Logique

Basé sur le cours de Natacha Portier
Notes prises par Hugo Salou

ENS DE LYON

31 janvier 2025

Table des matières

Introduction.

Dans ce cours, on s'intéressera à quatre thèmes :

- la théorie des modèles (▷ les « vraies » mathématiques) ;
- la théorie de la démonstration (▷ les preuves) ;
- la théorie des ensembles (▷ les objets) ;
- les théorèmes de Gödel (▷ les limites).

On ne s'intéressera pas à la calculabilité, car déjà vu en cours de FDI. Ce cours peut être utile à ceux préparant l'agrégation d'informatique.

1 Le calcul propositionnel.

Le *calcul propositionnel*, c'est la « grammaire » de la logique. Dans ce chapitre, on s'intéressera à

1. la construction des formules (▷ la syntaxe) ;
2. la sémantique et les théorèmes de compacité (▷ la compacité sémantique).

1.1 Syntaxe.

Définition 1.1. Le *langage*, ou *alphabet*, est un ensemble d'éléments fini ou pas. Les éléments sont les *lettres*, et les suites finies sont les *mots*.

Définition 1.2. On choisit l'alphabet :

- ▷ $\mathscr{P} = \{x_0, x_1, \ldots\}$ des variables propositionnelles ;
- ▷ un ensemble de *connecteurs* ou *symboles logiques*, défini par $\{\neg, \vee, \wedge, \to, \leftrightarrow\}$, il n'y a pas $\exists$ et $\forall$ pour l'instant.
- ▷ les parenthèses $\{\texttt{(},\texttt{)}\}$.

Les formules logiques sont des mots. On les fabriques avec des briques de base (les variables) et des opérations de construction : si F_1 et F_2 sont deux formules, alors $\neg F$, $\texttt{(}F_1 \vee F_2\texttt{)}$, $\texttt{(}F_1 \wedge F_2\texttt{)}$, $\texttt{(}F_1 \to F_2\texttt{)}$ et $\texttt{(}F_1 \leftrightarrow F_2\texttt{)}$ aussi.

Définition 1.3 (« par le haut », « mathématique »). L'ensemble $\mathscr{F}$ des formules du calcul propositionnel construit sur $\mathscr{P}$ est le plus petit ensemble contenant $\mathscr{P}$ et stable par les opérations de construction.

Définition 1.4 (« par le bas », « informatique »). L'ensemble $\mathscr{F}$ des formules logique du calcul propositionnel sur $\mathscr{P}$ est défini par

- ▷ $\mathscr{F}_0 = \mathscr{P}$;
- ▷ $\mathscr{F}_{n+1} = \mathscr{F}_n \cup \left\{ \begin{array}{c|c} \neg F_1 & \\ (F_1 \vee F_2) & \\ (F_1 \wedge F_2) & F_1, F_2 \in \mathscr{F} \\ (F_1 \to F_2) & \\ (F_1 \leftrightarrow F_2) & \end{array} \right\}$

puis on pose $\mathscr{F} = \bigcup_{n\in\mathbb{N}} \mathscr{F}_n$.

On peut montrer l'équivalence des deux définitions.

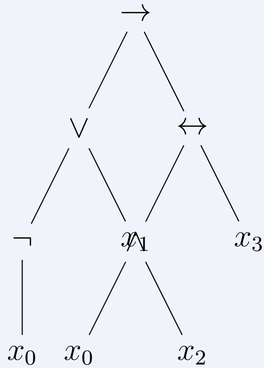
Théorème 1.1 (Lecture unique). Toute formule $G \in \mathscr{F}$ vérifie une et une seule de ces propriétés :

- ▷ $G \in \mathscr{P}$;
- ▷ il existe $F \in \mathscr{F}$ telle que $G = \neg F$;
- ▷ il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \vee F_2)$;
- ▷ il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \wedge F_2)$;
- ▷ il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \to F_2)$;
- ▷ il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \leftrightarrow F_2)$.

Preuve. En exercice. □

Corollaire 1.1. Il y a une bijection entre les formules et les arbres dont

- ▷ les feuilles sont étiquetés par des variables ;
- ▷ les nœuds internes sont étiquetés par des connecteurs ;
- ▷ ceux étiquetés par $\neg$ ont un fils, les autres deux.



Exemple 1.1.

1.2 Sémantique.

Lemme 1.1. Soit ν une fonction de $\mathscr{P}$ dans $\{0, 1\}$ appelé *valuation*. Alors ν s'étend de manière unique en une fonction $\bar{\nu}$ de $\mathscr{F}$ dans $\{0, 1\}$ telle que

- ▷ sur $\mathscr{P}$, $\nu = \bar{\nu}$;
- ▷ si $F, G \in \mathscr{F}$ sont des formules alors
  - – $\bar{\nu}(\neg F) = 1 - \bar{\nu}(F)$;
  - – $\bar{\nu}(F \vee G) = 1$ ssi $\bar{\nu}(F) = 1$ ou [1] $\bar{\nu}(G) = 1$;
  - – $\bar{\nu}(F \wedge G) = \bar{\nu}(F) \times \bar{\nu}(G)$;
  - – $\bar{\nu}(F \to G) = 1$ ssi $\bar{\nu}(G) = 1$ ou $\bar{\nu}(F) = 0$;
  - – $\bar{\nu}(F \leftrightarrow G) = 1$ ssi $\bar{\nu}(F) = \bar{\nu}(G)$.

Par abus de notations, on notera ν pour $\bar{\nu}$ par la suite.

Preuve. Existence. On définit en utilisant le lemme de lecture unique, et par induction sur $\mathscr{F}$:

- ▷ $\bar{\nu}$ est définie sur $\mathscr{F}_0 = \mathscr{P}$;
- ▷ si $\bar{\nu}$ est définie sur $\mathscr{F}_n$ alors pour $F \in \mathscr{F}_{n+1}$, on a la

1. C'est un « ou » inclusif : on peut avoir les deux (ce qui est très différent du « ou » exclusif dans la langue française).

disjonction de cas

- si $F = \neg G$ avec $G \in \mathscr{F}_n$, et on définit $\bar{\nu}(F) = 1 - \bar{\nu}(F_1)$;
- *etc* pour les autres cas.

Unicité. On montre que si $\lambda = \nu$ sur $\mathscr{P}$ alors $\bar{\lambda} = \bar{\nu}$ si $\bar{\lambda}$ et ν vérifient les égalités précédents.

□

Exemple 1.2 (Table de vérité)**.** Pour la formule

$$F = ((x_1 \to x_2) \to (x_2 \to x_1)),$$

on construit la table

x_1	0	0	1	1
x_2	0	1	0	1
$x_1 \to x_2$	1	1	0	1
$x_2 \to x_1$	1	0	1	1
F	1	0	1	1

Définition 1.5.

- ▷ Une formule F est dite *satisfaite par une valuation* ν si $\nu(F) = 1$.
- ▷ Une *tautologie* est une formule satisfaite pour toutes les valuations.
- ▷ Un ensemble $\mathscr{E}$ de formules est *satisfiable* s'il existe une valuation qui satisfait toutes les formules de $\mathscr{E}$.
- ▷ Un ensemble $\mathscr{E}$ de formules est *finiment satisfiable* si tout sous-ensemble fini de $\mathscr{E}$ est satisfiable.
- ▷ Une formule $F est conséquence sémantique$ d'un ensemble de formules $\mathscr{E}$ si toute valuation qui satisfait $\mathscr{E}$ satisfait F.
- ▷ Un ensemble de formules $\mathscr{E}$ est *contradictoire* s'il n'est pas satisfiable.
- ▷ Un ensemble de formules $\mathscr{E}$ est *finiment contradictoire* s'il

existe un sous-ensemble fini contradictoire de $\mathscr{E}$.

Théorème 1.2 (compacité du calcul propositionnel)**.** On donne trois énoncés équivalents (équivalence des trois énoncés laissé en exercice) du théorème de compacité du calcul propositionnel.

Version 1. Un ensemble de formules $\mathscr{E}$ est satisfiable si et seulement s'il est finiment satisfiable.

Version 2. Un ensemble de formules $\mathscr{E}$ est contradictoire si et seulement s'il est finiment contradictoire.

Version 3. Pour tout ensemble $\mathscr{E}$ de formules du calcul propositionnel, et toute formule F, F est conséquence sémantique de $\mathscr{E}$ si et seulement si F est conséquence sémantique d'un sous-ensemble fini de $\mathscr{E}$.

Preuve. Dans le cas où $\mathscr{P} = \{x_0, x_1, \dots\}$ est au plus dénombrable (le cas non dénombrable sera traité après). On démontre le cas « difficile » de la version 1 (*i.e.* finiment satisfiable implique satisfiable). Soit $\mathscr{E}$ un ensemble de formules finiment satisfiable. On construit par récurrence une valuation ν qui satisfasse $\mathscr{E}$ par récurrence : on construit $\varepsilon_0, \dots, \varepsilon_n, \dots$ tels que $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n, \dots$

- ▷ Cas de base. On définit la valeur de ε_n pour $x_0 \in \mathscr{P}$.
  1. soit, pour tout sous-ensemble fini B de $\mathscr{E}$, il existe une valuation λ qui satisfait B avec $\lambda(x_0) = 0$;
  2. soit, il existe un sous-ensemble fini B_0 de $\mathscr{E}$, pour toute valuation λ qui satisfait B_0, on a $\lambda(x_0) = 1$.

  Si on est dans le cas 1, on pose $\varepsilon_0 = 0$, et sinon (cas 2) on pose $\varepsilon_0 = 1$.
- ▷ Cas de récurrence. On montre, par récurrence sur n, la propriété suivante :

  > il existe une suite $\varepsilon_0, \dots, \varepsilon_n$ (que l'on étend, la suite ne change pas en fonction de n) de booléens telle que, pour tout sous-ensemble fini B de $\mathscr{E}$, il

existe une valuation ν satisfaisant B et telle que $\nu(x_0) = \varepsilon_0$, …, et $\nu(x_n) = \varepsilon_n$.

- Pour $n = 0$, soit on est dans le cas 1, et on prend $\varepsilon_0 = 0$ et on a la propriété ; soit on est dans le cas 2 ;, et on prend B un sous-ensemble fini de $\mathscr{E}$, alors $B \cup B_0$ est un ensemble fini donc satisfiable par une valuation ν. La valuation satisfait B_0 donc $\nu(x_0) = 1$ et ν satisfait B. On a donc la propriété au rang 0.
- Hérédité. Par hypothèse de récurrence, on a une suite $\varepsilon_0, \dots, \varepsilon_n$.
  1. Soit, pour tout sous-ensemble fini B de $\mathscr{E}$, il existe ν qui satisfait B et telle que $\nu(x_0) = \varepsilon_0$, …, $\nu(x_n) = \varepsilon_n$, et $\nu(x_{n+1}) = 0$. On pose $\varepsilon_{n+1} = 0$.
  2. Soit il existe B_{n+1} un sous-ensemble fini de $\mathscr{E}$ tel que, pour toute valuation ν telle que ν satisfait B_{n+1} et $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n$, on a $\nu(x_{n+1}) = 1$ et on pose $\varepsilon_{n+1} = 1$.

  Montrons l'hérédité :
  1. vrai par définition ;
  2. soit B un sous-ensemble fini de $\mathscr{E}$. On considère $B \cup B_{n+1}$, soit ν telle que $\nu(x_0) = \varepsilon_0$, …, $\nu(x_n) = \varepsilon_n$. On a que ν satisfait B_{n+1} donc $\nu(x_{n+1}) = 1 = \varepsilon_{n+1}$ et ν satisfait B.

On a donc la propriété pour tout n.

Finalement, soit δ une valuation telle que, pour tout i, $\delta(x_i) = \varepsilon_i$. Montrons que δ satisfait $\mathscr{E}$. Soit $F \in \mathscr{E}$. On sait que F est un mot (fini), donc contient un ensemble fini de variables inclus dans $\{x_0, \dots, x_n\}$. D'après la propriété par récurrence au rang n, il existe une valuation ν qui satisfait F et telle que $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n$, et donc ν et δ coïncident sur les variables de F. Donc (lemme simple), elles coïncident sur toutes les formules qui n'utilisent que ces variables. Donc, $\delta(F) = 1$, et on en conclut que δ satisfait $\mathscr{E}$. $\square$

Dans le cas non-dénombrable, on utilise le *lemme de Zorn*, un équivalent de l'*axiome du choix*.

Définition 1.6. Un ensemble ordonné $(X, \mathscr{R})$ est inductif si pour tout sous-ensemble Y de X totalement ordonné par $\mathscr{R}$ (*i.e.* une chaîne) admet un majorant dans X.

Remarque 1.1. On considère ici un majorant et non un plus grand élément (un maximum).

Exemple 1.3.
1. Dans le cas $(\mathscr{P}(X), \subseteq)$, le majorant est l'union des parties de la chaîne, il est donc inductif.
2. Dans le cas $(\mathbb{R}, \leq)$, il n'est pas inductif car $\mathbb{R}$ n'a pas de majorant dans $\mathbb{R}$.

Lemme 1.2 (Lemme de Zorn). Si $(X, \mathscr{R})$ est un ensemble ordonné inductif non-vide, il admet au moins un élément maximal.

Remarque 1.2. Un élément maximal n'est pas nécessairement le plus grand.

Preuve. Soit $\mathscr{E}$ un ensemble de formules finiment satisfiable, et $\mathscr{P}$ un ensemble de variables. On note $\mathscr{V}$ l'ensemble des valuations partielles prolongeables pour toute partie finie $\mathscr{C}$ de $\mathscr{E}$ en une valuation satisfaisant $\mathscr{C}$. C'est-à-dire :

$$\mathscr{V} := \left\{ \varphi \in \bigcup_{X \subseteq \mathscr{P}} \{0,1\}^X \;\middle|\; \forall \mathscr{C} \in \wp_{\mathrm{f}}(\mathscr{E}), \exists \delta \in \{0,1\}^{\mathscr{P}}, \begin{array}{l} \delta_{|\mathrm{dom}(\varphi)} = \varphi \\ \forall F \in \mathscr{C}, \delta(F) = 1 \end{array} \right\}.$$

L'ensemble $\mathscr{V}$ est non-vide car contient l'application vide de $\{0,1\}^\emptyset$ car $\mathscr{E}$ est finiment satisfiable. On défini la relation d'ordre $\preccurlyeq$ sur $\mathscr{V}$ par :

$$\varphi \preccurlyeq \psi \quad \text{ssi} \quad \psi \text{ prolonge } \varphi.$$

Montrons que $(\mathscr{V}, \preccurlyeq)$ est inductif. Soit $\mathscr{C}$ une chaîne de $\mathscr{V}$ et construisons un majorant de $\mathscr{C}$. Soit λ la valuation partielle définie sur $\operatorname{dom} \lambda = \bigcup_{\varphi \in \mathscr{C}} \operatorname{dom} \varphi$, par : si $x_i \in \operatorname{dom} \lambda$ alors il existe $\varphi \in \mathscr{C}$ tel que $x_i \in \operatorname{dom} \varphi$ et on pose $\lambda(x_i) = \varphi(x_i)$.

La valuation λ est définie de manière unique, *i.e.* ne dépend pas du choix de φ. En effet, si $\varphi \in \mathscr{C}$ et $\psi \in \mathscr{C}$, avec $x_i \in \operatorname{dom} \varphi \cap \operatorname{dom} \psi$, alors on a $\varphi \preccurlyeq \psi$ ou $\psi \preccurlyeq \varphi$, donc $\varphi(x_i) = \psi(x_i)$.

Autrement dit, λ est la limite de $\mathscr{C}$. Montrons que $\lambda \in \mathscr{V}$. Soit B une partie finie de $\mathscr{E}$. On cherche μ qui prolonge λ et satisfait B. L'ensemble de formules B est fini, donc utilise un ensemble fini de variables, dont un sous-ensemble fini $\{x_{i_1}, \ldots, x_{i_n}\} \subseteq \operatorname{dom}(\lambda)$. Il existe $\varphi_1, \ldots, \varphi_n$ dans $\mathscr{C}$ telle que $x_{i_1} \in \operatorname{dom} \varphi_1, \ldots, x_{i_n} \in \operatorname{dom} \varphi_n$. Comme $\mathscr{C}$ est une chaîne, donc soit $\varphi_0 = \max_{i \in [\![1,n]\!]} \varphi_i$ et on a $\varphi_0 \in \mathscr{C}$. On a, de plus, $x_{i_1}, \ldots, x_{i_n} \in \operatorname{dom}(\varphi_0)$. Soit $\varphi_0 \in \mathscr{V}$ prolongeable en ψ_0 qui satisfait B. On définit :

$$\begin{aligned} \mu : \mathscr{P} &\longrightarrow \{0,1\} \\ x \in \operatorname{dom} \lambda &\longmapsto \lambda(x) \\ x \in \operatorname{var} B &\longmapsto \psi_0(x) \\ \text{sinon} &\longmapsto 0. \end{aligned}$$

On vérifie que la définition est cohérente sur l'intersection car λ et ψ_0 prolongent tous les deux φ_0 et donc $\lambda \in \mathscr{V}$ d'où $\mathscr{V}$ est inductif.

Suite la preuve plus tard. □

2 La logique du premier ordre.

2.1 Les termes.

On commence par définir les *termes*, qui correspondent à des objets mathématiques. Tandis que les formules relient des termes et correspondent plus à des énoncés mathématiques.

Définition 2.1. Le langage $\mathscr{L}$ (du premier ordre) est la donnée d'une famille (pas nécessairement finie) de symboles de trois sortes :

- ▷ les symboles de *constantes*, notées c ;
- ▷ les symboles de *fonctions*, avec un entier associé, leur *arité*, notées $f(x_1, \ldots, x_n)$ où n est l'arité ;
- ▷ les symboles de *relations*, avec leur arité, notées $\mathscr{R}$, appelés *prédicats*.

Les trois ensembles sont disjoints.

Remarque 2.1.

- ▷ Les constantes peuvent être vues comme des fonctions d'arité 0.
- ▷ On aura toujours dans les relations : « $=$ » d'arité 2, et « $\perp$ » d'arité 0.
- ▷ On a toujours un ensemble de variables $\mathscr{V}$.

Exemple 2.1. Le langage $\mathscr{L}_{\mathrm{g}}$ de la théorie des groupes est défini par :

- ▷ une constante : c,

- deux fonctions : f_1 d'arité 2 et f_2 d'arité 1 ;
- la relation $=$.

Ces symboles sont notés usuellement e, $*$, $\square^{-1}$ ou bien 0, $+$, $-$.

Exemple 2.2. Le langage $\mathscr{L}_{\text{co}}$ des corps ordonnés est défini par :

- deux constantes 0 et 1,
- quatre fonctions $+$, $\times$, $-$ et $\square^{-1}$,
- deux relations $=$ et $\leq$.

Exemple 2.3. Le langage $\mathscr{L}_{\text{ens}}$ de la théorie des ensembles est défini par :

- une constante $\emptyset$,
- trois fonctions $\cap$, $\cup$ et $\square^{\mathsf{c}}$,
- trois relations $=$, $\in$ et $\subseteq$.

Définition 2.2. **Par le haut.** L'ensemble $\mathscr{T}$ des termes sur le langage $\mathscr{L}$ est le plus petit ensemble de mots sur $\mathscr{L} \cup \mathscr{V} \cup \{(,), ,\}$ tel

- qu'il contienne $\mathscr{V}$ et les constantes ;
- qui est stable par application des fonctions, c'est-à-dire que pour des termes $t_1, \dots, t_n$ et un symbole de fonction f d'arité n, alors $f(t_1, \dots, t_n)$ est un terme. [1]

Par le bas. On pose

$$\mathscr{T}_0 = \mathscr{V} \cup \{c \mid c \text{ est un symbole de constante de } \mathscr{L}\},$$

puis

$$\mathscr{T}_{k+1} = \mathscr{T}_k \cup \left\{ f(t_1, \dots t_n) \;\middle|\; \begin{array}{c} f \text{ fonction d'arité } n \\ t_1, \dots, t_n \in \mathscr{T}_k \end{array} \right\},$$

et enfin

$$\mathscr{T} = \bigcup_{n \in \mathbb{N}} \mathscr{T}_n.$$

Remarque 2.2. Dans la définition des termes, un n'utilise les relations.

Exemple 2.4.
- ▷ Dans $\mathscr{L}_\mathrm{g}$, $*(*(x, \square^{-1}(y)), e)$ est un terme, qu'on écrira plus simplement en $(x * y^{-1}) * e$.
- ▷ Dans $\mathscr{L}_\mathrm{co}$, $(x + x) + (-0)^{-1}$ est un terme.
- ▷ Dans $\mathscr{L}_\mathrm{ens}$, $(\emptyset^\mathsf{c} \cup \emptyset) \cap (x \cup y)^\mathsf{c}$ est un terme.

Définition 2.3. Si t et u sont des termes et x est une variable, alors $t[x : u]$ est le mot dans lequel les lettres de x ont été remplacées par le mot u. Le mot $t[x : u]$ est un terme (preuve en exercice).

Exemple 2.5. Avec $t = (x * y^{-1}) * e$ et $u = x * e$, alors on a

$$t[x : u] = ((x * e) * y^{-1}) * e.$$

Définition 2.4.
- ▷ Un terme *clos* est un terme sans variable (par exemple $(0 + 0)^{-1}$).
- ▷ La *hauteur* d'un terme est le plis petit k tel que $t \in \mathscr{T}_k$.

Exercice 2.1.
- ▷ Énoncer et prouver le lemme de lecture unique pour les termes.
- ▷ Énoncer et prouver un lemme de bijection entre les termes et un ensemble d'arbres étiquetés.

1. Attention : le « … » n'est pas un terme mais juste une manière d'écrire qu'on place les termes à côté des autres.

2.2 Les formules.

Définition 2.5. ▷ Les formules sont des mots sur l'alphabet

$$\mathscr{L} \cup \mathscr{V} \cup \{\,(\,,\,)\,,\,,\,,\exists,\forall,\wedge,\vee,\neg,\rightarrow\}.$$

▷ Une *formule atomique* est une formule de la forme $\mathscr{R}(t_1,\ldots,t_n)$ où $\mathscr{R}$ est un symbole de relation d'arité n et $t_1,\ldots,t_n$ des termes.

▷ L'ensemble des *formules* $\mathscr{F}$ du langage $\mathscr{L}$ est défini par

- on pose $\mathscr{F}_0$ l'ensemble des formules atomiques ;
- on pose $\mathscr{F}_{k+1} = \mathscr{F}_k \cup \left\{ \begin{matrix} (\neg F) \\ (F \to G) \\ (F \vee G) \\ (F \wedge G) \\ \exists x\; F \\ \exists x\; G \end{matrix} \;\middle|\; \begin{matrix} F, G \in \mathscr{F}_k \\ x \in \mathscr{V} \end{matrix} \right\}$;
- et on pose enfin $\mathscr{F} = \bigcup_{n\in\mathbb{N}} \mathscr{F}_n$.

Exercice 2.2. La définition ci-dessus est « par le bas ». Donner une définition par le haut de l'ensemble $\mathscr{F}$.

Exemple 2.6. ▷ Dans $\mathscr{L}_{\mathrm{g}}$, un des axiomes de la théorie des groupes s'écrit

$$\forall x\; \exists x\; (x * y = e \wedge y * x = e).$$

▷ Dans $\mathscr{L}_{\mathrm{co}}$, l'énoncé « le corps est de caractéristique 3 » s'écrit

$$\forall x\; (x + (x + x) = 0).$$

▷ Dans $\mathscr{L}_{\mathrm{ens}}$, la loi de De Morgan s'écrit

$$\forall x\; \forall y\; (x^{\mathsf{c}} \cup y^{\mathsf{c}} = (x \cap y)^{\mathsf{c}}).$$

Exercice 2.3. ▷ Donner et montrer le lemme de lecture unique.
▷ Énoncer et donner un lemme d'écriture en arbre.

Remarque 2.3 (Conventions d'écriture.). On note :
- ▷ $x \leq y$ au lieu de $\leq(x, y)$;
- ▷ $\exists x \geq 0\ (F)$ au lieu de $\exists x\ (x \geq 0 \wedge F)$;
- ▷ $\forall x \geq 0\ (F)$ au lieu de $\forall x\ (x \geq 0 \to F)$;
- ▷ $A \leftrightarrow B$ au lieu de $(A \to B) \wedge (B \to A)$;
- ▷ $t \neq u$ au lieu de $\neg(t = u)$.

On enlèves les parenthèses avec les conventions de priorité

0. les symboles de relations (le plus prioritaire) ;
1. les symboles $\neg, \exists, \forall$;
2. les symboles $\wedge$ et $\vee$;
3. le symbole $\to$ (le moins prioritaire).

Exemple 2.7. Ainsi, $\forall x\ A \wedge B \to \neg C \vee D$ s'écrit

$$(((\forall x\ A) \wedge B) \to ((\neg C) \vee D)).$$

Remarque 2.4. Le calcul propositionnel est un cas particulier de la logique du premier ordre où l'on ne manipule que des relations d'arité 0 (pas besoin des fonctions et des variables) : les « variables » du calcul propositionnel sont des formules atomiques ; et on n'a pas de relation « = ».

Remarque 2.5. On ne peut pas exprimer *a priori* :
- ▷ des quantifications sur en ensemble[2] ;
- ▷ « $\exists n\ \exists x_1 \ldots \exists x_n$ » une formule qui dépend d'un paramètre ;
- ▷ le principe de récurrence : si on a $\mathscr{P}(0)$ pour une propriété $\mathscr{P}$ et que si $\mathscr{P}(n) \to \mathscr{P}(n+1)$ alors on a $\mathscr{P}(n)$ pour tout n.

Quelques définitions techniques qui permettent de manipuler les formules.

Définition 2.6. L'ensemble des sous-formules de F, noté $\mathrm{S}(F)$ est défini par induction :

- ▷ si F est atomique, alors on définit $\mathrm{S}(F) = \{F\}$;
- ▷ si $F = F_1 \oplus F_2$ (avec $\oplus$ qui est $\vee$, $\to$ ou $\wedge$) alors on définit $\mathrm{S}(F) = \mathrm{S}(F_1) \cup \mathrm{S}(F_2) \cup \{F\}$;
- ▷ si $F = \neg F_1$, ou $F = \mathsf{Q}x\, F_1$ avec $\mathsf{Q} \in \{\forall, \exists\}$, alors on définit $\mathrm{S}(F) = \mathrm{S}(F_1) \cup \{F\}$.

C'est l'ensemble des formules que l'on voit comme des sous-arbres de l'arbre équivalent à la formule F.

Définition 2.7.
- ▷ La *taille* d'une formule, est le nombre de connecteurs ($\neg$, $\vee$, $\wedge$, $\to$), et de quantificateurs ($\forall$, $\exists$).
- ▷ La racine de l'arbre est
  - – rien su la formule est atomique ;
  - – « $\oplus$ » si $F = F_1 \oplus F_2$ avec $\oplus$ un connecteur (binaire ou unaire) ;
  - – « Q » si $F = \mathsf{Q}x\, F_1$ avec Q un quantificateur.

Définition 2.8.
- ▷ Une *occurrence* d'une variable est un endroit où la variable apparait dans la formule (*i.e.* une feuille étiquetée par cette variable).
- ▷ Une occurrence d'une variable est *liée* si elle se trouve dans une sous-formule dont l'opérateur principal est un quantificateur appelé à cette variable (*i.e.* un $\forall x\, F'$ ou un $\exists x\, F'$).
- ▷ Une occurrence d'une variable est *libre* quand elle n'est pas liée.
- ▷ Une variable est libre si elle a au moins une occurrence libre, sinon elle est liée.

2. En dehors de $\mathscr{L}_{\text{ens}}$, en tout cas.

Remarque 2.6. On note $F(x_1, \ldots, x_n)$ pour dire que les variables libres sont F sont parmi $\{x_1, \ldots, x_n\}$.

Définition 2.9. Une formule est *close* si elle n'a pas de variables libres.

Définition 2.10 (Substitution)**.** On note $F[x := t]$ la formule obtenue en remplaçant toutes les occurrences libres de x par t, après renommage éventuel des occurrences des variables liées de F qui apparaissent dans t.

Définition 2.11 (Renommage)**.** On donne une définition informelle et incomplète ici. On dit que les formules F et G sont α-équivalentes si elle sont syntaxiquement identiques à un renommage près des occurrences liées des variables.

Exemple 2.8. On pose

$$F(x, z) := \forall y\ (x * y = y * z) \wedge \forall x\ (x * x = 1),$$

et alors

- $F(z, z) = F[x := z] = \forall y\ (z * y = y * z) \wedge \forall x\ (x * x = 1)$;
- $F(y^{-1}, x) = F[x := y^{-1}] = \forall u (y^{-1} * u = u * z) \wedge \forall x (x * x = 1)$.

On a procédé à un renommage de y à u.

2.3 Les démonstrations en déduction naturelle.

Définition 2.12. Un *séquent* est un coupe noté $\Gamma \vdash F$ (où $\vdash$ se lit « montre » ou « thèse ») tel que Γ est un ensemble de formules appelé *contexte* (*i.e.* l'ensemble des hypothèses), la formule F est la *conséquence* du séquent.

Remarque 2.7. Les formules ne sont pas nécessairement closes. Et on note souvent Γ comme une liste.

Définition 2.13. On dit que $\Gamma \vdash F$ est *prouvable*, *démontrable* ou *dérivable*, s'il peut être obtenu par une suite finie de règles (*c.f.* ci-après). On dit qu'une formule F est *prouvable* si $\emptyset \vdash F$ l'est.

Définition 2.14 (Règles de la démonstration)**.** Une règle s'écrit

$$\frac{\textit{prémisses} : \text{des séquents}}{\textit{conclusion} : \text{un séquent}}\ \text{nom de la règle}\ .$$

Axiome.

$$\frac{}{\Gamma, A \vdash A}\ \mathsf{ax}$$

Affaiblissement.

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A}\ \mathsf{aff}$$

Implication.

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_{\mathsf{i}} \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \to_{\mathsf{e}}$$ [3]

Conjonction.

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_{\mathsf{i}} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \vee_{\mathsf{e}}^{\mathsf{g}} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \vee_{\mathsf{e}}^{\mathsf{d}}$$

Disjonction.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{i}}^{\mathsf{g}} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{i}}^{\mathsf{d}}$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_{\mathsf{e}}\ .$$ [4]

Négation.

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_\mathsf{i} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ \neg_\mathsf{e}$$

Absurdité classique.

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_\mathsf{e}$$

(En logique intuitionniste, on retire l'hypothèse $\neg A$ dans la prémisse.)

Quantificateur universel.

$$\text{si } x \text{ n'est pas libre dans les formules de } \Gamma \quad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ \forall_\mathsf{i}$$

$$\text{quitte à renommer les variables liées de } A \text{ qui apparaissent dans } t \quad \frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[x := t]}\ \forall_\mathsf{e}$$

Quantificateur existentiel.

$$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\ A}\ \exists_\mathsf{i}$$

$$\text{avec } x \text{ ni libre dans } C \text{ ou dans les formules de } \Gamma \quad \frac{\Gamma \vdash \exists x\ A \quad \Gamma, A \vdash C}{\Gamma \vdash C}\ \exists_\mathsf{e}$$

3. Aussi appelée *modus ponens*
4. C'est un raisonnement par cas