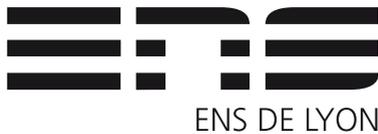


T.D. – Algèbre 1

Hugo SALOU



18 décembre 2024

Table des matières

1	Relations d'équivalence, quotients, premières propriétés des groupes.	4
1.1	Exercice 1.	4
1.2	Exercice 2. <i>Parties génératrices</i>	6
1.3	Exercice 3. <i>Ordre des éléments d'un groupe</i>	8
1.4	Exercice 4.	10
1.5	Exercice 5.	10
1.6	Exercice 6.	11
1.7	Exercice 7.	12
1.8	Exercice 8. <i>Classes à gauche et classes à droite</i>	13
1.9	Exercice 9. <i>Normalisateur</i>	13
1.10	Exercice 10. <i>Construction de \mathbb{Q}</i>	14
1.11	Exercice 11.	17
1.12	Exercice 12.	17
1.13	Exercice 13.	17
1.14	Exercice 14.	17
1.15	Exercice 15.	18
2	Théorèmes d'isomorphismes et actions de groupes.	19
2.1	Exercice 1. <i>Groupes monogènes</i>	19
2.2	Exercice 2.	20
2.3	Exercice 3.	21
2.4	Exercice 4.	22
2.5	Exercice 5.	22
2.6	Exercice 6. <i>Troisième théorème d'isomorphisme</i>	23
2.7	Exercice 7. <i>Sous-groupe d'un quotient</i>	25
2.8	Exercice 8. <i>Combinatoire algébrique</i>	27
2.9	Exercice 9. <i>Formule de BURNSIDE</i>	28
2.10	Exercice 10. <i>Automorphismes intérieurs.</i>	29

2.11 Exercice 11. 29

3 Actions de groupes et théorèmes de Sylow 31

4 Groupe symétrique 32

4.1 Exercice 1. 32

4.2 Exercice 2. *Générateurs de \mathfrak{A}_n* 32

4.3 Exercice 3. 33

5 Quotient et dualité 34

5.1 Exercice 1. 34

5.2 Exercice 2. *Théorèmes d'isomorphismes* 34

5.3 Exercice 3. *Changement de base duale* 35

6 Transposition, orthogonalité, et formes bilinéaires 36

7 Formes quadratiques 37

8 Formes quadratiques – épisode 2 38

9 Produits tensoriels 39

9.1 Exercice 1. 39

9.2 Exercice 2. *Isomorphismes canoniques* 41

10 Représentation de groupes. 44

11 Théorie des caractères. 45

11.1 Exercice 1. *Rappels de cours* 45

11.2 Exercice 2. *Représentation d'une action de groupe* . . . 46

12 Table de caractères. 50

12.1 Exercice 1. *Caractères linéaires* 50

12.2 Exercice 2. *Certaines propriétés des représentations de \mathfrak{S}_n* 51

12.3 Exercice 3. *Table de caractères de \mathfrak{A}_4* 51

12.4 Exercice 4. *Tables de caractères de D_8 et H_8* 53

1 Relations d'équivalence, quotients, premières propriétés des groupes.

Sommaire.

1.1 Exercice 1.	4
1.2 Exercice 2. <i>Parties génératrices</i>	6
1.3 Exercice 3. <i>Ordre des éléments d'un groupe</i>	8
1.4 Exercice 4.	10
1.5 Exercice 5.	10
1.6 Exercice 6.	11
1.7 Exercice 7.	12
1.8 Exercice 8. <i>Classes à gauche et classes à droite</i>	13
1.9 Exercice 9. <i>Normalisateur</i>	13
1.10 Exercice 10. <i>Construction de \mathbb{Q}</i>	14
1.11 Exercice 11.	17
1.12 Exercice 12.	17
1.13 Exercice 13.	17
1.14 Exercice 14.	17
1.15 Exercice 15.	18

1.1 Exercice 1.

1. Donner un isomorphisme $f : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$, où \mathbb{S}^1 est le cercle unité de \mathbb{R}^2 et \mathbb{R}/\mathbb{Z} est le groupe quotient de \mathbb{R} par son sous-groupe distingué \mathbb{Z} .

Soient E et F deux ensembles et soit $f : E \rightarrow F$ une application.

2. a) Montrer que la relation binaire sur E définie par

$$x \sim y \iff f(x) = f(y)$$

est une relation d'équivalence.

b) On pose $X := E/\sim$. Soit $\pi : E \rightarrow X$ l'application canonique. Montrer qu'il existe une unique application $\bar{f} : X \rightarrow F$ telle que $f = \bar{f} \circ \pi$.

c) Montrer que \bar{f} est une bijection sur son image.

1. On commence par considérer l'application

$$\begin{aligned} g : \mathbb{R}/\mathbb{Z} &\longrightarrow u^{-1}(\mathbb{S}^1) \\ x\mathbb{Z} &\longmapsto e^{2\pi i x}, \end{aligned}$$

où $u : \mathbb{C} \rightarrow \mathbb{R}^2$ est l'isomorphisme canonique de \mathbb{R}^2 et \mathbb{C} . Montrons trois propriétés.

- ▷ C'est bien défini. En effet, si $k \in \mathbb{Z}$, alors $e^{2i\pi(x+k)} = e^{2i\pi x}$ par la 2π -périodicité de \cos et \sin .
- ▷ C'est bien un morphisme. En effet, si $x\mathbb{Z}, y\mathbb{Z} \in \mathbb{R}/\mathbb{Z}$, alors on a

$$\begin{aligned} g(x\mathbb{Z} + y\mathbb{Z}) &= g((x + y)\mathbb{Z}) = \exp(2i\pi(x + y)) \\ &= \exp(2i\pi x) \cdot \exp(2i\pi y) \\ &= g(x\mathbb{Z}) \cdot g(y\mathbb{Z}). \end{aligned}$$

- ▷ C'est une bijection. En effet, l'application réciproque est l'application $u^{-1}(\mathbb{S}^1) \ni z \mapsto (\arg z)\mathbb{Z}$.

On en conclut en posant l'isomorphisme $f := u \circ g : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$.

2. a) On a trois propriétés à vérifier.

- ▷ Comme $f(x) = f(x)$, on a $x \sim x$ quel que soit $x \in E$.
- ▷ Si $x \sim y$, alors $f(x) = f(y)$ et donc $f(y) = f(x)$ et on en déduit $y \sim x$.

- ▷ Si $x \sim y$ et $y \sim z$, alors $f(x) = f(y) = f(z)$, et on a donc $x \sim z$.
- b) La fonction f est constante sur chaque classe d'équivalence de E par \sim . On procède par analyse synthèse.
 - ▷ *Analyse.* Si $\bar{f} : X \rightarrow F$ existe, alors $\bar{f}(\bar{x}) = f(x)$ quel que soit $x \in E$, où \bar{x} est la classe d'équivalence de x . L'application \bar{f} est donc unique, car déterminée uniquement par les valeurs de f sur les classes d'équivalences de x .
 - ▷ *Synthèse.* On pose $\bar{f}(\bar{x}) := f(x)$, qui est bien définie car f est constante sur les classes d'équivalences de \sim .
- c) Montrons que $\bar{f} : X \rightarrow \text{im } \bar{f}$ est injective et surjective.
 - ▷ Soient \bar{x} et \bar{y} dans X tels que $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$. Alors, on a $f(x) = f(y)$ et donc $x \sim y$ d'où $\bar{x} = \bar{y}$.
 - ▷ On a, par définition, $\text{im } \bar{f} = \bar{f}(X)$.
 D'où, \bar{f} est une bijection sur son image.

1.2 Exercice 2. Parties génératrices

1. Soit X une partie non vide d'un groupe G . Montrer que $\langle X \rangle$, le sous-groupe de G engendré par X , est exactement l'ensemble des produits finis d'éléments de $X \cup X^{-1}$, où X^{-1} est l'ensemble défini par $X^{-1} := \{x^{-1} \mid x \in X\}$.
2. Montrer que le groupe $(\mathbb{Q}, +)$ n'admet pas de partie génératrice finie.
3. Montrer que $(\mathbb{Q}^\times, \times) = \langle -1, p \in \mathbb{P} \rangle$, où \mathbb{P} est l'ensemble des nombres premiers.

1. Soit H l'ensemble des produits finis d'éléments de $X \cup X^{-1}$.
 - ▷ L'ensemble H contient X . De plus, H est un groupe. En effet, on a $H \neq \emptyset$ car $e = xx^{-1} \in H$ où $x \in X$. Puis, pour deux produits $x = x_1 \cdots x_n \in H$ et $y = y_1 \cdots y_m \in H$ (où les x_i et les y_j sont des éléments de $X \cup X^{-1}$) on a

$$xy^{-1} = x_1 \cdots x_n y_m^{-1} \cdots y_1^{-1},$$

qui est un produit fini d'éléments de $X \cup X^{-1}$, c'est donc un élément de H . On en conclut que H est un sous-groupe de G contenant X . D'où $H \geq \langle X \rangle$.

- ▷ Soit K un sous-groupe de G contenant X . D'une part, on sait que $X \cup X^{-1} \subseteq K$. D'autre part, si $x = x_1 \cdots x_n$ où l'on a $x_i \in X \cup X^{-1} \subseteq K$, alors $x \in K$ car K est un groupe. On en déduit que $H \leq K$.

Ainsi, H est le plus petit sous-groupe de G contenant X , il est donc égal à $\langle X \rangle$.

2. Supposons, par l'absurde, que $(\mathbb{Q}, +) = \langle \frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_n}{q_n} \rangle$. On pose $Q := \prod_{i=1}^n q_i$, puis on considère $\frac{1}{Q+1} \in \mathbb{Q}$.

Montrons que l'on peut écrire tout élément de $\langle \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} \rangle$ sous la forme $\frac{p}{Q}$. En effet, par la question 1, on considère

$$x := \sum_{i \in I} \varepsilon_i \frac{p_i}{q_i} \quad \text{avec} \quad \varepsilon_i \in \{-1, 1\} \quad \text{et} \quad I \text{ fini,}$$

un élément quelconque du sous-groupe engendré. Et, en mettant au même dénominateur, on obtient $p' / \prod_{i \in I} q_i = x$. On obtient donc bien

$$x = \frac{p' \times \prod_{i \notin I} p_i}{Q},$$

où le produit au numérateur contient un nombre fini de termes.

Or, $\frac{1}{Q+1} \in \mathbb{Q}$ ne peut pas être écrit sous la forme p/Q car $Q+1$ et Q sont premiers entre eux. C'est donc absurde ! On en conclut que $(\mathbb{Q}, +)$ n'admet pas de partie génératrice finie.

3. Notons $E := \langle -1, p \in \mathbb{P} \rangle$. Soit $\frac{a}{b}$ un rationnel strictement positif. On suppose a et b positifs. On décompose a et b en produit de nombre premiers :

$$a = \prod_{i \in I} p_i \quad \text{et} \quad b = \prod_{j \in J} p_j.$$

On a donc $a \in E$ et $b \in E$. On en conclut que $\frac{a}{b} \in E$.

Si $\frac{a}{b} \in \mathbb{Q}^\times$ est un rationnel tel que $a, b < 0$, on a $\frac{a}{b} = \frac{|a|}{|b|} \in E$ d'après ce qui précède.

Si $\frac{a}{b} \in \mathbb{Q}^\times$ est un rationnel négatif, alors on a $|\frac{a}{b}| \in E$, mais on a donc également $\frac{a}{b} = (-1) \times |\frac{a}{b}| \in E$.

On en conclut que $\mathbb{Q}^\times \subseteq E$ et on a égalité car $E \subseteq \mathbb{Q}^\times$ par définition de E comme sous-groupe de \mathbb{Q}^\times .

1.3 Exercice 3. *Ordre des éléments d'un groupe*

Soient g et h deux éléments d'un groupe G .

1. a) Montrer que g est d'ordre fini si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $g^n = e$.
 b) Montrer que si g est d'ordre fini, alors son ordre est le plus petit entier $n \in \mathbb{N}^*$ tel que $g^n = e$. Montrer, de plus, que pour $m \in \mathbb{Z}$, $g^m = e$ si et seulement si l'ordre de g divise m .
2. Montrer que les éléments g , g^{-1} et hgh^{-1} ont même ordre.
3. Montrer que gh et hg ont même ordre.
4. Soit $n \in \mathbb{N}$. Exprimer l'ordre de g^n en fonction de celui de g .
5. On suppose que g et h commutent et sont d'ordre fini m et n respectivement.
 - a) Exprimer l'ordre de gh lorsque $\langle g \rangle \cap \langle h \rangle = \{e\}$.
 - b) Même question lorsque m et n sont premiers entre eux.
 - c) (Plus difficile) On prend m et n quelconques. Soient $a := \min\{\ell \in \mathbb{N}^* \mid g^\ell \in \langle h \rangle\}$ et $b \in \mathbb{N}$ tel que $g^a = h^b$. Démontrer que l'ordre de gh est $an/\text{pgcd}(n, (a+b))$.

6. En considérant

$$A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad B := \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix},$$

montrer que le produit de deux éléments d'ordre fini ne l'est pas forcément.

1. On rappelle que l'ordre de g est défini comme $\#\langle g \rangle$. On le note naturellement $\text{ord } g$.
 - a) On procède par double implication.

- ▷ Si g est d'ordre fini, alors $\langle g \rangle$ est fini et donc l'application

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \langle g \rangle \\ n &\longmapsto g^n \end{aligned}$$

est un morphisme non injectif. Il existe donc un entier non nul $n \in \mathbb{Z} \setminus \{0\}$ tel que $n \in \ker \varphi$, i.e. $g^n = e$.

- ▷ Si $g^n = e$ alors $\langle g \rangle = \{g^i \mid i \in \llbracket 0, n-1 \rrbracket\}$, qui est fini. Ainsi g est d'ordre fini.

- b)** Si g est d'ordre fini, alors le morphisme φ (défini ci-avant) est surjectif et non injectif. Soit $p = \min(\ker \varphi \cap \mathbb{N}^*)$. Alors les g^i pour $i \in \llbracket 0, p-1 \rrbracket$ sont distincts et constituent $\langle g \rangle$.

Si $n \in \mathbb{Z}$ est tel que $g^n = e$. On écrit $n = q \times (\text{ord } g) + r$ la division euclidienne de n par $\text{ord } g$, avec $0 \leq r < \text{ord } g$. Et,

$$e = g^n = (g^{\text{ord } g})^q g^r = g^r,$$

d'où $g^r = e$. On en déduit que $r = 0$ et donc $\text{ord } g$ divise n .

- 2.** D'une part, $\langle g \rangle = \langle g^{-1} \rangle$, d'où $\text{ord } g = \text{ord } g^{-1}$. D'autre part, pour $n \in \mathbb{N}$, on a $(hgh^{-1})^n = hg^n h^{-1}$, et donc l'équivalence

$$g^n = e \iff (hgh^{-1})^n = e,$$

d'où $\text{ord } g = \text{ord}(hgh^{-1})$.

- 3.** On a $hg = h(gh)h^{-1}$ et par la question précédente, on a que $\text{ord}(hg) = \text{ord}(gh)$.
- 4.** On a

$$\begin{aligned} \text{ord } g^n &= \min\{k \in \mathbb{N}^* \mid g^{nk} = e\} \\ &= \frac{1}{n} \min((\text{ord } g)\mathbb{Z} \cap n\mathbb{Z} \cap \mathbb{N}^*) \\ &= \frac{\text{ppcm}(\text{ord } g, n)}{n} \\ &= \frac{\text{ord } g}{\text{pgcd}(\text{ord } g, n)}. \end{aligned}$$

- 5. a)** Si $\langle g \rangle \cap \langle h \rangle = \{e\}$ et $(gh)^k = e$ alors $g^k = h^{-k} \in \langle g \rangle \cap \langle h \rangle$. D'où, $g^k = h^{-k} = e$.

1.4 Exercice 4.

Soit G un groupe.

1. On suppose que tout élément g de G est d'ordre au plus 2. Montrer que G est commutatif.
 2. Montrer que G est commutatif si et seulement si l'application $g \mapsto g^{-1}$ est un morphisme de groupes.
1. Pour tout $g \in G$, on a $g^2 = e$. Ainsi, pour tout $g \in G$, on a g est son propre inverse. Ceci permet de calculer

$$gh = g^{-1}h = g^{-1}h^{-1} = (hg)^{-1} = hg,$$

d'où G est commutatif.

2. On note $\phi : g \mapsto g^{-1}$, et on procède par équivalence.

$$\begin{aligned} G \text{ est commutatif} &\iff \forall g, h \in G, \quad gh = hg \\ &\iff \forall g, h \in G, \quad (gh)^{-1} = (hg)^{-1} \\ &\iff \forall g, h \in G, \quad (gh)^{-1} = g^{-1}h^{-1} \\ &\iff \forall g, h \in G, \quad \phi(gh) = \phi(g)\phi(h) \\ &\iff \phi \text{ est un morphisme.} \end{aligned}$$

1.5 Exercice 5.

Soit $\phi : G_1 \rightarrow G_2$ un morphisme de groupes, et soit $g \in G_1$ d'ordre fini. Montrer que $\phi(g)$ est d'ordre fini et que son ordre divise l'ordre de g .

On utilise habilement l'exercice 1.3 : pour tout $h \in G$, $h^m = e$ si et seulement si l'ordre de h divise m . Soit n l'ordre de g (qui est fini car G_1 d'ordre fini). Ainsi,

$$(\phi(g))^n = \phi(g^n) = \phi(e_1) = e_2.$$

On en déduit donc que $\phi(g)$ est d'ordre fini et qu'il divise $n = \text{ord } g$.

1.6 Exercice 6.

Soient G_1 et G_2 des groupes, et $\phi : G_1 \rightarrow G_2$ un morphisme de groupes.

1. Soient H_1 (resp. H_2) un sous-groupe de G_1 (resp. G_2). Montrer que $\phi(H_1)$ (resp. $\phi^{-1}(H_2)$) est un sous-groupe de G_2 (resp. G_1).
 2. Montrer que H_2 est un sous-groupe distingué de G_2 , alors $\phi^{-1}(H_2)$ est un sous-groupe distingué de G_1 .
 3. Montrer que si ϕ est surjective, l'image d'un sous-groupe distingué de G_1 par ϕ est un sous-groupe distingué de G_2 .
 4. Donner un exemple d'un morphisme de groupes $\phi : G_1 \rightarrow G_2$ et de sous-groupe distingué $H_1 \triangleleft G_1$ tel que $\phi(H_1)$ n'est pas distingué dans G_2 .
1. Remarquons que $e_2 \in \phi(H_1) \neq \emptyset$ et que $e_1 \in \phi^{-1}(H_2) \neq \emptyset$ car on a $\phi(e_1) = e_2$. Pour $a, b \in \phi(H_1)$, on sait qu'il existe $x, y \in H_1$ tels que $\phi(x) = a$ et $\phi(y) = b$. Alors,

$$ab^{-1} = \phi(x) \phi(y)^{-1} = \underbrace{\phi(xy^{-1})}_{\in H_1} \in \phi(H_1),$$

d'où $\phi(H_1)$ est un sous-groupe de G_2 . Pour $a, b \in \phi^{-1}(H_2)$, on sait que $\phi(a), \phi(b) \in H_2$. Alors, on a

$$\phi(ab^{-1}) = \underbrace{\phi(a)}_{\in H_2} \underbrace{\phi(b)^{-1}}_{\in H_2} \in H_2,$$

d'où $ab^{-1} \in \phi^{-1}(H_2)$ et donc $\phi(H_1)$ est un sous-groupe de G_2 .

2. Supposons $H_2 \triangleleft G_2$ et montrons que $\phi^{-1}(H_2) \triangleleft G_1$. Soit un élément $g \in G_1$ quelconque, et soit $h \in \phi^{-1}(H_2)$. Alors,

$$\phi(ghg^{-1}) = \phi(g) \phi(h) \phi(g)^{-1} \in H_2,$$

car $\phi(h) \in H_2$ et que $H_2 \triangleleft G_2$. Ainsi, $ghg^{-1} \in \phi^{-1}(H_2)$. On a donc $g \phi^{-1}(H_2) g^{-1} \subseteq \phi^{-1}(H_2)$, quel que soit $g \in G_1$. On en déduit que $\phi^{-1}(H_2)$ est distingué dans G_1 .

3. Supposons ϕ surjective, on a donc l'égalité $\phi(G_1) = G_2$. Supposons de plus que $H_1 \triangleleft G_1$. Montrons que $\phi(H_1)$ est un sous-groupe distingué de G_2 . Soit $g \in G_2 = \phi(G_1)$ quelconque, et soit un élément $h \in \phi(H_1)$. Il existe donc $x \in G_1$ et $y \in H_1$ deux éléments tels que $\phi(y) = h$ et $\phi(x) = g$. Ainsi

$$ghg^{-1} = \phi(x) \phi(y) \phi(x)^{-1} = \phi(xyx^{-1}) \in \phi(H_1)$$

car H_1 distingué dans G_1 et donc $xyx^{-1} \in H_1$. Ainsi $\phi(H_1) \triangleleft G_2$.

4. On considère le morphisme

$$f : (\mathbb{R}, +) \longrightarrow (\text{GL}_2(\mathbb{R}), \cdot)$$

$$x \longmapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

et le sous-groupe distingué $\mathbb{R} \triangleleft \mathbb{R}$. On a

$$\forall x \in \mathbb{R} \setminus \{0\}, \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{M \in \text{GL}_2(\mathbb{R})} \underbrace{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}}_{f(x)} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{M^{-1} \in \text{GL}_2(\mathbb{R})} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \notin f(\mathbb{R}).$$

Ainsi, $f(\mathbb{R}) \not\triangleleft \text{GL}_2(\mathbb{R})$.

1.7 Exercice 7.

Soit G un groupe et soient H, K deux sous-groupes de G . Montrer que $H \cup K$ est un sous-groupe de G si et seulement si on a $H \subseteq K$ ou $K \subseteq H$.

On procède par double implications.

- ▷ « \implies ». Supposons que $H \cup K$ soit un sous-groupe de G . Par l'absurde, supposons que $H \not\subseteq K$ et $K \not\subseteq H$. Il existe donc deux éléments $h \in H \setminus K$ et $k \in K \setminus H$. Considérons $hk \in H \cup K$.
 - Si $hk \in H$, alors $h^{-1}(hk) \in H$ et donc $k \in H$, absurde!
 - Si $hk \in K$, alors $(hk)k^{-1} \in K$ et donc $h \in K$, absurde!

On en déduit que $H \subseteq K$ ou $K \subseteq H$.

- ▷ « \impliedby ». Sans perte de généralité, supposons $H \subseteq K$. Ainsi, on a $H \cup K = K$ qui est un sous-groupe de G .

1.8 Exercice 8. Classes à gauche et classes à droite

Soit H un sous-groupe d'un groupe G . Montrer que l'on a une bijection canonique $G/H \rightarrow H \backslash G$.

On note $S^{-1} = \{s^{-1} \mid s \in S\}$ pour un sous-ensemble S de G . Alors nous avons l'égalité $(aH)^{-1} = Ha^{-1}$ et $(Ha)^{-1} = a^{-1}H$. En effet,

$$\begin{aligned}
 (aH)^{-1} &= \{ah \mid h \in H\}^{-1} & (Ha)^{-1} &= \{ha \mid h \in H\}^{-1} \\
 &= \{(ah)^{-1} \mid h \in H\} & &= \{(ha)^{-1} \mid h \in H\} \\
 &= \{h^{-1}a^{-1} \mid h \in H\} & &= \{a^{-1}h^{-1} \mid h \in H\} \\
 &= \{ha^{-1} \mid h \in H\} & &= \{a^{-1}h \mid h \in H\} \\
 &= Ha^{-1} & &= a^{-1}H.
 \end{aligned}$$

Il existe donc une bijection canonique

$$\begin{aligned}
 f : G/H &\longrightarrow H \backslash G \\
 aH &\longmapsto (aH)^{-1} = Ha^{-1}.
 \end{aligned}$$

1.9 Exercice 9. Normalisateur

Soit $H \leq G$ un sous-groupe d'un groupe G . On dit que x normalise si $xHx^{-1} = H$. On note $N_G(H)$ l'ensemble des éléments de G qui normalisent H . C'est le normalisateur de H dans G .

1. Montrer que $N_G(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.
2. En déduire que H est distingué dans G si et seulement si on a l'égalité $G = N_G(H)$.

1. Commençons par montrer que $N_G(H)$ est un sous-groupe de G contenant H .

▷ L'élément neutre normalise H , car $eHe^{-1} = H$. D'où, le normalisateur de H est non vide.

- ▷ Soient x et y deux éléments qui normalisent H . Alors, xy normalise H :

$$(xy)H(xy)^{-1} = xyHy^{-1}x^{-1} = xHx^{-1} = H.$$

- ▷ Soit $x \in G$ qui normalise H . Alors x^{-1} normalise H :

$$x^{-1}Hx = H \iff Hx = xH \iff H = xHx^{-1},$$

et cette dernière condition est vérifiée car x normalise H .

- ▷ Soit $h \in H$. Alors h normalise H . En effet,

$$hHh^{-1} = Hh^{-1} = H,$$

car $h^{-1} \in H$ et puis car $h \in H$.

On en conclut que $N_G(H)$ est un sous-groupe de G contenant H .

Par définition de $N_G(H)$, on a que $H \triangleleft N_G(H)$: quel que soit x qui normalise H , on a (par définition) $xHx^{-1} = H$.

Il ne reste plus qu'à montrer que tout sous-groupe $N \supseteq H$ tel que $H \triangleleft N$ vérifie $N \subseteq N_G(H)$. Soit N un tel sous-groupe, et un élément $x \in N$. Ainsi $xHx^{-1} = H$, d'où x normalise H . On a donc bien l'inclusion $N \subseteq N_G(H)$.

Ceci démontre bien que $N_G(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H y est distingué.

2. D'une part, si H est distingué dans G , alors le plus grand sous-groupe de G contenant H et dans lequel H est distingué est G .

D'autre part, si $G = N_G(H)$, alors tout élément $x \in G$ vérifie l'égalité $xHx^{-1} = H$ et donc $H \triangleleft G$.

1.10 Exercice 10. Construction de \mathbb{Q}

Soit $E := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. On définit \sim sur E par $(a, b) \sim (a', b')$ dès lors que $ab' = a'b$.

1. Montrer que \sim est un relation d'équivalence sur E . Si $(a, b) \in E$, on note $\frac{a}{b}$ son image dans E/\sim .

2. Munir E/\sim d'une structure de corps telle que \mathbb{Z} s'injecte dans le corps E/\sim .
3. Similairement, pour un corps \mathbb{k} , construire $\mathbb{k}(X)$ à partir de l'ensemble $\mathbb{k}[X]$.
4. Construire \mathbb{Z} à partir de \mathbb{N} .

1. On a trois propriétés à vérifier.

- ▷ Si $(a, b) \in E$, alors $ab = ab$ donc $(a, b) \sim (a, b)$.
- ▷ Si $(a, b) \sim (a', b')$, alors $ab' = a'b$ et donc $(a', b') \sim (a, b)$.
- ▷ Si $(a, b) \sim (a', b')$ et $(a', b') \sim (a'', b'')$, alors

$$a'ab'b'' = a'a'bb'' = a'ba'b'' = a'ba''b',$$

et donc $a'b'(ab'' - a''b) = 0$. Par anneau intègre, on a une disjonction de cas :

- si $a' = 0$, alors $a = a'' = 0$;
- si $b' = 0$, alors **absurde** car $b' \in \mathbb{Z} \setminus \{0\}$;
- si $ab'' - a''b = 0$, alors on a $ab'' = a''b$.

Dans les deux cas, on obtient bien $(a, b) \sim (a'', b'')$.

2. On munit E/\sim de deux opérations « \oplus » et « \otimes ».

- ▷ On pose l'opération $\frac{a}{b} \oplus \frac{c}{d} := \frac{ad+bc}{bd}$ qui est bien définie car, si l'on a $(a, b) \sim (a', b')$, alors

$$\begin{aligned} (ad + bc, bd) \sim (a'd + b'c, b'd) &\iff (ad + bc)b'd = (a'd + b'c)bd \\ &\iff ab'd^2 = a'bd^2, \end{aligned}$$

ce qui est vrai car $(a, b) \sim (a', b')$. On peut procéder symétriquement pour $(c', d') \sim (c, d)$.

- ▷ On pose l'opération $\frac{a}{b} \otimes \frac{c}{d} := \frac{ac}{bd}$ qui est bien définie car, si l'on a $(a, b) \sim (a', b')$, alors

$$(ac, bd) \sim (a'c, b'd) \iff acb'd = a'cbd,$$

ce qui est vrai car $(a, b) \sim (a', b')$. On peut procéder symétriquement pour $(c', d') \sim (c, d)$.

Montrons que $(E/\sim, \oplus, \otimes)$ est un corps.

▷ La loi \oplus est associative : on a

$$\frac{a}{b} \oplus \left(\frac{c}{d} \oplus \frac{e}{f} \right) = \left(\frac{a}{b} \oplus \frac{c}{d} \right) \oplus \frac{e}{f} = \frac{adf+cbf+ebd}{bdf},$$

par associativité de $+$.

▷ La loi \oplus est commutative par commutativité de $+$.

▷ La loi \oplus possède un élément neutre $\frac{0}{1} \in E/\sim$.

▷ Tout élément $\frac{a}{b}$ possède un symétrique $(\frac{-a}{b})$ pour \oplus par rapport à $\frac{0}{1}$.

▷ La loi \otimes est associative : on a

$$\frac{a}{b} \otimes \left(\frac{c}{d} \otimes \frac{e}{f} \right) = \left(\frac{a}{b} \otimes \frac{c}{d} \right) \otimes \frac{e}{f} = \frac{ace}{bdf},$$

par associativité de \times .

▷ La loi \otimes est distributive par rapport à \oplus , par distributivité de \times par rapport à $+$.

▷ La loi \otimes possède un élément neutre $\frac{1}{1} \in E/\sim$ pour \otimes .

▷ Tout élément non nul $\frac{a}{b}$ possède un inverse $\frac{b}{a}$ par rapport à $\frac{1}{1}$.

On en conclut que $(E/\sim, \oplus, \otimes)$ est un corps.

Finalement, on considère l'injection

$$\begin{aligned} f : \mathbb{Z} &\hookrightarrow E/\sim \\ k &\longmapsto \frac{k}{1}. \end{aligned}$$

C'est bien une injection car, si $\frac{k}{1} = \frac{k'}{1}$, alors $k \times 1 = k' \times 1$ et donc $k = k'$. On a, de plus, que f est un morphisme de groupes $(\mathbb{Z}, +) \rightarrow (E/\sim, \oplus)$:

$$f(k) \oplus f(k') = \frac{k}{1} \oplus \frac{k'}{1} = \frac{k+k'}{1} = f(k+k').$$

3. On pose $F := \mathbb{k}[X] \times (\mathbb{k}[X] \setminus \{0_{\mathbb{k}[X]}\})$, et la relation

$$(P, Q) \sim (P', Q') \iff PQ' = P'Q.$$

Cette relation est une relation d'équivalences (comme pour la question précédente, et car \mathbb{k} est un anneau intègre). On pose

ensuite $\mathbb{k}(X) := F/\sim$. Comme dans la question précédente, on peut donner une structure de corps avec les mêmes définitions (en remplaçant les entiers par des polynômes de \mathbb{k}). Les propriétés découlent toutes du fait que $(\mathbb{k}, +, \times)$ est un corps.

4. On pose $Z := \mathbb{N}^2/\sim$, où la relation d'équivalence \sim est définie par

$$(a, b) \sim (a', b') \iff a + b' = b + a'.$$

1.11 Exercice 11.

Soit $E := \mathbb{C}[X]$ le \mathbb{C} -espace vectoriel des polynômes à coefficients dans \mathbb{C} et $P \in \mathbb{C}[X]$ un polynôme de degré $d \in \mathbb{N}^*$.

1. Montrer que l'ensemble $(P) := \{QP \mid Q \in \mathbb{C}[X]\}$ est un sous- \mathbb{C} -espace vectoriel de $\mathbb{C}[X]$.
2. Déterminer un isomorphisme entre $\mathbb{C}[X]/(P)$ et le \mathbb{C} -espace vectoriel $\mathbb{C}_{d-1}[X]$ des polynômes de degrés inférieurs à $d - 1$ de $\mathbb{C}[X]$.
3. Montrer que la multiplication dans $\mathbb{C}[X]$ induit une structure de \mathbb{C} -algèbre sur $\mathbb{C}[X]/(P)$.

1.12 Exercice 12.

Soit G un groupe et H un sous-groupe strict de G . Montrer que l'on a l'égalité $\langle G \setminus H \rangle = G$.

1.13 Exercice 13.

Soit G un groupe fini. Montrer que G contient un élément d'ordre 2 si et seulement si son cardinal est pair. Montrer de plus que, dans ce cas là, il en contient un nombre impair.

1.14 Exercice 14.

Soit G un groupe et \sim une relation d'équivalence sur G . On suppose que G/\sim est un groupe, et que la projection canonique $\pi : G \rightarrow G/\sim$ est un morphisme de groupes.

Montrer qu'il existe un sous-groupe distingué $H \triangleleft G$ tel que pour tous éléments $x, y \in G$, $x \sim y$ si et seulement si $xy^{-1} \in H$.

1.15 Exercice 15.

Soit G un groupe et S_G l'ensemble des sous-groupes de G .

1. Démontrer que si G est fini, alors S_G est fini.
2. Supposons S_G fini. Démontrer que tous les éléments de G sont d'ordre fini, en déduire que G est fini.
3. On ne suppose plus que S_G est fini. Si tous les éléments de G sont d'ordre fini, est-ce que G est fini ?

2 Théorèmes d'isomorphismes et actions de groupes.

Sommaire.

2.1	Exercice 1. <i>Groupes monogènes</i>	19
2.2	Exercice 2.	20
2.3	Exercice 3.	21
2.4	Exercice 4.	22
2.5	Exercice 5.	22
2.6	Exercice 6. <i>Troisième théorème d'isomorphisme</i>	23
2.7	Exercice 7. <i>Sous-groupe d'un quotient</i>	25
2.8	Exercice 8. <i>Combinatoire algébrique</i>	27
2.9	Exercice 9. <i>Formule de Burnside</i>	28
2.10	Exercice 10. <i>Automorphismes intérieurs.</i>	29
2.11	Exercice 11.	29

2.1 Exercice 1. *Groupes monogènes*

Soit G un groupe monogène. Montrer que soit $G \cong \mathbb{Z}$, soit $G \cong \mathbb{Z}/n\mathbb{Z}$ pour un entier strictement positif n .

Soit $g \in G$ tel que $\langle g \rangle = G$. Considérons le morphisme

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto g^k.\end{aligned}$$

On a $\text{im } \phi = \langle g \rangle = G$. De plus, par le premier théorème d'isomorphisme

$$\mathbb{Z}/\ker \phi \cong \text{im } \phi = G.$$

- ▷ Si $\ker \phi$ est le sous-groupe trivial $\{0\}$, on a donc $G \cong \mathbb{Z}$.
- ▷ Si $\ker \phi$ est un sous-groupe non trivial de \mathbb{Z} , alors $\ker \phi = n\mathbb{Z}$, et on a donc $G \cong \mathbb{Z}/n\mathbb{Z}$.

2.2 Exercice 2.

Soit $n > 0$ un entier.

1. Montrer que $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(n)$ éléments d'ordre n , où $\varphi(n)$ désigne le nombre d'entiers $k \in \llbracket 0, n-1 \rrbracket$ premiers à n .
 2. Montrer que pour tout $d > 0$ divisant n , $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe d'ordre d formé des multiples de $\overline{n/d}$.
 3. En déduire que pour tout diviseur $d > 0$ de n , $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d et que $\sum_{0 < d|n} \varphi(d) = n$.
1. Soit $k \in \llbracket 0, n-1 \rrbracket$. Montrons que $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(k, n) = 1$.
 - ▷ Si $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ alors il existe $a \in \mathbb{Z}$ tel que

$$a\bar{k} = \underbrace{\bar{k} + \dots + \bar{k}}_{a \text{ fois}} = \bar{1}.$$

Ainsi, il existe $b \in \mathbb{Z}$ tel que $ak - 1 = bn$, soit $ak + bn = 1$. On en conclut, par le théorème de Bézout, que k et n sont premiers entre-eux.

- ▷ Si $\text{pgcd}(k, n) = 1$ alors il existe $a, b \in \mathbb{Z}$ tels que $ak + bn = 1$ et donc $ak \equiv 1 \pmod{n}$. Ainsi, $k + \dots + k \equiv 1 \pmod{n}$. Or, $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ et donc, comme $\langle \bar{1} \rangle \subseteq \langle \bar{k} \rangle$ on a que

$$\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}.$$

Par bijection, on a donc

$$\varphi(n) = \#\{k \in \llbracket 0, n-1 \rrbracket \mid \text{pgcd}(k, n) = 1\}$$

éléments d'ordre n .

2. On sait que $\langle \overline{n/d} \rangle$ est un groupe, et $d \overline{n/d} = \bar{n} = \bar{0}$. Ainsi, on a que $\#\langle \overline{n/d} \rangle = d$. Il ne reste qu'à montrer l'unicité. Soit un sous-groupe $H \leq \mathbb{Z}/n\mathbb{Z}$ d'ordre d . Soit $\bar{a} \in H$ tel que $d\bar{a} = 0$. Ainsi, il existe $b \in \mathbb{Z}$ tel que $da = nb$, d'où $a = nb/d$ et donc $\bar{a} = b \overline{n/d}$. On en déduit que $\bar{a} \in \langle \overline{n/d} \rangle$. On conclut que $H = \langle \overline{n/d} \rangle$ par inclusion et égalité des cardinaux.
3. Soit \bar{a} un élément d'ordre d , et donc $\#\langle \bar{a} \rangle = d$. Par la question 2 et l'exercice 2.1, on a $\langle \bar{a} \rangle = \langle \overline{n/d} \rangle \cong \mathbb{Z}/d\mathbb{Z}$. Or, par la question 1, il y a $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/d\mathbb{Z}$. Ainsi, il y a $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.

Posons $A_d := \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \#\langle \bar{a} \rangle = d\}$. Si $d \nmid n$ alors $A_d = \emptyset$ car l'ordre d'un élément divise n (théorème de LAGRANGE). Si $d \mid n$ alors $\#A_d = \varphi(d)$ (question 2). De plus,

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d \mid n} A_d,$$

d'où

$$n = \sum_{d \mid n} \#A_d = \sum_{d \mid n} \varphi(d).$$

2.3 Exercice 3.

1. *Montrer que le groupe $\mathbb{Z}/n\mathbb{Z}$ est simple si, et seulement si, n est premier.*
 2. *Soit G un groupe fini abélien. Montrer que G est simple si et seulement si $G \cong \mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier.*
1. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est commutatif. Ainsi, tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est distingué. On a donc que $\mathbb{Z}/n\mathbb{Z}$ est simple si, et seulement si, $\mathbb{Z}/n\mathbb{Z}$ ne possède pas de sous-groupes non triviaux. De plus, un entier n n'a que des diviseurs triviaux (1 ou n) si et seulement si n est premier. Et, avec le théorème de LAGRANGE, on sait que l'ordre de tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ divise n . D'où l'équivalence.

2. Le groupe G est commutatif. Ainsi, tout sous-groupe de G est distingué. On a donc que G est simple si, et seulement si, G ne possède pas de sous-groupes non triviaux. Ainsi, par le théorème de LAGRANGE, l'ordre du groupe G est premier.

2.4 Exercice 4.

Soit G un groupe et H un sous-groupe de G d'indice 2. Montrer que H est distingué dans G . Montrer que le résultat n'est pas vrai si on remplace 2 par 3.

Soit $g \in G \setminus H$. On a la partition $G = H \sqcup gH$. Ainsi gH est le complément de H dans G . Similairement, Hg est le complément de H dans G . Ainsi, on a $gH = Hg$.

Si $h \in H$, alors $hH = H = Hh$ car H est un sous-groupe contenant les éléments h et h^{-1} .

On en conclut, dans les deux cas, que $H \triangleleft G$.

Pour montrer que le résultat est faux en remplaçant 2 par 3, on considère $G := \mathfrak{S}_3$ et $H := \{\text{id}, (1\ 2)\}$ un sous-groupe de G . Le sous-groupe H a pour indice $[G : H] = |\mathfrak{S}_3|/|H| = 3$. Cependant, H n'est pas un sous-groupe distingué de G :

$$(1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (2\ 3) \notin H.$$

2.5 Exercice 5.

Soit p un nombre premier.

1. *Rappeler pourquoi le centre d'un p -groupe est non trivial.*
2. *Montrer que tout groupe d'ordre p^2 est abélien, classifier ces groupes.*
3. *Soit G un groupe d'ordre p^n . Montrer que G admet un sous-groupe distingué d'ordre p^k pour tout $k \in \llbracket 0, n \rrbracket$.*

1. Soit G un p -groupe non trivial. On fait agir G sur G par conjugaison. Ainsi, par la formule des classes, on a

$$p^n = \#G = \#Z(G) + \sum_{g \in \mathcal{R}} \underbrace{[G : C_G(g)]}_{p^{x_i} > 1},$$

où \mathcal{R} est un système de représentants des classes de conjugaisons de G contenant plus d'un élément.

On sait donc que $p \mid \sum_{g \in \mathcal{R}} [G : C_G(g)]$ et $p \mid \#G$, ce qui permet d'en déduire que $p \mid \#Z(G)$. D'où, $Z(G)$ n'est pas trivial.

2. Le centre de G est un sous-groupe, d'où par le théorème de LAGRANGE et par la question 1, on sait que l'ordre de $Z(G)$ est p ou p^2 .
 - ▷ Dans le cas où $Z(G)$ est d'ordre p^2 , on a $Z(G) = G$, d'où G abélien.
 - ▷ Supposons $\#Z(G) = p$. Soit $x \in G \setminus Z(G)$, et considérons le sous-groupe

$$Z(x) := \{g \in G \mid gx = xg\} \leq G.$$

En deux temps, montrons que $Z(G) \subsetneq Z(x) \subsetneq G$.

- On a l'inclusion $Z(G) \subseteq Z(x)$ mais cette inclusion est stricte car $x \in Z(x) \setminus Z(G)$.
- Montrons que $Z(x) \neq G$. Par l'absurde, si $Z(x) = G$, alors x commute avec tout élément de G , et donc $x \in Z(G)$, **absurde**.

Quel est l'ordre de $Z(x)$? C'est nécessairement p ou p^2 , mais dans chacun des cas, on arrive à une contradiction avec les inclusions strictes plus-haut. C'est **absurde**.

2.6 Exercice 6. Troisième théorème d'isomorphisme

Soit H un groupe et soient H et K des sous-groupes tels que $H \triangleleft G$ et $H \leq K$. On notera $\pi_H : G \rightarrow G/H$.

1. Montrer que le groupe $\pi_H(K)$ est distingué dans G/H si et seulement si K est distingué dans G .
2. Justifier que H est distingué dans K et que l'on a un isomorphisme $\pi_H(K) \cong K/H$.
3. On suppose K distingué dans G . On note $\pi_K : G \rightarrow G/K$ la projection canonique.
 - a) Montrer que π_K induit un unique morphisme de groupes $\bar{\pi}_K : G/H \rightarrow G/K$ tel que $\pi_K = \bar{\pi}_K \circ \pi_H$.
 - b) Montrer que le noyau de $\bar{\pi}_K$ est $\pi_H(K) \cong K/H$.
 - c) En déduire le troisième théorème d'isomorphisme.

1. On procède en deux temps.

Dans un premier temps, supposons que $K \triangleleft G$ et montrons que l'on a $\pi_H(K) \triangleleft G/H$. Soit $\bar{g} \in G/H$ et soit $g \in G$ un élément tel que $\pi_H(g) = \bar{g}$ qui existe par surjectivité de π_H . Alors,

$$\pi_H(K) = \pi_H(gHg^{-1}) = \bar{g} \pi_H(K) \bar{g}^{-1},$$

d'où $\pi_H(K) \triangleleft G/H$.

Dans un second temps, supposons

$$\forall \bar{g} \in G/H, \quad \bar{g} \pi_H(K) \bar{g}^{-1} = \pi_H(K).$$

Soit $g \in G$ et $k \in K$, et montrons que $gkg^{-1} \in K$. On sait que l'on a $\bar{g} = gH$ et $\pi_H(k) = kH$. Alors,

$$gkg^{-1}H \subseteq (gH)(kH)(g^{-1}H) = k'H \subseteq K,$$

pour un certain $k' \in K$ (on applique ici l'hypothèse). Ainsi, comme $e \in H$, on a en particulier $gkg^{-1} \in K$. On en déduit ainsi que $K \triangleleft G$.

2. Pour tout $k \in K$, on a que $kHk^{-1} = H$ car $k \in G$, on en déduit $H \triangleleft K$. Montrons que $\pi_H(K) \cong K/H$. On a même égalité de ces deux ensembles si l'on voit K/H comme l'ensemble des classes à gauches de H . En effet,

$$\pi_H(k) = kH \quad \text{d'où} \quad \pi_H(K) = \{kH \mid k \in K\},$$

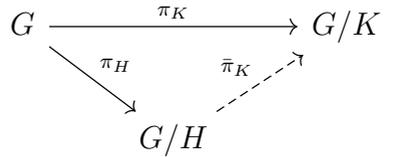
– 24/54 –

et

$$K/H = \{kH \mid k \in K\}.$$

On a donc l'égalité.

3. a) On factorise par le quotient :



qui est possible car $K = \ker \pi_K \supseteq H$. Le morphisme $\bar{\pi}_K : G/H \rightarrow G/K$ est l'unique morphisme faisant commuter le diagramme ci-dessus.

b) Par construction,

$$\begin{aligned}
 \ker \bar{\pi}_K &= \{\bar{g} \in G/H \mid \pi_K(g) = K\} \\
 &= \{\pi_H(g) \mid g \in \ker \pi_K\} \\
 &= \pi_H(\ker \pi_K) = \pi_H(K) \cong_{\mathbb{Q}2} K/H.
 \end{aligned}$$

c) Appliquons le premier théorème d'isomorphisme à $\bar{\pi}_K$, qui est surjectif :

$$(G/H)/(\ker \bar{\pi}_K) = (G/H)/\pi_H(K) \cong \text{im } \bar{\pi}_K = G/K,$$

c'est le troisième théorème d'isomorphisme.

2.7 Exercice 7. Sous-groupe d'un quotient

Soit G un groupe, et H un sous-groupe distingué de G . On note la projection canonique $\pi_H : G \rightarrow G/H$.

1. a) Soit K un sous-groupe de G . Montrer $\pi_H^{-1}(\pi_H(K)) = KH$.
 b) En déduire que π_H induit une bijection croissante entre les sous-groupes de G/H et les sous-groupes de G contenant H .
2. Montrer que les sous-groupes distingués de G/H sont en correspondance avec les sous-groupes distingués de G contenant H .

- 3.** Montrer que la correspondance précédente préserve l'indice : si K est un sous-groupe de G d'indice fini contenant H , alors on a $[G : K] = [G/H, \pi_H(K)]$.

1. a) On a

$$\begin{aligned} \pi_H^{-1}(\pi_H(K)) &= \{g \in G \mid \pi_H(g) \in \pi_H(K)\} \\ &= \{g \in H \mid gH = kH \text{ avec } k \in K\} \\ &= \bigcup_{k \in K} kH \\ &= \{kh \mid k \in K, h \in H\} \\ &= KH. \end{aligned}$$

b) L'image directe par π_H envoie un sous-groupe de G contenant H sur sous-groupe de G/H . De plus, l'image réciproque par π_H envoie un sous-groupe de G/H sur un sous-groupe de G contenant H . Montrons la bijection puis la croissance.

- ▷ Si $\pi_H(K_1) = \pi_H(K_2)$ où K_1, K_2 sont deux sous-groupes de G contenant H alors

$$K_1 = K_1H = \pi_H^{-1}(\pi_H(K_1)) = \pi_H^{-1}(\pi_H(K_2)) = K_2H = K_2.$$

D'où l'injectivité.

- ▷ On sait déjà que $\pi_H : G \rightarrow G/H$ est surjective, alors l'image directe $\tilde{\pi}_H : S_G \rightarrow S_{G/H}$ où S_G est l'ensemble des sous-groupes de G .
- ▷ L'image directe et l'image réciproque par π_H est une application croissante.

2. On procède en deux temps.

- ▷ Soit $L \triangleleft G/H$. Pour tout $g \in G$ et tout $x \in \pi_H^{-1}(L)$, on a

$$\pi_H(gxg^{-1}) = (gxg^{-1})H = (gH)(xH)(gH)^{-1} \in L,$$

car L est distingué dans G/H . Ainsi $xgx^{-1} \in \pi_H^{-1}(L)$ et donc $\pi_H^{-1}(L)$ est distingué dans G .

- ▷ Soit $K \triangleleft G$ un sous-groupe distingué contenant H . Pour tout $xH \in G/H$ et tout $kH \in \pi_H(K)$ avec $k \in K$, on a

$$(xH)(kH)(xH)^{-1} = (xkx^{-1})H.$$

Comme $K \triangleleft G$, on a $xkx^{-1} \in K$ d'où $(xkx^{-1})H \in \pi_H(K)$. On en déduit que $\pi_H(K)$ est distingué dans le groupe quotient G/H .

3.

2.8 Exercice 8. Combinatoire algébrique

Soit \mathbb{k} un corps fini à q éléments et $n \in \mathbb{N}^*$. On définit $\text{PGL}_n(\mathbb{k})$ comme le quotient $\text{GL}_n(\mathbb{k})/\mathbb{k}^\times$, où \mathbb{k}^\times correspond au sous-groupe distingué formé de la forme λI_n avec $\lambda \in \mathbb{k} \setminus \{0\}$. On considère l'action de $\text{GL}_n(\mathbb{k})$ sur l'ensemble des droites vectorielles de \mathbb{k}^n .

1. Déterminer le cardinal des groupes finis $\text{GL}_n(\mathbb{k})$, $\text{SL}_n(\mathbb{k})$ et $\text{PGL}_n(\mathbb{k})$.
Indication : compter les bases de \mathbb{k}^n .
2. On prend désormais $n = 2$.
 - a) Montrer que le nombre de droites vectorielles de \mathbb{k}^2 est égal à $q + 1$.
 - b) En déduire qu'il existe un morphisme de groupes injectif

$$\text{PGL}_2(\mathbb{k}) \hookrightarrow \mathfrak{S}_{q+1}.$$

3. Montrer que $\text{GL}_2(\mathbb{F}_2) = \text{SL}_2(\mathbb{F}_2) = \text{PGL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.
4. Montrer que $\text{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$.

1. L'application

$$\begin{aligned} \text{GL}_n(\mathbb{k}) &\longrightarrow \{\text{bases de } \mathbb{k}^n\} \\ (C_1 \ C_2 \ \cdots \ C_n) &\longmapsto (C_1, \dots, C_n) \end{aligned}$$

est une bijection. Construisons une base de \mathbb{k}^n :

- (1) On choisit le premier vecteur C_1 dans $\mathbb{k}^n \setminus \{0\}$, on a donc $q^n - 1$ choix.

- (2) On choisit le second vecteur C_2 dans $\mathbb{k}^n \setminus \text{vect}(C_1)$, on a donc $q^n - q$ choix.
- (3) On choisit le troisième vecteur C_3 dans $\mathbb{k}^n \setminus \text{vect}(C_1, C_2)$, on a donc $q^n - q^2$ choix.
- (4) *Et cetera.*

D'où,

$$\#\text{GL}_n(\mathbb{k}) = \prod_{i=0}^{n-1} (q^n - q^i).$$

L'application $\det : \text{GL}_n(\mathbb{k}) \rightarrow \mathbb{k}^\times$ est un morphisme de groupes surjectif. De plus, $\ker \det = \text{SL}_n(\mathbb{k})$. On a ainsi, par le premier théorème d'isomorphisme,

$$\text{GL}_n(\mathbb{k})/\text{SL}_n(\mathbb{k}) \cong \mathbb{k}^\times.$$

Ainsi,

$$\#\text{SL}_n(\mathbb{k}) = \frac{\#\text{GL}_n(\mathbb{k})}{\#\mathbb{k}^\times} = \frac{\prod_{i=0}^{n-1} (q^n - q^i)}{q - 1}.$$

Finalement, on a $\text{PGL}_n(\mathbb{k}) := \text{GL}_n(\mathbb{k})/\mathbb{k}^\times$ d'où

$$\#\text{PGL}_n(\mathbb{k}) = \frac{\prod_{i=0}^{n-1} (q^n - q^i)}{q - 1}.$$

2. a)

2.9 Exercice 9. Formule de Burnside

Soit G un groupe fini agissant sur un ensemble fini X . On note N le nombre d'orbites de l'action.

1. Soit $Y := \{(g, x) \in G \times X \mid g \cdot x = x\}$. Interpréter le cardinal de Y comme somme sur les éléments de X d'une part, et de G d'autre part.
2. En décomposant X en union d'orbites, montrer la formule de BURNSIDE :

$$N = \frac{1}{\#G} \sum_{g \in G} \#\text{Fix}(G).$$

– 28/54 –

3. Soit n un entier. Quel est le nombre moyen de points fixes des éléments de \mathfrak{S}_n pour l'action naturelle sur $\llbracket 1, n \rrbracket$.
4. On suppose que G agit transitivement sur X et que X contient au moins deux éléments. Montrer qu'il existe un $g \in G$ agissant sans point fixe.
5. En déduire qu'un groupe fini n'est jamais l'union des conjugués d'un sous-groupe strict.

2.10 Exercice 10. Automorphismes intérieurs.

Soit G un groupe. Pour $g \in G$, on note $\phi_g : G \rightarrow G$ la fonction définie par $h \mapsto ghg^{-1}$. On note $\text{Int}(G)$ l'ensemble des ϕ_g pour $g \in G$.

1. Soit $g \in G$, montrer que ϕ_g est un automorphisme de groupes.
2. Montrer que la fonction $\phi : G \rightarrow \text{Int}(G)$ qui à g associe ϕ_g est un morphisme de groupes.
3. Montrer l'isomorphisme $G/\text{Z}(G) \cong \text{Int}(G)$ où $\text{Z}(G)$ est le centre du groupe G .
4. (Plus difficile) Montrer que si le groupe des automorphismes $\text{Aut}(G)$ de G est cyclique alors G est abélien.
5. (Aussi difficile) Supposons que $\text{Aut}(G)$ est trivial. Démontrer que tous les éléments de G sont d'ordre au plus 2, puis que G est soit trivial, soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

2.11 Exercice 11.

Soit $n \in \mathbb{N}$ et $k \in \llbracket 0, n \rrbracket$. On note $\wp_k(\llbracket 1, n \rrbracket)$ l'ensemble des parties à k éléments de $\llbracket 1, n \rrbracket$.

1. Montrer que \mathfrak{S}_n agit naturellement sur $\wp_k(\llbracket 1, n \rrbracket)$.
2. Justifier que cette action est transitive.
3. Calculer le stabilisateur de $\llbracket 1, k \rrbracket \in \wp_k(\llbracket 1, n \rrbracket)$.
4. En appliquant la formule orbite-stabilisateur, retrouver la valeur de $\binom{n}{k}$.

1. Posons l'action de groupes :

$$\forall \sigma \in \mathfrak{S}_n, \forall i \in \wp_k(\llbracket 1, n \rrbracket), \quad \sigma \cdot I = \sigma(I) = \{\sigma(i) \mid i \in I\}.$$

La partie $\sigma(I)$ contient k éléments de $\llbracket 1, n \rrbracket$. Et, de plus, l'application $\sigma \mapsto (I \mapsto \sigma(I))$ est

3 Actions de groupes et théorèmes de Sylow

4 Groupe symétrique

Sommaire.

4.1 Exercice 1.	32
4.2 Exercice 2. <i>Générateurs de \mathfrak{A}_n</i>	32
4.3 Exercice 3.	33

4.1 Exercice 1.

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix} \in \mathfrak{S}_9$. Déterminer sa décomposition canonique en produit de cycles disjoints, son ordre, sa signature, une décomposition en produit de transposition ainsi que σ^{100} .

On a $\sigma = (1 \ 4 \ 7 \ 8)(2 \ 6 \ 5)(3 \ 9)$. Son ordre est le PPCM des ordres précédent, c'est donc 12. Sa signature est $(-1) \times 1 \times (-1) = 1$. On décompose en produit de transposition chaque cycle et on conclut. On calcule

$$\sigma^{100} = (1 \ 4 \ 7 \ 8)^{100} (2 \ 6 \ 5)^{100} (3 \ 9)^{100},$$

car les cycles à supports disjoints commutent, et donc

$$\sigma^{100} = (2 \ 6 \ 5).$$

4.2 Exercice 2. *Générateurs de \mathfrak{A}_n*

Soit $n \geq 3$.

1. Rappeler pourquoi \mathfrak{A}_n est engendré par les 3-cycles.

2. Démontrer que \mathfrak{A}_n est engendré par les carrés d'éléments de \mathfrak{S}_n . Est-ce que tout élément de \mathfrak{A}_n est un carré dans \mathfrak{S}_n ?
 3. Démontrer que pour $n \geq 5$, \mathfrak{A}_n est engendré par les bitranspositions.
 4. Démontrer que \mathfrak{A}_n est engendré par les 3-cycles de la forme $(1\ 2\ i)$ pour $i \in \llbracket 3, n \rrbracket$.
 5. En déduire que si $n \geq 5$ est impair, alors \mathfrak{A}_n est engendré par les permutations $(1\ 2\ 3)$ et $(3\ 4\ \dots\ n)$ et que si $n \geq 4$ est pair, alors \mathfrak{A}_n est engendré par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \dots\ n)$.
1. On utilise le fait que tout $\sigma \in \mathfrak{A}_n$ se décompose comme produit d'un nombre pair de transpositions. Puis, on utilise les égalités
 - ▷ $(i\ j)(i\ k) = (i\ j\ k)$,
 - ▷ $(i\ j)(i\ j) = \text{id}$,
 - ▷ $(i\ j)(k\ \ell) = (i\ \ell\ k)(i\ j\ k)$,
 pour déterminer un produit de 3-cycles égal à σ .
 2. On utilise la question précédente. Soit $(a\ b\ c)$ un 3-cycle. On a alors $(a\ b\ c)^4 = (a\ b\ c)$, et donc $\sigma = (a\ b\ c)^2$. Ceci permet d'en déduire que les carrés de permutations engendrent \mathfrak{A}_n .

4.3 Exercice 3.

Soit $n \leq 5$.

5 Quotient et dualité

Sommaire.

5.1 Exercice 1.	34
5.2 Exercice 2. <i>Théorèmes d'isomorphismes</i>	34
5.3 Exercice 3. <i>Changement de base duale</i>	35

5.1 Exercice 1.

Donner un exemple de \mathbb{k} -espace vectoriel E et de sous-espace vectoriel F de E où

1. $\dim F$ est finie et $\dim(E/F)$ est infinie ;
2. $\dim F$ est infinie et $\dim(E/F)$ est finie ;
3. $\dim F$ est infinie et $\dim(E/F)$ est infinie.

1. Considérons $E = \mathbb{R}^2$ et $F = \{(0, 0)\}$.
2. Considérons $E = \mathbb{R}^2$ et $F = \mathbb{R}^2$.
3. Considérons \mathbb{R}^2 et $F = \mathbb{R} \times \{0\}$.

5.2 Exercice 2. *Théorèmes d'isomorphismes*

Soient E un \mathbb{k} -espace vectoriel, et F et G deux sous-espaces vectoriels de E . On note $\pi : E \rightarrow E/F$ la projection canonique.

1. Montrer que l'application $G \mapsto \pi(G)$ induit une bijection croissante entre l'ensemble des sous-espaces vectoriels de E contenant F et l'ensemble des sous-espaces vectoriels de E/F . Quelle est sa bijection réciproque ?
2. Construire un isomorphisme entre $F/(F \cap G) = (F + G)/G$.

3. On suppose $F \subseteq G$. Montrer que G/F s'identifie à un sous-espace vectoriel de E/F et construire un isomorphisme entre $(E/F)/(G/F)$ et E/G .

5.3 Exercice 3. *Changement de base duale*

Soit E un \mathbb{k} -espace vectoriel de dimension finie. Soient $\mathbf{e} = (e_i)_{i \in \llbracket 1, n \rrbracket}$ et $\mathbf{f} = (f_i)_{i \in \llbracket 1, n \rrbracket}$ deux bases de E , et $\mathbf{e}^* = (e_i^*)_{i \in \llbracket 1, n \rrbracket}$ et $\mathbf{f}^* = (f_i^*)_{i \in \llbracket 1, n \rrbracket}$ leurs bases duales respectives. Soit $A = (a_{i,j})_{i,j}$ la matrice de passage de \mathbf{e} à \mathbf{f} .

1. Pour $j \in \llbracket 1, n \rrbracket$, on écrit $e_j^* = \sum_{i=1}^n \alpha_{i,j} f_i^*$ avec $\alpha_{i,j} \in \mathbb{k}$, pour tout $1 \leq i, j \leq n$. Déterminer $A' = (\alpha_{i,j})_{i,j}$ en fonction de A .
 2. En déduire la matrice de passage de \mathbf{e}^* à \mathbf{f}^* en fonction de A .
- 1.

6 Transposition, orthogonalité, et formes bilinéaires

7 Formes quadratiques

8 Formes quadratiques – épisode 2

9 Produits tensoriels

Sommaire.

9.1 Exercice 1.	39
9.2 Exercice 2. <i>Isomorphismes canoniques</i> . .	41

9.1 Exercice 1.

Soient E, F et G des espaces vectoriels de dimension finie supérieure à 2.

1. Donner un élément de $E \otimes F$ qui n'est pas un tenseur simple.
2. Donner un exemple d'espaces vectoriels E, F et G et d'application linéaire $h : E \otimes F \rightarrow G$ telle que $h(x \otimes y) \neq 0$ pour tout $x \in E \setminus \{0\}$ et $y \in F \setminus \{0\}$ mais qui n'est pas injective.
3. Que se passe-t-il si E ou F est de dimension 1 ?
4. Soient $f : E \rightarrow G$ et $g : F \rightarrow G$ des applications linéaires. Existe-t-il une application linéaire $\varphi : E \otimes F \rightarrow G$ telle que pour tout $x \in E$ et $y \in F$ on ait

$$\varphi(x \otimes y) = f(x) + f(y).$$

1. Considérons (e_1, e_2) une famille libre de E et (f_1, f_2) une famille libre de F . On considère

$$z = e_1 \otimes f_1 + e_2 \otimes f_2 \in E \otimes F.$$

L'élément z n'est pas simple. Par l'absurde, supposons le simple, et on écrit que $z = x \otimes y$ avec $x \in E$ et $y \in F$. On complète les familles (e_1, e_2) et (f_1, f_2) en deux bases $(e_i)_{i \in \llbracket 1, n \rrbracket}$ et $(f_j)_{j \in \llbracket 1, m \rrbracket}$ de

E et F respectivement. On écrit, avec les bases, $x = \sum_{i=1}^n \lambda_i x_i$ puis $y = \sum_{j=1}^m \mu_j f_j$. Alors $x \otimes y = \sum_{i,j} \lambda_i \mu_j (e_i \otimes f_j) = z$. Ceci permet d'en déduire que

$$\lambda_i \mu_j = \begin{cases} 1 & \text{si } i = j = 1 \text{ ou } i = j = 2 \\ 0 & \text{sinon.} \end{cases}$$

D'où, $\lambda_1 \mu_2 = 0$ et donc $\lambda_1 = 0$ ou $\mu_2 = 0$. Cependant, $\lambda_1 \mu_1 = \lambda_2 \mu_2 = 1$, ce qui est **absurde**. Ainsi z n'est pas un tenseur simple.

2. Considérons $\mathbb{k} = \mathbb{R}$ et $E = F = \mathbb{C}$ vu comme un \mathbb{k} -espace vectoriel de dimension 2. On pose l'application

$$\begin{aligned} \varphi : \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ (x, y) &\longmapsto xy, \end{aligned}$$

qui est bilinéaire. Ainsi, par propriété universelle, φ induit une unique application linéaire

$$\begin{aligned} h : \mathbb{C} \otimes \mathbb{C} &\longrightarrow \mathbb{C} \\ x \otimes y &\longmapsto xy. \end{aligned}$$

Alors, pour tout $x, y \in \mathbb{C} \setminus \{0\}$, alors $h(x \otimes y) = xy \neq 0$. Or, on a $h(1 \otimes i) = h(i \otimes i)$ et $1 \otimes i \neq i \otimes 1$ donne la non injectivité (car $(1 \otimes 1, i \otimes 1, 1 \otimes i, i \otimes i)$ forme une base de $\mathbb{C} \otimes \mathbb{C}$).

3. Si $\dim E = 1$ on écrit $E = \text{vect } e$. Soit $(f_i)_{i \in \llbracket 1, n \rrbracket}$ une base de F . Une base de $E \otimes F$ est $(e \otimes f_1, \dots, e \otimes f_n)$, et

$$\sum_{j=1}^n \lambda_j (e \otimes f_j) = e \otimes \left(\sum_{j=1}^n \lambda_j f_j \right).$$

Tout élément de $E \otimes F$ est donc un tenseur simple ! Ainsi, l'application

$$\begin{aligned} F &\longrightarrow E \otimes F \\ y &\longmapsto e \otimes y \end{aligned}$$

est un isomorphisme.

4. Montrons que l'application φ existe et est nécessairement nulle. On a, pour tout $x \in E$ et $y \in F$

$$f(x) = f(x) + 0 = \varphi(x \otimes 0) = 0 = \varphi(0 \otimes y) = g(y) = 0.$$

D'où, $f = 0$ et $g = 0$.

9.2 Exercice 2. *Isomorphismes canoniques*

Soient E et F deux espaces vectoriels de dimension finie.

1. a) Montrer que l'application $E \times F \rightarrow F \otimes E$ donnée par $(x, y) \mapsto y \otimes x$ est bilinéaire. En déduire qu'il existe une unique application linéaire

$$f : E \otimes F \rightarrow F \otimes E$$

qui vérifie $f(x \otimes y) = y \otimes x$, pour tout $x \in E$ et tout $y \in F$.

On construit de même une application linéaire

$$g : F \otimes E \rightarrow E \otimes F$$

telle que $g(y \otimes x) = x \otimes y$.

- b) Montrer que $f \circ g = \text{id}_{F \otimes E}$ et $g \circ f = \text{id}_{E \otimes F}$. En particulier, f et g réalisent des isomorphismes entre $E \otimes F$ et $F \otimes E$.

2.

1. a) L'application

$$\begin{aligned} \varphi : E \times F &\longrightarrow F \otimes E \\ (x, y) &\longmapsto y \otimes x \end{aligned}$$

est linéaire à gauche car $\cdot \otimes \cdot$ est linéaire à droite, et φ est linéaire à droite car $\cdot \otimes \cdot$ est linéaire à gauche. Par propriété universelle, on sait que φ induit une unique application linéaire $f : E \otimes F \rightarrow F \otimes E$.

- b)** Soit $z \in E \otimes F$. On pose $z = \sum_{i=1}^n (x_i \otimes y_i)$ avec $x_i \in E$ et $y_j \in F$. Alors,

$$\begin{aligned} g(f(z)) &= g\left(f\left(\sum_{i=1}^n x_i \otimes y_i\right)\right) \\ &= \sum_{i=1}^n g(f(x_i \otimes y_i)) \\ &= \sum_{i=1}^n g(y_i \otimes x_i) \\ &= \sum_{i=1}^n x_i \otimes y_i \\ &= z. \end{aligned}$$

D'où, $g \circ f = \text{id}_{E \otimes F}$. De même, $f \circ g = \text{id}_{F \otimes E}$.

- 2.** Pour $f \in E^*$ et $g \in F^*$, l'application

$$\begin{aligned} E \times F &\longrightarrow \mathbb{k} \\ (x, y) &\longmapsto f(x) g(y) \end{aligned}$$

est bilinéaire. Ainsi, par propriété universelle, elle induit une application linéaire

$$\begin{aligned} P(f, g) : E \otimes F &\longrightarrow \mathbb{k} \\ x \otimes y &\longmapsto f(x) g(y). \end{aligned}$$

L'application

$$\begin{aligned} P : E^* \times F^* &\longrightarrow (E \otimes F)^* \\ (f, g) &\longmapsto P(f, g) \end{aligned}$$

est bilinéaire donc, par propriété universelle, elle induit une unique application linéaire

$$\begin{aligned} \gamma : E^* \otimes F^* &\longrightarrow (E \otimes F)^* \\ f \otimes g &\longmapsto P(f, g). \end{aligned}$$

De plus, soit $(e_i)_i$ une base de E et $(f_j)_j$ une base de F . Une base de $(E \otimes F)^*$ est donnée par $((e_i \otimes f_j)^*)_{i,j}$. On vérifie que

$$\gamma(e_i^* \otimes f_j^*) = (e_i \otimes f_j)^*$$

par

$$\gamma(e_i^* \otimes f_j^*)(e_k \otimes f_\ell) = P(e_i^*, f_j^*)(e_i \otimes f_\ell) = e_i^*(e_k) \times f_j^*(f_\ell) = \delta_{i,k} \times \delta_{j,\ell}.$$

Ainsi γ est surjective. On conclut par égalité des dimensions :

$$\dim(E^* \otimes F^*) = \dim(E^*) \dim(F^*) = \dim(E) \dim(F) = \dim(E \otimes F) = \dim((E \otimes F)^*).$$

D'où, γ est un isomorphisme.

3. L'application

$$\begin{aligned} E^* \times F &\longrightarrow \text{Hom}(E, F) \\ (\lambda, y) &\longmapsto (x \mapsto \lambda(x)y) \end{aligned}$$

est bilinéaire, donc par propriété universelle, elle induit Φ .

Une base de $\text{Hom}(E, F)$ est donnée par les $h_{i,j} : x \mapsto e_i^*(x)f_j$. Or, $h_{i,j} = \Phi(e_i^*, f_j)$, donc Φ est surjective.

Enfin, on a

$$\dim(E^* \otimes F) = (\dim E^*)(\dim F) = (\dim E)(\dim F) = \dim(\text{Hom}(E, F)).$$

D'où, Φ est un isomorphisme.

10 Représentation de groupes.

11 Théorie des caractères.

Sommaire.

11.1 Exercice 1. <i>Rappels de cours</i>	45
11.2 Exercice 2. <i>Représentation d'une action de groupe</i>	46

11.1 Exercice 1. *Rappels de cours*

Montrer que :

1. une représentation (V, ρ) est irréductible si, et seulement si on a $\langle \chi_V, \chi_V \rangle = 1$;
2. deux représentations (V, ρ) et (V', ρ') sont isomorphes si, et seulement si $\chi_V = \chi_{V'}$.

1. On procède en deux temps.

- ▷ « \implies ». Si V est irréductible alors, par le lemme de Schur, on a $\dim \text{Hom}_G(V, V) = 1$ et donc

$$\langle \chi_V, \chi_V \rangle = \dim \text{Hom}_G(V, V) = 1$$

- ▷ « \impliedby ». Si on écrit $V = \bigoplus_{k=1}^r W_k^{n_k}$ où W_k est une représentation irréductible, deux) deux non isomorphe, et avec $n_k \geq 1$. Ainsi,

$$\langle \chi_V, \chi_V \rangle = \left\langle \chi_V, \sum_{k=1}^r n_k \chi_{W_k} \right\rangle = \sum_{k=1}^r n_k \langle \chi_V, \chi_{W_k} \rangle = \sum_{k=1}^r n_k^2.$$

Or, $\langle \chi_V, \chi_V \rangle = 1$ donc $\sum_{k=1}^r n_k^2 = 1$ avec $n_k \geq 1$. On en déduit que $r = 1$ et $n_1 = 1$. Ainsi V est irréductible.

2. Soient (V, ρ) et (V', ρ') deux représentations de G . On décompose $V = \sum_{W_k \in \mathcal{J}_G} W_k^{n_k}$ avec les W_k irréductibles, et deux à deux non isomorphes. Or, $\langle \chi_V, \chi_{W_k} \rangle = n_k$.

▷ « \implies ». Si $(V, \rho) \cong (V', \rho')$, alors il existe $u \in \text{GL}(V, W)$ tel que pour tout $g \in G$,

$$\rho'(g) = u \circ \rho(g) \circ u^{-1}.$$

Ainsi, $\chi_V(g) = \text{Tr}(\rho(g)) = \text{Tr}(\rho'(g)) = \chi_{V'}(g)$. On en conclut $\chi_V = \chi_{V'}$.

▷ « \impliedby ». Si $\chi_V = \chi_{V'}$ alors $\langle \chi_{V'}, \chi_{W_k} \rangle = n_k$ et donc

$$V' \cong \bigoplus_{W_k \in \mathcal{J}_G} W_k^{n_k} = V.$$

11.2 Exercice 2. Représentation d'une action de groupe

Soit G un groupe fini agissant sur un ensemble fini X . On note également $\mathcal{O}_1, \dots, \mathcal{O}_k$ les orbites de X sous l'action de G . On définit la représentation associée à cette action de la manière suivante : on pose

$$V_X := \bigoplus_{x \in X} \mathbb{C}e_x,$$

et $g \in G$ agit sur V_X par

$$g \cdot \left(\sum_{x \in X} a_x e_x \right) := \sum_{x \in X} a_x e_{g \cdot x}.$$

1. Montrer que $\chi_{V_X}(g) = \#\{x \in X \mid g \cdot x = x\}$.
2. a) Montrer que V_X^G est engendré par les $e_{\mathcal{O}_i} := \sum_{x \in \mathcal{O}_i} e_x$.
 b) En déduire que le nombre d'orbite de X est égal à $\dim(V_X^G)$.

On suppose que l'action de G est transitive. La représentation se décompose donc en $\mathbf{1} \oplus H$ où H ne contient pas de sous-représentation isomorphe à la représentation triviale.

3. On fait agir G sur $X \times X$ de manière diagonale. Montrer que $\chi_{V_{X \times X}} = \chi_{V_X}$.
4. On dit que G agit deux fois transitivement si $\#X \geq 2$ et pour tous couples $(x_1, y_1), (x_2, y_2) \in X \times X$ avec $x_1 \neq y_1$ et $x_2 \neq y_2$ il existe $g \in G$ tel que $g \cdot (x_1, y_1) = (x_2, y_2)$.

Montrer que G agit deux fois transitivement si et seulement si l'action $G \curvearrowright X \times X$ a deux orbites.

5. Montrer que G agit deux fois transitivement si et seulement si $\langle \chi_{V_X}^2, \mathbb{1} \rangle = 2$ si et seulement si H est irréductible.

Applications :

6. On prend l'action naturelle de \mathfrak{S}_n sur $\llbracket 1, n \rrbracket$.
 - a) Retrouver que V_X se décompose en une somme de deux représentations irréductibles $\mathbb{1} \oplus H$.
 - b) Calculer le caractère de la représentation standard.
7. On prend l'action par translation de G sur lui-même. Calculer le caractère de la représentation régulière.
1. On considère la base duale $(e_x^*)_{x \in X}$ de $(e_x)_{x \in X}$. Alors, pour tout $g \in G$, on a

$$\begin{aligned}
 \chi_{V_X}(g) &= \text{Tr}(\rho_X(g)) \\
 &= \sum_{x \in X} e_x^*(\rho_X(g)(e_x)) \\
 &= \sum_{x \in X} e_x^*(e_{g \cdot x}) \\
 &= \#\{x \in X \mid g \cdot x = x\}.
 \end{aligned}$$

2. a) On sait que

$$V_X^G = \{v \in V_X \mid \forall g \in G, g \cdot v = v\}.$$

Or,

$$g \cdot e_{\theta_i} = \sum_{x \in \theta_i} e_{g \cdot x} = \sum_{x \in \theta_i} e_x = e_{\theta_i},$$

donc $e_{\mathcal{O}_i} \in V_X^G$, et donc $\text{vect}((e_{\mathcal{O}_i})_i) \subseteq V_X^G$. Réciproquement, soit $v \in V_X^G$. On écrit $v = \sum_{x \in X} \lambda_x e_x$. Alors, pour tout élément $g \in G$, $g \cdot x = x$ donc $\lambda_{g \cdot x} = \lambda_x$ pour tout $x \in X$. Autrement dit, si $x, y \in \mathcal{O}_i$ alors $\lambda_x = \lambda_y =: \lambda_{\mathcal{O}_i}$. Donc

$$v = \sum_{x \in X} \lambda_x e_x = \sum_{i=1}^k \lambda_{\mathcal{O}_i} \sum_{x \in \mathcal{O}_i} e_x = \sum_{i=1}^k \lambda_{\mathcal{O}_i} e_{\mathcal{O}_i} \in \text{vect}((e_{\mathcal{O}_i})_i),$$

d'où l'inclusion réciproque et donc l'égalité.

- b)** Les $(e_{\mathcal{O}_i})$ forment une famille libre car les (e_i) le sont et car les \mathcal{O}_i forment une partition de X . Ainsi,

$$\dim(V_X^G) = \dim \text{vect}((e_{\mathcal{O}_i})_i) = k.$$

- 3.** On fait agir G sur $X \times X$ par *action diagonale*, c'est à dire que

$$g \cdot (x, y) := (g \cdot x, g \cdot y).$$

Ainsi, pour $g \in G$, par combinatoire,

$$\begin{aligned} \chi_{V_{X \times X}}(g) &= \#\{(x, y) \in X \times X \mid g \cdot (x, y) = (x, y)\} \\ &= (\#\{x \in X \mid g \cdot x = x\})^2 \\ &= (\chi_{V_X}(g))^2. \end{aligned}$$

- 4.** Soit $D := \{(x, x) \mid x \in X\}$. C'est une orbite de l'action de G sur $X \times X$ par transitivité de l'action $G \curvearrowright X$. Ainsi, on a la chaîne d'équivalences suivante :

$G \curvearrowright X \times X$ admet deux orbites



$(X \times X) \setminus D$ est une orbite



$$\forall x_1 \neq y_1, x_2 \neq y_2, \exists g \in G, g \cdot (x_1, x_2) = (x_2, y_2),$$

d'où l'équivalence.

5. On ré-écrit les propriétés étudiées :

- (i) G agit deux fois transitivement sur X ;
- (ii) $\langle \chi_{V_X}^2, \mathbf{1} \rangle = 2$;
- (iii) H irréductible.

▷ « (i) \implies (ii) »

$$\begin{aligned} \langle \chi_{V_X}^2, \mathbf{1} \rangle &= \langle \chi_{V_{X \times X}}, \mathbf{1} \rangle = \frac{1}{G} \sum_{g \in G} \overline{\chi_{V_X}(g)} \\ &= \overline{\dim(V_{X \times X}^G)} = \dim(V_{X \times X}^G). \end{aligned}$$

12 Table de caractères.

Sommaire.

12.1 Exercice 1. <i>Caractères linéaires</i>	50
12.2 Exercice 2. <i>Certaines propriétés des représentations de \mathfrak{S}_n</i>	51
12.3 Exercice 3. <i>Table de caractères de \mathfrak{A}_4</i>	51
12.4 Exercice 4. <i>Tables de caractères de D_8 et H_8</i>	53

12.1 Exercice 1. *Caractères linéaires*

Soit G un groupe fini.

1. Si G est abélien, montrer qu'il admet $\#G$ représentations de degré 1 à isomorphisme près.
2. En déduire que, dans le cas général, il en admet $[G : D(G)]$.

1. On sait que G est abélien. Alors, toutes les représentations irréductibles de G sont de degré 1. Ainsi,

$$\#G = \sum_{V \text{ irréductible}} (\dim V)^2 = \#\{\text{représentations irréductibles}\}.$$

Justifions le « toutes les représentations irréductibles de G sont de degré 1 ». Soit (V, ρ) une représentation irréductible de G . Alors, pour tout $g, h \in G$ alors $\rho(g)\rho(h) = \rho(h)\rho(g)$ et ainsi $\rho(g)$ et $\rho(h)$ sont diagonalisables. Donc elles sont co-diagonalisable. Alors il existe une base \mathfrak{B} de V qui co-diagonalise $\rho(g)$ et donc le premier vecteur de \mathfrak{B} engendre une droite propre D pour chaque $\rho(g)$. Et, D est donc stable par tous les $\rho(g)$, c'est donc

une sous-représentation de V . Par irréductibilité de V , on a $D = V$ et donc $\dim V = 1$.

- Le dual de G , noté G^* , est l'ensemble des caractères linéaires. On a vu dans le DM n°1 que $G^* \cong (G^{\text{ab}})^*$, où $G^{\text{ab}} := G/D(G)$. Ainsi, d'après la question 1, on sait que G^{ab} admet exactement $|G^{\text{ab}}|$ caractères linéaires. D'où, $|(G^{\text{ab}})^*| = |G^{\text{ab}}|$. On en conclut que

$$|G^*| = [G : D(G)].$$

12.2 Exercice 2. Certaines propriétés des représentations de \mathfrak{S}_n .

Soit $n \geq 2$ un entier.

- Soit $\sigma \in \mathfrak{S}_n$. Justifier que σ et σ^{-1} sont conjuguées dans \mathfrak{S}_n .
- En déduire que la table de caractère de \mathfrak{S}_n est à valeurs réelles.

Remarque : On peut même montrer que la table de caractère de \mathfrak{S}_n est toujours à valeurs entières, mais cela nécessite des arguments de théorie des corps du cours d'Algèbre 2.

- La classe de conjugaison de σ est déterminée par les longueurs des cycles apparaissant dans la décomposition en cycles à supports disjoints (*i.e.* le **type**). L'inverse d'un p -cycle est un p -cycle par tout $p \in \llbracket 2, n \rrbracket$ donc σ et σ^{-1} ont même type. On en conclut que σ et σ^{-1} sont conjugués.
- Pour tout caractère χ , pour toute permutation $\sigma \in \mathfrak{S}_n$, on a

$$\chi(\sigma) = \overline{\chi(\sigma^{-1})} = \overline{\chi(\sigma)},$$

car χ est constant sur les classes de conjugaisons. Ainsi, $\chi(\sigma) \in \mathbb{R}$ et la table de caractères de \mathfrak{S}_n est réelle.

12.3 Exercice 3. Table de caractères de \mathfrak{A}_4 .

- Montrer que \mathfrak{A}_4 a 4 classes de conjugaison : l'identité, la classe de $(1\ 2\ 3)$, la classe de $(1\ 3\ 2)$, et les doubles transpositions.

2. Montrer que le groupe dérivé de \mathfrak{A}_4 est le sous-groupe des doubles transpositions, et en déduire 3 caractères linéaires de \mathfrak{A}_4 .
 3. Déterminer la dimension de la dernière représentation irréductible de \mathfrak{A}_4 grâce aux propriétés de la représentation régulière.
 4. En utilisant l'orthogonalité des colonnes, déterminer alors la table de caractère de \mathfrak{A}_4 .
1. On connaît les classes de conjugaisons dans \mathfrak{S}_4 , et on regarde celles qui sont dans \mathfrak{A}_4 . Il faudra après re-vérifier que ces classes de conjugaisons ne se re-découpent pas dans \mathfrak{A}_4 .

Dans \mathfrak{S}_4 , on a

- ▷ $\{\text{id}\} \subseteq \mathfrak{A}_4$;
- ▷ $\{\text{transpositions}\} \not\subseteq \mathfrak{A}_4$;
- ▷ $\{\text{3-cycles}\} \subseteq \mathfrak{A}_4$;
- ▷ $\{\text{bi-transpositions}\} \subseteq \mathfrak{A}_4$;
- ▷ $\{\text{4-cycles}\} \not\subseteq \mathfrak{A}_4$.

Les classes $\{\text{id}\}$ et $\{\text{bi-transpositions}\}$ ne se re-découpent pas. Cependant, pour les 3-cycles, on les décompose en deux classes : celle de $(1\ 2\ 3)$ et $(1\ 3\ 2)$.

- ▷ Les deux permutations ne sont pas conjuguées car, si elles l'étaient, alors il existerait $\sigma \in \mathfrak{A}_4$ telle que

$$(\sigma(1)\ \sigma(2)\ \sigma(3)) = \sigma(1\ 2\ 3)\sigma^{-1} = (1\ 3\ 2).$$

Et, $\sigma(4) = 4$ donc σ permute 1, 2, 3. Par \mathfrak{A}_3 , on en déduit que l'on a $\sigma \in \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. On en conclut que σ et $(1\ 2\ 3)$ commutent : **absurde** car

$$\sigma(1\ 2\ 3)\sigma^{-1} = (1\ 2\ 3) \neq (1\ 3\ 2).$$

- ▷ On sait que $\#\text{Cl}_{\mathfrak{A}_4}((1\ 2\ 3)) = \#\mathfrak{A}_4/\#\text{C}_{\mathfrak{A}_4}((1\ 2\ 3))$ (par relation orbite-stabilisateur pour la conjugaison). De plus, on sait que $\#\text{Cl}_{\mathfrak{S}_4}((1\ 2\ 3)) = \#\mathfrak{S}_4/\#\text{C}_{\mathfrak{S}_4}((1\ 2\ 3))$. Ainsi, on a que $\#\text{C}_{\mathfrak{S}_4}((1\ 2\ 3)) = 3$. On a $\text{C}_{\mathfrak{S}_4}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$.

Or, $C_{\mathfrak{A}_4}((123)) = \mathfrak{A}_4 \cap C_{S_4}((123))$. Ainsi, $\#Cl_{S_4}((132)) = 4$.

Tous les 3-cycles de \mathfrak{A}_4 sont répartis dans deux classes de conjugaisons : celle de $(1\ 2\ 3)$ et celle de $(1\ 3\ 2)$.

- ▷ Et \mathfrak{A}_4 est 2-transitif donc $(12)(34)$ est conjugué à $(ab)(cd)$ pour tout a, b, c, d distincts avec $\sigma : 1 \mapsto a, 2 \mapsto b$ car

$$\sigma(1\ 2)(3\ 4)\sigma^{-1} = \dots = (a\ b)(c\ d).$$

Donc, les classes de conjugaisons de \mathfrak{A}_4 sont :

$\{\text{id}\}$ $\{\text{classe de } (123)\}$ $\{\text{classe de } (132)\}$ et $\{\text{bi-transpositions}\}$.

2. Si $H \triangleleft G$ et G/H est abélien alors $D(G) \subseteq H$. Le sous-groupe distingué $V_4 \triangleleft \mathfrak{A}_4$ est le sous-groupe contenant l'identité et les bi-transpositions. On a $|\mathfrak{A}_4/V_4| = 3$ donc \mathfrak{A}_4/V_4 est abélien, d'où on a $D(\mathfrak{A}_4) \subseteq V_4$. Or, $D(\mathfrak{A}_4) \triangleleft \mathfrak{A}_4$ donc c'est une union de classe de conjugaisons. Ainsi $D(\mathfrak{A}_4) = \{\text{id}\}$ et $D(\mathfrak{A}_4) = V_4$. Et, puisque \mathfrak{A}_4 est non-abélien, alors $D(\mathfrak{A}_4) \neq \{\text{id}\}$. On en déduit que $D(\mathfrak{A}_4) = V_4$. On a que \mathfrak{A}_4 a $3 = [\mathfrak{A}_4 : V_4]$ caractères linéaires (*c.f.* exercice 12.1). Un caractère linéaire χ de \mathfrak{A}_4 vérifie donc $\chi(V_4) = 1$ et est uniquement déterminé par $\chi(1\ 2\ 3) \in \{1, j, j^2\}$ où $j = e^{2i\pi/3}$.
3. On a que $\#\mathfrak{A}_4 = 12 = 1^2 + 1^2 + 1^2 + 3^2$.
4. On en déduit la table suivante.

12.4 Exercice 4. Tables de caractères de D_8 et H_8 .

On va calculer les tables de caractères des groupes D_8 et H_8 .

1. Soit D_8 le groupe diédral d'ordre 8. Il est engendré par deux éléments r et s tels que l'élément r est d'ordre 4, l'élément s est d'ordre 2 et l'égalité $sr s^{-1} = r^{-1}$ est vérifiée.
 - a) Montrer que les classes de conjugaisons de D_8 sont $\{1\}$, $\{r, r^3\}$, $\{r^2\}$ $\{s, sr^2\}$ et $\{sr, sr^3\}$.

- b) Montrer que le groupe dérivé de D_8 est $\{1, r^2\}$.*
- c) En déduire que D_8 a 4 représentations de degré 1, et une irréductible de degré 2, ainsi que la table de caractère de D_8 . À quelle action géométrique correspond la représentation irréductible de degré 2 ?*

1.