Logique

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

ENS DE LYON

28 février 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 $\{(,)\}$.

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 $\neg F$, $(F_1 \vee F_2)$, $(F_1 \wedge F_2)$, $(F_1 \to F_2)$ et $(F_1 \leftrightarrow F_2)$ 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

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

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 :

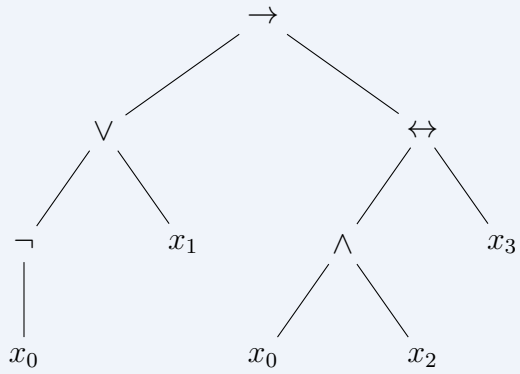
- $G \in \mathscr{P}$;
- il existe $F \in \mathscr{F}$ telle que $G = \neg F$;
- il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \vee F_2)$;
- il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \wedge F_2)$;
- il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \to F_2)$;
- il existe $F_1, F_2 \in \mathscr{F}$ 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. La formule $((\neg x_0 \vee x_1) \to ((x_0 \wedge x_2) \leftrightarrow x_3))$ correspond à l'arbre



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 disjonction de cas
  - si $F = \neg G$ avec $G \in \mathscr{F}_n$, 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 $\mathscr{P}$ 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 $\mathscr{P} = \{x_0, x_1, \ldots\}$ 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 $\varepsilon_0, \ldots, \varepsilon_n, \ldots$ tels que $\nu(x_0) = \varepsilon_0, \ldots, \nu(x_n) = \varepsilon_n, \ldots$

- ▷ 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 $\varepsilon_0, \ldots, \varepsilon_n$ (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 $\mathscr{C}$, 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 $\mathscr{C}$, 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 $\mathscr{C}$ 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 $\mathscr{C}$. 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 $\mathscr{C}$. Soit $F \in \mathscr{C}$. 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 $\mathscr{C}$. □

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-vide, il admet au moins un élément maximal.

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

Preuve. Soit $\mathscr{C}$ 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 $\mathscr{C}$ de $\mathscr{C}$ en une valuation satisfaisant $\mathscr{C}$. C'est-à-dire :

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

L'ensemble $\mathcal{V}$ est non-vide car contient l'application vide de $\{0,1\}^{\emptyset}$ car $\mathscr{C}$ 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 $\mathscr{C}$. 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 $\{x_{i_1}, \dots, x_{i_n}\} \subseteq \operatorname{dom}(\lambda)$. Il existe $\varphi_1, \dots, \varphi_n$ dans $\mathscr{C}$ telle que $x_{i_1} \in \operatorname{dom}\varphi_1, \dots, x_{i_n} \in \operatorname{dom}\varphi_n$. 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, $x_{i_1}, \dots, x_{i_n} \in \operatorname{dom}(\varphi_0)$. 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 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 « $\bot$ » 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

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

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

Exemple 2.4.
- ▷ Dans $\mathscr{L}_{\text{g}}$, $*(*(x, \square^{-1}(y)), e)$ est un terme, qu'on écrira plus simplement en $(x * y^{-1}) * e$.
- ▷ Dans $\mathscr{L}_{\text{co}}$, $(x + x) + (-0)^{-1}$ est un terme.
- ▷ Dans $\mathscr{L}_{\text{ens}}$, $(\emptyset^{\mathsf{c}} \cup \emptyset) \cap (x \cup y)^{\mathsf{c}}$ 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 $t \in \mathcal{T}_k$.

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

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

▷ 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* $\mathscr{F}$ du langage $\mathscr{L}$ est défini par

- on pose $\mathscr{F}_0$ l'ensemble des formules atomiques ;
- on pose $\mathscr{F}_{k+1} = \mathscr{F}_k \cup \left\{ \begin{array}{c|c} (\neg F) & \\ (F \to G) & \\ (F \vee G) & F, G \in \mathscr{F}_k \\ (F \wedge G) & x \in \mathscr{V} \\ \exists x\, F & \\ \exists x\, G & \end{array} \right\}$;
- 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 $\mathscr{L}_{\text{g}}$, un des axiomes de la théorie des groupes s'écrit

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

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

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

▷ Dans $\mathscr{L}_{\text{ens}}$, 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 $\mathscr{L}_{\mathrm{ens}}$, en tout cas.

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

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

Conjonction.

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

Disjonction.

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

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

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.

si x n'est pas libre dans les formules de Γ

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \forall_{\mathsf{i}}$$

quitte à renommer les variables liées de A qui apparaissent dans t

$$\frac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A[x := t]}\ \forall_{\mathsf{e}}$$

Quantificateur existentiel.

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

avec x ni libre dans C ou dans les formules de Γ

$$\frac{\Gamma \vdash \exists x\, A \qquad \Gamma, A \vdash C}{\Gamma \vdash C}\ \exists_{\mathsf{e}}$$

2.4 La sémantique.

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

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

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

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

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

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

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

Exemple 2.9. Avec $\mathscr{L}_{\text{corps}} = \{0, 1, +, \times, -, \square^{-1}\}$, on peut choisir
- ▷ $|\mathscr{M}| = \mathbb{R}$ avec $0_{\mathbb{R}}$, $1_{\mathbb{R}}$, $+_{\mathbb{R}}$, $\times_{\mathbb{R}}$, $-_{\mathbb{R}}$ et $\square^{-1}_{\mathbb{R}}$;
- ▷ ou $|\mathscr{M}| = \mathbb{R}$ avec $2_{\mathbb{R}}$, $2_{\mathbb{R}}$, $-_{\mathbb{R}}$, $+_{\mathbb{R}}$, *etc.*

Définissions la *vérité*.

Définition 2.16. Soit $\mathscr{M}$ une interprétation de $\mathscr{L}$.
- ▷ Un *environnement* est une fonction de l'ensemble des variables dans $|\mathscr{M}|$.
- ▷ Si e est un environnement et $a \in |\mathscr{M}|$, 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 $\mathscr{V}al_{\mathscr{M}}(t, e)$, est définie par induction sur l'ensemble des termes de la façon suivante :
  - $\mathscr{V}al_{\mathscr{M}}(c, e) = c_{\mathscr{M}}$ si c est une constante ;
  - $\mathscr{V}al_{\mathscr{M}}(c, e) = e(x)$ si x est une variable ;
  - $\mathscr{V}al_{\mathscr{M}}(f(t_1, \ldots, t_n), e) = f_{\mathscr{M}}(\mathscr{V}al_{\mathscr{M}}(t_1, e), \ldots, \mathscr{V}al_{\mathscr{M}}(t_n, e))$.

Remarque 2.9. La valeur est $\mathcal{V}al_{\mathcal{M}}(t, e)$ 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 $\mathcal{V}al_{\mathcal{M}}(t, e)$ ne dépend que de la valeur de e sur les variables de t. □

Notation.
- ▷ Lorsque cela est possible, on oublie $\mathcal{M}$ et e dans la notation, et on note $\mathcal{V}al(t)$.
- ▷ À la place de $\mathcal{V}al_{\mathcal{M}}(t, e)$ quand $x_1, \ldots, x_n$ sont les variables de t et $e(x_1) = a_1, \ldots, e(x_n) = a_n$, on note $t[a_1, \ldots, a_n]$ ou aussi $t[x_1 := a_1, \ldots, x_n := a_n]$. 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 $\mathcal{V}al_{\mathcal{M}}(F, e)$ et définie par induction sur l'ensemble des formules par

- ▷ $\mathcal{V}al_{\mathcal{M}}(R(t_1, \ldots, t_n), e) = 1$ ssi $(\mathcal{V}al_{\mathcal{M}}(t_1, e), \ldots, \mathcal{V}al_{\mathcal{M}}(t_n, e)) \in R_{\mathcal{M}}$;
- ▷ $\mathcal{V}al_{\mathcal{M}}(\bot, e) = 0$;
- ▷ $\mathcal{V}al_{\mathcal{M}}(\neg F, e) = 1 - \mathcal{V}al_{\mathcal{M}}(F, e)$;
- ▷ $\mathcal{V}al_{\mathcal{M}}(F \wedge G, e) = 1$ ssi $\mathcal{V}al_{\mathcal{M}}(F, e) = 1$ et $\mathcal{V}al_{\mathcal{M}}(G, e) = 1$;
- ▷ $\mathcal{V}al_{\mathcal{M}}(F \vee G, e) = 1$ ssi $\mathcal{V}al_{\mathcal{M}}(F, e) = 1$ ou $\mathcal{V}al_{\mathcal{M}}(G, e) = 1$;
- ▷ $\mathcal{V}al_{\mathcal{M}}(F \to G, e) = 1$ ssi $\mathcal{V}al_{\mathcal{M}}(F, e) = 0$ ou $\mathcal{V}al_{\mathcal{M}}(G, e) = 1$;
- ▷ $\mathcal{V}al_{\mathcal{M}}(\forall x\, F, e) = 1$ ssi pour tout $a \in |\mathcal{M}|$, $\mathcal{V}al_{\mathcal{M}}(F, e[x := a]) = 1$;

▷ $\mathcal{V}al_{\mathcal{M}}(\exists x\, F, e) = 1$ 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 possibilité :
  – 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
▷ $0 : \emptyset$,
▷ $1 : \{\emptyset\}$,
▷ $2 : \{\emptyset, \{\emptyset\}\}$,
▷ ⋮ ⋮
▷ $n + 1 : n \cup \{n\}$,
▷ ⋮ ⋮

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 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

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

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 : $\forall x\, \neg\bot$, et $\forall x\, x = x$ et même $x = x$ car on ne demande pas que la formule soit clause.

Dans $\mathcal{L}_{\mathrm{g}} = \{e, *, \square^{-1}\}$, 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 $G = \forall e' = \forall e'\, (\forall x\, (x * e' = e' * x = x) \to e = e')$.

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 $F \to G$ est un théorème logique.

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

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

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

- $\mathscr{M}$: $|\mathscr{M}| = \mathbb{Z}$ $e_{\mathscr{M}} = 0_{\mathbb{Z}}$ $*_{\mathscr{M}} = +_{\mathbb{Z}}$;
- $\mathscr{M}'$: $|\mathscr{M}'| = \mathbb{Z}$ $e_{\mathscr{M}'} = 0_{\mathbb{Z}}$ $*_{\mathscr{M}'} = +_{\mathbb{Z}}$ $\square^{-1}_{\mathscr{M}'} = \mathrm{id}_{\mathbb{Z}}$,

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

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

1. si t est un terme de $\mathscr{L}$, alors $\mathscr{V}al_{\mathscr{M}}(t, e) = \mathscr{V}al_{\mathscr{M}'}(t, e)$;
2. si F est une formule de $\mathscr{L}$ alors $\mathscr{V}al_{\mathscr{M}}(F, e) = \mathscr{V}al_{\mathscr{M}'}(F, e)$.

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 $\exists$. □

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

1. Un $\mathscr{L}$-*morphisme* de $\mathscr{M}$ est une fonction $\varphi : |\mathscr{M}| \to |\mathscr{N}|$ telle que
   - ▷ pour chaque symbole de constante c, on a $\varphi(c_{\mathscr{M}}) = c_{\mathscr{N}}$;
   - ▷ pour chaque symbole f de fonction n-aire, on a
   $$\varphi(f_{\mathscr{M}}(a_1, \dots, a_n)) = f_{\mathscr{N}}(\varphi(a_1), \dots, \varphi(a_n)) ;$$
   - ▷ pour chaque symbole R de relation n-aire (autre que « = »), on a
   $$(a_1, \dots, a_n) \in R_{\mathscr{M}} \text{ ssi } (\varphi(a_1), \dots, \varphi(a_n)) \in R_{\mathscr{N}}.$$
   - ▷ Un $\mathscr{L}$-*isomorphisme* est un $\mathscr{L}$-morphisme bijectif.
   - ▷ Si $\mathscr{M}$ et $\mathscr{N}$ sont *isomorphes* s'il existe un $\mathscr{L}$-isomorphisme de $\mathscr{M}$ à $\mathscr{N}$.

Remarque 2.13.
1. On ne dit rien sur « = » car si on impose la même condition que pour les autres relations alors nécessairement φ est injectif.
2. La notion dépend du langage $\mathscr{L}$.
3. Lorsqu'on a deux structures isomorphes, on les confonds, ce sont les mêmes, c'est un renommage.

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

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

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

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

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

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

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

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

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

$$\varphi(\mathscr{V}al_{\mathscr{M}}(t, e)) = \mathscr{V}al_{\mathscr{N}}(t, \varphi(e)).$$

□

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

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

Lemme 2.5. Soient $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$, et φ un ***isomorphisme***[5] de $\mathscr{M}$ dans $\mathscr{N}$. 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 $\mathscr{L} = \{\leq\}$, les interprétations $\mathbb{R}$ et $\mathbb{Q}$ satisfont les mêmes formules closes, mais ne sont pas isomorphes.

Définition 2.22. Soit $\mathscr{L}$ un langage, $\mathcal{M}$ et $\mathcal{N}$ deux interprétations de $\mathscr{L}$. On dit que $\mathcal{N}$ est une *extension* de $\mathcal{M}$ (ou $\mathcal{M}$ est une *sous-interprétation* de $\mathcal{N}$) si les conditions suivants 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 $f_{\mathcal{M}} = f_{\mathcal{N}}\big|_{|\mathcal{M}|^n}$ (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 $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$. Alors $\mathscr{M}$ est isomorphe à une sous-interprétation $\mathscr{M}'$ de $\mathscr{N}$ si et seulement si, il existe un morphisme injectif de $\mathscr{M}$ dans $\mathscr{N}$.

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 $\mathbb{N}^2/\sim \to \mathbb{Z}$ 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

$$T_{\text{groupe}} := \Big\{ \forall x\,(x * e = e * x = x),\\ \forall x\,(x * x^{-1} = e \wedge x^{-1} * x = e),\\ \forall x\,\forall y\,\forall z\,(x * (y * z) = (x * y) * z) \Big\}$$

dans le langage $\mathscr{L}_{\text{g}}$.

Exemple 2.18. La *théorie des ensembles infinis* est

$$T_{\text{ens infinis}} := \Big\{ \exists x\,(x = x),\\ \exists x\,\exists y\,(x \neq y),\\ \exists x\,\exists y\,\exists z\,(x \neq y \wedge y \neq z \wedge z \neq x)\\ \dots \Big\}$$

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

Définition 2.24 (Sémantique).
- ▷ Une interprétation $\mathscr{M}$ *satisfait* T (ou $\mathscr{M}$ est un *modèle* de T), noté $\mathscr{M} \models T$, si $\mathscr{M}$ 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_{groupes} et $T_{\text{ens infinis}}$, sont non-contradictoires.

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 $T \nvdash \bot$, sinon T est *inconsistante*.
- ▷ On dit que T est *complète* (« *axiome-complète* ») si T est consistante et, pour toute formule $F \in \mathscr{F}$, 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 $T \nvdash A$.
2. Soient A et B des formules closes. On a $T \vdash A \vee B$ ssi $T \vdash A$ ou $T \vdash B$.

Preuve.

▷ 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 $T' \cup T'' \vdash \bot$ par :

$$\dfrac{\dfrac{T' \vdash \neg A}{T' \cup T'' \vdash \neg A}\,\mathsf{aff} \qquad \dfrac{T'' \vdash A}{T' \cup T'' \vdash A}\,\mathsf{aff}}{T' \cup T'' \vdash \bot}\,\neg_{\mathsf{e}}$$

On en conclut que $T \vdash \bot$, absurde car T supposée complète donc consistante. On a donc $T \vdash \neg A$ implique $T \nvdash A$.

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

▷ Si $T \vdash A$ ou $T \vdash B$, alors par la règle $\vee^{\mathsf{g}}_{\mathsf{i}}$ ou $\vee^{\mathsf{d}}_{\mathsf{i}}$, on montre que $T \vdash A \vee B$.

Réciproquement, si $T \vdash A \vee B$ et $T \nvdash A$ et $T \nvdash B$ 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 $T \vdash \bot$ par $\neg_{\mathsf{e}}$. 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 [6] :

- 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 $\mathscr{M}$ tel que $\mathscr{M} \models T$ et $T \vdash \bot$. Or, par définition, $\mathscr{M} \not\models \bot$ donc $T \not\models \bot$.
- D'autre part, on montre « V2 implique V1 ». Soit T et F tels que $T \vdash F$. Ainsi, $T \cup \neg F \vdash \bot$, 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, touts 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 $T \models \bot$ d'où $T \vdash \bot$ 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 $T \cup \{\neg F\} \vdash \bot$ d'où $T \vdash F$ par $\bot_e$.

□

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, $\mathscr{M}$ un modèle et F une formule close. Si $\mathscr{M} \models T$ et $T \vdash F$ alors $\mathscr{M} \models F$.

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. □

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. □

On termine la preuve en montrant la proposition ci-dessous. □

Montrons cette proposition plus forte que le lemme.

Proposition 2.8. Soient Γ 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 $\Gamma \models A$ alors $\mathcal{M}, e \models A$.

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

- Cas inductif $\to_{\mathsf{i}}$. On sait que A est de la forme $B \to C$, et on montre que de $\Gamma, B \vdash C$ on montre $\Gamma \vdash B \to C$. Soient $\mathcal{M}$ et e tels que $\mathcal{M}, e \models \Gamma$. Montrons que $\mathcal{M}, e \models B \to C$. 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 $\forall_{\mathsf{e}}$. 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 autre cas inductifs sont laissé en exercices.

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

□

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 $\mathscr{L}$.

1. On enrichit le langage $\mathscr{L}$ en $\mathscr{L}'$ 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 Th sur $\mathscr{L}'$.
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 $\mathscr{L}$ en $\mathscr{L}'$ et T en T' consistante telle que, pour toute formule $F(x)$ de $\mathscr{L}'$, ayant pour seule variable libre x, il existe un symbole de constante c_F de $\mathscr{L}'$ telle que l'on ait $T' \vdash \exists x\, F(x) \to F(c_F)$, d'où le nom de témoin.

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

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

On commence par montrer quelques lemmes.

Lemme 2.9. Soient Γ un ensemble de formules et A une formule. Soit c un symbole de constante qui n'apparait ni dans Γ 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'apparait pas dans Γ, 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 replaçant c par x. Avec la règle $\forall_i$, on en conclut que $\Gamma \vdash \forall x\, A$. □

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

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

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

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 $T'' \vdash \bot$. Comme T'' fini, il existe un certain $n \in \mathbb{N}$ tel que $T'' \subseteq T_n$ et donc $T_n \vdash \bot$.

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 $T_{n+1} \vdash \bot$. Alors, il existe des formules à une variable libre $F_1, \dots, F_k$ écrites sur $\mathscr{L}_n$ et
$$T_n \cup \{\, \exists x\, F_i \to F_i(c_{F_i}) \mid 1 \leq i \leq k \,\} \vdash \bot.$$

Ainsi (exercice)

$$T_n \vdash \Big(\bigwedge_{1\leq i\leq k} \big(\exists x\, F_i \to F_i(c_{F_i})\big)\Big) \to \bot.$$

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

$$T_n \vdash \forall y_1\, \forall y_2\, \ldots \forall y_n \Big(\bigwedge_{1\leq i\leq k} \big(\exists x\, F_i \to F_i(y_i)\big)\Big) \to \bot.$$

On peut montrer que (théorème logique)

$$(\star) \qquad \vdash \forall y\, (A(y) \to \bot) \leftrightarrow (\exists y\, A(y) \to \bot),$$

d'où

$$T_n \vdash \Big(\exists y_1\, \exists y_2\, \ldots \exists y_n \bigwedge_{1\leq i\leq k} \big(\exists x\, F_i \to F_i(y_i)\big)\Big) \to \bot.$$

On a aussi

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

et pour y non libre dans A, on a

$$\vdash \exists y\, (A \to B) \leftrightarrow (A \to \exists y\, B).$$

On a donc

$$T_n \vdash \Big(\bigwedge_{1\leq i\leq k} (\exists x\, F_i(x) \to \exists y_i\, F_i(y_i))\Big) \to \bot.$$

Or,

$$(\star\star\star) \qquad \vdash \bigwedge_{1\leq i\leq k} (\exists x\, F_i(x) \to \exists y_i\, F_i(y_i)).$$

On a donc $T_n \vdash \bot$, 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 $T' \subseteq \mathrm{Th}$ et pour toute formule à une variable libre F de $\mathscr{L}'$, on a

$$\mathrm{Th} \vdash \exists x\, F \to F(c_F).$$

Faisons le cas dénombrable (sinon, lemme de Zorn) : supposons $\mathscr{L}'$ au plus dénombrable. Soit $(F_n)_{n\in\mathbb{N}}$ une énumération des formules closes de $\mathscr{L}'$. 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 $K_n \nvdash F_p$ et $K_n \nvdash \neg F_p$, et on pose $K_{n+1} := K_n \cup \{F_p\}$.

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

Preuve.

1. On a $T' \subseteq \mathrm{Th}$.
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 $K_n, F_p \vdash \bot$, 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 $\mathrm{Th} \nvdash F_p$ et $\mathrm{Th} \nvdash \neg F_p$. Ainsi, pour tout $n \in \mathbb{N}$, $K_n \nvdash F_p$ et $K_n \nvdash \neg F_p$, 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 $\mathscr{C}$ l'ensemble des termes clos de $\mathscr{L}'$, qui n'est pas vide car il contient les termes $c_{x=x}$ (avec la définition de c_F ci-avant). On définit sur $\mathscr{C}$ une relation $\sim$, où $t \sim t'$ ssi $\mathrm{Th} \vdash t = t'$.

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

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

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

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

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

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

Preuve.
- ▷ On a $\mathrm{Th} \vdash t_i = u_i$ pour tout i par hypothèse
- ▷ donc avec $=_{\mathsf{i}}$, on a $\mathrm{Th} \vdash f(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$
- ▷ donc avec $=_{\mathsf{e}}$, on a $\mathrm{Th} \vdash f(u_1, \ldots, t_n) = f(t_1, \ldots, t_n)$
- ▷ *...etc...*
- ▷ donc avec $=_{\mathsf{e}}$, on a $\mathrm{Th} \vdash f(u_1, \ldots, u_n) = f(t_1, \ldots, t_n)$

□

[*suite de la définition de l'interprétation*]

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

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

Exercice 2.7. Montrer que cette définition de 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, $\mathscr{M} \models F[\bar{t}_1, \dots, \bar{t}_n]$ ssi $\mathrm{Th} \vdash F[t_1, \dots, t_n]$, où l'on interprète la formule à paramètre dans l'environnement e avec $e(y_i) = \bar{t}_i$ alors $\mathscr{M}, e \models F(y_1, \dots, y_n)$.

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 $F = \bot$, alors on a $\mathrm{Th} \nvdash \bot$ car Th consistante et $\mathscr{M} \models \bot$ 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

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

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

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

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

  Or,

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

  par hypothèse. Ainsi,
  - avec $\vee_{\mathsf{i}}^{\mathsf{g}}$ et $\vee_{\mathsf{i}}^{\mathsf{d}}$, on a que $\mathrm{Th} \vdash F_1[t_1, \dots, t_n] \vee F_2[t_1, \dots, t_n]$;
  - réciproquement, on utilise le lemme 2.5 car 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 $\mathscr{M} \models \exists x\, G[\bar{t}_1, \dots, \bar{t}_n, x]$
  - ssi il existe $t \in \mathscr{C}$ tel que $\mathscr{M} \models G[\bar{t}_1, \dots, \bar{t}_n, \bar{t}]$
  - ssi il existe $t \in \mathscr{C}$ tel que $\mathrm{Th} \vdash G(t_1, \dots, t_n, t)$

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

□

Lemme 2.14. On a $\mathscr{M} \models \mathrm{Th}$ (et donc $\mathscr{M} \models T$).

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

alors

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

□

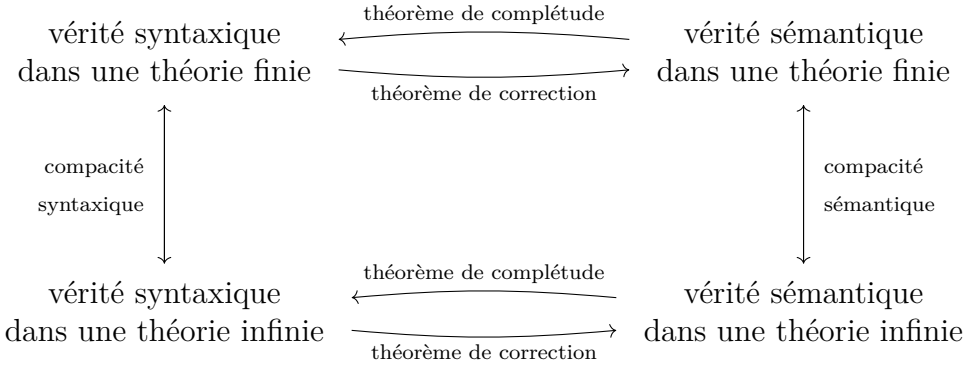
2.5.3 Compacité.

Théorème 2.2 (Compacité (sémantique))**.** Une théorie T et 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. □

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 $\mathscr{L}$ et κ un cardinal et $\kappa \geq \operatorname{card} \mathscr{L}$ et $\kappa \geq \aleph_0$.[7] Si T a un modèle infini, alors T a un modèle de cardinal κ.

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

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

3 L'arithmétique de Peano.

- ▷ Dedekind (1988) et Peano (1889) formalisent l'arithmétique.
- ▷ En 1900, David Hilbert, lors du 2ème ICM à Paris, donne un programme et dont le 2nd problème est la *cohérence de l'arithmétique*.
- ▷ En 1901, Russel donne son paradoxe concernant l'« ensemble » de tous les ensembles.
- ▷ En 1930, (Hilbert) est toujours optimiste : « On doit savoir, on saura ! »

La formalisation de l'arithmétique engendre deux questions :

1. est-ce que tout théorème est prouvable ? (▷ complétude)
2. existe-t-il un algorithme pour décider si un théorème est prouvable ? (▷ décidabilité)

Le second point est appelé « *Entscheidungsproblem* », le problème de décision, en 1928.

- ▷ En 1931, Gödel répond non à ces deux questions.

On a donné plusieurs formalisations des algorithmes :

- ▷ en 1930, le λ-calcul de Church ;
- ▷ en 1931–34, les fonctions récursives de Herbrand et Gödel ;
- ▷ en 1936, les machines de Turing.

On démontre que les trois modèles sont équivalents.

La thèse de Church–Turing nous convainc qu'il n'existe pas de modèle plus évolué « dans la vraie vie ».

3.1 Les axiomes.

On définit le langage $\mathscr{L}_0 = \{Ⓞ, Ⓢ, \oplus, \otimes\}$ où

- ▷ $Ⓞ$ est un symbole de constante ;
- ▷ $Ⓢ$ est un symbole de fonction unaire ;
- ▷ $\oplus$ et $\otimes$ sont deux symboles de fonctions binaires.

On verra plus tard que l'on peut ajouter une relation binaire $\leq$.

Remarque 3.1 (Convention). La structure $\mathbb{N}$ représente la $\mathscr{L}_0$-structure dans laquelle on interprète les symboles de manière habituelle :

- ▷ pour $Ⓞ$, c'est 0 ;
- ▷ pour $Ⓢ$, c'est $\lambda n.n+1$ (*i.e.* $x \mapsto x+1$) ;
- ▷ pour $\oplus$, c'est $\lambda n\, m.n+m$;
- ▷ pour $\otimes$, c'est $\lambda n\, m.n \times m$.

Les axiomes de Peano.

On se place dans le cas égalitaire. L'ensemble $\mathscr{P}$ est composé de $\mathscr{P}_0$ un ensemble fini d'axiomes (A1–A7) et d'un schéma d'induction (SI).

Trois axiomes pour le successeur :

A1. $\forall x\, \neg(Ⓢ\, x = Ⓞ)$

A2. $\forall x\, \exists y\, \Big(\neg(x = Ⓞ) \to x = Ⓢ\, y\Big)$

A3. $\forall x\, \forall y\, (Ⓢ\, x = Ⓢ\, y \to x = y)$

Deux axiomes pour l'addition :

A4. $\forall x\, (x \oplus Ⓞ = x)$

A5. $\forall x\, \forall y\, (x \oplus (Ⓢ\, y) = Ⓢ(x \oplus y))$

Deux axiomes pour la multiplication :

A6. $\forall x\, (x \otimes Ⓞ = Ⓞ)$

A7. $\forall x\, \forall y\, \Big(x \otimes (Ⓢ\, y) = (x \otimes y) \oplus x\Big)$

Et le schéma d'induction :

SI. Pour toute formule F de variables libres $x_0, \ldots, x_n$,

$$\forall x_1 \cdots \forall x_n \Big(\big(F(\textcircled{0}, \ldots, x_1, \ldots, x_n) \wedge \forall x \, (F(x, x_1, \ldots, x_n) \to F(\textcircled{S} x, x_1, \ldots, x_n)) \big) \to \forall x \, F(x, x_1, \ldots, x_n) \Big).$$

Remarque 3.2. ▷ Le schéma est le SI avec hypothèse faible, qui permet de montrer le SI avec hypothèse forte. On adopte la notation $\forall y \leq x \; F(y, x_1, \ldots, x_n)$ pour

$$\forall y \Big((\exists z \; z \oplus y = x) \to F(y, x_1, \ldots, x_n) \Big).$$

Le SI avec hypothèse forte est :

$$\forall x_1 \cdots \forall x_n \Big(\big(F(\textcircled{0}, \ldots, x_1, \ldots, x_n) \wedge \forall x \, \big((\forall y \leq x \; F(y, x_1, \ldots, x_n)) \to F(\textcircled{S} x, x_1, \ldots, x_n) \big) \big) \to \forall x \, F(x, x_1, \ldots, x_n) \Big)$$

- ▷ L'ensemble $\mathscr{P}$ est non-contradictoire car $\mathbb{N}$ est un modèle, appelé *modèle standard*.
- ▷ On peur remplacer le SI par une nouvelle règle de démonstration :

$$\frac{\Gamma \vdash F(\textcircled{0}) \qquad \Gamma \vdash \forall y \Big(F(y) \to F(\textcircled{S} y) \Big)}{\Gamma \vdash \forall x \, F(x)} \; \mathsf{rec} \; .$$

Exercice 3.1. Montrer l'équivalence entre SI et la nouvelle règle rec, *i.e.* on peut démontrer les mêmes théorèmes.

Notation. On note $\textcircled{n}$ le terme $\underbrace{\textcircled{S} \cdots \textcircled{S}}_{n \text{ fois}} \textcircled{0}$ pour $n \in \mathbb{N}$.

Définition 3.1. Dans une $\mathscr{L}_0$-structure, on dit qu'un élément est *standard* s'il est l'interprétation d'un terme $\textcircled{n}$ avec $n \in \mathbb{N}$.

Remarque 3.3. Dans $\mathbb{N}$ (le modèle standard), tout élément est standard.

Théorème 3.1. Il existe des modèles de $\mathscr{P}$ non isomorphes à $\mathbb{N}$.

Preuve. 1. Avec le théorème de Löwenheim-Skolem, il existe un modèle de $\mathscr{P}$ de cardinal κ pour tout $\kappa \geq \aleph_0$, et $\operatorname{card} \mathbb{N} = \aleph_0$.

2. Autre preuve, on considère un symbole de constante c et on pose $\mathscr{L} := \mathscr{L}_0 \cup \{c\}$. On considère la théorie

$$T := \mathscr{P} \cup \{ \neg(c = \underline{n}) \mid n \in \mathbb{N} \}.$$

Montrons que T a un modèle. Par le théorème de compacité de la logique du premier ordre, il suffit de montrer que T est finiment satisfiable. Soit $T' \subseteq_{\text{fini}} T$: par exemple,

$$T' \subseteq \mathscr{P} \cup \{\neg(c = \underline{n}_1), \neg(c = \underline{n}_2), \dots, (c = \underline{n}_k)\},$$

et $n_k \geq n_1, \dots, n_{k-1}$. On construit un modèle de T' correspondant à $\mathbb{N}$ où c est interprété par $n_k + 1$. Ainsi, T' est satisfiable et donc T aussi avec un modèle $\mathscr{M}$.

Montrons que $\mathbb{N}$ et $\mathscr{M}$ ne sont pas isomorphes. Par l'absurde, supposons que $\varphi : \mathscr{M} \to \mathbb{N}$ soit un isomorphisme. Alors $\gamma := \varphi(c_{\mathscr{M}})$ satisfait les mêmes formules que $c_{\mathscr{M}}$, par exemple, pour tout $n \in \mathbb{N}$, $\mathscr{M} \models \neg(c = \underline{n})$. Or, on ne peut pas avoir $\mathbb{N} \models \neg(\underline{\gamma} = \underline{n})$ pour tout $n \in \mathbb{N}$. ***Absurde.***

□

On a montré que tous les modèles isomorphes à $\mathbb{N}$ n'ont que des éléments standards.

Théorème 3.2. Dans tout modèle $\mathscr{M}$ de $\mathscr{P}$,

1. l'addition est commutative et associative ;
2. la multiplication aussi ;
3. la multiplication est distributive par rapport à l'addition ;
4. tout élément est *régulier* pour l'addition :

$$\mathscr{M} \models \forall x \, \forall y \, \forall z \, (x \oplus y = x \oplus z \to y = z) \, ;$$

5. tout élément non nul est régulier pour la multiplication :

$$\mathscr{M} \models \forall x\, \forall y\, \forall z\, ((\neg(x = \textcircled{0}) \wedge x \otimes y = x \otimes z) \to y = z)\ ;$$

6. la formule suivante définie un ordre total sur $\mathscr{M}$ compatible avec $+$ et $\times$:

$$x \leq y \text{ ssi } \exists z\, (x \oplus x = y).$$

Preuve. On prouve la commutativité de $+$ en trois étapes.

1. On montre $\mathscr{P} \vdash \forall x\, (\textcircled{0} \oplus x = x)$. On utilise le SI avec la formule $F(x) := (\textcircled{0} \oplus x = x)$.
   - ▷ On a $\mathscr{P} \vdash \textcircled{0} \oplus \textcircled{0} = \textcircled{0}$ par A4.
   - ▷ On montre $\mathscr{P} \vdash \forall x\, F(x) \to F(\textcircled{S} x)$, c'est à dire :

$$\forall x \left((\textcircled{0} \oplus x = x) \to (\textcircled{0} \oplus (\textcircled{S} x) = \textcircled{S} x) \right).$$

     On peut le montrer par A5.

   Questions/Remarques :
   - ▷ Pourquoi pas une récurrence normale ? On n'est pas forcément dans $\mathbb{N}$!
   - ▷ Grâce au théorème de complétude, on peut raisonner sur les modèles, donc en maths naïves.
2. On montre $\mathscr{P} \vdash \forall x \forall y\, \textcircled{S}(x \oplus y) = (\textcircled{S} x) \oplus y$. On veut utiliser le schéma d'induction avec $F(x, y) := \textcircled{S}(x \oplus y) = (\textcircled{S} x) \oplus y$. Mais ça ne marche pas...(Pourquoi ?)

   La bonne formule est $F(y, x) := \textcircled{S}(x \oplus y) = (\textcircled{S} x) \oplus y$.
   - ▷ On montre $\mathscr{P} \vdash F(\textcircled{0}, x)$, c'est à dire

$$\mathscr{P} \vdash \textcircled{S}(x \oplus \textcircled{0}) = (\textcircled{S} x) \oplus \textcircled{0}.$$

     Ceci est vrai car

$$\textcircled{S}(x \oplus \textcircled{0}) \underset{\text{A4}}{=} \textcircled{S} x \underset{\text{A4}}{=} (\textcircled{S} x) \oplus \textcircled{0}.$$

▷ On a $\mathscr{P} \vdash F(y,x) \to F(\textcircled{S}y, x)$ car : si $\textcircled{S}(x \oplus y) = (\textcircled{S}x) \oplus y$, alors

$$\textcircled{S}(x \oplus (\textcircled{S}y)) \underset{\text{A5}}{=} \textcircled{S}\textcircled{S}(x \oplus y) \underset{\text{hyp}}{=} \textcircled{S}((\textcircled{S}x) \oplus y) \underset{\text{A5}}{=} (\textcircled{S}x) = \oplus(\textcircled{S}y).$$

3. On utilise le SI avec $F(x,y) := (x \oplus y = y \oplus x)$. D'une part, on a $F(\textcircled{0}, y) = (\textcircled{0} \oplus y = y \oplus \textcircled{0})$ par 1 et A4. D'autre part, si l'on a $x \oplus y = y \oplus x$ alors $(\textcircled{S}x) \oplus y = y \oplus (\textcircled{S}x)$ par A5 et 2. Par le SI, on conclut.

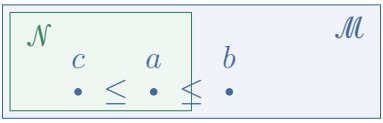
□

Exercice 3.2. Finir la preuve du théorème.

3.2 Liens entre $\mathbb{N}$ et un modèle $\mathscr{M}$ de $\mathscr{P}$.

Définition 3.2. Si $\mathscr{M} \models \mathscr{P}_0$ et $\mathscr{N} \models \mathscr{P}_0$ et $\mathscr{N}$ une sous-interprétation de $\mathscr{M}$, on dit que $\mathscr{N}$ est un segment initial de $\mathscr{M}$, ou que $\mathscr{M}$ est une extension finale de $\mathscr{N}$, si pour tous $a, b, c \in |\mathscr{M}|$ avec $a \in |\mathscr{N}|$ on a :

1. si $\mathscr{M} \models c \leq a$ alors $c \in |\mathscr{N}|$;
2. si $b \notin |\mathscr{N}|$ alors $\mathscr{M} \models a \leq b$.



Remarque 3.4.
▷ Les points peuvent être incomparables et dans $\mathscr{M}$.
▷ L'ensemble $\mathscr{P}_0$ est très faible, on ne montre même pas que $\oplus$ commute ou que $\leq$ est une relation d'ordre (*c.f.* TD).

Théorème 3.3. Soit $\mathscr{M} \models \mathscr{P}_0$. Alors, le sous-ensemble de $\mathscr{M}$ sui-

vant est une sous-interprétation de $\mathscr{M}$ qui est un segment initial et qui est isomorphe à $\mathbb{N}$:

$$\left\{ a \in |\mathscr{M}| \;\middle|\; \begin{array}{l} \text{il existe } n \in \mathbb{N} \text{ et } a \\ \text{est l'interprétation} \\ \text{de } \underline{n} \text{ dans } \mathscr{M} \end{array} \right\}.$$

Preuve.
1. Pour tout $n \in \mathbb{N}$, on a $\mathscr{P}_0 \vdash \underline{n+1} = \mathbf{S}\,\underline{n}$.
2. Pour tout $n, m \in \mathbb{N}$, on a $\mathscr{P}_0 \vdash \underline{m} \oplus \underline{n} = \underline{m+n}$.
3. Pour tout $n, m \in \mathbb{N}$, on a $\mathscr{P}_0 \vdash \underline{m} \otimes \underline{n} = \underline{m \times n}$.
4. Pour tout $n \in \mathbb{N}_\star$, on a $\mathscr{P}_0 \vdash \neg(\underline{n} = \underline{0})$.
5. Pour tout $n \neq m$, on a $\mathscr{P}_0 \vdash \neg(\underline{m} = \underline{n})$.
6. Pour tout $n \in \mathbb{N}$ (admis), on a
$$\mathscr{P}_0 \vdash \forall x \left(x \leq \underline{n} \to (x = \underline{0} \vee x = \underline{1} \vee \cdots \vee x = \underline{n}) \right).$$
7. Pour tout x, on a $\mathscr{P}_0 \vdash \forall x\, (x \leq \underline{n} \vee \underline{n} \leq x)$.

□

3.3 Les fonctions représentables.

Cette section détaille un outil technique pour montrer le théorème d'incomplétude de Gödel vu plus tard. On code tout avec des entiers !

Définition 3.3. Soit $f : \mathbb{N}^p \to \mathbb{N}$ une fonction totale et $F(x_0, \ldots, x_p)$ une formule de $\mathscr{L}_0$. On dit que F *représente* f si, pour tout p-uplet d'entiers $(n_1, \ldots, n_p)$ on a :

$$\mathscr{P}_0 \vdash \forall y \left(F(y, \underline{n_1}, \ldots, \underline{n_p}) \leftrightarrow y = \underline{f(n_1, \ldots, n_p)} \right).$$

On dit que f est *représentable* s'il existe une formule qui la représente.

Un ensemble de p-uplets $A \subseteq \mathbb{N}^p$ est *représenté* par $F(x_1, \ldots, x_p)$

si pour tout p-uplet d'entiers $(n_1, \dots, n_p)$, on a

1. si $(n_1, \dots, n_p) \in A$ alors $\mathscr{P}_0 \vdash F(n_1, \dots, n_p)$;
2. si $(n_1, \dots, n_p) \notin A$ alors $\mathscr{P}_0 \vdash \neg F(n_1, \dots, n_p)$.

On dit que A est *représentable* s'il existe une formule qui le représente.

Exercice 3.3. Montrer qu'un ensemble est représentable ssi sa fonction indicatrice l'est.

Exemple 3.1 (Les briques de base des fonctions récursives)**.**

- La fonction nulle $f : \mathbb{N} \to \mathbb{N}, x \mapsto 0$ est représentable par $F(x_0, x_1) := x_0 = \textcircled{0}$.
- Les fonctions constantes $f : \mathbb{N} \to \mathbb{N}, x \mapsto n$ sont représentables par $F(x_0, x_1) := x_0 = \textcircled{n}$, où $n \in \mathbb{N}$.
- Les projections $\pi_p^i : \mathbb{N}^p \to \mathbb{N}, (x_1, \dots, x_p) \mapsto x_i$ sont représentables par $F(x_0, x_1, \dots, x_p) := x_0 = x_i$.
- La fonction successeur $f : \mathbb{N} \to \mathbb{N}, x \mapsto x + 1$ est représentable par $F(x_0, x_1) := x_0 = (\textcircled{S}\, x_1)$.
- L'addition $f : \mathbb{N}^2 \to \mathbb{N}, (x, y) \mapsto x + y$ est représentable par $F(x_0, x_1, x_2) := x_0 = x_1 \oplus x_2$.
- La multiplication $f : \mathbb{N}^2 \to \mathbb{N}, (x, y) \mapsto x \times y$ est représentable par $F(x_0, x_1, x_2) := x_0 = x_1 \otimes x_2$.

Théorème 3.4. Toute fonction récursive totale est représentable.