CHAPITRE VII

Logique du premier ordre

RÉSUMÉ. • *La logique du premier ordre est la logique des formules usuelles, avec la contrainte que les variables représentent toutes des objets du même type.*
• *Une* signature Σ *est un choix de symboles de constante, d'opérations et de relations spécifiques, et on lui associe une logique du premier ordre* $\mathcal{L}_\Sigma$.
• *Les* termes *de* $\mathcal{L}_\Sigma$ *sont construits récursivement à partir des variables et des symboles de constantes à l'aide des symboles d'opération; les* formules atomiques *de* $\mathcal{L}_\Sigma$ *sont construites à partir des termes en utilisant l'égalité et les symboles de relation; les* formules *de* $\mathcal{L}_\Sigma$ *sont construites à partir des formules atomiques à l'aide des connecteurs booléens et des quantifications. Une formule* close *est une formule sans variable libre.*
• *La sémantique de* $\mathcal{L}_\Sigma$ *transcrit la notion usuelle de* satisfaction *d'une formule* F *dans une structure, ou réalisation,* $\mathcal{R}$*, notée* $\mathcal{R} \models \mathsf{F}$*. On dit qu'une réalisation* $\mathcal{M}$ *est un* modèle *d'un ensemble de formules* T *si* $\mathcal{M} \models \mathsf{F}$ *est vrai pour tout* F *dans* T.
• *Une* preuve *de* $\mathcal{L}_\Sigma$ *formalise la notion usuelle de démonstration ; on utilise les règles de coupure et de généralisation, plus des axiomes correspondant à des schémas usuels.*
• *Toute formule close prouvable est valide. Le* théorème de complétude *affirme la réciproque : toute formule close valide est prouvable. Plus généralement, tout ensemble consistant (fini ou infini) de formules closes a un modèle.*
• *Le* théorème de compacité *affirme l'existence d'un modèle pour une théorie du premier ordre dont tout sous-ensemble fini a un modèle.*
• *Le* théorème de Lowenheim–Skolem *affirme que toute théorie du premier ordre dans une signature dénombrable qui a des modèles infinis a des modèles infinis de toute cardinalité.*
• *La logique du premier ordre ne permet pas de caractériser la structure* $(\mathbb{N}, +, \times)$ *: il existe des* modèles non-standards *de l'arithmétique, structures non isomorphes à* $(\mathbb{N}, +, \times)$ *mais vérifiant exactement les mêmes formules closes du premier ordre.*
• *Pour toute propriété* $\mathcal{P}$ *exprimable en logique du premier ordre par une formule* F*, il est raisonnable de modéliser l'existence d'une démonstration pour* $\mathcal{P}$ *par l'existence d'une preuve formelle pour* F.
• *Comme tous les objets usuels peuvent être représentés par des ensembles purs, il est raisonnable d'adopter le cadre « théorie des ensembles + logique du premier ordre » comme cadre formel global, c'est-à-dire de tenir pour établis les résultats dont la formalisation a une preuve au sens de la logique du premier ordre à partir des axiomes de la théorie des ensembles.*
• *Chaque résultat de prouvabilité est lui-même établi dans un contexte métamathématique, qui peut être formalisé.*
• *La logique du second ordre a un pouvoir d'expression supérieur à la logique du premier ordre, mais elle ne satisfait aucun des théorèmes généraux satisfaits par celle-ci.*

► L'objet de ce chapitre est d'introduire la logique du premier ordre, et d'en démontrer les résultats de base qui seront utilisés dans la suite du texte, à savoir principalement le théorème de complétude de Gödel, le théorème de compacité, et le théorème de Lowenheim–Skolem.

Le plan du chapitre est le suivant. Dans la première partie, on définit la syntaxe de la logique $\mathcal{L}_\Sigma$, sa sémantique basée sur la notion de structure de type Σ, et on examine le pouvoir d'expression des logiques du premier ordre en discutant quelques exemples de propriétés exprimables par des formules du premier ordre. Dans la seconde partie, on définit une notion de preuve formelle fondée sur les règles de coupure et de généralisation et sur une famille infinie d'axiomes correspondant à des schémas de démonstration usuels. On établit ensuite par la méthode dite de Henkin le théorème de complétude de Gödel, qui garantit que toute formule valide est prouvable. La troisième partie regroupe quelques applications du théorème de complétude, à savoir le principe des démonstrations sémantiques, les théorèmes de compacité et de Lowenheim–Skolem, et la notion d'équivalence élémentaire, qu'on applique au cas des modèles non-standards de l'arithmétique, dont on montre qu'il existe une famille non dénombrable. Dans la quatrième partie, on discute l'adoption de la logique du premier ordre et de la notion de preuve associée comme modèle du raisonnement mathématique. Enfin, en appendice, on mentionne brièvement la logique du second ordre et on montre que celle-ci ne satisfait ni le théorème de compacité, ni le théorème de Lowenheim–Skolem. ◀

▷ *La logique du premier ordre, aussi appelée calcul des prédicats, est la logique des formules mathématiques usuelles, telles que*

$$\forall x, y\, \exists z\ (x + z = y + 1), \quad \textit{ou}$$
$$\forall \varepsilon{>}0\, \exists \delta{>}0\ (|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \varepsilon).$$

Il n'est pas surprenant qu'on puisse codifier l'emploi des différents symboles de façon à décrire précisément les formules, puis, suivant le schéma général présenté au chapitre VI, définir une sémantique calquée sur l'usage courant et pouvant être qualifiée de naturelle et, par ailleurs, dégager des règles de déduction valides elles aussi fondées sur les principes de démonstration habituels. Tout cela n'est que la mise en forme d'une sténographie.

L'intérêt de cette formalisation tient à la possibilité de démontrer des théorèmes portant sur les démonstrations prises elles-mêmes comme objet d'étude. On peut se douter qu'il n'y a à espérer aucune recette nouvelle pour inventer des démonstrations et résoudre miraculeusement des problèmes ouverts, mais on constatera que l'approche mène à des résultats non triviaux, dont certains ont eu récemment des applications inattendues dans divers domaines des mathématiques. Pour ce qui est de la théorie des ensembles, où les formules jouent un rôle fondamental, il n'est pas étonnant que les théorèmes de logique y soient importants et, de fait, on verra dans la troisième partie de ce texte que le théorème de complétude de la logique du premier ordre mène directement au changement radical de point de vue qui marque le début de la théorie moderne.

L'existence de résultats non triviaux, typiquement le théorème de complétude qui montre que les formules valides sont exactement celles qui possèdent une preuve d'un certain type syntaxique simple, explique l'intérêt spécifique apporté à la logique du premier ordre, par opposition à d'autres logiques peut-être aussi naturelles. Le cas des logiques du second ordre sera mentionné afin justement de mettre en évidence toutes les lacunes de celles-ci et faire ressortir par contraste les qualités propres à la logique du premier ordre. ◁

1. Logiques du premier ordre

▶ On décrit la syntaxe et la sémantique de la logique du premier ordre $\mathcal{L}_\Sigma$ associée à un choix de symboles Σ : on définit la famille des formules, et on montre comment attribuer une valeur de vérité à une

formule dans le cadre d'une réalisation convenable, ici une structure de type Σ. Cette section est purement descriptive. ◀

▷ *Comme au chapitre VI avec la logique propositionnelle, le principe est de mimer autant que faire se peut l'usage courant : autrement dit, il s'agit d'organiser en un système formel précis les énoncés mathématiques usuels. Les définitions dans la suite sont multiples, mais on devrait se convaincre rapidement que toutes les notions sont, au moins implicitement, déjà toutes familières : la logique du premier ordre est la prose du mathématicien...* ◁

1.1. Formules du premier ordre.

▶ On commence par la définition des formules. Le point spécifique, qui explique qu'il y ait *des* logiques du premier ordre plutôt qu'une seule, est l'option consistant à fixer un ensemble de symboles non logiques, appelé signature. ◀

▷ *L'examen d'un texte mathématique quelconque permet de constater que les formules qui y apparaissent obéissent à un même schéma général, à savoir assembler, à l'aide de connecteurs booléens $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$ et de quantifications $\forall$ et $\exists$, des formules simples du type $\mathsf{t}_1 = \mathsf{t}_2$, $\mathsf{t}_1 < \mathsf{t}_2$,..., d'une façon générale $\boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ où $\boldsymbol{r}$ désigne une relation k-aire, et où t_1,..., t_k représentent des éléments de la structure considérée et sont eux-mêmes soit des variables, soit des noms d'éléments particuliers, soit des combinaisons de variables et de noms à l'aide d'opérations ou de fonctions, sur le modèle de*

$$\forall \boldsymbol{x}_1\, \forall \boldsymbol{x}_2\ (\boldsymbol{x}_1 \leqslant \boldsymbol{x}_2 \Leftrightarrow \exists \boldsymbol{x}_3\, (\boldsymbol{x}_1 + \boldsymbol{x}_3 = \boldsymbol{x}_2)). \tag{1.1}$$

C'est ce type de formule qu'on se propose de définir et d'étudier ici sous le nom de formule du premier ordre.

Deux options sont retenues. La première est que, le but étant d'exprimer les propriétés de structures variées, il est plus commode d'introduire une famille de logiques plutôt qu'une logique unique. Ces logiques sont toutes bâties sur le même modèle, mais chacune dépend d'un choix spécifique des opérations et des relations considérées. Par exemple, en sus des variables et des symboles logiques (dont l'égalité) communs à toutes les logiques du premier ordre, la formule (1.1) *met en jeu une relation binaire $\leqslant$ et une opération binaire $+$, et on dira qu'il s'agit d'une formule du premier ordre relativement à la signature*[1] *consistant en un symbole de relation binaire $\leqslant$ et un symbole d'opération binaire $+$ ou, plus généralement, à toute signature contenant ces symboles.*

La seconde option est d'établir une claire distinction entre les symboles qui figurent dans une formule et les objets mathématiques qu'ils représentent : même si le contexte suggère que $\leqslant$ représente une relation d'ordre, voire plus précisément un certain ordre, par exemple l'ordre canonique des entiers naturels, il est utile pour la suite de maintenir les formules à un niveau purement syntaxique, afin notamment de pouvoir interpréter une même formule dans plusieurs contextes distincts et, par exemple, pouvoir déclarer que la même formule (1.1) *est vraie dans $\mathbb{N}$ et fausse dans $\mathbb{Z}$. De la sorte, la formule elle-même, qui n'est qu'un mot, n'est ni vraie ni fausse hors d'un contexte spécifique. Pour rendre cette distinction visible, on utilisera, au moins dans un premier temps, des notations distinctes, typiquement pour une relation (ensemble de k-uplets) et pour le symbole qui la représente ; pour ne pas compliquer, lorsqu'une notation pour une relation ou une opération est usuelle, on utilisera par défaut la même notation en gras pour le symbole correspondant. Par exemple, à côté de la relation d'appartenance $\in$, on utilisera $\boldsymbol{\in}$ comme un symbole de relation binaire. La distinction est que $\in$ est un ensemble de couples, alors que $\boldsymbol{\in}$ n'est qu'une lettre.* ◁

Définition 1.1. (signature) On appelle *signature* un ensemble, fini ou infini, de symboles avec, pour chacun, la spécification d'un type pouvant être

[1] ici au sens d'ensemble de signes

« constante »[2], « opération », ou « relation », et, dans les deux derniers cas, d'un entier naturel non nul appelé *arité*.

A chaque signature Σ on va associer une logique du premier ordre $\mathcal{L}_\Sigma$.

EXEMPLE 1.2. (signatures $\Sigma_{\rm ens}$, $\Sigma_{\rm arith}$, logiques $\mathcal{L}_{\rm ens}$, $\mathcal{L}_{\rm arith}$) On a déjà mentionné la signature ensembliste $\Sigma_{\rm ens}$ comprenant un unique symbole de relation binaire $\in$; on a donc $\Sigma_{\rm ens} = \{\in\}$, qu'on peut écrire plus précisément comme $\Sigma_{\rm ens} = \{\in_2^r\}$ pour indiquer que $\in$ est un symbole de relation (« r ») binaire. De même, les formules ensemblistes étendues du chapitre III correspondent à la signature $\{\emptyset^c, \{\bullet,\bullet\}_2^o, \bigcup_1^o, \cup_2^o, \mathfrak{P}_1^o, \in_2^r, \subseteq_2^r\}$, qu'on notera $\Sigma_{\rm ens^+}$, et l'arithmétique de Peano est exprimée par des formules mettant en jeu la signature $\{\mathbf{0}^c, \boldsymbol{S}_1^o, +_2^o, \cdot_2^o\}$, qu'on notera $\Sigma_{\rm arith}$, voire la signature $\{\mathbf{0}^c, \boldsymbol{S}_1^o, +_2^o, \cdot_2^o, \leqslant_2^r\}$ notée $\Sigma_{\rm arith^+}$. Dans toute la suite, on notera $\mathcal{L}_{\rm ens}$ la logique du premier ordre associée à la signature $\Sigma_{\rm ens}$, et, de même, $\mathcal{L}_{\rm ens^+}$, $\mathcal{L}_{\rm arith}$ et $\mathcal{L}_{\rm arith^+}$ les logiques associées à $\Sigma_{\rm ens^+}$, $\Sigma_{\rm arith}$ et $\Sigma_{\rm arith^+}$ respectivement.

La construction des formules de $\mathcal{L}_\Sigma$ se fait en plusieurs étapes. On commence avec des termes, destinés à représenter des objets mathématiques du domaine étudié. Comme dans le cas du calcul propositionnel, on fixe une suite infinie de variables $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots$; on s'autorise à utiliser des métavariables, c'est-à-dire à utiliser $\boldsymbol{x}, \boldsymbol{y}$, *etc.* pour représenter une variable non spécifiée.

DÉFINITION 1.3. (terme) Soit Σ une signature. On appelle *terme* de $\mathcal{L}_\Sigma$ tout mot obtenu à partir des variables $\boldsymbol{x}_{\mathsf{i}}$ et des constantes de Σ en appliquant un nombre fini de transformations $(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}) \mapsto \boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ avec $\boldsymbol{s}$ symbole d'opération k-aire dans Σ.

EXEMPLE 1.4. (terme) Les mots

$$\emptyset, \quad \boldsymbol{x}_2, \quad \mathfrak{P}(\emptyset) \cup \boldsymbol{x}_2, \quad \mathfrak{P}(\mathfrak{P}(\boldsymbol{x}_1 \cup \emptyset)) \cup \boldsymbol{x}_2 \tag{1.2}$$

sont des termes de $\mathcal{L}_{\rm ens^+}$. On suit l'usage d'écrire $(\mathsf{t}_1)\boldsymbol{s}(\mathsf{t}_2)$ pour $\boldsymbol{s}(\mathsf{t}_1, \mathsf{t}_2)$ quand $\boldsymbol{s}$ est un symbole binaire, et, comme pour le calcul propositionnel, on omet des parenthèses pour alléger l'écriture lorsqu'il n'y a pas d'ambiguïté. Noter que, si une signature Σ ne comporte aucun symbole de constante ou d'opération, ainsi que c'est le cas de la signature $\Sigma_{\rm ens}$, alors les seuls termes de $\mathcal{L}_\Sigma$ sont les variables $\boldsymbol{x}_{\mathsf{i}}$.

On introduit maintenant les formules, qui expriment des relations entre des termes.

DÉFINITION 1.5. (formule) Soit Σ une signature. On appelle *formule atomique* de $\mathcal{L}_\Sigma$ tout mot de la forme $\mathsf{t}_1 = \mathsf{t}_2$ ou $\boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ avec $\boldsymbol{r}$ symbole de relation k-aire de Σ, et $\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}$ termes de $\mathcal{L}_\Sigma$. On appelle *formule* de $\mathcal{L}_\Sigma$ tout mot pouvant s'obtenir à partir de formules atomiques en Σ en appliquant un

[2]L'usage qu'on en fera dans la suite montrera qu'on peut assimiler les constantes à des opérations à zéro argument, et donc ne distinguer que deux types de symboles, d'opération et de relation.

nombre fini de transformations $\mathsf{F} \mapsto \neg(\mathsf{F})$, $(\mathsf{F},\mathsf{G}) \mapsto (\mathsf{F})\wedge(\mathsf{G})$, $(\mathsf{F},\mathsf{G}) \mapsto (\mathsf{F})\vee(\mathsf{G})$, $(\mathsf{F},\mathsf{G}) \mapsto (\mathsf{F})\Rightarrow(\mathsf{G})$, $\mathsf{F} \mapsto \exists \boldsymbol{x}_{\mathsf{i}}(\mathsf{F})$, et $\mathsf{F} \mapsto \forall \boldsymbol{x}_{\mathsf{i}}(\mathsf{F})$.

Comme dans le cas des logiques propositionnelles du chapitre VI, et comme il est d'usage, on s'autorisera à supprimer des parenthèses dans les termes et les formules pour autant que ceci ne crée pas d'ambiguïté.

Exemple 1.6. (formule) Le mot $\boldsymbol{x}_2 \in \mathfrak{P}(\emptyset) \cup \boldsymbol{x}_2$ est une formule atomique de $\mathcal{L}_{\text{ens}^+}$, tandis que

$$\exists \boldsymbol{x}_2(\boldsymbol{x}_2 \in (\mathfrak{P}(\emptyset) \cup \boldsymbol{x}_2))\Rightarrow(\mathfrak{P}(\boldsymbol{x}_3) \subseteq \emptyset) \tag{1.3}$$

est une formule (non atomique) de $\mathcal{L}_{\text{ens}^+}$.

Tant l'ensemble des termes de $\mathcal{L}_\Sigma$ que celui des formules de $\mathcal{L}_\Sigma$ est défini comme clôture d'un ensemble de base par un certain nombre de transformations. Comme dans le cas des formules propositionnelles, on en déduit un critère de démonstration par induction.

Proposition 1.7. (induction) *Soit Σ une signature. Pour montrer qu'une propriété $\mathcal{P}$ est vraie pour tous les termes de $\mathcal{L}_\Sigma$, il suffit de montrer*

- *que $\mathcal{P}$ est vraie pour les variables $\boldsymbol{x}_{\mathsf{i}}$ et les symboles de constante de Σ,*
- *et que, pour chaque symbole d'opération k-aire $\boldsymbol{s}$ de Σ, si $\mathcal{P}$ est vraie pour t_1,..., t_k, alors elle est vraie aussi pour $\boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$.*

Pour montrer qu'une propriété $\mathcal{P}$ est vraie pour toutes les formules de $\mathcal{L}_\Sigma$, il suffit de montrer

- *que $\mathcal{P}$ est vraie pour les formules atomiques,*
- *que, si $\mathcal{P}$ est vraie pour F, alors elle est vraie aussi pour $\neg\mathsf{F}$,*
- *que, si $\mathcal{P}$ est vraie pour F et G, alors elle est vraie aussi pour $\mathsf{F}\wedge\mathsf{G}$, $\mathsf{F}\vee\mathsf{G}$, et $\mathsf{F}\Rightarrow\mathsf{G}$, et*
- *que, si $\mathcal{P}$ est vraie pour F, alors, pour toute variable $\boldsymbol{x}$, elle est vraie pour $\exists\boldsymbol{x}(\mathsf{F})$ et $\forall\boldsymbol{x}(\mathsf{F})$.*

Une formule étant un mot, chaque symbole qui y figure a une position bien définie, qu'on peut repérer par son rang en partant du début. On appelle *occurrence* d'un symbole s dans une formule F tout entier n tel que le n-ème symbole de F soit s. Par exemple, $\boldsymbol{x}_2$ a trois occurrences dans (1.3), à savoir 2, 4, et 12 [3].

Définition 1.8. (libre, liée) Pour chaque variable $\boldsymbol{x}_{\mathsf{i}}$ et chaque formule F, on définit inductivement l'ensemble des occurrences *liées* et *libres* de $\boldsymbol{x}_{\mathsf{i}}$ dans F par les règles suivantes :

- si F est sans quantificateur, toutes les occurrences de $\boldsymbol{x}_{\mathsf{i}}$ dans F sont libres ;
- si F est $\forall\boldsymbol{x}_{\mathsf{i}}(\mathsf{G})$ ou $\exists\boldsymbol{x}_{\mathsf{i}}(\mathsf{G})$, toutes les occurrences de $\boldsymbol{x}_{\mathsf{i}}$ dans F sont liées ;

[3] en prenant ici le parti de compter $\boldsymbol{x}_2$ comme un symbole unique ; une option alternative (plus pertinente pour les questions de complexité algorithmique) serait de considérer $\boldsymbol{x}_2$ comme étant un mot de longueur 2

• si F est $\neg\mathsf{G}$, ou $\mathsf{G}\,\mathsf{c}\,\mathsf{H}$, ou $\forall \boldsymbol{x}_\mathsf{j}(\mathsf{G})$ ou $\exists \boldsymbol{x}_\mathsf{j}(\mathsf{G})$ avec $\mathsf{j} \neq \mathsf{i}$, les occurrences libres et liées de $\boldsymbol{x}_\mathsf{i}$ dans F viennent [4] de celles de G et, le cas échéant, H.

Par exemple, dans (1.3), la variable $\boldsymbol{x}_2$ a trois occurrences liées, tandis que la variable $\boldsymbol{x}_3$ n'a qu'une occurrence, qui est libre. On prendra soin qu'une même variable peut avoir simultanément des occurrences libres et des occurrences liées à l'intérieur d'une formule.

▷ *Comme dans le cas des formules propositionnelles, on peut associer inductivement un arbre fini à tout terme, puis à toute formule, comme illustré sur la figure 1. Sous cette forme, la notion de portée d'un quantificateur est claire: une occurrence de la variable* $\boldsymbol{x}_\mathsf{i}$ *dans une formule* F *est liée si le sommet qui lui est associé dans l'arbre* $a(\mathsf{F})$ *se trouve sous au moins un quantificateur* $\exists$ *ou* $\forall$ *dont le fils gauche est étiqueté* $\boldsymbol{x}_\mathsf{i}$*, et libre sinon.* ◁

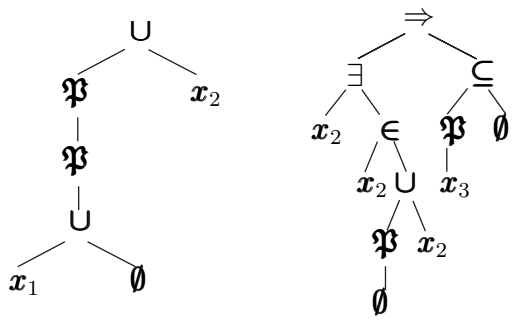

FIGURE 1. Arbres associés au terme $\mathfrak{P}(\mathfrak{P}(\boldsymbol{x}_1 \cup \emptyset)) \cup \boldsymbol{x}_2$ et à la formule $\exists \boldsymbol{x}_2(\boldsymbol{x}_2 \in (\mathfrak{P}(\emptyset) \cup \boldsymbol{x}_2)) \Rightarrow (\mathfrak{P}(\boldsymbol{x}_3) \subseteq \emptyset)$; on lit sur l'arbre associé que la variable $\boldsymbol{x}_2$ a trois occurrences liées puisque situées sous un quantificateur de même nom, ici $\exists \boldsymbol{x}_2$, tandis que la variable $\boldsymbol{x}_3$ n'a qu'une occurrence, qui est libre puisque située sous aucun quantificateur.

DÉFINITION 1.9. (formule close, théorie) Une formule sans occurrence libre de variable est dite *close* [5]. Une famille de formules closes est appelée une *théorie*.

EXEMPLE 1.10. (formule close) La formule $\exists \boldsymbol{x}_2(\boldsymbol{x}_1 = \boldsymbol{x}_2 + \mathbf{1}) \wedge \forall \boldsymbol{x}_1(\boldsymbol{x}_1 = \boldsymbol{x}_1)$ n'est pas close, puisque la première occurrence de $\boldsymbol{x}_1$ (qui en a quatre en tout) est libre. Par contre, $\forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2\, (\boldsymbol{x}_1 = \boldsymbol{x}_2 + \mathbf{1})$ est close.

On somplète la description de la syntaxe de $\mathcal{L}_\Sigma$ avec quelques conventions de notation supplémentaires.

CONVENTION 1.11. (i)(équivalence) On note $\mathsf{F} \Leftrightarrow \mathsf{G}$ pour $(\mathsf{F} \Rightarrow \mathsf{G}) \wedge (\mathsf{G} \Rightarrow \mathsf{F})$.

[4] Cette formulation est imprécise mais devrait être claire : par construction, G est un sous-mot de F, et donc chaque symbole apparaissant dans G a une contrepartie bien définie dans F, même si le rang compté depuis la gauche n'est pas le même.

[5] ou encore est appelée *énoncé*

(*ii*) (quantifications conditionnelles) Si $\boldsymbol{r}$ est un symbole de relation binaire, on note $\exists\boldsymbol{xry}(...)$ pour $\exists\boldsymbol{x}(\boldsymbol{xry}\wedge...)$, et $\forall\boldsymbol{xry}(...)$ pour $\forall\boldsymbol{x}(\boldsymbol{xry}\Rightarrow...)$ [6].

(*iii*) (abus d'écriture) • On écrit $\mathsf{t}_1\neq\mathsf{t}_2$ pour $\neg(\mathsf{t}_1=\mathsf{t}_2)$;

• On écrit $\mathsf{F}\wedge\mathsf{G}\wedge\mathsf{H}$ pour $\mathsf{F}\wedge(\mathsf{G}\wedge\mathsf{H})$, et $\mathsf{F}\vee\mathsf{G}\vee\mathsf{H}$ pour $\mathsf{F}\vee(\mathsf{G}\vee\mathsf{H})$;

• Pour $\boldsymbol{r},\boldsymbol{r}'$ symboles de relation binaire ou le symbole $=$, on écrit $\mathsf{t}_1\boldsymbol{r}\mathsf{t}_2\boldsymbol{r}'\mathsf{t}_3$ pour $(\mathsf{t}_1\boldsymbol{r}\mathsf{t}_2)\wedge(\mathsf{t}_2\boldsymbol{r}'\mathsf{t}_3)$;

• On écrit $\exists\boldsymbol{x},\boldsymbol{y}$ pour $\exists\boldsymbol{x}\exists\boldsymbol{y}$, et $\forall\boldsymbol{x},\boldsymbol{y}$ pour $\forall\boldsymbol{x}\forall\boldsymbol{y}$.

• On écrit $\exists!\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$ pour $\exists\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))\wedge\forall\boldsymbol{x},\boldsymbol{y}((\mathsf{F}(\boldsymbol{x})\wedge\mathsf{F}(\boldsymbol{y}))\Rightarrow\boldsymbol{x}=\boldsymbol{y})$.

▷ *Comme dans le cas de la logique propositionnelle au chapitre VI, la description précédente de la syntaxe de la logique du premier ordre $\mathcal{L}_\Sigma$ fait appel à divers symboles non définis, et, tant pour combler cette lacune que pour les développements ultérieurs, il est utile de définir ces éléments manquants ou, tout au moins, d'en fixer une contrepartie dans le monde des ensembles.* ◁

DÉFINITION 1.12. (logique $\underline{\mathcal{L}_\Sigma}$) (*i*) Pour chaque entier i non nul, on note $\underline{\boldsymbol{x}_i}$ pour $(0,i)$. On appelle *symbole de constante* toute suite finie de la forme $(1,0,a)$, et, pour k entier non nul, *symbole d'opération k-aire* toute suite finie de la forme $(1,k,a)$, et *symbole de relation k-aire* toute suite finie de la forme $(2,k,a)$; on appelle *signature* tout ensemble de symboles de constante, d'opération et de relation.

(*ii*) Pour toute signature Σ, l'ensemble des *termes* de $\underline{\mathcal{L}_\Sigma}$ est défini comme le plus petit ensemble contenant les variables $\underline{\boldsymbol{x}_i}$ et les symboles de constante de Σ, et clos par chacune des transformations $(t_1,...,t_k)\mapsto(s,t_1,...,t_k)$ pour s symbole d'opération k-aire de Σ.

(*iii*) On note $=$ la suite $(2,2,0)$. Pour toute signature Σ, l'ensemble des *formules atomiques* de $\underline{\mathcal{L}_\Sigma}$ est défini comme l'ensemble des suites de la forme $(=,t_1,t_2)$ et $(r,t_1,...,t_k)$, avec r symbole de relation k-aire de Σ et $t_1,...,t_k$ termes de $\underline{\mathcal{L}_\Sigma}$.

(*iv*) On pose $\underline{\neg}:=1$, $\underline{\Rightarrow}:=2$, $\underline{\vee}:=3$, $\underline{\wedge}:=4$, et, pour i entier non nul, on note $\underline{\exists\boldsymbol{x}_i}$ la suite $(3,i)$, et $\underline{\forall\boldsymbol{x}_i}$ la suite $(4,i)$. Pour toute signature Σ, l'ensemble des *formules* de $\underline{\mathcal{L}_\Sigma}$ est défini comme le plus petit ensemble contenant les formules atomiques de $\underline{\mathcal{L}_\Sigma}$, et clos par chacune des transformations $F\mapsto(\neg,F)$, $(F,G)\mapsto(\Rightarrow,F,G)$, $(F,G)\mapsto(\vee,F,G)$, $(F,G)\mapsto(\wedge,F,G)$, $F\mapsto(\underline{\exists\boldsymbol{x}_i},F)$, $F\mapsto(\underline{\forall\boldsymbol{x}_i},F)$,

▷ *La définition précédente calque et précise celles des définitions 1.1, 1.3, et 1.5, tout en rendant explicite la structure d'arbre des formules. De la sorte, on attribue à chaque terme t et à chaque formule F des contreparties $\underline{\mathsf{t}}$ et $\underline{\mathsf{F}}$ qui sont des ensembles (finis). Par exemple, si t est le terme $\mathfrak{P}(\mathfrak{P}(\boldsymbol{x}_1\cup\emptyset))\cup\boldsymbol{x}_2$ considéré dans la figure 1, l'ensemble $\underline{\mathsf{t}}$ qui en est la contrepartie est la suite $(\bigcup,(\mathfrak{P},(\mathfrak{P},(\cup,\underline{\boldsymbol{x}}_1,\emptyset))),\underline{\boldsymbol{x}}_2)$, soit, en supposant (par exemple) qu'on a choisi les représentations $\underline{\bigcup}=(1,1,2)$, $\underline{\mathfrak{P}}=(1,1,3)$, $\underline{\cup}=(1,2,3)$, et $\underline{\emptyset}=(1,0,2)$, la suite*

$$((1,1,2),((1,1,3),((1,1,3),((1,2,3),(0,1),(1,0,2)))),(0,2)),$$

dont on remarque qu'elle appartient à V_ω.

[6] L'apparente dissymétrie entre les cas de $\exists$ et $\forall$ est justifiée par le désir de maintenir le comportement vis-à-vis de la négation sous la forme d'une équivalence de $\neg(\exists\boldsymbol{xry}(...))$ et $\forall\boldsymbol{xry}(\neg(...))$.

Il sera commode dans la suite de fixer une signature une signature de référence. ◁

DÉFINITION 1.13. (signature $\Sigma_{\max}$) On note $\Sigma_{\max}$ la signature consistant en tous les symboles $(1,k,i)$ et $(2,k,i)$ avec i entier non nul. On note $\mathcal{L}_{\max}$ la logique du premier ordre associée à la signature $\Sigma_{\max}$.

▷ *Comme dans l'exemple précédent, on remarque que, pour toute signature Σ incluse dans $\Sigma_{\max}$, tout terme et toute formule de $\mathcal{L}_\Sigma$ est un ensemble fini appartenant à V_ω. Les signatures de l'exemple 1.2 entrent dans ce cadre, pour peu qu'on décide que le symboles de relation $\in$ et $\leqslant$ sont respectivement les suites $(2,2,1)$ et $(2,2,2)$, que le symbole de constante $\mathbf{0}$ est la suite $(1,0,1)$, et que les symboles d'opération $\boldsymbol{S}$, $+$, et $\cdot$ sont respectivement $(1,1,1)$, $(1,2,1)$, et $(1,2,2)$. On laisse au lecteur le soin de choisir des définitions pour les symboles de Σ_{ens^+}.*

Comme dans le cas propositionnel, on pourra dans la suite oublier la distinction entre une formule F et sa contrepartie ensembliste $\underline{\mathsf{F}}$. Malgré tout, en comme dans le cas des entiers, on continuera à utiliser des caractères spécifiques $\mathsf{F},\mathsf{G},\dots$ (plutôt que $F,G,\dots$) pour les formules afin d'insister sur le fait que, même s'ils sont représentables dans les ensembles, ces objets ne sont a priori pas des ensembles, et ne font donc pas partie du monde des ensembles. ◁

1.2. Sémantique.

► Comme dans le cas de la logique propositionnelle, on attribue des valeurs de vérité aux formules du premier ordre. L'évaluation d'une formule est définie par référence à une réalisation convenable, à savoir un contexte où on interprête les symboles de base pour ensuite déterminer de proche en proche la valeur de la formule. ◄

▷ *De même que la syntaxe, la sémantique des logiques du premier ordre n'est définie que pour refléter l'usage des formules comme sténographie des mathématiques, autrement dit déclarer une formule F formellement vraie quand la propriété qu'elle exprime est vraie dans un sens intuitif supposé clair.*

Dans le cas propositionnel, les seuls symboles non logiques sont les variables propositionnelles, et, pour initialiser l'évaluation, on attribue une valeur 0 ou 1 à ces variables. Dans le cas des logiques du premier ordre, les symboles non logiques sont d'une part les variables, et d'autre part les symboles de constante, d'opération et de relation spécifiques à la signature considérée. Calquée sur l'usage escompté des formules, l'initialisation de l'évaluation se fait en fixant un domaine où les variables sont astreintes à prendre leurs valeurs, et une interprétation de chaque symbole de la signature considére Σ par une opération ou une relation sur le domaine. Une telle donnée est appelée structure *de type Σ, ou, de façon exactement synomyme,* réalisation *de $\mathcal{L}_\Sigma$, une expression qui souligne bien l'idée du passage du niveau abstrait des formules où rien n'est ni vrai ni faux à un niveau concret où les valeurs de vérité prennent un sens.* ◁

DÉFINITION 1.14. (structure, réalisation) Soit Σ une signature. Une *structure* de type Σ, aussi appelée *réalisation* de $\mathcal{L}_\Sigma$, est une suite $\mathcal{R}$ composée d'un ensemble non vide $\mathrm{Dom}(\mathcal{R})$ appelé *domaine* de $\mathcal{R}$, et, pour chaque symbole s de Σ, d'une *interprétation* $\mathsf{s}^{\mathcal{R}}$ de s dans $\mathcal{R}$ consistant,

- pour un symbole de constante, en un élément de $\mathrm{Dom}(\mathcal{R})$,
- pour un symbole d'opération k-aire, en une application de $\mathrm{Dom}(\mathcal{R})^{\mathsf{k}}$ dans $\mathrm{Dom}(\mathcal{R})$,
- pour un symbole de relation k-aire, en une relation k-aire sur $\mathrm{Dom}(\mathcal{R})$, c'est-à-dire une application de $\mathrm{Dom}(\mathcal{R})^{\mathsf{k}}$ dans $\{0,1\}$ ou, de façon équivalente, une partie de $\mathrm{Dom}(\mathcal{R})^{\mathsf{k}}$.

EXEMPLE 1.15. (structure) Soit $\mathcal{R}$ la suite $(\mathbb{N}, 0, S, +, \cdot)$. Alors $\mathcal{R}$ est une réalisation de $\mathcal{L}_{\text{arith}}$: le domaine est l'ensemble $\mathbb{N}$ des entiers naturels, l'interprétation $\mathbf{0}^{\mathcal{R}}$ du symbole de constante $\mathbf{0}$ dans $\mathcal{R}$ est l'entier 0, et, de la même façon, l'interprétation $\boldsymbol{S}^{\mathcal{R}}$ du symbole $\boldsymbol{S}$ est l'application successeur, l'interprétation $+^{\mathcal{R}}$ du symbole $+$ est l'addition des entiers, *etc.* La suite $(\mathbb{Z}, 0, S, +, \cdot)$ [7] est une autre structure de type Σ_{arith}, dont le domaine est cette fois l'ensemble des entiers relatifs, et de même $(\mathbb{Q}, 0, S, +, \cdot)$, mais aussi $(\mathbb{N}, 2, ^2, +, +)$, ou $(\mathbb{R}, \pi, \sqrt{\ }, -, +)$.

▷ *Dès lors que les formules ne sont que de nature syntaxique, donc indépendante de toute interprétation et de toute structure, le choix des symboles est indifférent. Dans le cas de l'exemple 1.15 et des formules d'arithmétique, le choix de symboles tels que* $\mathbf{0}$ *ou de* $+$ *est bien sûr influencé par le souci de lisibilité dès lors qu'on a en vue l'interprétation dans la structure particulière* $\mathcal{R}$*. Mais rien n'interdirait d'utiliser d'autres symboles, de même que, symétriquement, rien (sinon les risques pratiques de confusion) n'interdit d'interpréter les symboles* $\mathbf{0}$ *ou* $+$ *par le réel* π *ou la soustraction des réels, comme dans la dernière structure considérée ci-dessus.*

Il est maintenant facile de définir inductivement la valeur d'une formule dans une structure en transcrivant la signification usuelle des connecteurs et des quantificateurs. Le but est d'obtenir une valeur « vrai » ou « faux » — ou, de façon équivalente, 1 *ou* 0 *— pour les formules closes, c'est-à-dire sans variable libre. Si* p *variables ont des occurrences libres, la valeur de la formule n'est définie que si des valeurs prises dans le domaine de la structure sont attribuées à ces variables, et la valeur de la formule dans une structure* $\mathcal{R}$ *se trouve naturellement définie comme une fonction de* $\mathrm{Dom}(\mathcal{R})^{\mathsf{p}}$ *dans* $\{0, 1\}$ *et non un élément défini de* $\{0, 1\}$*.* ◁

NOTATION 1.16. (variables) Ainsi qu'il est usuel, on note $\mathsf{t}(\boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{p}})$ un terme où n'apparaissent que des variables parmi $\boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{p}}$, et, de même, $\mathsf{F}(\boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{p}})$ une formule où les seules variables ayant des occurrences libres sont parmi $\boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{p}}$. Noter l'analogie avec les polynômes, qu'on peut voir comme des termes particuliers. Enfin, on utilise $\vec{a}$ comme abréviation pour une suite finie $(a_1, ..., a_{\mathsf{p}})$.

DÉFINITION 1.17. (p-valeur) Soit Σ une signature, et $\mathcal{R}$ une réalisation de $\mathcal{L}_\Sigma$. Pour $\mathsf{t}(\boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{p}})$ terme de $\mathcal{L}_\Sigma$, on appelle p-*valeur* de t dans $\mathcal{R}$ l'application $\mathsf{t}^{\mathcal{R},\mathsf{p}}$ de $\mathrm{Dom}(\mathcal{R})^{\mathsf{p}}$ dans $\mathrm{Dom}(\mathcal{R})$ définie inductivement par

$$\mathsf{t}^{\mathcal{R},\mathsf{p}}(\vec{a}) = \begin{cases} a_{\mathsf{i}} & \text{si } \mathsf{t} \text{ est } \boldsymbol{x}_{\mathsf{i}}, \\ \boldsymbol{s}^{\mathcal{R},\mathsf{p}}(\mathsf{t}_1^{\mathcal{R},\mathsf{p}}(\vec{a}), ..., \mathsf{t}_{\mathsf{k}}^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{t} \text{ est } \boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_{\mathsf{k}}). \end{cases}$$

[7] Il y a en principe une ambiguïté due à l'utilisation de la même notation pour les diverses additions : on pourrait noter plus précisément $+^{\mathbb{N}}$, $+^{\mathbb{Z}}$, *etc.* ; en pratique, on sait bien qu'il n'y a pas de danger puisque $+^{\mathbb{N}}$ est la restriction de $+^{\mathbb{Z}}$, il n'empêche que ce n'est pas la même opération

Pour $\mathsf{F}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{p})$ formule de $\mathcal{L}_\Sigma$, on appelle p-*valeur* de F dans $\mathcal{R}$ l'application $\mathsf{F}^{\mathcal{R},\mathsf{p}}$ de $\mathrm{Dom}(\mathcal{R})^\mathsf{p}$ dans $\{0,1\}$ définie récursivement par

$$\mathsf{F}^{\mathcal{R},\mathsf{p}}(\vec{a}) = \begin{cases} \mathbf{1}_=(\mathsf{t}_1^{\mathcal{R},\mathsf{p}}(\vec{a}), \mathsf{t}_2^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{F} \text{ est } \mathsf{t}_1 = \mathsf{t}_2, \\ \boldsymbol{r}^{\mathcal{R},\mathsf{p}}(\mathsf{t}_1^{\mathcal{R},\mathsf{p}}(\vec{a}), ..., \mathsf{t}_\mathsf{k}^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{F} \text{ est } \boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}), \\ 1 - \mathsf{G}^{\mathcal{R},\mathsf{p}}(\vec{a}) & \text{si } \mathsf{F} \text{ est } \neg\mathsf{G}, \\ \inf(\mathsf{G}^{\mathcal{R},\mathsf{p}}(\vec{a}), \mathsf{H}^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{F} \text{ est } \mathsf{G}\wedge\mathsf{H}, \\ \sup(\mathsf{G}^{\mathcal{R},\mathsf{p}}(\vec{a}), \mathsf{H}^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{F} \text{ est } \mathsf{G}\vee\mathsf{H}, \\ \sup(1 - \mathsf{G}^{\mathcal{R},\mathsf{p}}(\vec{a}), \mathsf{H}^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{F} \text{ est } \mathsf{G}\Rightarrow\mathsf{H}, \\ \mathbf{1}_=(\mathsf{G}^{\mathcal{R},\mathsf{p}}(\vec{a}), \mathsf{H}^{\mathcal{R},\mathsf{p}}(\vec{a})) & \text{si } \mathsf{F} \text{ est } \mathsf{G}\Leftrightarrow\mathsf{H}, \\ \sup\{\mathsf{G}^{\mathcal{R},\mathsf{p}}(a_1, ..., a_{\mathsf{i}-1}, x, a_{\mathsf{i}+1}, ..., a_\mathsf{p}); x \in \mathrm{Dom}(\mathcal{R})\} & \text{si } \mathsf{F} \text{ est } \exists\boldsymbol{x}_\mathsf{i}(\mathsf{G}), \\ \inf\{\mathsf{G}^{\mathcal{R},\mathsf{p}}(a_1, ..., a_{\mathsf{i}-1}, x, a_{\mathsf{i}+1}, ..., a_\mathsf{p}); x \in \mathrm{Dom}(\mathcal{R})\} & \text{si } \mathsf{F} \text{ est } \forall\boldsymbol{x}_\mathsf{i}(\mathsf{G}), \end{cases}$$

où $\mathbf{1}_=(x,y)$ vaut 1 si $x = y$ et 0 sinon, et où $\{0,1\}$ est ordonné par $0 < 1$. On note aussi $\mathrm{Val}_\mathsf{p}(\mathsf{F}, \mathcal{R}, \vec{a})$ pour $\mathsf{F}^{\mathcal{R},\mathsf{p}}(\vec{a})$.

▷ *La définition précédente est fastidieuse mais triviale: la valeur* $\mathsf{F}^{\mathcal{R},\mathsf{p}}(\vec{a})$ *correspond exactement à ce qu'on obtient lorsqu'on affecte la valeur* a_i *à la variable* $\boldsymbol{x}_\mathsf{i}$*, et qu'on évalue de proche en proche la formule en se servant des opérations et relations de* $\mathcal{R}$*. Par exemple, la* 1*-valeur du terme* $\boldsymbol{x}_1 + \mathbf{1}$ *dans la structure* $(\mathbb{N}, 1, +)$ *est l'application* $n \mapsto n+1$ *de* $\mathbb{N}$ *dans lui-même. De même, la* 1*-valeur en* n *de la formule* $\exists\boldsymbol{x}_2(\boldsymbol{x}_1 = \boldsymbol{x}_2 + \mathbf{1})$ *dans* $(\mathbb{N}, 1, +)$ *est* 1 *exactement pour* $\mathsf{n} \geqslant 1$*.*

On pourra noter que la définition 1.17 est à la fois claire et en même temps assez étrange : en déclarant que $\mathcal{R}$ *satisfait* $\mathsf{F}\wedge\mathsf{G}$ *si* $\mathcal{R}$ *satisfait* F *et* $\mathcal{R}$ *satisfait* G*, on ne fait que reporter la définition de* $\wedge$ *sur celle de la conjonction française « et » supposée pré-existante, et de même pour les autres connecteurs. Ceci ne pose pas de problème si on cherche seulement à mimer une situation métamathématique claire — ce qui est notre cas ici — mais ne serait guère satisfaisant pour qui prétendrait définir ainsi la sémantique ex nihilo (cf. section 4.5).*

Un point par contre qui n'est pas mystérieux est la dépendance de la valeur par rapport à l'entier p*, c'est-à-dire par rapport à la sélection de variables considérée. En effet, une induction facile donne :* ◁

Lemme 1.18. *Soient* $\mathsf{F}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{p})$ *une formule de* $\mathcal{L}_\Sigma$*, et* $\mathcal{R}$ *une réalisation de* $\mathcal{L}_\Sigma$*. Alors la fonction* $\mathsf{F}^{\mathcal{R},\mathsf{p}}$ *ne dépend que des variables* $\boldsymbol{x}_\mathsf{i}$ *qui ont au moins une occurrence libre dans* F*.*

On peut donc définir la valeur de façon non-ambiguë en ne considérant que les variables possédant au moins une occurrence libre.

Définition 1.19. (valeur, satisfaction, modèle, valide, satisfaisable) Soit Σ une signature, et $\mathcal{R}$ une réalisation de $\mathcal{L}_\Sigma$.

(*i*) Si F est une formule de $\mathcal{L}_\Sigma$ dont les variables libres sont $\boldsymbol{x}_{\mathsf{i}_1}, ..., \boldsymbol{x}_{\mathsf{i}_\mathsf{n}}$, alors, pour $\vec{a}$ dans $\mathrm{Dom}(\mathcal{R})^\mathsf{n}$, on définit la *valeur* $\mathsf{F}^{\mathcal{R}}(\vec{a})$, aussi notée $\mathrm{Val}(\mathsf{F}, \mathcal{R}, \vec{a})$, comme la valeur commune de $\mathrm{Val}_\mathsf{p}(\mathsf{F}, \mathcal{R}, \vec{b})$ pour toute suite $\vec{b}$ vérifiant $b_{\mathsf{i}_1} = a_1$,..., $b_{\mathsf{i}_\mathsf{n}} = a_\mathsf{n}$.

(*ii*) On dit qu'une formule F est *satisfaite*, ou *vraie*, *en* $\vec{a}$, ou encore que $\mathsf{F}(\vec{a})$ est *satisfaite*, ou *vraie*, dans $\mathcal{R}$, et on note $\mathcal{R} \models \mathsf{F}(\vec{a})$, si on a $\mathrm{Val}(\mathsf{F}, \mathcal{R}, \vec{a}) = 1$. On dit que F est *satisfaite*, ou *vraie* dans $\mathcal{R}$, et on note $\mathcal{R} \models \mathsf{F}$, si on a $\mathcal{R} \models \mathsf{F}(\vec{a})$ pour tout choix de $\vec{a}$ dans $\mathrm{Dom}(\mathcal{R})$.

(*iii*) Si T est une théorie de $\mathcal{L}_\Sigma$, on dit que $\mathcal{R}$ est *modèle* de T, noté $\mathcal{R} \models \mathsf{T}$, si $\mathcal{R}$ est une réalisation de $\mathcal{L}_\Sigma$ et qu'on a $\mathcal{R} \models \mathsf{F}$ pour chaque formule F dans T.

(*iv*) Une formule, ou un ensemble de formules, est dite *valide* (*resp. satisfaisable*) si elle est vraie dans toute (*resp.* au moins une) structure.

▷ *On notera que, lorsque $\vec{a}$ est une suite d'éléments dans le domaine d'une structure, l'objet $\mathsf{F}(\vec{a})$ n'est pas une formule : une formule est un objet purement syntaxique (un mot), alors qu'ici figurent les éléments $\vec{a}$, qui appartiennent au monde externe, à savoir au domaine dans lequel on évalue F. La notation usuelle $\mathcal{R} \models \mathsf{F}(\vec{a})$ est à considérer d'un seul tenant, et, de fait, il serait plus correct de noter $(\mathcal{R}, \vec{a}) \models \mathsf{F}(\vec{\boldsymbol{x}})$, en distinguant bien entre le sémantique, à gauche du symbole $\models$, et le syntaxique, à sa droite.* ◁

Exemple 1.20. (satisfaction) La formule close $\forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2\, (\boldsymbol{x}_1 = \boldsymbol{x}_2 + \mathbf{1})$ est satisfaite dans la structure $(\mathbb{Z}, 1, +^{\mathbb{Z}})$, mais pas dans $(\mathbb{N}, 1, +^{\mathbb{N}})$, ce qu'on écrit

$$(\mathbb{Z}, 1, +^{\mathbb{Z}}) \models \forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2\, (\boldsymbol{x}_1 = \boldsymbol{x}_2 + \mathbf{1}) \quad \text{et} \quad (\mathbb{N}, 1, +^{\mathbb{N}}) \not\models \forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2\, (\boldsymbol{x}_1 = \boldsymbol{x}_2 + \mathbf{1}),$$

voire simplement $\mathbb{Z} \models \forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2\, (\boldsymbol{x}_1 = \boldsymbol{x}_2 + 1)$ et $\mathbb{N} \not\models \forall \boldsymbol{x}_1\, \exists \boldsymbol{x}_2\, (\boldsymbol{x}_1 = \boldsymbol{x}_2 + 1)$ si les interprétations des symboles sont suffisamment évidentes — mais il s'agit d'un abus de langage : aucun symbole n'a d'interprétation canonique prédéfinie.

1.3. Exprimabilité au premier ordre.

► On discute brièvement le pouvoir d'expression des logiques du premier ordre : celui-ci est grand, mais, d'un autre côté, certaines propriétés simples semblent difficiles à exprimer. ◄

▷ *D'innombrables propriétés mathématiques sont exprimables en logique du premier ordre, ce qui est prévisible puisque les formules du premier ordre ont été introduites comme mise en forme précise des formules usuelles. C'est du reste pour cela qu'on a adopté une syntaxe aussi complète : une partie des fastidieuses vérifications pourrait être évitée en se restreignant par exemple aux symboles logiques $\neg$, $\vee$, $\exists$, mais on s'éloignerait ainsi de la pratique.* ◁

Définition 1.21. (exprimable) Une propriété $\mathcal{P}$ des structures de type Σ est dite *finiment exprimable*[8] *au premier ordre* (*resp. exprimable*[9] *au premier ordre*) s'il existe une formule F (*resp.* une famille T de formules) de $\mathcal{L}_\Sigma$ telle que, pour toute structure $\mathcal{R}$ de type Σ, la propriété $\mathcal{P}$ est vraie dans $\mathcal{R}$ si et seulement si la relation $\mathcal{R} \models \mathsf{F}$ (*resp.* $\mathcal{R} \models \mathsf{T}$) est satisfaite.

▷ *On pourrait penser que* toute *propriété peut être exprimée par une formule du premier ordre : ceci est essentiellement vrai dans la mesure où tous les objets mathématiques peuvent être représentés par des ensembles, et où la quasi-totalité des propriétés des ensembles mentionnées dans la suite sont exprimées par des formules ensemblistes du premier ordre (cf. exemple 1.27). Par contre, lorsqu'on étudie un type d'objet particulier dans un cadre spécifique, c'est-à-dire relativement à une signature fixée, alors les contraintes découlant de la définition des formules entraînent qu'il existe des propriétés non exprimables à l'aide de formules du premier ordre, ou, tout au moins, n'apparaissent a priori pas comme telles de façon claire.* ◁

[8] ou encore *finiment axiomatisable*

[9] ou encore *axiomatisable*

EXEMPLE 1.22. (ordres) La propriété que $(A, <)$ est un ordre (strict) est finiment exprimable au premier ordre en la signature restreinte à un symbole de relation binaire : $(A, <)$ est un ordre si et seulement si $(A, <)$ satisfait la formule du premier ordre

$$\forall \boldsymbol{x}\, \forall \boldsymbol{y}\, \forall \boldsymbol{z}(\neg(\boldsymbol{x} < \boldsymbol{x}) \wedge (\boldsymbol{x} < \boldsymbol{y} < \boldsymbol{z} \Rightarrow \boldsymbol{x} < \boldsymbol{z})).$$

De même la propriété que $(A, <)$ soit un ordre total ; par contre, la propriété d'être un bon ordre pose problème puisque la définition

$$\forall \boldsymbol{X}(\exists \boldsymbol{x}(\boldsymbol{x} \in \boldsymbol{X}) \Rightarrow \exists \boldsymbol{x}(\boldsymbol{x} \in \boldsymbol{X} \wedge \forall \boldsymbol{y} \in \boldsymbol{X}(\neg(\boldsymbol{y} < \boldsymbol{x})))),$$

alias

$$\forall \boldsymbol{X}(\exists \boldsymbol{x}(\boldsymbol{X}(\boldsymbol{x})) \Rightarrow \exists \boldsymbol{x}(\boldsymbol{X}(\boldsymbol{x}) \wedge \forall \boldsymbol{y}(\boldsymbol{X}(\boldsymbol{y}) \Rightarrow \neg(\boldsymbol{y} < \boldsymbol{x})))),$$

n'est pas du premier ordre, puisqu'elle utilise des variables référant à deux types d'objets distincts, ici les éléments et les sous-ensembles du domaine, *alias* les relations unaires sur celui-ci. On remarquera que $\neg(\exists \boldsymbol{x}_1, \boldsymbol{x}_2, ...)(\boldsymbol{x}_1 > \boldsymbol{x}_2 > ...)$, qui exprime une propriété équivalente *modulo* l'axiome des choix dépendants, n'est pas non plus du premier ordre puisqu'elle est de longueur infinie, pas davantage que $\neg(\exists \boldsymbol{s}\, \forall \boldsymbol{n} \in \mathbb{N}\, (\boldsymbol{s}(\boldsymbol{n}) > \boldsymbol{s}(\boldsymbol{n}+1)))$, qui fait appel à deux types d'objets.

EXEMPLE 1.23. (groupes) Que la structure $(G, *)$ composée d'un ensemble et d'une opération binaire $*$ sur cet ensemble soit un groupe est exprimé par la conjonction des deux formules

$$\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}\, (\boldsymbol{x} * (\boldsymbol{y} * \boldsymbol{z}) = (\boldsymbol{x} * \boldsymbol{y}) * \boldsymbol{z}),$$
$$\exists \boldsymbol{e}\, \forall \boldsymbol{x}\, (\boldsymbol{x} * \boldsymbol{e} = \boldsymbol{e} * \boldsymbol{x} = \boldsymbol{x} \wedge \exists \boldsymbol{y}(\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{y} * \boldsymbol{x} = \boldsymbol{e})),$$

et est donc finiment exprimable au premier ordre. Noter que la propriété que G est un groupe d'opération $*$, d'élément neutre 1 et d'inverse $^{-1}$ s'exprime également, relativement à la signature comprenant une constante $\mathbf{1}$, une opération unaire $^{-1}$ et une opération binaire $*$ par la formule alternative

$$\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}\, (\boldsymbol{x} * (\boldsymbol{y} * \boldsymbol{z}) = (\boldsymbol{x} * \boldsymbol{y}) * \boldsymbol{z} \wedge \boldsymbol{x} * \mathbf{1} = \mathbf{1} * \boldsymbol{x} = \boldsymbol{x} \wedge \boldsymbol{x} * \boldsymbol{x}^{-1} = \boldsymbol{x}^{-1} * \boldsymbol{x} = \mathbf{1})$$

ne comportant que des quantifications universelles. De même, la propriété d'être de p-torsion est exprimée par la formule $\forall \boldsymbol{x}(\boldsymbol{x} * \boldsymbol{x} * ... * \boldsymbol{x} = \mathbf{1})$, avec p fois $\boldsymbol{x}$ — où on convient que $\mathsf{t}_1 * \mathsf{t}_2 * \mathsf{t}_3$ signifie $\mathsf{t}_1 * (\mathsf{t}_2 * \mathsf{t}_3)$. Par contre, pour la propriété d'être de torsion, c'est-à-dire que chaque élément est de p-torsion pour au moins un p, dépendant éventuellement de l'élément, la formule $\forall \boldsymbol{x}\, \exists \mathsf{p} \in \mathbb{N}\, (\boldsymbol{x}^{\mathsf{p}} = \mathbf{1})$ ne convient pas, car elle fait intervenir deux variables de types différents. La formule alternative $\forall \boldsymbol{x}(\boldsymbol{x} = \mathbf{1} \vee \boldsymbol{x} * \boldsymbol{x} = \mathbf{1} \vee \boldsymbol{x} * \boldsymbol{x} * \boldsymbol{x} = \mathbf{1} \vee ...)$ ne convient pas davantage, puisqu'elle est infinie. La question reste donc ouverte pour le moment.

EXEMPLE 1.24. (corps) Etre un corps est finiment exprimable au premier ordre, par rapport à une signature comportant deux symboles d'opération binaire, et des symboles de constante pour les éléments neutres. La propriété additionnelle d'être algébriquement clos s'exprime à l'aide d'une liste (infinie) de formules du

premier ordre : il suffit d'exprimer, pour chaque entier n, que chaque polynôme de degré n a un zéro, ce que fait la formule close $\forall \boldsymbol{x}_0, \boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{n}}\, \exists \boldsymbol{y}\, (\boldsymbol{x}_{\mathsf{n}} * \boldsymbol{y}^{\mathsf{n}} + \cdots + \boldsymbol{x}_1 * \boldsymbol{y} + \boldsymbol{x}_0 = \mathbf{0})$, où $\boldsymbol{y}^{\mathsf{n}}$ est une notation abrégée pour $\boldsymbol{y} * (\boldsymbol{y} * ...))$, n fois $\boldsymbol{y}$. Il s'agit donc d'une propriété exprimable au premier ordre, mais, *a priori*, pas nécessairement finiment exprimable. La propriété d'être de caractéristique p est exprimée par l'unique formule $\mathbf{1}+\mathbf{1}+\cdots+\mathbf{1}=\mathbf{0}$, p fois $\mathbf{1}$, et elle est donc finiment exprimable au premier ordre. D'un autre côté, la propriété d'être de caractéristique nulle s'exprime à l'aide de la famille infinie de formules $\mathbf{1}+\mathbf{1} \neq \mathbf{0}$, $\mathbf{1}+\mathbf{1}+\mathbf{1} \neq \mathbf{0}$, $\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1} \neq \mathbf{0}$, *etc.* : la notion est donc exprimable au premier ordre, mais *a priori* pas nécessairement finiment exprimable.

Exemple 1.25. (espaces vectoriels) Il semble y avoir une difficulté, car deux types d'objets différents, les scalaires et les vecteurs, entrent en jeu. En fait, supposant le corps de base K fixé, on peut exprimer que E est un K-espace vectoriel à l'aide de formules du premier ordre en introduisant l'opération unaire $x \mapsto \lambda x$ pour chaque scalaire λ. Les seules variables à considérer sont alors les vecteurs, et les axiomes sont des formules du premier ordre.

Exemple 1.26. (arithmétique) Le système de Peano constitue une base commode, et il met en jeu la signature Σ_{arith} de l'exemple 1.2. Suivant la définition III.1.8, les six premiers axiomes du système de Peano sont des formules de $\mathcal{L}_{\mathrm{arith}}$. Par contre, l'axiome d'induction

$$\forall \boldsymbol{X}((\boldsymbol{X}(\mathbf{0}) \wedge \forall \boldsymbol{x}(\boldsymbol{X}(\boldsymbol{x}) \Rightarrow \boldsymbol{X}(\boldsymbol{S}(\boldsymbol{x})))) \Rightarrow \forall \boldsymbol{x}(\boldsymbol{X}(\boldsymbol{x}))), \tag{1.4}$$

n'est pas du premier ordre, puisqu'y figure la variable $\boldsymbol{X}$ qui réfère non à un élément, mais à un sous-ensemble du domaine dans lequel il s'agit d'évaluer la formule. Cette difficulté est contournée en introduisant un nouveau système PA_1, dit *Peano du premier ordre*, dans lequel on substitue à l'axiome d'induction 1.4 la liste infinie des formules du premier ordre

$$(\mathsf{F}(\mathbf{0}) \wedge \forall \boldsymbol{x}(\mathsf{F}(\boldsymbol{x}) \Rightarrow \mathsf{F}(\boldsymbol{S}(\boldsymbol{x})))) \Rightarrow \forall \boldsymbol{x}(\mathsf{F}(\boldsymbol{x})) \tag{1.5}$$

pour F formule de $\mathcal{L}_{\mathrm{arith}}$ à une variable libre. Ceci revient à restreindre l'induction aux ensembles du type $\{\boldsymbol{x}\,;\, \mathsf{F}(\boldsymbol{x})\}$, c'est-à-dire aux ensembles d'entiers qui peuvent être définis par une formule — lesquels forment une famille dénombrable, alors que la famille de tous les ensembles d'entiers est non dénombrable.

Exemple 1.27. (théorie des ensembles) Les axiomes de Zermelo–Fraenkel constituent une liste (infinie) de formules closes de $\mathcal{L}_{\mathrm{ens}}$. L'option de restreindre l'étude aux ensembles purs est essentielle ici, car c'est elle qui rend raisonnable de ne considérer qu'un seul type d'objet, à savoir des ensembles purs. La structure de référence dans laquelle il semble naturel d'évaluer les formules est la classe $\mathbf{V}$ de tous les ensembles purs, munie de l'appartenance : poser que les axiomes du système ZF sont satisfaits signifie admettre qu'on a $(\mathbf{V}, \in) \models \mathsf{A}$ pour chaque axiome A de ZF. Néanmoins, il y a une difficulté à parler ici d'une structure

dont le domaine n'est pas un ensemble, qui contredit au moins la lettre de la définition 1.14. Ceci sera précisé au chapitre IX.

2. Preuves en logique du premier ordre

► On décrit une notion de preuve pour les logiques du premier ordre calquée, comme dans le cas de la logique propositionnelle booléenne, sur des règles de déduction usuelles. On étudie ici les preuves ainsi obtenues et, en particulier, on établit le théorème de complétude de Gödel qui affirme la coïncidence entre validité et prouvabilité. ◄

▷ *Le théorème de complétude de Gödel est un des résultats fondamentaux de la logique. Sa portée est vaste car il garantit que, pour ce qui est des propriétés exprimables par une formule du premier ordre, les méthodes de démonstration usuelles — et, plus spécifiquement, celles qu'on choisit d'inclure ci-dessous dans la définition des preuves — sont exhaustives (cf. section 4).* ◁

2.1. Preuves.

► Comme dans le cas propositionnel, on introduit une notion de preuve pour la logique du premier ordre à l'aide de règles de déduction, un cas particulier étant constitué par les axiomes, qui sont des règles sans argument permettant de poser une formule comme point de départ. ◄

▷ *A titre de remarque préliminaire, notons qu'à la différence du cas propositionnel où la validité d'une formule peut toujours être décidée sémantiquement en testant toutes les affectations de valeurs de vérité possibles, il n'existe aucun algorithme naïf pour reconnaître si une formule du premier ordre est valide ou satisfaisable : aucune restriction n'est imposée aux structures à considérer et la validité met en jeu une infinité de structures possibles ; on peut tester si une formule est satisfaite ou non dans une structure de domaine fini, mais ceci est impossible dès qu'on considère des structures infinies, ou une infinité de structures même finies.* ◁

DÉFINITION 2.1. (libre) Si F est une formule, $\boldsymbol{x}$ une variable dont toutes les occurrences sont libres dans F, et t un terme, on note $\mathsf{F}(\boldsymbol{x}\leftarrow\mathsf{t})$ [10] la formule obtenue en remplaçant chaque occurrence de $\boldsymbol{x}$ dans F par t. On dit alors que t est *libre* pour $\boldsymbol{x}$ dans F si toutes les occurrences de variables dans t donnent des occurrences libres dans $\mathsf{F}(\boldsymbol{x}\leftarrow\mathsf{t})$.

EXEMPLE 2.2. (libre) Soit F la formule $\exists\boldsymbol{y}(\boldsymbol{y}\neq\boldsymbol{x})$. La variable $\boldsymbol{x}$ n'a qu'une occurrence, libre, dans F. Si $\boldsymbol{z}$ n'est pas $\boldsymbol{y}$, alors $\boldsymbol{z}$ est libre pour $\boldsymbol{x}$ dans F. Par contre $\boldsymbol{y}$ n'est pas libre pour $\boldsymbol{x}$, puisque, dans $\mathsf{F}(\boldsymbol{x}\leftarrow\boldsymbol{y})$, qui est $\exists\boldsymbol{y}(\boldsymbol{y}\neq\underline{\boldsymbol{y}})$, l'occurrence de $\boldsymbol{y}$ soulignée, créée par la substitution à $\boldsymbol{x}$, n'est pas libre.

DÉFINITION 2.3. (axiome, généralisation, preuve) (*i*) Soit Σ une signature. On appelle *axiomes* de $\mathcal{L}_\Sigma$

• les *instances* dans $\mathcal{L}_\Sigma$ des axiomes du calcul propositionnel, c'est-à-dire toutes les formules obtenues à partir d'un axiome de $\mathcal{L}_\bullet$ en substituant des formules de $\mathcal{L}_\Sigma$ aux variables propositionnelles,

• les formules $\forall\boldsymbol{x}(\mathsf{F}\Rightarrow\mathsf{G})\Rightarrow(\mathsf{F}\Rightarrow\forall\boldsymbol{x}(\mathsf{G}))$ avec $\boldsymbol{x}$ sans occurrence libre dans F,

[10] ou simplement $\mathsf{F}(\mathsf{t})$ s'il n'y a pas ambiguïté, et notamment lorsqu'on a écrit $\mathsf{F}(\boldsymbol{x})$ auparavant

- les formules $\forall \boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))\Rightarrow\mathsf{F}(\mathsf{t})$ avec t libre pour $\boldsymbol{x}$ dans $\mathsf{F}(\boldsymbol{x})$,
- les formules $\exists \boldsymbol{x}(\neg\mathsf{F})\Leftrightarrow\neg\,\forall \boldsymbol{x}\,(\mathsf{F})$,
- les formules $\boldsymbol{x}_1=\boldsymbol{x}_1$, $\boldsymbol{x}_1=\boldsymbol{x}_2\Rightarrow\boldsymbol{x}_2=\boldsymbol{x}_1$, $(\boldsymbol{x}_1=\boldsymbol{x}_2\wedge\boldsymbol{x}_2=\boldsymbol{x}_3)\Rightarrow\boldsymbol{x}_1=\boldsymbol{x}_3$, et $(\boldsymbol{x}_1=\boldsymbol{x}_{\mathsf{k}+1}\wedge\ldots\wedge\boldsymbol{x}_{\mathsf{k}}=\boldsymbol{x}_{2\mathsf{k}})\Rightarrow(\boldsymbol{s}(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{\mathsf{k}})=\boldsymbol{s}(\boldsymbol{x}_{\mathsf{k}+1},\ldots,\boldsymbol{x}_{2\mathsf{k}}))$,
  $(\boldsymbol{x}_1=\boldsymbol{x}_{\mathsf{k}+1}\wedge\ldots\wedge\boldsymbol{x}_{\mathsf{k}}=\boldsymbol{x}_{2\mathsf{k}})\Rightarrow(\mathsf{r}(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{\mathsf{k}})\Leftrightarrow\mathsf{r}(\boldsymbol{x}_{\mathsf{k}+1},\ldots,\boldsymbol{x}_{2\mathsf{k}}))$

avec $\boldsymbol{s}$, r respectivement symbole d'opération et de relation k-aire de Σ.

(*ii*) On dit que G se déduit de F par *généralisation* s'il existe i tel que G est $\forall \boldsymbol{x}_{\mathsf{i}}(\mathsf{F})$.

(*iii*) On dit que F_1, ..., F_{p} est une *preuve* (par coupure, généralisation et axiomes) à partir de T dans $\mathcal{L}_\Sigma$ si, pour chaque i, la formule F_{i} est dans T, ou est un axiome de $\mathcal{L}_\Sigma$, ou il existe $\mathsf{j}<\mathsf{i}$ tel que F_{i} est obtenu par généralisation à partir de F_{j}, ou il existe $\mathsf{j},\mathsf{k}<\mathsf{i}$ tels que F_{i} est obtenu par coupure[11] à partir de F_{j} et F_{k}. On note $\mathsf{T}\vdash_{\mathcal{L}_\Sigma}\mathsf{F}$, ou $\mathsf{T}\vdash\mathsf{F}$ s'il existe une preuve à partir de T se terminant par F.

▷ *Les axiomes et les règles de la définition 2.3 correspondent tous à des schémas de démonstration usuels et on peut donc s'attendre à ce qu'ils soient compatibles avec la sémantique : si ces règles ont été considérées comme pertinentes depuis des siècles, c'est qu'elles ne mènent pas à des conclusions réfutables. La vérification formelle de la compatiblité avec la sémantique de la définition 1.19 se fait par une induction facile qui paraphrase les arguments dits de bon sens, et qu'on ne détaillera pas. Les seuls points à remarquer sont la nécessité des restrictions posées. En effet, dans les axiomes du deuxième groupe, la restriction sur les variables libres est nécessaire pour que la formule soit valide : par exemple, si* $\mathbf{0}$ *est un symbole de constante, la formule* $\forall \boldsymbol{x}(\boldsymbol{x}{=}\mathbf{0}{\Rightarrow}\boldsymbol{x}{=}\mathbf{0})$ *est valide, alors que la formule* $\boldsymbol{x}{=}\mathbf{0}{\Rightarrow}\forall \boldsymbol{x}\,(\boldsymbol{x}{=}\mathbf{0})$ *ne l'est pas, puisque, si* $\mathcal{R}$ *est une réalisation dont le domaine a au moins deux éléments, il existe* a *dans* $\mathrm{Dom}\mathcal{R}$ *tel que* $a{=}\mathbf{0}$ *est satisfait dans* $\mathcal{R}$*, alors que* $\forall \boldsymbol{x}(\boldsymbol{x}{=}\mathbf{0})$ *ne l'est pas, soit* $\mathcal{R}\not\models a{=}\mathbf{0}{\Rightarrow}\,\forall \boldsymbol{x}\,(\boldsymbol{x}{=}\mathbf{0})$*. De même, dans les axiomes du troisième groupe, la restriction sur les termes pouvant être substitués est nécessaire : la formule* $\forall \boldsymbol{x}\,\exists \boldsymbol{y}\,(\boldsymbol{y}\neq\boldsymbol{x})\Rightarrow\exists \boldsymbol{y}(\boldsymbol{y}\neq\boldsymbol{y})$ *n'est pas valide, puisque* $\forall \boldsymbol{x}\,\exists \boldsymbol{y}\,(\boldsymbol{y}\neq\boldsymbol{x})$ *est satisfaisable alors que* $\exists \boldsymbol{y}(\boldsymbol{y}\neq\boldsymbol{y})$ *ne l'est pas.* ◁

Proposition 2.4. (cohérence) *Si* T *est une théorie et* F *une formule de* $\mathcal{L}_\Sigma$ *vérifiant* $\mathsf{T}\vdash\mathsf{F}$*, toute structure satisfaisant* T *satisfait aussi* F*. En particulier, si* T *est valide, il en est de même de* F*. Par conséquent,* $\vdash\mathsf{F}$ *entraîne* $\models\mathsf{F}$ *: toute formule prouvable est valide.*

▷ *Comme dans le cas propositionnel, c'est la réciproque de cette propriété, c'est-à-dire la complétude, qui constitue le résultat non trivial, puisqu'il s'agit de montrer que les quelques schémas de preuves introduits dans la définition 2.3 épuisent toutes les possiblités compatibles avec la sémantique. Comme au chapitre VI, on va établir une forme globale de complétude mettant en jeu une famille de formules plutôt qu'une formule unique, mais, à la différence du cas précédent, on va commencer par la forme globale. On verra plus loin que cette forme globale de complétude entraîne la forme locale (« toute formule valide est prouvable »), ainsi que plusieurs autres corollaires non triviaux.* ◁

Appelant comme on chapitre VI *consistante* toute théorie T qui ne prouve jamais à la fois une formule et sa négation, on va démontrer le résultat suivant, dû à Kurt Gödel :

[11] c'est-à-dire que F_{j} est la formule $\mathsf{F}_{\mathsf{i}}{\Rightarrow}\mathsf{F}_{\mathsf{k}}$

PROPOSITION 2.5. (théorème de complétude) *Soit* Σ *une signature bien ordonnable*[12]*. Alors toute théorie consistante de* $\mathcal{L}_\Sigma$ *admet un modèle dont le domaine est bien ordonnable de cardinal au plus* $\max(\aleph_0, \mathrm{card}(\Sigma))$.

2.2. Le théorème de la déduction.

► La démonstration du théorème de complétude passe par des résultats préparatoires, dont chacun pris séparément est facile. Le premier est un énoncé analogue au théorème de la déduction du calcul propositionnel. ◄

LEMME 2.6. (*i*) *Toute formule de* $\mathcal{L}_\Sigma$ *qui est une instance d'une formule propositionnelle valide est prouvable.*
(*ii*) *Soit* $\mathsf{H}(\boldsymbol{X}_1, ..., \boldsymbol{X}_\mathsf{n})$ *une formule propositionnelle dont les variables sont parmi* $\boldsymbol{X}_1$, ..., $\boldsymbol{X}_\mathsf{n}$. *Si une théorie* T *de* $\mathcal{L}_\Sigma$ *prouve* $\mathsf{F}_\mathsf{i} \Leftrightarrow \mathsf{G}_\mathsf{i}$ *pour* $\mathsf{i} = 1, ..., \mathsf{n}$, *alors* T *prouve* $\mathsf{H}(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n}) \Leftrightarrow \mathsf{H}(\mathsf{G}_1, ..., \mathsf{G}_\mathsf{n})$[13].

DÉMONSTRATION. (*i*) Supposons $\mathsf{F} = \mathsf{H}(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n})$, où H est une formule propositionnelle valide. Par le théorème de complétude propositionnel, H est prouvable par coupure à partir des axiomes de $\mathcal{L}_\bullet$: il existe une preuve H_1, ..., H_p dans $\mathcal{L}_\bullet$ se terminant par H. Alors la suite $\mathsf{H}_1(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n})$, ..., $\mathsf{H}_\mathsf{p}(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n})$[14] est une preuve dans $\mathcal{L}_\Sigma$: une instance d'un axiome de $\mathcal{L}_\bullet$ est un axiome de $\mathcal{L}_\Sigma$, et la coupure est, en un sens évident, compatible avec la substitution.

(*ii*) On applique (*i*) à la formule propositionnelle valide

$$(\boldsymbol{X}_1 \Leftrightarrow \boldsymbol{Y}_1) \Rightarrow ((\boldsymbol{X}_2 \Leftrightarrow \boldsymbol{Y}_2) \Rightarrow (...((\boldsymbol{X}_\mathsf{n} \Leftrightarrow \boldsymbol{Y}_\mathsf{n}) \Rightarrow \mathsf{H}(\boldsymbol{X}_1, ..., \boldsymbol{X}_\mathsf{n}) \Leftrightarrow \mathsf{H}(\boldsymbol{Y}_1, ..., \boldsymbol{Y}_\mathsf{n})))...))$$

pour obtenir

$$\mathsf{T} \vdash (\mathsf{F}_1 \Leftrightarrow \mathsf{G}_1) \Rightarrow ((\mathsf{F}_2 \Leftrightarrow \mathsf{G}_2) \Rightarrow (...((\mathsf{F}_\mathsf{n} \Leftrightarrow \mathsf{G}_\mathsf{n}) \Rightarrow \mathsf{H}(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n}) \Leftrightarrow \mathsf{H}(\mathsf{G}_1, ..., \mathsf{G}_\mathsf{n}))...)),$$

d'où $\mathsf{T} \vdash \mathsf{H}(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n}) \Leftrightarrow \mathsf{H}(\mathsf{G}_1, ..., \mathsf{G}_\mathsf{n}))$ en appliquant n coupures. □

PROPOSITION 2.7. (théorème de la déduction) *Soient* T *une théorie et* F, G *deux formules de* $\mathcal{L}_\Sigma$. *On suppose* F *close. Alors* $\mathsf{T} \vdash \mathsf{F} \Rightarrow \mathsf{G}$ *équivaut à* $\mathsf{T} \cup \{\mathsf{F}\} \vdash \mathsf{G}$.

DÉMONSTRATION. Comme dans le cas propositionnel, il est clair que la condition est nécessaire, car, si on a $\mathsf{T} \vdash \mathsf{F} \Rightarrow \mathsf{G}$, alors $\mathsf{T} \cup \{\mathsf{F}\}$ prouve à la fois F et $\mathsf{F} \Rightarrow \mathsf{G}$, donc G par coupure.

Inversement, on montre par récurrence sur n que, s'il existe une preuve de longueur n de G à partir de $\mathsf{T} \cup \{\mathsf{F}\}$, alors il existe une preuve de $\mathsf{F} \Rightarrow \mathsf{G}$ à partir de T. Supposons que H_1, ..., H_n est une preuve de G à partir de $\mathsf{T} \cup \{\mathsf{F}\}$. Par hypothèse de récurrence, il existe une preuve à partir de T pour chacune des formules $\mathsf{F} \Rightarrow \mathsf{H}_1$, ..., $\mathsf{F} \Rightarrow \mathsf{H}_{\mathsf{n}-1}$. On considère H_n, c'est-à-dire G. Quatre cas sont possibles.

(*i*) La formule G est un axiome, ou une formule de T. Comme $\boldsymbol{Y} \Rightarrow (\boldsymbol{X} \Rightarrow \boldsymbol{Y})$ est une formule propositionnelle valide, on a $\mathsf{T} \vdash \mathsf{G}$ et, par le lemme 2.6, $\vdash \mathsf{G} \Rightarrow (\mathsf{F} \Rightarrow \mathsf{G})$, d'où $\mathsf{T} \vdash \mathsf{G} \Rightarrow (\mathsf{F} \Rightarrow \mathsf{G})$ *a fortiori*, puis, par coupure, $\mathsf{T} \vdash \mathsf{F} \Rightarrow \mathsf{G}$.

(*ii*) La formule G est la formule F. La formule propositionnelle $\boldsymbol{X} \Rightarrow \boldsymbol{X}$ est valide, donc, par le

[12] On n'a pas posé de restriction sur la taille de la signature ; l'hypothèse que la signature est une liste bien ordonnée, automatiquement vérifiée si la signature est finie ou dénombrable, évite le recours ultérieur à l'axiome du choix

[13] en notant $\mathsf{H}(\mathsf{F}_1, ..., \mathsf{F}_\mathsf{n})$ la formule obtenue à partir de H en substituant F_i à $\boldsymbol{X}_\mathsf{i}$ pour $\mathsf{i} = 1, ..., \mathsf{n}$

[14] une récurrence montre qu'on peut toujours supposer que seules les variables propositionnelles apparaissant dans la dernière formule apparaissent dans les formules intermédiaires

lemme 2.6, on a $\vdash \mathsf{F}\Rightarrow\mathsf{F}$ et, *a fortiori*, $\mathsf{T}\vdash\mathsf{F}\Rightarrow\mathsf{G}$.
(*iii*) Il existe $\mathsf{j}<\mathsf{n}$ tel que G est $\forall\boldsymbol{x}(\mathsf{H}_\mathsf{j})$ pour une certaine variable $\boldsymbol{x}$. Par hypothèse de récurrence, il existe une preuve à partir de T pour $\mathsf{F}\Rightarrow\mathsf{H}_\mathsf{j}$. On obtient une preuve de $\mathsf{F}\Rightarrow\forall\boldsymbol{x}\,(\mathsf{H}_\mathsf{j}))$ en ajoutant à cette preuve

$\forall\boldsymbol{x}(\mathsf{F}\Rightarrow\mathsf{H}_\mathsf{j})$ (généralisation)
$\forall\boldsymbol{x}(\mathsf{F}\Rightarrow\mathsf{H}_\mathsf{j})\Rightarrow(\mathsf{F}\Rightarrow\forall\boldsymbol{x}\,(\mathsf{H}_\mathsf{j}))$ (axiome de $\mathcal{L}_\Sigma$ puisque F est close)
$\mathsf{F}\Rightarrow\forall\boldsymbol{x}\,(\mathsf{H}_\mathsf{j})$, (coupure)

(*iv*) Il existe $\mathsf{i},\mathsf{j}<\mathsf{n}$ tels que H_j est une formule $\mathsf{H}_\mathsf{i}\Rightarrow\mathsf{G}$. L'argument est alors rigoureusement le même que dans le cas propositionnel. □

COROLLAIRE 2.8. *Soient* T *est une théorie et* F *une formule de* $\mathcal{L}_\Sigma$.
(*i*) *La théorie* T *prouve* F *si et seulement si* $\mathsf{T}\cup\{\neg\mathsf{F}\}$ *est inconsistant.*
(*ii*) *Si* T *est consistante, l'une au moins des extensions* $\mathsf{T}\cup\{\mathsf{F}\}$, $\mathsf{T}\cup\{\neg\mathsf{F}\}$ *est consistante.*

DÉMONSTRATION. (*i*) Supposons $\mathsf{T}\vdash\mathsf{F}$. Alors $\mathsf{T}\cup\{\neg\mathsf{F}\}$ prouve à la fois F et $\neg\mathsf{F}$, donc est inconsistant. Inversement, supposons que $\mathsf{T}\cup\{\neg\mathsf{F}\}$ prouve à la fois G et $\neg\mathsf{G}$. Comme $\boldsymbol{Y}\Rightarrow(\neg\boldsymbol{Y}\Rightarrow\boldsymbol{X})$ est une formule propositionnelle valide, $\mathsf{G}\Rightarrow(\neg\mathsf{G}\Rightarrow\mathsf{F})$ est prouvable par le lemme 2.6, donc, par coupure, $\mathsf{T}\cup\{\neg\mathsf{F}\}$ prouve F. Par le théorème de la déduction, on a $\mathsf{T}\vdash\neg\mathsf{F}\Rightarrow\mathsf{F}$. Or $(\neg\boldsymbol{X}\Rightarrow\boldsymbol{X})\Rightarrow\boldsymbol{X}$ est une formule propositionnelle valide, donc, toujours par le lemme 2.6, $(\neg\mathsf{F}\Rightarrow\mathsf{F})\Rightarrow\mathsf{F}$ est prouvable, et, par coupure, on obtient $\mathsf{T}\vdash\mathsf{F}$.

(*ii*) Supposons $\mathsf{T}\cup\{\mathsf{F}\}$ et $\mathsf{T}\cup\{\neg\mathsf{F}\}$ inconsistantes. Alors $\mathsf{T}\cup\{\neg\neg\mathsf{F}\}$ est inconsistant, car $\neg\neg\mathsf{F}\Rightarrow\mathsf{F}$ est un axiome, et on déduit de toute preuve utilisant F comme hypothèse une preuve utilisant $\neg\neg\mathsf{F}$ à la place. Utilisant (*i*) on déduit que T prouve $\neg\mathsf{F}$ et F, donc est inconsistante. □

2.3. Théories explicitement complètes.

► On établit le résultat du théorème de complétude, c'est-à-dire l'existence d'un modèle, pour des théories consistantes d'un type particulier, dites explicitement complètes. ◄

▷ *La difficulté pour démontrer le théorème de complétude est de construire ex nihilo une réalisation de* $\mathcal{L}_\Sigma$ *satisfaisant des formules prescrites. Comme, a priori, les seuls objets disponibles sont les objets syntaxiques tels que termes ou formules, il est naturel de chercher à construire un modèle à partir de ces objets. Le principe de base consiste à construire un modèle* $\mathcal{M}$ *dont le domaine soit l'ensemble des termes construits à partir des seuls symboles de constante de la logique* $\mathcal{L}_\Sigma$ *considérée, de sorte que l'interprétation d'un terme* t *dans* $\mathcal{M}$ *soit* t *lui-même. Cette approche naïve ne peut certainement pas réussir dans tous les cas, et pour de multiples raisons : il se peut que* Σ *ne contienne aucun symbole de constante, il se peut que la théorie* T *prouve des égalités* $\mathsf{t}=\mathsf{t}'$ *entre des termes différents, enfin (et surtout) cette approche ne peut rien garantir pour les formules avec quantificateurs.*

Chacune de ces difficultés peut être contournée. Dans cette section, on montre comment construire un modèle suivant le schéma esquissé ci-dessus dans le cas où la théorie vérifie certaines hypothèses ad hoc. On montrera dans la section suivante qu'on peut toujours se ramener à ce cas favorable. ◁

DÉFINITION 2.9. (complète, explicitement complète) Une théorie consistante T de $\mathcal{L}_\Sigma$ est dite *complète* si, pour toute formule close F de $\mathcal{L}_\Sigma$, la théorie T prouve soit F, soit $\neg\mathsf{F}$; elle est dite *explicitement complète* si elle est complète et si, de plus, pour toute formule $\mathsf{F}(\boldsymbol{x})$ de $\mathcal{L}_\Sigma$ à une seule variable libre telle que T prouve $\exists\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$, il existe un symbole de constante $\boldsymbol{c}$ telle que T prouve $\mathsf{F}(\boldsymbol{c})$.

▷ *Une théorie explicitement complète a donc une opinion définie, positive ou négative, sur chaque formule close, et, par ailleurs, la signature est suffisamment riche pour contenir, pour chaque formule close existentielle, un nom pour un élément distingué la vérifiant dès qu'il en existe.*

Pour une théorie explicitement complète T*, la construction d'un modèle à partir des termes sans variable est facile, à ceci près que* T *peut prouver des égalités entre termes distincts. La solution est évidente : pour peu que la relation* $\mathsf{T} \vdash \mathsf{t} = \mathsf{t}'$ *soit une congruence, c'est-à-dire soit une relation d'équivalence compatible avec les opérations et les relations, il suffit de passer au quotient.* ◁

LEMME 2.10. *Supposons que* T *est une théorie explicitement complète de* $\mathcal{L}_\Sigma$*. Soit* C_Σ *l'ensemble des termes sans variable de* $\mathcal{L}_\Sigma$ *et soit* $\equiv$ *la relation sur* C_Σ *définie par* $\mathsf{t} \equiv \mathsf{t}' \Leftrightarrow \mathsf{T} \vdash \mathsf{t} = \mathsf{t}'$*. Alors* $\equiv$ *est une relation d'équivalence compatible avec les opérations et relations de* Σ *au sens où la conjonction de* $\mathsf{t}_1 \equiv \mathsf{t}'_1$*, ...,* $\mathsf{t}_\mathsf{k} \equiv \mathsf{t}'_\mathsf{k}$ *entraîne* $\boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}) \equiv \boldsymbol{s}(\mathsf{t}'_1, ..., \mathsf{t}'_\mathsf{k})$ *pour tout symbole* k*-aire d'opération* $\boldsymbol{s}$ *et* $\boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}) \Leftrightarrow \boldsymbol{r}(\mathsf{t}'_1, ..., \mathsf{t}'_\mathsf{k})$ *pour tout symbole* k*-aire de relation* $\boldsymbol{r}$*.*

DÉMONSTRATION. L'hypothèse que T est explicitement complète garantit qu'il existe au moins un symbole de constante dans Σ puisque T prouve au moins l'axiome $\exists \boldsymbol{x}(\boldsymbol{x} = \boldsymbol{x})$, et donc C_Σ n'est pas vide. Comme $\boldsymbol{x}_1 = \boldsymbol{x}_1$ est un axiome de $\mathcal{L}_\Sigma$, on déduit $\vdash \forall \boldsymbol{x}_1(\boldsymbol{x}_1 = \boldsymbol{x}_1)$ par généralisation, puis $\vdash \mathsf{t} = \mathsf{t}$ par particularisation, donc *a fortiori* $\mathsf{T} \vdash \mathsf{t} = \mathsf{t}$, soit $\mathsf{t} \equiv \mathsf{t}$. Utilisant de la même façon les axiomes $\boldsymbol{x}_1 = \boldsymbol{x}_2 \Rightarrow \boldsymbol{x}_2 = \boldsymbol{x}_1$ et $(\boldsymbol{x}_1 = \boldsymbol{x}_2 \wedge \boldsymbol{x}_2 = \boldsymbol{x}_3) \Rightarrow \boldsymbol{x}_1 = \boldsymbol{x}_3$, on obtient que $\equiv$ est symétrique et transitive, donc c'est une relation d'équivalence.

Pour $\boldsymbol{s}$ symbole d'opération k-aire, la formule $(\boldsymbol{x}_1 = \boldsymbol{x}_{\mathsf{k}+1} \wedge ... \wedge \boldsymbol{x}_\mathsf{k} = \boldsymbol{x}_{2\mathsf{k}}) \Rightarrow \boldsymbol{s}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}) = \boldsymbol{s}(\boldsymbol{x}_{\mathsf{k}+1}, ..., \boldsymbol{x}_{2\mathsf{k}})$ est un axiome de $\mathcal{L}_\Sigma$. Par généralisation et particularisation, on déduit que, si on a $\mathsf{t}_\mathsf{i} \equiv \mathsf{t}'_\mathsf{i}$ pour $\mathsf{i} = 1, ...\mathsf{k}$, alors on a $\mathsf{T} \vdash \boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}) = \boldsymbol{s}(\mathsf{t}'_1, ..., \mathsf{t}'_\mathsf{k})$, soit $\boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}) \equiv \boldsymbol{s}(\mathsf{t}'_1, ..., \mathsf{t}'_\mathsf{k})$. Par conséquent $\equiv$ est compatible avec $\boldsymbol{s}$.

Enfin, utilisant l'axiome $(\boldsymbol{x}_1 = \boldsymbol{x}_{\mathsf{k}+1} \wedge ... \wedge \boldsymbol{x}_\mathsf{k} = \boldsymbol{x}_{2\mathsf{k}}) \Rightarrow (\boldsymbol{r}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}) \Leftrightarrow \boldsymbol{r}(\boldsymbol{x}_{\mathsf{k}+1}, ..., \boldsymbol{x}_{2\mathsf{k}}))$ pour $\boldsymbol{r}$ symbole de relation k-aire de Σ, et supposant toujours $\mathsf{t}_\mathsf{i} \equiv \mathsf{t}'_\mathsf{i}$ pour $\mathsf{i} = 1, ...\mathsf{k}$, on déduit $\mathsf{T} \vdash \boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}) \Leftrightarrow \boldsymbol{r}(\mathsf{t}'_1, ..., \mathsf{t}'_\mathsf{k})$. Par conséquent $\equiv$ est compatible avec $\boldsymbol{r}$. □

LEMME 2.11. (*i*) *Toute théorie explicitement complète de* $\mathcal{L}_\Sigma$ *admet un modèle dont le domaine est un quotient de l'ensemble des termes sans variable de* $\mathcal{L}_\Sigma$*.*

(*ii*) *Si la signature* Σ *est bien ordonnable, toute théorie explicitement complète de* $\mathcal{L}_\Sigma$ *admet un modèle dont le domaine est un sous-ensemble de l'ensemble des termes sans variable de* $\mathcal{L}_\Sigma$*.*

DÉMONSTRATION. (*i*) Soit, comme dans le lemme 2.10, C_Σ l'ensemble des termes sans variable de $\mathcal{L}_\Sigma$. Pour t dans C_Σ, on note $[\mathsf{t}]$ la $\equiv$-classe de t. On définit une structure $\mathcal{M}$ de domaine $C_\Sigma/\equiv$ comme suit : pour $\boldsymbol{c}$ symbole de constante, $\boldsymbol{c}^\mathcal{M}$ est $[\boldsymbol{c}]$; pour $\boldsymbol{s}$ symbole d'opération k-aire, $\boldsymbol{s}^\mathcal{M}$ est définie par $\boldsymbol{s}^\mathcal{M}([\mathsf{t}_1], ..., [\mathsf{t}_\mathsf{k}]) := [\boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})]$; pour $\boldsymbol{r}$ symbole de relation k-aire, on déclare $\boldsymbol{r}^\mathcal{M}([\mathsf{t}_1], ..., [\mathsf{t}_\mathsf{k}])$ vrai pour $\mathsf{T} \vdash \boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$. Le lemme 2.10 légitime ces définitions, et une induction facile donne $\mathsf{t}^\mathcal{M} = [\mathsf{t}]$ pour tout terme sans variable t.

Il reste à voir que la structure $\mathcal{M}$ ainsi construite est un modèle de T. On va montrer que, pour toute formule close F de $\mathcal{L}_\Sigma$, la structure $\mathcal{M}$ satisfait F si et seulement si T prouve F. On raisonne par induction sur le nombre d'occurrences de quantificateurs dans F et, pour un nombre donné, par récurrence sur la longueur.

Si F est atomique, elle est du type $\mathsf{t} = \mathsf{t}'$ ou $\boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$, où $\mathsf{t}, \mathsf{t}', \mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}$ sont des termes sans variable. Dans le premier cas, $\mathcal{M} \models \mathsf{t} = \mathsf{t}'$ équivaut à $\mathsf{t} \equiv \mathsf{t}'$, donc à $\mathsf{T} \vdash \mathsf{t} = \mathsf{t}'$. Dans le second, $\mathcal{M} \models \boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ équivaut à $\mathsf{T} \vdash \boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ par définition de $\boldsymbol{r}^\mathcal{M}$.

Supposons $\mathsf{F} = \neg\mathsf{G}$. Si on a $\mathsf{T} \vdash \mathsf{F}$, alors, comme T est consistante, on a $\mathsf{T} \nvdash \mathsf{G}$, donc, par hypothèse d'induction, $\mathcal{M} \not\models \mathsf{G}$, donc $\mathcal{M} \models \neg\mathsf{G}$, soit $\mathcal{M} \models \mathsf{F}$. Inversement, supposons $\mathcal{M} \models \mathsf{F}$. Alors on a $\mathcal{M} \not\models \mathsf{G}$, donc, par hypothèse d'induction, $\mathsf{T} \nvdash \mathsf{G}$. L'hypothèse que T est explicitement complète implique $\mathsf{T} \vdash \mathsf{F}$.

Supposons $\mathsf{F} = \mathsf{G}\wedge\mathsf{H}$. Si on a $\mathsf{T} \vdash \mathsf{F}$, alors on a nécessairement $\mathsf{T} \vdash \mathsf{G}$ et $\mathsf{T} \vdash \mathsf{H}$, car G et H sont prouvables à partir de $\{\mathsf{G}\wedge\mathsf{H}\}$. Par hypothèse d'induction, on déduit $\mathcal{M} \models \mathsf{G}$ et $\mathcal{M} \models \mathsf{H}$, d'où $\mathcal{M} \models \mathsf{G}\wedge\mathsf{H}$, soit $\mathcal{M} \models \mathsf{F}$. Inversement, supposons $\mathcal{M} \models \mathsf{F}$, donc $\mathcal{M} \models \mathsf{G}$ et $\mathcal{M} \models \mathsf{H}$. Par hypothèse d'induction, on a $\mathsf{T} \vdash \mathsf{G}$ et $\mathsf{T} \vdash \mathsf{H}$, d'où $\mathsf{T} \vdash \mathsf{F}$ puisque $\mathsf{G}\wedge\mathsf{H}$ est prouvable à partir de $\{\mathsf{G}, \mathsf{H}\}$. Les cas de $\vee$, $\Rightarrow$, et $\Leftrightarrow$ sont similaires.

Supposons que F est $\forall\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$. Supposons $\mathsf{T} \vdash \mathsf{F}$. Soit t quelconque dans C_Σ. Comme $\forall\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))\Rightarrow\mathsf{G}(\mathsf{t})$ est un axiome, on a $\mathsf{T} \vdash \mathsf{G}(\mathsf{t})$, d'où, par hypothèse d'induction, $\mathcal{M} \models \mathsf{G}([\mathsf{t}])$. Ceci étant valable pour tout terme dans C_Σ, on a $\mathcal{M} \models \mathsf{F}$. Inversement, supposons $\mathsf{T} \nvdash \mathsf{F}$. L'hypothèse que T est explicitement complète entraîne $\mathsf{T} \vdash \neg\mathsf{F}$, soit $\mathsf{T} \vdash \neg\,\forall\boldsymbol{x}\,(\mathsf{G}(\boldsymbol{x}))$. Comme $\neg\,\forall\boldsymbol{x}\,(\mathsf{G}(\boldsymbol{x}))\Leftrightarrow\exists\boldsymbol{x}\,(\neg\mathsf{G}(\boldsymbol{x}))$ est un axiome, on déduit $\mathsf{T} \vdash \exists\boldsymbol{x}(\neg\mathsf{G}(\boldsymbol{x}))$. Puisque T est explicitement complète, il existe un symbole de constante $\boldsymbol{c}$ dans Σ tel qu'on ait $\mathsf{T} \vdash \neg\mathsf{G}(\boldsymbol{c})$. On a donc $\mathcal{M} \models \neg\mathsf{G}([\boldsymbol{c}])$ par hypothèse d'induction, et, par conséquent, $\mathcal{M} \models \exists\boldsymbol{x}(\neg\mathsf{G}(\boldsymbol{x}))$, donc $\mathcal{M} \not\models \forall\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$.

Supposons enfin que F est $\exists\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$. Si on a $\mathsf{T} \vdash \mathsf{F}$, alors, comme ci-dessus, on doit avoir $\mathsf{T} \vdash \mathsf{G}(\boldsymbol{c})$ pour un certain symbole de constante $\boldsymbol{c}$, d'où $\mathcal{M} \models \mathsf{G}([\boldsymbol{c}])$ par hypothèse d'induction, et donc $\mathcal{M} \models \mathsf{F}$. Inversement, si on a $\mathcal{M} \models \mathsf{F}$, il doit exister un terme t dans C_Σ vérifiant $\mathcal{M} \models \mathsf{G}([\mathsf{t}])$, d'où $\mathsf{T} \vdash \mathsf{G}(\mathsf{t})$ par hypothèse d'induction. L'hypothèse que T est explicitement complète entraîne que, si T ne prouvait pas F, il prouverait $\neg\mathsf{F}$, et, de là, $\forall\boldsymbol{x}(\neg\mathsf{G}(\boldsymbol{x}))$, puis $\neg\mathsf{F}(\mathsf{t})$, ce qui contredit le résultat précédent. On a donc $\mathsf{T} \vdash \mathsf{F}$.

(*ii*) Si on suppose la signature Σ bien ordonnable (donc en particulier si Σ est finie ou dénombrable), alors il existe une énumération $(\mathsf{t}_\alpha)_{\alpha<\kappa}$ des termes sans variable de $\mathcal{L}_\Sigma$, et, dans chaque classe d'équivalence $[\mathsf{t}]$, on peut sélectionner comme élément distingué le terme t_α de plus petit indice. On obtient ainsi une structure $\mathcal{M}'$ telle que l'interprétation $\mathsf{t}^{\mathcal{M}'}$ d'un terme sans variable est t_α avec α minimal tel que T prouve $\mathsf{t} = \mathsf{t}_\alpha$. Les détails sont faciles. □

2.4. La méthode de Henkin.

► On complète la démonstration du théorème de complétude en montrant que toute théorie consistante admet une extension explicitement complète. ◄

On va maintenant établir le résultat suivant :

LEMME 2.12. *Soit Σ une signature bien ordonnable et T une théorie consistante de $\mathcal{L}_\Sigma$. Alors il existe une signature Σ' de cardinal $\max(\aleph_0, \mathrm{card}(\Sigma))$ incluant Σ et une théorie explicitement complète T' de $\mathcal{L}_{\Sigma'}$ incluant T.*

Conjugué au lemme 2.11, le lemme 2.12 entraîne le théorème de complétude (proposition 2.5), puisqu'un modèle pour T' donne un modèle pour T lorsqu'on oublie les symboles de $\Sigma' \setminus \Sigma$.

▷ *Deux lacunes peuvent rendre une théorie consistante T non explicitement complète, à savoir l'existence de formules closes F telles que T ne prouve ni F, ni $\neg\mathsf{F}$, et celle de formules closes $\exists\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$ telles que T prouve $\exists\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$ mais qu'il n'existe pas de constante $\boldsymbol{c}$ telle que T prouve $\mathsf{F}(\boldsymbol{c})$. Le principe est d'ajouter de proche en proche à T des formules et à Σ des constantes de façon à combler ces lacunes. Un peu de soin est nécessaire pour garantir que la consistance est maintenue à chaque étape, et que rien n'a été oublié à la fin.* ◁

LEMME 2.13. *Supposons que Σ est une signature bien ordonnable de cardinal κ. Alors les termes, les formules, et les formules closes de $\mathcal{L}_\Sigma$ forment des ensembles bien ordonnables de cardinal* $\max(\aleph_0, \kappa)$.

DÉMONSTRATION. Il s'agit de fixer des énumérations des termes, formules, et formules closes de $\mathcal{L}_\Sigma$ à partir d'une énumération des symboles de Σ. La tâche est facile une fois fixée une bijection entre κ et les suites finies d'éléments de κ. On renvoie au chapitre VIII où ceci sera fait de façon explicite (dans le cas $\kappa = \aleph_0$). □

▷ *L'avant-dernier lemme préparatoire est une version formelle de la méthode usuelle consistant à démontrer une formule close en donnant un nom non encore utilisé à un objet plutôt qu'à utiliser partout une variable avec un quantificateur $\forall$.* ◁

LEMME 2.14. *Soient T une théorie, $\mathsf{F}(\boldsymbol{x})$ une formule à une seule variable libre, et $\boldsymbol{c}$ un symbole de constante n'apparaissant pas dans F ni dans T. Alors*
(i) la relation $\mathsf{T} \vdash \mathsf{F}(\boldsymbol{c})$ entraîne $\mathsf{T} \vdash \forall \boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$;
(ii) si $\mathsf{T} \cup \{\exists \boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))\}$ est consistant, il en est de même de $\mathsf{T} \cup \{\mathsf{F}(\boldsymbol{c})\}$.

DÉMONSTRATION. *(i)* Soit F_1, ..., F_n une preuve de $\mathsf{F}(\boldsymbol{c})$ à partir de T. Soit $\boldsymbol{x}$ une variable n'apparaissant dans aucune des formules F_i, et soit F'_i la formule obtenue en remplaçant partout $\boldsymbol{c}$ par $\boldsymbol{x}$. Alors F'_1, ..., F'_n est une preuve à partir de T : si F_i est un axiome, il en est de même de F'_i ; si F_i est dans T, on a $\mathsf{F}'_\mathsf{i} = \mathsf{F}_\mathsf{i}$ puisque, par hypothèse, $\boldsymbol{c}$ n'apparaît pas dans T ; si F_i est obtenue par généralisation à partir de F_j, il en est de même pour F'_i à partir de F'_j puisque la variable sur laquelle on quantifie n'est pas $\boldsymbol{x}$; enfin si F_i est obtenue par coupure à partir de F_j et F_k, il en est de même pour F'_i à partir de F'_j et F'_k. Donc T prouve F'_n, qui est $\mathsf{F}(\boldsymbol{x})$, puis, par généralisation, $\forall \boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$.

(ii) Supposons $\mathsf{T} \cup \{\mathsf{F}(\boldsymbol{c})\}$ non consistant. Par le corollaire 2.8 du théorème de la déduction, on obtient $\mathsf{T} \vdash \neg\mathsf{F}(\boldsymbol{c})$, d'où $\mathsf{T} \vdash \forall \boldsymbol{x}(\neg\mathsf{F}(\boldsymbol{x}))$ en appliquant *(i)* à $\neg\mathsf{F}$, puis $\mathsf{T} \vdash \neg\, \exists \boldsymbol{x}\, (\mathsf{F}(\boldsymbol{x}))$, qui contredit la consistance de $\mathsf{T} \cup \{\exists \boldsymbol{x}(\mathsf{F}(\boldsymbol{x})\}$. □

▷ *On en vient au dernier lemme préparatoire. Lorsqu'on passe d'une signature Σ à une signature plus riche Σ', il y a davantage de formules dans $\mathcal{L}_{\Sigma'}$ que dans $\mathcal{L}_\Sigma$, donc davantage de preuves, et il se pourrait a priori qu'une théorie consistante de $\mathcal{L}_\Sigma$ devienne inconsistante dans $\mathcal{L}_{\Sigma'}$. Ce n'est pas le cas :* ◁

LEMME 2.15. *Supposons que T est une théorie consistante de $\mathcal{L}_\Sigma$, et que Σ' est obtenue à partir de Σ en ajoutant des symboles de constantes. Alors T est une théorie consistante de $\mathcal{L}_{\Sigma'}$.*

DÉMONSTRATION. Supposons que F_1, ..., F_p et G_1, ..., G_q sont des preuves respectivement de H et de $\neg\mathsf{H}$ à partir de T dans $\mathcal{L}_{\Sigma'}$. Soient $\boldsymbol{c}_1$, ..., $\boldsymbol{c}_\mathsf{r}$ les symboles de constantes de $\Sigma' \setminus \Sigma$ apparaissant dans ces preuves, et soient $\boldsymbol{z}_1$, ..., $\boldsymbol{z}_\mathsf{r}$ des variables n'y apparaissant pas. Soient F'_i et G'_i les formules obtenues à partir de F_i et G_i en remplaçant chaque $\boldsymbol{c}_\mathsf{n}$ par $\boldsymbol{z}_\mathsf{n}$. Comme dans la démonstration du lemme 2.14, on voit que F'_1, ..., F'_p et G'_1, ..., G'_q sont des preuves de $\mathcal{L}_\Sigma$, et, par construction, F'_p est la négation de G'_q, donc T n'est pas consistante dans $\mathcal{L}_\Sigma$. □

Ce contexte précisé, on peut démontrer le lemme 2.12.

DÉMONSTRATION DU LEMME 2.12. Soit $\kappa := \max(\aleph_0, \mathrm{card}(\Sigma))$. On définit Σ' comme la signature obtenue en ajoutant à Σ une suite de symboles de constantes $(\boldsymbol{c}_\alpha)_{\alpha<\kappa}$ indexée par κ. Alors Σ' est une signature bien ordonnable de cardinal κ. Par le lemme 2.13, on peut fixer une énumération $(\mathsf{F}_\alpha)_{\alpha<\kappa}$ des formules closes de $\mathcal{L}_{\Sigma'}$.

Le but est d'étendre T en une théorie explicitement complète de $\mathcal{L}_{\Sigma'}$. Pour cela, on construit récursivement une suite croissante de théories consistantes $(\mathsf{T}_\alpha)_{\alpha\leqslant\kappa}$ de $\mathcal{L}_{\Sigma'}$ de sorte que T_κ soit explicitement complète. De plus, la construction assurera que, pour $\alpha<\kappa$, les ordinaux γ tels que $\boldsymbol{c}_\gamma$ figure dans au moins une des formules de T_α forment un segment initial propre de κ.

On part de $\mathsf{T}_0 := \mathsf{T}$. L'hypothèse que T est consistante comme théorie de $\mathcal{L}_\Sigma$ et le lemme 2.15 garantissent que T est consistante comme théorie de $\mathcal{L}_{\Sigma'}$, et l'induction peut commencer.

Pour λ ordinal limite, on pose $\mathsf{T}_\lambda := \bigcup_{\alpha<\lambda}\mathsf{T}_\alpha$. La seule chose à vérifier est la consistance de T_λ. Or une réunion croissante de théories consistantes est consistante, en vertu du lemme VI.3.12(*iii*), dont l'adaptation de $\mathcal{L}_\bullet$ à $\mathcal{L}_\Sigma$ est immédiate.

Supposons $\alpha=\beta+1$. Il s'agit de définir T_α à partir de T_β. On considère la formule F_β. Deux cas sont possibles. Si $\mathsf{T}_\beta\cup\{\mathsf{F}_\beta\}$ n'est pas consistante, alors, par le corollaire 2.8(*ii*), $\mathsf{T}_\beta\cup\{\neg\mathsf{F}_\beta\}$ est consistante, et on pose $\mathsf{T}_\alpha := \mathsf{T}_\beta\cup\{\neg\mathsf{F}_\beta\}$. Supposons maintenant $\mathsf{T}_\beta\cup\{\mathsf{F}_\beta\}$ consistante, avec F_β non du type $\exists\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$. On pose alors $\mathsf{T}_\alpha := \mathsf{T}_\beta\cup\{\mathsf{F}_\beta\}$. Supposons enfin $\mathsf{T}_\beta\cup\{\mathsf{F}_\beta\}$ consistante, avec $\mathsf{F}_\beta=\exists\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$ où G est une formule à une seule variable libre. On pose $\mathsf{T}_\alpha := \mathsf{T}_\beta\cup\{\mathsf{F}_\beta,\mathsf{G}(\boldsymbol{c}_\beta)\}$. Le lemme 2.14 garantit que T_α est consistante.

Soit T' la théorie T_κ. Alors T' est consistante comme union croissante de théories consistantes. Soit F une formule close quelconque de $\mathcal{L}_{\Sigma'}$. Alors il existe un ordinal α tel que F est F_α, et donc, par construction, F ou $\neg\mathsf{F}$ est dans $\mathsf{T}_{\alpha+1}$, donc dans T', et T' est complète. Enfin, supposons que $\mathsf{G}(\boldsymbol{x})$ est une formule de $\mathcal{L}_{\Sigma'}$ ayant $\boldsymbol{x}$ comme seule variable libre et que T' prouve $\exists\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$. Alors il existe α tel que $\exists\boldsymbol{x}(\mathsf{G}(\boldsymbol{x}))$ est F_α. A l'étape α, on a trouvé F_α consistant avec T_α car, sinon, $\neg\mathsf{F}_\alpha$ aurait été mis dans $\mathsf{T}_{\alpha+1}$ et serait donc dans T', contredisant l'hypothèse que T' prouve F_α. On a donc certainement posé $\mathsf{T}_{\alpha+1} := \mathsf{T}_\alpha\cup\{\mathsf{F}_\alpha,\mathsf{G}(\boldsymbol{c}_\alpha)\}$, et, par conséquent, T' contient $\mathsf{G}(\boldsymbol{c}_\alpha)$. Donc T' est une théorie explicitement complète. □

▷ *Comme dans le cas propositionnel, on pourra noter que tous les axiomes et règles de déduction de la logique $\mathcal{L}_\Sigma$ ont été utilisés dans la démonstration ci-dessus du théorème de complétude. Il n'y a là aucun hasard : au contraire, la liste des axiomes a été fixée a posteriori comme celle qui permet l'argument précédent, le seul point réellement important étant que la liste soit suffisamment explicite et, de façon précise, qu'il existe un algorithme permettant de décider si une formule est ou non un axiome de $\mathcal{L}_\Sigma$ dès que Σ est explicite.* ◁

2.5. Forme locale du théorème de complétude.

► Le théorème de complétude (proposition 2.5) est donc démontré dans sa forme globale concernant un ensemble de formules closes. On en déduit facilement une forme locale de complétude. ◄

PROPOSITION 2.16. (théorème de complétude, forme locale) *Toute formule du premier ordre valide est prouvable.*

DÉMONSTRATION. Supposons que F est une formule de $\mathcal{L}_\Sigma$ valide dont les variables libres sont parmi $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_\mathsf{p}$. Soit Σ' la sous-signature de Σ formée par les symboles apparaissant dans F. Alors Σ' est finie, donc bien ordonnable. Soit G la formule close $\forall\boldsymbol{x}_1\ldots\forall\boldsymbol{x}_\mathsf{p}\,(\mathsf{F})$ de $\mathcal{L}_{\Sigma'}$. Alors G est valide, et, par conséquent, la théorie $\{\neg\mathsf{G}\}$ n'a pas de modèle, donc, par la proposition 2.5, elle n'est pas consistante. Il résulte alors du corollaire 2.8(*i*) que G est prouvable, et, de là, que F l'est par particularisation. □

3. Applications du théorème de complétude

► On décrit ici deux types d'applications du théorème de complétude pour les logiques du premier ordre, à savoir d'une part la méthode

sémantique de prouvabilité, et d'autre part les conséquences de la complétude en termes de limitation du pouvoir d'expression. ◀

▷ *Le théorème de complétude est le point de départ de la théorie des modèles, qui est l'étude des structures du point de vue des formules du premier ordre qu'elles satisfont. A ce titre, un grand nombre de résultats peuvent être qualifiés d'applications de ce théorème. Orienté vers les développements ultérieurs de ce texte, l'aperçu donné ici est extrêmement partiel, et il ne donne qu'une très faible idée de ce qui est aujourd'hui un domaine entier des mathématiques, avec notamment des applications profondes à la théorie des groupes et à la géométrie algébrique.* ◁

3.1. La méthode sémantique.

▶ Le théorème de complétude permet de démontrer des résultats de prouvabilité : pour montrer qu'une formule F est prouvable à partir d'une théorie T, il suffit de montrer que F est satisfaite dans tout modèle de T. ◀

▷ *Les preuves en logique du premier ordre ont été définies en calquant des schémas de démonstration usuels, mais en minimisant les régles et les axiomes. Il en résulte qu'il est difficile ou, au moins, fastidieux de construire des preuves formelles. En rattachant la prouvabilité à la validité, le théorème de complétude fournit un moyen alternatif souvent beaucoup plus commode. Ce schéma, qui sera à la base du développement de la théorie axiomatique des ensembles dans la partie suivante de ce texte, est illustré ici sur des énoncés simples d'arithmétique.* ◁

Le point de départ est une application directe du théorème de complétude :

PROPOSITION 3.1. (conséquence) *Soit Σ une signature bien ordonnable, T une théorie de $\mathcal{L}_\Sigma$, et F une formule close de $\mathcal{L}_\Sigma$. Alors F est prouvable à partir de T si et seulement si tout modèle de T satisfait F.*

DÉMONSTRATION. (La démonstration est la même que dans le cas propositionnel). Soit $\mathcal{M}$ un modèle de T, s'il en existe. Comme les axiomes sont valides, ils sont satisfaits dans $\mathcal{M}$, et, inductivement, il en est de même de toute formule prouvable par coupure et généralisation à partir de T et des axiomes.

Inversement, supposons que tout modèle de T satisfait F. Alors $\mathsf{T} \cup \{\neg\mathsf{F}\}$ n'est pas satisfaisable, donc, par le théorème de complétude, cette théorie n'est pas consistante. Par le corollaire 2.8(i), on déduit que T prouve F. □

DÉFINITION 3.2. (système PA−Ind) On note PA−Ind le sous-système du système de Peano PA obtenu en otant l'axiome d'induction [15].

Par hypothèse, la structure $(\mathbb{N}, 0, S, +, \cdot)$ est un modèle de PA−Ind, mais, ainsi qu'on le verra dans la suite de cette section, il existe de nombreux autres modèles de PA−Ind. On se propose, à titre d'illustration de la méthode sémantique, de montrer le résultat suivant, où, pour n entier non nul, on note $\boldsymbol{S}^{\mathsf{n}}\boldsymbol{0}$ le terme $\boldsymbol{S}(...(\boldsymbol{S}(\boldsymbol{0}))...)$, n symboles $\boldsymbol{S}$.

LEMME 3.3. *Pour tous entiers $\mathsf{p}, \mathsf{q}, \mathsf{r}$ satisfaisant $\mathsf{p}+\mathsf{q} = \mathsf{r}$, le système* PA−Ind *prouve la formule $\boldsymbol{S}^{\mathsf{p}}\boldsymbol{0} + \boldsymbol{S}^{\mathsf{q}}\boldsymbol{0} = \boldsymbol{S}^{\mathsf{r}}\boldsymbol{0}$.*

[15] Noter que PA−Ind se compose de six formules, et donc est équivalent à l'unique formule qui en est la conjonction.

Démonstration syntaxique du lemme 3.3. On montre $\mathsf{PA}{-}\mathsf{Ind} \vdash \boldsymbol{S}^{\mathsf{r}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$ simultanément pour tout p en utilisant une récurrence sur q. Pour $\mathsf{q} = 0$, les formules à prouver sont $\mathsf{PA}{-}\mathsf{Ind} \vdash \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$. Voici une telle preuve :

F_1: $\forall \boldsymbol{x}(\boldsymbol{x} + \mathbf{0} = \boldsymbol{x})$ (axiome de $\mathsf{PA}{-}\mathsf{Ind}$)

F_2: $\forall \boldsymbol{x}(\boldsymbol{x} + \mathbf{0} = \boldsymbol{x}) \Rightarrow \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ (axiome de $\mathcal{L}_{\mathrm{arith}}$ puisque $\boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ est libre pour $\boldsymbol{x}$ dans F_1)

F_3: $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ (coupure à partir de F_1 et F_2)

Supposons maintenant $\mathsf{q} > 0$. Soit $\mathsf{q}' = \mathsf{q} - 1$, et $\mathsf{r}' = \mathsf{r} - 1$. Pour tout p, on a $\mathsf{r}' = \mathsf{p} + \mathsf{q}'$, donc, par hypothèse d'induction, $\mathsf{PA}{-}\mathsf{Ind}$ prouve $\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0}$. Il s'agit de construire une preuve de $\boldsymbol{S}^{\mathsf{r}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$ à partir de $\mathsf{PA}{-}\mathsf{Ind} \cup \{\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0}\}$. Voici une telle preuve :

F_1: $\boldsymbol{x}_1 = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{x}_1) = \boldsymbol{S}(\boldsymbol{x}_2)$ (axiome de $\mathcal{L}_{\mathrm{arith}}$)

F_2: $\forall \boldsymbol{x}_1(\boldsymbol{x}_1 = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{x}_1) = \boldsymbol{S}(\boldsymbol{x}_2))$ (généralisation à partir de F_1)

F_3: $\forall \boldsymbol{x}_1(\boldsymbol{x}_1 = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{x}_1) = \boldsymbol{S}(\boldsymbol{x}_2)) \Rightarrow (\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{x}_2))$ (axiome de $\mathcal{L}_{\mathrm{arith}}$, puisque $\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}$ est libre pour $\boldsymbol{x}_1$ dans F_2)

F_4: $\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{x}_2)$ (coupure à partir de F_2 et F_3)

F_5: $\forall \boldsymbol{x}_2(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{x}_2))$ (généralisation à partir de F_4)

F_6: $\forall \boldsymbol{x}_2(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{x}_2 \Rightarrow \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{x}_2)) \Rightarrow (\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0} \Rightarrow \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0}))$ (axiome de $\mathcal{L}_{\mathrm{arith}}$, puisque $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0}$ est libre pour $\boldsymbol{x}_2$ dans F_5)

F_7: $\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0} \Rightarrow \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0})$ (coupure à partir de F_5 et F_6)

F_8: $\boldsymbol{S}^{\mathsf{r}'}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0}$ (hypothèse)

F_9: $\boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0})$, soit encore $\boldsymbol{S}^{\mathsf{r}}\mathbf{0} = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0})$ puisque $\boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0})$ est $\boldsymbol{S}^{\mathsf{r}}\mathbf{0}$ (coupure à partir de F_8 et F_9)

F_{10}: $\forall \boldsymbol{x}_1\, \forall \boldsymbol{x}_2\, (\boldsymbol{x}_1 + \boldsymbol{S}(\boldsymbol{x}_2) = \boldsymbol{S}(\boldsymbol{x}_1 + \boldsymbol{x}_2))$ (axiome de $\mathsf{PA}{-}\mathsf{Ind}$)

F_{11}: $\forall \boldsymbol{x}_1\, \forall \boldsymbol{x}_2\, (\boldsymbol{x}_1 + \boldsymbol{S}(\boldsymbol{x}_2) = \boldsymbol{S}(\boldsymbol{x}_1 + \boldsymbol{x}_2)) \Rightarrow \forall \boldsymbol{x}_2(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}(\boldsymbol{x}_2) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{x}_2))$ (axiome de $\mathcal{L}_{\mathrm{arith}}$, puisque $\boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ est libre pour $\boldsymbol{x}_1$ dans F_{10})

F_{12}: $\forall \boldsymbol{x}_2(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}(\boldsymbol{x}_2) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{x}_2))$ (coupure à partir de F_{10} et F_{11})

F_{13}: $\forall \boldsymbol{x}_2(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}(\boldsymbol{x}_2) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{x}_2)) \Rightarrow \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}(\boldsymbol{S}^{\mathsf{q}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0})$ (axiome de $\mathcal{L}_{\mathrm{arith}}$, puisque $\boldsymbol{S}^{\mathsf{q}'}\mathbf{0}$ est libre pour $\boldsymbol{x}_2$ dans F_{12})

F_{14}: $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}(\boldsymbol{S}^{\mathsf{q}'}\mathbf{0}) = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0})$ (coupure à partir de F_{12} et F_{13})

et on tire $\boldsymbol{S}^{\mathsf{r}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$ de F_9 et F_{14} : la formule $(\boldsymbol{x}_1 = \boldsymbol{x}_3 \wedge \boldsymbol{x}_2 = \boldsymbol{x}_3) \Rightarrow \boldsymbol{x}_1 = \boldsymbol{x}_2$ (qui n'est *pas* un axiome) est valide, donc prouvable dans $\mathcal{L}_{\mathrm{arith}}$, donc *a fortiori* à partir de $\mathsf{PA}{-}\mathsf{Ind}$ (le faire !). □

Démonstration sémantique du lemme 3.3. Soit $\mathcal{M}$ un modèle de $\mathsf{PA}{-}\mathsf{Ind}$. On montre par récurrence sur q que $\mathsf{p} + \mathsf{q} = \mathsf{r}$ entraîne $\mathcal{M} \models \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$. On suppose d'abord $\mathsf{q} = 0$. Comme $\mathcal{M}$ satisfait l'axiome $\forall \boldsymbol{x}_1(\boldsymbol{x}_1 + \mathbf{0} = \boldsymbol{x}_1)$, on a $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$. Supposons ensuite $\mathsf{q} > 0$. Soit $\mathsf{q}' := \mathsf{q} - 1$, et $\mathsf{r}' := \mathsf{r} - 1$. On a alors $\mathsf{p} + \mathsf{q}' = \mathsf{r}'$, donc $\mathcal{M} \models \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}'}\mathbf{0}$ par hypothèse de récurrence. Comme $\mathcal{M}$ satisfait l'axiome Add_2, on obtient $\mathcal{M} \models \boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}'}\mathbf{0}) = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}(\boldsymbol{S}^{\mathsf{q}'}\mathbf{0}) = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$, donc $\mathcal{M} \models \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}(\boldsymbol{S}^{\mathsf{r}'}\mathbf{0}) = \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$. Par le théorème de complétude, $\mathsf{PA}{-}\mathsf{Ind}$ prouve donc $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$. □

▷ *La démonstration est la même dans les deux cas, seule diffère la façon de la rédiger ; pour ce qui est de la lisibilité et de l'intelligibilité, la comparaison devrait être éloquente — mais, d'un autre côté, il y a un certain prix à payer en termes de contexte métamathématique (cf. section 4.5), et, d'autre part, rien ne dit qu'un choix plus avisé des règles et des conventions ne pourrait pas améliorer significativement l'approche syntaxique.* ◁

3.2. Extensions par définition.

► Comme application de la méthode sémantique, on montre l'inocuité des extensions par définition consistant à enrichir la signature à l'aide de symboles additionnels représentant des notions définissables. ◄

▷ *Dans les chapitres I et III, on a plusieurs fois enrichi la signature* $\Sigma_{\rm ens}$ *de la théorie des ensembles de nouveaux symboles représentant diverses opérations et relations définissables, en présence des axiomes de Zermelo, à partir de l'unique relation d'appartenance. Il est facile de vérifier que, ce faisant, on ne modifie en rien la force logique de la théorie, c'est-à-dire les formules pouvant être prouvées.* ◁

PROPOSITION 3.4. (extension par définition 1) *Supposons que* T *est une théorie de* $\mathcal{L}_\Sigma$ *et que* $\mathsf{D}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k})$ *est une formule de* $\mathcal{L}_\Sigma$*. Soit* Σ^+ *la signature obtenue en ajoutant à* Σ *un nouveau symbole de relation* k*-aire* $\boldsymbol{r}$*, et* T^+ *la théorie obtenue en ajoutant à* T *la formule* $\mathsf{Intro}_{\boldsymbol{r}}$ *:*

$$\forall \boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k} (\boldsymbol{r}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}) \Leftrightarrow \mathsf{D}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k})).$$

Pour F *formule de* $\mathcal{L}_{\Sigma^+}$*, on note* $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$ *la formule de* $\mathcal{L}_\Sigma$ *obtenue en remplaçant dans* F *toutes les sous-formules atomiques de la forme* $\boldsymbol{r}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ *par* $\mathsf{D}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$*.*

(i) Tout modèle $\mathcal{M}$ *de* T *s'enrichit de façon unique en un modèle* $\mathcal{M}^+$ *de* T^+*, et, pour toute formule* F *de* $\mathcal{L}_{\Sigma^+}$*, il y a équivalence entre* $\mathcal{M}^+ \models \mathsf{F}$ *et* $\mathcal{M} \models \mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$*.*

(ii) Pour F *formule de* $\mathcal{L}_{\Sigma^+}$*, il y a équivalence entre* $\mathsf{T}^+ \vdash \mathsf{F}$ *et* $\mathsf{T} \vdash \mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$*.*

DÉMONSTRATION. *(i)* On enrichit la structure $\mathcal{M}$ en une structure $\mathcal{M}^+$ de type Σ^+ en ajoutant comme interprétation de $\boldsymbol{r}$ la relation r définie par $r(\vec{a}) \Leftrightarrow \mathcal{M} \models \mathsf{D}(\vec{a})$. Alors la formule $\mathsf{Intro}_{\boldsymbol{r}}$ est satisfaite dans $\mathcal{M}^+$, qui est donc modèle de T^+. Inversement, si $\mathcal{M}^+$ est une structure de type Σ^+ enrichissant $\mathcal{M}$ et satisfaisant $\mathsf{Intro}_{\boldsymbol{r}}$, l'interprétation de $\boldsymbol{r}$ dans $\mathcal{M}$ ne peut être que celle définie ci-dessus.

Dans les conditions précédentes, et pour toute formule F de $\mathcal{L}_{\Sigma^+}$, les formules F et $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$ sont simultanément vraie ou fausses dans $\mathcal{M}^+$ puisque $\mathcal{M}^+ \models \boldsymbol{r}(\vec{a})$ équivaut à $\mathcal{M}^+ \models \mathsf{D}(\vec{a})$. Enfin, puisque, par construction, $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$ est une formule de $\mathcal{L}_\Sigma$, il est équivalent de dire qu'elle est satisfaite dans $\mathcal{M}^+$ et dans $\mathcal{M}$.

(ii) Supposons $\mathsf{T}^+ \vdash \mathsf{F}$, et soit $\mathcal{M}$ un modèle quelconque de T. Par *(i)*, il existe un unique enrichissement $\mathcal{M}^+$ de $\mathcal{M}$ en un modèle de T^+. Par hypothèse, $\mathcal{M}^+$ satisfait F, donc, par *(i)*, $\mathcal{M}$ satisfait $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$. Par le théorème de complétude, on déduit que T prouve $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$. Inversement, supposons que T prouve $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$, et soit $\mathcal{M}$ un modèle quelconque de T^+. Puisque T est inclus dans T^+, la formule $\mathrm{elim}_{\boldsymbol{r}}(\mathsf{F})$ est *a fortiori* prouvable à partir de T^+, donc elle est satisfaite dans $\mathcal{M}$. Par *(ii)*, il en résulte que F est satisfaite dans $\mathcal{M}$, et donc, par le théorème de complétude, F est prouvable à partir de T^+. □

Sous les hypothèses précédentes, on déduit en particulier que, si F est une formule de $\mathcal{L}_\Sigma$, alors F est prouvable à partir de T si et seulement si elle est prouvable à partir de T^+ — ce qu'on traduit en disant que T^+ est une extension *conservative* de T.

Le cas des symboles d'opérations est similaire, mais sa formulation requiert un peu plus de soin, car on ne peut pas purement et simplement remplacer le symbole nouveau par sa définition, comme dans le cas des relations.

PROPOSITION 3.5. (extension par définition 2) *Supposons que* T *est une théorie de* $\mathcal{L}_\Sigma$ *prouvant la formule* $\forall \boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k} \exists ! \boldsymbol{y} (\mathsf{D}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}, \boldsymbol{y}))$*. Soit* Σ^+ *la signature*

obtenue en ajoutant à Σ *un nouveau symbole d'opération* k*-aire* $\boldsymbol{s}$*, et* T^+ *la théorie obtenue en ajoutant à* T *la formule* $\mathsf{Intro}_{\boldsymbol{s}}$ *:*

$$\forall \boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}, \boldsymbol{y}(\boldsymbol{y} = \boldsymbol{s}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}) \Leftrightarrow \mathsf{D}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}, \boldsymbol{y})).$$

Pour F *formule de* $\mathcal{L}_{\Sigma^+}$ *contenant au moins une occurrence de* $\boldsymbol{s}$*, on note* $\mathrm{elim}^1_{\boldsymbol{s}}(\mathsf{F})$ *la formule* $\exists \boldsymbol{x}_\mathsf{i}(\mathsf{D}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k}, \boldsymbol{x}_\mathsf{i}) \wedge \mathsf{F}')$ *où* $\boldsymbol{x}_\mathsf{i}$ *est la variable de plus petit indice n'apparaissant pas dans* F*, où* p *est la dernière occurrence de* $\boldsymbol{s}$ *dans* F*, où* $\boldsymbol{s}(\mathsf{t}_1, ..., \mathsf{t}_\mathsf{k})$ *est le sous-terme de* F *commençant à la position* p*, et où* F' *est obtenue en remplaçant dans* F *ledit sous-terme par* $\boldsymbol{x}_\mathsf{i}$ *; enfin, pour* F *contenant* m *fois* $\boldsymbol{s}$*, on note* $\mathrm{elim}_{\boldsymbol{s}}(\mathsf{F})$ *la formule obtenue en appliquant* m *fois l'opération* $\mathrm{elim}^1_{\boldsymbol{s}}$*.*

(*i*) *Tout modèle* $\mathcal{M}$ *de* T *s'enrichit de façon unique en un modèle* $\mathcal{M}^+$ *de* T^+*, et, pour toute formule* F *de* $\mathcal{L}_{\Sigma^+}$*, il y a équivalence entre* $\mathcal{M}^+ \models \mathsf{F}$ *et* $\mathcal{M} \models \mathrm{elim}_{\boldsymbol{s}}(\mathsf{F})$*.*

(*ii*) *Pour* F *formule de* $\mathcal{L}_{\Sigma^+}$*, il y a équivalence entre* $\mathsf{T}^+ \vdash \mathsf{F}$ *et* $\mathsf{T} \vdash \mathrm{elim}_{\boldsymbol{s}}(\mathsf{F})$*.*

Démonstration. On définit la structure $\mathcal{M}^+$ en ajoutant à $\mathcal{M}$ l'interprétation $\boldsymbol{s}^{\mathcal{M}^+}$ définie comme associant à tout k-uplet $\vec{a}$ du domaine de $\mathcal{M}$ l'unique élément b tel que $\mathcal{M}$ satisfasse $\mathsf{D}(\vec{a}, b)$: l'hypothèse que $\mathcal{M}$ est modèle de T garantit l'existence et l'unicité d'un tel élément b. Alors la formule $\mathsf{Intro}_{\boldsymbol{s}}$ est satisfaite dans $\mathcal{M}^+$, qui est donc un modèle de T^+. Inversement, si $\mathcal{M}^+$ est une structure de type Σ^+ enrichissant $\mathcal{M}$ et satisfaisant $\mathsf{Intro}_{\boldsymbol{s}}$, l'interprétation $\boldsymbol{s}^{\mathcal{M}^+}$ de $\boldsymbol{s}$ dans $\mathcal{M}$ ne peut être que celle définie ci-dessus puisque, par hypothèse, $\mathcal{M}$ satisfait $\forall \boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}\, \exists ! \boldsymbol{y}\, (\mathsf{D}(\boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}, \boldsymbol{y}))$. Le reste de la démonstration est exactement semblable à celui de la proposition 3.4. □

▷ *Ainsi se trouve formellement établi le fait intuitivement naturel que l'introduction de symboles aussi nombreux soient-ils ne change rien, ni dans un sens, ni dans l'autre, aux énoncés prouvables dans une théorie — et donc en particulier en théorie des ensembles où cette introduction est spécialement fréquente.* ◁

3.3. Le théorème de compacité.

► Le théorème de compacité relie la satisfaisabilité d'un ensemble de formules à celle de ses sous-ensembles finis ; il entraîne des limitations au pouvoir d'expression des logiques du premier ordre. ◄

▷ *Le théorème de complétude fournit un critère syntaxique caractérisant la satisfaisabilité, à savoir la consistance. Ce faisant, il entraîne que la satisfaisabilité a un caractère finitiste qui a priori n'était pas visible, et qui s'exprime dans le théorème de compacité. On pourra noter que, dans le cas propositionnel, on a établi un théorème de compacité similaire indépendamment du théorème de complétude, par un argument direct. Une démonstration directe existe aussi dans le cas du premier ordre (voir les exercices du chapitre* **??***).* ◁

Proposition 3.6. (théorème de compacité) *Supposons que* Σ *est une signature bien ordonnable et que* T *est une théorie de* $\mathcal{L}_\Sigma$ *dont tout sous-ensemble fini est satisfaisable. Alors* T *est satisfaisable.*

Démonstration. Supposons T non satisfaisable. Par le théorème de complétude, T est non consistante, donc, par l'adaptation à $\mathcal{L}_\Sigma$ du lemme VI.3.12(*iii*), il existe un sous-ensemble fini T_0 de T qui est non consistant (mettre dans T_0 toutes les formules apparaissant dans la preuve d'une contradiction à partir de T). Alors T_0 ne peut être satisfaisable. □

PROPOSITION 3.7. (taille des modèles) *Soit* T *une théorie du premier ordre. Alors ou bien il existe un entier naturel* n *tel que tous les modèles de* T *ont une taille bornée par* n*, ou bien* T *a des modèles infinis.*

DÉMONSTRATION. Supposons que T est un ensemble de formules de $\mathcal{L}_\Sigma$. Le résultat est trivialement vrai si T n'a pas de modèle fini. Supposons donc que T possède des modèles finis de taille arbitrairement grande. Soit Σ' la signature obtenue en ajoutant à Σ une suite $(\boldsymbol{c}_\mathsf{n})_{\mathsf{n}\in\mathbb{N}}$ de symboles de constante, et T' la théorie de $\mathcal{L}_{\Sigma'}$ obtenue en ajoutant à T toutes les formules $\boldsymbol{c}_\mathsf{i} \neq \boldsymbol{c}_\mathsf{j}$ pour $\mathsf{i} < \mathsf{j}$. Soit T_0 une sous-famille finie de T'. Par construction, T_0 consiste en des formules de T, plus un nombre fini de formules du type $\boldsymbol{c}_\mathsf{i} \neq \boldsymbol{c}_\mathsf{j}$. Supposons que n constantes $\boldsymbol{c}_\mathsf{i}$ distinctes apparaissent dans ces formules, et soit $\mathcal{M}$ un modèle de T de taille au moins n. On enrichit $\mathcal{M}$ en une structure $\mathcal{M}'$ de type Σ' en interprétant les constantes $\boldsymbol{c}_\mathsf{i}$ par n éléments du domaine de $\mathcal{M}$ distincts deux à deux. Par construction, $\mathcal{M}'$ est modèle de T_0, et donc T_0 est satisfaisable. Par le théorème de compacité, on déduit que T' est satisfaisable. Or un modèle de T' est un modèle de T, et il est nécessairement infini, puisque les interprétations des symboles $\boldsymbol{c}_\mathsf{i}$ doivent y être deux à deux distinctes. □

COROLLAIRE 3.8. *La finitude ne s'exprime pas au premier ordre : quelle que soit la signature* Σ*, il n'existe pas de théorie de* $\mathcal{L}_\Sigma$ *dont les modèles soient exactement les structures finies de type* Σ*.*

DÉMONSTRATION. Il existe des structures finies de taille arbitrairement grande, mais pas de structure finie infinie. □

▷ *La propriété d'être infini est exprimable au premier ordre, par exemple par la famille infinie des formules* $\exists \boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{n}(\boldsymbol{x}_1 \neq \boldsymbol{x}_2 \wedge ... \wedge \boldsymbol{x}_{\mathsf{n}-1} \neq \boldsymbol{x}_\mathsf{n})$ *(avec* $\binom{\mathsf{n}}{2}$ *inégalités). On déduit du corollaire 3.8 que cette propriété n'est pas finiment exprimable car, si une unique formule* F *exprimait le caractère infini, alors* $\neg\mathsf{F}$ *exprmierait le caractère fini, ce qui ne se peut.*

Il est facile d'adapter l'argument précédent pour obtenir une réponse négative aux questions laissées ouvertes dans la section 1.3 : ni la propriété pour un groupe d'être de torsion, ni celle pour un ordre total d'être un bon ordre, ne sont exprimables au premier ordre ; dans le même ordre d'idée, la propriété pour un corps d'être de caractéristique nulle, qui est exprimable au premier ordre, n'est pas finiment exprimable au premier ordre (cf. exercice 3). ◁

3.4. Le théorème de Lowenheim–Skolem.

► Autre conséquence du théorème de complétude, le théorème de Lowenheim–Skolem fournit des indications sur la taille possible des modèles d'une théorie du premier ordre. On déduit en particulier l'existence, pour toute structure infinie même non dénombrable, d'une structure dénombrable qui en est indiscernable du point de vue des formules du premier ordre. ◄

On appelle cardinal d'une structure le cardinal de son domaine.

PROPOSITION 3.9. (théorème de Lowenheim-Skolem) *Soit* Σ *une signature bien ordonnable, et soit* $\kappa := \max(\aleph_0, \mathrm{card}(\Sigma))$*. Alors, pour tout cardinal* $\lambda \geqslant \kappa$*, il y a équivalence entre*

(i) T *possède un modèle de cardinal* κ *;*

(ii) T *possède un modèle de cardinal* λ*;*

En particulier, pour Σ *finie ou dénombrable, toute théorie de* $\mathcal{L}_\Sigma$ *possédant un modèle infini possède un modèle de n'importe quelle cardinalité infinie.*

DÉMONSTRATION. Supposons (i), et soit $\lambda \geqslant \kappa$ quelconque. Alors T, possédant un modèle, est consistante. Soit Σ' la signature bien ordonnable obtenue en ajoutant à Σ une suite $(\boldsymbol{c}_\alpha)_{\alpha<\lambda}$ de symboles de constantes, et T' comme la théorie de $\mathcal{L}_{\Sigma'}$ obtenue en ajoutant à T la suite des formules $\boldsymbol{c}_\alpha \neq \boldsymbol{c}_\beta$ pour $\alpha < \beta < \lambda$. Alors T' est consistante, car une sous-famille finie T_0 de T' est composée d'une sous-famille de T et d'un nombre fini de formules $\boldsymbol{c}_\alpha \neq \boldsymbol{c}_\beta$. Par hypothèse, T possède un modèle de cardinal κ, qu'on peut enrichir en un modèle de T_0 en interprétant les constantes $\boldsymbol{c}_\alpha$ intervenant dans T_0 par des éléments du domaine deux à deux distincts. Par le théorème de complétude, T' possède un modèle dont le cardinal est $\max(\aleph_0, \mathrm{card}(\Sigma'))$, soit λ. Lorsqu'on oublie les interprétations des constantes $\boldsymbol{c}_\alpha$, il reste un modèle de T de cardinal λ.

Supposons maintenant (ii). A nouveau, T est consistante puisque possédant un modèle. Par le théorème de complétude, T possède un modèle de cardinal κ. □

On en déduit de nouveaux résultats de non-exprimabilité au premier ordre.

COROLLAIRE 3.10. (AC) *Soit κ un cardinal infini. Le fait d'avoir un cardinal au plus égal à κ ne s'exprime pas au premier ordre : quelle que soit la signature Σ, il n'existe pas de théorie de $\mathcal{L}_\Sigma$ dont les modèles soient exactement les structures de type Σ de cardinalité au plus κ.*

DÉMONSTRATION. Soit T une théorie de $\mathcal{L}_\Sigma$, et soit $\mu := \max(\aleph_0, \mathrm{card}(\Sigma))$. Si T admet pour modèle les structures de cardinal au plus κ, elle est consistante, et donc admet des modèles de cardinal λ pour tout $\lambda \geqslant \mu$, donc en particulier des modèles de cardinal plus grand que κ. □

▷ *Par contraste, on notera qu'il existe une théorie dont les modèles sont les structures de cardinal au moins κ : il suffit de choisir la signature contenant κ symboles de constante $\boldsymbol{c}_\alpha$ distincts, et de considérer la théorie formée par les formules $\boldsymbol{c}_\alpha \neq \boldsymbol{c}_\beta$ pour $\alpha < \beta < \kappa$.*

Une autre application du théorème de Lowenheim–Skolem est l'existence, pour toute structure même non dénombrable, d'une structure dénombrable qui en est indiscernable du point de vue des formules du premier ordre, pour autant que la signature soit elle-même finie ou dénombrable. ◁

COROLLAIRE 3.11. *Soit Σ une signature finie ou dénombrable. Alors, pour toute réalisation infinie $\mathcal{R}$ de $\mathcal{L}_\Sigma$, il existe une réalisation dénombrable satisfaisant les mêmes formules*[16] *que $\mathcal{R}$.*

DÉMONSTRATION. Soit T l'ensemble des formules closes satisfaites dans $\mathcal{R}$. Alors T est consistant, puisqu'il a au moins un modèle, à savoir $\mathcal{R}$. Par le théorème de Lowenheim-Skolem, T possède un modèle $\mathcal{R}'$ dont le domaine est fini ou dénombrable. Alors $\mathcal{R}$ et $\mathcal{R}'$ satisfont les mêmes formules closes, car $\mathcal{R} \models \mathsf{F}$ entraîne $\mathcal{R}' \models \mathsf{F}$ par construction, et, inversement, $\mathcal{R} \not\models \mathsf{F}$ entraîne $\mathcal{R} \models \neg\mathsf{F}$, donc $\mathcal{R}' \models \neg\mathsf{F}$, puis $\mathcal{R}' \not\models \mathsf{F}$.

Par ailleurs, une structure satisfaisant les mêmes formules closes qu'une structure infinie est nécessairement infinie, puisque la propriété d'être infinie est exprimable au premier ordre par la famille des formules (en la signature vide) $\exists \boldsymbol{x}_1 \ldots \exists \boldsymbol{x}_\mathsf{n}\ (\bigwedge_{\mathsf{i}<\mathsf{j}\leqslant\mathsf{n}} \boldsymbol{x}_\mathsf{i} \neq \boldsymbol{x}_\mathsf{j})$ pour $\mathsf{n} \geqslant 1$. Donc l'hypothèse que $\mathcal{R}$ et $\mathcal{R}'$ satisfont les mêmes formules implique que le domaine de $\mathcal{R}'$ est infini, puisque c'est le cas de celui de $\mathcal{R}$. □

▷ *Le résultat précédent montre par exemple qu'il existe un corps dénombrable satisfaisant les mêmes formules que le corps $(\mathbb{R}, +, \cdot)$, donc indiscernable de celui-ci par rapport à toutes les propriétés exprimables par des formules du premier ordre. Le résultat peut paraître paradoxal, mais, en fait, il reflète surtout les limitations du pouvoir d'expression au premier ordre : il y*

[16] ce qu'on exprime aussi en déclarant $\mathcal{R}'$ *élémentairement équivalente* à $\mathcal{R}$

a un grand écart entre le fait de satisfaire les mêmes formules du premier ordre et celui d'être isomorphes : deux structures isomorphes satisfont toujours les mêmes formules (closes), mais la réciproque est en général fausse. ◁

3.5. Modèles de l'arithmétique.

► Comme illustration de ce qui précède, on considère ici les structures satisfaisant les mêmes formules que la structure $(\mathbb{N}, 0, S, +, \cdot)$, appelées modèles de l'arithmétique. On établit l'existence d'une famille non dénombrable de tels modèles dénombrables deux à deux non isomorphes. ◄

▷ *Lorsqu'on part d'une théorie* T *dans* $\mathcal{L}_\Sigma$*, on a la notion naturelle de modèle pour* T*, c'est-à-dire de réalisation de* $\mathcal{L}_\Sigma$ *satisfaisant toutes les formules de* T*. En sens inverse, partant d'une structure* $\mathcal{R}$ *de type* Σ*, on peut considérer l'ensemble des formules closes satisfaites dans cette structure particulière.* ◁

Définition 3.12. (théorie) Si $\mathcal{R}$ est une structure de type Σ, on définit la *théorie du premier ordre* de $\mathcal{R}$ comme l'ensemble $\mathrm{Th}_1(\mathcal{R})$ de toutes les formules closes de $\mathcal{L}_\Sigma$ satisfaites dans $\mathcal{R}$.

▷ *Etant donné que, par définition, une formule* $\mathsf{F}(\vec{\boldsymbol{x}})$ *ayant des variables libres est dite satisfaite dans une réalisation* $\mathcal{R}$ *si et seulement si la formule close* $\forall\vec{\boldsymbol{x}}(\mathsf{F}(\vec{\boldsymbol{x}}))$ *l'est, dire que deux structures* $\mathcal{R}, \mathcal{R}'$ *satisfont les mêmes formules équivaut à dire qu'elles satisfont les mêmes formules closes, et donc à dire que* $\mathcal{R}'$ *est modèle de* $\mathrm{Th}_1(\mathcal{R})$*. Dans la suite, on s'intéresse au cas particulier de la structure* $(\mathbb{N}, 0, S, +, \cdot)$*, qui jouera un rôle fondamental au chapitre VIII. On appelle usuellement arithmétique du premier ordre l'ensemble* $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$*. Il est donc cohérent de poser'arithm la définition suivante :* ◁

Définition 3.13. (modèle de l'arithmétique, standard) On appelle *modèle de l'arithmétique* tout modèle de $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$, c'est-à-dire toute structure de type Σ_{arith} satisfaisant les mêmes formules closes que $(\mathbb{N}, 0, S, +, \cdot)$; un modèle est dit *standard* s'il est isomorphe à $(\mathbb{N}, 0, S, +, \cdot)$.

Le théorème de Lowenheim–Skolem entraîne qu'il existe des modèles non-standards de l'arithmétique de toute cardinalité infinie, mais ne dit *a priori* rien sur d'éventuels modèles non-standards dénombrables.

Proposition 3.14. (modèles non-standards) *Il existe* $2^{\aleph_0}$ *modèles non-standards dénombrables de l'arithmétique deux à deux non isomorphes.*

Démonstration. Soit κ le nombre de classes d'isomorphisme de modèles dénombrables de l'arithmétique. Comme tout modèle dénombrable est isomorphe à un modèle de domaine $\mathbb{N}$, et que spécifier une structure de type Σ_{arith} de domaine $\mathbb{N}$ consiste à choisir un élément de $\mathbb{N}$, une fonction de $\mathbb{N}$ dans $\mathbb{N}$, et deux fonctions de $\mathbb{N}^2$ dans $\mathbb{N}$, on a $\kappa \leqslant 2^{\aleph_0}$.

Soit $\mathbb{P}$ l'ensemble des nombres premiers. Pour chaque modèle (dénombrable) de l'arithmétique $\mathcal{M}$ et chaque a dans $\mathrm{Dom}(\mathcal{M})$, on note $\mathrm{Div}_{\mathcal{M}}(a)$ l'ensemble des nombres premiers p divisant a dans M, c'est-à-dire $\{\mathsf{p} \in \mathbb{P}\,;\, \mathcal{M} \models \mathsf{F}_{\mathsf{p}}(a)\}$, où $\mathsf{F}_{\mathsf{p}}(\boldsymbol{x})$ est la formule $\exists\boldsymbol{y}(\boldsymbol{x} = \boldsymbol{S}^{\mathsf{p}}\boldsymbol{0} \cdot \boldsymbol{y})$. On note D l'ensemble de toutes les parties de $\mathbb{P}$ qui sont de la forme $\mathrm{Div}_{\mathcal{M}}(a)$ pour au moins un modèle dénombrable $\mathcal{M}$ et un a.

Supposons que $\mathcal{M}, \mathcal{M}'$ sont des modèles de l'arithmétique et que f est un isomorphisme de $\mathcal{M}$ sur $\mathcal{M}'$. L'entier 0 est l'unique élément de $\mathbb{N}$ n'appartenant pas à l'image de S, donc $(\mathbb{N}, 0, S, +, \cdot)$

satisfait $\exists!\boldsymbol{x}\,\forall\boldsymbol{y}\,(\boldsymbol{S}(\boldsymbol{y}) \neq \boldsymbol{x})$ et $\forall\boldsymbol{y}(\boldsymbol{S}(\boldsymbol{y}) \neq \mathbf{0})$. Ces formules sont donc dans $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$, et par conséquent elles sont satisfaites dans $\mathcal{M}$ et dans $\mathcal{M}'$. L'interprétation $\mathbf{0}^{\mathcal{M}}$ de $\mathbf{0}$ dans $\mathcal{M}$ est donc le seul élément du domaine de $\mathcal{M}$ qui n'est pas dans l'image de $\boldsymbol{S}^{\mathcal{M}}$, et de même pour $\mathcal{M}'$. Puisque f est un isomorphisme, il envoie les éléments de l'image de $\boldsymbol{S}^{\mathcal{M}}$ sur les éléments de l'image de $\boldsymbol{S}^{\mathcal{M}'}$ et, par conséquent, il envoie nécessairement $\mathbf{0}^{\mathcal{M}}$ sur $\mathbf{0}^{\mathcal{M}'}$. De là, par récurrence, f, étant un homomorphisme vis-à-vis de $\boldsymbol{S}$, envoie $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$ sur $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}'}$ pour chaque entier naturel p. Enfin, f est un homomorphisme vis-à-vis de la multiplication, donc, pour tout a dans $\mathrm{Dom}(\mathcal{M})$, les entiers p tels que $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$ divise a dans $\mathcal{M}$ sont les mêmes que ceux qui sont tels que $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}'}$ divise $f(a)$ dans $\mathcal{M}'$. On a donc $\mathrm{Div}_{\mathcal{M}}(a) = \mathrm{Div}_{\mathcal{M}'}(f(a))$ pour tout a dans $\mathrm{Dom}(\mathcal{M})$, et, par conséquent les contributions des modèles $\mathcal{M}$ et $\mathcal{M}'$ à D sont les mêmes. Il en résulte qu'on a $\mathrm{card}(D) \leqslant \kappa \cdot \aleph_0$, puisqu'un modèle dénombrable ne peut contribuer que pour (au plus) $\aleph_0$ éléments à D.

Or D est $\mathfrak{P}(\mathbb{P})$ tout entier. En effet, soit Σ la signature obtenue en ajoutant à Σ_{arith} un nouveau symbole de constante $\boldsymbol{c}$. Soit X une partie quelconque (finie ou infinie) de $\mathbb{P}$. On définit T_X comme la théorie de $\mathcal{L}_\Sigma$ obtenue en ajoutant à $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$ les formules $\mathsf{F}_{\mathsf{p}}(\boldsymbol{c})$ pour p dans X et $\neg\mathsf{F}_{\mathsf{p}}(\boldsymbol{c})$ pour p dans le complémentaire de X. Un sous-ensemble fini de T_X consiste en un sous-ensemble fini de $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$ plus un nombre fini de formules $\mathsf{F}_{\mathsf{p}}(\boldsymbol{c})$ et $\neg\mathsf{F}_{\mathsf{q}}(\boldsymbol{c})$: un tel ensemble de formules est satisfaisable dans $(\mathbb{N}, 0, S, +, \cdot)$, car il existe toujours un entier naturel satisfaisant un nombre fini de contraintes de divisibilité et de non-divisibilité par des nombres premiers. Donc T_X a au moins un modèle dénombrable. Or dire que $\mathcal{M}$ est modèle de T_X signifie qu'il existe a dans $\mathrm{Dom}(\mathcal{M})$ vérifiant $\mathrm{Div}_{\mathcal{M}}(a) = X$. Par conséquent, on a $D = \mathfrak{P}(\mathbb{P})$, d'où $2^{\aleph_0} \leqslant \kappa \cdot \aleph_0$, qui entraîne $\kappa = 2^{\aleph_0}$ en présence de $\kappa \leqslant 2^{\aleph_0}$. □

▷ *On notera l'importance du théorème de compacité dans la démonstration précédente. Le résultat lui-même n'a rien de surprenant : il montre simplement que la théorie du premier ordre d'une structure ne capture qu'une partie des propriétés de celle-ci. Noter que, par hypothèse, la structure* $(\mathbb{N}, 0, S, +, \cdot)$ *est un modèle de la théorie de Peano du premier ordre* PA_1*, et on a donc* $\mathsf{PA}_1 \subseteq \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$*. Par conséquent, tout modèle non-standard de l'arithmétique est en particulier un modèle de la théorie* PA_1*, et donc il satisfait toutes les formules closes prouvables à partir de* PA_1*.*

Toute une étude des modèles non-standards de l'arithmétique a été développée. On se bornera ici au fait que tout modèle non-standard prolonge en un certain sens les entiers naturels. Jusqu'à présent, on n'a pas pris en compte l'ordre des entiers dans la description de l'arithmétique. Il est loisible de le rajouter, car il est définissable à partir de l'addition. De là, on déduit l'existence d'un ordre semblable sur tout modèle de l'arithmétique. On rappelle que $\Sigma_{\mathrm{arith}^+}$ *désigne la signature obtenue en ajoutant à* Σ_{arith} *un symbole de relation binaire* $\leqslant$*.* ◁

LEMME 3.15. *Soit* $\mathsf{Intro}_{\leqslant}$ *la formule*

$$\forall\boldsymbol{x}, \boldsymbol{y}(\boldsymbol{x} \leqslant \boldsymbol{y} \Leftrightarrow \exists\boldsymbol{z}(\boldsymbol{y} = \boldsymbol{z} + \boldsymbol{x})).$$

Alors tout modèle de l'arithmétique $\mathcal{M}$ *s'enrichit de façon unique en une structure* $\mathcal{M}^+$ *de type* $\Sigma_{\mathrm{arith}^+}$ *satisfaisant* $\mathsf{Intro}_{\leqslant}$*, et, alors, les structures* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *et* $\mathcal{M}^+$ *satisfont les mêmes formules de* $\mathcal{L}_{\mathrm{arith}^+}$ *; en particulier,* $\leqslant^{\mathcal{M}^+}$ *est un ordre total sur le domaine de* $\mathcal{M}$*.*

DÉMONSTRATION. Le résultat découle immédiatement de la proposition 3.4. On remarque que $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ est la structure $(\mathbb{N}, 0, S, +, \cdot)^+$. Soit F une formule quelconque de $\mathcal{L}_{\mathrm{arith}^+}$. Alors, avec les notations de la section 3.2, la formule F est satisfaite dans le modèle $\mathcal{M}^+$ si et seulement si la formule $\mathrm{elim}_{\leqslant}(\mathsf{F})$ est satisfaite dans $\mathcal{M}$, donc si et seulement si elle est satisfaite dans $(\mathbb{N}, 0, S, +, \cdot)$, donc si et seulement si F est satisfaite dans $(\mathbb{N}, 0, S, +, \cdot)^+$, c'est-à-dire dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$. Le fait que $\leqslant^{\mathcal{M}^+}$ soit un ordre total résulte du fait qu'être un ordre

total est exprimable au premier ordre, ainsi qu'on l'a vu dans l'exemple 1.22. Par contre, rien ne garantit *a priori* que $\leqslant^{\mathcal{M}^+}$ soit un bon ordre. □

Ainsi, lorsqu'on parle de modèles de l'arithmétique, on peut toujours supposer que l'ordre fait partie de la structure. Si $\mathcal{M}$ est un modèle de l'arithmétique, l'ordre $\leqslant^{\mathcal{M}^+}$ défini comme ci-dessus sera appelé *canonique*.

PROPOSITION 3.16. (segment initial) *Soit $\mathcal{M}$ un modèle de l'arithmétique. Soit $\mathbb{N}_\bullet$ le sous-ensemble du domaine de $\mathcal{M}$ formé par les éléments $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$ avec p entier naturel. Alors $\mathbb{N}_\bullet$ est un segment initial de* $\mathrm{Dom}(\mathcal{M})$ *pour l'ordre canonique, il est stable pour les opérations de $\mathcal{M}$, et la sous-structure $\mathcal{M}_\bullet$ de $\mathcal{M}$ induite sur $\mathbb{N}_\bullet$ est isomorphe à $(\mathbb{N}, 0, S, +, \cdot)$ (cf. figure 2).*

DÉMONSTRATION. On note $\preccurlyeq$ l'ordre canonique de $\mathcal{M}$. La formule close $\forall \boldsymbol{x}(\mathbf{0} \leqslant \boldsymbol{x})$ est satisfaite dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, donc dans $(\mathcal{M}, \preccurlyeq)$, et donc $\mathbf{0}^{\mathcal{M}}$ est élément minimum de $(\mathcal{M}, \preccurlyeq)$. De même, pour chaque entier naturel p, il existe une formule close exprimant que $\boldsymbol{S}^{\mathsf{p}+1}\mathbf{0}$ est le successeur immédiat de $\boldsymbol{S}^{\mathsf{p}}\mathbf{0}$, et cette formule, vraie dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, l'est aussi dans $(\mathcal{M}, \preccurlyeq)$. Par conséquent, $\mathbb{N}_\bullet$ est un segment initial de $(\mathrm{Dom}(\mathcal{M}), \preccurlyeq)$.

Par construction, $\mathbf{0}^{\mathcal{M}}$ est dans $\mathbb{N}_\bullet$, et $\mathbb{N}_\bullet$ est stable par $\boldsymbol{S}^{\mathcal{M}}$. Ensuite, chacune des formules $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}+\mathsf{q}}\mathbf{0}$ et $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} \cdot \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}\mathsf{q}}\mathbf{0}$ est satisfaite dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, donc dans $\mathcal{M}$, ce qui montre que $\mathbb{N}_\bullet$ est stable par $+^{\mathcal{M}}$ et $\cdot^{\mathcal{M}}$. Donc on obtient une structure $\mathcal{M}_\bullet$ bien définie en munissant $\mathbb{N}_\bullet$ des opérations induites par celles de $\mathcal{M}$. Enfin, par construction, l'application $\mathsf{p} \mapsto \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ est un isomorphisme de $(\mathbb{N}, 0, S, +, \cdot)$ sur $\mathcal{M}_\bullet$. □

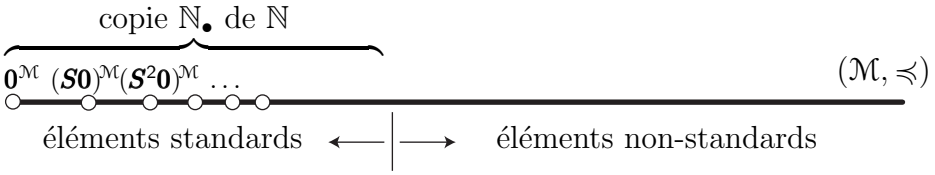

FIGURE 2. Tout modèle de l'arithmétique est un ensemble totalement ordonné commençant par une copie des entiers, suivie d'éventuels éléments dits non-standards.

COROLLAIRE 3.17. *Le modèle standard de l'arithmétique est le seul dont l'ordre canonique soit un bon ordre.*

DÉMONSTRATION. Soit $\mathcal{M}$ un modèle de l'arithmétique quelconque. Si tout élément du domaine de $\mathcal{M}$ est de la forme $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$ avec p dans $\mathbb{N}$, alors $\mathcal{M}$ est isomorphe à $(\mathbb{N}, 0, S, +, \cdot)$, donc standard par définition. Sinon, il existe un élément a_0 du domaine de $\mathcal{M}$ qui n'est pas de la forme $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$. On a alors $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} \prec a_0$ pour tout entier naturel p. Puisque a_0 n'est pas $\mathbf{0}^{\mathcal{M}}$, il existe a_1 vérifiant $a_0 = \boldsymbol{S}^{\mathcal{M}}(a_1)$, donc $a_1 \prec a_0$. A son tour, a_1 n'est pas de la forme $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$, sans quoi a_0 le serait. De proche en proche, on obtient une suite infinie décroissante dans $(\mathcal{M}, \preccurlyeq)$. □

▷ *L'argument montre qu'en tant qu'ensemble ordonné, un modèle non-standard de l'arithmétique commence par une copie de $\mathbb{N}$, puis est composé de copies de $\mathbb{Z}$ puisque chaque élément a un successeur et un précédesseur immédiats ; on peut vérifier que les copies de $\mathbb{Z}$ forment un ordre dense sans point extrémal, donc isomorphe à $\mathbb{Q}$ dans le cas dénombrable.*

Par définition, tout modèle de l'arithmétique est un modèle de la théorie de Peano PA_1. *Par contre, il n'est pas clair que tout modèle de* PA_1 *soit un modèle de l'arithmétique, et ceci mène aux questions suivantes.* ◁

QUESTION 3.18. *Toute formule du premier ordre satisfaite dans* $(\mathbb{N}, 0, S, +, \cdot)$ *est-elle prouvable à partir du système de Peano* PA_1 *?*

On rappelle (définition 2.9) qu'une théorie T de $\mathcal{L}_\Sigma$ est dite *complète* si, pour chaque formule close F de $\mathcal{L}_\Sigma$, on a $\mathsf{T} \vdash \mathsf{F}$ ou $\mathsf{T} \vdash \neg\mathsf{F}$, autrement dit si T est assez forte pour prouver ou réfuter toute propriété.

QUESTION 3.19. *Le système* PA_1 *est-il complet ?*

▷ *Moyennant l'hypothèse que la structure* $(\mathbb{N}, 0, S, +, \cdot)$ *existe et est un modèle de* PA_1*, les deux questions 3.18 et 3.19 sont équivalentes, puisqu'on sait que la théorie d'une structure est toujours un ensemble complet.*

Une réponse positive à la question 3.18 entraînerait que tout modèle de PA_1 *satisfait toutes les formules de* $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$*, donc satisfait les mêmes formules que* $(\mathbb{N}, 0, S, +, \cdot)$*. Inversement, une réponse négative entraînerait qu'il existe au moins une formule* F *satisfaite dans* $(\mathbb{N}, 0, S, +, \cdot)$ *et non prouvable à partir de* PA_1*, donc telle que* $\mathsf{PA}_1 \cup \{\neg\mathsf{F}\}$ *soit consistant. Il résulterait alors du théorème de complétude que* $\mathsf{PA}_1 \cup \{\neg\mathsf{F}\}$ *aurait un modèle dénombrable, lequel serait un modèle de* PA_1 *ne satisfaisant pas les mêmes formules que* $(\mathbb{N}, 0, S, +, \cdot)$*. Ce sera un des objets du chapitre VIII que d'apporter une réponse — négative — aux questions 3.18 et 3.19.* ◁

4. La logique du premier ordre comme modèle

► On discute brièvement l'adoption de la logique du premier ordre comme formalisation du raisonnement mathématique. ◄

▷ *Suivant le schéma général esquissé dans la section VI.1, adopter une logique consiste à la fois à fixer une famille de formules et adopter une notion de preuve adaptée. Dans le cas de la logique du premier ordre, les choix ont été faits pour calquer au mieux l'usage mathématique, et il n'est donc pas surprenant que la logique obtenue apparaisse comme la meilleure approximation formelle possible du discours mathématique. Néanmoins, comme pour toute modélisation, il est au moins naturel d'examiner l'adéquation du modèle à la réalité (?) qu'il copie et les bénéfices qu'on peut attendre de la modélisation.* ◁

4.1. Propriétés et formules.

► Le pouvoir d'expression des logiques du premier ordre est grand mais néanmoins limité, sauf dans le contexte de la théorie des ensembles. ◄

▷ *La sémantique des logiques du premier ordre a été définie de façon à calquer directement l'usage mathématique*[17]*. L'équivalence suivante n'est alors que la définition 1.21 de la notion d'exprimabilité :* ◁

LEMME 4.1. *Si une propriété* $\mathcal{P}$ *est exprimable par une formule du premier ordre* F *de* $\mathcal{L}_\Sigma$*, alors, pour tout objet* a*, il y a équivalence entre*

(*i*) *l'objet* a *a la propriété* $\mathcal{P}$ *;*

(*ii*) *la formule* $\mathsf{F}(a)$ *est satisfaite.*

[17] On a déjà noté certains aspects suspectement circulaires de la définition ; on y reviendra ci-dessous dans la section 4.5

▷ *Les exemples de la section 1.3 ont montré que de nombreuses propriétés élémentaires de structures mathématiques usuelles pouvaient étaient exprimées par des formules d'une logique du premier ordre convenable. En même temps, une des limitations les plus évidentes des logiques du premier ordre est l'interdiction de référer simultanément dans une même formule à plusieurs types d'objets distincts, et on a vu que ceci induit une forte limitation du pouvoir d'expression, puisque des notions aussi simples que la finitude du domaine considéré sont inexprimables, ou encore puisque, dans le cas de l'arithmétique, il semble impossible d'exprimer le schéma d'induction dans sa forme la plus générale. Il serait donc difficile de prétendre que, pour chaque type d'objet considéré séparément, typiquement les nombres entiers et l'arithmétique, les formules du premier ordre autorisent une formalisation de toutes les propriétés qu'on peut souhaiter étudier.*

On reviendra plus loin sur le moyen — ou l'absence de moyen — d'échapper aux limitations précédentes. Pour le moment, il est important de noter qu'il existe un cas où les limitations de la logique du premier ordre s'estompent, à savoir celui des théories des ensembles. Dans le contexte des ensembles, et plus précisément en présence des axiomes de Zermelo qui garantissent la possibilité de représenter chaque objet mathématique a par un ensemble pur $\underline{a}$, presque toute propriété $\mathcal{P}$ de l'objet a peuvent être exprimées comme la satisfaction par l'ensemble $\underline{a}$ d'une certaine formule ensembliste $\mathsf{F}(\boldsymbol{x})$ qui mime $\mathcal{P}$. On verra une exception au chapitre IX avec l'axiome dit de modèle standard, mais ces exceptions sont suffisamment mineures pour pouvoir être négligées en pratique, ce qui revient à considérer comme pratiquement illimité le pouvoir d'expression de la logique du premier ordre $\mathcal{L}_{\rm ens}$. Moyennant le lemme 4.1, on peut résumer la situation sous la forme : ◁

« PROPOSITION » 4.2. (exprimabilité) *Pour chaque propriété $\mathcal{P}$, il existe une formule ensembliste du premier ordre F telle que, pour tout objet a, il y ait équivalence entre*

(i) l'objet a a la propriété $\mathcal{P}$;

(ii) la formule ensembliste $\mathsf{F}(\underline{a})$ est satisfaite.

4.2. Démonstrations et preuves.

► L'intérêt majeur de la logique du premier ordre tient à l'existence d'une bonne notion de prouvabilité. ◄

▷ *On peut facilement imaginer des logiques dont le pouvoir d'expression soit plus grand que celui des logiques du premier ordre, par exemple les logiques du second ordre brièvement décrites dans l'appendice, ou des logiques mettant en jeu des conjonctions et des disjonctions infinies, ou encore des logiques mettant en jeu des quantifications plus générales que $\exists$ et $\forall$. Ce qui limite drastiquement l'intérêt et, de là l'usage, de telles logiques est l'absence d'une bonne notion de prouvabilité.*

La logique du premier ordre est munie d'une notion de prouvabilité possédant deux qualités essentielles : d'abord et avant tout, son adéquation avec la logique du bon sens, et, d'autre part, l'existence d'un théorème de complétude par rapport à la sémantique naturelle. Aucune autre logique développée à ce jour ne possède ces qualités : par exemple on montrera au chapitre VIII que les logiques du second ordre ne peuvent satisfaire aucun théorème de complétude. D'une façon générale, G. Lindstrom a démontré qu'en un sens précis les logiques du premier ordre sont les seules qui puissent à la fois vérifier un théorème de compacité et *un théorème de complétude* [**4**].

Du point de vue de la modélisation du raisonnement, on peut justifier comme suit le principe d'adopter les preuves de la logique du premier ordre comme modèle de référence. Supposons que $\mathcal{H}$ est une famille d'hypothèses s'exprimant par des formules du premier ordre T, et que $\mathcal{P}$ est une propriété s'exprimant par une formule du premier ordre F. Dans une direction, on peut argumenter que les régles de déduction et de généralisation, ainsi que les schémas correspondant aux axiomes propositionnels, correspondent à des raisonnements que le bon sens approuve[18]*. Il*

[18] néanmoins au moins un point peut être discuté et ne recueille pas un assentiment totalement unanime, à savoir le principe du tiers exclu exprimé dans l'axiome $\neg\neg\boldsymbol{X}\Rightarrow\boldsymbol{X}$

en résulte que toute preuve $\mathsf{T} \vdash \mathsf{F}$ *fournit une démonstration de* $\mathcal{P}$ *à partir de* $\mathcal{H}$*. Inversement, la question est de savoir si n'importe quelle démonstration mathématique de* $\mathcal{P}$ *à partir de* $\mathcal{H}$ *peut se formaliser en une preuve, autrement dit si tout argument de démonstration peut se réduire à une utilisation des règles de coupure et de généralisation et des instances des axiomes propositionnels. Il est a priori difficile de répondre à cette question, qui est vague. Mais le théorème de complétude apporte un argument décisif. Il semble naturel que, s'il existe une démonstration de* $\mathcal{P}$ *à partir de* $\mathcal{H}$*, quelle qu'elle soit, alors toute structure vérifiant* $\mathcal{H}$ *doive aussi vérifier* $\mathcal{P}$*, donc, moyennant la proposition 4.2, si tout modèle de* T *satisfait* F*. En vertu du théorème de complétude, ceci est précisément le cas si (et seulement si) on a* $\mathsf{T} \vdash \mathsf{F}$*. Ce type d'argument devrait rendre consensuel l'énoncé suivant :* ◁

« Proposition » 4.3. *Supposons que* $\mathcal{H}$ *est une famille d'hypothèses s'exprimant par des formules du premier ordre* T*, et que* $\mathcal{P}$ *est une propriété s'exprimant par une formule du premier ordre* F*. Alors il y a équivalence entre*

(*i*) *la propriété* $\mathcal{P}$ *est démontrable à partir de* $\mathcal{H}$ *;*

(*ii*) *la relation* $\mathsf{T} \vdash \mathsf{F}$ *est vérifiée.*

▷ *Adopter la logique du premier ordre comme modèle du raisonnement mathématique signifie accepter l'équivalence de la proposition 4.3, et, donc, fixer comme but aux mathématiques d'établir des relations du type* $\mathsf{T} \vdash \mathsf{F}$*.* ◁

4.3. Le cadre « théorie des ensembles + logique du premier ordre ».

► On parvient à ce qui sera le cadre formel pour toute la suite, à savoir la prouvabilité en logique du premier ordre à partir des axiomes d'une théorie des ensembles. ◄

▷ *Au chapitre III, on a vu que toute théorie des ensembles incluant la théorie de Zermelo offre un cadre universel permettant d'englober la quasi-intégralité du monde mathématique. Dès lors, un cas particulier important de la proposition 4.3 prend la forme suivante :* ◁

Corollaire 4.4. *Supposons que* T *est un système axiomatique incluant* Z *et adopté comme base axiomatique de la théorie des ensembles. Alors, pour toute propriété* $\mathcal{P}$ *mettant en jeu des objets* a*,* b*, ..., il y a équivalence entre:*

(*i*) *La propriété* $\mathcal{P}(a, b, ...)$ *est démontrable;*

(*ii*) *La relation* $\mathsf{T} \vdash \mathsf{F}(\underline{a}, \underline{b}, ...)$ *est satisfaite, où* F *est la traduction de* $\mathcal{P}$ *en une formule ensembliste, et où* $\underline{a}, \underline{b}, ...$ *sont les contreparties ensemblistes de* $a, b, ...$

▷ *Typiquement, le système* T *proposé peut être le système* ZFC *de Zermelo–Fraenkel, voire une extension de celui-ci. Il existe à ce jour un large consensus pour accepter ce cadre formel, qu'on peut résumer en « théorie des ensembles + logique du premier ordre ». En tout cas, c'est le cadre qui est adopté dans la suite de ce texte.*

A ce point, le lecteur devrait être d'accord pour reconnaître qu'un cadre formel complet est à notre disposition, et, par exemple, ce que pourrait être une réponse aux questions du chapitre I devrait être désormais clair : démontrer l'hypothèse du continu signifie établir la relation $\mathsf{ZFC} \vdash \mathrm{card}(\underline{\mathbb{R}}) = \aleph_1$*, voire* $\mathsf{T} \vdash \mathrm{card}(\underline{\mathbb{R}}) = \aleph_1$ *où* T *est une extension de* ZFC *en faveur de laquelle un consensus suffisant existe. D'une façon générale, ce qu'on cherchera à établir ou réfuter dans la suite sont des énoncés tels que* $\mathsf{ZFC} \vdash \mathrm{card}(\underline{\mathbb{R}}) = \aleph_4$ *ou* $\mathsf{ZF} \vdash \mathsf{AC}$*, ou encore* $\mathsf{ZFC} \vdash$ *« tout ensemble de réels est Lebesgue mesurable », où* $\vdash$ *fait référence à la prouvabilité en logique du premier ordre, et où des objets comme les réels interviennent par le biais des ensembles purs qui les représentent.*

Clairement, l'adoption du cadre « théorie des ensembles + logique du premier ordre » donne une place fondamentale aux deux questions suivantes : ◁

QUESTION 4.5. *Le système* ZFC *est-il consistant, c'est-à-dire est-il impossible d'avoir à la fois* $\mathsf{ZFC} \vdash \mathsf{F}$ *et* $\mathsf{ZFC} \vdash \neg\mathsf{F}$ *?*

QUESTION 4.6. *Le système* ZFC *est-il complet vis-à-vis de la relation de prouvabilité du premier ordre, c'est-à-dire, pour chaque formule ensembliste* F*, a-t-on nécessairement* $\mathsf{ZFC} \vdash \mathsf{F}$ *ou* $\mathsf{ZFC} \vdash \neg\mathsf{F}$ *? Une extension de ce système l'est-elle?*

▷ *Tout comme dans le cas de la question 3.18 concernant l'arithmétique de Peano, on verra au chapitre VIII que les réponses à ces questions sont plutôt décevantes — mais, au moins faute d'alternative, pas au point de remettre en cause le choix du cadre formel décrit ici.* ◁

4.4. Bénéfice de la formalisation en logique du premier ordre.

► Quel est l'intérêt de la proposition 4.3 et, d'une façon générale, quel bénéfice attendre de l'introduction d'une logique formelle ? ◄

▷ *En théorie, seule une formalisation complète semble de nature à garantir la rigueur d'une démonstration. En pratique, que ce soit le cas n'est rien moins que certain, tout au moins tant qu'il s'agit d'interlocuteurs humains, car il est bien clair qu'on ne descend jamais jusqu'au niveau de preuves syntaxiques du genre de celle du lemme 3.3. Quant à l'espoir que le recours à des systèmes automatisés aide à démontrer d'authentiques nouveaux théorèmes ou même à certifier des démonstrations existantes, il apparaît encore lointain — malgré des progrès récents comme la vérification par l'assistant de preuve* Coq *du théorème des quatre couleurs. Par contre, il est exact que la formalisation peut aider à expliciter des hypothèses qui risqueraient de rester implicites, par exemple des usages de l'axiome de choix.*

Il existe trois modes par lesquels l'utilisation d'une logique formelle, et en l'occurrence de la logique du premier ordre, apporte une contribution décisive, correspondant précisément à trois directions principales dans lesquelles des résultats non triviaux de logique ont été démontrés, à savoir la théorie de la démonstration, la théorie des ensembles, et la théorie des modèles.

Un premier point où l'introduction d'une logique formelle semble indispensable est la logique elle-même. Sans une formalisation convenable, il serait certainement difficile de démontrer des résultats précis, spécialement dans le cas des résultats négatifs. Etablir un résultat positif de prouvabilité peut se faire en décrivant explicitement une preuve, et il n'est pas forcément nécessaire que cela soit fait de façon formelle. Par contre, on voit mal comment établir des résultats négatifs de non-prouvabilité — typiquement le premier théorème d'incomplétude de Gödel du chapitre VIII qui affirme que, pour chaque théorie T*, une certaine formule* Δ_{T} *n'est pas prouvable à partir de* T *— sans une définition formelle de ce qu'est une preuve : montrer qu'un objet n'existe pas requiert la plupart du temps une description plus formelle que de montrer qu'il existe, car il est nécessaire de délimiter avec précision le champ des possibles.*

Un deuxième point où l'introduction d'une logique formelle est cruciale est la théorie des ensembles. Encore une fois, aussi longtemps qu'il s'agit d'établir des résultats positifs, par exemple la possibilité de démontrer à partir des axiomes de ZFC *le théorème de Silver sur l'hypothèse généralisée du continu en cofinalité non dénombrable (proposition V.4.9), aucun recours à un contexte formel de logique et de preuve n'est nécessaire. Par contre, comme on va le voir à partir du chapitre IX, seul le passage à la logique formelle et à la notion de modèle de* ZFC *permet d'aller plus loin et de démontrer des résultats négatifs, par exemple le fait que l'hypothèse du continu ne peut pas être démontrée à partir des axiomes de* ZFC*. C'est précisément cette raison qui a justifié l'insertion d'une introduction à la logique entre les parties A et C de ce texte.*

Enfin, un troisième point où l'introduction de la logique s'est avérée décisive est la théorie des modèles, qui est l'étude générale des structures définies par des formules du premier ordre. Depuis les années 1960, a été développée autour de la notion de structure stable due à S. Shelah toute une théorie de la classification pour les modèles des théories du premier ordre, à la façon dont on peut classifier les espaces vectoriels ou les surfaces compactes [**16**]*. On se doute qu'il n'y a pas de miracle à escompter : ce n'est pas parce qu'une propriété est exprimable par une formule du premier ordre qu'il devient automatiquement plus facile de la démontrer, et le fait que le théorème de Fermat puisse être exprimé par la suite des formules d'arithmétique du premier ordre* $\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \geqslant 1 (\boldsymbol{x}^{\mathsf{n}} + \boldsymbol{y}^{\mathsf{n}} \neq \boldsymbol{z}^{\mathsf{n}})$ *n'a pas beaucoup aidé à sa démonstration (les résultats*

décrits au chapitre X permettront tout au plus de garantir que, vue la forme syntaxiquement simple de l'énoncé, on peut utiliser à loisir l'axiome du choix ou l'hypothèse du continu, un procédé systématique permettant ensuite de les éliminer). Par contre, on peut mentionner ici que ce sont des questions d'exprimabilité et de définissabilité par des formules du premier ordre qui ont été à l'origine de résultats de géométrie algébrique nouveaux et hautement non triviaux, en particulier la démonstration par Ehud Hrushovski des conjectures dites de Mordell–Lang et de Manin–Mumford en toute caractéristique [**14, 1**]. ◁

4.5. Contexte métamathématique.

► Démontrer des énoncés du type $\mathsf{T} \vdash \mathsf{F}$ correspond à son tour à prouver des formules, ce qui conduit à distinguer le niveau des objets mathématiques de celui du discours sur ces objets. ◄

▷ *Moyennant la modélisation par la logique du premier ordre, le problème générique des mathématiques consiste à démontrer des énoncés du type* $\mathsf{T} \vdash \mathsf{F}$*, où* F *et* T *sont, respectivement, une formule et un ensemble de formules d'une certaine logique du premier ordre* $\mathfrak{L}_\Sigma$*, typiquement démontrer (ou réfuter) un énoncé tel que* $\mathsf{ZFC} \vdash \mathsf{HC}$*. Or une telle démonstration se place à son tour dans le cadre d'une logique ambiante qui précise les points de départ et les règles de démonstration licites, le tout constituant ce qu'on appelle souvent le* contexte métamathématique *de la démonstration, ou encore le niveau du discours, par opposition au niveau des objets mathématiques sur lesquels porte ce discours.*

Au départ, l'assertion $\mathsf{T} \vdash \mathsf{F}$ *n'est pas une formule d'une logique du premier ordre. Mais il est facile de définir un codage de tels énoncés par des formules du premier ordre. Typiquement, moyennant une numérotation des formules et des preuves, on peut coder les notions logiques, qui au départ mettent en jeu des mots sur un certain alphabet fini, à l'aide de formules d'arithmétique mettant en jeu des entiers. Ceci sera fait de façon explicite au chapitre VIII, mais, pour le moment, il n'est pas nécessaire d'entrer dans les détails, et on notera simplement* « $\mathsf{T} \vdash \mathsf{F}$ » *pour la formule (d'arithmétique) codant l'énoncé* $\mathsf{T} \vdash \mathsf{F}$*.*

La question est alors d'établir des formules du type « $\mathsf{T} \vdash \mathsf{F}$ »*, donc de les démontrer à partir d'une certaine base axiomatique* $\mathsf{T}^\star$*, au moyen d'une certaine notion de preuve* $\vdash^\star$*, et ce qu'on vise à établir, ce sont des énoncés dont la forme générale est*

$$\mathsf{T}^\star \vdash^\star \text{« } \mathsf{T} \vdash \mathsf{F} \text{ ».} \tag{4.1}$$

A supposer que le codage de la logique mette en jeu des entiers et que la formule « $\mathsf{T} \vdash \mathsf{F}$ » *soit une formule d'arithmétique, le système* $\mathsf{T}^\star$ *peut être par exemple le système de Peano* PA_1*, ou encore le système* ZFC *qui peut en être vu comme une extension. Par ailleurs, les mêmes arguments qui poussent à adopter les logiques du premier ordre comme outils de formalisation des énoncés mathématiques conduisent également à adopter ces logiques comme outils de formalisation du contexte métamathématique, auquel cas la relation de prouvabilité* $\vdash^\star$ *est la relation* $\vdash$*. Dans ce cas, la forme générale* (4.1) *devient simplement*

$$\mathsf{PA}_1 \vdash \text{« } \mathsf{T} \vdash \mathsf{F} \text{ ».} \quad \textit{ou} \quad \mathsf{ZFC} \vdash \text{« } \mathsf{T} \vdash \mathsf{F} \text{ ».} \tag{4.2}$$

Evidemment, la mise en abîme du passage de $\mathsf{T} \vdash \mathsf{F}$ *à* $\mathsf{T}^\star \vdash^\star$ « $\mathsf{T} \vdash \mathsf{F}$ » *pourrait être répétée. Il serait peut-être possible de défendre l'idée que l'itération se stabilise assez vite sur un système qui serait une forme faible du système de Peano* PA_1 *où le schéma d'induction est limité à des formules de forme syntaxique simple ; on pourrait aussi noter que cette régression potentiellement infinie traduit l'absence d'une définition intrinsèque de la sémantique des logiques du premier ordre puisque. Par exemple, et ainsi qu'on l'a déjà observé, la sémantique du* $\wedge$ *mathématique n'a été introduite qu'en référant à celle du* $\wedge$ *métamathématique, par une équivalence qu'on peut écrire*

$$\mathsf{T}^\star \vdash^\star \text{« } \models \mathsf{F} \wedge \mathsf{G} \text{ »} \iff \mathsf{T}^\star \vdash^\star \text{« } \models \mathsf{F} \text{ »} \wedge \text{« } \models \mathsf{G} \text{ »}$$

— mais une telle discussion n'est pas l'objet de ce texte. Ce qu'on veut souligner ici est simplement la distinction entre le niveau de $(\mathsf{T}^\star, \vdash^\star)$ *et celui de* $(\mathsf{T}, \vdash)$ *dans* (4.1)*, et le fait qu'il n'y a aucune raison de supposer que les logiques mises en jeu soient les mêmes, ni même que l'une inclue l'autre.*

Revenant par exemple au cas de l'assertion du lemme 3.3 $\mathsf{PA}{-}\mathsf{Ind} \vdash \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$ *pour* $\mathsf{p} + \mathsf{q} = \mathsf{r}$*, on peut alors comparer les contextes métamathématiques qui sous-tendent les deux démonstrations proposées, l'une syntaxique, l'autre sémantique. Même si l'arithmétisation des formules n'a pas encore été formalisée — ceci sera fait dans la section VIII.2 — il doit apparaître clair que la démonstration syntaxique n'utilise que des entiers et une induction sur ceux-ci, et donc peut être entièrement menée dans le contexte métamathématique de* PA_1 *(mais pas de* $\mathsf{PA}{-}\mathsf{Ind}$*). Avec les notations ci-dessus, ce qu'établit la démonstration syntaxique du lemme 3.3 est donc la relation*

$$\mathsf{PA}_1 \vdash \mathsf{p} + \mathsf{q} = \mathsf{r} \Rightarrow \text{« } \mathsf{PA}{-}\mathsf{Ind} \vdash \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0} \text{ ».} \tag{4.3}$$

Notons qu'une fois distingués clairement le niveau mathématique et le niveau métamathématique — c'est-à-dire le niveau des objets et celui du discours sur ces objets — toute interrogation concernant les entiers qu'on a appelés intuitifs devrait disparaître : les entiers intuitifs sont simplement ceux de la théorie $\mathsf{T}^\star$*, par opposition à ceux éventuellement présents dans la théorie* T *qu'on étudie. Dans l'exemple de la démonstration syntaxique du lemme 3.3, on montre des résultats sur les objets dont parle* $\mathsf{PA}{-}\mathsf{Ind}$ *— les entiers mathématiques donc — en utilisant dans* $\mathsf{T}^\star$*, ici* PA_1*, une induction sur les entiers métamathématiques (aussi appelés entiers intuitifs, ou entiers du discours), ce que le formalisme peut-être lourd de* (4.4) *a au moins l'avantage de rendre explicite.*

Considérons maintenant la démonstration sémantique du même lemme 3.3. La sémantique de la logique du premier ordre est définie par référence à des structures arbitraires : une structure est un ensemble muni d'opérations et de relations diverses, et, au moins a priori, cette sémantique ne peut être définie que dans un contexte permettant de parler d'ensembles et des notions dérivées. Jusqu'à preuve du contraire, le seul contexte métamathématique pour ce faire est une théorie des ensembles garantissant l'existence et les propriétés des structures alléguées, typiquement Z *ou* ZF*. Ce qu'établit la démonstration sémantique du lemme 3.3 correspond donc à*

$$\mathsf{ZF} \vdash \mathsf{p} + \mathsf{q} = \mathsf{r} \Rightarrow \text{« } \mathsf{PA}{-}\mathsf{Ind} \vdash \boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0} \text{ ».} \tag{4.4}$$

Dans l'énoncé ci-dessus, le contexte ZF *est certainement suffisant, mais, inversement, on n'affirme pas qu'il soit nécessaire : une théorie des ensembles plus faible pourrait suffire, par exemple* Z*, ou un fragment de celui-ci.*

On a souligné le gain d'efficacité apporté par la démonstration sémantique du lemme 3.3 par rapport à la démonstration syntaxique. On voit ici que ce gain a un coup : l'amélioration de l'efficacité est obtenue au prix d'un renforcement du contexte métamathématique, à savoir le passage de l'arithmétique à la théorie des ensembles. Ceci est très naturel : en adoptant des moyens de démonstrations plus puissants, on obtient des démonstrations plus rapides.

Par contre, adopter un contexte métamathématique fort affaiblit d'autant le poids d'une démonstration en termes de pouvoir de conviction. On a déjà souligné l'impossibilité de baser sur autre chose qu'un consensus l'adoption d'un système formel, et il paraît clair que, plus un système est faible, plus il est facile d'obtenir un consensus sur la validité des principes qu'il utilise : par exemple, tous les mathématiciens n'acceptent pas la validité d'un énoncé dont la démonstration utilise l'axiome du choix, et il sera certainement plus facile d'obtenir un consensus sur la validité d'une démonstration formalisable dans ZF *seul que sur celle d'une démonstration utilisant explicitement* AC*. De ce point de vue, le système de Peano* PA_1*, voire un fragment strict de celui-ci, est probablement un socle sur lequel le plus grand nombre pourra s'accorder. La même remarque vaut pour le système de preuve utilisé : si la prouvabilité du premier ordre* $\vdash$ *est le modèle le plus répandu, il existe des versions plus faibles, comme celles fondées sur la logique intuitionniste où le principe du tiers exclu est omis. De ce point de vue, un énoncé* $\mathsf{T} \vdash \mathsf{F}$ *établi dans le contexte* $(\mathsf{ZFC}, \vdash)$ *sera moins susceptible de recueillir un consensus que le même énoncé établi dans le contexte* $(\mathsf{PA}_1, \vdash_{int})$*, où* $\vdash_{int}$ *désigne la prouvabilité intuitionniste. Notons que la faiblesse du contexte métamathématique ne conditionne en rien celle du système mathématique considéré : ainsi,* F *étant une formule ensembliste quelconque, établir*

$$\mathsf{PA}_1 \vdash_{int} \text{« } \mathsf{ZFC} \vdash \mathsf{F} \text{ »}$$

fait sens : ceci signifie simplement fournir une démonstration de F *à partir des axiomes de* ZFC *qui soit entièrement formalisable dans l'arithmétique et n'utilise que des arguments syntaxiques de surcroît licites en logique intuitionniste. Là encore, et comme on l'a dit dans la section*

précédente, l'introduction de formalismes tels que celui de (4.1) *n'établit en lui-même aucun résultat nouveau, mais, à tout le moins, il permet de mettre les choses à plat et d'expliciter la place de chaque notion.*

Une dernière remarque en faveur du cadre « théorie des ensembles + logique du premier ordre » est la suivante. Certains mathématiciens, par exemple ceux qui travaillent sur des domaines proches de l'algorithmique ou de l'informatique théorique, peuvent n'être intéressés que par des objets effectifs et, de ce fait, préférer l'adoption d'un cadre logique plus strict où notamment le principe du tiers exclu n'est pas posé, typiquement adopter la logique intuitionniste. Ce point de vue est très défendable, mais, en pratique, il n'empêche pas de se placer dans le cadre usuel de la logique du premier ordre et, à l'intérieur de ce cadre, d'analyser les preuves pour déterminer si le tiers exclu y est utilisé ou non, à la façon dont on peut analyser si l'axiome du choix l'est. Qu'il s'agisse des axiomes ou des règles de déduction, le cadre libéral « théorie des ensembles + logique du premier ordre » apparaît comme une sorte de cadre maximal à l'intérieur duquel d'autres cadres plus spécifiques peuvent être isolés si on le souhaite. ◁

Appendice: logiques du second ordre

► On introduit les logiques du second ordre, et on montre que leur pouvoir d'expression est plus grand que celui des logiques du premier ordre, puisqu'on peut y caractériser la structure $(\mathbb{N}, 0, S, +, \cdot)$ ou y exprimer la finitude. Par contre, elles ne vérifient que très peu des résultats positifs obtenus pour les logiques du premier ordre. ◄

▷ *Constatant les limitations du pouvoir d'expression des logiques du premier ordre, il est naturel d'envisager des logiques plus riches. Un candidat naturel est la logique du second ordre, dont la syntaxe est du même type que la logique du premier ordre, à ceci près qu'on introduit, en plus des variables représentant les éléments du domaine de la structure qu'on veut analyser, de nouvelles variables représentant les sous-ensembles du domaine, ou, de façon synonyme, les relations sur le domaine : autrement dit, on s'autorise à quantifier sur les relations, donc, en particulier, sur les sous-ensembles du domaine vus comme relations unaires. Un exemple typique de formule du second ordre, par rapport à la signature usuelle de l'arithmétique, est l'axiome d'induction du système de Peano*

$$\forall \boldsymbol{X}((\boldsymbol{X}(\mathbf{0}) \wedge \forall \boldsymbol{x}(\boldsymbol{X}(\boldsymbol{x}) \Rightarrow \boldsymbol{X}(\boldsymbol{S}(\boldsymbol{x})))) \Rightarrow \forall \boldsymbol{x}(\boldsymbol{X}(\boldsymbol{x}))), \tag{4.5}$$

où $\boldsymbol{X}$ représente une relation unaire. La sémantique est définie de façon naturelle, par rapport à un contexte supposé spécifié de théorie des ensembles. ◁

On note $\mathrm{Th}_2(\mathcal{M})$ l'ensemble des formules closes du second ordre satisfaites dans une structure $\mathcal{M}$.

PROPOSITION. *Tout modèle de* $\mathrm{Th}_2(\mathbb{N}, 0, S, +, \cdot)$ *est isomorphe à* $(\mathbb{N}, 0, S, +, \cdot)$.

DÉMONSTRATION. Soit $\mathcal{M}$ un modèle de $\mathrm{Th}_2(\mathbb{N}, 0, S, +, \cdot)$. *A fortiori* $\mathcal{M}$ est modèle de $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$, et, d'après la proposition 3.16, l'application $f : \mathsf{n} \mapsto \boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ est un isomorphisme de $(\mathbb{N}, 0, S, +, \cdot)$ sur une sous-structure de $\mathcal{M}$ dont le domaine $\mathbb{N}_\bullet$ est un segment initial du domaine de $\mathcal{M}$. Or, par hypothèse, la formule (4.5) est satisfaite dans $(\mathbb{N}, 0, S, +, \cdot)$, donc aussi dans $\mathcal{M}$: en l'appliquant à $\mathbb{N}_\bullet$, qui est un ensemble contenant $\mathbf{0}^{\mathcal{M}}$ et clos par $\boldsymbol{S}^{\mathcal{M}}$, on conclut que $\mathbb{N}_\bullet$ est l'intégralité du domaine de $\mathcal{M}$, c'est-à-dire que $\mathcal{M}$ est isomorphe à $(\mathbb{N}, 0, S, +, \cdot)$. □

PROPOSITION. (AC_ω) *Il existe deux formules closes du second ordre dont les modèles sont respectivement les structures finies et et les structures finies ou dénombrables.*

DÉMONSTRATION. En présence de AC_ω, un ensemble M est fini si et seulement si toute injection de M dans M est surjective, c'est-à-dire si, pour toute fonction $f : M \to M$ on a

$$\forall \boldsymbol{x}, \boldsymbol{y}\, (f(\boldsymbol{x}){=}f(\boldsymbol{y}){\Rightarrow}\boldsymbol{x}{=}\boldsymbol{y}) \Rightarrow \forall \boldsymbol{y}\, \exists \boldsymbol{x}\, (f(\boldsymbol{x}){=}\boldsymbol{y}).$$

C'est encore dire que toute relation binaire R sur M qui est fonctionnelle, c'est-à-dire qui satisfait $\mathsf{G}(R)$:

$$\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}\, ((R(\boldsymbol{x}, \boldsymbol{y}) \wedge R(\boldsymbol{x}, \boldsymbol{z})) \Rightarrow \boldsymbol{y}{=}\boldsymbol{z}),$$

satisfait aussi $\mathsf{G}'(R)$:

$$\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}((R(\boldsymbol{x}, \boldsymbol{z}) \wedge R(\boldsymbol{y}, \boldsymbol{z}) \Rightarrow \boldsymbol{x}{=}\boldsymbol{y}) \Rightarrow \forall \boldsymbol{y}\, \exists \boldsymbol{x}\, (R(\boldsymbol{x}, \boldsymbol{y})).$$

Soit F la formule $\forall \boldsymbol{X}\, (\mathsf{G}(\boldsymbol{X}){\Rightarrow}\mathsf{G}'(\boldsymbol{X}))$. Alors une structure satisfait F si et seulement si son domaine est fini.

De même, un ensemble M est fini ou dénombrable s'il existe sur M un ordre total dont tout segment initial est fini. Or il existe une formule $\mathsf{H}(\boldsymbol{X})$ telle que $\mathsf{H}(R)$ est satisfaite si et seulement si R est un ordre total. Soit alors F' la formule

$$\exists \boldsymbol{X}\, (\mathsf{H}(\boldsymbol{X}) \wedge \forall \boldsymbol{x}\, \exists \boldsymbol{Y}\, (\mathsf{F}(\boldsymbol{Y}) \wedge \forall \boldsymbol{y}(\boldsymbol{Y}(\boldsymbol{y}){\Leftrightarrow}\boldsymbol{X}(\boldsymbol{y}, \boldsymbol{x})),$$

où $\mathsf{F}(\boldsymbol{Y})$ est la formule suivante, qui exprime que $\boldsymbol{Y}$ est finie,

$$\forall \boldsymbol{Z}\, \forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}\, (\boldsymbol{Z}(\boldsymbol{x}, \boldsymbol{y}){\Rightarrow}(\boldsymbol{Y}(\boldsymbol{x}){\wedge}\boldsymbol{Y}(\boldsymbol{y})) \wedge (\boldsymbol{Z}(\boldsymbol{x}, \boldsymbol{y}){\wedge}\boldsymbol{Z}(\boldsymbol{x}, \boldsymbol{z})){\Rightarrow}\boldsymbol{y}{=}\boldsymbol{z}) \Rightarrow$$
$$\forall \boldsymbol{x}\, \forall \boldsymbol{y}\, \forall \boldsymbol{z}\ ((\boldsymbol{Z}(\boldsymbol{x}, \boldsymbol{z}){\wedge}\boldsymbol{Z}(\boldsymbol{y}, \boldsymbol{z}){\Rightarrow}\boldsymbol{x}{=}\boldsymbol{y}) \Rightarrow \forall \boldsymbol{y}\, \exists \boldsymbol{x}\, (\boldsymbol{Z}(\boldsymbol{x}, \boldsymbol{y}))).$$

Alors une structure satisfait F' si et seulement si son domaine est fini ou dénombrable. □

▷ *On verra au chapitre VIII qu'il ne peut exister de notion de preuve garantissant un théorème de complétude raisonnable en logique du second ordre — et c'est là le point négatif principal. Pour le moment, on se borne à remarquer le résultat suivant.* ◁

PROPOSITION. *Les logiques du second ordre ne satisfont ni le théorème de compacité, ni le théorème de Lowenheim–Skolem.*

DÉMONSTRATION. Pour chaque entier naturel n, il existe une formule du premier ordre F_n exprimant que le domaine a au moins n éléments. La théorie du second ordre formée par la formule F du lemme 4.5 et de chacune des formules F_n n'est pas satisfaisable, alors que tout sous-ensemble fini l'est. Par conséquent le théorème de compacité est en défaut.

Par ailleurs, la formule F' du lemme 4.5 est un contre-exemple au théorème de Lowenheim–Skolem, puisqu'elle n'a que des modèles dénombrables. □

Exercices

EXERCICE 1. (axiomes) Montrer que, dans la liste des axiomes pour $\mathcal{L}_\Sigma$, on peut remplacer les axiomes pour l'égalité par les formules $\boldsymbol{x} = \boldsymbol{x}$ et $\boldsymbol{x} = \boldsymbol{y}{\Rightarrow}\mathsf{F}(\boldsymbol{x}){\Leftrightarrow}\mathsf{F}(\boldsymbol{y})$ avec $\boldsymbol{x}$ et $\boldsymbol{y}$ sont libres pour $\boldsymbol{z}$ dans $\mathsf{F}(\boldsymbol{z})$.

EXERCICE 2. (cycle) Pour R relation binaire sur X, on dit que $(a_1, ..., a_\mathsf{k})$ est un cycle de longueur k pour R si on a à la fois $a_1\, R\, a_2$, ..., $a_{k-1}\, R\, a_\mathsf{k}$, et $a_\mathsf{k}\, R\, a_1$. Que signifie le fait de ne pas avoir de cycle de longueur 1 ? de longueur 2 ? Montrer que la propriété d'avoir un cycle de longueur finie ne peut pas s'exprimer par une formule du premier ordre en R.

EXERCICE 3. (pouvoir d'expression) Montrer que la propriété pour un groupe d'être de torsion et la propriété pour un ordre total d'être un bon ordre ne sont pas exprimables au premier ordre. Montrer que la propriété pour un corps d'être de caractéristique zéro n'est pas finiment exprimable au premier ordre.

EXERCICE 4. (définissabilité) (*i*) On note $|$ la relation de divisibilité sur $\mathbb{N}$; montrer que l'entier 1 est définissable dans $(\mathbb{N}, |)$.

(*ii*) Montrer que la relation (unaire) « n est un nombre premier » est définissable dans $(\mathbb{N}, |)$.

(*iii*) Montrer que les opérations binaires pgcd et ppcm sont définissables dans $(\mathbb{N}, |)$.

(*iv*) On note S l'opération successeur de $\mathbb{N}$. Montrer que S est définissable dans $(\mathbb{N}, <)$.

(*v*) Montrer que, pour tous entiers $\mathsf{p}, \mathsf{q}, \mathsf{r}$ il y a équivalence entre $S(\mathsf{pr})S(\mathsf{qr}) = S(S(\mathsf{pq})r^2)$ et la disjonction $\mathsf{r} = 0$ ou $\mathsf{p} + \mathsf{q} = \mathsf{r}$. En déduire que l'addition est définissable dans $(\mathbb{N}, \times, <)$.

(*vi*) Montrer que 0 est définissable dans $(\mathbb{Z}, +)$, mais que 1 n'y est pas définissable.

EXERCICE 5. (définissabilité) Montrer que l'ordre usuel est définissable dans $(\mathbb{Z}, +, \times)$.

EXERCICE 6. (définissabilité) Montrer que l'ordre usuel des réels est définissable dans la structure $(\mathbb{R}, +, \times)$. En déduire que tout réel algébrique y est définissable.

EXERCICE 7. (définissabilité) Montrer que la relation « $x \in \mathbb{R}$ » est définissable dans la structure $(\mathbb{C}, +, \times, \sigma)$, où σ désigne la conjugaison. Montrer que le nombre complexe i n'est pas définissable dans $(\mathbb{C}, +, \times, \sigma)$, mais que tout nombre complexe algébrique est définissable dans la structure $(\mathbb{C}, +, \times, \sigma, i)$. Comment établir l'implication réciproque ?

EXERCICE 8. (théorie) Montrer que, pour toute structure $\mathcal{R}$ de type Σ, la famille $\mathrm{Th}_1(\mathcal{R})$ est une théorie complète de $\mathcal{L}_\Sigma$. Montrer que, si, en outre, la signature Σ contient un symbole de constante pour chaque élément du domaine de $\mathcal{R}$, alors $\mathrm{Th}_1(\mathcal{R})$ est explicitement complète.

EXERCICE 9. (arithmétique) Soit PA_0 la théorie de $\mathcal{L}_{\{\mathbf{0},\boldsymbol{S},+\}}$ constituée des formules $\forall \boldsymbol{x}(\boldsymbol{x} \neq \mathbf{0} \Leftrightarrow \exists \boldsymbol{y}(\boldsymbol{x} = \boldsymbol{S}(\boldsymbol{y})))$, $\forall \boldsymbol{x}, \boldsymbol{y}(S(\boldsymbol{x}) = S(\boldsymbol{y}) \Rightarrow \boldsymbol{x} = \boldsymbol{y})$, $\forall \boldsymbol{x}(\boldsymbol{x} + \mathbf{0} = \mathbf{0} + \boldsymbol{x} = \boldsymbol{x})$, $\forall \boldsymbol{x}, \boldsymbol{y}(\boldsymbol{x} + \boldsymbol{S}(\boldsymbol{y}) = \boldsymbol{S}(\boldsymbol{x} + \boldsymbol{y}))$. On définit une structure $\mathcal{M}$ de domaine $\mathbb{N} \cup \mathbb{N} \times \mathbb{Z}$ en posant $\mathbf{0}^{\mathcal{M}} = 0$, $\boldsymbol{S}^{\mathcal{M}}(\mathsf{p}) = \mathsf{p} + 1$, $\boldsymbol{S}^{\mathcal{M}}((\mathsf{n}, \mathsf{p})) = (\mathsf{n}, \mathsf{p} + 1)$, et $\mathsf{n}_1 +^{\mathcal{M}} \mathsf{n}_2 = \mathsf{n}_1 + \mathsf{n}_2$, $(\mathsf{n}_1, \mathsf{p}_1) +^{\mathcal{M}} \mathsf{n}_2 = (\mathsf{n}_1, \mathsf{n}_2 + \mathsf{p}_1)$, $\mathsf{n}_1 +^{\mathcal{M}} (\mathsf{n}_2, \mathsf{p}_2) = (\mathsf{n}_2, \mathsf{n}_1 + \mathsf{p}_2)$, $(\mathsf{n}_1, \mathsf{p}_1) +^{\mathcal{M}} (\mathsf{n}_1, \mathsf{p}_2) = (\mathsf{n}_1, \mathsf{p}_1 + \mathsf{p}_2)$, $(\mathsf{n}_1, \mathsf{p}_1) +^{\mathcal{M}} (\mathsf{n}_2, \mathsf{p}_2) = (\mathsf{n}_1 + 2\mathsf{n}_2, \mathsf{p}_1 + \mathsf{p}_2)$ pour $\mathsf{n}_1 \neq \mathsf{n}_2$. Montrer que $\mathcal{M}$ satisfait PA_0. Vérifier que $+^{\mathcal{M}}$ n'est ni commutative, ni associative, et en déduire que la commutativité et l'associativité de l'addition ne peuvent pas se prouver à partir de PA_0.