

# Logique

*Basé sur le cours de Natacha PORTIER  
Notes prises par Hugo SALOU*



*21 février 2025*

# Table des matières

<b>1</b>	<b>Le calcul propositionnel.</b>	<b>4</b>
1.1	Syntaxe. . . . .	4
1.2	Sémantique. . . . .	6
<b>2</b>	<b>La logique du premier ordre.</b>	<b>12</b>
2.1	Les termes. . . . .	12
2.2	Les formules. . . . .	15
2.3	Les démonstrations en déduction naturelle. . . . .	18
2.4	La sémantique. . . . .	20
2.5	Théorème de complétude de Gödel. . . . .	31
2.5.1	Preuve du théorème de correction. . . . .	33
2.5.2	Preuve du théorème de complétude. . . . .	35
2.5.3	Compacité. . . . .	42

# 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 ( $\triangleright$  la syntaxe) ;
2. la sémantique et les théorèmes de compacité ( $\triangleright$  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 :

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

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

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

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

$$\triangleright \mathcal{F}_0 = \mathcal{P};$$

$$\triangleright \mathcal{F}_{n+1} = \mathcal{F}_n \cup \left\{ \begin{array}{c} \neg F_1 \\ (F_1 \vee F_2) \\ (F_1 \wedge F_2) \\ (F_1 \rightarrow F_2) \\ (F_1 \leftrightarrow F_2) \end{array} \middle| F_1, F_2 \in \mathcal{F} \right\}$$

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

On peut montrer l'équivalence des deux définitions.

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

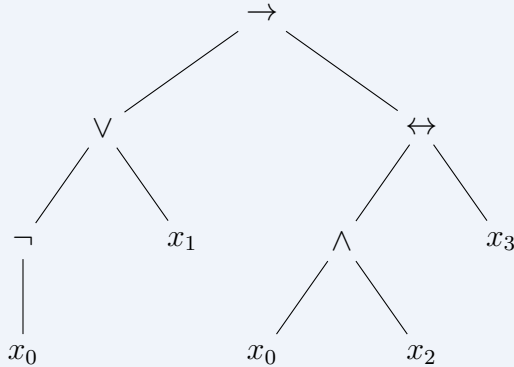
- $\triangleright G \in \mathcal{P}$ ;
- $\triangleright$  il existe  $F \in \mathcal{F}$  telle que  $G = \neg F$ ;
- $\triangleright$  il existe  $F_1, F_2 \in \mathcal{F}$  telle que  $G = (F_1 \vee F_2)$ ;
- $\triangleright$  il existe  $F_1, F_2 \in \mathcal{F}$  telle que  $G = (F_1 \wedge F_2)$ ;
- $\triangleright$  il existe  $F_1, F_2 \in \mathcal{F}$  telle que  $G = (F_1 \rightarrow F_2)$ ;
- $\triangleright$  il existe  $F_1, F_2 \in \mathcal{F}$  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

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

**Exemple 1.1.** La formule  $((\neg x_0 \vee x_1) \rightarrow ((x_0 \wedge x_2) \leftrightarrow x_3))$  correspond à l'arbre



## 1.2 Sémantique.

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

- ▷ sur  $\mathcal{P}$ ,  $\nu = \bar{\nu}$  ;
- ▷ si  $F, G \in \mathcal{F}$  sont des formules alors
  - $\bar{\nu}(\neg F) = 1 - \bar{\nu}(F)$  ;
  - $\bar{\nu}(F \vee G) = 1$  ssi  $\bar{\nu}(F) = 1$  ou <sup>1</sup>  $\bar{\nu}(G) = 1$  ;
  - $\bar{\nu}(F \wedge G) = \bar{\nu}(F) \times \bar{\nu}(G)$  ;
  - $\bar{\nu}(F \rightarrow G) = 1$  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  $\nu$  pour  $\bar{\nu}$  par la suite.

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

- ▷  $\bar{\nu}$  est définie sur  $\mathcal{F}_0 = \mathcal{P}$  ;
- ▷ si  $\bar{\nu}$  est définie sur  $\mathcal{F}_n$  alors pour  $F \in \mathcal{F}_{n+1}$ , on a la disjonction de cas
  - si  $F = \neg G$  avec  $G \in \mathcal{F}_n$ , et on définit  $\bar{\nu}(F) =$

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

- $1 - \bar{\nu}(F_1);$   
 – etc pour les autres cas.

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

□

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

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

on construit la table

$x_1$	0	0	1	1
$x_2$	0	1	0	1
$x_1 \rightarrow x_2$	1	1	0	1
$x_2 \rightarrow x_1$	1	0	1	1
$F$	1	0	1	1

**Définition 1.5.** ▷ Une formule  $F$  est dite *satisfaite par une valuation*  $\nu$  si  $\nu(F) = 1$ .

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

**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  $\mathcal{E}$  est satisfiable si et seulement s'il est finiment satisfiable.

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

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

**Preuve.** Dans le cas où  $\mathcal{P} = \{x_0, x_1, \dots\}$  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  $\mathcal{E}$  un ensemble de formules finiment satisfiable. On construit par récurrence une valuation  $\nu$  qui satisfasse  $\mathcal{E}$  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  $\varepsilon_n$  pour  $x_0 \in \mathcal{P}$ .

1. soit, pour tout sous-ensemble fini  $B$  de  $\mathcal{E}$ , il existe une valuation  $\lambda$  qui satisfait  $B$  avec  $\lambda(x_0) = 0$  ;
2. soit, il existe un sous-ensemble fini  $B_0$  de  $\mathcal{E}$ , pour toute valuation  $\lambda$  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  $\mathcal{E}$ , il existe une valuation  $\nu$  satisfaisant  $B$  et telle que  $\nu(x_0) = \varepsilon_0, \dots$ , 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  $\mathfrak{E}$ , alors  $B \cup B_0$  est un ensemble fini donc satisfiable par une valuation  $\nu$ . La valuation satisfait  $B_0$  donc  $\nu(x_0) = 1$  et  $\nu$  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  $\mathfrak{E}$ , il existe  $\nu$  qui satisfait  $B$  et telle que  $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n$ , et  $\nu(x_{n+1}) = 0$ . On pose  $\varepsilon_{n+1} = 0$ .
  2. Soit il existe  $B_{n+1}$  un sous-ensemble fini de  $\mathfrak{E}$  tel que, pour toute valuation  $\nu$  telle que  $\nu$  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  $\mathfrak{E}$ . On considère  $B \cup B_{n+1}$ , soit  $\nu$  telle que  $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n$ . On a que  $\nu$  satisfait  $B_{n+1}$  donc  $\nu(x_{n+1}) = 1 = \varepsilon_{n+1}$  et  $\nu$  satisfait  $B$ .

On a donc la propriété pour tout  $n$ .

Finalement, soit  $\delta$  une valuation telle que, pour tout  $i$ ,  $\delta(x_i) = \varepsilon_i$ . Montrons que  $\delta$  satisfait  $\mathfrak{E}$ . Soit  $F \in \mathfrak{E}$ . 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  $\nu$  qui satisfait  $F$  et telle que  $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n$ , et donc  $\nu$  et  $\delta$  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  $\delta$  satisfait  $\mathfrak{E}$ .  $\square$

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

**Définition 1.6.** Un ensemble ordonné  $(X, \mathcal{R})$  est inductif si pour tout sous-ensemble  $Y$  de  $X$  totalement ordonné par  $\mathcal{R}$  (*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  $(\mathcal{P}(X), \subseteq)$ , 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  $(X, \mathcal{R})$  est un ensemble ordonné inductif non-vidé, il admet au moins un élément maximal.

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

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

$$\mathcal{V} := \left\{ \varphi \in \bigcup_{X \subseteq \mathcal{P}} \{0, 1\}^X \mid \forall \mathcal{C} \in \wp_f(\mathcal{E}), \exists \delta \in \{0, 1\}^{\mathcal{P}}, \begin{array}{l} \delta|_{\text{dom}(\varphi)} = \varphi \\ \forall F \in \mathcal{C}, \delta(F) = 1 \end{array} \right\}.$$

L'ensemble  $\mathcal{V}$  est non-vidé car contient l'application vide de  $\{0, 1\}^{\emptyset}$  car  $\mathcal{E}$  est finiment satisfiable. On défini la relation

d'ordre  $\preceq$  sur  $\mathcal{V}$  par :

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

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

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

Autrement dit,  $\lambda$  est la limite de  $\mathcal{C}$ . Montrons que  $\lambda \in \mathcal{V}$ . Soit  $B$  une partie finie de  $\mathcal{E}$ . On cherche  $\mu$  qui prolonge  $\lambda$  et satisfait  $B$ . L'ensemble de formules  $B$  est fini, donc utilise un ensemble fini de variables, dont un sous-ensemble fini  $\{x_{i_1}, \dots, x_{i_n}\} \subseteq \text{dom}(\lambda)$ . Il existe  $\varphi_1, \dots, \varphi_n$  dans  $\mathcal{C}$  telle que  $x_{i_1} \in \text{dom } \varphi_1, \dots, x_{i_n} \in \text{dom } \varphi_n$ . Comme  $\mathcal{C}$  est une chaîne, donc soit  $\varphi_0 = \max_{i \in \llbracket 1, n \rrbracket} \varphi_i$  et on a  $\varphi_0 \in \mathcal{C}$ . On a, de plus,  $x_{i_1}, \dots, x_{i_n} \in \text{dom}(\varphi_0)$ . Soit  $\varphi_0 \in \mathcal{V}$  prolongeable en  $\psi_0$  qui satisfait  $B$ . On définit :

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

On vérifie que la définition est cohérente sur l'intersection car  $\lambda$  et  $\psi_0$  prolongent tous les deux  $\varphi_0$  et donc  $\lambda \in \mathcal{V}$  d'où  $\mathcal{V}$  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  $\mathcal{L}$  (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  $f(x_1, \dots, x_n)$  où  $n$  est l'arité ;
- ▷ les symboles de *relations*, avec leur arité, notées  $R$ , 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  $\mathcal{V}$ .

**Exemple 2.1.** Le langage  $\mathcal{L}_g$  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  $\mathcal{L}_{\text{co}}$  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  $\mathcal{L}_{\text{ens}}$  de la théorie des ensembles est défini par :

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

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

- ▷ qu'il contienne  $\mathcal{V}$  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. <sup>1</sup>

**Par le bas.** On pose

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

puis

$$\mathcal{T}_{k+1} = \mathcal{T}_k \cup \left\{ f(t_1, \dots, t_n) \mid \begin{array}{l} f \text{ fonction d'arité } n \\ t_1, \dots, t_n \in \mathcal{T}_k \end{array} \right\},$$

et enfin

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

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

**Exemple 2.4.** ▷ Dans  $\mathcal{L}_g$ ,  $*(x, \square^{-1}(y), e)$  est un terme, qu'on écrira plus simplement en  $(x * y^{-1}) * e$ .

▷ Dans  $\mathcal{L}_{co}$ ,  $(x + x) + (-0)^{-1}$  est un terme.

▷ Dans  $\mathcal{L}_{ens}$ ,  $(\emptyset^c \cup \emptyset) \cap (x \cup y)^c$  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 plus petit  $k$  tel que  $t \in \mathcal{T}_k$ .

**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

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

- ▷ Une *formule atomique* est une formule de la forme  $R(t_1, \dots, t_n)$  où  $R$  est un symbole de relation d'arité  $n$  et  $t_1, \dots, t_n$  des termes.
- ▷ L'ensemble des *formules*  $\mathcal{F}$  du langage  $\mathcal{L}$  est défini par
  - on pose  $\mathcal{F}_0$  l'ensemble des formules atomiques ;
  - on pose  $\mathcal{F}_{k+1} = \mathcal{F}_k \cup \left\{ \begin{array}{c} (\neg F) \\ (F \rightarrow G) \\ (F \vee G) \\ (F \wedge G) \\ \exists x F \\ \exists x G \end{array} \left| \begin{array}{c} F, G \in \mathcal{F}_k \\ x \in \mathcal{V} \end{array} \right. \right\} ;$
  - et on pose enfin  $\mathcal{F} = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$ .

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

**Exemple 2.6.** ▷ Dans  $\mathcal{L}_g$ , un des axiomes de la théorie des groupes s'écrit

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

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

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

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

$$\forall x \forall y (x^c \cup y^c = (x \cap y)^c).$$

**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  $\forall x (x \geq 0 \rightarrow F)$  ;
- ▷  $A \leftrightarrow B$  au lieu de  $(A \rightarrow B) \wedge (B \rightarrow A)$  ;
- ▷  $t \neq u$  au lieu de  $\neg(t = u)$ .

On enlève 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  $\rightarrow$  (le moins prioritaire).

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

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

**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<sup>2</sup> ;
- ▷ «  $\exists n \exists x_1 \dots \exists x_n$  » une formule qui dépend d'un paramètre ;
- ▷ le principe de récurrence : si on a  $\mathcal{P}(0)$  pour une propriété  $\mathcal{P}$  et que si  $\mathcal{P}(n) \rightarrow \mathcal{P}(n+1)$  alors on a  $\mathcal{P}(n)$  pour tout  $n$ .



Quelques définitions techniques qui permettent de manipuler les formules.

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

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

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 ( $\neg$ ,  $\vee$ ,  $\wedge$ ,  $\rightarrow$ ), et de quantificateurs ( $\forall$ ,  $\exists$ ).

- ▷ La racine de l'arbre est
  - rien si la formule est atomique ;
  - «  $\oplus$  » si  $F = F_1 \oplus F_2$  avec  $\oplus$  un connecteur (binaire ou unaire) ;
  - «  $Q$  » si  $F = Qx F_1$  avec  $Q$  un quantificateur.

**Définition 2.8.** ▷ Une *occurrence* d'une variable est un endroit où la variable apparaît 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.

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

**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  $\alpha$ -équivalentes si elles 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 couple noté  $\Gamma \vdash F$  (où  $\vdash$  se lit « montre » ou « thèse ») tel que  $\Gamma$  est un ensemble fini 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  $\Gamma$  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

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

**Axiome.**

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

**Affaiblissement.**

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

**Implication.**

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow_i \quad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow_e^3$$

**Conjonction.**

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge_i \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \vee_e^g \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \vee_e^d$$

**Disjonction.**

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_i^g \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee_i^d$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee_e^4 .$$

**Négation.**

$$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A} \neg_i \quad \frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \perp} \neg_e$$

**Absurdité classique.**

$$\frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A} \perp_e$$

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

**Quantificateur universel.**

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

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

**Quantificateur existentiel.**

$$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x A} \exists_i$$

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

## 2.4 La sémantique.

**Définition 2.15.** Soit  $\mathcal{L}$  un langage de la sémantique du premier ordre. On appelle *interprétation* (ou *modèle*, ou *structure*) du langage  $\mathcal{L}$  l'ensemble  $\mathcal{M}$  des données suivantes :

- ▷ un ensemble non vide, noté  $|\mathcal{M}|$ , appelé *domaine* ou *ensemble de base* de  $\mathcal{M}$  ;

---

3. Aussi appelée *modus ponens*

4. C'est un raisonnement par cas

- ▷ pour chaque symbole  $c$  de constante, un élément  $c_{\mathcal{M}}$  de  $|\mathcal{M}|$  ;
- ▷ pour chaque symbole  $f$  de fonction  $n$ -aire, une fonction  $f_{\mathcal{M}} : |\mathcal{M}|^n \rightarrow |\mathcal{M}|$  ;
- ▷ pour chaque symbole  $R$  de relation  $n$ -aire (sauf pour l'égalité « = »), un sous-ensemble  $R_{\mathcal{M}}$  de  $|\mathcal{M}|^n$ .

**Remarque 2.8.** ▷ La relation « = » est toujours interprétée par la vraie égalité :

$$\{(a, a) \mid a \in |\mathcal{M}|\}.$$

- ▷ On note, par abus de notation,  $\mathcal{M}$  pour  $|\mathcal{M}|$ .
- ▷ Par convention,  $|\mathcal{M}|^0 = \{\emptyset\}$ .

**Exemple 2.9.** Avec  $\mathcal{L}_{\text{corps}} = \{0, 1, +, \times, -, \square^{-1}\}$ , on peut choisir

- ▷  $|\mathcal{M}| = \mathbb{R}$  avec  $0_{\mathbb{R}}, 1_{\mathbb{R}}, +_{\mathbb{R}}, \times_{\mathbb{R}}, -_{\mathbb{R}}$  et  $\square_{\mathbb{R}}^{-1}$  ;
- ▷ ou  $|\mathcal{M}| = \mathbb{R}$  avec  $2_{\mathbb{R}}, 2_{\mathbb{R}}, -_{\mathbb{R}}, +_{\mathbb{R}}$ , etc.

Définissons la *vérité*.

**Définition 2.16.** Soit  $\mathcal{M}$  une interprétation de  $\mathcal{L}$ .

- ▷ Un *environnement* est une fonction de l'ensemble des variables dans  $|\mathcal{M}|$ .
- ▷ Si  $e$  est un environnement et  $a \in |\mathcal{M}|$ , on note  $e[x := a]$  l'environnement  $e'$  tel que  $e'(x) = a$  et pour  $y \neq x$ ,  $e(y) = e'(y)$ .
- ▷ La *valeur* d'un terme  $t$  dans l'environnement  $e$ , noté  $\text{Val}_{\mathcal{M}}(t, e)$ , est définie par induction sur l'ensemble des termes de la façon suivante :
  - $\text{Val}_{\mathcal{M}}(c, e) = c_{\mathcal{M}}$  si  $c$  est une constante ;
  - $\text{Val}_{\mathcal{M}}(x, e) = e(x)$  si  $x$  est une variable ;
  - $\text{Val}_{\mathcal{M}}(f(t_1, \dots, t_n), e) = f_{\mathcal{M}}(\text{Val}_{\mathcal{M}}(t_1, e), \dots, \text{Val}_{\mathcal{M}}(t_n, e))$ .

**Remarque 2.9.** La valeur est  $\mathcal{Val}_{\mathcal{M}}(t, e)$  est un élément de  $|\mathcal{M}|$ .

**Exemple 2.10.** Dans  $\mathcal{L}_{\text{arith}} = \{0, 1, +, \times\}$ , avec le modèle

$$\mathcal{M} : \mathbb{N}, 0_{\mathbb{N}}, 1_{\mathbb{N}}, +_{\mathbb{N}}, \times_{\mathbb{N}},$$

et l'environnement

$$e : \quad x_1 \mapsto 2_{\mathbb{N}} \quad x_2 \mapsto 0_{\mathbb{N}} \quad x_3 \mapsto 3_{\mathbb{N}},$$

alors la valeur du terme  $t := (1 \times x_1) + (x_2 \times x_3) + x_2$  est  $2_{\mathbb{N}} = (1 \times 2) + (0 \times 3) + 0$ .

**Lemme 2.1.** La valeur  $\mathcal{Val}_{\mathcal{M}}(t, e)$  ne dépend que de la valeur de  $e$  sur les variables de  $t$ .  $\square$

**Notation.**  $\triangleright$  Lorsque cela est possible, on oublie  $\mathcal{M}$  et  $e$  dans la notation, et on note  $\mathcal{Val}(t)$ .

- $\triangleright$  À la place de  $\mathcal{Val}_{\mathcal{M}}(t, e)$  quand  $x_1, \dots, x_n$  sont les variables de  $t$  et  $e(x_1) = a_1, \dots, e(x_n) = a_n$ , on note  $t[a_1, \dots, a_n]$  ou aussi  $t[x_1 := a_1, \dots, x_n := a_n]$ . C'est un *terme à paramètre*, mais attention ce n'est **ni un terme, ni une substitution**.

**Définition 2.17.** Soit  $\mathcal{M}$  une interprétation d'un langage  $\mathcal{L}$ . La *valeur* d'une formule  $F$  de  $\mathcal{L}$  dans l'environnement  $e$  est un élément de  $\{0, 1\}$  noté  $\mathcal{Val}_{\mathcal{M}}(F, e)$  et définie par induction sur l'ensemble des formules par

- $\triangleright \mathcal{Val}_{\mathcal{M}}(R(t_1, \dots, t_n), e) = 1$  ssi  $(\mathcal{Val}_{\mathcal{M}}(t_1, e), \dots, \mathcal{Val}_{\mathcal{M}}(t_n, e)) \in R_{\mathcal{M}}$ ;
- $\triangleright \mathcal{Val}_{\mathcal{M}}(\perp, e) = 0$ ;
- $\triangleright \mathcal{Val}_{\mathcal{M}}(\neg F, e) = 1 - \mathcal{Val}_{\mathcal{M}}(F, e)$ ;
- $\triangleright \mathcal{Val}_{\mathcal{M}}(F \wedge G, e) = 1$  ssi  $\mathcal{Val}_{\mathcal{M}}(F, e) = 1$  et  $\mathcal{Val}_{\mathcal{M}}(G, e) = 1$ ;
- $\triangleright \mathcal{Val}_{\mathcal{M}}(F \vee G, e) = 1$  ssi  $\mathcal{Val}_{\mathcal{M}}(F, e) = 1$  ou  $\mathcal{Val}_{\mathcal{M}}(G, e) = 1$ ;
- $\triangleright \mathcal{Val}_{\mathcal{M}}(F \rightarrow G, e) = 1$  ssi  $\mathcal{Val}_{\mathcal{M}}(F, e) = 0$  ou  $\mathcal{Val}_{\mathcal{M}}(G, e) = 1$ ;
- $\triangleright \mathcal{Val}_{\mathcal{M}}(\forall x F, e) = 1$  ssi pour tout  $a \in |\mathcal{M}|$ ,  $\mathcal{Val}_{\mathcal{M}}(F, e[x := a]) = 1$ ;

▷  $\mathcal{V}al_{\mathcal{M}}(\exists x F, e) = 1$  ssi il existe  $a \in |\mathcal{M}|$ ,  $\mathcal{V}al_{\mathcal{M}}(F, e[x := a]) = 1$ .

**Remarque 2.10.** ▷ On se débrouille pour que les connecteurs aient leur sens courant, les « mathématiques naïves ».

- ▷ Dans le cas du calcul propositionnel, si  $R$  est d'arité 0, *i.e.* une variable propositionnelle, comme  $|\mathcal{M}|^0 = \{\emptyset\}$  alors on a deux possibilités :
- ou bien  $R = \emptyset$ , et alors on convient que  $\mathcal{V}al_{\mathcal{M}}(R, e) = 0$  ;
  - ou bien  $R = \{\emptyset\}$ , et alors on convient que  $\mathcal{V}al_{\mathcal{M}}(R, e) = 1$ .

**Remarque 2.11.** On verra plus tard qu'on peut construire les entiers avec

- ▷  $0 : \emptyset$ ,
- ▷  $1 : \{\emptyset\}$ ,
- ▷  $2 : \{\emptyset, \{\emptyset\}\}$ ,
- ▷  $\vdots$
- ▷  $n + 1 : n \cup \{n\}$ ,
- ▷  $\vdots$

**Notation.** À la place de  $\mathcal{V}al_{\mathcal{M}}(F, e) = 1$ , on notera  $\mathcal{M}, e \models F$  ou bien  $\mathcal{M} \models F$ . On dit que  $\mathcal{M}$  *satisfait*  $F$ , que  $\mathcal{M}$  est un *modèle* de  $F$  (dans l'environnement  $e$ ), que  $F$  est vraie dans  $\mathcal{M}$ .

**Lemme 2.2.** La valeur  $\mathcal{V}al_{\mathcal{M}}(F, e)$  ne dépend que de la valeur de  $e$  sur les variables libres de  $F$ .

**Preuve.** En exercice. □

**Corollaire 2.1.** Si  $F$  est close, alors  $\mathcal{V}al_{\mathcal{M}}(F, e)$  ne dépend pas de  $e$  et on note  $\mathcal{M} \models F$  ou  $\mathcal{M} \not\models F$ .

**Remarque 2.12.** Dans le cas des formules closes, on doit passer un environnement à cause de  $\forall$  et  $\exists$ .

**Notation.** On note  $F[a_1, \dots, a_n]$  pour  $\mathcal{Val}_{\mathcal{M}}(F, e)$  avec  $e(x_1) = a_1, \dots, e(x_n) = a_n$ . C'est une *formule à paramètres*, mais ce n'est **pas une formule**.

**Exemple 2.11.** Dans  $\mathcal{L} = \{S\}$  où  $S$  est une relation binaire, on considère deux modèles :

- ▷  $\mathcal{N} : |\mathcal{N}| = \mathbb{N}$  avec  $S_{\mathcal{N}} = \{(x, y) \mid x < y\}$ ,
- ▷  $\mathcal{R} : |\mathcal{R}| = \mathbb{R}$  avec  $S_{\mathcal{R}} = \{(x, y) \mid x < y\}$ ;

et deux formules

- ▷  $F = \forall x \forall y (S x y \rightarrow \exists z (S x z \wedge S z y))$ ,
- ▷  $G = \exists x \forall y (x = y \vee S x y)$ ;

alors on a

$$\mathcal{N} \not\models F \quad \mathcal{R} \models F \quad \mathcal{N} \models G \quad \mathcal{R} \not\models G.$$

En effet, la formule  $F$  représente le fait d'être un ordre dense, et  $G$  d'avoir un plus petit élément.

**Définition 2.18.** Dans un langage  $\mathcal{L}$ , une formule  $F$  est un *théorème (logique)* si pour toute structure  $\mathcal{M}$  et tout environnement  $e$ , on a  $\mathcal{M}, e \models F$ .

**Exemple 2.12.** Quelques théorèmes simples :  $\forall x \neg \perp$ , et  $\forall x x = x$  et même  $x = x$  car on ne demande pas que la formule soit clause.

Dans  $\mathcal{L}_g = \{e, *, \square^{-1}\}$ , on considère deux formules

- ▷  $F = \forall x \forall y \forall z ((x * (y * z) = (x * y) * z) \wedge x * e = e * x = x \wedge \exists t (x * t = e \wedge t * x = e))$ ;
- ▷ et  $G = \forall e' = \forall e' (\forall x (x * e' = e' * x = x) \rightarrow e = e')$ .



Aucun des deux n'est un théorème (il n'est vrai que dans les groupes pour  $F$  (c'est même la définition de groupe) et dans les monoïdes pour  $G$  (unicité du neutre)), mais  $F \rightarrow G$  est un théorème logique.

**Définition 2.19.** Soient  $\mathcal{L}$  et  $\mathcal{L}'$  deux langages. On dit que  $\mathcal{L}'$  *enrichit*  $\mathcal{L}$  ou que  $\mathcal{L}$  est une *restriction* de  $\mathcal{L}'$  si  $\mathcal{L} \subseteq \mathcal{L}'$ .

Dans ce cas, si  $\mathcal{M}$  est une interprétation de  $\mathcal{L}$ , et si  $\mathcal{M}'$  est une interprétation de  $\mathcal{L}'$  alors on dit que  $\mathcal{M}'$  est un *enrichissement* de  $\mathcal{M}$  ou que  $\mathcal{M}$  est une *restriction* de  $\mathcal{M}'$  ssi  $|\mathcal{M}| = |\mathcal{M}'|$  et chaque symbole de  $\mathcal{L}$  a la même interprétation dans  $\mathcal{M}$  et  $\mathcal{M}'$ , i.e. du point de vue de  $\mathcal{L}$ ,  $\mathcal{M}$  et  $\mathcal{M}'$  sont les mêmes.

**Exemple 2.13.** Avec  $\mathcal{L} = \{e, *\}$  et  $\mathcal{L}' = \{e, *, \square^{-1}\}$  alors  $\mathcal{L}'$  est une extension de  $\mathcal{L}$ . On considère

- ▷  $\mathcal{M} : \quad |\mathcal{M}| = \mathbb{Z} \quad e_{\mathcal{M}} = 0_{\mathbb{Z}} \quad *_{\mathcal{M}} = +_{\mathbb{Z}} ;$
- ▷  $\mathcal{M}' : \quad |\mathcal{M}'| = \mathbb{Z} \quad e_{\mathcal{M}'} = 0_{\mathbb{Z}} \quad *_{\mathcal{M}'} = +_{\mathbb{Z}} \quad \square_{\mathcal{M}'}^{-1} = \text{id}_{\mathbb{Z}},$

et alors  $\mathcal{M}'$  est une extension de  $\mathcal{M}$ .

**Proposition 2.1.** Si  $\mathcal{M}$  une interprétation de  $\mathcal{L}$  est un enrichissement de  $\mathcal{M}'$ , une interprétation de  $\mathcal{L}'$ , alors pour tout environnement  $e$ ,

1. si  $t$  est un terme de  $\mathcal{L}$ , alors  $\text{Val}_{\mathcal{M}}(t, e) = \text{Val}_{\mathcal{M}'}(t, e) ;$
2. si  $F$  est une formule de  $\mathcal{L}$  alors  $\text{Val}_{\mathcal{M}}(F, e) = \text{Val}_{\mathcal{M}'}(F, e).$

**Preuve.** En exercice. □

**Corollaire 2.2.** La vérité d'une formule dans une interprétation ne dépend que de la restriction de cette interprétation au langage de la formule. □

**Définition 2.20.** Deux formules  $F$  et  $G$  sont *équivalentes* si  $F \leftrightarrow G$  est un théorème logique.

**Proposition 2.2.** Toute formule est équivalente à une formule n'utilisant que les connecteurs logiques  $\neg$ ,  $\vee$  et  $\exists$ .  $\square$

**Définition 2.21.** Soient  $\mathcal{M}$  et  $\mathcal{N}$  deux interprétations de  $\mathcal{L}$ .

1. Un  $\mathcal{L}$ -morphisme de  $\mathcal{M}$  est une fonction  $\varphi : |\mathcal{M}| \rightarrow |\mathcal{N}|$  telle que

- ▷ pour chaque symbole de constante  $c$ , on a  $\varphi(c_{\mathcal{M}}) = c_{\mathcal{N}}$  ;
- ▷ pour chaque symbole  $f$  de fonction  $n$ -aire, on a

$$\varphi(f_{\mathcal{M}}(a_1, \dots, a_n)) = f_{\mathcal{N}}(\varphi(a_1), \dots, \varphi(a_n)) ;$$

- ▷ pour chaque symbole  $R$  de relation  $n$ -aire (autre que « = »), on a

$$(a_1, \dots, a_n) \in R_{\mathcal{M}} \text{ ssi } (\varphi(a_1), \dots, \varphi(a_n)) \in R_{\mathcal{N}}.$$

- ▷ Un  $\mathcal{L}$ -isomorphisme est un  $\mathcal{L}$ -morphisme bijectif.
- ▷ Si  $\mathcal{M}$  et  $\mathcal{N}$  sont *isomorphes* s'il existe un  $\mathcal{L}$ -isomorphisme de  $\mathcal{M}$  à  $\mathcal{N}$ .

**Remarque 2.13.** 1. On ne dit rien sur « = » car si on impose la même condition que pour les autres relations alors nécessairement  $\varphi$  est injectif.

2. La notion dépend du langage  $\mathcal{L}$ .

3. Lorsqu'on a deux structures isomorphes, on les confonds, ce sont les mêmes, c'est un renommage.

**Exemple 2.14.** Avec  $\mathcal{L}_{\text{ann}} = \{0, +, \times, -\}$  et  $\mathcal{L}' = \mathcal{L}_{\text{ann}} \cup \{1\}$ , et les deux modèles  $\mathcal{M} : \mathbb{Z}/3\mathbb{Z}$  et  $\mathcal{N} = \mathbb{Z}/12\mathbb{Z}$ , on considère la

fonction définie (on néglige les cas inintéressants) par  $\varphi(\bar{n}) = \overline{4n}$ .

Est-ce que  $\varphi$  est un morphisme de  $\mathcal{M}$  dans  $\mathcal{N}$  ? Oui... et non... Dans  $\mathcal{L}$  c'est le cas, mais pas dans  $\mathcal{L}'$  car  $\varphi(1) = 4$ .

**Exemple 2.15.** Dans  $\mathcal{L} = \{c, f, R\}$  avec  $f$  une fonction binaire, et  $R$  une relation binaire, on considère

- ▷  $\mathcal{M} : \mathbb{R}, 0, +, \leq ;$
- ▷  $\mathcal{N} : ]0, +\infty[, 1, \times, \leq .$

Existe-t-il un morphisme de  $\mathcal{M}$  dans  $\mathcal{N}$  ? Oui, il suffit de poser le morphisme  $\varphi : x \mapsto e^x$ .

**Proposition 2.3.** La composée de deux morphismes (*resp.* isomorphisme) est un morphisme (*resp.* un isomorphisme).  $\square$

**Notation.** Si  $\varphi$  est un morphisme de  $\mathcal{M}$  dans  $\mathcal{N}$  et  $e$  un environnement de  $\mathcal{M}$ , alors on note  $\varphi(e)$  pour  $\varphi \circ e$ . C'est un environnement de  $\mathcal{N}$ .

**Lemme 2.3.** Soient  $\mathcal{M}$  et  $\mathcal{N}$  deux interprétations de  $\mathcal{L}$ , et  $\varphi$  un morphisme de  $\mathcal{M}$  dans  $\mathcal{N}$ . Alors pour tout terme  $t$  et environnement  $e$ , on a

$$\varphi(\text{Val}_{\mathcal{M}}(t, e)) = \text{Val}_{\mathcal{N}}(t, \varphi(e)).$$

$\square$

**Lemme 2.4.** Soient  $\mathcal{M}$  et  $\mathcal{N}$  deux interprétations de  $\mathcal{L}$ , et  $\varphi$  un morphisme **injectif** de  $\mathcal{M}$  dans  $\mathcal{N}$ . Alors pour toute formule atomique  $F$  et environnement  $e$ , on a

$$\mathcal{M}, e \models F \text{ ssi } \mathcal{N}, \varphi(e) \models F$$

**Lemme 2.5.** Soient  $\mathcal{M}$  et  $\mathcal{N}$  deux interprétations de  $\mathcal{L}$ , et  $\varphi$  un **isomorphisme**<sup>5</sup> de  $\mathcal{M}$  dans  $\mathcal{N}$ . Alors pour toute formule  $F$  et

environnement  $e$ , on a

$$\mathcal{M}, e \models F \text{ ssi } \mathcal{N}, \varphi(e) \models F$$

**Corollaire 2.3.** Deux interprétations isomorphismes satisfont les mêmes formules closes.

**Exercice 2.4.** Les groupes  $\mathbb{Z}/4\mathbb{Z}$  et  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  sont-ils isomorphes ? Non. En effet, les deux formules

- ▷  $\exists x (x \neq e \wedge x * x \neq e \wedge x * (x * x) \neq e \wedge x * (x * (x * x)) = e)$ ,
- ▷  $\forall x (x * x) = e$

ne sont pas vraies dans les deux (pour la première, elle est vraie dans  $\mathbb{Z}/4\mathbb{Z}$  mais pas dans  $(\mathbb{Z}/2\mathbb{Z})^2$  et pour la seconde, c'est l'inverse).

**Remarque 2.14.** La réciproque du corollaire est *fausse* : deux interprétations qui satisfont les mêmes formules closes ne sont pas nécessairement isomorphes. Par exemple, avec  $\mathcal{L} = \{\leq\}$ , les interprétations  $\mathbb{R}$  et  $\mathbb{Q}$  satisfont les mêmes formules closes, mais ne sont pas isomorphes.

**Définition 2.22.** Soit  $\mathcal{L}$  un langage,  $\mathcal{M}$  et  $\mathcal{N}$  deux interprétations de  $\mathcal{L}$ . On dit que  $\mathcal{N}$  est une *extension* de  $\mathcal{M}$  (ou  $\mathcal{M}$  est une *sous-interprétation* de  $\mathcal{N}$ ) si les conditions suivantes sont satisfaites :

- ▷  $|\mathcal{M}| \subseteq |\mathcal{N}|$  ;
- ▷ pour tout symbole de constante  $c$ , on a  $c_{\mathcal{M}} = c_{\mathcal{N}}$  ;
- ▷ pour tout symbole de fonction  $n$ -aire  $f$ , on a  $f_{\mathcal{M}} = f_{\mathcal{N}}|_{|\mathcal{M}|^n}$  (donc en particulier  $f_{\mathcal{N}}(|\mathcal{M}|^n) \subseteq |\mathcal{M}|$ ) ;
- ▷ pour tout symbole de relation  $n$ -aire  $R$ , on a  $R_{\mathcal{M}} = R_{\mathcal{N}} \cap |\mathcal{M}|^n$ .

5. On utilise ici la *surjectivité* pour le «  $\exists$  ».

**Proposition 2.4.** Soient  $\mathcal{M}$  et  $\mathcal{N}$  deux interprétations de  $\mathcal{L}$ . Alors  $\mathcal{M}$  est isomorphe à une sous-interprétation  $\mathcal{M}'$  de  $\mathcal{N}$  si et seulement si, il existe un morphisme injectif de  $\mathcal{M}$  dans  $\mathcal{N}$ .

**Exemple 2.16 (Construction de  $\mathbb{Z}$  à partir de  $\mathbb{N}$ ).** On pose la relation  $(p, q) \sim (p', q')$  si  $p + q' = p' + q$ . C'est une relation d'équivalence sur  $\mathbb{N}^2$ . On pose  $\mathbb{Z} := \mathbb{N}^2 / \sim$  (il y a un isomorphisme  $\mathbb{N}^2 / \sim \rightarrow \mathbb{Z}$  par  $(p, q) \mapsto p - q$ ). Est-ce qu'on a  $\mathbb{N} \subseteq \mathbb{N}^2 / \sim$ ? D'un point de vue ensembliste, non. Mais, généralement, l'inclusion signifie avoir un morphisme injectif de  $\mathbb{N}$  dans  $\mathbb{N}^2 / \sim$ .

**Définition 2.23.** Une *théorie* est un ensemble (fini ou pas) de formules closes. Les éléments de la théorie sont appelés *axiomes*.

**Exemple 2.17.** La *théorie des groupes* est

$$T_{\text{groupe}} := \left\{ \begin{aligned} &\forall x (x * e = e * x = x), \\ &\forall x (x * x^{-1} = e \wedge x^{-1} * x = e), \\ &\forall x \forall y \forall z (x * (y * z) = (x * y) * z) \end{aligned} \right\}$$

dans le langage  $\mathcal{L}_g$ .

**Exemple 2.18.** La *théorie des ensembles infinis* est

$$T_{\text{ens infinis}} := \left\{ \begin{aligned} &\exists x (x = x), \\ &\exists x \exists y (x \neq y), \\ &\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge z \neq x) \\ &\dots \end{aligned} \right\}$$

dans le langage  $\mathcal{L}_{\text{ens}}$ .

**Définition 2.24 (Sémantique).** ▷ Une interprétation  $\mathcal{M}$  *satisfait*  $T$  (ou  $\mathcal{M}$  est un *modèle* de  $T$ ), noté  $\mathcal{M} \models T$ , si  $\mathcal{M}$  satisfait toutes les formules de  $T$ .

▷ Une théorie  $T$  est *contradictoire* s'il n'existe pas de modèle de  $T$ . Sinon, on dit qu'elle est *non-contradictoire*, ou *satisfiable*, ou *satisfaisable*.

**Exemple 2.19.** Les deux théories précédentes,  $T_{\text{groupes}}$  et  $T_{\text{ens infinis}}$ , sont non-contradictaires.

**Définition 2.25 (Syntaxique).** Soit  $T$  une théorie.

- ▷ Soit  $A$  une formule. On note  $T \vdash A$  s'il existe un sous-ensemble fini  $T'$  tel que  $T' \subseteq T$  et  $T' \vdash A$ .
- ▷ On dit que  $T$  est *consistante* si  $T \not\vdash \perp$ , sinon  $T$  est *inconsistante*.
- ▷ On dit que  $T$  est *complète* (« *axiome-complète* ») si  $T$  est consistante et, pour toute formule  $F \in \mathcal{F}$ , on a  $T \vdash F$  ou on a  $T \vdash \neg F$ .

**Exemple 2.20.** La théorie des groupes n'est pas complète : par exemple,

$$F := \forall x \forall y (x * y = y * x)$$

est parfois vraie, parfois fausse, cela dépend du groupe considéré.

**Exemple 2.21.** La théorie

$$T = \mathbf{Th}(\mathbb{N}) := \{\text{les formules } F \text{ vraies dans } \mathbb{N}\}$$

est complète mais pas pratique.

De par le théorème d'*incomplétude de Gödel* (c'est un sens différent du « complet » défini avant), on montre qu'on ne peut pas avoir de *joli* ensemble d'axiomes pour  $\mathbb{N}$ .

**Proposition 2.5.** Soit  $T$  une théorie complète.

1. Soit  $A$  une formule close. On a  $T \vdash \neg A$  ssi  $T \not\vdash A$ .
2. Soient  $A$  et  $B$  des formules closes. On a  $T \vdash A \vee B$  ssi  $T \vdash A$  ou  $T \vdash B$ .

**Preuve.**  $\triangleright$  Si  $T \vdash \neg A$  et  $T \vdash A$ , alors il existe  $T', T'' \subseteq_{\text{fini}} T$  tels que  $T' \vdash \neg A$  et  $T'' \vdash A$ . On a donc  $T' \cup T'' \vdash \perp$  par :

$$\frac{\frac{T' \vdash \neg A}{T' \cup T'' \vdash \neg A} \text{ aff} \quad \frac{T'' \vdash A}{T' \cup T'' \vdash A} \text{ aff}}{T' \cup T'' \vdash \perp} \neg_e$$

On en conclut que  $T \vdash \perp$ , absurde car  $T$  supposée complète donc consistante. On a donc  $T \vdash \neg A$  implique  $T \not\vdash A$ .

Réciproquement, si  $T \not\vdash A$  et  $T \not\vdash \neg A$ , alors c'est impossible car  $T$  est complète. On a donc  $T \not\vdash A$  implique  $T \vdash \neg A$ .

- $\triangleright$  Si  $T \vdash A$  ou  $T \vdash B$ , alors par la règle  $\vee_i^g$  ou  $\vee_i^d$ , on montre que  $T \vdash A \vee B$ .

Réciproquement, si  $T \vdash A \vee B$  et  $T \not\vdash A$  et  $T \not\vdash B$  alors, par 1, on a  $T \vdash \neg A$  et  $T \vdash \neg B$ . On montre ainsi (en exercice) que  $T \vdash \neg(A \vee B)$  d'où  $T \vdash \perp$  par  $\neg_e$ . C'est impossible car  $T$  est complète donc consistante, d'où  $T \vdash A \vee B$  implique  $T \vdash A$  ou  $T \vdash B$ .

□

## 2.5 Théorème de complétude de Gödel.

**Théorème 2.1** (Complétude de Gödel (à double sens)).

**Version 1.** Soit  $T$  une théorie et  $F$  une formule close. On a  $T \vdash F$  ssi  $T \models F$ .

**Version 2.** Une théorie  $T$  est consistante (syntaxe) ssi elle est non-contradictoire (sémantique).

**Remarque 2.15.** La version 1 se décompose en deux théorèmes :

- ▷ le *théorème de correction* (ce que l'on prouve est vrai)

$$T \vdash F \implies T \models F ;$$

- ▷ le *théorème de complétude* (ce qui est vrai est prouvable)

$$T \models F \implies T \vdash F.$$

Pour la version 2, on peut aussi la décomposer en deux théorèmes<sup>6</sup> :

- ▷ la *correction*,  $T$  non-contradictoire implique  $T$  consistante ;
- ▷ la *complétude*,  $T$  consistante implique  $T$  non-contradictoire.

Par contraposée, on a aussi qu'une théorie contradictoire est inconsistante.

**Proposition 2.6.** Les deux versions du théorème de correction sont équivalentes.

**Preuve.** ▷ D'une part, on montre (par contraposée) « non V2 implique non V1 ». Soit  $T$  non-contradictoire et inconsistante. Il existe un modèle  $\mathcal{M}$  tel que  $\mathcal{M} \models T$  et  $T \vdash \perp$ . Or, par définition,  $\mathcal{M} \not\models \perp$  donc  $T \not\models \perp$ .

▷ D'autre part, on montre « V2 implique V1 ». Soit  $T$  et  $F$  tels que  $T \vdash F$ . Ainsi,  $T \cup \neg F \vdash \perp$ , d'où  $T \cup \{\neg F\}$  est inconsistante, et d'où, par la version 2 de la correction, on a que  $T \cup \{\neg F\}$  contradictoire, donc on n'a pas de modèle. On a alors que, tous les modèles de  $T$  sont des modèles de  $F$ , autrement dit  $T \models F$ .

□

6. On a une négation dans ce théorème, donc ce n'est pas syntaxe implique sémantique pour la correction, mais non sémantique implique non syntaxe.



**Proposition 2.7.** Les deux versions du théorème de complétude (sens unique) sont équivalentes.

**Preuve.** ▷ Soit  $T$  contradictoire. Elle n'a pas de modèle. Ainsi, on a  $T \models \perp$  d'où  $T \vdash \perp$  par la version 1, elle est donc inconsistante.

▷ Soit  $T \models F$ . Considérons  $T \cup \{\neg F\}$  : cette théorie n'a pas de modèle, donc est contradictoire, donc est inconsistante, et on a donc que  $T \cup \{\neg F\} \vdash \perp$  d'où  $T \vdash F$  par  $\perp_e$ .

□

**Remarque 2.16 (Attention !).** On utilise «  $\models$  » dans deux sens.

- ▷ Dans le sens *modèle*  $\models$  *formule*, on dit qu'une formule est vraie dans un modèle, c'est le sens des mathématiques classiques.
- ▷ Dans le sens *théorie*  $\models$  *formule*, on dit qu'une formule est vraie dans tous les modèles de la théorie, c'est un sens des mathématiques plus inhabituel.

## 2.5.1 Preuve du théorème de correction.

**Exercice 2.5.** Montrer que le lemme ci-dessous implique la version 1 de la correction.

**Lemme 2.6.** Soient  $T$  une théorie,  $\mathcal{M}$  un modèle et  $F$  une formule close. Si  $\mathcal{M} \models T$  et  $T \vdash F$  alors  $\mathcal{M} \models F$ .

**Preuve.** Comme d'habitude, pour montrer quelque chose sur les formules closes, on commence par les formules et même les termes. On commence par montrer que la substitution dans les termes a un sens sémantique.

**Lemme 2.7.** Soient  $t$  et  $u$  des termes et  $e$  un environnement. Soient  $v := t[x := u]$  et  $e' := e[x := \mathcal{V}al(u, e)]$ . Alors,  $\mathcal{V}al(v, e) = \mathcal{V}al(t, e')$ .

**Preuve.** En exercice.  $\square$

**Lemme 2.8.** Soit  $A$  une formule,  $t$  un terme, et  $e$  un environnement. Si  $e' := e[x := \mathcal{V}al(t, e)]$  alors  $\mathcal{M}, e \models A[x := t]$  ssi  $\mathcal{M}, e' \models A$ .

**Preuve.** En exercice.  $\square$

On termine la preuve en montrant la proposition ci-dessous.  $\square$

Montrons cette proposition plus forte que le lemme.

**Proposition 2.8.** Soient  $\Gamma$  un ensemble de formules et  $A$  une formule. Soit  $\mathcal{M}$  une interprétation et soit  $e$  un environnement. Si  $\mathcal{M}, e \models \Gamma$ , et  $\Gamma \vdash A$  alors  $\mathcal{M}, e \models A$ .

**Preuve.** Par induction sur la preuve de  $\Gamma \vdash A$ , on montre la proposition précédente.

- ▷ Cas inductif  $\rightarrow_i$ . On sait que  $A$  est de la forme  $B \rightarrow C$ , et on montre que de  $\Gamma, B \vdash C$  on montre  $\Gamma \vdash B \rightarrow C$ . Soient  $\mathcal{M}$  et  $e$  tels que  $\mathcal{M}, e \models \Gamma$ . Montrons que  $\mathcal{M}, e \models B \rightarrow C$ . Il faut donc montrer que si  $\mathcal{M}, e \models B$  alors  $\mathcal{M}, e \models C$ . Si  $\mathcal{M}, e \models B$  alors  $\mathcal{M}, e \models \Gamma \cup \{B\}$ . Or, comme  $\Gamma, B \vdash C$  alors par hypothèse d'induction, on a que  $\mathcal{M}, e \models C$ .
- ▷ Cas inductif  $\forall_e$ . Si  $A$  est de la forme  $B[x := t]$ , alors de  $\Gamma \vdash \forall x B$ , on en déduit que  $\Gamma \vdash B[x := t]$ . Soit  $\mathcal{M}, e \models \Gamma$  et  $a := \mathcal{V}al(t, e)$ . Par hypothèse de récurrence, on a que  $\mathcal{M}, e \models \forall x B$  donc  $\mathcal{M}, e[x := a] \models B$  et d'après le lemme précédent, on a que  $\mathcal{M}, e \models B[x := t]$ .
- ▷ Les autres cas inductifs sont laissés en exercices.

- ▷ Cas de base  $\mathbf{ax}$ . Si  $A \in \Gamma$  et  $\mathcal{M}, e \models \Gamma$  alors  $\mathcal{M}, e \models A$ .
- ▷ Cas de base  $=_i$ . On a, pour tout  $\mathcal{M}, e$  que  $\mathcal{M}, e \models t = t$ .  $\square$

Cette proposition permet de conclure la preuve du lemme précédent.

## 2.5.2 Preuve du théorème de complétude.

On va montrer la version 2, en *trois étapes*. Soit  $T$  une théorie consistante sur le langage  $\mathcal{L}$ .

1. On enrichit le langage  $\mathcal{L}$  en  $\mathcal{L}'$  avec des constantes, appelées *témoins de Henkin*, et qui nous donnerons les éléments de notre ensemble de base : les termes.
2. Pour définir complètement le modèle, on complète la théorie  $T$  en une théorie  $\text{Th}$  sur  $\mathcal{L}'$ .
3. On quotiente pour avoir la vraie égalité dans le modèle.

Cette construction est assez similaire à la définition de  $\mathbb{C}$  comme le quotient  $\mathbb{R}[X]/(X^2 + 1)$ .

**Proposition 2.9.** On peut étendre  $\mathcal{L}$  en  $\mathcal{L}'$  et  $T$  en  $T'$  consistante telle que, pour toute formule  $F(x)$  de  $\mathcal{L}'$ , ayant pour seule variable libre  $x$ , il existe un symbole de constante  $c_F$  de  $\mathcal{L}'$  telle que l'on ait  $T' \vdash \exists x F(x) \rightarrow F(c_F)$ , d'où le nom de témoin.

**Preuve.** On fait la construction « par le bas » :

- ▷  $\mathcal{L}_0 = \mathcal{L}$  ;
- ▷  $T_0 = T$  ;
- ▷  $\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{c_F \mid F \text{ formule à une variable libre de } \mathcal{L}_n\}$  ;
- ▷  $T_{n+1} = T_n \cup \{\exists x F \rightarrow F(c_F) \mid F \text{ formule de } \mathcal{L}_n\}$  ;
- ▷ et enfin  $\mathcal{L}' = \bigcup_{n \in \mathbb{N}} \mathcal{L}_n$  et  $T' = \bigcup_{n \in \mathbb{N}} T_n$ .

On commence par montrer quelques lemmes.

**Lemme 2.9.** Soient  $\Gamma$  un ensemble de formules et  $A$  une formule. Soit  $c$  un symbole de constante qui n'apparaît ni dans  $\Gamma$  ni dans  $A$ . Si  $\Gamma \vdash A[x := c]$  alors  $\Gamma \vdash \forall x A$ .

**Preuve.** Idée de la preuve. On peut supposer que  $x$  n'apparaît pas dans  $\Gamma$ , ni dans la preuve de  $\Gamma \vdash A[x := c]$ , sinon on renomme  $x$  en  $y$  dans l'énoncé du lemme. Alors, de la preuve de  $\Gamma \vdash A[x := c]$ , on peut déduire une preuve de  $\Gamma \vdash A(x)$  en remplaçant  $c$  par  $x$ . Avec la règle  $\forall_i$ , on en conclut que  $\Gamma \vdash \forall x A$ .  $\square$

**Lemme 2.10.** Pour toute formule  $F$  à une variable libre  $x$  sur le langage  $\mathcal{L}'$ ,

$$T' \vdash \exists x F(x) \rightarrow F(c_F).$$

**Preuve.** La formule  $F$  a un nombre fini de constantes (car c'est un mot fini), donc  $F$  est une formule sur  $\mathcal{L}_n$  pour un certain  $n \in \mathbb{N}$ , donc  $(\exists x F(x) \rightarrow F(c_F)) \in T_{n+1} \subseteq T'$ .  $\square$

Il nous reste à montrer que la théorie  $T'$  est consistante.

Il suffit de montrer que tous les  $T_n$  sont consistantes. En effet, si  $T'$  est non-consistante, il existe un ensemble fini  $T'' \subseteq T'$  et  $T'' \vdash \perp$ . Comme  $T''$  fini, il existe un certain  $n \in \mathbb{N}$  tel que  $T'' \subseteq T_n$  et donc  $T_n \vdash \perp$ .

On montre par récurrence sur  $n$  que  $T_n$  est consistante.

- ▷ On a  $T_0 = T$  qui est consistante par hypothèse.
- ▷ Supposons  $T_n$  consistante et que  $T_{n+1} \vdash \perp$ . Alors, il existe des formules à une variable libre  $F_1, \dots, F_k$  écrites sur  $\mathcal{L}_n$  et

$$T_n \cup \{ \exists x F_i \rightarrow F_i(c_{F_i}) \mid 1 \leq i \leq k \} \vdash \perp.$$

Ainsi (exercice)

$$T_n \vdash \left( \bigwedge_{1 \leq i \leq k} (\exists x F_i \rightarrow F_i(c_{F_i})) \right) \rightarrow \perp.$$

Les  $c_{F_i}$  ne sont pas dans  $T_n$  d'où, d'après le lemme 2.9, que

$$T_n \vdash \forall y_1 \forall y_2 \dots \forall y_n \left( \bigwedge_{1 \leq i \leq k} (\exists x F_i \rightarrow F_i(y_i)) \right) \rightarrow \perp.$$

On peut montrer que (théorème logique)

$$(\star) \quad \vdash \forall y (A(y) \rightarrow \perp) \leftrightarrow (\exists y A(y) \rightarrow \perp),$$

d'où

$$T_n \vdash \left( \exists y_1 \exists y_2 \dots \exists y_n \bigwedge_{1 \leq i \leq k} (\exists x F_i \rightarrow F_i(y_i)) \right) \rightarrow \perp.$$

On a aussi

$$(\star\star) \quad \vdash \exists y_1 \exists y_2 (A(y_1) \wedge A(y_2)) \leftrightarrow (\exists y_1 A(y_1)) \wedge (\exists y_2 A(y_2)),$$

et pour  $y$  non libre dans  $A$ , on a

$$\vdash \exists y (A \rightarrow B) \leftrightarrow (A \rightarrow \exists y B).$$

On a donc

$$T_n \vdash \left( \bigwedge_{1 \leq i \leq k} (\exists x F_i(x) \rightarrow \exists y_i F_i(y_i)) \right) \rightarrow \perp.$$

Or,

$$(\star\star\star) \quad \vdash \bigwedge_{1 \leq i \leq k} (\exists x F_i(x) \rightarrow \exists y_i F_i(y_i)).$$

On a donc  $T_n \vdash \perp$ , ce qui contredit l'hypothèse, d'où  $T_{n+1}$  consistante.

En exercice, on pourra montrer les théorèmes logiques  $(\star)$ ,  $(\star\star)$ , et  $(\star\star\star)$ .

□

Ensuite, on veut compléter  $T'$  en préservant le résultat de la proposition précédente. On cherche Th (axiome-)complète telle que  $T' \subseteq \text{Th}$  et pour toute formule à une variable libre  $F$  de  $\mathcal{L}'$ , on a

$$\text{Th} \vdash \exists x F \rightarrow F(c_F).$$

Faisons le cas dénombrable (sinon, lemme de Zorn) : supposons  $\mathcal{L}'$  au plus dénombrable. Soit  $(F_n)_{n \in \mathbb{N}}$  une énumération des formules closes de  $\mathcal{L}'$ . On définit par récurrence

- ▷  $K_0 := T'$  ;
- ▷ si  $K_n$  est complète, alors  $K_{n+1} := K_n$  ;
- ▷ si  $K_n$  n'est pas complet, alors soit le plus petit  $p \in \mathbb{N}$  tel que l'on ait  $K_n \not\vdash F_p$  et  $K_n \not\vdash \neg F_p$ , et on pose  $K_{n+1} := K_n \cup \{F_p\}$ .

**Lemme 2.11.** On pose  $\text{Th} := \bigcup_{n \in \mathbb{N}} T_n$ . La théorie Th a les propriétés voulues.

**Preuve.** 1. On a  $T' \subseteq \text{Th}$ .

2. La théorie Th est consistante. En effet, il suffit de montrer que tous les  $K_n$  le sont (par les mêmes argument que la preuve précédente). Montrons le par récurrence.
  - ▷ La théorie  $K_0 = T'$  est consistante par hypothèse.
  - ▷ Si  $K_{n+1} = K_n$  alors  $K_{n+1}$  est consistante par hypothèse de récurrence.
  - ▷ Si  $K_{n+1} = K_n \cup \{F_p\}$ , et si  $K_n, F_p \vdash \perp$ , alors par la règle  $\neg_i$ , on a  $K_n \vdash \neg F_p$ , ce qui est faux. Ainsi  $K_{n+1}$  est consistante.

On en conclut que Th est consistante.

3. La théorie Th est complète. Sinon, à chaque étape  $K_{n+1} =$

$K_n \cup \{F_{q_n}\}$  et il existe  $F_p$  telle que  $\text{Th} \not\vdash F_p$  et  $\text{Th} \not\vdash \neg F_p$ . Ainsi, pour tout  $n \in \mathbb{N}$ ,  $K_n \not\vdash F_p$  et  $K_n \not\vdash \neg F_p$ , d'où pour tout  $n \in \mathbb{N}$ ,  $p_n \leq p$  avec des  $p_n$  distincts. C'est absurde, il n'y a qu'un nombre fini d'entiers inférieurs à un entier donné.

□

On construit un quotient avec «  $=$  » comme relation d'équivalence, puis on vérifie que les fonctions et relations sont bien définies (ne dépendent pas du représentant choisit, comme pour les groupes quotients).

Soit  $\mathcal{E}$  l'ensemble des termes clos de  $\mathcal{L}'$ , qui n'est pas vide car il contient les termes  $c_{x=x}$  (avec la définition de  $c_F$  ci-avant). On définit sur  $\mathcal{E}$  une relation  $\sim$ , où  $t \sim t'$  ssi  $\text{Th} \vdash t = t'$ .

**Exercice 2.6.** Montrer que  $\sim$  est une relation d'équivalence.

On pose enfin  $|\mathcal{M}| := \mathcal{E}/\sim$ . On notera  $\bar{t}$  la casse de  $t$ . On définit l'interprétation des symboles de  $\mathcal{L}'$  :

- ▷ si  $c$  est une constante, alors  $c_{\mathcal{M}} := \bar{c}$ ;
- ▷ si  $f$  est un symbole de fonctions d'arité  $n$ ,

$$f_{\mathcal{M}}(\bar{t}_1, \dots, \bar{t}_n) := \overline{f(t_1, \dots, t_n)}.$$

**Lemme 2.12.** La définition de dépend pas des représentants choisis, c'est-à-dire si  $\bar{u}_1 = \bar{t}_1, \dots, \bar{u}_n = \bar{t}_n$  alors

$$\overline{f(t_1, \dots, t_n)} = \overline{f(u_1, \dots, u_n)}.$$

**Preuve.** ▷ On a  $\text{Th} \vdash t_i = u_i$  pour tout  $i$  par hypothèse

- ▷ donc avec  $=_i$ , on a  $\text{Th} \vdash f(t_1, \dots, t_n) = f(t_1, \dots, t_n)$
- ▷ donc avec  $=_e$ , on a  $\text{Th} \vdash f(u_1, \dots, t_n) = f(t_1, \dots, t_n)$
- ▷ ...etc...
- ▷ donc avec  $=_e$ , on a  $\text{Th} \vdash f(u_1, \dots, u_n) = f(t_1, \dots, t_n)$



[suite de la définition de l'interprétation]

▷ si  $R$  est un symbole de relation d'arité  $n$ , on définit

$$(\bar{t}_1, \dots, \bar{t}_n) \in R_{\mathcal{M}} \text{ ssi } \text{Th} \vdash R(t_1, \dots, t_n).$$

**Exercice 2.7.** Montrer que cette définition ne dépend pas des représentants choisis.

**Lemme 2.13.** Soit  $F$  une formule à  $n$  variables libres et  $t_1, \dots, t_n$  des termes clos. Alors,  $\mathcal{M} \models F[\bar{t}_1, \dots, \bar{t}_n]$  ssi  $\text{Th} \vdash F[t_1, \dots, t_n]$ , où l'on interprète la formule à paramètre dans l'environnement  $e$  avec  $e(y_i) = \bar{t}_i$  alors  $\mathcal{M}, e \models F(y_1, \dots, y_n)$ .

**Preuve.** Par induction sur  $F$  en supposant que  $F$  n'utilise que  $\neg$ ,  $\vee$ ,  $\exists$  comme connecteurs. En effet, on a pour toute formule  $G$ , il existe  $F$  qui n'utilise que  $\neg$ ,  $\vee$ ,  $\exists$  et  $\vdash F \leftrightarrow G$ , ce qui permet de conclure directement pour  $G$  si le résultat est vrai sur  $F$ .

- ▷ Pour  $F = \perp$ , alors on a  $\text{Th} \not\vdash \perp$  car  $\text{Th}$  consistante et  $\mathcal{M} \models \perp$  par définition.
- ▷ Pour  $F = R(u_1, \dots, u_m)$ , où les  $u_i$  sont des termes non nécessairement clos et où  $u_1, \dots, u_m$  sont des termes à  $n$  variables  $x_1, \dots, x_n$ . On pose

$$F[t_1, \dots, t_n] := R(\underbrace{u_1(t_1, \dots, t_n)}_{v_1}, \dots, \underbrace{u_m(t_1, \dots, t_n)}_{v_m})$$

où l'on définit  $v_i := u_i(t_1, \dots, t_n)$  qui est clos car les  $t_i$  sont clos. On veut montrer que

$$\mathcal{M} \models \underbrace{F[\bar{t}_1, \dots, \bar{t}_n]}_{R(\bar{v}_1, \dots, \bar{v}_m)} \text{ ssi } \text{Th} \vdash \underbrace{F[t_1, \dots, t_n]}_{R(v_1, \dots, v_m)}.$$



Or, on a l'équivalence  $\mathcal{M} \models R(\bar{v}_1, \dots, \bar{v}_m)$  ssi  $(\bar{v}_1, \dots, \bar{v}_m) \in R_{\mathcal{M}}$  ssi  $\text{Th} \vdash R(v_1, \dots, v_m)$ .

- ▷ Pour  $F = F_1 \vee F_2$ , et  $t_1, \dots, t_n$  sont des termes clos, on veut montrer que

$$\begin{aligned} \mathcal{M} &\models F_1[\bar{t}_1, \dots, \bar{t}_n] \vee F_2[\bar{t}_1, \dots, \bar{t}_n] \\ \text{ssi } \text{Th} &\vdash F_1[t_1, \dots, t_n] \vee F_2[t_1, \dots, t_n]. \end{aligned}$$

Or,

$$\begin{aligned} \mathcal{M} &\models F_1[\bar{t}_1, \dots, \bar{t}_n] \vee F_2[\bar{t}_1, \dots, \bar{t}_n] \\ \text{ssi } \mathcal{M} &\models F_1[\bar{t}_1, \dots, \bar{t}_n] \text{ ou } \mathcal{M} \models F_2[\bar{t}_1, \dots, \bar{t}_n] \\ \text{ssi } \text{Th} &\vdash F_1[t_1, \dots, t_n] \text{ ou } \text{Th} \vdash F_2[t_1, \dots, t_n] \end{aligned}$$

par hypothèse. Ainsi,

- avec  $\vee_i^g$  et  $\vee_i^d$ , on a que  $\text{Th} \vdash F_1[t_1, \dots, t_n] \vee F_2[t_1, \dots, t_n]$  ;
- réciproquement, on utilise le lemme 2.5 car  $\text{Th}$  est complète.

- ▷ Pour  $F = \neg G$ , en exercice.
- ▷ Si  $F = \exists x G$  et  $t_1, \dots, t_n$  des termes clos, on a
- on a  $\mathcal{M} \models \exists x G[\bar{t}_1, \dots, \bar{t}_n, x]$
  - ssi il existe  $t \in \mathcal{E}$  tel que  $\mathcal{M} \models G[\bar{t}_1, \dots, \bar{t}_n, t]$
  - ssi il existe  $t \in \mathcal{E}$  tel que  $\text{Th} \vdash G(t_1, \dots, t_n, t)$

et donc  $\text{Th} \vdash \exists x G(t_1, \dots, t_n, x)$  avec  $\exists_i$ . Réciproquement, si  $\text{Th} \vdash \exists x G(t_1, \dots, t_n, x)$  alors  $\text{Th} \vdash G(t_1, \dots, t_n, c_{G(t_1, \dots, t_n, x)})$ , donc il existe un terme  $t$  et  $\text{Th} \vdash G(t_1, \dots, t_n, t)$ .

□

**Lemme 2.14.** On a  $\mathcal{M} \models \text{Th}$  (et donc  $\mathcal{M} \models T$ ).

**Preuve.** On montre que, pour toute formule  $F$  de  $\text{Th}$ , on a que  $\mathcal{M} \models F$ . Pour cela, on utilise le lemme précédent : si  $F$  est close,

alors

$$\mathcal{M} \models F \text{ ssi } \text{Th} \vdash F.$$

□

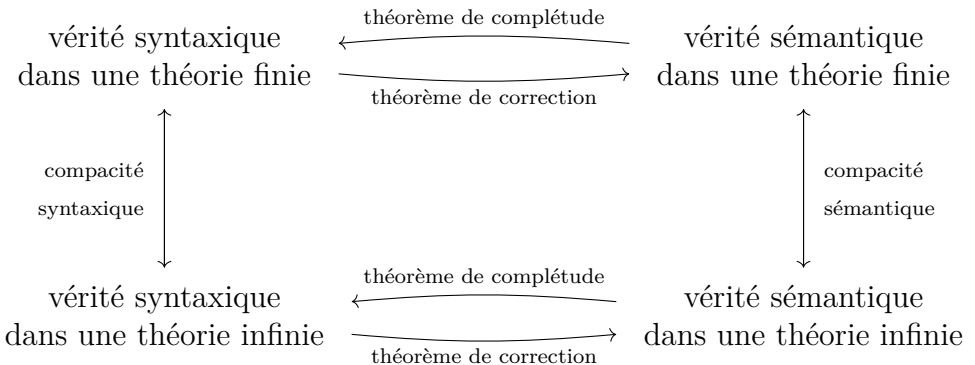
### 2.5.3 Compacité.

**Théorème 2.2** (Compacité (sémantique)). Une théorie  $T$  est contradictoire ssi elle est finiment contradictoire, *i.e.* il existe  $T' \subseteq_{\text{fini}} T$  telle que  $T'$  est contradictoire.

**Preuve.** Soit  $T$  contradictoire. On utilise le théorème de complétude. Ainsi  $T$  est inconsistante. Il existe donc  $T' \subseteq_{\text{fini}} T$  avec  $T'$  inconsistante par le théorème de compacité syntaxique ci-dessous (qui est trivialement vrai). On applique de nouveau le théorème de complétude pour en déduire que  $T'$  est contradictoire. □

**Théorème 2.3** (Compacité (syntaxique)). Une théorie  $T$  est inconsistante ssi elle est finiment inconsistante.

**Preuve.** Ceci est évident car une preuve est nécessairement finie. □



Dans la suite de cette sous-section, on étudie des applications du théorème de compacité.

**Théorème 2.4.** Si une théorie  $T$  a des modèles finis arbitrairement grands, alors elle a un modèle infini.  $\square$

**Corollaire 2.4.** Il n'y a pas de théorie des groupes finis *i.e.* un ensemble d'axiomes dont les modèles sont exactement les groupes finis.

**Théorème 2.5 (Löwenheim-Skolem).** Soit  $T$  une théorie dans un langage  $\mathcal{L}$  et  $\kappa$  un cardinal et  $\kappa \geq \text{card } \mathcal{L}$  et  $\kappa \geq \aleph_0$ .<sup>7</sup> Si  $T$  a un modèle infini, alors  $T$  a un modèle de cardinal  $\kappa$ .

**Exemple 2.22.**  $\triangleright$  Avec  $T = \mathbf{Th}(\mathbb{N})$ , on a  $\kappa = \text{card } \mathbb{R}$ .  
 $\triangleright$  Avec  $T = \mathbf{ZFC}$ , on a  $\kappa = \aleph_0 = \text{card } \mathbb{N}$ .

---

7. Ici,  $\aleph_0$  est le cardinal de  $\mathbb{N}$ , on dit donc que  $\kappa$  est infini.