Logique

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

ENS DE LYON

27 mai 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 :

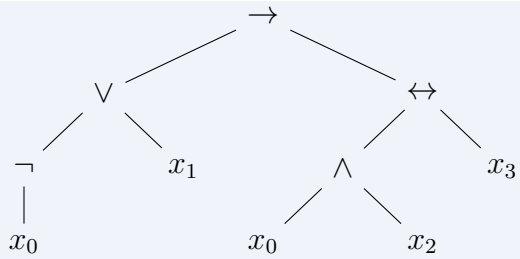
- $G \in \mathscr{P}$;
- il existe $F \in \mathscr{F}$ telle que $G = \neg F$;
- il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \vee F_2)$;
- il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \wedge F_2)$;
- il existe $F_1, F_2 \in \mathscr{F}$ telle que $G = (F_1 \to F_2)$;
- il existe $F_1, F_2 \in \mathscr{F}$ 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 $\bar{\nu}(F) = 1 - \bar{\nu}(F_1)$;
  - *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

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

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 $\mathscr{E}$, alors $B \cup B_0$ est

un ensemble fini donc satisfiable par une valuation ν. La valuation satisfait B_0 donc $\nu(x_0) = 1$ et ν satisfait B. On a donc la propriété au rang 0.

– Hérédité. Par hypothèse de récurrence, on a une suite $\varepsilon_0, \dots, \varepsilon_n$.

1. Soit, pour tout sous-ensemble fini B de $\mathscr{E}$, il existe ν qui satisfait B et telle que $\nu(x_0) = \varepsilon_0$, …, $\nu(x_n) = \varepsilon_n$, et $\nu(x_{n+1}) = 0$. On pose $\varepsilon_{n+1} = 0$.
2. Soit il existe B_{n+1} un sous-ensemble fini de $\mathscr{E}$ tel que, pour toute valuation ν telle que ν satisfait B_{n+1} et $\nu(x_0) = \varepsilon_0, \dots, \nu(x_n) = \varepsilon_n$, on a $\nu(x_{n+1}) = 1$ et on pose $\varepsilon_{n+1} = 1$.

Montrons l'hérédité :

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

On a donc la propriété pour tout n.

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

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

Définition 1.6. Un ensemble ordonné $(X, \mathscr{R})$ est inductif si pour

tout sous-ensemble Y de X totalement ordonné par $\mathcal{R}$ (*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 $\mathcal{V}$ 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.

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

Disjonction.

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

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

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 $\mathcal{M}$ et $\mathcal{N}$ deux interprétations de $\mathcal{L}$.

1. Un $\mathcal{L}$-*morphisme* de $\mathcal{M}$ est une fonction $\varphi : |\mathcal{M}| \to |\mathcal{N}|$ 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 φ 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 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

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

□

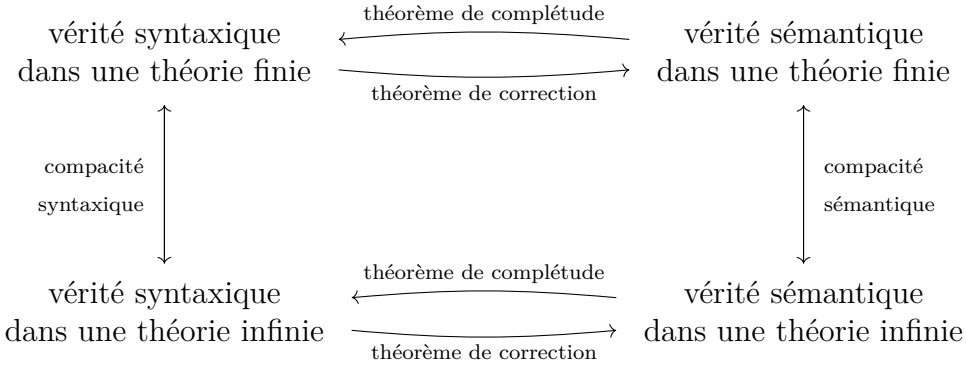
2.5.3 Compacité.

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 $\times$:

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

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.

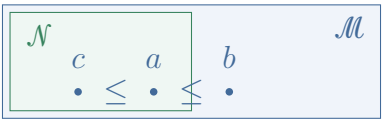
□

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 $F(x_0, x_1, x_2) := x_0 = x_1 \otimes x_2$.

On introduit trois nouvelles opérations.

Récurrence. Soient $g(x_1, \dots, x_p)$ et $h(x_1, \dots, x_{p+2})$ des fonctions partielles. On définit la fonction partielle f par :

- $f(0, x_1, \dots, x_p) := g(x_1, \dots, x_p)$;
- $f(x_0 + 1, x_1, \dots, x_p) := h(x_0, f(x_0, \dots, x_p), x_1, \dots, x_p)$.

Composition. Soient $f_1, \dots, f_n$ des fonctions partielles de p variables et g une fonction partielle de n variables. Alors, la fonction composée $g(f_1, \dots, f_n)$ est définie en $(x_1, \dots, x_p)$ ssi les fonctions f_i le sont et g est définie en $\big(f_1(x_1, \dots, x_p), \dots, f_n(x_1, \dots, x_p)\big)$.

Schéma μ. Soit $f(x_1, \dots x_{p+1})$ une fonction partielle. Soit

$$g(x_1, \dots, x_p) := \mu y.\ (f(x_1, \dots, x_p, y) = 0).$$

Elle est définie en $(x_1, \dots, x_p)$ si et seulement s'il existe y tel que $f(x_1, \dots, x_p, y) = 0$ et tous les $f(x_1, \dots, x_p, x)$ sont définies pour $x \leq y$. Dans ce cas, $g(x_1, \dots, x_p)$ est le plus petit y tel que $f(x_1, \dots, x_p, y) = 0$.

Définition 3.4. L'ensemble des fonctions récursives primitives (*resp.* récursives) est le plus petit ensemble des fonctions contenant les briques de base et stable par composition et récurrence (*resp.* par composition, récurrence et schéma μ).

Exemple 3.2. Les fonctions

$$f(x_1, x_2, y) := y^2 - (x_1 + x_2)y + x_1 x_2$$

et

$$f(x_1, x_2) := \min(x_1, x_2)$$

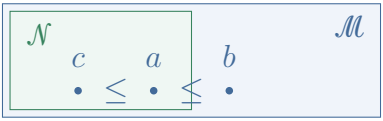
sont récursives primitives.

Définition 3.5. Une fonction récursive *totale* est une fonction récursive définie partout.

Remarque 3.5.
- ▷ Une fonction récursive primitive est totale.
- ▷ Une fonction récursive primitive peut se fabriquer avec un seul schéma μ à la fin (*c.f.* cours de FDI).
- ▷ *Rappel.* Une fonction $f : \mathbb{N}^p \to \mathbb{N}$ totale est représentée par la formule $F(x_0, \dots, x_p)$ de $\mathscr{L}_0$ su pour tout p-uplet d'entiers $(n_1, \dots, n_p)$ on a :

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

- ▷ *Rappel.* Si $\mathscr{M} \models \mathscr{P}_0$ alors l'ensemble de $|\mathscr{M}|$ constitué de l'interprétation des termes standards est une sous-interprétation de $\mathscr{M}$ qui en est un segment initial et qui est isomorphe à $\mathbb{N}$.
- ▷ *Rappel.* Une sous-interprétation $\mathscr{N}$ est un segment initial de $\mathscr{M}$ si
  - $a \in \mathscr{N}$ et $b \in \mathscr{M} \setminus \mathscr{N}$ alors $b \geq a$;
  - $a \in \mathscr{N}$ et $c \leq a$ alors $c \in \mathscr{N}$.



Théorème 3.4. Toute fonction récursive totale est représentable.

On a déjà montré que les briques de base sont représentables. On montre trois lemmes qui montreront le théorème ci-dessus.

Lemme 3.1. L'ensemble des fonctions représentables est clos par composition.

Preuve. Soient $f_1(x_1, \dots, x_p), \dots, f_n(x_1, \dots, x_p)$ et $g(x_1, \dots, x_n)$ des fonctions représentées par $F_1(x_0, \dots, x_p), \dots, F_n(x_0, \dots, x_p)$ et $G(x_0, \dots, G_n)$. On va montrer que $h = g(f_1, \dots, f_n)$ est représentée par

$$H(x_0, \dots, x_o) := \exists y_0 \cdots \exists y_n \Big(G(x_0, y_1, \dots, y_n) \wedge \bigwedge_{1 \leq i \leq n} F_i(y_i, x_1, \dots, x_p) \Big).$$

En effet, pour tous entiers $n_1, \dots, n_{\max(p,n)}$:

- ▷ $\mathscr{P}_0 \vdash \forall y \; F_i(y_1, \overline{n_1}, \dots, \overline{n_p}) \leftrightarrow y = \overline{f_i(n_1, \dots, n_p)}$;
- ▷ $\mathscr{P}_0 \vdash \forall y \; G(y_1, \overline{n_1}, \dots, \overline{n_n}) \leftrightarrow y = \overline{g(n_1, \dots, n_n)}$.

Dans tout modèle $\mathscr{M}$ de $\mathscr{P}_0$, pour tout $y \in |\mathscr{M}|$, et tous $n_1, \dots, n_p \in \mathbb{N}$ on a $H(y, n_1, \dots, n_p)$ est vraie ssi il existe $y_1, \dots, y_n$ dans $|\mathscr{M}|$ et pour tout i, $F_i(y_i, x_1, \dots, x_p)$ est vrai et $G(y, y_1, \dots, y_n)$. Donc, par les hypothèses précédents, on a $H(y, n_1, \dots, n_p)$ ssi il existe $y_1, \dots, y_n$ dans $|\mathscr{M}|$ et pour tout i, $y_i = f_i(n_1, \dots, n_p)$ et $y = g(y_1, \dots, y_p)$, ssi

$$y = g(f_1(n_1, \dots, n_p), \dots, f_n(n_1, \dots, n_p))$$

ssi $y = h(n_1, \dots, n_p)$. On conclut

$$\mathscr{P}_0 \vdash \forall y \left(H(y, \overline{n_1}, \dots, \overline{n_p}) \leftrightarrow y = \overline{h(n_1, \dots, n_p)} \right).$$

□

Lemme 3.2. Si, à partir d'une fonction représentable totale, on obtient par schéma μ une fonction totale, alors cette fonction est représentable.

Preuve. Soit $g : \mathbb{N}^{p+1} \to \mathbb{N}$ une fonction représentable totale, et soit $f : \mathbb{N}^p \to \mathbb{N}$ définie par

$$f(x_1, \dots, x_p) := \mu x_0. \left(g(x_0, \dots, x_p) = 0 \right).$$

Montrons que si f est totale alors elle est représentable. Soit $G(y, x_0, \dots, x_p)$ qui représente g. Alors, pour tous $n_1, \dots, n_p$ on a

$$\mathscr{P}_0 \vdash \forall y \, G(y, \overline{n_1}, \dots, \overline{n_p}) \leftrightarrow y = \overline{g(n_1, \dots, n_p)}.$$

Considérons la formule

$$F(y, n_1, \dots, n_p) := G(0, y, x_1, \dots, x_p) \wedge \forall z < y, \neg G(0, z, x_1, \dots, x_p),$$

où l'on note $\forall z < y \, H$ pour $\forall z \, (\exists u \, \neg(h = \overline{0}) \wedge z \oplus h = y) \to H$. Montrons que F représente f. Soit $\mathscr{M}$ un modèle de $\mathscr{P}_0$. Soient $n_1, \dots, n_p$ des entiers et $y \in |\mathscr{M}|$. On a $F(y, n_1, \dots, n_p)$ vrai ssi $G(0, y, n_1, \dots, n_p)$ vrai et, pour tout $z < y$, $\neg G(0, z, n_1, \dots, n_p)$

est vrai. Montrons que $b := f(n_1, \dots, n_p)$ est le seul élément à satisfaire $F(y, n_1, \dots, n_p)$. On a bien $G(0, b, n_1, \dots, n_p)$ par définition de f et pour tout entier $z < b$, on a $\neg G(0, z, n_1, \dots, n_p)$. Mais, si on a $z < b$ et z n'est pas un entier ? Ce cas n'existe pas car la sous-représentation isomorphe à $\mathbb{N}$ est un segment initial, il n'y a donc que des entiers qui sont inférieurs à b dans $|\mathscr{M}|$. Ainsi, $F(b, n_1, \dots, n_p)$. Montrons que b est le seul. Soit y tel que $F(y, n_1, \dots, n_p)$. Montrons que $y = b$.

- Si y est un entier, c'est vrai par définition de b.
- Si y n'est pas un entier, alors $y > b$. Donc, $g(y, x_1, \dots, x_p) = 0$ et $b < y$ avec $g(b, x_1, \dots, x_p) = 0$. Ainsi, $\forall z < y \neg G(0, z, x_1, \dots, x_p)$ est fausse, et donc $F(y, n_1, \dots, n_p)$ est fausse.

□

Lemme 3.3. L'ensemble des fonctions totales est stable par définition par récurrence.

Preuve. Soient f, g, h telles que

- $f(0, x_1, \dots, x_p) = g(x_1, \dots, x_p)$
- $f(x_0 + 1, x_1, \dots, x_p) = h(x_0, f(x_0, \dots, x_p), x_1, \dots, x_p)$

Soient G, H représentant g et h. On a dans $\mathbb{N}$: $y = f(x_0, \dots, x_p)$ ssi il existe $z_0, \dots, z_{x_0}$ tel que

- $z_0 = g(x_1, \dots, x_p)$
- $z_1 = h(0, z_0, x_1, \dots, x_p)$
- $z_2 = h(1, z_1, x_1, \dots, x_p)$
- ⋮
- $z_{x_0} = h(x_0 - 1, z_{x_0 - 1}, x_1, \dots, x_p)$
- $y = z_{x_0}$

Zut ! On ne peut pas écrire $\exists z_0 \cdots \exists z_{x_0}$! On va utiliser une fonction qui permet de coder une suite d'entiers dans un couple d'entier (a, b). Interruption de la preuve. □

Lemme 3.4 (Fonction β de Gödel)**.** Il existe une fonction β à trois variables, récursive primitive et représentable, tel que pour tout $p \in \mathbb{N}$ et toute suite $(n_0, \dots, n_p) \in \mathbb{N}^{p+1}$, il existe des entiers a et b tels que pour tout $0 \leq i \leq p$, on ait $\beta(i, a, b) = n_i$.

Preuve. Soient $(a_0, \dots, a_p)$ une suite d'entiers deux à deux premiers, et $(n_0, \dots, n_p)$ une suite d'entiers. Alors il existe $b \in \mathbb{N}$ tel que, pour tout $0 \leq i \leq p$, $b \equiv n_i \pmod{a_i}$ (par le théorème Chinois).

Choisissons a et les a_i (qui induisent b) ? On pose $a = m!$. Alors, on pose $a_i := a(i+1)+1$ pour tout $0 \leq i \leq p$. Les a_i sont bien deux à deux premiers. En effet, pour $j > i$, si $c \mid a_i$ et $c \mid a_j$ avec c premier, alors $c \mid (a_i - a_j)$ donc $c \mid a(j-i)$ et donc $c \leq m$, donc $c \mid m$. Ainsi, il existe bien b tel que $b \equiv n_i \pmod{a_i}$. On définit ainsi $\beta(i, a, b)$ comme le reste de la division de b par $a(i+1)+1$. La fonction β est représentée par

$$B(x_0, i, a, b) := \exists x_4\, b = x_4 \otimes \textcircled{S}(a \otimes (\textcircled{S} i)) \wedge x_4 < \textcircled{S}(x \otimes \textcircled{S} i).$$

On considère $B'(x_0, x_1, x_2, x_3) := B(x_0, x_1, x_2, x_3) \wedge \forall x_4 < x_0\ \neg B(x_4, x_1, x_2, x_3)$. Cette dernière formule représente aussi β mais aussi que x_0 sera un entier standard. □

On reprend la preuve du lemme 3.3.

Preuve. Soient f, g, h telles que

- $f(0, x_1, \dots, x_p) = g(x_1, \dots, x_p)$
- $f(x_0 + 1, x_1, \dots, x_p) = h(x_0, f(x_0, \dots, x_p), x_1, \dots, x_p)$

Soient G, H représentant g et h. On a dans $\mathbb{N}$: $y = f(x_0, \dots, x_p)$ ssi il existe $z_0, \dots, z_{x_0}$ tel que

- $z_0 = g(x_1, \dots, x_p)$
- $z_1 = h(0, z_0, x_1, \dots, x_p)$

- ▷ $z_2 = h(1, z_1, x_1, \dots, x_p)$
- ▷ $\vdots$
- ▷ $z_{x_0} = h(x_0 - 1, z_{x_0-1}, x_1, \dots, x_p)$
- ▷ $y = z_{x_0}$

ssi

$$\exists a\, \exists b \Big[(\exists z_0\, B'(z_0, \textcircled{0}, a, b) \wedge G(z_0, x_1, \dots, x_p)) \wedge \forall i < x_0\, \exists z\, \exists z' \begin{pmatrix} B'(z, i, a, b) \\ \wedge \quad B'(z', \textcircled{S} i, a, b) \\ \wedge \quad H(z', i, z, x_1, \dots, x_p) \end{pmatrix} \wedge B'(y, x_0, a, b) \Big]$$

est vraie. Montrons que F représente f.

Soit $\mathscr{M} \models \mathscr{P}_0$, et $n_0, \dots, n_p$ des entiers et $c \in |\mathscr{M}|$.

- ▷ Si c interprète $\overline{f(n_0, \dots, n_p)}$ alors en choisissant a et b avec le lemme précédent sur la fonction β, on a bien $F(c, n_0, \dots, n_p)$.
- ▷ Réciproquement, si $\mathscr{M} \models F(d, \overline{n_0}, \dots, \overline{n_p})$ alors il existe a, b, z_0 tels que $B'(z_0, \textcircled{0}, a, b)$ et $G(z_0, n_1, \dots, n_p)$, et donc $z_0 = g(n_1, \dots, n_p)$. Et, pour tout $i \leq n_0$, il existe r_i et s_i tels que

  $$B'(r_i, i, a, b) \wedge B'(s_i, i + 1, a, b) \wedge H(s_i, i, r_i, n_1, \dots, n_p)$$

  donc $r_i = f(i, n_1, \dots, n_p)$ grâce aux propriétés de B' et car r_i est un entier naturel, et donc par récurrence $d = f(n_0, \dots, n_p)$.

□

Ceci conclut la preuve du théorème 3.4.

Maintenant que l'on a transformé les fonctions en formules, on va faire l'opposé. Notre but est de montrer le théorème suivant : soit

T une théorie consistante contenant $\mathscr{P}_0$ alors T est indécidable. La « partie technique » de l'indécidabilité de Gödel est la preuve par diagonalisation.

3.4 Indécidabilité des théories consistantes contenant $\mathscr{P}_0$.

On va coder :

1. les suites d'entiers ;
2. les termes ;
3. les formules ;
4. les preuves.

Lemme 3.5 (Récursion). Soient $p, n \in \mathbb{N}$ et

- $k_1, \dots, k_n : \mathbb{N} \to \mathbb{N}$ telles que $\forall y, \forall i,\ k_i(y) < y$;
- $g : \mathbb{N}^p \to \mathbb{N}$;
- $h : \mathbb{N}^{p+n+1} \to \mathbb{N}$

des fonctions récursives primitives (*resp.* récursives). Alors, la fonction $f : \mathbb{N}^{p+1} \to \mathbb{N}$ définie de la façon suivante est récursive primitive (*resp.* récursive primitive) :

$$f(0, x_1, \dots, x_p) := g(x_1, \dots, x_p)$$

et $f(y, x_1, \dots, x_p) := h(y, f(k_1(y), x_1, \dots, x_p), \dots, f(k_n(y), x_1, \dots, x_p), x_1, \dots, x_p)$. □

Lemme 3.6 (Définition par cas). Soient $P_1, \dots, P_n$ des ensembles récursifs primitifs (*resp.* récursifs) disjoints de $\mathbb{N}^m$ et $f_1, \dots, f_{n+1}$ des fonctions récursives primitives (*resp.* récursives) $\mathbb{N}^m \to \mathbb{N}$

alors la fonction suivante est récursive primitive (*resp.* récursive) :

$$f(x_1,\dots,x_m) := \begin{cases} f_1(x_1,\dots,x_m) & \text{si } P_1(x_1,\dots,x_m) \\ f_2(x_1,\dots,x_m) & \text{si } P_2(x_1,\dots,x_m) \\ \vdots & \vdots \\ f_n(x_1,\dots,x_m) & \text{si } P_n(x_1,\dots,x_m) \\ f_{n+1}(x_1,\dots,x_m) & \text{sinon} \end{cases}$$

□

Lemme 3.7 (Définition par cas et récursion)**.** Soient $p, n, m \in \mathbb{N}$, et

- $g : \mathbb{N}^p \to \mathbb{N}$
- $k_1, \dots, k_m : \mathbb{N} \to \mathbb{N}$
- $f_1, \dots, f_n : \mathbb{N}^{m+p+1} \to \mathbb{N}$
- $f_{n+1} : \mathbb{N}^p \to \mathbb{N}$

des fonctions récursives primitives (*resp.* récursives) et $P_1, \dots, P_n$ des ensembles disjoints de $\mathbb{N}^p$ récursifs primitifs (*resp.* récursifs) alors la fonction suivante est récursive primitive :

$$f(0, x_1, \dots, x_p) := g(x_1, \dots, x_p)$$

et

$$f(y, x_1, \dots, x_p) := \begin{cases} f_1(y, f(k_1(y), x_1, \dots, x_p), \dots, f(k_m(y), x_1, \dots, x_p), x_1, \dots, x_p) & \text{si } P_1(x_1, \dots, x_p) \\ f_2(y, f(k_1(y), x_1, \dots, x_p), \dots, f(k_m(y), x_1, \dots, x_p), x_1, \dots, x_p) & \text{si } P_2(x_1, \dots, x_p) \\ \vdots & \\ f_n(y, f(k_1(y), x_1, \dots, x_p), \dots, f(k_m(y), x_1, \dots, x_p), x_1, \dots, x_p) & \text{si } P_n(x_1, \dots, x_p) \\ f_{n+1}(x_1, \dots, x_p) & \end{cases}$$

□

3.4.1 Codage des suites d'entiers.

Proposition 3.1. Pour tout entier non nul p il existe des fonctions récursives primitives bijectives $\alpha_p : \mathbb{N}^p \to \mathbb{N}$ et $\beta_p^1, \dots, \beta_p^p : \mathbb{N} \to$

$\mathbb{N}$ telles que la réciproque de α_p est $(\beta_p^1, \ldots, \beta_p^p)$ et, de plus, si $x > 1$ et $p \geq 2$ alors $\beta_p^i(x) < x$.

Preuve. L'idée est qu'on utilise la fonction de Cantor (ou l'énumération de Peano) :

$$\alpha_2(n, m) := \frac{(n+m)(n+m+1)}{2} + n$$

et on pose

$$\alpha_{p+1}(x_1, \ldots, x_{p+1}) := \alpha_p(x_1, \ldots, x_{p-1}, \alpha_2(x_p, x_{p+1})).$$

Ainsi,

$$\alpha_p(x_1, \ldots, x_p) = \alpha_2(x_1, \alpha_2(x_2, \ldots)).$$

□

3.4.2 Les termes.

On suppose que l'ensemble des variables est $\{x_i \mid i \in \mathbb{N}\}$.

Définition 3.6. Le nombre de Gödel d'un terme t sur $\mathscr{L}$, noté $\sharp t$, est défini par :

- $t = \textcircled{0}$ alors $\sharp t := \alpha_3(0, 0, 0)$;
- $t = x_n$ alors $\sharp t := \alpha_3(n+1, 0, 0)$;
- $t = \textcircled{S}\, t_1$ alors $\sharp t := \alpha_3(\sharp t_1, 0, 1)$;
- $t = t_1 \oplus t_2$ alors $\sharp t := \alpha_3(\sharp t_1, \sharp t_2, 2)$;
- $t = t_1 \otimes t_2$ alors $\sharp t := \alpha_3(\sharp t_1, \sharp t_2, 3)$.

Lemme 3.8. Le codage est injectif.

Preuve. Expliciter la fonction de décodage définie sur l'espace image. □

Lemme 3.9. L'ensemble Term := $\{\sharp t \mid t$ est un terme de $\mathscr{L}_0\}$ est récursif primitif.

Preuve. Montrons que la fonction caractéristique T de Term est récursif primitif. On utilise le lemme de définition par cas et récursion donné précédemment :

- si $\beta_3^3(x) = 0$ et $\beta_3^2(x) = 0$ alors $T(x) = 1$ (x est le code de Ⓞ ou $x_{\beta_3^1(x)-1}$) ;
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$ alors $T(x) = T(\beta_3^1(x))$ (x est le code de Ⓢt) ;
- si $\beta_3^3(x) = 2$ alors $T(x) = T(\beta_3^1(x)) \cdot T(\beta_3^2(x))$ (x est le code de $t \oplus t$) ;
- si $\beta_3^3(x) = 3$ alors $T(x) = T(\beta_3^1(x)) \cdot T(\beta_3^2(x))$ (x est le code de $t \otimes t$) ;
- sinon, $T(x) = 0$.

□

3.4.3 Les formules.

Définition 3.7. On étend $\sharp\cdot$ aux formules :

- $\sharp(t_1 = t_2) := \alpha_3(\sharp t_1, \sharp t_2, 0)$
- $\sharp(\neg F) := \alpha_3(\sharp F, 0, 1)$
- $\sharp(F_1 \vee F_2) := \alpha_3(\sharp F_1, \sharp F_2, 2)$
- $\sharp(F_1 \wedge F_2) := \alpha_3(\sharp F_1, \sharp F_2, 3)$
- $\sharp(F_1 \to F_2) := \alpha_3(\sharp F_1, \sharp F_2, 4)$
- $\sharp(\forall x_k\, F) := \alpha_3(\sharp F, k, 5)$
- $\sharp(\exists x_k\, F) := \alpha_3(\sharp F, k, 6)$
- $\sharp\bot = \alpha_3(0, 0, 7)$.

Lemme 3.10. Le codage ci-dessus est injectif. □

Lemme 3.11. L'ensemble Form := $\{\sharp F \mid F \text{ formule de } \mathscr{L}_0\}$ est récursif primitif. □

3.4.4 Opérations sur les formules.

Lemme 3.12. Les ensembles suivants sont récursifs primitifs :

- $\theta_0 := \{(\sharp t, n) \mid t \text{ est un terme et } x_n \text{ n'a pas d'occurrence dans } t\}$
- $\theta_1 := \{(\sharp t, n) \mid t \text{ est un terme et } x_n \text{ a une occurrence dans } t\}$
- $\phi_0 := \{(\sharp F, n) \mid F \text{ est une formule et } x_n \text{ n'a pas d'occurrence dans } F\}$
- $\phi_1 := \{(\sharp F, n) \mid F \text{ est une formule et } x_n \text{ n'a pas d'occurrence libre dans } F\}$
- $\phi_2 := \{(\sharp F, n) \mid F \text{ est une formule et } x_n \text{ n'a pas d'occurrence liée dans } F\}$
- $\phi_3 := \{(\sharp F, n) \mid F \text{ est une formule et } x_n \text{ a une occurrence libre dans } F\}$
- $\phi_4 := \{(\sharp F, n) \mid F \text{ est une formule et } x_n \text{ a une occurrence liée dans } F\}$
- $\phi_5 := \{\sharp F \mid F \text{ est une formule close }\}$

Preuve. On montre le résultat pour θ_0 (le reste en exercice). On définit la fonction caractéristique de θ_0, notée $g_0(x, y)$, par (en utilisant le lemme de définition par cas et récursion) :

- si $\beta_3^3(x) = \beta_3^2(x) = 0$ et $\beta_3^1(x) - 1 \neq y$ alors $g_0(x, y) := 1$;
- si $\beta_3^2(x) = 1$ et $\beta_3^2(x) = 0$ alors $g_0(x, y) := g_0(\beta_3^2(x), y)$;
- si $\beta_3^3(x) = 2$ ou 3 alors $g_0(x, y) := g_0(\beta_3^1(x), y) \times g_0(\beta_3^2(x), y)$;
- sinon, $g_0(x, y) := 0$.

□

Lemme 3.13 (Substitutions). Il existe des fonctions récursives primitives Subst_t et Subst_f à trois variables telles que, si t t u sont des termes, et si G est une formule, alors pour tout entier n,

- $\text{Subst}_\text{t}(n, \sharp t, \sharp u) := \sharp(u[x_n := t])$
- $\text{Subst}_\text{f}(n, \sharp t, \sharp F) := \sharp(F[x_n := t])$.

Preuve. On définit Subst_t par cas/récursion. Pour (n, y, x), on a :

- si $\beta_3^3(x) = 0$ alors

- si $\beta_3^1(x) = n+1$ alors $\mathrm{Subst_t}(n,y,x) := y$,
- sinon $\mathrm{Subst_t}(n,y,x) := x$;

▷ si $\beta_3^3(x) = 1$ alors $\mathrm{Subst_t}(n,y,x) := \alpha_3(\mathrm{Subst_t}(n,y,\beta_3^1(x)),0,1)$;
▷ si $\beta_3^3(x) = 1$ alors
$\mathrm{Subst_t}(n,y,x) := \alpha_3(\mathrm{Subst_t}(n,y,\beta_3^1(x)),\mathrm{Subst_t}(n,y,\beta_3^2(x)),\beta_3^3(x))$;
▷ sinon $\mathrm{Subst_t}(n,y,x) := 0$.

Puis, on définit $\mathrm{Subst_f}$ par :

▷ si $\beta_3^3(x) = 0$ alors $\mathrm{Subst_f}(n,y,x) = \alpha_3(\mathrm{Subst_t}(n,y,\beta_3^1(x))),\mathrm{Subst_t}(n,y,\beta_3^1(x)),0)$;
▷ si $\beta_3^3(x) = 1$ alors $\mathrm{Subst_f}(n,y,x) = \alpha_3(\mathrm{Subst_f}(n,y,\beta_3^1(x)),0,1)$;
▷ si $\beta_3^3(x) = 2,3,$ ou 4 alors $\mathrm{Subst_f}(n,y,x) = \alpha_3(\mathrm{Subst_f}(n,y,\beta_3^1(x)),\mathrm{Subst_f}(n,y,\beta_3^2(x)),\beta_3^3(x))$;
▷ si $\beta_3^3(x) = 5$ ou 6 alors
  – si $\beta_3^2(x) = n$ et x_n est liée dans F donc $\mathrm{Subst_f}(n,y,x) := x$;
  – sinon donc $\mathrm{Subst_f}(n,y,x) := \alpha_3(\mathrm{Subst_f}(n,y,\beta_3^1(x)),\beta_3^2(x),\beta_3^3(x))$;
▷ si $\beta_3^3(x) = 7$ alors $\mathrm{Subst_f}(n,x,y) := x$;
▷ sinon, $\mathrm{Subst_f}(n,x,y) := 0$.

□

3.4.5 Codage des preuves.

On code un contexte comme des suites finies, *i.e.* des listes, de formules (c'est plus facile que pour les ensembles).

Définition 3.8. On définit le codage par :

▷ $\sharp[\,] := 0$;
▷ $\sharp(F::\Gamma) := 1 + \alpha_2(\sharp\Gamma,\sharp F)$.

Lemme 3.14. Le décodage est unique. □

Lemme 3.15. La substitution d'une formule dans un contexte est récursif primitif. Tester si une variable est libre (*resp.* liée) dans un contexte est récursif primitif. □

3.4.6 Codage des preuves en déduction naturelle.

Remarque 3.6. Le contexte de la conclusion et des prémisses est

le même sauf pour

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A}\ \mathsf{aff} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_{\mathsf{i}} \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \to_{\mathsf{i}}$$

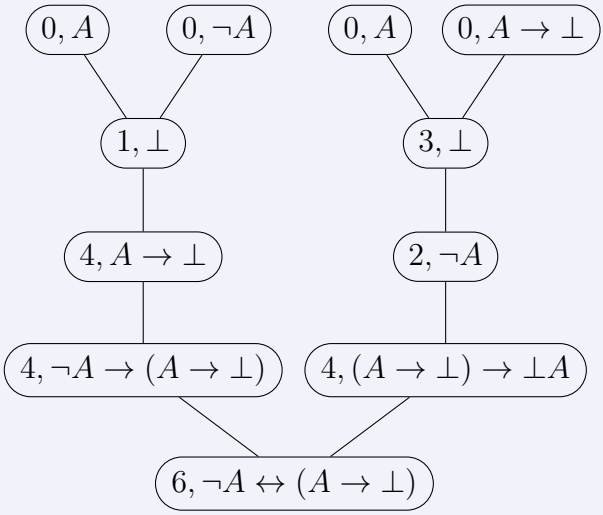
$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_{\mathsf{c}} \qquad \frac{}{\Gamma \vdash A}\ \mathsf{ax}.$$

On peut toujours déterminer le contexte du haut à partir du bas donc donner le contexte de la racine suffit. Une preuve est donc finalement un contexte et un arbre de dérivation où les nœuds sont étiquetés par une formule et un numéro de règle.

Exemple 3.3. La preuve

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A, A \vdash A}\ \mathsf{ax} \quad \dfrac{}{\neg A, A \vdash \neg A}\ \mathsf{ax}}{\neg A, A \vdash \bot}\ \neg_{\mathsf{e}}}{\neg A \vdash A \to \bot}\ \to_{\mathsf{i}}}{\vdash \neg A \to (A \to \bot)}\ \to_{\mathsf{i}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \to \bot, A \vdash A}\ \mathsf{ax} \quad \dfrac{}{A \to \bot, A \vdash A \to \bot}\ \mathsf{ax}}{A \to \bot, A \vdash \bot}\ \to_{\mathsf{e}}}{A \to \bot \vdash \neg A}\ \neg_{\mathsf{i}}}{\vdash (A \to \bot) \to \neg A}\ \to_{\mathsf{i}}}{\vdash \neg A \leftrightarrow (A \to \bot)}\ \wedge_{\mathsf{i}}$$

peut être codée par l'arbre suivant avec le contexte `[ ]` à la racine :



Définition 3.9. On numérote

- ♯ax := 0
- ♯$\neg_e$:= 1
- ♯$\neg_i$:= 2
- ♯ $\to_e$:= 3
- ♯ $\to_i$:= 4
- ♯$\wedge_e$:= 5
- ♯$\wedge_i$:= 6
- *etc.*

Définition 3.10 (Nombre de Gödel des preuves). ▷ Si $D^\star$ est un arbre de preuve à un seul nœud étiqueté par la formule F et la règle n alors $\sharp D^\star := \alpha_3(n, \sharp F, 0)$.

▷ Si $D^\star$ est un arbre de preuve dont la racine est étiquetée par la formule F et la règle n à k prémisses avec les sous arbres $D_1^\star, \dots, D_k^\star$

$$\frac{D_1^\star \quad \cdots \quad D_k^\star}{F} \text{ règle } n$$

alors $\sharp D^\star := \alpha_3(n, \sharp F, \alpha_k(\sharp D_1^\star, \dots, \sharp D_k^\star) + 1)$.

On pose ensuite $\sharp D := \alpha_2(\sharp D^\star, \sharp \Gamma)$ pour une preuve D.

Lemme 3.16. C'est un code injectif.

Lemme 3.17. L'ensemble Preuve := $\{\sharp D \mid D \text{ est une preuve}\}$ est récursif primitif.

3.4.7 Théories (in)décidables.

Définition 3.11. Un ensemble A de formules est un ensemble d'*axiomes* de la théorie T si $A \vdash T$ et $T \vdash A$.

Définition 3.12. Une théorie T sur $\mathscr{L}_0$ a un ensemble d'axiomes Ax_T récursif si l'ensemble des numéros de formules de Ax_T est récursif.

Remarque 3.7. Si Ax_T est fini, alors il est récursif (exemple : $\mathscr{P}_0$).

Lemme 3.18. L'ensemble des axiomes de Peano $\mathscr{P}$ est récursif.

Preuve. Il suffit de montrer que l'ensemble des axiomes du schéma de récurrence est récursif. On définit

$$A_F := \forall x_1 \cdots \forall x_n \Big(\big(F(0, x_1, \ldots, x_n) \wedge \forall x_0 \, (F(x_0, \ldots, x_n) \to F(\textcircled{S} x_0, x_1, \ldots, x_n)) \big) \to \forall x_0 \, F(x_0, \ldots, x_n) \Big).$$

Idée pour décider si N est le code d'une formule A_F :

1. décoder pour trouver n et F ;
2. calculer $\sharp A_F$ et vérifier si c'est N.

□

Proposition 3.2. Si une théorie T a un ensemble d'axiomes Ax_T alors l'ensemble

$$\mathrm{Dem}_T = \{ \, (\sharp D, \sharp F) \mid D \text{ est une preuve de } F \text{ dans } T \text{ avec } \mathrm{Ax}_T \, \}.$$

Preuve. L'idée de la preuve est la suivante :

1. décider x et y ;
2. vérifier que x est une preuve et y une formule ;
3. vérifier que D est une preuve de F ;
4. vérifier que le contexte final ne contient que des éléments de Ax_T.

□

Dans la suite, on prend $\mathscr{L} \supseteq \mathscr{L}_0$.

Définition 3.13. Une théorie est *décidable* si l'ensemble de ses théorèmes est récursif.

Remarque 3.8 (Rappel)**.** Une théorie est *consistante* si elle a un modèle.

Théorème 3.5. Soit T une théorie consistante contenant $\mathscr{P}_0$. Alors, T est indécidable.

Preuve. On suppose que T est décidable et on construit par diagonalisation une formule F telle que $T \vdash F$ et $T \vdash \neg F$. Soit

$$\theta := \{\, (m,n) \mid m = \sharp(F(n)) \text{ et } T \vdash F(\textcircled{n}) \,\}.$$

L'ensemble T est décidable donc T aussi. On pose

$$B := \{\, n \in \mathbb{N} \mid (n,n) \notin \theta \,\},$$

qui est récursif.

D'après le théorème de représentation, il existe une formule $G(x)$ représentant B :

- $n \in B \implies \mathscr{P}_0 \vdash G(\textcircled{n})$ donc $T \vdash G(\textcircled{n})$;
- $n \notin B \implies \mathscr{P}_0 \vdash \neg G(\textcircled{n})$ donc $T \vdash \neg G(\textcircled{n})$.

Soit $a = \sharp(G(x))$. Est-ce que $a \in B$?

- On a $a \in B \iff (a,a) \notin \theta \iff T \nvdash G(@)$. Or, si $a \in B$ alors, par définition de G, on a $T \vdash G(@)$. ***Absurde !***
- On a $a \notin B \iff (a,a) \in \theta \iff T \vdash G(@)$. Or, si $a \notin B$ alors, par définition de G, on a $T \vdash \neg G(@)$. Donc T non consistante. ***Absurde !***

□

Exemple 3.4 (Application du théorème)**.** La théorie $T = \mathbf{Th}(\mathbb{N})$ est indécidable.

Exemple 3.5 (Quelques théories décidables).
- ▷ Les ordres denses sans extrémités (la théorie linéaire des rationnels) est une théorie décidable.
- ▷ Les corps réels clos (*théorème de Tarski*) est une théorie décidable.
- ▷ L'arithmétique de Presburger (la théorie linéaire des entiers) est une théorie décidable.
- ▷ Pour chaque p, les corps algébriquement clos de caractéristique p est une théorie décidable.

On peut donc répondre à l'Entscheidungsproblem, le problème de décision.

Théorème 3.6 (Church, indécidabilité du calcul des prédicats). Si $\mathscr{L} \supseteq \mathscr{L}_0$, l'ensemble T des théorèmes logiques sur $\mathscr{L}$ n'est pas récursif.

Preuve. Soit T_0 l'ensemble des théorèmes logiques sur $\mathscr{L}_0$. Soit G la conjonction des axiomes de $\mathscr{P}_0$. Pour toute formule F, on a $\mathscr{P}_0 \vdash F$ ssi $T_0 \vdash (G \to F)$. Donc, si T_0 est récursif alors $\mathscr{P}_0$ est décidable. Donc, si T est récursif, alors T_0 aussi. Donc $\mathscr{P}_0$ est décidable, ***absurde***. □

3.5 Théorèmes d'incomplétude de Gödel

Théorème 3.7 (Premier théorème d'incomplétude de Gödel). Soit T une théorie qui a un ensemble d'axiomes récursifs, et qui est consistante, et qui contient $\mathscr{P}_0$. Alors, T n'est pas axiome-complète.

Preuve. Une théorie qui a un ensemble d'axiomes récursifs et qui est complète, est décidable, ce qui est faux.

En effet, pour F une formule, comment déterminer (algorithmiquement) su $T \vdash F$? On énumère toutes les preuves jusqu'à en trouver une de F ou de $\neg F$. □

Corollaire 3.1. La théorie $\mathscr{P}$ n'est pas complète.

Question.

Peut-on exhiber une formule F telle que $T \nvdash F$ et $T \nvdash \neg F$?

On va construire F qui « dit » que T est consistante.

Définition 3.14. On pose :

- $\mathrm{Dem}_T := \{ (\sharp D, \sharp F) \mid D \text{ preuve de } F \text{ dans } T \}$;
- $\mathrm{Dem}_{\mathscr{P}_0} := \{ (\sharp D, \sharp F) \mid D \text{ preuve de } F \text{ dans } \mathscr{P}_0 \}$.

Proposition 3.3.

- Ces ensembles sont récursifs donc représentés par F_T et $F_{\mathscr{P}_0}$.
- La fonction $\mathrm{neg} : \mathbb{N} \to \mathbb{N}, \sharp F \mapsto \sharp(\neg F) = \alpha_3(\sharp F, 0, 1)$ est récursive et représentée par $F_{\mathrm{neg}}(x_0, x_1)$:

$$\forall n \in \mathbb{N}, \quad \mathscr{P}_0 \vdash \forall x \, (F_{\mathrm{neg}}(x, \underline{n}) \leftrightarrow x = \underline{\mathrm{neg}(n)}).$$

□

Définition 3.15. On pose

$$\mathrm{Coh}(T) := \neg \exists x_0 \cdots \exists x_3 \Big(F_T(x_0, x_2) \wedge F_T(x_1, x_3) \wedge F_{\mathrm{neg}}(x_2, x_3) \Big).$$

Remarque 3.9. La fonction Coh n'est pas complètement définie, car elle dépend du choix de F_T et de F_{neg}.

Proposition 3.4. La théorie T est consistante ssi $\mathbb{N} \models \mathrm{Coh}(T)$.

Remarque 3.10. On pourrait avoir $\mathscr{M} \models T$, avec T consistante et $\mathscr{M} \models \neg\mathrm{Coh}(T)$. En effet, il suffit que x_0, x_1, x_2, x_3 ne soient pas

des entiers standards.

Théorème 3.8 (Second théorème d'incomplétude de Gödel)**.** Soit T une théorie consistante, axiome-récursive, et contenant $\mathscr{P}_0$. Alors, $T \nvdash \mathrm{Coh}(T)$.

Remarque 3.11. Si $\mathbb{N} \models T$, ce théorème implique le 1er théorème d'incomplétude car $\mathbb{N} \not\models \neg\mathrm{Coh}(T)$, donc $T \not\models \neg\mathrm{Coh}(T)$ et donc T incomplète.

Dans le cas général, ce n'est pas vrai : $T \cup \{\neg\mathrm{Coh}(T)\}$ est une théorie consistante. Par exemple, $\mathscr{P} \cup \{\neg\mathrm{Coh}(\mathscr{P})\}$ est consistante mais $\mathbb{N}$ n'en est pas un modèle.

Définition 3.16. L'ensemble Σ est le plus petit ensemble de formules contenant $\mathscr{L}_0$ qui

- ▷ contient les formules sans quantificateurs ;
- ▷ est clos par $\wedge, \vee, \exists$;
- ▷ est clos par quantification universelle bornée, *i.e.* si $F \in \Sigma$ alors
$$\Big(\forall v_0\, (v_0 < v_1) \to F\Big) \in \Sigma.$$

Exemple 3.6. Les relations « $n \mid m$ » et « m est premier » peuvent s'exprimer avec des formules de Σ.

Lemme 3.19 (Représentation (bis))**.** Toute fonction récursive totale est représentable par une formule de Σ.

Preuve. Les formules que l'on construit dans le lemme 3.3 sont des formules de Σ. □

Lemme 3.20. Il existe des formules F_T et $F_{\mathscr{P}_0}$ qui satisfont :

1. $\vdash \forall v_0\, \forall v_1\, F_{\mathscr{P}_0}(v_0, v_1) \to F_T(v_0, v_1)$;
2. F_T et $F_{\mathscr{P}_0}$ sont dans Σ ;
3. si F est une formule close de Σ alors

$$\mathscr{P} \vdash (F \to \exists x\, F_{\mathscr{P}_0}(x_1, \sharp F)).$$

Preuve. 1. Il suffit de remplacer F_T par par $F_T \vee F_{\mathscr{P}_0}$.
2. C'est une conséquence du lemme précédent.
3. On va le montrer pour une théorie $\mathscr{P}_1$ contenant $\mathscr{P}_0$ et conséquence de $\mathscr{P}$ mais, *a priori*, plus faible que $\mathscr{P}$. Puis, on l'admet pour $\mathscr{P}$, et on admet que $\mathscr{P} \vdash \mathscr{P}_1$. On a le montrer par la proposition suivante.

□

Proposition 3.5. Soit F une formule close sur $\mathscr{L}_0$ dans Σ. Alors,

$$\mathbb{N} \models F \to \exists x_1\, F_{\mathscr{P}_0}(x_1, \sharp F).$$

Preuve. ▷ Si F est fausse, c'est montré.
▷ Si $\mathbb{N} \models F$, il faut montrer que F a une preuve dans $\mathscr{P}_0$, *i.e.* que tout modèle $\mathscr{M} \models \mathscr{P}_0$, on a $\mathscr{M} \models F$ *i.e.* que dans tout extension finale $\mathscr{M}$ de $\mathbb{N}$ alors $\mathscr{M} \models F$, pour cela il suffit de montrer le lemme suivant.

□

Lemme 3.21. Soient $\mathscr{N}$ une $\mathscr{L}_0$-structure et $\mathscr{M}$ une extension finale de $\mathscr{N}$. Soient $F(x_1, \ldots, x_p) \in \Sigma$ et $a_1, \ldots, a_p \in \mathscr{N}$. Alors, $\mathscr{N} \models F(a_1, \ldots, a_p)$ implique $\mathscr{M} \models F(a_1, \ldots, a_p)$.

Preuve. Par induction sur $F(x_1, \ldots, x_p) \in \Sigma$. □

On termine la preuve du point 3.

Preuve. On pose

$$\mathscr{P}_1 := \mathscr{P}_0 \cup \{\, F \to \exists x\, F_F(x_1, \sharp F) \mid F \text{ formule close de } \Sigma \,\}.$$

On a montré que $\mathbb{N} \models \mathscr{P}$. On admet que $\mathscr{P} \vdash \mathscr{P}_1$ donc $T \vdash \mathscr{P}_1$. □

Lemme 3.22 (Cœur du 2nd théorème d'incomplétude)**.** Soit T une théorie consistante, axiome-récursive, et contenant $\mathscr{P}_0$. Alors, $T \nvdash \mathrm{Coh}(T)$.

Preuve. ▷ Soit $g : \mathbb{N} \to \mathbb{N}$ définie par $n = \sharp F(x_0) \mapsto \sharp F(\textcircled{n}) = \sharp F(\textcircled{\sharp F(x_0)})$. C'est *la formule appliquée à elle-même*. La fonction g est primitive récursive, donc représentée par une formule $G(x, y)$ telle que

$$\forall n \in \mathbb{N}, \quad \mathscr{P}_0 \vdash \forall x\, G(x, \textcircled{n}) \leftrightarrow x = \textcircled{g(n)}.$$

- ▷ On considère la formule « il existe une preuve de x_0 appliquée à elle-même » :

$$\varepsilon(x_0) := \exists x_1\, \exists x_2\, F_T(x_1, x_2) \wedge G(x_2, x_0).$$

- ▷ On pose $a := \sharp(\neg\varepsilon(x_0))$, « il n'existe pas de preuve de x_0 appliquée à elle-même ».
- ▷ On pose $b := g(a) = \sharp(\neg\varepsilon(\textcircled{@}))$, « il n'existe pas du preuve du fait qu'il n'existe pas de preuve de x_0 appliquée à elle-même ».
- ▷ Dans $\mathscr{P}_0$, on a $\forall x_2\, G(x_2, \textcircled{@}) \leftrightarrow x_2 = \textcircled{b}$.
- ▷ Par définition, $\varepsilon(\textcircled{@})$ est $\exists x_1\, \exists x_2\, F_T(x_1, x_2) \wedge G(x_0, \textcircled{@})$. « Il existe une preuve du fait qu'il n'existe pas de preuve de nous-même ». Dans $\mathscr{P}_0$, $\varepsilon(\textcircled{@})$ est équivalent à $\exists x_1 F_T(x_1, \textcircled{b}) \wedge G(\textcircled{b})$, ce qui est équivalent à $\exists x_1\, F_T(x_1, \textcircled{b})$ car $b = g(a)$ $(\star)$. Ainsi, on a « $\varepsilon(\textcircled{@})$ ssi il y a une preuve de $\neg\varepsilon(\textcircled{@})$ »

Voici le paradoxe :

- ▷ Prouvons que $T \vdash \mathrm{Coh}(T) \to \neg\varepsilon(@)$. Il suffit de montrer que $\mathscr{P}_1 \vdash \varepsilon(@) \to \neg\mathrm{Coh}(T)$. Soit $T_1 := \mathscr{P}_1 \cup \{\varepsilon(@)\}$. Alors $T_1 \vdash \exists v_1\, F_T(v_1, \textcircled{b})$ et $b = \sharp(\neg\varepsilon(@))$ On a donc une preuve de $\varepsilon(@)$ et une preuve de $\neg\varepsilon(@)$, donc de $\neg\mathrm{Coh}(T)$.
- ▷ On va montrer que $T \vdash \neg\varepsilon(@)$ mène à un paradoxe. Si c'est vrai, soit C le numéro d'une preuve de $\neg\varepsilon(@)$ dans T. Alors, $\mathscr{P}_0 \vdash F_T(\textcircled{c}, \textcircled{b})$. D'où, avec $(\star)$, $\mathscr{P}_0 \vdash \varepsilon(@)$ impossible car T consistante. Donc $T \nvdash \neg\varepsilon(@)$ et donc $T \nvdash \mathrm{Coh}(T)$.

□

4 La théorie des ensembles.

On se place dans la logique du 1er ordre avec $\mathscr{L} = \{\in, =\}$. On se place dans un univers $\mathcal{U}$ non vide, le modèle, dont les éléments sont appelés des *ensembles*.

Il faudra faire la différence entre les ensembles « naïfs » (les ensembles habituels), et les ensembles « formels » (les éléments de $\mathcal{U}$).

On a le paradoxe de Russel. On peut l'écrire

> « On a un barbier qui rase tous les hommes qui ne se rasent pas eux-mêmes. Qui rase le barbier ? ».

Si $\mathcal{U}$ est l'ensemble de tous les ensembles, alors

$$a := \{\, x \in \mathcal{U} \mid x \notin x \,\}$$

vérifie $a \in a \iff a \notin a$, ***paradoxe***. Pour éviter ce paradoxe, on choisit donc de ne pas faire $\mathcal{U}$ un ensemble.

4.1 Les axiomes de la théorie de Zermelo-Fraenkel.

ZF 1. *Axiome d'extensionnalité* : deux ensembles sont égaux ssi ils ont les mêmes éléments

$$\forall x\, \forall y \Big(\forall z\, (z \in x \leftrightarrow z \in y) \leftrightarrow x = y\Big).$$

- *Axiome de la paire*[1] : il existe une paire $\{x, y\}$ pour tout élément x et y

$$\forall x\, \forall y\, \exists z\, \forall t\Big(t \in z \leftrightarrow (t = x \vee t = y)\Big).$$

1. On verra plus tard que cet axiome est une conséquence des autres (de ZF 3 et ZF 4).

[*continué plus tard...*]

Remarque 4.1. Cela nous donne l'existence du *singleton* $\{x\}$ si x est un ensemble. En effet, il suffit de faire la paire $\{x, x\}$ avec l'Axiome de la paire.

Définition 4.1. Si a et b sont des ensembles, alors (a, b) est l'ensemble $\{\{a\}, \{a, b\}\}$. Ainsi, (a, a) est l'ensemble $\{\{a\}\}$.

Lemme 4.1. Pour tous ensembles a, b, a', b', on a $(a, b) = (a', b')$ ssi $a = a'$ et $b = b'$.

Preuve. En exercice. □

Définition 4.2. On peut construire des 3-uplets (a_1, a_2, a_3) avec $(a_1, (a_2, a_3))$, et ainsi de suite pour les n-uplets.

Notation. On utilise les raccourcis

- $t = \{a\}$ pour $\forall x\,(x \in t \leftrightarrow x = a)$;
- $t = \{a, b\}$ pour $\forall x\,(x \in t \leftrightarrow (x = a \vee x = b))$;
- $t \subseteq a$ pour $\forall x\,(z \in t \to z \in a)$.

ZF 3. *Axiome des parties* : l'ensemble des parties $\wp(a)$ existe pour tout ensemble a

$$\forall a\, \exists b\, \forall t\, (t \in b \leftrightarrow t \subseteq a).$$

ZF 2. *Axiome de la réunion* : l'ensemble $y = \bigcup_{z \in x} z$ existe

$$\forall x\, \exists y\, \forall t (t \in y \leftrightarrow \exists z (t \in z \wedge z \in x)).$$

Remarque 4.2. Comment faire $a \cup b$? La paire $x = \{a, b\}$ existe par l'Axiome de la paire, et $\bigcup_{z \in x} z = a \cup b$ est un ensemble

par ZF 2.

ZF 4'. *Schéma de compréhension* : pour toute formule $\varphi(y, v_1, \dots, v_n)$, on a l'ensemble $x = \{ y \in v_{n+1} \mid \varphi(y, v_1, \dots, v_n) \}$

$$\forall v_1 \ \dots \ \forall v_n \ \exists x \ \forall y \ \Big(y \in x \leftrightarrow (y \in v_{n+1} \wedge \varphi(y, v_1, \dots, v_n)) \Big).$$

Remarque 4.3. Peut-on faire le paradoxe de Russel ? On ne peut pas faire $a := \{z \in \mathcal{U} \mid z \notin z\}$ car $\mathcal{U}$ n'est pas un ensemble ! Et, on ne peut pas avoir de paradoxe avec $b := \{z \in E \mid z \notin z\}$, car on a l'ajout de la condition $b \in E$.

Définition 4.3. Une *relation fonctionnelle* en w_0 est une formule $\varphi(w_1, w_2, a_1, \dots, w_n)$ *à paramètres* (où les a_i sont dans $\mathcal{U}$) telle que

$$\mathcal{U} \models \forall w_0 \ \forall w_1 \ \forall w_2 \ \Big(\varphi(w_0, w_1, a_1, \dots, a_n) \wedge \varphi(w_0, w_2, a_1, \dots, w_n) \to w_1 = w_2 \Big).$$

En termes naïfs, c'est une fonction partielle. On garde le terme *fonction* quand le domaine et la collection d'arrivée sont des *ensembles*, autrement dit, des éléments de $\mathcal{U}$.

ZF 4. *Schéma de substitution/de remplacement* : « la collection des images par une relation fonctionnelle des éléments d'un ensemble est aussi un ensemble ». Pour tout n-uplet $\bar{a}$, si la formule à paramètres $\varphi(w_0, w_1, \bar{a})$ définit une relation fonctionnelle $f_{\bar{a}}$ en w_0 et si a_0 est un ensemble alors la collection des images par $f_{\bar{a}}$ des éléments de a_0 est un ensemble nommé a_{n+1}

$$\forall a_0 \ \cdots \ \forall a_n$$
$$\Big(\forall w_0 \ \forall w_1 \ \forall w_2 (\varphi(w_0, w_1, a_1, \dots, a_n) \wedge \varphi(w_0, w_2, a_1, \dots, a_n)) \to w_1 = w_2 \Big)$$
$$\downarrow$$
$$\exists a_{n+1} \ \forall a_{n+2} (a_{n+2} \in a_{n+1} \leftrightarrow \exists w_0 \ w_0 \in a_0 \wedge \varphi(w_0, a_{n+2}, v_1, \dots, v_n)).$$

Théorème 4.1. Si ZF 1, ZF 2, ZF 3 et ZF 4 sont vrais dans $\mathcal{U}$, il existe (dans $\mathcal{U}$) un et un seul ensemble sans élément, que l'on notera $\emptyset$.

Preuve.
- ▷ *Unicité* par ZF 1.
- ▷ *Existence.* On procède par compréhension : l'univers $\mathcal{U}$ est non vide, donc a un élément x. On considère la formule $\varphi(w_0, w_1) := \bot$ qui est une relation fonctionnelle. Par ZF 4 (avec la formule φ et l'ensemble $a_0 := x$) un ensemble a_{n+1} qui est vide.

□

Proposition 4.1. Si ZF 1, ZF 2, ZF 3 et ZF 4 sont vrais dans $\mathcal{U}$, alors l'Axiome de la paire est vrai dans $\mathcal{U}$.

Preuve. On a $\emptyset$ dans $\mathcal{U}$ et également $\wp(\emptyset) = \{\emptyset\}$ et $\wp(\wp(\emptyset)) = \{\emptyset, \{\emptyset\}\}$ par ZF 3.

Étant donné deux ensemble a et b, on veut montrer que $\{a, b\}$ est un ensemble avec ZF 4

$$\varphi(w_0, w_1, a, b) := (w_0 = \emptyset \wedge w_1 = a) \vee (w_0 = \{\emptyset\} \wedge w_1 = b),$$

où

- ▷ $w_0 = \emptyset$ est un raccourci pour $\forall z\ (z \notin w_0)$;
- ▷ $w_0 = \{\emptyset\}$ est un raccourci pour $\forall z\ (z \in w_0 \leftrightarrow (\forall t\ t \notin z))$.

Ces notations sont compatibles avec celles données précédemment.

Comme φ est bien une relation fonctionnelle et $\{a, b\}$ est l'image de $\{\emptyset, \{\emptyset\}\}$. □

Proposition 4.2. Si ZF 1, ZF 2, ZF 3 et ZF 4 sont vrais dans $\mathcal{U}$, alors ZF 4' est vrai dans $\mathcal{U}$.

Preuve. On a la formule $\varphi(y, v_1, \dots, v_n)$ et on veut montrer que

$$\mathcal{U} \models \forall v_1 \ \cdots \ \forall v_{n+1} \ \exists x \ \forall y \ \Big(y \in x \leftrightarrow (y \in v_{n+1} \wedge \varphi(y, v_1, v_n)) \Big).$$

On considère la formule $\psi(w_0, w_1, \bar{v}) := w_0 = w_1 \wedge \varphi(w_0, \bar{v})$, qui est bien une relation fonctionnelle en w_0. La collection

$$\{ \, x \in v_{n+1} \mid \varphi(y, v_1, \dots, v_n) \, \}$$

est l'image de v_{n+1} par ψ par ZF 4. □

Remarque 4.4. La réciproque du théorème précédent est fausse ! Les axiomes ZF 4 et ZF 4' ne sont pas équivalents. On le verra en TD (probablement).

Proposition 4.3. Le produit ensembliste de deux ensembles est un ensemble.

Preuve. Soient v_1 et v_2 deux ensembles. On considère

$$X := v_1 \times v_2 = \{ \, (x, y) \mid x \in v_1 \text{ et } y \in v_2 \, \} \text{ (en naïf)} \ .$$

La notation (x, y) correspond à l'ensemble $\{\{x\}, \{x, y\}\} \in \wp(\wp(v_1 \cup v_2))$.

On applique ZF 4' dans l'ensemble ambiant $\wp(\wp(v_1 \cup v_2))$, on définit le produit comme la compréhension à l'aide de la formule

$$\varphi(z, v_1, v_2) := \exists x \ \exists y \ \Big(z = \{\{x\}, \{x, y\}\} \wedge x \in v_1 \wedge y \in v_2 \Big).$$

C'est bien un élément de $\mathcal{U}$. □

Définition 4.4. Une *fonction* (sous-entendu *totale*) d'un ensemble a dans un ensemble b est un sous-ensemble de $a \times b$ qui vérifie la

propriété

$$\varphi(f,a,b) := \left(\begin{array}{c} f \subseteq a \times b \\ \wedge \\ \forall x\, \forall y\, \forall y'\, (x,y) \in f \wedge (x,y') \in f \to y = y' \\ \wedge \\ \forall x\, x \in a \to \exists y\, y \in b \wedge (x,y) \in f \end{array}\right).$$

On identifie ainsi f et son graphe.

Une *fonction partielle* d'un ensemble a dans un ensemble b est un sous-ensemble de $a \times b$ qui vérifie la propriété

$$\varphi(f,a,b) := \left(\begin{array}{c} f \subseteq a \times b \\ \wedge \\ \forall x\, \forall y\, \forall y'\, (x,y) \in f \wedge (x,y') \in f \to y = y' \end{array}\right).$$

On note b^a la collection des fonctions partielles de a dans b.

Proposition 4.4. La collection b^a est un ensemble, *i.e.* si a et b sont dans $\mathcal{U}$ alors b^a aussi.

Preuve. En exercice. □

Remarque 4.5 (Réunion indexée)**.** Soit a une famille d'ensemble indexée par l'ensemble I, *i.e.* a est une fonction de domaine I. Si $i \in I$, on note a_i pour $a(i)$.

Proposition 4.5. Si I est un ensemble et a est une fonction de domaine I, alors $\bigcup_{i\in I} a_i$ est un ensemble. Autrement dit, si dans $\mathcal{U}$, ZF 1, ZF 2, ZF 3, ZF 4 sont vraies, et que I et a sont dans $\mathcal{U}$, et a est une fonction, alors la collection définie naïvement par $\bigcup_{i\in I} a_i$ appartient à $\mathcal{U}$.

Preuve. On pose $b := \{a_i \mid i \in I\}$. C'est bien un ensemble car b

est l'ensemble des images des éléments de I par a. On peut écrire a comme relation fonctionnelle :

$$\varphi(w_0, w_1, a) := (w_0, w_1) \in a.$$

On a donc que b est un ensemble avec ZF 4.

Et, $\bigcup_{i\in I} a_i = \bigcup_{z\in b} z$ donc on conclut par ZF 2. □

Proposition 4.6 (Propriété d'intersection)**.** Si I est un ensemble non vide et a est une fonction de domaine I alors $\bigcap_{i\in I} a_i$ est un ensemble.

Preuve. On pose $c := \bigcup_{i\in I} a_i$ qui est un ensemble par ZF 2. On considère

$$\varphi(x, a, I) := \forall i\, i \in I \to x \in a_i.$$

Par compréhension (ZF 4') on construit l'ensemble

$$\bigcap_{i\in I} a_i := \{x \in c \mid \varphi(x, a, I)\}.$$

□

Proposition 4.7. Si I est un ensemble et a une fonction de domaine i alors $\prod_{i\in I} a_i$ est un ensemble.

Preuve. La collection $\prod_{i\in I} a_i$ est l'ensemble des fonctions de I dans $\bigcup_{i\in I} a_i$ telles que $f(i) \in a_i$ pour tout i. □

ZF 5 *Axiome de l'infini* : il existe un ensemble ayant une infinité d'élément

$$\exists x\, (\emptyset \in x \wedge \forall y\, (y \in x \to y \cup \{y\} \in x)).$$

On encode les entiers avec des ensembles :

- $0 \rightsquigarrow \emptyset$
- $1 \rightsquigarrow \{\emptyset\}$

- $2 \rightsquigarrow \{\emptyset, \{\emptyset\}\}$
- $\vdots$
- $n+1 \rightsquigarrow n \cup \{n\}$
- $\vdots$

Ainsi, on a bien $n = \{0, 1, \ldots, n-1\}$.

Remarque 4.6. Si on retire $\emptyset \in x$, on peut avoir $x = \emptyset$ qui satisfait la version modifiée de ZF 5.

Cependant, sans retirer $\emptyset \in x$, on peut quand même avoir un ensemble fini s'il existe un ensemble fini y tel que $y \in y$. Ceci est impossible avec l'axiome de bonne fondation.

Remarque 4.7. Les français sont les seuls à considérer que l'axiome de bonne fondation ne fait pas partie de la théorie de ZF.

4.2 Ordinaux et induction transfinie.

Théorème 4.2 (Cantor).
1. Soient A et B deux ensembles et supposons qu'il existe des injections $A \to B$ et $B \to A$ alors il existe une bijection $A \to B$.
2. Il n'existe pas de surjection de $A \to \wp(A)$.

Preuve. En TD. □

Définition 4.5. Deux ensembles sont *équipotents* s'il existe une bijection entre-eux.

Définition 4.6. Soit A un ensemble. Un *ordre* (*partiel*, *strict*) sur A est une relation binaire $<$ (donnée par un sous-ensemble de $A \times A$) telle que

1. *transitivité* : $\forall x\, \forall y\, \forall z\, x < y \to y < z \to x < z$;
2. *anti-réflexif* : $\forall x, x \not< x$.

Notation. On note $x \leq y$ pour $x < y$ ou $x = y$.

Exemple 4.1. L'ordre $\subsetneq$ sur $\wp(\mathbb{N})$ est partiel. Les ordres $<_{\mathbb{N}}$, $<_{\mathbb{R}}$, $<_{\mathbb{Z}}$ sur $\mathbb{N}, \mathbb{R}, \mathbb{Z}$ sont totaux.

Définition 4.7. Soit $(A, <)$ ordonné. Soient $a, a' \in A$ et $B \subseteq A$. On dit que

- a est un plus petit élément de B si $a \in B$ et pour tout $b \in B$ et si $b \neq a$ alors $b > a$;
- a est un élément minimal de B si $a \in B$ et pour tout $b \in B$, $b \not< a$;
- a est un minorant de B si pour tout $b \in B$, $a \leq b$;
- de la même manière, on définit plus grand élément, élément maximal, majorant ;
- a est une borne inférieure de B si a est un plus grand élément de l'exemple des minorants de B ;
- a et a' sont incomparables si $a \neq a'$ et $a \not< a'$ et $a' \not< a$;
- un ordre est bien fondé si toute partie non vide de A a un élément minimal ;
- un bon ordre est un ordre total bien fondé.

Proposition 4.8. Un ordre total est bien fondé ssi il n'existe pas de suite infinie décroissante.

Preuve. En exercice. □

Exemple 4.2.
- L'ordre $<$ sur $\mathbb{N}$ est bien fondé.
- L'ordre $<$ sur $\mathbb{Z}$ n'est pas bien fondé.
- L'ordre $\subsetneq$ sur $\wp_{\text{finies}}(\mathbb{N})$ est bien fondé.
- L'ordre $\subsetneq$ sur $\wp(\mathbb{N})$ n'est pas bien fondé.

Définition 4.8.
- ▷ Deux ensembles ordonnés sont *isomorphes* s'il existe une bijection préservant l'ordre de l'un vers l'autre. On note $A \simeq B$.
- ▷ Soit X totalement ordonné. Un sous-ensemble $J \subseteq X$ est un *segment initial* si pour tous $a, b \in X$ avec $a < b$ alors $b \in J$ implique $a \in J$.
- ▷ Un ensemble X est *transitif* si pour tout $x \in X$ et $y \in x$ alors $y \in X$.
- ▷ Un ensemble X est un *ordinal* s'il est transitif et que $\in$ défini un bon ordre sur X.
- ▷ On note $\mathbb{O}$ la *classe des ordinaux*, et on note indifféremment les relations $\in$ et $<$.

Exemple 4.3. Les entiers de Von Neumann sont des ordinaux.

Proposition 4.9. Soient α et β des ordinaux. On a les propriétés suivantes :

1. $\emptyset$ est un ordinal ;
2. si $\alpha \neq \emptyset$ alors $\emptyset \in \alpha$;
3. $\alpha \notin \alpha$;
4. si $x \in \alpha$ alors $x = \{y \in \alpha \mid y < x\}$.
5. si $x \in \alpha$ alors x est un ordinal (on a l'abus de notation $x \in \mathbb{O}$) ;
6. $\beta \leq \alpha$ ssi $\beta = \alpha$ ou $\beta \in \alpha$;
7. $x = \alpha \cup \{\alpha\}$ est un ordinal noté $\alpha + 1$.

Preuve.
1. C'est vrai.
2. La relation $\in$ est un bon-ordre sur α, soit β le plus petit élément. Si $\beta \neq \emptyset$ alors il contient au moins un élément γ d'où $\gamma < \beta$ et $\gamma \in \alpha$ (par transitivité), *absurde* car β minimal.
3. Le reste sera vu en TD ou en exercice.

□

Proposition 4.10. ▷ Si α et β sont des ordinaux et que l'on a $\alpha \leq \beta \leq \alpha + 1$ alors $\beta = \alpha$ ou $\beta = \alpha + 1$.

▷ Si X est un ensemble non vide d'ordinaux alors $\bigcap_{\alpha \in X} \alpha$ est le plus petit élément de X.

□

Définition 4.9. Soit β un ordinal.

▷ S'il existe α tel que $\beta = \alpha + 1$ alors on dit que β est un ordinal successeur ;

▷ Sinon, c'est un ordinal limite.

Exemple 4.4. Quelques ordinaux limites :

$$\omega \qquad \omega \cdot 2 \qquad \omega \cdot 3 \qquad \omega \cdot \omega$$

$$\omega^2 + \omega \qquad \omega^\omega \qquad \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}} .$$

Lemme 4.2. Soit X un ensemble d'ordinaux. Le plus petit élément de X est $\bigcap_{\alpha \in X} \alpha$.

Théorème 4.3. Si α et β sont des ordinaux alors une et une seule de ces propriétés est vérifiée :

$$\alpha = \beta \qquad \alpha \in \beta \qquad \alpha \ni \beta.$$

Preuve. Soit $X = \{\alpha, \beta\}$, on sait que $\alpha \cap \beta$ est le plus petit élément de X.

▷ Si $\alpha \cap \beta = \alpha$ alors $a \subseteq \beta$ donc $\alpha = \beta$ ou $\alpha \in \beta$.

▷ Si $\alpha \cap \beta = \beta$ alors $a \supseteq \beta$ donc $\alpha = \beta$ ou $\alpha \ni \beta$.

□

Proposition 4.11. Soit X un ensemble d'ordinaux. Alors l'ensemble $b := \bigcup_{\alpha \in X} \alpha$ est un ordinal. On le note $b = \sup_{\alpha \in X} \alpha$. De plus si $\gamma \in b$ alors il existe un certain $\alpha \in X$ tel que $\gamma \in \alpha$.

Preuve. En exercice. □

Proposition 4.12. Soit λ un ordinal non vide. On a :

$$\overbrace{\lambda \text{ est limite}}^{(1)} \iff \overbrace{\lambda = \bigcup_{\alpha \in \lambda} \lambda}^{(2)}.$$

Preuve.

1. Par contraposée, si λ n'est pas limite, c'est donc un successeur d'un certain ordinal β et donc $\lambda = \beta \cup \{\beta\}$. On a
$$\bigcup_{\alpha \in \lambda} \alpha = \beta \cup \bigcup_{\alpha \in \beta} = \beta \neq \lambda.$$
2. Soit λ limite. Montrons qu'il n'a pas de plus grand élément β. Sinon, $\lambda = \beta \cup \{\beta\}$. Donc, pour tout $\alpha \in \lambda$ il existe un certain $\gamma \in \lambda$ tel que $\alpha < \gamma$, *i.e.* $\alpha \in \gamma$. On en conclut que $\lambda = \bigcup_{\gamma \in \lambda} \gamma$.

□

Théorème 4.4 (Induction transfinie)**.** Soit $\mathscr{P}$ une propriété sur les ordinaux. On suppose que :

- $\emptyset$ satisfait $\mathscr{P}$;
- pour tout ordinal α tel que, pour tout $\beta < \alpha$ satisfait $\mathscr{P}$, alors α satisfait $\mathscr{P}$:

$$\forall \alpha,\ (\forall \beta < \alpha,\ \mathscr{P}(\beta)) \implies \mathscr{P}(\alpha)\ ;$$

alors tous les ordinaux satisfont $\mathscr{P}$.

Preuve. Par l'absurde, soit α ne satisfaisant pas $\mathscr{P}$. Soit β le plus

petit ordinal de $\alpha \cup \{\alpha\}$ ne satisfaisant pas $\mathcal{P}$. Tous les ordinaux plus petit que β satisfont $\mathcal{P}$, d'où $\mathcal{P}(\alpha)$, ***absurde***. On en conclut que α n'existe pas. □

Remarque 4.8. En pratique on décompose :

- ▷ on montre pour $\emptyset$;
- ▷ on montre pour α successeur ;
- ▷ on montre pour α limite.

Définition 4.10. Un ordinal α est *fini* si $\alpha = \emptyset$ ou si α et sous ses éléments sont des successeurs.

Proposition 4.13. L'ensemble des ordinaux finis ω est un ordinal. C'est le plus petit ordinal limite.

Preuve. En exercice. □

Lemme 4.3. Soit $f : \alpha \to \alpha'$ une fonction strictement croissante entre deux ordinaux α et α'. Alors $f(\beta) \geq \beta$ pour tout $\beta \in \alpha$. De plus, on a $\alpha' \geq \alpha$. Aussi si f est un isomorphisme alors $\alpha = \alpha'$ et f est l'identité.

Preuve.

- ▷ Soit β_0 le plus petit élément tel que $f(\beta_0) < \beta_0$. Comme f strictement croissante, on a $f(f(\beta_0)) < f(\beta_0) < \beta_0$ absurde car β_0 est le plus petit.
- ▷ Soit $\beta \in \alpha$. On a $f(\beta) \in \alpha'$ et $\beta \leq f(\beta)$ donc $\beta \in \alpha'$, donc $\beta \in \alpha'$, d'où $\alpha \subseteq \alpha'$ et donc $\alpha \leq \alpha'$.
- ▷ Si f est un isomorphisme alors f^{-1} est strictement croissante. On applique le point précédent à f^{-1}, d'où $\alpha = \alpha'$.
- ▷ Montrons que f est l'identité. On sait que, pour tout $\beta \in \alpha$, on a $f_{|\beta}$ strictement croissante de β dans $f(\beta)$, d'où $\beta = f(\beta)$ par le point précédent. D'où f est l'identité.

□

Théorème 4.5. Tout ensemble bien ordonné est isomorphe à un ordinal. Cet ordinal ainsi que l'isomorphisme sont uniques.

Preuve. Cette preuve ressemble à une induction sans en être une. On aura le droit d'en faire quand on aura le théorème.

Si l'isomorphisme existe, il est unique grâce au lemme précédent. En effet, s'il y en a deux f et g alors $f \circ g^{-1}$ est un isomorphisme entre deux ordinaux égaux, donc c'est l'identité.

Notons $\mathscr{P}(x)$ la propriété « il existe un ordinal α_x et un isomorphisme $f_x : S_{\leq x} \to \alpha_x$ » où $S_{\leq x} := \{y \in X \mid y \leq x\}$. Pour montrer $\mathscr{P}(x)$ pour tout $x \in X$, on pose

$$Y := \{x \in X \mid \mathscr{P}(x) \text{ est vraie}\}.$$

et on montre $Y = X$.

Supposons $Y \neq X$ et soit $a = \min(X \setminus Y)$.

- ▷ Si Y a un plus grand élément b, alors il existe un isomorphisme $f_b : S_{\leq b} \to \alpha_b$ (car $\mathscr{P}(b)$). Or, $S_{\leq a} = S_{\leq b} \cup \{a\}$ (il faudrait montrer que Y est un segment initial de X). Et, on construit $f_a : S_{\leq a} \to \alpha_b \cup \{\alpha\}_b$ qui est un isomorphisme, donc $a \in Y$, ***absurde***.
- ▷ Si Y n'a pas de plus grand élément, on considère $\alpha := \bigcup_{x \in Y} \alpha_x$ un ordinal. Pour tout $x < \alpha$ il existe un isomorphisme de $S_{\leq x}$ dans α_x. Si on prend $x < y < \alpha$ alors $(f_y)_{|S_{\leq x}}$ est un isomorphisme et, par unicité, on a donc que f_y prolonge f_x. On peut définir un isomorphisme $f_{\leq \alpha}$ comme limite des f_x pour $x < \alpha$. C'est un isomorphisme de $S_{<a}$ dans $\beta := \bigcup_{x<\alpha} \alpha_x$. On peut prolonger f en $f_X : S_{\leq \alpha} \to \beta + 1$ où $\alpha \mapsto \beta$, d'où $\alpha \leq Y$, ***absurde***.

□

Lemme 4.4 (Définition récursive transfinie des fonctions)**.** Soient

- ▷ α un ordinal ;

- ▷ S une collection ;
- ▷ $\mathscr{F}$ la collection des applications définies sur les ordinaux $\beta \leq \alpha$ et prenant leur valeurs dans S ;
- ▷ F une relation fonctionnelle de domaine $\mathscr{F}$ à valeur dans S.

Alors il existe une fonction f dans $\mathscr{F}$ (et une unique définie sur α) telle que :

$$(\star) \qquad \text{pour tout } \beta < \alpha \qquad f(\beta) = F(f_{|\beta}).$$

Preuve. **Unicité.** Soient f et g satisfaisant $(\star)$. Montrons $\mathscr{P}(\beta)$: « si $\beta < \alpha$ alors $f(\beta) = g(\beta)$ » par induction transfinie.

- ▷ On a directement $\mathscr{P}(\emptyset)$ car il y a une unique fonction de $\emptyset \to \emptyset$.
- ▷ Supposons que $f(\gamma) = g(\gamma)$ pour tout $\gamma < \beta$. Alors $f_{|\beta} = g_{|\beta}$ et donc par $(\star)$ on a $f(\beta) = g(\beta)$.

Existence. Soit τ l'ensemble des ordinaux $\gamma \in \alpha$ tels qu'il existe $f_\gamma \in \mathscr{F}$ définie sur γ et vérifiant $(\star)$. Alors τ est un segment initial de α donc un ordinal. Par unicité si $\gamma < \gamma'$ alors $f_{\gamma'}$ prolonge f_γ. On définit f_τ par $f_\tau(\gamma) := F(f_\gamma)$ si $\gamma < \tau$.

- ▷ Si $\tau \in \alpha$ alors f_τ prolonge tous les f_γ et donc $\tau \in \tau$, ***impossible***.
- ▷ D'où $\tau = \alpha$.

□

Exercice 4.1. Généraliser la preuve ci-dessus en replaçant α par la classe de tous les ordinaux $\mathfrak{O}$ (et remplacer $\mathscr{F}$ par autre chose).

Proposition 4.14.
1. La classe $\mathfrak{O}$ n'est pas un ensemble.
2. Il n'existe pas de relation fonctionnelle bijective entre $\mathfrak{O}$ et un ensemble a.

Preuve.
1. En effet, supposons $\mathfrak{O}$ un ensemble. On a que $\mathfrak{O}$ est transitif et $\in$ y définit un ordre total, donc $\mathfrak{O}$ est un ordinal.

D'où $\mathfrak{O} \in \mathfrak{O}$ ce qui est impossible pour un ordinal.

2. Sinon $\mathfrak{O}$ serait un ensemble.

□

4.3 Axiome de choix et variantes équivalentes.

Les axiomes du choix sont exprimable au premier ordre !

AC 1. Le produit d'une famille d'ensembles non vides est non vide.

AC 2. Pour tout ensemble a non vide, il existe une fonction de $\mathcal{P}(a)$ dans a tel que si $x \subseteq a$ est non vide alors $f(x) \in x$. (C'est une fonction de choix.)

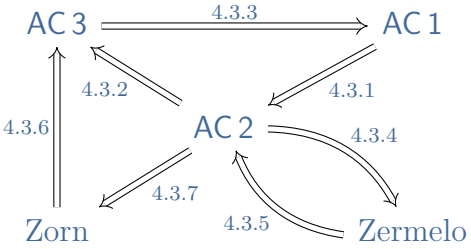
AC 3. Si a est un ensemble dont tous les éléments sont non vides et deux à deux disjoints alors il existe un ensemble c tel que, pour tout $x \in a$, $x \cap c$ a exactement un élément.

(Lemme de) Zorn. Tout ensemble non vide partiellement ordonné et inductif admet un élément maximal.

On rappelle qu'un ensemble partiellement ordonné X est inductif si $X \neq \emptyset$ et si tout sous-ensemble $Y \subseteq X$ totalement ordonné admet un majorant dans X.

(Lemme de) Zermelo. Tout ensemble non vide peut être mini d'un bon ordre (*i.e.* un ordre total où toute partie non vide a un plus petit élément).

En supposant les axiomes ZF 1, . . . , ZF 5, on va montrer les implications suivantes :



4.3.1 AC 1 implique AC 2.

On rappelle que l'ensemble $\prod_{i\in I} a_i$ est l'ensemble de fonctions f de la forme $f : I \to \bigcup_{i\in I} a_i$ tel que $f(i) \in a_i$ pour tout i.

Soit a non vide. On considère $\prod_{\emptyset\neq x\subseteq a} x$ qui est non vide par AC 1. Soit f un de ces éléments. On a, pour tout $\emptyset \neq x \subseteq a$, que $f(x) \in x$ donc f est une fonction de choix.

4.3.2 AC 2 implique AC 3.

Soit a un ensemble dont les éléments sont non vides et deux à deux disjoints. On considère $b = \bigcup_{x\in a} x$ qui est un ensemble. Par AC 2, on a une fonction de choix f sur $\wp(b)$. On prend $c = \{f(x) \mid x \in a\}$. Comme les x sont disjoints, on obtient la propriété recherchée.

4.3.3 AC 3 implique AC 1.

Soit $X = \prod_{i\in I} a_i$ un produit d'ensemble non vides. On considère $A := \{\, \{i\} \times a_i \mid i \in I \,\}$. Par AC 3, il existe c tel que, pour tout $x \in A$, $x \cap c$ a exactement un élément. D'où, c peut s'écrire

$$c = \{(i, d_i) \mid i \in I \text{ et } d_i \in a_i\}.$$

On a donc $c \in \prod_{i\in I} a_i$ (c'est le graphe d'une fonction) et donc $\prod_{i\in I} a_i \neq \emptyset$.

4.3.4 AC 2 implique Zermelo.

Soit a un ensemble non vide.

> **Remarque 4.9** (Idée). L'idée est qu'on utilise $f : \mathcal{P}(a) \to a$ une fonction de choix pour définir l'ordre. On peut imaginer définir $x \leq y$ ssi $f(\{x, y\}) = x$ (on traite donc f comme la fonction minimum), mais on n'a pas la transitivité. Il faut être plus futé.
>
> On va construire en partant du plus petit une bijection entre a et un ordinal.

- $h(0) := f(a)$
- $h(1) := f(a \setminus \{h(0)\})$
- $h(2) := f(a \setminus \{h(0), h(1)\})$
- $\vdots$
- $h(\omega) = f(a \setminus \{h(0), h(1), \ldots\})$
- $\vdots$

On s'arrête quand $a \setminus \{h(0), h(1), \ldots\}$ est vide.

Soit $\theta \notin a$ (pour « détecter » quand l'ensemble $a \setminus \{h(0), \ldots\}$ est vide). Il existe car a est un ensemble donc pas l'univers tout entier.

On définit

$$F(\alpha) := \begin{cases} f(a \setminus \{F(\beta) \mid \beta < \alpha\}) & \text{si } a \setminus \{F(\beta) \mid \beta < \alpha\} \neq \emptyset \\ \theta & \text{sinon} \end{cases}.$$

D'après le dernier lemme de la section précédente, on peut construire l'application F ainsi et elle est unique.

S'il n'existe pas d'ordinal α tel que $F(\alpha) = \theta$ alors F est une injection de $\mathbb{O}$ dans a. ***Absurde***. Il existe donc α tel que $F(\alpha) = \theta$.

Le sous-ensemble $\{\beta \in \alpha \mid F(\beta) = \theta\}$ a un plus petit élément β. Montrons que $F_{|\beta}$ est une bijection de β dans α.

- D'une part, on sait que c'est une injection.
- D'autre part, $F(\beta) = \theta$ implique $\{F(\gamma) \mid \gamma < \beta\} = a$ donc $F_{|\beta}$ est une surjection.

On définit le bon ordre $x \prec y$ ssi $F^{-1}(x) < F^{-1}(y)$.

4.3.5 Zermelo implique AC 2.

Soit a non vide. Il existe un bon-ordre $<$ sur a. Soit $\emptyset \neq x \subseteq a$. On définit $f(x) = \min x$, c'est bien une fonction de choix.

4.3.6 Zorn implique AC 3.

Soit a un ensemble dont les éléments sont disjoints et non vides. On pose :

$$b := \bigcup_{x \in a} x \quad \text{et} \quad X := \{c \subseteq b \mid \forall x \in a,\ |c \cap x| \leq 1\}.$$

Montrons que l'ensemble $(X, \subsetneq)$ est inductif.

Si $y \subseteq X$ est totalement ordonné. Montrons que Y a un majorant dans X. On pose $z = \bigcup_{y \in Y} y$ qui majore Y. On a bien $z \in X$ (on ne duplique pas les éléments). On en conclut que X est inductif. Soit d un élément maximal de X (il existe par Zorn).

- ▷ S'il existe $x \in a$ tel que $x \cap d = \emptyset$ alors prenons $u \in x$ et posons $d_1 := d \cup \{u\}$. D'où $d_1 \in X$ et $d \subsetneq d_1$ donc d non maximal, ***absurde***.
- ▷ Pour tout $x \in a$, on a $|d \cap x| = 1$, d'où d est l'ensemble recherché (appelé c dans AC 3).

4.3.7 AC 2 implique Zorn.

Soit a un ensemble inductif.

> **Remarque 4.10** (Idée). On construit une chaîne dans a (*i.e.* un ensemble totalement ordonné) de taille maximale (c'est ici qu'on utilise la fonction de choix de AC 2). Elle a un majorant car a est inductif. Ce majorant va être l'élément maximal.

Soit $f : \wp(a) \to a$ une fonction de choix donnée par AC 2. Si $x \subseteq a$ on appelle majorant strict de x un $y \in a$ tel que $z < y$ pour tout $y \in x$.

> **Remarque 4.11** (Idée – suite).
> - ▷ On part de $\emptyset$: tout élément de a a un majorant strict de $\emptyset$ en choisissant $a_1 = f(a)$.
> - ▷ Soit X_1 l'ensemble des majorants de $\{a_1\}$. On pose $a_2 := f(X_1)$.

▷ Soit X_2 l'ensemble des majorants de $\{a_1, a_2\}$. On pose $a_3 := f(X_2)$.

Formellement, soit $C := \{x \subseteq a \mid x \text{ a un majorant strict dans } a\}$. On a $\emptyset \in C$. On définit

$$\begin{aligned} m : C &\longrightarrow a \\ x &\longmapsto f(\{y \in a \mid y \text{ est un majorant strict de } x \text{ dans } a\}). \end{aligned}$$

On définit par induction la chaîne maximale (dernier lemme de la section précédente). Soit $\theta \notin a$. On définit :

$$F(\alpha) := \begin{cases} m(\{F(\beta) \mid \beta < \alpha\}) & \text{si } \{F(\beta) \mid \beta < \alpha\} \in C \\ \theta & \text{sinon} \end{cases}.$$

La fonction F n'est pas une injection de $\mathbb{O}$ dans a donc il existe un ordinal α tel que $F(\alpha) = \theta$. Comme $\alpha + 1$ est un ordinal, l'ensemble $\{\beta \in \alpha + 1 \mid F(\beta) = \theta\}$ a un plus petit élément α_0. D'où l'ensemble $\{F(\beta) \mid \beta < \alpha_0\}$ n'a pas de majorant strict mais a un majorant M car a inductif. Et, a n'a pas d'élément plus grand que a. Ainsi M est maximal dans a.

4.3.8 Indépendance de ZF et de l'axiome du choix.

On a les deux théorèmes suivants (que l'on admet).

Théorème 4.6 (Gödel, 1938)**.** S'il est cohérent, ZF ne réfute pas l'axiome du choix.

Théorème 4.7 (Cohen, 1963)**.** S'il est cohérent, ZF ne montre pas l'axiome du choix.

Ainsi l'axiome du choix est indépendant de ZF. Cependant, il existe des versions plus faibles : axiome du choix dépendant (ACD), axiome du choix dénombrable (AC_ω).

5 Exemple de théories décidables.

Dans ce chapitre, on traite de l'élimination des quantificateurs dans les corps réels clos (et les corps algébriquement clos).

5.1 De quoi on parle ?

5.1.1 L'élimination des quantificateurs.

Définition 5.1. Une théorie T (de la logique du 1er ordre) admet *l'élimination des quantificateurs* si pour toute formule $\varphi(\bar{y})$, il existe une formule sans quantificateurs $\psi(\bar{y})$ telle que $T \vdash \forall \bar{y}\, (\varphi(\bar{y}) \leftrightarrow \psi(\bar{y}))$.

Lemme 5.1. Une théorie T élimine les quantificateurs si pour toute formule $\varphi(x, \bar{y})$ sans quantificateurs, il existe une formule $\psi(\bar{y})$ sans quantificateurs et $T \vdash \forall \bar{y}\, (\exists x\, \varphi(x, \bar{y}) \leftrightarrow \psi(\bar{y}))$.

Preuve. Idée de la preuve :

- ▷ « $\Longrightarrow$ ». C'est un cas particulier.
- ▷ « $\Longleftarrow$ ». Toute formule est équivalente à une formule prénexe, c'est-à-dire une formule où les quantificateurs sont à la racine :

$$\mathsf{Q}_1 x_1\, \mathsf{Q}_2 x_2\, \ldots\, \mathsf{Q}_n x_n\, \varphi(x_1, \ldots, x_n),$$

où $\varphi(\cdots)$ est sans quantificateurs. Pour démontrer que

toute formule est équivalente à une formule prénexe, on procède par induction sur la formule, et on doit potentiellement procéder à des cas d'α-renommage au besoin.

Pour toute formule sous forme prénexe, le lemme est vrai.

□

Exemple 5.1. La théorie des booléens est la théorie

$$T_{\text{bool}} := \{\forall x\, x = 0 \vee x = 1, 0 \neq 1\},$$

sur le langage $\mathscr{L} = \{0, 1\}$. Cette théorie admet l'élimination des quantificateurs. En effet, par exemple, une formule

$$F := \exists x_1 \cdots \exists x_n\, (x_1 = 1 \vee x_2 = 0 \vee x_4 = 1) \wedge \cdots),$$

est équivalente à $\top$ ou $\bot$.

Exemple 5.2. Sur le langage $\mathscr{L}_{\text{co}} = \{0, 1, +, \times, \leq\}$, la théorie $T := \mathbf{Th}(\mathbb{R})$ admet l'élimination des quantificateurs. En effet, par exemple, la formule

$$\varphi(a, b, c) := \exists x\, (a \times x \times x + b \times x + c = 0)$$

est équivalente à la formule sans quantificateurs

$$\psi(a, b, c) := (a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)\ .$$

5.1.2 Les corps réels clos et le théorème de Tarski.

Définition 5.2. Un *corps réel clos* est un corps commutatif ordonné dans lequel on a le théorème des valeurs intermédiaires pour les polynômes à 1 variable.

La théorie T_{CRC} est la théorie du 1er ordre et ses axiomes sont :

- ▷ axiomes de corps commutatifs ;

- ▷ axiomes de relation d'ordre total ;
- ▷ $1 > 0$;
- ▷ axiomes de corps ordonné (compatibilité de $+$ et $\times$ avec $\leq$) :

$$\forall x\, \forall y\, \forall z \begin{pmatrix} x \leq y \to x + z \leq y + z \\ \wedge \\ (z \geq 0 \wedge x \leq y) \to x \times y \leq y \times z \\ \wedge \\ (z \leq 0 \wedge x \leq y) \to x \times y \geq y \times z \end{pmatrix} ;$$

- ▷ schéma d'axiomes pour le théorème des valeurs intermédiaires : pour $n \in \mathbb{N}$,

$$\begin{gathered} \forall a_0 \dots a_n\, \forall x\, \forall y \\ a_0 + a_1 x + \dots + a_n x^n \geq 0 \wedge a_0 + a_1 y + \dots + a_n y^n \leq 0 \\ \downarrow \\ \exists z\, (x \leq z \leq y \vee y \leq z \leq x) \wedge a_0 + a_1 z + \dots + a_n z^n = 0. \end{gathered}$$

Exemple 5.3. Exemples de corps réels clos : $\mathbb{R}$ les réels, $\bar{\mathbb{Q}} \cap \mathbb{R}$ les nombres réels algébriquement clos.

Qu'en est-il de $\mathbb{C}$? Si on a $i \geq 0$ et on a $1 \leq 2$ donc $i \leq 2i$ et par multiplication par i on a $-1 \leq -2$, absurde ! Le même procédé fonctionne si l'on suppose $i \leq 0$. Il n'y a pas de manière d'ordonner $\mathbb{C}$ de telle sorte à ce qu'il soit un corps réel clos.

Proposition 5.1.
1. Un corps réel clos est de caractéristique 0.
2. Dans un corps réel clos, on a le théorème de Rolle (entre deux racines d'un polynôme, la dérivée s'annule).

Preuve. Idée de la preuve :

1. On a $1 > 0$ donc $2 > 1 > 0$ donc $3 > 0$, *etc.* On montre, par récurrence, pour tout n que $n > 0$ et donc $n \neq 0$.

2. On montre que si la dérivée est de signe constant alors le polynôme est monotone d'où le théorème de Rolle.

□

À quoi ressemblent les formules dans $\mathscr{L}_{\text{co}}$?

- Les termes représentent des polynômes à plusieurs variables et à coefficients dans $\mathbb{N}$.
- Les formules atomiques représentent des équations et inéquations entre polynômes :

$$P(X) \leq Q(X) \text{ ou } P(X) = Q(X),$$

et même $P(X) \geq 0$ ou $P(X) = 0$ avec P à coefficient dans $\mathbb{Z}$.

- Les formules sans quantificateur sont équivalentes à des formules de la forme

$$\bigvee_i \bigwedge_j (P_{i,j} \ \Delta_{i,j} \ 0),$$

où $\Delta_{i,j} \in \{<, >, =\}$.

- Les formules sont équivalentes à des formules sous forme prénexe de la forme

$$\mathsf{Q}_1 x_1 \dots \mathsf{Q}_n x_n \bigvee_i \bigwedge_j (P_{i,j} \ \Delta_{i,j} \ 0),$$

avec $\mathsf{Q}_i \in \{\forall, \exists\}$.

Théorème 5.1 (Tarski)**.** La théorie des corps réels clos admet l'élimination des quantificateurs. Elle est axiome-complète et décidable.

Preuve. En supposant que T_{CRC} admet l'élimination des quantificateurs, alors on a une théorie axiome-récursive ~~qui contient les entiers donc indécidable par Gödel~~. Non ! On ne contient pas $\mathscr{P}_0$! En effet, l'axiome A1 n'est pas vérifié : on n'a pas $\textcircled{\textsf{S}}x \neq 0$!

Soit F une formule close de $\mathscr{L}_{\text{co}}$. Montrer que $T_{\text{CRC}} \vdash F$ ou $T_{\text{CRC}} \vdash \neg F$. Il existe une formule sans quantificateurs G et $T_{\text{CRC}} \vdash F \leftrightarrow G$ et G n'a pas de variable. Ainsi G est équivalent à une conjonction

de disjonction de formules équivalentes à

$$\textcircled{n} > \textcircled{m} \text{ ou } \textcircled{n} = \textcircled{m}.$$

La valeur de vérité ne dépend pas du modèle, d'où $T_{\text{CRC}} \vdash G$ ou $T_{\text{CRC}} \vdash \neg G$, donc $T_{\text{CRC}} \vdash F$ ou $T_{\text{CRC}} \vdash \neg F$, et donc T_{CRC} est axiome-complète.

Comme T_{CRC} est axiome-récursive, pour décider si $T_{\text{CRC}} \vdash F$, il suffit d'énumérer toutes les preuves jusqu'à en trouver une de F ou de $\neg F$. □

5.2 La méthode d'élimination.

5.2.1 Rappels et exemples.

Il suffit de montrer le lemme ci-dessous.

Lemme 5.2. Si pour toute formule F de la forme $\exists x \bigvee_i \bigwedge_k P_{i,j} \ \Delta_{i,j} 0$ avec $P_{i,j}$ des polynômes et $\Delta_{i,j} \in \{<, >, =\}$, il existe une formule sans quantificateurs G telle que

$$T_{\text{CRC}} \vdash \forall \bar{y} \, G(\bar{y}) \leftrightarrow F(\bar{y})$$

alors T_{CRC} admet l'élimination des quantificateurs.

Idée de la méthode :

- ▷ On part d'un polynôme, par exemple $ax^2 + bx + 1$.
- ▷ On calcule des « quantités importantes » (des polynômes de degré 0 en x), ici a et $a^2 - 4a$.
- ▷ On trouve des « conditions de signe » qui permettent de satisfaire la formule, ici $a \neq 0 \wedge a^2 - 4a \geq 0$.

Définition 5.3. Avec $P \in \mathbb{Z}[\bar{Y}][X] = \mathbb{Z}[Y_1, \ldots, Y_n][X]$, les poly-

nômes s'écrivent comme

$$P(X) = a_n X^n + \cdots + a_0 \text{ où } n \geq 1,\ a_n \neq 0 \text{ et } a_i \in \mathbb{Z}[\bar{Y}],$$

et on définit les opérations :

- ▷ *dérivée* $\mathrm{D}(P) := \frac{\partial P(X)}{\partial X}$;
- ▷ *extraction du coefficient dominant* $\mathrm{E}(P) := a_n$;
- ▷ *omission du terme dominant* $\mathrm{O}(P) := a_{n-1}X^{n-1} + \cdots + a_0$;
- ▷ *reste modifié* $\mathrm{MR}(P, Q)$:
  si $P = a_n X^n + \cdots + a_0$ et $Q = b_n X^n + \cdots + b_0$ où

$$n = \deg P \geq m = \deg Q \geq 1$$

et $P \neq Q$ alors $\mathrm{MR}(P, Q)$ est l'unique polynôme de $\mathbb{Z}[\bar{Y}][X]$ de degré $r < m$ tel qu'il existe $L \in \mathbb{Z}[\bar{Y}][X]$ et

$$(b_n)^{nm+1} \times P = Q \times L + R.$$

Exemple 5.4. Si $P = X^4$ et $Q = 3X^2 + X + 1$ alors

$$\begin{array}{rl|l}
X^4 & & 3X^2 + X + 1 \\
\cline{3-3}
-X^4 - \frac{1}{3}X^3 - \frac{1}{3}X^2 & & \frac{1}{3}X^2 - \frac{1}{9}X - \frac{2}{27} \\
\cline{1-1}
-\frac{1}{3}X^3 - \frac{1}{3}X^2 & & \\
\frac{1}{3}X^3 + \frac{1}{9}X^2 + \frac{1}{9}X & & \\
\cline{1-1}
-\frac{2}{9}X^2 + \frac{1}{9}X & & \\
\frac{2}{9}X^2 + \frac{2}{27}X + \frac{2}{27} & & \\
\cline{1-1}
\frac{5}{27}X + \frac{2}{27} & &
\end{array}$$

et le reste modifié est $\mathrm{MR}(P, Q) = 3^3(\frac{5}{27}X + \frac{2}{27}) = 5X + 2$.

5.2.2 Énoncé comme lemme clé.

Lemme 5.3 (Informel). À partir d'un ensemble de polynômes S, on obtient en temps fini un ensemble fini de polynômes $\mathrm{BC}S$ de degré 0 en appliquant les quatre opérations D, E, O et MR. [1]

Exemple 5.5. À partir de $S = \{\overbrace{aX^2 + bX + 1}^{p_0}\}$, on a

- ▷ on commence par ajouter p_0 ;
- ▷ d'abord les dérivées, omissions et extractions : on ajoute les polynômes $2aX + a$, a et $aX + 1$, $2a$, 1 et 0 ;
- ▷ ensuite on calcule le reste modifié

$$\mathrm{MR}(aX^2 + aX + 1, 2aX + a) = 4a^2 - a^3,$$

et on l'ajoute ;

- ▷ on calcule le reste modifié

$$\mathrm{MR}(aX^2 + aX + 1, aX + 1) = a,$$

et on l'ajoute (il y est déjà) ;

- ▷ on calcule le reste modifié

$$\mathrm{MR}(3aX + a, aX + 1) = a^2 - 2a,$$

et on l'ajoute ;

- ▷ on ne conserve que les polynômes de degré 0.

Dans l'exemple on obtient (après suppression des termes inutiles pour les comparaisons à 0),

$$\mathrm{BC}S = \{a, 4a^2 - a^3, a^2 - 2a\}.$$

On a, en théorie, 27 conditions de signe possibles ($3^{|\mathrm{BC}S|}$) :

- ▷ $a > 0$ et $4a^2 - a^3 > 0$ et $A^2 - 2a < 0$,
- ▷ $a > 0$ et $4a^2 - a^3 < 0$ et $a^2 - 2a < 0$,
- ▷ $a = 0$ et $a^2 - a^3 > 0$ et $a^2 - 2a > 0$,
- ▷ *etc* pour les 24 autre cas.

1. I ♡ le lemme de König.

On traite deux cas : $a > 0$ et $4a^2 - a^3$ et $a^2 - 2a$.

X	$-\infty$		γ_2		γ_1		$+\infty$
a		$>$	$>$	$>$	$>$	$>$	
$4a^2 - a^3$		$>$	$>$	$>$	$>$	$>$	
$a^2 - 2a$		$<$	$<$	$<$	$<$	$<$	
$aX + 1$	$-\infty$	$<$	$<$	$<$	0	$>$	$+\infty$
$2aX + a$	$-\infty$	$<$	0	$>$	$>$	$>$	$+\infty$
$aX^2 + aX + 1$	$+\infty$	$>$	$>$	$>$	$>$	$>$	$+\infty$

5.3 Corps algébriquement clos.

Définition 5.4. Un *corps algébriquement clos* est un corps commutatif dans lequel tout polynôme a une racine.

Exemple 5.6. Le corps $\mathbb{C}$ est algébriquement clos. En effet, il s'agit du *théorème fondamental de l'algèbre*, *i.e.* un polynôme de degré n a n racines comptées avec multiplicité.

Tout polynôme est ainsi un produit de polynômes de degré 1.

Définition 5.5. La *théorie des corps algébriquement clos* est la théorie formée des :

- ▷ axiomes de corps ;
- ▷ du schémas d'axiomes, noté Clos_n, pour tout $n \in \mathbb{N}$,

$$\forall a_0 \dots \forall a_n \, (a_1 \neq 0 \vee \dots \vee a_n \neq 0 \to \exists b \, a_0 + a_1 b + \dots + a_n b^n = 0).$$

Définition 5.6. Un corps est de *caractéristique* $p \in \mathbb{N}^\star$ s'il est modèle de l'ensemble Car_p définie par

$$\{(1 \neq 0) \wedge (1+1 \neq 0) \wedge \dots \wedge (\underbrace{1 + \dots + 1}_{p-1} \neq 0) \wedge (\underbrace{1 + \dots + 1}_{p} = 0)\}.$$

Un corps est de *caractéristique* 0 s'il est modèle de l'ensemble Car_0 définie par

$$\{1 \neq 0, 1+1 \neq 0, 1+1+1 \neq 0, \ldots\}.$$

La *théorie des corps algébriquement clos de caractéristique* $p \in \mathbb{N}$ est :

$$\mathrm{ACF}_p := \{\text{Axiomes des corps}\} \cup \{\, \mathrm{Clos}_n \mid n \in \mathbb{N} \,\} \cup \mathrm{Car}_p.$$

Exemple 5.7. Les corps $\mathbb{C}$ et $\bar{\mathbb{Q}}$ sont modèles de cette théorie. ***Attention***, $\mathbb{F}_p$ ne l'est pas (et $\mathbb{F}_{p^n}$ non plus), il faut prendre sa clôture algébrique $\bar{\mathbb{F}}_p$ et $\bar{\mathbb{F}}_{p^n}$.

Remarque 5.1.
- ▷ Tous les corps finis sont de la forme $\mathbb{F}_{p^n}$ avec p premier.
- ▷ Un élément a est dit *algébrique* sur le corps $\Bbbk$ si c'est la racine d'un polynôme à coefficient dans $\Bbbk$. On dit que a est *algébrique de degré* q si le polynôme minimal dont a est racine est de degré q.

Exemple 5.8.
- ▷ Le nombre $\sqrt{3}$ est algébrique sur $\mathbb{Q}$ de degré 2.
- ▷ Le nombre i est algébrique sur $\mathbb{Q}$ de degré 2.
- ▷ Le nombre $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ de degré 3.
- ▷ Le nombre π n'est pas algébrique sur $\mathbb{Q}$.

Remarque 5.2. Si a est algébrique de degré q sur $\Bbbk$ alors $\Bbbk(a)$ est le corps engendré par $\Bbbk$ et a. C'est l'ensemble des polynômes de degré $\leq q-1$ sur $\Bbbk$, et on définie le produit modulo un polynôme minimal de a.

Exemple 5.9. On a $\mathbb{R}(i) = \mathbb{R}[X]/(X^2 - 1) \cong \mathbb{C}$. Le produit est :

$$\begin{aligned}(aX + b)(cX + d) &= acX^2 + X(ad + bc) + bd \\ &= (ad + bc)X + bd - ac.\end{aligned}$$

En particulier, si a est de degré q sur $\mathbb{F}_{p^n}$ alors $\mathbb{F}_{p^n}(a) = \mathbb{F}_{p^{qn}}$.

Théorème 5.2 (Tarski–bis)**.** Pour tout p, la théorie des corps algébriquement clos de caractéristique p admet l'élimination des quantificateurs. Elle est complète et décidable.

Preuve. Comme la dernière fois, il suffit de montrer pour toute formule de la forme

$$\exists x\, (P_1(x) = 0 \wedge \cdots \wedge P_n(x) = 0 \wedge Q(x) \neq 0),$$

il existe une formule sans quantificateurs équivalente dans ACF_p. On continue la preuve sur un exemple. □

Exemple 5.10. On élimine les quantificateurs sur

$$\exists x\, (ax^2 + ax + 1 = 0 \wedge ax + 1 \neq 0),$$

avec la caractéristique $p = 0$. On a les polynômes suivants :

- $p_0(X) = aX^2 + aX + 1$
- $p_1(X) = \mathrm{D}p_0(X) = 2aX + a$
- $p_2(X) = \mathrm{E}p_0 = a$
- $p_3(X) = aX + 1$
- $p_4(X) = \mathrm{MR}(p_0, p_1) = 4a^2 - a^3$
- $p_2(X) = \mathrm{MR}(p_0, p_3) = a$
- $p_5(X) = \mathrm{MR}(p_1, p_3) = a^2 - 2a.$

Les « conditions de signe » sont $= 0$ ou $\neq 0$ (notés 0 et $\neq$).

On se place dans un cas exemple :

	autres	γ_1	γ_2	γ_3	γ_4
a	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$
$4a^2 + a^3$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$
$a^2 - 2a$	$\neq$	$\neq$	$\neq$	$\neq$	$\neq$
$aX + 1$	$\neq$	0	$\neq$	$\neq$	$\neq$
$2aX + a$	$\neq$	$\neq$	0	$\neq$	$\neq$
$aX^2 + aX + 1$	$\neq$	$\neq$	$\neq$	0	0

.

Ainsi, pour $a \neq 0$, $4a^2 - a^3 \neq 0$, $a^2 - 2a \neq 0$ alors on a

$$\exists x\ (ax^2 + ax + 1 = 0 \wedge ax + 1 \neq 0).$$

Avec les autres cas, on peut en déduire que

$$\exists x\ (ax^2 + ax + 1 = 0 \wedge ax + 1 \neq 0)$$

est équivalente à

$$\bigvee_{\substack{\text{tableau de la condition de signe} \\ \text{a une colonne qui convient}}} \text{(conditions de signe)}.$$

Exercice 5.1. En déduire que ACF_p est complète et décidable.

Remarque 5.3. En 2010, une preuve ~~Coq~~ Rocq de l'élimination des quantificateurs de cette théorie a été publiée par Cyril Cohen et Assia Mahboubi.

5.3.1 Applications aux mathématiques.

Théorème d'Ax–Grothendieck.

Théorème 5.3 (Ax–Grothendieck)**.** Si P est un polynôme de $\mathbb{C}^n$ dans $\mathbb{C}^n$ injectif alors il est bijectif (et son inverse est un polynôme !).

On va prouver ce théorème en trois lemmes.

Lemme 5.4. Si φ est une formule qui admet comme modèle un corps algébriquement clos de caractéristique arbitrairement grande, alors φ admet comme modèle un corps algébriquement clos de caractéristique 0.

Preuve. On utilise le théorème de compacité de la logique du 1er ordre. Soit $T := \mathrm{ACF}_0 \cup \{\varphi\}$. Montrons que T a un modèle. Pour cela, on montre que T est finiment satisfiable. Soit $T' \subseteq_{\text{fini}} T$. Soit n le plus grand entier tel que

$$(\underbrace{1+1+\cdots+1}_{n} \neq 0) \in T'.$$

Soit $p > n$ un nombre premier tel que φ admet comme modèle un corps algébriquement clos $\Bbbk$ de caractéristique p (qui existe par hypothèse). D'où $\Bbbk \models \varphi$, et

$$\Bbbk \models \{\text{Axiomes des corps}\} \cup \{\, \mathrm{Clos}_n \mid n \in \mathbb{N} \,\}.$$

D'où, $\Bbbk \models \mathrm{ACF}_p$, et donc $\Bbbk \models T'$. Ainsi T finiment satisfiable donc T satisfiable. On en déduit que φ admet un modèle de caractéristique 0. □

Lemme 5.5. Soit $\Bbbk$ un corps fini et soient $n \in \mathbb{N}^\star$ et $P : \Bbbk^n \to \Bbbk^n$ un polynôme injectif. Alors P est bijectif.

Preuve. Comme $\Bbbk^n$ est fini alors P est bijectif. □

Lemme 5.6. Soit $\Bbbk$ un corps fini et soient $n \in \mathbb{N}^\star$ et $\bar{\Bbbk}$ la clôture

algébrique de $\Bbbk$. Soit $P : \bar{\Bbbk}^n \to \bar{\Bbbk}^n$ un polynôme injectif. Alors P est bijectif.

Preuve. On suppose P non surjectif, il existe donc $\bar{b} = (b_1, \dots, b_n) \in \bar{\Bbbk}^n \setminus P(\bar{\Bbbk}^n)$ des nombres algébriques dans $\Bbbk$. Ils sont raciles de polynômes minimaux à coefficients dans $\Bbbk$. Soient $\bar{a} = (a_1, \dots, a_m)$ les coefficients de ces polynômes, ce sont des éléments de $\bar{\Bbbk}$. Soient $\bar{c}$ les coefficients de P.

Soit $\Bbbk' := \Bbbk(\bar{a}, \bar{b}, \bar{c})$, c'est un corps fini. On a $P : \Bbbk'^n \to \Bbbk'^n$ injectif pas surjectif, qui est impossible d'après le lemme précédent. □

On peut donc montrer le théorème d'Ax–Grothendieck.

Pour un degré d fini et un entier n fixé, on va construire la formule $\phi_{n,d}$ qui exprime qu'un polynôme de degré $\leq d$ de $\Bbbk^n$ dans $\Bbbk^n$ qui est injectif et surjectif. Soit $M(n,d)$ l'ensemble fini des monômes unitaires de degré $\leq d$ avec n variables $x_1, \dots, x_n$:

$$M(n,d) := \{1, x_1, x_2, x_1x_2, \dots, x_1^d, x_1^{d-1}x_2, \dots\}.$$

On pose la formule, notée $\varphi_{n,d}$.

$$\forall (a_{m,i})_{m \in M(n,d), i \in [\![1,n]\!]}$$

$$\left(\forall x_1 \dots x_n \forall y_1 \dots y_n \bigwedge_{i=1}^{n} \sum_{m \in M(n,d)} a_{m,i} m(x_i) = \sum_{m \in M(n,d)} a_{m,i} m(y_i) \to \bigwedge_{i=1}^{n} x_i = y_i \right)$$

$$\downarrow$$

$$\forall y_1 \dots y_n \exists x_1 \dots x_n \bigwedge_{i=1}^{n} y_i = \sum_{m \in M(n,d)} a_{m,i} m(x_i).$$

Par le troisième lemme, pour tout corps fini $\Bbbk$, on a $\bar{\Bbbk} \models \varphi_{n,d}$ donc pour tout p premier, on a $\bar{\mathbb{F}}_p \models \varphi_{n,d}$. Par le premier lemme, il existe donc $\Bbbk$ de caractéristique 0 telle que $\Bbbk \models \varphi_{n,d}$. Par la complétude de la théorie des corps algébriquement clos, on a que $\mathbb{C} \models \varphi_{n,d}$.

Conjecture de la Jacobienne (1939).

C'est une question encore ouverte. On reçoit plein de preuves fausses.

Définition 5.7. Soit $P : \mathbb{C}^n \to \mathbb{C}^n$ un polynôme. Son *jacobien* est le déterminant de la matrice jacobienne

$$\operatorname{Jac} P = \left| \left(\frac{\partial P_i}{\partial x_j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right|.$$

C'est un polynôme.

Proposition 5.2. Si P est injectif sur $\mathbb{C}^n$ alors P est localement injectif. Et donc, pour tout x (théorème des fonctions implicites), $\operatorname{Jac}(P)$ n'est jamais nul, d'où $\operatorname{Jac} P$ est un polynôme constant non nul.

Remarque 5.4 (Conjecture (problème 16 de la liste de Steve Smale))**.** En caractéristique 0, on a $\operatorname{Jac} P$ non nul implique P injectif.

Remarque 5.5. En caractéristique p, c'est faux : $P(x) := x - x^p$ est non-inversible et $P'(x) = 1 - px = 1$.

Exemple 5.11. ▷ Avec $n = 1$ et $d = 1$, on considère

$$\begin{aligned} P : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\longmapsto P(x) := ax + b. \end{aligned}$$

On a $\operatorname{Jac} P = a$ et, $a \neq 0$ implique P injectif.

- Avec $n = 1$ et $d = 2$, on considère

$$\begin{aligned} P : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\longmapsto P(x) := ax^2 + bx + c. \end{aligned}$$

  On a, si $\operatorname{Jac} P = 2ax + b$ non nul, alors $a = 0$ et $b \neq 0$. C'est le cas précédent !
- Avec $n = 2$ et $d = 1$, on considère

$$\begin{aligned} P : \mathbb{C}^2 &\longrightarrow \mathbb{C}^2 \\ x &\longmapsto P(x, y) := (ax + by + c, dx + ey + f). \end{aligned}$$

  On a $\operatorname{Jac} P = \begin{vmatrix} a & b \\ d & e \end{vmatrix} = ae - bd$. On a $\operatorname{Jac} P$ non nul implique $ae - bd \neq 0$ ce qui implique que le système

$$\begin{cases} ax + bj + c = 0 \\ dx + ej + f = 0 \end{cases}$$

  est inversible, donc la conjecture est vrai.

On a montré quelques résultats partiels :

- pour $d \leq 2$ en 1980 ;
- pour $d \leq 3$ dans le cas général.