d'événements presque certains est un événement presque certain.

Preuve :
1. La série $\sum P(A_n) = \sum 0$ converge, et donc $0 \leqslant P\big(\bigcup_{n\in\mathbb{N}} A_n\big) \leqslant \sum_{n=0}^{\infty} 0 = 0$. On en déduit que $P\big(\bigcup_{n\in\mathbb{N}} A_n\big) = 0$.
2. On passe aux événements contraires : le contraire d'un événement presque certain est un événement négligeable et le contraire de l'union est l'intersection des contraires.

□

VII.4 L'indépendance

Définition : Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé.

On dit que deux événements $A, B \in \mathscr{A}$ sont *indépendants* si $P(A \cap B) = P(A) \times P(B)$.

On dit qu'une famille d'événements $(A_i)_{i\in I}$ est

— *deux-à-deux indépendants* si $\forall i \neq j,\ P(A_i \cap A_j) = P(A_i) \times P(A_j)$;

— *indépendants* si, pour toute partie $J \subset I$ **finie**,

$$P\Big(\bigcap_{j\in J} A_j\Big) = \prod_{j\in J} P(A_j).$$

Exercice : 1. *Si A et B indépendants, alors A et $\bar{B}$ aussi.* On a $P(A\cap B) = P(A)\times P(B)$. Or, $P(A\cap B)+P(A\cap\bar{B}) = P(A)$ car $(A\cap B)\cup(A\cap\bar{B}) = A$. D'où,

$$\begin{aligned} P(A\cap\bar{B}) &= P(A) - P(A\cap B)\\ &= P(A) - P(A)\times P(B) \text{ par hypothèse}\\ &= P(A)\times\big(1-P(B)\big)\\ &= P(A)\times P(\bar{B}) \end{aligned}$$

Donc A et $\bar{B}$ sont indépendants.

2. *Si A est presque impossible, alors A et B sont indépendants.* On suppose $P(A) = 0$. On veut montrer que $\forall B \in \mathscr{A}$, $P(A\cap B) = P(A)\times P(B) = 0$. Or, $A\cap B \subset A$, d'où, par croissance de la probabilité, $0 \leqslant P(A\cap B) \leqslant P(A) = 0$. On en déduit que $P(A\cap B) = 0 = P(A)\times P(B)$.

Exercice :
On considère deux lancers d'une pièce. On note les événements

— *A : « La pièce tombe la première fois sur Pile, »*

— *B : « La pièce tombe la deuxième fois sur Face, »*

— *C : « La pièce tombe au moins une fois sur Face, »*

— *D : « La pièce tombe deux fois du même côté. »*

Montrer que les événements A, B et D sont deux-à-deux indépendants et ne sont pas indépendants. Montrer que les événements A et C ne sont pas indépendants.

L'univers Ω de cette expérience est $\Omega = \{\mathbf{P},\mathbf{F}\}^2$ *i.e.* un résultat est un couple (u_1,u_2) où u_1 et u_2 appartiennent à $\{\mathbf{P},\mathbf{F}\}$. Et, il y a équiprobabilité.

On a $A = \{(\mathbf{P},\mathbf{P}),(\mathbf{P},\mathbf{F})\}$, d'où $P(A) = \dfrac{\operatorname{Card} A}{\operatorname{Card}\Omega} = \dfrac{2}{4} = \dfrac{1}{2}$. De même, $P(B) = \dfrac{1}{2}$.

On a $C = \{(\mathbf{P},\mathbf{F}),(\mathbf{F},\mathbf{P}),(\mathbf{F},\mathbf{F})\}$, d'où $P(C) = \dfrac{3}{4}$.

On a $D = \{(\mathbf{P},\mathbf{P}),(\mathbf{F},\mathbf{F})\}$, d'où $P(D) = \dfrac{2}{4} = \dfrac{1}{2}$.

— $A\cap B = \{(\mathbf{P},\mathbf{F})\}$, d'où $P(A\cap B) = \frac{1}{4} = \frac{1}{2}\times\frac{1}{2} = P(A)\times P(B)$.

— $B \cap D = \{(\mathbf{F}, \mathbf{F})\}$, d'où $P(B \cap D) = P(B) \times P(D)$.
— $A \cap D = \{(\mathbf{P}, \mathbf{P})\}$, d'où $P(A \cap D) = P(A) \times P(D)$.
— $A \cap B \cap D = $, mais $P(A) \times P(B) \times P(D) \neq 0 = P() = P(A \cap B \cap D)$.

Proposition : Soit $(B_n)_{n\in\mathbb{N}}$ une suite d'événements indépendants. On a

$$P\Big(\bigcap_{n\in\mathbb{N}} B_n\Big) = \lim_{n\to\infty} \prod_{k=0}^{n} P(B_k).$$

Preuve :
Par continuité décroissante, on sait que $P\big(\bigcap_{n\in\mathbb{N}} B_n\big) = \lim_{n\to\infty} P\big(\bigcap_{k=0}^{n} B_k\big)$. Or, les événements B_k sont indépendants, donc $P\big(\bigcap_{k=0}^{n} B_k\big) = \prod_{k=0}^{n} P(B_k)$. D'où

$$P\Big(\bigcap_{n\in\mathbb{N}}\Big) = \lim_{n\to\infty} \prod_{k=0}^{n} P(B_k).$$

□

VII.5 Probabilité conditionnelle

Proposition–Définition : Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé. Soient $A, B \in \mathcal{A}$ deux événements. Si la probabilité de l'événement A n'est pas nulle, alors

1. on appelle *probabilité de B sachant A*, et on note $P_A(B)$ ou $P(B \mid A)$, le rapport
$$P_A(B) = P(B \mid A) = \frac{P(A \cap B)}{P(A)} ;$$
2. l'application
$$\begin{aligned} P_A : \mathcal{A} &\longrightarrow [0,1] \\ B &\longmapsto P(B \mid A) \end{aligned}$$
est une probabilité sur l'espace probabilisable $(\Omega, \mathcal{A})$.

Preuve :
c.f. poly. □

Proposition : Soient A et B deux événements, où $P(A) \neq 0$.

1. Si A et B sont indépendants, alors $P(B) = P_A(B)$.
2. Si $A \subset B$, alors $P_A(B) = 1$.

Preuve : 1. On a $P_A(B) = P(A \cap B) \,/\, P(A) = P(A) \times P(B) \,/\, P(A) = P(B)$.
2. On a $A \cap B = A$, donc $P_A(B) = P(A \cap B) \,/\, P(A) = P(A) \,/\, P(A) = 1$.

□

Remarque :
Attention : $B \mid A$ n'est pas un événement, c'est une notation différente.
« Calculer une probabilité conditionnelle, c'est *changer d'observateur.* »

Exercice :
On lance deux fois une pièce. Calculer

1. *la probabilité que la pièce tombe deux fois sur Pile sachant qu'elle tombe la première fois sur Pile ;*
2. *la probabilité que la pièce tombe deux fois sur Pile sachant qu'elle tombe au moins une fois sur Pile.*

1. On note A l'événement « la pièce tombe deux fois sur Pile, » et B l'événement « la pièce tombe la première fois sur Pile. »
$$P_B(A) = P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{1/4}{1/2} = \frac{1}{2}.$$
2. On note C l'événement « la pièce tombe au moins une fois sur Pile. » Ainsi,
$$P(A \mid C) = \frac{P(A \cap C)}{P(C)} = \frac{1/4}{3/4} = \frac{1}{3}.$$

VII.6 La formule des probabilités totales

Définition : Soit I un ensemble fini ou dénombrable. On dit qu'une famille d'événements $(A_i)_{i \in I}$ est un *système complet d'événements* si leur union est disjointe et certaine, autrement dit :

$$\forall i \neq j,\ A_i \cap A_j = \qquad \text{et} \qquad \bigcup_{i \in I} A_i = \Omega.$$

On dit que c'est un *système quasi complet d'événements* si leur union est disjointe et presque certaine, autrement dit :

$$\forall i \neq j,\ A_i \cap A_j = \qquad \text{et} \qquad P\Big(\bigcup_{i \in I} A_i\Big) = 1.$$

Remarque : 1. Si on fait une expérience aléatoire, alors un unique événement du système complet se réalise.

2. Si A est un événement, alors $\{A, \bar{A}\}$ est un système complet d'événements.

3. Pour tout système quasi complet d'événements, $\sum_{i\in I} P(A_i) = 1$ par σ-additivité.

Méthode :
Un système complet d'événements $(A_i)_{i\in I}$ permet de décomposer un événement B quelconque : on a $\bigcup_{i\in I} A_i = \Omega$, d'où $\forall B \in \mathcal{A}, \bigcup_{i\in I}(B\cap A_i) = B\cap\big(\bigcup_{i\in I} A_i\big) = B \cap \Omega = B$, par distributivité de $\cap$ par rapport à $\cup$. Ainsi, on a $P(B) = \sum_{i\in I} P(B \cap A_i)$.

Théorème (Probabilités totales) **:** Soit $(A_i)_{i\in I}$ un système quasi complet d'événements. Alors,

$$P(B) = \sum_{i\in I} P(B \cap A_i).$$

Si les événements A_i ne sont pas de probabilités nulles, alors

$$P(B) = \sum_{i\in I} P(A_i) \times P(B \mid A_i).$$

Preuve :
On complète la famille d'événements $(A_i)_{i\in I}$ en un système complet d'événements en posant $C = \Omega \setminus \bigcup_{i\in I} A_i$. Alors, $\big(\bigcup\!\!\cdot_{i\in I} A_i\big) \cup C = \Omega$, et cet union est disjointe. D'où, pour tout événement $B \in \mathcal{A}$, $P(B) = P(B \cap C) + \sum_{i\in I} P(B \cap A_i)$. Or, $P(B \cap C) = 0$, car $\sum_{i\in I} P(A_i) = 1$, et $\Omega = C \cup \big(\bigcup_{i\in I} A_i\big)$ et cette union est disjointe, d'où $P(\Omega) = 1 = P(C) + 1$, donc $P(C) = 0$; mais, comme $B \cap C \subset C$, alors $P(B \cap C) \leqslant P(C) = 0$. On a donc bien $P(B \cap C) = 0$. □

Exercice :
On lance un dé à cinq faces. Calculer, pour chaque $n \in \mathbb{N}^\star$, la probabilité u_n de l'événement S_n : « la somme des résultats obtenus lors des n premiers lancers est paire. »

On considère le système complet d'événements $\{S_n, \bar{S}_n\}$. On a $P_{S_n}(S_{n+1}) = \frac{2}{5}$, et $P_{\bar{S}_n}(S_{n+1}) = \frac{3}{5}$. Or, $S_{n+1} = (S_{n+1} \cap S_n) \uplus (S_{n+1} \cap \bar{S}_n)$, et cette union est

disjointe. D'où

$$\begin{aligned}\overbrace{P(S_{n+1})}^{u_{n+1}} &= P(S_{n+1}\cap S_n) + P(S_{n+1}\cap \bar{S}_n)\\ &= P(S_n)\times P_{S_n}(S_{n+1}) + P(\bar{S}_n)\times P_{\bar{S}_n}(S_{n+1})\\ &= \frac{2}{5}u_n + \frac{3}{5}(1-u_n)\\ &= \frac{3}{5} - \frac{1}{5}u_n\end{aligned}$$

On résout cette suite définie par une relation de récurrence arithmético-géométrique. Pour cela, on commence par chercher un point fixe de cette relation (une suite constante vérifiant cette relation) : on résout

$$\ell = \frac{3}{5} - \frac{1}{5}\ell \iff \frac{6}{5}\ell = \frac{3}{5} \iff \ell = \frac{1}{2}.$$

D'où,

$$\begin{array}{rrcrcl} & u_{n+1} & = & -\frac{1}{5}u_n & + & \frac{3}{5}\\ - & \ell & = & -\frac{1}{5}\ell & + & \frac{3}{5}\\ \hline & \underbrace{(u_{n+1}-\ell)}_{v_{n+1}} & = & -\frac{1}{5}\underbrace{(u_n-\ell)}_{v_n} & & \end{array}$$

On a donc $v_n = \left(-\frac{1}{5}\right)^{n-1} v_1$, d'où

$$u_n - \ell = \left(-\frac{1}{5}\right)^{n-1}(u_1-\ell)$$

donc

$$u_n = \left(-\frac{1}{5}\right)^{n-1}(u_1-\ell)+\ell = -\left(-\frac{1}{5}\right)^{n-1}\left(\frac{3}{5}\right)+\frac{1}{2} = 3\left(-\frac{1}{5}\right)^{n}+\frac{1}{2}.$$

VII.7 La formule des probabilités composées

Exercice :
Une urne contient 5 boules blanches et 2 boules noires. On tire 2 boules l'une après l'autre et sans remise. Calculer la probabilité que les deux premières boules tirées soient blanches.

On pose B_1 : « la première boule est blanche » et B_2 : « la seconde boule est blanche. » On a, d'après la formule des probabilités composées,

$$P(B_1\cap B_2) = P(B_1)\times P(B_2 \mid B_1).$$

Or, par équiprobabilité, $P(B_1) = 5/7$, et $P(B_2 \mid B_1) = 4/6$. On en déduit que

$$P(B_1\cap B_2) = \frac{5}{7}\times\frac{4}{6} = \frac{10}{21}.$$

Théorème (Formule des probabilités composées) **:** Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé, et soit $(A_1, \ldots, A_n)$ une famille finie d'événements. Si la probabilité de $A_1 \cap A_2 \cap \cdots \cap A_n$ n'est pas nulle, alors

$$P(A_1 \cap \cdots \cap A_n) = P(A_1) \times P(A_1 \mid A_2) \times P(A_3 \mid A_1 \cap A_2) \cdots P(A_n \mid A_1 \cap \cdots \cap A_{n-1}).$$

Preuve (par récurrence sur n) *:* — On a bien $P(A_1 \cap A_2) = P(A_1) \times P(A_2 \mid A_1)$ par définition de $P(A_2 \mid A_1)$.
— *c.f.* le poly

□

VII.8 Formule de Bayes

Théorème (Formule de Bayes) **:** Soient A et B deux événements de probabilités non-nulles. Alors,

$$P(A \mid B) = \frac{P(A) \times P(B \mid A)}{P(B)}.$$

Preuve :
Par définition, on a

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \qquad \text{et} \qquad P(B \mid A) = \frac{P(A \cap B)}{P(A)}.$$

Ainsi, par produit en croix, on a

$$P(A \mid B) = \frac{P(A) \times P(B \mid A)}{P(B)}.$$

□

Méthode :
On peut utiliser la formule de Bayes avec la formule des probabilités totales, comme dans l'exercice suivant.

Exercice :
Un joueur tire une carte dans un jeu de 52 cartes (il y a 4 as dans ce jeu). On suppose qu'un tricheur est certain de tirer un as et qu'il y a, parmi les joueurs, une proportion $p \in]0, 1[$ de tricheurs :

— *quelle est la probabilité qu'un joueur, pris au hasard, tire un as ?*
— *le joueur vient de tirer un as, quelle est la probabilité qu'il ait triché ?*

On pose les événements T : « le joueur est un tricheur » et A : « le joueur tire

un as. » On a donc $P(A \mid T) = 1$, et $P(A \mid \bar{T}) = \frac{4}{52} = \frac{1}{13}$. $(T, \bar{T})$ est un système complet d'événements, d'où

$$P(A) = P(T) \times P(A \mid T) + P(\bar{T}) \times P(A \mid \bar{T}),$$

d'après la formule des probabilités totales. D'où,

$$P(A) = p + \frac{1-p}{13} = \frac{12}{13}p + \frac{1}{13}.$$

On nous demande $P(T \mid A)$. On a calculé $P(A \mid T)$, et d'après la formule de Bayes, on a

$$P(T) \times P(A \mid T) = P(A) \times P(T \mid A).$$

D'où,

$$\begin{aligned} P(T \mid A) &= \frac{P(T) \times P(A \mid T)}{P(A)} \\ &= \frac{p}{\frac{12}{13}p + \frac{1}{13}} \\ &= \frac{13p}{12p+1} \end{aligned}$$

Chapitre 8

Intégrales à paramètre

Il ne pas confondre les deux intégrales $\int_7^x f(t)\,\mathrm{d}t = F(x)$ (la fonction $F : x \mapsto F(x)$ une primitive [1] de la fonction f, si f est continue) et $\int_7^{+\infty} g(x,t)\,\mathrm{d}t = G(x)$ si l'intégrale converge (c'est une *intégrale à paramètre*, où le paramètre est x et la variable est t).

VII.1 Continuité

Théorème : Soient X et T deux intervalles de $\mathbb{R}$, et soit $f : X \times T \to \mathbb{R}$. Si

1. pour chaque $t \in T$, la fonction $x \mapsto f(x,t)$ est continue sur X ;
2. pour chaque $x \in X$, la fonction $x \mapsto f(x,t)$ est continue par morceaux sur T ;
3. il existe une fonction φ continue par morceaux et intégrable [a] sur T telle que
$$\forall (x,t) \in X \times T,\ |f(x,t)| \leqslant \varphi(t),$$

alors la fonction $\displaystyle\int_T f(x,t)\,\mathrm{d}t$ est continue sur X.

a. *i.e.* l'intégrale $\int_T \varphi(t)\,\mathrm{d}t$ converge.

Preuve (théorème de la convergence dominée & caractérisation séquentielle de la limite) *:*
Soit $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans X quelconque tendant, quand $n \to \infty$, vers un réel $a \in X$. Soit alors la fonction

$$\begin{aligned} h_n : T &\longrightarrow \mathbb{R} \\ t &\longmapsto f(u_n, t). \end{aligned}$$

Soit $t \in T$, on a $h_n(t) = f(u_n, t) \longrightarrow f(a,t)$ quand $n \to \infty$, car la fonction

1. F est dérivable et sa dérivée est $F' = f$, autrement dit : $\forall x,\ F'(x) = f(x)$.

$x \mapsto f(x,t)$ est continue sur X (1.). Donc, la suite de fonctions $(h_n)_{n\in\mathbb{N}}$ converge simplement vers une fonction h définie comme

$$\begin{aligned} h : T &\longrightarrow \mathbb{R} \\ t &\longmapsto f(a,t). \end{aligned}$$

On a $|h_n(t)| = |f(u_n,t)| \leqslant \varphi(t)$, et φ est intégrable (3.). Ainsi, d'après le théorème de la convergence dominée,

$$\lim_{n\to\infty} \overbrace{\int_T h_n(t)\,\mathrm{d}t}^{g(u_n)} = \int_T \underbrace{\lim_{n\to\infty} h_n(t)}_{f(a,t)}\,\mathrm{d}x = \int_T f(a,t)\,\mathrm{d}t = g(a).$$

D'où, $g(u_n) \longrightarrow a$, quand $n \to \infty$. Ceci est vrai quelle que soit la suite $(u_n)_{n\in\mathbb{N}}$ tendant vers a, donc par caractérisation de la limite, $\lim_{x\to a} g(x) = g(a)$. Ainsi, g est continue en a. Ceci étant vrai pour tout $a \in X$, on en déduit que g est continue sur X. □

Exercice (La fonction Gamma) : *1. Pour quelles valeurs du paramètre réel x, les intégrales impropres*

$$\Gamma_1(x) = \int_0^1 t^{x-1} \times \mathrm{e}^{-t}\,\mathrm{d}t \qquad \text{et} \qquad \Gamma_2(x) = \int_1^{+\infty} t^{x-1} \times \mathrm{e}^{-t}\,\mathrm{d}t$$

convergent-elles ?

2. Montrer que l'intégrale impropre

$$\Gamma(x) = \int_0^{+\infty} t^{x-1} \times \mathrm{e}^{-t}\,\mathrm{d}t$$

converge si, et seulement si $x > 0$.

3. Monter que, pour tout $x > 0$, $\Gamma(x+1) = x \cdot \Gamma(x)$.

4. En déduire que $\Gamma(n+1) = n!$ pour tout $n \in \mathbb{N}$.

5. En étudiant les fonctions Γ_1 et Γ_2, montrer que la fonction Γ est continue sur $]0,+\infty[$.

6. En déduire que, $\Gamma(x) \sim_{x\to 0^+} \frac{1}{x}$.

1. L'intégrale $\Gamma_1(x)$ est impropre en 0. On a

$$t^{x-1} \times \underbrace{\mathrm{e}^{-t}}_{\longrightarrow 1} \underset{t\to 0}{\sim} t^{x-1} = \frac{1}{t^{1-x}}$$

qui ne change pas de signe. Or, $\int_0^1 \frac{1}{t^{1-x}}\,\mathrm{d}t$ converge si et seulement si $1-x<1$ d'après le critère de Riemann, *i.e.* $x > 0$.

L'intégrale $\Gamma_2(x)$ est impropre en $+\infty$. Or, $t^{x-1} \times \mathrm{e}^{-t} = (t^{x-1}\mathrm{e}^{-t/2}) \times \mathrm{e}^{-t/2} = \mathcal{O}_{t\to+\infty}(\mathrm{e}^{-t/2})$, et $\mathrm{e}^{-t/2}$ ne change pas de signe. Or, l'intégrale $\int_1^{+\infty} \mathrm{e}^{-t/2}\,\mathrm{d}x$. Donc, l'intégrale $\Gamma_2(x)$ converge pour tout $x \in \mathbb{R}$.

2. L'intégrale $\Gamma(x)$ converge si et seulement si les deux intégrales $\Gamma_1(x)$ et $\Gamma_2(x)$ convergent, donc si et seulement si $x > 0$.
3. Soit $x > 0$. On a $\Gamma(x+1) = \int_0^{+\infty} t^x \mathrm{e}^{-t}\,\mathrm{d}t$. Ainsi, soient $y \in]0,1]$, et
$$f(y) = \int_y^1 t^x \mathrm{e}^{-t}\,\mathrm{d}t = \left[-t^x \cdot \mathrm{e}^{-t}\right]_y^1 + x\int_y^1 t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}x$$
par intégration par parties car $t \mapsto t^x$ est $\mathscr{C}^1$ et $t \mapsto -\mathrm{e}^{-t}$ est $\mathscr{C}^1$. Or, $y^x \cdot \mathrm{e}^{-y}$ tend vers 0 quand $y \to 0$, et $\int_y^1 t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$ tend vers $\Gamma_1(x)$, quand $y \to 0$. Donc,
$$\Gamma_1(x+1) = -\mathrm{e}^{-1} + x\Gamma_1(x).$$
De même, $\Gamma_2(x+1) = \mathrm{e}^{-1} + x\Gamma_2(x)$. On en déduit que
$$\forall x > 0, \quad \Gamma(x+1) = x\Gamma(x).$$
4. On a $\Gamma(1) = \int_0^{+\infty} t^{1-1}\mathrm{e}^{-t}\,\mathrm{d}t = \int_0^{+\infty} \mathrm{e}^{-t}\,\mathrm{d}t = 1$. D'où, $\forall n \in \mathbb{N}^\star, \quad \Gamma(n+1) = n\Gamma(n)$. Par récurrence, on en déduit que $\Gamma(n+1) = n!$, pour $n \in \mathbb{N}$.
5. On veut montrer que $\Gamma_1 : x \mapsto \Gamma_1(x)$, et $\Gamma_2 : x \mapsto \Gamma_2(x)$ sont continues. Soit $a > 0$. Soient $T =]0,1]$, $X = [a, +\infty[$, et
$$\begin{aligned} f : X \times T &\longrightarrow \mathbb{R} \\ (x,t) &\longmapsto t^{x-1} \cdot \mathrm{e}^{-t} \end{aligned}$$
Ainsi, on a bien $\Gamma_1(x) = \int_T f(x,t)\,\mathrm{d}t$.
   - Pour tout $t \in T$, la fonction $x \mapsto f(x,t)$ est continue sur X. En effet, soit $t \in T$, on a $f(x,t) = t^{x-1} \cdot \mathrm{e}^{-t} = \mathrm{e}^{(x-1)\ln t} \cdot \mathrm{e}^{-t}$ qui est continue par continuité de l'exponentielle.
   - (—) Pour tout $x \in X$, la fonction $t \mapsto f(x,t)$ est continue par morceaux sur T.
   - Pour tout $t \in T$, et pour $x \in X$, $|f(x,t)| \leqslant t^{a-1} \cdot \mathrm{e}^{-t} = \varphi(t)$, et l'intégrale $\int_T \varphi(t)\,\mathrm{d}t$ converge. En effet, pour $x \in X$, et $t \in T$, $|f(x,t)| = t^{x-1} \cdot \mathrm{e}^{-t} \leqslant t^{a-1} \cdot \mathrm{e}^{-t}$, et l'intégrale $\int_T t^{a-1} \cdot \mathrm{e}^{-t}\,\mathrm{d}t$ (car il s'agit de $\Gamma_1(a)$, et $a > 0$).

   Donc, Γ_1 est continue sur $X = [a, +\infty[$. Ceci est vrai pour tout $a > 0$. On en déduit que Γ_1 est continue sur $]0, +\infty[$.

   On procède de même pour montrer que $\Gamma_2 : x \mapsto \Gamma_2(x)$ est continue. Soit $b > 0$. Soient $T = [1, +\infty[$, $X =]0, b]$, et
$$\begin{aligned} f : X \times T &\longrightarrow \mathbb{R} \\ (x,t) &\longmapsto t^{x-1} \cdot \mathrm{e}^{-t} \end{aligned}$$
Ainsi, on a bien $\Gamma_2(x) = \int_T f(x,t)\,\mathrm{d}t$.
   - Pour tout $t \in T$, la fonction $x \mapsto f(x,t)$ est continue sur X. En effet, soit $t \in T$, on a $f(x,t) = t^{x-1} \cdot \mathrm{e}^{-t} = \mathrm{e}^{(x-1)\ln t} \cdot \mathrm{e}^{-t}$ qui est continue par continuité de l'exponentielle. (De même que pour Γ_1.)
   - (—) Pour tout $x \in X$, la fonction $t \mapsto f(x,t)$ est continue par morceaux sur T.

— Pour tout $t \in T$, et pour $x \in X$, $|f(x,t)| \leqslant t^{b-1} \cdot \mathrm{e}^{-t} = \psi(t)$, et l'intégrale $\int_T \psi(t)\,\mathrm{d}t$ converge (car il s'agit de $\Gamma_2(b)$ avec $b > 0$).

Donc, Γ_2 est continue sur $X =]0, b]$. Ceci est vrai pour tout $b > 0$. On en déduit que Γ_2 est continue sur $]0, +\infty[$. On en déduit que $\Gamma = \Gamma_1 + \Gamma_2$ est continue sur $]0, +\infty[$, comme somme de deux fonctions continue sur $]0, +\infty[$.

6. On veut montrer que $x\Gamma(x) = \frac{\Gamma(x)}{1/x} \longrightarrow 1$ quand $x \to 0^+$. Or, $x\Gamma(x) = \Gamma(x+1)$ d'après la question 3. Et, $x + 1 \longrightarrow 1$ quand $x \to 0^+$. Or, d'après la question 5., la fonction Γ est continue en 1. Donc, $\Gamma(x+1) \longrightarrow \Gamma(1)$. De plus, $\Gamma(1) = 0! = 1$ d'après la question 4. On en déduit que

$$x\Gamma(x) \xrightarrow[x \to 0^+]{} 1.$$

VII.2 Dérivabilité

Dans le théorème suivant, on montre que, avec les hypothèses demandées,

$$\frac{\mathrm{d}}{\mathrm{d}x} \int_T f(x,t)\,\mathrm{d}t = \int_T \frac{\partial f}{\partial x}(x,t)\,\mathrm{d}t.$$

Théorème : Soient $X \subset \mathbb{R}$ et $T \subset \mathbb{R}$ deux intervalles, et soit $f : X \times T \to \mathbb{R}$. Si,

1. pour $t \in T$, la fonction $x \mapsto f(x,t)$ est de classe $\mathscr{C}^1$ sur X ;
2. pour $x \in X$, la fonction $t \mapsto f(x,t)$ est continue par morceaux et intégrable [a] sur T, **et** la fonction $t \mapsto \frac{\partial f}{\partial x}(x,t)$ est continue par morceaux ;
3. il existe une fonction intégrable φ continue par morceaux telle que $\forall (x,t) \in X \times T$, $\left|\frac{\partial f}{\partial x}(x,t)\right| \leqslant \varphi(t)$,

alors, $g : x \mapsto \int_T f(x,t)\,\mathrm{d}t$ est de classe $\mathscr{C}^1$, et

$$g'(x) = \frac{\mathrm{d}g}{\mathrm{d}x}(x) = \int_T \frac{\partial}{\partial x} f(x,t)\,\mathrm{d}t.$$

a. *i.e.* l'intégrale de cette fonction converge absolument.

Exercice (La fonction Gamma – suite) :

(a) Montrons que la fonction $\Gamma_1 : x \mapsto \int_0^1 t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$ *est* $\mathscr{C}^1$ *;*
(b) Montrons que la fonction $\Gamma_2 : x \mapsto \int_1^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$ *est* $\mathscr{C}^1$ *;*
(c) Donc, comme $\Gamma = \Gamma_1 + \Gamma_2$*, alors* Γ *est de classe* $\mathscr{C}^1$*.*

(a) Soit $a > 0$. Soient $T =]0, 1]$, $X = [a, +\infty[$ et $f(x,t) = t^{x-1}\mathrm{e}^{-t}$, pour $x \in X$ et $t \in T$.

1. Pour $t \in T$, la fonction $x \mapsto f(x,t)$ est de classe $\mathscr{C}^1$ sur X. En effet, soit $t \in T$. Comme $f(x,t) = \mathrm{e}^{(x-1)\ln t} \cdot \mathrm{e}^t$, et exp est $\mathscr{C}^\infty$, d'où $x \mapsto f(x,t)$ est $\mathscr{C}^1$, et
$$\frac{\partial f}{\partial x}(x,t) = \ln t \cdot \mathrm{e}^{(x-1)\ln t} \cdot \mathrm{e}^{-t} = \ln t \cdot t^{x-1} \cdot \mathrm{e}^{-t}.$$
2. Pour $x \in X$, la fonction $t \mapsto f(x,t)$ est *cpm* et $\int_T \left|f(x,t)\right| \mathrm{d}t$ converge (*c.f.* exercice 2). Et, la fonction $t \mapsto \frac{\partial}{\partial x} f(x,t)$ est *cpm*.
3. $\forall t \in T, \forall x \in X, \left|\frac{\partial f}{\partial x}(x,t)\right| \leqslant -\ln t \cdot t^{x-1} \cdot \mathrm{e}^{-t} \leqslant -\ln t \cdot t^{a-1} \cdot \mathrm{e}^{-t} = \varphi(t)$. Et, $\int_T \varphi(t)\,\mathrm{d}t$ converge. En effet,
$$(-\ln t) \cdot t^{a-1} = \underbrace{(-\ln t) \cdot t^{\varepsilon}}_{\longrightarrow 0} \cdot t^{a-\varepsilon-1} \cdot \mathrm{e}^{-t} = \underset{t\to 0^+}{\mathcal{O}}\left(t^{a-\varepsilon-1}\right).$$
Or, l'intégrale $\int_T t^{(a-\varepsilon)-1}\mathrm{e}^{-t}\,\mathrm{d}t$ converge (car $a-\varepsilon > 0$), et elle vaut $\Gamma_1(a-\varepsilon)$. On en déduit que $\int_T \varphi(t)\,\mathrm{d}t$ converge.

Alors, Γ_1 est $\mathscr{C}^1$ sur X. Ceci étant vrai pour tout $a > 0$, on en On en déduit que Γ_1 est de classe $\mathscr{C}^1$ sur $]0,+\infty[$ et que
$$\forall x > 0,\ \Gamma_1'(x) = \int_T (\ln t) t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t.$$

(b) Soit $b > 0$. Soient $T = [1,+\infty[$, $X =]0,b]$ et $f(x,t) = t^{x-1}\mathrm{e}^{-t}$, pour $x \in X$ et $t \in T$.

1. Pour $t \in T$, la fonction $x \mapsto f(x,t)$ est de classe $\mathscr{C}^1$ sur X. En effet, soit $t \in T$. Comme $f(x,t) = \mathrm{e}^{(x-1)\ln t} \cdot \mathrm{e}^t$, et exp est $\mathscr{C}^\infty$, d'où $x \mapsto f(x,t)$ est $\mathscr{C}^1$, et
$$\frac{\partial f}{\partial x}(x,t) = \ln t \cdot \mathrm{e}^{(x-1)\ln t} \cdot \mathrm{e}^{-t} = \ln t \cdot t^{x-1} \cdot \mathrm{e}^{-t}.$$
2. Pour $x \in X$, la fonction $t \mapsto f(x,t)$ est *cpm* et $\int_T \left|f(x,t)\right| \mathrm{d}t$ converge (*c.f.* exercice 2). Et, la fonction $t \mapsto \frac{\partial}{\partial x} f(x,t)$ est *cpm*.
3. $\forall t \in T, \forall x \in X, \left|\frac{\partial f}{\partial x}(x,t)\right| \leqslant -\ln t \cdot t^{x-1} \cdot \mathrm{e}^{-t} \leqslant -\ln t \cdot t^{b-1} \cdot \mathrm{e}^{-t} = \varphi(t)$. Et, $\int_T \varphi(t)\,\mathrm{d}t$ converge. En effet,
$$\ln t \cdot t^{b-1} \cdot e^{-t} = (\ln t \cdot \mathrm{e}^{-t/3}) \cdot (t^{b-1} \cdot \mathrm{e}^{-t/3}) \cdot \mathrm{e}^{-t/3}.$$
Or, l'intégrale $\int_T \mathrm{e}^{-t/3}\,\mathrm{d}t$ converge. On en déduit que $\int_T \varphi(t)\,\mathrm{d}t$ converge.

Alors, Γ_2 est $\mathscr{C}^1$ sur X. Ceci étant vrai pour tout $b > 0$, on en On en déduit que Γ_2 est de classe $\mathscr{C}^1$ sur $]0,+\infty[$ et que
$$\forall x > 0,\ \Gamma_2'(x) = \int_T (\ln t) t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t.$$

Corollaire : On peut appliquer le théorème plusieurs fois :

1. pour $t \in T$, la fonction $x \mapsto f(x,t)$ est $\mathscr{C}^k$ sur X ;
2. pour $x \in X$, la fonction $t \mapsto \frac{\partial^i f}{\partial x^i}(x,t)$ est *cmp* et intégrable sur T pour tout $j \in [\![0, k-1]\!]$, et la fonction $t \mapsto \frac{\partial^k f}{\partial x^k}(x,t)$ est *cmp* sur T.
3. il existe φ *cmp* et intégrable telle que $\forall x \in X$, $\forall t \in T$, $\left|\frac{\partial^k f}{\partial x^k} f(x,t)\right| \leqslant \varphi(t)$,

alors la fonction $g : x \mapsto \int_T f(x,t)\,\mathrm{d}t$ est de classe $\mathscr{C}^k$ et

$$\forall i \leqslant k, \quad g^{(i)}(x) = \int_T \frac{\partial^i f}{\partial x^i}(x,t)\,\mathrm{d}t.$$

Rappel (théorème de Rolle) :
Soit f une fonction continue sur $[a,b]$ et dérivable sur $]a,b[$. On suppose que $f(a) = f(b)$. Ainsi,

$$\exists c \in]a,b[,\ f'(c) = 0.$$

Exercice (La fonction Γ – fin) : 1.

2. La fonction Γ est continue sur $[1,2]$, et dérivable sur $]1,2[$. En effet, Γ est $\mathscr{C}^1$ sur $[1,2]$. Or, $\Gamma(1) = 0! = 1 = 1! = \Gamma(2)$. Donc, d'après le théorème de Rolle, il existe $\alpha \in]1,2[$ tel que $\Gamma(\alpha) = 0$. De plus, Γ'' est strictement positive (*c.f.* raisonnent ci-après) donc Γ est strictement croissante, d'où Γ' est injective. On en déduit que α est unique. En effet, par l'absurde : si l'intégrale de la fonction est nulle et que la fonction est continue et ne change pas de signes, alors la fonction est nulle. $\lightning$
3.

x	0	1	α	$+\infty$
$\Gamma'(x)$	‖	$-$	0	$+$
$\Gamma(x)$	‖	↘	$\Gamma(\alpha)$	↗

On sait que $\forall n \in \mathbb{N}$, $\Gamma(n+1) = n!$. D'où, $\Gamma(n) \longrightarrow +\infty$ quand $n \to +\infty$. De plus, Γ est monotone (car strictement croissante) sur $[2, +\infty[$, donc $\lim_{x\to+\infty} \Gamma(x)$ existe. Par unicité de la limite,

$$\lim_{x\to+\infty} \Gamma(x) = \lim_{n\to\infty} \Gamma(n) = +\infty.$$

4. D'après la formule de STIRLING,

$$n! \underset{n\to\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n.$$

Et, pour $x > 0$, $\Gamma(\lfloor x\rfloor)/x^k \leqslant \Gamma(x)/x^k$. Or, $\Gamma(\lfloor x\rfloor) = (\lfloor x\rfloor - 1)! \sim_{x\to+\infty} \sqrt{2\pi n(x)}\left(\frac{n(x)}{\mathrm{e}}\right)^{n(x)}$ où $n(x) = \lfloor x\rfloor - 1$. D'où,

$$\frac{\Gamma(\lfloor x\rfloor)}{x^k} \underset{x\to+\infty}{\sim} \frac{\sqrt{2\pi n(x)}\left(\frac{n(x)}{\mathrm{e}}\right)^{n(x)}}{x^k} \xrightarrow[x\to+\infty]{} +\infty.$$

Chapitre 9

Produits scalaires

VII.1 Qu'est-ce qu'un produit scalaire ?

Définition : Soient E un $\mathbb{R}$-espace vectoriel et $\varphi : E \times E \to \mathbb{R}$ une application. On dit que φ est une forme

- *bilinéaire* si $\forall (\vec{x},\vec{y},\vec{z}) \in E^3, \forall (\alpha,\beta) \in \mathbb{R}^2, \begin{cases} \varphi(\alpha\vec{x}+\beta\vec{y},\vec{z}) = \alpha\varphi(\vec{x},\vec{z}) + \beta\varphi(\vec{y},\vec{z}) \\ \varphi(\vec{x},\alpha\vec{y}+\beta\vec{z}) = \alpha\varphi(\vec{x},\vec{y}) + \beta\varphi(\vec{x},\vec{z}), \end{cases}$
- *symétrique* si $\forall (\vec{x},\vec{y}) \in E^2$, $\varphi(\vec{x},\vec{y}) = \varphi(\vec{y},\vec{x})$,
- *définie* si $\forall \vec{x} \in E, \quad \varphi(\vec{x},\vec{x}) = 0 \implies \vec{x} = \vec{0}$,
- *positive* si $\forall \vec{x} \in E$, $\varphi(x,x) \geqslant 0$.

Définition : Soit E un $\mathbb{R}$-espace vectoriel. Si $\varphi : E^2 \to \mathbb{R}$ une forme bilinéaire symétrique définie positive, alors

- on dit que φ est un *produit scalaire*. Le produit scalaire $\varphi(\vec{x},\vec{y})$ de deux vecteurs $\vec{x}$ et $\vec{y} \in E$ est aussi noté $\langle \vec{x} \mid \vec{y} \rangle$, $\langle \vec{x},\vec{y} \rangle$, $(\vec{x} \mid \vec{y})$ ou $\vec{x} \cdot \vec{y}$.
- le carré scalaire $\varphi(\vec{x},\vec{x}) = \langle \vec{x} \mid \vec{x} \rangle$ étant positif, on appelle le réel

$$\|\vec{x}\|_2 = \|\vec{x}\| = \sqrt{\langle \vec{x} \mid \vec{x} \rangle}$$

norme (associée à ce produit scalaire) du vecteur $\vec{x}$.

En TD, il est, en général, plus efficace de le montrer dans l'ordre suivant :

$$\text{symétrie} \longrightarrow \text{bilinéaire} \longrightarrow \text{positive} \longrightarrow \text{définie}.$$

EXEMPLE : 1. L'espace vectoriel $\mathbb{R}^n$ est un espace euclidien [1] avec le produit

1. *i.e.* un $\mathbb{R}$-espace vectoriel de dimension finie muni d'un produit scalaire.

scalaire : si $\vec{x} = (x_1, x_2, \dots, x_n)$ et $\vec{y} = (y_1, y_2, \dots, y_n)$, alors

$$\langle \vec{x} \mid \vec{y} \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = \sum_{i=1}^{n} x_i y_i.$$

2. L'espace vectoriel $\mathscr{M}_n(\mathbb{R})$ est un espace euclidien avec le produit scalaire : pour $A = (a_{i,j})_{(i,j)\in[\![1,n]\!]^2}$ et $B = (b_{i,j})_{(i,j)\in[\![1,n]\!]^2}$,

$$\langle A \mid B \rangle = \sum_{\substack{i\in[\![1,n]\!]\\ j\in[\![1,n]\!]}} a_{i,j} b_{i,j} = \operatorname{tr}(A^\top \cdot B).$$

En effet, soit $C = A^\top \cdot B$, alors

$$\begin{aligned}(C)_{i,j} &= \sum_{k=1}^{n} (A^\top)_{i,k} \times (B)_{k,j} \\ &= \sum_{k=1}^{n} (A)_{k,i} \times (B)_{k,j}\end{aligned}$$

et donc

$$\langle A \mid B \rangle = \operatorname{tr}(C) = \sum_{i=1}^{n} (C)_{i,i} = \sum_{i=1}^{n}\sum_{k=1}^{n} (A)_{k,i} \times (B)_{k,i}.$$

Montrons qu'il s'agit bien d'un produit scalaire.

1ère méthode Il s'agit de la même formule que pour l'espace vectoriel $\mathbb{R}^n$.

2nde méthode symétrique $\langle A \mid B \rangle = \operatorname{tr}(A^T \cdot B) = \operatorname{tr}\left((A^\top \cdot B)^\top\right) = \operatorname{tr}(B^\top \cdot A) = \langle B \mid A \rangle$.

bilinéaire Le produit matriciel est linéaire, et la trace est linéaire, d'où $\langle \cdot \mid \cdot \rangle$ est bilinéaire.

positive $\langle A \mid A \rangle = \sum_{p,q} \left((A)_{p,q}\right)^2 \geqslant 0$.

définie On suppose $\langle A \mid A \rangle = 0$, alors $\forall p, q$, $\left((A)_{p,q}\right)^2 = 0$, et donc $\forall p, q$, $(A)_{p,q} = 0$, d'où $A = 0_{\mathscr{M}_n(\mathbb{R})}$.

3. L'espace vectoriel $\mathscr{C}([a, b])$ des fonctions continue sur un segment $[a, b]$ est un espace préhilbertien [2] avec le produit scalaire

$$\langle f \mid g \rangle = \int_a^b f(t)\, g(t)\, \mathrm{d}t.$$

En effet,

symétrique $\forall f, g \in \mathscr{C}([a, b])$, $\langle f \mid g \rangle = \int_a^b f(t)\, g(t)\, \mathrm{d}t = \int_a^b g(t)\, f(t)\, \mathrm{d}t = \langle f \mid g \rangle$.

2. *i.e.* un $\mathbb{R}$-espace vectoriel de dimension potentiellement infinie muni d'un produit scalaire.

bilinéaire $\forall(\alpha,\beta)\in\mathbb{R}^2$, $\forall(f_1,f_2,g)\in\mathscr{C}([a,b])^3$,

$$\begin{aligned}\langle\alpha_1 f_1+\alpha_2 f_2\mid g\rangle &= \int_a^b \big(\alpha_1 f_1(t)+\alpha_2 f_2(t)\big)g(t)\,\mathrm{d}t\\ &= \alpha_1\int_a^b f_1(t)\,g(t)\,\mathrm{d}t+\alpha_2\int_a^b f_2(t)\,g(t)\,\mathrm{d}t\\ &= \alpha_1\,\langle f_1\mid g\rangle+\alpha_2\,\langle f_2\mid g\rangle\end{aligned}$$

Ainsi $\langle\,\cdot\mid\cdot\,\rangle$ est linéaire à gauche, donc par symétrie, ce produit scalaire est bilinéaire.

positive $\forall f\in\mathscr{C}([a,b])$, $\int_a^b f^2(t)\,\mathrm{d}t\geqslant 0$.

définie On suppose que $\langle f\mid f\rangle=\int_a^b f^2(t)\,\mathrm{d}t=0$, avec $f\in\mathscr{C}([a,b])$. Or, la fonction $f^2:t\mapsto f^2(t)$ ne change pas de signe et elle est continue. On en déduit que $f=0_{\mathscr{C}([a,b])}$.

Exercice :
Soit $L_2(I)$ l'ensemble des fonctions f continues par morceaux et de carré intégrable sur I, où I est un intervalle, c'est à dire : l'intégrale $\int_I f^2(t)\,\mathrm{d}t$ converge. Montrer que

1. *le produit de deux fonctions de carré intégrable est intégrable ;*
2. *l'ensemble $L_2(I)$ est un espace vectoriel ;*
3. *l'ensemble $L_2(I)\cap\mathscr{C}(I)$ des fonctions continues de carré intégrable sur I est aussi un espace vectoriel ;*
4. *l'application $\langle f\mid g\rangle=\int_I f(t)\,g(t)\,\mathrm{d}t$ est défini pour tout couple $(f,g)\in L_2(I)^2$, et que c'est un produit scalaire sur $L_2(I)\cap\mathscr{C}(I)$ mais pas sur $L_2(I)$.*

1. Soient $f\in L_2(I)$ et $g\in L_2(I)$, alors les intégrales $\int_I f^2(t)\,\mathrm{d}t$ et $\int_I g^2(t)\,\mathrm{d}t$ convergent. Or,

$$\forall t\in I,\quad \Big(\big|f(t)\big|-\big|g(t)\big|\Big)^2=f^2(t)+g^2(t)-2\big|f(t)\times g(t)\big|\geqslant 0.$$

D'où, $f^2(t)+g^2(t)\geqslant 2\big|f(t)\times g(t)\big|\geqslant 0$. Or, les intégrales $\int_I f^2(t)\,\mathrm{d}t$ et $\int_I g^2(t)\,\mathrm{d}t$ convergent. D'où l'intégrale $\int_I\big(f^2(t)+g^2(t)\big)\,\mathrm{d}t$. On en déduit donc que l'intégrale $\int_I f(t)\times g(t)\,\mathrm{d}t$ converge, *i.e.* $f\times g\in L_2(I)$.

2. Il "suffit" de montrer que $L_2(I)$ est un sous-espace vectoriel $\mathrm{Cpm}(I)$ des fonctions continues par morceaux sur I, *i.e.* la fonction nulle $0_{\mathrm{Cpm}(I)}\in L_2(I)$ et que $L_2(I)$ est stable par combinaison linéaire. L'intégrale $\int_I 0^2\,\mathrm{d}t$ converge, donc la fonction nulle est bien de carré intégrable. Et, pour $t\in I$, $\big(\alpha f(t)+\beta g(t)\big)=\alpha^2 f^2(t)+\beta^2 g(t)+2\alpha\beta\,f(t)\,g(t)$; or, $f\in L_2(I)$, donc l'intégrale $\int_I f^2(t)\,\mathrm{d}t$ converge, et de même, l'intégrale $\int_I g^2(t)\,\mathrm{d}t$ converge. De plus, d'après la question précédente, l'intégrale $\int_I f(t)\times g(t)\,\mathrm{d}t$ converge. On en déduit que l'intégrale $\int_I(\alpha f+\beta g)^2\,\mathrm{d}t$ converge, *i.e.* $\alpha f+\beta g\in L_2(I)$.
3. L'intersection de deux sous-espaces vectoriels est un sous-espace vectoriel. Or, $L_2(I)$ est un *sev* de $\mathrm{Cpm}(I)$, et $\mathscr{C}(I)$ est un *sev* de $\mathrm{Cpm}(I)$. D'où $L_2(I)\cap\mathscr{C}(I)$ est un *sev* de $\mathrm{Cpm}(I)$. On en déduit que $L_2(I)\cap\mathscr{C}(I)$ est un espace vectoriel.

4. — Soit $a \in I$. On pose la fonction continue par morceaux

$$\begin{aligned} \varphi : I &\longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 0 & \text{si } x \neq a \\ 1 & \text{si } x = a. \end{cases} \end{aligned}$$

On a bien $\varphi \in L_2(I)$, et $\int_I \varphi^2(t)\,\mathrm{d}t = 0$ alors que $\varphi \neq 0$ car $\varphi(a) \neq 0$. Ainsi, l'application $\langle \cdot \mid \cdot \rangle$ n'est pas définie, ce n'est donc pas un produit scalaire.

— Par linéarité de l'intégrale, l'application $\langle \cdot \mid \cdot \rangle$ est bilinéaire. Par commutativité de la multiplication de réels, elle est symétrique. Par croissance de l'intégrale, elle est aussi positive. Finalement, si $f \in L_2(I) \cap \mathscr{C}(I)$, et que $\int_I f^2(t)\,\mathrm{d}t = 0$ alors $f = 0$ car f^2 est continue et ne change pas de signe.

["Secret"] On dit que $f \in L_1(I)$ si, et seulement si l'intégrale $\int_I \big|f(t)\big|\,\mathrm{d}t$ converge.

Exercice :
Soit $n \in \mathbb{N}$.

1. *Montrer que les applications*

$$\varphi(P,Q) = \int_{-1}^{1} P(t)\,Q(t)\,\mathrm{d}t \qquad \text{et} \qquad \psi(P,Q) = \sum_{k=0}^{n} P(k)\,Q(k)$$

sont deux produits scalaires sur l'espace vectoriel $\mathbb{R}_n[X]$, et écrire la norme associé à chaque produit scalaire.

2. *Montrer que φ est encore un produit scalaire sur l'espace vectoriel $\mathbb{R}[X]$ mais que ψ ne l'est plus.*

1. On a $E = \mathbb{R}_n[X] \subset \mathscr{C}([-1,1])$. Or, φ est déjà un produit scalaire donc c'est encore un produit scalaire sur le sous-espace vectoriel $\mathbb{R}_n[X]$. Sinon, on remontre les conditions pour que φ soit un produit scalaire. On voit clairement que φ est bilinéaire (par linéarité de l'intégrale), symétrique (par commutativité du produit), et positive (par croissance de l'intégrale). Montrons que l'application φ est définie : si $\langle P \mid P \rangle = 0$, alors $\int_{-1}^{1} P^2(t)\,\mathrm{d}t = 0$; ainsi, la fonction $[-1,1] \to \mathbb{R}, t \mapsto P(t)$ est nulle car P^2 est continue et ne change pas de signe. On en déduit que le polynôme P a une infinité de racines, c'est donc le polynôme nul.

   On voit clairement que l'application ψ est bilinéaire (par linéarité de la somme), symétrique (par commutativité du produit), positive (par croissance de la somme). Montrons que la fonction ψ est définie : soit $P \in \mathbb{R}_n[X]$ tel que $\psi(P,P) = 0$, alors $\sum_{k=0}^{n} P^2(k) = 0$, d'où $\forall k \in [\![0,n]\!]$, $P(k) = 0$, le polynôme P a donc au moins $n+1$ racines. Or, comme P pour degré au plus n, on en déduit que P est le polynôme nul. La fonction ψ est donc un produit scalaire.

   La norme associée au produit scalaire φ est

$$\|\cdot\|_\varphi : P \mapsto \|P\|_\varphi = \sqrt{\int_{-1}^{b} P^2(t)\,\mathrm{d}t}.$$

Et, la norme associée au produit scalaire ψ est

$$\|\cdot\|_\psi : P \mapsto \|P\|_\psi = \sqrt{\sum_{k=0}^{n} P^2(k)}.$$

2. On a $\mathbb{R}[X] \subset \mathscr{C}([-1,1])$, le produit scalaire φ en est toujours un sur l'espace vectoriel $\mathbb{R}[X]$. Mais, ψ n'est plus un produit scalaire sur $\mathbb{R}[X]$. En effet, on considère le polynôme $P(X) = X \cdot (X-1) \cdots (X-n) \neq 0$ de $\mathbb{R}_n[X]$, et $\psi(P,P) = \sum_{k=0}^{n} P^2(k) = \sum_{k=0}^{n} 0 = 0$.

VII.2 (In)égalités

Théorème (Inégalité de Cauchy-Schwarz) **:** Soit $\langle \cdot \mid \cdot \rangle$ un produit scalaire sur un espace vectoriel E. Alors,

$$\forall (\vec{x}, \vec{y}) \in E^2, \quad \big| \langle \vec{x} \mid \vec{y} \rangle \big| \leqslant \|\vec{x}\| \cdot \|\vec{y}\|.$$

Et, il y a égalité si et seulement si les vecteurs $\vec{x}$ et $\vec{y}$ sont colinéaires.

L'inégalité ci-dessous est toujours vrai si l'on n'a pas un produit scalaire mais une application bilinéaire, symétrique et positive (*i.e.* on n'utilise pas le caractère défini de l'application). Mais, le cas de l'égalité n'est pas toujours vrai si l'application n'est pas définie.

Preuve :
On suppose $\vec{y} \neq \vec{0}$. En effet, si $\vec{x} = \vec{0}$, l'inégalité est clairement vérifiée. Posons la fonction f définie comme

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ \lambda &\longmapsto \langle \vec{x} + \lambda \vec{y} \mid \vec{x} + \lambda \vec{y} \rangle \end{aligned}$$

Par bilinéarité, on a

$$\forall \lambda \in \mathbb{R}, \quad f(\lambda) = \lambda^2 \langle \vec{y} \mid \vec{y} \rangle + \lambda \big(\langle \vec{x} \mid \vec{y} \rangle + \langle \vec{y} \mid \vec{x} \rangle \big) + \langle \vec{x} \mid \vec{x} \rangle .$$

Et, par symétrie, on en déduit que

$$\forall \lambda \in \mathbb{R}, \quad f(\lambda) = \lambda^2 \langle \vec{y} \mid \vec{y} \rangle + 2\lambda \langle \vec{x} \mid \vec{y} \rangle + \langle \vec{x} \mid \vec{x} \rangle ,$$

qui est un polynôme de degré 2 (car $\langle y \mid y \rangle \neq 0$) Or, pour $\lambda \in \mathbb{R}$, on a $f(\lambda) \geqslant 0$ par positivité du produit scalaire. Donc le discriminant du polynôme $f(\lambda)$ en λ est négatif ou nul (pour ne pas que $f(\lambda)$ ne change de signe). Or, le discriminant Δ est

$$\Delta = \big(2 \langle \vec{x} \mid \vec{y} \rangle \big)^2 - 4 \cdot \|\vec{x}\|^2 \cdot \|\vec{y}\|^2 \leqslant 0.$$

" $\Longleftarrow$ " Si $\vec{x}$ et $\vec{y}$ sont colinéaires, alors il existe $\lambda \in \mathbb{R}$ tel que $\vec{y} = \lambda\vec{x}$ ou $\vec{x} = \lambda\vec{y}$. Quite à utiliser le caractère symétrique du produit scalaire, on suppose, sans perdre de généralités, que $\vec{x} = \lambda\vec{y}$. On a donc $\langle \vec{x} \mid \vec{y} \rangle = \langle \vec{x} \mid \lambda\vec{y} \rangle = \lambda \cdot \|\vec{x}\|^2$. Et, $\|\vec{x}\| \cdot \|\vec{y}\| = \|\vec{x}\| \cdot \|\lambda\vec{x}\| = \|x\| \cdot |y| \cdot \|\vec{x}\|$, d'où l'égalité.

" $\Longrightarrow$ " On suppose $|\langle \vec{x} \mid \vec{y} \rangle| = \|\vec{x}\| \cdot \|\vec{y}\|$. Alors, $\Delta = 0$ et donc il existe $\lambda \in \mathbb{R}$ tel que $f(\lambda) = 0$, *i.e.* $\langle \vec{x} + \lambda\vec{y} \mid \vec{x} + \lambda\vec{y} \rangle = 0$. Ainsi, par le caractère défini du produit scalaire, alors $x + \lambda\vec{y} = \vec{0}$, *i.e.* $\vec{x}$ et $\vec{y}$ sont colinéaires.

□

EXEMPLE : 1. On munit $\mathbb{R}^n$ de son produit scalaire canonique :

$$\langle \vec{x} \mid \vec{y} \rangle = \sum_{i=1}^{n} x_i y_i.$$

Ainsi, par inégalité de CAUCHY-SCHWARZ ($|\langle \vec{x} \mid \vec{y} \rangle| \leqslant \|\vec{x}\| \cdot \|\vec{y}\|$),

$$\Big| \sum_{i=1}^{n} x_i y_i \Big| \leqslant \sqrt{\sum_{i=1}^{n} x_i^2} \cdot \sqrt{\sum_{i=1}^{n} y_i^2}.$$

Mieux, en appliquant l'inégalité de CAUCHY-SCHWARZ aux vecteurs $(|x_1|, \ldots, |x_n|)$ et $(|y_1|, \ldots, |y_n|)$, on a donc

$$\Big| \sum_{i=1}^{n} x_i y_i \Big| \leqslant \sum_{i=1}^{n} |x_i y_i| \leqslant \sqrt{\sum_{i=1}^{n} x_i^2} \cdot \sqrt{\sum_{i=1}^{n} y_i^2}.$$

2. On munit $\mathscr{C}([a,b])$ de son produit scalaire canonique $\langle f \mid y \rangle = \int_a^b f(t)\, g(t)\, \mathrm{d}t$. Ainsi,

$$\Big| \int_a^b f(t)\, g(t)\, \mathrm{d}t \Big| \leqslant \int_a^b |f(t)\, g(t)|\, \mathrm{d}t \leqslant \sqrt{\int_a^b f^2(t)\, \mathrm{d}t} \cdot \sqrt{\int_a^b g^2(t)\, \mathrm{d}t}$$

en appliquant CAUCHY-SCHWARZ aux fonctions f et g, puis aux fonctions $|f|$ et $|g|$.

3. On munit l'espace vectoriel $L_2(I)$ de la fonction ("pseudo-produit scalaire") $\langle f \mid g \rangle = \int_I f(t)\, g(t)\, \mathrm{d}t$. Cette formule vérifie les hypothèses de bilinéarité, de symétrie et de positivité. Et, avec ces hypothèses, l'inégalité de CAUCHY-SCHWARZ :

$$\Big| \int_a^b f(t)\, g(t)\, \mathrm{d}t \Big| \leqslant \int_a^b |f(t)\, g(t)|\, \mathrm{d}t \leqslant \sqrt{\int_a^b f^2(t)\, \mathrm{d}t} \cdot \sqrt{\int_a^b g^2(t)\, \mathrm{d}t}.$$

Corollaire : Soit $\langle \cdot \mid \cdot \rangle$ un produit scalaire sur un $\mathbb{R}$-espace vectoriel E. La norme

$$\begin{aligned} \|\cdot\| : E &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto \sqrt{\langle x \mid x \rangle} \end{aligned}$$

vérifie

1. $\forall x \in E$, si $\|x\| = 0$, alors $x = 0$;
2. $\forall x \in E$, $\forall \lambda \in \mathbb{R}$, on a $\|\lambda \cdot x\| = |\lambda| \cdot \|x\|$;
3. $\forall (x, y) \in E^2$, on a $\|x + y\| \leqslant \|x\| + \|y\|$. (inégalité triangulaire)

Corollaire : Si x et y sont deux vecteurs non nuls, alors il existe un unique $\theta \in [0, \pi]$ tel que

$$\langle x \mid y \rangle = \|x\| \, \|y\| \, \cos\theta.$$

On appelle θ l'*écart angulaire* des deux vecteurs. Également,

$$x \text{ et } y \text{ sont colinéaires} \iff \theta = 0 \text{ ou } \theta = \pi.$$

Remarque :
On munit un espace vectoriel E d'un produit scalaire $\langle \cdot \mid \cdot \rangle$, et on calcule

$$\begin{cases} \|x + y\|^2 = \langle x + y \mid x + y \rangle = \|x\|^2 + 2\langle x \mid y \rangle + \|y\|^2 \\ \|x - y\|^2 = \langle x + y \mid x + y \rangle = \|x\|^2 + 2\langle x \mid y \rangle + \|y\|^2. \end{cases}$$

Par somme et produit, il en résulte l'égalité

$$2\|x\|^2 + 2\|y\|^2 = \|x + y\|^2 + \|x - y\|^2.$$

Et, en isolant les termes du premier système, on trouve

$$\begin{cases} 2\langle x \mid y \rangle = \|x + y\|^2 - \|x\|^2 - \|y\|^2 \\ 2\langle x \mid y \rangle = \|x\|^2 + \|y\|^2 - \|x - y\|^2 \end{cases}.$$

Par somme, on trouve aussi

$$4\langle x \mid y \rangle = \|x + y\|^2 - \|x - y\|^2.$$

VII.3 Orthogonalité

Définition :

Exemple :
On munit l'espace vectoriel $E = \mathscr{C}([-1, 1])$ de son produit scalaire canonique.

1. Montrons que les fonctions $u : x \mapsto 1 + x^2$ et $v : x \mapsto 2 - 5x^2$ sont orthogonales (*i.e.* $u \perp v$) :

$$\langle u \mid v \rangle = \int_{-1}^{1} (1 + x^2)(2 - 5x^2) \, \mathrm{d}x = 0$$

en développant l'intégrande.

2. Montrons que les sous-espaces vectoriel $\mathscr{P}$ des fonctions paires et $\mathscr{I}$ des fonctions impaires sont orthogonales (*i.e.* $\mathscr{P} \perp \mathscr{I}$). Soit $f \in \mathscr{P}$ et $g \in \mathscr{I}$.

$$\begin{aligned}\langle f \mid g\rangle &= \int_{-1}^{1} f(t)\, g(t)\, \mathrm{d}t \\ &= \int_{1}^{-1} f(-u)\, g(-u) \quad -\mathrm{d}u \text{ avec le } cdv\ u = -t \text{ qui est } \mathscr{C}^1 \\ &= \int_{-1}^{1} f(u) \cdot \big(-g(u)\big)\, \mathrm{d}u \\ &= 0.\end{aligned}$$

Proposition : Si n vecteurs $v_1, \dots, v_n$ sont orthogonaux deux à deux [a], alors

$$\Big\| \sum_{i=1}^{n} v_i \Big\|^2 = \sum_{i=1}^{n} \|v_i\|^2.$$

a. *i.e.* $\forall i \neq j,\ v_i \perp v_j$

Preuve :
Par définition,

$$\begin{aligned}\Big\| \sum_{i=1}^{n} \vec{v}_i \Big\|^2 &= \Big\langle \sum_{i=1}^{n} \vec{v}_i \,\Big|\, \sum_{j=1}^{n} \vec{v}_i \Big\rangle \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \langle \vec{v}_i \mid \vec{v}_j \rangle \text{ par bilinéarité} \\ &= \sum_{(i,j)\in[\![1,n]\!]^2} \langle \vec{v}_i \mid \vec{v}_j \rangle \\ &= \sum_{(i,j)\in[\![1,n]\!]^2} \delta_{i,j}\, \langle \vec{v}_i \mid \vec{v}_j \rangle \\ &= \sum_{i=1}^{n} \langle \vec{v}_i \mid \vec{v}_i \rangle \\ &= \sum_{i=1}^{n} \|\vec{v}_i\|^2\end{aligned}$$

□

REMARQUE : 1. On a, **pour deux vecteurs** u et v

$$u \perp v \iff \|u+v\|^2 = \|u\|^2 + \|v\|^2.$$

2. Mais, ce résultat est **faux** en général pour plus de deux vecteurs. Contre-exemple : soit $\vec{u} \in E$ un vecteur non nul d'un espace vectoriel E ; on pose $\vec{v} = \vec{w} = -2\vec{u}$. D'une part, $\|\vec{u}\|^2 + \|\vec{v}\|^2 + \|\vec{w}\|^2 = (1+4+4)\,\|\vec{u}\|^2 = 9\|\vec{u}\|^2$. D'autre part $\|\vec{u} + \vec{v} + \vec{w}\|^2 = \| -3\vec{u}\|^2 = 9\|\vec{u}\|^2$. Mais, $\vec{u}$, $\vec{v}$ et $\vec{w}$ sont colinéaires.

Proposition : Si n vecteurs non nuls sont orthogonaux deux à deux, alors ils sont linéairement indépendants. *Autrement dit*, une famille orthogonale de vecteurs non nuls est libre.

Preuve :
Soit $(v_1, \dots, v_n)$ une famille de vecteurs non nuls, orthogonaux deux à deux. On suppose que $\alpha_1\vec{v}_1 + \cdots + \alpha_n\vec{v}_n = \vec{0}$. D'où,

$$0 = \langle \alpha_1\vec{v}_1 + \cdots + \alpha_n\vec{v}_n \mid \vec{v_1}\rangle = \alpha_1 \langle \vec{v}_1 \mid \vec{v}_1\rangle .$$

Or, $\langle \vec{v}_1 \mid \vec{v}_1\rangle \neq 0$ car $\vec{v}_1 \neq \vec{0}$, donc $\alpha_1 = 0$. De même pour $\vec{v}_2, \dots, \vec{v}_n$. On en déduit que $\alpha_1 = \cdots = \alpha_n = 0$, la famille est donc libre. □

Définition : Soit A un sous-espace vectoriel d'un espace préhilbertien E. L'ensemble des vecteurs orthogonaux à A est appelé l'*orthogonal* de A et est noté $A^\perp$:

$$A^\perp = \{\vec{x} \in E \mid \vec{x} \perp A\} = \{\vec{x} \in E \mid \forall \vec{y} \in A,\ \vec{x} \perp \vec{y}\}.$$

Exercice :

1. *Montrer que* $\{0_E\}^\perp = E$ *et que* $E^\perp = \{0_E\}$.
2. *Soit l'espace vectoriel* $\mathbb{R}^3$ *muni du produit scalaire canonique. Soit* $\vec{u} = (1, 2, 3)$. *Déterminer une base de* $\mathrm{Vect}(\vec{u})^\perp$.
3. *Soit le produit scalaire* $\langle P \mid Q\rangle = \int_{-1}^{1} P(t)\,Q(t)\,\mathrm{d}t$ *sur l'espace vectoriel* $E = \mathbb{R}_2[X]$. *Soit le polynôme* $U = 1 + X^2$. *Déterminer une base de* $(\mathrm{Vect}\, U)^\perp$.

1.

2. Soit $\vec{x} = (a, b, c) \in \mathbb{R}^3$.

$$\begin{aligned}
\vec{x} \in (\operatorname{Vect} u)^\perp &\iff \vec{x} \perp \operatorname{Vect}(\vec{u}) \\
&\iff \forall \vec{y} \in \operatorname{Vect}(\vec{u}),\ \vec{x} \perp \vec{y} \\
&\iff \vec{x} \perp \vec{u} \\
&\iff 1a + 2b + 3c = 0 \\
&\iff a = -2b - 3c \\
&\iff \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} -2b - 3c \\ b \\ c \end{pmatrix} = b \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} + c \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix}
\end{aligned}$$

Donc $(\operatorname{Vect} \vec{u})^\perp = \operatorname{Vect}(\vec{v}, \vec{w})$ où $\vec{v} = (-2, 1, 0)$ et $\vec{w} = (-3, 0, 1)$.

3. Soit $P = a + bX + cX^2 \in \mathbb{R}_2[X]$.

$$\begin{aligned}
P \in (\operatorname{Vect} U)^\perp &\iff P \perp \operatorname{Vect}(U) \\
&\iff \forall Q \in \operatorname{Vect}(U),\ P \perp Q \\
&\iff P \perp U \\
&\iff \left\langle a + bX + cX^2 \mid 1 + X^2 \right\rangle = 0 \\
&\iff \int_{-1}^{1} (a + bt + ct^2)(1 + t^2)\ \mathrm{d}t = 0 \\
&\iff \int_{-1}^{1} \left(ct^4 + bt^3 + (a + c)t^2 + bt + a\right)\ \mathrm{d}t = 0 \\
&\iff \frac{2}{5}c + \frac{2}{3}(a + c) + 2a = 0 \\
&\iff \frac{8}{3}a + \frac{16}{5}c = 0 \\
&\iff 5a + 2c = 0 \\
&\iff b = b \text{ et } c = -\frac{5}{2}a \\
&\iff \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ -\frac{5}{2}a \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ -\frac{5}{2} \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}
\end{aligned}$$

Ainsi, $(\operatorname{Vect} U)^\perp = \operatorname{Vect}(P, Q)$ où $P = 1 - \frac{5}{2}X^2$ et $Q = X$.

Proposition : Soient A et B deux sous-espaces vectoriels d'un espace préhilbertien E. On a

1. $A^\perp$ est un sous-espace vectoriel de E ;
2. $A \cap A^\perp = \{0_E\}$;
3. $A \perp B \iff A \subset B^\perp \iff B \subset A^\perp$;
4. $A \subset (A^\perp)^\perp$.

Preuve : 2. Tout d'abord, $\{0_E\} \subset A \cap A^\perp$; en effet, $0_E \in A$ et $0_E \in A^\perp$ car A et $A^\perp$ sont des sous-espaces vectoriels de E. Réciproquement, soit $\vec{x} \in A \cap A^\perp$. Alors, $\vec{x} \in A$ et $\vec{x} \in A^\perp$, d'où $\vec{x} \perp A$. Ainsi, pour tout vecteur $\vec{y} \in A$, $\vec{x} \perp \vec{y}$. En particulier, on a $\vec{x} \perp \vec{x}$. Ainsi, $\langle \vec{x} \mid \vec{x} \rangle = 0$ et donc $\vec{x} = 0_E$ par le caractère défini du produit scalaire.

3.
$$\begin{aligned} A \perp B &\iff \forall \vec{x} \in A,\ \vec{x} \perp B \\ &\iff \forall \vec{x} \in A,\ \vec{x} \in B^\perp \\ &\iff A \subset B^\perp \end{aligned}$$

De même, par symétrique de la relation $\perp$,

$$A \perp B \iff B \perp A \iff B \subset A^\perp.$$

4. On $A \perp A^\perp$, et d'après 3., $A \subset (A^\perp)^\perp$.

□

VII.4 Bases orthonormées

Définition : 1. Un vecteur $\vec{x}$ est *normé* si $\|\vec{x}\| = 1$.

2. Une famille $(\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_n)$ est *orthonormée* si

$$\forall i \neq j \in [\![1, n]\!], \quad \langle \vec{\varepsilon}_i | \vec{\varepsilon}_j \rangle = \delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$

Soit $\mathscr{C} = (\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_n)$ une base orthonormée d'un espace vectoriel E. Soient $E \ni \vec{x} = x_1\vec{\varepsilon}_1 + \cdots + x_n\vec{\varepsilon}_n$, et $E \ni \vec{y} = y_1\vec{\varepsilon}_1 + \cdots + y_n\vec{\varepsilon}_n$.

1. Pour $i \in [\![1, n]\!]$, $\langle \vec{x} \mid \varepsilon_i \rangle = x_i$ par bilinéarité du produit scalaire et car la famille est orthonormée.
2. $\langle \vec{x} \mid \vec{y} \rangle = x_1y_1 + \cdots + x_ny_n$ par bilinéarité du produit scalaire et la propriété précédente.
3. $\|\vec{x}\|^2 = x_1^2 + \cdots + x_n^2$, avec la propriété précédente et $\vec{x} = \vec{y}$.
4. Soit $f \in \mathscr{L}(E)$, et soit $A = (a_{i,j})_{i,j \in [\![1,n]\!]} = \left[f\right]_{\mathscr{C}}$. Alors, $\langle \vec{\varepsilon}_i \mid f(\vec{\varepsilon}_j) \rangle = a_{i,j}$. En effet, $f(\vec{\varepsilon}_j) = a_{1,j}\vec{\varepsilon}_1 + \cdots + a_{n,j}\vec{\varepsilon}_n$. Ainsi,
$$\langle \vec{\varepsilon}_i \mid f(\vec{\varepsilon}_j) \rangle = \langle \vec{\varepsilon}_i \mid a_{1,j}\vec{\varepsilon}_1 + \cdots a_{n,j}\vec{\varepsilon}_n \rangle = a_{i,j} \langle \varepsilon_i \mid \varepsilon_i \rangle = a_{i,j}.$$

VII.5 Lalgorithme de Gram-Schmidt

Remarque :

Exercice :
Déterminer une base orthonormée de l'espace euclidien $\mathbb{R}_2[X]$ muni du produit

scalaire

$$\langle P \mid Q\rangle = \int_{-1}^{1} P(t)\,Q(t)\,\mathrm{d}t.$$

On pose la base canonique $\mathscr{B} = (1, X, X^2)$ et on construit, à l'aide de l'algorithme de GRAM-SCHMIDT, une base orthonormée $\mathscr{C} = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$.

1. On a $\varepsilon_1 = \frac{1}{\|1\|}$. Or, $\|1\| = \sqrt{\langle 1 \mid 1\rangle}$, et $\langle 1 \mid 1\rangle = \int_{-1}^{1} 1\ \mathrm{d}t = 2$, donc $\|1\| = \sqrt{2}$. On a donc
$$\varepsilon_1 = 1/\sqrt{2}.$$

2. On pose $\hat{\varepsilon}_2 = X - a\varepsilon_1$.
$$\hat{\varepsilon}_2 \perp \varepsilon_1 \iff \langle X - a\varepsilon_1 \mid \varepsilon_1\rangle = 0 \iff \langle X \mid \varepsilon_1\rangle = a\,\langle \varepsilon_1 \mid \varepsilon_1\rangle = a.$$
Calculons $a = \langle X \mid \varepsilon_1\rangle$: $\langle X \mid \varepsilon_1\rangle = \int_{-1}^{1} \frac{t}{\sqrt{2}}\,\mathrm{d}t = 0$. D'où, $\hat{\varepsilon}_2 = X$. On pose $\varepsilon_2 = X/\|X\|$. Or, $\|X\| = \sqrt{\int_{-1}^{1} t^2\,\mathrm{d}t} = \sqrt{\frac{2}{3}}$. On en déduit que
$$\varepsilon_2 = \sqrt{\frac{3}{2}}X.$$

3. On pose $\hat{\varepsilon}_3 = X^2 - a\varepsilon_1 - b\varepsilon_2$.
$$\hat{\varepsilon}_3 \perp \varepsilon_1 \iff \left\langle X^2 - a\varepsilon_1 - b\varepsilon_2 \mid \varepsilon_1\right\rangle = 0 \iff \left\langle X^2 \mid \varepsilon_1\right\rangle - a = 0 \hat{\varepsilon}_3 \perp \varepsilon_2 \iff \left\langle X^2 - a\varepsilon_1 - b\varepsilon_2 \mid \varepsilon\right.$$
On calcule a et b, et on trouve $\hat{\varepsilon}_3 = X^2 - \frac{1}{3}$. Or, $\|\hat{\varepsilon}_3\| = \sqrt{\int_{-1}^{1} \left(t^2 - \frac{1}{3}\right)^2\,\mathrm{d}t} = \frac{2\sqrt{3}}{3\sqrt{5}}$.

VII.6 Projection orthogonale (sur un *sev* de dimension finie)

Proposition–Définition : Soit E un espace préhilbertien[3], et soit F un sous-espace vectoriel de dimension **finie** n de E. Il existe une unique application linéaire $p \in \mathscr{L}(E)$ telle que

$$\forall \vec{x} \in E, \qquad (\star)\ p(\vec{x}) \in F \quad \text{et} \quad (\star\star)\ \vec{x} - p(\vec{x}) \perp F.$$

On dit que p est la *projection orthogonale*, et $p(\vec{x})$ le *projeté orthogonal* de $\vec{x}$ sur F. Dans une base orthonormée $\mathscr{B} = (\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n)$, on a

$$\forall \vec{x} \in E, \quad p(\vec{x}) = \langle \vec{x} \mid \vec{\varepsilon}_1\rangle\,\vec{\varepsilon}_1 + \cdots + \langle \vec{x} \mid \vec{\varepsilon}_n\rangle\,\vec{\varepsilon}_n = \sum_{i=1}^{n} \langle \vec{x} \mid \vec{\varepsilon}_i\rangle\,\vec{\varepsilon}_i.$$

Preuve :
On choisit une base $(\vec{e}_1, \ldots, \vec{e}_n)$ de F. On l'orthonormalise en une base

3. il peut être de dimension infinie.

$(\vec{\varepsilon}_1,\dots,\vec{\varepsilon}_n)$. Soit $\vec{x}\in E$. On a

$$(\star) \iff \exists(\lambda_1,\dots,\lambda_n)\in\mathbb{R}^n,\ p(\vec{x})=\lambda_1\vec{\varepsilon}_1+\cdots+\lambda_n\vec{\varepsilon}_n$$

et

$$\begin{aligned}(\star\star) &\iff \forall i\in[\![1,n]\!],\ \vec{x}-p(\vec{x})\perp\vec{\varepsilon}_i\\ &\iff \forall i\in[\![1,n]\!],\langle\vec{x}-p(\vec{x})\mid\vec{\varepsilon}_i\rangle=0\\ &\iff \forall i\in[\![1,n]\!],\ \langle\vec{x}-(\lambda_1\vec{\varepsilon}_1+\cdots+\lambda_n\vec{\varepsilon}_n)\mid\vec{\varepsilon}_i\rangle=0\\ &\iff \forall i\in[\![1,n]\!],\ \langle\vec{x}\mid\vec{\varepsilon}_i\rangle-\lambda_i=0\end{aligned}$$

Ainsi, on a bien

$$p(\vec{x})=\sum_{i=1}^{n}\langle\vec{x}\mid\vec{\varepsilon}_i\rangle\,\vec{\varepsilon}_i.$$

□

Exercice : 1. On pose $E=\mathbb{R}^3$, F le plan d'équation $x+y=0$, et le produit scalaire $\langle\vec{x}\mid\vec{y}\rangle = x_1y_1+\cdots+x_ny_n$. Le sous-espace vectoriel F est de dimension finie, d'où

$$\forall\vec{x}=(x,y,z)\in E,\ p(\vec{x})=\langle\vec{x}\mid\vec{\varepsilon}_1\rangle\,\vec{\varepsilon}_1+\langle\vec{x}\mid\vec{\varepsilon}_2\rangle\,\vec{\varepsilon}_2$$

où $(\vec{\varepsilon}_1,\vec{\varepsilon}_2)$ est une base orthonormée de F.

$$\begin{aligned}\vec{x}=(x,y,z)\in F &\iff x+y=0\\ &\iff z=0 \text{ et } y=-x\\ &\iff (x,y,z)=(x,-x,z)=x\underbrace{(1,-1,0)}_{\vec{e}_1}+z\underbrace{(0,0,1)}_{\vec{e}_2}\end{aligned}$$

On orthonormalise la base $(\vec{e}_1,\vec{e}_2)$ en $(\vec{\varepsilon}_1,\vec{\varepsilon}_2)$ en posant

$$\vec{\varepsilon}_1=\frac{1}{\sqrt{2}}(1,-1,0)\quad\text{et}\quad\vec{\varepsilon}_2=(0,0,1).$$

Ainsi,

$$\begin{aligned}p(\vec{x})&=\langle\vec{x}\mid\vec{\varepsilon}_1\rangle\,\vec{\varepsilon}_1+\langle\vec{x}\mid\vec{\varepsilon}_2\rangle\,\vec{\varepsilon}_2\\ &=\frac{x-y}{\sqrt{2}}\vec{\varepsilon}_1+z\vec{\varepsilon}_2.\end{aligned}$$

D'où,

$$\big[p\big]_{(\vec{\imath},\vec{\jmath},\vec{k})}=\begin{array}{c}\begin{pmatrix}\frac{1}{2} & -\frac{1}{2} & 0\\ -\frac{1}{2} & \frac{1}{2} & 0\\ 0 & 0 & 1\end{pmatrix}\begin{matrix}\vec{\imath}\\ \vec{\jmath}\\ \vec{k}\end{matrix}\\ \begin{matrix}p(\vec{\imath}) & p(\vec{\jmath}) & p(\vec{k})\end{matrix}\end{array}$$

2. On pose $E = \mathbb{R}[X]$, $F = \mathbb{R}_2[X]$, et le produit scalaire $\langle P \mid Q \rangle = \int_{-1}^{1} P(t)\,Q(t)\,\mathrm{d}t$. Le *sev* F est de dimension finie, égale à 3. On construit une base $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ orthonormée de F en posant

$$\varepsilon_1 = \frac{1}{\sqrt{2}}, \qquad \varepsilon_2 = \sqrt{\frac{3}{2}}X, \qquad \text{et} \qquad \varepsilon_3 = \frac{3\sqrt{5}}{2\sqrt{2}}\left(X^2 - \frac{1}{3}\right).$$

D'où,

$$p(X^3) = \left\langle X^3 \mid \varepsilon_1 \right\rangle \varepsilon_1 + \left\langle X^3 \mid \varepsilon_2 \right\rangle \varepsilon_2 + \left\langle X^3 \mid \varepsilon_3 \right\rangle \varepsilon_3.$$

D'une part, $\left\langle X^3 \mid \varepsilon_1 \right\rangle = \int_{-1}^{1} \frac{t^3}{\sqrt{2}}\,\mathrm{d}x = 0$. De même pour les autres produits scalaires. On en déduit que

$$\frac{3}{5}X.$$

Corollaire : Soit F un sous-espace vectoriel de dimension **finie** d'un espace préhilbertien $(E, \langle \cdot \mid \cdot \rangle)$.

1. F et son orthogonal sont supplémentaires : $F \oplus F^\perp = E$;
2. Par suite,
   (a) la projection orthogonale sur F est le projecteur sur F parallèlement à $F^\perp$;
   (b) $F = (F^\perp)^\perp$.

Preuve :
D'après la proposition 18, $F \cap F^\perp = \{\vec{0}\}$, leur somme est donc directe. Montrons que $F + F^\perp = E$: soit $\vec{x} \in E$, alors $p(\vec{x}) \in F$ et $\vec{x} - p(\vec{x}) \in F^\perp$; en sommant ces deux vecteurs, on a bien $\vec{x} \in F + F^\perp = E$. □

Théorème (moindres carrés) **:** Soit F un sous-espace de dimension **finie** d'un espace préhilbertien E. Soit $\vec{x} \in E$. Le projeté orthogonal $p(\vec{x})$ de $\vec{x}$ sur F est l'unique vecteur tel que

$$\forall \vec{y} \in F, \quad \|\vec{x} - p(\vec{x})\| \leqslant \|\vec{x} - \vec{y}\|.$$

Preuve :
Soient $\vec{x} \in E$ et $\vec{y} \in F$. On a $\vec{x} - p(\vec{x}) \perp F$ et $p(\vec{x}) - \vec{y} \in F$, d'où $\vec{x} - p(\vec{x}) \perp p(\vec{x}) - \vec{y}$. Ainsi, d'après le théorème de Pythagore,

$$\|\vec{x} - \vec{y}\|^2 = \|\vec{x} + p(\vec{x})\|^2 + \|\vec{y} - p(\vec{x})\|^2.$$

On a donc bien $\|\vec{x} - \vec{y}\| \geqslant \|\vec{x} - p(\vec{x})\|$. Également,

$$\begin{aligned} \|\vec{x} - \vec{y}\| = \|\vec{x} - p(\vec{x})\| &\iff \|\vec{y} - p(\vec{x})\| = 0 \\ &\iff \vec{y} = p(\vec{x}). \end{aligned}$$

□

Remarque : 1. D'après le théorème précédent, la fonction

$$\begin{aligned} F &\longrightarrow \mathbb{R} \\ \vec{y} &\longmapsto \|\vec{x}-\vec{y}\| \end{aligned}$$

admet un minimum en $p(\vec{x})$.

2. Le réel $\|\vec{x}-p(\vec{x})\|$ est la *distance* entre le vecteur $\vec{x}$ et le *sev* F. On le note $d(\vec{x},F)$.
3. On a l'inégalité de Bessel : pour tout vecteur $\vec{x}\in E$, $\|p(\vec{x})\|\leqslant\|\vec{x}\|$.

Exercice :
On pose $E=\mathbb{R}_3[X]$ muni du produit scalaire

$$\langle P\mid Q\rangle=\int_{-1}^{1}P(t)\,Q(t)\,\mathrm{d}t.$$

Puis, on pose $F=\mathbb{R}_2[X]$. Alors,

$$\begin{aligned} f(a,b,c)&=\int_{-1}^{1}\left(t^3-(at^2+bt+c)\right)^2\,\mathrm{d}t\\ &=\left\langle X^3-(aX^2+bX+c)\mid X^3-(aX^2+bX+c)\right\rangle\\ &=\|X^3-(aX^2+bX+c)\|^2. \end{aligned}$$

Or, d'après le théorème des moindres carrés, $f(a,b,c)$ est minimal pour $aX^2+bX+c=p(X^3)$, où p est la projection de E sur F, et ce minimum est atteint une seule fois :

$$\min_{(a,b,c)\in\mathbb{R}^3}f(a,b,c)=\|X^3-p(X^3)\|^2.$$

Calculons $p(X^3)$:

— On orthonormalise la base $(1,X,X^2)$ en $\mathscr{B}=(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ avec l'algorithme de Gram-Schmidt. On a déjà fait ce calcul à l'exercice 21 : $\varepsilon_1=1/\sqrt{2}$, $\varepsilon_2=\sqrt{\frac{3}{2}}X$ et $\frac{3\sqrt{5}}{2\sqrt{2}}\left(X^2-\frac{1}{3}\right)$.
— On utilise la formule de la projection orthogonale, qu'on a déjà fait à l'exercice 23 : $p(X^3)=\frac{3}{5}X$.
— On en conclut que $a=0$, $b=\frac{3}{5}$ et $c=0$.

Pour calculer la valeur de $f(0,\frac{3}{5},0)$, on pourrait calculer l'intégrale (ou de manière équivalente utiliser la norme). Mais, on utilise le théorème de Pythagore :

$$\|X^3-p(X^3)\|^2=\|X^3\|^2-\|p(X^3)\|^2.$$

Et, $\|X^3\|^2=\int_{-1}^{1}t^6\,\mathrm{d}^2=\frac{2}{7}$, et $\|p(X^3\|^2=\int_{-1}^{1}\left(-\frac{3}{5}t\right)^2\,\mathrm{d}t=\frac{9}{25}\cdot\frac{2}{3}$. Ainsi

$$f\left(0,\frac{3}{5},0\right)=\frac{2}{7}-\frac{6}{25}.$$

VII.7 Hyperplans

RAPPEL :
Un *hyperplan* H de E est le noyau d'une forme linéaire non nulle :

$$H = \operatorname{Ker}\varphi \qquad \text{où} \qquad \tilde{0} \neq \varphi : \begin{array}{ccc} E & \xrightarrow{\text{linéaire}} & \mathbb{R} \\ \vec{x} & \longmapsto & \varphi(\vec{x}) \end{array}.$$

Si E est de dimension finie n, alors

$$H \text{ est un hyperplan} \iff \dim F = n - 1.$$

Toute forme linéaire est, ou bien nulle, ou bien surjective. Si deux formes linéaires ont le même noyau, alors elles sont proportionnelles.

Proposition : Soit E un espace préhilbertien.

1. L'orthogonal d'une droite vectorielle D est un hyperplan H : $D^\perp = H$.
2. Si E est de dimension finie, l'orthogonal d'un hyperplan H est une droite vectorielle D : $H^\perp = D$. Autrement dit, toutes les équations d'un hyperplan sont proportionnelles (*i.e.* les mêmes à un facteur près).

Preuve : 1. Il existe un vecteur $\vec{a} \in E \setminus \{\vec{0}\}$ tel que $D = \operatorname{Vect}(\vec{a})$. Soit $\vec{x} \in E$.

$$\begin{aligned} \vec{x} \in D^\perp &\iff \vec{x} \perp D \\ &\iff \forall \vec{y} \in D,\ \vec{x} \perp \vec{y} \\ &\iff \vec{x} \perp \vec{a} \\ &\iff \langle \vec{x} \mid \vec{a} \rangle = 0 \end{aligned}$$

Soit $\varphi(\vec{x}) = \langle \vec{x} \mid \vec{a} \rangle$. L'application φ est une forme linéaire par bilinéarité du produit scalaire. Ainsi, on a bien $\vec{x} \in D^\perp \iff \vec{x} \in \operatorname{Ker}\varphi$. Or, la forme linéaire n'est pas nulle car $\varphi(\vec{a}) \neq 0$, par le caractère défini du produit scalaire.

2. D'après le corolaire 24, comme E est de dimension finie n, $H \oplus H^\perp = E$. Or, $\dim H = n - 1$ et donc $\dim(H^\perp) = n - (n-1) = 1$. L'espace vectoriel $H^\perp$ est bien une droite vectorielle.

□

Théorème (représentation de RIESZ) **:** Soit E un espace **euclidien**. Pour toute forme linéaire $\varphi : E \to \mathbb{R}$, alors il existe un unique vecteur

$\vec{a} \in E$ tel que $\varphi = \langle \vec{a} \mid \cdot \rangle$, *i.e.*

$$\forall \vec{x} \in E, \quad \varphi(\vec{x}) = \langle \vec{a} \mid \vec{x} \rangle .$$

Preuve :
Soit $\mathcal{B} = (\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_n)$ une base orthonormée de E (que l'on peut trouver à l'aide de l'algorithme de Gram-Schmidt). Soit $\vec{x} \in E$. On pose $\vec{x} = x_1\vec{\varepsilon}_1 + x_2\vec{\varepsilon}_2 + \cdots + x_n\vec{\varepsilon}_n$. L'application φ est linéaire, donc $\varphi(\vec{x}) = x_1\varphi(\vec{\varepsilon}_1) + \cdots + x_n\varphi(\vec{\varepsilon}_n)$. On pose, pour $i \in [\![1, n]\!]$, $a_i = \varphi(\vec{\varepsilon}_i)$. Ainsi,

$$\varphi(\vec{x}) = x_1a_1 + \cdots + x_na_n.$$

On pose $\vec{a} = a_1\vec{\varepsilon}_1 + \cdots + a_n\vec{\varepsilon}_n$. Ainsi, $\langle \vec{a} \mid \vec{x} \rangle = \varphi(\vec{x})$. Montrons que ce vecteur $\vec{a}$ est unique. Par l'absurde, on suppose que $\vec{a} \neq \vec{b}$ et $\langle \vec{a} \mid \vec{x} \rangle = \left\langle \vec{b} \mid \vec{x} \right\rangle$. Alors, $\forall \vec{x} \in E$, $\left\langle \vec{x} \mid \vec{a} - \vec{b} \right\rangle = 0$ par bilinéarité. En particulier, $\vec{a} - \vec{b} \in E$, et donc $\left\langle \vec{a} - \vec{b} \mid \vec{a} - \vec{b} \right\rangle = 0$, ce qui est absurde car $\vec{a} - \vec{b} \neq \vec{0}$. □

Exercice : 1. On sait que $d(\vec{x}, H) = \|\vec{x} - p(\vec{x})\|$ où p est la projection orthogonale sur H, qui existe car H est de dimension finie, car E est euclidien. On veut montrer que

$$d(\vec{x}, H) = \frac{|\langle \vec{x} \mid \vec{a} \rangle|}{\|\vec{a}\|}$$

où $\vec{a} \neq \vec{0}$ et est orthogonal à H. On sait déjà que $\mathrm{Vect}(\vec{a}) \perp H$, d'où $\mathrm{Vect}(\vec{a}) \subset H^\perp$. Par un argument de dimensions, on a $H^\perp = \mathrm{Vect}(\vec{a})$ car $H \oplus H^\perp = E$. On sait déjà que $\vec{x} - p(\vec{x}) \in H^\perp$, il existe donc $\lambda \in \mathbb{R}$ tel que $\vec{x} - p(\vec{x}) = \lambda\vec{a}$. D'où,

$$\begin{aligned} \langle \vec{x} - p(\vec{x}) \rangle &= \lambda \langle \vec{a} \mid \vec{a} \rangle = \lambda \|a\|^2 \\ &= \langle \vec{x} \mid \vec{a} \rangle \end{aligned}$$

car $p(\vec{x}) \perp \vec{a}$. D'où, $\lambda = \langle \vec{x} \mid \vec{a} \rangle / \|\vec{a}\|^2$. Ainsi,

$$\begin{aligned} \|\vec{x} - p(\vec{x})\|^2 &= \left\| \frac{\langle \vec{x} \mid \vec{a} \rangle}{\|\vec{a}\|^2} \cdot \vec{a} \right\| \\ &= \frac{\langle \vec{x} \mid \vec{a} \rangle^2}{\|\vec{a}\|^4} \|\vec{a}\|^2 \\ &= \left(\frac{\langle \vec{x} \mid \vec{a} \rangle}{\|a\|} \right)^2 \end{aligned}$$

D'où

$$d(\vec{x}, H) = \left| \frac{\langle \vec{x} \mid \vec{a} \rangle}{\|\vec{a}\|} \right| = \frac{|\langle \vec{x} \mid \vec{a} \rangle|}{\|\vec{a}\|}.$$

2. D'après le théorème de Pythagore,

$$d^2(\vec{x}, D) + d^2(\vec{x}, H) = \|\vec{x}\|^2$$

d'où

$$\begin{aligned} d(\vec{x}, D) &= \sqrt{\|\vec{x}\|^2 - d^2(\vec{x}, H)} \\ &= \sqrt{\|\vec{x}\|^2 - \frac{\langle \vec{x} \mid \vec{a} \rangle^2}{\|a\|^2}} \\ &= \frac{\sqrt{\|\vec{a}\|^2 \cdot \|\vec{x}\|^2 - \langle \vec{x} \mid \vec{a} \rangle}}{\|\vec{a}\|} \end{aligned}$$

Chapitre 10

Séries entières

On rappelle qu'il existe des séries numériques $\sum u_n$, des séries de fonctions $\sum f_n$ (à ne pas confondre avec la série numérique $\sum f_n(x)$). Dans ce chapitre, on s'intéresse à un cas particulier de séries de fonctions, celles de la forme $\sum a_n x^n$ (qui est un abus de langage, il ne s'agit pas d'une série numérique malgré son apparence). Ainsi, la somme des termes de cette série est de la forme

$$\sum_{k=0}^{\infty} a_n x^n = a_0 x^0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \cdots .$$

Si, à partir d'un certain rang, la suite $(a_n)_{n\in\mathbb{N}}$ est nulle, alors il s'agit d'un polynôme. Une série entière est une généralisation des polynômes. Toute troncature de la somme des termes d'une série entière est un développement limité.

Définition : Une série de fonctions $\sum f_n$ est appelée *série entière* s'il existe une suite de réels $(a_n)_{n\in\mathbb{N}}$ tels que

$$\forall n \in \mathbb{N},\ \forall x \in \mathbb{R}, \quad f_n(x) = a_n\, x^n.$$

Somme	Rayon de convergence
$\dfrac{1}{1-x} = \displaystyle\sum_{k=0}^{\infty} x^k$	1
$\dfrac{1}{1+x} = \displaystyle\sum_{k=0}^{\infty} (-1)^k\, x^k$	1
$\dfrac{1}{1+x^2} = \displaystyle\sum_{k=0}^{\infty} \left(-x^2\right)^k$	1
$\ln(1+x) = \displaystyle\sum_{k=1}^{\infty} (-1)^k \dfrac{x^k}{k}$	1
$\operatorname{Arctan} x = \displaystyle\sum_{k=0}^{\infty} (-1)^k \dfrac{x^{2k+1}}{2k+1}$	1
$\mathrm{e}^x = \displaystyle\sum_{k=0}^{\infty} \dfrac{x^k}{k!}$	∞
$\operatorname{ch} x = \displaystyle\sum_{k=0}^{\infty} \dfrac{x^{2k}}{(2k)!}$	∞
$\operatorname{sh} x = \displaystyle\sum_{k=0}^{\infty} \dfrac{x^{2k+1}}{(2k+1)!}$	∞
$\cos x = \displaystyle\sum_{k=0}^{\infty} (-1)^k \dfrac{x^{2k}}{(2k)!}$	∞
$\sin x = \displaystyle\sum_{k=0}^{\infty} (-1)^k \dfrac{x^{2k+1}}{(2k+1)!}$	∞
$(1+x)^\alpha = 1 + \displaystyle\sum_{k=1}^{\infty} \big(\alpha(\alpha-1)\cdots(\alpha-k+1)\big) \dfrac{x^k}{k!}$	1

TABLE 10.1 – Séries entières usuelles

EXERCICE :
On admet les formules de la table précédente. On applique la formule de la

dernière ligne dans le cas $\alpha = -1/2$:

$$\begin{aligned}
\forall x \in]-1,1[, \quad & \frac{1}{\sqrt{1-x}} \\
&= 1 + \alpha(-x) + \frac{\alpha(\alpha-1)}{2!}(-x)^2 + \cdots + \frac{\alpha(\alpha-1)\cdots\big(\alpha-(n-1)\big)}{n!}(-x)^n + \cdots \\
&= 1 + \frac{1}{2}\sum_{n=1}^{\infty} \frac{\left(\frac{1}{2}+1\right)\cdots\left(\frac{1}{2}+n-1\right)}{n!}x^n \\
&= 1 + \frac{1}{2}\sum_{n=1}^{\infty} \frac{3\times\cdots\times(2n-1)}{2^n\times n!}x^n \\
&= 1 + \frac{1}{2}\sum_{n=1}^{\infty} \frac{1\times 2\times 3\times\cdots\times(2n-1)\times 2n}{2^n\times n!\times 2\times 4\times\cdots\times(2n-2)\times 2n}x^n \\
&= 1 + \frac{1}{2}\sum_{n=1}^{\infty} \frac{(2n)!}{n!\times 2^n\times 2^n(n!)}x^n \\
&= 1 + \frac{1}{2}\sum_{n=1}^{\infty} \binom{2n}{n}\frac{x^n}{4^n}.
\end{aligned}$$

VII.1 Rayon de convergence

Lemme (d'Abel) **:** Soit un réel $x_0 > 0$. Si la suite $(a_n x_0^n)_{n\in\mathbb{N}}$ est bornée, alors la série $\sum a_n x^n$ converge absolument pour tout réel $x \in]-x_0, x_0[$.

Preuve :
On veut montrer que si la suite $(a_n x_0^n)_{n\in\mathbb{N}}$ est bornée, alors, pour $x \in]-x_0, x_0[$, la série numérique $\sum a_n x^n$ converge absolument. On suppose la suite $(a_n x_0^n)_{n\in\mathbb{N}}$ bornée. Ainsi, il existe $M \in \mathbb{R}^+$ tel que pour tout $n \in \mathbb{N}$, $|a_n x_0^n| \leqslant M$. Ce lemme est vrai si $x_0 = 0$; on suppose à présent $x_0 \neq 0$. Alors,

$$|a_n x^n| = \left|a_n x_0^n \frac{x^n}{x_0^n}\right| \leqslant M \times \left|\frac{x}{x_0}\right|^n.$$

Or, la série $\sum M\left|\frac{x}{x_0}\right|^n = M\sum\left|\frac{x}{x_0}\right|^n$ converge si $\left|\frac{x}{x_0}\right| < 1$. Donc, si $\left|\frac{x}{x_0}\right| < 1$, alors la série $\sum |a_n x^n|$ converge. □

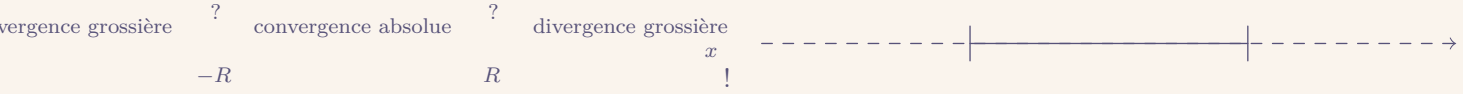


Figure 10.1 – Rayon de convergence – convergence absolue et divergence grossière

Proposition–Définition : Soit $\sum a_n x^n$ une série entière. Il existe un unique $R \in \bar{\mathbb{R}}_+ = \mathbb{R}_+ \cup \{+\infty\}$ tel que

— si $|x| < R$, alors la série $\sum a_n x^n$ converge absolument ;

— si $|x| > R$, alors la série $\sum a_n x^n$ diverge grossièrement ;

Le réel R est appelé *rayon de convergence* de la série entière. Il vaut

$$R = \sup\{\, r \in \mathbb{R}^+ \mid (a_n r^n) \text{ bornée} \,\}.$$

Preuve :
Soit $x \in \mathbb{R}$.

1er cas $|x| < R$. Soit $x_0 = (|x| + R)/2 < R$. Alors, la suite $(a_n x_0^n)_{n\in\mathbb{N}}$ est bornée. D'où, d'après le lemme d'Abel, la série numérique $\sum a_n x^n$ converge absolument.

2nd cas $|x| > R$. Alors, la suite $(a_n x^n)_{n\in\mathbb{N}}$ n'est plus bornée. D'où la suite $(a_n x^n)_{n\in\mathbb{N}}$ n'est pas convergente, et ne tend pas vers 0. On en déduit que la série numérique $\sum a_n x^n$ diverge grossièrement.

□

Remarque :
On a

$$\begin{aligned} R &= \sup\{\, r \in \mathbb{R}^+ \mid (a_n r^n)_{n\in\mathbb{N}} \text{ bornée} \,\} \text{ par définition} \\ &= \sup\{\, r \in \mathbb{R}^+ \mid \textstyle\sum a_n r^n \text{ converge} \,\} \text{ par le théorème 4} \\ &= \sup\{\, r \in \mathbb{R}^+ \mid \textstyle\sum |a_n r^n| \text{ converge} \,\} \text{ par le théorème 4} \\ &= \sup\{\, r \in \mathbb{R}^+ \mid (a_n r^n)_{n\in\mathbb{N}} \text{ tend vers } 0 \,\} \end{aligned}$$

Exemple ($R = +\infty$) :
On considère la série $\sum \frac{x^n}{n!}$. *Calculons son rayon de convergence.* Soit $u_n = \left|\frac{x^n}{n!}\right|$. Si $x = 0$, la série $\sum u_n$ converge vers 1. On suppose $x \neq 0$. On calcule

$$\frac{u_{n+1}}{u_n} = \frac{|x|}{n+1} \xrightarrow[n\to\infty]{} 0.$$

D'où, d'après le critère de D'Alembert, la série $\sum u_n$ converge. On en déduit que, pour tout $x \in \mathbb{R}$, la série $\sum a_n x^n$ converge, *i.e.* son rayon de convergence vaut $R = +\infty$.

Exemple ($R = 0$) :
On considère la série $\sum n^n x^n$. *Calculons son rayon de convergence.* Si $x = 0$, la série converge vers 1. On suppose maintenant $x \neq 0$. Alors, à partir d'un certain rang, $|nx| \geqslant 7$. Or, la somme $\sum 7^n$ diverge grossièrement. D'où, la série $\sum |nx|^n$ diverge aussi. Comme la série $\sum (nx)^n$ ne converge pas absolument, on en déduit que la série $\sum n^n x^n$ ne converge absolument que si $x = 0$. On en déduit que $R = 0$.

Exemple ($R \in]0,+\infty[$, et diverge aux deux bords) :
On considère la série $\sum x^n$. *Calculons son rayon de convergence.* Il s'agit d'une série géométrique, mais il s'agit aussi d'une série entière, où $\forall n \in \mathbb{N}$, $a_n = 1$. Or, on sait que

$$\sum_{k=0}^{n} x^k = \begin{cases} \frac{1-x^{n+1}}{1-x} & \text{si } x \neq 1 \quad \text{qui converge si et seulement si } |x| < 1 \\ n+1 & \text{si } x = 1 \quad \text{qui diverge.} \end{cases}$$

Donc, la série $\sum x^n$ converge si et seulement si $|x| < 1$. On en déduit que $R = 1$.

Exemple ($R \in]0,+\infty[$, et diverge d'un bord, converge de l'autre) :
On considère la série $\sum \frac{x^n}{n}$. Si $x = 1$, alors la série $\sum \frac{1}{n}$ diverge par critère de Riemann. Si $x \neq -1$, alors la série $\sum \frac{(-1)^n}{n}$ converge d'après le théorème des séries alternées car $\left(\frac{1}{n}\right)^{\searrow}_{n\in\mathbb{N}}$ tend vers 0 en décroissant. Cette situation dissymétrique nous montre que $R = 1$.

Exemple ($R \in]0,+\infty[$, et converge aux deux bords) :
On considère la série $\sum \frac{x^n}{n^2}$. *Calculons son rayon de convergence.*

— Si $x = 1$, la série $\sum \frac{1}{n^2}$ converge par critère de Riemann. D'où $R \geqslant 1$.

— Si $|x| > 1$, alors

$$\frac{\left|\frac{x^{n+1}}{(n+1)^2}\right|}{\left|\frac{x^n}{n^2}\right|} = \left(\frac{n}{n+1}\right)^2 \times |x| \xrightarrow[n\to\infty]{} |x|.$$

D'où, d'après le critère de d'Alembert, la série $\sum \frac{|x|^n}{n}$ diverge. D'où $R \leqslant 1$.

On en déduit que $R = 1$.

Autre méthode :

— Si $|x| > 1$, alors $\frac{x^n}{n^2} \xrightarrow[n\to\infty]{} +\infty$ par croissances comparées. D'où $R \leqslant 1$.

— Si $|x| < 1$, alors $\frac{|x|^n}{n^2} \xrightarrow[n\to\infty]{} 0$. D'où $R \geqslant 1$.

Proposition : Soient R_a et R_b les rayons de convergence des séries entières $\sum a_n x^n$ et $\sum b_n x^n$ respectivement.

1. Si, à partir d'un certain rang, $|a_n| \leqslant |b_n|$, alors $R_a \geqslant R_b$.
2. Si $a_n = \mathcal{O}_{n\to\infty}(b_n)$, alors $R_a \geqslant R_b$.
3. Si $a_n \sim_{n\to\infty} b_n$, alors $R_a = R_b$.

Preuve :
1. Ainsi, à partir d'un certain rang, $|a_n x^n| \leqslant |b_n x^n|$. D'où, si la série $\sum |b_n x^n|$ converge, alors la série $\sum |a_n x^n|$ converge. On a donc $R_b \leqslant R_a$.
2. Ainsi, $a_n = b_n \times u_n$ où $(u_n)_{n\in\mathbb{N}}$ est une suite bornée. Il existe donc $M \in \mathbb{R}^+$ tel que $|u_n| \leqslant M$. D'où, $|a_n| = |b_n| \times |u_n| \leqslant M\,|b_n|$. Donc, $R_a \geqslant R'$ où R' est le rayon de convergence de la série $\sum M b_n x^n = M \sum b_n x^n$. On en déduit que $R_a \geqslant R_b$.

3. Ainsi, $a_n = \mathcal{O}(b_n)$ et $b_n = \mathcal{O}(a_n)$, d'où d'après le cas précédent, $R_a \geqslant R_b$, et $R_b \geqslant R_a$. On en déduit que $R_a = R_b$.

□

EXERCICE : 1. On considère la série entière $\sum \mathrm{e}^{\cos n} x^n$. Or, pour tout $n \in \mathbb{N}$, $0 \leqslant \mathrm{e}^{-1} \leqslant a_n = \mathrm{e}^{\cos n} \leqslant \mathrm{e}^1$ car $-1 \leqslant \cos n \leqslant 1$ et exp est croissante. D'une part, $|a_n| \leqslant |\mathrm{e}^1|$, d'où R_a est supérieur ou égal au rayon de convergence de la série $\sum \mathrm{e}^1 x^n = \mathrm{e} \sum x^n$. D'où $R_a \geqslant 1$. D'autre part, $R_a \leqslant 1$ de même. On en déduit que $R_a = 1$.

2. On considère la série entière $\sum \frac{n!}{2^{2n}\sqrt{(2n)!}} x^n$, de terme général u_n.

   (a) MÉTHODE 1 (D'ALEMBERT).

$$\frac{|u_{n+1}|}{|u_n|} = |x| \times \frac{n+1}{4\sqrt{(2n+2)(2n+1)}} \xrightarrow[n\to\infty]{} \frac{1}{8}|x|.$$

   Alors, la série $\sum u_n$ diverge si $|x|/8 > 1$; et, la série $\sum u_n$ converge si $|x| < 1$, par le critère de D'ALEMBERT. On en déduit que $R = 8$.

   (b) MÉTHODE 2 (STIRLING)... à tenter

VII.2 Convergence normale et continuité

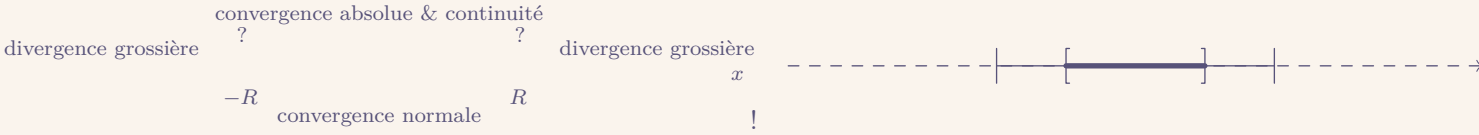


FIGURE 10.2 – Convergence normale d'une série entière

Théorème : 1. La série entière $\sum a_n x^n$ converge normalement (donc uniformément) sur tout segment inclus dans $]-R, R[$. Mais, la convergence normale étant une propriété globale, on ne peut pas « faire sauter la barrière. »

2. La somme $x \mapsto \sum_{n=0}^{\infty} a_n x^n$ est une fonction continue sur $]-R, R[$.

Théorème (ABEL radial) **:** Si la série numérique $\sum a_n R^n$ converge, alors

$$\sum_{n=0}^{\infty} a_n x^n \xrightarrow[x\to R^-]{} \sum_{n=0}^{\infty} a_n R^n.$$

VII.3 Intégrer

Théorème : Soit R le rayon de convergence d'une série entière.

1. Le rayon de convergence de la série entière $\sum \frac{a_n}{n+1}x^{n+1}$ est aussi égal à R.
2. $$\sum_{n=0}^{\infty} \frac{a_n}{n+1}x^{n+1} = \int_0^x \left(\sum_{n=0}^{\infty} a_n t^n\right) \mathrm{d}t.$$

« On peut intégrer terme à terme sans changer son rayon de convergence. »

Exemple :

Exercice :

VII.4 Dériver

Théorème : Avec les notations précédentes,

1. le rayon de convergence de la série entière $\sum n a_n x^{n-1}$ est aussi égal à R,
2. pour $x \in]-R, R[$,
$$\sum_{n=1}^{\infty} n a_n x^{n-1} = \frac{\mathrm{d}}{\mathrm{d}x} \sum_{n=0}^{\infty} a_n x^n,$$
3. la somme
$$\begin{aligned} f :]-R, R[&\longrightarrow \mathbb{R} \\ x &\longmapsto \sum_{n=0}^{\infty} a_n x^n \end{aligned}$$
est de classe $\mathscr{C}^\infty$, et $\forall n \in \mathbb{N}$, $a_n = \frac{f^{(n)}(0)}{n!}$.

« On peut dériver terme à terme sans changer son rayon de convergence. »

Exercice :
On considère la série entière $\sum \frac{n+5}{(n+2)(n+2)}x^n$. *Calculons son rayon de convergence.*

Idée : On intègre terme à terme la série entière $\sum x^n$, et on obtient la série entière $\sum \frac{x^{n+1}}{n+1}$. On ré-intègre la série : $\sum \frac{x^{n+2}}{(n+1)(n+2)}$. On multiplie par x^3, et on obtient la série entière $\sum \frac{x^{n+5}}{(n+1)(n+2)}$, que l'on peut dériver terme à terme pour obtenir la série entière $\sum \frac{n+5}{(n+1)(n+2)}x^{n+4}$. On divise [1] par x^4 pour

1. On suppose dans ce cas $x \neq 0$, et on s'occupera du cas $x = 0$ à part.

« Mieux vaut intégrer le plus tôt possible pour déterminer le rayon de convergence »

trouver la série demandée : $\sum \frac{(n+5)}{(n+1)(n+2)} x^n$. Cette méthode fonctionne car on peut intégrer/dériver sans changer son rayon de convergence. Le rayon de convergence de la série $\sum x^n$ est $R = 1$, donc le rayon de convergence de la série $\sum \frac{n+5}{(n+1)(n+2)} x^n$ est $R = 1$.

Rédaction : On a $\forall x \in]-1,1[$, $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$, d'où en intégrant, $\forall x \in]-1,1[$, $\sum_{n=0}^{\infty} \frac{x^{n+1}}{n+1} = \int_0^x \frac{1}{1-t}\,\mathrm{d}t = -\ln(1-x)$. D'où, en intégrant,

$$\begin{aligned}
\forall x \in]-1,1[, \quad \sum_{n=0}^{\infty} \frac{x^{n+2}}{(n+1)(n+2)} &= -\int_0^x 1 \times \ln(1-t)\,\mathrm{d}t \\
&= -\big[t\ln(1-t)\big] - \int_0^x \frac{t}{1-t}\,\mathrm{d}t \\
&= x\ln(1-x) - \int_0^x \left[-1 + \frac{1}{1-t}\right]\mathrm{d}t \\
&= -x\ln(1-x) - \big[-x - \ln(1-x)\big] \\
&= (1-x)\ln(1-x) + x.
\end{aligned}$$

De même pour les autres étapes du raisonnement.

Autre méthode : on a $\frac{n+5}{(n+1)(n+2)} \sim_{n\to\infty} \frac{1}{n}$ d'où, les séries entières $\sum \frac{(n+5)}{(n+1)(n+2)} x^n$, et $\sum \frac{x^n}{n}$ ont le même rayon de convergence, qui vaut $R = 1$. [2]

Exemple (séries entières & équations différentielles) : 1. On pose

$$\begin{aligned}
\exp : \mathbb{R} &\longrightarrow \mathbb{R} \\
x &\longmapsto \mathrm{e}^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.
\end{aligned}$$

En dérivant terme à terme, et on retrouve bien $x \mapsto \exp(x)$, et son rayon de convergence est le même. On a donc montré que exp est *une* solution de $y' = y$. De plus, la fonction $x \mapsto K\,\mathrm{e}^x$ est aussi une solution de cette équation différentielle. Montrons, avec la méthode de la variation de la constante, que ces fonctions sont les seules solutions de $y' = y$. On pose $y(x) = k(x)\mathrm{e}^k$, et on a

$$\begin{aligned}
y'(x) = y(x) &\iff k'(x)\mathrm{e}^x + \cancel{k(x)\mathrm{e}^x} = \cancel{k(x)\mathrm{e}^x} \\
&\iff k'(x)\,\mathrm{e}^x = 0 \\
&\iff k'(x) = 0 \\
&\iff \exists K \in \mathbb{R},\ k(x) = K.
\end{aligned}$$

D'où, la solution générale de l'équation $y' = y$ est : $\forall x \in \mathbb{R}$, $y(x) = K\mathrm{e}^x$.

2. Soit $\alpha \in \mathbb{R}$. On considère la série entière $\sum a_n x^n$ où

$$a_0 = 1 \quad \text{et} \quad a_n = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} \text{ si } n > 0.$$

2. Il s'agit de la série entière convergent vers $\ln(1-x)$.

Soit $(u_n)_{n\in\mathbb{N}}$ défini comme $u_n = |a_n x^n|$, et on calcule, si $\alpha \notin \mathbb{N}$,

$$\begin{aligned}\frac{u_{n+1}}{u_n} &= \left|\frac{a_{n+1}}{a_n} \times \frac{x^{n+1}}{x^n}\right| \\ &= |x| \times \left|\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)(\alpha-n)}{\alpha(\alpha-1)\cdots(\alpha-n+1)}\right| \times \frac{n!}{(n+1)!} \\ &= \frac{|\alpha-n|}{n+1}\,|x| \xrightarrow[n\to+\infty]{} |x|\end{aligned}$$

D'après le critère de D'ALEMBERT, si $|x| > 1$, alors la série diverge, et si $|x| < 1$, alors la série converge. On en déduit que $R = 1$. Soit, pour tout $x \in]-1,1[$, $f(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$. On peut dériver terme à terme sans changer le rayon de convergence. D'où

$$\forall x \in]-1,1[, \quad f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1} = \sum_{n=1}^{\infty} \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{(n-1)!} x^{n-1}.$$

Montrons que f est solution de l'équation $\alpha y - (1+x)y' = 0$:

$$\begin{aligned}\alpha\, f(x) - (1+x)\, f'(x) &= \alpha\Big(1 + \sum_{n=1}^{\infty} a_n x^n\Big) - (1+x)\sum_{n=1}^{\infty} n a_n x^{n-1} \\ &= \alpha + \sum_{n=1}^{\infty} x^n(\alpha a_n - n a_n) - \sum_{n=1}^{\infty} n a_n x^{n-1} \\ &= \alpha + \sum_{n=1}^{\infty} \big(x^n a_n(\alpha-n) - n a_n x^{n-1}\big) \\ &= 0\end{aligned}$$

En effet, $(n+1)a_{n+1} = (\alpha-n)a_n$, par construction de la suite $(a_n)_{n\in\mathbb{N}}$, et

$$\alpha + \sum_{n=1}^{N} \big(x^n(n+1)a_{n+1} - x^{n+1} n a_n\big) = \alpha - \alpha + x^N(N+1)a_{N+1} \xrightarrow[N\to\infty]{} 0.$$

D'où, f est solution de l'équation différentielle $\alpha y - (1+x)y' = 0$. Or, $x \mapsto K(1+x)^\alpha$ est une solution de cette équation différentielle. On fait varier la constante : on pose, pour $x \in]-1,1[$, $y(x) = k(x)\,(1+x)^\alpha$

$$\begin{aligned}&\alpha y(x) - (1+x)\, y'(x) - \alpha k(x)\,(1+x)^\alpha \\ &\quad - (1+x)\big(k'(x)(1+x)^\alpha + \alpha\, k(x)(1+x)^{\alpha-1}\big) = 0 \\ \iff &\forall x \in]-1,1[,\ (1+x)^{\alpha+1}k'(x) = 0 \\ \iff &\forall x \in]-1,1[, k'(x) = 0 \\ \iff &\exists K \in \mathbb{R},\ k(x) = K \\ \iff &\exists K \in \mathbb{R},\ \forall x \in]-1,1[, f(x) = K(1+x)^\alpha\end{aligned}$$

Or, $f(0) = 1$ et donc $K = 1$.

VII.5 (Ne pas) être développable en série entière

Définition : Soit $r \in \mathbb{R}_\star^+ \cup \{+\infty\}$. On dit qu'une fonction f est *développable en série entière* sur $]-r,r[$ s'il existe une série entière $\sum a_n x^n$ qui a un rayon de convergence $R \geqslant r$ telle que

$$\forall x \in]-r,r[, \quad f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Exemple :

Remarque :

Exercice :

Soit f : $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \mathrm{e}^{-1/x^2} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{array}$

1. Montrons que, pour $n \in \mathbb{N}$, f est $\mathscr{C}^n$ sur $\mathbb{R}^\star$, et il existe un polynôme P_n tel que $\forall x \neq 0$, $f^{(n)}(x) = P_n(x)\,\frac{1}{x^{3n}}\,\mathrm{e}^{-1/x^2}$.
   - Pour $n = 0$, alors $f^{(0)}(x) = \mathrm{e}^{-1/x^2} = \frac{1}{x^{3\times 0}} \times \mathrm{e}^{-1/x^2}$, d'où $P_0(X) = 1$.
   - On suppose $f^{(n)}(x) = \frac{P_n(x)}{x^{3n}}\mathrm{e}^{-1/x^2}$. D'où $f^{(n)}$ est de classe $\mathscr{C}^1$ et

$$\begin{aligned} f^{(n+1)}(x) &= \frac{\mathrm{d}}{\mathrm{d}x} f^{(n)}(x) \\ &= \frac{\mathrm{d}}{\mathrm{d}x}\left[P_n(x)x^{-3n}\mathrm{e}^{-1/x^2}\right] \\ &= \frac{\mathrm{d}}{\mathrm{d}x}\left[P_n(x)x^{-3n}\right] + P_n(x)x^{-3n} \times \frac{2}{x^3}\mathrm{e}^{-1/x^2} \\ &= \left(P_n'(x)x^{-3n} - 3nP_n(x)x^{-3n-1} + 2P_n(x)x^{-3n-3}\right)\mathrm{e}^{-1/x^2} \\ &= \frac{x^3P_n'(x) - 3nx^2P_n(x) + 2P_n(x)}{x^{3n+3}}\mathrm{e}^{-1/x^2} \\ &= \frac{P_{n+1}(x)}{x^{3(n+1)}}\mathrm{e}^{-1/x^2} \end{aligned}$$

2. Par récurrence :
   - $f^{(0)}(0) = f(0) = 0$ par définition, et $f(x) = \mathrm{e}^{-1/x^2} \xrightarrow[x\to 0]{} 0 = f(0)$, donc f est $\mathscr{C}^0$.
   - On suppose f $\mathscr{C}^n$ sur $\mathbb{R}$ et $f^{(n)}(0) = 0$. On sait que, $f^{(n)}$ est continue sur $\mathbb{R}$ par hypothèse, $f^{(n)}$ est dérivable sur $\mathbb{R}^\star$ car f est $\mathscr{C}^\infty$ d'après

la question 1. Et,

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}f^{(n)}(x) &= f^{(n+1)}(x)\\ &= \frac{P_{n+1}(x)}{x^{3n+3}}\mathrm{e}^{-1/x^2}\\ &\xrightarrow[x\to 0]{} 0 \text{ par croissances comparées.}\end{aligned}$$

3. f est $\mathscr{C}^\infty$ mais pas développable en série entière. Par l'absurde, si f est développable en série entière, alors $f(x)=\sum_{n=0}^{\infty} a_n x^n$ et $a_n = \frac{f^{(n)}(0)}{n!} = 0$, d'où $\forall x,\ f(x)=0$, ce qui est absurde.

Rappel (Théorème de la limite de la dérivée) :
Si f est continue sur $[a,b]$, dérivable sur $]a,b[$ et

1. $\lim_{x\to a^+} f'(x) = \ell \in \mathbb{R}$, alors f est dérivable en a et $f'(a)=\ell$.
2. $\lim_{x\to a^+} f'(x) = \pm\infty$, alors f n'est pas dérivable en a, et la courbe possède une tangente verticale.
3. $\lim_{x\to a^+} f'(x)$ n'existe pas, alors on ne peut pas conclure.

Proposition : Une fonction f est développable en série entière sur $]-r,r[$ si, et seulement si

1. f est $\mathscr{C}^\infty$ sur $]-r,r[$
2. $\forall x\in]-r,r[,\ R_N(x) \xrightarrow[N\to\infty]{} 0$ où $R_N(x) = f(x) - \sum_{n=0}^{N} \frac{f^{(n)}(0)}{n!}x^n$.

En effet, on a

$$f(x) = \sum_{n=0}^{N} \frac{f^{(n)}(0)}{n!}x^n + R_N(x),$$

ainsi $\sum_{n=0}^{N} f^n(0)/n! \xrightarrow[N\to\infty]{} f(x) \iff R_N(x) \xrightarrow[N\to\infty]{} 0$.

Rappel (Formules de Taylor) :
Formule de Taylor-Young : si f est de classe $\mathscr{C}^n$, alors

$$\begin{aligned}f(x) &= f(0) + o(1)\\ &= f(0) + x\,f'(0) + o(x)\\ &= f(0) + x\,f'(0) + \frac{x^2}{2!}\,f''(0) + o(x^2)\\ &= f(0) + x\,f'(0) + \frac{x^2}{2!}\,f''(0) + \cdots + \frac{x^n}{n!}\,f^{(n)}(0) + o(x^n)\end{aligned}$$

Formule de TAYLOR avec reste intégral[3] : si f est de classe $\mathscr{C}^{n+1}$, alors

$$\begin{aligned} f(x) &= f(0) + \int_0^x f'(t)\,\mathrm{d}t \\ &= f(0) + x\,f'(0) + \int_0^x (x-t)\,f''(t)\,\mathrm{d}t \\ &= f(0) + x\,f'(0) + \frac{x^2}{2!}\,f''(0) + \int_0^x \frac{(x-t)^2}{2!}\,f'''(t)\,\mathrm{d}t \\ &= f(0) + x\,f'(0) + \cdots + \frac{x^n}{n!}\,f^{(n)}(0) + \int_0^x \frac{(x-t)^n}{n!}\,f^{(n+1)}(t)\,\mathrm{d}t \end{aligned}$$

EXERCICE : 1. Montrons que, pour $x \in \mathbb{R}$, $\cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$. Pour $n \in \mathbb{N}$, $R_n(x) = \int_0^x \frac{(x-t)^n}{n!} \cos^{(n+1)}(t)\,\mathrm{d}t$ car cos est $\mathscr{C}^{n+1}$. Soit $x \in \mathbb{R}$. Montrons que $R_n(x) \xrightarrow[n\to\infty]{} 0$.

$$\begin{aligned} 0 \leqslant |R_n(x)| &= \left| \int_0^x \frac{(x-t)^n}{n!} \cos^{(n+1)}(t)\,\mathrm{d}t \right| \\ &\leqslant \left| \int_0^x \left| \frac{(x-t)^n}{n!} \cos^{(n+1)}(t) \right| \mathrm{d}t \right| \\ &\leqslant \left| \int_0^x \frac{|x-t|^n}{n!}\,\mathrm{d}t \right| \end{aligned}$$

car $|\cos^{(n+1)}(t)| \leqslant 1$, $\forall t \in [0,x]$. D'où,

$$0 \leqslant |R_n(x)| \leqslant \left| \int_0^x \frac{x^n}{n!}\,\mathrm{d}t \right| = \frac{|x|^{n+1}}{n!} \xrightarrow[n\to\infty]{} 0,$$

car on sait que la série $\sum \frac{x^n}{n!}$ converge, donc le terme général tend donc vers 0. Donc cos est développable en série entière sur $\mathbb{R}$.

2. De même pour sin.

VII.6 Produit de Cauchy et somme de deux séries entières

RAPPEL (produit de CAUCHY) :
On rappelle le produit de deux polynômes : on pose $A = \sum_{n=0}^{\deg A} a_n X^n$ et $B = \sum_{p=0}^{\deg B} b_p X^p$, le produit de ces deux polynômes est donc

$$\begin{aligned} A \times B &= \Big(\sum_{n=0}^{\deg A} a_n X^n \Big) \Big(\sum_{p=0}^{\deg B} b_p X^p \Big) \\ &= \sum_{k=0}^{\deg A + \deg B} c_k X^k \qquad \text{où } c_k = \sum_{n+p=k} a_n b_p. \end{aligned}$$

3. aussi appelé formule de TAYLOR-LAPLACE

On définit alors le *produit de* CAUCHY de deux séries : si $\sum u_n$ et $\sum v_n$ convergent absolument, alors $\sum w_n$ converge absolument, en posant $w_k = \sum_{n+p=k} u_n v_p$. De plus,

$$\sum_{k=0}^{\infty} w_k = \Big(\sum_{n=0}^{\infty} u_n\Big)\Big(\sum_{p=0}^{\infty} v_p\Big).$$

Proposition : 1. Soit $c_n = a_n + b_n$. Le rayon de convergence de la série $\sum c_n x^n$ vaut $R_c = \min(R_a, R_b)$ (ou plus sur $R_a = R_b$) et

$$\forall x \in]-R_c, R_c[, \quad \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n.$$

2. Si $\sum a_n x^n$ et $\sum b_n x^n$ ont respectivement pour rayons de convergence R_a et R_b, alors $\sum c_n x^n$ a pour rayon de convergence $R_c \geqslant \min(R_a, R_b)$, où $c_k = \sum_{n+p=k} a_n + b_p$, et

$$\forall x \in]-R_c, R_c[, \ \Big(\sum_{n=0}^{\infty} a_n x^n\Big)\Big(\sum_{p=0}^{\infty} b_p x^p\Big) = \sum_{k=0}^{\infty} c_k x^k$$

EXEMPLE : 1. La série $\sum x^n$ a pour rayon de convergence 1, et la série entière $1-x$ a pour rayon de convergence $+\infty$. Et, $\forall x \in]-1,1,[$, $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$. Le produit de CAUCHY des deux séries entières $\sum x^n = \sum a_k x^k$ et $1 - x = \sum b_\ell x^\ell$ est la série $\sum c_n x^n$, où

$$\begin{aligned} c_n &= \sum_{k+\ell=n} a_k b_\ell \\ &= \sum_{\ell=0}^{n} a_{n-\ell} b_\ell \end{aligned}$$

D'où, $c_0 = 1$, $c_1 = 1 - 1 = 0$ et $\forall n \geqslant 2$, $c_n = 0$. Donc $\sum c_n x^n = 1$, qui a pour rayon de convergence $+\infty \neq \min(R_a, R_b)$. On retrouve ce résultat car

$$\underbrace{\frac{1}{1-x}}_{\sum_{n=0}^{\infty} x^n} \times (1-x) = 1.$$

2. (tarte à la crème) La série entière $\sum H_n x^n$,[4] est le produit de CAUCHY des deux séries entières $\sum \frac{x^n}{n}$ et $\sum x^n$. En effet,

$$c_n x^n = \sum_{k+\ell=n} \frac{x^k}{k} x^\ell = \sum_{k=1}^{n} \frac{1}{k} x^n = H_n x^n.$$

4. où $H_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}$.

Or, $R_c \geqslant \min(R_a, R_b) = \min(1,1) = 1$. D'où,

$$\forall x \in]-1,1[, \Big(\sum_{n=1}^{\infty} \frac{x^n}{n}\Big)\Big(\sum_{n=0}^{\infty} x^n\Big) = \sum_{n=1}^{\infty} H_n x^n$$

et donc

$$-\ln(1-x) \times \frac{1}{1-x} = \sum_{n=1}^{\infty} H_n x^n.$$

EXERCICE (tarte à la crème) :
Soient $x, y \in \mathbb{R}$. Montrer que $\mathrm{e}^x \cdot \mathrm{e}^y = \mathrm{e}^{x+y}$. On sait que $\mathrm{e}^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. On veut montrer que $\big(\sum_{n=0}^{\infty} \frac{x^n}{n!}\big)\big(\sum_{n=0}^{\infty} \frac{x^n}{n!}\big) = \sum_{n=0}^{\infty} \frac{(x+y)^k}{k!}$. Le rayon de convergence de la série exp est $+\infty$, le rayon de convergence du produit de CAUCHY de deux séries exp est supérieur à $\min(+\infty, +\infty)$, *i.e.* il faut $+\infty$. Le produit de CAUCHY de ces deux séries est la série $\sum w_k$ avec

$$\begin{aligned} w_k = \sum_{n+p=k} u_n v_p = \sum_{n+p=k} \frac{x^n}{n!}\frac{y^p}{p!} &= \sum_{n=0}^{k} \frac{x^n\, y^{k-n}}{n!\,(k-n)!} \\ &= \frac{1}{k!}\sum_{n=0}^{k} \frac{k!}{n!\,(n-k)!} x^n y^{n-k} \\ &= \frac{1}{k!}(x+y)^k \end{aligned}$$

VII.7 Séries entières complexes

EXERCICE :
Montrer que, pour tout $\theta \in \mathbb{R}$,

$$\mathrm{e}^{i\theta} = \cos\theta + i\sin\theta.$$

On a $\forall z \in \mathbb{C}$, $\mathrm{e}^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$. En particulier, si $z = i\theta$, on a

$$\mathrm{e}^{i\theta} = \sum_{n=0}^{\infty} \frac{(i\theta)^n}{n!} = \sum_{n=0}^{\infty} (-1)^n \frac{\theta^{2n}}{(2n)!} + i\sum_{n=0}^{\infty} (-1)^{2n+1} \frac{\theta^{2n+1}}{(2n+1)!} = \cos\theta + i\sin\theta.$$

Chapitre 11

Variables aléatoires

VII.1 Variables aléatoires discrètes

Définition : 1. Soit $(\Omega, \mathscr{A})$ un espace probabilisable. Une *variable aléatoire discrète* (*vad*) est une fonction X définie sur l'unitvers Ω telle que

(a) l'ensemble $X(\Omega)$ des valeurs prises par X est fini ou dénombrable ;

(b) pour chaque valeur $a \in X(\Omega)$ prise par X, l'ensemble $X^{-1}(\{a\})$ est un événement, noté $(X = a)$. Autrement dit,

$$\forall a \in X(\Omega), (X = a) = X^{-1}(\{a\}) \in \mathscr{A}.$$

2. Soient $(\Omega, \mathscr{A}, P)$ un espace probabilisé, et X une variable aléatoire discrète. La *loi de probabilité* de X est la fonction

$$\begin{aligned} X(\Omega) &\longrightarrow [0,1] \\ a &\longmapsto P(X = a). \end{aligned}$$

Rappel :
Soit $f : E \to F$ une fonction. On a

$$\forall A \in \wp(E),\ f(A) = \{y \in F \mid \exists x \in A,\ y = f(x)\},$$

et

$$\forall B \in \wp(F),\ f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

Ainsi, $x \in f^{-1}(B) \iff f(x) \in B$.

Exercice :
L'univers Ω, ensemble des résultats, est $[\![1,6]\!]^2$. Soit X la variable aléatoire, qui

est la somme des deux dés : on a

$$\begin{aligned} X : \Omega &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto x + y. \end{aligned}$$

Ainsi, $X(\Omega) = [\![2, 12]\!]$.

a	2	3	4	5	6	7	8	9	10	11	12
$P(X = a)$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

TABLE 11.1 – Loi de probabilité de X

REMARQUE : 1. On a $f^{-1}\Big(\bigcup_{i\in I} A_i\Big) = \bigcup_{i\in I} f^{-1}(A_i)$, et $f^{-1}\Big(\bigcap_{i\in I} A_i\Big) = \bigcap_{i\in I} f^{-1}(A_i)$.

EXEMPLE :
c.f. polycopié

Proposition–Définition : Soient $(\Omega, \mathcal{A}, P)$ un espace probabilisé, et une *vad* $X : \Omega \to E$ à valeurs dans un ensemble E.

1. Pour tout $A \in \wp(E)$, $X^{-1}(A) \in \mathcal{A}$ est un événement noté $(X \in A)$.
2. L'application

$$\begin{aligned} P_X : \wp(E) &\longrightarrow A \\ A &\longmapsto P(X \in A) \end{aligned}$$

est une probabilité sur l'espace probabilisable $\big(E, \wp(E)\big)$.

EXERCICE (tarte à la crème) :
L'univers Ω est défini comme $\Omega = [\![1, N]\!]^n$: c'est l'ensemble des n-uplets de $[\![1, N]\!]$. La variable X est la fonction définie comme

$$\begin{aligned} X : \Omega &\longrightarrow [\![1, N]\!] \\ (x_1, \dots, x_n) &\longmapsto \max_{i\in[\![1,n]\!]} x_i. \end{aligned}$$

On cherche la loi de probabilité de X. ATTENTION, on ne cherche pas $P(X = a)$ pour tout a, mais $P(X \leqslant a)$ pour tout a. Cela correspond à l'événement « tous les numérons tirés sont inférieurs à a. » Par équiprobabilité,

$$\begin{aligned} P(X \leqslant a) &= \frac{\mathrm{Card}(X \leqslant a)}{\mathrm{Card}(\Omega)} \\ &= \frac{a^n}{N^n} \end{aligned}$$

Finalemement, pour tout $a \in [\![1, N]\!]$, $P(X = a) + P(X \leqslant a - 1) = P(X \leqslant a)$; en effet, $(X \leqslant a - 1) \cup (X = a) = (X \leqslant a)$, et cette union est disjointe. D'où,

$\forall a \in [\![1, N]\!]$,

$$\begin{aligned} P(X = a) &= P(X \leqslant a) - P(X \leqslant a - 1) \\ &= \left(\frac{a}{N}\right)^n - \left(\frac{a-1}{N}\right)^n \end{aligned}$$

VII.2 La loi binomiale

Définition : Soient $n \in \mathbb{N}^\star$, $p \in]0, 1[$, et $q = 1-p$. On dit qu'une variable aléatoire discrète X suit une *loi de binomiale* de paramètres (n, p), et on note $X \sim \mathcal{B}(n, p)$ si

$$X(\Omega) = [\![1, n]\!], \quad \text{et} \quad \forall k \in X(\Omega),\ P(X = k) = \binom{n}{k} \cdot p^k \cdot q^{n-k}.$$

Une *épreuve de Bernoulli* de paramètre $p \in]0, 1[$ est une expérience aléatoire qui peut donner deux résultats : un « succès » S avec une probabilité p, ou un « échec » E avec la probabilité $q = 1 - p$.

Proposition : Soient $n \in \mathbb{N}^\star$ et $p \in]0, 1[$. Soit X la *vad* égale au nombre de succès parmi n épreuves de Bernoulli de paramètre p. Si ces épreuves sont indépendantes, alors $X \sim \mathcal{B}(n, p)$.

Preuve :
L'ensemble $(X = k)$ est l'événement « obtenir k succès parmi n essais. » Autrement dit, c'est l'ensemble des n-listes $(x_1, x_2, \ldots, x_n)$ dont le nombre de succès vaut k, et chaque $x_i \in \{S, E\}$. Réaliser cet événement, c'est (1) placer k succès parmi les n essais, et il y en a $\binom{n}{k}$ manières ; (2) placer les $n-k$ échecs, il y a 1 manière. Il y a donc $\binom{n}{k}$ listes favorables. La prboabilité de chacune de ces listes est $p^k \times q^{n-k}$ par indépendance. □

Exemple :
c.f. polycopié

Exercice :
On a $X \sim \mathcal{B}(n, p)$. Ainsi, d'après la définition 7, $X(\Omega) = [\![1, n]\!]$, et $\forall k \in X(\Omega)$, $P(X = k) = \binom{n}{k} p^k q^{n-k}$. *Montrons que* $n - X \sim \mathcal{B}(n, q)$ avec $q = 1 - p$. On veut

donc montrer que $\forall k \in (n-X)(\Omega)$, $P(n-X=k) = \binom{n}{k} \cdot q^k \cdot p^{n-k}$.

$$\begin{aligned} P(X = n-k) &= \binom{n}{n-k} p^{n-k} q^{n-(n-k)} \\ &= \binom{n}{n-k} q^k p^{n-k} \\ &= \binom{n}{k} q^k p^{n-k} \quad \text{par symétrie des coefficients binomiaux.} \end{aligned}$$

On peut également remarquer que la variable aléatoire $n - X$ est le nombre d'echecs.

VII.3 La loi géométrique

Définition : Soit $p \in]0,1[$. On pose $q = 1-p$. On dit qu'une *vad* T suit une *loi géométrique* de paramètre p, et on note $T \sim \mathcal{G}(p)$ si

$$T(\Omega) = \mathbb{N}^\star \quad \text{et} \quad \forall k \in T(\Omega),\ P(T=k) = p \cdot q^{k-1}.$$

On vérifie bien que $\sum_{k\in\mathbb{N}^\star} P(X=k) = 1$. En effet, elle vaut

$$\begin{aligned} \sum_{k\in\mathbb{N}^\star} pq^{k-1} &= p\sum_{k=1}^{\infty} q^{k-1} \\ &= p\sum_{k=0}^{\infty} q^k \\ &= p \times \frac{1}{1-q} \\ &= \frac{1-q}{1-q} = 1 \end{aligned}$$

Proposition : Soit $p \in]0,1[$. Soit T la *vad* égale au temps d'attente du 1$^{\underline{\text{er}}}$ succès lors d'une suite d'épreuve de Bernoulli de paramètre p. Si ces épreuves sont indépendantes, alors $T \sim \mathcal{G}(p)$.

Preuve :
L'événement $(X=k)$ vaut $E_1 \cap E_2 \cap \cdots \cap E_{k-1} \cap S_k$, où S_i est l'événement « obtenir un succès au i-ème essai, » et E_i est l'événement « obtenir un échec au i-ème essai. [1] » Par hypothèse d'indépendance, on a

$$P(E_1 \cap E_2 \cap \cdots \cap E_{k-1} \cap S_k) = P(E_1) \times P(E_2) \times \cdots \times P(E_{k-1}) \times P(S_k).$$

□

Exercice (« Remettre le compteur à zéro ») :
Soit X une vad *à valeurs dans $\mathbb{N}^\star$ telle que*

$$\forall k \in \mathbb{N},\ P(X > k) > 0.$$

On dit que X est sans mémoire si

$$\forall k \in \mathbb{N},\ \forall n \in \mathbb{N},\quad P(X > n+k \mid X > k) = P(X > n).$$

On veut montrer que la loi géométrique est une loi sans mémoire, et que c'est la seule.

1. *Montrer que, X est sans mémoire*
   (a) *si, et seulement si $\forall k \in \mathbb{N},\ \forall n \in \mathbb{N},\ P(X > n+k) = P(X > n) \cdot P(X > k)$.*
   (b) *si, et seulement si $\forall k \in \mathbb{N},\ \forall n \in \mathbb{N},\ P(X = n+k \mid X > k) = P(X = n)$.*
2. *On suppose que X suit une loi géométrique de paramètre $p \in]0,1[$.*
   (a) *Calculer la probabilité $P(X > k)$ pour chaque $k \in \mathbb{N}$.*
   (b) *Montrer que X est sans mémoire.*
3. *Réciproquement, montrer que si X est sans mémoire, alors X suit une loi géométrique.*

1. (a)

$$\begin{aligned} X \text{ est sans mémoire} &\overset{\text{def.}}{\iff} \forall k,\ \forall n,\ P_{(X>k)}(X > n+k) = P(X > n) \\ &\iff P(X > n+k) = P(X > n) \cdot P(X > k) \end{aligned}$$

car

$$P(X > n+k \mid X > k) = \frac{P\big((X > n+k) \cap (X > k)\big)}{P(X > k)} = \frac{P(X > n+k)}{P(X > k)}$$

comme $\big((X > n+k) \cap (X > k)\big) = (X > n+k)$ (par inclusion).

(b) On a $(X > n+k-1) = (X = n+k) \cup (X > n+k)$ et cette union est disjointe, d'où

$$P_{(X>k)}(X > n+k-1) = P_{(X>k)}(X = n+k) + P_{(X>k)}(X > n+k).$$

D'où,

$$\begin{aligned} P_{(X>k)}(X = n+k) &= P_{(X>k)}(X > n+k-1) - P(X > n+k) \\ &= P(X > n-1) - P(X > n) \text{ par définition} \\ &= P(X = n) \text{ de même.} \end{aligned}$$

Réciproque à faire.

1. Ainsi, on a $S_i = \bar{E}_i$.

2. On suppose $X \sim \mathcal{G}(p)$. Ainsi, $X(\Omega) = \mathbb{N}^\star$ et $\forall k \in X(\Omega)$, $P(X = k) = p \times q^{k-1}$.
   (a) On a $(X > k) = \bigcup_{\ell=k+1}^{\infty}(X = \ell)$, et cette union est disjointe. D'où,

$$\begin{aligned} P(X > k) &= \sum_{\ell=k+1}^{\infty} P(X = \ell) \\ &= \sum_{\ell=k+1}^{\infty} p \times q^{\ell-1} \\ &= p \times q^k \sum_{\ell=0}^{\infty} q^\ell \\ &= p \times q^k \times \frac{1}{1-q} \text{ car } |q| < 1 \\ &= q^k \end{aligned}$$

   On en déduit que

$$\forall k \in \mathbb{N},\ P(X > k) = q^k.$$

   (b) On utilise le 1.(a) et la question précédente :

$$P(X > n + k) = q^{n+k} = q^n \cdot q^k = P(X > n) \cdot P(X > k).$$

3. On suppose X sans mémoire. On utilise 1.(a) :

$$\forall k,\ \forall n,\ P(X > n + k) = P(X > n) \cdot P(X > k).$$

   On cherche une relation de récurrence, on pose donc $k = 1$. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_n = P(X > n)$. Ainsi,

$$u_{n+1} = u_n \cdot \underbrace{P(X > 1)}_{\heartsuit}.$$

   D'où, par récurrence, $\forall n \in \mathbb{N}$, $u_n = \heartsuit^n \cdot u_0$, et $u_0 = P(X > 0) = 1$ comme $(X > 0) = \Omega$. Ainsi,

$$\forall n \in \mathbb{N},\ u_n = \heartsuit^n = P(X > n).$$

   On a, pour $n \in \mathbb{N}^\star$, $(X > n-1) = (X = 1) \cup (X > n) = (X = n) \cup P(X > n)$, et cette union est disjointe. D'où, $\heartsuit^{n-1} = P(X = n)/\heartsuit^{n-1} - \heartsuit^n$.

VII.4 La loi de Poisson

Définition : Soit un réel $\lambda > 0$. On dit qu'une variable aléaroire discrète X suit *une loi de Poisson* de paramètre λ, et on note $X \sim \mathcal{P}(\lambda)$ si

$$X(\Omega) = \mathbb{N} \quad \text{et} \quad \forall k \in X(\Omega),\ P(X = k) = \mathrm{e}^{-\lambda} \cdot \frac{\lambda^k}{k!}.$$

On vérifie que $\sum_{k\in X(\Omega)} P(X=k) = 1$. En effet,

$$\begin{aligned}\sum_{k\in X(\Omega)} P(X=k) &= \sum_{k=0}^{\infty} \mathrm{e}^{-\lambda}\frac{\lambda^k}{k!}\\ &= \mathrm{e}^{-\lambda}\sum_{k=0}^{\infty}\frac{\lambda^k}{k!}\\ &= \mathrm{e}^{-\lambda}\cdot\mathrm{e}^{\lambda} = 1\end{aligned}$$

Proposition : Soit un réel $\lambda > 0$, et pour $n \in \mathbb{N}^\star$, soit X_n une variable aléatoire suivant la loi binomiale $\mathcal{B}(n, p_n)$ avec $p_n \in]0,1[$. Si $n\cdot p_n \xrightarrow[n\to\infty]{} \lambda$, alors

$$\forall k \in \mathbb{N},\ P(X_n = k) \xrightarrow[n\to\infty]{} \mathrm{e}^{-\lambda}\cdot\frac{\lambda^k}{k!}.$$

Preuve :
On pose, $q_n = 1 - p_n$. On a

$$\binom{n}{k} p_n^k\,(1-p_n)^{n-k} = \frac{n!}{k!\cdot(n-k)!}\cdot p_n^k\cdot(1-p_n)^{n-k}..$$

Or,

$$\begin{aligned}p_n^k\cdot\frac{n!}{(n-k)!} &= p_n^k\cdot n\times(n-1)\times\cdots\times(n-k+1)\\ &= p_n^k\cdot n\times n\left(1-\frac{1}{n}\right)\cdots n\left(1-\frac{k-1}{n}\right)\\ &= (p_n n)^k\cdot\underbrace{\left(1-\frac{1}{k}\right)\times\cdots\times\left(1-\frac{k-1}{n}\right)}_{\xrightarrow[n\to\infty]{}1}\\ &\to \lambda^k.\end{aligned}$$

De plus, $(1-p_n)^{n-k} = \mathrm{e}^{(n-k)\ln(1-p_n)}$, et

$$\begin{aligned}(n-k)\ln(1-p_n) &= (n-k)\big(-p_n + \mathrm{o}(p_n)\big)\\ &= -np_n + \mathrm{o}(np_n)\\ &\to -\lambda.\end{aligned}$$

Par continuité de l'exponentielle, on a $(1-p_n)^{n-k} \xrightarrow[n\to\infty]{} \mathrm{e}^{-\lambda}$. Ainsi,

$$\forall k \in \mathbb{N},\ P(X_n = k) \xrightarrow[n\to\infty]{} \mathrm{e}^{-\lambda}\cdot\frac{\lambda^k}{k!}.$$

□

REMARQUE :
c.f. polycopié

VII.5 Espérance

Définition : Soient $(\Omega, \mathcal{A}, P)$ un espace probabilisé, et X une variable aléatoire réelle discrète (*vard*) telle que $X(\Omega) = \{a_i \mid i \in I\} \subset \mathbb{R}$. Si la série $\sum a_i\, P(X = a_i)$ converge absolument [2], alors

1. on dit que X est *d'espérance finie* ou que X *possède une espérance*, ou que $X \in L^1$;
2. cette *espérance*, notée $\mathrm{E}(X)$ est le nombre réel

$$\mathrm{E}(X) = \sum_{i \in I} a_i\, P(X = a_i).$$

REMARQUE : 1. La valeur de l'espérance ne dépend pas de l'ordre des valeurs a_i, c'est pour cela que l'on demande la convergence absolue.

2. Une *vard* peut ne pas avoir une espérance finie, par exemple $p_n = \frac{6}{\pi^2\, n^2}$. On a bien $\sum_{n=1}^{\infty} p_n = 1$ mais la série $\sum n\, p_n$ diverge.
3. Si $X(\Omega)$ est fini, alors X est nécessairement d'espérance finie, car $\mathrm{E}(X)$ est une somme finie.
4. Si X est bornée [3](vue comme une fonction), alors X est d'espérance finie.

   Preuve :
   En effet, $\forall a \in X(\Omega)$, $0 \leqslant |a\, P(X = a)| \leqslant M\, P(X = a)$ d'où la série $\sum |a\, P(X = a)|$ converge, car $\sum M\, P(X = a) = M \sum P(X = a)$ et $\sum P(X = a)$ converge. □
5. L'espérance est linéaire : si X est un *vard* d'espérance finie, alors $\alpha X + \beta$ aussi, et
   $$\mathrm{E}(\alpha X + \beta) = \alpha\, \mathrm{E}(X) + \beta.$$
   De plus, l'application
   $$\begin{aligned} \mathrm{E} : \text{ensemble des } \textit{vard} &\longrightarrow \mathbb{R} \\ X &\longmapsto \mathrm{E}(X) \end{aligned}$$
   est une forme linéaire.
6. Si X est d'espérance finie, alors $|X|$ aussi, et $\big|\mathrm{E}(X)\big| \leqslant \mathrm{E}\big(|X|\big)$ (par inégalité triangulaire). En particulier, si X est positive, alors son espérance est positive.

EXERCICE :
Montrer que

2. Ainsi, la série devient une famille sommable, et la somme devient commutative, même si elle est infinie.
3. *i.e.* $\exists M \in \mathbb{R}^+$, $\forall \omega \in \Omega$ $|X(\omega)| \leqslant M$.

1. *si $X \sim \mathcal{B}(n,p)$, alors X est d'espérance finie, et $\mathrm{E}(X) = n \cdot p$. Indication, utiliser la formule*
$$\forall k \in \mathbb{N}^\star,\ \forall n \geqslant k,\ k\binom{n}{k} = n\binom{n-1}{k-1}.$$
2. *si $T \sim \mathcal{G}(p)$, alors T est d'espérance finie, et $\mathrm{E}(T) = \frac{1}{p}$.*
3. *si $X \sim \mathcal{P}(\lambda)$, alors X est d'espérance finie, et $\mathrm{E}(X) = \lambda$.*

1. La variable aléatoire X représente le nombre de succès, de n épreuves de Bernoulli indépendantes, et la probabilité d'un succès est p. De plus, on a $X(\Omega) = [\![0,n]\!]$, qui est un ensemble fini, il possède une espérance. On calcule
$$\begin{aligned}
\mathrm{E}(X) &= \sum_{k=0}^{n} k\,P(X=k) & &= n\sum_{k=1}^{n}\binom{n-1}{k-1}p^k\,q^{n-k}\\
&= \sum_{k=0}^{n} k\binom{n}{k}p^k\,q^{n-k} & &= n\sum_{k=0}^{n-1}\binom{n-1}{k}p^{k+1}\,q^{n-k-1}\\
&= \sum_{k=1}^{n} k\binom{n}{k}p^k\,q^{n-k} & &= n\,p\sum_{k=0}^{n-1}\binom{n-1}{k}p^k\,q^{(n-1)-k}\\
&= \sum_{k=1}^{n} n\binom{n-1}{k-1}p^k\,q^{n-k} & &= n\,p\,(n+p)^{n-1}\\
& & &= n\,p.
\end{aligned}$$

2. La variable T correspond au temps d'attente du 1er succès, sachant que la probabilité d'un succès est p. Ainsi, $T(\Omega) = \mathbb{N}^\star$, et $\forall x \in T(\Omega)$, $P(T=k) = p\cdot q^{k-1}$. La variable aléatoire est d'espérance finie car la série $\sum k\,P(T=k)$ converge absolument :
$$\big|k\,P(T=k)\big| = k\,P(T=k) = k\,p\,q^{k-1}.$$
D'où $\sum |k\,P(T=k)| = \sum k\,p\,q^{k-1} = p\sum k\,q^{k-1}$. Or, la série entière $\sum x^k$ a pour rayon de converge 1. Et, on peut dériver terme à terme une série entière sans changer son rayon de convergence. D'où, le rayon de convergence de $\sum k\,x^{k-1}$ est aussi égal à 1. Or, $q \in\ ]-1,1[$, d'où la série $\sum k\,q^{k-1}$ converge.

De plus,
$$\forall x \in\ ]-1,1[,\quad \sum_{k=0}^{\infty} x^k = \frac{1}{1-x}.$$
Et, on peut dériver terme à terme une série entière sans changer son rayon de convergence. D'où,
$$\forall x \in\ ]-1,1[,\quad \sum_{k=1}^{\infty} kx^{k-1} = \frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{1-x} = \frac{1}{(1-x)^2}.$$

D'où,
$$\mathrm{E}(T) = \sum_{k=1}^{\infty} k\,P(T=k) = p \times \frac{1}{(1-q)^2} = \frac{1}{1-q} = \frac{1}{p}.$$

3. On a $X(\Omega) = \mathbb{N}$, et $\forall k \in X(\Omega)$, $P(X=k) = \mathrm{e}^{-k}\,\frac{\lambda^k}{k!}$. La *vard* X possède une espérance car la série $\sum k\,P(X=k)$ converge absolument. En effet, $\sum \left|k\,\mathrm{e}^{-\lambda}\frac{\lambda^k}{k!}\right| = \lambda \mathrm{e}^{-\lambda}\sum k\frac{\lambda^{k-1}}{k!}$. Or, la série entière $\sum x^{\frac{k}{k!}}$ a pour rayon de converge $+\infty$. Et, on peut dériver terme à terme une série entière sans changer son rayon de convergence. D'où, le rayon de convergence de $\sum k\,\frac{x^{k-1}}{k!}$ est aussi égal à $+\infty$. De plus,

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{k\in X(\Omega)} k\,P(X=k) & &= \mathrm{e}^{-\lambda}\,\lambda \sum_{k=1}^{\infty} k\,\frac{\lambda^{k-1}}{k!}\\
&= \sum_{k=0}^{\infty} k\,\mathrm{e}^{-\lambda}\,\frac{\lambda^k}{k!} & &= \lambda\,\mathrm{e}^{-\lambda}\sum_{k=0}^{\infty}\frac{\lambda^k}{k!}\\
&= \sum_{k=1}^{\infty} k\,\mathrm{e}^{-\lambda}\,\frac{\lambda^k}{k!} & &= \lambda\,\mathrm{e}^{-\lambda}\,\mathrm{e}^{\lambda} = \lambda
\end{aligned}$$

Proposition (version non rigoureuse) **:**

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{k=0}^{\infty} k\,P(X=k)\\
&= 0\times P(X=0) + 1\times P(X=1) + 2\times P(X=2) + 3\times P(X=3) + \cdots\\
&= \quad P(X=1)\\
&\quad + P(X=2) + P(X=2)\\
&\quad + P(X=3) + P(X=3) + P(X=3)\\
&\quad + \quad \vdots \quad + \quad \vdots \quad + \quad \vdots \quad + \quad \ddots\\
&= \quad P(X\geqslant 1) + P(X\geqslant 2) + P(X\geqslant 3) + \quad \cdots
\end{aligned}$$

Les hypothèse de ce théorème sont

la variable X est d'espérance finie.

— la série $\sum P(X\geqslant n)$ converge (c'est donc une famille sommable, car $P(X\geqslant n)\geqslant 0$).

Ainsi, on peut sommer par paquets.

Remarque :
Si X est une *vard* est $\varphi : X(\Omega) \to \mathbb{R}$, alors

1. $\varphi \circ X$ est aussi une *vard* notée $\varphi(X)$;

2. on pose $(\varphi \circ X)(\Omega) = \{b_j \mid j \in J\}$. Si $\varphi(X)$ possède une espérance $\mathrm{E}\big(\varphi(X)\big)$, alors cette espérance est égale à

$$\sum_{j\in J} b_j \, P\big(\varphi(X) = b_j\big)$$

par définition de l'espérance, mais aussi à

$$\sum_{i\in I} \varphi(a_i) \, P(X = a_i),$$

d'après le théorème suivant, que nous admettrons.

Théorème : Soient $\Omega, \mathscr{A}, P$ un espace probabilisé, X une *vard*, et $\varphi : X(\Omega) \to \mathbb{R}$. On pose $X(\Omega) = \{a_i \mid i \in I\}$. Alors, $\varphi(X)$ est d'espérance finie si, et seulement si la série $\sum \varphi(a_i)\, P(X = a_i)$ converge absolument. Et, alors, $\mathrm{E}(\varphi(X))$ vaut la somme $\sum_{i\in I} \varphi(a_i)\, P(X = a_i)$ de cette série.

VII.6 Variance et écart-type

Plus tard (définition 25), on définira respectivement la *variance* et l'*écart-type* comme

$$\mathrm{V}(X) = \mathrm{E}\Big(\big[X - E(X)\big]^2\Big) \qquad \sigma(X) = \sqrt{\mathrm{V}(X)}.$$

Définition : On définit le *moment d'ordre* $k \in \mathbb{N}$ comme

$$\sum_{a\in X(\Omega)} a^k \, P(X = a).$$

On dit qu'une variable aléatoire *possède un moment d'ordre* k si la série $\sum {a_n}^k P(X = a_n)$ converge absolument.

Ainsi, le moment d'ordre 1 est $\mathrm{E}(X)$, le moment d'ordre 2 est $\mathrm{E}(X^2)$, le moment d'ordre 3 est $\mathrm{E}(X^3)$, etc.

Lemme : Si une *vard* possède un moment d'ordre $k+1$, alors elle possède aussi un moment d'ordre k.

Preuve :
Pour tout réel, $x \geqslant 0$, alors $0 \leqslant x^k \leqslant x^{k+1} + 1$ (distinguer le cas $x \geqslant 1$ et $x < 1$). Ainsi, en multipliant par $P(X = a)$, on a

$$x^k \, P(X = a) \leqslant x^{k+1} \, P(X = a) + P(X = a).$$

La série $\sum P(X = a)$ converge absolument, et la série $\sum a^{k+1} \, P(X =$

a) converge absolument aussi. Alors, la série $\sum a^k\, P(X = a)$ converge absolument. □

Proposition–Définition : Soit $(\Omega, \mathscr{A}, P)$ un espace probabilisé, et soit X une *vard*. Si X^2 est d'espérance finie, alors X aussi, et on appelle *variance* le réel positif

$$\mathrm{V}(X) = \mathrm{E}\Big(\big[X - \mathrm{E}(X)\big]^2\Big) = \underbrace{\mathrm{E}(X^2) - \big(\mathrm{E}(X)\big)^2}_{\text{Relation de König \& Huygens}} \geqslant 0.$$

L'*écart-type* $\sigma(X)$ est la racine carrée de la variance :

$$\sigma(X) = \sqrt{\mathrm{V}(X)}.$$

Preuve :
On pose $\mu = \mathrm{E}(X)$, et on a $[X - \mu]^2 = X^2 - 2\mu X + \mu^2$. D'où, par linéarité de l'espérance,

$$\begin{aligned}\mathrm{E}\big((X-\mu)^2\big) &= \mathrm{E}(X^2 - 2\mu X + \mu^2)\\ &= \mathrm{E}(X^2) - 2\mu\mathrm{E}(X) + \mu^2\\ &= \mathrm{E}(X^2) - 2\mu^2 + \mu^2\\ &= \mathrm{E}(X^2) - \big(\mathrm{E}(X)\big)^2.\end{aligned}$$

De plus, d'après le lemme précédent, si X^2 est d'espérance finie, alors X est d'espérance finie. □

Remarque : 1. La variance mesure la *dispersion*, ou l'*étalement* des valeurs a_i autour de l'espérance $\mathrm{E}(X)$. En particulier, s'il existe $a \in \mathbb{R}$ tel que $P(X = a) = 1$, alors $\mathrm{E}(X) = a$ et $\mathrm{V}(X) = 0$. (C'est même une équivalence.)

2. Si la variable X a une unité (km/s, V/m, etc.), alors l'écart type a la même unité (d'où l'intérêt de calculer la racine carrée de la variance).
3. Soient α et β deux réels. Si X^2 est d'espérance finie, alors

$$\mathrm{V}(\alpha X + \beta) = \alpha^2 \cdot \mathrm{V}(X).$$

(Une translation ne change pas la dispersion des valeurs, et multiplier par un réel multiplie l'espérance, mais aussi la dispersion, d'où le carré.)

Exercice :
Montrer que

1. *si* $X \sim \mathscr{B}(n,p)$, *alors* X^2 *est d'espérance finie et* $\mathrm{V}(X) = n \cdot p \cdot q$.
2. *si* $T \sim \mathscr{G}(p)$, *alors* T^2 *est d'espérance finie et* $\mathrm{V}(T) = \frac{q}{p^2}$.

3. si $X \sim \mathcal{P}(\lambda)$, alors X^2 est d'espérance finie et $\mathrm{V}(X) = \lambda$.

1. Si $X \sim \mathcal{B}(n,p)$, alors $X(\Omega) = [\![0,n]\!]$ et, pour $k \in X(\Omega)$, $P(X=k) = \binom{n}{k} p^k\, q^{n-k}$. On a déjà montré que $\mathrm{E}(X) = n \cdot p$. On va montrer que $\mathrm{V}(X) = n\,p\,q$. La variable aléatoire X^2 est d'espérance finie car $X(\Omega)$ est fini. Et,

$$\begin{aligned}\mathrm{E}(X^2) &= \sum_{k=0}^{n} k^2\, P(X=k)\\ &= \sum_{k=0}^{n} k^2 \binom{n}{p} p^k q^{n-k}\\ &= \dots\end{aligned}$$

En effet, d'après la "petite formule," on a

$$\forall k \geqslant 1, \quad k\binom{n}{k} = n\binom{n-1}{k-1}$$

d'où, $\binom{(k-1)\binom{n-1}{k-1}=(n-1)}{\binom{n-2}{k-2}}$. Ainsi,

$$\forall k \geqslant 2, \quad k(k-1)\binom{n}{k} = n(n+1)\binom{n-2}{k-2}.$$

2. Si $T \sim \mathcal{G}(p)$, alors $T(\Omega) = \mathbb{N}^\star$ et $\forall k \in T(\Omega)$, $P(T=k) = p \times q^{k-1}$. On a déjà prouvé que $\mathrm{E}(T) = \frac{1}{p}$. On veut montrer que $\mathrm{V}(T) = \frac{q}{p^2}$. Montrons que la variable T^2 possède une espérance : la série $\sum k^2\, P(T=k)$ converge absolument car $k^2\, P(T=k) = k^2 \cdot p \cdot q^{k-1}$. Or, pour $k \geqslant 2$, $\frac{\mathrm{d}^2}{\mathrm{d}x^2} x^k = k(k-1)\, x^{k-2}$. Et, on peut dériver terme à terme une série entière sans changer son rayon de convergence, et la série $\sum x^k$ a pour rayon de convergence 1. D'où, $\sum k(k-1)\, x^{k-2}$ a pour rayon de convergence 1. Or, $q \in]0,1[\subset]-1,1[$ donc la série $\sum k(k-1) q^{k-2}$ converge. De plus, $\sum k(k-1)\, q^{k-2} = \sum k^2\, q^{k-2} - \sum k\, q^{k-2}$. D'où, $\sum k^2 q^{k-2} = \sum k(k-1)\, q^{k-2} + \sum k\, q^{k-2}$, qui

converge. Par suite,

$$\begin{aligned}
\sum_{k=1}^{\infty} k^2\, P(T=k) &= \sum_{k=1}^{\infty} k^2\, p\, q^{k-1} \\
&= p + pq \sum_{k=2}^{\infty} k^2 q^{k-2} \\
&= p + pq \sum_{k=2}^{\infty} k(k-1)\, q^{k-2} + p \sum_{k=2}^{\infty} k\, q^{k-1} \\
&= p + pq\, \frac{2}{(1-q)^3} + p\left(\frac{1}{(1-q)^2} - 1\right) \qquad \textit{c.f.} \text{ en effet après} \\
&= p + pq\, \frac{2}{p^3} + p\left(\frac{1}{p^2} - 1\right) \\
&= \frac{2q}{p^2} + \frac{1}{p} \\
&= \frac{2q+p}{p^2} \\
&= \frac{2q + (1-q)}{p^2} \\
&= \frac{q+1}{p^2}.
\end{aligned}$$

En effet, $\forall x \in \,]-1,1[$, $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$. D'où, pour $x \in \,]-1,1[$,

$$\sum_{k=1}^{\infty} k\, x^{k-1} = \frac{1}{(1-x)^2} \quad \text{et} \quad \sum_{k=2}^{\infty} k(k-1)\, x^{k-2} = \frac{2}{(1-x)^3}.$$

Ainsi, $\mathrm{E}(T^2) = \frac{q^{+1}}{p^2}$. D'où

$$\begin{aligned}
\mathrm{V}(T) &= \mathrm{E}(T^2) - \big(\mathrm{E}(T)\big)^2 \\
&= \frac{q+1}{p^2} - \left(\frac{1}{p}\right)^2 \\
&= \frac{q}{p^2}
\end{aligned}$$

3. À tenter

VII.7 Les inégalités de Markov et de Bienaymé–Tchebychev, inégalités de concentration

Lemme (Markov) **:** Soit $(\Omega, \mathscr{A}, P)$ un espace probabilisé, et soit X une

variable aléatoire positive. Si X est d'espérance finie, alors

$$\forall a > 0, \quad P(X \geqslant a) \leqslant \frac{\mathrm{E}(X)}{a}.$$

Preuve :
On suppose X d'espérance finie. Ainsi, on a

$$\mathrm{E}(X) = \sum_{x \in X(\Omega)} x\, P(X = x).$$

Soit I l'ensemble $I = \{x \in X(\Omega) \mid x \geqslant a\}$. Alors,

$$\mathrm{E}(X) = \underbrace{\sum_{x \in I} x\, P(X = x)}_{\text{ici } x \geqslant a} + \underbrace{\sum_{x \in X(\Omega) \setminus I} x\, P(X = x)}_{\geqslant 0 \text{ par hypothèse}}.$$

D'où,

$$\mathrm{E}(X) \geqslant \sum_{x \in I} x P(X = x) \geqslant \sum_{x \in I} a P(X = x) = a \sum_{x \in I} P(X = x) \geqslant a P(x \geqslant a).$$

□

Proposition (Bienaymé–Tchebychev) **:** Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé, et soit X une *vard.* Si X^2 est d'espérance finie, alors

$$\forall a > 0, \qquad P\Big(\big|X - \mathrm{E}(X)\big| \geqslant a\Big) \leqslant \frac{\mathrm{V}(X)}{a^2}.$$

Preuve :
On pose $\mu = \mathrm{E}(X)$. L'événement $\big(|X - \mu| \geqslant a\big) = \big((X - \mu)^2 \geqslant a^2\big)$, d'où, les probabilités

$$P\big(|X - \mu| \geqslant a\big) = P\big(\underbrace{(X - \mu)^2}_{\geqslant 0} \geqslant \underbrace{a^2}_{\text{ř} \geqslant 0}\big).$$

On valide donc *une* des hypothèses de l'inégalité de Markov. De plus, l'autre hypothèse est vérifiée : X^2 est d'espérance finie, donc $(X - \mu)^2$ aussi. On en déduit, d'après le lemme de Markov, que

$$P\big((X - \mu)^2 \geqslant a^2\big) \leqslant \frac{\mathrm{E}\big((X - \mu)^2\big)}{a^2} = \frac{\mathrm{V}(X)}{a^2}.$$

□

VII.8 Série génératrice

Définition : Soit X une *vad* telle que $X(\Omega) \subset \mathbb{N}$. La *série génératrice* de X est la série entière $\sum a_n x^n$ de coefficients $a_n = P(X = n)$.

La série $\sum a_n$ converge car sa somme vaut $\sum_{n=0}^{\infty} a_n = 1$. D'où,

- le rayon de convergence R de la série est supérieur ou égal à 1.
- la série génératrice converge normalement sur $[-1, 1]$, car la série $\sum |a_n|$ converge, or, $\forall x \in [-1, 1]$, $|p_n t^n| \leqslant |p_n|$, d'où la convergence normale. D'où la *fonction génératrice*

$$\mathrm{G}_X : t \longmapsto \sum_{n=0}^{\infty} p_n t^n$$

  est définie et même continue sur $[-1, 1]$, car la convergence est uniforme.
- la fonction génératrice G_X est de classe $\mathscr{C}^\infty$ sur $]-1, 1[$ et

$$\forall k \in \mathbb{N}, \quad P(X = k) = a_n \frac{{\mathrm{G}_X}^{(k)}(0)}{k!}.$$

  La fonction génératrice de X permet donc de retrouver la loi de probabilité de X.

Cette série génératrice permet de calculer l'espérance et la variance de X. Si $R > 1$, alors $1 \in]-R, R[$, d'où

$$\mathrm{G}'_X(1) = \sum_{n=1}^{\infty} n a_n \qquad \text{et} \qquad \mathrm{G}''_X(1) = \sum_{n=2}^{\infty} n(n-1)\, a_n,$$

car on peut dériver terme à terme sans changer de convergence. On en déduit que X^2 est d'espérance finie et que

$$\mathrm{E}(X) = \mathrm{G}'_X(1) \qquad \text{et} \qquad \mathrm{V}(X) = G''_X(1) + G'_X(1) - \left[G'_X(1)\right]^2.$$

Également, même si inintéressant du point de vue théorique, ceci peut être utile pour vérifier les résultats en exercice

$$\mathrm{G}_X(1) = \sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} P(X = n) = 1.$$

Proposition : Soit X une *vard* telle que $X(\Omega) \subset \mathbb{N}$, et soit G_X sa fonction génératrice.

1. X est d'espérance finie si, et seulement si la fonction G_X est dérivable en 1. Dans ce cas,
$$\mathrm{E}(X) = \mathrm{G}'_X(1).$$
2. X^2 est d'espérance finie si, et seulement si la fonction G_X est deux

fois dérivable en 1. Dans ce cas,

$$\mathrm{V}(X) = \mathrm{G}''_X(1) + \mathrm{G}'_X(1) - \big[\mathrm{G}'_X(1)\big]^2.$$

Preuve :
On remarque que $\mathrm{G}''_X(1) = \sum_{n=2}^{\infty} n(n-1)\,a_n = \mathrm{E}\big(X(X-1)\big) = \mathrm{E}(X^2) - \mathrm{E}(X)$. Ainsi,

$$\begin{aligned}\mathrm{V}(X) &= \mathrm{E}\Big[\big(X - \mathrm{E}(X)\big)^2\Big] \\ &= \mathrm{E}(X^2) - \big(\mathrm{E}(X)\big)^2 \\ &= \mathrm{E}(X^2) - \mathrm{E}(X) + \mathrm{E}(X) - \big(\mathrm{E}(X)\big)^2 \\ &= \mathrm{G}''_X(1) + \mathrm{G}'_X(1) - \big(\mathrm{G}'_X(1)\big)^2\end{aligned}$$

Mais, la fonction G_X est elle,
— dérivable en 1 ? Oui, si la variable X est d'espérance finie.
— dérivable deux fois en 1 ? Oui, si la variable X^2 est d'espérance finie.

□

Le programme dit que l'on doit être capable de le retrouver rapidement.

Exercice :
Soient $p \in]0,1[$, et $\lambda > 0$. On pose $q = 1-p$. Soit X une variable aléatoire. Montrer que

1. *si $X \sim \mathcal{B}(n,p)$, alors* $\quad \forall t \in \mathbb{R}, \quad \mathrm{G}_X(t) = (pt+q)^n$;
2. *si $T \sim \mathcal{G}(p)$, alors* $\quad \forall t \in \left]-\frac{1}{q}, \frac{1}{q}\right[\quad \mathrm{G}_T(t) = \frac{pt}{1-qt}$;
3. *si $X \sim \mathcal{P}(\lambda)$, alors* $\quad \forall t \in \mathbb{R}, \quad \mathrm{G}_X(t) = \mathrm{e}^{-\lambda} \cdot \mathrm{e}^{\lambda t}$.

En déduire l'espérance et la variance de chacune de ces vard.

1. La série génératrice est $\sum P(X = k)\,t^k$, et la fonction génératrice est $\sum_{k \in X(\Omega)} P(X = k)\,t^k$. Comme $X \sim \mathcal{B}(n,p)$, on a $X(\Omega) = [\![0,n]\!]$, et $\forall k \in X(\Omega)$, $P(X=k) = \binom{n}{k} p^k\, q^{n-k}$. La série ne peut pas diverger, car il y a un nombre fini de termes. D'où,

$$\begin{aligned}\forall t \in]-\infty,+\infty[, \quad \mathrm{G}_X(t) &= \sum_{k=0}^{n} \binom{n}{k} q^{n-k}\, t^k \\ &= (pt+q)^n\end{aligned}$$

La fonction G_X est dérivable en 1, donc la variable aléatoire X est d'espérance finie, et $\mathrm{E}(X) = \mathrm{G}'_X(1)$. Or, $\forall t \in \mathbb{R}$, $\mathrm{G}'_X(t) = n\,p\,(pt+q)^{n-1}$. D'où, $\mathrm{E}(X) = \mathrm{G}'_X(1) = n\,p$. Mieux : G_X est deux fois dérivable en 1.

Ainsi, X^2 est d'espérance finie, et

$$\begin{aligned} \mathrm{V}(X) &= \mathrm{G}''_X(1) + \mathrm{G}'_X(1) - \left[\mathrm{G}'_X(1)\right]^2 \\ &= n\cdot(n-1)\cdot p^2 + n\cdot p - (n\cdot p)^2 \\ &= n\cdot p - n\cdot p^2 = n\cdot p\cdot(1-p) \\ &= n\cdot p\cdot q \end{aligned}$$

2. Si $T \sim \mathcal{G}(p)$, alors $T(\Omega) = \mathbb{N}^\star$, et $\forall k \in T(\Omega)$, $P(T=k) = p \times q^{k-1}$. La série génératrice de la variable T est

$$\sum P(T=k)t^k = \sum p\, q^{k-1}\, t^k = p\, t \sum (qt)^{k-1},$$

c'est une série géométrique de raison qt. Elle converge si, et seulement si $|qt| < 1$. D'où, le rayon de convergence de la série génératrice vaut $R = \frac{1}{q}$. Et,

$$\begin{aligned} \forall t \in \left]-\frac{1}{q}, \frac{1}{q}\right[, \quad \mathrm{G}_T(t) &= p\, t \sum_{k=1}^{\infty} (qt)^{k-1} \\ &= pt \sum_{k=0}^{\infty} (qt)^k \\ &= pt \cdot \frac{1}{1-qt} \text{ car } |qt| < 1 \end{aligned}$$

G_X est dérivable en 1, d'où, la variable aléatoire T est d'espérance finie, et $\mathrm{E}(T) = \mathrm{G}'_T(1)$.

$$\forall t \in \left]-\frac{1}{q}, \frac{1}{q}\right[, \quad \mathrm{G}'_T(t) = \frac{p(1-qt) - pt(-q)}{(1-qt)^2} = \frac{p}{(1-qt)^2}.$$

D'où, $\mathrm{E}(t) = \frac{p}{(1-q)^2} = \frac{1}{p}$.

Chapitre 12

Endomorphismes remarquables d'un espace euclidien

VII.1 Qu'est ce qu'une matrice orthogonale ?

Définition : On dit qu'une matrice carrée $A \in \mathscr{M}_n(\mathbb{R})$ est *orthogonale* si $A^\top \cdot A = I_n$. L'ensemble des matrices orthogonales de $\mathscr{M}_n(\mathbb{R})$ est noté $\mathrm{O}_n(\mathbb{R})$ ou $\mathrm{O}(n)$, et est appelé le *groupe orthogonal* d'ordre n.

Remarque :
Le déterminant d'une matrice orthogonale vaut ± 1. En effet, $1 = \det I_n = \det(A^\top \cdot A) = \det A^\top \cdot \det A = \big[\det A\big]^2$. Ainsi, toute matrice orthogonale est inversible :

$$A \in \mathrm{O}_n(\mathbb{R}) \implies \det A = \pm 1 \implies \det A \neq 0 \implies A \in \mathrm{GL}_n(\mathbb{R}).$$

On en déduit que

$$A \in \mathrm{O}_n(\mathbb{R}) \iff A^\top \cdot A = I_n \iff A^\top \cdot A^{-1} \iff A \cdot A^\top = I_n.$$

En effet, $A^\top \cdot A = I_n$ et donc $A^\top \cdot A \cdot A^{-1} = A^{-1}$. D'où, $A^\top = A^{-1}$.

Le sous-ensemble des matrices orthogonales dont le déterminant vaut $+1$ est noté $\mathrm{SO}_n(\mathbb{R})$, ou $\mathrm{SO}(n)$, et est appelé *groupe spécial orthogonal* d'ordre n. Ainsi,

$$\mathrm{SO}_n(\mathbb{R}) \subset \mathrm{O}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R}).$$

Exercice :
Montrer que $\mathrm{SO}_n(\mathbb{R})$ *est un sous-groupe de* $\mathrm{O}_n(\mathbb{R})$*, qui est un sous-groupe de* $\mathrm{GL}_n(\mathbb{R})$*. Vérifier, par ailleurs, que ces ensembles sont stables par transposition.*

L'ensemble $\mathrm{O}_n(\mathbb{R})$ est non vide. En effet, $I_n \in \mathrm{SO}_n(\mathbb{R})$ car $\det I_n = 1$ et $I_n^\top \cdot I_n = I_n \cdot I_n = I_n$. De plus, si $A \in \mathrm{O}_n(\mathbb{R})$ et $B \in \mathrm{O}_n(\mathbb{R})$, alors $(A \cdot B^{-1})^{-1} = B \cdot A^{-1} = (B^\top)^\top \cdot A^\top = (A \cdot B)^\top$, d'où $A \cdot B \in \mathrm{O}_n(\mathbb{R})$. On en déduit que $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

L'ensemble $\mathrm{SO}_n(\mathbb{R})$ est non vide. En effet, $I_n \in \mathrm{SO}_n(\mathbb{R})$ car $\det I_n = 1$ et $I_n^\top \cdot I_n = I_n \cdot I_n = I_n$. De plus, si $A \in \mathrm{SO}_n(\mathbb{R})$ et $B \in \mathrm{SO}_n(\mathbb{R})$, alors $\det(A \cdot B^{-1}) = \det A \cdot \det(B^{-1}) = 1 \times \frac{1}{1} = 1$, et $(A \cdot B^{-1})^{-1} = B \cdot A^{-1} = (B^\top)^\top \cdot A^\top = (A \cdot B)^\top$, d'où $A \cdot B \in \mathrm{SO}_n(\mathbb{R})$. On en déduit que $\mathrm{SO}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{O}_n(\mathbb{R})$.

Pour toute matrice $A \in \mathrm{O}_n(\mathbb{R})$, on a $A^{-1} = A^\top$, et $A^{-1} \in \mathrm{O}_n(\mathbb{R})$, d'où $A^\top \in \mathrm{O}_n(\mathbb{R})$. On en déduit que $\mathrm{O}_n(\mathbb{R})$ est stable par transposition. Ce raisonnement reste valide en remplaçant $\mathrm{O}_n(\mathbb{R})$ par $\mathrm{SO}_n(\mathbb{R})$.

> **Proposition :** Une matrice est orthogonale si, et seulement si, ses colonnes (ou ses lignes) forment une base orthonormée de $\mathbb{R}^n$ (muni du produit scalaire canonique). Autrement dit : une matrice est orthogonale si, et seulement si c'est la matrice de passage d'une base orthonormée de E vers une autre base orthonormée de E.

> *Preuve :*
> On note C_n, C_2, …, C_n les colonnes de $A \in \mathrm{O}_n(\mathbb{R})$.
>
> $$\begin{aligned} A^\top \cdot A = I_n &\iff \forall (i,j) \in [\![1,n]\!]^2,\ \langle C_i \mid C_j \rangle = \delta_{i,j} \\ &\iff (C_1, \ldots, C_n) \text{ est une base orthonormée.} \end{aligned}$$
>
> Et, si A est orthogonale, $A^\top$ l'est aussi. Or, la transposition change les colonnes en lignes. □

Méthode :
En particulier, soit A une matrice 3×3 de colonnes C_1, C_2, et C_3. Il suffit de vérifier que

- (C_1, C_2) est une famille orthonormée, et $C_1 \wedge C_2 = \pm C_3$ pour montrer $A \in \mathrm{O}_3(\mathbb{R})$;
- (C_1, C_2) est une famille orthonormée, et $C_1 \wedge C_2 = +C_3$ pour montrer $A \in \mathrm{SO}_3(\mathbb{R})$.

Exercice :

Soit $\theta \in \mathbb{R}$. Étudier les matrices

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \\ f(\vec{\imath}) & f(\vec{\jmath}) \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \end{matrix} = \big[\, f \,\big]_{(\vec{\imath},\vec{\jmath})} \in \mathrm{SO}_2(\mathbb{R}),$$

$$B = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \\ g(\vec{\imath}) & g(\vec{\jmath}) \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \end{matrix} = \big[\, g \,\big]_{(\vec{\imath},\vec{\jmath})} \in \mathrm{O}_2(\mathbb{R}),$$

$$C = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \\ h(\vec{\imath}) & h(\vec{\jmath}) & h(\vec{k}) \\ C_1 & C_2 & C_3 \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \\ \vec{k} \end{matrix} = \big[\, h \,\big]_{(\vec{\imath},\vec{\jmath},\vec{k})}$$

$$D = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ u(\vec{\imath}) & u(\vec{\jmath}) & u(\vec{k}) \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \\ \vec{k} \end{matrix} = \big[\, u \,\big]_{(\vec{\imath},\vec{\jmath},\vec{k})}$$

La matrice A est la rotation d'angle θ. La matrice B est la symétrie orthogonale par rapport à $\mathrm{Vect}(\vec{a})$. De plus, $B^\top = B^{-1} = B$, et, dans une base adaptée $(\vec{a},\vec{b})$, l'endomorphisme g devient

$$\big[\, g \,\big]_{(\vec{a},\vec{b})} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ g(\vec{a}) & g(\vec{b}) \end{pmatrix} \begin{matrix} \vec{a} \\ \vec{b} \end{matrix} = B'.$$

La matrice C est diagonale par blocs, donc triangulaire par blocs, donc $\det C = \det A \times 1 = +1$. Les colonnes C_1, C_2 et C_3 de la matrice C forment une base orthonormée, d'où $C \in \mathrm{O}_3(\mathbb{R})$. De plus, $\det C = +1$, donc $C \in \mathrm{SO}_3(\mathbb{R})$. On remarque que $h(\vec{k}) = \vec{k}$. La matrice C est donc la rotation d'angle θ de l'axe $(O,\vec{k})$. On remarque que $u(\vec{\jmath}) = \vec{\jmath}$, $u(\vec{\imath}+\vec{\jmath}+\vec{k}) = \vec{\imath}+\vec{\jmath}+\vec{k}$, $u(\vec{\imath},\vec{k}) = \vec{\imath}+\vec{k}$ et $g(\vec{\imath}-\vec{k}) = \vec{k}-\vec{\imath}$. Ainsi, $\mathrm{SEP}(1) = \mathrm{Vect}(\vec{\jmath},\vec{\imath}+\vec{k})$, et $\mathrm{SEP}(-1) = \mathrm{Vect}(\vec{\imath}-\vec{k})$. Les colonnes de D forment une base orthonormée, d'où $D \in \mathrm{O}_3(\mathbb{R})$. Or, $\det D = -1$ en développant, d'où $D \notin \mathrm{SO}_3(\mathbb{R})$. Enfin, $\vec{u}$ est la symétrie de orthogonale par rapport à $\mathrm{SEP}(1) = \mathrm{Vect}(\vec{\jmath},\vec{\imath}+\vec{k})$. Ainsi,

$$\big[\, u \,\big]_{(\vec{\jmath},\vec{\imath}+\vec{k},\vec{\imath}-\vec{k})} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{matrix} \vec{\jmath} \\ \vec{\imath}+\vec{k} \\ \vec{\imath}-\vec{k} \end{matrix}$$

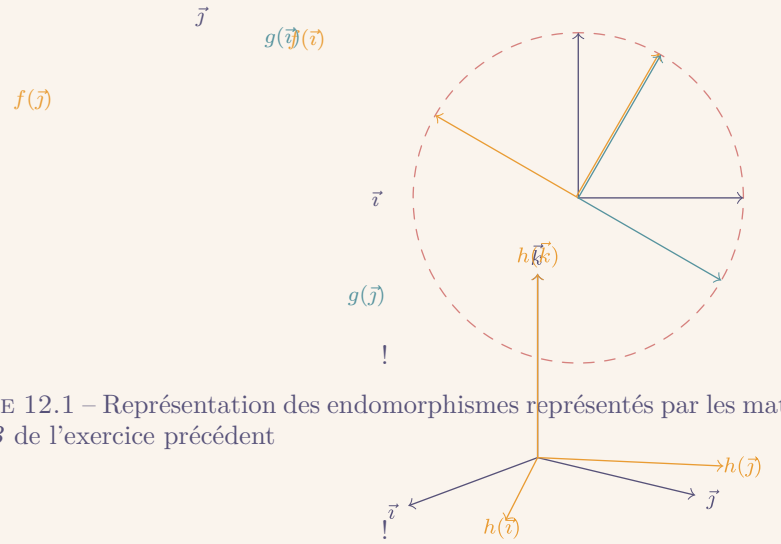


FIGURE 12.1 – Représentation des endomorphismes représentés par les matrices A et B de l'exercice précédent

FIGURE 12.2 – Représentation de l'endomorphisme représenté par la matrices C de l'exercice précédent

VII.2 Isométries vectorielles

Définition : Soit un espace euclidien E, et soit $f : E \to E$. On dit que f est une *isométrie vectorielle* si f conserve le produit scalaire

$$\forall (u, v) \in E^2, \quad \langle f(u) \mid f(v) \rangle = \langle u \mid v \rangle.$$

L'ensemble des isométries vectorielles de E est noté $\mathrm{O}(E)$. Une isométrie vectorielle est aussi appelé un *automorphisme orthogonal* d'après les propositions suivantes.

Proposition : Toute isométrie vectorielle de E est linéaire et bijective. Autrement dit, toute symétrie vectorielle de E est un automorphisme de E. Mieux : l'ensemble $\mathrm{O}(E)$ des isométries de E est un sous-groupe de $\mathrm{GL}(E)$ des automorphismes de E.

Preuve :
Soit $f \in \mathrm{O}(E)$ une isométrie de E. Soient $(a, b) \in \mathbb{R}$ et soient $(\vec{u}, \vec{v}) \in E^2$.

On veut montrer que :

$$\begin{aligned} & f(a\,\vec{u}+b\,\vec{v}) = a\,f(\vec{u})+b\,f(\vec{v}) \\ \iff & f(a\,\vec{u}+b\,\vec{v}) = \vec{0} \\ \iff & \big\|f(a\,\vec{u}+b\,\vec{v})\big\| = \|\vec{0}\| = 0_{\mathbb{R}} \\ \iff & \big\langle f(a\,\vec{u}+b\,\vec{v}-a\,f(\vec{u})+b\,f(\vec{v}) \;\big|\; f(a\,\vec{u}+b\,\vec{v}-a\,f(\vec{u})+b\,f(\vec{v})\big\rangle = 0 \end{aligned}$$

Par bilinéarité du produit scalaire, ce grand produit scalaire peut-être décomposé en 9 facteurs, et on n'en traitera qu'un :

$$\big\langle -a\,f(\vec{u})\big|-b\,f(\vec{v})\big\rangle = (-a)(-b)\big\langle f(\vec{u})\big|f(\vec{v})\big\rangle = (-a)(-b)\langle \vec{u}\mid\vec{v}\rangle = \langle -a\vec{u}\mid -b\vec{v}\rangle.$$

En répétant 9 fois ce calcul, on arrive à l'équivalence

$$\iff \|\underbrace{a\,\vec{u}+b\,\vec{v}-a\,\vec{u}-b\,\vec{v}}_{\vec{0}}\| = 0,$$

ce qui est vrai.

Montrons la bijectivité de f. Mais, comme $f : E \to E$, avec E de dimension finie, et f est linéaire, on a donc

$$f \text{ bijective} \iff f \text{ injective} \iff f \text{ surjective},$$

d'après le théorème du rang. Soit $\vec{x} \in E$:

$$\begin{aligned} \vec{x} \in \operatorname{Ker} f \iff & f(\vec{x}) = \vec{0} \\ \implies & \big\|f(\vec{x})\big\| = 0 \\ \implies & \big\langle f(\vec{x}) \;\big|\; f(\vec{x})\big\rangle = 0 \\ \implies & \langle \vec{x}\mid\vec{x}\rangle = 0 \text{ car } f \text{ est une isométrie} \\ \implies & \vec{x} = \vec{0} \text{ par le caractère défini du produit scalaire.} \end{aligned}$$

Réciproquement, on a bien $f(\vec{0}) = \vec{0}$, et donc $\operatorname{Ker} f = \{\vec{0}\}$, d'où f injective, et donc bijective.

La suite de la preuve se trouve sur le poly. □

Théorème (3/4 caractérisations d'une isométrie) **:** Soit E un espace euclidien, et soit $f : E \to E$. *Il existe 4 manières de caractériser une*

isométrie, dont 3 sont prouvés ici.

f conserve le produit scalaire

$\Updownarrow$

f est linéaire et conserve la norme :
$\forall \vec{u} \in E, \quad \|f(\vec{u})\| = \|\vec{u}\|$

$\Updownarrow$

f est linéaire et transforme une base orthonormée de E en une base orthonormée de E.

Preuve :
Cette preuve se déroule en trois étapes :

$$\begin{array}{ccc} & (2) & \\ \swarrow & & \nwarrow \\ (1) & \Longrightarrow & (3) \end{array}$$

— On suppose f linéaire, et $\forall \vec{u} \in E$, $\|f(\vec{u})\| = \|\vec{u}\|$. On veut montrer que $\forall (\vec{u}, \vec{v}) \in E^2$, $\langle f(\vec{u}) \mid f(\vec{v}) \rangle = \langle u \mid v \rangle$. On se rappelle que $\langle \vec{a} \mid \vec{b} \rangle = \frac{1}{2}\left(\|\vec{a} + \vec{b}\|^2 - \|\vec{a}\| - \|\vec{b}\|^2\right)$. D'où,

$$\begin{aligned} \langle f(\vec{u}) \mid f(\vec{v}) \rangle &= \frac{1}{2}\left(\|f(\vec{u}) + f(\vec{v})\|^2 - \|f(\vec{u})\|^2 - \|f(v)\|^2\right) \\ &= \frac{1}{2}\left(\|f(\vec{u} + \vec{v})\|^2 - \|f(\vec{u})\|^2 - \|f(v)\|^2\right) \\ &= \frac{1}{2}\left(\|\vec{u} + \vec{v}\|^2 - \|\vec{u}\|^2 - \|v\|^2\right) \\ &= \langle u \mid v \rangle \end{aligned}$$

— On suppose f une isométrie. Alors f est linéaire d'après la proposition 8, et l'application f transforme une base orthonormée en une autre base orthonormée.

— B Tarte à la crème. On suppose f linéaire, et qu'elle transforme une base orthonormée en une autre base orthonormée. On veut montrer f linéaire (vrai par hypothèse), et que $\forall \vec{u} \in E$, $\|f(\vec{u})\| = \|\vec{u}\|$. Soit $\vec{u} \in E$. On le décompose dans la base orthonormée $\mathcal{B} = (\vec{\varepsilon_1}, \vec{\varepsilon_2}, \ldots, \vec{\varepsilon_n})$:

$$\vec{u} = x_1\vec{\varepsilon_1} + x_2\vec{\varepsilon_2} + \cdots + x_n\vec{\varepsilon_n}.$$

Par linéarité de f, on a $f(\vec{u}) = x_1\, f(\vec{\varepsilon}_1) + x_2\, f(\vec{\varepsilon}_2) + \cdots + x_n\, f(\vec{\varepsilon}_n)$. Ainsi, comme la base $\mathscr{B}$ est une famille orthogonale, d'après le théorème de PYTHAGORE, on a

$$\begin{aligned}\|\vec{u}\|^2 &= \|x_1\,\vec{\varepsilon}_1\|^2 + \|x_1\,\vec{\varepsilon}_2\|^2 + \cdots + \|x_1\,\vec{\varepsilon}_n\|^2\\ &= x_1^2\,\|\vec{\varepsilon}_1\|^2 + x_2^2\,\|\vec{\varepsilon}_2\|^2 + \cdots + x_n^2\,\|\vec{\varepsilon}_n\|^2\\ &= x_1^2 + x_2^2 + \cdots + x_n^2\end{aligned}$$

La base $\mathscr{B}' = \big(f(\vec{\varepsilon}_1), f(\vec{\varepsilon}_2), \ldots, f(\vec{\varepsilon}_n)\big)$ est orthonormée, on a de même,

$$\|f(\vec{u})\|^2 = x_1^2 + \cdots + x_n^2.$$

□

Proposition : Soit E un espace euclidien de dimension n.

$$f \text{ est une isométrie de } E \iff \begin{array}{l}\text{la matrice de } f, \text{ dans}\\ \text{une } \underline{\text{base orthonormée}},\\ \text{est orthogonale.}\end{array}$$

Autrement dit,

$$f \in \mathrm{O}(E) \iff \big[\, f \,\big]_{\mathscr{B}} \in \mathrm{O}_n(\mathbb{R}),$$

où $\mathscr{B}$ est une base <u>orthonormée</u>.

VII.3 Endomorphismes adjoints

Définition : On dit qu'un endomorphisme $f : E \to E$ est *autoadjoint* si

$$\forall (\vec{u}, \vec{v}) \in E^2, \quad \big\langle f(\vec{u}) \,\big|\, \vec{v} \big\rangle = \big\langle \vec{u} \,\big|\, f(\vec{v}) \big\rangle.$$

Un endomorphisme autoadjoint est aussi appelé endomorphisme *symétrique* (*c.f.* proposition suivante). L'ensemble des endomorphismes autoadjoints est noté $\mathcal{S}(E)$.

Proposition : Un endomorphism est autoadjoint si, et seulement si la matrice de F dans une base <u>orthonormée</u> $\mathscr{B}$ est orthogonale. Autrement dit :

$$f \in \mathcal{S}(E) \iff \big[\, f \,\big]_{\mathscr{B}} \in \mathcal{S}_n(\mathbb{R}).$$

Preuve : $\Longrightarrow$ Soit $\mathcal{B} = (\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_n)$ une base orthonormée de E. Ainsi,

$$\forall i,\ \forall j, \quad \left\langle f(\vec{\varepsilon}_i) \,\middle|\, \vec{\varepsilon}_j \right\rangle = \left\langle \vec{\varepsilon}_i \,\middle|\, f(\vec{\varepsilon}_j) \right\rangle.$$

On pose $\left[\, f \,\right]_{\mathcal{B}} = (a_{i,j})$:

$$\begin{array}{c} \begin{pmatrix} & a_{1,j} & \\ & & \\ & a_{i,j} & \\ & & \\ & a_{n,j} & \end{pmatrix} \begin{matrix} \vec{\varepsilon}_i \\ \\ \vec{\varepsilon}_i \\ \\ \vec{\varepsilon}_n \end{matrix} \\ \begin{matrix} f(\vec{\varepsilon}_i) & f(\vec{\varepsilon}_j) & f(\vec{\varepsilon}_n) \end{matrix} \end{array}.$$

Ainsi, $f(\vec{\varepsilon}_j) = a_{1,j}\vec{\varepsilon}_1 + \cdots + a_{i,j}\vec{\varepsilon}_i + \cdots + a_{n,j}\vec{\varepsilon}_n$. D'où, $\langle \vec{\varepsilon}_i \mid f(\vec{\varepsilon}_j) \rangle = a_{i,j}$ car la base $\mathcal{B}$ est orthonormée. De même avec l'autre produit scalaire, $\langle f(\vec{\varepsilon}_i) \mid \vec{\varepsilon}_j \rangle$, d'où $a_{i,j} = a_{j,i}$ par symétrie du produit scalaire. On en déduit que $\left[\, f \,\right]_{\mathcal{B}} \in \mathcal{S}_n(\mathbb{R})$.

$\Longleftarrow$ Si $\left[\, f \,\right]_{\mathcal{B}} \in \mathcal{S}_n(\mathbb{R})$, alors $\langle f(\vec{\varepsilon}_i) \mid \vec{\varepsilon}_j \rangle = \langle \vec{\varepsilon}_i \mid f(\vec{\varepsilon}_j) \rangle$. Or, on pose $\vec{u} = x_1\vec{\varepsilon}_1 + \cdots + x_n\vec{\varepsilon}_n$, et $\vec{v} = y_1\vec{\varepsilon}_1 + \cdots + y_n\vec{\varepsilon}_n$.

$$\begin{aligned} \langle f(\vec{u}) \mid \vec{v} \rangle &= \langle x_1 f(\vec{\varepsilon}_1) + \cdots + x_n f(\vec{\varepsilon}_n) \mid y_1 f(\vec{\varepsilon}_1) + \cdots + y_n f(\vec{\varepsilon}_n) \rangle \\ &= \left\langle \sum_{i=1}^{n} x_i f(\vec{\varepsilon}_i) \,\middle|\, \sum_{j=1}^{n} y_j \vec{\varepsilon}_j \right\rangle \\ &= \sum_{i,j \in [\![1,n]\!]} x_i y_j \left\langle f(\vec{\varepsilon}_i) \mid \vec{\varepsilon}_j \right\rangle \end{aligned}$$

De même en inversant $\vec{u}$ et $\vec{v}$. On en déduit donc $\langle f(\vec{u} \mid \vec{v} \rangle = \langle \vec{u} \mid f(\vec{v}) \rangle$.

□

Exercice : 1. Si f est autoadjoint, montrons que $\operatorname{Ker} f \perp \operatorname{\mathfrak{Im}} f$, et $\operatorname{Ker} f \oplus \operatorname{\mathfrak{Im}} f$. On suppose $\forall \vec{u}, \forall \vec{v}, \langle f(\vec{u}) \mid \vec{v} \rangle = \langle \vec{u} \mid f(\vec{v}) \rangle$. Soit $\vec{u} \in \operatorname{Ker} f$, et soit $\vec{v} \in \operatorname{\mathfrak{Im}} f$. On sait que $f(\vec{u}) = \vec{0}$, et qu'il existe $\vec{x} \in E$ tel que $\vec{v} = f(\vec{x})$. Ainsi,

$$\langle \vec{u} \mid \vec{v} \rangle = \langle \vec{u} \mid f(\vec{x}) \rangle = \langle f(\vec{u}) \mid \vec{x} \rangle = 0.$$

D'où $\vec{u} \perp \vec{v}$. Ainsi, $\operatorname{Ker} f \perp \operatorname{\mathfrak{Im}} f$.

De plus, E est de dimension finie, d'où, d'après le théorème du rang,

$$\dim \operatorname{Ker} f + \dim \operatorname{\mathfrak{Im}} f = \dim E.$$

Aussi, $\operatorname{Ker} f \oplus (\operatorname{Ker} f)^{\perp} = E$, donc $\dim(\operatorname{Ker} f) + \dim(\operatorname{Ker} f)^{\perp} = \dim E$. On en déduit donc que $\dim(\operatorname{\mathfrak{Im}} f) = \dim(\operatorname{Ker} f)^{\perp}$. Or, $\operatorname{\mathfrak{Im}} f \subset (\operatorname{Ker} f)^{\perp}$ car $\operatorname{\mathfrak{Im}} f \perp \operatorname{Ker} f$. Ainsi $\operatorname{\mathfrak{Im}} f = (\operatorname{Ker} f)^{\perp}$, on en déduit que

$$\operatorname{\mathfrak{Im}} f \oplus \operatorname{Ker} f = E.$$

$\Longleftarrow$ Soit p la projection sur F parallèlement à G. Supposons l'endomorphisme P autoadjoint. D'après la question 1., le

$\operatorname{Ker} p \perp \operatorname{Im} p$. Ainsi, $F = \operatorname{Im} p$ et $G = \operatorname{Ker} p$. D'où, $F \perp G$, p est donc une projection orthogonale.

$\Longrightarrow$ Réciproquement, supposons p une projection orthogonale. Soit $\mathcal{B} = (\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_q)$ une base orthonormée de F. Ainsi, pour tout $\vec{x} \in E$,

$$p(\vec{x}) = \sum_{i=1}^{q} \langle \vec{x} \mid \vec{\varepsilon}_i \rangle \ \vec{\varepsilon}_i.$$

On veut montrer que l'endomorphisme p est autoadjoint. Soient $\vec{u}$ et $\vec{v}$ deux vecteurs de E.

$$\begin{aligned}\langle p(\vec{u}) \mid \vec{v} \rangle = \left\langle \sum_{i=1}^{q} \langle \vec{u} \mid \vec{\varepsilon}_i \rangle \, \vec{\varepsilon}_i \,\middle|\, \vec{v} \right\rangle &= \sum_{i=1}^{q} \langle u \mid \vec{\varepsilon}_i \rangle \ \langle \vec{\varepsilon}_i \mid v \rangle \\ &= \sum_{i=1}^{q} \langle v \mid \vec{\varepsilon}_i \rangle \ \langle \vec{\varepsilon}_i \mid u \rangle \\ &= \langle \vec{u} \mid p(\vec{v}) \rangle\end{aligned}$$

Autre méthode, pour tous vecteurs $\vec{u}$ et $\vec{v}$ de E,

$$\begin{aligned}\langle p(\vec{u}) \mid \vec{v} \rangle &= \langle p(\vec{u}) \mid p(\vec{v}) + \vec{v} - p(\vec{v}) \rangle \\ &= \langle p(\vec{u}) \mid p(\vec{v}) \rangle + \langle p(\vec{u}) \mid \vec{v} - p(\vec{v}) \rangle \\ &= \langle p(\vec{u}) \mid p(\vec{v}) \rangle + \langle u - p(\vec{u}) \mid p(\vec{v}) \rangle \\ &= \langle \vec{u} \mid p(\vec{v}) \rangle\end{aligned}$$

car p est orthogonale.

Proposition–Définition : Si f est un endomorphisme d'un espace euclidien E, alors il existe un unique endomorphisme de E, noté $f^\star$ et appelé l'*adjoint* de f, tel que

$$\forall (\vec{u}, \vec{v}) \in E^2, \qquad \langle f^\star(\vec{u}) \mid \vec{v} \rangle = \langle \vec{u} \mid f(\vec{v}) \rangle .$$

Si A est la matrice f dans une base orthonormée $\mathcal{B}$ de E, alors $A^\top$ est la matrice de $f^\star$ dans $\mathcal{B}$:

$$[\, f \,]_{\mathcal{B}} = [\, f \,]_{\mathcal{B}}^{\top}.$$

Preuve :
Soit $\vec{u} \in E$. L'application

$$\begin{aligned}\varphi : E &\longrightarrow \mathbb{R} \\ \vec{v} &\longmapsto \langle \vec{u} \mid f(\vec{v}) \rangle .\end{aligned}$$

La forme φ est linéaire car $\varphi(\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2) = \langle \vec{u} \mid f(\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2) \rangle = \langle \vec{u} \mid \alpha_1 f(\vec{v}_1) + \alpha_2 f(\vec{v}_2) \rangle = \alpha_1 \langle \vec{u} \mid f(\vec{v}) \rangle + \alpha_2 \langle \vec{u} \mid f(\vec{v}_2) \rangle = \alpha_1 \varphi(\vec{v}_1) +$

$\alpha_2\varphi(\vec{v}_2)$. D'où, d'après le théorème de Riesz, il existe un unique vecteur $\vec{a} \in E$ tel que $\varphi(\vec{v}) = \langle \vec{a} \mid \vec{v} \rangle$ pour tout $\vec{v} \in E$. Ainsi, pour tout vecteur $\vec{v} \in E$, $\langle \vec{u} \mid f(\vec{v}) \rangle = \langle \vec{a} \mid \vec{v} \rangle$. On note $\vec{a} = f^\star(\vec{u})$. Soit l'application

$$\begin{aligned} f^\star : E &\longrightarrow E \\ \vec{u} &\longmapsto f^\star(\vec{u}). \end{aligned}$$

La démonstration telle que $f^\star$ est linéaire est dans le poly. L'application $f^\star$ vérifie : $\langle \vec{u} \mid f(\vec{v}) \rangle = \langle f^\star(\vec{u}) \mid \vec{v} \rangle$, pour tous vecteurs $\vec{u}$ et $\vec{v}$. *Quelle est la matrice de $f^\star$, dans une base orthonormée ?* Soit $\mathscr{B}$ une base orthonormée de E, et soient $A = \left[f \right]_{\mathscr{B}}$, $B = \left[f^\star \right]_{\mathscr{B}}$, $U = \left[\vec{u} \right]_{\mathscr{B}}$, et $V = \left[\vec{v} \right]_{\mathscr{B}}$. Les matrices U et V sont des vecteurs colonnes, et A et B sont des matrices carrées. Ainsi,

$$U^\top \cdot A \cdot V = \langle \vec{u} \mid f(\vec{v}) \rangle = \langle f^\star(\vec{u}) \mid \vec{v} \rangle = (B \cdot U)^\top \cdot V,$$

ce qui est vrai quelque soit les vecteurs colonnes U et V. D'où, $\forall U$, $\forall V$, $U^\top \cdot \big(A \cdot V\big) = U^\top \cdot \big(B^\top \cdot V\big)$. Ainsi, pour tous vecteurs U et V,

$$U^\top \cdot \Big[(AV) - (B^\top V) \Big] = 0.$$

En particulier, si $U = (AV) - (B^\top V)$, le produit scalaire $\langle \vec{u} \mid \vec{u} \rangle$ est nul, donc $U = 0$. Ainsi,

$$\forall V, \quad A \cdot V = B^\top \cdot V.$$

De même, on conclut que $A = B^\top$. On en déduit donc que

$$\left[f^\star \right]_{\mathscr{B}} = \left[f \right]_{\mathscr{B}}^\top.$$

□

Les propriétés suivantes sont vrais :

— $(f \circ g)^\star = g^\star \circ f^\star$, $\quad (f^\star)^\star = f$, $\quad$ et $\quad (\alpha f + \beta g)^\star = \alpha f^\star + \beta g^\star$;
— $(A \cdot B)^\top = B^\top \cdot A^\top$, $\quad (A^\top)^\top = A$, $\quad$ et $\quad (\alpha A + \beta B)^\top = \alpha A^\top + \beta B^\top$.

Des deuxièmes et troisièmes points, il en résulte que les applications $f \mapsto f^\star$, et $A \mapsto A^\top$ sont des applications involutives.

On rappelle que $\langle \vec{u} \mid f(\vec{v}) \rangle = \langle f^\star(\vec{u}) \mid \vec{v} \rangle$, pour tous vecteurs $\vec{u}$ et $\vec{v}$.

Proposition : Soit $f : E \to E$, un endomorphisme d'un espace euclidien E.

1. f est autoadjoint si, et seulement si, $f^\star = f$;
2. f est une isométrie si, et seulement si, $f^\star = f^{-1}$.

Ainsi, on a

$$\begin{aligned} f \text{ est autoadjoint} &\overset{\text{def.}}{\iff} \langle \vec{u} \mid f(\vec{v}) \rangle = \langle f(\vec{u}) \mid \vec{v} \rangle \text{ pour tous vecteurs } \vec{u} \text{ et } \vec{v} \\ &\iff f^\star = f \\ &\iff \left[f \right]_{\mathscr{B}}^{\top} = \left[f \right]_{\mathscr{B}} \text{ dans une base orthonormée } \mathscr{B}. \end{aligned}$$

Et,

$$\begin{aligned} f \text{ est une isométrie} &\overset{\text{def.}}{\iff} \langle f(\vec{u}) \mid f(\vec{v}) \rangle = \langle \vec{u} \mid \vec{v} \rangle \text{ pour tous vecteurs } \vec{u} \text{ et } \vec{v} \\ &\iff \left[f \right]_{\mathscr{B}}^{\top} = \left[f \right]_{\mathscr{B}}^{-1} \text{ dans une base orthonormée } \mathscr{B} \\ &\iff f^\star = f^{-1}. \end{aligned}$$

Ce qui prove la proposition précédente.

Exercice :
Soit E un espace euclidien, et soit F un sous-espace vectoriel de E. On a $F \oplus F^\perp = E$. Soit $\mathfrak{s} \in \mathscr{L}(E,E)$. Montrons que $\mathfrak{s}$ est une symétrie orthogonale si, et seulement si $\mathfrak{s}$ est une symétrie autoadjointe.

" $\Longleftarrow$ " L'application $\mathfrak{s}$ est une isométrie donc $\mathfrak{s}^\star = \mathfrak{s}^{-1}$. L'application $\mathfrak{s}$ est un endomorphisme autoadjoint donc $\mathfrak{s}^\star = \mathfrak{s}$. D'où $\mathfrak{s} = \mathfrak{s}^{-1}$, donc $\mathfrak{s}$ est une symétrie. Ainsi $\mathrm{Ker}(\mathfrak{s} - \mathrm{id}) \perp \mathrm{Ker}(\mathfrak{s} + \mathrm{id})$.

" $\Longrightarrow$ " L'application $\mathfrak{s}$ est une symétrie orthogonale, d'où $E = F + F^\perp$ en appelant $F = \mathrm{Ker}(\mathfrak{s} - \mathrm{id})$. Ainsi, pour tout vecteur $\vec{x} \in E$, il existe un unique couple $(\vec{a}, \vec{b}) \in F \times F^\perp$ tel que $\vec{x} = \vec{a} + \vec{b}$. D'où, $\mathfrak{s}(\vec{x}) = \mathfrak{s}(\vec{a}) + \mathfrak{s}(\vec{b}) = \vec{a} - \vec{b}$. D'où $\|\vec{x}\|^2 = \|\vec{a}\|^2 + \|\vec{b}\|^2$ et $\|\mathfrak{s}(\vec{x})\|^2 = \|\vec{a}\| + \|\vec{b}\|$. Ainsi, $\mathfrak{s}$ conserve la norme, c'est donc une isométrie, donc $\mathfrak{s}^\star = \mathfrak{s}^{-1}$ De plus, $\mathfrak{s}$ est une symétrie donc $\mathfrak{s} = \mathfrak{s}^{-1}$. D'où, $\mathfrak{s} = \mathfrak{s}^\star$, donc $\mathfrak{s}$ est autoadjoint.

VII.4 Stabilité de l'orthogonal

Proposition : Soit f un endomorphisme autoadjoint de E, et soit f un sous-espace vectoriel de E. Si F est stable par f, alors $F^\perp$ est aussi stable par f.

Preuve :
On suppose, pour tous vecteurs $\vec{u}$ et $\vec{v}$, $\langle f(\vec{u}) \mid \vec{v} \rangle = \langle \vec{u} \mid f(\vec{v}) \rangle$, et pour tout vecteur $\vec{x} \in F$, $f(\vec{x}) \in F$. Soit $\vec{x} \in F^\perp$. Soit $\vec{y} \in F$. On calcule : $\langle f(\vec{x}) \mid \vec{y} \rangle = \langle \vec{x} \mid f(\vec{y}) \rangle$. Or, $\vec{y} \in F$, et donc $f(\vec{y}) \in F$ par hypothèse. Comme $\vec{x} \in F^\perp$. Ainsi, $\langle \vec{x} \mid f(\vec{y}) \rangle = 0$, et donc $\langle f(\vec{x}) \mid \vec{y} \rangle = 0$. D'où, $f(\vec{x}) \perp \vec{y}$. Ainsi, $f(\vec{x}) \in F^\perp$, d'où $F^\perp$ est stable par f. □

Proposition : Soit f une isométrie vectorielle de E, et soit f un sous-espace vectoriel de E. Si F est stable par f, alors $F^\perp$ est aussi stable par f.

Preuve :
On suppose, pour tous vecteurs $\vec{u}$ et $\vec{v}$, $\langle f(\vec{u}) \mid f(\vec{v}-\rangle = \langle \vec{u} \mid \vec{v}\rangle$, et pour tout vecteur $\vec{x} \in F$, $f(\vec{x}) \in F$. Soit $\vec{x} \in F^\perp$. Soit $\vec{y_0} \in F$. Comme f est bijective, il existe $\vec{y} \in F$ tel que $f(\vec{y_0}) = \vec{y}$. Ainsi $\langle f(\vec{x}) \mid \vec{y_0}\rangle = \langle f(\vec{x}) \mid f(\vec{y})\rangle = \langle \vec{x}|\vec{y}\rangle = 0$. D'où, $f(\vec{x}) \perp \vec{y_0}$. Ainsi, $f(\vec{x}) \in F^\perp$, d'où $F^\perp$ est stable par f. □

Proposition : Un sous-espace vectoriel F de E est stable par f si, et seulement si, $F^\perp$ est stable par $f^\star$.

Preuve : $\Longrightarrow$ On suppose, pour tout $\vec{x} \in F$, $f(\vec{x}) \in F$. Soit $\vec{y} \in F^\perp$, et soit $\vec{x} \in F$. Par définition de l'adjoint, $\langle f^\star(\vec{y}) \mid \vec{x}\rangle = \langle \vec{y} \mid f(\vec{x})\rangle$. Or, $f(\vec{x}) \in F$ par hypothèse, et $\vec{y} \in F^\perp$. D'où $f^\star(\vec{y}) \perp \vec{x}$, et donc $f^\star(\vec{y}) \in F^\perp$.

$\Longleftarrow$ On applique le cas précédent avec $G = F^\perp$, et $g = f^\star$. En effet, $G^\perp = F^{\perp\perp} = F$, car E de dimension fini, et $g^\star = f^{\star\star} = f$.

□

VII.5 Le théorème spectral

Lemme : Soit $f : E \to E$ un endomorphisme autoadjoint.

1. Les sous-espaces propres de f sont deux à deux orthogonaux. Autrement dit, si deux vecteurs propres sont associés à des valeurs propres distinctes, alors ils sont orthogonaux.
2. Les valeurs propres de f sont toutes réelles $\mathrm{Sp}_{\mathbb{C}}(f) \subset \mathbb{R}$.

Ce lemme reste valide en replaçant l'endomorphisme autoadjoint f par la matrice réelle symétrique A.

B Attention, E doit être un $\mathbb{R}$-espace vectoriel ; la matrice A doit être à coefficients réels. Sinon, les résultats du cours ne s'appliquent pas.

Preuve :
On suppose f autoadjoint (H) : pour tous vecteurs $\vec{u}$ et $\vec{v}$, $\langle f(\vec{u}) \mid \vec{v}\rangle = \langle \vec{u} \mid f(\vec{v})\rangle$. Soient deux vecteurs $\vec{u}$ et $\vec{v}$ tels que $f(\vec{u}) = \lambda\vec{u}$ et $f(\vec{v}) = \mu\vec{v}$

avec $\lambda \neq \mu$. Montrons $u \perp v$.

$$\begin{aligned} \langle f(\vec{u}) \mid \vec{v} \rangle &= \langle \lambda \vec{u} \mid \vec{v} \rangle = \lambda \langle \vec{u} \mid \vec{v} \rangle \\ \text{(H)} &= \langle \vec{u} \mid f(\vec{v}) \rangle = \langle \vec{u} \mid \mu \vec{v} \rangle = \mu \langle \vec{u} \mid \vec{v} \rangle . \end{aligned}$$

D'où, par différence $(\lambda - \mu) \langle \vec{u} \mid \vec{v} \rangle = 0$. Comme $\lambda \neq \mu$, on en conclut que $\langle \vec{u} \mid \vec{v} \rangle = 0$ d'où $\vec{u} \perp \vec{v}$.

Pour montrer 2., on utilise les matrices : dans une base $\mathscr{B}$ orthonormée de E, soit $A \in \mathcal{S}_n(\mathbb{R})$ la matrice de f dans $\mathscr{B}$. Soit $X \in \mathscr{M}_{n,1}(\mathbb{C})$ un vecteur propre associé de A, et soit $\lambda \in \mathbb{C}$ sa valeur propre (complexe) associée. Ainsi, $X \neq 0_{\mathscr{M}_{n,1}(\mathbb{C})}$, et $A \cdot X = \lambda X$. Montrons $\lambda = \bar{\lambda}$. On calcule $\bar{X}^\top \cdot (A \cdot X) = \bar{X}^\top \cdot \lambda X = \lambda \bar{X}^\top \cdot X$ Or,

$$\bar{X}^\top \cdot X = \begin{pmatrix} \bar{z}_1 & \bar{z}_2 & \dots & \bar{z}_n \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = |z_1|^2 + |z_2|^2 + \cdots + |z_n|^2.$$

C'est un réel strictement positif (en effet, s'il était nul, X serait nul). Autre calcul,

$$\begin{aligned} \bar{X}^\top \cdot A \cdot X = \left(\bar{X}^\top \cdot A \cdot X\right)^\top & \\ &= X^\top \cdot A^\top \cdot (\bar{X}^\top)^\top \\ &= X^\top \cdot A \cdot \bar{X} \text{ car } A \in \underline{\mathcal{S}_n}(\mathbb{R}) \\ &= \overline{\bar{X}^\top \cdot \bar{A} \cdot X} \\ &= \overline{\bar{X}^\top \cdot A \cdot X} \text{ car } A \in \mathcal{S}_n(\underline{\mathbb{R}}) \end{aligned}$$

D'où, $\bar{X}^\top \cdot A \cdot X \in \mathbb{R}$. Mais, $\bar{X}^\top \cdot A \cdot X = \lambda \left(|z_1|^2 + \cdots + |z_n|^2\right)$. Comme $\left(|z_1|^2 + \cdots + |z_n|^2\right) \neq 0$, d'où $\lambda \in \mathbb{R}$. □

Théorème (Théorème spéctral – endomorphismes) **:** Un endomorphisme f d'un espace euclidien E est autoadjoint si, et seulement s'il est diagonalisable dans une base orthonormée. Autrement dit, si, et seulement s'il existe une base orthonormée de E formée de vecteurs propres de f. Ou encore, si, et seulement si E est la somme orthogonale des sous-espaces propres de f.

Preuve (Par récurrence sur $n = \dim E$) *:*

Initialisation Pour $n = 1$, soit $\vec{v} \in E$ un vecteur non nul, alors la base

$\left(\frac{\vec{v}}{\|\vec{v}\|}\right)$ convient.

Hérédité Soit $n \geqslant 1$. On suppose le théorème vrai en dimension n. Soit $f : E \to E$ un endomorphisme autoadjoint d'un espace euclidien E de dimension $n+1$. Soit $\chi_f(X)$ le polynôme caractéristique de f. Il est de degré $n+1$, il a donc au moins une racine complexe λ. D'où, l'endomorphisme f a au moins une valeur propre $\lambda \in \mathbb{C}$. D'après le lemme précédent, on sait maintenant que $\lambda \in \mathbb{R}$. Il existe $\vec{u} \in E$ un vecteur non nul tel que $f(\vec{u}) = \lambda\vec{u}$. La droite $\mathrm{Vect}(\vec{u})$ est stable par f. Par stabilité de l'orthogonal, $\mathrm{Vect}(\vec{u})^\perp$ est aussi stable par f. Or, on a $\dim[\mathrm{Vect}\,\vec{u}]^\perp = n$. On s'intéresse alors à l'endomorphisme induit à $\mathrm{Vect}(\vec{u})^\perp$: $f\big|_{\mathrm{Vect}(\vec{u})^\perp} = g$. Or, pour tous vecteurs $\vec{x}$ et $\vec{y}$ de $\mathrm{Vect}(\vec{u})^\perp$, $\langle g(\vec{x}) \mid \vec{y}\rangle = \langle f(\vec{x}) \mid \vec{y}\rangle = \langle \vec{x} \mid f(\vec{y})\rangle = \langle \vec{x} \mid g(\vec{y})\rangle$. D'où, l'endomorphisme g est autoadjoint, on applique l'hypothèse de récurrence (*i.e.* le théorème spectral) à g. Ainsi, $\left(\frac{\vec{u}}{\|\vec{u}\|}, \vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n\right)$ est une base orthonormée de E formée de vecteurs propres de f, où $(\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n)$ est une base orthonormée de $\mathrm{Vect}(\vec{u})^\perp$ formée de vecteurs propres de f.

Le théorème spectral est donc vrai pour tout espace vectoriel de dimension finie n. □

Corollaire (Théorème spéctral – matrices) **:** Si une matrice $A \in \mathcal{S}_n(\mathbb{R})$ est symétrique réelle, alors il existe une matrice orthogonale $P \in \mathrm{O}_n(\mathbb{R})$ telle que $P^{-1} \cdot A \cdot P = P^\top \cdot A \cdot P$ est diagonale. Autrement dit, toute matrice symétrique réelle est orthogonalement diagonalisable :

$$A \in \mathcal{S}_n(\mathbb{R}) \qquad \Longrightarrow \qquad \exists P \in \mathrm{O}_n(\mathbb{R}),\ P^{-1} \cdot A \cdot P \text{ diagonale.}$$

Preuve :
Soit f l'endomorphisme représenté par A dans une base orthonormée $\mathscr{B}$. La matrice A étant symétrique, d'où l'endomorphisme f est autoadjoint. On applique le théorème précédent à f : soit $\mathscr{B}'$ une base orthonormée dans laquelle f est diagonal. Soit alors P la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$: la matrice $D = P^{-1} \cdot A \cdot P$ est diagonale, et la matrice P est orthogonale car c'est la matrice de passage d'une base orthonormée $\mathscr{B}$ vers une autre base orthonormée $\mathscr{B}'$. □

Définition : On dit d'un endomorphisme autoadjoint $f \in \mathcal{S}(E)$ qu'il est :

1. *positif* si $\forall \vec{x} \in E$, $\langle \vec{x} \mid f(\vec{x})\rangle \geqslant 0$;
2. *défini positif* s'il est positif, et que $\forall \vec{x} \in E$, si $\langle \vec{x} \mid f(\vec{x})\rangle = 0$, alors $\vec{x} = \vec{0}$. Autrement dit, si

$$\forall \vec{x} \in E \setminus \{\vec{0}\}, \quad \langle \vec{x} \mid f(\vec{x})\rangle > 0.$$

De même, on dit d'une matrice $A \in \mathcal{S}_n(\mathbb{R})$, qu'elle est :

1. *positive* si $\forall X \in \mathcal{M}_{n,1}(\mathbb{R})$, $X^\top \cdot M \cdot X \geqslant 0$;
2. *définie positive* si elle est positive, et que $\forall X \in \mathcal{M}_{n,1}(\mathbb{R})$, si $X^\top \cdot M \cdot X = 0$, alors $X = 0$. Autrement dit, si

$$\forall X \in \mathcal{M}_{n,1}(\mathbb{R}) \setminus \{0_{\mathcal{M}_{n,1}(\mathbb{R})}\}, \quad X^\top \cdot M \cdot X > 0.$$

On note $\mathcal{S}^+(E)$ l'ensemble des endomorphismes autoadjoints positifs, et $\mathcal{S}^{++}(E)$ l'ensemble des endomorphismes autoadjoints définis positifs De même, on note $\mathcal{S}_n^+(\mathbb{R})$ l'ensemble des matrices symétriques positives, et $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques définies positives.

Théorème : Un endomorphisme autoadjoint est :

1. positif, si, et seulement si toutes ses valeurs propres sont positives ;
2. défini positif si, et seulement si toutes ses valeurs propres sont strictement positives.

Ainsi, on a

$$\begin{array}{rcll} f \in \mathcal{S}^+(E) & \iff & f \in \mathcal{S}(E) & \text{et} \quad \mathrm{Sp}(f) \subset \mathbb{R}^+, \\ f \in \mathcal{S}^{++}(E) & \iff & f \in \mathcal{S}(E) & \text{et} \quad \mathrm{Sp}(f) \subset \mathbb{R}_\star^+, \\ M \in \mathcal{S}_n^+(\mathbb{R}) & \iff & M \in \mathcal{S}_n(\mathbb{R}) & \text{et} \quad \mathrm{Sp}(M) \subset \mathbb{R}^+, \\ M \in \mathcal{S}_n^{++}(\mathbb{R}) & \iff & M \in \mathcal{S}_n(\mathbb{R}) & \text{et} \quad \mathrm{Sp}(M) \subset \mathbb{R}_\star^+. \end{array}$$

Tarte à la *double* crème

Preuve : "1$\Longrightarrow$" On suppose $f \in \mathcal{S}^+$, *i.e.* pour tout vecteur $\vec{x}$, $\langle \vec{x} \mid f(\vec{x}) \rangle \geqslant 0$. Soit $\lambda \in \mathrm{Sp}(f)$: il existe un vecteur $\vec{u}$ non nul tel que $f(\vec{u}) = \lambda \vec{u}$. D'où, par hypothèse,

$$0 \leqslant \langle \vec{u} \mid f(\vec{u}) \rangle = \langle \vec{u} \mid \lambda \vec{u} \rangle = \lambda \langle \vec{u} \mid \vec{u} \rangle .$$

Or, $\langle \vec{u} \mid \vec{u} \rangle > 0$. D'où, $\lambda \geqslant 0$.

"$\Longleftarrow$" Supposons $\mathrm{Sp}(f) \subset \mathbb{R}_+$ et $f \in \mathcal{S}(E)$. On veut montrer que $f \in \mathcal{S}^+(E)$, *i.e.* pour tout vecteur $\vec{x}$, $\langle \vec{x} \mid f(\vec{x}) \rangle \geqslant 0$. On se place dans une base adaptée, grâce à la seconde hypothèse. En effet, d'après le théorème spectral, il existe une base orthonormée $\mathcal{B}$ de E formée de vecteurs propres de f. On pose $\mathcal{B} = (\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n)$, cette base. Soit $\vec{x} \in E$: on pose $\vec{x} = x_1\vec{\varepsilon}_1 + x_n\vec{\varepsilon}_2 + \cdots + x_n\vec{\varepsilon}_n$. Ainsi,

$$f(\vec{x}) = x_1 f(\vec{\varepsilon}_1) + x_2 f(\vec{\varepsilon}_2) + \cdots + x_n f(\vec{\varepsilon}_n) = x_1\lambda_1\vec{\varepsilon}_1 + x_2\lambda_2\vec{\varepsilon}_2 + \cdots + x_n\lambda_n\vec{\varepsilon}_n.$$

D'où, $\langle \vec{x} \mid f(\vec{x}) \rangle = \lambda_1 x_1^2 + \lambda_2 x_2^2 + \cdots + \lambda_n x_n^2$. Or, $\forall i \in [\![1, n]\!]$, $\lambda_i \geqslant 0$ par hypothèse. D'où $\langle \vec{x} \mid f(\vec{x}) \rangle \geqslant 0$.

"2$\Longrightarrow$" On suppose $f \in \mathcal{S}^{++}$, *i.e.* pour tout vecteur $\vec{x}$, $\langle \vec{x} \mid f(\vec{x}) \rangle > 0$. Soit $\lambda \in \mathrm{Sp}(f)$: il existe un vecteur $\vec{u}$ non nul tel que $f(\vec{u}) = \lambda \vec{u}$.

D'où, par hypothèse,

$$0 < \langle \vec{u} \mid f(\vec{u}) \rangle = \langle \vec{u} \mid \lambda \vec{u} \rangle = \lambda \langle \vec{u} \mid \vec{u} \rangle .$$

Or, $\langle \vec{u} \mid \vec{u} \rangle > 0$. D'où, $\lambda > 0$.

" $\Longleftarrow$ " Supposons $\mathrm{Sp}(f) \subset \mathbb{R}_+^\star$ et $f \in \mathcal{S}(E)$. On veut montrer que $f \in \mathcal{S}^{++}(E)$, *i.e.* pour tout vecteur $\vec{x}$ non nul, $\langle \vec{x} \mid f(\vec{x}) \rangle > 0$. On se place dans une base adaptée, grâce à la seconde hypothèse. En effet, d'après le théorème spectral, il existe une base orthonormée $\mathcal{B}$ de E formée de vecteurs propres de f. On pose $\mathcal{B} = (\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n)$, cette base. Soit $\vec{x} \in E$ un vecteur non nul : on pose $\vec{x} = x_1\vec{\varepsilon}_1 + x_n\vec{\varepsilon}_2 + \cdots + x_n\vec{\varepsilon}_n$. Ainsi,

$$f(\vec{x}) = x_1 f(\vec{\varepsilon}_1) + x_2 f(\vec{\varepsilon}_2) + \cdots + x_n f(\vec{\varepsilon}_n) = x_1\lambda_1\vec{\varepsilon}_1 + x_2\lambda_2\vec{\varepsilon}_2 + \cdots + x_n\lambda_n\vec{\varepsilon}_n.$$

D'où, $\langle \vec{x} \mid f(\vec{x}) \rangle = \lambda_1 x_1^2 + \lambda_2 x_2^2 + \cdots + \lambda_n x_n^2$. Or, $\forall i \in [\![1, n]\!]$, $\lambda_i > 0$ par hypothèse, et il existe $i \in [\![1, n]\!]$, tel que $x_i \neq 0$ car $\vec{x} \neq \vec{0}$. D'où $\langle \vec{x} \mid f(\vec{x}) \rangle > 0$.

□

VII.6 Rotations et réflexions

Définition : Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. On dit que deux bases $\mathcal{B}_0$ et $\mathcal{B}$ de E ont la même *orientation* si le déterminant de la matrice P de passage de $\mathcal{B}_0$ à $\mathcal{B}$ est positif :

$$\det P = \det_{\mathcal{B}_0}(\mathcal{B}) > 0.$$

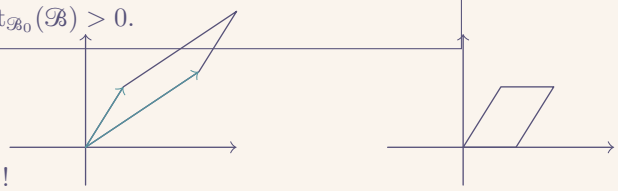


FIGURE 12.3 – Aire d'un parallélogramme

EXEMPLE :
On oriente le plan $\mathbb{R}^2$ en décidant que la base canonique $\mathcal{B}_0 = (\vec{\imath}, \vec{\jmath})$ est directe, puis on munit $\mathbb{R}^2$ du produit canonique : $\mathcal{B}_0$ est alors une base orthonormée directe de $\mathbb{R}^2$. Soient deux vecteurs $\vec{u} = a\,\vec{\imath} + b\,\vec{\jmath}$ et $\vec{v} = c\,\vec{\imath} + b\,\vec{\jmath}$. Le déterminant

$$\det(\vec{u}, \vec{v}) = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc$$

possède

- un signe (s'il est strictement positif, alors $(\vec{u}, \vec{v})$ est une base directe, s'il est strictement négatif, alors $(\vec{u}, \vec{v})$ est une base indirecte, s'il est nul alors $(\vec{u}, \vec{v})$ n'est pas une base car $\vec{u}$ et $\vec{v}$ sont liés) ;
- une valeur absolue, égale à l'aire du parallélogramme construit sur les vecteurs $\vec{u}$ et $\vec{v}$. Les trois parallélogrammes de la figure précédente ont la

même aire :

$$\big|\det(\vec{u},\vec{v})\big| = |ad-bc|.$$

Exemple :
On oriente l'espace $\mathbb{R}^3$ en décidant que la base canonique $\mathscr{B}_0 = (\vec{\imath},\vec{\jmath},\vec{k})$ est directe.

Définition : Soit E un espace euclidien de dimension n. Soit $\mathscr{B}$ une base orthonormée de E. On dit que

- f est une *rotation* si f est une isométrie de déterminant $+1$, autrement dit, si $\big[\, f \,\big]_{\mathscr{B}} \in \mathrm{SO}_n(\mathbb{R})$;
- f est une *réflexion* si f est une symétrie orthogonale par rapport à un hyperplan de E.

Remarque : 1. D'après la définition et les théorèmes précédents, on a les équivalences :

$$\begin{aligned} f \text{ est une rotation} &\iff f \text{ est une isométrie et } \det f = +1 \\ &\iff f \in \mathrm{O}(E) \text{ et } \det f = +1 \\ &\iff f \text{ conserve } \begin{cases} \text{le produit scalaire} \\ \text{et l'orientation} \end{cases} \\ &\iff f \text{ transforme une base orthonormée directe} \\ &\qquad\qquad \text{en une base orthonormée directe.} \end{aligned}$$

2. Les rotations de E forment un groupe, noté $\mathrm{SO}(E)$; c'est un sous-groupe de $\mathrm{O}(E)$ des isométries de E.
3. Si f est une réflexion par rapport à un hyperplan H de E, alors sa matrice dans une base adaptée à la somme directe $H \oplus H^\perp$ s'écrit

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & -1 \end{pmatrix}.$$

Ainsi, le déterminant d'une réflexion est donc toujours égal à -1. Et, la composée de deux réflexions est donc une rotation.

Théorème : Une matrice appartient à $\mathrm{O}_2(\mathbb{R})$ si, et seulement si elle est de la forme

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{ou} \qquad S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Son déterminant vaut $+1$ dans le premier cas, -1 dans le second.

La première matrice représente une rotation d'angle θ ; la seconde représente une symétrie par rapport à la droite d'angle $\theta/2$.

Preuve " $\Longrightarrow$ " Les colonnes des deux matrices forment une base de $\mathbb{R}^2$. D'où, $R_\theta \in \mathrm{O}_2(\mathbb{R})$ et $S_\theta \in \mathrm{O}_2(\mathbb{R})$.

" $\Longleftarrow$ " La matrice A est dans le groupe $\mathrm{O}_2(\mathbb{R})$, d'où

$$\begin{cases} a^2+b^2=1 & (1)\\ c^2+d^2=1 & (2)\\ ac+bd=0. & (3)\end{cases}$$

Il existe donc $\theta \in \mathbb{R}$ tel que $(a,b)=(\cos\theta,\sin\theta)$, d'après (1). De même, il existe $\varphi\in\mathbb{R}$, tel que $(c,d)=(\cos\varphi,\sin\varphi)$, d'après (2).

$$\begin{aligned}
&(3)\ \text{d'où } ab+cd=0\\
&\text{d'où } \cos\theta\cos\varphi+\sin\theta\sin\varphi=0\\
&\text{d'où } \cos(\theta-\varphi)=0\\
&\text{d'où } \theta-\varphi\equiv\frac{\pi}{2}\ [\pi]\\
&\text{d'où } \begin{cases}\exists k\in\mathbb{Z},\ \theta-\varphi=2k\pi+\frac{\pi}{2}\\ \text{ ou bien}\\ \exists k\in\mathbb{Z},\ \theta-\varphi=2k\pi-\frac{\pi}{2}\end{cases}\\
&\text{d'où } \begin{cases}\exists k\in\mathbb{Z},\ \theta=\varphi+\frac{\pi}{2}+2k\pi\\ \text{ ou bien}\\ \exists k\in\mathbb{Z},\ \theta=\varphi-\frac{\pi}{2}+2k\pi.\end{cases}\\
&\text{d'où } \begin{cases}A=R_\theta\\ \text{ ou bien}\\ A=S_\theta\end{cases}
\end{aligned}$$

□

Corollaire : Les isométries du plan sont les rotations (autour de l'origine) et les réflexions (par rapport à une droite passant par l'origine).

Remarque :
Pour tout $(\theta,\varphi)\in\mathbb{R}^2$, $R_\theta\cdot R_\varphi=R_{\theta+\varphi}=R_\varphi\cdot R_\theta$. Le groupe $\mathrm{SO}_2(\mathbb{R})$ est donc commutatif. De plus, l'application

$$\begin{aligned}\Phi:\mathbb{R}&\longrightarrow \mathrm{SO}_2(\mathbb{R})\\ \theta&\longmapsto R_\theta\\ \varphi&\longmapsto R_\varphi\\ \theta+\varphi&\longmapsto R_{\theta+\varphi}\end{aligned}$$

est un morphisme du groupe $(\mathbb{R},+)$ vers le groupe $(\mathrm{SO}_2(\mathbb{R}),\cdot\,)$. Ce morphisme est surjectif, mais pas injectif (car son noyau est $2\pi\,\mathbb{Z}$) : $\Phi(0)=\Phi(2\pi)=I_2$.

De plus, au lieu de repérer un point du plan par ses coordonnées $(x, y) \in \mathbb{R}^2$, on peut le repérer par son affixe $z = x + iy \in \mathbb{C}$.

(a) Après une rotation, la position du point M' sera repérée par les coordonnées

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = S_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix} \qquad \Longleftrightarrow \qquad z' = \mathrm{e}^{i\theta} \cdot z.$$

En effet, $z' = \mathrm{e}^{i\theta} \cdot z \iff x' + iy' = (\cos\theta + i\sin\theta)(x + iy) = (x\cos\theta - y\sin\theta) + i(x\sin\theta + y\cos\theta)$, et

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = R_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

Ainsi, l'application

$$\begin{aligned} \Psi : \mathbb{U} &\longrightarrow \mathrm{SO}_2(\mathbb{R}) \\ \mathrm{e}^{i\theta} &\longmapsto R_\theta \end{aligned}$$

est un isomorphisme de groupes (*i.e.* un morphisme de groupe bijectif).

(b) Après une symétrie, la position du point M' sera repérée par les coordonnées

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = R_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix} \qquad \Longleftrightarrow \qquad z' = \mathrm{e}^{i\theta} \cdot \bar{z}.$$

En effet, $z' = \mathrm{e}^{i\theta} \cdot \bar{z} \iff x' + iy' = (\cos\theta + i\sin\theta)(x - iy) = (x\cos\theta + y\sin\theta) + i(x\sin\theta - y\cos\theta)$, et

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = S_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta + y\sin\theta \\ x\sin\theta - y\cos\theta \end{pmatrix}.$$

D'où,

$$S_\theta = \underbrace{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}}_{R_\theta} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{S_0}.$$

Théorème : Une application f est une isométrie de l'espace si, et seulement s'il existe un angle $\theta \in \mathbb{R}$ et une base orthonormée directe $\mathscr{B} = (\vec{u}, \vec{v}, \vec{w})$ tels que

$$\big[\, f \,\big]_{\mathscr{B}} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \\ f(\vec{u}) & f(\vec{v}) & f(\vec{w}) \end{pmatrix} \begin{matrix} \vec{u} \\ \vec{v} \\ \vec{w} \end{matrix}$$

ou

$$\big[\, f \,\big]_{\mathscr{B}} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & -1 \\ f(\vec{u}) & f(\vec{v}) & f(\vec{w}) \end{pmatrix} \begin{matrix} \vec{u} \\ \vec{v} \\ \vec{w} \end{matrix}$$

[]

Une isométrie f est, ou bien une rotation d'un angle θ autour de l'axe $\mathrm{Vect}(\vec{w})$, ou bien la composée d'une rotation d'angle θ autour de l'axe $\mathrm{Vect}(\vec{w})$ et d'une symétrie par rapport au plan $\mathrm{Vect}(\vec{u},\vec{v})$.

Preuve (tarte à la crème) *:*
Comme f est une isométrie, on a, pour tout vecteur $\vec{x} \in E$, $\|f(\vec{x})\| = \|\vec{x}\|$. Or, il existe un vecteur $\vec{x}$ non nul tel qu'il existe $\lambda \in \mathbb{R}$ tel que $f(\vec{x}) = \lambda\vec{x}$, d'où $\|\lambda\vec{x}\| = \|\vec{x}\|$, donc $|\lambda| \cdot \|\vec{x}\| = 1 \cdot \|\vec{x}\|$. On en déduit que $\lambda \in \{-1, 1\}$ car $\|\vec{x}\| \neq 0$. La suite de la démonstration est dans le poly. □

Théorème : Soit E un espace euclidien, et soit f une isométrie : E est la somme directe et orthogonale de $\mathrm{Ker}(\mathrm{id}_E - f)$, de $\mathrm{Ker}(-\mathrm{id}_E - f)$, et/ou de plans P_i stables par f sur lesquels f induit une rotation.

Corollaire : Si f est une isométrie d'un espace euclidien E, alors il existe $(p, q) \in \mathbb{N}^2$, des réels $\theta_1, \ldots, \theta_k$, et une base $\mathcal{B}$ orthonormée de E tels que

$$[\, f \,]_{\mathcal{B}} = \begin{pmatrix} R_{\theta_1} & & & & \\ & \ddots & (0) & & \\ & (0) & R_{\theta_k} & & \\ & & & I_p & \\ & & & & -I_q \end{pmatrix}.$$

Chapitre 13

Espaces vectoriels normés

VII.1 Normes et distances

Définition : Soit E un $\mathbb{R}$ ou $\mathbb{C}$-espace vectoriel. Une application $N : E \to \mathbb{R}^+$ est appelée une *norme* si, pour tous vecteurs $\vec{x}$ et $\vec{y}$ de E, et pour tout scalaire $\alpha \in \mathbb{K}$, [1]

1. $N(\vec{x}) = 0 \implies \vec{x} = \vec{0}$, (axiome de séparation)
2. $N(\alpha\,\vec{x}) = |\alpha|\, N(\vec{x})$, (homogénéité, au sens physicien)
3. $N(\vec{x} + \vec{y}) \leqslant N(\vec{x}) + N(\vec{y})$. (inégalité triangulaire)

Un espace vectoriel muni d'une norme est appelé un *espace vectoriel normé* (*evn*).

Une norme peut-être définie sur un $\mathbb{C}$-espace vectoriel, même si un produit scalaire ne peut être défini que sur un $\mathbb{R}$-espace vectoriel. On note en général l'application N comme $\|\cdot\|$.

Exercice :

1. *La valeur absolue est une norme sur le $\mathbb{R}$-espace vectoriel $\mathbb{R}$: y en a-t-il d'autres ? Le module est une norme sur le $\mathbb{C}$-espace vectoriel $\mathbb{C}$: y en a-t-il d'autres ?*
2. *Par définition, toute norme N vérifie la propriété 3., appelée inégalité triangulaire. En déduire que*

$$\forall (\vec{x}, \vec{y}) \in E^2, \qquad |N(\vec{x}) - N(\vec{y})| \leqslant N(\vec{x} - \vec{y}).$$

1. Ici, $n = 1$, l'espace vectoriel normé est $\mathbb{K}^1 = \mathbb{R}$ ou $\mathbb{C}$. On vérifie bien les

1. $\mathbb{K}$ correspond à $\mathbb{R}$ ou $\mathbb{C}$, le corps associé à l'espace vectoriel.

hypothèses pour que la valeur absolue (resp. module) :

$$\begin{aligned}
&\forall x \in \mathbb{K}, \qquad |x| = 0 \implies x = 0\\
&\forall \alpha \in \mathbb{K}, \forall x \in \mathbb{K}, \qquad |\alpha x| = |\alpha|\,|x|\\
&\forall (x,y) \in \mathbb{K}^2, \qquad |x+y| \leqslant |x| + |y|
\end{aligned}$$

Ce n'est pas la seule norme, on peut multiplier par un nombre k strictement positif, et la norme $x \mapsto k|x|$ obtenue est toujours une norme. Il n'y en a pas d'autres ; montrons le. Soit N une norme sur l'espace vectoriel $\mathbb{K}$. Pour tout $z \in \mathbb{C}$, $z = z \times 1$, d'où $N(z) = |z| \cdot N(1)$, et $N(1) > 0$.

2. (Tarte à la crème) Soit N une norme sur un espace vectoriel $\mathbb{K}$. Soient $\vec{x}$ et $\vec{y}$ deux vecteurs de E.

$$\begin{aligned}
&\big|N(\vec{x}) - N(\vec{y})\big| \leqslant N(\vec{x}-\vec{y})\\
\iff &-N(\vec{x}-\vec{y}) \leqslant N(\vec{x}) - N(\vec{y}) \leqslant N(\vec{x}-\vec{y})\\
\iff &\begin{cases} N(\vec{x}) \leqslant N(\vec{y}) + N(\vec{x}-\vec{y}) & (1)\\ N(\vec{y}) \leqslant N(\vec{x}) + N(\vec{x}-\vec{y}) & (2)\end{cases}
\end{aligned}$$

La propriété (1) est vraie car $\vec{x} = \vec{y} + (\vec{x}-\vec{y})$, et application de l'inégalité triangulaire. De même pour (2) en échangeant $\vec{x}$ et $\vec{y}$.

Sur le même espace vectoriel, on peut définir plusieurs normes.

Exemple : 1. Sur l'espace vectoriel $\mathbb{K}^n$ ($\mathbb{R}^n$ ou $\mathbb{C}^n$), avec $n \in \mathbb{N}^\star$, on définit trois normes classiques : soit $\vec{x} = (x_1, \dots, x_n) \in \mathbb{K}^n$,

$$\|\vec{x}\|_1 = |x_1| + \cdots + |x_n| \qquad \|\vec{x}\|_2 = |x_1|^2 + \cdots + |x_n|^2 \qquad \|\vec{x}\|_\infty = \max\big(|x_1|, \dots, |x_n|\big).$$

2. Sur l'espace vectoriel $\mathscr{C}([a,b], \mathbb{K})$ des fonctions f continues sur un segment $[a,b]$ vers $\mathbb{K}$,

$$\|f\|_1 = \int_a^b |f(t)|\,\mathrm{d}t \qquad \|f\|_2 = \int_a^b |f(t)|^2\,\mathrm{d}t \qquad \|f\|_\infty = \max_{t\in[a,b]} |f(t)|.$$

On définit la norme p-ième comme

$$\|\vec{x}\|_p = \sqrt[p]{\sum_{i=1}^n |x_i|^p} \xrightarrow[p\to+\infty]{} \|\vec{x}\|_\infty.$$

On a déjà montré que $\|\cdot\|_2$ est une norme au chapitre produit scalaire : par le caractère défini du produit scalaire canonique de $\mathbb{R}^n$, par la bilinéarité de ce produit scalaire, et par inégalité de Cauchy-Schwarz, on vérifie chacune des hypothèses de la norme. Pour les autres normes, on vérifie aisément les hypothèses, ce sont donc bien des normes.

Définition : La *distance* associée à une norme N est l'application

$$\begin{aligned} d : E^2 &\longrightarrow \mathbb{R}^+\\ (\vec{x}, \vec{y}) &\longmapsto N(\vec{y} - \vec{x}).\end{aligned}$$

(C'est une distance entre deux vecteurs.)

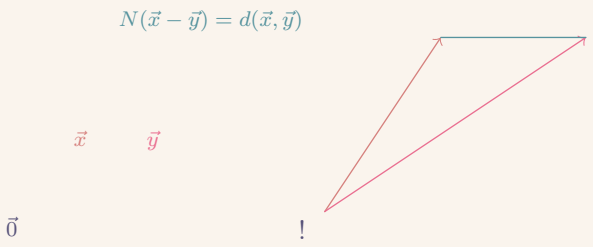


FIGURE 13.1 – Distance entre deux vecteurs $\vec{x}$ et $\vec{y}$

De la définition de *norme*, il en résulte les deux propriétés

1. $\forall(\vec{x},\vec{y}) \in E^2, \quad d(\vec{x},\vec{y}) = 0 \iff \vec{x} = \vec{y}$;
2. $\forall(\vec{x},\vec{y},\vec{z}) \in E^3, \quad d(\vec{x},\vec{z}) \leqslant d(\vec{x},\vec{y}) + d$

La distance entre deux fonctions est

— pour la norme infinie, il s'agit de la longt érence maximale entre les deux fonctions ;

— pour la norme 1, il s'agit de l'aire entre les de arbes.

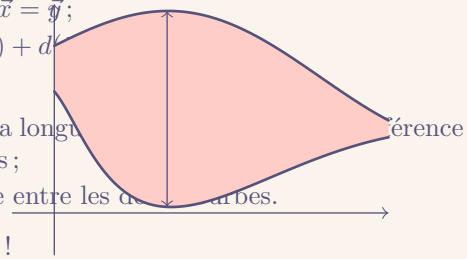


FIGURE 13.2 – Distance entre deux fonctions

REMARQUE :
Si une norme provient d'un produit scalaire, alors on dit que cette norme est *euclidienne*. Ce produit scalaire est alors unique (car on peut le calculer grâce aux égalités de polarisations) et cette norme vérifie l'égalité du parallélogramme.

Mais, certaines normes ne proviennent pas d'un produit scalaire, par exemple la norme infinie : $\|(x,y)\|_\infty = \max(|x|,|y|)$ sur l'espace $\mathbb{R}^2$. En effet, avec $\vec{u} = (2,1)$ et $(1,2)$, alors $\|\vec{u}+\vec{v}\|_\infty = 3$, $\|\vec{u}-\vec{v}\| = 1$, $\|\vec{u}\|_\infty = 2$ et $\|\vec{v}\|_\infty = 2$; mais,

$$\|\vec{u}+\vec{v}\|_\infty^2 + \|\vec{u}-\vec{v}\|_\infty^2 \neq 2\|\vec{u}\|_\infty^2 + 2\|\vec{v}\|_\infty^2.$$

L'égalité du parallélogramme n'est pas vérifiée.

VII.2 Boules

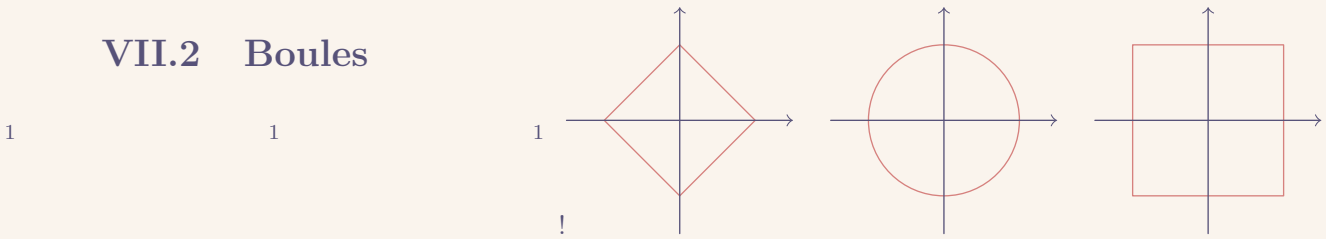


FIGURE 13.3 – Sphère de centre $\vec{0}$ et de rayon 1 pour les normes 1, 2 et ∞ de $\mathbb{R}^2$

Définition : Soit E un espace vectoriel normé par N. Soient $\vec{a}$ un vecteur de E, et $r > 0$. On appelle

1. *sphère* de centre $\vec{a}$ et de raton r la partie de E définie par
$$\{\vec{x} \in E \mid N(\vec{x} - \vec{a}) = r\} ;$$
2. *boule fermée* de centre $\vec{a}$ et de rayon r la partie de E définie par
$$\{\vec{x} \in E \mid N(\vec{x} - \vec{a}) \leqslant r\} ;$$
3. *boule ouverte* de centre $\vec{a}$ et de rayon r la partie de E définie par
$$\{\vec{x} \in E \mid N(\vec{x} - \vec{a}) < r\}.$$

On note $B(\vec{a}, r)$ la boule ouverte de centre $\vec{a}$ et de rayon r, la boule fermée est notée $\bar{B}(\vec{a}, r)$. La sphère est $\bar{B}(\vec{a}, r) \setminus B(\vec{a}, r)$.

Exercice :
Montrer que, pour tout vecteur $\vec{x}$ de $\mathbb{R}^2$,
$$\|\vec{x}\|_\infty \leqslant \|\vec{x}\|_2 \leqslant \|\vec{x}\|_1 \leqslant \sqrt{n} \cdot \|\vec{x}\|_2 \leqslant n \cdot \|\vec{x}\|_\infty.$$

Soit $\vec{x} \in \mathbb{R}^n$.

— On a $\|\vec{x}\|_\infty \leqslant \|\vec{x}\|_2$ car, pour $i \in [\![1, n]\!]$, $\sqrt{x_1^2 + \cdots + x_n^2} \geqslant \sqrt{x_i^2} = |x_i|$, d'où $\sqrt{x_1^2 + \cdots + x_n^2} \geqslant \max_{i \in [\![1,n]\!]}(|x_i|)$.
— On a $\|\vec{x}\|_2 \leqslant \|\vec{x}\|_1$ car $\sqrt{x_1^2 + \cdots + x_n^2} \leqslant |x_1| + \cdots + |x_n|$, car $x_1^2 + \cdots + x_n^2 \leqslant |x_1|^2 + \cdots + |x_n|^2 +$ tous les doubles produits, qui sont positifs.
— On a $\|\vec{x}\|_1 \geqslant \sqrt{n} \cdot \|\vec{x}\|_2$, car
$$\begin{aligned} |x_1| + \cdots + |x_n| &= \left\langle \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \middle| \begin{pmatrix} |x_1| \\ \vdots \\ |x_n| \end{pmatrix} \right\rangle \\ &\leqslant \sqrt{1^2 + 1^2 + \cdot + 1^2} \cdot \sqrt{|x_1|^2 + \cdots + |x_n|^2} \\ &= \sqrt{n} \cdot \sqrt{|x_1|^2 + \cdots + |x_n|^2} \end{aligned}$$
par inégalité de Cauchy-Schwarz.
— On a $\|\vec{x}\|_2 \leqslant \sqrt{n} \cdot \|\vec{x}\|_\infty$ car $\sqrt{x_1^2 + \cdots + x_n^2} \leqslant \sqrt{n} \cdot \max_{i \in [\![1,n]\!]} |x_i|$.

Définition : Soit E un espace vectoriel normé.

1. Une partie $A \subset E$ est *bornée* s'il existe $M \in \mathbb{R}$ tel que, pour tout vecteur $\vec{x} \in A$,
$$\|\vec{x}\| \leqslant M ;$$
2. une suite $u : \begin{array}{ccc} \mathbb{N} & \longrightarrow & E \\ n & \longmapsto & u_n \end{array}$ de vecteurs est *bornée* s'il existe $M \in \mathbb{R}$

tel que, pour tout $n \in \mathbb{N}$,

$$\|u_n\| \leqslant M \ ;$$

3. une fonction $f : \begin{array}{ccc} D & \longrightarrow & E \\ x & \longmapsto & f(x) \end{array}$ est *bornée* s'il existe M, tel que, pour tout $t \in D$,

$$\|f(t)\| \leqslant M.$$

Autrement dit, il existe M tel que

1. $A \subset \bar{B}(\vec{0}, M)$, 2. $\forall n \in \mathbb{N}, u_n \in \bar{B}(\vec{0}, M)$, 3. $f(D) \subset \bar{B}(\vec{0}, M)$.

VII.3 Limite d'une suite

Dans $\mathbb{R}$, pour dire qu'un nombre x tend vers un nombre a, on utilise la valeur absolue :

$$x \to a \iff x - a \to 0 \iff |x - a| \to 0.$$

De même, dans un espace vectoriel E, pour dire qu'un vecteur $\vec{x}$ tend vers un vecteur $\vec{a}$, on utilisera une norme :

$$\vec{x} \to \vec{a} \iff \vec{x} - \vec{a} \iff \|\vec{x} - \vec{a}\| \to 0 \iff \mathrm{d}(\vec{x}, \vec{a}) \to 0.$$

Définition : Soit E un espace vectoriel normé par $\|\cdot\|$. Soit $(\vec{u}_n)_{n\in\mathbb{N}}$ une suite d'éléments de E. Soit un vecteur $\vec{\ell} \in E$. On dit que $\vec{u}_n$ *tend vers* $\vec{\ell}$ si $\|\vec{u}_n - \vec{\ell}\|$ tend vers $0_{\mathbb{R}}$. Autrement dit, si

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N, \quad \|\vec{u}_n - \vec{\ell}\| \leqslant \varepsilon.$$

Proposition : Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de E.

1. (unicité de la limite) Il n'existe pas toujours de limite $\vec{\ell}$, mais, quand elle existe, elle est unique. On peut donc parler de *la* limite de $\vec{u}_n$, et écrire $\vec{\ell} = \lim_{n\to\infty} \vec{u}_n$.
2. (convergence $\implies$ bornée) Si la suite de vecteurs $(\vec{u}_n)$ converge, alors elle est bornée. La réciproque est fausse.

Preuve : 1. On suppose que $\vec{u}_n \to \vec{\ell}_1$, et $\vec{u}_n \to \vec{\ell}_2$ avec $\vec{\ell}_1 \neq \vec{\ell}_2$. Ainsi,

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N, \quad \|\vec{u}_n - \vec{\ell}_1\| \leqslant \varepsilon$$
$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N, \quad \|\vec{u}_n - \vec{\ell}_2\| \leqslant \varepsilon$$

On pose $\varepsilon = \frac{1}{3}\|\vec{\ell}_1 - \vec{\ell}_2\|$. D'où, pour tout $n \geqslant N$, $\|\vec{u}_n - \vec{\ell}_1\| \leqslant \varepsilon$ et $\|\vec{u}_n - \vec{\ell}_2\| \leqslant \varepsilon$, et donc $\|\vec{u}_n - \vec{\ell}_1\| + \|\vec{u}_n - \ell_2\| \leqslant 2\varepsilon = \frac{2}{3}\|\vec{\ell}_1 - \vec{\ell}_2\|$. Or, d'après l'inégalité triangulaire,

$$\|\vec{\ell}_1 - \vec{\ell}_2\| \leqslant \|\vec{u}_n - \vec{\ell}_1\| + \|\vec{u}_n - \vec{\ell}_2\| \leqslant \frac{2}{3}\|\vec{\ell}_1 - \vec{\ell}_2\|.$$

C'est absurde car $\|\vec{\ell}_1 - \vec{\ell}_2\| > 0$.

2. On suppose qu'il existe $\vec{\ell} \in E$ tel que $\vec{u}_n \to \vec{\ell}$, d'où,

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N, \quad \|\vec{u}_n - \vec{\ell}\| \leqslant \varepsilon.$$

On choisit $\varepsilon = 7$. Comme $\vec{u}_n = \vec{u}_n - \vec{\ell} + \vec{\ell}$, d'après l'inégalité triangulaire, on a

$$\forall n \geqslant N, \quad \|\vec{u}_n\| \leqslant \|\vec{u}_n - \vec{\ell}\| + \|\vec{\ell}\| \leqslant 7 + \|\vec{\ell}\|.$$

Soit $m = \max_{n \in [\![0,N]\!]} \|\vec{u}_n\|$. Alors,

$$\forall n \in \mathbb{N}, \qquad \|\vec{u}_n\| \leqslant m + 7 + \|\vec{\ell}\|.$$

□

Exercice :
La suite de fonctions $f_n : [0,1] \to \mathbb{R}$ représentée dans la figure 3 du poly est-elle bornée ? convergente ? (Utiliser la norme ∞ puis la norme 1 pour répondre.)

Avec la norme ∞, pour tout $n \in \mathbb{N}$,

$$\|f_n\|_\infty = \max_{t \in [0,1]} |f(t)| = 2n + 2 \xrightarrow[n \to +\infty]{} +\infty.$$

D'où, la suite $(f_n)_{n \in \mathbb{N}}$ n'est pas bornée. Et, cette suite n'est pas convergente car elle n'est pas bornée.

Avec la norme 1, pour tout $n \in \mathbb{N}$,

$$\|f_n\|_1 = \int_0^1 |f_n(t)|\ \mathrm{d}t = \frac{1}{2n+2} \times 2n + 2 = 1$$

car il s'agit de l'aire d'un triangle. La suite $(f_n)_{n \in \mathbb{N}}$ est donc bornée. Pour cette norme, la suite (f_n) est-elle convergente ? Autrement dit : existe-t-il une fonction $\ell \in \mathscr{C}([0,1], \mathbb{R})$ telle que $f_n \xrightarrow[n \to \infty]{} \ell$? *i.e.* telle que $\|f_n - \ell\|_1 \xrightarrow[n \to \infty]{} 0$. Non, la suite de fonctions (f_n) ne converge pas pour la norme 1. En effet, montrons le par l'absurde.

— Ou bien $\ell = 0$, alors $\|f_n - \ell\|_1 = \|f_n - 0\|_1 = \|f_n\|_1 = 1 \xrightarrow[n \to \infty]{\not}\ 0$.

— Ou bien $\ell \neq 0$, alors il existe $x \in [0,1]$, $f(x) \neq 0$. Il existe donc $x \in]0,1[$ tel que $f(x) \neq 0$. Soit alors $y = f(x)$. Il existe donc h tel que, pour tout $t \in [x-h, x+h]$, $\ell(t) \geqslant y/2$. Alors,

$$\|f_n - \ell\| \geqslant \frac{y}{2} \times 2h,$$

à partir d'un certain rang. D'où, $\|f_n - \ell\| \not\xrightarrow[n\to\infty]{} 0$.

REMARQUE (La norme infinie est la norme de la convergence uniforme) :
Si I est une partie de $\mathbb{R}$, alors l'ensemble E des fonctions bornées de I vers $\mathbb{R}$ ou $\mathbb{C}$ est un espace vectoriel, qu'on peut munir d'une norme

$$\forall f \in E, \quad \|f\|_\infty = \sup_{t\in I} |f(t)|.$$

Dans cet espace vectoriel normé E,

$$\begin{aligned} f_n \xrightarrow[n\to\infty]{} f &\iff \|f_n - f\|_\infty \xrightarrow[t\to\infty]{} 0 \\ &\iff \sup_{t\in I} |f_n(t) - f(t)| \xrightarrow[n\to\infty]{} 0 \\ &\iff \text{la suite de fonctions } (f_n)_{n\in\mathbb{N}} \text{ converge uniformément vers } f \text{ sur } I. \end{aligned}$$

Définition : Soit $(u_n)_{n\in\mathbb{N}}$ une suite de vecteurs de E. On dit qu'une suite (v_n) est *extraite* de (u_n) s'il existe une application $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que

$$\forall n \in \mathbb{N}, \qquad v_n = u_{\varphi(n)}.$$

La stricte croissance de φ implique que

$$\forall n \in \mathbb{N}, \qquad \varphi(n) \geqslant n.$$

Proposition : Si une suite converge, alors toute suite extraite converge vers la même limite.

Preuve :
On suppose $\vec{u} \xrightarrow[n\to\infty]{} \vec{\ell}$. D'où, $\|\vec{u}_n - \vec{\ell}\| \xrightarrow[n\to\infty]{} 0$, et donc

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N, \quad \|\vec{u}_n - \vec{\ell}\| \leqslant \varepsilon.$$

Soit $(\vec{v}_n) = (\vec{u}_{\varphi(n)})$ une suite extraite. On veut montrer que $\vec{v}_n \xrightarrow[n\to\infty]{} \vec{\ell}$.
Or, $\varphi(n) \geqslant n$, pour tout $n \in \mathbb{N}$, d'où $\varphi(n) \geqslant N$ pour $n \geqslant N$. D'où, $\|\vec{u}_{\varphi(n)} - \vec{\ell}\| \leqslant \varepsilon$ et donc $\|\vec{v}_n - \vec{\ell}\| \leqslant \varepsilon$. □

VII.4 Comparer des normes

Définition : Soient N et $\|\cdot\|$ deux normes sur un espace vectoriel E. On dit que ces deux normes sont *équivalentes* s'il existe deux réels α et β tels

que
$$\forall \vec{x} \in E, \qquad N(\vec{x}) \leqslant \alpha \cdot \|\vec{x}\| \quad \text{et} \quad \|\vec{x}\| \leqslant \beta \cdot N(\vec{x}).$$

Remarque : 1. Cette relation entre deux normes est une relation d'équivalence. En effet, elle est réflexive, symétrique et transitive.

2. Si deux normes sont équivalentes, alors ce qui converge pour l'une, converge aussi pour l'autre :
$$N(\vec{x} - \vec{a}) \to 0 \quad \Longleftrightarrow \quad \|\vec{x} - \vec{a}\| \to 0.$$
En effet, si $N(\vec{x}-\vec{a})$ tend vers 0, alors $\|\vec{x}-\vec{a}\|$ aussi : $\|\vec{x}-\vec{a}\| \leqslant \beta \cdot N(\vec{x}-\vec{a})$.
3. De même, être ou ne pas être borné est indépendant du choix de la norme, si les normes sont équivalentes.
4. Les trois normes classiques sur $\mathbb{R}^n$ sont équivalentes. En effet, on a
$$\forall \vec{x} \in \mathbb{R}^n, \qquad \|\vec{x}\|_\infty \leqslant \|\vec{x}\|_1 \leqslant n \cdot \|\vec{x}\|_\infty \quad \text{et} \quad \|\vec{x}\|_\infty \leqslant \|\vec{x}\|_2 \leqslant \sqrt{n}\|\vec{x}\|_\infty,$$
d'après l'exercice 7. Mais, ceci est faux dans l'espace $\mathscr{C}([0,1])$, d'après l'exercice 11.

Pour des normes équivalentes,
— la nature d'une suite ne dépend pas de la norme,
— la limite d'une suite ne dépend pas de la norme,
— le caractère borné d'une suite ne dépend pas de la norme.

Théorème : Sur un espace vectoriel de dimension **finie**, toutes les normes sont équivalentes.

Preuve :
Voir l'annexe B. □

Exercice :

1. *Soit E l'espace vectoriel de fonctions de $[0,1]$ vers $\mathbb{R}$ continues : $E = \mathscr{C}([0,1],\mathbb{R})$. Déterminer un réel α tel que*
$$\forall f \in E, \qquad \|f\|_1 \leqslant \alpha \|f\|_\infty.$$
2. *Pour tout $n \in \mathbb{N}$, on considère les fonctions f_n et g_n définies sur $[0,1]$ et représentées sur le poly. Étudier $\|f_n\|_1$ et $\|f_n\|_\infty$ ainsi que $\|g_n\|_1$ et $\|g_n\|_\infty$. Conclure.*

1. On sait que $\|f\|_1 = \int_0^1 |f(t)| \, \mathrm{d}t$. Et, $\forall t \in [0,1]$, $|f(t)| \leqslant \sup_{t\in[0,1]} |f(t)| = \|f\|_\infty$. D'où,
$$\begin{aligned}\|f\|_1 = \int_0^1 |f(t)| \, \mathrm{d}t &\leqslant \int_0^1 \|f\|_\infty \, \mathrm{d}t \\ &\leqslant (1-0) \times \|f\|_\infty\end{aligned}$$

2. On a $\|f_n\|_\infty = 1$ et $\|f_n\|_1 = \frac{1}{2n+2}$. De même, on a $\|g_n\|_\infty = 2n+2$, et $\|g_n\|_1 = 1$. On a déjà montré que $\|\cdot\|_1 \leqslant 1 \times \|\cdot\|_\infty$. On veut savoir s'il existe un réel β, tel que $\|\cdot\|_\infty \leqslant \beta \times \|\cdot\|_1$. Par l'absurde, supposons qu'il existe un réel β tel que $\|\cdot\|_\infty \leqslant \beta \times \|\cdot\|_1$. En particulier, $\|f_n\|_\infty \leqslant \beta \cdot \|f_n\|_1$, d'où $1 \leqslant \beta \times \frac{1}{2n+2}$. Les inégalités larges passent à la limite, d'où $1 \leqslant 0$, ce qui est absurde.

Corollaire (coordonnée par coordonnée) **:** Soit E un espace vectoriel de dimension **finie**, et soient $(\vec{u}_n)$ une suite de vecteurs de E et $\vec{\ell}$ un vecteur. La suite $(\vec{u}_n)$ tend vers $\vec{\ell}$ si, et seulement si, chaque coordonnée de $\vec{u}_n$ tend vers chaque coordonnée de $\vec{\ell}$.

Preuve :
Soit $\mathcal{B} = (\vec{e}_1, \dots, \vec{e}_d)$ une base de E. Soit N la norme de E définie comme

$$\begin{aligned} N : E &\longrightarrow \mathbb{R}^+ \\ x_1\vec{e}_1 + \cdots + x_d\vec{e}_d &\longmapsto \max(|x_1|, \dots, |x_d|) \end{aligned}$$

On veut montrer que $\vec{u}_n \to \vec{\ell}$ si, et seulement si, pour $i \in [\![1, d]\!]$, $x_i \to \ell_i$.

$$\begin{aligned} \vec{u}_n \xrightarrow[n\to+\infty]{} \vec{\ell} &\iff N(\vec{u}_n - \vec{\ell}) \xrightarrow[n\to\infty]{} 0 \\ &\iff \max(|u_{n,1} - \ell_1|, \dots, |u_{n,d} - \ell_d|) \xrightarrow[n\to\infty]{} 0 \\ &\iff \forall i \in [\![1, d]\!], \quad |u_{n,i} - \ell| \xrightarrow[n\to\infty]{} 0 \end{aligned}$$

□

Exercice :
On a $E = \mathcal{M}_{2,2}(\mathbb{R})$, espace de dimension finie. D'où, toutes les normes sur E sont équivalentes. En particulier, $A_n \to L$ si, et seulement si chaque élément de matrice de A_n tend vers chaque élément de matrice de L. Ici,

$$A_n = \begin{pmatrix} 1 & -a/n \\ a/n & 1 \end{pmatrix}^n.$$

On a

$$\begin{pmatrix} 1 & -\frac{a}{n} \\ \frac{a}{n} & 1 \end{pmatrix} = \sqrt{1+\frac{a^2}{n^2}} \cdot \underbrace{\begin{pmatrix} \frac{1}{\sqrt{1+a^2/n^2}} & \frac{-a/n}{\sqrt{1+a^2/n^2}} \\ \frac{a/n}{\sqrt{1+a^2/n^2}} & \frac{1}{\sqrt{1+a^2/n^2}} \end{pmatrix}}_{(C_1,C_2) \text{ b.o.n}} = \sqrt{1+\frac{a^2}{n^2}} \begin{pmatrix} \cos\theta_n & -\sin\theta_n \\ \sin\theta_n & \cos\theta_n \end{pmatrix}.$$

D'où,

$$A_n = \begin{pmatrix} 1 & -\frac{a}{n} \\ \frac{a}{n} & 1 \end{pmatrix}^n = \left(\sqrt{1+\frac{a^2}{n^2}}\right)^n \cdot \begin{pmatrix} \cos\theta_n & -\sin\theta_n \\ \sin\theta_n & \cos\theta_n \end{pmatrix}^n$$
$$= \left(\sqrt{1+\frac{a^2}{n^2}}\right)^n \cdot \begin{pmatrix} \cos(n\theta_n) & -\sin(n\theta_n) \\ \sin(n\theta_n) & \cos(n\theta_n) \end{pmatrix}$$

On veut montrer que

$$\begin{cases} \left(\sqrt{1+\frac{a^2}{n^2}}\right)^n \cos(n\theta_n) \xrightarrow[n\to\infty]{} \cos a, \\ \left(\sqrt{1+\frac{a^2}{n^2}}\right)^n \sin(n\theta_n) \xrightarrow[n\to\infty]{} \sin a. \end{cases}$$

On a $\left(\sqrt{1+\frac{a^2}{n^2}}\right)^n = \exp\left(n \ln \sqrt{1+\frac{a^2}{n^2}}\right)$. Or,

$$n \ln \sqrt{1+\frac{a^2}{n^2}} = \frac{1}{2} n \ln\left(1+\frac{a^2}{n^2}\right) = \frac{1}{2} n \left(\frac{a^2}{n^2} + \mathcal{o}\left(\frac{a^2}{n^2}\right)\right) = \frac{a^2}{2n} + \mathcal{o}\left(\frac{1}{n}\right) \xrightarrow[n\to\infty]{} 0.$$

D'où, $\left(\sqrt{1+\frac{a^2}{n^2}}\right)^n \xrightarrow[n\to\infty]{} 1$ par continuité de l'exponentielle. Il nous reste à montrer que $n\theta_n \xrightarrow[n\to\infty]{} a$, car, ensuite par continuité du cosinus et du sinus :

$$\begin{cases} \sin(n\theta_n) \xrightarrow[n\to\infty]{} \sin a \\ \cos(n\theta_n) \xrightarrow[n\to\infty]{} \cos a \end{cases}.$$

On a $\cos\theta_n = 1/\sqrt{1+a^2/n^2}$ et $\sin\theta_n = (a/n)/\sqrt{1+a^2/n^2}$. On a donc $\sin\theta_n \to 0$, d'où $\sin\theta_n \to 0$ par continuité de Arcsin, d'où $\sin\theta_n \sim \theta_n$. Et, donc

$$\theta_n \underset{n\to\infty}{\sim} \frac{a/n}{\sqrt{1+\frac{a^2}{n^2}}}.$$

D'où, $n\theta_n \sim a/\sqrt{1+a^2/n^2} \xrightarrow[n\to\infty]{} a$.

VII.5 Adhérence

Définition : Soit A une partie de E, un espace vectoriel. On dit qu'un vecteur $\vec{\ell} \in E$ est *adhérent* à A, si toute boule centrée en $\vec{\ell}$ rencontre A :

$$\forall \varepsilon > 0, \qquad B(\vec{\ell}, \varepsilon) \cap A \neq .$$

L'*adhérence* de A, notée $\bar{A}$, est l'ensemble des vecteurs adhérents à A.

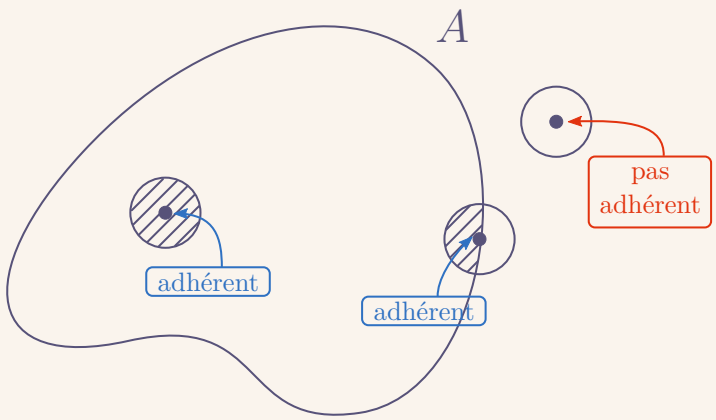


FIGURE 13.4 – Point adhérent

On a toujours $A \subset \bar{A}$, mais pas forcément $\bar{A} \subset A$ (*c.f.* exemple ci-après).

EXEMPLE : — Soient $I = [0,1]$, $J =]0,1]$ et $K =]0,+\infty[$ trois intervalles de $\mathbb{R}$. On a $\bar{I} = I$, $\bar{J} = I$ et $\bar{K} = [0,+\infty[$.

— L'adhérence $\overline{B(\vec{a},r)}$ d'une boule ouverte $B(\vec{a},r)$ est la boule fermée de même centre $\vec{a}$ et de même rayon r : $\bar{B}(\vec{a},r)$.

Proposition (Caractérisation séquentielle de l'adhérence) **:** Un vecteur $\vec{\ell} \in E$ est adhérent à $A \subset E$ si, et seulement si $\vec{\ell}$ est la limite d'une suite $(\vec{u}_n)_{n\in\mathbb{N}}$ d'éléments de A.

Preuve :

" $\Longrightarrow$ " On suppose qu'il existe une suite $(\vec{u}_n)_{n\in\mathbb{N}}$ de A telle que $\vec{u}_n \to \vec{a}$. Soit $\varepsilon > 0$. Comme $\vec{u}_n \to \vec{a}$ (par hypothèse), il existe un rang $N \in \mathbb{N}$ tel que, pour tout $n \geqslant N$, $\|\vec{u}_n - \vec{a}\| < \varepsilon$. D'où, $\vec{u}_n \in B(\vec{a},\varepsilon)$. Or, par hypothèse, $\vec{u}_n \in A$. On en déduit que

$$B(\vec{a},\varepsilon) \cap A \neq .$$

" $\Longleftarrow$ " Réciproquement, on suppose que, pour tout $\varepsilon > 0$, $B(\vec{a},\varepsilon) \cap A \neq .$ Soit $n \in \mathbb{N}^\star$ et soit $\varepsilon = \frac{1}{n}$. D'où, par hypothèse, $B(\vec{a},\varepsilon) \cap A \neq .$ On choisit un élément $\vec{u}_n \in B(\vec{a},\varepsilon) \cap A$, qui est non vide. D'où, $\vec{u}_n \in A$ et $\|\vec{u}_n - \vec{a}\| < \frac{1}{n}$. Ainsi, pour tout $n \in \mathbb{N}$, $\vec{u}_n \in A$ et $\vec{u}_n \to \vec{a}$.

□

Définition : Soit A une partie d'un espace vectoriel E. On dit que A est *dense* dans E si $\bar{A} = E$. Autrement dit, tout vecteur de E est adhérent à A. Ou encore, tout vecteur de E est la limite d'une suite de vecteurs de A.

Rappel (Caractère archimédien de $\mathbb{R}$) :
Pour tout $\varepsilon \in \mathbb{R}_\star^+$, il existe un entier $n \in \mathbb{N}$ tel que $n \cdot \varepsilon > 1$.

Rappel (Théorème d'approximation de Weierstrass) :
Si $f \in \mathscr{C}([a,b])$, il existe une suite $(P_n)_{n\in\mathbb{N}}$ de polynômes convergent uniformément vers f sur $[a,b]$:

$$0 \xleftarrow[\infty\leftarrow n]{} \|P_n - f\|_\infty = \sup_{t\in[a,b]} \big|P_n(t) - f(t)\big| \xrightarrow[n\to\infty]{} 0.$$

Tartes à la crème

Exemple : 1. $\mathbb{Q}$ est dense dans $\mathbb{R}$, et $\mathbb{R}\setminus\mathbb{Q}$ est dense dans $\mathbb{R}$.

2. D'après le théorème d'approximation de Weierstrass, l'ensemble des fonctions polynomiales est dense dans l'espace vectoriel $\mathscr{C}([a,b])$ des fonctions continues sur un segment muni de la norme infinie (par la caractérisation séquentielle de l'adhérence).

Exercice :
Montrer que l'ensemble $\mathrm{GL}_n(\mathbb{K})$ *des matrices inversibles est dense dans* $\mathscr{M}_{n,n}(\mathbb{K})$.

Montrons que toute matrice est la limite d'une suite de matrices inversibles. Soit $A \in \mathscr{M}_{n,n}(\mathbb{K})$ une matrice carrée. Soit $(B_p)_{p\in\mathbb{N}^\star}$ la suite matrice définie comme

$$\forall p \in \mathbb{N}^\star, \qquad B_p = A - \frac{1}{p} I_n.$$

D'une part, $B_p \xrightarrow[p\to\infty]{} A$, car $\|B_p - A\| \to 0_\mathbb{R}$ en choisissant une norme (peu importe laquelle car l'espace vectoriel $\mathscr{M}_{n,n}(\mathbb{K})$ est de dimension finie) ; en particulier, $B_p \to A$ si, et seulement si chaque élément de B_p tend vers A. D'autre part, à partir d'un certain rang, toutes les matrices B_p sont inversibles, car $\det B_p \neq 0$, car $\det\left(A - \frac{1}{p} I_n\right) \neq 0$, car $\chi_A\left(\frac{1}{p}\right) \neq 0$, car le polynôme χ_A n'a pas infinité de racines.

VII.6 Limite d'une fonction

Définition : Soient E et F deux espaces vectoriels normés. Soit f la fonction définie comme

$$\begin{aligned} f : D &\longrightarrow F \\ \vec{x} &\longmapsto f(\vec{x}) \end{aligned}$$

où $D \subset E$ est une partie de E. Soit $\vec{a}$ un point adhérent à D et $\vec{\ell} \in F$. On

dit que $f(\vec{x})$ *tend vers* $\vec{\ell}$ *quand* $\vec{x}$ *tend vers* $\vec{a}$, et on note $f(\vec{x}) \xrightarrow[\vec{x}\to\vec{a}]{} \vec{\ell}$ si

$$\left\|f(\vec{x}) - \vec{\ell}\right\| \xrightarrow[\|\vec{x}-\vec{a}\|\to 0]{} 0.$$

Autrement dit,

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall \vec{x} \in D,\quad \|\vec{x} - \vec{a}\| \leqslant \delta \implies \|f(\vec{x}) - \vec{\ell}\| \leqslant \varepsilon.$$

Avec cette définition, on a l'équivalence :

$$\begin{aligned} f(\vec{x}) \xrightarrow[\vec{x}\to\vec{a}]{} \vec{\ell} &\iff f(\vec{x}) - \vec{\ell} \xrightarrow[\vec{x}-\vec{a}\to\vec{0}]{} \vec{0} \\ &\iff \|f(\vec{x}) - \vec{\ell}\| \xrightarrow[\|\vec{x}-\vec{a}\|\to 0]{} 0 \end{aligned}$$

Remarque : 1. Il y a un abus de notation, la norme $\|\vec{x} - \vec{a}\|$ est une norme sur E tandis que $\|f(\vec{x}) - \vec{\ell}\|$ est une norme sur F.

2. Il 'existe pas toujours de limite $\vec{\ell}$, mais, quand elle existe, elle est unique. On peut donc parler de **la** limite de f en $\vec{a}$ et écrire $\vec{\ell} = \lim_{\vec{x}\to\vec{a}} f(\vec{x})$ ou $\vec{\ell} = \lim_{\vec{a}} f$.

Proposition (Caractérisation séquentielle de la limite) **:** Le vecteur $f(\vec{x})$ tend vers $\vec{\ell}$ quand $\vec{x}$ tend vers $\vec{a}$ si, et seulement si, pour toute suite $(\vec{u}_n)_{n\in\mathbb{N}}$ convergent vers $\vec{a}$, la suite $f(\vec{u}_n)$ tend vers $\vec{\ell}$.

Exercice :
Soient les fonctions définies de $\mathbb{R}^2 \setminus \{(0,0)\}$ *vers* $\mathbb{R}$ *par*

$$f(x,y) = \frac{xy}{x^2+y^2} \qquad \text{et} \qquad g(x,y) = \frac{xy}{\sqrt{x^2+2y^2}}$$

possèdent-elles une limite quand (x,y) *tend vers* $(0,0)$ *?*

Étude de *f*. On a $f(x,x) = \frac{xx}{x^2+x^2} = \frac{1}{2} \xrightarrow[x\to 0]{} \frac{1}{2}$, et $f(x,0) = \frac{x\times 0}{x^2+0^2} = 0 \xrightarrow[x\to 0]{}$. Or $0 \neq \frac{1}{2}$. D'où, par unicité de la limite, il n'y a pas de limite.

Autre rédaction, on a $f\left(\frac{1}{n}, \frac{1}{n}\right) = \frac{1}{2} \xrightarrow[n\to\infty]{} \frac{1}{2}$ et $f\left(\frac{1}{n}, 0\right) = 0 \xrightarrow[n\to\infty]{} 0$.

Étude de *g*. Pour tout couple $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$,

$$0 \leqslant |f(x,y)| = \frac{|x|\,|y|}{\sqrt{x^2+y^2}} \leqslant \frac{\|(x,y)\|_2^2}{\|(x,y)\|_2} = \|(x,y)\|_2 \xrightarrow[(x,y)\to(0,0)]{} 0$$

car $\sqrt{x^2+y^2} \geqslant \sqrt{x^2+y^2} = \|(x,y)\|_2$, et $|x|\,|y| \leqslant \|(x,y)\|_2^2$; en effet, $|x| = \sqrt{x^2} \leqslant \sqrt{x^2+y^2} = \|(x,y)\|_2$, et de même $|y| \leqslant \|(x,y)\|_2$. Par le théorème des gendarmes, on a $|f(x,y)| \to 0$.

VII.7 Continuité d'une fonction

Définition : Soient E et F deux espaces vectoriels normés. Soit $f : D \to F$ une fonction définie sur une partie $D \subset E$ de E.

— Soit $\vec{a} \in D$. On dit que f est *continue* en $\vec{a}$ su $f(\vec{x}) \xrightarrow[\vec{x}\to\vec{a}]{} f(\vec{a})$.

— Soit $A \subset D$. On dit que f est *continue* sur A si f est continue en tout point de A.

Tarte à la crème

Exercice :
Soient f et g deux applications continues sur un espace vectoriel normé E. Soit A une partie de E dense dans E. Montrer que, si $\forall \vec{x} \in A$, $f(\vec{x}) = g(\vec{x})$, alors $\forall \vec{x} \in E$, $f(\vec{x}) = g(\vec{x})$. Autrement dit, deux applications continues qui coïncident sur une partie dense sont égales.

Soit $\vec{y} \in E$. Comme A est dense dans E, il existe une suite $(\vec{a}_n)_{n\in\mathbb{N}}$ de A convergent vers $\vec{y}$. Or, pour tout $n \in \mathbb{N}$, $f(\vec{a}_n) = g(\vec{a}_n)$. De plus, $f(\vec{a}_n) \xrightarrow[n\to\infty]{} f(\vec{y})$ car f est continue, et $\vec{a}_n \xrightarrow[n\to\infty]{} \vec{y}$. De même, $g(\vec{a}_n) \xrightarrow[n\to\infty]{} f(\vec{y})$. Par unicité de la même limite, on en déduit que $f(\vec{y}) = g(\vec{y})$.

Rappel :
On rappelle que f est *continue* si, et seulement si

$$\forall \vec{a} \in A,\ \forall \varepsilon > 0,\ \exists \delta_{\vec{a}} > 0,\ \forall \vec{x} \in A, \qquad \|\vec{x} - \vec{a}\| \leqslant \delta_{\vec{a}} \implies \|f(\vec{x}) - f(\vec{a})\| \leqslant \varepsilon.$$

Définition : Soit A une partie d'un espace vectoriel normé E. On dit qu'une fonction f est

— *uniformément continue* sur A si

$$\forall \varepsilon > 0, \exists \delta > 0, \forall (\vec{a}, \vec{x}) \in A^2, \qquad \|\vec{x} - \vec{a}\| \leqslant \delta \implies \|f(\vec{x}) - f(\vec{a})\| \leqslant \varepsilon\ ;$$

— *lipschitzienne* sur A si

$$\exists k \in \mathbb{R},\ \forall (\vec{a}, \vec{x}) \in A^2, \qquad \|f(\vec{x}) - f(\vec{a})\| \leqslant k \cdot \|\vec{x} - \vec{a}\|.$$

Exemple :
D'après l'exercice 2, toute norme N vérifie l'inégalité

$$\forall (\vec{x}, \vec{y}) \in E^2, \qquad \big|N(\vec{x}) - N(\vec{y})\big| \leqslant 1 \cdot N(\vec{x} - \vec{y}).$$

L'application N est donc 1-lipschitzienne de l'espace vectoriel normé E vers $\mathbb{R}$.

Toute norme est lipschitzienne, donc, *a fortiori*, uniformément continue.

Proposition : On a

$$\text{lipschitzienne} \implies \not\impliedby \text{ uniformément continue} \implies \not\impliedby \text{ continue.}$$

Preuve :
Pour la première implication, on pose $\delta = \varepsilon/k$, et ça marche bien. Pour la seconde implication, on revient à la définition de uniformément continue, ce qui vérifie la définition de continue. □

Exercice : *1. Montrer que la fonction $x \mapsto x^2$ est continue mais pas uniformément continue sur $\mathbb{R}$.*

2. Montrer que la fonction $x \mapsto \sqrt{x}$ est uniformément continue mais pas lipschitzienne sur $[0,1]$.

1. La fonction $g : x \mapsto x^2$ est continue mais pas uniformément continue sur $\mathbb{R}$. En effet,
$$\forall a \in \mathbb{R},\ \forall \varepsilon > 0,\ \exists \delta > 0, \qquad |h| \leqslant \delta \implies \big|g(a+h) - g(a)\big| \leqslant \varepsilon$$
car $|g(a+h)-g(a)| = |(a+h)^2 - a^2| = |2ah+h^2| \leqslant \varepsilon$ si $2|a|\,|h| + |h|^2 - \varepsilon \leqslant 0$, donc si $X^2 + 2|a|\,X - \varepsilon$ a un discriminant négatif ou nul, mais ce discriminant, donc les racines du polynôme dépend de a.
2. La fonction $x \mapsto \sqrt{x}$ est continue sur $[0,1]$, donc uniformément continue sur $[0,1]$, grâce au théorème de Heine. Mais, $f : x \mapsto \sqrt{x}$ n'est pas lipschitzienne sur $[0,1]$. Par l'absurde, supposons la lipschitzienne. Il existe donc $k \in \mathbb{R}$ tel que, pour tous $(a,x) \in [0,1]^2$, $\big|f(x) - f(a)\big| \leqslant k\,|x-a|$. D'où, pour tous $x \neq a$,
$$\left|\frac{f(x) - f(a)}{x - a}\right| \leqslant k.$$
Ainsi, comme f est dérivable sur $]0,1]$,
$$\forall a \neq 0, \quad \frac{1}{2\sqrt{a}} = f'(a) = \lim_{x \to a} \left|\frac{f(x) - f(a)}{x - a}\right| \leqslant K$$
car les inégalités larges passent à la limite. C'est absurde car
$$k \geqslant \lim_{a \to 0^+} \frac{1}{2\sqrt{a}} = +\infty.$$

VII.8 Linéarité & continuité

Théorème : Soient E et F deux espaces vectoriels normés. Soit f une application **linéaire** de E vers F. Il y a équivalence entre

1. f est continue sur E ;
2. f est continue en $\vec{0}$;
3. f est bornée dans la boule unité de E ;
5. f est lipschitzienne sur E ;
6. f est uniformément continue ;
4. il existe un réel k tel que $\forall \vec{x} \in E$, $\|f(\vec{x})\| \leqslant k\,\|\vec{x}\|$.

Preuve :
D'après la proposition 35, on a 5 $\Longrightarrow$ 6 $\Longrightarrow$ 1, et 1 $\Longrightarrow$ 2. Montrons ces équivalences avec un « cycle. »

"2 $\Longrightarrow$ 3" Supposons $f \in \mathscr{L}(E,F)$ et $f(\vec{x}) \xrightarrow[\vec{x}\to\vec{0}]{} f(\vec{0}) = \vec{0}$. En particulier,

$$\big\|f(\vec{x}) - \vec{0}\big\| \xrightarrow[\|\vec{x}-\vec{0}\|]{} 0.$$

Montrons que f est bornée sur la boule unité $B(\vec{0},1)$, *i.e.* montrons qu'il existe $M \in \mathbb{R}$ tel que, pour tout vecteur $\vec{x} \in B(\vec{0},1)$, $\|f(\vec{x})\| \leqslant M$. Or, par hypothèse,

$$\forall \varepsilon > 0,\ \exists \delta > 0, \forall \vec{x} \in E, \qquad \|f(\vec{x})\| \leqslant \delta \implies \|f(\vec{x})\| \leqslant \varepsilon.$$

On pose $\varepsilon = 1$, il existe donc $\delta > 0$ tel que $\forall \vec{x} \in E$, $\|\vec{x}\| \leqslant \delta \implies \|f(\vec{x})\| \leqslant 1$. D'où, par linéarité de f,

$$\left\|f\left(\frac{\vec{x}}{\delta}\right)\right\| = \left\|f\left(\frac{1}{\delta}\cdot\vec{x}\right)\right\| = \left\|\frac{1}{\delta}f(\vec{x})\right\| = \frac{1}{\delta}\cdot\|f(\vec{x})\|.$$

Ainsi, pour tout vecteur $\vec{y} \in B(\vec{0},1)$, on a $\|f(\vec{y})\| \leqslant 1/\delta$.

"3 $\Longrightarrow$ 4" On suppose $f \in \mathscr{L}(E,F)$, et que f est bornée sur $B(\vec{0},1)$. On veut montrer qu'il existe un réel $K \in \mathbb{R}$ tel que, pour tout vecteur $\vec{x} \in E$, $\|f(\vec{x})\| \leqslant K\|\vec{x}\|$. Par hypothèse, il existe un réel M tel que, pour tout vecteur $\vec{y} \in B(\vec{0},1)$, $\|f(\vec{y})\| \leqslant M$. Soit $\vec{x} \in E$.

— Si $\vec{x} \neq \vec{0}$, soit alors $\vec{y} = \vec{x}/7\|\vec{x}\| \in B(\vec{0},1)$. D'où, $\|f(\vec{y})\| \leqslant M$. Or, $f(\vec{x}/7\|\vec{x}\|) = f(\vec{x})/7\|\vec{x}\|$, car f est linéaire. D'où, $\|f(\vec{x})/7\|\vec{x}\|\| \leqslant M$, et donc $\|f(\vec{x})\|/7\|\vec{x}\| \leqslant M$. On en déduit que

$$\|f(\vec{x})\| \leqslant 7M \times \|\vec{x}\|.$$

— Si $\vec{x} = \vec{0}$, alors $\|f(\vec{0})\| = \|\vec{0}\| \leqslant K \cdot \|\vec{0}\|$, par linéarité.

"4 $\Longrightarrow$ 5" On suppose $f \in \mathscr{L}(E,F)$, et qu'il existe un réel K tel que, pour tout vecteur $\vec{x} \in E$, $\|f(\vec{x})\| \leqslant K \cdot \|\vec{x}\|$. On veut montrer qu'il existe un réel K tel que, pour tous vecteurs $\vec{x}$ et $\vec{y} \in E$, $\|f(\vec{x}) - f(\vec{y})\| \leqslant K \cdot \|\vec{x} - \vec{y}\|$. Par linéarité, $f(\vec{x}) - f(\vec{y}) = f(\vec{x} - \vec{y})$. Et, par hypothèse, $\|f(\vec{x} - \vec{y})\| \leqslant K\|\vec{x} - \vec{y}\|$. Ainsi,

$$\|f(\vec{x}) - f(\vec{y})\| \leqslant K\|\vec{x} - \vec{y}\|.$$

□

Exercice :
Soit d l'application linéaire définie par

$$\begin{aligned} d : \mathbb{K}[X] &\longrightarrow \mathbb{K}[X] \\ P &\longmapsto P'. \end{aligned}$$

1. *On munit l'espace vectoriel $\mathbb{K}[X]$ des polynômes de la norme N définie par*
$$\begin{aligned} N : \mathbb{K}[X] &\longrightarrow \mathbb{R} \\ a_0 + a_1X + \cdots + a_nX^n &\longmapsto \max_{i\in[\![0,n]\!]} |a_i|. \end{aligned}$$
Montrer que d n'est pas continue.
2. *On munit le même espace vectoriel de la norme $\|\cdot\|$ définie par $\|P\| = \max_{i\in[\![0,n]\!]} |a_i|/(i+1)$. Montrer que d est continue.*

1. On utilise le théorème précédent. On a, pour tout $n \in \mathbb{N}^\star$, $\|X^n\| = 1$, et $d(X^n) = nX^{n-1}$. Ainsi,
$$\|d(X^n)\| = n \xrightarrow[n\to\infty]{} +\infty.$$
Donc d n'est pas bornée sur la boule unité $B(0,1)$. Cette démonstration est **fausse** en dimension finie dans l'espace vectoriel $\mathbb{K}_n[X]$.
2. Soit $P \in B(0_{\mathbb{R}[X]}, 1)$. On pose $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$. Ainsi, $1 \geqslant \max_{i\in[\![1,n]\!]} |a_i|/(i+1)$. On a $P' = a_1 + 2a_2X + \cdots + na_nX^{n-1} = \sum_{i=1}^{n} ia_iX^{i-1}$. D'où, $\|P'\| = \max_{i\in[\![0,n]\!]} \frac{|ia_i|}{i}$. ???? Non, cette question est fausse, la fonction d n'est pas continue même pour cette nouvelle norme.

Théorème : Soient E et F deux espaces vectoriels normées, et soit $f : E \to F$ une application linéaire. Si E est de dimension **finie**, alors f est lipschitzienne, donc continue sur E.

Preuve :
Soit $f \in \mathscr{L}(E,F)$. On suppose E de dimension finie n. On veut montrer qu'il existe un réel k tel que $\|f(\vec{x})\| \leqslant k\, N(\vec{x})$. Par hypothèse, on peut se placer dans une base $(\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n)$ de E. On peut munir E de la norme N : $x_1\vec{\varepsilon}_1 + \cdots + x_n\vec{\varepsilon}_n = \max_{i\in[\![1,n]\!]} |x_i|$. On réalise la démonstration avec cette norme car toutes les normes sur E sont équivalentes, comme $\dim E = n$. Soit $\vec{x} \in E$. On pose $\vec{x} = x_1\vec{\varepsilon}_1 + \cdots + x_n\vec{\varepsilon}_n$. On calcule

$$\begin{aligned} \|f(\vec{x})\| &= \|f(x_1\vec{\varepsilon}_1) + \cdots + x_n\vec{\varepsilon}_n\| \\ &= \|x_1 f(\vec{\varepsilon}_1) + \cdots + x_n f(\vec{\varepsilon}_n)\| \\ &\leqslant \|x_1 f(\vec{\varepsilon}_1)\| + \cdots + \|x_n f(\vec{\varepsilon}_n)\| \\ &\leqslant |x_1| \cdot \|f(\vec{\varepsilon}_1)\| + \cdots + |x_n| \cdot \|f(\vec{\varepsilon}_n)\| \\ &\leqslant N(\vec{x})\big(\underbrace{\|f(\vec{\varepsilon}_1)\| + \cdots + \|f(\vec{\varepsilon}_n)\|}_{k}\big). \end{aligned}$$

Ainsi, on a bien $\|f(\vec{x})\| \leqslant k \cdot \|\vec{x}\|$. □

Exemple :
L'espace vectoriel $\mathscr{M}_n(\mathbb{K})$ est de dimension finie, les applications sont continues car linéaires :

1. la trace $\mathrm{tr} : \mathscr{M}_n(\mathbb{K}) \to \mathbb{K}, A \mapsto \mathrm{tr}\, A$;
2. la transposée $\square^\top : \mathscr{M}_n(\mathbb{K}) \to \mathscr{M}_n(\mathbb{K}),\ A \mapsto A^\top$;
3. une changement de base $\mathscr{M}_n(\mathbb{K}) \to \mathscr{M}_n(\mathbb{K}),\ A \mapsto P^{-1} \cdot A \cdot P$ où $P \in \mathrm{GL}_n(\mathbb{K})$.

Proposition : Soient $E_1, E_2, \ldots, E_n$ et F des espaces vectoriels normés. Soit $f : E_1 \times E_2 \times \cdots \times E_n \to F$ une application multilinéaire. Alors, f est continue si, et seulement s'il existe une réel K tel que

$$\forall \vec{v}_1 \in E_1, \forall \vec{v}_2 \in E_2, \ldots, \forall \vec{v}_n \in E_n, \qquad \|f(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)\| \leqslant K\|\vec{v}_1\|\|\vec{v}_2\| \cdots \|\vec{v}_n\|.$$

C'est le cas si les espaces vectoriels $E_1, \ldots, E_n$ sont de dimensions finies.

Exemple : 1. Si E est un $\mathbb{R}$-espace vectoriel muni d'un produit scalaire, alors ce produit scalaire est continu de E^2 vers $\mathbb{R}$ car il est bilinéaire : $|\langle \vec{x} \mid \vec{y} \rangle| \leqslant \|\vec{x}\|\,\|\vec{y}\|$ pour tous vecteurs $\vec{x}$ et $\vec{y}$ d'après l'inégalité de Cauchy-Schwarz.
2. La multiplication matricielle, vue comme une application de $\mathscr{M}_{n,p}(\mathbb{R}) \times \mathscr{M}_{p,n} \to \mathscr{M}_{n,n}(\mathbb{R})$, est bilinéaire et donc continue, car les espaces sont de dimensions finies.
3. Si $\mathscr{B}$ est une base d'un $\mathbb{K}$-espace vectoriel E de dimension n, alors le déterminant $\det_{\mathscr{B}}$ est continu par sa multilinéarité, car E est de dimension finie.

VII.9 Norme subordonnée

Remarque : 1. L'ensemble des applications linéaires d'un espace vectoriel E vers un espace vectoriel F, est noté $\mathscr{L}(E, F)$. Cet ensemble est un espace vectoriel ; mieux, c'est aussi un anneau (pour les lois $+$ et $\circ$) ; encore mieux, c'est une algèbre.
2. Si on munit chacun des espaces vectoriels E et F d'une norme, alors une application linéaire $f \in \mathscr{L}(E, F)$ peut être ou ne pas être continue. On note $\mathscr{L}_{\mathrm{c}}(E, F)$ l'ensemble des applications linéaires continues de E vers F. C'est une sous-algèbre de $\mathscr{L}(E, F)$.
3. Si E est de dimension finie, les ensembles $\mathscr{L}(E, F)$ et $\mathscr{L}_{\mathrm{c}}(E, F)$ sont égaux (théorème 39).

Proposition–Définition : Soient E et F deux espaces vectoriels normés. Soit $f \in \mathscr{L}_{\mathrm{c}}(E, F)$ une application linéaire de E vers F.

1. On appelle *norme subordonnée* (ou norme d'opérateur) de f, notée

$|||f|||$, le plus petit réel K tel que

$$\forall \vec{x} \in E, \qquad \|f(\vec{x})\| \leqslant \|\vec{x}\|.$$

Ainsi, il vaut donc

$$|||f||| = \sup_{\vec{x}\neq\vec{0}} \frac{\|f(\vec{x})\|}{\|\vec{x}\|} = \sup_{\|\vec{x}\|=1} \|f(\vec{x})\|.$$

2. La norme subordonnée est une norme sur l'espace vectoriel $\mathscr{L}_c(E,F)$. Et, cette norme est *sous-multiplicative* :

$$\forall f, g \in \mathscr{L}_c(E,F), \qquad |||f\circ g||| \leqslant |||f||| \cdot |||g|||.$$

(Cette propriété est vraie si l'on peut composer, *i.e.* $F \subset E$.)

Preuve : 1. Comme f est continue, on sait que $\forall \vec{x} \in E$, $\|f(\vec{x})\| \leqslant K\cdot\|\vec{x}\|$. Et, ce réel est minoré par 0. L'ensemble des valeurs de K forment une partie de $\mathbb{R}$ minorée, elle a donc une borne inférieure : $|||f|||$. Et, pour tout vecteur $\vec{x} \neq \vec{0}$, $\|f(\vec{x})\|/\|\vec{x}\| \leqslant K$. D'où, le "meilleur" K est $\sup_{\vec{x}\neq\vec{0}} \|f(\vec{x})\|/\|\vec{x}\|$ car c'est le plus petit majorant. Finalement, pour tout vecteur $\vec{x} \neq 0$, $\|f(\vec{x})\|/\|\vec{x}\| = \big\|f(\vec{x})/\|\vec{x}\|\big\| = \big\|f(\vec{x}/\|\vec{x}\|)\big\|$, et le vecteur $\vec{x}/\|\vec{x}\|$ a pour norme 1. D'où $|||f||| = \sup_{\|\vec{x}\|\neq 1} \|f(\vec{x})\|$.

2. Montrons que l'application $|||\cdot||| : f \mapsto |||f|||$ est une norme.
   - Si $|||f||| = 0_{\mathbb{R}}$, alors, pour tout vecteur $\vec{x} \in E$, $\|f(\vec{x})\| \leqslant 0\cdot\|\vec{x}\|$, d'où $\|f(\vec{x})\| = 0_{\mathbb{R}}$, pour tout vecteur $\vec{x} \in E$. Ainsi, pour tout vecteur $\vec{x} \in E$, $f(\vec{x}) = \vec{0}$. On en déduit $f = 0$.
   - Soit $\alpha \in \mathbb{K}$. Ainsi, $|||\alpha f||| = \sup_{\|\vec{x}\|=1} \|\alpha f(\vec{x})\| = |\alpha| \sup_{\|\vec{x}\|=1} \|f(\vec{x})\| = |\alpha|\,|||f|||$.
   - On sait que $|||f+g||| = \sup_{\|\vec{x}\|=1} \|(f+g)(\vec{x})\|$. Or, $\forall \vec{x} \in B(\vec{0},1)$, $\|(f+g)(\vec{x})\| = \|f(\vec{x})+g(\vec{x})\| \leqslant \|f(\vec{x})\| + \|g(\vec{x})\| \leqslant |||f||| + |||g|||$, qui est un majorant. Et, le plus petit majorant est $|||f+g|||$. D'où, $|||f+g||| \leqslant |||f||| + |||g|||$.

   Mieux, montrons qu'elle est sous-multiplicative : $|||f\circ g||| \leqslant |||f|||\cdot|||g|||$, *i.e.* $\sup_{\|\vec{x}\|=1} \|f\circ g(\vec{x})\| \leqslant |||f|||\cdot|||g|||$. Pour tout vecteur $\vec{x}$, $\|f\circ g(\vec{x})\| = \big\|f\big(g(\vec{x})\big)\big\| \leqslant |||f|||\cdot\|g(\vec{x})\| \leqslant |||f|||\cdot|||g|||\cdot\|\vec{x}\|$. D'où, pour tout vecteur $\vec{x}$, $\|f\circ g(\vec{x})\| \leqslant \underbrace{|||f|||\cdot|||g|||}_{K}\cdot\|\vec{x}\|$. Or, le plus petit K possible est $|||f\circ g|||$.

   Ainsi, $|||f\circ g||| \leqslant |||f|||\cdot|||g|||$.

□

Exemple :
On munit l'espace vectoriel $\mathscr{M}_{n,1}(\mathbb{K})$ de la norme définie par $\|X\|_\infty = \max_{j\in[\![1,n]\!]} |x_j|$ pour tout vecteur colonne $X = (x_j)_{j\in[\![1,n]\!]}$. Soit $A \in \mathscr{M}_{n,1}(\mathbb{K})$

une matrice carrée :

$$\forall X \in \mathscr{M}_{n,1}(\mathbb{K}), \qquad \|AX\|_\infty \leqslant K \cdot \|X\|_\infty \qquad \text{avec } K = \max_{i\in[\![1,n]\!]} \sum_{j=1}^{n} |a_{i,j}|.$$

On a $|||A|||_\infty = \max_{i\in[\![1,n]\!]} \sum_{j=1}^n |a_{i,j}|$.

On détermine le plus petit réel K tel que $\|AX\|_\infty \leqslant K \cdot \|X\|$, pour tout vecteur colonne $X \in \mathscr{M}_{n,1}(\mathbb{K})$. On pose $Y = AX$, et on a $y_i = \sum_{j=1}^n a_{i,j}x_j$. Ainsi, $\|AX\| = \max_{i\in[\![1,n]\!]} |y_i|$. Or, pour tout $i \in [\![1,n]\!]$, $|y_i| = |\sum_{i=1}^n a_{i,j}x_j| \leqslant \sum_{i=1}^n |a_{i,j}| \cdot |x_j| \leqslant \sum_{j=1}^n |a_{i,j}| \cdot \|X\|_\infty \leqslant \|X\|_\infty \sum_{j=1}^n |a_{i,j}|$. On pose ainsi $K = \max_{i\in[\![1,n]\!]} \sum_{j=1}^n |a_{i,j}|$, et on a donc $\|AX\|_\infty \leqslant K \cdot \|X\|_\infty$.

Pour montrer $K = |||A|||_\infty$, il suffit de réaliser l'égalité $\|AX\|_\infty = K \cdot \|X\|_\infty$, pour un vecteur X non nul. On voudrait que $\max_{i\in[\![1,n]\!]} \left|\sum_{j=1}^n a_{i,j}x_j\right| = \left(\max_{i\in[\![1,n]\!]} \sum_{i=1}^n |a_{i,j}|\right) \times \left(\max_{i\in[\![1,n]\!]} |x_i|\right)$. Il existe $k \in [\![1,n]\!]$, tel que $K = \sum_{j=1}^n |a_{k,j}|$. On choisit $x_j = +1$ si $a_{k,j} > 0$, et $x_j = -1$ si $a_{k,j} \leqslant 0$. (Autrement dit, on a $x_j = \operatorname{sgn} a_{k,j}$.)

Exercice (itérées et projecteurs) :
Soit E un espace vectoriel normé, et soit $f \in \mathscr{L}_c(E)$ un endomorphisme continu. On suppose que la suite $(f^n)_{n\in\mathbb{N}}$ des itérées de f converge. Montrer que :

1. *sa limite est un projecteur,*
2. *sa limite est nulle si $|||f||| < 1$.*

Soit $f \in \mathscr{L}_c(E)$. Soit $\ell \in \mathscr{L}(E)$ telle que $f^n \xrightarrow[n\to\infty]{} \ell$.

1. On a $f^{2n} \xrightarrow[n\to\infty]{} \ell$, car la suite $(f^{2n})_{n\in\mathbb{N}}$ est une suite extraite de la suite $(f^n)_{n\in\mathbb{N}}$. L'application $|||\cdot|||$ est sous-multiplicative, d'où

   $$\forall (f,g) \in \mathscr{L}_c(E), \qquad |||f \circ g||| \leqslant |||f||| \cdot |||g|||.$$

   Ainsi, l'application $\circ$ est continue. D'où, $f^{2n} = f^n \circ f^n \xrightarrow[n\to\infty]{} \ell^2$. Par unicité de la limite, $\ell^2 = \ell$, c'est donc un projecteur.

   Autre méthode :

   $$\begin{aligned} 0 \leqslant |||f^{2n} - \ell^2||| &= |||f^n \circ f^n - \ell \circ \ell||| \\ &= |||f^n \circ f^n - f^n \circ \ell + f^n \circ \ell - \ell \circ \ell||| \\ &\leqslant |||f^n \circ f^n - f^n \circ \ell||| + |||f^n \circ \ell - \ell \circ \ell||| \end{aligned}$$

   par inégalité triangulaire. Ainsi,

   $$\begin{aligned} 0 \leqslant |||f^{2n} - \ell^2||| &\leqslant |||f^n \circ (f^n - \ell)||| + |||(f^n - \ell) \circ \ell||| \\ &\leqslant |||f^n||| \times \underbrace{|||f^n - \ell|||}_{\to 0} + \underbrace{|||f^n - \ell|||}_{\to 0} \times |||\ell||| \xrightarrow[n\to\infty]{} 0 \end{aligned}$$

   car, $|||f^n||| \to |||\ell|||$ par hypothèse et continuité de la norme. Par le théorème des gendarmes, on en déduit que $f^{2n} \to \ell^2$.

2. On a $|||f^2||| \leqslant |||f|||^2$, d'où, par récurrence, on a $\forall n \in \mathbb{N}^\star$, $0 \leqslant |||f^n||| \leqslant |||f|||^n \xrightarrow[n\to\infty]{} 0$ (car $|||f||| \leqslant 1$ par hypothèse). D'après le théorème des gendarmes, on a $|||f^n||| \xrightarrow[n\to\infty]{} 0$. Or, l'application $|||\cdot|||$ est continue, $|||f^n||| \xrightarrow[n\to\infty]{} |||\ell|||$. Par unicité de la limite, on trouve $|||\ell||| = 0$. On en déduit que $\ell = 0$.

VII.10 Ouverts et fermés

Définition : Soit A une partie d'un espace vectoriel normé E. On dit que

1. un point $\vec{a} \in E$ est *intérieur à* A s'il existe $\varepsilon > 0$ tel que $B(\vec{a}, \varepsilon) \subset A$;
2. l'ensemble A est un *ouvert* ou une *partie ouverte* de E si, pour tout vecteur $\vec{a} \in A$, il existe $\varepsilon > 0$ tel que $B(\vec{a}, \varepsilon) \subset A$;
3. l'ensemble A est un *fermé* ou une *partie fermée* de E si son complémentaire $E \setminus A$ est un ouvert de E.

Avec cette définition, la partie A est un ouvert de E si, et seulement si, tout vecteur $\vec{a}$ de A est intérieur à A.

Remarque : 1. L'intersection d'une famille d'ouverts n'est pas toujours un ouvert. Contre-exemple :

$$\bigcap_{n\in\mathbb{N}^\star} \left]-\frac{1}{n}, \frac{1}{n}\right[= \{0\}.$$

2. L'union d'une famille de fermés n'est pas toujours un fermé. Contre-exemple :

$$\bigcup_{n\in\mathbb{N}^\star} \left[-1+\frac{1}{n}, 1-\frac{1}{n}\right] =]-1, 1[.$$

3. La réunion d'une famille d'ouverts est toujours un ouvert. L'intersection d'une famille de fermés est toujours un fermé.

Preuve :
Soit $(A_i)_{i\in I}$ une famille d'ouverts. On pose $A = \bigcup_{i\in I} A_i$. Montrons que, pour tout $\vec{x} \in A$, il existe $\varepsilon > 0$ tel que $B(\vec{x}, \varepsilon) \subset A$. Soit $\vec{x} \in A$. Il existe $i \in I$ tel que $\vec{x} \in A_i$. Or A_i est un ouvert, il existe down $\varepsilon > 0$, tel que $B(\vec{x}, \varepsilon) \subset A_i \subset B$. L'ensemble B est donc un ouvert.

Soit $(F_i)_{i\in I}$ une famille de fermés. On pose $F = \bigcap_{i\in I} F_i$. Montrons que $E \setminus F$ est un ouvert. Or, $E \setminus F = \bigcup_{i\in I}(E \setminus F_i)$, et pour tout $i \in I$, $E \setminus F_i$ est un ouvert. L'union d'une famille d'ouverts est un ouvert. On en déduit que F est un fermé. □

4. L'intersection d'une famille **finie** d'ouverts est un ouvert. L'union d'une famille **finie** de fermés est toujours un fermé.

Preuve :
Soit $(A_i)_{i\in I}$ une famille **finie** d'ouverts. Soit $\vec{x} \in \bigcap_{i\in I} A_i$. Ainsi, pour tout $i \in I$, $\vec{x} \in A_i$. Or, A_i est un ouvert. Il existe donc $\varepsilon_i > 0$ tel que $B(\vec{x}, \varepsilon_i) \subset A_i$. On pose donc $\varepsilon = \min_{i\in I} \varepsilon_i$. Alors, $B(\vec{x}, \varepsilon) \subset \bigcap_{i\in I} A_i$.

On passe au complémentaire, et on conclut comme dans la démonstration précédente. □

Exercice :
Soient a et b deux réels tels que $a < b$. Montrer que

1. *les intervalles $]-\infty, b[$, $]a, b[$, et $]a, +\infty[$ sont des ouverts de $\mathbb{R}$;*
2. *les intervalles $]-\infty, b]$, $[a, b]$, et $[a, +\infty[$ sont des fermés de $\mathbb{R}$;*
3. *l'intervalle $[a, b[$ n'est, ni ouvert, ni fermé.*

1. Montrons que $]-\infty, b[$ est un ouvert. Soit $x \in]-\infty, b[$. On pose $\varepsilon = (b - x)/2$. Ainsi, on a bien $]x - \varepsilon, x + \varepsilon[\subset]-\infty, b[$. De même pour les autre cas.
2. L'intervalle $]-\infty, b]$ est un fermé, car $\mathbb{R} \setminus]-\infty, b[=]b, +\infty[$ est un ouvert d'après la question précédente. De même pour les autres cas.
3. L'intervalle $[a, b[$ n'est pas un ouvert car, pour tout $\varepsilon > 0$, $B(a, \varepsilon) \not\subset [a, b[$. Et, l'intervalle $[a, b[$ n'est pas un fermé car $\mathbb{R} \setminus [a, b[=]-\infty, a[\cup [b, +\infty[$ n'est pas un ouvert.

Proposition : Soient E et F deux espaces vectoriels normés, et soit $f : E \to F$ une application **continue**. Si B est un ouvert (resp. un fermé) de F, alors $f^{-1}(B)$ est un ouvert (resp. un fermé) de E. Autrement dit, l'image réciproque d'un ouvert (resp. d'un fermé) par une application continue est un ouvert (resp. d'un fermé).

Rappel :
Sans hypothèse sur f et sur B, l'ensemble $f^{-1}(B)$ est l'ensemble des antécédents des éléments de B. Ainsi,

$$\vec{x} \in f^{-1}(B) \overset{\text{def.}}{\iff} f(\vec{x}) \in B.$$

Preuve :
Soit $\vec{x} \in f^{-1}(B)$. Ainsi, $f(\vec{x}) \in B$. Or, B est un ouvert de F. Il existe donc $\zeta > 0$ tel que $B\big(f(\vec{x}), \zeta\big) \subset B$. Or, pour tout vecteur $\vec{y} \in F$, il existe $\varepsilon > 0$ tel que $\|\vec{x} - \vec{y}\| \leqslant \varepsilon \implies \|f(\vec{x}) - f(\vec{y})\| \leqslant \zeta$, comme f est continue. D'où, $B(\vec{x}, \varepsilon) \subset f^{-1}(B)$. On en déduit que $f^{-1}(B)$ est un ouvert. De même pour un fermé car $E \setminus f^{-1}(B) = f^{-1}(F \setminus B)$. □

Exercice :
Soit $f : E \to \mathbb{R}$ une application continue d'un espace vectoriel normé E vers $\mathbb{R}$. Montrer que

1. *l'ensemble* $A = \{\vec{x} \in E \mid f(\vec{x}) > 0\}$ *des solution de l'inéquation* $f(\vec{x}) > 0$ *est un ouvert de* E *;*
2. *l'ensemble* $B = \{\vec{x} \in E \mid f(\vec{x}) \geqslant 0\}$ *des solution de l'inéquation* $f(\vec{x}) \geqslant 0$ *est un fermé de* E *;*
3. *l'ensemble* $C = \{\vec{x} \in E \mid f(\vec{x}) = 0\}$ *des solution de l'équation* $f(\vec{x}) = 0$ *est un fermé de* E *;*

1. On a, $A = f^{-1}(]0, +\infty[)$. Or $]0, +\infty[$ est un ouvert de $\mathbb{R}$. L'ensemble A est donc l'image réciproque d'un ouvert par une fonction continue donc A est un ouvert.
2. On a, $B = f^{-1}([0, +\infty[)$. Or $[0, +\infty[$ est un fermé de $\mathbb{R}$. L'ensemble B est donc l'image réciproque d'un fermé par une fonction continue donc B est un fermé.
3. On a, $C = f^{-1}(\{0\}) \neq f^{-1}(0)$, qui n'existe pas car f n'est pas forcément bijective. Or $\{0\}$ est un fermé de $\mathbb{R}$. L'ensemble C est donc l'image réciproque d'un fermé par une fonction continue donc C est un fermé.

L'équation $y = x^2$ est celle d'une parabole, et cette parabole est un fermé de $\mathbb{R}^2$. En effet, l'ensemble $\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\} = f^{-1}(\{0\})$ avec $f(x, y) = y - x^2$. Or, $\{0\}$ est un fermé de $\mathbb{R}$, et l'application f est continue. Donc, la parabole d'équation $y = x^2$ est l'image réciproque d'une fonction continue, donc c'est un fermé.

De même, pour la courbe d'équation $y^3 - 3x^2 = 7$ est aussi un courbe fermée du plan $\mathbb{R}^2$: c'est l'image réciproque du fermé $\{0\}$ par l'application continue $f : (x, y) \mapsto y^3 - 3x^2 - 7$.

Exemple :
Une boule ouverte est un ouvert. Une boule fermée est un fermé. Une sphère est un fermé.

En effet, $B(\vec{a}, r) = \{\vec{x} \in E \mid \|\vec{x} - \vec{a}\| < r\} = f^{-1}(]-\infty, r[)$ en choisissant $f : \vec{x} \mapsto \|\vec{x} - \vec{a}\|$. Or, $]-\infty, r[$ est un ouvert de $\mathbb{R}$, f est continue car toute norme est 1-lipschitzienne. Donc $B(\vec{a}, r)$ est un ouvert. De même pour $\bar{B}(\vec{a}, r)$ et $\bar{B}(\vec{a}, r) \setminus B(\vec{a}, r)$.

Exercice :
Soit E *un espace vectoriel de dimension finie. Montrer que tout hyperplan de* E *est un fermé.* Soit H un hyperplan d'un espace vectoriel normé de dimension finie. L'hyperplan H est le noyau d'une forme linéaire φ non nulle. Ainsi, $H = \operatorname{Ker}\varphi$, et $\varphi : E \xrightarrow{\text{linéaire}} \mathbb{R}$. L'application φ est continue comme le sont toutes les applications linéaires sur un espace vectoriel normé de dimension finie. Soit $\vec{x} \in E : \vec{x} \in H \iff \varphi(\vec{x}) = 0$. Donc $H = \varphi^{-1}(\{0\})$. D'où, H est l'image réciproque du fermé $\{0\}$ par la fonction continue φ : c'est donc un fermé de E.

Proposition : Soit A une partie d'un espace vectoriel normé E.

1. Son adhérence $\bar{A}$ est un fermé de E.
2. La partie A est un fermé de E si, et seulement si $A = \bar{A}$.
3. L'ensemble A est un fermé de E si, et seulement si, à chaque fois

qu'une suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de A converge, la limite de $(u_n)_{n\in\mathbb{N}}$ appartient à A. (caractérisation séquentielle d'un fermé).

Preuve : 1. Montrons que $E \setminus \bar{A}$ est un ouvert. Soit $\vec{x} \in E \setminus \bar{A}$. Alors $x \notin \bar{A}$. Il existe $\varepsilon > 0$ tel que $B(\vec{x}, \varepsilon) \cap A = $. Soit $\vec{y} \in B(\vec{x}, \varepsilon)$. Ainsi, $\vec{y} \notin \bar{A}$. Or, $B(\vec{x}, \varepsilon)$ est in ouvert, il existe donc $\zeta > 0$ tel que $B(\vec{y}, \zeta) \subset B(\vec{x}, \varepsilon)$. D'où, il existe $\zeta > 0$ tel que $B(\vec{y}, \zeta) \cap A = $. Alors, $\vec{y} \notin \bar{A}$. D'où, $B(\vec{x}, \varepsilon) \cap \bar{A} = $. On en déduit $B(\vec{x}, \varepsilon) \subset E \setminus \bar{A}$.

2. Le point 1 démontre déjà la réciproque. Il nous suffit de montrer l'implication, *c.f.* poly.
3. On utilise la caractérisation séquentielle de l'adhérence (proposition 23).

□

Chapitre 14

Couples de variables aléatoires discrètes

VII.1 Lois conjointe et marginales

Proposition–Définition : Soit $(\Omega, \mathscr{A}, P)$ un espace probabilisé. Si X et Y sont deux variables aléatoires discrètes, alors l'application

$$\begin{aligned}(X,Y) : \Omega &\longrightarrow X(\Omega) \times Y(\Omega)\\ \omega &\longmapsto \big(X(\omega), Y(\omega)\big)\end{aligned}$$

est aussi une variable aléatoire discrète, appelée *couple de variables aléatoires discrètes* (X,Y).

La loi de probabilité du couple (X,Y) est appelée *loi conjointe* :

$$\forall (i,j) \in I\times J, \qquad P\big((X,Y)=(a_i,b_j)\big) = P(X=a_i, Y=b_j) = P\big((X=a_i)\cap(Y=b_j)\big) = p_{i,j}$$

où chaque $p_{i,j}$ appartient à $[0,1]$. On vérifie bien $\sum_{i\in I}\sum_{j\in J} p_{i,j} = 1$.

Les lois de de X et de Y sont appelées *lois marginales*. La loi conjointe permet de retrouver les lois marginales :

$$\forall i \in I, \qquad P(X=a_i) = \sum_{j\in J} P(X=a_i, Y=b_j)$$

$$\forall j \in J, \qquad P(Y=b_j) = \sum_{i\in I} P(X=a_i, Y=b_j).$$

En effet, $(X=a_i) = \bigcup_{j\in J}\big[(X=a_i)\cap(Y=b_j)\big]$, et cette union est disjointe. Ainsi, $P(X=a_i) = \sum_{j\in J} P\big[(X=a_i)\cap(Y=b_j)\big] = \sum_{j\in J} p_{i,j}$. De même pour la probabilité $P(Y=b_j) = \sum_{i\in I} p_{i,j}$.

B Attention Les lois marginales ne permettent pas toujours de retrouver la loi conjointe : « on perd la notion de corrélation entre les deux variables aléatoires. »

Exercice :
Une boîte contient 3 boules blanches et 4 boules noires. On tire au hasard, l'une après l'autre, deux boules. Soient X et Y les variables aléatoires définies par : X est égale à 0 si la première boule tirée est blanche, à 1 si elle est noire. De même pour Y avec la seconde boule.

Compléter les tableaux suivants dans les deux cas :

1. *si le tirage se fait sans remise.*

	$Y=0$	$Y=1$	total
$X=0$	$p_{00}=\frac{3}{7}\times\frac{2}{6}=\frac{1}{7}$	$p_{01}=\frac{3}{7}\times\frac{2}{6}=\frac{2}{7}$	$P(X=0)=\frac{3}{7}$
$X=1$	$p_{10}=\frac{4}{7}\times\frac{3}{6}=\frac{2}{7}$	$p_{11}=\frac{4}{7}\times\frac{2}{6}=\frac{2}{7}$	$P(X=1)=\frac{4}{7}$
total	$P(Y=0)=\frac{3}{7}$	$P(Y=1)=\frac{4}{6}$	1

.

2. *si le tirage se fait avec remise.*

	$Y=0$	$Y=1$	total
$X=0$	$p_{00}=\frac{3}{7}\times\frac{3}{7}=\frac{9}{49}$	$p_{01}=\frac{3}{7}\times\frac{4}{7}=\frac{12}{49}$	$P(X=0)=\frac{3}{7}$
$X=1$	$p_{10}=\frac{4}{7}\times\frac{3}{7}=\frac{12}{49}$	$p_{11}=\frac{4}{7}\times\frac{4}{7}=\frac{16}{49}$	$P(X=1)=\frac{4}{7}$
total	$P(Y=0)=\frac{3}{7}$	$P(Y=1)=\frac{4}{6}$	1

.

Définition : Soit $(\Omega,\mathcal{A},P)$ un espace probabilisé. On dit que deux variables aléatoires X et Y sont *indépendantes*, et on note $X \perp\!\!\!\perp Y$, si

$$\forall (a,b)\in X(\Omega)\times Y(\Omega),\qquad P(X=a,Y=b)=P(X=a)\cdot P(Y=b).$$

Soit $(X_i)_{i\in I}$ une famille (finie ou non) de variables aléatoires. On dit que ces variables aléatoires ont

— *deux à deux indépendantes* si

$$\forall i\neq j\in I,\forall (a,b),\qquad P(X_i=a_i,X_j=b)=P(X_i=a)\cdot P(X_j=b),$$

— *indépendantes* si, pour toute partie finie non vide $J\subset I$,

$$\forall (a_j)_{j\in J},\qquad P\Big(\bigcap_{j\in J}(X_j=a_j)\Big)=\prod_{j\in J}P(X_j=a_j).$$

Les propriétés ci-dessous sont admises.

Proposition : Soient X et Y deux variables aléatoires indépendantes d'un espace probabilisé $(\mathscr{W}, \mathscr{A}, P)$,

1. $\forall A \subset X(\Omega), \forall B \in Y(\Omega), \qquad P(X \in A, Y \in B) = P(X \in A) \cdot P(X \in B)$,
2. pour toutes fonctions φ et ψ, les *vad* $\varphi(X)$ et $\psi(Y)$ sont indépendantes.

Lemme des coalitions : Soit φ et ψ deux fonctions. Si $X_1, \dots, X_n$ sont des variables aléatoires indépendantes, alors

$$\forall p \in [\![1, n-1]\!], \qquad \varphi(X_1, \dots, X_p) \perp\!\!\!\perp \psi(X_{p+1}, \dots, X_n).$$

VII.2 La somme de deux variables aléatoires

Soit $(\Omega, \mathscr{A}, P)$ un espace probabilisé. La *somme* Z de deux *vard* X et Y définie par

$$\forall \omega \in \Omega, \qquad Z(\omega) = X(\omega) + Y(\omega).$$

La loi conjointe du couple (X, Y) permet de calculer la loi de probabilité de la forme

$$\forall c \in Z(\Omega), \qquad P(Z = c) = \sum_{\substack{i \in I \\ j \in J \\ a_i + b_j = c}} p_{i,j}.$$

Exercice :
Soit X_1 et X_2 deux variables aléatoires ***indépendantes****. Montrer que*

1. *si $X_1 \sim \mathscr{B}(n_1, p)$ et $X_2 \sim \mathscr{B}(n_2, p)$, alors*

   $$X_1 + X_2 \sim \mathscr{B}(n_1 + n_2, p)$$

   où $n_1 \in \mathbb{N}^\star$, $n_2 \in \mathbb{N}^\star$ et $p \in]0, 1[$ a la même valeur pour les deux viables aléatoires. En déduire $\mathrm{E}(X_1 + X_2)$ et $\mathrm{V}(X_1 + X_2)$. ***(stabilité de la loi binomiale)***
2. *si $X_1 \sim \mathscr{P}(\lambda_1)$ et $X_2 \sim \mathscr{P}(\lambda_2)$, alors*

   $$X_1 + X_2 \sim \mathscr{P}(\lambda_1 + \lambda_2)$$

   où $\lambda_1 \in \mathbb{R}_\star^+$, et $\lambda_2 \in \mathbb{R}_\star^+$. En déduire $\mathrm{E}(X_1 + X_2)$ et $\mathrm{V}(X_1 + X_2)$. ***(stabilité de la loi de* Poisson*)***

1. On a

   $$\forall s \in [\![0, n_1 + n_2]\!], \qquad (X_1 + X_2 = s) = \bigcup_{k_1 + k_2 = s} (X_1 = k_1, X_2 = k_2)$$
   $$= \bigcup_{k_1 + k_2 = s} \big[(X_1 = k_1) \cap (X_2 = k_2)\big]$$

et cette union est disjointe. D'où,

$$\begin{aligned}
P(X_1+X_2=s) &= \sum_{k_1+k_2=s} P\big((X_1=k_1)\cap(X_2=k_2)\big)\\
&= \sum_{k_1+k_2=s} P(X_1=k_1)\cdot P(X_2=k_2) && \text{car } X_1\\
&= \sum_{k_1+k_2=s} \binom{n_1}{k_1} p^{k_1} q^{n_1-k_1} \times \binom{n_2}{k_2} p^{k_2} q^{n_2-k_2}\\
&= \sum_{k_1+k_2=s} p^{k_1+k_2}\cdot q^{n_1+n_2-k_1-k_2} \binom{n_1}{k_1}\binom{n_2}{k_2}\\
&= p^s\cdot q^{n_1+n_2-s} \sum_{k_1+k_2=s} \binom{n_1}{k_1}\binom{n_2}{k_2}\\
&= p^s\cdot q^{n_1+n_2-s} \binom{n_1+n_2}{s} && \text{d'après la formule de VANDERM}
\end{aligned}$$

D'où, $X_1+X_2\sim\mathscr{B}(n_1+n_2,p)$. On en déduit que

$$\mathrm{E}(X_1+X_2)=(n_1+n_2)p \qquad \mathrm{V}(X_1+X_2)=(n_1+n_2)pq.$$

2. On a $X_1(\Omega)=X_2(\Omega)=\mathbb{N}$, et $\forall k\in X_1(\Omega)$, $P(X_1=k_1)=\mathrm{e}^{-\lambda_1}\cdot\lambda_1^{k_1}/k_1!$, de même pour X_2. Ainsi, $(X_1+X_2)(\Omega)=\mathbb{N}$. On a

$$(X_1+X_2=s)=\bigcup_{k_1+k_2=s}\big[(X_1=k_1)\cap(X_2=k_2)\big]$$

et cette union est disjointe, d'où

$$\begin{aligned}
P(X_1+X_2=s) &= \sum_{k_1+k_2=s} P\big[(X_1=k_1)\cap(X_2=k_2)\big]\\
&= \sum_{k_1+k_2=s} P(X=k_1)\cdot P(X_2=k_2) \qquad \text{car } X_1 \perp\!\!\!\perp X_2\\
&= \sum_{k_1+k_2=s} \mathrm{e}^{-\lambda_1}\cdot\frac{\lambda_1^{k_1}}{k_1!}\cdot\mathrm{e}^{-\lambda_2}\cdot\frac{\lambda_2^{k_2}}{k_2!}\\
&= \mathrm{e}^{-(\lambda_1+\lambda_2)} \sum_{k_1+k_2=s} \frac{\lambda_1^{k_1}\cdot\lambda_2^{k_2}}{k_1!\cdot k_1!}\\
&= \mathrm{e}^{-(\lambda_1+\lambda_2)} \sum_{k=0}^{s} \frac{\lambda_1^{k}\cdot\lambda_2^{s-k}}{k!\cdot(s-k)!}\\
&= \mathrm{e}^{-(\lambda_1+\lambda_2)}\cdot\frac{1}{s!}\sum_{k=0}^{s}\binom{s_1}{k}\lambda_1^k\lambda_2^{s-k}\\
&= \mathrm{e}^{-(\lambda_1+\lambda_2)}\cdot\frac{1}{s!}(\lambda_1+\lambda_2)^s.
\end{aligned}$$

Ainsi, $X_1+X_2\sim\mathscr{P}(\lambda_1+\lambda_2)$. On en déduit que

$$\mathrm{E}(X_1+X_2)=\lambda_1+\lambda_2 \qquad \mathrm{V}(X_1+X_2)=\lambda_1+\lambda_2.$$

VII.3 Espérance et variance d'une somme

Proposition : Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé. Si deux variables aléatoires X et Y sont d'espérance finie, alors leur somme $X+Y$ est aussi d'espérance finie et

$$\mathrm{E}(X) + \mathrm{E}(Y) = \mathrm{E}(X+Y).$$

Mieux, pour tout couple de réels $(\alpha, \beta) \in \mathbb{R}^2$, la variable aléatoire $\alpha X + \beta Y$ est d'espérance finie et

$$\mathrm{E}(\alpha X + \beta Y) = \alpha \mathrm{E}(X) + \beta \mathrm{E}(Y).$$

Proposition–Définition : Soit (X, Y) un couple de variables aléatoires réelles discrètes d'un espace probabilisé. Si X^2 et Y^2 sont d'espérance finie, alors

$$\mathrm{V}(X+Y) = \mathrm{V}(X) + \mathrm{V}(Y) + 2\,\mathrm{Cov}(X,Y)$$

où $\mathrm{Cov}(X,Y)$ est appelée la *covariance* de (X,Y) et est définie par

$$\mathrm{Cov}(X,Y) = \mathrm{E}\Big[\big(X - \mathrm{E}(X)\big)\cdot\big(Y - \mathrm{E}(Y)\big)\Big] = \mathrm{E}(X\cdot Y) - \mathrm{E}(X)\cdot\mathrm{E}(Y).$$

Preuve :
On a $\mathrm{V}(X) = \mathrm{E}\big(\big(X - \mathrm{E}(X)\big)^2\big) = \mathrm{E}(X^2) - \big[\mathrm{E}(X)\big]^2$. De même, $\mathrm{V}(Y) = \mathrm{E}\big(\big(Y - \mathrm{E}(Y)\big)^2\big) = \mathrm{E}(Y^2) - \big[\mathrm{E}(Y)\big]^2$, et $\mathrm{V}(X+Y) = \mathrm{E}\big(\big(X+Y - \mathrm{E}(X+Y)\big)^2\big) = \mathrm{E}\big((X+Y)^2\big) - \big[\mathrm{E}(X+Y)\big]^2$. Ainsi,

$$\begin{aligned}\mathrm{V}(X+Y) &= \mathrm{E}(X^2+Y^2-2XY) - \big(\mathrm{E}(X)+\mathrm{E}(Y)\big)^2\\ &= \mathrm{E}(X^2) + \mathrm{E}(Y^2) + 2\mathrm{E}(XY) - [\mathrm{E}(X)]^2 - [\mathrm{E}(Y)]^2 - 2\mathrm{E}(X)\mathrm{E}(Y)\\ &= \mathrm{V}(X) + \mathrm{V}(Y) + 2\big[\mathrm{E}(XY) - \mathrm{E}(X)\mathrm{E}(Y)\big]\end{aligned}$$

□

Remarque : 1. $\mathrm{Cov}(X,X) = \mathrm{E}(X^2) - [\mathrm{E}(X)]^2 = \mathrm{V}(X)$.

2. La covariance est une forme bilinéaire symétrique ~~définie~~ positive. En effet, la symétrie est assurée par commutativité du produit ; la bilinéarité est assurée par la linéarité de l'espérance ; la positivité est assurée par le fait que $\big(X - \mathrm{E}(X)\big)^2$ est une *vard* à valeurs positive.

Proposition (inégalité de Cauchy-Schwarz) **:** Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé, et (X,Y) un couple de variables aléatoires réelles

discrètes. Si X^2 et Y^2 sont d'espérance finie, alors

$$\big(\mathrm{E}(XY)\big)^2 \leqslant \mathrm{E}(X^2)\cdot\mathrm{E}(Y^2) \qquad \text{et} \qquad \big[\mathrm{Cov}(X,Y)\big]^2 \leqslant \mathrm{V}(X)\cdot\mathrm{V}(Y).$$

Preuve :
Pour la seconde formule, on utilise l'inégalité de Cauchy-Scharz pour les produits scalaires (le caractère défini n'a pas été utilisé dans la démonstration) : $|\mathrm{Cov}(X,Y)| \leqslant \sqrt{\mathrm{V}(X)}\cdot\sqrt{\mathrm{V}(y)}$ et donc $\big[\mathrm{Cov}(X,Y)\big]^2 \leqslant \mathrm{V}(X)\times\mathrm{V}(Y)$. De même pour l'autre inégalité. □

Définition : Soit un couple (X,Y) de variables aléatoires réelles discrètes, tel que X^2 et Y^2 sint d'espérances finies. On dit que X et Y ne sont pas *corrélées* si $\mathrm{Cov}(X,Y)=0$.

Théorème : Soit (X,Y) un couple de variables aléatoires tel que X^2 et Y^2 sont d'espérance finie. On a

$$X \text{ et } Y \text{ indépendantes} \implies \mathrm{E}(XY)=\mathrm{E}(X)\,\mathrm{E}(Y) \iff \mathrm{Cov}(X,Y)=0 \iff \mathrm{V}(X+Y)=\mathrm{V}(X)+\mathrm{V}(Y)$$

On a donc

$$X \text{ et } Y \text{ indépendantes} \quad \begin{array}{c}\Longrightarrow\\ \not\Longleftarrow\end{array} \quad X \text{ et } Y \text{ non corrélées.}$$

Exercice :
Soit X une variable aléatoire qui prend, de manière équiprobable, les valeurs 3 valeurs -1, 0 et 1. Soit $Y=|X|$.

1. *Calculer* $\mathrm{E}(X)$, $\mathrm{E}(Y)$, $\mathrm{E}(XY)$, $\mathrm{V}(X)$, $\mathrm{V}(Y)$, *et* $\mathrm{V}(X+Y)$.
2. *Les variables aléatoires X et Y sont-elles indépendantes ?*

1. Par équiprobabilité, $P(X=1)=P(X=0)=P(X=-1)=1/3$. Ainsi,

$$\mathrm{E}(X)=\sum_{k\in[\![-1,1]\!]} kP(X=k) = -1\times\frac{1}{3}+0\times\frac{1}{3}+1\times\frac{1}{3}=0.$$

Et,

$$\mathrm{E}(Y)=\sum_{k\in[\![-1,1]\!]} |k|\,P(X=k) = \frac{1}{3}+0+\frac{1}{3}=\frac{2}{3}$$

d'après le théorème de transfert. Or,

$$\begin{aligned}\mathrm{E}(XY) &= P(XY=1) - P(XY=-1)\\ &= P(X=1)\cdot P_{(X=1)}(Y=1) - P(X=-1)\cdot P_{(X=-1)}(Y=1)\\ &= \frac{1}{3}\times 1 - \frac{1}{3}\times 1\\ &= 0.\end{aligned}$$

Également,

$$\begin{aligned}\mathrm{V}(X) &= \mathrm{E}(X^2) - \big[\mathrm{E}(X)\big]^2\\ &= \mathrm{E}(X^2) - 0^2\\ &= (-1)^2\,P(X=-1) + 0^2\,P(X=0) + 1^2\,P(X=1)\\ &= \frac{2}{3}\end{aligned}$$

De plus,

$$\mathrm{V}(Y) = \mathrm{E}(Y^2) - \big[\mathrm{E}(Y)\big]^2 = \mathrm{E}(X^2) - \left(\frac{2}{3}\right)^2 = \frac{2}{3}\left(1-\frac{1}{3}\right) = \frac{2}{9}.$$

On calcule

$$\begin{aligned}\mathrm{V}(X+Y) &= \mathrm{V}(X) + \mathrm{V}(Y) + 2\,\mathrm{Cov}(X,Y)\\ &= \frac{2}{3} + \frac{2}{9} + 2\big(\mathrm{E}(XY) - \mathrm{E}(X)\cdot\mathrm{E}(Y)\big)\\ &= \frac{2}{3} + \frac{2}{9} + 2\underbrace{\left(0 - 0\times\frac{2}{3}\right)}_{\mathrm{Cov}(X,Y)=0}\end{aligned}$$

2. On a $\mathrm{Cov}(X,Y)=0$, les variables aléatoires X et Y ne sont pas corrélées (*i.e.* sont *décarrelées*). Mais, elles ne sont pas indépendantes :

$$\frac{1}{3} = P(X=-1, Y=1) \neq P(X=-1)\times P(Y=1) = \frac{2}{9}.$$

Corollaire : Si $X_1,\dots,X_n$ sont des variables aléatoires réelles discrètes indépendantes deux à deux, alors la variance de la somme est égale à la somme des variances :

$$\mathrm{V}(X_1+\cdots+X_n) = \mathrm{V}(X_1)+\cdots+\mathrm{V}(X_n).$$

Preuve :

$$\begin{aligned}\mathrm{V}(X_1+\cdots+X_n) &= \mathrm{Cov}(X_1+\cdots+X_n, X_1+\cdots+X_n)\\ &= \mathrm{Cov}\Big(\sum_{i=1}^n X_i, \sum_{j=1}^n X_j\Big)\\ &= \sum_{i=1}^n\sum_{j=1}^n \mathrm{Cov}(X_i,X_j) \qquad \text{par bilinéarité}\end{aligned}$$

Or, pour tout $i \neq j$, $X_i \perp\!\!\!\perp X_j$, d'où $\mathrm{Cov}(X_i,X_j)=0$. Ainsi,

$$\mathrm{V}(X_1+\cdots+X_n) = \sum_{i=1}^n \mathrm{Cov}(X_i,X_i) = \sum_{i=1}^n \mathrm{V}(X_i).$$

□

RAPPEL :
La *série génératrice* de la variable aléatoire X est G_X définie comme

$$\forall t \in]-R,R[, \quad \mathrm{G}_X(t) = \sum_{n=0}^{\infty} P(X=n)\cdot t^n.$$

De plus, on a $P(X=k) = {\mathrm{G}_X}^{(k)}(0)/k!$.

Proposition : Soient X et Y deux variables aléatoires à valeurs dans $\mathbb{N}$. Soient G_X, G_Y et G_{X+Y} les fonctions génératrices des variables aléatoires X, Y et $X+Y$. Si X et Y sont indépendantes, alors

$$\forall t \in [-1,1], \qquad \mathrm{G}_{X+Y}(t) = \mathrm{G}_X(t)\cdot \mathrm{G}_Y(t).$$

▷ Chapitre 11, entre la définition 30 et la proposition 31.

Preuve :
L'événement $(X+Y=n)$ est égal à $\bigcup_{k=0}^n \big[(X=k)\cap(Y=n-k)\big]$, et cette union est disjointe. D'où, $P(X+Y=n) = \sum_{k=0}^n P\big[(X=k)\cap(Y=n-k)\big]$. Or, $X \perp\!\!\!\perp Y$, d'où $P\big[(X=k)\cap(Y=n-k)\big] = P(X=k)\cdot P(Y=n-k)$. Ainsi,

$$P(X+Y=n) = \sum_{k=0}^n \underbrace{a_k}_{P(X=k)} \times \overbrace{b_{n-k}}^{P(Y=n-k)}.$$

Or, les séries convergent absolument, d'où, par produit de CAUCHY, $\mathrm{G}_{X+Y}(t) = \mathrm{G}_X(t)\cdot\mathrm{G}_Y(t)$, pour tout $t \in]-1,1[$. En $t=-1$, et en $t=1$,

les séries convergent absolument également. Ainsi,

$$\forall t \in [-1,1], \qquad \mathrm{G}_{X+Y}(t) = \mathrm{G}_X(t) \cdot \mathrm{G}_Y(t).$$

□

Tarte à la crème
▷ Chapitre 11, exercice 32

Exercice :
Refaire l'exercice 5, mais utiliser la proposition précédente.

1. On rappelle que $X_1 \sim \mathscr{B}(n_1, p)$, $X_2 \sim \mathscr{B}(n_2, p)$ et $X_1 \perp\!\!\!\perp X_2$. Ainsi, pour tout $t \in [-1,1]$, $\mathrm{G}_{X_1+X_2}(t) = \mathrm{G}_{X_1}(t) \cdot \mathrm{G}_{X_2}(t)$. Et, $\forall t$, $\mathrm{G}_{X_1}(t) = (pt+q)^{n_1}$ et $\mathrm{G}_{X_2}(t) = (pt+q)^{n_2}$. D'où,

   $$\forall t \in [-1,1], \quad \mathrm{G}_{X_1+X_2}(t) = (pt+q)^{n_1} \cdot (pt+q)^{n_2} = (pt+q)^{n_1+n_2}.$$

   Par égalité des séries génératrices [1], on en déduit que $X+Y \sim \mathscr{B}(n_1+n_2, p)$.
2. De même, comme $X_1 \sim \mathscr{P}(\lambda_1)$, $\forall t$, $\mathrm{G}_{X_1}(t) = \mathrm{e}^{-\lambda_1} \cdot \mathrm{e}^{-\lambda_1 t}$; et comme $X_2 \sim \mathscr{P}(\lambda_2)$, $\forall t$, $\mathrm{G}_{X_2}(t) = \mathrm{e}^{-\lambda_2} \cdot \mathrm{e}^{-\lambda_2 t}$. De plus, $X_1 \perp\!\!\!\perp X_2$, d'où $\forall t \in [-1,1], \mathrm{G}_{X_1+X_2}(t) = \mathrm{G}_{X_1}(t) \times \mathrm{G}_{X_2}(t) = \mathrm{e}^{-(\lambda_1+\lambda_2)} \cdot \mathrm{e}^{-(\lambda_1+\lambda_2)t}$. D'où, $X_1 + X_2 \sim \mathscr{P}(\lambda_1+\lambda_2)$.

VII.4 La loi faible des grands nombres

Théorème (Loi faible des grands nombres) **:** Soit $(\Omega, \mathscr{A}, P)$ un espace probabilisé. Soient $(X_k)_{n\in\mathbb{N}}$ une suite de variables aléatoires discrètes. Et, pour tout $n \in \mathbb{N}^\star$, $Z_n = \frac{1}{n}\sum_{k=1}^n X_k$. Si les variables aléatoires sont deux à deux indépendantes, et si elles sont de même espérance μ, et de même variance σ^2, alors

$$\forall a > 0, \qquad P(|Z_n - \mu| \geqslant a) \leqslant \frac{1}{n} \cdot \left(\frac{\sigma}{a}\right)^2 \xrightarrow[n\to\infty]{} 0.$$

« S'éloigner de la moyenne théorique est de plus en plus rare en itérant les mesures. »

Preuve :
On applique l'inégalité de Bienaimé-Thebychev à la variable aléatoire Z_n :

$$\forall a > 0, \qquad P\big(\big|Z_n - \mathrm{E}(Z_n)\big| \geqslant a\big) \leqslant \frac{\mathrm{V}(Z_n)}{a^2}.$$

Or, $\mathrm{E}(Z_n) = \frac{1}{n}\sum_{i=1}^n \mathrm{E}(X_i) = \frac{1}{n} \cdot n\mu = \mu$ par linéarité de l'espérance. De

1. En effet, la série génératrice permet de déterminer les probabilités, d'où la loi d'une variable aléatoire.

plus,

$$\begin{aligned}
\mathrm{V}(Z_n) &= \mathrm{V}\left(\frac{X_1+\cdots+X_n}{n}\right)\\
&= \frac{1}{n^2}\mathrm{V}(X_1+\cdots+X_n)\\
&= \frac{1}{n^2}\big(\mathrm{V}(X_1)+\cdots+\mathrm{V}(X_n)\big) \quad \text{par indépendance deux à deux des } X_i\\
&= \frac{1}{n^2}\cdot n\sigma^2\\
&= \frac{\sigma^2}{n}.
\end{aligned}$$

D'où, $\forall a>0,\ P\big(|Z_n-\mu|\geqslant a\big)\leqslant \sigma^2/(n\cdot a^2)$. □

Exemple (Règle d'or de Bernoulli) :
On répète indépendamment une épreuve de Bernoulli, c'est à dire une expérience aléatoire qui peut donner deux résultats : un succès avec la probabilité p, ou un échec avec la probabilité $q=1-p$. Soit Z_n la *fréquence*[2] des succès après n épreuves.

On pose X_k la variable aléatoire valant 1 en cas de succès de la k-ième épreuve de Bernoulli, 0 sinon. D'une part, $\mu=\mathrm{E}(X_i)=0\times P(X_i=0)+1\times P(X_i=1)=p$. D'autre part, $\sigma^2=\mathrm{V}(X_i)=p\cdot q$ car $X_i\sim\mathscr{B}(1,p)$. On applique la loi faible des grands nombres :

$$\forall a>0,\qquad P(|Z_n-p|\geqslant a)\leqslant \frac{pq}{na^2}\xrightarrow[n\to\infty]{}0.$$

Donc la probabilité que « la fréquence Z_n des succès s'écarte de la probabilité p » tend vers 0 quand le nombre n d'épreuves de Bernoulli tend vers $+\infty$.

2. *i.e.* le nombre moyens de succès : $\frac{1}{n}\sum_{i=1}^{n}X_i$.

Chapitre 15

Calcul différentiel

Exemple :
Dans le plan $\mathbb{R}^2$, soit $\mathscr{C}$ le cercle de centre $(0,0)$ et de rayon 1 :

$$(x,y) \in \mathscr{C} \iff \underbrace{x^2+y^2=1}_{\text{équation implicite}} \iff \overbrace{\exists t \in \mathbb{R}, \begin{cases} x = \cos t \\ y = \sin t. \end{cases}}^{\text{équations paramétrées}}$$

Plus généralement, soient deux réels $a > 0$ et $b > 0$. La courbe $\mathscr{E}$ d'équation implicite

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

est appelée *ellipse*. Elle est représentée sur la figure ci-dessous. C'est aussi une *courbe paramétrée* :

$$(x,y) \in \mathscr{E} \iff \exists t \in \mathbb{R}, \begin{cases} x = a\cos t \\ y = b\sin t. \end{cases}$$

Les deux courbes sont *bornées*. On peut passer de $\mathscr{C}$ à $\mathscr{E}$ au moyen des changements de variables $X = x/a$ et $Y = y/b$. On nomme a le « demi grand axe » et b le « demi petit axe » de l'ellipse $\mathscr{E}$.

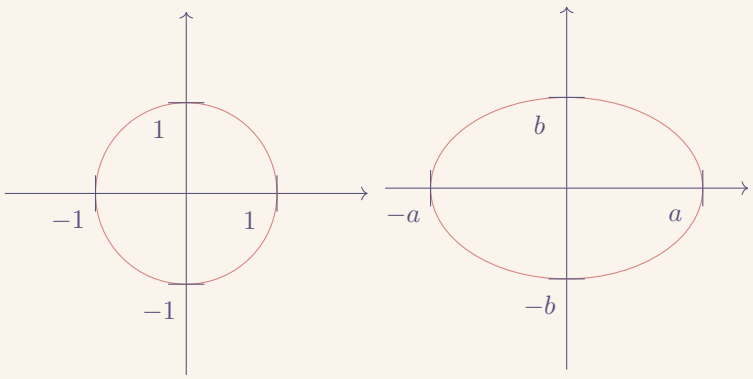


FIGURE 15.1 – Cercle $\mathscr{C}$ et ellipse $\mathscr{E}$

EXEMPLE :
Soient deux réels $a>0$ et $b>0$. La courbe $\mathscr{H}$ d'équation implicite

$$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1$$

est appelée *hyperbole*. Elle est représentée sur la figure ci-dessous. Cette hyperbole est la réunion de deux branches $\mathscr{H}_+=\{(x,y)\in\mathscr{H}\mid x\geqslant 0\}$ et $\mathscr{H}_-=\{(x,y)\in\mathscr{H}\mid x\leqslant 0\}$. La courbe $\mathscr{H}_+$ est une courbe paramétrée

$$(x,y)\in\mathscr{H}_+ \iff \exists t\in\mathbb{R},\ \begin{cases}x=a\operatorname{ch}t\\ y=b\operatorname{sh}t.\end{cases}$$

L'hyperbole $\mathscr{H}$ possède deux asymptotes $\frac{y}{b}=\frac{x}{a}$ et $\frac{y}{b}=-\frac{x}{a}$.

$$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1 \iff X^2-Y^2=1 \quad \text{où } \begin{cases}X=x/a\\ Y=y/b\end{cases}$$

$$\iff U\cdot V=1 \quad \text{où } \begin{cases}U=X+Y\\ V=X-Y\end{cases}$$

$$\iff V=\frac{1}{U}$$

L'hyperbole $\mathscr{H}$ a une *zone interdite* entre -1 et 1. En effet

$$X^2-Y^2=1 \iff X^2=1+Y^2 \implies X^2\geqslant 1.$$

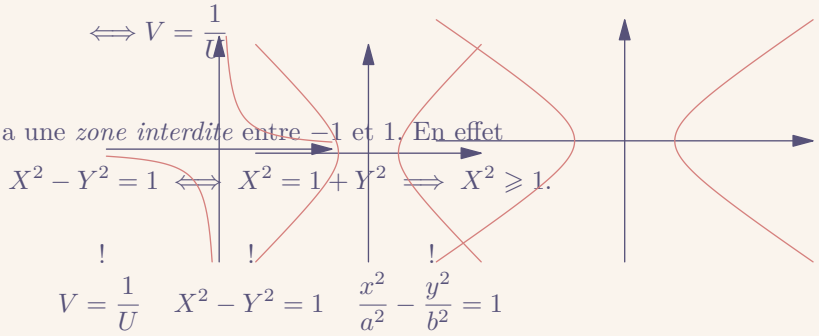


FIGURE 15.2 – Hyperboles

Définition : Soit $D \subset \mathbb{R}^2$ une partie du plan et soit $f : D \to \mathbb{R}$ une fonction définie sur D. Pour chaque réel K, la *courbe de niveau* K de la fonction f est l'ensemble C_K des points $(x, y) \in D$ tels que

$$f(x, y) = K.$$

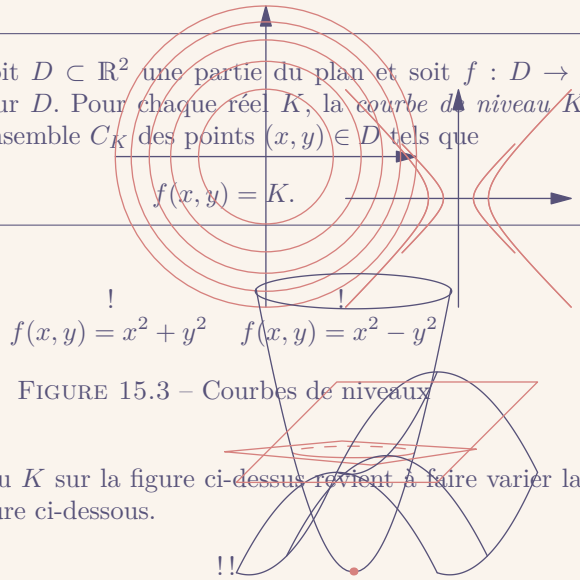


FIGURE 15.3 – Courbes de niveaux

Faire varier le niveau K sur la figure ci-dessus revient à faire varier la hauteur K du plan de la figure ci-dessous.

FIGURE 15.4 – L'intersection d'un paraboloïde et d'un plan (à gauche), d'une selle de cheval et d'un plan (à droite)

VII.1 Dérivées partielles

VII.2 Dérivées partielles

Définition : Soit $D \subset \mathbb{R}^2$ un ouvert, et soit $f : D \to \mathbb{R}, (x, y) \mapsto f(x, y)$ une fonction. Soit un point $(a, b) \in D$.

1. Si
$$\lim_{h \to 0} \frac{f(a+h, b) - f(a, b)}{h}$$
existe et est finie, alors ce nombre réel est noté $\partial_1 f(a, b)$ ou $\frac{\partial f}{\partial x}$ et est appelé la première *dérivée partielle* de f en (a, b).
2. Si
$$\lim_{h \to 0} \frac{f(a, b+h) - f(a, b)}{h}$$
existe et est finie, alors ce nombre réel est noté $\partial_2 f(a, b)$ ou $\frac{\partial f}{\partial y}$ et est appelé la seconde *dérivée partielle* de f en (a, b).
3. Pour $i \in [\![1, 2]\!]$, si $\partial_i f(a, b)$ existe pour tout $(a, b) \in D$, alors al fonction $\partial_i f : D \to \mathbb{R}$ est appelée la i-ème *dérivée partielle* de f.
4. On dit que la fonction f est de classe $\mathscr{C}^1$ sur D si les deux dérivées partielles $\partial_1 f$ et $\partial_2 f$ existent et sont continues sur D.

EXERCICE (Une fonction qui possède des dérivées partielles non continues) : *Soit $f : \mathbb{R}^2 \to \mathbb{R}$ la fonction définie par*

$$f(x, y) = x^2 \cdot \sin\left(\frac{y}{x}\right) \quad \text{si } x \neq 0 \quad \text{et} \quad f(0, y) = 0 \text{ sinon.}.$$

1. *Montrer que f est continue sur $\mathbb{R}^2$.*
2. *Montrer que les dérivées partielles $\partial_1 f(x,y)$ et $\partial_2 f(x,y)$ existent si $x \neq 0$, et les calculer.*
3. *Montrer que les dérivées partielles $\partial_1 f(0,y)$ et $\partial_2 f(0,y)$ existent et les calculer.*
4. *Montrer que la fonction f n'est pas de classe $\mathscr{C}^1$.*

1. La fonction f est continue sur $\mathbb{R}^\star \times \mathbb{R}$ d'après les théorèmes généraux (par produit et par composition). Montrons que $f(0+h, y+k) \xrightarrow[(h,k)\to(0,0)]{} f(0,y)$, *i.e.* $|f(0+h,y+k) - f(0,y)| \to 0$. On a
$$\begin{aligned} 0 \leqslant |f(0+h,y+k) - f(0,y)| &= \left| h^2 \sin\left(\frac{y+k}{h}\right) - 0 \right| \\ &= h^2 \left| \sin\left(\frac{y+k}{h}\right) \right| \\ &\leqslant h^2 \leqslant \sqrt{h^2+k^2}^2 \leqslant \|(h,k)\|_2^2 \end{aligned}$$
D'après le théorème des gendarmes, f est continue en $(0,y)$, f est donc continue sur $\mathbb{R}^2$.
2. En tout point de $\mathbb{R}^2 \times \mathbb{R}$, $\partial_1 f$ et $\partial_2 f$ existent par composition et par produit. Et,
$$\begin{aligned} \partial_1 f(x,y) &= \frac{\partial f}{\partial x}(x,y) \\ &= 2x \sin\left(\frac{y}{x}\right) + x^2 \times \frac{-y}{x^2} \cos\left(\frac{y}{x}\right) \\ &= 2x \sin\left(\frac{y}{x}\right) - y \cos\left(\frac{y}{x}\right) \end{aligned} \qquad \begin{aligned} \partial_2 f(x,y) &= \frac{\partial f}{\partial y}(x,y) \\ &= x^2 \cdot \frac{1}{x} \cdot \cos\left(\frac{y}{x}\right) \\ &= x \cos\left(\frac{y}{x}\right) \end{aligned}$$
3. Calculons
$$\frac{f(0+h,y) - f(0,y)}{h} = \frac{h^2 \sin\left(\frac{y}{h}\right) - 0}{h} = h \sin\left(\frac{y}{h}\right) \xrightarrow[h\to 0]{} 0$$
car $h \to 0$ et sin est borné. D'où, $\partial_1 f(0,y)$ existe et $\partial_1 f(0,y) = 0$. De plus, $\big[f(0,y+h) - f(0,y)\big]/k = (0-0)/k = 0 \xrightarrow[k\to 0]{} 0$. D'où $\partial_2 f(0,y)$ existe et $\partial_2 f(0,y) = 0$.
4. On a $\partial_1 f(x,1) \xrightarrow[x\to 0]{\not\longrightarrow} \partial_1 f(0,1)$ car $1 \times \cos\left(\frac{1}{x}\right)$ n'a pas de limite.

Théorème (Formule de Taylor & Young à l'ordre 1) **:** Soit $D \subset \mathbb{R}^2$ un ouvert, et soit $f : D \to \mathbb{R}$ une fonction. Si f est de classe $\mathscr{C}^1$, alors, pour tout $(a,b) \in D$,
$$f(a+h,b+k) = f(a,b) + h\,\partial_1 f(a,b) + k\,\partial_2 f(a,b) + \underbrace{\|(h,k)\| \cdot \varepsilon(h,k)}_{o(h,k)}$$

où $\varepsilon(h,k) \xrightarrow[(h,k)\to(0,0)]{} 0$.

RAPPEL (Accroissements finis) :
Si φ est une fonction continue sur un segment $[\alpha,\beta]$, et qu'elle est dérivable sur $]\alpha,\beta[$, alors il existe $c \in]\alpha,\beta[$ tel que

$$\varphi(\beta) - \varphi(\alpha) = \varphi'(c)\cdot(\beta-\alpha).$$

Preuve :
On a $f(a+h,b+k) - f(a,b) = \big[f(a+h,b+k) - f(a,b+k)\big] + \big[f(a,b+k) - f(a+k,b+k)\big]$. Soit $\varphi(\vec{x}) = f(x,b+k)$. Alors, d'après le théorème des accroissements finis, il existe $c \in]a,a+h[$ tel que $\varphi(a+h)-\varphi(a) = \varphi'(c)\cdot\big((a+h)-a\big)$. D'où, $f(a+h,b+k)-f(a,b+k) = \partial_1 f(c,b+k)\times h$. De même, soit $\psi(y) = f(a,y)$; alors, il existe $d \in]b,b+k[$ tel que $f(a,b+k)-f(a,b) = \partial_2 f(a,d)\times k$. Or, f est de classe $\mathscr{C}^1$, d'où $\partial_1 f(c,b+k) \to \partial_1 f(a,b)$ quand $(h,k)\to(0,0)$, car $(c,b+k)\to(a,b)$ et $\partial_1 f$ est continue. De même, $\partial_2 f(a,d) \to \partial_2 f(a,b)$ quand $(h,k)\to(0,0)$. Ainsi, $\partial_1 f(c,b+k) = \partial_1 f(a,b) + \varepsilon_1(h,k)$ où $\varepsilon_1(h,k)\to 0$ quand $(h,k)\to(0,0)$. De même, $\partial_2 f(a,d) = \partial_2 f(a,b) + \varepsilon_2(h,k)$ avec $\varepsilon(h,k)\to 0$ quand $(h,k)\to(0,0)$. On a donc $f(a+h,b+k)-f(a,b) = h\,\partial_1 f(a,b) + h\,\varepsilon_1(h,k) + k\,\partial_2 f(a,b) + k\,\varepsilon_2(h,k)$. On pose $R(h,k)$ le reste.

$$\begin{aligned} 0 \leqslant |R(h,k)| &\leqslant |h|\cdot|\varepsilon_1(h,k)| + |k|\cdot|\varepsilon_2(h,k)| \\ &\leqslant \sqrt{h^2+k^2} \times \underbrace{\big[|\varepsilon_1(h,k)| + |\varepsilon_2(h,k)|\big]}_{\varepsilon(h,k)} \\ &= \|(h,k)\|\cdot\varepsilon(h,k) = \mathrm{o}(h,k) \end{aligned}$$

□

REMARQUE : 1. (fonctions de $\mathbb{R}^p$ vers $\mathbb{R}$) Soit $p \in \mathbb{N}^\star$. De même que les fonctions de $\mathbb{R}^2$ vers $\mathbb{R}$, on peut étudier une fonction de $\mathbb{R}^p$ vers $\mathbb{R}$, définir ses p dérivées partielles $\partial_1 f, \dots, \partial_p f$ si elles existent, et dire que la fonction f est de classe $\mathscr{C}^1$ sur un ouvert $U \subset \mathbb{R}^p$ si ses p dérivées partielles sont continues.

D'après la formule de Taylor & Young, si la fonction f est de classe $\mathscr{C}^1$ sur U, alors : en tout point $\vec{a} = (a_1,\dots,a_p) \in U$,

$$f(\vec{a}+\vec{h}) = f(\vec{a}) + h_1\,\partial_1 f(\vec{a}) + \cdots + h_p\,\partial_p f(\vec{a}) + \mathrm{o}(\vec{h})$$

où $\vec{h} = (h_1,\dots,h_p)$.

2. (fonctions de $\mathbb{R}^p$ vers $\mathbb{R}^n$) Soient $p \in \mathbb{N}^\star$ et $n \in \mathbb{N}^\star$, un ouvert $U \subset \mathbb{R}^p$ et

une fonction

$$\begin{aligned} f : U &\longrightarrow \mathbb{R}^n \\ \vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} &\longmapsto \begin{pmatrix} f_1(\vec{x}) \\ \vdots \\ f_n(\vec{x}) \end{pmatrix} \end{aligned}$$

Soit $\vec{a} \in U$. Si chacune des n fonctions $f_i : U \to \mathbb{R}$ est de classe $\mathscr{C}^1$ sur U, alors

$$\forall i \in [\![1, n]\!], \qquad f_i(\vec{a}+\vec{h}) = f_i(\vec{a}) + h_1\,\partial_1 f_i(\vec{a}) + \cdots + h_p\,\partial_p f_i(\vec{a}) + \wp(\vec{h}).$$

Matriciellement, cette égalité s'écrit

$$\underbrace{\begin{pmatrix} f_1(\vec{a}+\vec{h}) \\ \vdots \\ f_n(\vec{a}+\vec{h}) \end{pmatrix}}_{f(\vec{a}+\vec{h})} = \underbrace{\begin{pmatrix} f_1(\vec{a}) \\ \vdots \\ f_n(\vec{a}) \end{pmatrix}}_{f(\vec{a})} + \underbrace{\begin{pmatrix} \partial_1 f_1(\vec{a}) & \cdots & \partial_p f_1(\vec{a}) \\ \vdots & \ddots & \vdots \\ \partial_1 f_n(\vec{a}) & \cdots & \partial_p f_n(\vec{a}) \end{pmatrix}}_{\mathrm{J}_f(\vec{a})} \cdot \underbrace{\begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix}}_{\vec{h}} + \|\vec{h}\| \cdot \underbrace{\begin{pmatrix} \varepsilon_1(\vec{h}) \\ \vdots \\ \varepsilon_n(\vec{h}) \end{pmatrix}}_{\varepsilon(\vec{h})}.$$

Définition : Soit f une fonction définie sur un ouvert $U \subset \mathbb{R}^p$ comme

$$\begin{aligned} f : U &\longrightarrow \mathbb{R}^n \\ \vec{x} = (x_1, \ldots, x_p) &\longmapsto \big(f_1(\vec{x}), \ldots, f_n(\vec{x})\big). \end{aligned}$$

Si chaque fonction f_i admet p dérivées partielles en $\vec{a}$, alors la matrice $\mathrm{J}_f(\vec{a}) \in \mathscr{M}_{n,p}(\mathbb{R})$ définie par $\big(\mathrm{J}_f(\vec{a})\big)_{i,j} = \frac{\partial f_i}{\partial x_j}(\vec{a})$, pour tout $i \in [\![1, n]\!]$ et $j \in [\![1, p]\!]$, est appelée *jacobienne* de f en $\vec{a}$.

$$\begin{array}{c} \\ \nabla f_1 \to \\ \vdots \\ \nabla f_n \to \end{array} \begin{array}{c} \begin{array}{ccc} \partial_1 f(\vec{a}) & \cdots & \partial_p f(\vec{a}) \end{array} \\ \downarrow \qquad\qquad \downarrow \\ \begin{pmatrix} \partial_1 f_1(\vec{a}) & \cdots & \partial_p f_1(\vec{a}) \\ \vdots & \ddots & \vdots \\ \partial_1 f_n(\vec{a}) & \cdots & \partial_p f_n(\vec{a}) \end{pmatrix} \end{array} = \mathrm{J}_f(\vec{a}).$$

Exemple :
La fonction

$$\begin{aligned} M : \mathbb{R}_\star^+ \times \mathbb{R} &\longrightarrow \mathbb{R}^2 \\ (r, \varphi) &\longmapsto (x, y) = (r\cos\varphi, r\sin\varphi) \end{aligned}$$

change les coordonnées polaires (r, φ) en coordonnées cartésiennes (x, y). La fonction M possède des dérivées partielles et sa matrice jacobienne est

$$\mathrm{J}_M(r,\varphi) = \begin{pmatrix} \frac{\partial x}{\partial r}(r,\varphi) & \frac{\partial x}{\partial \varphi}(r,\varphi) \\ \frac{\partial y}{\partial r}(r,\varphi) & \frac{\partial y}{\partial \varphi}(r,\varphi) \end{pmatrix} = \begin{array}{c} \begin{array}{cc} \frac{\partial M}{\partial r} & \frac{\partial M}{\partial \varphi} \end{array} \\ \downarrow \qquad \downarrow \\ \begin{pmatrix} \cos\varphi & -r\sin\varphi \\ \sin\varphi & r\cos\varphi \end{pmatrix} \end{array}.$$

Ses vecteurs colonnes sont représentés sur la figure ci-dessous. Le vecteur $\frac{\partial M}{\partial r}$ est tangent à la droite paramétrée par $r \mapsto M(r,\varphi)$; le vecteur $\frac{\partial M}{\partial \varphi}$ est tangent au cercle paramétré par $\varphi \mapsto M(r,\varphi)$.

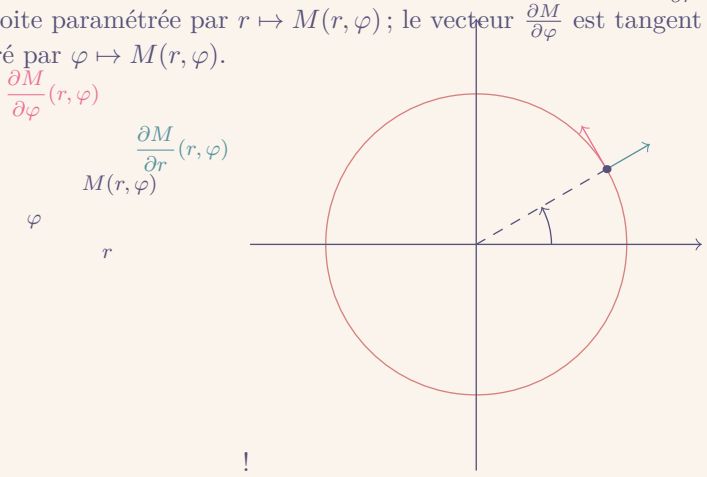


FIGURE 15.5 – Coordonnées polaires

VII.3 La différentielle d'une fonction

Dans toute la suite, E et F sont des espaces vectoriels normés de dimensions finies $p = \dim E$ et $n = \dim F$. Si l'on choisit une base de E et une base de F, alors on pourra confondre $\vec{x} \in E$ et $(x_1, \dots, x_p) \in \mathbb{R}^p$ d'une part, et $f(\vec{x}) \in F$ et $\big((f_1(\vec{x}), \dots, f_n(\vec{x})\big) \in \mathbb{R}^n$ d'autre part.

Proposition–Définition : Soient U un ouvert de E, un point $\vec{a} \in U$, et une fonction $f : U \to F$. On dit que f est *différentiable* en $\vec{a}$ s'il existe une application linéaire $\ell_{\vec{a}} : E \to F$ telle que

$$f(\vec{a}+\vec{h}) = f(\vec{a}) + \ell_{\vec{a}}(\vec{h}) + \wr(\vec{h}).$$

Si f est différentiable en $\vec{a}$, alors

1. l'application $\ell_{\vec{a}}$ est unique, on l'appelle *la différentielle* de f en $\vec{a}$, et on note

$$\begin{aligned} \ell_{\vec{a}} = \mathrm{d}f(\vec{a}) : E &\longrightarrow F \\ \vec{h} &\longmapsto \ell_{\vec{a}}(\vec{h}) = \mathrm{d}f(\vec{a}) \cdot \vec{h}\ ; \end{aligned}$$

2. les dérivées partielles de f en $\vec{a}$ existent et

$$\forall \vec{h} \in E, \qquad \mathrm{d}f(\vec{a}) \cdot \vec{h} = h_1\, \partial_1 f(\vec{a}) + \cdot + h_p\, \partial_p f(\vec{a}) = \sum_{i=1}^{p} h_i\, \partial_i f(\vec{a}).$$

Preuve :

1ère preuve de l'unicité. Supposons qu'il existe L_1 et L_2 deux applications linéaires telles que, pour tout vecteur $\vec{h}$, $f(\vec{a}+\vec{h}) = f(\vec{a}) + L_1(\vec{h}) + \wp(\vec{h})$ et $f(\vec{a}+\vec{h}) = f(\vec{a}) + L_2(\vec{h}) + \wp(\vec{h})$. Montrons que $L_1 = L_2$. On soustrait les deux expressions de $f(\vec{a}+\vec{h})$ et on trouve $\vec{0} = \vec{0} + L_1(\vec{h}) - L_2(\vec{h}) + \wp(\vec{h})$. On fixe $\vec{h} \in E$, et soit $t \in \mathbb{R}^\star$: $L_1(t\vec{h}) - L_2(t\vec{h}) = \wp(t\vec{h}) = \|t\vec{h}\|\varepsilon(t\vec{h})$. Ainsi, par homogénéité de la norme et par linéarité de L_1 et L_2, on a $tL_1(\vec{h}) - tL_2(\vec{h}) = |t|\cdot\|\vec{h}\|\cdot\varepsilon(t\vec{h})$. Ainsi, $L_1(\vec{h}) - L_2(\vec{h}) = \|\vec{h}\|\cdot\hat{\varepsilon}(t\vec{h})$ où $\hat{\varepsilon}(t\vec{h}) = \pm\varepsilon(t\vec{h})$. On fait tendre t vers 0, et donc $L_1(\vec{h}) - L_2(\vec{h}) \to 0$. D'où, $L_1(\vec{h}) - L_2(\vec{h}) = \vec{0}$ pour tout vecteur $\vec{h} \in E$. On en déduit $L_1 = L_2$.

2nde preuve de l'unicité & formule. Soit $\ell_{\vec{a}}$ une application linéaire telle que $f(\vec{a}+\vec{h}) = f(\vec{a}) + \ell_{\vec{a}}(\vec{h}) + \|\vec{h}\|\,\varepsilon(\vec{h})$, pour tout vecteur $\vec{h} \in E$. En particulier, on pose $\vec{h} = t\,\vec{e}_i$, où $\vec{e}_i$ est l'un des vecteurs d'une base de E, et $t \in \mathbb{R}^\star$. Ainsi, $f(\vec{a}+t\vec{e}_i) = f(\vec{a}) + \ell_{\vec{a}}(t\vec{e}_i) + \|t\vec{e}_i\|\,\varepsilon(t\vec{e}_i)$. En développant, on trouve $f(a_1,\dots,a_{i-1},a_i+t,a_{i+1},\dots,a_p) - f(a_1,a_2,\dots,a_{i-1},a_i,a_{i+1},\dots,a_p) = t\ell_{\vec{a}}(\vec{e}_i) + |t|\,\|\vec{e}_i\|\,\varepsilon(t\vec{e}_i)$, par linéarité de $\ell_{\vec{a}}$ et par homogénéité de la norme. On divise par t et on trouve

$$\frac{f(a_1,\dots,a_{i-1},a_i+t,a_{i+1},\dots,a_p) - f(a_1,a_2,\dots,a_{i-1},a_i,a_{i+1},\dots,a_p)}{t} = \ell_{\vec{a}}(\vec{e}_i) + \|\vec{e}_i\|\,\hat{\varepsilon}(t\vec{e}_i) \xrightarrow[t\to 0]{} \ell_{\vec{a}}(\vec{e}_i)$$

D'où, $\partial_i f(\vec{a})$ existe et vaut $\ell_{\vec{a}}(\vec{e}_i)$.

Si $\vec{h}$ est quelconque, alors on pose $\vec{h} = h_1\vec{e}_1 + \cdots + h_p\vec{e}_p$. Par linéarité de $\ell_{\vec{a}}$, on a

$$\mathrm{d}f(\vec{a})\cdot\vec{h} = \ell_{\vec{a}}(\vec{h}) = h_1\ell_{\vec{a}}(\vec{e}_1) + \cdots + h_p\ell_{\vec{a}}(\vec{e}_p) = h_1\partial_1 f(\vec{a}) + \cdots + h_p\,\partial_p f(\vec{a}).$$

□

Exemple : 1. La fonction

$$\begin{aligned} f : \mathscr{M}_n(\mathbb{R}) &\longrightarrow \mathscr{M}_n(\mathbb{R}) \\ A &\longmapsto A^2 \end{aligned}$$

est différentiable en chaque point $A \in \mathscr{M}_n(\mathbb{R})$ et $\mathrm{d}f(A)\cdot H = AH + HA$. En effet, $f(A+H) = (A+H)^2 = A^2 + AH + HA + H^2 = f(A) + [AH + HA] + H^2$. La formule entre crochets est linéaire en H, et dépend de A, on la note $\ell_A(H)$. Et, montrons que $H^2 = \wp(H)$ *i.e.* $H^2 = \|H\|\varepsilon(H)$, avec $\varepsilon(H) \to 0$ quand $H \to 0$. Montrons alors que $H^2/\|H\| \to 0$ quand $H \to 0$, *i.e.* montrons que $\|H^2\|/\|H\| \to 0$ quand $\|H\| \to 0$.[1] On choisit une norme sous-multiplicative. Alors, $\|H^2\| \leqslant \|H\| \times \|H\|$. D'où, $0 \leqslant \|H^2\|/\|H\| \leqslant \|H\|^2/\|H\| \leqslant \|H\|$. Par le théorème des gendarmes, on a bien $\|H^2\|/\|H\| \to 0$ quand $H \to 0$.

1. L'enjeu est de choisir une norme adaptée à la question : toutes les normes sont

Rappel (comatrice) :

$$\det A = \begin{matrix} \\ i \to \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} j \\ \downarrow \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix}$$

$$= (-1)^{1+j} a_{1j} \Delta_{1j} + (-1)^{2+j} a_{2j} \Delta_{2j} + \cdots + (-1)^{n+j} a_{n,j} \Delta_{n,j}$$

$$= \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \Delta_{i,j},$$

où la matrice $\Delta_{i,j}$ est le déterminant de la matrice carrée obtenue en supprimant la colonne j et la ligne i. La matrice $\Delta_{i,j}$ s'appelle le *mineur* ; le *cofacteur* est le terme $(-1)^{i+j}\Delta_{i,j}$. Si $j \neq k$, alors $\sum_{i=1}^{n}(-1)^{i+j} a_{i,k}\Delta_{i,j} = 0$, car il s'agit du déterminant où deux colonnes sont égales. Ainsi, $\sum_{i=1}^{n}(-1)^{i+j} a_{i,k}\Delta_{i,j} = \det(A)\cdot\delta_{j,k}$, où $\delta_{j,k}$ est le symbole de Kronecker. On pose $b_{j,i} = (-1)^{i+j}\Delta_{i,j}$, et on a donc $\sum_{i=1}^{n}(-1)^{i+j} a_{i,k}\Delta_{i,j} = \sum_{i=1}^{n} b_{i,j} a_{i,k}$. En nommant $(b_{j,i}) = B$, on trouve donc $B \cdot A = \det(A)\cdot I_n$. Si $\det A \neq 0$, alors

$$\left(\frac{1}{\det A} B\right) \cdot A = I_n \qquad \text{et donc} \qquad A^{-1} = \frac{1}{\det A} B.$$

La *comatrice* est la matrice B transposée : $[\operatorname{com} A]_{i,j} = (-1)^{i+j}\cdot\Delta_{i,j}$ Avec cette définition, on a donc

$$A^{-1} = \frac{1}{\det A} \cdot (\operatorname{com} A)^{\top}.$$

Rappel (déterminant) :

$$\det A = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Exercice : 1. *Soient $H \in \mathscr{M}_n(\mathbb{R})$ et I_n la matrice identité. Montrer que*

$$\det(I_n + H) = 1 + \operatorname{tr} H + \wp(H).$$

2. *En déduire que la fonction* det : $\mathscr{M}_n(\mathbb{R}) \to \mathbb{R}$ *est différentiable en I_n. Quelle est sa différentielle en I_n ?*
3. *Soit $A \in \mathscr{M}_n(\mathbb{R})$ une matrice inversible. Montrer que* det *est différentiable en A. Quelle est sa différentielle en A ?*

équivalentes en dimension finie.

1. On calcule, en utilisant la formule du déterminant rappelée précédemment :

$$\begin{aligned}\det(I_n + H) &= \begin{vmatrix} 1+h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & 1+h_{22} & \dots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n1} & h_{n2} & \dots & 1+h_{nn} \end{vmatrix} \\ &= 1 + (h_{11} + h_{22} + \cdots + h_{nn}) + \text{termes d'ordre supérieur ou égal à 2 en } h \\ &= 1 + \operatorname{tr} H + \wp(H)\end{aligned}$$

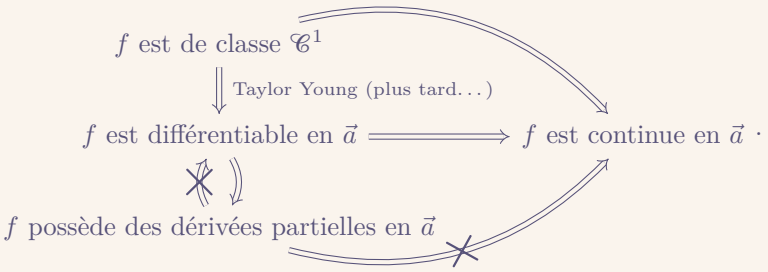
2. Or, tr est une forme linéaire, donc det est différentiable en I_n et $\mathrm{ddet}(I_n) \cdot H = \operatorname{tr} H$ (oui, c'est moche).
3. Comme $A \in \mathrm{GL}_n(\mathbb{R})$, on a

$$\begin{aligned}\det(A+H) = \det\big(A \cdot (I_n + A^{-1} \cdot H)\big) &= \det A \times \det(I_n + A^{-1} \cdot H) \\ &= \det A \times (1 + \operatorname{tr}(A^{-1}H) + \text{reste}') \\ &= \det A + \det A \times \operatorname{tr}(A^{-1}H) + \text{reste}\end{aligned}$$

où reste $= \det(A) \cdot \|A^{-1}H\|\varepsilon(A^{-1}H) = \|H\|\varepsilon'(H)$ car $\|A^{-1}H\| \leqslant \|A^{-1}\| \times \|H\|$ en choisissant une norme sous-multiplicative et $\|A^{-1}\| \times \det(A)\varepsilon(A^{-1}H) \to 0$ quand $H \to 0$ car $A^{-1}H \to 0$, car $0 \leqslant \|A^{-1}H\| \leqslant \|H\| \to 0$ quand $\|H\| \to 0$ avec la norme sous-multiplicative. Donc, det est différentiable en $A \in \mathrm{GL}_n(\mathbb{R})$ et

$$\mathrm{ddet}(A) \cdot H = \det(A) \times \operatorname{tr}(A^{-1}H).$$

Proposition :



Preuve :
Supposons f différentiable en $\vec{a}$. Montrons que f est continue en $\vec{a}$. On sait que $f(\vec{a}+\vec{h}) = f(\vec{a}) + \mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\|\varepsilon(\vec{h})$. Montrons que $f(\vec{a}+\vec{h}) \to f(\vec{a})$ quand $\vec{a} \to \vec{h}$. Montrons donc que $f(\vec{a}+\vec{h}) - f(\vec{a}) = \hat{\varepsilon}(\vec{h})$. Or, $f(\vec{a}+\vec{h}) - f(\vec{a}) = \mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\|\varepsilon(\vec{h})$. On a $\|\vec{h}\|\varepsilon(\vec{h}) \to 0$ quand $\vec{h} \to \vec{0}$. Et, $\mathrm{d}f(\vec{a})$ est linéaire sur un espace vectoriel de dimension finie, donc $\mathrm{d}f(\vec{a})$ est continue,

d'où $\mathrm{d}f(\vec{a})\cdot\vec{h} \to \mathrm{d}f(\vec{a})\cdot\vec{0} = \vec{0}$ car $\mathrm{d}f(\vec{a})$ est linéaire. D'où,

$$f(\vec{a}+\vec{h}) - f(\vec{a}) = \underbrace{\mathrm{d}f(\vec{a})\cdot\vec{h}}_{\to 0} + \underbrace{\|\vec{h}\|\varepsilon(\vec{h})}_{\to 0} \xrightarrow[\vec{h}\to\vec{0}]{} \vec{0}.$$

□

Exercice (Une fonction qui possède des dérivées partielles, mais pas continue) :
Soit la fonction $f : \mathbb{R}^2 \to \mathbb{R}$ *définie par*

$$f(x,y) = \frac{xy}{x^2+y^2} \text{ si } (x,y) \neq (0,0) \qquad \text{et} \qquad f(0,0) = 0.$$

Montrer que la fonction f *possède des dérivées partielles* $\partial_1 f(0,0)$ *et* $\partial_2 f(0,0)$ *en* $(0,0)$ *mais que* f *n'est pas continue en* $(0,0)$.

La fonction f n'est pas continue en $(0,0)$ car $f(x,x) \to \frac{1}{2} \neq f(0,0)$ quand $x \to 0$. D'une part, $\big(f(0+h,0) - f(0,0)\big)/h = \big(f(h,0)\big)/h = 0/h = 0 \to 0$, lorsque $h \to 0$. D'où, $\partial_1 f(0,0)$ existe et $\partial_1 f(0,0) = 0$. De même, $\partial_2 f(0,0) = 0$ par symétrie.

Remarque :
Soit a un élément de $I \subset \mathbb{R}$ un intervalle ouvert. Une fonction $f : I \to \mathbb{R}$ est dérivable en a si, et seulement si elle est différentiable en a. Et alors, $f'(a) = \mathrm{d}f(a)\cdot 1$.

Définition : Si $f : E \to F$ est une fonction différentiable en chaque point $\vec{a} \in U$ d'une partie $U \subset E$, alors on dit que f est *différentiable* sur U et l'application

$$\begin{aligned} \mathrm{d}f : U &\longrightarrow \mathscr{L}(E,F) \\ \vec{a} &\longmapsto \mathrm{d}f(\vec{a}) \end{aligned}$$

est appelée la *différentielle* de f sur U. Si chacune des n fonctions f_i est de classe $\mathscr{C}^1$ sur U, alors on dit que f est de classe $\mathscr{C}^1$ sur U.

Proposition : 1.

f est de classe $\mathscr{C}^1$ sur U ⇒ f est différentiable sur U ⇏ .

2. La fonction f est $\mathscr{C}^1$ sur U si, et seulement si f est différentiable sur U et sa différentielle $\mathrm{d}f$ est continue sur U.

Exercice (Une fonction différentiable mais pas $\mathscr{C}^1$) :
Montrer que la fonction f *définie à l'exercice 5 est différentiable sur* $\mathbb{R}^2$ *mais*

n'est pas $\mathscr{C}^1$ sur $\mathbb{R}^2$.

On a déjà montré que f n'est pas $\mathscr{C}^1$, *i.e.* $\partial_1 f$ ou $\partial_2 f$ n'est pas continue (*c.f.* exercice 5). Mais f est différentiable. En effet, montrons qu'il existe α et β deux réels tels que pour tout vecteur $\vec{h} = (h,k) \in \mathbb{R}^2$, $f(a+h,b+k) = f(a,b) + \alpha h + \beta k + \mathscr{o}(\vec{h})$.

— si $a \neq 0$, alors f est $\mathscr{C}^1$ et, d'après la formule de Taylor-Young, f est différentiable.

— si $a = 0$, alors $f(0+h,b+k) = h \times h \sin\left(\frac{b+k}{h}\right) = h \times \mathscr{o}(h)$ car $\sin\left(\frac{b+k}{h}\right)$ est bornée. Ainsi, $f(h,b+k) = f(0,b) + 0h + 0k + \mathscr{o}(h)$.

La fonction f est donc différentiable sur $\mathbb{R}^2$.

Exemple : 1. La norme « deux » définie sur $\mathbb{R}^p$ par $N(\vec{x}) = \sqrt{{x_1}^2 + \cdots + {x_p}^2}$ est de classe $\mathscr{C}^1$ sur $\mathbb{R}^p \setminus \{\vec{0}\}$ et

$$\forall \vec{a} \in \mathbb{R}^p \setminus \{\vec{0}\},\ \forall \vec{h} \in \mathbb{R}^p, \qquad \mathrm{d}N(\vec{a}) \cdot \vec{h} = \frac{\langle\, \vec{a} \mid \vec{h} \,\rangle}{N(\vec{a})},$$

où $\langle\, \vec{a} \mid \vec{h} \,\rangle = \sum_{i=1}^p a_i h_i$ est le produit scalaire des vecteurs $\vec{a}$ et $\vec{b}$.

2. La fonction $\det : \mathscr{M}_n(\mathbb{R}) \to \mathbb{R}$ est de classe $\mathscr{C}^1$ et

$$\forall A \in \mathscr{M}_n(\mathbb{R}),\ \forall H \in \mathscr{M}_n(\mathbb{R}), \qquad \det(A+H) = \det A + \mathrm{tr}(B^\top \cdot H) + \mathscr{o}(H),$$

où $B = \mathrm{com}\, A$ est la comatrice de A.

On a déjà montré le résultat pour $A \in \mathrm{GL}_n(\mathbb{R})$ (exercice 12). En effet, $B^\top = \det(A) A^{-1}$, et on conclut par linéarité de tr.

Montrons maintenant le résultat pour A quelconque. On sait déjà que det est de classe $\mathscr{C}^\infty$ car $\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$ (par les « théorèmes généraux »). En développant selon la colonne j, pour la ligne i, on trouve que le terme devant $a_{i,j}$ est $(-1)^{i+j}\Delta_{i,j}$. En effet, aucun terme ne contient $a_{i,j}$ car on supprime la j-ième colonne. Ainsi,

$$\frac{\partial \det}{\partial a_{i,j}} = (-1)^{i+j}\Delta_{i,j},$$

qui est une fonction continue. Ainsi, det est de classe $\mathscr{C}^1$, et, d'après le formule de Taylor-Young,

$$\begin{aligned}
\det(A+H) &= \det A + \sum_{i=1}^n \sum_{j=1}^n h_{i,j} \overbrace{(-1)^{i+j}\Delta_{i,j}}^{[\mathrm{com}\, A]_{i,j}} + \mathscr{o}(H) \\
&= \det A + \sum_{(i,j) \in [\![1,n]\!]^2} h_{i,j} b_{i,j} + \mathscr{o}(H) \\
&= \det A + \mathrm{tr}(B^\top \cdot H) + \mathscr{o}(H)
\end{aligned}$$

car on reconnaît la formule du produit scalaire sur $\mathscr{M}_n(\mathbb{R})$.

Remarque :
De ce dernier exemple, il en résulte que la fonction det : $\mathscr{M}_n(\mathbb{R}) \to \mathbb{R}$ est continue (car $\mathscr{C}^1 \implies$ différentiable $\implies \mathscr{C}^0$). D'où, $\mathrm{GL}_n(\mathbb{R}) = \det^{-1}(\mathbb{R}^\star)$ est l'image réciproque, par la fonction continue det, de l'ouvert $\mathbb{R}^\star$. Ainsi, $\mathrm{GL}_n(\mathbb{R})$ est un ouvert de $\mathscr{M}_n(\mathbb{R})$. On avait aussi montré que $\mathrm{GL}_n(\mathbb{R})$ est dense dans $\mathscr{M}_n(\mathbb{R})$ (exercice 26 du chapitre 13).

VII.4 Le gradient

L'espace vectoriel E était, jusqu'ici, normé et de dimension finie. On le munit désormais d'un produit scalaire ; E est donc un espace euclidien.

Proposition–Définition : Si $f : E \to \mathbb{R}$ est différentiable en $\vec{a} \in E$, alors il existe un unique vecteur de E, appelé le *gradient* de f en $\vec{a}$, et noté $\nabla f(\vec{a})$ ou $\mathrm{grad}\, f(\vec{a})$, tel que

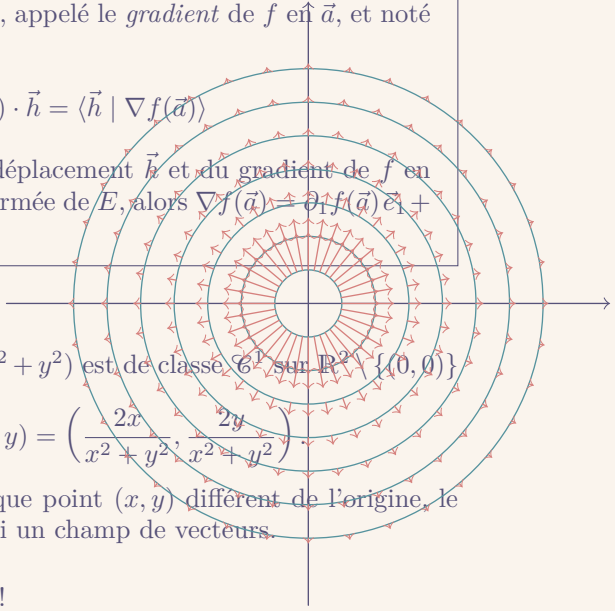
$$\forall \vec{h} \in E, \qquad \mathrm{d}f(\vec{a}) \cdot \vec{h} = \langle \vec{h} \mid \nabla f(\vec{a}) \rangle$$

est le le produit scalaire du vecteur déplacement $\vec{h}$ et du gradient de f en $\vec{a}$. Si $(\vec{e}_1, \dots, \vec{e}_p)$ est une base orthonormée de E, alors $\nabla f(\vec{a}) = \partial_1 f(\vec{a})\, \vec{e}_1 + \cdots + \partial_p f(\vec{a})\, \vec{e}_p$.

Exemple :
La fonction f définie par $f(x,y) = \ln(x^2+y^2)$ est de classe $\mathscr{C}^1$ sur $\mathbb{R}^2 \setminus \{(0,0)\}$ et

$$\forall (x,y) \neq (0,0), \qquad \nabla f(x,y) = \left(\frac{2x}{x^2+y^2}, \frac{2y}{x^2+y^2} \right).$$

La figure ci-dessous représente, en chaque point (x,y) différent de l'origine, le gradient de f en (x,y). On obtient ainsi un champ de vecteurs.



!

Figure 15.6 – Le champ des gradients de $(x,y) \mapsto \ln(x^2+y^2)$

On se déplace dans un espace euclidien E, le long d'une courbe paramétrée par $M : t \mapsto M(t)$, et on évalue, à chaque instant t, la valeur de $f\big(M(t)\big)$ prise par une fonction scalaire f en un point $M(t)$.

Lemme (Règle de la chaîne) **:** Soit $f : U \to \mathbb{R}$ définie sur un ouvert U de l'espace euclidien E. (Dans ce lemme, on se place en dimension 2, mais ce résultat est vrai dans un espace E de dimension p.) Soit $M : I \to E$ définie sur un intervalle I de $\mathbb{R}$. Si $M(I) \subset U$ et les fonctions f et M sont différentiables, alors $f \circ M : t \mapsto f\big(M(t)\big)$ est différentiable et, pout tout

$t \in I$,

$$\begin{aligned}(f\circ M)'(t) &= \frac{\mathrm{d}}{\mathrm{d}t} f\big(M(t)\big)\\ &= x'(t)\cdot \frac{\partial f}{\partial x}\big(M(t)\big) + y'(t)\frac{\partial f}{\partial y}\big(M(t)\big)\\ &= \langle\, M'(t) \mid \nabla f(M(t))\,\rangle\\ &= \mathrm{d}f\big(M(t)\big)\cdot M'(t)\end{aligned}$$

est le produit scalaire du vecteur vitesse $M'(t)$ et du gradient de f en M. De plus, si f et M sont de classe $\mathscr{C}^1$, alors $f\circ M$ l'est aussi.

Preuve :
On pose, pour tout réel t, $M(t) = \big(x(t), y(t)\big)$. On suppose f différentiable, et M dérivable (par rapport à t). Montrons que $f\circ M$ est dérivable, et calculer $(f\circ M)'(t)$. On calcule $f\circ M(t+u) - f\circ M(t) = f\big(x(t+u), y(t+u)\big) - f\big(x(t), y(t)\big)$. Or, comme x est dérivable, et $x(t+u) = x(t) + u\,x'(t) + u\varepsilon_1(u)$. En effet, cette expression est équivalente à $\big(x(t+u) - x(t)\big)/u = x'(t) + \varepsilon_1(u)$, qui tend vers $x'(t)$ quand $u \to 0$. De même, $y(t+u) = y(t) + u\,y'(t) + u\varepsilon_2(u)$. D'où,

$$f\big(x(t+u), y(t+u)\big) = f\big(x(t) + \underbrace{u\,x'(t) + u\,\varepsilon_1(u)}_{h}, y(t) + \underbrace{u\,y'(t) + u\,\varepsilon_2(u)}_{k}\big).$$

Or, par hypothèse, f est différentiable, d'où $\delta = f(x(t), y(t)) + \mathrm{d}f(x(t), (y))\cdot \vec{h} + \|\vec{h}\|\,\varepsilon(\vec{h})$, en posant $\vec{h} = (h, k)$. Ainsi,

$$\begin{aligned}f\circ M(t+u) - f\circ M(t) &= \mathrm{d}f\big(x(t), y(t)\big)\cdot \vec{h} + \|\vec{h}\|\cdot\varepsilon(\vec{h})\\ &= \big\langle \nabla f(M(t)) \,\big|\, (u\,x'(t) + u\,\varepsilon_1(u), u\,y'(t) + u\,\varepsilon_2(u))\big\rangle\\ &+ \|(u\,x'(t) + u\,\varepsilon_1(u), u\,y'(t) + u\,\varepsilon_2(u))\| + \varepsilon\big((u\,x'(t) + u\,\varepsilon_1(u), u\,y'(t) + u\,\varepsilon_2\\ &= u\Big(\big\langle \nabla f(M(t)) \,\big|\, (x'(t) + \varepsilon_1(u), y'(t) + \varepsilon_2(u))\big\rangle\\ &+ \|(x'(t) + \varepsilon_1(u), y'(t) + \varepsilon_2(u))\| + \varepsilon\big((x'(t) + \varepsilon_1(u), y'(t) + \varepsilon_2(u))\big)\Big)\end{aligned}$$

D'où,

$$\frac{f\circ M(t+u) - f\circ M(t)}{u} \xrightarrow[u\to 0]{} \big\langle \nabla f\big(M(t)\big) \,\big|\, M'(t)\big\rangle.$$

□

Dans le lemme précédent, les fonctions f et M ont la représentation suivante.

$$t \overset{M}{\longmapsto} M(t) \overset{f}{\longmapsto} f\big(M(t)\big)$$

$$I \longrightarrow U \longrightarrow \mathbb{R}$$

$$t \overset{f\circ M}{\longmapsto} f \circ M(t)$$

On en déduit que $(f \circ M)'(t) = 0$ si, et seulement si, le vecteur vitesse $M'(t)$ est orthogonal au gradient de f en $M(t)$, à un instant t. En particulier, si la fonction f est constante le long de la trajectoire, *i.e.* si la trajectoire $M(I)$ est incluse dans la courbe de niveau de f, alors le gradient de f est orthogonal au vecteur vitesse en chaque point de la trajectoire.

Définition : On dit qu'un vecteur $\vec{v} \in E$ est *tangent* à une partie $C \subset E$ en un point $\vec{a} \in C$ s'il existe un application dérivable $M : I \to E$ telle que $M(I) \subset C$, et s'il existe $t_0 \in I$ tel que $M(t_0) = \vec{a}$ et $M'(t_0) = \vec{v}$. On note $\mathrm{T}_{\vec{a}}C$ l'ensemble des vecteurs tangents à C en $\vec{a}$, il est nommé *l'espace tangent*.

On dit alors qu'un vecteur est *orthogonal* à la partie C s'il est orthogonal à $\mathrm{T}_{\vec{a}}C$.

« Un vecteur est tangent s'il est un vecteur vitesse. »

Théorème (admis) **:** Soient $f : E \to \mathbb{R}$ une fonction de classe $\mathscr{C}^1$, et une partie $C \subset E$, telle que f est constante sur C. Soit $\vec{a} \in C$. Si $\nabla f(\vec{a}) \neq \vec{0}$, alors un vecteur $\vec{v} \in E$ est tangent à C si, et seulement si $\vec{v}$ est orthogonal à $\nabla f(\vec{a})$.

Autrement dit : $\mathrm{T}_{\vec{a}}C$ est l'hyperplan $\big[\mathrm{Vect}\big(\nabla f(\vec{a})\big)\big]^{\perp} = \mathrm{Ker}\,\mathrm{d}f(\vec{a})$.

Le gradient de f en $\vec{a}$ est donc orthogonal à C : $\nabla f(\vec{a}) \perp \mathrm{T}_{\vec{a}}C$. Ainsi, le champ électrostatique est orthogonal aux équipotentielles, la ligne de plus petite pente est orthogonal aux lignes de niveau, *etc.*

Exercice :
Déterminer une équation de la droite tangente à l'hyperbole d'équation $x^2 - y^2 = 1$ *au point* $(\sqrt{2}, 1)$.

On nomme $\mathscr{H}$ l'hyperbole donnée dans l'énoncé. On a bien $A = (\sqrt{2}, 1) \in \mathscr{H}$ car $\sqrt{2}^2 - 1^2 = 1$. On cherche une équation de $\mathrm{T}_A\mathscr{H}$.

— **Avec le théorème 25.** Soit la fonction f définie comme

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto x^2 - y^2. \end{aligned}$$

Cette fonction f est de classe $\mathscr{C}^1$ et est constante sur $\mathscr{H}$. On calcule le gradient de f en A : $\nabla f(A) = (\partial f(\sqrt{2},1)/\partial x, \partial f(\sqrt{2},1)/\partial y) = 2(\sqrt{2},-1)$.

$$\begin{aligned} N = (x,y) \in \mathrm{T}_A\mathscr{H} &\iff \overrightarrow{AN} \perp \nabla f(A) \\ &\iff (x-\sqrt{2}, y-1) \perp (\sqrt{2},-1) \\ &\iff \sqrt{2}(x-\sqrt{2}) - 1(y-1) = 0 \\ &\iff \sqrt{2}x - y = 1 \\ &\iff y = \sqrt{2}x - 1 \end{aligned}$$

— **Avec la définition 24.** On rappelle que

$$(x,y) \in \mathscr{H}_+ \iff (x>0 \text{ et } x^2-y^2=1) \iff \exists t \in \mathbb{R}, (x = \operatorname{ch} t \text{ et } y = \operatorname{sh} t).$$

Soit $M : t \mapsto \big(x(t), y(t)\big) = (\operatorname{ch} t, \operatorname{sh} t)$ un point de $\mathscr{H}_+$. Il existe un instant $t_0 \in \mathbb{R}$ tel que $M(t_0) = (\sqrt{2}, 1)$. La fonction M est dérivable et $M'(t) = (\operatorname{sh} t, \operatorname{ch} t) = (1, \sqrt{2})$ est tangent à $\mathscr{H}$.

$$N = (x,y) \in \mathrm{T}_A\mathscr{H} \iff \overrightarrow{AN} \,/\!/\, M'(t_0) \iff \begin{vmatrix} x-\sqrt{2} & 1 \\ y-1 & \sqrt{2} \end{vmatrix} = 0 \iff y = \sqrt{2}x - 1.$$

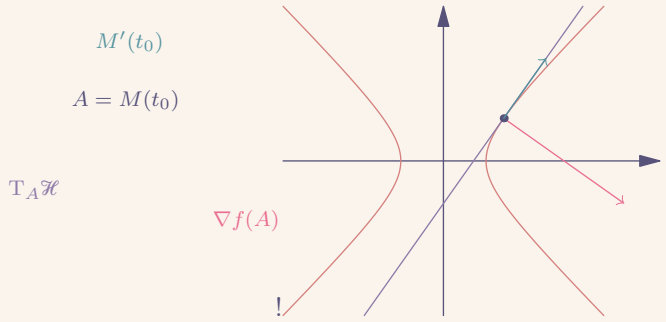


FIGURE 15.7 – Hyperbole $\mathscr{H}$, gradient en A et tangente en A.

EXEMPLE :
La sphère $S \subset \mathbb{R}^3$ de rayon 1 et de centre $\vec{0} = (0,0,0)$ est la surface paramétrée par

$$\forall (\varphi,\theta) \in \mathbb{R}^2, \qquad \begin{cases} x(\varphi,\theta) = \cos\theta\cos\varphi \\ y(\varphi,\theta) = \cos\theta\sin\varphi \\ z(\varphi,\theta) = \sin\theta. \end{cases}$$

Les vecteurs $\partial M(\varphi,\theta)/\partial\varphi = (-\cos\theta\sin\varphi, \cos\theta\cos\varphi, 0)$ et $\partial M(\varphi,\theta)/\partial\theta = (-\sin\theta\cos\varphi, -\sin\theta\sin\varphi, \cos\theta)$ sont tangents à la sphère en le point $M(\varphi,\theta)$. Le plan tangent à la sphère au point (a,b,c) est orthogonal au vecteur

$$\frac{\partial M}{\partial\varphi}(\varphi,\theta) \wedge \frac{\partial M}{\partial\theta}(\varphi,\theta) = (\cos^2\theta\cos\varphi, \cos^{\theta}\sin\varphi, \cos\theta\sin\varphi) = \cos\theta\,(a,b,c),$$

qui est non nul si $\cos\theta \neq 0$ (*i.e.* si le point $M(\varphi,\theta) = (a,b,c)$ n'est, si au pôle Sud, ni au pôle Nord).

En effet, on cherche une équation du plan P tangent.

$$\begin{aligned} N(x,y,z) \in P &\iff \det(\overrightarrow{MN}, \partial M/\partial\varphi, \partial M/\partial\theta) = 0 \\ &\iff \begin{vmatrix} x-a & ? & ? \\ y-b & ? & ? \\ z-c & ? & ? \end{vmatrix} = 0 \\ &\iff ?\cdot(x-a) + ?\cdot(y-b) + ?\cdot(z-c) = 0 \end{aligned}$$

Autre méthode : $N(x,y,z) \in P \iff \overrightarrow{MN} \perp \left(\dfrac{\partial M}{\partial\varphi} \wedge \dfrac{\partial M}{\partial\theta}\right) \iff \left\langle \vec{MN} \,\middle|\, \dfrac{\partial M}{\partial\varphi} \wedge \dfrac{\partial M}{\partial\theta} \right\rangle = 0.$

Autre autre méthode : la même sphère S est la surface de niveau 1 de la fonction $f : \mathbb{R}^3 \to \mathbb{R},\ (x,y,z) \mapsto x^2+y^2+z^2$. En chaque point (a,b,c) de la sphère le plan tangent a pour équation $ax+by+cz=0$. On calcule le gradient de f au point (a,b,c) :

$$\nabla f(a,b,c) = \big(\partial_1 f(a,b,c), \partial_2 f(a,b,c), \partial_3 f(a,b,c)\big) = (2a,2b,2c) = 2(a,b,c).$$

Ainsi,

$$\begin{aligned} N(x,y,z) \in P \iff \overrightarrow{MN} \perp \nabla f(M) &\iff \left\langle \begin{pmatrix} x-a \\ y-b \\ z-c \end{pmatrix} \middle| \begin{pmatrix} a \\ b \\ c \end{pmatrix} \right\rangle = 0 \\ &\iff a(x-a)+b(y-b)+c(z-c) = 0 \\ &\iff ax+by+cz = a^2+b^2+c^2 = 1 \end{aligned}$$

Définition : 1. On dit d'une partie D d'un espace vectoriel qu'elle est *convexe* si, pour tous vecteurs $\vec{a}$ et $\vec{b}$ de D, pour tout $t \in [0,1]$, alors $\vec{a}+t(\vec{b}-\vec{a}) = (1-t)\vec{a}-t\vec{b}$.

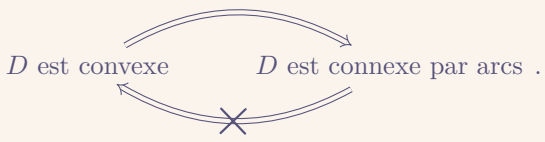
« D est convexe si tout segment $[\vec{a},\vec{b}]$ est inclus dans D. »

2. On dit d'une partie D d'un espace vectoriel normé quelle est *connexe par arcs* si, pour tous vecteurs $\vec{a}$ et $\vec{b}$ de D, il existe une application continue $M : [0,1] \to E$ telle que $M(0)=a$, $M(1)=b$ et $\forall t \in [0,1]$, $M(t) \in D$.

« D est connexe par arcs s'il existe un chemin de $\vec{a}$ vers $\vec{b}$ pour tous vecteurs $\vec{a}$ et $\vec{b}$. »

Remarque : 1. Le segment $[\vec{a},\vec{b}]$ est l'ensemble des vecteurs $M(t) = \vec{a}+t(\vec{b}-\vec{a}) = (1-t)\vec{a}+t\vec{b}$, où $t \in [0,1]$.

2.



Mais, **dans** $\mathbb{R}$, on a bien D connexe $\iff$ D connexe par arcs $\iff$ D est un intervalle.

3. L'image directe $f(D)$ d'une partie D connexe par arcs de E par une application continue $f : E \to F$ est une partie connexe par arcs de F.

   Preuve :
   En effet, soient $\vec{a}'$ et $\vec{b}'$ deux vecteurs de $f(D)$. Il existe $\vec{a}$ et $\vec{b}$ deux vecteurs de D tels que $f(\vec{a}) = \vec{a}'$ et $f(\vec{b}) = \vec{b}'$. Par hypothèse, il existe une application $M : [0,1] \to E$ continue telle que $M([0,1]) \subset D$, $M(\vec{0}) = \vec{a}$ et $M(1) = \vec{b}$.

   $$t \xmapsto{\quad f \circ M \quad} f \circ M(t)$$

   $$\longrightarrow F \quad .$$

   $$t \xmapsto{M} M(t) \xmapsto{f} f(M(t))$$

   Or, $f \circ M(0) = f(M(0)) = f(\vec{a}) = \vec{a}'$, $f \circ M(1) = f(M(1)) = f(\vec{b}) = \vec{b}'$. De plus $f \circ M$ est continue car c'est la composée de deux fonctions continues f et M (par hypothèse). Ainsi, $f \circ M([a,b]) \subset f(D)$. On en déduit que $f(D)$ est connexe par arcs. □

4. D'après les deux points précédents, toute fonction continue sur partie connexe par arcs vérifie le théorème des valeurs intermédiaires.

Rappel (Théorème des valeurs intermédiaires) :
Soit $f : \mathbb{R} \supset [a,b] \to \mathbb{R}$ une fonction continue sur $[a,b]$. Pour tout $y \in [f(a), f(b)] \cup [f(b), f(a)]$, il existe $x \in [a,b]$ tel que $y = f(x)$.

Le théorème des valeurs intermédiaires devient donc, si $f : D \to \mathbb{R}$ est continue, où $\vec{a}, \vec{b} \in D$ est une partie connexe par arcs de E, alors, pour tout $y \in [f(\vec{a}), f(\vec{b})] \cup [f(\vec{b}), f(\vec{a})]$, il existe $\vec{c} \in D$ tel que $y = f(\vec{c})$.

Preuve :
De $\vec{a}$ à $\vec{b}$, il existe un chemin : il existe une fonction $M : [0,1] \to D$ continue telle que $M(0) = \vec{a}$, $M(1) = \vec{b}$, et $\forall t \in [0,1]$, $M(t) \in D$. La fonction $f \circ M : t \mapsto f(M(t))$ est continue par composition. On conclut par le théorème des valeurs intermédiaires appliqué à $f \circ M$. □

Exercice : *1. Montrer que toute boule de tout espace vectoriel normé est convexe.*

2. *Montrer que l'hyperbole $\mathscr{H}$ d'équation $y^2 - x^2 = 1$ n'est pas connexe par arcs.*
3. *Montrer que le produit cartésien $D_1 \times D_2$ de deux parties connexes par arcs $D_1 \subset E_1$ et $D_2 \subset E_2$ est une partie connexe par arcs de $E_1 \times E_2$. En déduire que la sphère $\{\vec{x} \in \mathbb{R}^3 \mid \|\vec{x}\|_2 = 1\}$ est une partie connexe par arcs*

de $\mathbb{R}^3$, et que, pour aller d'un pôle à l'autre, il faut traverser l'équateur.

1. On considère la boule $B(\vec{\Omega}, R)$, où $\vec{\Omega}$ est un vecteur d'un espace vectoriel normé $(E, \|\cdot\|)$, et $R > 0$. Soient $\vec{a}, \vec{b} \in B(\vec{\Omega}, R)$; ainsi, $\|\vec{a} - \vec{\Omega}\| < R$ et $\|\vec{a} - \vec{\Omega}\| < R$. Montrons que, pour tout $t \in [0,1]$, $(1-t)\vec{a} + t\vec{b} \in B(\vec{\Omega}, R)$.

$$\begin{aligned}\|(1-t)\vec{a} + t\vec{b} - \vec{\Omega}\| &= \|(1-t)\vec{a} + t\vec{b} - \vec{\Omega}(1-t) - t\vec{\Omega}\| \\ &= \|(1-t)(\vec{a} - \vec{\Omega}) + t(\vec{b} - \vec{\Omega})\| \\ &\leqslant (1-t)\|\vec{a} - \vec{\Omega}\| + t\|\vec{b} - \vec{\Omega}\| \\ &\leqslant (1-t)\cdot R + t \cdot R \\ &= R\end{aligned}$$

   D'où, $\big((1-t)\vec{a} + t\vec{b}\big) \in B(\vec{\Omega}, R)$.
2. Par l'absurde, on suppose $\mathscr{H}$ connexe. Soit la fonction $f : (x, y) \mapsto y$ continue. L'image d'un connexe par une fonction continue est connexe, d'où $f(\mathscr{H})$ est connexe. Or, $f(\mathscr{H}) = \mathbb{R} \setminus]-1, 1[=]-\infty, -1[\cup]-1, \infty[$, qui n'est pas connexe.

Proposition : Soit f une fonction de classe $\mathscr{C}^1$ sur un **convexe** D. La fonction f est constante sur D si, et seulement si, son gradient $\nabla f(\vec{x})$ est nul en tout point $\vec{x} \in D$. De même si D est connexe par arcs.

Preuve :
L'implication est évidente, une fonction constante a un gradient nul. Montrons la réciproque. D'après la règle de la chaîne, pour toute fonction dérivable M, on a $(f \circ M)'(t) = \langle \nabla f(M(t)) \mid M'(t) \rangle = 0$ car $\nabla f(M(t))$ est nul par hypothèse. Montrons que, pour tout vecteurs $\vec{a}$ et $\vec{b}$ de D, $f(\vec{a}) = f(\vec{b})$. On suppose f de classe $\mathscr{C}^1$. On pose M un chemin de $\vec{a}$ vers $\vec{b}$, on admet que M est de classe $\mathscr{C}^1$, et on a

$$f(\vec{b}) - f(\vec{a}) = f \circ M(1) - f \circ M(0) = \int_0^1 (f \circ M)'(t)\, \mathrm{d}t = \int_0^1 0\, \mathrm{d}t = 0.$$

□

VII.5 La différentielle d'une composée

Proposition : Soient E, F et G trois espaces vectoriels normés, et soient $U \subset E$ et $V \subset F$ des ouverts. Soit $f : U \to F$ et $g : V \to G$ deux fonctions

telles que $f(U \subset V)$. Ainsi,

$$E \supset U \longrightarrow F \supset V \longrightarrow\!\!\!\!\!\!\longrightarrow G$$

.

$$\vec{x} \overset{f}{\longmapsto} \vec{y} = f(\vec{x}) \overset{g}{\longmapsto} g(\vec{y}) = (g \circ f)(\vec{x})$$

Si f est différentiable en $\vec{a} \in U$, et g est différentiable en $\vec{b} = f(\vec{a})$, alors $g \circ f$ est différentiable en $\vec{a}$, et

$$\boxed{\mathrm{d}(g \circ f)(\vec{a}) = \mathrm{d}g(\vec{b}) \circ \mathrm{d}f(\vec{a}).}$$

Preuve :
On suppose f et g différentiable. Montrons que $g \circ f$ est différentiable. La fonction f est différentiable, on calcule donc $f(\vec{a}+\vec{h}) = f(\vec{a}) + \mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h}) = \vec{b} + \vec{k}$, en posant $\vec{b} = f(\vec{a})$. Et,

$$\begin{aligned} g(\vec{b}+\vec{k}) &= g(\vec{b}) + \mathrm{d}g(\vec{b}) \cdot \vec{k} + \|\vec{k}\| \, \varepsilon_2(\vec{k}) \\ &= g \circ f(\vec{a}) + \mathrm{d}g(\vec{b}) \cdot \big[\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h})\big] + \|\mathrm{d}f(\vec{a}) \cdot \vec{h} + \vec{h} \, \varepsilon_1(\vec{h})\| \, \varepsilon_2(\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h})) \\ &= g \circ f(\vec{a}) + \big[\mathrm{d}g(\vec{b}) \circ \mathrm{d}f(\vec{a})\big] \cdot \vec{h} + \text{ɷ}(\vec{h}) \end{aligned}$$

En effet, en nommant $\vec{R}$ le (futur) reste de $g(\vec{b}+\vec{k})$, on a $\vec{R} = \mathrm{d}f(\vec{b}) \cdot [\|\vec{h}\| \, \varepsilon_1(\vec{h})] + \|\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h})\| \, \varepsilon_2\big(\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h})\big)$. D'où,

$$\begin{aligned} 0 &\leqslant \left\| \frac{\mathrm{d}g(\vec{b}) \cdot \big[\|\vec{h}\| \, \varepsilon_1(\vec{h})\big] + \big\|\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h})\big\| \, \varepsilon_2(\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h}))}{\|\vec{h}\|} \right\| \\ &\leqslant \frac{\big\|\mathrm{d}g(\vec{b}) \cdot \big[\|\vec{h}\| \, \varepsilon_1(\vec{h})\big]\big\| + \big\|\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h})\big\| \, \big\|\varepsilon_2(\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h}))\big\|}{\|\vec{h}\|} \quad \text{par inégalité tria} \\ &\leqslant \frac{\|\vec{h}\| \cdot \big\|\mathrm{d}g(\vec{b}) \cdot \big[\, \varepsilon_1(\vec{h})\big]\big\| + \big(\big\|\mathrm{d}f(\vec{a}) \cdot \vec{h}\big\| + \big\|\|\vec{h}\| \, \varepsilon_1(\vec{h})\big\|\big) \, \big\|\varepsilon_2(\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h}))\big\|}{\|\vec{h}\|} \\ &\leqslant \frac{\|\vec{h}\| \cdot \big\|\mathrm{d}g(\vec{b}) \cdot \big[\, \varepsilon_1(\vec{h})\big]\big\| + \big(\|\|\mathrm{d}f(\vec{a})\|\| \cdot \|\vec{h}\| + \|\varepsilon_1(\vec{h})\| \cdot \|\vec{h}\|\big) \, \big\|\varepsilon_2(\mathrm{d}f(\vec{a}) \cdot \vec{h} + \|\vec{h}\| \, \varepsilon_1(\vec{h}))\big\|}{\|\vec{h}\|} \\ &\leqslant \|\mathrm{d}g(\vec{b}) \cdot \varepsilon_1(\vec{h})\| + \|(\|\|\mathrm{d}f(\vec{a})\|\| + \|\varepsilon_1(\vec{h})\|) \cdot \varepsilon_2(\ldots)\| \\ &\leqslant \|\|\mathrm{d}f(\vec{b})\|\| \cdot \|\varepsilon_1(\vec{h})\| + (\|\|\mathrm{d}f(\vec{a})\|\| + \|\varepsilon_1(\vec{h})\|) \cdot \|\varepsilon_2(\ldots)\| \xrightarrow[\vec{h} \to \vec{0}]{} 0 \end{aligned}$$

□

En généralisant la règle de la chaîne

$$\frac{\mathrm{d}}{\mathrm{d}t} f \circ M(t) = \frac{\partial f}{\partial x} \cdot \frac{\mathrm{d}x}{\mathrm{d}t} + \frac{\partial f}{\partial y} \cdot \frac{\mathrm{d}y}{\mathrm{d}t},$$

on obtient le corolaire suivant.

Corollaire : Avec les hypothèses précédentes, en notant $p = \dim E$, $q = \dim F$, $n = \dim G$, et $(y_1, \dots, y_k) = \vec{y} = f(\vec{x})$, on a

$$\forall j \in [\![1, p]\!], \qquad \frac{\partial}{\partial x_j} g \circ f(\vec{a}) = \sum_{k=0}^{q} \underbrace{\frac{\partial g}{\partial y_k}}_{\partial_k g} \cdot \frac{\partial f_k}{\partial x_k}.$$

On peut exprimer le même résultat avec la jacobienne :

$$\boxed{\mathrm{J}_{g \circ f}(\vec{a}) = \mathrm{J}_g(\vec{b}) \cdot \mathrm{J}_f(\vec{a}),}$$

qui représente matriciellement l'égalité $\mathrm{d}(g \circ f)(\vec{a}) = \mathrm{d}g(\vec{b}) \circ \mathrm{d}f(\vec{a})$.

Preuve :
On a

$$\underbrace{\begin{pmatrix} \partial_1(g \circ f)_1 & \partial_2(g \circ f)_1 & \dots & \partial_p(g \circ f)_1 \\ \partial_1(g \circ f)_2 & \partial_2(g \circ f)_2 & \dots & \partial_p(g \circ f)_2 \\ \vdots & \vdots & \ddots & \vdots \\ \partial_1(g \circ f)_p & \partial_2(g \circ f)_p & \dots & \partial_p(g \circ f)_p \end{pmatrix}}_{\mathrm{J}_{g \circ f}} = \underbrace{\begin{pmatrix} \partial_1 g_1 & \partial_2 g_2 & \dots & \partial_q g_1 \\ \partial_1 g_2 & \partial_2 g_2 & \dots & \partial_q g_2 \\ \vdots & \vdots & \ddots & \vdots \\ \partial_1 g_n & \partial_2 g_n & \dots & \partial_q g_n \end{pmatrix}}_{\mathrm{J}_g} \cdot \underbrace{\begin{pmatrix} \partial_1 f_1 & \partial_2 f_1 & \dots & \partial_p f_1 \\ \partial_1 f_2 & \partial_2 f_2 & \dots & \partial_p f_2 \\ \vdots & \vdots & \ddots & \vdots \\ \partial_1 f_q & \partial_2 f_q & \dots & \partial_p f_q \end{pmatrix}}_{\mathrm{J}_f},$$

ce qui donne l'autre expression en « regardant coordonnées par coordonnées. » □

Exemple (Le gradient en coordonnées polaires) :
Soit $f : \mathbb{R}^2 \to \mathbb{R}$ une fonction différentiable. La fonction F définie par $F(r, \varphi) = f(r \cos \varphi, r \sin \varphi)$ pour $r > 0$ et $\varphi \in \mathbb{R}$. Cette fonction s'écrit également $f \circ M$, avec la fonction M définie à l'exercice 9.

$$(r, \varphi) \xmapsto{M} M(r, \varphi) = (x, y) \xmapsto{f} f(x, y)(r, \varphi)\text{ă} \xmapsto{F = f \circ M} F(r, \varphi) \ .$$

La fonction F est différentiable car f et M le sont[2]. Ainsi,

$$\left.\begin{aligned} \frac{\partial F}{\partial r} &= \frac{\partial x}{\partial r} \cdot \frac{\partial f}{\partial x} + \frac{\partial y}{\partial r} \cdot \frac{\partial f}{\partial y} &&= \cos \varphi \cdot \frac{\partial f}{\partial x} + \sin \varphi \cdot \frac{\partial f}{\partial y} \\ \frac{\partial F}{\partial \varphi} &= \frac{\partial x}{\partial \varphi} \cdot \frac{\partial f}{\partial x} + \frac{\partial y}{\partial \varphi} \cdot \frac{\partial f}{\partial y} &&= -r \sin \varphi \cdot \frac{\partial f}{\partial x} + r \cos \varphi \cdot \frac{\partial f}{\partial y} \end{aligned}\right\} \underset{\substack{L_1 \leftarrow \cos \varphi L_1 - \\ \sin \varphi L_1 + \mathrm{co}}}{\Longleftrightarrow}$$

On retrouve donc

$$\nabla f(x, y) = \frac{\partial F}{\partial r} \cdot \vec{u}_r + \frac{1}{r} \cdot \frac{\partial F}{\partial \varphi} \cdot \vec{u}_\varphi,$$

en posant $\vec{u}_r = (\cos \varphi, \sin \varphi)$ et $\vec{u}_\theta = (-\sin \varphi, \cos \varphi)$.

2. f différentiable par hypothèse, et M est de classe $\mathscr{C}^1$, donc différentiable.

VII.6 Dérivées secondes

Définition : Soit $p \in \mathbb{N}^\star$, un ouvert $D \subset \mathbb{R}^p$ et une fonction $f : D \to \mathbb{R}, (x_1, \dots, x_p) \mapsto f(x_1, \dots, x_p)$.

1. Soit un point $\vec{a} = (a_1, \dots, a_p) \in D$. Si la i-ème dérivée partielle $\partial_i f$ existe sur D et possède une j-ième dérivée partielle en $\vec{a}$, alors le nombre réel $\partial_j(\partial_i f)(\vec{a})$ est une *dérivée partielle* en $\vec{a}$, et est noté $\partial_j\partial_i f(\vec{a})$ ou $\partial^2 f(\vec{a})/\partial x_j \partial x_i$.[3] Cette dérivée seconde s'écrit aussi parfois $\partial_{1,2} f$.
2. On dit que f est de classe $\mathscr{C}^2$ sur D si les p^2 fonctions $\partial_j\partial_i f$ sont continues sur D.

A priori, $\partial_1\partial_2 f$ est différent de $\partial_2\partial_1 f$.

Exercice :
Soit la fonction $f : \mathbb{R}^2 \to \mathbb{R}$ définie par

$$f(x,y) = xy \cdot \frac{x^2 - y^2}{x^2 + y^2} \text{ si } (x,y) \neq (0,0) \qquad \text{et} \qquad f(0,0) = 0.$$

Montrer que $\dfrac{\partial^2 f}{\partial x\, \partial y}(0,0) = +1$ *et* $\dfrac{\partial^2 f}{\partial y\, \partial x}(0,0) = -1$.

Si $(x,y) \neq (0,0)$, alors

$$\begin{aligned}\partial_1 f(x,y) &= \frac{\dfrac{\partial}{\partial x}\big(xy(x^2-y^2)\big)\cdot(x^2+y^2) - xy(x^2-y^2)\cdot\dfrac{\partial}{\partial x}(x^2-y^2)}{(x^2+y^2)^2} \\ &= \frac{[y(x^2-y^2)+2x^2y](x^2+y^2) - 2x^2y(x^2-y^2)}{(x^2+y^2)^2}\end{aligned}$$

Et, pour $h > 0$, $\big(f(h,0) - f(0,0)\big)/h = 0 \to 0$ quand $h \to 0$, d'où $\partial_1 f(0,0) = 0$. De plus,

$$\frac{\dfrac{\partial}{\partial x} f(0,h) - \dfrac{\partial}{\partial x} f(0,0)}{h} = \frac{-h^5/h^4}{h} = -1 \xrightarrow[h\to 0]{} -1.$$

D'où, $\dfrac{\partial f}{\partial y \partial x}(0,0) = -1$.

On procède de même pour montrer que $\dfrac{\partial f}{\partial x \partial y}(0,0) = 1$ car $f(x,y) = -f(y,x)$.

Proposition (Théorème de Schwarz) **:** Soit D un ouvert de $\mathbb{R}^p$, et f :

3. Cette notation vient de $\frac{\partial}{\partial x_j}\left(\frac{\partial f}{\partial x_i}\right)$.

$D \to \mathbb{R}$ une fonction de classe $\mathscr{C}^2$. Alors,

$$\partial_i \partial_j f = \partial_j \partial_i f, \qquad \text{pour tout } (i,j) \in [\![1,p]\!]^2.$$

Théorème (Formule de Taylor & Young à l'ordre 2, admise) **:** (On se place dans $\mathbb{R}^2$, mais ce résultat s'étend à $\mathbb{R}^p$ de la même manière.) Si $f : D \to \mathbb{R}$ est de classe $\mathscr{C}^2$, alors

$$\begin{aligned} f(a+h,b+k) = {} & f(a,b) && \text{ordre 0}\\ & + h\,\partial_1 f(a,b) + k\,\partial_2 f(a,b) && \text{ordre 1}\\ & + \frac{h^2}{2}\,\partial_1\partial_1 f(a,b) + hk\,\partial_1\partial_2 f(a,b) + \frac{k^2}{2}\,\partial_2\partial_2 f(a,b) && \text{ordre 2}\\ & + \|\vec{h}\|^2\,\varepsilon(\vec{h}) && \text{reste} \end{aligned}$$

où $\vec{h} = (h,k)$, et $\varepsilon(\vec{h}) \to \vec{0}$.

On note le développement à l'ordre 2 comme $\alpha h^2 + 2\beta hk + \gamma k^2$. [4] On note cette application $q_{(a,b)}$. On peut calculer le terme d'ordre 2 par produit matriciel :

$$\underbrace{\begin{pmatrix} h & k \end{pmatrix}}_{\left[\vec{h}\right]^\top} \cdot \underbrace{\begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}}_{\mathrm{H}_f(a,b)} \cdot \underbrace{\begin{pmatrix} h \\ k \end{pmatrix}}_{\left[\vec{h}\right]}.$$

Définition : Soit f une fonction admettant des dérivées partielles secondes en $\vec{a}$. La *hessienne* de f en $\vec{a}$ est la matrice

$$\mathrm{H}_f(\vec{a}) = \left(\partial_i\partial_j f\right)_{i,j} = \begin{pmatrix} \dfrac{\partial^2 f}{\partial {x_1}^2}(\vec{a}) & \dfrac{\partial^2 f}{\partial x_1\,\partial x_2}(\vec{a}) & \cdots & \dfrac{\partial^2 f}{\partial x_1\,\partial x_p}(\vec{a}) \\ \dfrac{\partial^2 f}{\partial x_2 \partial x_1}(\vec{a}) & \dfrac{\partial^2 f}{\partial {x_2}^2}(\vec{a}) & \cdots & \dfrac{\partial^2 f}{\partial x_2\,\partial x_p}(\vec{a}) \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{\partial^2 f}{\partial x_p\,\partial x_1}(\vec{a}) & \dfrac{\partial^2 f}{\partial x_p\,\partial x_2}(\vec{a}) & \cdots & \dfrac{\partial^2 f}{\partial {x_p}^2}(\vec{a}) \end{pmatrix} \in \mathscr{M}_{pp}(\mathbb{R}).$$

Si la fonction f est de classe $\mathscr{C}^2$, alors, par le théorème de Schwarz, la hessienne de f est une matrice symétrique.

VII.7 Optimisation

4. C'est une forme quadratique.

Définition : Soit $\vec{a}$ un vecteur d'une partie $D \subset \mathbb{R}^p$, où $p \in \mathbb{N}^\star$. Soit $f : D \to \mathbb{R}$ une fonction scalaire. On dit que

1. la fonction f possède un *minimum global* sur D en $\vec{a}$ si $\forall \vec{x} \in D, \quad f(\vec{x}) \geqslant f(\vec{a})$,
2. la fonction f possède un *minimum global* en $\vec{a}$ s'il existe $\varepsilon > 0$ tel que pour tout $\vec{x} \in D \cap \bar{B}(\vec{a}, \varepsilon)$, $f(\vec{x}) \geqslant f(\vec{a})$.

On définit de même un *maximum local* en $\vec{a}$ et un *maximum global* sur D en $\vec{a}$. On dit que f possède un *extremum* (*local* en $\vec{a}$, *global* sur D) si f possède un maximum ou un minimum (local en $\vec{a}$, global en D). Un extremum global est *a fortiori* local.

Théorème : Soit $f : E \to \mathbb{R}$. Si D est une partie fermée et bornée de E et si f est une fonction continue sur D, alors f possède un maximum et un minimum globaux. Autrement dit, toute fonction réelle continue sur un fermé borné est bornée et atteint ses bornes.

La preuve sera faite dans l'annexe B.

Proposition–Définition : Soient $D \subset \mathbb{R}^p$ et $\vec{a}$ un point intérieur de D. Soit $f : D \to \mathbb{R}$ une fonction scalaire différentiable en $\vec{a}$.

1. On dit que $\vec{a}$ est un *point critique* de f si $\nabla f(\vec{a}) = \vec{0}$ (*i.e.* si $\mathrm{d}f(\vec{a})$ est l'application nulle).
2.

.

Preuve :
Généralisation d'un théorème vu précédemment, la preuve est dans la section 14.4 du cours de *MP2I*. □

Proposition : Soit $\vec{a} \in D$ un point d'un ouvert de $\mathbb{R}^p$, et soit $f : D \to \mathbb{R}^2$ une fonction scalaire de classe $\mathscr{C}^2$. Soient $(\lambda_1, \ldots, \lambda_p)$ les valeurs propres de la hessienne de f en $\vec{a}$.

1. **Condition nécessaire de minimum local en un point**

intérieur. Si f possède un minimum local en $\vec{a}$, alors

$$\nabla f(\vec{a}) = \vec{0} \quad \text{et} \quad \forall i \in [\![1,p]\!],\ \lambda_i \geqslant 0.$$

Autrement dit, $\nabla f(\vec{a}) = \vec{0}$ et $\mathrm{H}_f(\vec{a}) \in \mathcal{S}_p^+$.

2. **Condition suffisante de minimum local en un point intérieur.** Si $\nabla f(\vec{a}) = \vec{0}$, et $\forall i \in [\![1,p]\!]$, $\lambda_i > 0$, autrement dit si $\nabla f(\vec{a}) = \vec{0}$ et $\mathrm{H}_f(\vec{a}) \in \mathcal{S}_p^{++}$, alors f possède un minimum local en $\vec{a}$.

Preuve : — Si f possède un minimum local, alors $\vec{a}$ est un point critique, donc $\nabla f(\vec{a}) = \vec{0}$. D'où, $f(\vec{a}+\vec{h}) = f(\vec{a}) + \frac{1}{2}q_{\vec{a}}(\vec{h}) + \|h\|^2\,\varepsilon(\vec{h})$. Comme $\vec{a}$ est un minimum local, alors $\frac{1}{2}q_{\vec{a}}(\vec{h}) + \|\vec{h}\|^2\,\varepsilon(\vec{h}) \geqslant 0$, pour tout $\vec{h}$ suffisamment petit (le minimum est local). Or, $\frac{1}{2}q_{\vec{a}}(\vec{h}) + \|\vec{h}\|^2\,\varepsilon(\vec{h}) = \frac{1}{2}\begin{bmatrix}\vec{h}\end{bmatrix}^\top \cdot \mathrm{H}_f(\vec{a}) \cdot \begin{bmatrix}\vec{h}\end{bmatrix} + \|\vec{h}\|^2\,\varepsilon(\vec{h})$. Et, la matrice $\mathrm{H}_f(\vec{a})$ est symétrique et à coefficients réels d'où, d'après le théorème spectral, elle est diagonalisable dans une base $\mathcal{B}$ orthonormée formée de vecteurs propres. D'où, $\frac{1}{2}q_{\vec{a}}(\vec{h}) + \|\vec{h}\|^2\,\varepsilon(\vec{h}) = \frac{1}{2}\begin{bmatrix}\vec{h}\end{bmatrix}_{\mathcal{B}}^\top \cdot \mathrm{diag}(\lambda_1,\dots,\lambda_n) \cdot \begin{bmatrix}\vec{h}\end{bmatrix}_{\mathcal{B}} + \|\vec{h}\|^2\,\varepsilon(\vec{h}) = \frac{1}{2}(\lambda_1 h_1^2 + \cdots + \lambda_p h_p^2) + (h_1^2 + \cdots + h_p^2)\,\varepsilon(\vec{h}) \geqslant 0$, pour tout vecteur $\vec{h}$ suffisamment petit. Montrons que $\forall i$, $\lambda_i \geqslant 0$. Par l'absurde, supposons qu'il existe $i \in [\![1,p]\!]$ tel que $\lambda_i \leqslant 0$. On considère le vecteur $\vec{h} = (0,\dots,0,h,0,\dots,0)$ qui est non nul à la i-ème coordonnée. Alors,

$$\frac{1}{2}\lambda_i\,h^2 + h^2\varepsilon(\vec{h}) = h^2\big(\frac{1}{2}\lambda_i + \varepsilon(\vec{h})\big) \geqslant 0.$$

Or, $\varepsilon(\vec{h}) \to 0$ lorsque $\vec{h} \to 0$. D'où, $\frac{1}{2}\lambda_i + \varepsilon(\vec{h}) < 0$ pour $\vec{h}$ assez petit. Absurde.

□

Ceci reste vrai pour un maximum en replaçant f par $-f$.

Méthode (Démontrer les extrema locaux en dimension 2) :

1. On détermine les points critique de la fonction f.
2. Pour chaque point critique $\vec{a}$, on calcule le déterminant et la trace de la hessienne $\mathrm{H}_f(\vec{a})$.
   (a) Si le déterminant est strictement positif, alors il y a un extremum local en $\vec{a}$:
      — si la trace est strictement positive, alors f admet un minimum local en $\vec{a}$,
      — si la trace est strictement négative, alors f admet un maximum local en $\vec{a}$.
   (b) Si le déterminant est strictement négatif, alors f n'admet pas d'extremum local en $\vec{a}$.

(c) Si le déterminant est nul, alors la proposition ne permet pas de conclure.

EXERCICE :
Étudier les extrema de la fonction

$$\begin{aligned} f : \bar{B}(\vec{0},1) &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto x^2 - y^2 \end{aligned}$$

définie sur la boule $\bar{B}(\vec{0},1) = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 \leqslant 1\}$ *fermée de centre* $\vec{0}$ *et de rayon* 1.

La fonction f est continue sur le fermé borné $\bar{B}(\vec{0},1)$, donc elle possède un maximum et un minimum globaux.

— À l'intérieur de la boule $\bar{B}(\vec{0},1)$, on procède par analyse–synthèse.
  — **Analyse.** S'il existe un extremum en un point $(a,b) \in \mathring{B}(\vec{0},1)$, alors $\nabla f(a,b) = (2a,-2b) = (0,0)$ d'où $(a,b) = \vec{0}$.
  — **Synthèse.** En $(a,b) = \vec{0}$, alors $f(a,b) = f(0,0) = 0$. Or, $f(0,k) = -k^2 < 0$, pour tout $k > 0$. Et, $f(h,0) = h^2 > 0$, pour tout $h > 0$. Le point $\vec{0}$ n'est, ni un minimum local, ni un maximum local,pour la fonction f.
  — **Suite de l'analyse.** (deuxième méthode) On calcule la hessienne de f en $\vec{0}$. On trouve
  $$\mathrm{H}_f(\vec{0}) = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}.$$
  Les deux valeurs propres ont des signes différents, il n'y a donc ni maximum, ni minium en $\vec{0}$.
— Et au bord, il y a un minimum global et un maximum global par continuité de f. Sur le bord, $x^2+y^2 = 1$, donc $f(x,y) = x^2 - y^2 = x^2 - (1-y^2) = 2x^2 - 1$, pour tout $x \in [-1,1]$. Soit $g : x \mapsto x^2 - 1$ définie sur $[-1,1]$.
  — Sur l'ouvert $]-1,1[$, s'il y a un extremum local en x, alors $g'(x) = 4x = 0$ et donc $x = 0$. Et alors, $f(x,y) = g(x) = -1$, et c'est un minimum global (au vu de la fonction f) atteint aux points $(0,1)$ et $(0,-1)$.
  — Et, au bord de $[-1,1]$, alors : si $x = 1$ ou si $x = -1$, alors $y = 0$ et donc $f(x,y) = 1$, et c'est un maximum global.

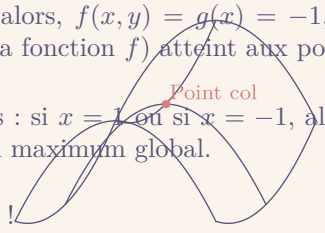


FIGURE 15.8 – Représentation graphique de la fonction f

Proposition (Théorème des extrema liés : c'est une condition nécessaire) **:** Soient f et g deux foncions de classe $\mathscr{C}^1$ de E vers $\mathbb{R}$. Si f est constante sur une partie $C \subset E$, et si la restriction de g à C admet un extremum

local en $\vec{x} \in C$, et si $\vec{x}$ n'est pas un point critique de f, alors

$$\exists \lambda \in \mathbb{R}, \qquad \nabla g(\vec{x}) = \lambda \, \nabla f(\vec{x}).$$

Preuve :
La fonction g est extrémale sous la contrainte $f(x_1, \ldots, x_n) = \mathrm{C}^{\underline{\mathrm{te}}}$. Le gradient est orthogonal aux lignes de niveaux de la fonction. En particulier, $\nabla f(\vec{a})$ est orthogonal à C en tout point $\vec{a} \in C$. On considère un point $M(t) \in C$. À un instant t_0, on aura $M(t_0) = \vec{a}$. Si $g\big|_C$ possède un extremum local en $\vec{a}$, alors, à la date t_0, $\frac{\mathrm{d}}{\mathrm{d}t} g \circ M(t_0) = 0$. Or, d'après la règle de la chaîne, $\frac{\mathrm{d}}{\mathrm{d}t} g \circ M(t_0) = \langle \, \nabla g(M(t_0)) \mid M'(t_0) \, \rangle = 0$. □

Exemple :
Soit C une courbe de niveau d'une fonction $f : \mathbb{R}^2 \to \mathbb{R}$ de classe $\mathscr{C}^1$. Soit A un point du plan. Si la distance AM du point A à un point non critique $M \in C$ possède un extremum local, alors le vecteur $\overrightarrow{AM}$ est orthogonal à la courbe C.

En effet, s'il y a un extremum local de g en (x, y) sous la contrainte $f(x, y) = \mathrm{C}^{\underline{\mathrm{te}}}$, alors $\nabla g(x, y) \,/\!/\, \nabla f(a, b)$.

Exercice :
Déterminer les points du cercle d'équation $x^2 + y^2 = 5$ qui rendent extrémale la valeur $2x + y$.

Soient f et g deux fonctions de classe $\mathscr{C}^1$ définies par $f(x, y) = x^2 + y^2$ et $g(x, y) = 2x + y$. On applique le théorème des extrema liés : s'il existe un extremum en (a, b), alors $\nabla g(a, b) \,/\!/\, \nabla f(a, b)$, *i.e.* $(2, 1) \,/\!/\, (2a, 2b)$. D'où, $\left|\begin{smallmatrix} 2 & 2a \\ 1 & 2b \end{smallmatrix}\right| = 0$, d'où $2b - a = 0$. De plus, $a^2 + b^2 = 5$.

Partie VIII

MPI – Mathématiques – Annexes

Chapitre 1

Structures algébriques et division euclidienne

VIII.1 Division euclidienne

Théorème (divison euclidienne dans $\mathbb{N}$) **:** Soient deux entiers $a, b \in \mathbb{N}$. Si b est non-nul, alors

$$\exists!(q,r) \in \mathbb{N}^2, \qquad a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

$\mathbb{N}$	$\mathbb{N}^\star$
$\cap$	$\cap$
a	b
r	q
$\uparrow$	$\uparrow$
reste	quotient

Exercice : 1. On a

$$\begin{array}{cccc|l} 4 & 9 & 0 & & 133 \\ \hline 3 & 9 & 9 & & 0{,}368421\ldots \\ \hline & 9 & 1 & 0 & \\ & \vdots & & & \end{array}.$$

2. On veut montrer que le réel x possède un développement limité implique qu'il est rationnel. On prend pour exemple $0{,}\overline{147} = 0{,}147147147\ldots$ On a

$$\begin{aligned} 0{,}\overline{147} &= 147 \times \left(10^{-3} + 10^{-6} + 10^{-9} + \cdots\right) \\ &= 147 \times 10^{-3}(1 + 10^{-3} + 10^{-6} + \cdots) \\ &= \frac{147}{100} \times \sum_{k=0}^{\infty} (10^{-3})^k = \frac{147}{100} \times \frac{1}{1 - 10^{-3}} \end{aligned}$$

D'où $0,\overline{147} = \frac{147}{999} = \frac{49}{333} \in \mathbb{Q}$.

On démontre maintenant montrer le "sens inverse." On prend pour exemple $49 \div 333$:

$$\begin{array}{ccccccc|c} 4 & 9 & 0 & & & & & 333 \\ \hline 1 & 5 & 7 & 0 & & & & 0,\overline{147} \\ 1 & 3 & 3 & 2 & & & & \\ & 2 & 3 & 8 & 0 & & & \\ & 2 & 3 & 3 & 1 & & & \\ & & & 4 & 9 & 0 & & \end{array}$$

Il n'y a pas, par contre, unicité du développement décimal : $1 = 1,\overline{0} = 0,\overline{9}$.

Théorème : Soient deux polynômes A et $B \in \mathbb{K}[X]$. Si B est non-nul,

$$\exists!(Q,R) \in \mathbb{K}[X]^2, \qquad A = BQ + R \quad \text{et} \quad \deg R < \deg B.$$

$$\begin{array}{c|c} \mathbb{K}[X] \ni A & B \in \mathbb{K}[X] \setminus \{0\} \\ \hline R & Q \end{array}$$

Exercice :
Soit $n \in \mathbb{N}$. On va calculer $R_n(X)$ sans calculer $Q_n(X)$.

$$\begin{array}{c|c} X^n & X^2 - (n-2)X - (n-1) \\ \hline R_n = ? & Q_n \end{array}$$

On sait, d'après le théorème de la division euclidienne, que $\deg R_n < 2$ d'où $R_n = \alpha_n X + \beta_n$. De plus, $X^n = \big(X^2 - (n-2)X - (n-1)\big)\, Q_n(X) + R_n(X)$. On sait que, pour un polynôme de la forme $X^2 - sX + p$, s est la somme des racines de ce polynôme et p est le produit des racines. On en déduit que les racines de $X^2 - (n-2)X - (n-1)$ sont $n-1$ et -1. D'où, $X^n = \big(X - (n-1)\big)\big(X+1\big)Q_n(X) + \alpha_n X + \beta_n$. On choisit des valeurs de X qui permettent de calculer α_n et β_n. Par exemple, avec $X = n-1$, on a $(n-1)^n = \alpha_n(n-1) + \beta_n$; et, avec $X = -1$, on a $(-1)^n = -\alpha_n + \beta_n$. On résout ce système d'équations :

$$\left.\begin{array}{l} (n-1)^n = \alpha_n(n-1) + \beta_n \\ (-1)^n = \beta_n - \alpha_n \end{array}\right\} \underset{\substack{L_1 \leftarrow L_1 + (n-1)L_2 \\ L_2 \leftarrow L_2 - L_1}}{\iff} \begin{cases} (n-1)^n + (n-1)(-1)^n = \beta_n + (n-1)^n\beta_n \\ \dots \end{cases}$$

$$\iff \begin{cases} \alpha_n = \dots \\ \beta_n = \dots \end{cases}$$

VIII.2 Structures algébriques

— Exemples de groupes : $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}^\star,\times)$, $(S_n,\circ)$, $\big(\mathscr{M}_{n,m}(\mathbb{K}),+\big)$, $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$.

— $(A,+,\times)$ est un *anneau* si

  — $(A,+)$ est un groupe commutatif

— $\times$ est associative
— le neutre de $\times$ est 1_A
— x est distributive par rapport à $+$ (dans les deux sens) :

$$(a+b)\times c = a\times c + b\times c \qquad \text{et} \qquad c\times(a+b) = c\times a + c\times b.$$

Exemple d'anneau : $\big(\mathbb{K}[X],+,\times\big)$ est un anneau *commutatif* (car $\times$ est commutative) ; $\big(\mathscr{M}_n(\mathbb{K}),+,\times\big)$ est un anneau non-commutatif.

— $(K,+,\times)$ est un corps si $(A,+,\times)$ est un anneau commutatif et tout élément différent de 0_K est inversible.

Exemple de corps : $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ MAIS $\big(\mathrm{GL}_n(\mathbb{K}),+,\times\big)$ n'est pas un corps (et ce n'est pas un anneau non plus).

— La définition d'un espace vectoriel n'est pas *vraiment* à connaître... On utilisera, en général, plus la définition d'un sous-espace vectoriel.

— $(M,+,\times,\cdot)$ est une K-algèbre si
  — $(M,+,\times)$ est un anneau ;
  — $(M,+,\cdot)$ est un K-espace vectoriel ;
  — prop3

Par exemple, $(\mathbb{R}^2,+,\cdot)$ est un espace vectoriel. $+$ est une opération interne (vecteur+vecteur = vecteur) mais $\cdot$ est une opération externe $(\mathscr{M}_n(\mathbb{K},+,\cdot)$ est un espace vectoriel. $+$ est interne (matrice + matrice = matrice), $\cdot$ est externe (réel $\cdot$ matrice = matrice), et $\times$ est interne (matrice $\times$ matrice = matrice). On dit alors que $(\mathscr{M}_n(\mathbb{K}),+,\times,\cdot)$ est une K-algèbre.

FIGURE 1.1 – Structure d'un sous-groupe $H \subset G$

[Sous-groupe] Soit H une partie de G ($H \subset G$) et H est stable par $+$ ($\forall x,y \in H$, $x+y \in H$) et avec la loi $+$ induite sur H, $(H,+)$ est un groupe. Dans ce cas, H est un sous-groupe de $(G,+)$.

Dans la pratique, on montre

$$(H,+) \text{ est un sous-groupe} \iff \begin{cases} H \subset G \\ H \text{ stable par } + \\ 0_G \in H \\ \forall x \in H,\ -x \in H \end{cases} \iff \begin{cases} \neq H \subset G \\ \forall x,y \in H,\ x-y \in H. \end{cases}$$

EXERCICE :
On va montrer que H est un sous-groupe de $(\mathbb{Z},+)$ si et seulement s'il existe un entier $n \in \mathbb{Z}$, tel que $H = n\mathbb{Z} = \{n\times k \mid k \in \mathbb{Z}\}$.

1. Soit $H = n\mathbb{Z}$. On veut montrer que H est un sous-groupe de $(\mathbb{Z}, +)$. On a bien $H \subset G$ et, pour tout $x, y \in \mathbb{Z}$, on a

$$\underbrace{nx}_{\in H} + \underbrace{ny}_{\in H} = \underbrace{n(x+y)}_{\in H}.$$

   On a aussi $0 \in H$ car $0 = 0 \times n$. Enfin, pour tout entier $x \in \mathbb{Z}$, on a $-(nx) = n \times (-x) \in H$.

   On en conclut que $(H, +)$ est un sous groupe de $(\mathbb{Z}, +)$.
2. Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Si $H \neq \{0\}$, alors il existe $n \in \mathbb{Z}$, $n \in H$. D'où $-n \in H$, et d'où, il existe un élément positif dans H. On considère sans perte de généralité qu'il s'agit de n. On en déduit que $n\mathbb{Z} \subset H$.

   On choisit, à présent, le plus petit n. On procède par l'absurde : on suppose qu'il existe $x \in H$ tel que $x \notin n\mathbb{Z}$. On fait la division euclidienne de x par n : $x = nq + r$ et $r < n$. D'où, $x - nq = r < n$. Or, x et nq sont deux éléments de H. On en conclut que $r \in H$. C'est absurde car $r < n$ et n est le plus petit.

VIII.3 Idéaux

FIGURE 1.2 – Sous-groupe de $(\mathbb{Z}, +)$

Définition : Soit $(A, +, \times)$ un anneau commutatif. On appelle *idéal* de A tout sous-groupe I de $(A, +)$ tel que $\forall (i, a) \in I \times A$, $i \times a \in I$.

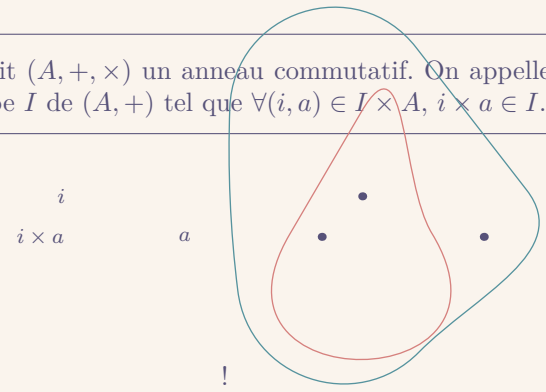


FIGURE 1.3 – Structure d'un idéal $I \subset A$

[B] Un idéal n'est pas forcément un sous-anneau car on n'a pas forcément $1_A \in I$.

EXEMPLE : 1. Soit $a \in \mathbb{K}$. On pose $I = \{P \in \mathbb{K}[X] \mid P(a) = 0\}$. On vérifie aisément que $(I, +)$ est bien un sous-groupe de $(\mathbb{K}[X], +)$:

   $0_{\mathbb{K}[X]}$ s'annule en a et si $P(a) = 0$ et $Q(a) = 0$ alors, $(P+Q)(a) = 0$ et $(P-Q)(a) = 0$.

   Pour tout polynôme $Q \in \mathbb{K}[X]$, on a, si $P(a) = 0$, alors $(P \times Q)(a) = 0$.
   On en conclut que I est un idéal de $(A, +, \times)$.

2. On considère l'ensemble des suites qui tendent vers 0, I. Ce n'est pas un idéal de l'ensemble des suites, $\mathbb{R}^{\mathbb{N}}$: on a bien que I est un sous-groupe de $(\mathbb{R}^{\mathbb{N}},+)$ mais, par exemple la suite $\left(\frac{1}{n}\right) \in I$ multipliée par la suite $(n) \in \mathbb{R}^{\mathbb{N}}$ ne donne pas une suite tendant vers 0. En effet, $\frac{1}{n} \times n = 1 \not\to 0$. Mais, c'est bien un idéal de l'ensemble des suites bornées.

Proposition (les idéaux de $\mathbb{Z}$ et $\mathbb{K}[\boldsymbol{X}]$) **:**
1. Dans l'anneau commutatif $(A,+,\times)$, pour tout $k \in A$, l'ensemble $k \times A$ des multiples de k est un idéal de A, appelé *idéal engendré* de A par k.
2. I est un idéal de $\mathbb{Z}$ si et seulement s'il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.
3. I est un idéal de $\mathbb{K}[X]$ si et seulement s'il existe un polynôme $P(X) \in \mathbb{K}[X]$ tel que $I = P(X) \cdot \mathbb{K}[X]$.

Preuve (2.) " $\Longrightarrow$ " Soit I un idéal de $\mathbb{Z}$. En particulier, $(I,+)$ est un sous-groupe de $(\mathbb{Z},+)$ et donc, d'après l'EXERCICE 5, il existe un entier n tel que $I = n\mathbb{Z}$.

" $\Longleftarrow$ " Réciproquement, si $I = n\mathbb{Z}$, alors c'est un idéal car :
- $(n\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$ d'après l'EXERCICE 5.
- $\underbrace{(nx)}_{\in I} \times \overbrace{y}^{\in \mathbb{Z}} = \underbrace{n(x \times y)}_{\in I}$.

□

EXERCICE :
Montrer que le noyau d'un morphisme d'anneaux commutatif est idéal.

Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. Soit $\varphi : A \to B$ un morphisme d'anneaux :

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \varphi(a \times b) = \varphi(a) \times \varphi(b) \qquad \varphi(1_A) = 1_B.$$

Montrons que $(\operatorname{Ker}\varphi,+)$ est un sous-groupe de $(A,+)$. On sait que $\varphi(0_A) = 0_B$ donc $0_A \in \operatorname{Ker}\varphi$ et donc $\operatorname{Ker}\varphi \neq$. Soient $a,b \in \operatorname{Ker}\varphi$. On a $\varphi(a-b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$ donc $(a-b) \in \operatorname{Ker}\varphi$.

Soient $\varepsilon \in \operatorname{Ker}\varphi$ et $b \in A$. On a $\varphi(\varepsilon \times b) = \varphi(\varepsilon) \times \varphi(b) = 0$.

Proposition : Dans l'anneau commutatif $(A,+,\times)$, la somme de deux idéaux et l'intersection de deux sont encore un idéal. En particulier, dans l'anneau $(\mathbb{Z},+,\times)$ des entiers relatifs,

$$\forall (p,q) \in \mathbb{Z}^2, \quad p\mathbb{Z}+q\mathbb{Z} = \operatorname{pgcd}(p,q)\mathbb{Z} \qquad \text{et} \qquad p\mathbb{Z} \cap q\mathbb{N} = \operatorname{ppcm}(p,q)\mathbb{Z}$$

car $d \mid p \iff p\mathbb{Z} \subset d\mathbb{Z}$ (*i.e.* tout multiple de p est un multiple de d). [1]

Preuve :
Soient I et J deux idéaux. L'intersection de deux sous-groupes est un sous-groupe. De plus, pour tout élément i de $I \cap J$, pour tout élément a de A, on a $a \times i \in I$ car I est un idéal, et $a \times i \in J$ car J est un idéal. D'où, $I \cap J$ est un idéal. De plus, pour tout élément $i + j$ de $I + J$, on a $(i + j) \times a = ia + ja \in I + J$.

Montrons $p\mathbb{Z} + q\mathbb{Z} = \text{pgcd}(p, q)\,\mathbb{Z}$. On pourra montrer, d'une manière similaire, $p\mathbb{Z} \cap q\mathbb{Z} = \text{ppcm}(p, q)\,\mathbb{Z}$. On sait que $p\mathbb{Z} + q\mathbb{Z}$ est un idéal de $\mathbb{Z}$, il existe $d \in \mathbb{Z}$ tel que $p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z}$ $(\heartsuit)$. Montrons que $d = \text{pgcd}(p, q) = p \wedge q$. D'après $(\heartsuit)$, il en résulte que $p\mathbb{Z} \subset d\mathbb{Z}$, d'où $p \mid d$; et, $q\mathbb{Z} \subset d\mathbb{Z}$, d'où $d \mid q$. Ainsi, d est un diviseur commun à p et q. Montrons que c'est le plus grand. On suppose que δ est un diviseur commun à p et q. On veut montrer que $\delta \mid d$. Ainsi, $\delta \mid p$ et $\delta \mid q$, alors δ est un diviseur de tout élément de $p\mathbb{Z} + q\mathbb{Z}$ et en particulier de d. D'où, $\delta \mid d$. □

Corollaire :
Lemme de Bézout. Deux entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe $(u, v) \in \mathbb{Z}^2$ tels que $a \times u + b \times v = 1$.
Lemme de Gauß. Si $a \mid bc$ et a est premier avec b, alors $a \mid c$.

Preuve :
Lemme de Bézout. D'une part, si $a \wedge b = 1$, alors $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$ et en particulier $1 \in 1\mathbb{Z}$. D'autre part, si $au + bv = 1$, alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ d'où $a \wedge b = 1$.
Lemme de Gauß. On a $a \wedge b$ d'où, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$, tels que $au + bv = 1$. Ainsi, $acu + bcv = c$. Or, $a \mid bc$, et $a \mid ac$ d'où $a \mid c$.

□

Exercice :
Montrer que, si b et c sont premiers entre eux et divisent a, alors bc divise a.

Comme $b \mid a$, il existe $k \in \mathbb{Z}$ tel que $a = kb$. De plus, $b \wedge c = 1$, et $c \mid a = kb$, d'où $c \mid k$. Il existe donc $k' \in \mathbb{Z}$ tel que $k = k'\,c$. Ainsi, $a = kk'bc$, d'où $bc \mid ăa$.

VIII.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition : Soit $n \in \mathbb{N}^\star$. La relation $x \equiv a\ [n]$ (« x est congru à a modulo n ») définie par $n \mid (x - a)$ est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a\ [n]\}$ est la *classe d'équivalence* de a. L'ensemble $\{\bar{1}, \bar{2}, \ldots, \bar{n}\}$ des classes d'équivalences est noté $\mathbb{Z}/n\mathbb{Z}$.

1. Rappel : $d \mid p$ si, et seulement si, d divise p si, et seulement si, p est un multiple de d si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $p = k \times d$.

Ainsi, $\bar{x} = \bar{y} \iff x \equiv y \ [n]$. De plus, si $x \equiv a \ [n]$ et $y \equiv b \ [n]$, on a $(x+y) \equiv (a+b) \ [n]$, on note donc $\bar{x} + \bar{y} = \overline{x+y}$. De même pour le produit.

Proposition : Un entier $x \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^\star$ si, et seulement si, $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ est inversible. Par suite, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un corps (aussi noté $\mathbb{F}_n$) si, et seulement si, $n \in \mathbb{N}^\star$ est un nombre premier.

Contre-exemple : avec le corps nul $0 = \{0\}$, ce théorème est faux.

Preuve :

$$\begin{aligned}
\bar{x} \in \mathbb{Z}/n\mathbb{Z} \text{ est inversible} &\iff \exists u \in \mathbb{Z},\ \bar{u} \times \bar{x} = \bar{1} \\
&\iff \exists u \in \mathbb{Z},\ \overline{u \times x} = \bar{1} \\
&\iff \exists u \in \mathbb{Z},\ u \times x \equiv 1 \ [n] \\
&\iff \exists u \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ u \times x = 1 + k \times n \\
&\iff \exists (u,k) \in \mathbb{Z}^2,\ u \times x - k \times n = 1 \\
&\iff x \wedge n = 1
\end{aligned}$$

En particulier, tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles. □

Théorème (Théorème chinois) **:** Si a et b sont premiers entre eux, alors deux congruences modulo a et modulo b équivalent à une congruence modulo ab car les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes.

Preuve :
Pour tout $x \in \mathbb{Z}$, on note $\pi_a(x) \in \mathbb{Z}/a\mathbb{Z}$ la classe d'équivalence de x dans $\mathbb{Z}/a\mathbb{Z}$; de même, on note $\pi_b(x) \in \mathbb{Z}/b\mathbb{Z}$ et $\pi_{ab}(x) \in \mathbb{Z}/(ab)\mathbb{Z}$. On construit la fonction

$$\begin{aligned}
f : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\longrightarrow \mathbb{Z}/(ab)\mathbb{Z} \\
\big(\pi_a(x), \pi_b(x)\big) &\longmapsto \pi_{ab}(x).
\end{aligned}$$

Elle est bien définie car : si $\pi_a(y) = \pi_a(x)$ et $\pi_b(y) = \pi_b(x)$, alors $y \equiv x \ [a]$ et $y \equiv x \ [b]$, d'où il existe $k \in \mathbb{Z}$ tel que $y = x + ka$ et il existe $\ell \in \mathbb{Z}$ tel que $y = x + \ell b$, donc $ka = \ell a$ et donc $b \mid ka$; et, $a \wedge b$, par le théorème de Gauss, on a $b \mid k$, il existe donc $m \in \mathbb{Z}$ tel que $k = mb$ donc $y = x + m \cdot ab$, d'où $\pi_{ab}(y) = \pi_{ab}(x)$. L'application f est un morphisme d'anneaux par les propriétés des classes d'équivalences vues précédemment ($\bar{x}+\bar{y} = \overline{x+y}$ et $\bar{x}\times\bar{y} = \overline{x \times y}$), et par construction. De plus, f est injective car $\operatorname{Ker} f = \{(0,0)\}$ ($x \equiv 0 \ [ab]$ implique $x \equiv 0 \ [a]$ et $x \equiv 0 \ [b]$). De plus, $\operatorname{Card}(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) = a \times b = \operatorname{Card}(\mathbb{Z}/(ab)\mathbb{Z})$. D'où, f est bijective. □

Exercice :
Déterminer tous les entiers relatifs tels que $x \equiv 2\ [4]$ *et* $x \equiv 3\ [5]$.

On note (S) le système $x \equiv 2\ [4]$ et $x \equiv 3\ [5]$, (S_1) et (S_2) les deux équations. Comme $4 \wedge 5 = 1$, d'après le théorème chinois, le système (S) est équivalent à $x \equiv ?\ [4 \times 5]$.

1ère méthode. (On devine « ? ».) Avec 18 est une solution car $18 \equiv 2\ [4]$ (car $4 \mid (18-2)$) et $18 \equiv 3\ [5]$ (car $5 \mid (18-3)$).

2nde méthode. Analyse. L'équation (S_1) est équivalente à $\exists t \in \mathbb{Z}$, $x = 2+4t$. On choisit ce t. D'où, d'après l'équation (S_2), on a $2+4t \equiv 3\ [5]$, d'où $4t \equiv 1\ [5]$. Or, $\bar{4}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$, car $4 \wedge 5 = 1$. On trouve cet inverse : 4. Ainsi, $t \equiv 4\ [5]$. Synthèse : *c.f.* 1ère méthode.

Définition : Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ (*i.e.* le nombre d'entiers de $[\![1, n]\!]$ premiers avec n) est noté $\varphi(n)$. L'application $\varphi : n \mapsto \varphi(n)$ est appelée l'*indicatrice d'Euler*.

On a $\varphi(8)$ car les entiers de $[\![1, 7]\!]$ premiers avec 8 sont 1, 3, 5, 7.

Méthode (Comment calculer l'indicatrice d'Euler) :

(*i*) Si p est premier, alors $\varphi(p) = p-1$ car tous les éléments de $[\![1, p-1]\!]$ sont premiers avec p. Et, $\forall k \in \mathbb{N}^\star$, on a $\varphi(p^k) = p^k \cdot (1 - 1/p)$.

(*ii*) Si a et b sont premiers entre eux, alors $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. En effet, d'après le théorème chinois, il y a autant d'éléments inversibles dans $\mathbb{Z}/(ab)\mathbb{Z}$ et dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ par isomorphisme.

(*iii*) Si $p_1, \ldots, p_k$ sont les diviseurs premiers de n, alors

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right).$$

En effet, on a $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, d'où $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$. Calculons $\varphi(p_1^{\alpha_1})$: on cherche tous les entiers de $[\![1, p_1^{\alpha_1}]\!]$ premiers avec $p_1^{\alpha_1}$. On cherche donc tous les entiers $[\![1, p_1^{\alpha_1}]\!]$. Les multiples de p_1 dans $[\![1, p_1^{\alpha_1}]\!]$ sont $p_1, 2p_1, \ldots, p_1^{\alpha_1-1} \times p_1$: il y en a $p_1^{\alpha_1-1}$. Il y a donc $p_1^{\alpha_1} - p_1^{\alpha_1-1}$ non multiples de p_1. D'où, $\varphi(p_1^{\alpha_1}) = p_1^{\alpha_1} \cdot (1 - 1/p_1)$. Ainsi, on en déduit la formule de $\varphi(n)$ précédente.

VIII.5 L'ordre d'un élément

Si a est un élément d'un groupe $(G, \cdot)$ d'élément neutre 1, alors l'ensemble $\{\ldots, a^{-2}, a^{-1}, 1, a^1, a^2, \ldots\} = \{a^k \mid k \in \mathbb{Z}\}$ est un sous-groupe de G, appelé le sous-groupe engendré par a, et il est noté $\langle a \rangle$. C'est le plus petit sous-groupe de G contenant a.

Si ce sous-groupe est un ensemble fini, alors son cardinal est appelé l'*ordre* de a. L'ordre de a est le plus petit entier k strictement positif tel que $a^k = 1$. Et, les entiers k tels que $a^k = 1$ sont les multiples de l'ordre de a. On dit que le groupe G est *monogène* s'il est, lui-même, engendré par un élément et qu'il est *cyclique* s'il est monogène et fini.

Exercice :
Décomposer en cycle disjoints la permutation σ du groupe symétrique $\mathfrak{S}_7$ et en déduire l'ordre de σ, où

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 2 & 6 & 1 & 3 \end{pmatrix}.$$

Les images successives de 1 sont 1, 5 et 6 ; celles de 2 sont 2 et 4 ; celles de 3 sont 3 et 7. D'où, $\sigma = (1 \quad 5 \quad 6)\cdot(2 \quad 4)\cdot(3 \quad 7)$. L'ordre de σ est 6, ce qui correspond au plus petit commun multiple des ordres des cycles (donc $\mathrm{ppcm}(2,2,3)$).

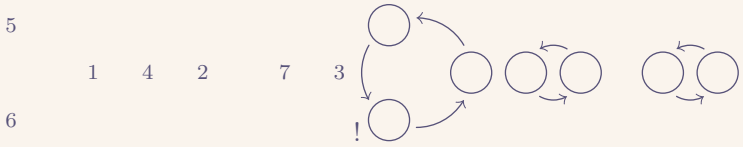


Figure 1.4 – Décomposition en cycles de la permutation σ

Le groupe $(\mathbb{Z}, +)$ est monogène car $\mathbb{Z} = \langle 1 \rangle$. Mais, $(\mathfrak{S}_n, \cdot)$ n'est pas monogène.

Proposition : Si G est un groupe fini, alors $\forall a \in G$, $o(a) \mid \mathrm{Card}\, G$, où $o(a)$ est l'ordre de a. □

Corollaire : Théorème d'Euler. Si $a \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^\star$, alors $a^{\varphi(n)} \equiv 1 \ [n]$.

Petit théorème de Fermat. Si p est un nombre premier, alors $\forall a \in \mathbb{Z}$, on a $a^p \equiv a \ [p]$.

Exercice :
Calculer $\varphi(10)$ et en déduire que le dernier chiffre de l'écriture décimale de 3^{345} est 3. Calculer $\varphi(100)$ et en déduire que les deux derniers chiffres de l'écriture décimale de 3^{345} sont 4 et 3.

On trouve $\varphi(10) = 4$ car les entiers de $[\![1, 10]\!]$ premiers avec 10 sont 1, 3, 7 et 9. On trouve aussi $\varphi(100) = 40$ car $100 = 4 \times 25 = 2^2 \times 5^2$, d'où les diviseurs premiers de 100 sont 2 et 5, et donc $\varphi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 50 \times 4/5 = 40$.

On cherche $r \in [\![0, 9]\!]$ tel que $3^{385} \equiv 1 \ [10]$. On a $3 \wedge 10 = 1$, d'où, d'après le théorème d'Euler, $3^{\varphi(10)} \equiv 1 \ [1]\, 0$ et donc $3^4 \equiv 1 \ [1]\, 0$. Or,

$$3^{345} = 3^{344} \times 3 = (3^4)^{86} \times 3 \equiv 1^{86} \times 3 \equiv 3 \ [10]\,.$$

Donc $r = 3$.

On cherche $r \in [\![0, 99]\!]$ tel que $3^{345} \equiv r \ [100]$. De même, d'après le théorème d'Euler, $3^{\varphi(100)} \equiv 1 \ [100]$, d'où $3^{40} \equiv 1 \ [100]$. Or, $3^{345} = (3^{40})^8 \times 3^{25} \equiv 3^{25} \ [100]$. Et, $3^{25} = 3^5 \times (3^5)^4 = 3 \cdot 81 \cdot (3^5)^4 \equiv 43 \times (3^4)^5 \equiv 43 \ [100]$. D'où, $3^{345} \equiv 43 \ [100]$.

Chapitre 2

La compacité

Définition : On dit qu'une partie $K \subset E$ d'un espace vectoriel normé (de dimension potentiellement infinie) E est *compacte* si, de toute suite $(\vec{u}_n)$ de vecteurs de K, on peut extraire une suite convergent vers un vecteur $\vec{\ell} \in K$, *i.e.*, il existe une fonction $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $\lim_{n\to\infty} \vec{u}_{\varphi(n)}$ existe et appartient à K.

Théorème (Bolzano-Weierstaß) **:** De toute suite réelle bornée, on peut extraire une suite convergente (*i.e.* tout segment de $\mathbb{R}$ est compacte). □

Remarque :
Soit $(\vec{u}_n)_{n\in\mathbb{N}}$ une suite de vecteurs d'un espace vectoriel normé E. On dit qu'un vecteur $\vec{a} \in E$ est une *valeur d'adhérence* de $(\vec{u}_n)_{n\in\mathbb{N}}$ si on peut extraire de $(\vec{u}_n)_{n\in\mathbb{N}}$ une suite convergent vers $\vec{a}$.

1. Par définition, une partie K de E est compacte si, et seulement si, toute suite de vecteurs possède au moins une valeur d'adhérence.
2. La suite réelle définie par $u_n = n$ ne possède aucune valeur d'adhérence, et elle n'est pas bornée.
3. Une suite réelle, même bornée, peut posséder plusieurs valeurs d'adhérence. Par exemple, les valeurs d'adhérence de la suite de réels $(-1)^n$ sont -1 et 1.
4. Mais, si une suite de vecteurs est convergente, alors elle possède une unique valeur d'adhérence (égale à sa limite) : c'est la proposition 14 du chapitre 13. En contraposant, on a : si une suite possède plusieurs valeurs d'adhérence, alors elle diverge (on prouve ainsi que la suite des réels $(-1)^n$ diverge).
5. La réciproque est fausse : la suite (u_n) définie par $u_{2p} == 1$ et $u_{2p+1} = p$ possède une unique valeur d'adhérence (égale à 1), mais elle diverge.
6. Hormis dans un compact, où elle est vraie. ▷ Proposition suivante

Proposition : Une suite de vecteurs d'un compact K converge si, et seulement si, elle possède une unique valeur d'adhérence.

Preuve « $\Longrightarrow$ » Si une suite $(\vec{u}_n)_{n\in\mathbb{N}}$ converge vers une limite $\vec{\ell}$, alors toute suite extraite de $(\vec{u}_n)_{n\in\mathbb{N}}$ converge aussi vers $\vec{\ell}$. D'où, $\vec{\ell}$ est l'unique valeur d'adhérence de $(\vec{u}_n)_{n\in\mathbb{N}}$.

« $\Longleftarrow$ » On suppose que $(\vec{u})_{n\in\mathbb{N}}$ possède une unique valeur d'adhérence $\vec{\ell}$. Montrons, par l'absurde, que la suite $\vec{u}_n$ converge. Supposons donc que $(\vec{u}_n)_{n\in\mathbb{N}}$ ne converge pas vers $\vec{\ell}$. Autrement dit, il existe $\varepsilon > 0$ tel que, pour tout $N \in \mathbb{N}$, il existe $n \geqslant N$ tel que $\|\vec{u}_n - \vec{\ell}\| \geqslant \varepsilon$. On en déduit que l'on peut extraire de $(\vec{u}_n)_{n\in\mathbb{N}}$ une suite $(\vec{v}_n)_{n\in\mathbb{N}}$ qui ne rentre jamais dans la boule $\bar{B}(\vec{\ell}, \varepsilon)$. Or, pour tout $n \in \mathbb{N}$, le vecteur $\vec{v}_n$ appartient à K, un compact. D'où, par définition, on peut extraire de la suite $(\vec{v}_n)_{n\in\mathbb{N}}$ une suite $(\vec{w}_n)_{n\in\mathbb{N}}$ qui converge vers $\vec{\ell}'$. Et, $(\vec{w}_n)_{n\in\mathbb{N}}$ est une suite extraite de $(\vec{u}_n)$. D'où, $\vec{\ell}'$ est une valeur d'adhérence de $(u_n)_{n\in\mathbb{N}}$. Or, $\vec{\ell} \neq \vec{\ell}'$, ce qui est absurde.

□

Lemme : (i) Toute partie fermée d'un compact est un compact.
$((ii))$ Le produit cartésien de deux compacts est un compact. (Par récurrence pour un produit fini de compact)

Preuve : (i) On suppose $F \subset K$, où F est un fermé et K est un compact. Montrons que F est compact. Soit $(\vec{u}_n)_{n\in\mathbb{N}}$ une suite de vecteurs de $F : \forall n \in \mathbb{N}, \vec{u}_n \in F$. Or, $F \subset K$, d'où, $\forall n \in \mathbb{N}, \vec{u}_n \in K$. Et, K est un compact, on peut donc extraire de $(\vec{u}_n)$ une suite $(\vec{v}_n)$ qui converge dans K. Soit ainsi $\vec{\ell} = \lim \vec{v}_n$. De plus, pour tout $n \in \mathbb{N}$, $\vec{v}_n \in F$ et F est un fermé. D'où, $\vec{\ell} \in F$ par la caractérisation séquentielle d'un fermé.

$((ii))$ Soient K_1 et K_2 deux compacts. Montrons que $K_1 \times K_2$ est un compact. Soit $\big((\vec{u}_n, \vec{v}_n)\big)_{n\in\mathbb{N}}$ une suite d'éléments de $K_1 \times K_2$. Pour tout $n \in \mathbb{N}$, $\vec{u}_n \in K_1$, qui est un compact. On extrait donc de $(\vec{u}_n)$ une suite $(\vec{u}_{\varphi(n)})$ qui converge dans K_1. De la suite $(\vec{v}_{\varphi(n)}$, on extrait la suite $(\vec{v}_{\varphi(\psi(n))})$ qui converge dans K_2. La suite $\big((\vec{u}_{\varphi(\psi(n))}, \vec{v}_{\varphi(\psi(n))})\big)$ converge dans $K_1 \times K_2$ car $(\vec{u}_{\varphi(\psi(n))})$ converge dans K_1 et $\vec{v}_{\varphi(\psi(n))}$ converge dans K_2.

□

Proposition : (i) Toute partie compacte d'un espace vectoriel normé

est fermée et bornée.

(*ii*) La réciproque est vraie dans $\mathbb{R}^n$: une partie de $\mathbb{R}^n$ est fermée si, et seulement si, elle est fermée et bornée.

Exercice :
Montrer que

(*a*) *toute intersection de compacts est un compact ;*

(*b*) *l'union de deux compacts est un compact (de même, par récurrence, pour une union finie de compacts).*

width=!,height=!,pages=-

Proposition : Soient E et F deux *evn* de dimensions potentiellement infinies. Soit une fonction continue $f : E \to F$. Si $K \subset E$ est un compact de E, alors $f(K)$ est un compact de F. Autrement dit, « l'image d'un compact par une fonction continue est un compact. » En particulier, toute fonction réelle continue sur un compact est bornée et atteint ses bornes.

Preuve :
Soit $(\vec{v}_n)$ une suite de vecteurs de $f(K)$. On veut extraire une suite de $f(K)$ qui converge dans $f(K)$. Pour tout $n \in \mathbb{N}$, il existe $\vec{u}_n \in K$ tel que $\vec{v}_n = f(\vec{u}_n)$. Or, K est un compact. On peut donc extraire de $(\vec{u}_n)$ de vecteurs $(\vec{u}_{\varphi(n)})$ qui converge dans K, on note $\vec{\ell}$ sa limite. Ainsi, $\vec{u}_{\varphi(n)} \to \vec{\ell}$ et, comme f est continue, $f(\vec{u}_{\varphi(n)}) \to f(\vec{\ell})$. D'où, $f(K)$ est un compact. □

Proposition : ...

Exercice :
On munit l'espace vectoriel $\mathbb{R}[X]$ *de la norme définie par* $\|P\| = \max_{k\in[\![0,\deg P]\!]} |a_k|$ *pour tout polynôme* $P = \sum_{k=0}^{\deg P} a_k X^k$. *Montrer que la partie* $F = \{P \in \mathbb{R}[X] \mid \|P\| = 1\}$ *est une partie fermée et bornée de* $\mathbb{R}[X]$, *mais ce n'est pas un compact.*

Afin de valider que $\|\cdot\|$ est une norme, on pose $\|0\| = 0$. La partie F est la sphère centrée en 0 et de rayon 1 : $\mathcal{S}(0,1) = \bar{B}(0,1) \setminus \mathring{B}(0,1)$. Elle est donc bornée : $\forall P \in F$, $\|P\| = 1 \leqslant 1$. De plus, F est un fermé car $F = \|\cdot\|^{-1}(\{1\})$, $\|\cdot\|$ est continue (car toute norme est 1-lipschitzienne) et $\{1\}$ est un fermée. Mais, F n'est pas un compact. En effet, on considère la suite de polynôme (P_n) définie par $P_n = X^n$. Pour tout $n \in \mathbb{N}$, $\|P_n\| = \max(0,1) = 1$. Par l'absurde, supposons que l'on peut extraire de (P_n) une suite $(X^{\varphi(n)})$ convergente, et on note ℓ sa limite. Or, $\|X^{\varphi(n)} - X^{\varphi(n+1)}\| = \max(-1,0,1) = 1$. Et, les égalités passent à la limite, $0 = \|\ell - \ell\| = 1$, ce qui est absurde.

Théorème (Heine) **:** Toute fonction continue sur un compact est uniformément continue.

Chapitre 3

Séries de vecteurs et exponentielle de matrices

Nous avons vu au chapitre 12 que toute application linéaire ou multilinéaire sur un espace vectoriel normé de dimension finie est continue et que, par conséquent, sont des applications continues :

— la transposée $\square^\top : \mathscr{M}_{n,n}(\mathbb{K}) \ni A \mapsto A^\top$,
— un changement de base $\mathscr{M}_{n,n}(\mathbb{K}) \ni A \mapsto P^{-1} \cdot A \cdot P$,
— la multiplication matricielle : $\big(\mathscr{M}_{n,n}(\mathbb{K})\big)^2 \ni (A, B) \mapsto A \cdot B$.

Par suite, si $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ sont deux suites de matrices carrées telles que $A_n \xrightarrow[n\to\infty]{} A$ et $B_n \xrightarrow[n\to\infty]{} B$ alors

(1) $A_n^\top \xrightarrow[n\to\infty]{} A^\top$,
(2) $P^{-1} \cdot A_n \cdot P \xrightarrow[n\to\infty]{} P^{-1} \cdot A \cdot P$,
(3) $A_n \cdot B_n \xrightarrow[n\to\infty]{} A \cdot B$.

On s'intéresse maintenant, non plus à des suites, mais à des séries de vecteurs.

Définition : Soit $(\vec{u}_n)_{n\in\mathbb{N}}$ une suite de vecteurs d'un espace vectoriel normé E. On dit que la série de vecteurs $\sum \vec{u}_n$:

— *converge* si la suite de vecteurs $(\vec{S}_n)_{n\in\mathbb{N}} = \big(\sum_{k=0}^n \vec{u}_k\big)_{n\in\mathbb{N}}$ converge ;
— *converge absolument* si la série de réels $\sum \|\vec{u}_n\|$ converge.

Proposition : Dans un espace vectoriel normé de dimension finie, si une série de vecteurs converge absolument, elle converge (simplement).

Preuve :
On suppose l'espace vectoriel E de dimension d. Toutes les normes étant

équivalentes en dimensions finie, on choisit une norme adaptée : $\|\vec{u}_n\|_\infty = \max(|u_{n,1}|, \dots, |u_{n,d}|)$ où les $u_{n,i}$ sont les coordonnées du vecteur $\vec{u}_n$ dans une base de E. Pour tout $n \in \mathbb{N}$ et tout $i \in [\![1, n]\!]$, on a $0 \leqslant |u_{n,i}| \leqslant \|\vec{u}_n\|_\infty$. Or, par hypothèse, la série $\sum \|\vec{u}_n\|_\infty$ converge. D'où, pour tout $i \in [\![1, d]\!]$, la série $\sum |u_{n,i}|$ converge. D'où, la série $\sum u_{n,i}$ converge. Et, en dimension finie, la convergence implique une convergence coordonnées par coordonnées. On en déduit que la série $\sum \vec{u}_n$ converge. □

On munit l'espace vectoriel normé $\mathscr{M}_{n,n}(\mathbb{K})$ d'une norme sous-multiplicative. Soient $A \in \mathscr{M}_{n,n}(\mathbb{K})$ une matrice carrée et $\sum a_n z^n$ une série entière (réelle ou complexe) de rayon de convergence R : si $\|A\| < R$, alors la série de matrices $\sum a_k A^k$ converge.

En effet, la norme étant sous-multiplicative, on a $\|A^k\| \leqslant \|A\|^k$ pour $k \in \mathbb{N}^\star$. Pour tout entier $k \in \mathbb{N}^\star$, on a $\|a_k A^k\| = |a_k| \cdot \|A^k\| \leqslant |a_k| \cdot \|A\|^k$. Or, $\|A\| < R$ et la série $\sum a_k \cdot \|A\|^k$ converge absolument. On en déduit que la série $\sum a_k A^k$ converge absolument, donc converge (simplement).

Exemple (Séries géométriques) :
On munit l'espace vectoriel $\mathscr{M}_{n,n}(\mathbb{K})$ d'une norme sous-multiplicative. Si $\|A\| < 1$, alors $I_n - A$ est inversible et

$$(I_n - A)^{-1} = \sum_{k=0}^{\infty} A^k.$$

De même si la matrice A est nilpotente. [1]

En effet, la série entière $\sum z^n$ a pour rayon de convergence $R = 1$. Soit $N \in \mathbb{N}$. On calcule

$$(I_n - A) \cdot \sum_{k=0}^{N} A^k = \sum_{k=0}^{N} A^k - \sum_{k=1}^{N+1} A^k = A^0 - A^{N+1} = I_n - A^{N+1}.$$

On a $0 \leqslant \|A^{N+1}\| \leqslant \|A\|^{n+1}$ qui tend vers 0 quand $N \to \infty$ car $\|A\| < 1$. D'où, d'après le théorème des gendarmes, on a A^{N+1} converge vers la matrice nulle quand $N \to \infty$. Et, comme $\|A\| < 1$, la suite $\left(\sum_{k=0}^{N} A^k\right)$ converge. Ainsi, par continuité de l'application linéaire $\mathscr{M}_{n,n}(\mathbb{K}) \ni M \mapsto (I_n - A) \cdot M$ sur l'espace $\mathscr{M}_{n,n}(\mathbb{K})$ de dimension finie. *Autre rédaction* : par continuité du produit matriciel. Par unicité de la limite, on a $(I_n - A) \cdot \sum_{k=0}^{\infty} A^k = I_n$. On en déduit que

$$\sum_{k=0}^{\infty} A^k = (I_n - A)^{-1}.$$

Si A est nilpotent d'ordre ν, alors

$$(I_n - A) \cdot \sum_{k=0}^{\nu-1} A^k = \sum_{k=0}^{\nu-1} A^k - \sum_{k=1}^{\nu} A^k = I_n - A^\nu = A.$$

1. À savoir, l'hypothèse $\|A\| < 1$ n'est plus obligatoire.

Définition : On appelle *exponentielle d'une matrice* $A \in \mathscr{M}_{n,n}(\mathbb{K})$ quelconque, que l'on note $\exp A$ ou e^A, la matrice

$$\exp A = \mathrm{e}^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k.$$

Cette définition reste vraie peu importe la norme choisie, comme le rayon de convergence de la série entière $\sum z^n/k!$ a un rayon de convergence infini.

Exemple : 1. L'exponentielle de la matrice nulle (0) est I_n car $\sum_{k=0}^{\infty} (0)^k/k! = I_n + (0) + \cdots = I_n$.

2. L'exponentielle d'une matrice diagonale $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ est $\exp \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \mathrm{diag}(\mathrm{e}^{\lambda_1}, \ldots, \mathrm{e}^{\lambda_n})$. En effet,

$$\exp \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} + \frac{1}{1!} \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} + \frac{1}{2!} \begin{pmatrix} \lambda_1^2 & & \\ & \ddots & \\ & & \lambda_n^2 \end{pmatrix} + \cdots = \begin{pmatrix} \mathrm{e}^{\lambda_1} & & \\ & \ddots & \\ & & \mathrm{e}^{\lambda_n} \end{pmatrix}$$

3. D'une part, on a

$$\exp \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix} = I_n + \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix} + \frac{1}{2!} \begin{pmatrix} -\theta^2 & 0 \\ 0 & -\theta^2 \end{pmatrix} + \frac{1}{3!} \begin{pmatrix} 0 & \theta^3 \\ -\theta^3 & 0 \end{pmatrix} + \frac{1}{4!} \begin{pmatrix} \theta^4 & 0 \\ 0 & \theta^4 \end{pmatrix} + \cdots$$

Or, $\sum_{p=0}^{\infty} \frac{1}{(2p)!} \cdot A^{2p} = \begin{pmatrix} \cos\theta & 0 \\ 0 & \cos\theta \end{pmatrix}$ et $\sum_{p=0}^{\infty} \frac{1}{(2p)!} \cdot A^{2p} = \begin{pmatrix} 0 & -\sin\theta \\ \sin\theta & 0 \end{pmatrix}$. Enfin, on en conclut que

$$\exp \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Proposition : Soient $P \in \mathrm{GL}_n(\mathbb{K})$ et $A \in \mathscr{M}_{n,n}(\mathbb{K})$ et $B \in \mathscr{M}_{n,n}(\mathbb{K})$.

1. Si $AB = BA$, alors $\mathrm{e}^{A+B} = \mathrm{e}^A \cdot \mathrm{e}^B$.
2. La matrice e^A est inversible et $(\mathrm{e}^A)^{-1} = \mathrm{e}^{-A}$.
3. La transposée de l'exponentielle est l'exponentielle de la transposée : $(\exp A)^\top = \exp(A^\top)$.
4. L'exponentielle d'une matrice est invariante par changement de base : $\exp(P^{-1} \cdot A \cdot P) = P^{-1} \cdot \exp A \cdot P$.
5. La fonction $t \mapsto \mathrm{e}^{tA}$ est dérivable et $\dfrac{\mathrm{d}}{\mathrm{d}t} \mathrm{e}^{tA} = A \cdot \mathrm{e}^{tA} = \mathrm{e}^{tA} \cdot A$.

Preuve : 1. La démonstration de ce point est dans le poly.

2. Les matrices A et $-A$ commutent, d'où $\mathrm{e}^{A+(-A)} = \mathrm{e}^A \cdot \mathrm{e}^{-A}$. On a donc $I_n = \mathrm{e}^A \cdot \mathrm{e}^{-A}$.

3. Pour tout $N \in \mathbb{N}$, on a

$$\exp(A^\top) \xleftarrow[N\to\infty]{(\star\star)} \sum_{n=0}^{N} \frac{1}{n!}(A^\top)^n = \Big(\sum_{n=0}^{N} \frac{1}{n!}(A^n)\Big)^\top \xrightarrow[N\to\infty]{(\star)} (\exp A)^\top.$$

par continuité de la transposée (pour $(\star)$) et par définition (pour $(\star\star)$).

4. On procède comme le point précédent, par continuité du changement de base.
5. On pose $f : t \mapsto \mathrm{e}^{tA}$, et on calcule

$$\frac{f(t+h)-f(t)}{h} = \frac{\mathrm{e}^{(t+h)A}-\mathrm{e}^{tA}}{h} = \frac{\mathrm{e}^{hA}\cdot\mathrm{e}^{tA}-\mathrm{e}^{tA}}{h} = \frac{(\mathrm{e}^{hA}-I_n)\cdot\mathrm{e}^{tA}}{h}.$$

De plus, $(\exp(hA)-I_n)/h \to A$ quand $h \to 0$ car

$$\exp(hA) = I_n + hA + (hA)^2 \underbrace{\Big(\sum_{k=2}^{\infty} \frac{1}{k!}(hA)^{k-2}\Big)}_{\varepsilon(h)}$$

d'où $(\exp(hA)-I_n)/h = (hA+h^2\varepsilon(h))/h = A+h\varepsilon(h) \to A$. De plus, le produit matriciel est continu. Donc f est dérivable et $f'(t) = A\cdot\mathrm{e}^{tA}$. De plus, $A\cdot\mathrm{e}^{tA} = \mathrm{e}^{tA}\cdot A$.

□

[Cadeaux]

(a) *En supposant connaître les éléments de* $\operatorname{Sp} A$*, quelles sont les valeurs propres de* $\operatorname{Sp}\mathrm{e}^A$ *?* (▷ $\operatorname{Sp}\mathrm{e}^A = \exp(\operatorname{Sp} A)$)

(b) *Que vaut* $\det \mathrm{e}^A$ *?* (▷ $\det \mathrm{e}^A = \mathrm{e}^{\operatorname{tr} A}$)

(c) *Interpréter géométriquement l'égalité* $\exp\begin{pmatrix}0 & -\theta\\ \theta & 0\end{pmatrix} = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$.

(a) Rappel : une matrice est trigonalisable si, et seulement si, son polynôme caractéristique χ_A est scindé. En particulier, pour toute matrice $A \in \mathscr{M}_{n,n}(\mathbb{C})$, A est trigonalisable. Soit $A \in \mathscr{M}_{n,n}(\mathbb{C})$. Soit $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $P^{-1}\cdot A\cdot P = T$ soit triangulaire. Ainsi,

$$T = \begin{pmatrix}\lambda_1 & & \star\\ & \lambda_2 & \\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}.$$

D'où,

$$\begin{aligned}\mathrm{e}^T &= I_n + T + \frac{T^2}{2!} + \frac{T^3}{3!} + \cdots \\ &= \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1 \end{pmatrix} + \begin{pmatrix} \lambda_1 & & \star \\ & \lambda_2 & \\ 0 & & \ddots \\ & & & \lambda_n \end{pmatrix} + \frac{1}{2!}\begin{pmatrix} \lambda_1^2 & & \star \\ & \lambda_2^2 & \\ 0 & & \ddots \\ & & & \lambda_n^2 \end{pmatrix} + \cdots \\ &= \begin{pmatrix} \mathrm{e}^{\lambda_1} & & \star \\ & \mathrm{e}^{\lambda_2} & \\ 0 & & \ddots \\ & & & \mathrm{e}^{\lambda_n} \end{pmatrix}\end{aligned}$$

D'où, $\operatorname{Sp} \mathrm{e}^T = \{\mathrm{e}^{\lambda_1}, \ldots, \mathrm{e}^{\lambda_n}\}$. Or, $\mathrm{e}^T = \mathrm{e}^{P^{-1}\cdot A\cdot P} = P^{-1}\cdot \mathrm{e}^A \cdot P$. D'où, e^T et e^A sont semblables. On en déduit que $\operatorname{Sp} \mathrm{e}^A = \operatorname{Sp} \mathrm{e}^T = \exp(\operatorname{Sp} A)$, car le spectre est un invariant de similitude.

(b) De même, $\det \mathrm{e}^T = \det \mathrm{e}^A$ car le déterminant et la trace sont des invariants de similitude. Or,

$$\det \mathrm{e}^T = \mathrm{e}^{\lambda_1} \times \mathrm{e}^{\lambda_2} \times \cdots \times \mathrm{e}^{\lambda_n} = \mathrm{e}^{\lambda_1 + \cdots + \lambda_n} = \mathrm{e}^{\operatorname{tr} T}.$$

On en déduit que $\det \mathrm{e}^A = \det \mathrm{e}^T = \exp(\operatorname{tr} T) = \exp(\operatorname{tr} A)$.

(c) On relie cette question avec l'exercice 6 du TD 16 :

$$\begin{aligned}(E) &\iff \underbrace{\begin{pmatrix} x' \\ y' \end{pmatrix}}_{X'} = \underbrace{\begin{pmatrix} 0 & -\omega \\ \omega & 0 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{X} \\ &\iff X'(t) = A \cdot X(t) \\ &\iff \forall t \in \mathbb{R},\ X(t) = \underbrace{\begin{pmatrix} \cos \omega t & -\sin \omega t \\ \sin \omega t & \cos \omega t \end{pmatrix}}_{\exp \begin{pmatrix} 0 & -\omega t \\ \omega t & 0 \end{pmatrix} = \exp(tA)} \cdot X(0)\end{aligned}$$

Et alors ? On utilise la proposition 6 : $\dfrac{\mathrm{d}}{\mathrm{d}t}\mathrm{e}^{tA}\cdot X(0) = A\cdot \mathrm{e}^{tA} X(0)$. En posant $X(t) = \mathrm{e}^{tA}\cdot X(0)$, on obtient $\dfrac{\mathrm{d}}{\mathrm{d}t} X(t) = A \cdot X(t)$, ce qui est l'équation (E). On peut résoudre des équations différentielles avec l'exponentielle de matrices.

Chapitre 4

Cadeaux

Cadeaux du 14/09/22

Cadeau 1 :
Soit A un anneau commutatif et soit $x \in A$. On dit que x est nilpotent (ou nihilpotent) si

$$\exists n \in \mathbb{N},\ x^n = 0_A.$$

1. *Montrer que, si x est nilpotent, alors x n'est pas inversible mais $1_A - x$ est inversible.*
2. *Montrer que l'ensemble des éléments nilpotents de A est un idéal de A.*

Réponse du cadeau 1 :

1. On procède par l'absurde. On suppose que x est nilpotent. Soit $n \in \mathbb{N}$ le plus petit possible tel que $x^n = 0_A$. On suppose qu'il existe $y \in A$ tel que $x \cdot y = 1_A$. D'où, $(xy)^n$ est, d'une part $x^n \cdot y^n = 0_A \cdot y^n = 0_A$ par commutativité, et d'autre part, $(xy)^n = {1_A}^n = 1_A \neq 0_A$. Ce qui est absurde.

   On suppose à présent $x \neq 1_A$. On sait que $A \ni \sum_{k=0}^{n-1} x^k = (1-x^n)/(1-x) = 1/(1-x)$. On a donc trouvé l'inverse de $1-x$.
2. Soit x un élément nilpotent de A, et y un élément de A. Soit $n \in \mathbb{N}$ tel que $x^n = 0_A$. $x \cdot y$ est aussi un élément nilpotent de A. En effet, $(xy)^n = x^n \cdot y^n = 0_A \cdot y^n = 0_A$. On nomme $\mathcal{I}$ l'ensemble des éléments nilpotents de A. Montrons que $(\mathcal{I}, +)$ est un sous-groupe additif de $(A, +)$. On a bien $0 \in \mathcal{I}$ car $0^k = 0$. Soient x et y deux éléments nilpotents. Montrons que $x - y \in \mathcal{I}$. Soient n_1 et $n_2 \in \mathbb{N}^\star$ tels que $x^{n_1} = 0$ et $y^{n_2} = 0$. On veut montrer qu'il existe $n \in \mathbb{N}^\star$ tel que $(x-y)^n = 0$. Soit $n = n_1 + n_2$. On a

$$(x-y)^n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} x^k y^{n-k} = \underbrace{\sum_{k=0}^{n_1} (-1)^{n-k} \binom{n}{k} x^y y^{n-k}}_{(1)} + \underbrace{\sum_{k=n_1+1}^{n_1+n_2} (-1)^{n-k} \binom{n}{k} x^y y^{n-k}}_{(2)}.$$

Or, dans la somme (1), $n-k = n_1+n_2-k = n_2+(n_1-k) \geqslant n_2$ et, dans la somme (2), $k \geqslant n_1$.

Cadeau 2 :
Soit F l'ensemble des matrices de la forme $\left(\begin{smallmatrix} x & y \\ -5y & x+4y \end{smallmatrix}\right)$ où $(x,y) \in \mathbb{R}^2$. On note $J = \left(\begin{smallmatrix} -2 & 1 \\ -5 & 2 \end{smallmatrix}\right)$.

1. *Montrer que F est un sous-espace vectoriel de $\mathscr{M}_{2,2}(\mathbb{R})$ et que (I_2, J) est une base de F.*
2. *Calculer J^2 puis $(x\,I_2 + yJ)\cdot(x'\,I + y'\,J)$ pour tout $(x,y,x',y') \in \mathbb{R}^4$. Qu'en déduire ?*

Réponse du cadeau 2 :

1. On cherche à trouver $\alpha, \beta \in \mathbb{R}^2$ tels que $\left(\begin{smallmatrix} x & y \\ -5 & x+4y \end{smallmatrix}\right) = \alpha I_2 + \beta J$. On a
$$\begin{aligned} \alpha I_2 + \beta J &\iff \begin{pmatrix} x & y \\ -5y & x+4y \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} -2\beta & \beta \\ -5\beta & 2\beta \end{pmatrix} \\ &\iff \begin{cases} x = \alpha - 2\beta \\ y = \beta \\ -5\beta = -5y \\ 2\beta + \alpha = x + y \end{cases} \\ &\iff \begin{cases} \beta = y \\ \alpha = x + 2y \end{cases} \end{aligned}$$
2. On a $J^2 = -I_2$ et, en calculant minutieusement, on trouve, pour tout $(x,y,x',y') \in \mathbb{R}^4$, $(x\,I_2 + y\,J)\cdot(x'\,I_2 + y'\,J) = \cdots = (xx' - yy')\,I_2 + (x'y + xy')\,J$. On remarque que $(F,+,\cdot)$ est isomorphe à $(\mathbb{C},+,\times)$. C'est un isomorphisme d'anneaux. Or, comme l'anneau $(\mathbb{C},+,\times)$ est un corps donc F l'est aussi.

Cadeau du 19/09/22

Cadeau :
Soit $(\vec{\imath},\vec{\jmath},\vec{k})$ *une base orthonormée de* $\mathbb{R}^3$. *On pose* $f : \mathbb{R}^3 \to \mathbb{R}^3$ *un endomorphisme défini tel que*

$$A = \begin{array}{c} \left[\begin{array}{ccc} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right] \begin{array}{l}\vec{\imath}\\ \vec{\jmath}\\ \vec{k}\end{array} = \big[f\big]_{(\vec{\imath},\vec{\jmath},\vec{k})}. \\ f(\vec{\imath}) \quad f(\vec{\jmath}) \quad f(\vec{k}) \end{array}$$

Interpréter géométriquement f.

Réponse du cadeau :
Soit $\mathcal{B}$ une base et $A = [f]_{\mathcal{B}}$, alors $f(\vec{\imath}) = \vec{\jmath}$, $f(\vec{\jmath}) = \vec{k}$, et $f(\vec{k}) = \vec{\imath}$. f est la rotation d'angle $2\pi/3$ autour de $\mathrm{Vect}(\vec{\imath}+\vec{\jmath}+\vec{k})$.

On peut également le montrer en décomposant $f = g \circ h$, où g est la symétrie par rapport à $\mathrm{Vect}(\vec{\imath}+\vec{\jmath},\vec{k})$ et parallèlement à $\mathrm{Vect}(\vec{\imath},\vec{\jmath})$; et h la symétrie par rapport à $\mathrm{Vect}(\vec{\imath}+\vec{k},\vec{\jmath})$ parallèlement à $\mathrm{Vect}(\vec{\imath},\vec{k})$.

Cadeaux du 22/09/22

Cadeau 1 :
Soit $(u_n)_{n\in\mathbb{N}}$ une suite positive, telle que la suite $S_n = \sum_{k=0}^{n} u_k$ diverge. En calculant $\ln \frac{S_n}{S_{n-1}}$, montrer que la série $\sum \frac{u_n}{S_n}$ diverge.

Cadeau 2 :
On pose

$$D(x) = \begin{vmatrix} 7-x & 14-x & 3-x \\ 8-x & 2-x & -x \\ 13-x & -1-x & 2-x \end{vmatrix}.$$

Montrer qu'il existe deux réels α et β tels que, pour tout $x \in \mathbb{R}$, $D(x) = \alpha x + \beta$. Déterminer α et β.

Cadeau du 23/09/22

Cadeau :
Montrer qu'il n'existe pas $P \in \mathrm{GL}_2(\mathbb{R})$ *telle que,* $A' = P^{-1}AP$ *où*

$$A = \begin{bmatrix} 0 & 7 \\ 0 & 0 \end{bmatrix} \qquad \textit{et} \qquad A' = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}.$$

Réponse du cadeau :

Analyse On suppose $P^{-1}AP = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$. Alors, $\det A = \det A'$, d'où $0 = \lambda \cdot \mu$. Et, $\operatorname{tr} A = \operatorname{tr} A'$, d'où $\lambda + \mu = 0$. On en déduit donc que $\lambda = 0 = \mu$.

Synthèse On a

$$P^{-1}AP = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

D'où, en multipliant à gauche par P et à droite par P^{-1}, on a

$$A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

On en conclut que la matrice A n'est pas diagonalisable.

Cadeaux du 28/09/22

Cadeau 1 :
On considère la matrice

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ f(\vec{\imath}) & f(\vec{\jmath}) & f(\vec{k}) \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \\ \vec{k} \end{matrix} = \Big[\, f \,\Big]_{(\vec{\imath},\vec{\jmath},\vec{k})}.$$

Trouver et interpréter un vecteur propre et une valeur propre de M (et, de même, de f).

Indication :
On a $M\begin{pmatrix}1\\1\\1\end{pmatrix} = 1 \times \begin{pmatrix}1\\1\\1\end{pmatrix}$. Le vecteur $\vec{\imath}+\vec{\jmath}+\vec{k}$ est un vecteur directeur de l'axe de rotation. Montrer que les seuls vecteurs propres sont colinéaire au vecteur $\begin{pmatrix}1\\1\\1\end{pmatrix}$.

Cadeaux du 06/10/22

Cadeau :
On considère la matrice

$$A = \begin{pmatrix} 0 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & 1 & 2 \end{pmatrix}.$$

1. *Quel est le spectre de la matrice A ?*
2. *Déterminer une base de chaque sous-espace propre de la matrice A.*
3. *Montrer que la matrice A est trigonalisable mais pas diagonalisable.*
4. *Soit T la matrice ci-dessous. Déterminer une matrice P telle que $P^{-1} \cdot A \cdot P = T$:*

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

5. *Résoudre sur $\mathbb{R}$ le système d'équation différentielle (Σ) ci-dessous :*

$$(\Sigma) : \begin{cases} x'(t) = y(t) + z(t) \\ y'(t) = -x(t) + y(t) + z(t) \\ z'(t) = -x(t) + y(t) + 2z(t) \end{cases}$$

Réponse au cadeau 1 :

1. On calcule

$$\begin{aligned} \chi_A(x) = \det(xI_3 - A) &= \begin{vmatrix} x & -1 & -1 \\ 1 & x-1 & -1 \\ 1 & -1 & x-2 \end{vmatrix} \\ &= x \begin{vmatrix} x-1 & -1 \\ -1 & x-2 \end{vmatrix} - \begin{vmatrix} -1 & -1 \\ -1 & x-2 \end{vmatrix} + \begin{vmatrix} -1 & -1 \\ x-1 & -1 \end{vmatrix} \\ &= x\big((x-1)(x-2)-1\big) - (2-x) - 1 + (-1+x-1) \\ &= x(x^2 - 3x + 1) - 2 + 2x \\ &= x^3 - 3x^2 + 3x - 1 \\ &= (x-1)^3 \end{aligned}$$

On en déduit que

$$\boxed{\mathrm{Sp}(A) = \{1\}.}$$

2. On cherche une base de SEP(1) : on cherche $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{M}_{3,1}(\mathbb{R})$, tel que $AX = X$.

$$\begin{pmatrix} 0 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \iff \begin{cases} y + z = x \\ -x + y + z = y \\ -x + y + 2z = z \end{cases}$$
$$\iff \begin{cases} y = 0 \\ x = z \end{cases}$$
$$\iff X = x \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$
$$\iff X \in \text{Vect} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

   Ainsi, la base $\mathscr{B} = \left(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right)$.

3. La matrice A n'est pas diagonalisable : en effet, on a $\dim \mathbb{R}^3 = 3 \neq \dim(\text{SEP}(1)) = 1$. Mais, le polynôme χ_A est scindé donc la matrice A est trigonalisable.

4. On cherche $P \in \text{GL}_n(\mathbb{R})$ tel que

$$P^{-1} \cdot A \cdot P = T = \begin{array}{c} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \end{matrix} \\ \begin{matrix} f(\varepsilon_1) & f(\varepsilon_2) & f(\varepsilon_3) \end{matrix} \end{array}$$

   On cherche donc $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ une base de $\mathbb{R}^3$ tel que

$$\begin{cases} f(\varepsilon_1) = \varepsilon_1 & (1) \\ f(\varepsilon_2) = \varepsilon_1 + \varepsilon_2 & (2) \\ f(\varepsilon_3) = \varepsilon_2 + \varepsilon_3 & (3). \end{cases}$$

   On choisit $\varepsilon_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, d'après la question 2. Puis, on calcule

$$\underbrace{\begin{pmatrix} 0 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & 1 & 2 \end{pmatrix}}_{A} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} x \\ y \\ z \end{pmatrix} \iff \begin{cases} -x + y + z = 1 \\ -x + z = 0 \\ -x + y + z = 1 \end{cases}$$
$$\iff \begin{cases} -x + y + z = 1 \\ -x + z = 0 \end{cases}$$
$$\iff \begin{cases} x = z \\ y = 1 \end{cases}$$
$$\iff \varepsilon_2 = \begin{pmatrix} x \\ 1 \\ x \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} + x \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

On choisit donc $\varepsilon_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ (en choisissant $x = 0$). De même, on choisit $\varepsilon_3 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$. Donc, si

$$P = \begin{array}{c} \\ \\ \\ \varepsilon_1 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{array} \\ \begin{array}{ccc} \varepsilon_1 & \varepsilon_2 & \varepsilon_3 \end{array} \end{array} \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \end{array}$$

alors $P^{-1} \cdot A \cdot P$, et on a bien $\det P = 1$.

5.

$$\begin{aligned}
(\Sigma) &\iff X'(t) = A \cdot X(t) \text{ où } X(t) \begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix} \\
&\iff U'(t) = T \cdot U(t) \text{ où } U(t) = \begin{pmatrix} u(t) \\ v(t) \\ w(t) \end{pmatrix} = P^{-1} \cdot X(t) \\
&\iff \begin{cases} u'(t) = u(t) + v(t) & (1) \\ v'(t) = v(t) + w(t) & (2) \\ w'(t) = w(t) & (3) \end{cases}
\end{aligned}$$

D'où

$$(3) \iff \exists K \in \mathbb{R},\ \forall t \in \mathbb{R},\ w(t) = K\mathrm{e}^t,$$

et

$$(2) \iff v'(t) - v(t) = K\mathrm{e}^t.$$

On résout l'équation homogène associé :

$$v'(t) = v(t) \iff \exists L \in \mathbb{R},\ \forall t \in \mathbb{R},\ v(t) = L\mathrm{e}^t.$$

On pose $v(t) = \ell(t)\,\mathrm{e}^t$, et donc

$$\begin{aligned}
(2) &\iff \ell'(t)\,\mathrm{e}^t + \ell(t)\,\mathrm{e}^t - \ell(t)\,\mathrm{e}^t = K\mathrm{e}^t \\
&\iff \ell'(t) = K \\
&\iff \ell(t) = K\,t + L \\
&\iff v(t) = (Kt + L)\,\mathrm{e}^t
\end{aligned}$$

Et donc

$$\begin{aligned}
(1) &\iff u'(t) = u(t) + v(t) = u(t) + (Kt + L)\,\mathrm{e}^t \\
&\iff u(t) - u(t) = (Kt + L)\,\mathrm{e}^t
\end{aligned}$$

On résout l'équation homogène associée :

$$u'(t) - u(t) = 0 \iff \exists M \in \mathbb{R},\ \forall t \in \mathbb{R}\, u(t) = M\mathrm{e}^t.$$

On pose $u(t) = m(t)\,\mathrm{e}^t$.

$$\begin{aligned}(2) &\iff m'(t)\,\mathrm{e}^t - m(t) = (Kt+L)\,\mathrm{e}^t\\ &\iff m'(t) = Kt + L\\ &\iff m(t) = \frac{1}{2}Kt^2 + Lt + M\\ &\iff u(t) = \left(\frac{1}{2}Kt^2 + Lt + M\right)\,\mathrm{e}^t\end{aligned}$$

Ainsi,

$$(\Sigma) \iff \exists (K,L,M)\in\mathbb{R}^3,\ \forall t\in\mathbb{R},\ \begin{cases} u(t) = \left(\frac{1}{2}Kt^2 + Lt + M\right)\,\mathrm{e}^t\\ v(t) = (Kt+L)\,\mathrm{e}^t\\ w(t) = K\,\mathrm{e}^t.\end{cases}$$

Or, $X(t) = P\cdot U(t)$, et donc

$$\begin{aligned}(2) &\iff \exists (K,L,M)\in\mathbb{R}^3,\ \forall t\in\mathbb{R},\ \begin{cases} x(t) = u(t)\\ y(t) = v(t) - w(t)\\ z(t) = u(t) + w(t)\end{cases}\\ &\iff \exists (K,L,M)\in\mathbb{R}^3,\ \forall t\in\mathbb{R},\ \begin{cases} x(t) = \left(\frac{1}{2}Kt^2 + LT + M\right)\mathrm{e}^t\\ y(t) = (Kt+L-K)\,\mathrm{e}^t\\ z(t) = \left(\frac{1}{2}Kt^2 + Lt + M + K\right)\mathrm{e}^t\end{cases}\end{aligned}$$

Cadeau 2 (matrices stochastiques) :
Soit une matrice carrée $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{R})$ telle que

$$\forall i,j\in[\![1,n]\!],\ a_{i,j}\geqslant 0 \qquad \text{et} \qquad \forall i\in[\![1,n]\!],\ \sum_{j=1}^{n} a_{i,j} = 1.$$

1. *Montrer que $1\in\mathrm{Sp}(A)$.*
2. *Montrer que, si λ est une valeur propre de A, alors $|\lambda|\leqslant 1$.*

Cadeau 3 (matrices à diagonale strictement dominante) :
Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{R})$ telle que

$$\forall i\in[\![1,n]\!],\ |a_{i,j}| > \sum_{j\neq i} |a_{i,j}|.$$

Montrer que A est inversible.

Cadeau du 12/10/22

Cadeau :
Soit $A \in \mathscr{M}_2(\mathbb{R})$ tell que $A^2 = -I_2$. Montrer qu'il existe P une matrice inversible telle que

$$P^{-1} \cdot A \cdot P = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = M.$$

Réponse au cadeau

On remarque que $A \sim \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. D'où, il existe $\varepsilon \in \mathscr{M}_{2,1}(\mathbb{C})$, tel que $A \cdot \varepsilon = i\varepsilon$. Également, $A \cdot \bar{\varepsilon} = -i\bar{\varepsilon}$. Soient $U = \varepsilon + \bar{\varepsilon} \in \mathscr{M}_{2,1}(\mathbb{R})$, et $V = i(\varepsilon + \bar{\varepsilon}) \in \mathscr{M}_{2,1}(\mathbb{R})$, puis on calcule

$$\begin{aligned} A \cdot U &= A \cdot \varepsilon + A \cdot \bar{\varepsilon} \\ &= i\varepsilon - i\bar{\varepsilon} \\ &= i(\varepsilon - \bar{\varepsilon}) \\ &= V. \end{aligned}$$

Cadeau du 19/10/22

Cadeau :

Soit f une fonction continue sur $[0,+\infty[$, telle que $\displaystyle\int_0^{+\infty} f(t)\,\mathrm{d}t$ converge.

1. *Montrer que ça n'implique pas que $f(x) \xrightarrow[x\to+\infty]{} 0$.*
2. *Montrer que, si $f(x) \xrightarrow[x\to+\infty]{} \ell \in \mathbb{R}$, alors $\ell = 0$.*
3. *Montrer que, si f est uniformément continue, alors $f(x) \xrightarrow[x\to+\infty]{} 0$.*

Réponse du cadeau :

1. c.f. remarque 7 du cours
2. Quitte à remplacer ℓ par $-\ell$, on suppose $\ell > 0$. Ainsi, il existe $X \geqslant 0$ tel que
$$\forall x \geqslant X,\ f(x) \geqslant \frac{\ell}{2}.$$
Or, l'intégrale
$$\int_X^{+\infty} \frac{\ell}{2}\,\mathrm{d}x$$
diverge. D'où
$$\int_X^{+\infty} f(x)\,\mathrm{d}x$$
diverge également. Ce qui est absurde. On en déduit que $\ell = 0$.
3. On suppose f uniformément continue. Par l'absurde, supposons que $f(x) \xrightarrow[x\to+\infty]{\not}\ 0$, d'où
$$\exists \varepsilon > 0,\ \exists (u_n)_{n\in\mathbb{N}} \text{ tendant vers } +\infty,\ \forall n \in \mathbb{N},\ f(u_n) \geqslant \varepsilon.$$
Or, comme f est uniformément continue, il existe $\delta > 0$ tel que
$$\forall n \in \mathbb{N},\ \forall x \in \mathbb{R}^+,\quad |x - u_n| \leqslant \delta \implies |f(x) - f(y)| \leqslant \frac{\varepsilon}{2}.$$
D'où,
$$\int_0^{+\infty} f(x)\,\mathrm{d}x \geqslant \int_0^{+\infty} \frac{\varepsilon}{2}\,\mathrm{d}t$$
qui diverge. Ce qui est absurde.

Cadeau du 21/10/22

Théorème d'interpolation de Lagrange

Cadeau :
Soient $(a_0, a_1, \dots, a_n)$ une suite de $n+1$ réels distincts deux à deux. Soient aussi $(b_0, b_1, \dots, b_n)$ une suite de $n+1$ réels (qui peuvent être égales). Alors,

$$\exists! P \in \mathbb{R}_n[X],\ \forall k \in [\![0, n]\!],\ P(a_k) = b_k.$$

Réponse du cadeau :

MÉTHODE 1 Soient $n+1$ réels a_0, a_1, …, a_n distincts deux à deux. L'application

$$\begin{aligned} f : \mathbb{R}_n[X] &\longrightarrow \mathbb{R}^{n+1} \\ P &\longmapsto \Big(P(a_0), P(a_1), \dots, P(a_n)\Big) \end{aligned}$$

est linéaire et la dimension de l'espace vectoriel de départ est égale à la dimension de l'espace vectoriel d'arrivée. Soit P un polynôme réel de degré au plus n.

$$\begin{aligned} P \in \operatorname{Ker} f &\iff f(P) = (0, 0, \dots, 0) \\ &\implies P(a_1) = P(a_2) = \dots = P(a_n) = 0 \\ &\implies P \text{ a au moins } n+1 \text{ racines} \\ &\implies P = 0_{\mathbb{R}_n[X]} \text{ car } \#\text{racines} > \deg(P) \end{aligned}$$

D'où $\operatorname{Ker} f = \{0_{\mathbb{R}_n[X]}\}$. On en déduit que f est injective. Et, d'après le théorème du rang, f est surjective (car $\dim \mathbb{R}_n[X] = \dim \mathbb{R}^{n+1}$).

MÉTHODE 2 On reprend la fonction f de la MÉTHODE 1. Soit $\mathscr{B}$ la base canonique de $\mathbb{R}_n[X]$: $\mathscr{B} = (1, X, \dots, X^n)$; et, soit $\mathscr{C}$ la base canonique de $\mathbb{R}^{n+1}$: $\mathscr{C} = (e_1, e_2, \dots, e_{n+1})$. On a

$$\big[f\big]_{\mathscr{B}}^{\mathscr{C}} = \operatorname{Mat}_{\mathscr{B},\mathscr{C}}(f) = \begin{pmatrix} 1 & a_0 & a_0^n & \cdots & a_0^n \\ 1 & a_1 & a_1^n & \cdots & a_1^n \\ 1 & a_2 & a_2^n & \cdots & a_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^n \\ f(1) & f(X) & f(X^2) & \dots & f(X^n) \end{pmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_{n+1} \end{matrix} = V.$$

On reconnaît un déterminant de VANDERMONDE :

$$\begin{aligned}\det V &= (a_n - a_{n-1}) \cdots (a_n - a_1)(a_n - a_0) \\ &\quad \times (a_{n-1} - a_{n-2}) \cdots (a_{n-1} - a_{n-2}) \cdots (a_{n-1} - a_0) \\ &\quad \times \\ &\quad \vdots \\ &\quad \times (a_2 - a_1) \cdot (a_2 - a_0) \\ &\quad \times (a_1 - a_0) \\ &\quad = \prod_{i>j} (a_i - a_j)\end{aligned}$$

D'où $\det V \neq 0$ car les (a_i) sont distincts deux à deux. Donc V est inversible, et d'où f est bijective.

MÉTHODE 3 On va prouver la surjectivité en déterminant **un** polynôme P tel que $P(a_0) = b_0$, $P(a_1) = b_1$, …, $P(a_n) = b_n$. Le voilà :

$$\begin{aligned}P = b_0 &\frac{(X - a_1)(X - a_2) \cdots (X - a_n)}{(a_0 - a_1)(a_0 - a_2) \cdots (a_0 - a_n)} \\ + b_1 &\frac{(X - a_0)(X - a_1) \cdots (X - a_n)}{(a_1 - a_0)(a_1 - a_2) \cdots (a_1 - a_n)} \\ &\vdots \\ + b_n &\frac{(X - a_0)(X - a_1) \cdots (X - a_{n-1})}{(a_n - a_0)(a_n - a_1) \cdots (a_n - a_{n-1})}.\end{aligned}$$

Ce polynôme interpole les $n + 1$ points et $\deg P \leqslant n$.

Cadeau du 08/11/22

Dénombrement

Cadeau :

1. *Calculer, de deux manières,* $\sum_{k=0}^{n}\binom{n}{k}$. *(binôme et dénombrement)*
2. *(Petite formule de* Pascal*) Calculer* $p\binom{n}{p} = n\binom{n-1}{p-1}$.
3. *(Formule de* Vandermonde*) Montrer, de deux manières, que* $\sum_{k=0}^{n}\binom{a}{p}\binom{b}{n-p} = \binom{a+b}{n}$. *(développement de* $(1+x)^{a+b}$ *et dénombrement)*
4. *Montrer, de deux manières, que* $\sum_{k=p}^{n}\binom{k}{p} = \binom{n+1}{p+1}$ *(télescope et dénombrement)*

Réponse du cadeau :

1. On développe, à l'aide du binôme de Newton, $2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}\cdot 1^k\cdot 1^{n-k} = \sum_{k=0}^{n}\binom{n}{k}$.

   Autre méthode : $\sum_{k=0}^{n}\binom{n}{k}$ est le nombre de parties d'un ensemble à n éléments. Construire une partie à n éléments, c'est : choisir ou non le premier élément (2 manières), choisir ou non le second élément (2 manière), ..., etc jusqu'au n-ième élément. Il y a donc 2^n manières.
2. Soit E un ensemble à n éléments. Soit A une partie de E à p éléments, et soit B sont complémentaire dans E. L'application

$$f : \{X \subset A \mid |X| = a+b\} \longrightarrow \bigcup_{k=0}^{n}{}^{\cdot}\,\{X \subset A \mid |X| = k\} \cup \{X \subset B \mid |X| = n-k\}$$
$$X \longmapsto (X \cap A, X \cap B)$$

   est bijective. (L'application $(X,Y) \mapsto X \cup Y$ est sa réciproque.) Ainsi,

$$|\{X \subset A \mid |X| = a+b\}| = \sum_{k=0}^{n} |\{X \subset A \mid |X| = k\}|\cdot|\{X \subset A \mid |X| = n-k\}|,$$

   d'où $\binom{a+b}{n} = \sum_{k=0}^{n}\binom{a}{k}\binom{b}{n-k}$.

   Moins rigoureusement, choisir n éléments de E, c'est choisir 0 éléments de A et n éléments de B (il y en a $\binom{a}{0}\binom{b}{n}$), ou 1 élément de A et $n-1$ éléments de B (il y en a $\binom{a}{1}\binom{b}{n-1}$), ou... On en conclut qu'il y a $\sum_{p=0}^{n}\binom{a}{p}\binom{b}{n-p}$ manières de choisir n éléments dans E. Mais, c'est aussi $\binom{a+b}{n}$.

   Autre méthode : on a d'une part $(1+X)^{a+b} = \sum_{k=0}^{a+b}\binom{a+b}{k}X^k$. Et, d'autre part,

$$(1+X)^{a+b} = (1+X)^a \times (1+X)^b = \Big(\sum_{p=0}^{a}\binom{a}{p}X^p\Big)\Big(\sum_{q=0}^{b}\binom{b}{q}X^q\Big).$$

Or, deux polynômes sont égaux si et seulement si leurs coefficients sont égaux deux-à-deux. D'où

$$\binom{a+b}{n} = \sum_{p+q=n} \binom{a}{p}\binom{b}{q} = \sum_{p=0}^{n} \binom{a}{p}\binom{b}{n-p}.$$

3. On a

$$\sum_{k=p}^{n} \binom{k}{p} = \sum_{k=p}^{n} \left(\binom{k+1}{p+1} - \binom{k}{p+1} \right) = \binom{n+1}{p+1} - \binom{p}{p+1} = \binom{n+1}{p+1}.$$

Autre méthode : dénombrement. Je choisis $p+1$ éléments parmi $n+1$. On pose $k+1$ le plus grand éléments de ces éléments choisis : $p+1 \leqslant k+1 \leqslant n+1$, d'où $p \leqslant k \leqslant n$. Ainsi, on doit donc choisir encore p autres éléments dans $[\![1, k]\!]$ (car ces éléments sont plus petits que n).

Cadeau du 01/12/22

Cadeau :
Soit $A \in \mathscr{M}_n(\mathbb{R})$. *Montrer que* $\operatorname{Ker}(A^\top \cdot A) = \operatorname{Ker} A$.

Réponse du cadeau :
On procède par double-inclusion.

"$\supset$" Soit $X \in \operatorname{Ker} A$. Alors, $A \cdot X = 0$. Ainsi, $A^\top \cdot A \cdot X = A^\top \cdot 0 = 0$. On a bien $\operatorname{Ker}(A^\top \cdot A) \supset A$.

"$\subset$" Soit $X \in \operatorname{Ker}(A^\top \cdot A)$. Alors $A^\top \cdot A \cdot X = 0$, d'où $X^\top \cdot (A^\top \cdot A \cdot X) = 0$. Ainsi, $(X^\top \cdot A^\top) \cdot (A \cdot X) = 0$, donc $(A \cdot X)^\top \cdot (A \cdot X) = 0$. Mais, avec le produit scalaire canonique sur $\mathscr{M}_{n,1}(\mathbb{R})$, on a donc $\|A \cdot X\|^2 = 0$. Par le caractère défini du produit scalaire, on a bien $A \cdot X = 0$ et donc $X \in \operatorname{Ker} A$. D'où $\operatorname{Ker}(A^\top \cdot A) \subset \operatorname{Ker} A$.

Cadeau du 02/12/22

Lemme de Borel-Cantelli

Cadeau :
Soit $(\Omega, \mathscr{A}, P)$ un espace probabilisé, et soit $(E_n)_{n\in\mathbb{N}}$ une suite d'événements. On pose $F = \bigcap_{n\in\mathbb{N}} \big(\bigcup_{k\geqslant n} E_k\big)$.

1. *On suppose que la série $\sum P(E_n)$ converge. En encadrement judicieusement $P(F)$, montrer que $P(F) = 0$.*
2. *On suppose à présent que les événements E_n sont indépendants et que la série $\sum P(E_n)$ diverge.*
   (a) *Soit $n \in \mathbb{N}$. Montrer que, pour tout $N \geqslant n$, $\ln P\big(\bigcap_{p=n}^{N} \bar{E}_p\big) \leqslant -\sum_{p=n}^{N} P(E_p)$.*
   (b) *En déduire $\lim_{N\to\infty} P\big(\bigcap_{p=n}^{N} \bar{E}_p\big)$.*
   (c) *Montrer que, pour tout $n \in \mathbb{N}$, $P\big(\bigcap_{p\geqslant n} \bar{E}_p\big) = 0$.*
   (d) *Conclure que $P(F) = 1$.*

Réponse du cadeau :

1. On pose, pour $k \in \mathbb{N}$, l'événement $A_n = \bigcup_{k\geqslant n} E_k$. On a $A_n = A_{n+1} \cup E_n \supset A_{n+1}$, la suite d'événements $(A_n)_{n\in\mathbb{N}}$ est décroissante (pour l'inclusion). Ainsi, par continuité décroissante,
$$P\Big(\bigcap_{n\in\mathbb{N}} A_n\Big) = \lim_{n\to\infty} P(A_n).$$
Or, comme la série $\sum P(E_n)$ converge, on a, pour tout $n \in \mathbb{N}$, par σ-sous-additivité,
$$0 \leqslant P(A_n) = P\Big(\bigcup_{k\geqslant n} E_k\Big) \leqslant \sum_{k\geqslant n} P(E_k),$$
et il s'agit du reste de la série convergente $\sum P(E_n)$, qui tends vers 0. D'où, par le théorème des gendarmes, $P(A_n)$ tend vers 0 quand $n \to \infty$. On en déduit que
$$\boxed{P(F) = 0.}$$
2. (a) Comme les événements E_p sont indépendants, les événements $\bar{E}_p$ le

sont aussi. Ainsi, $P\big(\bigcap_{p=n}^{N} \bar{E}_p\big) = \prod_{p=n}^{N} P(\bar{E}_p)$, et donc

$$\begin{aligned}
\ln P\Big(\bigcap_{p=n}^{N} \bar{E}_p\Big) &= \sum_{p=n}^{N} \ln P(\bar{E}_p) \\
&= \sum_{p=n}^{N} \ln\big(1 - P(E_p)\big) \\
&\leqslant \sum_{p=n}^{N} \big(-P(E_p)\big) \text{ car } \ln(1+x) \leqslant x \\
&\leqslant -\sum_{p=n}^{N} P(E_p).
\end{aligned}$$

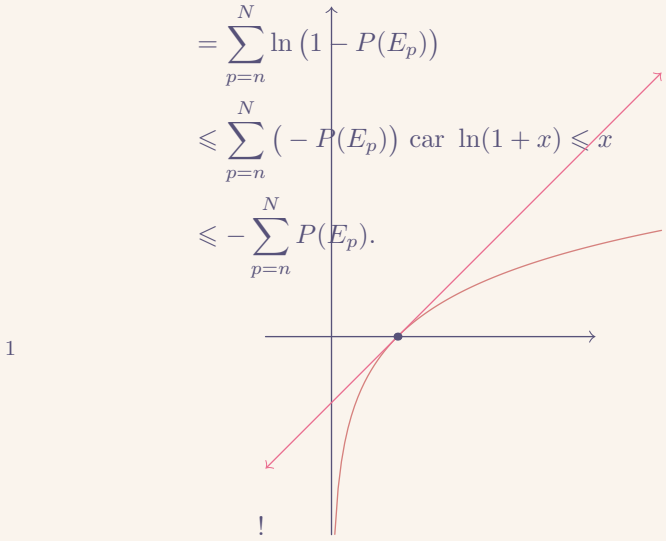


FIGURE 4.1 – Concavité de la fonction ln

(b) Comme, pour tout $p \in \mathbb{N}$, $P(E_p) \geqslant 0$, donc la suite $(S_N)_{N\in\mathbb{N}} = \big(\sum_{p=n}^{N} P(E_p)\big)_{N\in\mathbb{N}}$ est croissante, elle admet donc une limite. De plus, par hypothèse, la série $\sum P(E_p)$ diverge donc $\lim_{N\to\infty} -S_n = -\infty$. Par composition des limites, $\lim_{N\to\infty} \ln P\big(\bigcap_{p=n}^{N} \bar{E}_p\big) = -\infty$. Enfin, comme l'exponentielle est croissante,

$$0 \leqslant P\Big(\bigcap_{p=n}^{N} \bar{E}_p\Big) \leqslant \exp\Big(-\sum_{p=n}^{N} P(E_p)\Big).$$

Comme $\lim_{x\to-\infty} \mathrm{e}^x = 0$, on en déduit par le théorème des gendarmes, que

$$\lim_{N\to\infty} P\Big(\bigcap_{p=n}^{N} \bar{E}_p\Big) = 0.$$

(c) Par continuité décroissante, on a donc

$$P\Big(\bigcap_{n\geqslant p} \bar{E}_p\Big) = \lim_{N\to\infty} P\Big(\bigcap_{p=n}^{N} \bar{E}_p\Big) = 0.$$

(d) On rappelle que $F = \bigcap_{n\in\mathbb{N}} \bigcup_{p\geqslant n} E_p$. Or, on sait que $\bigcap_{p\geqslant n} \bar{E}_p = \overline{\bigcup_{p\geqslant n} E_p}$. On a doc $P\big(\bigcup_{p\geqslant N}\big) = 1 - P\big(\bigcap_{p\geqslant n} \bar{E}_p\big) = 1$. Do,c les événements $\bigcup_{p\geqslant n} E_p$ sont presque certains. Or, l'intersection d'événements presque certains est presque certaine. D'où $P(F) = 1$.

Cadeau du 05/12/22

Oral CCP PSI 2018

Cadeau :
Soit $(A_k)_{k\in[\![1,n]\!]}$ une famille d'événements d'un espace probabilisé $(\Omega, \mathcal{A}, P)$. Montrer que

$$\sum_{k=1}^{n} P(A_k) \leqslant P\Big(\bigcap_{k=1}^{n} A_k\Big) + n - 1.$$

Réponse du cadeau :
On a

$$\begin{aligned} n - \sum_{k=1}^{n} P(\bar{A}_k) &= \sum_{k=1}^{n} \big(1 - P(A_k)\big) \\ &= \sum_{k=1}^{n} P(\bar{A}_k) \\ &\geqslant P\Big(\bigcup_{k=1}^{n} \bar{A}_k\Big) \\ &= 1 - P\Big(\bigcap_{k=1}^{n} A_k\Big) \end{aligned}$$

D'où,

$$\sum_{k=1}^{n} P(\bar{A}_k) \leqslant P\Big(\bigcap_{k=1}^{n} A_k\Big) + n - 1.$$

Cadeau du 08/12/22

Cadeau :
La forme

$$\begin{aligned}\varphi : \mathbb{R}[X] \times \mathbb{R}[X] &\longrightarrow \mathbb{R} \\ (P, Q) &\longmapsto \int_0^\pi P(\cos t)Q(\cos t)\ \mathrm{d}t\end{aligned}$$

est un produit scalaire ?

Cadeau du 13/12/22

Cadeau :

1. *Soit $n \in \mathbb{N}$. En remarquant que $(1+X)^n \cdot (1+X)^n = (1+X)^{2n}$, montrer que*
$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$
2. *Montrer que*
$$\Big(\sum_{n=0}^{\infty} \frac{1}{(n!)^2}\Big)^2 = \sum_{n=0}^{\infty} \frac{1}{(2n)!} \binom{2n}{n}^2.$$

Réponse du cadeau :

1. Soit $n \in \mathbb{N}$. On sait que
$$\begin{aligned}(1+X)^n \cdot (1+X)^n &= \Big(\sum_{k=0}^{n} \binom{n}{k} X^k\Big)\Big(\sum_{k=0}^{n} \binom{n}{k} X^k\Big) \\ &= \sum_{k=0}^{2n} \sum_{p+q=k} \binom{n}{p}\binom{n}{q} X^k\end{aligned}$$

   D'autre part, on sait que
$$(1+X)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} X^k.$$

   Or, deux polynômes sont égaux si, et seulement s'ils ont les mêmes coefficients. On regarde le coefficient X^n en posant $k = n$:
$$\binom{2n}{n} = \sum_{p+q=n} \binom{n}{p}\binom{n}{q} = \sum_{p=0}^{n} \binom{n}{p}\binom{n}{n-p} = \sum_{k=0}^{n} \binom{n}{k}^2.$$
2. La série $\sum \frac{1}{(n!)}$ converge absolument car $\frac{1}{(n!)^2} = \wr\left(\frac{1}{n^2}\right)$. Ainsi, par produit

de Cauchy,

$$\begin{aligned}
\Big(\sum_{n=0}^{\infty}\frac{1}{(n!)^2}\Big)\Big(\sum_{n=0}^{\infty}\frac{1}{(n!)^2}\Big) &= \sum_{n=0}^{\infty}\sum_{p+q=n}\frac{1}{(p!)^2}\frac{1}{(q!)^2}\\
&= \sum_{n=0}^{\infty}\sum_{p=0}^{n}\frac{1}{(p!)^2}\frac{1}{(n-p)!^2}\\
&= \sum_{n=0}^{\infty}\sum_{p=0}^{n}\binom{n}{p}^2\frac{1}{(n!)^2}\\
&= \sum_{n=0}^{\infty}\frac{1}{(n!)^2}\times\Big(\sum_{p=0}^{n}\binom{n}{p}^2\Big)\\
&= \sum_{n=0}^{\infty}\frac{1}{(n!)^2}\times\binom{2n}{n}\\
&= \sum_{n=0}^{\infty}\frac{1}{(n!)^2}\times\frac{(2n)!}{n!\times n!}\\
&= \sum_{n=0}^{\infty}\frac{1}{(2n!)}\binom{2n}{n}^2.
\end{aligned}$$

Cadeaux du 14/12/22

CCP PSI 2010, Centrale PSI 2014 & TPE PSI 2014

Cadeau 1 :
Soient $n \geqslant 2$ et

$$\begin{aligned}\Phi : \mathscr{M}_n(\mathbb{R}) &\longrightarrow \mathscr{M}_n(\mathbb{R}) \\ M &\longmapsto M^\top.\end{aligned}$$

Déterminer les éléments propres, la trace et le déterminant de Φ.

Correction du cadeau 1 :
On a $\Phi^2 = \mathrm{id}$ donc $X^2 - 1$ annule Φ. D'où, $\mathrm{Sp}(\Phi) \subset \{-1, 1\}$. Et, $\forall M \in \mathcal{S}_n(\mathbb{R})$, $\Phi(M) = M^\top = M = 1 \times M$. De plus, $\forall M \in \mathcal{A}_n(\mathbb{R})$, $\Phi(M) = M^\top = -M = -1 \times M$. D'où $\mathcal{S}_n(\mathbb{R}) \subset \mathrm{SEP}(1)$ et $\mathcal{A}_n(\mathbb{R}) \subset \mathrm{SEP}(-1)$. Mais, $\dim \mathcal{S}_n(\mathbb{R}) = n(n+1)/2$ et $\dim \mathcal{A}_n(\mathbb{R}) = n(n-1)/2$. Donc $\mathrm{SEP}(1) = \mathcal{S}_n(\mathbb{R})$ et $\mathrm{SEP}(-1) = \mathcal{A}_n(\mathbb{R})$. L'endomorphisme Φ possède un polynôme annulateur scindé à racines simples, il est donc diagonalisable. En se plaçant dans une base $\mathscr{B}$ adaptée : la concaténation d'une base de $\mathcal{S}_n$ et d'une base de $\mathcal{A}_n$, on a

$$\big[\Phi\big]_{\mathscr{B}} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \frac{n(n+1)}{2} \\ \\ \cdot \\ \\ \frac{n(n-1)}{2} \\ \end{matrix}$$

On a donc $\mathrm{tr}\,\Phi = \frac{n(n+1)}{2} - \frac{n(n-1)}{2} = \frac{2}{2}n = n$, et $\det \Phi = (-1)^{\frac{n(n-1)}{2}}$.

Cadeau 2 :
Soit $V = \big\{u \in \mathscr{L}\big(\mathscr{M}_n(\mathbb{R})\big) \mid \forall M \in \mathscr{M}_n(\mathbb{R}),\ u(M^\top) = \big[u(M)\big]^\top\big\}$. Montrer que V est un sous-espace vectoriel de $\mathscr{L}\big(\mathscr{M}_n(\mathbb{R})\big)$ et déterminer sa dimension.

Correction du cadeau 2 :
On a bien $\tilde{0} \in V$ donc $V \neq$. Soient $u, v \in V$ et $\lambda, \mu \in \mathbb{R}$. Pour toute matrice $M \in \mathscr{M}_n(\mathbb{R})$,

$$\begin{aligned}(\lambda u + \mu v)(M^\top) &= \lambda u(M^\top) + \mu v(M^\top) \\ &= \lambda\big(u(M)\big)^\top + \mu\big(v(M)\big)^\top \\ &= (\lambda u + \mu v)(M)^\top\end{aligned}$$

donc $\lambda u + \mu v \in V$. Ainsi, V est un sous-espace vectoriel de $\mathscr{L}\big(\mathscr{M}_n(\mathbb{R})\big)$.

— Soit $u \in V$. Pour toute matrice antisymétrique $A \in \mathcal{A}_n$, $u(A^\top) = u(A^\top) = -u(A)$, d'où $u(A) \in \mathcal{A}_n$. De même, pour toute matrice symétrique $S \in \mathcal{S}_n$, $u(S^\top) = u(S) = u(S)^\top$ donc $u(S) \in \mathcal{S}_n$.
— Soit $u \in \mathscr{L}\big(\mathcal{M}_n(\mathbb{R})\big)$ un endomorphisme tel que $u(\mathcal{A}_n) \subset \mathcal{A}_n$ et $u(\mathcal{S}_n) \subset \mathcal{S}_n$. Soit $M \in \mathcal{M}_n(\mathbb{R})$. On décompose M en $M = A+S$ avec $A \in \mathcal{A}_n$ et $S \in \mathcal{S}_n$.

$$\begin{aligned} u(M^\top) &= u(A^\top + S^\top) \\ &= u(A^\top) + u(S^\top) \\ &= -u(A) + u(S) \\ &= u(A)^\top + u(S)^\top \\ &= u(M)^\top \end{aligned}$$

donc

$$\begin{aligned} \dim V &= \dim^2 \mathcal{A}_n + \dim^2 \mathcal{S}_n \\ &= \left(\frac{n(n-1)}{2}\right)^2 + \left(\frac{n(n+1)}{2}\right)^2 \\ &= \frac{n^2}{4}(n^2 - 2n + 1 + n^2 + 2n + 1) \\ &= \frac{1}{2}n^2(n^2+1). \end{aligned}$$

En effet, soit $\mathcal{B}$ une base adaptée à la somme $\mathcal{A}_n \oplus \mathcal{S}_n = \mathcal{M}_n(\mathbb{R})$,

$$[u]_{\mathcal{B}} = \begin{pmatrix} \star & 0 \\ 0 & \star \end{pmatrix}.$$

Cadeau 3 :

(a) *Soit $d \in \mathbb{N}^\star$, $a \in \mathbb{C}$ et*

$$\begin{aligned} u : \mathbb{C}_d[X] &\longrightarrow \mathbb{C}_d[X] \\ P &\longmapsto (X-a)P'. \end{aligned}$$

Déterminer les éléments propres de u.
(b) *En déduire l'ensemble des polynômes de $\mathbb{C}[X]$ divisibles par leur dérivée.*

Réponse du cadeau 3 :

(a) On a $u(k) = 0 = 0 \times k$ avec $k \in \mathbb{C}$. De même, on remarque que,

$$\forall k \in [\![1, d]\!],\ u\big((X-a)^k\big) = k(X-a)^{k-1} \cdot (X-a) = k \times (X-a)^k.$$

Ainsi, $(X-a)^k \in \mathrm{Ker}(k\,\mathrm{id} - u)$. L'endomorphisme u possède $d+1$ valeurs propres distinctes deux à deux. Or, $\dim \mathbb{C}_d[X] = d+1$, donc u est diagonalisable. Et, $\forall k \in [\![0, d]\!]$, $\mathrm{Ker}(k\,\mathrm{id} - u) = \mathrm{Vect}\left[(X-a)^k\right]$. Donc $\mathrm{Sp}(u) = [\![0, d]\!]$.

Autre solution : la base $\mathscr{B} = \big((X-a)^0, (X-a)^1, \ldots, (X-a)^d\big)$ est adaptée. En effet, dans cette base

$$[u]_{\mathscr{B}} = \begin{pmatrix} 0 & & & & \\ & 1 & & & \\ & & 2 & & \\ & & & \ddots & \\ & & & & d \end{pmatrix}.$$

(b)
— Analyse. Soit P un polynôme de degré $d \geqslant 1$, tel que $P' \mid P$. Alors, $P = \frac{1}{d}(X-a) \times P'$. D'où, $u(P) = (X-a)P' = dP$.
— Synthèse. ok.

Cadeaux du 15/12/22

Centrale PC 2016, X ESPCI PC 2013 & X ESPCI PC 2014, 2015

Cadeau 1 :
Soit $\mathcal{D}_n$ l'espace des matrices diagonales et $D = \mathrm{diag}(d_1, \dots, d_n)$. Montrer que $(I_n, D, \dots, D^{n-1})$ est une base de $\mathcal{D}_n$ si, et seulement si les réels d_i sont distincts deux à deux.

Réponse du cadeau 1 :

$$
\begin{aligned}
&(I_n, D, \dots, D^{n-1}) \text{ est une base de } \mathcal{D}_n \\
\iff &\forall (a_0, \dots, a_{n-1}), \quad a_0 I_n + a_1 D + \cdots + a_{n-1} D^{n-1} = 0 \implies a_0 = a_1 = \cdots = a_{n-1} \\
\iff &\forall (a_0, \dots, a_{n-1}), \quad \begin{cases} a_0 + a_1 d_1 + \cdots + a_{n-1} d_1^{n-1} &= 0 \\ \vdots & \ddots \vdots \\ a_0 + a_1 d_n + \cdots + a_{n-1} d^{n-1} &= 0 \end{cases} \implies a_0 = \cdots = a_{n-1} = 0 \\
\iff &\forall (a_0, \dots, a_{n-1}), \begin{pmatrix} 1 & d_1 & \dots & d_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & d_n & \dots & d_n^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0 \implies a_0 = \cdots = a_{n-1} = 0 \\
\iff &\text{ les réels } d_i \text{ sont distincts deux à deux.}
\end{aligned}
$$

car on reconnaît le déterminant de Vandermonde.

Cadeau 2 :
Soit $X \in \mathcal{M}_{n,1}(\mathbb{R})$ non nul.

(a) Montrer que $V = \{M \in \mathcal{M}_n(\mathbb{R}) \mid M \cdot X = 0\}$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$, et déterminer la dimension.

(b) Montrer que l'ensemble W des matrices de $\mathcal{M}_n(\mathbb{R})$ dont X est un vecteur propre, est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ et que $\dim W = ?$.

Réponse du cadeau 2 :

(a) Soit $M = 0_{\mathcal{M}_n(\mathbb{R})}$ la matrice nulle. On a $M \cdot X = 0$, donc $0_{\mathcal{M}_n(\mathbb{R})} \in V$. Soient $M, N \in V$ et $\lambda, \mu \in \mathbb{R}$. On a $(\lambda M + \mu N) \cdot X = \lambda M \cdot X + \mu N \cdot X = 0$, donc $\lambda M + \mu N \in V$. On en déduit que V est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$.

On se place dans une base adaptée $\mathscr{B} = (X, X_2, \dots, X_n)$ où on a complété la famille X par des vecteurs $X_2, \dots, X_n$. Soit f l'endomorphisme représenté, dans une base, par M. Ainsi,

$$\begin{aligned} M \in V &\iff M \cdot X = 0 \\ &\iff f(x) = 0 \text{ où } X \text{ est la matrice de } x \text{ dans la même base} \\ &\iff \exists P \in \mathrm{GL}_n(\mathbb{R}),\ P^{-1} \cdot M \cdot P = \begin{pmatrix} 0 & \star & \dots & \star \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \star & \dots & \star \end{pmatrix} \end{aligned}$$

Ainsi,

$$\boxed{\dim V = n^2 - n.}$$

(b) Soit $M = 0_{\mathscr{M}_n(\mathbb{R})}$ la matrice nulle. On a $M \cdot X = 0_{\mathscr{M}_n(\mathbb{R})} = 0_{\mathbb{R}} \cdot X$, donc $0_{\mathscr{M}_n(\mathbb{R})} \in W$. Soient $M, N \in W$ et $\lambda, \mu \in \mathbb{R}$. Soit α la valeur propre associée au vecteur propre X pour la matrice M. Soit β la valeur propre associée au vecteur propre X pour la matrice N. Ainsi, $(\lambda M + \mu N) \cdot X = \lambda M \cdot X + \mu N \cdot X = \lambda\alpha X + \mu\beta X = (\lambda\alpha + \mu\beta) \cdot X$. On en déduit que $\lambda M + \mu N \in W$. Ainsi, W est un sous-espace vectoriel de $\mathscr{M}_n(\mathbb{R})$.

De même, dans la même base adaptée

$$M \in W \iff \exists P \in \mathrm{GL}_n(\mathbb{R}),\ P^{-1} \cdot A \cdot P = \begin{pmatrix} \star & \star & \dots & \dots & \star \\ 0 & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & \star & \dots & \dots & \star \end{pmatrix}$$

D'où,

$$\boxed{\dim W = n^2 - n + 1.}$$

Cadeau du 10/01/23

Cadeau :
Déterminer le rayon de convergence de la série entière $\sum x^{(n^2)}$.

Réponse du cadeau :
On pose (u_n) le terme général de la série. Son rayon de convergence vaut 1. En effet, si $x = 1$, la série $\sum 1$ diverge, d'où $R \leqslant 1$. De plus, si $|x| < 1$, alors $\forall n \in \mathbb{N}$, $|u_n| \leqslant |x|^n$. Or, la série $\sum |x|^n$ converge, donc $\sum |u_n|$ aussi, d'où $R \geqslant 1$ et donc $R = 1$.

Cadeau du 13/01/23

Cadeau :
Soient F et G deux espaces d'un espace préhilbertien[1] *Montrer que, si $F \oplus G = E$ et $F \perp G$, alors $G = F^\top$ et $F = G^\top$.*

1. il n'y a donc aucune hypothèses sur la dimension de E.

Cadeau du 18/01/23

Cadeau :
Soient $\sum a_n z^n$ une série entière, et R son rayon de convergence. On considère la série entière $\sum {a_n}^n z^n$ de rayon de convergence R'.

1. *Montrer que,*
   (a) *si $R > 1$, alors $R' = +\infty$;*
   (b) *si $R < 1$, alors $R' = 0$.*
2. *Que se passe-t-il si $R = 1$?*

Réponse du cadeau :

1. (a) Soit $x \in]-R, R[$. On a $R > 1$, d'où $\sum |a_n| 1^n$ converge, d'où $a_n \xrightarrow[n\to\infty]{} 0$. Ainsi, à partir d'un certain rang, $|a_n x| \leqslant \lambda$, où $0 < \lambda < 1$ et donc $|a_n x|^n \leqslant \lambda^n$. Or, la série $\sum \lambda^n$ converge, d'où $\sum a_n x^n$ converge. On en déduit $R' = +\infty$.
   (b)
2. On considère la série géométrique $\sum x^n$: on pose $a_n = 1$ pour tout $n \in \mathbb{N}$. Le rayon de convergence de cette série est $R = 1$. Mais, $\sum {a_n}^n x^n = \sum x^n$, et donc $R' = 1$.
   On considère la série $\sum \frac{x^n}{n}$. On pose, pour $n \in \mathbb{N}^\star$, $a_n = \frac{1}{n}$. Soit $x \in R$. On pose $u_n = |{a_n}^n x^n|$ pour $n \in \mathbb{N}$. Pour tout entier $n \in \mathbb{N}^\star$,

$$\begin{aligned} \frac{u_{n+1}}{u_n} &= \left|\frac{a_{n+1}}{a_n}\right|^n |a_{n+1}|\,|x| \\ &= \left(\frac{n}{n+1}\right)^n \cdot \frac{1}{n+1}|x| \xrightarrow[n\to+\infty]{} 0 \end{aligned}$$

   D'où $\sum u_n$ converge, et donc $R' = +\infty$.

Cadeau du 18/01/23

Banque PT 2006 Maths C

Cadeau :
Trouver les solutions développables en séries entières de l'équation différentielle

$$16\,(x^2-x)\,y'' + (16x-8)\,y' - y = 0.$$

Indication : Il faut montrer que

$$f : x \mapsto \sum_{n=0}^{\infty} a_n x^n \text{ est une solution } \iff \forall n,\ a_{n+1} = \frac{(4n+1)(4n-1)}{8(n+1)(2n+1)}\,a_n.$$

Trouver le rayon de convergence de la série, et calculer a_n en fonction de n.

Réponse du cadeau :
Soit R le rayon de convergence d'une série entière $\sum a_n x^n$. Soit, pour tout $x \in]-R,R[$, $f(x) = \sum_{n=0}^{\infty} a_n x^n$. On peut dériver terme à terme une série entière sans changer son rayon de convergence, d'où

$$\forall x \in]-R,R[,\quad \begin{cases} f'(x) = \displaystyle\sum_{n=1}^{\infty} n a_n x^{n-1} \\ f''(x) = \displaystyle\sum_{n=2}^{\infty} n(n-1) a_n x^{n-2} \end{cases}.$$

$$
\begin{aligned}
f \text{ est une solution} &\iff \forall x \in]-R,R[,\ 16(x^2-x)\sum_{n=2}^{\infty} n(n-1)a_n x^{n-2} + (16x-8)\sum_{n=1}^{\infty} n a_n x^{n-1} - \sum_{n=0}^{\infty} a_n x^n = 0 \\
&\iff \forall x \in]-R,R[,\ \sum_{n=2}^{\infty} 16n(n-1)a_n x^n - \sum_{n=2}^{\infty} 16n(n-1)a_n x^{n-1} \\
&\qquad + \sum_{n=2}^{\infty} 16 n a_n x^n + 16 x a_1 - \sum_{n=2}^{\infty} 8 n a_n x^{n-1} - \sum_{n=0}^{\infty} a_n x^n = 0 \\
&\iff \forall x \in]-R,R[,\ \sum_{n=2}^{\infty} 16n(n-1)a_n x^n - \sum_{n=1}^{\infty} 16n(n+1)a_{n+1} x^n \\
&\qquad + \sum_{n=2}^{\infty} 16 n a_n x^n + 16 x a_1 - \sum_{n=1}^{\infty} 8(n+1) a_{n+1} x^n - \sum_{n=0}^{\infty} a_n x^n = 0 \\
&\iff \forall x \in]-R,R[,\ \sum_{n=2}^{\infty} \Big(16n(n-1)a_n - 16n(n+1)a_{n+1} + 16 n a_n - 8(n+1)a_{n+1} - a_n\Big) x^n \\
&\qquad + 16 a_1 x - 32 a_2 x - 16 a_2 x - a_1 x = 0 \\
\text{(par unicité du DSE)} &\iff \begin{cases} \forall n \geqslant 2, \quad \big(-16n(n+1) - 8(n+1)\big)a_{n+1} - \big(16n(n-1) + 16n - 1\big)a_n = 0 \\ 15a_1 - 48 a_2 = 0 \end{cases} \\
&\iff \begin{cases} \forall n \geqslant 2,\ a_{n+1} = a_n \times \dfrac{16n(n-1) + 16n - 1}{16n(n+1) + 8(n+1)} \\ a_2 = \dfrac{15}{48} a_1 \end{cases} \\
&\iff \begin{cases} \forall n \geqslant 2,\ a_{n+1} = a_n \times \dfrac{16n^2 - 16n + 16n - 1}{16n^2 + 16n + 8n + 8} \\ a_2 = \dfrac{15}{48} a_1 \end{cases} \\
&\iff \begin{cases} \forall n \geqslant 2,\ a_{n+1} = a_n \times \dfrac{(4n-1)(4n+1)}{8(2n^2+3n+1)} \\ a_2 = \dfrac{15}{48} a_1 \end{cases} \\
&\iff \begin{cases} \forall n \geqslant 2,\ a_{n+1} = a_n \times \dfrac{(4n-1)(4n+1)}{8(n+1)(2n+1)} \\ a_2 = \dfrac{15}{48} a_1 \end{cases}
\end{aligned}
$$

Soit $x \neq 0$. On a

$$\left|\frac{a_{n+1}x^{n+1}}{a_n x^n}\right| = \frac{a_{n+1}}{a_n}|x| = \frac{(4n-1)(4n+1)}{8(n+1)(2n+1)}|x| \sim \frac{16n^2}{16n^2}|x| \xrightarrow[n\to\infty]{} |x|$$

D'où, par le critère de D'ALEMBERT, $R = 1$. On a $a_1 = \frac{1\times(-1)}{4\times 2}a_0$, $a_2 = \frac{5\times 3}{4\times 4\times 3}a_1$, et $a_3 = \frac{9\times 7}{4\times 6\times 5}a_2$. On devine la formule

$$\forall n \in \mathbb{N}, \quad a_n = -\frac{(4n-3)\times\cdots\times 9\times 7\times 5\times 3\times 1}{4^n \times 2n \times \cdots \times 6\times 5\times 4\times 3\times 2}a_0.$$

Montrons par récurrence la formule

$$\forall n \in \mathbb{N}, \qquad a_n = -\frac{(4n-2)!}{4^n \times (2n)! \times 2^{2n-1} \times (2n-1)!}.$$

Cadeaux du 31/01/23

Cadeau 1 :
Soit A la matrice

$$A = \frac{1}{4}\begin{pmatrix} -2 & -\sqrt{6} & \sqrt{6} \\ \sqrt{6} & 1 & 3 \\ -\sqrt{6} & 3 & 1 \end{pmatrix}.$$

Interpréter géométriquement l'endomorphisme f représenté par A dans la base orthonormée $(\vec{\imath}, \vec{\jmath}, \vec{k})$.

Cadeau 2 (Exercice 6 du TD) :
Écrire la matrice, dans la base orthonormée directe $(\vec{\imath}, \vec{\jmath}, \vec{k})$ de $\mathbb{R}^3$, de la rotation d'angle $\frac{\pi}{6}$ autour de l'axe dirigé et orienté $\vec{\imath} + \vec{\jmath}$.

Réponse du cadeau 2 :

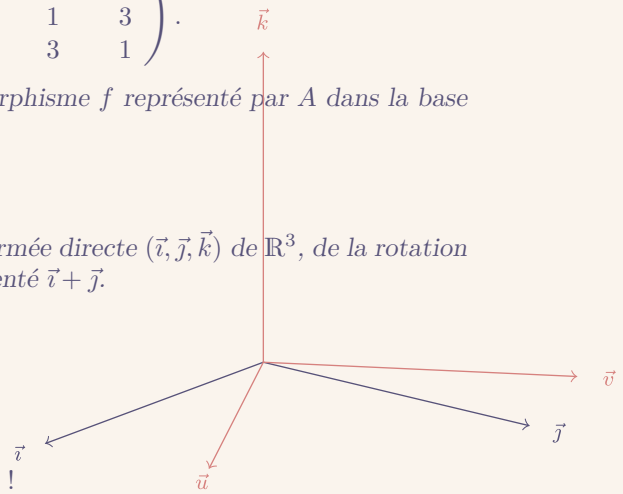


FIGURE 4.2 – Rotation d'angle $\frac{\pi}{6}$ autour de l'axe dirigé orienté $\vec{\imath} + \vec{\jmath}$.

On cherche $\mathscr{B}' = (\vec{k}, \vec{u}, \vec{v})$ une base orthonormée directe. On pose $\vec{v} = (\vec{\imath}+\vec{\jmath})/\sqrt{2}$, et $\vec{u} = \vec{v} \wedge \vec{k}$. On a

$$\vec{u} = \vec{v} \wedge \vec{k} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{pmatrix} \wedge \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \end{pmatrix}.$$

Soit f la rotation d'angle $\frac{\pi}{6}$ autour de l'axe dirigé et orienté par $(\vec{\imath} + \vec{\jmath})/\sqrt{2}$. Ainsi,

$$[\, f \,] = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} & 0 \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} & 0 \\ 0 & 0 & 1 \\ f(\vec{k}) & f(\vec{u}) & f(\vec{v}) \end{pmatrix} \begin{matrix} \vec{k} \\ \vec{u} \\ \vec{v} \end{matrix} = A'.$$

Ainsi, par un changement de base $\mathscr{B} = (\vec{\imath}, \vec{\jmath}, \vec{k})$ vers $\mathscr{B}' = (\vec{k}, \vec{u}, \vec{v})$. Ainsi, $A' = P^{-1} \cdot A \cdot P$ d'où $A = P \cdot A' \cdot P^{-1}$, et

$$P = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 1 & 0 & 0 \\ \vec{k} & \vec{u} & \vec{v} \end{pmatrix} \begin{matrix} \vec{\imath} \\ \vec{\jmath} \\ \vec{k} \end{matrix}$$

De plus, $P^{-1} = P^{\top}$ car les bases $\mathscr{B}$ et $\mathscr{B}'$ sont orthonormées.

Réponse du cadeau 1 :
Les colonnes de cette matrice forment une base orthonormée : $\langle C_1 \mid C_2\rangle = \langle C_2 \mid C_3\rangle = \langle C_3 \mid C_1\rangle = 0$, et $\|C_1\|^2 = \|C_2\|^2 = \|C_3\|^2 = \sqrt{(4+6+6)/16} = 1$. Cette base est directe car $C_1 \wedge C_2 = C_3$ en calculant le produit vectoriel. (Ou, on peut aussi calculer $\det A$, et on trouve 1.) Ainsi, on a $A \in \mathrm{SO}_3(\mathbb{R})$. C'est la matrice d'une rotation, d'où, dans une base adaptée, l'endomorphisme est représenté par la matrice

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Comme la trace est un invariant de similitude, $\operatorname{tr} A = 0 = 2\cos\theta + 1$. Ainsi, $\cos\theta = -\frac{1}{2}$, donc $\theta \equiv \pm\frac{2\pi}{3}\ [2\pi]$. On résout donc $AX = 1X$ avec X^3 :

$$A \cdot X = 1X \iff \begin{cases} -2x - \sqrt{6}y + \sqrt{6}z = 4x \\ \sqrt{6}x + y + 3z = 4y \\ -\sqrt{6}x + 3y + z = 4z \end{cases}$$

$$\vdots$$

$$\iff X \in \mathrm{Vect}(\vec{\jmath} + \vec{k})$$

— Soit $\vec{w} = (\vec{\jmath} + \vec{k})/\sqrt{2}$. Cherchons le signe de θ, modulo 2π. Calculons $f(\vec{\imath}) = -\frac{1}{2}\vec{\imath} + \frac{\sqrt{6}}{4}\vec{\jmath} - \frac{\sqrt{6}}{4}\vec{k}$. Et, on calcule $\vec{\imath} \wedge f(\vec{\imath})$:

$$\vec{\imath} \wedge f(\vec{\imath}) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \wedge \frac{1}{4}\begin{pmatrix} -2 \\ \sqrt{6} \\ -\sqrt{6} \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 0 \\ \sqrt{6} \\ -\sqrt{6} \end{pmatrix} = \frac{\sqrt{6}}{4}(\vec{\jmath} + \vec{k}),$$

qui a le même sens que $\vec{w}$, d'où $\theta = +\frac{2\pi}{3}$.

— Si $\vec{w} = -(\vec{\jmath} + \vec{k})/\sqrt{2}$. De la même manière, on a $\theta = -\frac{2\pi}{3}$.

Cadeau du 01/02/23

Cadeau :
Soit A la matrice

$$A = \frac{1}{4}\begin{pmatrix} -2 & \sqrt{6} & -\sqrt{6} \\ \sqrt{6} & 3 & 1 \\ -\sqrt{6} & 1 & 3 \end{pmatrix}.$$

Interpréter géométriquement l'endomorphisme f représenté par A dans la base orthonormée $(\vec{\imath}, \vec{\jmath}, \vec{k})$.

Réponse du cadeau :
On remarque que,

$$B = A \times \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{S}.$$

On pose s, a et b les endomorphismes représentés par S, A et B. Ainsi $b = a \circ s$. Et, s est la reflection par rapport au plan $\text{Vect}(\vec{\imath}, \vec{\jmath} + \vec{k})$.

Autre méthode :
On diagonalise la matrice, et on conclut. Les valeurs propres sont *sympathiques*.

Cadeau du 02/02/23

Cadeau :
Soit E un espace euclidien, et soit $\vec{a} \in E$ un vecteur non-nul. Montrer que l'application

$$\begin{aligned} \mathcal{s} : E &\longrightarrow E \\ \vec{x} &\longmapsto \vec{x} - 2\frac{\langle \vec{a} \mid \vec{x} \rangle}{\|\vec{a}\|^2}\vec{a} \end{aligned}$$

est une réflexion.

Réponse du cadeau :
Soit $\mathcal{B} = (\vec{e}_1, \dots, \vec{e}_{n-1}, \vec{a})$, où $(\vec{e}_1, \dots, \vec{e}_n)$ est une base de $H = [\operatorname{Vect} \vec{a}]^\perp$. Ainsi, dans cette base,

$$\left[\mathcal{s}\right]_{\mathcal{B}} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ \mathcal{s}(\vec{e}_1) & \dots & \mathcal{s}(\vec{e}_{n-1}) & \mathcal{s}(\vec{a}) & \end{pmatrix} \begin{matrix} \vec{e}_1 \\ \vdots \\ \vec{e}_{n-1} \\ \vec{a} \end{matrix}.$$

Donc, $\mathcal{s}$ est la symétrie orthogonale par rapport à l'hyperplan H, (*i.e.* c'est une réflexion).

Corrigé (partiel) de l'exercice 3 du td 13 :

- $\|\vec{u}\| = 0 \implies \sup\limits_{n\in\mathbb{N}} |u_n| = 0 \implies u = 0_E$;
- Soit $\alpha \in \mathbb{R}$. $\|\alpha u\| = \sup\limits_{n\in\mathbb{N}} |\alpha u_n| = |\alpha| \sup\limits_{n\in\mathbb{N}} |u_n| = |\alpha| \, \|\vec{u}\|$;
- Soient $u, v \in E$. $\|u+v\| = \sup_{n\in\mathbb{N}} |u_n + v_n|$. Or, $\forall n \in \mathbb{N}$, $|u_n + v_n| \leqslant |u_n| + |v_n|$ par inégalité triangulaire. Et, $\forall n \in \mathbb{N}$, $|u_n| \leqslant \sup_{n\in\mathbb{N}} |u_n|$ car le sup est un majorant. De même, $\forall n \in \mathbb{N}$, $|v_n| \leqslant \sup_{n\in\mathbb{N}} |v_n|$ car le sup est un majorant. D'où, $|u_n + v_n| \leqslant \sup_{n\in\mathbb{N}} |u_n| + \sup_{n\in\mathbb{N}} |v_n|$ qui est un majorant. Or, $\sup_{n\in\mathbb{N}} |u_n + v_n|$ est le plus petit majorant. On a donc $\sup_{n\in\mathbb{N}} |u_n + v_n| \leqslant \sup_{n\in\mathbb{N}} |u_n| + \sup_{n\in\mathbb{N}} |v_n|$ donc $\|u+v\| \leqslant \|u\| + \|v\|$.

Cadeau du 03/02/23

Suite du cadeau du 02/02/2023

Cadeau :
Soient $\vec{u}$ et $\vec{v}$ deux vecteurs distincts et de même norme. Montrer qu'il existe une unique réflexion s telle que $s(\vec{u}) = \vec{v}$.

Réponse du cadeau :
On procède par Analyse-Synthèse.

Analyse On suppose que s est une réflexion par rapport à un hyperplan H, et que $s(\vec{u}) = \vec{v}$. Alors, $s(\vec{x}) - \vec{x} \perp H$, démontré plus tard. En particulier, $s(\vec{u}) - \vec{u} = \vec{v} - \vec{u} \perp H$, d'où l'unicité de H.

Synthèse Soient $\vec{a} = \vec{v} - \vec{u}$ et $H \perp \vec{a}$. Alors $s : \vec{x} \mapsto \vec{x} - 2\langle \vec{a} \mid \vec{x} \rangle \ \vec{a}/\|\vec{a}\|^2$ est une réflexion. Il reste à montrer que $s(\vec{u}) = \vec{v}$:

$$s(\vec{u}) = \vec{u} - \frac{\langle \vec{v} - 2\vec{u} \mid \vec{u} \rangle}{\|\vec{v} - \vec{u}\|}(\vec{v} - \vec{u}).$$

On veut montrer que $\langle \vec{v} - \vec{u} \mid \vec{u} \rangle / \|\vec{v} - \vec{u}\|^2 = -\frac{1}{2}$. On calcule $\langle \vec{u} - \vec{v} \mid \vec{v} \rangle = \langle \vec{u} \mid \vec{u} \rangle - \langle \vec{v} \mid \vec{u} \rangle$. Par ailleurs, $\frac{1}{2}\|\vec{v} - \vec{u}\| = \frac{1}{2}\langle \vec{v} - \vec{u} \mid \vec{v} - \vec{u} \rangle = \frac{1}{2}(\|\vec{v}\|^2 - 2\langle \vec{u} \mid \vec{v} \rangle + \|\vec{u}\|^2) = \|\vec{u}\|^2 - \langle \vec{u} \mid \vec{v} \rangle$. Or, par hypothèse $\|\vec{u}\| = \|\vec{v}\|$.

Montrons que $s(\vec{x}) - \vec{x} \perp H$. On sait que $H \oplus H^\perp = E$. Pour tout vecteur $\vec{x}$, il existe un unique couple de vecteurs $(a, b) \in H \times H^\perp$ tel que $\vec{x} = \vec{a} + \vec{b}$. Ainsi, $s(\vec{x}) = s(\vec{a}) + s(\vec{b}) = \vec{a} - \vec{b}$. Et, donc $s(\vec{x}) - \vec{x} = \vec{a} - \vec{b} - \vec{a} - \vec{b} = -2\vec{b} \in H^\perp$.

Cadeau du 03/03/23

Cadeau de Corentin en khôlle avec JJ. Mallet

Cadeau :
On considère sur $E = \mathbb{R}[X]$ les normes N_1 et N_2 ainsi que l'application φ définie par

$$\forall P \in E, \quad N_1(P) = \sup_{t\in[0,1]} |P(t)| \qquad N_2 = \sup_{t\in[1,2]} |P(t)| \qquad \varphi(P) = P(0).$$

1. *Montrer que φ définit une application de (E, N_1) vers $\mathbb{R}$, mais discontinue de (E, N_2) vers $\mathbb{R}$. (On pourra utiliser la suite définie par $P_n(t) = (1 - t/2)^n$.)*
2. *Monter que $\operatorname{Ker}\varphi$ est fermé dans (E, N_1). L'est-il dans (E, N_2) ?*

Réponse du cadeau :

1. L'application φ est linéaire. Montrons qu'il existe $M \in \mathbb{R}^+$ tel que, pour tout polynôme P, $|\varphi(P)| \leqslant M\, N_1(P)$. On a $|\varphi(P)| = |P(0)| \leqslant \sup_{t\in[0,1]} |P(t)| = N_1(P)$, car c'est un majorant. D'où, $|\varphi(P)| \leqslant N_1(P)$ pour tout polynôme P.

   On pose la suite de polynômes définie comme $P_n(t) = (1 - t/2)^n$. On a $N_2(P_n) = \sup_{t\in[1,2]} |(1-t/2)^n| = (1/2)^n$ car la fonction $t \mapsto (1-t/2)^n$ est décroissante et positive. Et, $|\varphi(P_n)| = 1$. Par l'absurde, supposons qu'il existe $K \in \mathbb{R}$ tel que, pour tout polynôme P, $|\varphi(P)| \leqslant K \cdot N_2(P)$. Ainsi, pour tout $n \in \mathbb{N}$, $1 \leqslant K\left(\frac{1}{2}\right)^n$. Les inégalités larges passent à la limite, d'où $1 \leqslant 0$, ce qui est absurde.
2. L'ensemble $\{0\}$ est un fermé, φ est continue sur (E, N_1), et, par définition de Ker, $\varphi^{-1}(\{0\}) = \operatorname{Ker}\varphi$. Ainsi, $\operatorname{Ker}\varphi$ est un fermé (l'image réciproque d'un fermé est un fermé).

   On a $\varphi(P_n) = 1$, donc $P_n \in E \setminus \operatorname{Ker}\varphi$. Or, $N_2(P_n) = \frac{1}{2^n} \to 0$, quand $n \to \infty$. Et, $0 \in \operatorname{Ker}\varphi$ car φ est linéaire. Ainsi, $E \setminus \operatorname{Ker}\varphi$ n'est pas un fermé. On en déduit que $\operatorname{Ker}\varphi$ n'est pas un ouvert pour N_2.

   Posons $Q_n = P_n - 1$ et alors $\varphi(Q_n) = 0$. On a $N_2(Q_n + 1) = N_2(P_n) = \left(\frac{1}{2}\right)^n \to 0$ quand $n \to \infty$. Donc, $Q_n \to -1$. Donc, pour tout $n \in \mathbb{N}$, $Q_n \in \operatorname{Ker}\varphi$ mais $\lim_{n\to\infty} Q_n \notin \operatorname{Ker}\varphi$. Par caractérisation séquentielle d'un fermé, on en déduit que $\operatorname{Ker}\varphi$ n'est pas un fermé.

Cadeau du 27/03/23

Cadeau :
On considère la matrice A définie comme

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{pmatrix}.$$

1. *Déterminer le polynôme minimal μ_A de la matrice A.*
2. *En déduire, pour tout entier $n \in \mathbb{N}$, A^n en fonction de I_3, A et A^2.*
3. *Calculer* $\exp A$.

Réponse du cadeau :

1. On calcule le polynôme caractéristique χ_A, et on trouve $\chi_A = (X-1)\cdot(X-2)^2$. (Vérification : pour un polynôme scindé, $\operatorname{tr} A = \sum_{\lambda\in\operatorname{Sp} A} m_\lambda \cdot \lambda$, et $\det A = \prod_{\lambda\in\operatorname{Sp} A} \lambda^{m_\lambda}$.) Le polynôme minimal, μ_A, divise tous les polynômes annulateurs de A. En particulier, il divise χ_A, d'après le théorème de Cayley & Hamilton. En plus, le spectre de A est l'ensemble des racines de χ_A, mais c'est aussi l'ensemble des racines de μ_A. On peut donc calculer $(A-I_3)\cdot(A-2I_3)$, qui n'est pas nul. D'où, $\chi_A = \mu_A$.

   Autre méthode : on trouve $\dim \operatorname{SEP}(2) = 1$, d'où A n'est pas diagonalisable, elle ne possède donc pas de polynôme annulateur scindé à racines simples. Ainsi, μ_A n'est pas scindé à racines simples. On en déduit donc que $\mu_A = \chi_A$.

   Autre autre méthode : la famille (I_3, A, A^2) est libre, il n'existe donc pas de polynôme annulateur de degré inférieur ou égal à 2.
2. On réalise la division euclidienne $X^n \div \mu_A(X)$, pour obtenir un quotient $Q_n(X)$ et un reste $R_n(X)$. Ainsi, $X^n = \mu_A(X)\cdot Q_n(X) + R_n(X)$, et $\deg R_n < \deg \mu_A$. Et donc, $A^n = R_n(A)$. Or, $R_n(X) = a_nX^2 + b_nX + c_n$. Il y a 3 inconnues, on cherche 3 équations. On a $1^n = 0\times Q_n(1) + R_n(1) = a_n + b_n + c_n$. De plus, $2^n = 0\times Q_n(2) + R_n(2) = 4a_n + 2b_n + c_n$. Finalement, en dérivant, on trouve $nX^{n-1} + \mu_A'\cdot Q_n + \mu_A\cdot Q_n' + R_n'$, et donc, pour $X=2$, on trouve $n2^{n-1} = 0\cdot Q_n(2) + 0\cdot Q_n'(2) + R_n'(2) = 4a_n + b_n$. On résout donc le système

$$\begin{cases} a_n + b_n + c_n = 1 \\ 4a_n + 2b_n + c_n = 2^n \\ 4a_n + b_n = n2^{n-1} \end{cases}.$$

   On trouve donc que $a_n = n2^{n-1} - 2^n + 1$, $b_n = -3n\cdot 2^{n-1} + 2^{n+2} - 4$ et $c_n = n2^n - 3\cdot 2^n + 4$. On en déduit que $A^n = a_nA^2 + b_nA + c_nI_3$. Vérification : pour $n=0$, on a $(a_n, b_n, c_n) = (0,0,1)$; pour $n=1$, on a $(a_n, b_n, c_n) = (0,1,0)$; pour $n=2$, on a $(a_n, b_n, c_n) = (1,0,0)$.

3. Enfin, on calcule

$$\exp A = \sum_{n=0}^{\infty} \frac{A^n}{n!} = \sum_{n=0}^{\infty} \frac{a_n A^2 + b_n A + c_n I_3}{n!} = \alpha A^2 + \beta A + \gamma I_3.$$

On calcule γ, et on procèdera de même pour les autres coefficients.

$$\begin{aligned}\alpha &= \sum_{n=0}^{\infty} \frac{c_n}{n!} = \sum_{n=0}^{\infty} \frac{n2^n - 3 \cdot 2^n + 4}{n!} \\ &= \sum_{n=1}^{\infty} \frac{n_2^n}{n!} - 3\check{a} \sum_{n=0}^{\infty} \frac{2^n}{n!} + 4 \sum_{n=0}^{\infty} \frac{1}{n!} \\ &= 2\,\mathrm{e}^2 - 3\,\mathrm{e}^2 + 4\mathrm{e}\end{aligned}$$

En effet, $x \sum_{n=1}^{\infty} nx^{n-1}/n! = x\mathrm{d}\,\mathrm{e}^x/\mathrm{d}x = xe^x$, car on peut dériver terme à terme une série entière sans changer son rayon de convergence.

Cadeau du 28/03/23

Comment utiliser la trigonalisation pour calculer l'exponentielle d'une matrice ?

Cadeau :
La matrice B est-elle diagonalisable et calculer $\exp B$*, où B est la matrice 2×2 définie comme*

$$B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Réponse du cadeau :

1. Non. En effet, son unique valeur propre sont 1, et, si B serait diagonalisable, alors B serait semblable à I_2, ce qui est absurde car $B \neq I_2$.
2. On remarque que $B^2 = \left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)$. On peut montrer par récurrence que

$$B^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}.$$

Ainsi, pour calculer $\exp B$, on procède pour chaque coefficient de la matrice. En effet,

$$\mathrm{e}^B = \begin{pmatrix} \sum_{n=0}^{\infty} 1/n! & \sum_{n=0}^{\infty} 2n/n! \\ 0 & \sum_{n=0}^{\infty} 1/n! \end{pmatrix} = \begin{pmatrix} \mathrm{e} & 2\mathrm{e} \\ 0 & \mathrm{e} \end{pmatrix}$$

car

$$\sum_{n=0}^{\infty} \frac{2n}{n!} = 2 \sum_{n=1}^{\infty} \frac{1}{(n-1)!} = 2\mathrm{e}.$$

Autre réponse du cadeau :
On remarque que $B = I_2 + \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right) = I_2 + A$. Et, comme I_2 et A commutent, alors

$$\mathrm{e}^B = \mathrm{e}^{I_2} \cdot \mathrm{e}^A = \sum_{n=0}^{\infty} \frac{I_n^n}{n!} \times \sum_{n=0}^{\infty} \frac{A^n}{n!} = \sum_{n=0}^{\infty} \frac{I_n}{n!} \cdot (I_n + A) = \mathrm{e} \cdot B$$

car la matrice A est nilpotente : A^2 est la matrice nulle.

Cadeau du 29/03/23

Cadeau :
Soit $A \in \mathcal{M}_{n,n}(\mathbb{R})$.

1. *Montrer que A est antisymétrique si, et seulement si, $\forall X \in \mathcal{M}_{n,1}(\mathbb{R})$, $X^\top \cdot A \cdot X = 0$.*
2. *Que peut-on dire de e^A si A est antisymétrique ?*

Réponse du cadeau :

1. Le sens direct a déjà été démontré. Montrons la réciproque. On suppose $\forall X \in \mathcal{M}_{n,1}(\mathbb{R})$, $X^\top AX = 0$. Soient X et Y deux vecteurs colonnes de $\mathcal{M}_{n,1}(\mathbb{R})$. On a

$$\begin{aligned} 0 &= (X+Y)^\top A(X+Y) \\ &= X^\top AX + Y^\top AY + X^\top AY + Y^\top AX \\ &= X^\top AY + Y^\top AY \\ &= X^\top AY + X^\top A^\top Y \text{ car } X^\top A^\top Y \in \mathbb{R} \\ &= X^\top (A + A^\top) Y \end{aligned}$$

   Ainsi, en notant $M = A + A^\top$, $\langle X \mid MY \rangle = X^\top \cdot (MY) = 0$, pour tout X. D'où, $MY = 0$, et ce, quel que soit Y. D'où, $M = 0$. La matrice A est donc antisymétrique : $A = -A^\top$.
2. On sait que $(\exp A)^\top = \exp(A^T) = \exp(-A) = (\exp A)^{-1}$, d'où $\mathrm{e}^A \in \mathrm{O}_n(\mathbb{R})$. De plus, $\det(\exp A) = \exp(\operatorname{tr} A) = 1$ et donc $\mathrm{e}^A \in \mathrm{SO}_n(\mathbb{R})$.

Autre réponse du cadeau :

1. On suppose que, pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$, $X^\top AX = 0 \in \mathbb{R}$. Donc $X^\top A^\top X = 0$, par application de la transposée. D'où, $\forall X \in \mathcal{M}_{n,1}(\mathbb{R})$, $X^\top (A + A^\top) X = 0$ et donc $A + A^\top \in \mathcal{S}_n(\mathbb{R})$. D'après le théorème spectral, il existe $P \in \mathrm{O}_n(\mathbb{R})$ tel que $P^\top (A + A^\top) P = D$, où D est diagonale. Ainsi, pour tout vecteur X, $X^\top PDP^\top = (P^\top X)^\top D(P^\top X) = 0$. D'où, par changement de base, pour tout vecteur U, $U^\top DU = 0$. Ainsi, $D = 0$ et donc $A + A^\top = 0$. On en déduit que $A^\top = -A$, la matrice A est antisymétrique.

Cadeau du 30/03/23

polynômes interpolateurs de Lagrange.

Cadeau :
Soit $p \in \mathbb{N}$. Pour tout entier non nul $n \in \mathbb{N}^\star$, notons P_n l'unique polynôme de $\mathbb{R}_p[X]$ vérifiant, pour tout $i \in [\![0, p]\!]$, $P_n(i) = (-1)^n/(n+i)$. Montrer que la série de "vecteurs" $\sum_{n\geqslant 1} P_n$ est convergente.

Réponse du cadeau :
Posons, pour tout $i \in [\![1, p]\!]$, $L_i(X)$ le i-ème polynôme interpolateur de Lagrange :

$$L_i(X) = \prod_{\substack{j=0 \\ j\neq i}}^{p} \frac{X-j}{i-j}.$$

Ainsi, pour tout entier n, $P_n(X) = \sum_{i=1}^{p} (-1)^n L_i(X)/(n+i)$. Or, les polynômes interpolateurs de Lagrange forment une base de $\mathbb{R}_p[X]$. Ainsi, $\mathscr{B} = (L_0, \dots, L_p)$ est une base de $\mathbb{R}_p[X]$. Or, $\mathbb{R}_p[X]$ est de dimension finie. Et, dans un espace vectoriel normé de dimension finie, une série de vecteurs converge si, et seulement si, les sommes partielles de chaque coefficients convergent. Pour tout $i \in [\![1, p]\!]$, la série $\sum (-1)^k/(k+1)$ converge. On en déduit que la série de polynômes $\sum P_n$ converge.

Cadeau du 31/03/23

(Khôlle 21 ?)

Cadeau A :
Soit, pour tout réel $x \in]0,+\infty[$, pour tout entier $n \in \mathbb{N}^\star$, $f_n(x) = 1/(n+n^2x)$.

1. *Montrer que la série de fonctions $\sum f_n$ converge simplement sur $]0,+\infty[$.*
2. *Soit, pour $x \in]0,+\infty[$, $f(x) = \sum_{n=1}^{\infty} f_n(x)$. Montrer que f est continue sur $]0,+\infty[$.*

2,5. Montrer que la convergence de la série $\sum f_n$ n'est pas normale.

3. *La convergence de la série de fonctions $\sum f_n$ est-elle uniforme sur $]0,+\infty[$?*
4. *Déterminer un équivalent de $f(x)$ quand x tend vers $+\infty$.*

Cadeau B :
Soient α et β deux scalaires d'un espace vectoriel $\mathbb{K}$ de dimension finie. Soient f, u et v trois endomorphismes de $\mathbb{K}$ tels que

$$\begin{cases} f = \alpha u + \beta v, \\ f^2 = \alpha^2 u + \beta^2 v, \\ f^3 = \alpha^3 u + \beta^3 v. \end{cases}$$

1. *Déterminer un polynôme annulateur de f.*
2. *Montrer que f est diagonalisable.*

Cadeau C :
Soit $z \in \mathbb{C}$ tel que $|z| < 1$. Montrer que

$$\sum_{n=1}^{\infty} \frac{z^{2n-1}}{1-z^{2n-1}} = \sum_{k=1}^{\infty} \frac{z^k}{1-z^{2k}}.$$

Réponse du cadeau A :

1. Soit $x \in]0,+\infty[$: $1/(n+n^2x) \sim 1/n^2x$, qui ne change pas de signe. Or, la série numérique $\sum 1/n^2x = (1/x)\sum 1/n^2$ converge par le critère de Riemann. D'où, la série de fonctions $\sum f_n$ converge simplement sur $]0,+\infty[$.
2. Soit $a > 0$. Pour tout entier $n \in \mathbb{N}^\star$, pour tout réel $x \in [a,+\infty[$,

$$\big|f_n(x)\big| = \frac{1}{n+n^2x} \leqslant \frac{1}{n^2a},$$

et $\sum 1/n^2a$ converge par critère de Riemann. Ainsi, la série de fonctions $\sum f_n$ converge normalement sur $[a,+\infty[$, donc uniformément sur $[a,+\infty[$.

Chaque fonction f_n est continue sur $[a,+\infty[$, la fonction f est donc continue sur $[a,+\infty[$. Ceci étant vrai pour tout a, et la continuité étant une propriété *locale*, on en déduit que la fonction f est continue sur $]0,+\infty[$.

2,5. Pour tout entier $n \in \mathbb{N}$, $\sup_{x\in]0,+\infty[} |f_n(x)| = 1/n$. Or, la série numérique $\sum 1/n$ diverge, donc la série de fonctions $\sum f_n$ ne converge pas normalement sur $]0,+\infty[$.

3. Supposons, par l'absurde, que la série de fonctions $\sum f_n$ converge uniformément sur $]0,+\infty[$. Pour tout $n \in \mathbb{N}^\star$, $f_n(x) \to 1/n$ quand $x \to 0$. D'après le théorème de la double limite, on en déduit que la série $\sum 1/n$ converge, ce qui est absurde. D'où, $\sum f_n$ ne converge pas uniformément sur $]0,+\infty[$.

4. Soit $n \in \mathbb{N}^\star$, et $x > 1$. On encadre $f_n(x)$:

$$\frac{1}{n^2(x+1)} \leqslant f_n(x) = \frac{1}{n+n^2x} \leqslant \frac{1}{n^2x}.$$

D'où, par somme, pour tout entier $N \in \mathbb{N}^\star$,

$$\frac{1}{(x+1)} \sum_{n=1}^{N} \frac{1}{n^2} \leqslant \sum_{n=1}^{N} f_n(x) \leqslant \frac{1}{x} \sum_{n=1}^{N} \frac{1}{n^2}.$$

Or, les inégalités larges passent à la limite, d'où

$$\frac{\pi^2}{6(x+1)} \leqslant \sum_{n=1}^{\infty} f_n(x) = f(x) \leqslant \frac{\pi^2}{6x}.$$

D'où, en divisant par $x+1$,

$$\frac{x}{x+1} \leqslant \frac{6x}{\pi^2} f(x) \leqslant 1.$$

D'après le théorème des gendarmes, on en déduit que $\frac{6x}{\pi^2} f(x) \to 1$ quand $x \to \infty$ car $x/(x+1) \to 1$. D'où, $f(x) \sim_{x\to\infty} \pi^2/6x$.

Réponse du cadeau B :

1. On calcule

$$(\alpha+\beta)f^2 = \alpha^3 u + \beta^3 v + \alpha^2\beta u + \alpha\beta^2 v = f^3 + \alpha\beta f.$$

On en déduit que le polynôme $\mu(X) = X^3 - (\alpha+\beta)X^2 + \alpha\beta X$ annule f.

2. On procède par disjonction de cas.
   (a) Si $\alpha \neq 0$, $\beta \neq 0$ et $\alpha \neq \beta$, alors μ est un polynôme scindé à racines simples annulateur de f. L'endomorphisme f est donc diagonalisable.
   (b) Si $\alpha = 0$ et $\beta = 0$, alors $f = 0$ qui est diagonal.
   (c) Si $\alpha = 0$ et $\beta \neq 0$, alors $f = \beta v$ et $f^2 = \beta^2 v$. Ainsi, $f^2 - \beta f = 0$ et donc $X^2 - \beta X = X(X-\beta)$ est un polynôme scindé à racines simple annulateur de f. D'où, f est diagonalisable.

(d) Si $\alpha \neq 0$ et $\beta = 0$, on procède comme le cas (c).

(e) Si $\alpha \neq 0$, $\beta \neq 0$, et $\alpha = \beta$, alors $f = \alpha(u+v)$ et $f^2 = \alpha^2(u+v)$. D'où, $f^2 = \alpha f$. Ainsi, $X^2 - \alpha X = X(X-\alpha)$ est un polynôme annulateur de f, il est scindé à racines simples et donc f est diagonalisable.

Réponse (partielle) **du cadeau C** :

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{z^{2n-1}}{1-z^{2n-1}} &= \sum_{n=1}^{\infty} z^{2n-1} \Big(\sum_{k=0}^{\infty} (z^{2n-1})^k \Big) && \text{car } |z^{2n-1}| = |z|^{2n-1} < 1 \\
&= \sum_{n=1}^{\infty} \Big(\sum_{k=0}^{\infty} z^{2n-1} \cdot (z^{2n-1})^k \Big) \\
&= \sum_{k=0}^{\infty} \Big(\sum_{n=1}^{\infty} z^{2n-1} (z^{2n-1})^k \Big) && \text{car } (\heartsuit) \\
&= \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} (z^{2n-1})^{k+1} \\
&= \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} (z^{k+1})^{2n-1} \\
&= \dots
\end{aligned}$$

($\heartsuit$) : la série converge absolument, c'est donc une famille sommable et on applique le théorème de Fubini.

Cadeau du 01/30423

(Cadeau ultime)

Cadeau :
On considère l'ensemble $\mathcal{S}$ défini comme $\mathcal{S} = \{(x, y, z) \in \mathbb{R}^3 \mid \sqrt{x} + \sqrt{y} + \sqrt{z} = 1\}$.

1. Déterminer trois plans de symétries de la surface $\mathcal{S}$. Déterminer une rotation par laquelle $\mathcal{S}$ est stable.
2. Montrer que, pour tout $(x, y, z) \in \mathcal{S}$, $x + y + z \leqslant 1$. En déduire que la surface $\mathcal{S}$ est incluse dans un tétraèdre.

Réponse au cadeau :
Rotation de $2\pi/3$ autour de l'axe orienté par $\vec{u} = (1, 1, 1)$, d'où les plans de symétries. Comme $0 \leqslant x \leqslant 1$, $0 \leqslant y \leqslant 1$ et $0 \leqslant z \leqslant 1$ donc $x \leqslant \sqrt{x}$, $y \leqslant \sqrt{y}$ et $z \leqslant \sqrt{z}$. D'où, par somme, $x + y + z \leqslant 1$. Ainsi, pour tout vecteur $(x, y, z) \in \mathcal{S}$, $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$ et $x + y + z \leqslant 1$. On en déduit que $\mathcal{S}$ est incluse dans un tétraèdre.