Logique

Silvain Rideau-Kikuchi*

1er novembre 2024

1 Logique propositionnelle

1.1 Algèbres de Boole et dualité de Stone

Définition 1.1. Un ensemble ordonné $(A, \leqslant)$ est appelé une algèbre de Boole si :

- Tout sous-ensemble fini de A a une borne supérieure[1] et une borne inférieure[2]. En particulier,
  - A a un plus petit élément $\bot = \sup(\varnothing)$;
  - A a un plus grand élément $\top = \inf(\varnothing)$;
  - tous $a, b \in A$ ont une borne supérieure $a \vee b$;
  - tous $a, b \in A$ ont une borne inférieure $a \wedge b$.
- Tout $a \in A$ admet un complémentaire $\neg a \in A$, tel que :

$$a \vee \neg a = \top \text{ et } a \wedge \neg a = \bot.$$

- $\wedge$ distribue sur $\vee$, et réciproquement.

Le complémentaire est unique. En effet, si b et b' sont deux complémentaires de a, on a :

$$b = b \wedge \top = b \wedge (a \vee b') = \bot \vee (b \wedge b') = b \wedge b' = b'.$$

Exemple 1.2.

- $\{\bot, \top\}$ avec $\bot \leqslant \top$ est une algèbre de Boole.
- Pour tout ensemble X, $(\mathcal{P}(X), \subseteq)$ est une algèbre de Boole.
- Si $(R, +, \cdot)$ est un anneau commutatif unitaire tel que, pour tout $x \in R$, $x^2 = x$, alors la relation $a \leqslant b$ sur R définie par $ab = a$ est un ordre qui fait de R une algèbre de Boole. On a alors $\bot = 0$, $\top = 1$, $a \wedge b = ab$, $a \vee b = a + b + ab$ et $\neg a = 1 - a$. On dit que R est un anneau de Boole.
  Réciproquement, si $(A, \leqslant)$ est une algèbre de Boole, alors si, pour tout $a, b \in A$, on définit $a \Delta b = (a \wedge \neg b) \vee (b \wedge \neg a)$, alors, $(A, \Delta, \wedge)$ est un anneau commutatif unitaire et pour tous $a \in A$, $a^2 = a \wedge a = a$. De plus, itérer ces deux constructions nous ramène à l'algèbre ou l'anneau de départ ; ce sont des équivalences de catégories.

*This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

[1] C'est-à-dire un plus petit majorant.

[2] C'est-à-dire un plus grand minorant

- Si $(A, \leqslant)$ est une algèbre de Boole, $(A, \geqslant)$ est aussi une algèbre de Boole, appelée l'algèbre duale.

Définition 1.3. Soient $(A, \leqslant)$ et $(B, \leqslant)$ des algèbres de Boole. Un morphisme $f : A \to B$ est une application de A dans B qui préserve tous les infimums et supremuns finis.

Un isomorphismes entre A et B est un morphisme $A \to B$ bijectif dont l'inverse est aussi un morphisme.

Exemple 1.4. Le complémentaire est un isomorphisme entre $(A, \leqslant)$ et $(A, \geqslant)$.

Remarque 1.5. Soit $f : A \to B$ une application.
- C'est un morphisme si et seulement si $f(\bot) = \bot$, $f(\top) = \top$ et, pour tous $a_1, a_2 \in A$, $f(a_1 \vee a_2) = f(a_1) \vee f(a_2)$ et $f(a_1 \wedge a_2) = f(a_1) \wedge f(a_2)$.
- C'est un isomorphisme si et seulement elle est bijective croissante d'inverse croissante.

Définition 1.6. Soit $(A, \leqslant)$ une algèbre de Boole. Une sous-algèbre de A est une partie $B \subseteq A$ qui est contient tous les infimums et supremums de parties finies de B.

Exemple 1.7. L'ensemble $\{Y \subseteq X \text{ finis ou de complémentaire fini}\}$ est une sous-algèbre de $(\mathcal{P}(X), \subseteq)$.

Remarque 1.8. Soit $(A, \leqslant)$ une algèbre de Boole et soit $B \subseteq A$.
- L'ensemble B est une sous-algèbre de A si et seulement si il contient $\bot$, $\top$ et $b_1 \vee b_2$ et $b_1 \wedge b_2$, pour tous b_1, b_2.
- Si B est une sous-algèbre de A alors c'est une algèbre de Boole et l'inclusion est un morphisme.

Soit $(A, \leqslant)$ une algèbre de Boole. On souhaite maintenant isoler une notion de « partie cohérente de A » :

Définition 1.9. Une partie $F \subseteq A$ est un filtre si, pour tous $a, b \in A$:
- $\bot \notin F$ et $\top \in F$;
- si $a \in F$ et $a \leqslant b$, alors $b \in F$;
- si $a, b \in F$ alors $a \wedge b \in F$.

Un filtre maximal pour l'inclusion est appelé un ultrafiltre.

Exemple 1.10.
- L'ensemble $\{\top\}$ est un filtre.
- Pour tout élément a d'une algèbre de Boole $(A, \leqslant)$, l'ensemble $\langle a \rangle = \{b \in A : a \leqslant b\}$ est un filtre. C'est un ultrafiltre si et seulement si a est un atome : pour tout $b \in A$, si $b < a$ alors $b = \bot$. En, effet, si $\bot \neq b < a$ alors le filtre $\langle b \rangle$ contient strictement $\langle a \rangle$.
- Soit X un ensemble infini, l'ensemble des parties cofinies de X est un filtre sur $(\mathcal{P}(X), \subseteq)$, appelé le filtre de Fréchet.§

Remarque 1.11. Soit I un filtre pour l'algèbre duale $(A, \geqslant)$. On a donc :
- $\top \notin I$ et $\bot \in I$ — c'est-à-dire $1 \notin I$ et $0 \in I$ dans l'anneau associé ;
- si $a \in I$ et $b \leqslant a$, alors $b \in I$ — c'est-à-dire, pour tout $c \in I$, comme $ac \leqslant a$, $ac \in I$;
- si $a, b \in I$ alors $a \vee b \in I$ — et donc $a + b = a(1 - b) \vee b(1 - a) \in I$. Réciproquement, si $I \subseteq A$ est clos par addition, alors, pour tous $a, b \in I$, $a \vee b = a + b + ab \in I$.

La notion de filtre est donc la notion duale de celle d'idéal, et les ultrafiltres sont les idéaux maximaux de l'algèbre duale.

Proposition 1.12. *Tout filtre F de A est inclus dans un ultrafiltre.*

Cette proposition est une conséquence de l'axiome du choix que l'on utilisera sous la forme du lemme de Zorn :

- Un ensemble ordonné $(X, \leqslant)$ est dit inductif si toute chaîne de X (c'est-à-dire toute partie totalement ordonnée de X) admet un majorant.
- Lemme de Zorn : tout ensemble inductif non vide admet un élément maximal.

Démonstration. Montrons que l'ensemble des filtres contenant un filtre F est inductif pour l'inclusion. La proposition 1.12 découle alors du lemme de Zorn. Soit donc $(F_i)_{i\in I}$ une chaîne de filtres contenant F. Alors $E = \bigcup_i F_i$ est un filtre qui contient F. En effet, $\bot \notin E$, $\top \in E$ et pour tous $a \in E$, $b \in A$ et $i \in I$ tels que $a \in F_i$ et $a \leqslant b$, alors $b \in F_i \subseteq E$. Enfin, si $a, b \in E$, comme les F_i forment une chaîne, on trouve i tel que $a, b \in F_i$ et donc $a \wedge b \in F_i \subseteq E$. □

Proposition 1.13. *Soit $X \subseteq A$ dont toute partie finie a une borne inférieure distincte de $\bot$. Alors*

$$F = \{b \geqslant \bigwedge_{i<n} a_i : a_i \in X\}$$

est le plus petit filtre contenant X.

On l'appelle le filtre engendré par X et un tel X est appelé une base de filtre.

Démonstration. Vérifions que F est un filtre. Tout d'abord, l'intersection de la famille vide étant $\top$, on a bien $\top \in F$. Si on avait $\bot \in F$, alors il existerait $a_i \in X$, pour $i < n$, tels que $\bot \geqslant \bigwedge_{i<n} a_i$ et donc $\bigwedge_{i<n} a_i = \bot$, ce qui contredit que X est une base de filtre. De plus, si $b \geqslant \bigwedge_{i<n} a_i$ et $c \bigwedge_{i<m} c_i$, avec $a_i, c_i \in X$, alors $b \wedge c \geqslant \bigwedge_{i<n} a_i \wedge \bigwedge_{i<m} c_i$ et donc $c \wedge b \in F$. Enfin, si $c \geqslant b \bigwedge_{i<n} a_i$, alors on a bien $c \in F$. Donc F est un filtre.

Réciproquement, si E est un filtre qui contient X, alors, pour tous $a_i \in X$, pour $i < n$, on a (par récurrence), $\bigwedge_{i<n} a_i \in E$ et donc si $b \geqslant \bigwedge_{i<n} a_i$, on $b \in E$. D'où $F \subseteq E$. □

Proposition 1.14. *Soit F un filtre de A, sont équivalents :*

(i) *F est un ultrafiltre;*
(ii) *pour tous $a, b \in A$, si $a \vee b \in F$ alors $a \in F$ ou $b \in F$;*
(iii) *pour tout $a \in A$, $a \in F$ ou $\neg a \in F$.*

Démonstration.

(i)⇒(ii) Supposons tout d'abord que F est un ultrafiltre et soient $a, b \in A$ tels que $a \vee b \in F$. Si $F \cup \{a\}$ est une base de filtre, comme F est maximal, le filtre engendré par $F \cup \{a\}$ est F lui-même et donc $a \in F$. Sinon, il existe $c \in F$ tel que $a \wedge c = \bot$. On a alors $b \geqslant b \wedge c = \bot \vee (b \wedge c) = (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge c \in F$ et donc $b \in F$.

(ii)⇒(iii) Soit $a \in A$. Comme $a \vee \neg a = \top \in F$, il découle de la condition (ii) que $a \in F$ ou $\neg a \in F$.

(iii)⇒(i) Soit $E \supseteq F$ un filtre. Si $a \in E \setminus F$, par la condition (iii), on a $\neg a \in F$ et donc $\bot = a \wedge \neg a \in E$, ce qui contredit le fait que E est un filtre. Donc $E \subseteq F$ et F est bien maximal. □

Remarque 1.15.
- Un ultrafiltre décide donc pour toute proposition $a \in A$ si elle est vraie ou fausse en respectant la relation de conséquence. On peut donc voir un ultrafiltre F comme un « modèle » de A. Pour tout $a \in A$, on note alors $F \vDash a$ — F est un modèle de A — si $a \in F$.
- On rappelle que les filtres maximaux sont exactement les filtres duaux des idéaux maximaux. Puisque pour tout x dans un algèbre de Boole, on a $x^2 - x = 0$, la seule algèbre de Boole intègre est le corps $\mathbb{Z}/2\mathbb{Z}$. Il s'ensuit que tous les idéaux premiers d'un anneau de Boole sont maximaux. Ceci donne une preuve alternative du fait qu'un filtre F d'une algèbre de Boole $(A, \leqslant)$ est un ultrafiltre si et seulement si la condition (ii) de proposition 1.14 est vérifiée.

Rappel 1.16. Soit X un ensemble.
- Une partie $\tau \subseteq \mathcal{P}(X)$ est appelé une topologie si elle est close par intersection finie et union quelconque (en particulier, elle contient $\varnothing$ et X).
- Une partie $U \in \tau$ est appelé un ouvert et le complémentaire d'un ouvert est dit fermé.
- Étant donné $B \subseteq \mathcal{P}(X)$, la topologie engendrée par B est la plus petite topologie τ contenant B. On a
$$\tau = \{\bigcup_i \bigcap_{j<n_i} U_{ij} : U_{ij} \in B\}.$$
- Soient X et Y des espaces topologiques. Une application $f : X \to Y$ est continue si, pour tout $U \subseteq Y$ ouvert, $f^{-1}(U)$ est ouvert. C'est un homéomorphisme si elle est bijective et que son inverse est aussi continu. En d'autres termes, pour tout $U \subseteq Y$, U est ouvert si et seulement si $f^{-1}(U)$ est ouvert.

Définition 1.17. On note $\mathcal{S}(A)$ l'ensemble des ultrafiltres de A. On le munit de la topologie engendrée par les $[a] = \{F \in \mathcal{S}(A) : a \in F\}$, pour tout $a \in A$.

Remarque 1.18.
1. Pour tout $a \in A$, $[\neg a] = \mathcal{S}(A) \setminus [a]$; en effet, un ultrafiltre ne peut pas contenir à la fois a et $\neg a$ et s'il ne contient pas a, il contient $\neg a$, par la proposition 1.14.
2. Pour tous $a, b \in A$, $[a \wedge b] = [a] \cap [b]$; en effet, si $a, b \in F$ alors, par définition $a \wedge b \in F$, et réciproquement, si $a \wedge b \in F$, comme $a \wedge b \leqslant a, b$, on a $a, b \in F$.
3. Pour tous $a, b \in A$, $[a \vee b] = [a] \cup [b]$; en effet, si $a \vee b \in F$ alors $a \in F$ ou $b \in F$ par proposition 1.14, et réciproquement, si $a \in F$ alors, comme $a \leqslant a \vee b$, on a $a \vee b \in F$ (et de même si $b \in F$).

Proposition 1.19. *La topologie sur $\mathcal{S}(A)$ est :*
- *séparée : pour tous $x, y \in \mathcal{S}(A)$ distincts, il existe des ouverts $U, V \subseteq \mathcal{S}(A)$ disjoints tels que $x \in U$ et $y \in V$;*
- *engendrée par des ensembles ouverts fermés ;*
- *(quasi-)compacte : pour tout recouvrement $\bigcup_{i\in I} U_i = \mathcal{S}(A)$ d'ouverts, il existe $I_0 \subseteq I$ fini tel que $\bigcup_{i\in I_0} U_i = \mathcal{S}(A)$ — de manière équivalente, toute famille $(X_i)_{i\in I}$ de fermés de $\mathcal{S}(A)$, dont toute intersection finie est non vide[3], a une intersection non vide.*

On dit que $\mathcal{S}(A)$ est un espace de Stone. On remarque que la séparation peut être renforcée : pour tout $x, y \in \mathcal{S}(A)$ distincts, il existe un ouvert fermé U tel que $x \in U$ et $y \notin U$.

[3] C'est-à-dire que c'est une base de filtre dans l'algèbre $(\mathcal{P}(\mathcal{S}(A)), \subseteq)$.

Démonstration. D'après la remarque 1.18.1, l'ensemble $[a]$ est ouvert fermé, ce qui conclut la deuxième affirmation. De plus, si F et E sont des ultrafiltres distincts de A, Il existe $a \in F \setminus E$ et on a donc $F \in [a]$ et $E \in [\neg a]$.

Enfin, soient $X_i \subseteq \mathcal{S}(A)$ des fermés, pour $i \in I$, dont toute intersection finie est non vide. On a $X_i = \bigcap_j [a_{ij}]$ et il suffit donc de montrer que $\bigcap_{ij} [a_{ij}]$ est non vide. Notons de plus que pour tous I_0 et J_{i0} finis, on a $\bigcap_{i\in I_0, j\in J_{i0}} [a_{ij}] \supseteq \bigcap_{i\in I_0} X_i \neq \varnothing$. Donc, quitte à remplacer les X_i par les $[a_{ij}]$, on peut donc supposer que $X_i = [a_i]$. L'ensemble $\{a_i : i \in I\}$ est alors une base de filtre. En effet, s'il existe $I_0 \subseteq I$ fini tel que $\bigwedge_{i\in I_0} a_i = \bot$, alors $\bigcap_{i\in I_0} [a_i] = \{F \in \mathcal{S}(A) : a_i \in F,$ pour tout $i \in I_0\} \subseteq \{F \in \mathcal{S}(A) : \bot \in F\}$ est vide.

Soit donc F un ultrafiltre contenant le filtre engendré par les a_i. Pour tout i, on a $a_i \in F$ et donc $F \in [a_i]$. □

Exemple 1.20. Pour tout ensemble X, l'ensemble 2^X muni de la topologie produit — engendrée par les $\{f : f(x) = \varepsilon\}$ pour tout $x \in X$ et $\varepsilon \in \{0, 1\}$ — est un espace de Stone. Sa compacité n'est pas évidente, mais elle est assurée par le théorème de Tychonoff. Par ailleurs, on verra plus tard qu'il est homéomorphe à l'espace de Stone d'une algèbre de Boole dont on vient de démontrer la compacité.

Si X est dénombrable, on l'appelle l'espace de Cantor.

Proposition 1.21. *Pour tout espace de Stone X, l'ensemble $\mathfrak{B}(X)$ des ouverts fermés de X forme une sous-algèbre de Boole de $(\mathcal{P}(X), \subseteq)$.*

Démonstration. Les ensembles X et $\varnothing$ sont bien ouverts et fermés. Et si $Y, Z \subseteq X$ sont ouverts fermés, alors c'est aussi le cas de $Y \cap Z$, $Y \cup Z$ et $X \setminus Y$. □

Théorème 1.22 (Dualité de Stone). *Soit A une algèbre de Boole et X un espace de Stone. Alors :*

$$f : \begin{cases} A & \to & \mathfrak{B}(\mathcal{S}(A)) \\ a & \mapsto & [a] \end{cases} \qquad \textit{et} \qquad g : \begin{cases} X & \to & \mathcal{S}(\mathfrak{B}(X)) \\ x & \mapsto & F_x = \{\textit{ouverts fermés contenant } x\} \end{cases}$$

sont, respectivement, un isomorphisme d'algèbre de Boole et un homéomorphisme.

Plus précisément il y a une équivalence de catégorie entre la catégorie des algèbres de Boole et la catégorie opposée des espaces de Stone.

Démonstration. Montrons tout d'abord que si $a, b \in A$, alors

$$a \leqslant b \text{ si et seulement si } [a] \subseteq [b].$$

On suppose tout d'abord que $a \leqslant b$. Soit $F \in [a]$, c'est-à-dire $a \in F$. On a alors $b \in F$ et donc $F \in [b]$. Réciproquement, supposons que $[a] \subseteq [b]$. Tout filtre qui contient a contient donc aussi b et donc $\{a, \neg b\}$ n'est pas une base de filtre. c'est-à-dire $a \wedge \neg b = \bot$. On a donc $a = a \wedge (b \vee \neg b) = (a \wedge b) \vee (a \wedge \neg b) = a \wedge b$ et donc $a \leqslant b$.

On a prouvé que l'application f est strictement croissante — en particulier, injective. Il reste à montrer sa surjectivité. Soit $X \subseteq \mathcal{S}(A)$ un ouvert fermé. Comme X est ouvert, on a donc $X = \bigcup_{i\in I} [a_i]$, où $a_i \in A$. Comme $\mathcal{S}(A) = (\mathcal{S}(A) \setminus X) \cup \bigcup_i [a_i]$ est un recouvrement ouvert,

il existe donc un ensemble fini $I_0 \subseteq I$ tel que $\mathcal{S}(A) = (\mathcal{S}(A) \setminus X) \cup \bigcup_{i\in I_0}[a_i]$. On a donc $X = \bigcup_{i\in I_0}[a_i] = [\vee_{i\in I_0} a_i]$. L'application f est donc bien surjective.

Considérons maintenant l'application g. Pour tout x, on vérifie que F_x est un ultrafiltre : il contient X et pas $\varnothing$, il est clos par sur-ensemble et intersection, et pour tout ouvert fermé $Y \subseteq X$, x appartient soit à X, soit à son complémentaire (qui est, lui aussi, ouvert fermé). De plus, si $x, y \in X$ sont distincts, comme la topologie de X est séparée et engendrée par des ouverts fermés, il existe un ouvert fermé $Y \subseteq X$ tel que $x \in Y$ et $y \notin Y$. On a donc $Y \in F_x \setminus F_y$. L'application g est donc injective. Enfin, si F est un ultrafiltre de $\mathfrak{B}(X)$, par compacité, $\bigcap_{Y\in F} Y$ contient un point x. On a alors $F \subseteq F_x$, et comme F est maximal, $F = F_x$. Donc g est surjective.

Il reste à montrer qu'elle est bicontinue. Soit donc $U \subseteq X$ un ouvert fermé. On a

$$g(U) = \{F_x : x \in U\} = \{F_x : U \in F_x\} = [U],$$

puisque g est surjective. Ceci conclut la preuve. □

1.2 Formules propositionnelles

On va maintenant introduire une algèbre de Boole importante : l'algèbre de Boole des formules propositionnelles. On fixe V un ensemble (dénombrable infini).

Définition 1.23. L'ensemble des formules en les variables V est le plus petit ensemble $\mathfrak{F}(V)$ qui contient :

- X, pour tout $X \in V$;
- $\bot$;
- $\varphi \to \psi$, pour tous φ et $\psi \in \mathfrak{F}(V)$.

On considère, étant donné une formule, que l'on sait de quelle forme elle est (c'est une variable, $\bot$ ou l'implication entre deux formules). En termes de représentation concrète, on peut considérer que les formules sont certains mots sur l'alphabet $V \sqcup \{\bot, \to\}$, mais se posent alors des questions (pénibles) de lecture unique et potentiellement de parenthèses. On considèrera donc plutôt les formules comme des arbres binaires dont les feuilles sont étiquetées par $V \sqcup \{\bot\}$.

Par définition, on peut raisonner par récurrence sur les formules : pour définir une fonction f sur $\mathfrak{F}(V)$, il suffit de préciser $f(X)$, pour tout $X \in V$, $f(\bot)$ et $f(\varphi \to \psi)$ en fonction de $f(\varphi)$ et $f(\psi)$.

On souhaite donner un « sens » aux formules en les interprétant comme des fonctions qui associent à chaque assignation des variables aux valeurs 0 ou 1, une valeur égale à 0 ou 1. On définit donc la sémantique (naturelle) suivante :

Définition 1.24. Soit $\varphi \in \mathfrak{F}(V)$. On définit $[\![\varphi]\!] : \{0,1\}^V \to \{0,1\}$ par récurrence sur φ. Pour tout $\alpha : V \to \{0,1\}$ on pose :

- $[\![X]\!](\alpha) = \alpha(X)$;
- $[\![\bot]\!](\alpha) = 0$;
- $[\![\varphi \to \psi]\!](\alpha) = \sup\{1 - [\![\varphi]\!](\alpha), [\![\psi]\!](\alpha)\} = \begin{cases} 0 & \text{si } [\![\varphi]\!](\alpha) = 1 \text{ et } [\![\psi]\!](\alpha) = 0 \\ 1 & \text{sinon — c'est-à-dire } [\![\varphi]\!](\alpha) \leqslant [\![\psi]\!](\alpha). \end{cases}$

Soit $\Psi \subseteq \mathfrak{F}(V)$. On dit que Ψ est valide pour l'assignation α, ce qu'on note $\alpha \vDash \Psi$, si, pour tout $\psi \in \Psi$, $[\![\psi]\!](\alpha) = 1$ — en d'autres termes $[\![\Psi]\!](\alpha) = \inf_{\psi\in\Psi}[\![\psi]\!](\alpha) = 1$ avec comme convention que $\inf \varnothing = 1$. Soit $\varphi \in \mathfrak{F}(V)$, on dit que φ est une conséquence (sémantique) de Ψ, ce qu'on note $\Psi \vDash \varphi$, si, pour tout α tel que $[\![\Psi]\!](\alpha) = 1$, on ait $[\![\varphi]\!](\alpha) = 1$ — c'est-à-dire $[\![\Psi]\!](\alpha) \leqslant [\![\varphi]\!](\alpha)$.

La relation $\varphi \vDash \psi$ est un pré-ordre[4] : on a $\varphi \vDash \psi$ si et seulement si, pour tout $\alpha : V \to \{0,1\}$, $[\![\varphi]\!](\alpha) \leqslant [\![\psi]\!](\alpha)$. Soit $\equiv$ la relation d'équivalence associée — on a donc $\varphi \equiv \psi$ si, pour tout $\alpha : V \to \{0,1\}$, $[\![\varphi]\!](\alpha) = [\![\psi]\!](\alpha)$. On peut donc identifier la classe de φ avec la fonction $[\![\varphi]\!] : \{0,1\}^V \to \{0,1\}$. Cet espace de fonction est une algèbre de Boole pour l'ordre « point par point » défini par $f \leqslant g$ si pour tout $\alpha : \{0,1\}^V$, $f(\alpha) \leqslant g(\alpha)$ — cette algèbre est isomorphe à $\mathcal{P}(\mathcal{P}(V))$. Dans la suite, on sera surtout intéressé par les formules à équivalence près et on identifiera souvent une formule avec sa classe dans l'algèbre de Boole $\mathfrak{F}_\vDash(V)$.

On peut alors vérifier que $\mathfrak{F}_\vDash(V) = (\mathfrak{F}(V)/\equiv, \vDash)$ est une sous-algèbre de Boole :

- la fonction $[\![\bot]\!]$ est constante égale à 0, fonction qui est bien le plus petit élément;
- pour toute formule φ et toute $\alpha : \{0,1\}^V$, on a $[\![\varphi \to \bot]\!](\alpha) = 1$ si et seulement si $[\![\varphi]\!](\alpha) = 0$, et donc $[\![\varphi \to \bot]\!] = 1 - [\![\varphi]\!]$ est bien le complémtaire;
- la fonction $[\![\bot \to \bot]\!]$ est constante égale à 1, fonction qui est bien plus grand élément;
- pour toutes formules φ et ψ et toute $\alpha : \{0,1\}^V$, on a $[\![(\varphi \to \bot) \to \psi]\!](\alpha) = 0$ si et seulement si $[\![\varphi]\!](\alpha) = [\![\psi]\!](\alpha) = 0$ et donc $[\![(\varphi \to \bot) \to \psi]\!] = \inf\{[\![\varphi]\!], [\![\psi]\!]\}$;
- pour toutes formules φ et ψ et toute $\alpha : \{0,1\}^V$, on a $[\![(\varphi \to (\psi \to \bot)) \to \bot]\!](\alpha) = 1$ si et seulement si $[\![\varphi]\!](\alpha) = [\![\psi]\!](\alpha) = 1$ et donc $[\![(\varphi \to (\psi \to \bot)) \to \bot]\!] = \sup\{[\![\varphi]\!], [\![\psi]\!]\}$.

Remarque 1.25. L'algèbre de Boole $\mathfrak{F}_\vDash(V)$ est l'algèbre de Boole libre sur V. Elle vérifie la propriété universelle suivante : si A est une algèbre de Boole et $f : V \to A$ une fonction, il existe un unique morphisme d'algèbre de Boole $\mathfrak{F}_\vDash(V) \to A$ qui étend f.

La sémantique définie dans la définition 1.24 est exactement cet unique prolongement des assignations de variables dans l'algèbre de Boole $\mathbb{Z}/2\mathbb{Z}$.

On vérifie que

$$\begin{array}{ccc} \mathcal{S}(\mathfrak{F}_\vDash(V)) & \simeq & 2^V \\ F & \mapsto & \mathbb{1}_{X\in F} \\ \{\varphi : [\![\varphi]\!](\alpha) = 1\} & \mapsfrom & \alpha \end{array}$$

où 2^V est muni de la topologie produit. Un point crucial est de vérifier, par récurrence sur φ, que :

$$\varphi \in F \text{ si et seulement si } [\![\varphi]\!](\mathbb{1}_{X\in F}) = 1.$$

Par définition, on a $[\![X]\!](\mathbb{1}_{X\in F}) = 1$ si et seulement si $X \in F$. De plus, $[\![\bot]\!](\mathbb{1}_{X\in F}) = 0$ et $\bot \notin F$. Enfin, Supposons que $[\![\varphi \to \psi]\!](\mathbb{1}_{X\in F}) = 1$, et donc, par récurrence $\varphi \notin F$ ou $\psi \in F$. On vérifie alors (par calcul) que $\neg\varphi \vDash \varphi \to \psi$ et $\psi \vDash \varphi \to \psi$, et donc, dans les deux cas, $\varphi \to \psi \in F$. Réciproquement, si $\varphi \to \psi \in F$ et $[\![\varphi]\!](\mathbb{1}_{X\in F}) = 1$ (et donc $\varphi \in F$), comme $\varphi \wedge (\varphi \to \psi) \vDash \psi$, on a $\psi \in F$, et donc $[\![\psi]\!](\mathbb{1}_{X\in F}) = 1$. On a donc bien que si $\varphi \to \psi \in F$, alors $[\![\varphi \to \psi]\!](\mathbb{1}_{X\in F}) = 1$.

[4] Elle est transitive et réflexive.

Définition 1.26. Une partie $\Psi \subseteq \mathfrak{F}(V)$ est dite consistante s'il existe $\alpha : V \to \{0,1\}$ telle que $\alpha \vDash \Psi$ — en d'autres termes $\Psi \nvDash \bot$.

En effet, $\Psi \nvDash \bot$ si et seulement s'il existe $\alpha : V \to \{0,1\}$ telle que $[\![\Psi]\!](\alpha) = 1 > 0 = [\![\bot]\!](\alpha)$.

Corollaire 1.27 (Compacité de la logique propositionnelle)**.** *Soit $\Psi \subseteq \mathfrak{F}(V)$ et soit $\varphi \in \mathfrak{F}(V)$.*

1. *La partie Ψ est consistante si et seulement si, toute $\Psi_0 \subseteq \Psi$ finie est consistante.*
2. *On a $\Psi \vDash \varphi$ si et seulement s'il existe $\Psi_0 \subseteq \Psi$ finie telle que $\Psi_0 \vDash \varphi$.*

Démonstration. Supposons que toute $\Psi_0 \subseteq \Psi$ est consistante et montrons que Ψ est consistante — la réciproque est claire puisque toute partie d'un ensemble consistant est consistante. Comme Ψ_0 est consistante, $\bigwedge_{\psi \in \Psi_0} \psi \not\equiv \bot$ et donc Ψ est une base de filtre de $\mathfrak{F}_{\vDash}(V)$. Elle est donc incluse dans un ultrafiltre F. Pour tout $\psi \in \Psi$, on a $[\![\psi]\!](\mathbb{1}_{X \in F}) = 1$; c'est-à-dire $\mathbb{1}_{X \in F} \vDash \Psi$ et donc Ψ est consistante.

La deuxième assertion découle alors de la première et du fait que $\Psi \vDash \varphi$ si et seulement si $\Psi \cup \{\neg\varphi\}$ n'est pas consistante. En effet, pour tout $\alpha : V \to \{0,1\}$ telle que $[\![\Psi]\!](\alpha) = 1$, $[\![\varphi]\!](\alpha) = 1$ — et donc $\Psi \vDash \varphi$ — si et seulement si $[\![\neg\varphi]\!](\alpha) = 0$ — et donc $\Psi \cup \{\neg\varphi\}$ n'est pas consistante. □

2 Logique du premier ordre

2.1 Langages, structures, formules

Définition 2.1. Un langage (du premier ordre) est la donnée, pour chaque entier $n \geqslant 0$,

- D'un ensemble $\mathfrak{F}_n$ — les fonctions d'arité n;
- D'un ensemble $\mathfrak{R}_n$ — les relations d'arité n.

Voir [HL19, Exemple 2.1.1].

Remarque 2.2. La définition ci-dessus est un cas particulier de *langage du premier ordre avec sortes* qui est la donnée :

- D'un ensemble $\mathfrak{X}$ de sortes;
- Pour tout uplet de sortes $X = (X_i)_{0 \leqslant i \leqslant n}$, d'un ensemble $\mathfrak{F}_X$ des fonctions $\prod_{i>0} S_i \to S_0$;
- Pour tout uplet de sortes $X = (X_i)_{0 < i \leqslant n}$, d'un ensemble $\mathfrak{R}_X$ des relations sur $\prod_{i>0} S_i$.

La définition 2.1 est le cas particulier où l'ensemble des sortes est un singleton. Toutes les définitions et les résultats que l'on prouvera par la suite s'adaptent à ce cadre général, mais on s'en tiendra aux langages à une sorte pour alléger les notations.

On fixe, à présent, un langage $\mathfrak{L}$.

Définition 2.3. Une $\mathfrak{L}$-structure M est la donnée :

- D'un ensemble $\mathrm{A}(M)$ non vide[5];
- Pour tout $F \in \mathfrak{F}_n$, d'une fonction $F^M : \mathrm{A}(M)^n \to \mathrm{A}(M)$;
- Pour tout $R \in \mathfrak{R}_n$, d'une partie $R^M \subseteq \mathrm{A}(M)^n$.

[5] On pourrait tout à fait autoriser les structures vides, mais cela compliquerait un peu certaines constructions par la suite. On se permettra donc d'ignorer ici cette (unique) structure.

Voir [HL19, Exemple 2.1.2].

On fixe, à présent, un ensemble infini (dénombrable) V de variables.

Définition 2.4. L'ensemble $\mathfrak{T}^{\mathfrak{L}}(V)$ des termes du langage $\mathfrak{L}$ en les variables V est le plus petit ensemble qui contient :

- x, pour tout $x \in V$;
- $Ft_1 \dots t_n$, pour tout $F \in \mathfrak{F}_n$ et tous $t_1, \dots, t_n \in \mathfrak{T}^{\mathfrak{L}}(V)$.

Définition 2.5. L'ensemble $\mathfrak{F}^{\mathfrak{L}}(V)$ des formules du langage $\mathfrak{L}$ en les variables V est le plus petit ensemble qui contient :

- $t_1 = t_2$, pour tous t_1 et $t_2 \in \mathfrak{T}^{\mathfrak{L}}(V)$;
- $Rt_1 \dots t_n$, pour tout $R \in \mathfrak{R}_n$ et tous $t_1, \dots, t_n \in \mathfrak{T}^{\mathfrak{L}}(V)$;
- $\bot$;
- $\varphi \to \psi$, pour tous φ et $\psi \in \mathfrak{F}^{\mathfrak{L}}(V)$;
- $\forall x\, \varphi$, pour tout $x \in V$ et $\varphi \in \mathfrak{F}^{\mathfrak{L}}(V)$.

Les formules de la forme $Rt_1 \dots t_n$, où $R \in \mathfrak{R}_n$ et $t_1, \dots, t_n \in \mathfrak{T}^{\mathfrak{L}}(V)$, celles de la forme $t_1 = t_2$, où t_1 et $t_2 \in \mathfrak{T}^{\mathfrak{L}}(V)$, ainsi que la formule $\bot$ sont dites atomiques.

La question de la représentation concrète des formules est ici plus cruciale puisque la manière dont on décide de gérer les variables liées par des quantificateurs aura des conséquences sur la suite. On pourrait choisir de les représenter par des arbres dont les sommets sont annotés par $V \sqcup \{=, \bot, \to, \forall\} \sqcup \bigsqcup_n (\mathfrak{F}_n \sqcup \mathfrak{R}_n)$. Cela pose cependant la question du statut des variables liées par des quantificateurs, du fait que la même variable peut être liée ou libre dans la même formule, voire liée par des quantificateurs disctints. Il faut donc travailler « à renommage des variables liées » près, ce qui peut être assez pénible quand on fera des choses plus syntactiques.

Ici, on choisira donc plutôt de ne pas nommer les variables liées et de représenter les formules comme des arbres où les variables liées sont remplacée par un lien vers leur quantificateur. Techniquement, les formules sont donc des graphes orientés pointés dont les sommets sont annotés par $V \sqcup \{=, \bot, \to, \forall\} \sqcup \bigsqcup_n (\mathfrak{F}_n \sqcup \mathfrak{R}_n)$.

L'intérêt de cette représentation et que pour tous φ et $\psi \in \mathfrak{F}^{\mathfrak{L}}(V)$ et tous x et $y \in V$,

$$\forall x\, \varphi = \forall y\, \psi \text{ si et seulement si } y \text{ n'a pas d'occurrence dans } \varphi \text{ et } \psi = \varphi(y/x)$$

qui est la formule obtenue en remplaçant toutes les occurences de x par y. Cette représentation sera aussi très pratique pour définir la substitution puisqu'elle évite la capture de variables par les quantificateurs.

On interprète la « vérité » d'une formule suivant la sémantique naturelle suivante :

Définition 2.6. Soit M une structure et $t \in \mathfrak{T}^{\mathfrak{L}}(V)$. On définit $[\![t]\!]_M : \mathrm{A}(M)^V \to \mathrm{A}(M)$ par récurrence sur t. Pour tout $\alpha : V \to \mathrm{A}(M)$, on pose :

- $[\![x]\!]_M(\alpha) = \alpha(x)$;
- $[\![Ft_1 \dots t_n]\!]_M(\alpha) = F^M([\![t_1]\!]_M(\alpha), \dots, [\![t_1]\!]_M(\alpha))$.

Soit $\varphi \in \mathfrak{F}^{\mathfrak{L}}(V)$. On définit aussi $[\![\varphi]\!]_M : \mathrm{A}(M)^V \to \{0, 1\}$ par récurrence sur φ. Pour tout $\alpha : V \to M$, on pose :

- $[\![t_1 = t_2]\!]_M(\alpha) = \mathbb{1}_{[\![t_1]\!]_M(\alpha) = [\![t_2]\!]_M(\alpha)}$;
- $[\![Rt_1 \dots t_n]\!]_M(\alpha) = \mathbb{1}_{R^M}([\![t_1]\!]_M(\alpha), \dots, [\![t_1]\!]_M(\alpha))$;

- $[\![\bot]\!]_M(\alpha) = 0$;
- $[\![\varphi \to \psi]\!]_M(\alpha) = \sup\{1 - [\![\varphi]\!]_M(\alpha), [\![\psi]\!]_M(\alpha)\}$;
- $[\![\forall x\, \varphi]\!]_M(\alpha) = \inf_{a \in \mathrm{A}(M)} [\![\varphi]\!]_M(\alpha_{x \mapsto a})$[6] où $\alpha_{x\mapsto a}(x) = a$ et $\alpha_{x\mapsto a}(y) = \alpha(y)$ si $y \neq x$.

Si $[\![\varphi]\!]_M(\alpha)$, on dit que φ est satisfaite par α dans M, ce que l'on note $M \vDash \varphi(\alpha)$.

Remarque 2.7. On peut vérifier, par récurrence sur φ, que $[\![\varphi]\!]_M(\alpha)$ ne dépend que des valeurs de α pour les variables ayant une occurrence (libre) dans φ; on rappelle que, par construction, les variables liées par des quantificateurs n'apparaissent pas dans la formule φ.

On écrira $\varphi(x_1, \dots, x_n)$ pour indiquer que les variables de φ apparaissent toutes parmi les variables (distinctes deux à deux) $x_1, \dots, x_n$. Pour tout $a_1, \dots, a_n \in \mathrm{A}(M)$ on écrit alors $M \vDash \varphi(a_1, \dots, a_n)$ pour signifier que $M \vDash \varphi(\alpha)$ pour tout choix de $\alpha : V \to \mathrm{A}(M)$ telle que $\alpha(x_i) = a_i$, pour tout $i \leqslant n$.

Une formule est dite close, on parle aussi d'énoncé, si aucune variable n'apparaît dans φ. On écrit alors $M \vDash \varphi$ si pour un choix de $\alpha : V \to \mathrm{A}(M)$ (et donc pour tous), $M \vDash \varphi(\alpha)$. Un ensemble de formules closes T est aussi appelé une théorie. On dit qu'une structure M est un modèle de T, ce que l'on note $M \vDash T$, si pour tout $\varphi \in T$, $M \vDash \varphi$ — c'est-à-dire que $[\![T]\!]_M$ est la fonction constante égale à 1.

Comme pour la logique propositionnelle, la relation $\varphi \vDash \psi$ est un pré-ordre et on note $\equiv$ la relation d'équivalence associée. L'ensemble ordonné $\mathfrak{F}^{\mathfrak{L}}_{\vDash}(V) = (\mathfrak{F}^{\mathfrak{L}}(V)/\equiv, \vDash)$ est alors une algèbre de Boole. Pour toutes formules φ et ψ, on a :

- un complémentaire $\neg\varphi \equiv \varphi \to \bot$;
- un supremum $\varphi \vee \psi \equiv (\neg\varphi) \to \psi$;
- un infimum $\varphi \wedge \psi \equiv \neg(\varphi \to (\neg\psi))$.

On introduit aussi l'équivalence $\varphi \leftrightarrow \psi \equiv (\varphi \to \psi) \wedge (\psi \to \varphi)$ et le quantificateur existentiel $\exists x\, \varphi \equiv \neg\forall x\, \neg\varphi$.

On peut alors calculer la sémantique de ces nouveaux symboles. Pour toute structure M et toute $\alpha : V \to \mathrm{A}(M)$, on a :

- $[\![\neg\varphi]\!]_M(\alpha) = 1 - [\![\varphi]\!]_M(\alpha)$;
- $[\![\varphi \vee \psi]\!]_M(\alpha) = \sup\{[\![\varphi]\!]_M(\alpha), [\![\psi]\!]_M(\alpha)\}$;
- $[\![\varphi \wedge \psi]\!]_M(\alpha) = \inf\{[\![\varphi]\!]_M(\alpha), [\![\psi]\!]_M(\alpha)\}$;
- $[\![\varphi \leftrightarrow \psi]\!]_M(\alpha) = \mathbb{1}_{[\![\varphi]\!]_M(\alpha) = [\![\psi]\!]_M(\alpha)}$;
- $[\![\exists x\, \varphi]\!]_M(\alpha) = \sup_{a \in \mathrm{A}(M)} [\![\varphi]\!]_M(\alpha_{x\mapsto a})$.

2.2 Ultraproduits

On fixe dorénavant un langage $\mathfrak{L}$ et un ensemble de variables V. Soient $(M_i)_{i\in I}$ des structures et $\mathfrak{U}$ un ultrafiltre sur l'algèbre de Boole $(P(I), \subseteq)$.

Définition 2.8. L'ultraproduit $N = \prod_{i\to\mathfrak{U}} M_i$ est la $\mathcal{L}$-structure avec :

[6] Pour être parfaitement correct, puisque $\forall x\, \varphi$ n'est défini qu'à renommage de x près, il faudrait plutôt considérer $\inf_{a\in\mathrm{A}(M), y\notin\mathrm{var}(\forall x\, \varphi)} [\![\varphi(y/x)]\!]_M(\alpha_{y\mapsto a})$. Mais on peut vérifier, *a posteriori*, par récurrence sur φ que ces deux quantités sont égales.

- ensemble sous-jacent $\mathrm{A}(N) = \prod_i \mathrm{A}(M_i)/\sim$ où

$$a \sim b \text{ si et seulement si } \{i \in I : a_i = b_i\} \in \mathfrak{U};$$

- pour tout symbole de fonction $F \in \mathfrak{F}_n$ d'arité n et $a_1, \dots, a_n \in \mathrm{A}(N)$,

$$F^N(a_1, \dots, a_n) = (F^{M_i}(a_{1,i}, \dots, a_{n,i}))/\sim,$$

où $a_j = (a_{j,i})/\sim$;
- pour tout symbole de relation $R \in \mathfrak{R}_n$ d'arité n et $a_1, \dots, a_n \in \mathrm{A}(N)$,

$$(a_1, \dots, a_n) \in R^N \text{ si et seulement si } \{i \in I : (a_{1,i}, \dots, a_{n,i}) \in R^{M_i}\} \in \mathfrak{U},$$

où $a_j = (a_{j,i})_i/\sim$.

Il faut tout de même montrer que $\sim$ est bien une relation d'équivalence et que les définitions de F^N et R^N ne dépendent pas de choix de coordonnées.

Démonstration. Vérifions d'abord que $\sim$ est bien une relation d'équivalence. Elle est réflexive puisque pour tout $a \in \prod_i \mathrm{A}(M_i)$, $\{i \in I : a_i = a_i\} = I \in \mathfrak{U}$. Elle est aussi symétrique puisque, pour tout $b \in \prod_i \mathrm{A}(M_i)$, $\{i \in I : a_i = b_i\} = \{i \in I : b_i = a_i\}$. Montrons enfin qu'elle est transitive. Pour tout $c \in \prod_i \mathrm{A}(M_i)$, si $a \sim b$ et $b \sim c$, on a $X = \{i \in I : a_i = b_i\} \in \mathfrak{U}$ et $Y = \{i \in I : a_i = b_i\} \in \mathfrak{U}$. On a alors

$$X \cap Y \subseteq \{i \in I : a_i = c_i\}$$

qui est donc aussi un élément de $\mathfrak{U}$. On a donc bien $a \sim c$ et $\sim$ est transitive.

Soit maintenant F un symbole de fonction d'arité n et $a, b \in N^n$ tels que, pour tous $j \leqslant n$, $a_j \sim b_j$; et donc $X_j = \{i \in I : a_{j,i} = b_{j,i}\} \in \mathfrak{U}$, où $a_j = (a_{j,i})_{i \in I}/\sim$ et $b_j = (b_{j,i})_{i \in I}/\sim$. Comme

$$\bigcap_{j \leqslant n} X_j \subseteq \{i \in I : F^{M_i}(a_{1,i}, \dots, a_{n,i}) = F^{M_i}(b_{1,i}, \dots, b_{n,i})\}$$

ce dernier ensemble est un élément de $\mathfrak{U}$ et donc

$$(F^{M_i}(a_{1,i}, \dots, a_{n,i}))_{i \in I} \sim F^{M_i}(b_{1,i}, \dots, b_{n,i});$$

c'est-à-dire que F^N est bien défini. De même, si R est un symbole de relation d'arité n,

$$\bigcap_{j \leqslant n} X_j \cap \{i \in I : (a_{1,i}, \dots, a_{n,i}) \in R^{M_i}\} \subseteq \{i \in I : (b_{1,i}, \dots, b_{n,i}) \in R^{M_i}\}$$

et donc, par symétrie,

$$\{i \in I : (a_{1,i}, \dots, a_{n,i}) \in R^{M_i}\} \in \mathfrak{U} \text{ si et seulement si } \{i \in I : (b_{1,i}, \dots, b_{n,i}) \in R^{M_i}\} \in \mathfrak{U};$$

ce qui montre que R^N est bien défini. □

On n'a pas encore utilisé que $\mathfrak{U}$ est un ultrafiltre, mais simplement que c'est un filtre. Le fait que c'est un ultrafiltre est cependant nécessaire pour le résultat suivant :

Théorème 2.9 (Łoš). *Pour toute formule φ et tous $\alpha_i : V \to \mathrm{A}(M_i)$, on a*

$$\prod_{i \to \mathfrak{U}} M_i \vDash \varphi(\alpha) \text{ si et seulement si } \{i : M_i \vDash \varphi(\alpha_i)\} \in \mathfrak{U},$$

où $\alpha(x) = (\alpha_i(x))_{i \in I}/\sim$, pour tout $x \in V$.

En d'autres termes, la définition choisie pour l'interprétation des relations dans l'ultraproduit s'étend aux formules.

Démonstration. Montrons tout d'abord que pour tout terme t, on a

$$[\![t]\!]_N(\alpha) = ([\![t]\!]_{M_i}(\alpha_i))_{i \in I}/\sim$$

On procède par récurrence sur le terme t. Si t est une variable $x \in V$, $[\![x]\!]_N(\alpha) = (\alpha_i(x))_{i \in I}/\sim = ([\![x]\!]_{M_i}(\alpha_i))_{i \in I}/\sim$ par définition. Si t est de la forme $Ft_1 \dots t_n$, on a

$$\begin{aligned}
[\![t]\!]_N(\alpha) &= F^N([\![t_1]\!]_N(\alpha), \dots, [\![t_n]\!]_N(\alpha)) && \text{par définition de } [\![t]\!]_N \\
&= F^N(([\![t_1]\!]_{M_i}(\alpha_i))_{i \in I}/\sim, \dots, ([\![t_n]\!]_{M_i}(\alpha_i))_{i \in I}/\sim) && \text{par récurrence} \\
&= (F^{M_i}([\![t_1]\!]_{M_i}(\alpha_i), \dots, [\![t_n]\!]_{M_i}(\alpha_i)))_{i \in I}/\sim && \text{par définition de } F^N \\
&= ([\![Ft_1 \dots t_n]\!]_{M_i}(\alpha_i))_{i \in I}/\sim. && \text{par définition de } [\![t]\!]
\end{aligned}$$

On prouve alors le théorème par récurrence sur la formule φ. Si c'est une formule atomique de la forme $t_1 = t_2$, on a $N \vDash (t_1 = t_2)(\alpha)$ si et seulement si $[\![t_1]\!]_N(\alpha) = [\![t_2]\!]_N(\alpha)$, c'est-à-dire

$$\{i \in I : M_i \vDash (t_1 = t_2)(\alpha_i)\} = \{i \in I : [\![t_1]\!]_{M_i}(\alpha_i) = [\![t_2]\!]_{M_i}(\alpha_i)\} \in \mathfrak{U}.$$

Si φ est de la forme $Rt_1 \dots t_n$, par définition de R^N, on a $N \vDash (Rt_1 \dots t_n)(\alpha)$ si et seulement si

$$\{i \in I : M_i \vDash (Rt_1 \dots t_n)(\alpha_i)\} = \{i \in I : ([\![t_1]\!]_{M_i}(\alpha_i), \dots, [\![t_n]\!]_{M_i}(\alpha_i)) \in R^{M_i}\} \in \mathfrak{U}.$$

Si φ est $\bot$, on a $N \nvDash \bot(\alpha)$ et $\{i \in I : M_i \vDash \bot(\alpha_i)\} = \varnothing \notin \mathfrak{U}$.

Pour ce qui est des formules de forme $\psi_1 \to \psi_2$, on commence par considérer le cas des formules de la forme $\neg\psi$ et $\psi_1 \wedge \psi_2$. Le cas de l'implication en découle puisque $[\![\psi_1 \to \psi_2]\!] = [\![\neg(\psi_1 \wedge \neg\psi_2)]\!]$.

Si φ est de la forme $\neg\psi$,

$$\begin{aligned}
N \vDash (\neg\psi)(\alpha) &\Leftrightarrow N \nvDash \psi(\alpha) \\
&\Leftrightarrow \{i \in I : M_i \vDash \psi(\alpha_i)\} \notin \mathfrak{U} && \text{par récurrence} \\
&\Leftrightarrow \{i \in I : M_i \nvDash \psi(\alpha_i)\} \in \mathfrak{U} && \text{puisque } \mathfrak{U} \text{ est un ultrafiltre} \\
&\Leftrightarrow \{i \in I : M_i \vDash \neg\psi(\alpha_i)\} \in \mathfrak{U}.
\end{aligned}$$

Si φ est de la forme $\psi_1 \wedge \psi_2$,

$$\begin{aligned}
N \vDash (\psi_1 \wedge \psi_2)(\alpha) &\Leftrightarrow N \vDash \psi_1(\alpha) \text{ et } N \vDash \psi_2(\alpha) \\
&\Leftrightarrow X_j = \{i \in I : M_i \vDash \psi_1(\alpha_i)\} \in \mathfrak{U} \text{ pour } j = 1, 2 \\
&\Leftrightarrow X_1 \cap X_2 \in \mathfrak{U} \\
&\Leftrightarrow \{i \in I : M_i \vDash (\psi_1 \wedge \psi_2)(\alpha_i)\}.
\end{aligned}$$

La troisième équivalence découle du fait que $\mathfrak{U}$ est un filtre. En effet, si $X_1 \cap X_2 \in \mathfrak{U}$, alors comme $X_1 \cap X_2 \subseteq X_j$, on a bien $X_j \in \mathfrak{U}$. La réciproque est vraie par définition des filtres. Cela conclut le cas de la disjonction.

Il reste à traiter le cas où φ est de la forme $\forall x\, \varphi$. Pour cela on considère d'abord le cas où φ est de la forme $\exists x\, \varphi$. Le cas du quantificateur universel s'en déduit puisque $[\![\forall x\, \varphi]\!] = [\![\neg \exists x\, \neg \varphi]\!]$.

Si φ est de la forme $\exists x\, \psi$. On a,

$$\begin{aligned} N \vDash (\exists x\, \psi)(\alpha) &\Leftrightarrow \text{ il existe } a \in \mathrm{A}(N) \text{ tel que } N \vDash \varphi(\alpha_{x \mapsto a}) \\ &\Leftrightarrow \text{il existe } a_i \in \prod_i \mathrm{A}(M_i) \text{ tel que } X_{a_i} = \{i \in I : M_i \vDash \varphi(\alpha_{x \mapsto a_i})\} \in \mathfrak{U} \\ &\Leftrightarrow Y = \{i \in I : M_i \vDash \exists x\, \varphi(\alpha)\} \in \mathfrak{U}. \end{aligned}$$

La deuxième équivalence découle de l'hypothèse de récurrence[7]. Pour ce qui est de la dernière équivalence, l'implication de haut en bas suit du fait que $X_{a_i} \subseteq Y$. Pour la réciproque, pour tout $i \in Y$, soit a_i tel que $M_i \vDash \varphi(\alpha_{x \mapsto a_i})$ et a_i quelconque sinon. On a alors $Y \subseteq X_{a_i}$, ce qui prouve l'implication de bas en haut. Ceci conclut la preuve. □

Définition 2.10. Soit Φ un ensemble de formules et ψ une formule.

- On dit que Φ est consistant s'il existe une structure M et une assignation $\alpha : V \to M$ telles que, pour tout $\varphi \in \Phi$, $M \vDash \varphi(\alpha)$; c'est-à-dire $[\![\Phi]\!]_M(\alpha) = \inf_{\varphi \in \Phi} [\![\varphi]\!]_M(\alpha) = 1$. On dit aussi que α satisfait Φ dans M et on écrit $M \vDash \Phi(\alpha)$.
- On dit que Φ est finiment consistant si toute $\Phi_0 \subseteq \Phi$ finie est consistante.
- On dit que Φ a pour conséquence (sémantique) ψ — ce qu'on note $\Phi \vDash \psi$ — si, pour toute structure M et toute assignation $\alpha : V \to M$, on a :

$$[\![\Phi]\!]_M(\alpha) \leqslant \alpha(\psi).$$

Théorème 2.11 (Compacité de la logique du premier ordre)**.** *Soit Φ un ensemble de formules et ψ une formule.*

1. *L'ensemble Φ est consistant si et seulement s'il est finiment consistant.*
2. *On a $\Phi \vDash \psi$ si et seulement s'il existe $\Phi_0 \subseteq \Phi$ finie telle que $\Phi_0 \vDash \psi$.*

Démonstration. Montrons tout d'abord la première assertion et supposons que Φ est finiment consistant et prouvons qu'il est consistant — la réciproque découle du fait que toute partie d'un ensemble consistant est elle-même consistante. Soit I l'ensemble des formules consistantes. Pour tout $\varphi \in I$, soit M_φ une structure et $\alpha_\varphi : V \to \mathrm{A}(M_\varphi)$ une assignation telles que $M_\varphi \vDash \varphi(\alpha_\varphi)$. Pour tout $\varphi \in I$, on note $\langle \varphi \rangle = \{\psi \in I : \psi \vDash \varphi\}$. L'ensemble $\langle \Phi \rangle = \{\langle \varphi \rangle : \varphi \in \Phi\}$ est alors une base de filtre. En effet, comme Φ est finiment consistante, pour tout ensemble fini $\Phi_0 \subseteq \Phi$, la formule $\bigwedge_{\varphi \in \Phi_0} \varphi$ est consistante et, pour tout φ dans Φ_0, elle appartient à $\langle \varphi \rangle$.

Soit $\mathfrak{U}$ un ultrafiltre qui contient $\langle \Phi \rangle$, $M = \prod_{\varphi \to \mathfrak{U}} M_\varphi$ et $\alpha : V \to \mathrm{A}(M)$ définie par $x \mapsto (\alpha_\varphi(x))/\sim$. Par le théorème de Łoš (théorème 2.9), pour toute formule $\varphi \in \Phi$, on a :

$$M \vDash \varphi(\alpha) \text{ si et seulement si } \{\psi : M_\psi \vDash \varphi(\alpha_\psi)\} \in \mathfrak{U}.$$

[7] Et d'un petit usage discret de l'axiome du choix

Mais si $\psi \in \langle\varphi\rangle$, comme $\psi \vDash \varphi$, on a $M_\psi \vDash \varphi(\alpha_\psi)$ et donc

$$\{\psi : M_\psi \vDash \varphi(\alpha_\psi)\} \supseteq \langle\varphi\rangle \in \mathfrak{U}.$$

Il s'ensuit que, $M \vDash \Phi(\alpha)$, ce qui conclut la preuve de la première assertion.

La seconde assertion en découle puisque $\Phi \vDash \psi$ si et seulement si $\Phi \cup \{\neg\psi\}$ n'est pas consistante. En effet, on a $\Psi \vDash \varphi$ si et seulement si, pour toute structure M et $\alpha : V \to M$ telle que $\inf_{\varphi\in\Phi} \alpha(\varphi) = 1$, on ait $[\![\psi]\!](\alpha) = 1$ et donc $[\![\neg\psi]\!](\alpha) = 0$; ce qui est équivalent au fait que $\Phi \cup \{\neg\psi\}$ n'est pas consistante. □

Remarque 2.12. Soit T une théorie telle que pour tout entier n il existe une structure $M \vDash T$ avec $\mathrm{A}(M)$ de cardinal plus grand que n. Alors T admet des modèles infinis. En effet, soit ψ_n les formule $\exists x_1 \dots \exists x_n \bigwedge_{i\neq j} \neg x_i = x_j$. On a

$$M \vDash \psi_n \Leftrightarrow M \text{ est de taille au moins } n.$$

L'ensemble $T \cup \{\psi_n : n \geqslant 1\}$ est finiment consistant, en effet, n'importe quel $M \vDash T$ de cardinal plus grand que m satisfait $T \cup \{\psi_n : n \leqslant m\}$. Par le théorème de compacité (théorème 2.11), il est alors satisfait par une structure M. Cette structure est infinie puisque M satisfait ψ_n pour tout $n \geqslant 1$.

En particulier, il n'existe pas de théorie dont les modèles sont exactement les structures finies.

3 Théorie des modèles

3.1 Équivalence et morphismes élémentaires

On rappelle qu'on a fixé un langage $\mathfrak{L}$ et un ensemble de variables V infini (dénombrable).

Définition 3.1. Soient M et N des structures.

1. On appelle théorie de M l'ensemble $\mathrm{Th}(M) = \{\varphi \text{ formule close} : M \vDash \varphi\}$.
2. On dit que M et N sont élémentairement équivalents, ce que l'on note $M \equiv N$ si pour toute formule close φ,
$$M \vDash \varphi \text{ si et seulement si } N \vDash \varphi.$$
En d'autres termes, $M \equiv N$ si $\mathrm{Th}(M) = \mathrm{Th}(N)$.
3. La théorie T est complète si pour tous $M, N \vDash T$, on a $M \equiv N$.

Remarque 3.2. Une théorie est complète si et seulement si pour toute formule close φ, $T \vDash \varphi$ ou $T \vDash \neg\varphi$. En effet, si c'est le cas, pour tous $M, N \vDash T$ et toute formule close φ, on a $M \vDash \varphi$ si et seulement si $T \vDash \varphi$ si et seulement si $N \vDash \varphi$. Réciproquement, si T n'est pas complète, il existe $M, N \vDash T$ qui ne sont pas élémentairement équivalents. Il existe don une formule clos φ telle que $M \vDash \varphi$ et $N \vDash \neg\varphi$. On a donc ni $T \vDash \varphi$, ni $T \vDash \neg\varphi$.

Exemple 3.3.

- Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ ne sont pas élémentairement équivalents. On a

$$\mathbb{R} \vDash \exists x\, x \cdot x = 1 + 1 \text{ mais } \mathbb{Q} \nvDash \exists x\, x \cdot x = 1 + 1.$$

  et

$$\mathbb{C} \vDash \exists x\, x \cdot x + 1 = 0$$

  mais ce n'est pas le cas des deux autres structures.
- Les groupes additifs $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont élémentairement équivalents (voir exemple 3.26, mais on ne sait pas encore le démontrer).
- Les anneaux $\mathbb{Q}^{\mathrm{a}}$ (clôture algébrique de $\mathbb{Q}$) et $\mathbb{C}$ sont élémentairement équivalents (on le démontrera plus tard aussi). On verra que la théorie des corps algébriquement clos de caractéristique fixée est complète.
- Les anneaux $\mathbb{Q}^{\mathrm{a}} \cap \mathbb{R}$ et $\mathbb{R}$ le sont aussi (mais on ne le démontrera pas).

Définition 3.4. Soient M et N deux structures et $f : \mathrm{A}(M) \to \mathrm{A}(N)$ une fonction.

- C'est un morphisme[8] si, pour tout $a = (a_i)_{i<n} \in \mathrm{A}(M)^n$, tout $F \in \mathfrak{F}_n$ et tout $R \in \mathfrak{R}_n$,

$$f(F^M(a)) = F^N(f(a)) \text{ et si } a \in R^M \text{ alors } f(a) \in R^N$$

  où $f(a) = (f(a_i))_{i<n}$.
- C'est un plongement si f est injective et si, pour tout $a = (a_i)_{i<n} \in \mathrm{A}(M)^n$, tout $F \in \mathfrak{F}_n$ et tout $R \in \mathfrak{R}_n$,

$$f(F^M(a)) = F^N(f(a)) \text{ et } a \in R^M \text{ si et seulement si } f(a) \in R^N.$$

- C'est un isomorphisme si c'est un plongement surjectif.

Remarque 3.5. Un isomorphisme est exactement un plongement inversible, dont l'inverse est encore un plongement. C'est aussi exactement un morphisme inversible, dont l'inverse est un morphisme.

Proposition 3.6. *Soient M et N des structures et soit $f : \mathrm{A}(M) \to \mathrm{A}(N)$ une application.*

1. *Si f est un plongement $M \to N$, alors pour tout $\alpha : V \to \mathrm{A}(M)$ et tout terme t,*

$$f([\![t]\!]_M(\alpha)) = [\![t]\!]_N(f \circ \alpha).$$

2. *La fonction f est un plongement $M \to N$ si et seulement si, pour toute formule sans quantificateurs[9] $\varphi(x)$ et toute $\alpha : V \to \mathrm{A}(M)$,*

$$[\![\varphi]\!]_M(\alpha) = [\![\varphi]\!]_N(f \circ \alpha).$$

C'est-à-dire que pour toute formule sans quantificateurs $\varphi(x_1, \ldots, x_n)$ et tout $a_1, \ldots, a_n \in \mathrm{A}(M)$,

$$M \vDash \varphi(a_1, \ldots, a_n) \text{ si et seulement si } N \vDash \varphi(f(a_1), \ldots, f(a_n)).$$

[8] On utilisera très peu cette notion.

[9] L'ensemble des formules sans quantificateurs est le plus petit ensemble de formules clos par implication et qui contient $\bot$ et les formules atomiques.

Démonstration. Supposons que f est un plongement et montrons la première assertion par récurrence sur t. Si t est une variable x, on a $f([\![x]\!]_M(\alpha)) = f(\alpha(x)) = [\![x]\!]_N(f \circ \alpha)$. Si t est de la forme $Ft_1 \dots t_n$, on a

$$\begin{aligned} f([\![Ft_1 \dots t_n]\!]_M(\alpha)) &= f(F^M([\![t_1]\!]_M(\alpha), \dots, [\![t_n]\!]_M(\alpha))) \\ &= F^N(f([\![t_1]\!]_M(\alpha)), \dots, f([\![t_n]\!]_M(\alpha))) \\ &= F^N([\![t_1]\!]_N(f \circ \alpha), \dots, [\![t_n]\!]_N(f \circ \alpha)) \\ &= [\![Ft_1 \dots t_n]\!]_N(f \circ \alpha). \end{aligned}$$

Montrons maintenant, en supposant toujours que f est un plongement, que $M \vDash \varphi(\alpha)$ si et seulement si $N \vDash \varphi(f \circ \alpha)$, par récurrence sur φ — ce qui prouvera la seconde assertion puisque que la réciproque se déduit en considérant les formules $Fx_1, \dots, x_n = y$, pour $F \in \mathfrak{F}_n$ et $Rx_1, \dots, x_n$, pour $R \in \mathfrak{R}_n$.

Si φ est de la forme $t_1 = t_2$, on a

$$\begin{aligned} M \vDash (t_1 = t_2)(\alpha) &\Leftrightarrow [\![t_1]\!]_M(\alpha) = [\![t_2]\!]_M(\alpha) \\ &\Leftrightarrow f([\![t_1]\!]_M(\alpha)) = f([\![t_2]\!]_M(\alpha)) \\ &\Leftrightarrow [\![t_1]\!]_N(f \circ \alpha) = [\![t_2]\!]_N(f \circ \alpha) \\ N \vDash (t_1 = t_2)(f \circ \alpha). \end{aligned}$$

Si φ est de la forme $Rt_1 \dots t_n$, on a

$$\begin{aligned} M \vDash (Rt_1 \dots t_n)(\alpha) &\Leftrightarrow ([\![t_1]\!]_M(\alpha), \dots, [\![t_n]\!]_M(\alpha)) \in R^M \\ &\Leftrightarrow (f([\![t_1]\!]_M(\alpha)), \dots, f([\![t_n]\!]_M(\alpha))) \in R^N \\ &\Leftrightarrow ([\![t_1]\!]_N(f \circ \alpha), \dots, [\![t_n]\!]_N(f \circ \alpha)) \in R^N \\ &\Leftrightarrow N \vDash (Rt_1 \dots t_n)(f \circ \alpha). \end{aligned}$$

Si φ est de la forme $\bot$, on a

$$[\![\bot]\!]_M(\alpha) = 0 = [\![\bot]\!]_N(f \circ \alpha).$$

Finalement, si φ est de la forme $\psi \to \theta$, on a

$$\begin{aligned} M \vDash (\psi \to \theta)(\alpha) &\Leftrightarrow [\![\psi]\!]_M(\alpha) \leqslant [\![\theta]\!]_M(\alpha) \\ &\Leftrightarrow [\![\psi]\!]_N(f \circ \alpha) \leqslant [\![\theta]\!]_N(f \circ \alpha) \\ &\Leftrightarrow N \vDash (\psi \to \theta)(f \circ \alpha). \end{aligned}$$

□

Remarque 3.7. Plus précisément, ce qu'on a démontré, c'est que si $f : M \to N$ est un plongement, l'ensemble des formules telles que, pour tout $\alpha : V \to \mathrm{A}(M)$, $[\![\varphi]\!]_M(\alpha) = [\![\varphi]\!]_N(f \circ \alpha)$, contient les formules atomiques et est clos par implication (et donc par toutes les opérations booléennes).

Remarque 3.8. Pour montrer que f est un plongement, il suffit de vérifier que pour toute formule sans quantificateurs $\varphi(x)$ et toute $\alpha : V \to \mathrm{A}(M)$, si $M \vDash \varphi(\alpha)$ alors $N \vDash \varphi(f \circ \alpha)$.

En effet, on a alors aussi que si $N \vDash \varphi(f \circ \alpha)$ alors $N \nvDash \neg\varphi(f \circ \alpha)$ et donc $M \nvDash \varphi(\alpha)$, dont il découle que $M \vDash \varphi(\alpha)$.

Définition 3.9. Soient M et N des structures et $f : \mathrm{A}(M) \to \mathrm{A}(N)$ une fonction. On dit que c'est un morphisme élémentaire de M dans N si pour toute formule φ et tout $\alpha : V \to \mathrm{A}(M)$,

$$[\![\varphi]\!]_M(\alpha) = [\![\varphi]\!]_N(f \circ \alpha).$$

En d'autres termes, pour toute formule $\varphi(x_1, \dots, x_n)$ et tout $a_1, \dots, a_n \in \mathrm{A}(M)$,

$$M \vDash \varphi(a_1, \dots, a_n) \text{ si et seulement si } N \vDash \varphi(f(a_1), \dots, f(a_n)).$$

Il suffit aussi de vérifier que, pour toute formule φ et toute $\alpha : V \to \mathrm{A}(M)$, si $M \vDash \varphi(\alpha)$ alors $N \vDash \varphi(f \circ \alpha)$.

Exemple 3.10. On considère la structure $Z = (\mathbb{Z}, +)$. Le plongement $f : Z \to Z$ tel que $f(x) = 2x$ n'est pas élémentaire :

$$Z \nvDash \exists x\, x + x = 1 \text{ alors que } Z \vDash \exists x\, x + x = f(1).$$

Cet exemple montre qu'un plongement entre structures élémentairement équivalentes (ici identiques) n'est pas toujours élémentaire.

Par contre, si $f : M \to N$ est élémentaire, alors $M \equiv N$.

C'est en général compliqué de prouver qu'un morphisme est élémentaire, à moins que ce soit un isomorphisme :

Proposition 3.11. *Soient M et N des structures. Tout isomorphisme $f : M \to N$ est élémentaire.*

Démonstration. On montre par récurrence sur φ que, pour tout $\alpha : V \to \mathrm{A}(M)$, $M \vDash \varphi(\alpha)$ si et seulement si $M \vDash \varphi(f \circ \alpha)$. Comme f est un plongement, d'après remarque 3.7, le seul nouveau cas à considérer est celui où φ est de la forme $\forall x\, \psi$. On a alors

$$\begin{aligned}
M \vDash (\forall x\, \psi)(\alpha) &\Leftrightarrow \text{pour tout } a \in \mathrm{A}(M),\ M \vDash \psi(\alpha_{x \mapsto a}) \\
&\Leftrightarrow \text{pour tout } a \in \mathrm{A}(M),\ M \vDash \psi((f \circ \alpha)_{x \mapsto f(a)}) \\
&\Leftrightarrow \text{pour tout } b \in \mathrm{A}(N),\ N \vDash \psi((f \circ \alpha)_{x \mapsto b}) \qquad \text{puisque } f \text{ est surjective} \\
&\Leftrightarrow N \vDash (\forall x\, \psi)(f \circ \alpha). \qquad \square
\end{aligned}$$

Remarque 3.12. Les ultraproduits fournissent un autre exemple de morphisme élémentaire. Soit M une structure, I un ensemble et $\mathfrak{U}$ un ultrafiltre sur I. On note $M^{\mathfrak{U}}$ l'ultraproduit $\prod_{i \to \mathfrak{U}} M$. Alors le morphisme diagonal $d : M \to M^{\mathfrak{U}}$ défini par $x \mapsto (x)_{i \in I}/\sim$ est élémentaire.

En effet, pour toute formule φ et tout $\alpha : V \to \mathrm{A}(M)$, par le théorème de Łoš (théorème 2.9), on a $M^{\mathfrak{U}} \vDash \varphi(d \circ \alpha)$ si et seulement si $X = \{i : M \vDash \varphi(\alpha)\} =\in \mathfrak{U}$. Si $M \vDash \varphi(\alpha)$, on a $X = I \in \mathfrak{U}$ et donc $M^{\mathfrak{U}} \vDash \varphi(d \circ \alpha)$, sinon, on a $X = \varnothing \notin \mathfrak{U}$ et donc $M^{\mathfrak{U}} \nvDash \varphi(d \circ \alpha)$.

On va maintenant considérer une caractérisation alternative des morphismes élémentaires (proposition 3.15). Cette caractérisation d'apparence plus simple est très utile, comme on le verra, dans les arguments abstraits. Cependant, dans la pratique, elle n'aide pas vraiment puisqu'il faut encore considérer toutes les formules. Commençons par introduire la notion de sous-structure.

Définition 3.13. Soit M une structure et soit $E \subseteq \mathrm{A}(M)$ non vide.

1. On dit que E est une sous-structure de M, ce qu'on note $E \leqslant M$ si, pour tout $F \in \mathfrak{F}_n$ et tout $a \in E^n$, $f(a) \in E$. Il existe alors une unique structure (induite par M) sur E qui fait de l'inclusion $E \to \mathrm{A}(M)$ un plongement.
2. Si ce plongement est élémentaire, on dit que E est une sous-structure élémentaire de M, ce qu'on note $E \preccurlyeq M$.

Une sous-structure $E \leqslant M$ est donc élémentaire si pour toute formule $\varphi(x_1, \dots, x_n)$ et tous $e_1, \dots, e_n \in E$,

$$M \vDash \varphi(e_1, \dots, e_n) \text{ si et seulement si } E \vDash \varphi(e_1, \dots, e_n).$$

Remarque 3.14. Un plongement $f : M \to N$ est élémentaire si et seulement si $f(\mathrm{A}(M)) \preccurlyeq N$. Comme, de plus, tout plongement est élémentaire sur son image par proposition 3.11, les plongements élémentaires sont exactement les composées d'une inclusion élémentaire et d'un isomorphisme.

Proposition 3.15 (Test de Tarski-Vaught)**.** *Soit M une structure et soit $E \subseteq \mathrm{A}(M)$ un ensemble. Si, pour toute formule $\varphi(x, y_1, \dots, y_n)$ et tous $e_1 \dots e_n \in E$ tels que $M \vDash \exists x\, \varphi(x, e_1, \dots, e_n)$, il existe $e \in E$ tel que $M \vDash \varphi(e, e_1, \dots, e_n)$, alors $E \preccurlyeq M$.*

Démonstration. Montrons tout d'abord que $E \leqslant M$. Soit $F \in \mathfrak{F}_n$ et $e \in E^n$. Comme $M \vDash \exists x\, f(e) = x$, par hypothèse, il existe $a \in E$ tel que $M \vDash f(e) = a$ et donc $f(e) = a \in E$. Notons aussi E la structure induite par M sur l'ensemble E.

Prouvons à présent, par récurrence sur φ que pour tout $\alpha : V \to E$, $M \vDash \varphi(\alpha)$ si et seulement si $E \vDash \varphi(\alpha)$. Comme l'inclusion $E \to \mathrm{A}(M)$ est un plongement, par la remarque 3.7, il reste à vérifier que, le cas où φ est de la forme $\exists x\, \psi$. On a alors,

$$\begin{aligned} M \vDash (\exists x\, \psi)(\alpha) &\Rightarrow \text{il existe } e \in E,\ M \vDash \psi(\alpha_{x \mapsto e}) && \text{par hypothèse} \\ &\Leftrightarrow \text{il existe } e \in E,\ E \vDash \psi(\alpha_{x \mapsto e}) && \text{par récurrence} \\ &\Leftrightarrow E \vDash (\exists x\, \psi)(\alpha). \end{aligned}$$

Ce qui conclut la preuve puisque la réciproque est claire : s'il existe un $e \in E$ tel que $M \vDash \psi(\alpha_{x \mapsto e})$ alors $M \vDash (\exists x\, \psi)(\alpha)$. □

Petit *a parte* sur la cardinalité. Étant donné deux ensembles X et Y, on dit que le cardinal de X est plus petit que le cardinal de Y s'il existe une injection de X dans Y. On dit que X et Y sont équipotents s'il existe une bijection entre X et Y.

D'après le théorème de Cantor-Bernstein, si le cardinal de X est plus petit que le cardinal de Y qui est lui-même plus petit que le cardinal de X, X et Y sont équipotents. C'est-à-dire que « avoir plus petite cardinalité » est une relation d'ordre sur les classes d'équipotences. Il découle de l'axiome du choix que cet ordre est total ; c'est-à-dire que l'on peut toujours comparer la cardinalité de deux ensembles. Il en découle aussi que la cardinalité de X est plus grande que la cardinalité de Y si et seulement s'il existe une surjection de X sur Y.

Pour tout ensemble X, on note $|X|$ sa classe d'équipotence, qu'on appelle aussi sa cardinalité. Un résultat important que l'on démontrera plus tard est que :

Fait 3.16. *Pour tout ensemble infini X est équipotent à son carré cartésien X^2.*

On en déduit alors que la cardinalité de d'une union $\bigcup_{i\in I} X_i$, où les X_i sont de même cardinalité, est inférieure au maximum de la cardinalité des X_i et de celle de I.

On peut alors vérifier que la cardinalité de l'ensemble des formules est égale au maximum de la cardinalité de $\mathfrak{L}$ (c'est-à-dire la cardinalité de l'union disjointe des ensembles $\mathfrak{F}_n$ et $\mathfrak{R}_n$) et de la cardinalité de V (que l'on a supposé dénombrable). En effet, le nombre d'arbres finis est dénombrable et à chaque formule on peut associer un arbre fini t (vu comme l'ensemble de ses noeuds dans l'arbre binaire infini $\{0,1\}^{\mathbb{N}}$) et une fonction de t — qui est un ensemble fini — vers $\mathfrak{L} \cup V \cup t$ — qui est un ensemble de cardinalité inférieure au maximum de celles de $\mathfrak{L}$ et V.

Théorème 3.17 (Lowenheim-Skolem descendant)**.** *Soit M une structure et soit $E \subseteq \mathrm{A}(M)$. Il existe $N \preccurlyeq M$ contenant E de cardinalité inférieure au maximum des cardinalités de $\mathfrak{L}$ et E et de la cardinalité dénombrable.*

Démonstration. On construit, par récurrence sur $i \in \mathbb{N}$, un ensemble $E_i \subseteq \mathrm{A}(M)$ contenant E et de cardinalité inférieure au maximum de la cardinalité de l'ensemble des formules et de celle de E.

On pose $E_0 = E$ et supposons E_i construit. Pour tout i, toute formule $\varphi(x, y_1, \dots, y_n)$ et $e = (e_i)_{i<n} \in E^n$ tels que $M \vDash \exists x\, \varphi(x, e_1, \dots, e_n)$, soit $a_{\varphi,e} \in \mathrm{A}(M)$ tel que $M \vDash \varphi(a, e_1, \dots, e_n)$. L'ensemble E_{i+1} est alors l'union de E_i et de l'ensemble des $a_{\varphi,e}$ tels qu'au-dessus. La cardinalité de E_{i+1} est donc inférieure à celle du produit de l'ensemble des formules et du $\bigcup_{n\geqslant 0} E_i^n$, qui est inférieure au maximum de celle de E_i et celle de l'ensemble des formules. Elle est donc bien inférieure au maximum de la cardinalité de l'ensemble des formules et de celle de E.

Soit $N = \bigcup_i E_i$ dont la cardinalité est aussi inférieure au maximum de la cardinalité de l'ensemble des formules et de celle de E. Par construction, N vérifie l'hypothèse du test de Tarski-Vaught (proposition 3.15). En effet, soit $\varphi(x, y_1, \dots, y_n)$ une formule et soient $e_1 \dots, e_n \in N$ tels que $M \vDash \exists y\, \varphi(y, e_1, \dots, e_n)$. Il existe un entier m tel que $e_i \in E_m$, pour tout $i \leqslant n$, et il existe donc $e \in E_{m+1} \subseteq N$ tel que $M \vDash \varphi(e, e_1, \dots, e_n)$. Il en découle que $N \preccurlyeq M$. □

Remarque 3.18.

1. D'après le théorème de Lowenheim-Skolem descendant (théorème 3.17), il existe une sous-structure élémentaire dénombrable de l'anneau ordonné $\mathbb{R}$, qui ne peut donc pas être complète. La théorie de l'anneau ordonné $\mathbb{R}$ n'implique donc pas la complétude.
2. De même, il existe une sous-structure élémentaire dénombrable de l'anneau $\mathbb{C}$. Sa théorie n'implique donc pas non plus la complétude.

Concluons cette section par la définition des sous-ensembles définissables d'une structure qui sont (plus que les structures ou leurs théories) l'objet principal d'étude de la théorie des modèles moderne.

Définition 3.19. Soit M une structure et $E \subseteq \mathrm{A}(M)$. Un sous-ensemble $X \subseteq \mathrm{A}(M)^n$ est dit définissable sur E s'il existe une formule $\varphi(x_1, \dots, x_n, y_1, \dots, y_m)$, et $a \in E^m$ tels que

$$X = \{b \in \mathrm{A}(M)^n : M \vDash \varphi(b_1, \dots, b_n, a_1, \dots, a_m)\} = \varphi(M, a).$$

Proposition 3.20. *Soit $f : M \to N$ un morphisme élémentaire. Soit $\varphi(x_1, \dots, x_n, y_1, \dots, y_m)$ une formule et soient $a_1, \dots, a_m \in \mathrm{A}(M)$. Le sous-ensemble définissable $\varphi(N, f(a))$ est l'unique sous-ensemble $Y \subseteq \mathrm{A}(N)^n$ définissable sur $f(\mathrm{A}(M))$ tel que*

$$f^{-1}(Y) = \varphi(M, a),$$

où on étend f à $\mathrm{A}(M)^n$ coordonnée par coordonnée.

Démonstration. Prouvons tout d'abord que $f^{-1}(\varphi(N, f(a))) = \varphi(M, a)$. Pour tous $b_1, \dots, b_n \in \mathrm{A}(M)$, $f(b) \in \varphi(N, f(a))$ si et seulement si $N \vDash \varphi(f(b), f(a))$, c'est-à-dire que, puisque f est élémentaire, $M \vDash \varphi(b, a)$, *i.e.* $b \in \varphi(M, a)$.

Soit maintenant Y définissable sur $f(\mathrm{A}(M))$ tel que $f^{-1}(Y) = \varphi(M, a)$. Par définition, il existe $\psi(x_1, \dots, x_n, z_1, \dots, z_r)$ et $c_1, \dots, c_r \in \mathrm{A}(M)$ tel que $Y = \psi(N, f(c))$. On a alors $\psi(M, c) = f^{-1}(Y) = \varphi(M, a)$, c'est-à-dire $M \vDash \forall x\, \psi(x, c) \leftrightarrow \varphi(x, a)$. Comme f est élémentaire, il s'ensuit que $N \vDash \forall x\, \psi(x, f(c)) \leftrightarrow \varphi(x, f(a))$, et donc $Y = \psi(N, f(c)) = \varphi(N, f(a))$. □

Remarque 3.21. Un sous-ensemble définissable de $\mathrm{A}(M)^n$ s'étend donc naturellement à toutes les extensions élémentaires de M. Plus précisément, à la formule $\varphi(x, y)$ et a, on associe un « foncteur des points » qui a tout morphisme élémentaire $f : M \to N$ associe le sous-ensemble définissable $\varphi(N, f(a))$.

Ce foncteur est entièrement déterminé par n'importe laquelle de ses images et il détermine $\varphi(x, a)$ à équivalence près.

3.2 Diagrammes

On rappelle qu'on a fixé un langage $\mathfrak{L}$ et un ensemble de variables V infini dénombrable.

Définition 3.22. Soit M une $\mathfrak{L}$-structure. On note $\mathfrak{L}(M)$ le langage obtenu en rajoutant à $\mathfrak{L}$ une nouvelle constante c_a (c'est-à-dire une fonction d'arité zéro) pour chaque élément $a \in \mathrm{A}(M)$. On munit M de sa $\mathfrak{L}(M)$-structure naturelle obtenue en interprétant c_a par a.

- Le diagramme élémentaire de M, noté $\mathcal{D}^{\mathrm{el}}(M)$ est la théorie de la $\mathfrak{L}(M)$-structure M. C'est-à-dire,
$$\mathcal{D}^{\mathrm{el}}(M) = \{\varphi(c_{a_1}, \dots, c_{a_n}) : M \vDash \varphi(a_1, \dots, a_n)\}.$$
- Le diagramme sans quantificateurs de M, noté $\mathcal{D}^{\mathrm{sq}}(M)$ est la théorie
$$\mathcal{D}^{\mathrm{sq}}(M) = \{\varphi(c_{a_1}, \dots, c_{a_n}) : \varphi \text{ sans quantificateurs et } M \vDash \varphi(a_1, \dots, a_n)\}.$$

Ces diagrammes caractérisent l'existence d'un morphisme élémentaire (respectivement d'un plongement) :

Proposition 3.23. *Soit N une $\mathfrak{L}$-structure.*

1. *Il existe un plongement $f : M \to N$ si et seulement s'il existe une $\mathfrak{L}(M)$-structure N_M sur $\mathrm{A}(N)$ qui étend N et telle que $N_M \vDash \mathcal{D}^{\mathrm{sq}}(M)$.*
2. *Il existe un morphisme élémentaire $f : M \to N$ si et seulement s'il existe une $\mathfrak{L}(M)$-structure N_M sur $\mathrm{A}(N)$ qui étend N et telle que $N_M \vDash \mathcal{D}^{\mathrm{el}}(M)$.*

Démonstration. Supposons tout d'abord qu'il existe une $\mathfrak{L}(M)$-structure N_M sur $\mathrm{A}(N)$ qui étend N et telle que $N_M \vDash \mathcal{D}^{\mathrm{sq}}(M)$. On définit alors, pour tout $a \in \mathrm{A}(M)$, $f(a) = c_a^{N_M} \in \mathrm{A}(N)$. On a alors, pour toute $\mathfrak{L}$-formule $\varphi(x_1, \dots, x_n)$ sans quantificateurs,

$$\begin{aligned} M \vDash \varphi(a_1, \dots, a_n) &\Leftrightarrow \varphi(c_{a_1}, \dots, c_{a_n}) \in \mathcal{D}^{\mathrm{sq}}(M) \\ &\Rightarrow N_M \vDash \varphi(c_{a_1}, \dots, c_{a_n}) \\ &\Leftrightarrow N \vDash \varphi(f(a_1), \dots, f(a_n)). \end{aligned}$$

On conclut alors que f est un plongement par la remarque 3.8. Si, de plus $N_M \vDash \mathcal{D}^{\mathrm{el}}(M)$, alors en considérant une $\mathfrak{L}$-formule φ quelconque, on montre comme ci-dessus que f est élémentaire.

Réciproquement, soit $f : M \to N$ un plongement. On enrichit N en une $\mathfrak{L}(M)$-structure N_M en posant $c_a^{N_M} = f(a)$. Pour toute formule $\varphi(c_{a_1}, \dots, c_{a_n}) \in \mathcal{D}^{\mathrm{sq}}(M)$, par définition $M \vDash \varphi(a_1, \dots, a_n)$ et, comme φ est sans quantificateurs, $N \vDash \varphi(f(a_1), \dots, f(a_n))$. Il s'ensuit que $N_M \vDash \varphi(c_{a_1}, \dots, c_{a_n})$ et donc $N_M \vDash \mathcal{D}^{\mathrm{sq}}(M)$.

Si le plongement f est élémentaire, on déduit de même que $N_M \vDash \mathcal{D}^{\mathrm{el}}(M)$. □

Théorème 3.24 (Lowenheim-Skolem ascendant)**.** *Soit M une structure infinie et X un ensemble infini de cardinalité plus grande que celles de $\mathfrak{L}$ et M. Alors il existe un plongement élémentaire $f : M \to N$ tel que N est équipotent à X.*

Ici, la cardinalité d'une structure M fait référence à celle de $\mathrm{A}(M)$.

Démonstration. Soit $\mathfrak{L}'$ le langage obtenu en rajoutant à $\mathfrak{L}(M)$ une nouvelle constante d_x pour tout élément $x \in X$. La $\mathfrak{L}'$-théorie $\mathcal{D}^{\mathrm{el}}(M) \cup \{c_x \neq c_y : x \neq y \in X\}$ est finiment consistante. En effet, pour toute partie finie $X_0 \subseteq X$, on peut construire une $\mathfrak{L}'$-structure M' qui étend M et qui est un modèle de $\mathcal{D}^{\mathrm{el}}(M) \cup \{c_x \neq c_y : x \neq y \in X_0\}$ en choisissant une injection $X_0 \to \mathrm{A}(M)$ et en posant $d_x^{M'} = f(x)$ pour tout $x \in X_0$ — en prenant $d_x^{M'}$ quelconque sinon.

Par compacité de la logique de premier ordre (théorème 2.11), il existe une $\mathfrak{L}'$-structure $\widehat{N}'$ qui est un modèle de $\mathcal{D}^{\mathrm{el}}(M) \cup \{c_x \neq c_y : x \neq y \in X\}$. Soit $\widehat{N}$ la $\mathfrak{L}$-structure sous-jacente. D'après la proposition 3.23, il existe un morphisme élémentaire $f : M \to \widehat{N}$.

Soit $g : X \to \mathrm{A}(\widehat{N})$ la fonction telle que $g(x) = d_x^{N'}$. Elle est injective par construction. Par le théorème de Lowenheim-Skolem descendant (théorème 3.17), il existe une sous-structure élémentaire $N \preccurlyeq \widehat{N}$, contenant $f(\mathrm{A}(M))$ et $g(X)$, de cardinalité inférieure à celle de X. Les ensembles $\mathrm{A}(N)$ et X sont alors équipotents.

Enfin, pour toute $\mathfrak{L}$-formule φ et toute $\alpha : V \to \mathrm{A}(M)$, $M \vDash \varphi(\alpha)$ si et seulement si $\widehat{N} \vDash \varphi(f \circ \alpha)$, ce qui est équivalent, puisque $f \circ \alpha : V \to \mathrm{A}(N)$, à $N \vDash \varphi(f \circ \alpha)$. Ceci montre que $f : M \to N$ est élémentaire. □

Corollaire 3.25. *Soit T une théorie qui admet un modèle infini. Elle admet un modèle de toute cardinalité infinie plus grande que celle de $\mathfrak{L}$.*

Démonstration. Soit $M \vDash T$ infini. Alors par le théorème 3.17 il existe une sous-structure élémentaire N de M, qui est donc aussi un modèle de T de cardinalité infinie inférieure à celle de $\mathfrak{L}$. Par le théorème 3.24, N se plonge élémentairement dans des structures, qui sont dont aussi des modèles de T, de tout cardinalité infinie plus grande celle de $\mathfrak{L}$. □

Exemple 3.26. Soit K un corps. On considére le langage $\mathfrak{L}_{K-\mathrm{ev}}$ qui contient une opération binaire $+$, une constante 0 et, pour tous $a \in K$, une fonction unaire λ_a (interprétée, dans les K-espaces vectoriels par la multiplication scalaire par a). Soient V et W deux K-espaces vectoriels infinis et $f : V \to W$ une application K-linéaire injective — *i.e.* un $\mathfrak{L}_{K-\mathrm{ev}}$-plongement.

Par le théorème de Lowenheim-Skolem ascendant (théorème 3.24), il existe des espaces vectoriels $V^\star$ et $W^\star$ de même cardinalité infinie strictement plus grande que celles de K et V et des morphismes élémentaires $g : V \to V^\star$ et $h : W \to W^\star$. Soit $V_0^\star$ un supplémentaire de $g(V)$ dans $V^\star$ et $W_0^\star$ un supplémentaire de $h(f(V))$ dans $W^\star$. Le cardinal d'une base de $V_0^\star$ est alors égal au cardinal de $V^\star$ qui est donc égal au cardinal d'une base de $W_0^\star$ et ces deux espaces vectoriels sont donc isomorphes. On en déduit un isomorphisme $l : V^\star = g(V) \oplus V_0^\star \to h(f(V)) \oplus W_0^\star$ tel que le diagramme

$$\begin{array}{ccc} V^\star & \xrightarrow{\ l\ } & W^\star \\ {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle h} \\ V & \xrightarrow{\ f\ } & W \end{array}$$

commute. Il s'ensuit que f est élémentaire. En particulier, V et W sont élémentairement équivalents et donc la théorie des K-espaces vectoriels infinis est complète.

En prenant $K = \mathbb{Q}$, on en déduit que les inclusions $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sont élémentaires, en tant que $\mathbb{Q}$-espaces vectoriels, mais donc aussi en tant que groupes additifs.

Concluons cette section par un résultat qui relie l'équivalence élémentaire à des morphismes élémentaires.

Proposition 3.27 (Plongement joint de A. Robinson)**.** *Soient M_1 et M_2 des structures. Elles sont élémentairement équivalentes si et seulement s'il existe une structure N et des plongements élémentaires $f_1 : M_1 \to N$ et $f_2 : M_2 \to N$.*

Démonstration. Si de tels plongements existent, on a bien $M_1 \equiv N \equiv M_2$, il reste donc à démontrer la réciproque. Supposons que $M_1 \equiv M_2$, d'après la proposition 3.23, il suffit de démontrer que la théorie $\mathcal{D}^{\mathrm{el}}(M_1) \cup \mathcal{D}^{\mathrm{el}}(M_2)$ est consistante — ici, et c'est très important, on considère que les constantes rajoutées dans $\mathfrak{L}(M_1)$ et $\mathfrak{L}(M_2)$ sont distinctes.

Si ce n'est pas le cas, d'après le théorème de compacité (théorème 2.11), il existe des $\mathfrak{L}(M_1)$-formules $\varphi_i \in \mathcal{D}^{\mathrm{el}}(M_1)$, pour $i \leqslant n$, et des $\mathfrak{L}(M_2)$-formules $\psi_j \in \mathcal{D}^{\mathrm{el}}(M_2)$, pour $j \leqslant m$, telles que $\{\varphi_i : i \leqslant n\} \cup \{\psi_j : j \leqslant m\}$ est inconsistante. Soit φ une $\mathfrak{L}(M_1)$-formule, soit $\psi(x_1, \dots, x_r)$ une $\mathfrak{L}$-formule et soient $a_1, \dots, a_r \in \mathrm{A}(M_2)$ tels que $\varphi = \bigwedge_{i \leqslant n} \varphi_i$ et $\psi(c_{a_1}, \dots, c_{a_r}) = \bigwedge_{j \leqslant m} \psi_j \in \mathcal{D}^{\mathrm{el}}(M_2)$. On a alors $\varphi \vDash \neg\psi(c_{a_1}, \dots, c_{a_r})$. Comme les constantes c_a, pour $a \in M_2$, n'apparaissent pas dans φ (qui est une $\mathfrak{L}(M_1)$-formule), il en découle que

$$\varphi \vDash \forall x_1 \dots \forall x_r \neg\psi.$$

En effet, Pour toute $\mathfrak{L}(M_1)$-structure N et toute $\alpha : V \to \mathrm{A}(N)$ telle que $N \vDash \varphi(\alpha)$, quitte à interpréter c_{a_i} comme $\alpha(x_i)$, on obtient une $\mathfrak{L}(M_1) \cup \mathfrak{L}(M_2)$-structure qui vérifie donc $\neg\psi(c_{a_1}, \dots, c_{a_r})$, c'est-à-dire $N \vDash \neg\psi(\alpha)$.

Comme $M_1 \vDash \varphi$, il en découle que $M_1 \vDash \forall x_1 \dots \forall x_r \neg\psi$, qui est une $\mathfrak{L}$-formule close. Comme $M_2 \equiv M_1$ en tant que $\mathfrak{L}$-structure, on a donc aussi $M_2 \vDash \forall x_1 \dots \forall x_r \neg\psi$ et donc

$M_2 \vDash \neg\psi(a_1, \dots, a_n)$, ce qui contredit que $\psi(c_{a_1}, \dots, c_{a_r}) \in \mathcal{D}^{\mathrm{el}}(M_2)$. On a donc montré que $\mathcal{D}^{\mathrm{el}}(M_1) \cup \mathcal{D}^{\mathrm{el}}(M_2)$ est consistante, ce qui conclut la preuve, par proposition 3.23. □

Remarque 3.28. Un théorème (beaucoup plus tardif) de Keisler et Shelah donne une forme plus « concrète » à N : il existe un ultrafiltre $\mathfrak{U}$ (qui ne dépend que la cardinalité de $\mathfrak{L}$) tel que $M_1 \equiv M_2$ si et seulement si $M_1^{\mathfrak{U}} \simeq M_2^{\mathfrak{U}}$ — on rappelle (remarque 3.12) que le plongement diagonal $M_i \to M_i^{\mathfrak{U}}$ est élémentaire.

3.3 Élimination des quantificateurs

Comme mentionné précédemment, prouver qu'un morphisme est élémentaire est souvent difficile. Une solution radicale à ce problème est de se restreindre aux théories telles que les plongements entre modèles sont toujours élémentaires (on parle alors de théorie modèle complète). Ces théories sont moins rares qu'on ne pourrait le croire.

Ici, on étudiera une propriété encore plus forte, l'élimination des quantificateurs. On rappelle qu'on a fixé un langage $\mathfrak{L}$ et un ensemble de variables V infini.

Définition 3.29. Soit T une théorie. Elle élimine les quantificateurs si pour toute formule $\varphi(x_1, \dots, x_n)$, il existe une formule sans quantificateurs $\psi(x_1, \dots, x_n)$ telle que

$$T \vDash \forall x_1 \dots \forall x_n \, \varphi \leftrightarrow \psi.$$

Remarque 3.30. Supposons que T élimine les quantificateurs.

- Tout plongement $f : M \to N$ entre modèles de T est élémentaire. Soit $\varphi(x_1, \dots, x_n)$ une formule et soient $a_1, \dots, a_n \in \mathrm{A}(M)$. Par élimination des quantificateurs, il existe une formule $\psi(x_1, \dots, x_n)$ sans quantificateurs telle que $T \vDash \forall x_1, \dots, x_n \, \varphi \leftrightarrow \psi$. On a donc

$$\begin{aligned} M \vDash \varphi(a_1, \dots, a_n) &\Leftrightarrow M \vDash \psi(a_1, \dots, a_n) \\ &\Leftrightarrow N \vDash \psi(f(a_1), \dots, f(a_n)) \\ &\Leftrightarrow N \vDash \varphi(f(a_1), \dots, f(a_n)). \end{aligned}$$

- Si le langage $\mathfrak{L}$ ne contient pas de constante, la théorie T est complète. En effet, toute formule close φ est équivalente à une formule close sans quantificateurs qui est donc, comme $\mathfrak{L}$ ne contient pas de constantes, une combinaison booléenne de $\bot$. Une telle formule est équivalente, soit à $\top$, en quel cas $T \vDash \varphi$, soit à $\bot$, en quel cas $T \vDash \neg\varphi$.

Proposition 3.31. *Soit T une théorie et soit $\varphi(x_1, \dots, x_n)$ une formule. Sont équivalents :*

1. *Il existe une formule $\psi(x_1, \dots, x_n)$ sans quantificateurs telle que*

$$T \vDash \forall x_1 \dots \forall x_n \, \varphi \leftrightarrow \psi;$$

2. *Pour tout $M, N \vDash T$, tous $a_1, \dots, a_n \in \mathrm{A}(M)$ et tous $b_1, \dots, b_n \in \mathrm{A}(N)$, si pour toute formule sans quantificateurs $\psi(x_1, \dots, x_n)$,*

$$M \vDash \psi(a_1, \dots, a_n) \textit{ implique } N \vDash \psi(b_1, \dots, b_n)$$

alors

$$M \vDash \varphi(a_1, \dots, a_n) \textit{ implique } N \vDash \varphi(b_1, \dots, b_n).$$

Au vu de la condition 2, il est naturel d'introduire la définition suivante :

Définition 3.32. Soit M, N des structures, soit $E \subseteq \mathrm{A}(M)$ (potentiellement vide). Une fonction $f : E \to \mathrm{A}(M)$ est un plongement de E dans N — on parle aussi de plongement partiel de M dans N de domaine E — si pour toute formule sans quantificateurs $\psi(x_1, \dots, x_n)$ et tous $e_1 \dots, e_n \in E$, on a

$$M \vDash \psi(e_1, \dots, e_n) \text{ si et seulement si } N \vDash \psi(f(e_1), \dots, f(e_n)).$$

Il suffit, de nouveau de vérifier l'implication.

Remarque 3.33. La condition 2 de la proposition 3.31 se réécrit alors :

2'. Pour tout $M, N \vDash T$, tout $E \subseteq \mathrm{A}(M)$, tout plongement $f : E \to N$ et tous $e_1, \dots, e_n \in E$,
$$M \vDash \varphi(e_1, \dots, e_n) \text{ implique } N \vDash \varphi(f(e_1), \dots, f(e_n)).$$

Preuve de la proposition 3.31. Si φ est équivalente (dans T) à une formule sans quantificateurs, alors la condition 2 est trivialement vérifiée. Réciproquement, supposons la condition 2. Soit $M \vDash T$ et soit $a \in \mathrm{A}(M)^n$ tel que $M \vDash \varphi(a)$. On définit $\Psi_a = \{\psi \text{ sans quantificateurs} : M \vDash \psi(a)\}$. La condition 2 exprime exactement que

$$T \cup \Psi_a \vDash \varphi.$$

Par compacité (théorème 2.11), il existe $\psi_1, \dots, \psi_m \in \Psi_a$ tel que $T \cup \{\psi_i : i \leqslant m\} \vDash \varphi(a)$, c'est-à-dire, en notant $\theta_a = \bigwedge_i \psi_i$, tel que $T \vDash \theta_a \to \varphi$.

L'ensemble $T \cup \{\varphi\} \cup \{\neg\theta_a : \text{il existe } M \vDash T \text{ et } a \in \mathrm{A}(M)^n \text{ tels que } M \vDash \varphi(a)\}$ est inconsistant. En effet, si $M \vDash T$ et $a \in \mathrm{A}(M)^n$ est tel que $M \vDash \varphi(a)$, alors, par construction, $M \vDash \theta_a(a)$. Par compacité (théorème 2.11), il existe des a_j, pour $j \leqslant r$, tels que $T \cup \{\varphi\} \cup \{\theta_{a_j} : j \leqslant r\}$ est inconstante. En notant $\theta = \bigvee_j \theta_{a_j}$, on a alors $T \vDash \varphi \to \theta$. Comme, pour tout j, $T \vDash \theta_{a_j} \to \varphi$, il en découle que $T \vDash \varphi \leftrightarrow \theta$, et donc $T \vDash \forall x_1 \dots \forall x_n \, \varphi \leftrightarrow \theta$, où θ est bien sans quantificateurs. □

Remarque 3.34.

- La preuve ci-dessus est la traduction d'une preuve purement topologique. Soit $\mathcal{S}_x(T)$ l'espace de Stone des formules à variables dans le uplet x à équivalence dans T près et soit $\mathcal{S}_x^{\mathrm{sq}}(T)$ l'espace de Stone de la sous-algèbre des formules sans quantificateurs. L'application naturelle $r : \mathcal{S}_x(T) \to \mathcal{S}_x^{\mathrm{sq}}(T)$ est continue surjective entre espaces compacts. La condition 2 exprime exactement que $r^{-1}(r([\varphi])) = [\varphi]$. L'ensemble $r([\varphi])$ est donc un ouvert fermé de $\mathcal{S}_x^{\mathrm{sq}}(T)$ qui est donc de la forme $[\psi]$ pour une certaine formule $\psi(x)$ sans quantificateurs.
- La proposition 3.31 est un cas particulier d'un résultat plus général où en remplace « sans quantificateurs » par « appartenant à un ensemble de formules Δ » où Δ est clos par $\wedge$ et $\vee$ (à équivalence dans T près).

Nous allons maintenant montrer notre principal outil pour prouver qu'une théorie élimine les quantificateurs.

Définition 3.35. Soit M une structure et $E \subseteq \mathrm{A}(M)$. On note $\mathfrak{L}(E)$ le langage obtenu en rajoutant à $\mathfrak{L}$ une nouvelle constante c_e pour tout élément de E. On note $\mathcal{D}_M^{\mathrm{sq}}(E)$ la théorie $\{\varphi(c_{e_1}, \dots, c_{e_n}) : \varphi \text{ sans quantificateurs et } M \vDash \varphi(e_1, \dots, e_n)\}$.

Théorème 3.36. *Soit T une théorie. Sont équivalents :*

1. *La théorie T élimine les quantificateurs;*
2. *pour tout $M \models T$ et tout $E \subseteq \mathrm{A}(M)$, la $\mathfrak{L}(E)$-théorie $T \cup \mathcal{D}^{\mathrm{sq}}_M(E)$ est complète;*
3. *Pour tous $M, N \models T$, tout $E \subseteq \mathrm{A}(M)$ et tout plongement $f : E \to N$ et tout $a \in \mathrm{A}(M)$, il existe une structure $N^\star$, un morphisme élémentaire $h : N \to N^\star$ et un plongement $g : E \cup \{a\} \to N^\star$ tels que $g|_E = h \circ f$, c'est-à-dire que le diagramme*

$$\begin{array}{ccc} E \cup \{a\} & \overset{g}{\dashrightarrow} & N^\star \\ \big| & & \uparrow h \\ E & \xrightarrow{\ f\ } & N \end{array}$$

   commute;
4. *Pour tous $M, N \models T$, tout $E \subseteq \mathrm{A}(M)$, tout plongement $f : E \to N$, toute formule $\varphi(y, x_1, \dots, x_n)$ sans quantificateurs, tous $e_1, \dots, e_n \in E$ et tout $a \in \mathrm{A}(M)$ tel que $M \models \varphi(a, e_1, \dots, e_n)$, il existe $b \in \mathrm{A}(N)$ tel que $N \models \varphi(b, f(e_1), \dots, f(e_n))$;*
5. *Pour toute formule sans quantificateurs $\varphi(y, x_1, \dots, x_n)$, il existe une formule sans quantificateurs $\psi(x_1, \dots, x_n)$ telle que*

$$T \models \forall x_1 \dots \forall x_n \, (\exists y \, \varphi) \leftrightarrow \psi.$$

Dans les conditions 2, 3 et 4, E peut être vide (et c'est très important pour que l'équivalence soit vérifiée).

Démonstration. Prouvons les implications suivantes $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 5 \Rightarrow 1$.

1 ⇒ 2 Supposons que T élimine les quantificateurs. Soit $\varphi(x_1, \dots, x_n)$ une $\mathfrak{L}$-formule et soient $e_1, \dots, e_n \in E$. Par élimination des quantificateurs, il existe une $\mathfrak{L}$-formule $\psi(x_1, \dots, x_n)$ telle que $T \models \varphi \leftrightarrow \psi$. Soit $N \models T \cup \mathcal{D}^{\mathrm{sq}}_M(E)$. On a $N \models \varphi(c_{e_1}, \dots, c_{e_n})$ si et seulement si $N \models \psi(c_{e_1}, \dots, c_{e_n})$, si et seulement si $\psi(c_{e_1}, \dots, c_{e_n}) \in \mathcal{D}^{\mathrm{sq}}_M(E)$. Comme cette dernière caractérisation ne dépend pas de N, la théorie $T \cup \mathcal{D}^{\mathrm{sq}}_M(E)$ est bien complète.

2⇒ 3 Soit $M, N \models T$, $E \subseteq \mathrm{A}(M)$ et $f : E \to N$ un plongement et supposons que la théorie $T \cup \mathcal{D}^{\mathrm{sq}}_M(E)$ est complète. Par définition, la $\mathfrak{L}(E)$-structure naturelle M_E qui étend M est un modèle de $T \cup \mathcal{D}^{\mathrm{sq}}_M(E)$. De même, en interprétant c_e par $f(e)$, pour tout $e \in E$, on munit N d'une $\mathfrak{L}(E)$-structure $N_E \models T \cup \mathcal{D}^{\mathrm{sq}}_M(E)$. Comme cette théorie est complète, par le théorème de plongement joint de Robinson (proposition 3.27), il existe une $\mathfrak{L}(E)$-structure $N^\star_E$ (de $\mathfrak{L}$-structure sous-jacente $N^\star$), un $\mathfrak{L}(E)$-morphisme élémentaire $h : N \to N^\star$ et un $\mathfrak{L}(E)$-plongement (élémentaire) $g : M \to N^\star$. Pour tout $e \in E$, on a alors

$$h(f(e)) = c_e^{N^\star_E} = g(e).$$

En particulier, h est $\mathfrak{L}$-élémentaire et $g|_{E \cup \{a\}}$ est un $\mathfrak{L}$-plongement et la condition 3 est vérifiée.

3⇒ 4 Soient M, N, E, f, φ, $e_1, \dots, e_n$ et a tels que dans la condition 4. D'après la condition 3, il existe un morphisme élémentaire $h : N \to N^\star$ et un plongement $g : E \cup \{a\} \to N^\star$ tel que $g|_E = h \circ f$. On a alors $N^\star \models \varphi(g(a), g(e_1), \dots, g(e_n))$ et donc $N^\star \models \exists y \, \varphi(y, h(f(e_1)), \dots, h(f(e_n)))$, d'où $N \models \exists y \, \varphi(y, f(e_1), \dots, f(e_n))$.

4⇒ 5 D'après la proposition 3.31, la condition 2 implique que, pour toute formule sans quantifcateurs $\varphi(y, x_1, \dots, x_n)$, la formule $\exists y\, \varphi$ est équivalente à une formule sans quantificateurs $\psi(x_1, \dots, x_n)$.

5⇒ 1 Supposons la condition 5 et montrons, par récurrence, que toute formule $\varphi(x_1, \dots, x_n)$ est équivalente à une formule sans quantificateurs $\psi(x_1, \dots, x_n)$ dans T. Si φ est atomique ou de la forme $\psi \to \theta$, on conclut immédiatement (par récurrence dans le dernier cas). Il reste donc à considérer le cas où φ est de la forme $\exists y\, \psi$. Par récurrence, $\psi(y, x_1, \dots, x_n)$ est équivalente dans T à une formule sans quantificateurs $\theta(y, x_1, \dots, x_n)$. La formule φ est donc équivalente à $\exists y\, \theta$ qui est équivalente à une formule sans quantificateurs, d'après la condition 5. □

Remarque 3.37. Il existe de nombreuses autres énoncés équivalents à l'élimination des quantificateurs.

- Dans les conditions 3 et 4, on peut supposer que E est fini. En effet, dans la condition 4, il suffit de considérer $E = \{e_1, \dots, e_n\}$, et la condition 3 avec E fini est un cas particulier qui suffit donc à prouver la condition 4.
- Comme on le voit dans la preuve de 2⇒ 3, dans la condition 3, on peut même, *a posteriori*, trouver un tel g défini sur tout M et qui plus est élémentaire.

Exemple 3.38. On reprend les notations de l'exemple 3.26. Soit V et W des espaces vectoriels et soit $E \subseteq V$. Tout plongement $f : E \to W$ induit une (unique) application K-linéaire injective $U \to W$. Soient $V^\star$ et $W^\star$ des extensions élémentaires de V et W respectivement de même grande cardinalité. On peut alors construire (exactement comme dans la exemple 3.26) un isomorphisme $V^\star \to W^\star$ qui étend f. On a donc montré que la condition 3 du théorème 3.36 est vérifiée pour la théorie des K-espaces vectoriels infinis. Cette théorie élimine donc les quantificateurs.

Exemple 3.39. On considère le langage des ordres $\mathfrak{L}_{\text{ord}}$ dont le seul symbole est un symbole relationnel binaire $<$. La théorie des ordres totaux denses sans extrémité est la théorie constituée des énoncés suivants :

$$\forall x \forall y \forall z\, (x < y \wedge y < z) \to x < z \qquad \text{(transitif)}$$
$$\forall x\, \neg x < x \qquad \text{(anti-réflexif)}$$
$$\forall x \forall y\, x < y \vee x = y \vee y < x \qquad \text{(total)}$$
$$\forall x \forall y\, x < y \to (\exists z\, x < z \wedge z < y) \qquad \text{(dense)}$$
$$\forall x \exists y \exists z\, x < y \wedge z < x \qquad \text{(sans extrémités)}$$

Par exemple $(\mathbb{Q}, <)$ et $(\mathbb{R}, <)$ sont des modèles de cette théorie.

La théorie des ordres denses sans extrémités élimine les quantificateurs. On va montrer la condition 2 du théorème 3.36. Soient M et N des modèles de cette théorie, soit $E \subseteq \mathrm{A}(M)$ fini, soit $f : E \to \mathrm{A}(N)$ croissante, soit $a \in \mathrm{A}(M)$ et soit $\varphi(x)$ une $\mathfrak{L}(E)$-formule sans quantificateurs telle que $M \vDash \varphi(a)$. On munit N de la $\mathfrak{L}(E)$-structure obtenue en interprétant c_e par $f(e)$ pour tout $e \in E$.

Si $a \in E$, alors $\vDash \varphi(f(a))$. On peut donc supposer $a \notin E$. Soit $g = \max\{e \in E : a \leqslant e\}$ (on pose $g = -\infty$ si cet ensemble est vide) et soit $d = \min\{e \in E : a \leqslant e\}$ (on pose $d = +\infty$

si cet ensemble est vide). La formule $c_g < x < c_d$ — avec les conventions évidentes si $g = -\infty$ ou $d = +\infty$ — implique (dans $T \cup \mathcal{D}^{\mathrm{sq}}(E)$) toutes les $\mathfrak{L}(E)$-formules atomiques et négations de $\mathfrak{L}(E)$-formules atomiques $\theta(x)$ qui sont vérifiés par a[10], elle implique donc toute $\mathfrak{L}(E)$-formule sans quantificateurs $\theta(x)$ qui est vérifié par a. En particulier, on a

$$T \cup \mathcal{D}^{\mathrm{sq}}_M(E) \vDash (c_g < x < c_d) \to \varphi(x).$$

Tout $b \in \mathrm{A}(N)$ tel que $f(g) < b < f(d)$ — qui existe puisque l'ordre est dense sans extrémités — vérifie alors $\varphi(x)$. Ce qui conclut la preuve de la condition 2.

On en déduit, par exemple, que l'inclusion $\mathbb{Q} \subseteq \mathbb{R}$ est élémentaire (en temps qu'ordre) et que, puisque le langage $\mathfrak{L}_{\mathrm{ord}}$ ne contient pas de constante, la théorie des ordres dense sans extrémités est complète — *cf.* remarque 3.30.

3.4 Corps algébriquement clos

On travaille dans cette section dans le langage $\mathfrak{L}_{\mathrm{ann}}$ des anneaux qui contient deux fonctions binaires + et ·, une fonction unaire − et deux constantes 0 et 1. On considère la théorie CAC des corps algébriquement clos qui contient la théorie des corps, et pour tout entier $n \geqslant 0$, la formule

$$\forall x_0 \dots \forall x_n \exists y \, y^{n+1} + \sum_{i \leqslant n} x_i y^i = 0.$$

Théorème 3.40 (Tarski). *La théorie des corps algébriquement clos élimine les quantificateurs.*

Démonstration. Montrons la condition 3 du théorème 3.36. Soient M et N des corps algébriquement clos, soit $E \subseteq \mathrm{A}(M)$, soit $f : E \to N$ un plongement et soit $a \in \mathrm{A}(M)$. Soit $E_0 \leqslant M$ le corps engendré par E. Le plongement f s'étend uniquement à E_0 en posant

$$f(P(e_1, \dots, e_n)/Q(e_1 \dots, e_n)) = P(f(e_1), \dots, f(e_n))/Q(f(e_1), \dots, f(e_n)),$$

où $P, Q \in \mathbb{Z}[x_1, \dots, x_n]$. Ce morphisme est bien défini puisque $P_1(e)/Q_1(e) = P_2(e)/Q_2(e)$ (où $e \in E^n$) si et seulement si $P_1(e)Q_2(e) = P_2(e)Q_1(e)$ qui est une formule sans quantificateurs et donc préservée par f. On peut donc supposer que $E = E_0 \leqslant M$ est un sous-corps.

Supposons qu'il existe un polynôme unitaire $P \in E[x]$ tel que $P(a) = 0$, que l'on peut supposer de degré minimal. Alors pour tout $Q \in E[x]$, $Q(a) = 0$ si et seulement si P divise Q. En effet, par division euclidienne $Q = SP + R$ où $\deg(R) < \deg(P)$. Comme $0 = Q(a) = S(a)P(a) + R(a) = R(a)$, par minimalité du degré de P, $R = 0$ et donc $Q = SP$. Soit $b \in \mathrm{A}(N)$ une racine $f(P) \in f(E)[x]$. On a alors $f(Q)(b) = 0$ si et seulement si $f(P)$ divisie $f(Q)$, si et seulement si P divise Q, si et seulement si $P(a) = 0$. Le morphisme d'anneau $E[a] \to N$ défini par $Q(a) \mapsto f(Q)(b)$ est donc bien défini et il étend f.

Supposons maintenant que pour tout polynôme non nul $P \in E[x]$, $P(a) \neq 0$. L'ensemble de formules $\mathcal{D}^{\mathrm{el}}(N) \cup \{P(x) \neq 0 : P \in f(E)[x] \text{ non nul}\}$ est finiment consistant puisque tout polynôme non nul à un nombre fini de racines et le corps N est infini puisque algébriquement clos. Il existe donc $h : N \to N^\star$ élémentaire et $b \in N^\star$ tel que $P(b) \neq 0$ pour tout $P \in f(E)[x]$. Le orphisme d'anneau $E[a] \to N$ défini par $P(a) \mapsto f(P)(b)$ est alors bien défini et il étend f. Ceci conclut la preuve de la condition 3 et donc de l'élimination des quantificateurs. □

[10] Un dessin aide!

Corollaire 3.41 (Chevalley). *Tout ensemble définissable dans un corps algébriquement clos est combinaison booléenne d'ensembles de zéro d'équations polynomiales (en plusieurs variables) — on parle d'ensembles constructibles.*

En particulier, si K est un corps algébriquement clos, si $X \subseteq K^n$ est constructible et si $f : K^n \to K^m$ est polynomiale, alors $f(X)$ est constructible.

Corollaire 3.42. *Les complétions de la théorie des corps algébriquement clos sont exactement les théories CAC_p des corps algébriquement clos de caractéristique p, pour p premier ou nul.*

Démonstration. À équivalence prés, les seuls énoncés sans quantificateurs dans CAC sont des combinaisons booléennes de formules de la forme $n = 0$ où $n \in \mathbb{Z}$. Si $M \models \mathrm{CAC}_0$, toutes ces formules sont équivalentes à $\bot$ si n est non nul. Si $M \models \mathrm{CAC}_p$, pour $p > 0$, cette formule est équivalente à $\top$ si p divise n et équivalente à $\bot$ sinon. Dans les deux cas, tous les énoncés sans quantificateurs sont équivalents à des combinaisons booléennes de $\bot$ (indépendamment du modèle de CAC_p choisi), c'est-à-dire à $\bot$ ou $\top$. Comme tous les énoncés sont équivalents à des énoncés sans quantificateurs (théorème 3.40), ces théories sont complètes. □

Remarque 3.43. Soit $K \models \mathrm{CAC}$. Soit $x = (x_i)_{i \leqslant n}$. On note $\mathcal{S}_x(K)$ l'espace de Stone de l'algèbre de Boole des $\mathfrak{L}_{\mathrm{ann}}(K)$-formules $\varphi(x)$. On a alors une bijection continue

$$\begin{array}{rcl} S_x(K) & \to & \{\text{idéaux premier } \mathfrak{p} \subseteq K[x]\} \\ p & \mapsto & \{P \in K[x] : p \models P = 0\} \end{array}$$

où l'ensemble à droite (le spectre de $K[x]$) est muni de la topologie de Zariski dont les fermés sont engendrés par les ensembles de la forme $[P] = \{\mathfrak{p} \subseteq K[x] : P \in \mathfrak{p}\}$. L'injectivité de cette application découle de l'élimination des quantificateurs (théorème 3.40).

Corollaire 3.44 (Nullstellensatz faible). *Soit K un corps algébriquement clos et soient $P_1 \ldots, P_m \in K[x_1, \ldots, x_n]$. Si l'idéal engendré par les P_i est propre, alors il existe $a \in K^n$ tel que $P_i(a) = 0$ pour tout $i \leqslant m$.*

Démonstration. Soit $\mathfrak{m} \subseteq K[x_1, \ldots, x_n]$ un idéal maximal qui contient l'idéal engendré par les P_i et soit $L = K[x]/\mathfrak{m}$. Soit c la classe de x dans L. On a $L \models \bigwedge_i P_i(c) = 0$. Si L^{a} une clôture algébrique de L, on a $L^{\mathrm{a}} \models \exists x \bigwedge_i P_i(c) = 0$. Par élimination des quantificateurs (théorème 3.40), l'inclusion $K \leqslant L^{\mathrm{a}}$ est élémentaire, et donc $K \models \exists x \bigwedge_i P_i(c) = 0$. □

Remarque 3.45. On peut raffiner un peu cet argument pour obtenir le Nullstellensatz fort. Soit $Q \in K[x]$ un polynôme qui s'annule sur le lieu des zéros communs des polynômes P_i. Pour tout idéal premier $\mathfrak{p}$ qui tous les P_i, soit L un corps algébriquement clos qui contient $K[x]/\mathfrak{p}$. On a $K \models \forall x \bigwedge_i P_i(x) = 0 \to Q(x) = 0$, d'où $L \models \forall x \bigwedge_i P_i(x) = 0 \to Q(x) = 0$ et donc $K[x]/\mathfrak{p} \models \forall x \bigwedge_i P_i(x) = 0 \to Q(x) = 0$. Soit c la classe de x dans $K[x]/\mathfrak{p}$. Comme $P_i \in \mathfrak{p}$, on a $P_i(c) = 0$, pour tout i, et donc $Q(c)$, c'est-à-dire, $Q \in \mathfrak{p}$.

On a montré que Q est dans tous les idéaux premiers qui contiennent les P_i et donc dans le radical de l'idéal engendré par les P_i.

Corollaire 3.46 (Principe de Lefshetz). *Soit φ un énoncé (du langage des anneaux). Sont équivalents :*

1. *Pour tout corps K algébriquement clos de caractéristique zéro $K \vDash \varphi$;*
2. *Il existe un corps K algébriquement clos de caractéristique zéro tel que $K \vDash \varphi$;*
3. *Il existe un entier $n > 0$ tel que tout corps algébriquement clos de caractéristique plus grande que n satisfait φ.*
4. *Il existe un ensemble infini de corps algébriquement clos de caractéristiques positives distinctes qui satisfont tous φ;*

Démonstration. L'équivalence entre les conditions 1 et 2 est une conséquence de la complétude de la théorie des corps algébriquement clos de caractéristique zéro (corollaire 3.42).

Si la condition 1 est vérifiée alors $\mathrm{CAC}_0 = \mathrm{CAC} \cup \{n \neq 0 : n > 0\} \vDash \varphi$. Par compacité (théorème 2.11), il existe m tel que $\mathrm{CAC} \cup \{n \neq 0 : n \geqslant m\} \vDash \varphi$. Donc pour tout $p \geqslant n$, $\mathrm{CAC}_p \vDash \varphi$ et la condition 3 est vérifiée.

Puisqu'il existe de modèles de CAC_p pour tout p premier, la condition 3 implique la condition 4.

Enfin, si la condition 1 n'est pas vérifiée, par complétude de CAC_0, $\mathrm{CAC}_0 \vDash \neg\varphi$ et donc (comme la condition 1 implique la condition 3), il existe un entier $m > 0$ tel que pour tout $p \geqslant m$, $\mathrm{CAC}_p \vDash \neg\varphi$. Les modèles de φ sont donc tous de caractéristique inférieure à m, ce qui contredit la condition 4. Ceci conclut la preuve. □

Théorème 3.47 (Ax). *Soit $f : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale injective. Alors f est surjective.*

Démonstration. Pour tout entiers n et d, soit $\varphi_{n,d}$ l'énoncé du langage des anneaux qui exprime que toute application polynomiale $K^n \to K^n$ de degré borné par d qui est injective est surjective.

Par le principe de Lefshetz (corollaire 3.46), pour montrer que $\mathbb{C} \vDash \varphi_{n,d}$, il suffit de le montrer dans la clôture algébrique $\mathbb{F}_p^{\mathrm{a}}$ de $\mathbb{F}_p$ pour tout premier p. Soit $f : (\mathbb{F}_p^{\mathrm{a}})^n \to (\mathbb{F}_p^{\mathrm{a}})^n$ polynomiale et $a \in (\mathbb{F}_p^{\mathrm{a}})^n$. Comme $\mathbb{F}_p^{\mathrm{a}} = \bigcup_n \mathbb{F}_{p^n}$, il existe un entier $m > 0$ tel que tous les coefficients de f et toutes les coordonnées de a sont dans $\mathbb{F}_{p^m}$. Alors $f(\mathbb{F}_{p^m}^n) \subseteq \mathbb{F}_{p^m}^n$ et comme f est injective sur le corps fini $\mathbb{F}_{p^m}^n$, elle est aussi surjective sur $\mathbb{F}_{p^m}^n$. Il s'ensuit que $a \in f(\mathbb{F}_{p^m}^n) \subseteq f((\mathbb{F}_p^{\mathrm{a}})^n)$ et f est bien surjective. □

4 Preuves formelles

4.1 Logique propositionnelle

On fixe V un ensemble de variables propositionnelles.

Définition 4.1. Un séquent est une paire de deux ensembles finis de formules Γ et Δ[11].

On dit que le séquent $\Gamma; \Delta$ est (universellement) valide — ce qu'on note $\Gamma \vDash_\vee \Delta$ — si, pour tout $\alpha : V \to \{0,1\}$, il existe $\varphi \in \Gamma$ tel que $[\![\varphi]\!](\alpha) = 0$ ou $\psi \in \Delta$ tel que $[\![\psi]\!](\alpha) = 1$ — en d'autres termes, $\inf_{\varphi\in\Gamma}[\![\varphi]\!](\alpha) \leqslant \sup_{\psi\in\Delta}[\![\psi]\!](\alpha)$[12], ou encore, si $\bigwedge_{\varphi\in\Gamma}\varphi$ est valide alors $\bigvee_{\psi\in\Delta}\psi$ est valide (pour α).

[11] Pour alléger les notations, étant donné $\Gamma \subseteq \mathfrak{F}$ et $\varphi \in \mathfrak{F}$, on notera Γ, φ l'ensemble $\Gamma \cup \{\varphi\}$. Pour éviter les confusions, on notera donc les séquents $\Gamma; \Delta$

[12] Avec la convention que $\inf(\varnothing) = 1$ et $\sup(\varnothing) = 0$

Définition 4.2. L'ensemble $\mathfrak{D}$ des séquents démontrables est le plus petit ensemble de séquents tel que, pour tous $\Gamma, \Delta \subseteq \mathfrak{F}(V)$ finis et tous $\varphi, \psi \in \mathfrak{F}(V)$:

- $\Gamma, \varphi; \Delta, \varphi$;
- Si $\Gamma; \Delta, \bot \in \mathfrak{D}$ alors $\Gamma; \Delta \in \mathfrak{D}$;
- Si $\Gamma, \varphi; \Delta, \psi \in \mathfrak{D}$ alors $\Gamma; \Delta, (\varphi \to \psi) \in \mathfrak{D}$;
- Si $\Gamma; \Delta, \varphi \to \psi \in \mathfrak{D}$ et $\Gamma; \Delta, \varphi$ alors $\Gamma; \Delta, \psi \in \mathfrak{D}$.

On note $\Gamma \vdash \Delta$ le fait que $\Gamma; \Delta$ est dénombrable.

Notation 4.3. Étant donné des ensembles de formule $\Gamma_{i \leqslant n}$, $\Delta_{i \leqslant n}$, Γ et Δ. On note :

$$\frac{\Gamma_1 \vdash \Delta_1 \qquad \cdots \qquad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

le fait que si les séquents $\Gamma_i; \Delta_i$, pour $i \leqslant n$, sont démontrables, le séquent $\Gamma; \Delta$ l'est aussi. On note aussi

$$\frac{\Gamma_1 \vdash \Delta_1 \quad \cdots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

le fait que les séquents $\Gamma_i; \Delta_i$, pour $i \leqslant n$, sont démontrables si et seulement si le séquent $\Gamma; \Delta$ l'est.

Les règles de démonstration données par la définition 4.1 sont donc les suivantes, pour tous $\Gamma, \Delta \subseteq \mathfrak{F}(V)$ et $\varphi, \psi \in \mathfrak{F}$:

$$\frac{}{\Gamma, \varphi \vdash \Delta, \varphi}\,\mathrm{I} \qquad \frac{\Gamma \vdash \Delta, \bot}{\Gamma \vdash \Delta}\,\mathrm{E}_\bot$$

$$\frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \to \psi}\,\mathrm{D}_\to \qquad \frac{\Gamma \vdash \Delta, \varphi \to \psi \qquad \Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \psi}\,\mathrm{E}_\to$$

On représentera aussi les enchaînements de règles qui montrent qu'un séquent est démontrable par des « arbres de preuve ». Par exemple :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(\varphi \to \bot) \to \bot \vdash \varphi, (\varphi \to \bot) \to \bot}\,\mathrm{I} \qquad \dfrac{\dfrac{}{(\varphi \to \bot) \to \bot, \varphi \vdash \varphi, \bot}\,\mathrm{I}}{(\varphi \to \bot) \to \bot \vdash \varphi, \varphi \to \bot}\,\mathrm{D}_\to}{(\varphi \to \bot) \to \bot \vdash \varphi, \bot}\,\mathrm{E}_\to}{(\varphi \to \bot) \to \bot \vdash \varphi}\,\mathrm{E}_\bot}{\vdash ((\varphi \to \bot) \to \bot) \to \varphi}\,\mathrm{D}_\to$$

La conclusion de cette preuve est une forme du tiers exclus qu'on on vient donc de démontrer dans notre système logique.

Montrons tout d'abord que nos règles de démonstration ne contredisent pas la sémantique que l'on s'est fixée :

Proposition 4.4. *Pour tous* $\Gamma, \Delta \subseteq \mathfrak{F}(V)$ *finis, si* $\Gamma \vdash \Delta$ *alors* $\Gamma \vDash_\vee \Delta$.

Démonstration. Par récurrence, il suffit de montrer que si les prémisses d'une des quatre règles sont valides, alors sa conclusion l'est aussi. Soit $\alpha : V \to \{0,1\}$. Pour I, comme φ apparaît des deux cotés, on a bien $\inf\{[\![\varphi]\!](\alpha), [\![\theta]\!](\alpha) : \theta \in \Gamma\} \leqslant [\![\varphi]\!](\alpha) \leqslant \sup\{[\![\varphi]\!](\alpha), [\![\chi]\!](\alpha) : \chi \in \Delta\}$. Pour $\mathrm{E}_\bot$, si $\Gamma \vDash_\vee \Delta, \bot$, puisque $[\![\bot]\!](\alpha) = 0$, soit $\inf_{\theta\in\Gamma}[\![\theta]\!](\alpha) = 0$, soit $\sup_{\chi\in\Delta}[\![\chi]\!](\alpha) = 1$ et donc $\Gamma \vDash_\vee \Delta$.

Pour $\mathrm{D}_\to$, si $\Gamma, \varphi \vDash_\vee \Delta, \psi$, alors, soit $\inf_{\theta\in\Gamma}[\![\theta]\!](\alpha) = 0$, soit $\sup_{\chi\in\Delta}[\![\chi]\!](\alpha) = 1$ — en quels cas $\Gamma \vDash_\vee \Delta$ et donc $\Gamma \vDash_\vee \Delta, \varphi \to \psi$ — $[\![\varphi]\!](\alpha) = 0$, soit $[\![\psi]\!](\alpha) = 1$ — en quels cas $[\![\varphi \to \psi]\!](\alpha) = 1$ et donc $\Gamma \vDash_\vee \Delta, \varphi \to \psi$.

Enfin, pour $\mathrm{E}_\to$, si $\Gamma \vDash_\vee \Delta, \varphi \to \psi$ et $\Gamma \vDash_\vee \Delta, \varphi$, mais que $\inf_{\theta\in\Gamma}[\![\theta]\!](\alpha) \neq 0$ et $\sup_{\chi\in\Delta}[\![\chi]\!](\alpha) \neq 1$, on a alors $[\![\varphi \to \psi]\!](\alpha) = 1$ — et donc $[\![\varphi]\!](\alpha) \leqslant [\![\psi]\!](\alpha)$ — et $[\![\varphi]\!](\alpha) = 1$. D'où $[\![\psi]\!](\alpha) = 1$ et $\Gamma \vDash_\vee \Delta, \psi$. □

On verra plus loin le fait remarquable que la réciproque est aussi vraie. Mais avant cela, nous allons introduire d'autres règles utiles qui découlent des quatre règles de base :

Proposition 4.5. *Pour tous $\Gamma, \Delta \subseteq \mathfrak{F}(V)$ finis et $\varphi, \psi \in \mathfrak{F}(V)$:*

$$\frac{\Gamma \vdash \Delta}{\Gamma, \varphi \vdash \Delta}\,\mathrm{AG} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi}\,\mathrm{AD} \qquad \frac{}{\Gamma, \bot \vdash \Delta}\,\mathrm{G}_\bot$$

$$\frac{\Gamma \vdash \Delta, \varphi \to \psi}{\Gamma, \varphi \vdash \Delta, \psi}\,{\uparrow}\mathrm{D}_\to \qquad \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta}\,\mathrm{C} \qquad \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \to \psi \vdash \Delta}\,\mathrm{G}_\to$$

De plus ces règles (et leurs réciproques, le cas échéant) préservent la validité des séquents.

Démonstration. Pour AG— et AD— on remarque tout d'abord que tout les quatre règles de base, si on rajoute un formule à Γ ou Δ, on obtient encore une instance de la même règle. L'ensemble des séquents $\Gamma; \Delta$ tels que $\Gamma, \varphi \vdash \Delta$ et $\Gamma \vdash \Delta, \varphi$ est donc préservé par toutes les règles et contient donc $\mathfrak{D}$. En d'autres termes, si $\Gamma \vdash \Delta$ alors $\Gamma, \varphi \vdash \Delta$ et $\Gamma \vdash \Delta, \varphi$.

De plus, si $\Gamma \vDash_\vee \Delta$, alors, pour tout $\alpha : V \to \{0,1\}$, $\inf_{\theta\in\Gamma}[\![\theta]\!](\alpha) \leqslant \sup_{\chi\in\Delta}[\![\chi]\!](\alpha)$. D'où

$$\inf\{[\![\varphi]\!](\alpha), [\![\theta]\!](\alpha) : \theta \in \Gamma\} \leqslant \sup_{\chi\in\Delta}[\![\chi]\!](\alpha)$$

et

$$\inf_{\theta\in\Gamma}[\![\theta]\!](\alpha) \leqslant \sup\{[\![\varphi]\!](\alpha), [\![\chi]\!](\alpha) : \chi \in \Delta\},$$

ce qui montre que les règles AG et AD préservent la validité des séquents.

Pour ce qui est des quatre autres règles, les déductions suivantes :

$$\frac{\dfrac{}{\Gamma, \bot \vdash \Delta, \bot}\,\mathrm{I}}{\Gamma, \bot \vdash \Delta}\,\mathrm{E}_\bot \qquad \frac{\dfrac{\dfrac{\Gamma \vdash \Delta, \varphi \to \psi}{\Gamma, \varphi \vdash \Delta, \varphi \to \psi}\,\mathrm{AG} \qquad \Gamma, \varphi \vdash \Delta, \varphi}{\Gamma, \varphi \vdash \Delta, \psi}\,\mathrm{E}_\to}{\Gamma \vdash \Delta, \varphi \to \psi}\,\mathrm{D}_\to \qquad \Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \bot}\,\mathrm{E}_\to$$

$$\frac{\dfrac{\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma, \varphi \vdash \Delta, \bot}\,\mathrm{AD}}{\Gamma \vdash \Delta, \varphi \to \bot}\,\mathrm{D}_\to \qquad \Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \bot}\,\mathrm{E}_\to}{\Gamma \vdash \Delta}\,\mathrm{E}_\bot$$

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \varphi \to \psi \vdash \Delta, \varphi \to \psi}\,\mathrm{I} \qquad \Gamma \vdash \Delta, \varphi}{\Gamma, \varphi \to \psi \vdash \Delta, \psi}\,\mathrm{E}_{\to} \qquad \dfrac{\Gamma, \psi \vdash \Delta}{\Gamma, \varphi \to \psi, \psi \vdash \Delta}\,\mathrm{AG}}{\Gamma, \varphi \to \psi \vdash \Delta}\,\mathrm{C}$$

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi, \psi}\,\mathrm{I}}{\Gamma \vdash \Delta, \varphi, \varphi \to \psi}\,\mathrm{D}_{\to} \qquad \dfrac{\Gamma, \varphi \to \psi \vdash \Delta}{\Gamma, \varphi \to \psi \vdash \Delta, \varphi}\,\mathrm{AD}}{\Gamma \vdash \Delta, \varphi}\,\mathrm{C}$$

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \psi, \varphi \vdash \Delta, \psi}\,\mathrm{I}}{\Gamma, \psi \vdash \Delta, \varphi \to \psi}\,\mathrm{D}_{\to} \qquad \dfrac{\Gamma, \varphi \to \psi \vdash \Delta}{\Gamma, \psi, \varphi \to \psi \vdash \Delta}\,\mathrm{AD}}{\Gamma, \psi \vdash \Delta}\,\mathrm{C}$$

permettent de conclure non seulement que ces règles préservent bien la démonstrabilité, mais aussi aussi qu'elles préservent la validitié puisque les 4 règles de base et les règles d'affaiblissement la préservent. □

On rappelle que pour toutes formules φ et ψ, on avait défini :

- $\neg\varphi = \varphi \to \bot$;
- $\top = \neg\bot$;
- $\varphi \vee \psi = (\neg\varphi) \to \psi$;
- $\varphi \wedge \psi = \neg(\varphi \to (\neg\psi))$.

Proposition 4.6. *Pour tous* $\Gamma, \Delta \subseteq \mathfrak{F}(V)$ *et* $\varphi, \psi \in \mathfrak{F}(V)$ *:*

$$\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}\,\mathrm{G}_{\neg} \qquad \dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}\,\mathrm{D}_{\neg} \qquad \dfrac{}{\Gamma \vdash \Delta, \top}\,\mathrm{D}_{\top}$$

$$\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}\,\mathrm{G}_{\vee} \qquad \dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}\,\mathrm{D}_{\vee}$$

$$\dfrac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}\,\mathrm{G}_{\wedge} \qquad \dfrac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}\,\mathrm{D}_{\wedge}$$

Démonstration. On a, par exemple :

$$\dfrac{\Gamma \vdash \Delta, \varphi \qquad \dfrac{}{\Gamma, \bot \vdash \Delta}\,\mathrm{G}_{\bot}}{\Gamma, \varphi \to \bot \vdash \Delta}\,\mathrm{G}_{\to} \qquad \dfrac{\dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma, \neg\varphi \vdash \Delta, \psi}\,\mathrm{G}_{\neg}}{\Gamma \vdash \Delta, (\neg\varphi) \to \psi}\,\mathrm{D}_{\to}$$

□

On voudrait à présent prouver que la réciproque de la proposition 4.4 est vraie :

Proposition 4.7. *Si* $\Gamma \vDash_{\vee} \Delta$ *alors* $\Gamma \vdash \Delta$.

Démonstration. On procède par récurrence sur le nombre de $\to$ qui apparaissent dans Γ et Δ. S'il n'y en a aucun alors Γ et Δ ne contiennent que des variables propositionnelles et la formule $\bot$. Si $\bot \in \Gamma$, alors $\Gamma \vdash \Delta$ par la règle $G_\bot$. Sinon, comme $\Gamma \vDash_V \Delta$ est valide, la même variable X apparaît à droite et à gauche — sinon, tout assignation qui vaut 1 sur (les variables qui composent) Γ et 0 sur (celles qui composent) Δ contredit sa validité. Mais on a alors $\Gamma \vdash \Delta$ par I.

Supposons maintnenant que Γ contienne une formule de la forme $\varphi \to \psi$ et soit $\Gamma_0 = \Gamma \setminus \{\varphi \to \psi\}$. Alors, $\Gamma_0 \vDash_V \Delta, \varphi$ et $\Gamma_0, \psi \vDash_V \Delta$. Cela suit soit d'un calcul explicite, soit de la proposition 4.5 qui montre que les réciproques de la règle $G_\to$ préserve la validité des séquents. Par récurrence, ces séquents (qui contiennent une $\to$ de moins) sont démontrables, et donc $\Gamma_0, \varphi \to \psi \vdash \Delta$ par la règle $G_\to$.

Supposons enfin que Δ contienne une formule de la forme $\varphi \to \psi$ et soit $\Delta_0 = \Delta \setminus \{\varphi \to \psi\}$. Par la proposition 4.5, on a $\Gamma, \varphi \vDash_V \Delta_0, \psi$ et ce séquent est donc démontrable par récurrence. On a donc aussi $\Gamma \vdash \Delta_0, \varphi \to \psi$ par la règle $D_\to$. □

Corollaire 4.8 (Complétude de la logique propositionnelle)**.** *Pour tous* $\Gamma, \Delta \subseteq \mathfrak{F}(V)$*,*

$$\Gamma \vdash \Delta \textit{ si et seulement si } \Gamma \vDash_V \Delta.$$

Corollaire 4.9 (Élimination des coupures pour la logique propositionnelle)**.** *Pour tous* $\Gamma, \Delta \subseteq \mathfrak{F}(V)$*, si* $\Gamma \vdash \Delta$*, ce séquent est démontrable en utilisant seulement les règles* I, $G_\bot$, $G_\to$ *et* $D_\to$*.*

Démonstration. On remarque que dans la preuve de la proposition 4.7, on a utilisé uniquement les règles I, $G_\bot$, $G_\to$ et $D_\to$. On a donc en fait démontré que si $\Gamma \vDash_V \Delta$ alors ce séquent est démontrable en utilisant uniquement les règles I, $G_\bot$, $G_\to$ et $D_\to$. Si $\Gamma \vdash \Delta$, on a donc, par la proposition 4.4, que $\Gamma \vDash_V \Delta$ et la remarque ci-dessus permet donc de conclure. □

Remarque 4.10. On peut alors revisiter la dualité de Stone pour l'algèbre de Boole des formules. Soit $\mathfrak{F}_\vdash(V)$ l'algèbre de Boole associée au préordre $\vdash$ sur $\mathfrak{F}(V)$. Le fait que ce soit une algèbre de Boole découle des règles de démonstration que l'on a introduites. Par exemple, la règle C est la transitivité de $\vdash$, la règle I est sa réflexivité. La règle $G_\wedge$ implique que $\varphi \wedge \psi$ est un minorant de φ et ψ et la règle $D_\wedge$ que c'est le plus grand minorant.

Le théorème de complétude peut alors se réinterpréter comme l'homéomorphisme :

$$\begin{array}{ccc} \mathcal{S}(\mathfrak{F}_\vdash(V)) & \simeq & 2^V \\ F & \mapsto & \mathbb{1}_{X \in F} \\ \text{filtre engendré par } \{X^{\alpha(X)} : X \in V\} & \leftarrow\!\shortmid & \alpha \end{array}$$

où $X^1 = X$ et $X^0 = \neg X$. C'est un homéomorphisme entre un objet syntactique à gauche et un objet sémantique à droite.

Pour être précis, l'homéomorphisme ci-dessus identifie les points de $[\varphi] \subseteq \mathcal{S}(\mathfrak{F}_\vdash(V))$ avec les assignations $\alpha \in 2^V$ telles que $[\![\varphi]\!]\alpha = 1$; ceci se vérifie par récurrence sur φ (voir la remarque 1.25). Il indique donc bien (entre autres choses) que si $\varphi \not\equiv \bot$, c'est-à-dire $[\varphi] \neq \varnothing$, alors il existe $\alpha \in 2^V$ telle que $[\![\varphi]\!]\alpha = 1$.

4.2 Logique du premier ordre

On fixe un langage $\mathfrak{L}$ et un ensemble V infini (dénombrable) de variables. Pour définir les preuves en logique du premier ordre, il nous faut (enfin) définir la substitution :

Définition 4.11. Soit t, s des termes et x une variable. On définit, par induction sur s la substitution $s(t/x)$ comme étant le terme obtenu en remplaçant toutes les occurrences de x dans (l'arbre encodant) s par (l'arbre encodant) le terme t.

Soit φ une formule, on définit aussi, la substitution $\varphi(t/x)$ comme étant la formule obtenue en remplaçant toutes les occurrences de x dans (le graphe encodant) φ par (l'arbre encodant) le terme t.

On a alors que
- $x(t/x)$ est égale à t ;
- $y(t/x)$ est égale à y, si $y \neq x$;
- $(Fs_1 \dots s_n)(t/x)$ est égale à $Fs_1(t/x) \dots s_n(t/x)$.
- $(s_1 = s_2)(t/x)$ est égale à $s_1(t/x) = s_2(t/x)$;
- $(Rs_1 \dots s_n)(t/x)$ est égale à $Rs_1(t/x) \dots s_n(t/x)$;
- $\bot(t/x)$ est égale à $\bot$;
- $(\psi_1 \to \psi_2)(t/x)$ est égale à $\psi_1(t/x) \to \psi_2(t/x)$;
- $(\forall x\, \psi)(t/x)$ est égale à $\forall x\, \psi$;
- $(\forall y\, \psi)(t/x)$ est égale à $\forall y\, \psi(t/x)$, si $y \neq x$ et y n'apparaît pas dans t.

On peut vérifier alors que la substitution est compatible à la substitution au sens suivant :

Lemme 4.12. *Pour toute structure M, toute assignation $\alpha : V \to \mathrm{A}(M)$, tout variable x, tous termes t et s et toute formule φ,*

$$[\![s(t/x)]\!]_M(\alpha) = [\![s]\!]_M(\alpha_{x \mapsto [\![t]\!]_M(\alpha)})$$

et

$$[\![\varphi(t/x)]\!]_M(\alpha) = [\![\varphi]\!]_M(\alpha_{x \mapsto [\![t]\!]_M(\alpha)}).$$

Démonstration. Ces égalités se prouvent par induction sur s, respectivement φ. Le cas subtil est celui du calcul de $[\![(\forall y\, \varphi)(t/x)]\!]_M(\alpha)$ si y est différent de x. Soit z un variable distincte de x qui n'apparaît pas dans t ni dans φ, alors $\forall y\, \varphi = \forall z\, \varphi(z/y)$. On a alors

$$\begin{aligned}
[\![(\forall y\, \varphi)(t/x)]\!]_M(\alpha) &= [\![(\forall z\, \varphi(z/y))(t/x)]\!]_M(\alpha) \\
&= [\![\forall z\, \varphi(z/y)(t/x)]\!]_M(\alpha) \\
&= \inf_{a \in \mathrm{A}(M)} [\![\varphi(z/y)(t/x)]\!]_M(\alpha_{z \mapsto a}) \\
&= \inf_{a \in \mathrm{A}(M)} [\![\varphi(z/y)]\!]_M(\alpha_{z \mapsto a, x \mapsto [\![t]\!]_M(\alpha_{z \mapsto a})}) \\
&= \inf_{a \in \mathrm{A}(M)} [\![\varphi(z/y)]\!]_M(\alpha_{x \mapsto [\![t]\!]_M(\alpha), z \mapsto a}) \\
&= [\![\forall z\, \varphi(z/y)]\!]_M(\alpha_{x \mapsto [\![t]\!]_M(\alpha)}) \\
&= [\![\forall y\, \varphi]\!]_M(\alpha_{x \mapsto [\![t]\!]_M(\alpha)})
\end{aligned}$$

L'avant-dernière égalité est due au fait que z n'apparaît pas dans t. □

Définition 4.13. La relation $(\Gamma;\Delta) \in \mathfrak{D}$ sur les paires d'ensembles finis de formules Γ et Δ est la plut petite relation telle que, pour tous ensembles finis de formules Γ et Δ, pour toutes formules φ et ψ, toute variable x (qui n'apparaît ni dans Γ ni dans Δ pour la règle $\mathrm{D}_\forall$) et pour tous termes t et s :

$$\frac{\Gamma \vdash \Delta}{\Gamma, \varphi \vdash \Delta}\,\mathrm{AG} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi}\,\mathrm{AD}$$

$$\frac{}{\Gamma, \varphi \vdash \Delta, \varphi}\,\mathrm{I} \qquad \frac{\Gamma \vdash \Delta, \bot}{\Gamma \vdash \Delta}\,\mathrm{E}_\bot$$

$$\frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \to \psi}\,\mathrm{D}_\to \qquad \frac{\Gamma \vdash \Delta, \varphi \to \psi \qquad \Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \psi}\,\mathrm{E}_\to$$

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \forall x\, \varphi}\,\mathrm{D}_\forall \qquad \frac{\Gamma \vdash \Delta, \forall x\, \varphi}{\Gamma \vdash \Delta, \varphi(t/x)}\,\mathrm{E}_\forall$$

$$\frac{}{\Gamma \vdash \Delta, t = t}\,\mathrm{D}_= \qquad \frac{\Gamma \vdash \Delta, t = s \qquad \Gamma \vdash \Delta, \varphi(t/x)}{\Gamma \vdash \Delta, \varphi(s/x)}\,\mathrm{E}_=$$

On écrit aussi $\Gamma \vDash_\vee \Delta$ si pour toute structure M et assignation $\alpha : V \to \mathrm{A}(M)$,

$$\inf_{\varphi\in\Gamma} [\![\varphi]\!]_M(\alpha) \leqslant \sup_{\psi\in\Delta} [\![\psi]\!]_M(\alpha).$$

Proposition 4.14. *Les règles ci-dessus préservent la validité des séquents : si les prémisses sont valides, les conclusions aussi. En particulier, pour tous ensembles finis de formules Γ et Δ,*

$$\Gamma \vdash \Delta \textit{ implique } \Gamma \vDash_\vee \Delta.$$

Démonstration. Pour les six premières règles, la preuve est la même que pour la logique propositionnelle. Considérons maintenant $\mathrm{D}_\forall$. Supposons donc que $\Gamma \vDash_\vee \Delta, \varphi$ et soit M une structure et $\alpha : V \to \mathrm{A}(M)$ une assignation. Si $\inf_{\theta\in\Gamma} [\![\theta]\!]_M(\alpha) = 0$ ou $\sup_{\chi\in\Delta} [\![\chi]\!](\alpha) = 1$, alors $\Gamma \vDash_\vee \Delta, \forall x\, \varphi$. Sinon, on doit avoir $[\![\varphi]\!]_M = 1$. De plus, comme x n'apparaît ni dans Γ ni dans Δ, pour tout $a \in M$, $\inf_{\theta\in\Gamma} [\![\theta]\!]_M(\alpha_{x\mapsto a}) = \inf_{\theta\in\Gamma} [\![\theta]\!]_M(\alpha) = 0$ et $\sup_{\chi\in\Delta} [\![\chi]\!](\alpha_{x\mapsto a}) = \sup_{\chi\in\Delta} [\![\chi]\!](\alpha) = 1$. On a donc aussi $[\![\varphi]\!]_M(\alpha_{x\mapsto a}) = 1$ et donc $[\![\forall x\, \varphi]\!]_M(\alpha) = 1$.

On considère maintenant $\mathrm{E}_\forall$ et supposons que $\Gamma \vDash_\vee \Delta, \forall x\, \varphi$, que $\inf_{\theta\in\Gamma} [\![\theta]\!]_M(\alpha) = 1$ et que $\sup_{\chi\in\Delta} [\![\chi]\!](\alpha) = 0$. On a donc $[\![\forall x\, \varphi]\!]_M(\alpha) = 1$ et donc, $[\![\varphi(t/x)]\!]_M(\alpha) = [\![\varphi]\!]_M(\alpha_{x\mapsto [\![t]\!]_M(\alpha)}) = 1$.

Pour ce qui est de $\mathrm{D}_=$, comme $[\![t = t]\!]_M(\alpha) = 1$, on a bien $\Gamma \vDash_\vee \Delta, t = t$. Il reste donc à considérer $\mathrm{E}_=$. Supposons donc que $\Gamma \vDash_\vee \Delta, t = s$, que $\Gamma \vDash_\vee \Delta, \varphi(t/x)$, que $\inf_{\theta\in\Gamma} [\![\theta]\!]_M(\alpha) = 1$ et que $\sup_{\chi\in\Delta} [\![\chi]\!](\alpha) = 0$. On a donc $[\![t = s]\!]_M(\alpha) = 1$ — et donc $[\![t]\!]_M(\alpha) = [\![s]\!]_M(\alpha)$ — et $[\![\varphi(t/x)]\!]_M(\alpha) = 1$. On a alors

$$\begin{aligned}
[\![\varphi(s/x)]\!]_M(\alpha) &= [\![\varphi]\!]_M(\alpha_{x\mapsto [\![s]\!]_M(\alpha)}) \\
&= [\![\varphi]\!]_M(\alpha_{x\mapsto [\![t]\!]_M(\alpha)}) \\
&= [\![\varphi(t/x)]\!]_M(\alpha) \\
&= 1.
\end{aligned}$$

□

Les règles supplémentaires introduites en logique propositionelle (proposition 4.5) restent vérifiées. Mais on peut aussi en introduire de nouvelles en lien avec la quantification universelle et l'égalité :

Proposition 4.15. *Pour tous ensembles finis de formules Γ et Δ, toutes formules φ et ψ, toute variable x, tout symbole de fonction F et tout symbole de relation R d'arité n et tous termes t, s, t_i et s_i, pour $i \leqslant n$:*

$$\frac{\Gamma \vdash \Delta, \forall x\, \varphi}{\Gamma \vdash \Delta, \varphi}\ {\uparrow}\mathrm{D}_\forall \qquad \frac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, \forall x\, \varphi \vdash \Delta}\ \mathrm{G}_\forall$$

$$\frac{\Gamma \vdash \Delta, t = s}{\Gamma \vdash \Delta, s = t}\ \mathrm{S}_= \qquad \frac{\Gamma \vdash \Delta, t = s \qquad \Gamma \vdash \Delta, s = u}{\Gamma \vdash \Delta, t = u}\ \mathrm{T}_=$$

$$\frac{\Gamma \vdash \Delta, t_1 = s_1 \qquad \cdots \qquad \Gamma \vdash \Delta, t_n = s_n}{\Gamma \vdash \Delta, Ft_1 \dots t_n = Fs_1 \dots s_n}\ \mathrm{F}_=$$

$$\frac{\Gamma \vdash \Delta, t_1 = s_1 \qquad \cdots \qquad \Gamma \vdash \Delta, t_n = s_n \qquad \Gamma \vdash \Delta, Rt_1 \dots t_n}{\Gamma \vdash \Delta, Rs_1 \dots s_n}\ \mathrm{R}_=$$

Démonstration. La règle ${\uparrow}\mathrm{D}_\forall$ est un cas particulier de $\mathrm{E}_\forall$. Pour la règle $\mathrm{G}_\forall$, on a

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \forall x\, \varphi \vdash \Delta, \forall x\, \varphi}\ \mathrm{I}}{\Gamma, \forall x\, \varphi \vdash \Delta, \varphi(t/x)}\ \mathrm{E}_\forall \qquad \dfrac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, \forall x\, \varphi, \varphi(t/x) \vdash \Delta}\ \mathrm{AG}}{\Gamma, \forall x\, \varphi \vdash \Delta}\ \mathrm{C}$$

Pour la règle $\mathrm{S}_=$, on remplace t par s dans $(x = t)(t/x)$ avec la règle $\mathrm{E}_=$. Pour $\mathrm{T}_=$, on remplace s par u dans $(t = x)(s/x)$. De même, $\mathrm{F}_=$ et $\mathrm{R}_=$ se montrent en itérant $\mathrm{E}_=$ pour remplacer certains des t_i par des s_i dans les formules $Ft_1 \dots t_n = Ft_1 \dots t_n$ et $Rt_1 \dots t_n$. □

Les règles pour la négation, la conjonction, la disjonction et le vrai (proposition 4.6) restent valides mais on aussi les règles suivantes pour le quantificateur existentiel. On rappele que, par définition, $\exists x\, \varphi = \neg \forall x\, \neg \varphi$.

Proposition 4.16. *Pour tous ensembles finis de formules Γ et Δ, toutes formules φ et ψ, toute variable x (qui n'est libre ni dans Γ ni dans Δ pour la règle $G_\exists$) et tout terme t,*

$$\frac{\Gamma, \varphi \vdash \Delta}{\Gamma, \exists x\, \varphi \vdash \Delta}\ G_\exists \qquad \frac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma \vdash \Delta, \exists x\, \varphi}\ D_\exists$$

Démonstration. Cela résulte des preuves suivantes :

$$\dfrac{\dfrac{\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg \varphi}\ \mathrm{D}_\neg}{\Gamma \vdash \Delta, \forall x\, \neg \varphi}\ \mathrm{D}_\forall}{\Gamma, \neg \forall x\, \neg \varphi \vdash \Delta}\ \mathrm{G}_\neg \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma, \neg \varphi(t/x) \vdash \Delta}\ \mathrm{G}_\neg}{\Gamma, \forall x\, \neg \varphi \vdash \Delta}\ \mathrm{G}_\forall}{\Gamma \vdash \Delta, \neg \forall x\, \neg \varphi}\ \mathrm{D}_\neg$$

□

On peut alors vérifier que $\mathfrak{F}^{\mathfrak{L}}_{\vdash}(V) := (\mathfrak{F}^{\mathfrak{L}}(V)/\equiv, \vdash)$ est une algèbre de Boole. De plus, elle garde une trace des quantificateurs :

Lemme 4.17. *Pour toute formule φ et toute variable x,*

$$\forall x\, \varphi = \inf_{t \in \mathfrak{T}^{\mathfrak{L}}(V)} \varphi(t/x).$$

Démonstration. Par la règle $\mathrm{E}_\forall$, $\forall x \varphi \vdash \varphi(t/x)$ pour tout terme t. Il reste donc à vérifier que c'est un plus grand minorant. Soit donc ψ telle que $\psi \vdash \varphi(t/x)$ pour tout terme t. Soit y une variable qui n'apparaît ni dans φ, ni dans ψ. Comme $\psi \vdash \varphi(y/x)$, par $\mathrm{D}_\forall$, on a $\psi \vdash \forall y\, \varphi(y/x)$ et cette dernière formule est égal à $\forall x\, \varphi$. Ce qui conclut la preuve que c'est un plus grand minorant. □

Définition 4.18. Un ultrafiltre $\mathfrak{U}$ sur $\mathfrak{F}^{\mathfrak{L}}_{\vdash}(V)$ est $\forall$-complet, si pour toute formule φ et toute variable x telle que, pour tout terme t, $\varphi(t/x) \in \mathfrak{U}$, on a $\forall x\, \varphi \in \mathfrak{U}$.

On remarque que, puisque $\forall x\, \varphi \vdash \varphi(t/x)$, par la règle $\mathrm{G}_\forall$, la réciproque est toujours vraie.

Soit $\mathfrak{U}$ un ultrafiltre $\forall$-complet. On définit la relation $\simeq$ sur l'ensemble $\mathfrak{T}^{\mathcal{L}}(V)$ des termes par $t \simeq s$ si $t = s \in \mathfrak{U}$. C'est une relation d'équivalence. Soit $\mathrm{A}(M) = \mathfrak{T}^{\mathcal{L}}(V)/\simeq$. On en fait une $\mathcal{L}$-structure en posant, pour toute fonction F et relation R d'arité n :

$$F^M(t_1/\simeq, \dots, t_n/\simeq) = (Ft_1 \dots t_n)/\simeq$$

et

$$(t_1/\simeq, \dots, t_n/\simeq) \in R^M \text{ si } Rt_1 \dots t_n \in \mathfrak{U}.$$

Ces interprétations sont bien définies par les règles $\mathrm{F}_=$ et $\mathrm{R}_=$.

Proposition 4.19. *Soit $\alpha : V \to \mathrm{A}(M)$ telle que, pour tout $x \in V$, $\alpha(x) = x/\simeq$. Pour toute formule φ,*

$$M \vDash \varphi(\alpha) \textit{ si et seulement si } \varphi \in \mathfrak{U}.$$

Démonstration. On prouve d'abord par induction sur les termes t que $[\![t]\!]_M(\alpha) = t/\simeq$. On prouve ensuite la proposition par induction sur les formules.

Le cas nouveau est celui des formules de la forme $\forall x\, \varphi$. Si $M \vDash \forall x\, \varphi(\alpha)$, alors pour tout terme t, d'après le lemme 4.12, on a $[\![\varphi(t/x)]\!]_M(\alpha) = [\![\varphi]\!]_M(\alpha_{x \mapsto t/\simeq}) = 1$. Par induction, on a donc $\varphi(t/x) \in \mathfrak{U}$. Comme $\mathfrak{U}$ est $\forall$-complet, on a donc $\forall x\, \varphi \in \mathfrak{U}$.

Réciproquement, supposons que $\forall x\, \varphi \in \mathfrak{U}$ et fixons un terme t. Alors, comme $\forall x\, \varphi \vdash \varphi(t/x)$, on a $\varphi(t/x) \in \mathfrak{U}$. Par induction, on a donc $[\![\varphi]\!]_M(\alpha_{x \mapsto t/\simeq}) = [\![\varphi(t/x)]\!]_M(\alpha) = 1$ et donc $M \vDash \forall x\, \varphi$. □

Proposition 4.20. *Supposons que le langage $\mathcal{L}$ est dénombrable. L'ensemble des ultrafiltres $\forall$-complets dans $\mathcal{S}(\mathfrak{F}^{\mathfrak{L}}_{\vdash}(V))$ est alors une intersection dénombrable d'ouverts denses.*

Démonstration. Un ultrafiltre $\mathfrak{U}$ n'est pas $\forall$-complet s'il existe une formule φ et une variable x telle que $\mathfrak{U}$ est dans l'ensemble :

$$X_\varphi = \bigcap_t [\varphi(t/x)] \setminus [\forall x\, \varphi].$$

Comme l'ensemble des formules est dénombrable, il suffit donc de démontrer que l'ensemble X_φ est fermé d'intérieur vide. Comme les $[\varphi(t/x)]$ sont fermés et que $[\forall x\, \varphi]$ est ouvert, il est bien fermé. Considérons maintenant une formule ψ telle que $[\psi] \subseteq X_\varphi$. Pour tout terme t, on a $[\psi] \subseteq [\varphi(t/x)]$ et donc $\psi \vdash \varphi(t/x)$. Il découle donc du lemme 4.17, que $\psi \vdash \forall x\, \varphi$. Mais comme $[\psi] \cap [\forall x\, \varphi] = \varnothing$, on doit avoir $[\psi] = \varnothing$. L'ensemble X_φ est donc bien d'intérieur vide. □

Proposition 4.21 (Baire–Čech)**.** *Soit X un espace compact (séparé). Toute intersection dénombrable d'ouverts denses de X est dense dans X.*

Démonstration. Soit $F \subseteq X$ un fermé et soit $x \in X \setminus F$. Pour tout $y \in F$, puisque X est séparé, il existe U_y et V_y ouverts disjoints tels que $x \in U_y$ et $y \in V_y$. On a alors $X = (X \setminus F) \cup \bigcup_y V_y$, un recouvrement ouvert. Par compacité, il existe $y_1, \dots, y_n$ tels que $F \subseteq \bigcup_{i \leqslant n} V_{y_i}$. Soit $V = \bigcup_i V_{y_i}$ et $U = \bigcap_i U_{y_i}$. Ce sont des ouverts disjoints, et on a $x \in U$ et $F \subseteq V$. En particulier, on a $x \in \overline{U} \subseteq X \setminus V \subseteq X \setminus F$.

Revenons à la preuve de la proposition. Soient $(U_i)_{i \geqslant 0}$ des ouverts denses de X et soit $U \subseteq X$ un ouvert. Comme U_0 est dense, il existe $x_0 \in U_0 \cap U \neq \varnothing$. Par le paragraphe précédent, il existe un ouvert $V_0 \subseteq X$ tel que $x \in V_0 \subseteq \overline{V}_0 \subseteq U_0 \cap U$. Par récurrence, on construit de même $x_{i+1} \in U_{i+1} \cap V_i$ et $V_{i+1} \subseteq X$ ouvert tel que $x_{i+1} \in V_{i+1} \subseteq \overline{V}_{i+1} \subseteq U_{i+1} \cap V_i$.

Les $\overline{V}_i$ forment une suite décroissante de fermés non vide. Par compacité, il existe $x \in \bigcap_{i \geqslant 0} \overline{V}_i \subseteq \bigcap_i U_i \cap U$. L'ensemble $\bigcap_i U_i$ est donc bien dense dans X. □

Théorème 4.22. *Pour toute formule φ si $\varphi \nvdash \bot$, il existe une structure M et une assignation $\alpha : V \to \mathrm{A}(M)$ telle que*

$$M \vDash \varphi(\alpha).$$

Démonstration. Supposons tout d'abord que $\mathcal{L}$ est dénombrable. Par la proposition 4.20, l'ensemble des ultrafiltres $\forall$-complets dans $\mathcal{S}(\mathfrak{F}^{\mathfrak{L}}_{\vdash}(V))$ est alors une intersection dénombrable d'ouverts denses. Par la proposition 4.21, il existe donc un ultrafiltre $\mathfrak{U}$ dans $[\varphi]$ qui soit $\forall$-complet. Soit M et α tels que dans la proposition 4.19. Comme $\varphi \in \mathfrak{U}$, a alors $M \vDash \varphi(\alpha)$.

En général, soit $\mathcal{L}_0 \subseteq \mathcal{L}$ un langage dénombrable qui contient tous les symboles qui apparaissent dans φ. Comme toute preuve dans $\mathcal{L}_0$ est une preuve dans $\mathcal{L}$, on n'a pas non plus $\varphi \vdash \bot$ dans $\mathcal{L}_0$, et donc, par le cas précédent, on trouve une $\mathcal{L}_0$-structure M_0 et une assignation $\alpha : V \to \mathrm{A}(M_0)$ telle que $M_0 \vDash \varphi(\alpha)$. Soit M une $\mathcal{L}$-structure d'ensemble de base $\mathrm{A}(M_0)$ et dans laquelle les interprétations des symboles de $\mathcal{L}_0$ coïncident avec celles de M_0 — une telle structure existe toujours en choisissant les interprétations des symboles de $\mathcal{L} \setminus \mathcal{L}_0$ de manière arbitraire. Comme les seuls symboles qui apparaissent dans φ sont dans $\mathcal{L}_0$, on a toujours $M \vDash \varphi(\alpha)$. □

Corollaire 4.23 (Complétude de la logique du premier ordre)**.** *Pour tous ensembles finis de formules Γ et Δ,*

$$\Gamma \vdash \Delta \textit{ si et seulement si } \Gamma \vDash_\vee \Delta.$$

Démonstration. Au vue de la proposition 4.14, il reste à montrer que si $\Gamma \vDash_\vee \Delta$ alors $\Gamma \vdash \Delta$. Si $\Gamma \vDash_\vee \Delta$, alors $\bigwedge_{\varphi \in \Gamma} \varphi \wedge \bigwedge_{\psi \in \Delta} \neg\psi$ est inconsistante. Par le théorème 4.22, $\bigwedge_{\varphi \in \Gamma} \varphi \wedge \bigwedge_{\psi \in \Delta} \neg\psi \vdash \bot$ et donc $\Gamma \vdash \Delta$ par les règles $\mathrm{E}_\bot$, $\uparrow\mathrm{G}_\wedge$ et $\uparrow\mathrm{G}_\neg$. □

5 Arithmétique de Peano

5.1 Formules Σ_1

Soit $\mathfrak{L}_{\mathrm{ar}}$ le langage contenant une constant 0, un symbole fonctionnel unaire S, deux symboles fonctionnels binaire $+$ et $\cdot$. On souhaite comprendre la théorie de la structure $(\mathbb{N}, 0, S, +, \cdot)$, que l'on notera $\mathbb{N}_{\mathrm{st}}$.

Définition 5.1. On note PA_0 la théorie (appelée arithmétique de Robinson) :
- $\forall x\, Sx \neq 0$;
- $\forall x\, x \neq 0 \to (\exists y\, Sy = x)$;
- $\forall x \forall y\, Sx = Sy \to x = y$;
- $\forall x\, x + 0 = x$;
- $\forall x \forall y\, x + S(y) = S(x + y)$;
- $\forall x\, x \cdot 0 = 0$;
- $\forall x \forall y\, x \cdot S(y) = x \cdot y + x$;

On note PA la théorie (appellée arithmétique de Peano) obtenue en ajoutant à PA_0 le principe de récurrence suivant :
- Pour toute formule $\varphi(x, y)$, où y est le uple de variables $y_1, \ldots, y_n$,

$$\forall y\ (\varphi(0, y) \wedge (\forall x\, \varphi(x, y) \to \varphi(S(x), y))) \to \forall x\, \varphi(x, y).$$

On note $x \leqslant y$ la formule $\exists z\, z + x = y$. Si $+$ est associatif, c'est un ordre.

Remarque 5.2.
1. On a $\mathbb{N}_{\mathrm{st}} \vDash \mathrm{PA}$.
2. Il existe des modèles de PA_0 dans lesquels $+$ et $\cdot$ ne sont pas commutatifs ni associatifs.
3. Il existe des modèles de PA_0 dans lesquels $\leqslant$ est un ordre qui n'est pas total.

Le principal intérêt de la théorie PA_0 est qu'elle axiomatise un fragment (important) de la théorie de $\mathbb{N}_{\mathrm{st}}$.

Pour tout $n \in \mathbb{N}$, on défini par récurrence le terme $\underline{n}$ par :
- $\underline{0} = 0$;
- $\underline{n+1} = S\underline{n}$.

Lemme 5.3. *Soit $M \vDash \mathrm{PA}_0$, alors $f : n \mapsto \underline{n}^M$ est un plongement $\mathbb{N}_{\mathrm{st}} \to M$ et son image est un segment inital : pour tout $a \in \mathrm{A}(M)$ s'il existe $n \in \mathbb{N}$ tel que $a \leqslant \underline{n}^M$, alors il existe $m \in \mathbb{N}$ tel que $a = \underline{n}^M$.*

Démonstration. On vérifie (par récurrence sur $n \in \mathbb{N}$) que, pour tout $m \in \mathbb{N}$:
- $\mathrm{PA}_0 \vDash \underline{n+m+1} \neq \underline{n}$ (et donc f est injective);
- $\mathrm{PA}_0 \vDash \underline{m+n} = \underline{m} + \underline{n}$ (et donc f préserve $+$);
- $\mathrm{PA}_0 \vDash \underline{m \cdot n} = \underline{m} \cdot \underline{n}$ (et donc f préserve $\cdot$).
- $\mathrm{PA}_0 \vDash \forall x\, x \leqslant \underline{n} \to \bigvee_{i \leqslant n} x = \underline{i}$ (et donc l'image est un segment initial).

Prouvons la dernière assertion. Soit $M \vDash \mathrm{PA}_0$ et $a \in \mathrm{A}(M)$ tel que $a \leqslant \underline{n}^M$. Par définition, il existe $b \in \mathrm{A}(M)$ tel que $b + a = \underline{n}$. Si $a = \underline{0}$, on a rien à démontrer. Sinon, il existe $c \in \mathrm{A}(M)$ tel que $a = S(c)$. On a alors $S(b + c) = b + S(c) = b + a = \underline{n}$. Le cas $n = 0$ contredit le fait que $\underline{0}$ n'est pas dans l'image de S. On a donc $n = m + 1$ et $S(b + c) = S\underline{m}$; et donc $b + c = \underline{m}$,

comme S est injective. Par récurrence sur n, on a donc $c = \underline{i}$ pour un $i \leqslant m$. Il s'ensuit que $a = Sc = S\underline{i} = \underline{i+1}$. □

Définition 5.4. L'ensemble des formules Σ_1 est le plus petit ensemble de formules qui :
- contient les formules atomiques et leurs négations ;
- est clos par $\wedge$ et $\vee$;
- est clos par quantification universelle bornée : si φ est Σ_1 alors $\forall x\, x \leqslant y \to \varphi$ est aussi Σ_1 ;
- par quantification existentielle.

Proposition 5.5. *Soit $\varphi(x_1, \dots, x_n)$ une formule Σ_1 et $a_1, \dots, a_n \in \mathbb{N}$, alors*

$$\mathbb{N}_{\mathrm{st}} \vDash \varphi(a_1, \dots, a_n) \text{ si et seulement si } \mathrm{PA}_0 \vDash \varphi(\underline{a}_1, \dots, \underline{a}_n).$$

Démonstration. Puisque $\mathbb{N}_{\mathrm{st}} \vDash \mathrm{PA}_0$, il suffit de démonter que si $\mathbb{N}_{\mathrm{st}} \vDash \varphi(a_1, \dots, a_n)$, alors pour tout $M \vDash \mathrm{PA}_0$, si $\mathbb{N}_{\mathrm{st}} \vDash \varphi(a_1, \dots, a_n)$ alors $M \vDash \varphi(\underline{a}_1, \dots, \underline{a}_n)$.

On procède par récurrence sur φ. Si φ est atomique (ou négation d'atomique, voire plus généralement sans quantificateurs), alors d'après le lemme 5.3, on a $\mathbb{N}_{\mathrm{st}} \vDash \varphi(a_1, \dots, a_n)$ si et seulement si $M \vDash \varphi(\underline{a}_1, \dots, \underline{a}_n)$.

Si φ est de la forme $\psi_1 \wedge \psi_2$ alors, par récurrence,

$$\begin{aligned}\mathbb{N}_{\mathrm{st}} \vDash \varphi(a_1, \dots, a_n) &\Leftrightarrow \mathbb{N}_{\mathrm{st}} \vDash \psi_1(a_1, \dots, a_n) \text{ et } \mathbb{N}_{\mathrm{st}} \vDash \psi_2(a_1, \dots, a_n)\\ &\Leftrightarrow M \vDash \psi_1(\underline{a}_1, \dots, \underline{a}_n) \text{ et } M \vDash \psi_2(\underline{a}_1, \dots, \underline{a}_n)\\ &\Leftrightarrow M \vDash \varphi(\underline{a}_1, \dots, \underline{a}_n).\end{aligned}$$

Le cas où φ est de la forme $\psi_1 \vee \psi_2$ est traité de manière similaire.

Supposons à présent que φ est de la forme $\forall x_0\, x_0 \leqslant x_1 \to \psi$. Pour tout $a \in \mathrm{A}(M)$, si $a \leqslant \underline{a}_1$ alors, comme l'image de f est un segment initial, $a = \underline{a}_0$ pour un certain $a_0 \in \mathbb{N}$ inférieur à a_0. Si $\mathbb{N}_{\mathrm{st}} \vDash \forall x_0\, x_0 \leqslant x_1 \to \psi(y, a_1, \dots, a_n)$, on a $\mathbb{N}_{\mathrm{st}} \vDash \psi(a_0, a_1, \dots, a_n)$ et donc, par récurrence, on a $M \vDash \psi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_n)$. On a donc bien $M \vDash \forall x_0\, x_0 \leqslant x_1 \to \psi(\underline{a}_1, \dots, \underline{a}_n)$.

Considérons enfin le cas où φ est de la forme $\exists y\, \psi$. Si $\mathbb{N} \vDash \exists y\, \varphi(y, a_1, \dots, a_n)$ alors il exists $a_0 \in \mathbb{N}$ tel que $\mathbb{N}_{\mathrm{st}} \vDash \psi(a_0, a_1, \dots, a_n)$. Par récurrence, on a alors $M \vDash \varphi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_n)$, et donc $M \vDash \exists y\, \varphi(y, \underline{a}_1, \dots, \underline{a}_n)$. □

5.2 Fonction récursives

La théorie de $\mathbb{N}_{\mathrm{st}}$ est liée de manière intrinsèque à la calculabilité. On va donc introduire dans cette section ce qu'on entend par une fonction « calculable » (on appellera ca une fonction récursive totale ici). Puis on expliquera le lien entre calculabilité et PA_0.

Définition 5.6. L'ensemble des fonction récursives (totales) est le plus petit ensemble R de fonctions $f : \mathbb{N}^n \to \mathbb{N}$ (pour un n qui n'est pas fixé) qui :
- contient la fonction constante nulle, la fonction $S : x \mapsto x + 1$ et $\pi_i^n : (x_j)_{0<j\leqslant n} \mapsto x_i$, pour tout $n > 0$ et $0 < i \leqslant n$;
- est stable par composition : si $f : \mathbb{N}^n \to \mathbb{N}$ est récursive, ainsi que $g_i : \mathbb{N}^m \to \mathbb{N}$, pour tout $0 < i \leqslant n$, alors la fonction $x \in \mathbb{N}^m \mapsto f(g_1(x), \dots, g_n(x))$ est récursive ;

- stable par récurrence : si $g : \mathbb{N}^m \to \mathbb{N}$ et $h : \mathbb{N}^{m+2}$ sont récursives alors la fonction $f : \mathbb{N}^{m+1} \to \mathbb{N}$ définie par :

$$\begin{cases} f(x,0) &= g(x) \\ f(x,y+1) &= h(x,y,f(x,y)) \end{cases}$$

  est récursive ;
- stable par schéma μ total : si $f : \mathbb{N}^{n+1} \to \mathbb{N}$ est récursive et que pour tout $x \in \mathbb{N}^n$ il existe $y \in \mathbb{N}$ tel que $f(x,y) = 0$ alors $\mu y\, f : \mathbb{N} \to \mathbb{N}$ définie par

$$\mu y\, f : x \in \mathbb{N}^m \mapsto \min\{y \in \mathbb{N} : f(x,y) = 0\}$$

  est récursive.

Exemple 5.7.
- L'addition est récursive. Elle est définie par la récurrence suivante :

$$\begin{cases} x+0 &= x \\ x+(y+1) &= (x+y)+1. \end{cases}$$

- De même la multiplication et l'exponentiation $(x,y) \mapsto x^y$ sont récursives.
- La fonction $x \dot{-} y = \max\{x-y, 0\}$ est récursive. Elle est définie par les deux schémas de récurrences suivants :

$$\begin{cases} 0\dot{-}1 &= 0 \\ (x+1)\dot{-}1 &= x \end{cases} \text{ et } \begin{cases} x\dot{-}0 &= x \\ x\dot{-}(y+1) &= (x\dot{-}y)\dot{-}1. \end{cases}$$

- La fonction $\mathbb{1}_{=0}$ est récursive. Elle est définie par le schéma de récurrence suivant :

$$\begin{cases} \mathbb{1}_{=0}(0) &= 1 \\ \mathbb{1}_{=0}(x+1) &= 0. \end{cases}$$

- On en déduit que $\mathbb{1}_{\leqslant}(x,y) = \mathbb{1}_{=0}(x\dot{-}y)$ est récursice, ainsi que $\mathbb{1}_{=}(x,y) = \mathbb{1}_{\leqslant}(x,y) \cdot \mathbb{1}_{\leqslant}(y,x)$ ou encore $\mathbb{1}_{<}(x,y) = S(0)\dot{-}\mathbb{1}_{\leqslant}(y,x)$.

Remarque 5.8. Toutes ces fonctions sont en fait « primitives récursives », le schéma μ total n'est pas nécessaire pour les définir. Une fonction récursice non primitive récursive est la fonction d'Ackermann $A : \mathbb{N}^2 \to \mathbb{N}$ (voir [HL19, proposition 4.5.4]) définie par le schéma (qui n'est pas un schéma de récurrence au sens de la définition définition 5.6) :

$$\begin{cases} A(x,0) &= x+1 \\ A(0,y+1) &= A(1,y) \\ A(x+1,y+1) &= A(A(x,y+1),y). \end{cases}$$

Définition 5.9. Un ensemble $X \subseteq \mathbb{N}^n$ est dit récursif si sa fonction caractéristique $\mathbb{1}_X$ l'est.

Remarque 5.10. Les ensembles récursifs sont clos par combinaisons booléennes. En effet :
- si $X \subseteq \mathbb{N}^n$, alors $\mathbb{1}_{\mathbb{N}^n \setminus X}(x) = S(0)\dot{-}\mathbb{1}_X(x)$;
- si $X, Y \subseteq \mathbb{N}^n$, alors $\mathbb{1}_{X\cap Y}(x) = \mathbb{1}_X(x) \cdot \mathbb{1}_Y(x)$.

Le principal résulat que l'on utilisera sur les fonctions récursives est que contrairement à ce que leur nom indique, la récurrence n'est pas nécessaire dans leur définition si l'on rajoute suffisament de fonctions de base.

Proposition 5.11. *L'ensemble des fonctions récursives est le plus petit ensemble qui :*
- *contient la fonction constante* 0*, les fonctions* S*,* $+$*,* $\cdot$ *et* $\mathbb{1}_<$ *ainsi que les fonctions* π_i^n *pour tout* i, n*;*
- *est stable par composition ;*
- *est stable par schéma* μ *total.*

En termes informatiques, le schéma μ est une « boucle while » (dont on s'est assuré qu'elle termine toujours). Le résultat énoncé dans le théorème est ce que fait tout compilateur de langage fonctionnel vers un language impératif : simuler la récurrence avec des « boucles while », habituellement en introduisant des listes.

Démonstration. Pour les besoins de la preuve, appelons fortement récursive une fonction dans l'ensemble défini ci-dessus (et faiblement récursif tout ensemble dont la fonction caractéristique est faiblement récursive). Toute fonction récursive est fortement récursive (voir exemple 5.7 pour les nouvelles fonctions de base).

Pour prouver la réciproque on établi un liste de résultat intermédiaires sur les fonctions fortement récursives. Tout d'abord, on remarque que, puisque[13] $x \dot{-} y = \mu z\, x < S(y + z)$, cette fonction est fortement récursive. Il en découle que les ensembles fortement récursifs sont clos par combinaisons booléennes (*cf.* remarque 5.10).

De plus les ensembles fortement récursifs sont clos par quantification bornée : si $X \subseteq \mathbb{N}^{n+1}$ est fortement récursif alors l'ensemble $\{(x, z) \in \mathbb{N}^n : \exists y < z,\ (x, y) \in X\}$ est fortement récursif (par passage au complémentaire, c'est aussi le cas de $\{(x, z) \in \mathbb{N}^n : \forall y < z,\ (x, y) \in X\}$). En effet, posons $f(x, z) = \mu y,\ (x, y) \in X \vee y = z$ qui est fortement récursive. Alors $\exists y < z,\ (x, y) \in X$ si et seulement si $f(x, z) < S(z)$.

Affirmation 5.11.1 (Fonction β de Gödel)**.** *Il existe une fonction* $\beta : \mathbb{N}^3 \to \mathbb{N}$ *fortement récursive telle que, pour tous* $c_0, \dots, c_n$*. il existe* $a, b \in \mathbb{N}$ *tels que, pour tout* $i \leqslant n$*,* $\beta(a, b, i) = c_i$*.*

Démonstration. L'ensemble $\{(x, y, z) \in \mathbb{N}^3 : x \equiv y \mod z\} = \{(x, y, z) \in \mathbb{N}^3 : \exists w < x + y,\ x = y + zw \vee y = x + zw\}$ est faiblement récursif.

Soit $b \in \mathbb{N}$ divisible par $n!$ et tel que $b > \max_i c_i$. Alors, pour tous $i \leqslant n$, les $(i + 1)b + 1$ sont premiers deux à deux. En effet, si $i < j$ et p premier divise $(i+1)b+1$ et $(j+1)b+1$, alors p divise $(j-i)b$ mais ne divise pas b. Il s'ensuit que p divise $j - i$ et donc $n!$. Ceci contredit le fait que p ne divise pas b. D'après le théorème des restes, il existe donc $a \in \mathbb{N}$ tel que $a \equiv c_i \mod (i + 1)b + 1$, pour tous $0 \leqslant i \leqslant n$.

On pose $\beta(x, y, z) = \mu s,\ s \equiv x \mod (z + 1)y + 1$. Comme $c_i < (i + 1)b + 1$, on a bien $\beta(a, b, i) = c_i$. ◊

Pour conclure la preuve de la proposition 5.11, il suffit de montrer que l'ensemble des fonctions fortement récursives est clos par récurrence. Soient $g : \mathbb{N}^n \to \mathbb{N}$ et $h : \mathbb{N}^{n+2} \to \mathbb{N}$ et soit

[13] Pour alléger les notations, on écrit souvent $\mu y\, \varphi(x, y)$ pour la fonction $\mu y,\ 1 \dot{-} \mathbb{1}_{\varphi(x,y)}$.

$f : \mathbb{N}^{n+1} \to \mathbb{N}$ définie par le schéma de récurrence :

$$\begin{cases} f(x,0) &= g(x) \\ f(x,y+1) &= h(x,y,f(x,y)) \end{cases}$$

Posons X l'ensemble fortement récursif défini par[14] $(x,y,a,b) \in \mathbb{N}^{n+3}$ si $\beta(a,b,0) = g(x)$ et si pour tout $i < y$, $\beta(a,b,i+1) = h(x,i,\beta(a,b,i))$. On vérifie par récurrence sur $i \leqslant y$ que, si $(x,y,a,b) \in X$ alors $\beta(a,b,i) = f(x,i)$.

En effet, $\beta(a,b,0) = g(x) = f(x,0)$ et si $\beta(a,b,i) = f(x,i)$ et $i < y$, alors

$$\begin{aligned} \beta(a,b,i+1) &= h(x,i,\beta(a,b,i)) \\ &= h(x,i,f(x,i)) \\ &= f(x,i+1). \end{aligned}$$

On pose alors $e(x,y) = \mu s,\ \exists a \leqslant s \exists b \leqslant s,\ (x,y,a,b) \in X$ et on a alors

$$f(x,y) = \mu z,\ \exists a \leqslant e(x,y) \exists b \leqslant e(x,y),\ (x,y,a,b) \in X \wedge z = \beta(a,b,y).$$

□

On peut maintenant expliciter le lien entre les fonctions récursives et PA_0.

Définition 5.12. Une fonction $f : \mathbb{N}^n \to \mathbb{N}$ est dite Σ_1-représentable s'il existe une formule de $\mathfrak{L}_{\mathrm{ar}}$ $\varphi(x_1,\dots,x_n,y)$ qui est Σ_1 et telle que, pour tous $a = (a_1,\dots,a_n) \in \mathbb{N}^n$, on ait

$$\mathrm{PA}_0 \vDash \forall y \varphi(\underline{a},y) \leftrightarrow y = \underline{f(a)}.$$

Théorème 5.13. *Toute fonction récursive est Σ_1-représentable.*

Démonstration. D'après la proposition 5.11, il nous faut montrer que l'ensemble des fonctions Σ_1-représentables contient les fonctions 0, S, $+$, $\cdot$, $\mathbb{1}_<$ et π_i^n, est stable par composition et par schéma μ total.

Pour ce qui est est des fonctions de base, la fonction constante0 est représentée par $\varphi(x,y) \equiv y = 0$. En effet, on a bien $\mathrm{PA}_0 \vDash \forall y,\ y = \underline{0} \leftrightarrow y = \underline{0}$. De même les fonctions S, $+$, $\cdot$ et π_i^n sont représentées (respectivement) par $y = S(x)$, $y = x_1 + x_2$, $y = x_1 \cdot x_2$ et $y = x_i$. La fonction $\mathbb{1}_<$ est représentée par

$$(y = 0 \wedge \exists z \leqslant x_2,\ S(x_1 + z) = x_2) \vee (y = S(0) \wedge \forall z \leqslant x_2,\ S(x_1 + z) \neq x_2).$$

Montrons à présent que cet ensemble est stable par composition. Soit $f : \mathbb{N}^n \to \mathbb{N}$ représentée par $\varphi(x_1,\dots,x_n,y)$ et soient $g_i : \mathbb{N}^m \to \mathbb{N}$ représentée par $\psi_i(x_1,\dots,x_m,y)$, pour $0 < i \leqslant n$. Alors $x \mapsto f(g_1(x),\dots,g_n(x))$ est représentée par

$$\theta(x_1,\dots,x_m,y) \equiv \exists z_1 \dots \exists z_n,\ \varphi(y,z_1,\dots,z_n) \wedge \bigwedge_i \psi_i(x_1,\dots,x_m,z_i).$$

[14] En d'autres termes, X est l'ensemble des (x,y,a,b) tels que (a,b) encode via β la liste des valeurs de f en les (x,i), pour $i < y$.

En effet, pour tout $a \in \mathbb{N}^n$, tout $M \vDash \mathrm{PA}_0$ et tout $b \in \mathrm{A}(M)$, on a

$$\begin{aligned} M \vDash \theta(\underline{a}, b) &\leftrightarrow \varphi(\underline{g(a)}, b) \wedge \bigwedge_i \psi_i(\underline{a}, \underline{g_i(a)}) \\ &\leftrightarrow b = \underline{f(g(a))}, \end{aligned}$$

où $g(a) = (g_i(a))_{0<i\leqslant n}$.

Enfin montrons que cet ensemble est clos par schéma μ total. Soit $f : \mathbb{N}^{n+1} \to \mathbb{N}$ représentée par $\varphi(x_1, \ldots, x_n, z, y)$ telle que, pour tout $a \in \mathbb{N}^n$, il existe $b \in \mathbb{N}$ tel que $f(a, b) = 0$. Alors $\mu z\, f$ est représentée par

$$\theta(x_1, \ldots, x_n, y) \equiv \varphi(x, z, \underline{0}) \wedge \forall t \leqslant z,\ t = z \vee \exists s\, (\varphi(x, z, s) \wedge s \neq \underline{0}).$$

En effet, pour tout $a \in \mathbb{N}^n$, soit $b \in \mathbb{N}$ minimal tel que $f(a, b) = 0$. On alors $\mathrm{PA}_0 \vDash \varphi(\underline{a}, \underline{b}, \underline{0})$. De plus, pour tout $c \in M \vDash \mathrm{PA}_0$, si $c < \underline{b}$ alors, d'après le lemme 5.3, $c = \underline{d}$ avec $d \in \mathbb{N}$ et $d < b$. Alors $e = f(a, d) \neq 0$ et donc $M \vDash \varphi(\underline{a}, \underline{d}, \underline{e}) \wedge s \neq \underline{0}$. Il s'ensuit que $M \vDash \theta(\underline{a}, \underline{b})$.

Réciproquement, soit $c \in \mathrm{A}(M)$ tel que $M \vDash \theta(\underline{a}, c)$. Si $c = \underline{i}$ avec $i < b$, alors comme $f(a, i) \neq 0$, on a $M \vDash \neg\varphi(\underline{a}, c, \underline{0})$, ce qui contredit que $M \vDash \theta(\underline{a}, c)$. Comme $M \vDash \bigvee_{i<b} c = \underline{i} \vee \underline{b} \leqslant c$ (ceci se vérifie par récurrence sur b), on a donc $\underline{b} \leqslant c$. Si $c \neq \underline{b}$, il existe $e \neq \underline{0}$ tel que $M \vDash \varphi(\underline{a}, \underline{b}, e)$. Mais alors, $e = f(a, b) = 0$, ce qui contredit notre hypothèse sur e. Il s'ensuit que $c = \underline{b}$, ce qui conclut la preuve. □

Définition 5.14. Un ensemble $X \subseteq \mathbb{N}^n$ est dit récursivement énumérable s'il existe $Y \subseteq \mathbb{N}^{n+1}$ récrusif tel que $X = \pi(Y)$, où π est la projection sur les n premières variables.

Proposition 5.15. *Un ensemble $X \subseteq \mathbb{N}^n$ est récursif si et seulement si X et $\mathbb{N}^n \setminus X$ sont récursivement énumérables.*

Démonstration. Supposons que X est récursif. Comme $X = \pi(X \times \mathbb{N})$, il est aussi récursivement énumérable. De même, comme $\mathbb{N}^n \setminus X$ est aussi récursif, il est récursivement énumérable.

Réciproquement, si $X = \pi(Y)$ et $\mathbb{N}^n \setminus X = \pi(Z)$ alors $\mathbb{1}_X(x) = \mathbb{1}_y(\mu t,\ (x, t) \in Y \cup Z)$ qui est bien récusive si $\mathbb{1}_Y$ et $\mathbb{1}_Z$ le sont. □

Proposition 5.16. *Un ensemble X est récursivement énumérable si et seulement s'il est définissables dans $\mathbb{N}_{\mathrm{st}}$ par une formule Σ_1 ; c'est-à-dire qu'il existe une formule $\varphi(x_1, \ldots, x_n)$ qui soit Σ_1 et telle que $X = \varphi(\mathbb{N}_{\mathrm{st}})$.*

Démonstration. Supposons X récursivement énumérable et donc qu'il existe $Y \subseteq \mathbb{N}^{n+1}$ récursif tel que $X = \pi(Y)$, où pi est la projection sur les n premières variables. Alors, par théorème 5.13, il existe une formule $\varphi(x_1, \ldots, x_n, z, y)$ qui est Σ_1 et qui représente $\mathbb{1}_Y$. Alors X est défini dans $\mathbb{N}_{\mathrm{st}}$ par $\exists z\varphi$, qui est bien Σ_1.

Réciproquement, Comme les interprétations des symboles fonctionels de $\mathfrak{L}_{\mathrm{ar}}$ dans $\mathbb{N}_{\mathrm{st}}$ sont toutes récursives, il s'ensuit que l'interprétation de tout terme l'est aussi. Comme $\mathbb{1}_=$ est récursive, les ensembles définissables par les formules atomiques sont aussi récursifs. Les ensembles définis par des formules atomiques et des négations de formules atomiques sont donc bien récursivement énumérables[15].

[15] Il découle de la remarque 5.10 que c'est aussi le cas des formules définissables sans quantificateurs.

Il reste donc à vérifier que les ensembles récursivement énumérables sont clos par disjonction, conjonction, quantification bornée et quantification existentielle. Avant cela, on va introduire des fonctions auxilliaires pour coder les uplets.

Lemme 5.17. *Il existe des fonctions récursives $\alpha_2 : \mathbb{N}^2 \to \mathbb{N}$ et $\beta_i : \mathbb{N} \to \mathbb{N}$, pour $i = 1, 2$ telles que $x \mapsto (\beta_1(x), \beta_2(x))$ est l'inverse de α.*

Démonstration. La fonction définie par $\alpha(x, y) = \frac{1}{2}(x+y)(x+y+1)+x$ est récursive est bijective. Notons que, pour tout $x, y \in \mathbb{N}$, $\alpha(x, y) \leqslant \max\{x, y\}$. Les fonctions $\beta_1(z) = \mu x, (\exists y \leqslant z, \alpha(x, y) = z)$ et $\beta_1(z) = \mu y, (\exists x \leqslant z, \alpha(x, y) = z)$ ont donc les propriétés requises. ◊

Soient $Y_1, Y_2 \subseteq \mathbb{N}^{n+1}$ des ensembles récursifs, alors $x \in \pi(Y_1) \cup \pi(Y_2)$ si et seulement si $x \in \pi(Y_1 \cup Y_2)$. Les ensembles récursivement énumérables sont donc bien clos par disjonction. Pour ce qui est de la conjonction, on a $x \in \pi(Y_1) \cap \pi(Y_2)$ si et seulement s'il existe $y \in \mathbb{N}$ tel que $(x, \beta_1(y)) \in Y_1$ et $(x, \beta_2(y)) \in Y_2$.

Pour ce qui est de la quantification universelle bornée, on a $\forall z \leqslant s, (x, z) \in \pi(Y)$ si et seulement s'il existe $y_0, \dots, y_s \in \mathbb{N}$ tels que pour tout $z \leqslant s$, $(z, x, y_z) \in Y$; en d'autres termes, il existe $y \in \mathbb{N}$ tel que pour tout $z \leqslant s$, $(x, z, \beta(\beta_1(y), \beta_2(y), z)) \in Y$. Enfin, pour la quantification universelle, on a $\exists z, (x, y) \in \pi(Y)$ si et seulement s'il existe $y \in \mathbb{N}$ tel que $(x, \beta_1(y), \beta_2(y)) \in Y$, ce qui conclut la preuve. □

Remarque 5.18. Pour tout n, il existe une fonction récursive bijective $\alpha_n : \mathbb{N}^n \to \mathbb{N}$ d'inverse bijective. On peut par exemple considérer $\alpha_{n+1}(x_0, \dots, x_n) = \alpha_2(x_0, \alpha_n(x_1, \dots, x_n))$. On note $(\beta_0^{n+1}, \dots, \beta_n^{n+1})$ son inverse.

Théorème 5.19. *Soit $f : \mathbb{N}^n \to \mathbb{N}$. Sont équivalents :*
(i) la fonction f est récursive ;
(ii) la fonction f est Σ_1-représentable ;
(iii) le graphe de f est récursivement énumérable.

Démonstration. On a montré que (i)⇒(ii) dans la théorème 5.13. Si f est représentée par une formule $\varphi(x, y)$ qui est Σ_1 alors, pour tout $a \in \mathbb{N}^n$ et $b \in \mathbb{N}$, $b = f(a)$ si et seulement si $\mathbb{N}_{\mathrm{st}} \vDash \varphi(a, b)$ et donc φ définie le graphe de f dans $\mathbb{N}_{\mathrm{st}}$; c'est-à-dire que (ii)⇒(iii).

Enfin montrons que (iii)⇒(i). Si, pour tout $a \in \mathbb{N}^n$ et $b \in \mathbb{N}$, $b = f(a)$ si et seulement si $(a, b) \in \pi(Y)$, où $Y \subseteq \mathbb{N}^{n+2}$ est récursif, alors $f(a) = \beta_1(\mu z \, \mathbb{1}_Y(a, \beta_1(z), \beta_2(z)))$, qui est bien récusive. □

Remarque 5.20. Un théorème ultérieur remarquable (du à Davis–Putmnam–J. Robinson–Matyasevitch) raffine l'équivalence que l'on vient de démontrer : un ensemble $X \subseteq \mathbb{N}^n$ est récursivement énumérable si et seulement s'il est de la forme $\exists y_1 \dots \exists y_m, P(x_1, \dots, x_n, y_1, \dots y_n) = 0$, où P est un polynôme à coefficient dans $\mathbb{Z}$.

Ceci donne une réponse négative au 10e problème de Hilbert qui demandait si, pour tout polynôme $P(x_1, \dots, x_n, y_1, \dots y_n)$ à coefficients entiers, l'ensemble $x \in \exists y P(x, y) = 0$ est récursive — en d'autres termes si l'on peut décider de manière algorithmique l'existence de solutions aux équations diophantiennes. La solution négative au 10e problème de Hilbert est alors une conséquence immédiate de l'existence d'ensembles récursivement énumérables non récursifs (voir, par exemple, corollaire 5.32).

5.3 Incomplétude

Fixons $\mathfrak{L}$ un language au plus dénombrable et V un ensemble dénombrable. On veut associer à chaque formule $\varphi \in \mathfrak{F}(V)$ un entier (son code) de manière injective telle que diverses opérations (combinaison booléenne, substitution, ...) soient récursives sur les codes. La manière exacte de le faire n'a aucune importance, mais on choisit le codage (arbitraire) suivant.

On fixe des énumérations $(f_i^n)_i$ des symboles fonctionnels de $\mathfrak{L}$ d'arité n, $(R_i^n)_i$ des symboles relationnels de $\mathfrak{L}$ d'arité n et $(x_i)_i$ de V.

Définition 5.21. Pour tout terme $t \in \mathfrak{T}(V)$, on définit $\#t$ par récurrence sur t :
- $\#x_i = \alpha_2(0, i)$, pour tout $i \in \mathbb{N}$;
- $\#(f_i^n t_1 \dots t_n) = \alpha_{n+2}(1, i, \#t_1, \dots, \#t_n)$, pour tous i et n.

Pour toute formule $\varphi \in \mathfrak{F}(V)$, on définit $\#\varphi$ par récurrence sur φ :
- $\#\bot = 0$;
- $\#(R_i^n t_1 \dots t_n) = \alpha_{n+1}(1, i, \#t_1, \dots, \#t_n)$, pour tous i et n;
- $\#(t_1 = t_2)$ est $\alpha_3(2, \#\psi_1, \#\psi_2)$;
- $\#(\psi_1 \to \psi_2) = \alpha_3(3, \#\psi_1, \#\psi_2)$;
- $\#(\forall x_i \psi) = \alpha_3(4, i, \psi)$, où i est minimal parmi les j tels que $\forall x_i \varphi = \forall x_j \varphi(x_j/x_i)$.

On vérifie alors :

Lemme 5.22. *Les ensembles suivants sont récursifs :*
- $\{\#t : t \in \mathfrak{T}(V)\}$;
- $\{\#\varphi : \varphi \in \mathfrak{T}(V)\}$;
- $\{\#\varphi : \varphi$ *énoncé*$\}$;
- $\{(i, \#\varphi) : i$ *est libre dans* $\varphi\}$.

Les fonctions suivantes sont récursives[16] *:*
- $(\#t, \#s, i) \mapsto \#t(s/x_i)$;
- $(\#\varphi, \#s, i) \mapsto \#\varphi(s/x_i)$.

Enfin, on définit $\#(\varphi_1, \dots, \varphi_n) = \alpha_{n+1}(n, \#\varphi_1, \dots, \#\varphi_n)$. Dans ce qui suit on identifie un uplet de formules avec l'ensemble de ses coordonnées. On vérifie alors que :

Proposition 5.23. *L'ensemble D des $\alpha_{n+1}(n, (\#\Gamma_1, \#\Delta_1), \dots, (\#\Gamma_n, \#\Delta_n))$, tels que la liste des séquents*[17] *$\Gamma_i ; \Delta_i$ est une preuve, est récursif.*

On a alors $\Gamma \vdash \Delta$ si et seulement s'il existe $n \geqslant 1$ et $d \in D$ tel que $\beta_0^{n+1}(d) = n$ et $\beta_n^{n+1}(d) = (\#\Gamma, \#\Delta)$. On en déduit donc que :

Corollaire 5.24. *L'ensemble des $(\#\Gamma, \#\Delta)$ tels que $\Gamma \vdash \Delta$ est récursif.*

Définition 5.25. Soit T une théorie.
1. On note $\#T = \{\#\varphi : \varphi \in T\}$;
2. On note $\mathrm{Thm}(T) = \{$ énoncés $\varphi : T \vDash \varphi\}$;

[16] Par convention, ces fonctions sont nulles là où on ne les a pas définies.
[17] En identifiant un uplet avec l'ensemble de ses coordonnées

3. T est dite récursivement axiomatisable s'il existe une théorie T' telle que $\#T'$ est récursif et $\mathrm{Thm}(T) = \mathrm{Thm}(T')$.
4. T est dite décidable si $\#\mathrm{Thm}(T)$ est récursif.

Lemme 5.26. *Soit T une théorie.*
1. *Si T est récursivement axiomatisable alors $\#\mathrm{Thm}(T)$ est récursivement énumérable.*
2. *Si T est récursivement axiomatisable et complète alors T est décidable.*

Démonstration. 1. Si T est récursivement axiomatisable, on peut supposer que $\#T$ est récursif sans changer $\mathrm{Thm}(T)$. Par compacité et complétude, $T \vDash \varphi$ si et seulement s'il existe $T_0 \subseteq T$ fini tel que $T_0 \vdash \varphi$. On a donc $T \vDash \varphi$ si et seulement s'il existe $n \geqslant 1$ et $d \in D$ qui encode une preuve de longueur n dont le dernier élément est $\Gamma; \varphi$ avec $\Gamma \subseteq T_0$. C'est donc bien un ensemble récursivement énumérable.
2. Si T est de plus complète alors $T \nvDash \varphi$ si et seulement si $T \vDash \neg\varphi$. L'ensemble $\#T$ et son complémentaire (dans l'ensemble récursif des codes d'énoncés) sont donc récursivement énumérable par l'énoncé précédent. Il sons donc récursifs par la proposition 5.15.

□

Exemple 5.27.
- La théorie CAC_p, pour p premier ou nul, est décidable.
- La théorie CAC est décidable.

Le premier exemple découle du lemme précédent mais le second énoncé nécessite une preuve. D'après le lemme précédent $\#\mathrm{CAC}$ est récursivement énumérable. Par ailleurs, par la corollaire 3.46, on a $\mathrm{CAC} \nvDash \varphi$ si et seulement s'il existe un premier p tel que $\mathrm{CAC}_p \nvDash \varphi$; en d'autres termes, $\mathrm{CAC} \vDash p = 0 \to \neg\varphi$. Le complémentaire de $\#\mathrm{CAC}$ est donc bien récursivement énumérable et donc $\#\mathrm{CAC}$ est récursif.

Pour l'instant, nous avons démontré deux énoncés positifs[18] :
- L'arithmétique (PA_0 pour être précis) est suffisamment riche pour définir toutes les fonctions récursives — il suffit même de formules Σ_1 pour le faire.
- Si une théorie a une axiomatique raisonnable (comprendre, récursive) alors on sait en calculer les conséquences.

Cependant mis ensemble ces deux énoncés disent que l'arithmétique est suffisamment expressive pour parler de ses propres conséquences, ce qui ouvre la porte au paradoxe du menteur : on peut trouver une formule qui énonce que sa négation est une conséquence de l'arithmétique ! Ni cette formule, ni sa négation ne peuvent donc être conséquence de l'arithmétique.

Formellement la construction de cette formule suit du théorème de point fixe suivant[19].

Théorème 5.28 (Point fixe de PA_0). *Pour toute formule $\varphi(x)$, il existe ψ un énoncé Σ_1 tel que*

$$\mathrm{PA}_0 \vDash \varphi(\#\psi) \leftrightarrow \psi.$$

[18] Au sens où ce sont des énoncés d'existence et pas de non existence.

[19] Ce théorème revient essentiellement à écrire un programme qui écrit son propre code. Je vous invite à le faire dans votre langage de programmation favori ! Vous arriverez vraisemblablement à une solution similaire à celle de la preuve ci-dessous

Démonstration. La fonction $s : (\#\varphi, n) \mapsto \#\varphi(\underline{n})$ est récursive. Soit $\sigma(x, y, z)$ une formule Σ_1 qui la représente. Soit $H_\varphi = \exists z,\ (\sigma(x, x, z) \wedge \varphi(z))$, soit $n_\varphi = \#H_\varphi$ et $\Delta_\varphi = H_\varphi(\underline{n_\varphi})$.

Puisque σ représente s, on a $\mathrm{PA}_0 \vDash \forall z\, \sigma(\underline{n_\varphi}, \underline{n_\varphi}, z) \leftrightarrow z = \#\Delta_\varphi$. Il s'ensuit que

$$\mathrm{PA}_0 \vDash \varphi(\#\Delta_\varphi) \leftrightarrow \exists z,\ (G(\underline{n_\varphi}, \underline{n_\varphi}, z) \wedge \varphi(z)).$$

Mais cette dernière formule n'est autre que $H_\varphi(\underline{n_\varphi}) = \Delta_\varphi$. □

En appliquant l'énoncé ci-dessus à $\neg\varphi$, on obtient l'énoncé, beaucoup plus problématique, suivant :

Corollaire 5.29. *Pour toute formule $\varphi(x)$, il existe ψ un énoncé Σ_1 tel que*

$$\mathrm{PA}_0 \vDash \varphi(\#\psi) \leftrightarrow \neg\psi.$$

Corollaire 5.30 (Tarski)**.** *Soit $M \vDash \mathrm{PA}_0$. Il n'existe pas de formule $\varphi(x)$ telle que, pour tout énoncé ψ, $M \vDash \varphi(\#\psi)$ si et seulement si $M \vDash \psi$.*

Démonstration. Supposons qu'une telle φ existe. Soit ψ telle que $\mathrm{PA}_0 \vDash \varphi(\#\psi) \leftrightarrow \neg\psi$. On aurait alors $M \vDash \psi$ si et seulement si $M \vDash \varphi(\#\psi)$, si et seulement si $M \vDash \neg\varphi$. Une telle φ ne peut donc pas exister. □

Corollaire 5.31 (Church)**.** *Si $T \supseteq \mathrm{PA}_0$ est décidable alors T est inconsistante.*

Démonstration. Soit $\varphi(x, y)$ une formule Σ_1 qui représente $\mathbb{1}_{\#\mathrm{Thm}(T)}$. Soit Δ telle que $\mathrm{PA}_0 \vDash \varphi(\#\Delta, \underline{1}) \leftrightarrow \neg\Delta$. On a alors

$$\begin{aligned} T \vDash \Delta &\Leftrightarrow \mathbb{N}_{\mathrm{st}} \vDash \varphi(\underline{\#\Delta}, \underline{1}) \\ &\Leftrightarrow \mathrm{PA}_0 \vDash \varphi(\underline{\#\Delta}, \underline{1}) \\ &\Leftrightarrow \mathrm{PA}_0 \vDash \neg\Delta \\ &\Rightarrow T \vDash \neg\Delta. \end{aligned}$$

Il s'ensuit donc que $T \vDash \neg\Delta$ et donc

$$\begin{aligned} \mathrm{PA}_0 \vDash \forall z,\ \varphi(\underline{\#\Delta}, z) \leftrightarrow z = \underline{0} &\Rightarrow \mathrm{PA}_0 \vDash \neg\varphi(\underline{\#\Delta}, \underline{1}) \\ &\Leftrightarrow \mathrm{PA}_0 \vDash \Delta \\ &\Rightarrow T \vDash \Delta, \end{aligned}$$

et donc T est inconsistante. □

Corollaire 5.32. *L'ensemble $\#\mathrm{Thm}(\mathrm{PA}_0)$ est récursivement énumérable mais il n'est pas récursif.*

En fait, puique PA_0 est fini, $\{\#\varphi : \varphi \text{ est universellement valide}\}$ est récursivement énumérable non récursif.

Corollaire 5.33 (Premier théorème d'incomplétude, Gödel)**.** *Toute théorie $T \subseteq \mathrm{PA}_0$ récursivement axiomatisable et consistante est incomplète.*

Démonstration. Si T était complète, elle serait décidable par lemme 5.26, ce qui contredit le corollaire 5.31. □

6 La théorie des ensembles de von Neumann-Bernays-Gödel

On travaille dans le langage $\mathfrak{L}_{\text{ens}}$ contenant un unique symbole binaire $\in$. On souhaite définir une théorie NBG mais certains de ces axiomes nécessitent des constructions qui dépendent des axiomes précédents. On va donc introduire les axiomes un à un en faisant les constructions nécessaires au fur et à mesure. Les points d'un « modèle » de NBG s'appellent des classes. Les ensembles sont les éléments des classes. Ils sont définis par la formule

$$U(x) = \exists A\, x \in A.$$

On notera $\forall^U$ le quantificateur universel restreint à U, c'est-à-dire, $\forall^U x\, \varphi \equiv \forall x\, U(x) \to \varphi$. De même, on définit le quantificateur existentiel restrient à U par $\exists^U x\, \varphi \equiv \exists x\, U(x) \wedge \varphi$.

Le premier axiome de NBG est l'axiome d'extensionalité, il spécifie l'égalité entre classes :

$$\forall A \forall B\ (\forall C\ C \in A \leftrightarrow C \in B) \to A = B. \tag{Ext}$$

Si A et B sont des classes, on dit que A est incluse dans B, ce qu'on note $A \subseteq B$, si tout élément de X et un élément de Y. L'extensionalité peut alors se réécrire $B \subseteq A \wedge A \subseteq B \to A = B$.

Le second axiome de NBG est l'axiome de la paire, qui, étant donné deux ensembles x et y, spécifie l'existence d'un (unique) ensemble $\{x, y\}$ dont les deux seuls éléments sont x et y.

$$\forall^U x \forall^U y \exists^U z \forall A\ A \in z \leftrightarrow (A = x \vee A = y). \tag{Pair}$$

L'axiome de la paire implique aussi l'existence pour tout ensemble x du singleton $\{x\}$ dont le seul élément est x. Si x et y sont des ensembles, on notera aussi (x, y) le couple $\{\{x\}, \{x, y\}\}$.

Remarque 6.1. Si x_1, x_2, y_1, y_2 sont des ensembles et $(x_1, y_1) = (x_2, y_2)$ alors $x_1 = x_2$ et $y_1 = y_2$. En effet, si $\{\{x_1\}, \{x_1, y_1\}\} = \{\{x_2\}, \{x_2, y_2\}\}$, le singleton $\{x_1\}$ est un élément de la paire $\{\{x_2\}, \{x_2, y_2\}\}$ et donc il est égal à $\{x_2\}$ ou à $\{x_2, y_2\}$. S'il est égal à $\{x_2, y_2\}$ alors $x_1 = x_2 = y_2$ et donc $\{x_2\} = \{x_2, y_2\}$. On a donc aussi $\{x_1, y_1\} = \{x_2\}$ et donc $y_1 = x_2 = y_2$.

Sinon $\{x_1\} = \{x_2\}$, alors $x_1 = x_2$. Si $\{x_1, y_1\} = \{x_2\}$, comme précédemment, on a $x_1 = y_1 = x_2 = y_2$. On peut donc supposer $\{x_1, y_1\} = \{x_2, y_2\}$ et donc $y_1 = x_2$ (en quel cas $y_1 = x_2 = x_1 = y_2$) ou $y_1 = y_2$.

On définit aussi, par récurrence, pour tous ensembles $x_1, \ldots, x_n$,

$$(x_1, \ldots, x_n) = ((x_1, \ldots, x_{n-1}), x_n)$$

, et $(x_1) = x_1$.

Les axiomes suivants sont les axiomes d'existence de classe, tout d'abord l'existence du graphe de $\in$ sur les ensembles :

$$\exists C \forall^U x \forall^U y\ (x, y) \in C \leftrightarrow x \in y, \tag{E$\in$}$$

l'existence de l'intersection $A \cap B$ de deux classes A et B :

$$\forall A \forall B \exists C \forall S\ S \in C \leftrightarrow (S \in A \wedge S \in B), \tag{E$\wedge$}$$

l'existence du complémentaire A^{c} d'une classe A :

$$\forall A \exists C \forall^U x \; x \in C \leftrightarrow (x \notin A) \tag{E$\neg$}$$

la clôture des classes sous projection :

$$\forall A \exists C \forall^U x \; x \in C \leftrightarrow (\exists^U y \; (x, y) \in A), \tag{E$\exists$}$$

l'existence du produit avec U :

$$\forall A \exists C \forall^U x \forall^U y \; (x, y) \in C \leftrightarrow x \in A, \tag{E$\times U$}$$

la clôture sous transposition des triplets :

$$\forall A \exists C \forall^U x \forall^U y \forall^U z \; (x, y, z) \in C \leftrightarrow (y, x, z) \in A, \tag{E$\tau_{1,2}$}$$

et

$$\forall A \exists C \forall^U x \forall^U y \forall^U z \; (x, y, z) \in C \leftrightarrow (x, z, y) \in A. \tag{E$\tau_{2,3}$}$$

On remarque que l'axiome (E$\in$) stipule l'existence d'une classe E. Par l'intersection et le complémentaire, il existe alors une classe $\varnothing = E \cap E^{\mathrm{c}}$. Par définition, cette classe n'a pas d'éléments. On note $U = \varnothing^{\mathrm{c}}$. On a alors $\mathrm{NBG} \vDash U(x) \leftrightarrow x \in U$ — ce qui justifie l'abus de notation.

La clôture par intersection et complémentaire implique la clôture des classes par union. Si A et B sont des classes, on note $A \cup B$ leur union.

Remarque 6.2. Toute classe C est une sous classe de U. En effet, si x est un élément de C alors, par définition, $\mathrm{NBG} \vDash U(x)$ et donc $x \in U$.

Définition 6.3. L'ensemble des formules prédicatives est le plus petit ensemble de $\mathfrak{L}_{\mathrm{ens}}$-formules qui contient les formules atomiques, qui est clos par opérations booléennes et par les quantificateurs ensemblistes $\forall^U$ et $\exists^U$.

Théorème 6.4 (Existence de classes)**.** *Soit $\varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ une formule prédicative alors*

$$\mathrm{NBG} \vDash \forall Y_1 \ldots \forall Y_m \exists C \forall^U x_1 \forall^U x_n \; (x_1, \ldots, x_n) \in C \leftrightarrow \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m).$$

Démonstration. On commence par démontrer le cas particulier suivant : pour toute fonction injective $f : \{1, \ldots, m\} \to \{1, \ldots n\}$ (avec $m \leqslant n$), on a

$$\mathrm{NBG} \vDash \forall A \exists C \forall^U x_1 \forall^U x_n \; (x_1, \ldots, x_n) \in C \leftrightarrow (x_{f(1)}, \ldots, x_{f(m)}) \in A.$$

Le cas où f est l'injection $\{1, \ldots, m\} \to \{1, \ldots m + n\}$ est démontré par récurrence sur n en utilisant l'axiome (E$\times U$). Il suffit donc de considérer le cas ou $m = n$ — et donc f est bijective. Si $n \geqslant 3$, l'axiome E$\tau_{2,3}$ implique l'existence de toutes les permutations de la forme $\tau_{i,i+1}$ pour $i > 1$ — par le choix de définition des n-uplets — et l'axiome E$\tau_{1,2}$ implique celle de $\tau_{1,2}$. Ces transpositions engendrent le groupe symétrique. Si $n = 2$, on se ramène au cas $n = 3$ avec l'axiome E$\times U$.

Soit φ une formule prédicative. Si on remplace toutes les formules atomiques de la forme $s \in t$, où s est un Y_i ou alors s et t sont la même variable, par la formule $\exists^U y\ y = s \wedge y \in t$ et, ensuite, toutes les formules atomiques de la forme $s = t$ par $\forall^U y\ y \in s \leftrightarrow y \in t$, on obtient une formule prédicative équivalente à φ dans laquelle les seules formules atomiques qui apparaissent sont de la forme $s \in t$ où s est soit quantifiées, soit une variable x_i et t est soit quantifiée, soit une variable x_i, soit une variable Y_j et les variables s et t sont distinctes. On peut donc supposer que φ est de cette forme et démontrons maintenant le théorème par récurrence sur φ.

Si φ est atomique elle est soit de la forme $x_i \in x_j$, soit de la forme $x_i \in Y_j$. Si elle est de la forme $x_i \in Y_j$, il suffit de prendre C telle que $(x_1, \dots, x_n) \in C$ si et seulement si $x_i \in Y_j$. Si elle est de la forme $x_i \in x_j$, soit E telle que dans l'axiome (E$\in$). Il suffit alors de prendre C telle que $(x_1, \dots, x_n) \in C$ si et seulement si $(x_i, x_j) \in E$.

Si φ est de la forme $\neg\psi$ et que C est telle que dans le théorème pour ψ alors il suffit de considérer C^c. Si φ est de la forme $\psi_1 \wedge \psi_2$ et C_i est tel que dans le théorème pour ψ_i, alors il suffit de considérer $C_1 \cap C_2$. Comme $\neg$ et $\wedge$ suffisent à engendrer l'algèbre de Boole, cela conclut le cas où φ est une combinaison booléenne de formules auxquelles le théorèmes s'applique.

Enfin, si φ est de la forme $\exists^U y \psi(x_1, \dots, x_n, y, Y_1, \dots, Y_m)$ et que C est telle que dans le théorème pour ψ, alors il suffit de considérer la projection de C sur les n premières variables. Comme le quantificateur universel ensembliste est obtenu par combinaison Booléenne à partir du quantificateur universel ensembliste, ceci conclut la preuve. □

On peut maintenant écrire les axiomes d'existence d'ensembles. Si X est une classe, on note $\bigcup X$ l'union de X. C'est la classe telle que $x \in \bigcup X$ si et seulement si $\exists^U y\ y \in X \wedge x \in y$. L'axiome de l'union stipule alors que l'union d'un ensemble est un ensemble :

$$\forall^U x\ U(\bigcup x).$$

Si X est une classe, on note $\mathfrak{P}(X)$ la classe des sous-ensembles de X. C'est la classe telle que $x \in \mathfrak{P}(X)$ si et seulement si $\forall^U y\ y \in x \to x \in X$. L'axiome des parties stipule alors que la classe des sous-ensembles d'un ensemble est un ensemble :

$$\forall^U x\ U(\mathfrak{P}(x)).$$

Soient C et F deux classes. On définit l'image de C par F, notée $F(C)$ comme la classe définie par $x \in F(C)$ si et seulement si $\exists^U y\ y \in C \wedge (y, x) \in F$. L'axiome de remplacement stipule que l'image d'un ensemble par une classe fonctionnelle est un ensemble :

$$\forall F\ [\forall^U s \forall^U t_1 \forall^U t_2\ ((s, t_1) \in F \wedge (s, t_2) \in F) \to s_1 = s_2] \to \forall^U x\ U(F(x)).$$

Proposition 6.5 (Principe de compréhension)**.** *Si C est une classe et x un ensemble, la classe $C \cap x$ est un ensemble.*

Démonstration. Par le théorème d'existence de classes, il existe une classe D telle que $(s, t) \in D$ si et seulement si $s = t \wedge s \in C$. C'est une classe fonctionnelle et l'image de x par D est la classe $C \cap x$ qui est donc un ensemble. □

Enfin, l'axiome de l'infini[20] stipule l'existence d'un ensemble infini :

$$\exists^U x\ (\varnothing \in x \wedge \forall^U y\ y \in x \to y \cup \{y\} \in x).$$

Remarque 6.6. Une conséquence de l'axiome de l'infini est que la classe vide est un ensemble (on ne le savait pas encore !). En fait, on ne savait pas encore qu'il existe des ensembles...

La classe U ne peut pas être un ensemble. C'est le paradoxe de Russell. En effet, par compréhension, toute classe serait un ensemble, en particulier la classe C des ensembles x tels que $x \notin x$. On a alors $C \in C$ si et seulement si $C \notin C$.

Remarque 6.7. La classe U est un modèle de la théorie ZF de Zermelo-Frankel. Elle vérifie :

- l'extensionalité : $\forall x \forall y (\forall z\ z \in x \leftrightarrow z \in y) \to x = y$;
- l'axiome de l'union : $\forall x \exists y \forall z\ (z \in y) \leftrightarrow \exists s\ s \in x \wedge z \in s$;
- l'axiome des parties : $\forall x \exists y \forall z\ (z \in y) \leftrightarrow (\forall s\ s \in z \to s \in x)$;
- le schéma d'axiomes de remplacement : pour toute formule $\varphi(s, t, u_1, \ldots, u_n)$,

$$\begin{aligned}\forall u_1 \ldots \forall u_n\ [\forall s \forall t_1 \forall t_2 (\varphi(s, t_1, u_1 \ldots, u_n) \wedge \varphi(s, t_2, u_1 \ldots, u_n)) \to t_1 = t_2] \\ \to \forall x \exists y \forall z\ (z \in y) \leftrightarrow (\exists s\ s \in x \wedge \varphi(s, z, u_1 \ldots, u_n));\end{aligned}$$

- l'axiome de l'infini : $\exists x\ \varnothing \in x \wedge (\forall y\ y \in x \to y \cup \{y\} \in x)$[21].

Si A et B sont deux classes, on définit leur produit $A \times B$ comme la classe telle que $x \in A \times B$ si et seulement s'il existe $a \in A$ et $b \in B$ tel que x soit égal au couple (a, b).

Proposition 6.8. *Soient X et Y des ensembles. La classe $X \times Y$ est un ensemble.*

Démonstration. En effet, si $x \in X$ et $y \in Y$, alors $(x, y) = \{\{x\}, \{x, y\}\} \in \mathfrak{P}(\mathfrak{P}(X \cup Y))$. La classe $X \times Y$ est donc incluse dans l'ensemble $\mathfrak{P}(\mathfrak{P}(X \cup Y))$ et c'est donc un ensemble. □

Définition 6.9. Soient A et B deux classes, on appelle application de A dans B une sous-classe $F \subseteq A \times B$ est qui fonctionnelle et telle que la projection sur la première variable soit égale à A. En d'autres termes :

$$\forall^U x \in A (\exists^U y\ (x, y) \in F) \wedge (\forall^U y_1 \forall^U y_2\ (x, y_1) \in F \wedge (x, y_2) \in F \to y_1 = y_2).$$

On écrit alors $F : A \to B$. Pour tout $a \in A$, on note $F(a)$, ou F_a, l'unique ensemble tel que $(a, F(a)) \in F$.

Soient I et X des ensembles. Toute application $f : I \to X$ est une sous-classe de l'ensemble $I \times X$ et c'est donc un ensemble. La classe des applications de I dans X est une sous-classe de l'ensemble $\mathfrak{P}(I \times X)$ et c'est donc aussi un ensemble.

Soit $a : I \to X$ une application. On définit le produit $\prod_{i \in I} a_i$ comme le sous-ensemble des applications f de I dans $\bigcup X$ telles que pour tout $i \in I$, $f(i) \in a_i$.

[20] Contrairement à l'habitude, on ne considère pas ici que NBG contient l'axiome du choix et l'axiome de fondation dont on discutera plus tard.

[21] Pour que cet axiome ait un sens, il faut d'abord construire un ensemble à deux éléments (par exemple, $\mathfrak{P}(\varnothing)$) puis l'utiliser pour construire la paire par remplacement et enfin construire l'union binaire en considérant l'union de la paire.

Références

[1] M. Hils et F. Loeser. *A first journey through logic*. T. 89. Stud. Math. Libr. Providence, RI : American Mathematical Society (AMS), 2019.