CHAPITRE VIII

Les théorèmes de limitation

RÉSUMÉ. • *Les fonctions* primitives récursives *s'obtiennent à partir des fonctions constante, successeur et projections par composition et récursion.*
• *La plupart des fonctions usuelles sur* $\mathbb{N}^{\mathsf{p}}$ *sont primitives récursives. En particulier, il existe des numérotations primitives récursives des suites d'entiers.*
• *Les fonctions* récursives *s'obtiennent de même mais en ajoutant l'opération de minimalisation.*
• *Les fonctions récursives coïncident avec les fonctions calculables par machine de Turing, donc, modulo la* thèse de Church–Turing, *avec les fonctions calculables.*
• *On peut numéroter les formules de la logique du premier ordre de façon à ce que toutes les manipulations syntaxiques correspondent à des fonctions récursives.*
• *Soit* $\mathsf{PA}_{\text{faible}}$ *le système de Robinson, qui est le système de Peano sans induction mais avec une définition de l'ordre. Il existe des modèles de* $\mathsf{PA}_{\text{faible}}$ *très différents de* $(\mathbb{N}, 0, S, +, \cdot)$*, mais tout modèle de* $\mathsf{PA}_{\text{faible}}$ *est une* extension finale *de* $(\mathbb{N}, 0, S, +, \cdot)$*.*
• *Les formules* Σ_1 *sont les formules où toutes les quantifications universelles sont bornées* $\forall \boldsymbol{x} \leqslant \boldsymbol{y}$*. Toute formule close* Σ_1 *vraie dans* $(\mathbb{N}, 0, S, +, \cdot)$ *est prouvable à partir de* $\mathsf{PA}_{\text{faible}}$*.*
• *Toute fonction récursive totale* f *est représentable dans* $\mathsf{PA}_{\text{faible}}$*: il existe une formule* F *telle que* $\mathsf{m} = f(\vec{\mathsf{n}})$ *implique* $\mathsf{PA}_{\text{faible}} \vdash \mathsf{F}(\boldsymbol{S}^{\vec{\mathsf{n}}}\boldsymbol{0}, \boldsymbol{x}) \Leftrightarrow \boldsymbol{x} = \boldsymbol{S}^{\mathsf{m}}\boldsymbol{0}$*.*
• *La numérotation des formules et l'argument diagonal (autoréférence plus négation) mènent aux « grands » résultats d'impossibilité.*
• *Le théorème de Tarski affirme qu'aucune formule ne définit les numéros des formules closes vraies dans* $\mathbb{N}$*.*
• *Le premier théorème d'incomplétude de Gödel affirme qu'aucun système récursif du premier ordre* T *ne peut axiomatiser l'arithmétique: il existe toujours une formule vraie dans* $\mathbb{N}$ *et non prouvable à partir de* T*. Ceci s'applique en particulier au système de Peano* PA_1*, qui est donc incomplet.*
• *Le second théorème d'incomplétude de Gödel affime qu'aucune théorie consistante incluant le système de Peano* PA_1 *ne prouve sa propre consistance.*

▶ L'objet de ce chapitre est de démontrer des théorèmes établis dans les années 1930 exprimant des limitations intrinsèques de la logique du premier ordre, au premier rang desquels les célèbres théorèmes d'incomplétude de Gödel.

La démonstration de ces théorèmes de limitation repose sur un argument diagonal assez simple et en tout cas rapide, et elle est exposée dans la section 4 de ce chapitre — et rien n'empêche le lecteur curieux de commencer par là. Pour obtenir des démonstrations complètes, on doit auparavant introduire plusieurs notions auxiliaires et établir divers résultats préparatoires, qui du reste ont un intérêt indépendant. La section 1 est consacrée aux fonctions récursives, qui sont une formalisation de la notion informelle de fonction effectivement calculable. Dans la section 2, on montre comment, par une numérotation soigneuse, on

peut coder les notions de base de la logique à l'intérieur de la structure $(\mathbb{N}, 0, S, +, \cdot)$ à l'aide de fonctions et de relations récursives. Dans la section 3, on montre que la version affaiblie $\mathsf{PA}_{\text{faible}}$ de l'arithmétique de Peano dans laquelle l'induction est omise prouve suffisamment de formules pour représenter en un sens convenable toutes les fonctions récursives. ◀

▷ *Au chapitre précédent, on a établi pour la logique du premier ordre un résultat positif important, à savoir le théorème de complétude, ainsi que quelques résultats négatifs exprimant des limitations à son pouvoir d'expression. Ces résultats pourraient suggérer que la logique du premier ordre est relativement rudimentaire, à la façon de la logique propositionnelle du chapitre VI. On va voir ici qu'il n'en est rien : la logique du premier ordre est extrêmement compliquée et riche, au sens où en particulier il ne peut exister de moyen effectif exhaustif pour reconnaître les formules valides ou pour prouver la consistance d'une théorie : c'est ce qu'exprime toute une famille de résultats négatifs incluant en particulier les célèbres théorèmes d'incomplétude de Gödel qui affirment d'une part l'existence de formules vraies dans la structure* $(\mathbb{N}, 0, S, +, \cdot)$ *et non prouvables à partir du système de Peano du premier ordre* PA_1*, et d'autre part l'impossibilité pour une théorie consistante incluant* PA_1 *de prouver sa propre consistance. On donne ici une démonstration qui n'est complète que pour les théories incluant* Z. ◁

1. Fonctions et relations récursives

▶ On définit les fonctions et les relations récursives sur $\mathbb{N}$ et on en établit les propriétés de base, en particulier en montrant que la plupart des fonctions usuelles sont récursives. On observe également que les fonctions récursives sont exactement celles qui sont calculables par machine de Turing. ◀

▷ *Dans bien des situations, on a besoin de contrôler la complexité des objets considérés, et en particulier d'en connaître une définition explicite. On considère ici le cas des fonctions sur les entiers, et on étudie sous le nom de fonctions récursives une famille particulière de telles fonctions qui possèdent des définitions simples, en l'occurrence les fonctions qu'on obtient à partir de fonctions de base au moyen de règles de construction fixées. Avant toute description précise, on pourra noter que, quel que soit le type de définition considéré, pour peu qu'une définition soit un mot sur un alphabet fini, il existe au plus une infinité dénombrable de fonctions définissables, alors que l'ensemble de toutes les fonctions de* $\mathbb{N}$ *dans* $\mathbb{N}$ *envisagées jusqu'à présent est un ensemble non dénombrable, d'où il résulte qu'il existe nécessairement une infinité non dénombrable de fonctions non définissables*[1]*.*

Une fois les notions de base définies, l'objet principal de cette section est de vérifier que la plupart des fonctions et relations usuelles sur les entiers sont récursives. Il s'agit de vérifications fastidieuses mais faciles : à partir des fonctions de base (qui jouent le rôle d'axiomes), on construit de proche en proche une liste de fonctions de plus en plus riche, et, à chaque étape, la question est de vérifier que la nouvelle fonction ou la nouvelle relation dont on veut établir le caractère récursif possède bien une définition du type autorisé à partir des éléments précédents de la liste. C'est typiquement le genre de vérification qu'il est indispensable d'effectuer une fois, mais qu'on peut ensuite oublier sans grand dommage. ◁

Dans cette section, toutes les fonctions considérées sont des fonctions de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$, partout définies dans les sous-sections 1.1 à 1.3, puis quelconques à partir de la sous-section 1.4.

[1] et même qu'en un sens informel la densité des fonctions définissables est nulle

1.1. Fonctions primitives récursives.

▶ Avant d'introduire les fonctions récursives générales, on commence par la famille plus restreinte des fonctions dites *primitives récursives*. ◀

▷ *Le point de vue retenu ici est qu'une fontion est effective si elle peut être construite à partir de quelques fonctions de base simples telles que la fonction successeur par des opérations préservant le caractère effectif, typiquement des définitions récursives du type considéré dans la section III.3.* ◁

DÉFINITION 1.1. (primitif récursif) Pour $f_1, \ldots, f_q$ fonctions de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$, et g de $\mathbb{N}^{\mathsf{q}}$ dans $\mathbb{N}$, on note $\mathtt{comp}(g, f_1, \ldots, f_{\mathsf{q}})$ la fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ définie par

$$f(\vec{\mathsf{n}}) := g(f_1(\vec{\mathsf{n}}), \ldots, f_q(\vec{\mathsf{n}})),$$

et on dit que f est définie par *composition* à partir de g, f_1, $\ldots$, f_{q}. Pour g, h fonctions de $\mathbb{N}^{\mathsf{p}}$ et $\mathbb{N}^{\mathsf{p}+2}$ dans $\mathbb{N}$, on note $\mathtt{rec}(g, h)$ la fonction f de $\mathbb{N}^{\mathsf{p}+1}$ dans $\mathbb{N}$ définie par

$$f(\vec{\mathsf{n}}, \mathsf{k}) := \begin{cases} g(\vec{\mathsf{n}}) & \text{pour } \mathsf{k} = 0, \\ h(\vec{\mathsf{n}}, \mathsf{k}, f(\vec{\mathsf{n}}, \mathsf{k}-1)) & \text{pour } \mathsf{k} > 0, \end{cases}$$

et on dit que f est définie par *récursion* de base g et de pas h. Une fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ est dite *primitive récursive* si elle peut s'obtenir par un nombre fini de compositions et de récursions à partir des fonctions $\mathtt{zero}$, $\mathtt{succ}$ et $\mathtt{proj}_{\mathsf{p},\mathsf{i}}$ avec $1 \leqslant \mathsf{i} \leqslant \mathsf{p}$, où

- $\mathtt{zero}$ est la fonction de $\mathbb{N}^0$ dans $\mathbb{N}$ définie par $\mathtt{zero} := 0$ [2],
- $\mathtt{succ}$ est la fonction de $\mathbb{N}$ dans $\mathbb{N}$ définie par $\mathtt{succ}(\mathsf{n}) := S(\mathsf{n}) = \mathsf{n} + 1$,
- $\mathtt{proj}_{\mathsf{p},\mathsf{i}}$ est la fonction de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ définie par $\mathtt{proj}_{\mathsf{p},\mathsf{i}}(\mathsf{n}_1, ..., \mathsf{n}_{\mathsf{p}}) := \mathsf{n}_{\mathsf{i}}$.

Une relation R sur $\mathbb{N}^{\mathsf{p}}$ — ou, de façon équivalente, un sous-ensemble R de $\mathbb{N}^{\mathsf{p}}$ — est dite *primitive récursive* si sa fonction indicatrice $\mathbf{1}_R$, définie par $\mathbf{1}_R(\vec{\mathsf{n}}) := 1$ pour $\vec{\mathsf{n}}$ dans R et $\mathbf{1}_R(\vec{\mathsf{n}}) := 0$ sinon, est primitive récursive.

EXEMPLE 1.2. (primitive récursive) L'addition $\mathtt{add}$ est une fonction primitive récursive, puisqu'elle obéit à la définition récursive

$$\mathtt{add}(\mathsf{n}, \mathsf{k}) = \mathsf{n} + \mathsf{k} := \begin{cases} \mathsf{n} & \text{pour } \mathsf{k} = 0, \\ S(\mathsf{n} + (\mathsf{k} - 1)) = \mathtt{succ}(\mathtt{add}(\mathsf{n}, \mathsf{k} - 1)) & \text{pour } \mathsf{k} > 0. \end{cases}$$

On a donc $\mathtt{add} = \mathtt{rec}(g, h)$, où g est la fonction identité de $\mathbb{N}$, c'est-à-dire $\mathtt{proj}_{1,1}$, et où h est la fonction de $\mathbb{N}^3$ dans $\mathbb{N}$ définie par $h(\mathsf{n}, \mathsf{k}, \mathsf{m}) := \mathtt{succ}(\mathsf{m})$. On a donc $h = \mathtt{comp}(\mathtt{succ}, \mathtt{proj}_{3,3})$, et, finalement, $\mathtt{add} = \mathtt{rec}(\mathtt{proj}_{1,1}, \mathtt{comp}(\mathtt{succ}, \mathtt{proj}_{3,3}))$.

[2] c'est-à-dire la constante 0 ; on pourrait éviter le recours à des fonctions à zéro argument en partant d'une fonction constante à un argument, mais définir par récursion les fonctions de $\mathbb{N}$ dans $\mathbb{N}$ poserait ensuite un problème (mineur) qui obligerait à traiter ce cas séparément

LEMME 1.3. (*i*) *Soit π une permutation de $\{1, ..., \mathsf{p}\}$. Si une fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ est primitive récursive, il en est de même de la fonction f^π de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ définie par $f^\pi(\mathsf{n}_1, ..., \mathsf{n}_{\mathsf{p}}) := f(\mathsf{n}_{\pi(1)}, ..., f(\mathsf{n}_{\pi(\mathsf{p})}))$.*

(*ii*) *Sont primitifs récursifs :*

- *pour tous p, m, la fonction constante $\mathtt{const}_{\mathsf{p},\mathsf{m}}$ de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ de valeur m ;*
- *l'addition, la multiplication et l'exponentiation ;*
- *les relations d'égalité et d'ordre ;*
- *les singletons.*

DÉMONSTRATION. (*i*) Par définition, on a

$$f^\pi = \mathtt{comp}(f, \mathtt{proj}_{\mathsf{p},\pi(1)}, ..., \mathtt{proj}_{\mathsf{p},\pi(\mathsf{p})}),$$

et, en substituant à f dans cette expression une définition de f en termes des fonctions de base, on obtient une définition de f^π en termes des mêmes fonctions de base, ce qui atteste du caractère primitif récursif de f^π.

(*ii*) On montre par récurrence sur p que la fonction $\mathtt{const}_{\mathsf{p},0}$ est primitive récursive. Pour $\mathsf{p} = 0$, la fonction est $\mathtt{zero}$, et le résultat est vrai par définition. Pour $\mathsf{p} = 1$, la fonction $\mathtt{const}_{1,0}$ est définie par la récursion

$$\mathtt{const}_{1,0}(\mathsf{k}) = \begin{cases} 0 & \text{pour } \mathsf{k} = 0, \\ \mathtt{const}_{1,0}(\mathsf{k}-1) & \text{pour } \mathsf{k} > 0, \end{cases}$$

donc $\mathtt{const}_{1,0}$ est définie par récursion de base $\mathtt{zero}$ et de pas h, où h est définie par $h(\mathsf{n}, \mathsf{m}) = \mathsf{m}$, soit $h = \mathtt{proj}_{2,2}$; on a donc $\mathtt{const}_{1,0} = \mathtt{rec}(\mathtt{zero}, \mathtt{proj}_{2,2})$, et $\mathtt{const}_{1,0}$ est primitive récursive. Enfin, pour $\mathsf{p} \geqslant 2$, on a $\mathtt{const}_{\mathsf{p},0}(\vec{\mathsf{n}}) = \mathtt{const}_{1,0}(\mathsf{n}_1) = \mathtt{const}_{1,0}(\mathtt{proj}_{\mathsf{p},1}(\vec{\mathsf{n}}))$, donc par conséquent $\mathtt{const}_{\mathsf{p},0} = \mathtt{comp}(\mathtt{const}_{1,0}, \mathtt{proj}_{\mathsf{p},1})$, à nouveau une fonction primitive récursive. Ensuite, on montre par récurrence sur m que $\mathtt{const}_{\mathsf{p},\mathsf{m}}$ est primitive récursive pour tout m. Pour $\mathsf{m} = 0$, le résultat vient d'être démontré. Pour $\mathsf{m} > 0$, on a $\mathtt{const}_{\mathsf{p},\mathsf{m}}(\vec{\mathsf{n}}) = S(\mathtt{const}_{\mathsf{p},\mathsf{m}-1}(\vec{\mathsf{n}}))$ pour tout $\vec{\mathsf{n}}$, soit $\mathtt{const}_{\mathsf{p},\mathsf{m}} = \mathtt{comp}(\mathtt{succ}, \mathtt{const}_{\mathsf{p},\mathsf{m}-1})$. Par hypothèse de récurrence, $\mathtt{const}_{\mathsf{p},\mathsf{m}-1}$ est primitive récursive, donc il en est de même de $\mathtt{const}_{\mathsf{p},\mathsf{m}}$.

On a vu dans l'exemple 1.2 que l'addition est primitive récursive puisque définie par récursion à partir de la fonction successeur. La multiplication $\mathtt{mult}$ est définie à partir de l'addition par la récursion

$$\mathtt{mult}(\mathsf{n}, \mathsf{k}) = \mathsf{n} \cdot \mathsf{k} := \begin{cases} 0 & \text{pour } \mathsf{k} = 0, \\ (\mathsf{n} \cdot (\mathsf{k}-1)) + \mathsf{n} & \text{pour } \mathsf{k} > 0, \end{cases}$$

d'où $\mathtt{mult} = \mathtt{rec}(\mathtt{const}_{1,0}, f)$, où h est la fonction de $\mathbb{N}^3$ dans $\mathbb{N}$ définie par $h(\mathsf{n}, \mathsf{k}, \mathsf{m}) := \mathsf{m} + \mathsf{n}$, soit $\mathtt{comp}(\mathtt{add}, \mathtt{proj}_{3,3}, \mathtt{proj}_{3,1})$, d'où $\mathtt{mult} = \mathtt{rec}(\mathtt{const}_{1,0}, \mathtt{comp}(\mathtt{add}, \mathtt{proj}_{3,3}, \mathtt{proj}_{3,1}))$. Comme $\mathtt{const}_{1,0}$ et $\mathtt{add}$ sont primitives récursives, $\mathtt{mult}$ l'est également. De même encore, l'exponentielle $\mathtt{exp}$ est primitive récursive puisque définie par la récursion

$$\mathtt{exp}(\mathsf{n}, \mathsf{k}) = \mathsf{n}^{\mathsf{k}} := \begin{cases} 1 & \text{pour } \mathsf{k} = 0, \\ \mathtt{mult}(\mathtt{exp}(\mathsf{n}, \mathsf{k}-1)), \mathsf{n}) & \text{pour } \mathsf{k} > 0. \end{cases}$$

Ensuite, le singleton $\{0\}$ est primitif récursif, puisque sa fonction indicatrice $\mathbf{1}_{\{0\}}$ est définie par la récursion

$$\mathbf{1}_{\{0\}}(\mathsf{k}) := \begin{cases} 1 & \text{pour } \mathsf{k} = 0, \\ 0 & \text{pour } \mathsf{k} > 0, \end{cases}$$

d'où $\mathbf{1}_{\{0\}} = \mathtt{rec}(\mathtt{const}_{0,1}, \mathtt{const}_{2,0})$. Puis l'ensemble $2\mathbb{N}$ des nombres pairs est primitif récursif puisqu'on a

$$\mathbf{1}_{2\mathbb{N}}(\mathsf{k}) := \begin{cases} 1 & \text{pour } \mathsf{k} = 0, \\ \mathbf{1}_{\{0\}}(\mathbf{1}_{2\mathbb{N}}(\mathsf{k}-1)) & \text{pour } \mathsf{k} > 0, \end{cases}$$

d'où $\mathbf{1}_{2\mathbb{N}} = \mathtt{rec}(\mathtt{const}_{0,1}, \mathtt{comp}(\mathbf{1}_{\{0\}}, \mathtt{proj}_{2,2}))$. Ensuite, la fonction `moitie` telle que $\mathtt{moitie}(\mathsf{n})$ est la partie entière de $\mathsf{n}/2$ est primitive récursive, car on a

$$\mathtt{moitie}(\mathsf{k}) := \begin{cases} 0 & \text{pour } \mathsf{k} = 0, \\ \mathtt{moitie}(\mathsf{k}-1) + \mathbf{1}_{2\mathbb{N}}(\mathsf{k}) & \text{pour } \mathsf{k} > 0, \end{cases}$$

donc `moitie` est définie par récursion de base `zero` et de pas la fonction h telle que $h(\mathsf{k}, \mathsf{m})$ est $\mathsf{m} + \mathbf{1}_{2\mathbb{N}}(\mathsf{k})$, d'où $\mathtt{moitie} = \mathtt{rec}(\mathtt{zero}, \mathtt{comp}(\mathtt{add}, \mathtt{proj}_{2,2}, \mathtt{comp}(\mathbf{1}_{2\mathbb{N}}, \mathtt{proj}_{2,1})))$.

Considérons alors la décrémentation `decr` définie par $\mathtt{decr}(\mathsf{n}) := 0$ pour $\mathsf{n} = 0$ et $\mathtt{decr}(\mathsf{n}) := \mathsf{n} - 1$ sinon. Pour $\mathsf{n} \geqslant 1$, on a

$$\mathtt{decr}(\mathsf{n}) = \mathtt{moitie}(\mathsf{n}) + \mathtt{moitie}(\mathtt{decr}(\mathsf{n}-1) + 1),$$

ainsi qu'on le vérifie en séparant les cas de n pair et impair. Comme `decr` est définie par la récursion

$$\mathtt{decr}(\mathsf{k}) := \begin{cases} 0 & \text{pour } \mathsf{k} = 0, \\ \mathtt{moitie}(\mathtt{decr}(\mathsf{k}-1) + 1) + \mathtt{moitie}(\mathsf{k}) & \text{pour } \mathsf{k} > 0, \end{cases}$$

elle est primitive récursive, puisque définie par récursion de base `zero` et de pas la fonction h définie par $h(\mathsf{k}, \mathsf{m}) = \mathtt{moitie}(\mathsf{m}+1) + \mathtt{moitie}(\mathsf{k})$, laquelle est primitive récursive puisque `add` et `moitie` le sont. Ensuite, la différence positive `diff` est primitive récursive puisque définie par la récursion

$$\mathtt{diff}(\mathsf{n}, \mathsf{k}) := \begin{cases} \mathsf{n} & \text{pour } \mathsf{k} = 0, \\ \mathtt{decr}(\mathtt{diff}(\mathsf{n}, \mathsf{k}-1)) & \text{pour } \mathsf{k} > 0. \end{cases}$$

Comme la fonction indicatrice $\mathbf{1}_=$ de la relation d'égalité est définie par

$$\mathbf{1}_=(\mathsf{n}_1, \mathsf{n}_2) = \mathbf{1}_{\{0\}}(\mathtt{diff}(\mathsf{n}_1, \mathsf{n}_2) + \mathtt{diff}(\mathsf{n}_2, \mathsf{n}_1)),$$

on en déduit qu'elle est primitive récursive comme composée de fonctions primitives récursives, le caractère primitif récursif de de la fonction $(\mathsf{n}_1, \mathsf{n}_2) \mapsto \mathtt{diff}(\mathsf{n}_2, \mathsf{n}_1)$ résultant de celui de `diff` et du point (i). De même, les fonctions indicatrices des relations $\leqslant$ et $<$ sont primitives récursives puisqu'on a

$$\mathbf{1}_{\leqslant}(\mathsf{n}_1, \mathsf{n}_2) = \mathbf{1}_{\{0\}}(\mathtt{diff}(\mathsf{n}_1, \mathsf{n}_2)),$$

et $\mathbf{1}_<(\mathsf{n}_1, \mathsf{n}_2) = \mathbf{1}_{\leqslant}(\mathsf{n}_1 + 1, \mathsf{n}_2)$.

Enfin, pour tous $\mathsf{m}_1, \ldots, \mathsf{m}_\mathsf{p}$, on a

$$\mathbf{1}_{\{\vec{\mathsf{m}}\}}(\vec{\mathsf{n}}) = \mathbf{1}_=(\mathsf{m}_1, \mathsf{n}_1) \cdot \ldots \cdot \mathbf{1}_=(\mathsf{m}_\mathsf{p}, \mathsf{n}_\mathsf{p}).$$

Pour $\mathsf{p} = 1$, on a $\mathbf{1}_{\{\mathsf{m}\}} = \mathtt{comp}(\mathbf{1}_=, \mathtt{proj}_{1,1}, \mathtt{const}_{1,\mathsf{m}})$, donc $\mathbf{1}_{\{\mathsf{m}\}}$ est primitive récursive. Ensuite, on utilise une récurrence sur p, et, comme la multiplication est primitive récursive, on conclut que $\mathbf{1}_{\{\vec{\mathsf{m}}\}}$ l'est aussi. □

▷ *L'argument utilisé pour montrer que la fonction décrémentation est primitive récursive est bien compliqué. De fait, on l'évite souvent en plaçant* `decr` *dans les fonctions de base ; noter aussi que, si la récursion est introduite de sorte que c'est $f(\vec{\mathsf{n}}, \mathsf{k}+1)$ qui est exprimé en fonction de $\vec{\mathsf{n}}$, k et $f(\vec{\mathsf{n}}, \mathsf{k})$ — et non comme ici $f(\vec{\mathsf{n}}, \mathsf{k})$ en fonction de $\vec{\mathsf{n}}$, k et $f(\vec{\mathsf{n}}, \mathsf{k}-1)$ — alors* `decr` *est définie par la récursion évidente $\mathtt{decr}(\mathsf{k}+1) := \mathsf{k}$ pour $\mathsf{k} > 0$. D'une façon générale, il existe de nombreuses variantes dans la définition des fonctions (primitives) récursives, le point important étant que ces variantes mènent toutes finalement à la même famille de fonctions, où on trouve toutes les fonctions arithmétiques de base.*

On notera bien que la propriété pour une fonction f d'être primitive récursive est une propriété globale, mettant en jeu la construction de f comme un tout : par conséquent, ce n'est jamais l'obtention d'une valeur $f(\mathsf{n})$ particulière qui indique quoi que ce soit quant au caractère (primitif) récursif de f. Pour rendre l'approche familière, il est recommandé de manipuler soi-même les opérations comp *et* rec*, et, notamment, d'expliciter totalement quelques-unes des définitions mentionnées dans la démonstration du 1.3, en vérifiant par exemple que*

$\mathtt{rec}(\mathtt{rec}(\mathtt{zero}, \mathtt{proj}_{2,2}), \mathtt{comp}(\mathtt{rec}(\mathtt{proj}_{1,1}, \mathtt{comp}(\mathtt{succ}, \mathtt{proj}_{3,3})), \mathtt{proj}_{3,3}, \mathtt{proj}_{3,1}))$,

est une définition primitive récursive de la multiplication. ◁

1.2. Propriétés de clôture.

► On montre que la famille des fonctions primitives récursives et celle des relations primitives récursives sont closes par des opérations simples, notamment la minimalisation bornée qui est une sorte de projection tronquée. ◄

Le résultat suivant montre qu'on peut définir des fonctions primitives récursives en amalgamant des fragments de fonctions primitives récursives, pourvu que la relation discriminante soit elle-même primitive récursive.

LEMME 1.4. *Supposons que f_1 et f_2 sont des fonctions primitives récursives et que R est une relation primitive récursive. Alors la fonction f définie par*

$$f(\vec{\mathsf{n}}) := \begin{cases} f_1(\vec{\mathsf{n}}) & \text{si } R(\vec{\mathsf{n}}) \text{ est vraie,} \\ f_2(\vec{\mathsf{n}}) & \text{sinon} \end{cases}$$

est primitive récursive.

DÉMONSTRATION. On a $f(\vec{\mathsf{n}}) = f_1(\vec{\mathsf{n}}) \cdot \mathbf{1}_R(\vec{\mathsf{n}}) + f_2(\vec{\mathsf{n}}) \cdot \mathbf{1}_{\{0\}}(\mathbf{1}_R(\vec{\mathsf{n}}))$, donc

$$f = \mathtt{comp}(\mathtt{add}, \mathtt{comp}(\mathtt{mult}, f_1, \mathbf{1}_R), \mathtt{comp}(\mathtt{mult}, f_2, \mathtt{comp}(\mathbf{1}_{\{0\}}, \mathbf{1}_R))),$$

et f est primitive récursive puisque add, mult, $\mathbf{1}_{\{0\}}$ le sont par le lemme 1.3 et f_1, f_2 et $\mathbf{1}_R$ par hypothèse. □

L'ensemble des fonctions primitives récursives est clos par sommations et produits finis :

LEMME 1.5. *Supposons que f est une fonction primitive récursive de $\mathbb{N}^{\mathsf{p}+1}$ dans $\mathbb{N}$. Alors il en est de même des fonctions f_1 et f_2 définies par*

$$f_1(\vec{\mathsf{n}}, \mathsf{k}) := \sum_{\mathsf{i} \leqslant \mathsf{k}} f(\vec{\mathsf{n}}, \mathsf{i}) \qquad \text{et} \qquad f_2(\vec{\mathsf{n}}, \mathsf{k}) := \prod_{\mathsf{i} \leqslant \mathsf{k}} f(\vec{\mathsf{n}}, \mathsf{i}).$$

DÉMONSTRATION. Les fonctions f_1 et f_2 sont définies par les récursions

$$f_1(\vec{\mathsf{n}}, \mathsf{k}) := \begin{cases} f(\vec{\mathsf{n}}, 0) \\ f_1(\vec{\mathsf{n}}, \mathsf{k}-1) + f(\vec{\mathsf{n}}, \mathsf{k}) \end{cases} \qquad f_2(\vec{\mathsf{n}}, \mathsf{k}) := \begin{cases} f(\vec{\mathsf{n}}, 0) & \text{pour } \mathsf{k} = 0, \\ f_2(\vec{\mathsf{n}}, \mathsf{k}-1) \cdot f(\vec{\mathsf{n}}, \mathsf{k}) & \text{pour } \mathsf{k} > 0, \end{cases}$$

donc sont primitives récursives. □

PROPOSITION 1.6. (clôture) *Pour chaque entier* p*, la famille des sous-ensembles primitifs récursifs de $\mathbb{N}^{\mathsf{p}}$ est close par union, intersection, complémentaire, et elle contient tous les sous-ensembles finis et co-finis de $\mathbb{N}^{\mathsf{p}}$.*

DÉMONSTRATION. Soient R_1, R_2 des sous-ensembles primitifs récursifs de $\mathbb{N}^{\mathsf{p}}$. Alors $R_1 \cap R_2$ est primitif récursif, puisqu'on a $\mathbf{1}_{R_1\cap R_2}(\vec{\mathsf{n}}) = \mathbf{1}_{R_1}(\vec{\mathsf{n}})\cdot\mathbf{1}_{R_2}(\vec{\mathsf{n}})$, soit $\mathbf{1}_{R_1\cap R_2} = \mathtt{comp}(\mathtt{mult}, \mathbf{1}_{R_1}, \mathbf{1}_{R_2})$. Ensuite, $\mathbb{N}^{\mathsf{p}} \setminus R_1$ est primitif récursif, puisqu'on a $\mathbf{1}_{\mathbb{N}^{\mathsf{p}}\setminus R_1}(\vec{\mathsf{n}}) = \mathbf{1}_{\{0\}}(\mathbf{1}_{R_1}(\vec{\mathsf{n}}))$, soit $\mathbf{1}_{\mathbb{N}^{\mathsf{p}}\setminus R_1} = \mathtt{comp}(\mathbf{1}_{\{0\}}, \mathbf{1}_{R_1})$. On en déduit que $R_1 \cup R_2$ est primitif récursif puisque c'est le complémentaire de l'intersection des complémentaires de R_1 et R_2.

D'après le lemme 1.3 tous les singletons sont primitifs récursifs. Par union finie de tels singletons, on obtient tous les sous-ensembles finis de $\mathbb{N}^{\mathsf{p}}$, et, par complémentation, tous les sous-ensembles co-finis. □

▷ *On verra plus loin que, si R est une relation primitive récursive sur $\mathbb{N}^{\mathsf{p}+1}$, il est faux en général que la projection de R sur $\mathbb{N}^{\mathsf{p}}$, c'est-à-dire la relation $\exists\mathsf{i}(R(\vec{\mathsf{n}},\mathsf{i}))$, soit primitive récursive. Par contre, on a un résultat de clôture lorsqu'on considère une quantification bornée, c'est-à-dire lorsqu'on remplace $\exists\mathsf{i}$ par $\exists\mathsf{i}\leqslant\mathsf{k}$.* ◁

LEMME 1.7. *Soit R une relation primitive récursive sur $\mathbb{N}^{\mathsf{p}+1}$. Alors les relations $R_\exists$ et $R_\forall$ sur $\mathbb{N}^{\mathsf{p}}$ définies par*

$$(\vec{\mathsf{n}},\mathsf{k}) \in R_\exists \Leftrightarrow \exists\mathsf{i}\leqslant\mathsf{k}(R(\vec{\mathsf{n}},\mathsf{i})), \quad (\vec{\mathsf{n}},\mathsf{k}) \in R_\forall \Leftrightarrow \forall\mathsf{i}\leqslant\mathsf{k}(R(\vec{\mathsf{n}},\mathsf{i})) \tag{1.1}$$

sont primitives récursives.

DÉMONSTRATION. Par définition, on a

$$\mathbf{1}_{R_\exists}(\vec{\mathsf{n}},\mathsf{k}) = \mathbf{1}_{\geqslant 1}(\sum_{\mathsf{i}\leqslant\mathsf{k}} \mathbf{1}_R(\vec{\mathsf{n}},\mathsf{i})) \quad \text{et} \quad \mathbf{1}_{R_\forall}(\vec{\mathsf{n}},\mathsf{k}) = \prod_{\mathsf{i}\leqslant\mathsf{k}} \mathbf{1}_R(\vec{\mathsf{n}},\mathsf{i}),$$

donc, par le lemme 1.5, $R_\exists$ et $R_\forall$ sont primitives récursives. □

PROPOSITION 1.8. (quantification bornée) *Soient R une relation primitive récursive sur $\mathbb{N}^{\mathsf{p}+1}$ et h une fonction primitive récursive sur $\mathbb{N}^{\mathsf{p}}$. Alors les relations R_1 et R_2 sur $\mathbb{N}^{\mathsf{p}}$ définies par*

$$R_1(\vec{\mathsf{n}}) \Leftrightarrow \exists\mathsf{i}\leqslant h(\vec{\mathsf{n}})\,(R(\vec{\mathsf{n}},\mathsf{i})) \quad \textit{et} \quad R_2(\vec{\mathsf{n}}) \Leftrightarrow \forall\mathsf{i}\leqslant h(\vec{\mathsf{n}})\,(R(\vec{\mathsf{n}},\mathsf{i}))$$

sont primitives récursives.

DÉMONSTRATION. Avec les notations de (1.1), on a

$$\mathbf{1}_{R_1} = \mathtt{comp}(\mathbf{1}_{R_\exists}, \mathtt{proj}_{\mathsf{p},1}, \ldots, \mathtt{proj}_{\mathsf{p},\mathsf{p}}, \mathtt{comp}(h, \mathtt{proj}_{\mathsf{p},1}, \ldots, \mathtt{proj}_{\mathsf{p},\mathsf{p}})),$$

et, de même pour R_2 avec $R_\forall$. □

La contre-partie en termes de fonctions s'exprime à l'aide de l'opérateur de minimalisation.

DÉFINITION 1.9. (minimalisation bornée) Pour h fonction de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ et R relation sur $\mathbb{N}^{\mathsf{p}+1}$, on pose

$$\mu\mathsf{m}{<}h(\vec{\mathsf{n}})\,(R(\vec{\mathsf{n}},\mathsf{m})) := \begin{cases} \text{le plus petit } \mathsf{m} < h(\vec{\mathsf{n}}) \text{ vérifiant } R(\vec{\mathsf{n}},\mathsf{m}) \text{ s'il existe,} \\ h(\vec{\mathsf{n}}) \text{ sinon ;} \end{cases}$$

la fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ définie par $f(\vec{\mathsf{n}}) := \mu\mathsf{m}{<}h(\vec{\mathsf{n}})\,(R(\vec{\mathsf{n}},\mathsf{m}))$ est dite définie par *minimalisation bornée* à partir de h et R, et notée $\mathtt{min}_<(h,R)$.

EXEMPLE 1.10. (minimalisation bornée) Un cas typique est celui où, partant de g définie sur $\mathbb{N}^{\mathsf{p}+1}$ et de h définie sur $\mathbb{N}^{\mathsf{p}}$, on définit f par

$$f(\vec{\mathsf{n}}) := \mu\mathsf{m}{<}h(\vec{\mathsf{n}})\,(g(\vec{\mathsf{n}},\mathsf{m}) = 0)$$

qui associe à $(\vec{\mathsf{n}})$ le plus petit m tel que $g(\vec{\mathsf{n}},\mathsf{m})$ s'annule s'il en existe un inférieur à $h(\vec{\mathsf{n}})$, et $h(\vec{\mathsf{n}})$ à défaut. Remarquer que, si g est une fonction primitive récursive, il en est de même de la relation $g(\vec{\mathsf{n}},\mathsf{m}) = 0$.

PROPOSITION 1.11. (minimalisation bornée) *Si h et R sont primitives récursives, il en est de même de la fonction $\mathtt{min}_<(h,R)$.*

DÉMONSTRATION. Soit f la fonction $\mathtt{min}_<(h,R)$. Dire que m est le premier entier pour lequel $R(\vec{\mathsf{n}},\mathsf{m})$ est vrai signifie qu'il existe exactement m entiers i avec la propriété que R est faux pour tous les $\mathsf{j} \leqslant \mathsf{i}$. Par ailleurs, $h(\vec{\mathsf{n}})$ est le nombre d'entiers inférieurs à $h(\vec{\mathsf{n}})$ (!). On a donc dans tous les cas $f(\vec{\mathsf{n}}) = \sum_{\mathsf{i}\leqslant h(\vec{\mathsf{n}})} g(\vec{\mathsf{n}},\mathsf{i})$, où g est définie par

$$g(\vec{\mathsf{n}},\mathsf{i}) = \begin{cases} 1 & \text{si } \forall \mathsf{j}{\leqslant}\mathsf{i}(\neg R(\vec{\mathsf{n}},\mathsf{j})), \\ 0 & \text{si } \exists \mathsf{j}{\leqslant}\mathsf{i}(R(\vec{\mathsf{n}},\mathsf{j})). \end{cases}$$

En vertu du lemme 1.7, la relation « $\exists \mathsf{j}{\leqslant}\mathsf{i}(R(\vec{\mathsf{n}},\mathsf{j}))$ » est primitive récursive, et il en est de même de g qui est définie par cas à partir de fonctions et relations primitives récursives (lemme 1.4). Enfin f est obtenue par sommation à partir de g et h, donc elle est primitive récursive par le lemme 1.5. □

▷ *On notera que l'introduction de la borne h est essentielle dans le résultat précédent, d'abord pour garantir que la fonction f est partout définie, puis pour montrer qu'elle est primitive récursive. De fait, on verra plus loin que le résultat est en défaut si la borne est omise.* ◁

1.3. Représentation des suites finies.

► On montre l'existence de codages des suites finies d'entiers par des entiers suffisamment uniformes pour que toutes les opéartions associées soient primitives récursives. ◄

▷ *L'ensemble des suites finies d'entiers est un ensemble dénombrable, ce qui signifie qu'on peut numéroter toutes les suites finies d'entiers naturels. Il existe plusieurs façons de le faire ; pour les besoins de ce chapitre, on utilisera deux numérotations distinctes. Ces numérotations sont non bijectives, au sens où toute suite d'entiers reçoit un numéro, mais il existe des numéros ne correspondant à aucune suite.*

La première numérotation utilise la fonction traditionnellement appelée fonction β de Gödel: elle est très simple, mais elle n'est pas univoque, au sens où une même suite peut recevoir plusieurs numéros distincts. Le but cherché est simplement de pouvoir remplacer une quantification du type « il existe une suite finie d'entiers telle que... » par une quantification « il existe un entier tel que... », ce qui est le point essentiel dans la démonstration de la proposition 3.13 dans la section 3. ◁

LEMME 1.12. *Il existe une fonction primitive récursive* $\mathtt{beta}$ *de* $\mathbb{N}^3$ *dans* $\mathbb{N}$ *telle que, pour toute suite finie d'entiers naturels* $(\mathsf{n}_0,\dots,\mathsf{n}_\mathsf{k})$*, il existe (au moins) deux entiers* s,t *vérifiant* $\mathtt{beta}(\mathsf{s},\mathsf{t},\mathsf{i}) = \mathsf{n}_\mathsf{i}$ *pour* $0 \leqslant \mathsf{i} \leqslant \mathsf{k}$.

DÉMONSTRATION. Soient $\mathtt{quot}(\mathsf{n},\mathsf{k})$ et $\mathtt{reste}(\mathsf{n},\mathsf{k})$ le quotient et le reste de la division euclidienne de n par k pour $\mathsf{k}\neq 0$. On complète par $\mathtt{quot}(\mathsf{n},0):=0$ et $\mathtt{reste}(\mathsf{n},0):=\mathsf{n}$. Alors $\mathtt{quot}$ est définie par la minimalisation bornée

$$\mathtt{quot}(\mathsf{n},\mathsf{k})=\mu\mathsf{q}\leqslant\mathsf{n}\,((\mathsf{k}=0\wedge\mathsf{q}=0)\vee((\mathsf{k}>0\wedge\mathsf{k}\cdot\mathsf{q}\leqslant\mathsf{n}<\mathsf{k}\cdot(\mathsf{q}+1))). \tag{1.2}$$

La relation dans (1.2) est une combinaison booléenne de conditions mettant en jeu la multiplication et l'ordre, donc elle est primitive récursive, et la fonction $\mathtt{quot}$ est primitive récursive par la proposition 1.11. Alors, la fonction $\mathtt{reste}$ est définie par $\mathtt{reste}(\mathsf{n},\mathsf{k})=\mathtt{diff}(\mathsf{n},\mathsf{k}\cdot\mathtt{quot}(\mathsf{n},\mathsf{k}))$, donc elle est primitive récursive puisque les fonction $\mathtt{diff}$, $\mathtt{mult}$, et $\mathtt{quot}$ le sont.

Soit alors $\mathtt{beta}$ la fonction de $\mathbb{N}^3$ dans $\mathbb{N}$ définie par

$$\mathtt{beta}(\mathsf{s},\mathsf{t},\mathsf{i}):=\mathtt{reste}(\mathsf{s},(\mathsf{i}+1)\mathsf{t}+1).$$

Que $\mathtt{beta}$ soit primitive récursive résulte de ce que l'addition, la multiplication, et la fonction $\mathtt{reste}$ le sont.

Soit $(\mathsf{n}_0,\ldots,\mathsf{n}_\mathsf{k})$ une suite finie d'entiers. Posons $\mathsf{m}=\max(\mathsf{n}_0,\ldots,\mathsf{n}_\mathsf{k},\mathsf{k})$ et $\mathsf{t}=\mathsf{m}!$. Supposons qu'un entier r divise à la fois $(\mathsf{i}+1)\mathsf{t}+1$ et $(\mathsf{j}+1)\mathsf{t}+1$ avec $0\leqslant\mathsf{i}<\mathsf{j}\leqslant\mathsf{k}$. Alors r divise $(\mathsf{i}-\mathsf{j})\mathsf{t}$. Or t et $(\mathsf{i}+1)\mathsf{t}+1$ sont premiers entre eux, donc r doit diviser $\mathsf{i}-\mathsf{j}$. Mais alors on a $\mathsf{r}\leqslant\mathsf{k}$, donc $\mathsf{r}\leqslant\mathsf{m}$, et, par construction, r divise t. Comme r divise $(\mathsf{i}+1)\mathsf{t}+1$ par hypothèse, r ne peut être que 1. Autrement dit les nombres $\mathsf{t}+1$, $2\mathsf{t}+1$, … ,$(\mathsf{k}+1)\mathsf{t}+1$ sont deux à deux premiers entre eux. Par le lemme des restes chinois, il existe donc un entier s tel que le reste de la division de s par $(\mathsf{i}+1)\mathsf{t}+1$ soit n_i, c'est-à-dire un entier s satisfaisant $\mathtt{beta}(\mathsf{s},\mathsf{t},\mathsf{i})=\mathsf{n}_\mathsf{i}$ pour $0\leqslant\mathsf{i}\leqslant\mathsf{k}$. □

▷ *Le codage de Gödel n'est pas très naturel, et il n'est pas immédiat de déterminer les couples d'entiers codant une suite donnée. D'un autre côté, sa définition ne requiert que des opérations arithmétiques très simples, ce qui sera un élément important pour son application ultérieure dans la section 3.3. À titre d'exemple, considérons le cas de la suite* $(2,1)$. *On a ici* $\mathsf{m}=\mathsf{t}=2$, *et les couples d'entiers* (s,t) *vérifiant* $\mathtt{beta}(\mathsf{s},\mathsf{t},0)=2$ *et* $\mathtt{beta}(\mathsf{s},\mathsf{t},1)=1$, *c'est-à-dire codant, au sens de la fonction* $\mathtt{beta}$, *la suite* $(2,1)$ *sont tous les couples* $(\mathsf{s},2)$ *avec* $\mathsf{s}\equiv 2 \pmod 3$ *et* $\mathsf{s}\equiv 1 \pmod 5$, *c'est-à-dire les couples* $(11+15\mathsf{r},2)$ *avec* $\mathsf{r}\geqslant 0$.

On utilisera également une seconde numérotation des suites finies d'entiers, dans laquelle chaque suite ne correspond qu'à un seul entier, et qui repose sur l'existence d'une unique décomposition de tout entier en produit de facteurs premiers. Le principe est ici de représenter la suite $(\mathsf{n}_0,\ldots,\mathsf{n}_\mathsf{k})$ *par l'entier* $\mathsf{p}_0^{\mathsf{n}_0+1}\ldots\mathsf{p}_\mathsf{k}^{\mathsf{n}_\mathsf{k}+1}$, *où* p_i *est le* i*ème nombre premier. Par exemple, l'unique numéro associé à la suite* $(2,1)$ *via ce second codage est* $2^3\cdot 3^2$, *c'est-à-dire* 72. *Le codage ainsi défini est injectif (un seul entier par suite), mais non surjectif (tous les entiers ne sont pas des numéros de suite) : seuls les entiers dont les facteurs premiers forment un segment initial de la suite des nombres premiers codent une suite.* ◁

DÉFINITION 1.13. (codage des suites) On définit le *code* $\langle\mathsf{n}_0,\ldots,\mathsf{n}_\mathsf{k}\rangle$ de la suite $(\mathsf{n}_0,\ldots,\mathsf{n}_\mathsf{k})$ comme l'entier $\mathsf{p}_0^{\mathsf{n}_0+1}\ldots\mathsf{p}_\mathsf{k}^{\mathsf{n}_\mathsf{k}+1}$; on pose $\langle\rangle:=1$. On note $\mathtt{Suite}$ l'ensemble des codes de suite. Si n est un code, on note $\mathtt{lg}(\mathsf{n})$ la longueur de la suite de code n, et, pour $\mathsf{i}\leqslant\mathtt{lg}(\mathsf{n})$, on note $\mathtt{coord}(\mathsf{n},\mathsf{i})$ le i-ème facteur de la suite de code n. Si n,m sont des codes, on note $\mathtt{concat}(\mathsf{n},\mathsf{m})$ le code de la concaténation des suites de codes n et m. On prolonge $\mathtt{lg}$, $\mathtt{coord}$ et $\mathtt{concat}$ par 0 là où les clauses précédentes n'attribuent pas de valeur.

Le point important pour la suite est que chacune des relations et fonctions définies ci-dessus est primitive récursive.

PROPOSITION 1.14. (codage des suites) *L'ensemble* `Suite` *et les fonctions* `lg`, `coord`, *et* `concat` *sont primitifs récursifs.*

DÉMONSTRATION. La relation « k divise n », notée $\mathsf{k} \mid \mathsf{n}$, est primitive récursive puisque définie par la quantification bornée $\exists \mathsf{q} \leqslant \mathsf{n}\,(\mathsf{n} = \mathsf{k} \cdot \mathsf{q})$. La relation « p est premier » est primitive récursive puisqu'à son tour définie à partir d'une quantification bornée

$$\mathsf{p} \neq 0 \ \wedge\ \mathsf{p} \neq 1 \ \wedge\ \forall \mathsf{k} \leqslant \mathsf{p}\,(\mathsf{k} \mid \mathsf{p} \Rightarrow (\mathsf{k} = 1 \vee \mathsf{k} = \mathsf{p})).$$

Ensuite, la fonction « factorielle » est primitive récursive puisque définie par récurrence à partir de la multiplication. De là, la fonction `prem` associant à chaque entier k le k-ème nombre premier est primitive récursive puisque définie par récurrence et minimalisation bornée

$$\mathtt{prem}(\mathsf{k}) = \begin{cases} 2 & \text{pour } \mathsf{k} = 0, \\ \mu \mathsf{p} \leqslant \mathtt{prem}(\mathsf{k}-1)!+1\,(\text{« } \mathsf{p} \text{ est premier » et } \mathsf{p} > \mathtt{prem}(\mathsf{k}-1)) & \text{sinon,} \end{cases}$$

définition légitime puisque tous les facteurs premiers de $\mathtt{prem}(\mathsf{k}-1)!+1$ sont plus grands que $\mathtt{prem}(\mathsf{k}-1)$, et donc $\mathtt{prem}(\mathsf{k})$ est borné supérieurement par $\mathtt{prem}(\mathsf{k}-1)!+1$. Alors n code une suite, c'est-à-dire appartient à l'ensemble `Suite`, si et seulement si les diviseurs premiers de n forment un segment initial de la suite des nombres premiers, donc si et seulement si on a

$$\mathsf{n} = 1 \vee (\mathsf{n} > 1 \wedge \forall \mathsf{k} \leqslant \mathsf{n}\,(\mathtt{prem}(\mathsf{k}) \mid \mathsf{n} \Rightarrow \mathtt{prem}(\mathsf{k}-1) \mid \mathsf{n})),$$

et donc `Suite` est un ensemble primitif récursif. Alors $\mathtt{lg}(\mathsf{n})$ est l'indice du plus petit nombre premier ne divisant pas n, donc encore le nombre de facteurs premiers de n, donc la fonction longueur `lg` est à son tour définie par minimalisation bornée :

$$\mathtt{lg}(\mathsf{n}) = \begin{cases} 0 & \text{pour } \mathsf{n} \notin \mathtt{Suite} \text{ ou } \mathsf{n} = 1, \\ \mu \mathsf{k} \leqslant \mathsf{n}\,(\mathtt{prem}(\mathsf{k}+1) \not\mid \mathsf{n}) & \text{sinon.} \end{cases}$$

Ensuite, $\mathtt{coord}(\mathsf{n}, \mathsf{i})$ est le plus grand k tel que $\mathsf{p}_\mathsf{i}^{\mathsf{k}+1}$ divise n, donc la fonction coordonnée `coord` admet la définition par minimalisation bornée

$$\mathtt{coord}(\mathsf{n}, \mathsf{i}) = \mu \mathsf{k} \leqslant \mathsf{n}+1\,(\mathtt{exp}(\mathtt{prem}(\mathsf{i}), \mathsf{k}+2) \not\mid \mathsf{n}).$$

Enfin $\mathtt{concat}(\mathsf{n}_1, \mathsf{n}_2)$ s'obtient en multipliant n_1 par l'entier obtenu en translatant de $\mathtt{lg}(\mathsf{n}_1)$ les indices des facteurs premiers de n_2, donc la fonction concaténation `concat` est définie par

$$\mathtt{concat}(\mathsf{n}_1, \mathsf{n}_2) = \begin{cases} 0 & \text{pour } \mathsf{n}_1 \notin \mathtt{Suite} \text{ ou } \mathsf{n}_2 \notin \mathtt{Suite}, \\ \mathsf{n}_1 & \text{pour } \mathsf{n}_1 \in \mathtt{Suite} \text{ et } \mathsf{n}_2 = 1, \\ \mathsf{n}_1 \cdot \prod_{\mathsf{i} \leqslant \mathtt{lg}(\mathsf{n}_2)} \mathtt{exp}(\mathtt{prem}(\mathtt{lg}(\mathsf{n}_1) + \mathsf{i} + 1), \mathtt{coord}(\mathsf{n}_2, \mathsf{i}) + 1) & \text{sinon.} \end{cases}$$

Toutes les fonctions précédentes sont donc primitives récursives. □

▷ *De la même façon que l'existence d'un codage primitif récursif des couples permet de passer des définitions par récursion simple aux définitions par récursion simultanée (proposition* **??***), l'existence d'un codage primitif récursif des suites finies quelconques permet de passer aux définitions par récursion complète, où la valeur en* k *de la fonction dépend non seulement de la valeur en* $\mathsf{k}-1$ *mais, plus généralement, de l'ensemble des valeurs en* $0, 1, \ldots, \mathsf{k}-1$. ◁

PROPOSITION 1.15. (récursion complète) *Soient* g, h *des fonctions primitives récursives respectivement de* $\mathbb{N}^{\mathsf{p}}$ *et* $\mathbb{N}^{\mathsf{p}+2}$ *dans* $\mathbb{N}$. *Alors la fonction* f *définie par*

$$f(\vec{\mathsf{n}}, \mathsf{k}) := \begin{cases} g(\vec{\mathsf{n}}) & \textit{pour } \mathsf{k} = 0, \\ h(\vec{\mathsf{n}}, \mathsf{k}, \langle f(\vec{\mathsf{n}}, 0), \ldots, f(\vec{\mathsf{n}}, \mathsf{k}-1) \rangle) & \textit{pour } \mathsf{k} > 0 \end{cases}$$

est primitive récursive.

DÉMONSTRATION. Définissons f^* par $f^*(\vec{n},k) = \langle f(\vec{n},0),\dots,f(\vec{n},k)\rangle$. Alors f^* est primitive récursive, puisque définie par

$$f^*(\vec{n},k) = \begin{cases} \langle g(\vec{n})\rangle & \text{pour } k=0,\\ \mathtt{concat}(f^*(\vec{n},k-1), h(\vec{n},k,f^*(\vec{n},k-1)) & \text{pour } k>0,\end{cases}$$

et que, par construction, $\langle m\rangle$ est p_0^{m+1}, c'est-à-dire $\mathtt{exp}(2,m+1)$, une fonction primitive récursive de m. Or on a $f(\vec{n},k) = \mathtt{coord}(f^*(\vec{n},k),k)$, d'où $f = \mathtt{comp}(\mathtt{coord}, f^*, \mathtt{proj}_{p+1,p+1})$, et f est primitive récursive puisque f^* et $\mathtt{coord}$ le sont. □

1.4. Fonctions et relations récursives.

► Jusqu'à présent on n'a considéré que des fonctions et relations primitives récursives. On définit ici les fonctions et relations récursives générales en passant aux fonctions partielles et en ajoutant la minimalisation aux opérations de base. ◄

▷ *Les fonctions primitives récursives ont été définies comme la clôture de fonctions de base par rapport aux définitions par composition et par récursion. Les fonctions récursives générales sont définies à partir des mêmes fonctions de base, mais en autorisant une opération supplémentaire, à savoir la définition par minimalisation (non bornée) qui fait passer d'une fonction g à la fonction f définie par par $f(\vec{n}) := \mu m(g(\vec{n},m)=0)$, où $\mu m(...)$ signifie « le plus petit m tel que... ». Le changement de point de vue par rapport à la minimalisation bornée de la proposition 1.11 est important car, rien ne garantissant a priori l'existence d'un entier m tel que $f(\vec{n},m)$ soit nul, il se peut que $f(\vec{n})$ ne soit pas définie, et il faut donc quitter le cadre des fonctions totales pour passer à celui des fonctions partielles, dont le domaine est une partie éventuellement propre de $\mathbb{N}^p$ (une fonction totale est un cas particulier de fonction partielle).*

Dans toutes la suite, $f(\vec{n}) = m$ signifie « $f(\vec{n})$ est définie et vaut m », et, de même, $f(\vec{n}) \geqslant m$ signifie « $f(\vec{n})$ est définie et vaut m ou plus ». On étend à de telles fonctions partielles les opérations de composition et de récursion : si g, h_1, ... , h_q sont des fonctions partielles de $\mathbb{N}^q$ et $\mathbb{N}^p$ dans $\mathbb{N}$, on note $\mathtt{comp}(g,h_1,\dots,h_q)$ la fonction partielle f telle que $f(\vec{n}) = m$ est vraie si et seulement si il existe m_1, ... , m_q vérifiant $h_i(\vec{n}) = m_i$ pour $1 \leqslant i \leqslant q$, et $g(m_1,\dots,m_q) = m$. De même, on note $\mathtt{rec}(g,h)$ la fonction f telle que $f(\vec{n},k) = m$ est vraie si et seulement si il existe une suite finie d'entiers m_0, m_1, ... , $m_k = m$ vérifiant $g(\vec{n}) = m_0$ et $h(\vec{n},i,m_{i-1}) = m_i$ pour $i = 1,...,k$. Noter que, dans ce cas, si $f(\vec{n},k)$ n'est pas définie, il en est de même de $f(\vec{n},j)$ pour $j \geqslant k$. ◁

DÉFINITION 1.16. (minimalisation, récursif) Pour g fonction partielle de $\mathbb{N}^{p+1}$ dans $\mathbb{N}$, on note $\mathtt{min}(g)$ la fonction partielle f de $\mathbb{N}^p$ dans $\mathbb{N}$ définie par

$$(1.3)\quad \begin{cases} f(\vec{n}) := m \text{ si on a } g(\vec{n},k) > 0 \text{ pour } k = 0,1,...,m-1 \text{ et } g(\vec{n},m) = 0.\\ f(\vec{n}) \text{ non définie sinon,}\end{cases}$$

et on dit que f est obtenue par *minimalisation* à partir de g. Une fonction partielle f de $\mathbb{N}^p$ dans $\mathbb{N}$ est dite *récursive* si elle peut s'obtenir par un nombre fini de compositions, de récursions, et de minimalisations à partir des fonctions $\mathtt{zero}$, $\mathtt{succ}$ et $\mathtt{proj}_{p,i}$. Une relation sur $\mathbb{N}^p$ — ou un sous-ensemble de $\mathbb{N}^p$ — est dite *récursive* si sa fonction indicatrice est récursive.

EXEMPLE 1.17. (récursif) Il est clair que toute fonction primitive récursive est récursive, et que toute relation primitive récursive est récursive. Si R est un sous-ensemble récursif de $\mathbb{N}^p$, la fonction g de $\mathbb{N}^{p+1}$ dans $\mathbb{N}$ définie par $g(\vec{n},k) = \mathbf{1}_{\mathbb{N}^p\setminus R}(\vec{n})$

vaut 0 pour $\vec{\mathsf{n}}$ dans R, et 1 sinon, indépendamment de k, et elle est récursive puisque R l'est. Soit $f := \mathtt{min}(g)$. Par construction, $f(\vec{\mathsf{n}})$ est définie et vaut 0 pour $\vec{\mathsf{n}}$ dans R, et n'est pas définie pour $\vec{\mathsf{n}}$ hors de R : ainsi, pour tout ensemble récursif (donc en particulier tout ensemble primitif récursif) il existe une fonction récursive dont le domaine est exactement R. Si R est une partie propre de $\mathbb{N}^{\mathsf{p}}$, la fonction ainsi définie ne peut être primitive récursive puisqu'elle n'est pas partout définie [3].

▷ *Il existe toute une théorie de la récursivité dont les résultats précédents ne sont que les étapes préliminaires. En particulier, il existe plusieurs hiérarchies de complexité dont les ensembles récursifs constituent le premier niveau.*

Comme dernière remarque, on peut noter la similarité entre la notion de fonction (primitive) récursive et celle de formule prouvable d'une logique : dans les deux cas, la propriété est l'existence d'un témoin qui est une suite finie (un mot) obéissant à des règles syntaxiques, une définition par règles de formation à partir de fonctions de base dans le cas de la récursivité, une preuve par règles de déduction à partir d'axiomes dans le cas de la prouvabilité. ◁

1.5. Fonctions MT-calculables.

► On mentionne le lien entre la notion de fonction récursive et celle de fonction calculable par machine de Turing, au sens défini au chapitre VI. On en déduit un lemme technique sur la possibilité de définir toute fonction récursive avec au plus une minimalisation. ◄

▷ *Lorsqu'on invoque l'axiome du choix pour justifier l'existence d'une fonction de choix sur un ensemble, l'objet ainsi introduit n'est qu'incomplètement spécifié : en particulier, on n'obtient pas d'algorithme permettant, pour chaque élément non vide du domaine, de déterminer effectivement la valeur de la fonction. On qualifie généralement de non effectif un argument qui repose sur la considération de tels objets incomplètement spécifiés. A l'opposé, on considère ici les fonctions pour lesquelles un tel algorithme de calcul existe.* ◁

« Définition » 1.18. (calculable, décidable) Une fonction f est dite *calculable* s'il existe un algorithme uniforme [4] déterminant la valeur de $f(x)$ pour chaque x dans le domaine de f. De même, une relation R est dite *décidable* s'il existe un algorithme uniforme déterminant si $R(x)$ est vraie pour chaque x dans le domaine de R.

▷ *La définition précédente ne devient formelle que lorsqu'on précise le type d'algorithme considéré, c'est-à-dire lorqu'on fixe un modèle de calcul. On a brièvement évoqué l'un d'entre eux au chapitre VI, à savoir les machines de Turing. La notion informelle de fonction calculable peut donc être approchée par la notion, formelle, de fonction calculable par machine de Turing.* ◁

Pour n entier naturel, on note $[\mathsf{n}]$ le nombre (suite de chiffres 0 à 9) représentant n en base dix. Le caractère □ désigne un blanc séparateur.

[3] Cet exemple laisse ouverte la question de l'existence d'une fonction récursive partout définie mais non primitive récursive : on verra plus loin que de telles fonctions existent.

[4] on insiste sur le fait que l'algorithme doit être le même pour chaque valeur de l'argument

Définition 1.19. (MT-calculable, MT-décidable) Une fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ est dite *calculable par machine de Turing*, ou *MT-calculable*, s'il existe une machine de Turing déterministe M d'alphabet $\{0, 1, \ldots, 9\}$ calculant f au sens suivant : quels que soient les entiers n_1, ... , n_{p}, le calcul de M à partir de la configuration initiale associée au mot $[\mathsf{n}_1]\square[\mathsf{n}_2]\square\ldots\square[\mathsf{n}_{\mathsf{p}}]$ se termine avec la configuration finale associée au mot $[f(\vec{\mathsf{n}})]$ si $f(\vec{\mathsf{n}})$ est défini, et ne se termine pas si $f(\vec{\mathsf{n}})$ n'est pas défini.

De même, une relation R sur $\mathbb{N}^{\mathsf{p}}$ est dite *décidable par machine de Turing*, ou *MT-décidable*, s'il existe une machine de Turing déterministe M d'alphabet $\{0, 1, \ldots, 9\}$ décidant R au sens suivant : quels que soient n_1, ... , n_{p}, le calcul de M à partir de la configuration initiale associée au mot $[\mathsf{n}_1]\square[\mathsf{n}_2]\square\ldots\square[\mathsf{n}_{\mathsf{p}}]$ se termine dans un état acceptant si $R(\vec{\mathsf{n}})$ est vraie, et dans un état refusant si $R(\vec{\mathsf{n}})$ est fausse.

▷ *Autrement dit, une fonction f est MT-calculable s'il existe un algorithme calculant f et implantable sur machine de Turing. La définition explicite des machines de Turing rend clair que les calculs de machine de Turing correspondent à l'exécution d'un algorithme, et, par conséquent, toute fonction MT-calculable doit être considérée comme calculable. La thèse de Church–Turing, notée ici* TC*, est l'opinion affirmant que, réciproquement, tout algorithme est implantable sur machine de Turing, et donc en particulier toute fonction calculable est MT-calculable. A ce jour, aucun modèle de calcul ne contredit la thèse de Church–Turing, ce qui justifie les approximations « calculable ⇔ MT-calculable » et « décidable ⇔ MT-décidable ».*

Noter que l'acceptation ou le rejet de la thèse de Church–Turing ne met pas en cause la correction des résultats ultérieurs ; par contre, si la thèse de Church–Turing venait à être rejetée, la portée des résultats serait limitée, puisqu'ils réfèrent à un modèle qui serait jugé non pertinent.

Pour ce qui nous concerne ici, le point essentiel est que la MT-calculabilité est exactement équivalente à la propriété d'être récursive. On peut également voir cette équivalence comme celle des langages de programmation impératifs — dont les machines de Turing constituent une formalisation — et des langages de programmation fonctionnels — dont les fonctions récursives constituent une formalisation. ◁

Proposition 1.20. (équivalence) *Une fonction de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ est récursive si et seulement si elle est calculable par machine de Turing ; une relation sur $\mathbb{N}^{\mathsf{p}}$ est récursive si et seulement si elle est décidable par machine de Turing.*

Principe de la démonstration. Dans une direction, il suffit de vérifier que les fonctions de base $\mathtt{zero}$, $\mathtt{succ}$, $\mathtt{proj}_{\mathsf{p},\mathsf{i}}$ sont MT-calculables, puis que la famille des fonctions MT-calculables est close par composition, récursion, et minimalisation, ce qui est facile une fois les machines de Turing précisément définies.

Dans l'autre direction, *a priori* plus difficile, il s'agit de coder les configurations de machines de Turing par des entiers. Soit g_M la fonction associant à chaque choix de valeurs initiales $\vec{\mathsf{n}}$ et chaque entier t, le code de la configuration obtenue après t étapes de calcul de M à partir des données $\vec{\mathsf{n}}$. Par définition d'une machine de Turing, la configuration à l'instant t s'obtient de façon simple à partir de la configuration à l'instant $\mathsf{t}-1$ et de la machine M, qui est un objet fini. De là, si le codage des configurations est fait de façon raisonnable, on peut s'attendre à ce que la fonction g_M soit définie par une récursion sur t et, de ce fait, soit primitive récursive, puis que f puisse être extraite de g_M à l'aide d'une unique minimalisation correspondant à la recherche du plus petit t pour lequel la t-ième étape du calcul est une configuration finale de M. On conclut alors que f est récursive. □

Comme la thèse de Church–Turing TC est l'affirmation que toute fonction calculable est calculable par machine de Turing, et que toute relation décidable est décidable par machine de Turing, on obtient :

COROLLAIRE 1.21. (TC) *Une fonction de $\mathbb{N}^p$ dans $\mathbb{N}$ est récursive si et seulement si elle est calculable ; une relation sur $\mathbb{N}^p$ est récursive si et seulement si elle est décidable.*

De la démonstration de la proposition 1.20 on tire le corollaire[5] suivant :

COROLLAIRE 1.22. *Toute fonction récursive peut s'obtenir par une unique minimalisation à partir d'une fonction primitive récursive.*

DÉMONSTRATION. Si f est récursive, elle est MT-calculable ; or, si M est une machine de Turing calculant f, on a vu dans la démonstration de la proposition 1.20 qu'il existe une fonction primitive récursive g_M codant les calculs de M à partir de laquelle la fonction calculée par M, à savoir ici f, s'obtient par une unique minimalisation. □

▷ *La différence principale entre le point de vue de la calculabilité et celui de la récursivité est que le premier est local en ce qu'il met en jeu la valeur de la fonction pour chaque choix de valeurs pour les arguments, alors que le second est global en ce qu'il considère la fonction comme un tout, indépendamment de son évaluation en quelque valeur que ce soit. Les deux approches ne sont néanmoins pas si opposées — puisqu'en fait elles mènent exactement aux mêmes fonctions : l'approche « fonction calculable » n'est pas si locale qu'il paraît puisque le point important est l'uniformité du programme calculant les valeurs, une propriété globale. On notera que l'approche « fonction récursive » est spécialement éloignée de l'approche ensembliste identifiant une fonction à son graphe vu comme un ensemble de couples.* ◁

2. Arithmétisation de la syntaxe

► On montre qu'on peut numéroter les formules d'une logique du premier ordre de façon suffisamment régulière pour que tous les ensembles et fonctions mis en jeu soient primitifs récursifs. ◄

▷ *Tous les composants syntaxiques d'une logique du premier ordre $\mathcal{L}_\Sigma$, termes, formules, preuves, ont été définis comme des mots sur un alphabet ad hoc composé de divers symboles logiques et des symboles de la signature Σ. Dans le cas d'une signature finie ou dénombrable, les ensembles de mots concernés sont dénombrables, et il est facile d'en fixer une numérotation par des entiers, obtenant ce qu'on appelle une arithmétisation de la syntaxe de $\mathcal{L}_\Sigma$. Le seul point requérant un peu de soin est que, pour la suite, on aura besoin que les numéros des formules forment un ensemble récursif et, surtout, que la fonction qui, aux numéros d'une formule F et d'un terme t et à un indice i associe celui de la formule $\mathsf{F}(\boldsymbol{x}_\mathsf{i} \leftarrow \mathsf{t})$ soit récursive. Comme dans la section précédente, il s'agit de vérifications fastidieuses mais dépourvues de difficulté.* ◁

[5] ... qu'on devrait appeler porisme : un corollaire est une application de l'énoncé d'une proposition antérieure ; un porisme est une application de la démonstration d'une proposition antérieure.

2.1. Numérotation de Gödel.

► Le principe est simple : les formules sont des suites finies de symboles, donc, une fois ceux-ci numérotés, on déduit une numérotation des formules de celle des suites finies d'entiers. ◄

Dans toute la suite, on considère des signatures au plus dénombrables, qu'on peut donc sans perte de généralité supposer incluses dans la signature $\Sigma_{\max}$ de la définition VII.1.13, c'est-à-dire la signature qui contient une suite infinie dénombrable de symboles de chacun des types possibles.

Au chapitre VII, on a, avec la définition VII.1.12, associé à chaque formule F de $\mathcal{L}_{\max}$ un ensemble $\underline{\mathsf{F}}$ appartenant à V_ω, qui, par construction, s'obtient à partir des entiers à l'aide de l'unique opération de formation de suite finie. Or, on vient, avec la fonction $\langle\rangle$, de définir une numérotation des suites finies d'entiers. Il est alors immédiat d'obtenir une numérotation des formules de $\mathcal{L}_{\max}$.

Définition 2.1. (numérotation) Pour chaque symbole, terme, formule, preuve x de $\mathcal{L}_{\max}$, on note $\ulcorner x \urcorner$ l'entier obtenu en évaluant à l'aide de la fonction $\langle\rangle$ l'ensemble $\underline{x}$.

Exemple 2.2. (numérotation) Suivant la définition VII.1.12, la représentation ensembliste $\underline{\boldsymbol{x}_2}$ de la variable $\boldsymbol{x}_2$ est la suite $(0, 2)$. Son numéro $\ulcorner \boldsymbol{x}_2 \urcorner$ est donc l'entier $\langle 0, 2\rangle$, c'est-à-dire $2^{1+0}{\cdot}3^{1+2}$, soit 54. De même, la représentation ensembliste du symbole $\mathbf{0}$ est la suite $(1, 0, 1)$, donc son numéro est l'entier $\langle 1, 0, 1\rangle$, qui est $2^{1+1}{\cdot}3^{1+0}{\cdot}5^{1+2}$, soit 300, tandis que la représentation ensembliste du symbole $=$ est $(2, 2, 0)$, donc son numéro $\ulcorner = \urcorner$ est $\langle 2, 2, 0\rangle$, qui est $2^{1+2}{\cdot}3^{1+2}{\cdot}5^{1+1}$, soit 1080. Enfin, la représentation ensembliste $\underline{\boldsymbol{x}_2 = \mathbf{0}}$ de la formule $\boldsymbol{x}_2 = \mathbf{0}$ est la suite $(\underline{=}, \underline{\boldsymbol{x}_2}, \underline{\mathbf{0}})$, soit $((2, 2, 0), (0, 2), (1, 0, 1))$, donc son numéro $\ulcorner \boldsymbol{x}_2 = \mathbf{0} \urcorner$ est $\langle\langle 2, 2, 0\rangle, \langle 0, 2\rangle, \langle 1, 0, 1\rangle\rangle$, qui est $\langle 1080, 54, 300\rangle$, soit le (grand) entier $2^{1081}{\cdot}3^{55}{\cdot}5^{301}$.

▷ *L'exemple précédent souligne le caractère contingent de la représentation : le choix des numéros des symboles de base est essentiellement arbitraire, de même que celui de l'ordre de description des objets. Le point important est que le codage ainsi obtenu soit non-ambigu, et suffisamment simple au sens où, partant d'un entier, on peut effectivement retrouver le terme ou la formule dont il est le code. Dans le contexte présent, la notion de simplicité correspond à celle d'ensemble (primitif) récursif, et le premier résultat indispensable est le suivant.* ◁

Lemme 2.3. *L'ensemble* `Var` *des numéros des variables de* $\mathcal{L}_{\max}$ *est un ensemble primitif récursif. Il en est de même de l'ensemble* `Term` *des numéros des termes, et de l'ensemble* `Form` *des numéros des formules.*

Démonstration. Par construction, on a $\mathsf{n}_\mathsf{i} < \mathsf{n}$ si n est le code de la suite $(\mathsf{n}_0, \ldots, \mathsf{n}_\mathsf{k})$. Il en résulte qu'on peut inverser les définitions en utilisant des quantifications bornées et déduire par la proposition 1.8 qu'on ne sort pas du cadre primitif récursif. Ainsi, on peut caractériser l'ensemble `Var` des numéros de variables en définissant `Var`(n) comme étant

$$\exists \mathsf{i} < \mathsf{n}\,(\mathsf{i} \geqslant 1 \wedge \mathsf{n} = \langle 0, \mathsf{i}\rangle),$$

et l'ensemble `Var` est donc primitif récursif. Le même argument montre que l'ensemble `Const` des numéros des symboles de constantes de $\mathcal{L}_{\max}$, c'est-à-dire les entiers de la forme $\langle 1, 0, \mathsf{i}\rangle$ avec $\mathsf{i} \geqslant 1$, est primitif récursif.

Pour les termes, comme le numéro de $\boldsymbol{s}(\mathsf{t}_1,\dots,\mathsf{t}_k)$ est plus grand que celui de $\boldsymbol{s}$ et de chaque t_i, on peut à nouveau utiliser des quantifications bornées. Mais, comme la définition est récursive et non directe, il faut en outre utiliser une récursion, et même une récursion complète, puisque le numéro de $\boldsymbol{s}(\mathsf{t}_1,\dots,\mathsf{t}_k)$ s'obtient à partir des numéros de $\boldsymbol{s}$ et des t_i, dont on sait seulement qu'ils sont des prédécesseurs du numéro à définir, mais pas le prédecesseur immédiat en général. On peut caractériser l'ensemble $\mathtt{Term}$ des numéros de termes en définissant $\mathtt{Term}(\mathsf{n})$ comme étant

$$\begin{aligned}&\mathtt{Var}(\mathsf{n})\vee\mathtt{Const}(\mathsf{n})\\&\quad\vee(\mathtt{Suite}(\mathsf{n})\wedge\exists\mathsf{k},\mathsf{i}{<}\mathsf{n}\,(\mathtt{lg}(\mathsf{n})=\mathsf{k}+1\wedge\mathtt{coord}(\mathsf{n},0)=\langle1,\mathsf{k},\mathsf{i}\rangle\\&\qquad\qquad\wedge\forall\mathsf{j}{\leqslant}\mathsf{k}\,(\mathsf{j}\geqslant1{\Rightarrow}\mathtt{Term}(\mathtt{coord}(\mathsf{n},\mathsf{j}))))),\end{aligned}$$

une définition par récursion complète, où la valeur (0 ou 1) de $\mathtt{Term}(\mathsf{n})$ est définie à partir de la suite des valeurs $\mathtt{Term}(\mathsf{k})$ pour $0\leqslant\mathsf{k}<\mathsf{n}$: avec les notations de la proposition 1.15, on a

$$\mathbf{1}_{\mathtt{Term}}(\mathsf{n})=\begin{cases}0&\text{pour }\mathsf{n}=0,\\ f(\mathsf{n},\langle\mathbf{1}_{\mathtt{Term}}(0),\dots,\mathbf{1}_{\mathtt{Term}}(\mathsf{n}-1)\rangle)&\text{pour }\mathsf{n}>0,\end{cases}$$

où f est définie par

$$\begin{aligned}&f(\mathsf{n},\mathsf{m})=\mathbf{1}_{\mathtt{Var}}(\mathsf{n})+\mathbf{1}_{\mathtt{Const}}(\mathsf{n})+\mathbf{1}_{\mathtt{Suite}}(\mathsf{n})\cdot\textstyle\sum_{\mathsf{k}<\mathsf{n},\mathsf{i}<\mathsf{n}}\\&\quad\Big(\mathbf{1}_{\ll\,\mathtt{coord}(\mathsf{n},0)=\langle1,\mathsf{k},\mathsf{i}\rangle\,\gg}(\mathsf{n})\cdot\mathbf{1}_{\ll\,\mathtt{lg}(\mathsf{n})=\mathsf{k}+1\,\gg}(\mathsf{n})\cdot\textstyle\prod_{1\leqslant\mathsf{j}\leqslant\mathsf{k}}\mathtt{coord}(\mathsf{m},\mathtt{coord}(\mathsf{n},\mathsf{j}))\Big).\end{aligned}$$

On conclut que $\mathtt{Term}$ est un ensemble primitif récursif. Ensuite on peut caractériser l'ensemble $\mathtt{Atom}$ des numéros de formules atomiques en définissant $\mathtt{Atom}(\mathsf{n})$ comme

$$\begin{aligned}&\mathtt{Suite}(\mathsf{n})\wedge\\&\quad((\mathtt{lg}(\mathsf{n})=3\wedge\mathtt{coord}(\mathsf{n},0)=\ulcorner{=}\urcorner\wedge\mathtt{Term}(\mathtt{coord}(\mathsf{n},1))\wedge\mathtt{Term}(\mathtt{coord}(\mathsf{n},2)))\\&\quad\vee\exists\mathsf{k},\mathsf{i}{<}\mathsf{n}\,(\mathtt{lg}(\mathsf{n})=\mathsf{k}+1\wedge\mathtt{coord}(\mathsf{n},0)=\langle2,\mathsf{k},\mathsf{i}\rangle\\&\qquad\qquad\wedge\forall\mathsf{j}{\leqslant}\mathsf{k}\,(\mathsf{j}\geqslant1{\Rightarrow}\mathtt{Term}(\mathtt{coord}(\mathsf{n},\mathsf{j}))))),\end{aligned}$$

et il est donc primitif récursif. Enfin l'argument pour l'ensemble $\mathtt{Form}$ des numéros de formules est du même type que pour les termes, en définissant $\mathtt{Form}(\mathsf{n})$ comme

$$\begin{aligned}&\mathtt{Atom}(\mathsf{n})\vee(\mathtt{Suite}(\mathsf{n})\wedge\\&\quad((\mathtt{coord}(\mathsf{n},0)=\ulcorner\neg\urcorner\wedge\mathtt{lg}(\mathsf{n})=2\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},1)))\\&\qquad\vee((\mathtt{coord}(\mathsf{n},0)=\ulcorner\Rightarrow\urcorner\wedge\mathtt{lg}(\mathsf{n})=3\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},1))\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},2)))\\&\qquad\vee((\mathtt{coord}(\mathsf{n},0)=\ulcorner\wedge\urcorner\wedge\mathtt{lg}(\mathsf{n})=3\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},1))\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},2)))\\&\qquad\vee((\mathtt{coord}(\mathsf{n},0)=\ulcorner\vee\urcorner\wedge\mathtt{lg}(\mathsf{n})=3\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},1))\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},2)))\\&\qquad\vee\exists\mathsf{i}<\mathsf{n}((\mathtt{coord}(\mathsf{n},0)=\ulcorner\exists\boldsymbol{x}_\mathsf{i}\urcorner\wedge\mathtt{lg}(\mathsf{n})=2\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},1)))\\&\qquad\vee\exists\mathsf{i}<\mathsf{n}((\mathtt{coord}(\mathsf{n},0)=\ulcorner\forall\boldsymbol{x}_\mathsf{i}\urcorner\wedge\mathtt{lg}(\mathsf{n})=2\wedge\mathtt{Form}(\mathtt{coord}(\mathsf{n},1))))).\end{aligned}$$

Il s'agit à nouveau d'une définition par récursion complète, et donc l'ensemble $\mathtt{Form}$ est primitif récursif. □

2.2. La fonction de substitution.

► On montre que la contre-partie, au niveau des numéros, de la fonction de substitution est une fonction primitive récursive. ◄

▷ *Si* F *est une formule,* t *un terme et* i *un entier naturel, la substitution de* t *aux occurrences libres de la variable* $\boldsymbol{x}_\mathsf{i}$ *dans* F *fournit une nouvelle formule* $\mathsf{F}(\boldsymbol{x}_\mathsf{i}{\leftarrow}\mathsf{t})$. *Passant au niveau des numéros des termes et des formules, on obtient ainsi une fonction de* $\mathbb{N}^3$ *dans* $\mathbb{N}$. *Il est important pour la suite de s'assurer que cette fonction est suffisamment simple, à savoir qu'elle est primitive récursive.* ◁

PROPOSITION 2.4. (substitution) *La fonction de* $\mathbb{N}^3$ *dans* $\mathbb{N}$ *définie par*

$$\mathtt{subst}_{\mathtt{Form}}(\ulcorner \mathsf{F} \urcorner, \ulcorner \mathsf{t} \urcorner, \mathsf{i}) := \ulcorner \mathsf{F}(\boldsymbol{x}_{\mathsf{i}} \leftarrow \mathsf{t}) \urcorner, \tag{2.1}$$

et prolongée par 0 *hors de* $\mathtt{Form} \times \mathtt{Term} \times \mathbb{N}$, *est primitive récursive.*

DÉMONSTRATION. On définit d'abord une fonction de substitution $\mathtt{subst}_{\mathtt{Termes}}$ pour les termes par

$$\begin{aligned}
&\mathtt{subst}_{\mathtt{Termes}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = 0 \text{ pour } \neg\mathtt{Term}(\mathsf{n}) \text{ ou } \neg\mathtt{Term}(\mathsf{m}),\\
&\mathtt{subst}_{\mathtt{Termes}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \mathsf{n} \text{ pour } \mathtt{Const}(\mathsf{n}) \text{ ou } \mathtt{Var}(\mathsf{n}) \text{ avec } \mathtt{coord}(\mathsf{n}, 1) \neq \mathsf{i},\\
&\mathtt{subst}_{\mathtt{Termes}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \mathsf{m} \text{ pour } \mathsf{n} = \langle 0, \mathsf{i} \rangle,\\
&\mathtt{subst}_{\mathtt{Termes}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) =\\
&\quad \langle \mathtt{coord}(\mathsf{n}, 0), \mathtt{subst}_{\mathtt{Termes}}(\mathtt{coord}(\mathsf{n}, 1), \mathsf{m}, \mathsf{i}), \ldots, \mathtt{subst}_{\mathtt{Termes}}(\mathtt{coord}(\mathsf{n}, \mathsf{k}), \mathsf{m}, \mathsf{i}) \rangle\\
&\qquad \text{pour } \mathtt{Term}(\mathsf{n}) \text{ et } \neg\mathtt{Var}(\mathsf{n}) \text{ et } \neg\mathtt{Const}(\mathsf{n}) \text{ et } \mathtt{lg}(\mathsf{n}) = \mathsf{k} + 1.
\end{aligned}$$

Comme les clauses ci-dessus correspondent à une récursion complète, la fonction $\mathtt{subst}_{\mathtt{Termes}}$ ainsi définie est primitive récursive, et, par construction, on a

$$\mathtt{subst}_{\mathtt{Termes}}(\ulcorner \mathsf{t} \urcorner, \ulcorner \mathsf{u} \urcorner, \mathsf{i}) := \ulcorner \mathsf{t}(\boldsymbol{x}_{\mathsf{i}} \leftarrow \mathsf{u}) \urcorner, \tag{2.2}$$

quels que soient les termes t, u et l'indice i. Ensuite, on définit de même une fonction de substitution pour les formules par

$$\begin{aligned}
&\mathtt{subst}_{\mathtt{Form}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = 0 \text{ pour } \neg\mathtt{Form}(\mathsf{n}) \text{ ou } \neg\mathtt{Term}(\mathsf{m}),\\
&\mathtt{subst}_{\mathtt{Form}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \langle \mathtt{coord}(\mathsf{n}, 0), \mathtt{subst}_{\mathtt{Termes}}(\mathtt{coord}(\mathsf{n}, 1), \mathsf{m}, \mathsf{i}), \ldots,\\
&\qquad\qquad \mathtt{subst}_{\mathtt{Termes}}(\mathtt{coord}(\mathsf{n}, \mathsf{k}), \mathsf{m}, \mathsf{i}) \rangle\\
&\quad \text{pour } \mathtt{Atom}(\mathsf{n}) \text{ et } \mathtt{lg}(\mathsf{n}) = \mathsf{k} + 1,\\
&\mathtt{subst}_{\mathtt{Form}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \langle \mathtt{coord}(\mathsf{n}, 0), \mathtt{subst}_{\mathtt{Form}}(\mathtt{coord}(\mathsf{n}, 1), \mathsf{m}, \mathsf{i}) \rangle\\
&\quad \text{pour } \mathtt{Form}(\mathsf{n}) \text{ et } \neg\mathtt{Atom}(\mathsf{n}) \text{ et } \mathtt{coord}(\mathsf{n}, 0) = \ulcorner\neg\urcorner,\\
&\mathtt{subst}_{\mathtt{Form}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \langle \mathtt{coord}(\mathsf{n}, 0), \mathtt{subst}_{\mathtt{Form}}(\mathtt{coord}(\mathsf{n}, 1), \mathsf{m}, \mathsf{i}), \mathtt{subst}_{\mathtt{Form}}(\mathtt{coord}(\mathsf{n}, 2), \mathsf{m}, \mathsf{i}) \rangle\\
&\quad \text{pour } \mathtt{Form}(\mathsf{n}) \text{ et } \neg\mathtt{Atom}(\mathsf{n}) \text{ et } \mathtt{coord}(\mathsf{n}, 0) = \ulcorner\Rightarrow\urcorner, \ulcorner\vee\urcorner, \text{ ou } \ulcorner\wedge\urcorner,\\
&\mathtt{subst}_{\mathtt{Form}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \langle \mathtt{coord}(\mathsf{n}, 0), \mathtt{subst}_{\mathtt{Form}}(\mathtt{coord}(\mathsf{n}, 2), \mathsf{m}, \mathsf{i}) \rangle\\
&\quad \text{pour } \mathtt{Form}(\mathsf{n}) \text{ et } \neg\mathtt{Atom}(\mathsf{n}) \text{ et } \mathtt{Suite}(\mathtt{coord}(\mathsf{n}, 0))\\
&\qquad \text{et } \mathtt{coord}(\mathtt{coord}(\mathsf{n}, 0), 0) = 3 \text{ ou } 4 \text{ et } \mathtt{coord}(\mathtt{coord}(\mathsf{n}, 0), 1) = \mathsf{i},\\
&\mathtt{subst}_{\mathtt{Form}}(\mathsf{n}, \mathsf{m}, \mathsf{i}) = \mathsf{n}\\
&\quad \text{pour } \mathtt{Form}(\mathsf{n}) \text{ et } \neg\mathtt{Atom}(\mathsf{n}) \text{ et } \mathtt{Suite}(\mathtt{coord}(\mathsf{n}, 0))\\
&\qquad \text{et } \mathtt{coord}(\mathtt{coord}(\mathsf{n}, 0), 0) = 3 \text{ ou } 4 \text{ et } \mathtt{coord}(\mathtt{coord}(\mathsf{n}, 0), 1) \neq \mathsf{i},
\end{aligned}$$

La fonction $\mathtt{subst}_{\mathtt{Form}}$ est définie par une récursion complète par rapport à la variable n, et elle est donc primitive récursive. Par ailleurs, on a $\mathrm{subst}(\ulcorner \mathsf{F} \urcorner, \ulcorner \mathsf{t} \urcorner, \mathsf{i}) = \ulcorner \mathsf{F}(\boldsymbol{x}_{\mathsf{i}} \leftarrow \mathsf{t}) \urcorner$ par construction. □

COROLLAIRE 2.5. *La fonction* subst *associant à tout couple de la forme* $(\ulcorner \mathsf{F} \urcorner, \mathsf{k})$ *avec* $\mathsf{F}(\boldsymbol{x}_1)$ *formule à une variable libre de* $\mathcal{L}_{\max}$ *le numéro de la formule* $\mathsf{F}(\boldsymbol{S}^{\mathsf{k}}\mathbf{0})$ *est primitive récursive.*

DÉMONSTRATION. La fonction f qui associe à tout entier k le numéro du terme $\boldsymbol{S}^{\mathsf{k}}\mathbf{0}$ est primitive récursive, puisque définie par la récursion

$$f(\mathsf{k}) = \begin{cases} \langle 1, 0, 1 \rangle & \text{pour } \mathsf{k} = 0,\\ \langle \langle 1, 2, 1 \rangle, f(\mathsf{k} - 1) \rangle & \text{pour } \mathsf{k} > 0. \end{cases}.$$

En la composant avec la fonction $\mathtt{subst}_{\mathtt{Form}}$ de la proposition 2.4, et avec la fonction constante de valeur 1, on obtient une fonction du type cherché. □

2.3. Numérotation des preuves.

▶ L'étape finale consiste à numéroter les preuves : on obtient une relation « p est le numéro d'une preuve de la formule de numéro n » sur $\mathbb{N}^2$. On montre que cette relation est primitive récursive. ◀

Si T est un ensemble de formules de $\mathcal{L}_{\max}$, on note $\ulcorner\mathsf{T}\urcorner$ l'ensemble des numéros des formules composant T. Afin de simplifier les énoncés, il est commode de poser

CONVENTION 2.6. (récursif) On dit qu'un ensemble de formules T est primitif récursif (*resp.* récursif,*resp.* semi-récursif) si l'ensemble $\ulcorner\mathsf{T}\urcorner$ l'est.

On commence par étudier les numéros des axiomes de $\mathcal{L}_{\max}$.

LEMME 2.7. *L'ensemble des axiomes de $\mathcal{L}_{\max}$ est primitif récursif.*

DÉMONSTRATION. Les axiomes se répartissent en plusieurs familles. La première est celle des instances d'axiomes de la logique propositionnelle. Considérons l'axiome $\boldsymbol{X}_1 \Rightarrow (\boldsymbol{X}_2 \Rightarrow \boldsymbol{X}_1)$. Une formule F de $\mathcal{L}_{\max}$ est une instance de cet axiome si et seulement si il existe des formules $\mathsf{F}_1, \mathsf{F}_2$ telles que F est $\mathsf{F}_1 \Rightarrow (\mathsf{F}_2 \Rightarrow \mathsf{F}_1)$. Un entier n est le numéro d'une telle formule si et seulement si il existe des numéros de formule n_1, n_2, nécessairement inférieurs à n, tels que F est $\mathsf{F}_1 \Rightarrow (\mathsf{F}_2 \Rightarrow \mathsf{F}_1)$ en appelant F_i la formule de numéro n_i, donc si et seulement si n satisfait

$$\exists \mathsf{n}_1, \mathsf{n}_2 < \mathsf{n}\, (\mathtt{Form}(\mathsf{n}_1) \wedge \mathtt{Form}(\mathsf{n}_2) \wedge \mathsf{n} = \langle \ulcorner\Rightarrow\urcorner, \mathsf{n}_1, \langle \ulcorner\Rightarrow\urcorner, \mathsf{n}_2, \mathsf{n}_1\rangle\rangle).$$

Cette condition ne met en jeu que des quantifications bornées et des fonctions primitives récursives, et elle définit donc un ensemble primitif récursif. Il en est de même des instances de chacun des axiomes de la logique propositionnelle, et, comme il existe un nombre fini de ceux-ci, on déduit que l'ensemble des instances d'axiomes de $\mathcal{L}_\bullet$ est un sous-ensemble primitif récursif de $\mathtt{Form}$.

La seconde famille d'axiomes comprend les formules du type $\forall \boldsymbol{x}(\mathsf{F} \Rightarrow \mathsf{G}) \Rightarrow (\mathsf{F} \Rightarrow \forall \boldsymbol{x}\,(\mathsf{G}))$. Là encore, il s'agit d'une condition purement syntaxique et un entier n est le numéro d'un tel axiome si et seulement si il existe des entiers i, n_1, n_2 strictement inférieurs à n correspondant respectivement à l'indice de la variable $\boldsymbol{x}$ et aux numéros des formules F et G et donc à partir desquels n s'exprime de façon primitive récursive. L'argument est similaire pour les axiomes du type $\neg\, \forall \boldsymbol{x}\, (\mathsf{F}) \Leftrightarrow \exists \boldsymbol{x}\, (\neg \mathsf{F})$.

Le cas des axiomes $\forall \boldsymbol{x}(\mathsf{F}) \Rightarrow \mathsf{F}(\boldsymbol{x} \leftarrow \mathsf{t})$ est *a priori* plus délicat puisqu'y figure la substitution et que, de surcroît, on requiert la condition supplémentaire que le terme t soit libre pour la variable $\boldsymbol{x}$ dans F. Or, la question de la substitution est réglée par la proposition 2.4. Ensuite, il est facile de définir récursivement une relation primitive récursive $\mathtt{Occure}(\mathsf{m}, \mathsf{i})$ telle que, si m est le numéro d'un terme t ou d'une formule F, alors $\mathtt{Occure}(\mathsf{m}, \mathsf{i})$ est vrai si et seulement si la variable $\boldsymbol{x}_\mathsf{i}$ a au moins une occurrence dans t ou dans F. Par construction, $\mathtt{Occure}(\mathsf{m}, \mathsf{i})$ ne peut être vraie que pour $\mathsf{i} < \mathsf{m}$. Alors, une récursion parallèle à celle utilisée pour définir la fonction $\mathtt{subst}_{\mathtt{Form}}$ permet de définir une relation $\mathtt{Libre}(\mathsf{n}, \mathsf{m}, \mathsf{i})$ de sorte que, si n est le numéro d'une formule F et m le numéro d'un terme t, alors $\mathtt{Libre}(\mathsf{n}, \mathsf{m}, \mathsf{i})$ est vraie si et seulement si t est libre pour $\boldsymbol{x}_\mathsf{i}$ dans F. La récursion se fait sur n, et on observe que t est libre pour $\boldsymbol{x}_\mathsf{i}$ dans $Q\boldsymbol{x}(\mathsf{G})$ si ou bien $\boldsymbol{x}_\mathsf{i}$ n'apparaît pas dans $Q\boldsymbol{x}(\mathsf{G})$, ou bien $\boldsymbol{x}$ n'apparaît pas dans t et t est libre pour $\boldsymbol{x}_\mathsf{i}$

dans G. On peut donc prendre comme clauses de définition

$\mathtt{Libre}(\mathsf{n},\mathsf{m},\mathsf{i}) = 0$ pour $\neg\mathtt{Form}(\mathsf{n})$ ou $\neg\mathtt{Term}(\mathsf{m})$,
$\mathtt{Libre}(\mathsf{n},\mathsf{m},\mathsf{i}) = 1$ pour $\mathtt{Atom}(\mathsf{n})$,
$\mathtt{Libre}(\mathsf{n},\mathsf{m},\mathsf{i}) = \mathtt{Libre}(\mathtt{coord}(\mathsf{n},1),\mathsf{m},\mathsf{i})$ pour $\mathtt{Form}(\mathsf{n})$ et $\neg\mathtt{Atom}(\mathsf{n})$ et $\mathtt{coord}(\mathsf{n},0) = \ulcorner\neg\urcorner$,
$\mathtt{Libre}(\mathsf{n},\mathsf{m},\mathsf{i}) = \inf(\mathtt{Libre}(\mathtt{coord}(\mathsf{n},1),\mathsf{m},\mathsf{i}),\mathtt{Libre}(\mathtt{coord}(\mathsf{n},2),\mathsf{m},\mathsf{i}))$
pour $\mathtt{Form}(\mathsf{n})$ et $\neg\mathtt{Atom}(\mathsf{n})$ et $\mathtt{coord}(\mathsf{n},0) = \ulcorner\wedge\urcorner, \ulcorner\vee\urcorner, \ulcorner\Rightarrow\urcorner$ ou $\ulcorner\Leftrightarrow\urcorner$,
$\mathtt{Libre}(\mathsf{n},\mathsf{m},\mathsf{i}) = \sup(\neg\mathtt{Occure}(\mathsf{n},\mathsf{i}),\inf(\mathtt{Occure}(\mathsf{n},\mathsf{i}),\mathtt{Libre}(\mathtt{coord}(\mathsf{n},3),\mathsf{m},\mathsf{i})$
pour $\mathtt{Form}(\mathsf{n})$ et $\neg\mathtt{Atom}(\mathsf{n})$ et $\mathtt{coord}(\mathsf{n},0) = \ulcorner\exists\urcorner$ ou $\ulcorner\forall\urcorner$.

La relation $\mathtt{Libre}$ est donc primitive récursive. A partir de là, il est facile d'établir que les numéros des axiomes du type $\forall\boldsymbol{x}(\mathsf{F})\Rightarrow\mathsf{F}(\boldsymbol{x}\leftarrow\mathsf{t})$ avec t libre pour $\boldsymbol{x}$ dans F est un ensemble primitif récursif.

Enfin les axiomes pour l'égalité ne posent pas de problème, puisqu'on peut écrire une formule directe explicite. □

PROPOSITION 2.8. (preuve) *Supposons que* T *est un ensemble primitif récursif (resp. récursif,resp. semi-récursif) de formules de* $\mathcal{L}_{\max}$. *Alors la relation* $\mathtt{Preuve}_{\mathsf{T}}(\mathsf{n},\mathsf{m})$ *exprimant que* m *est le numéro d'une preuve à partir de* T *pour la formule de numéro* n *est primitive récursive (resp. récursive,resp. semi-récursive).*

DÉMONSTRATION. Supposons que n est le numéro de la formule F. Alors un entier m est le numéro d'une preuve de F à partir de T si et seulement si c'est le numéro d'une suite finie de formules finissant avec F et telle que chaque formule est un axiome, ou un élément de T, ou obtenue par généralisation à partir d'une formule antérieure de la suite, ou obtenue par coupure à partir de deux formules antérieures de la suite. En notant $\mathtt{Axio}(\mathsf{n})$ la relation récursive caractérisant les numéros d'axiomes construite dans le lemme 2.7, on peut définir $\mathtt{Preuve}_{\mathsf{T}}(\mathsf{n},\mathsf{m})$ comme

$$\begin{aligned}&\mathtt{Form}(\mathsf{n}) \wedge \mathtt{Suite}(\mathsf{m}) \wedge \mathtt{coord}(\mathsf{m},\mathtt{lg}(\mathsf{m})-1) = \mathsf{n}\\ &\quad\wedge \forall \mathsf{k}{<}\,\mathtt{lg}(\mathsf{m})\,(\mathtt{Form}(\mathtt{coord}(\mathsf{m},\mathsf{k}))\\ &\qquad\wedge (\mathtt{Axio}(\mathtt{coord}(\mathsf{m},\mathsf{k}))\\ &\qquad\vee \mathbf{1}_{\ulcorner\mathsf{T}\urcorner}(\mathtt{coord}(\mathsf{m},\mathsf{k}))\\ &\qquad\vee \exists \mathsf{i}{<}\,\mathsf{k}\,(\mathtt{coord}(\mathsf{m},\mathsf{k}) = \mathtt{generalisation}(\mathtt{coord}(\mathsf{m},\mathsf{i}),\mathtt{coord}(\mathtt{coord}(\mathsf{m},\mathsf{k}),1)))\\ &\qquad\vee \exists \mathsf{i},\mathsf{j}{<}\,\mathsf{k}\,(\mathtt{coord}(\mathsf{m},\mathsf{k}) = \mathtt{coupure}(\mathtt{coord}(\mathsf{m},\mathsf{i}),\mathtt{coord}(\mathsf{m},\mathsf{j})))),\end{aligned}$$

où $\mathtt{generalisation}$ et $\mathtt{coupure}$ sont les deux fonctions primitives récursives définies par

$\mathtt{generalisation}(\mathsf{n},\mathsf{i}) := \langle\ulcorner\forall\boldsymbol{x}_{\mathsf{i}}\urcorner,\mathsf{n}\rangle$,
$\mathtt{coupure}(\mathsf{n},\mathsf{p}) := \mathtt{coord}(\mathsf{p},2)$ si $\mathtt{Form}(\mathsf{p}) \wedge \mathtt{coord}(\mathsf{p},0) = \ulcorner\Rightarrow\urcorner \wedge \mathtt{coord}(\mathsf{p},1) = \mathsf{n}$,
$\mathtt{coupure}(\mathsf{n},\mathsf{p}) := 0$ sinon.

C'est alors la complexité de T qui dicte la complexité de $\mathtt{Preuve}_{\mathsf{T}}$: si T est primitif récursif, c'est-à-dire si la fonction $\mathbf{1}_{\ulcorner\mathsf{T}\urcorner}$ est primitive récursive, alors $\mathtt{Preuve}_{\mathsf{T}}$ est une relation primitive récursive, et de même avec récursif et semi-récursif. □

EXEMPLE 2.9. (système de Peano) Les axiomes du système de Peano du premier ordre PA_1 forment une famille infinie de formules closes de $\mathcal{L}_{\mathrm{arith}}$, donc *a fortiori* de $\mathcal{L}_{\max}$. Cette famille est primitive récursive. En effet, les axiomes d'induction sont obtenus en énumérant les formules $\mathsf{Ind}_{\mathsf{F}}$:

$$(\mathsf{F}(\boldsymbol{x}_1\leftarrow\mathbf{0}) \wedge \forall\boldsymbol{x}_1(\mathsf{F}\Rightarrow\mathsf{F}(\boldsymbol{x}_1\leftarrow\boldsymbol{S}(\boldsymbol{x}_1)))) \Rightarrow \forall\boldsymbol{x}_1(\mathsf{F})$$

pour F formule de $\mathcal{L}_{\mathrm{arith}}$, et il existe une fonction primitive récursive associant au numéro de toute formule F le numéro de la formule $\mathsf{Ind}_{\mathsf{F}}$ correspondant. On déduit

de la proposition 2.8 que la relation $\mathtt{Preuve}_{\mathsf{PA}_1}(\mathsf{n},\mathsf{m})$ exprimant que m code une preuve à partir de PA_1 pour la formule de code n est primitive récursive.

▷ *On déduit de ce qui précède que l'ensemble des formules prouvables à partir d'un ensemble récursif de formules est la* ***projection*** *d'un ensemble récursif. On a vu dans la section 1 que la famille des relations primitives récursives est close par quantification bornée, et le même argument montre qu'il en est de même de la famille des relations récursives. Par contre, on n'a rien affirmé quant aux quantifications quelconques, ou, ce qui revient au même, aux projections d'ensembles (primitifs) récursifs, et, de fait, on verra dans la section 4 qu'il existe des projections de relations récursives qui ne sont pas récursives. Ceci conduit à introduire la nouvelle notion d'ensemble semi-récursif.* ◁

DÉFINITION 2.10. (semi-récursif) Une relation S sur $\mathbb{N}^{\mathsf{p}}$ est dite *semi-récursive* s'il existe $\mathsf{q} \geqslant \mathsf{p}$ et une relation récursive R sur $\mathbb{N}^{\mathsf{q}}$ telle que S est la projection de R, c'est-à-dire que $S(\vec{\mathsf{n}})$ est vraie si et seulement si il existe $\vec{\mathsf{m}}$ tel que $R(\vec{\mathsf{n}},\vec{\mathsf{m}})$ le soit.

Par définition, toute relation récursive est semi-récursive.

COROLLAIRE 2.11. *Supposons que* T *est un ensemble (semi)-récursif de formules closes de* $\mathcal{L}_{\max}$. *Alors l'ensemble des formules closes prouvables à partir de* T *est semi-récursif.*

DÉMONSTRATION. Une formule close F de numéro n est prouvable à partir de T si et seulement si il existe un entier m tel que m est le numéro d'une preuve de F à partir de T, si et seulement si la relation $\exists \boldsymbol{x}\,(\mathtt{Preuve}_{\mathsf{T}}(\mathsf{n},\boldsymbol{x}))$ est satisfaite dans $(\mathbb{N},0,S,+,\cdot)$. □

3. L'arithmétique de Robinson

▶ On établit des résultats de prouvabilité à partir du système $\mathsf{PA}_{\text{faible}}$ dit de Robinson constitué des axiomes de Peano à l'exclusion des axiomes d'induction et d'une définition de l'ordre. En particulier, on montre que toute fonction récursive est, en un sens technique convenable, représentable dans ce système. ◀

▷ *Les fonctions et relations récursives sur* $\mathbb{N}$ *ou plus généralement* $\mathbb{N}^{\mathsf{p}}$ *sont, en un certain sens, simples : par exemple, elles sont calculables par machine de Turing, c'est-à-dire au moyen d'un programme rudimentaire. Dans cette section, on passe du point de vue de la calculabilité à celui de la prouvabilité. On va montrer qu'on peut* prouver *l'existence de toute fonction récursive à partir du fragment fini du système de Peano obtenu en omettant les axiomes d'induction. Ce résultat technique est essentiel pour l'obtention des résultats d'impossibilité de la section 4, et, en un sens, c'est lui qui constitue le noyau dur de la démonstration de ces résultats. Plus précisément, en sus de prévisibles vérifications plus ou moins automatiques, il y a dans cette section un point non trivial qui est la clôture de la famille des fonctions représentables par définition récursive : la difficulté tient à la nécessité de pouvoir parler de suites d'entiers à l'intérieur de la structure* $(\mathbb{N},0,S,+,\cdot)$. *Au plan purement technique, on a préparé le terrain avec le codage des suites dans la section 1, et les choses s'enchaîneront désormais bien, mais il n'empêche qu'il y a là un point délicat.* ◁

3.1. Modèles du système $\mathsf{PA}_{\text{faible}}$.

► On fait provision de résultats d'arithmétique prouvables à partir des axiomes de Robinson. ◄

▷ *Comme la plupart des propriétés d'arithmétique prouvables à partir des axiomes de Peano ont des preuves qui utilisent l'induction, on peut s'attendre à ce que très peu de propriétés puissent être prouvées lorsqu'on omet les axiomes d'induction. De fait, on peut démontrer que même des propriétés très simples comme la commutativité de l'addition ne peuvent pas être prouvées sans induction. Par contre, on va voir que, malgré tout, un assez grand nombre de propriétés restent accessibles dans ce qu'on va appeler l'arithmétique de Robinson.*

Dans toute la suite, le problème n'est pas de se convaincre du fait que les propriétés considérées sont vraies dans la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, ce qui est généralement évident, mais de ce qu'elles sont formellement prouvables à partir de* $\mathsf{PA}_{\text{faible}}$*, donc, en particulier, sans induction. Comme on l'a vu au chapitre VII, la méthode la plus commode pour montrer qu'une formule* F *est prouvable à partir de* $\mathsf{PA}_{\text{faible}}$ *est la méthode sémantique consistant à établir que* F *est vraie dans tous les modèles de* $\mathsf{PA}_{\text{faible}}$*, et donc notre première tâche est d'étudier (un peu) les modèles de* $\mathsf{PA}_{\text{faible}}$*. Le principal résultat est que tout modèle de* $\mathsf{PA}_{\text{faible}}$ *admet un segment initial qui est une copie de* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, ce qui permet d'affirmer que toutes le formules suffisamment simples, en l'occurrence celles dont les seules quantifications non bornées sont existentielles, sont automatiquement prouvables dans* $\mathsf{PA}_{\text{faible}}$ *si elles sont satisfaites dans* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*.* ◁

Définition 3.1. (système $\mathsf{PA}_{\text{faible}}$) On appelle *système de Robinson* le système $\mathsf{PA}_{\text{faible}}$ de $\mathcal{L}_{\text{arith}^+}$ obtenu en otant du système de Peano PA l'axiome d'induction et en ajoutant l'axiome de définition $\mathsf{Def}_{\leqslant}$: $\forall \boldsymbol{x}, \boldsymbol{y}(\boldsymbol{x} \leqslant \boldsymbol{y} \Leftrightarrow \exists \boldsymbol{z}\,(\boldsymbol{z} + \boldsymbol{x} = \boldsymbol{y}))$.

▷ *Le système* $\mathsf{PA}_{\text{faible}}$ *est une famille finie constituée de sept formules de la logique du premier ordre* $\mathcal{L}_{\text{arith}^+}$*, et il est donc équivalent à l'unique formule qui est la conjonction de ces sept formules. Par hypothèse, la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *est un modèle de* $\mathsf{PA}_{\text{faible}}$*, puisque l'axiome définissant la relation additionnelle correspond à la construction de l'ordre usuel des entiers à partir de l'addition. On notera que la définition proposée utilise l'addition de* $\boldsymbol{z}$ *à gauche : dans le cas de la structure usuelle sur* $\mathbb{N}$*, l'addition est commutative, et il est donc indifférent de l'utiliser à gauche ou à droite dans la définition de l'ordre. Ici par contre, comme on l'a mentionné ci-dessus, le cadre axiomatique de* $\mathsf{PA}_{\text{faible}}$ *est si faible qu'il ne garantit pas la commutativité de l'addition, et il n'est donc pas indifférent de référer à une addition à gauche ou à droite dans l'introduction de* $\leqslant$*.*

On notera que $\mathsf{PA}_{\text{faible}}$ *n'est pas formellement un sous-système de* PA_1 *puisqu'il contient un axiome supplémentaire. En fait,* $\mathsf{PA}_{\text{faible}}$ *est un sous-système du système* PA_1^+ *obtenu en ajoutant à* PA_1 *la définition* $\mathsf{Def}_{\leqslant}$*, lequel est une extension* conservative *de* PA_1*, c'est-à-dire que toute formule ne contenant pas le symbole* $\leqslant$ *prouvable à partir de* PA_1^+ *est prouvable à partir de* PA_1*, ainsi qu'il en va toujours pour les extensions par définition.*

On rappelle qu'on écrit $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ *pour* $\boldsymbol{S}(...(\boldsymbol{S}(\mathbf{0}))...)$*,* n *symboles* $\boldsymbol{S}$*. Le but est d'établir que, dans tout modèle de* $\mathsf{PA}_{\text{faible}}$*, les interprétations des termes* $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ *forment une copie de* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*. Pour cela, on commence par établir que* $\mathsf{PA}_{\text{faible}}$ *prouve diverses propriétés des termes* $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ *mettant en jeu le successeur, l'addition, et la multiplication, puis l'ordre.* ◁

Lemme 3.2. *Le système* $\mathsf{PA}_{\text{faible}}$ *prouve les formules suivantes :*

(3.1) • $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} \neq \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$ *pour* $\mathsf{p} \neq \mathsf{q}$.

(3.2) • $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} + \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$ *pour* $\mathsf{p} + \mathsf{q} = \mathsf{r}$*;*

(3.3) • $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} \cdot \boldsymbol{S}^{\mathsf{q}}\mathbf{0} = \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$ *pour* $\mathsf{p} \cdot \mathsf{q} = \mathsf{r}$*;*

(3.4) • $\forall \boldsymbol{x}, \boldsymbol{y}\,(\boldsymbol{x} + \boldsymbol{y} = \mathbf{0} \Rightarrow (\boldsymbol{x} = \mathbf{0} \wedge \boldsymbol{y} = \mathbf{0}))$;

DÉMONSTRATION. Soit $\mathcal{M}$ un modèle quelconque de $\mathsf{PA}_{\text{faible}}$. Pour (3.1), on montre que $\mathsf{p} < \mathsf{q}$ entraîne $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} \neq (\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}}$ pour tout q en utilisant une récurrence sur p. On suppose $\mathsf{p} < \mathsf{q}$. Alors q n'est pas nul, et on pose $\mathsf{q}' := \mathsf{q} - 1$. Supposons d'abord $\mathsf{p} = 0$. On a $(\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}} = \boldsymbol{S}^{\mathcal{M}}((\boldsymbol{S}^{\mathsf{q}'}\mathbf{0})^{\mathcal{M}})$, donc $\mathbf{0}^{\mathcal{M}} \neq (\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}}$ puisque $\mathcal{M}$ satisfait Succ_1. Supposons $\mathsf{p} > 0$. Soit $\mathsf{p}' := \mathsf{p} - 1$. On a alors $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} = \boldsymbol{S}^{\mathcal{M}}((\boldsymbol{S}^{\mathsf{p}'}\mathbf{0})^{\mathcal{M}})$. L'hypothèse de récurrence entraîne $(\boldsymbol{S}^{\mathsf{p}'}\mathbf{0})^{\mathcal{M}} \neq (\boldsymbol{S}^{\mathsf{q}'}\mathbf{0})^{\mathcal{M}}$, d'où $\boldsymbol{S}((\boldsymbol{S}^{\mathsf{p}'}\mathbf{0})^{\mathcal{M}}) \neq \boldsymbol{S}((\boldsymbol{S}^{\mathsf{q}'}\mathbf{0})^{\mathcal{M}})$, qui est $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} \neq (\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}}$.

La prouvabilité des formules (3.2) a été établie dans le lemme VII.3.3 comme illustration de la méthode sémantique. Pour (3.3), l'argument est similaire, en utilisant les axiomes Mult_1 et Mult_2.

Pour (3.4), soient a, b des éléments quelconques du domaine de $\mathcal{M}$. Il s'agit de montrer que $a +^{\mathcal{M}} b = \mathbf{0}^{\mathcal{M}}$ entraîne $a = \mathbf{0}^{\mathcal{M}}$ et $b = \mathbf{0}^{\mathcal{M}}$. Or, par Succ_1, $b \neq \mathbf{0}^{\mathcal{M}}$ entraîne l'existence de b' dans le domaine de $\mathcal{M}$ vérifiant $b = \boldsymbol{S}^{\mathcal{M}}(b')$. Par Add_2, on a alors $a +^{\mathcal{M}} b = \boldsymbol{S}^{\mathcal{M}}(a +^{\mathcal{M}} b')$, et, par Succ_1 à nouveau, ce dernier élément n'est pas $\mathbf{0}^{\mathcal{M}}$. Donc $a +^{\mathcal{M}} b = \mathbf{0}^{\mathcal{M}}$ entraîne $b = \mathbf{0}^{\mathcal{M}}$, et, de là, $a = \mathbf{0}^{\mathcal{M}}$ par Add_1. □

LEMME 3.3. *Le système* $\mathsf{PA}_{\text{faible}}$ *prouve les formules suivantes :*

(3.5) • $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} \leqslant \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$ *pour* $\mathsf{p} \leqslant \mathsf{q}$,

(3.6) • $\forall \boldsymbol{x}, \boldsymbol{y}\, (\boldsymbol{x} \leqslant \boldsymbol{y} \Rightarrow \boldsymbol{S}(\boldsymbol{x}) \leqslant \boldsymbol{S}(\boldsymbol{y}))$;

(3.7) • $\forall \boldsymbol{x}\, (\boldsymbol{x} \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0} \Leftrightarrow (\boldsymbol{x} = \mathbf{0} \vee \boldsymbol{x} = \boldsymbol{S}^{1}\mathbf{0} \vee \ldots \vee \boldsymbol{x} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0}))$;

(3.8) • $\forall \boldsymbol{x}\, (\boldsymbol{x} \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0} \vee \boldsymbol{S}^{\mathsf{p}}\mathbf{0} \leqslant \boldsymbol{x})$.

DÉMONSTRATION. Soit $\mathcal{M}$ un modèle de $\mathsf{PA}_{\text{faible}}$. Supposons $\mathsf{p} \leqslant \mathsf{q}$. Soit $\mathsf{r} := \mathsf{q} - \mathsf{p}$. On a alors $\mathsf{r} + \mathsf{p} = \mathsf{q}$, donc, par (3.2), $\mathsf{PA}_{\text{faible}}$ prouve $\boldsymbol{S}^{\mathsf{r}}\mathbf{0} + \boldsymbol{S}^{\mathsf{p}}\mathbf{0} = \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$, donc *a fortiori* $\exists \boldsymbol{z}(\boldsymbol{z} + \boldsymbol{S}^{\mathsf{p}}\mathbf{0} = \boldsymbol{S}^{\mathsf{q}}\mathbf{0})$, soit $\boldsymbol{S}^{\mathsf{p}}\mathbf{0} \leqslant \boldsymbol{S}^{\mathsf{q}}\mathbf{0}$.

Supposons maintenant $\mathcal{M} \models a \leqslant b$, soit $c +^{\mathcal{M}} a = b$. Comme $\mathcal{M}$ satisfait Add_2, on déduit $c +^{\mathcal{M}} \boldsymbol{S}^{\mathcal{M}}(a) = \boldsymbol{S}^{\mathcal{M}}(b)$, donc $\boldsymbol{S}^{\mathcal{M}}(a) \leqslant^{\mathcal{M}} \boldsymbol{S}^{\mathcal{M}}(b)$.

Pour (3.7), une direction résulte directement de (3.5), à savoir $\boldsymbol{x} = \boldsymbol{S}^{\mathsf{q}}\mathbf{0} \Rightarrow \boldsymbol{x} \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ pour $\mathsf{q} \leqslant \mathsf{p}$. Pour la réciproque, on utilise une récurrence sur p. Supposons $\mathcal{M} \models a \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$: il existe donc c vérifiant $c +^{\mathcal{M}} a = (\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$. Supposons d'abord $\mathsf{p} = 0$. Alors (3.4) entraîne $a = \mathbf{0}^{\mathcal{M}}$, ce qui est (3.7). Supposons ensuite $\mathsf{p} > 0$. Soit $\mathsf{p}' := \mathsf{p} - 1$. Si a est $\mathbf{0}^{\mathcal{M}}$, on a fini. Sinon, il existe a' tel que a est $\boldsymbol{S}^{\mathcal{M}}(a')$. Par Add_2, $c +^{\mathcal{M}} a$ est $\boldsymbol{S}^{\mathcal{M}}(c +^{\mathcal{M}} a')$, et, par Succ_2, on déduit $c +^{\mathcal{M}} a' = (\boldsymbol{S}^{\mathsf{p}'}\mathbf{0})^{\mathcal{M}}$, d'où $a' \leqslant (\boldsymbol{S}^{\mathsf{p}'}\mathbf{0})^{\mathcal{M}}$. Par hypothèse de récurrence, on déduit que a' est $(\boldsymbol{S}^{\mathsf{i}}\mathbf{0})^{\mathcal{M}}$ pour l'un (au moins) des entiers $\mathsf{i} = 0, 1, \ldots, \mathsf{p}'$, et, de là, que a est $(\boldsymbol{S}^{\mathsf{i}}\mathbf{0})^{\mathcal{M}}$ pour l'un (au moins) des entiers $\mathsf{i} = 1, 2, \ldots, \mathsf{p}$.

Enfin, on montre (3.8) par récurrence sur p. Soit a un élément quelconque du domaine de $\mathcal{M}$. Supposons $\mathsf{p} = 0$. Puisque $\mathcal{M}$ satisfait Add_1, on a $a +^{\mathcal{M}} \mathbf{0} = a$, donc $\mathbf{0}^{\mathcal{M}} \leqslant^{\mathcal{M}} a$. Supposons $\mathsf{p} > 0$, et soit $\mathsf{p}' = \mathsf{p} - 1$. Si a est $\mathbf{0}^{\mathcal{M}}$, on a $a \leqslant^{\mathcal{M}} (\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$ par (3.5). Sinon, par Succ_1, il existe a' tel que a soit $\boldsymbol{S}^{\mathcal{M}}(a')$. Par hypothèse de récurrence, on a $a' \leqslant^{\mathcal{M}} (\boldsymbol{S}^{\mathsf{p}'}\mathbf{0})^{\mathcal{M}}$ ou $\boldsymbol{S}^{\mathsf{p}'}\mathbf{0}^{\mathcal{M}} \leqslant^{\mathcal{M}} a'$. Dans le premier cas, on déduit $a \leqslant^{\mathcal{M}} \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ de (3.6). Dans le second cas, on déduit $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} \leqslant^{\mathcal{M}} a$ de même. On notera qu'à ce point rien ne permet d'affirmer que $\mathsf{PA}_{\text{faible}}$ prouve que $\leqslant$ soit une relation d'ordre — et, de fait, il ne le prouve pas: il existe des modèles de $\mathsf{PA}_{\text{faible}}$ où l'interprétation de $\leqslant$ n'est pas un ordre. □

▷ *Pour décrire la situation, on introduit les notions de sous-structure et d'extension finale d'une structure : comme un sous-groupe d'un groupe,* $\mathcal{M}_\bullet$ *est sous-structure de* $\mathcal{M}$ *si* $\mathcal{M}_\bullet$ *est obtenue à partir de* $\mathcal{M}$ *en restreignant le domaine, et, dans un contexte où une relation binaire* $\leqslant$ *est distinguée, que* $\mathcal{M}$ *est extension finale de* $\mathcal{M}_\bullet$ *si* $\mathcal{M}_\bullet$ *est sous-structure de* $\mathcal{M}$ *et, de plus, tous les éléments du domaine de* $\mathcal{M}$ *qui ne sont pas dans le domaine de* $\mathcal{M}_\bullet$ *sont plus grands au sens de* $\leqslant$ *(qui peut être ou ne pas être un ordre) que tous les éléments du domaine de* $\mathcal{M}_\bullet$.

Le résultat est alors que tout modèle de l'arithmétique de Robinson est une extension finale de la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, c'est-à-dire est constitué d'une copie de* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *suivie éventuellement d'éléments tous strictement plus grands que les (copies des) entiers naturels.* ◁

DÉFINITION 3.4. (sous-structure, extension, extension finale) (*i*) Soient Σ une signature, et $\mathcal{M}, \mathcal{M}_\bullet$ deux structures de type Σ. On dit que $\mathcal{M}$ est *extension* de $\mathcal{M}_\bullet$, ou encore que $\mathcal{M}_\bullet$ est *sous-structure* de $\mathcal{M}$, si $\mathrm{Dom}(\mathcal{M}_\bullet)$ est inclus dans $\mathrm{Dom}(\mathcal{M})$ et que les opérations et relations de $\mathcal{M}_\bullet$ sont les restrictions de celles de $\mathcal{M}$.

(*ii*) Supposons que $\boldsymbol{r}$ est un symbole de relation binaire appartenant à Σ. On dit que $\mathcal{M}$ est extension $\boldsymbol{r}$*-finale* de $\mathcal{M}_\bullet$ si $\mathcal{M}$ est extension de $\mathcal{M}_\bullet$ et si tout $\boldsymbol{r}^{\mathcal{M}}$-prédécesseur d'un élément de $\mathrm{Dom}(\mathcal{M}_\bullet)$ est élément de $\mathrm{Dom}(\mathcal{M}_\bullet)$, c'est-à-dire si $a\,\boldsymbol{r}^{\mathcal{M}}\,b \in \mathrm{Dom}(\mathcal{M}_\bullet)$ entraîne $a \in \mathrm{Dom}(\mathcal{M}_\bullet)$.

LEMME 3.5. *Soient* $\mathcal{M}$ *une structure de type* Σ*, et* A *un sous-ensemble du domaine de* $\mathcal{M}$*. Alors les opérations et relations de* $\mathcal{M}$ *induisent une sous-structure de domaine* A *si et seulement si* A *est clos par toutes les opérations de* $\mathcal{M}$*, donc en particulier si* A *contient* $\boldsymbol{c}^{\mathcal{M}}$ *pour chaque symbole de constante* $\boldsymbol{c}$ *de* Σ*.*

DÉMONSTRATION. Supposons que $\mathcal{M}_\bullet$ est une structure de type Σ de domaine A. Pour chaque symbole d'opération $\boldsymbol{s}$ de Σ, l'interprétation de $\boldsymbol{s}$ dans $\mathcal{M}_\bullet$ doit être une opération partout définie. Par définition, ceci n'est vérifié par la restriction de $\boldsymbol{s}^{\mathcal{M}}$ que si, et seulement si, l'ensemble A est clos par $\boldsymbol{s}^{\mathcal{M}}$. □

PROPOSITION 3.6. (extension finale) *Soit* $\mathcal{M}$ *un modèle de* $\mathsf{PA}_{\mathrm{faible}}$*. Alors il existe une sous-structure* $\mathcal{M}_\bullet$ *de* $\mathcal{M}$ *dont le domaine est* $\{(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})^{\mathcal{M}}\,;\,\mathsf{n} \in \mathbb{N}\}$*. La structure* $\mathcal{M}_\bullet$ *est isomorphe à* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, et* $\mathcal{M}$ *est extension* $\leqslant$*-finale de* $\mathcal{M}_\bullet$ *(cf. figure 1).*

DÉMONSTRATION. Posons $\mathbb{N}_\bullet := \{(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})^{\mathcal{M}}\,;\,\mathsf{n} \in \mathbb{N}\}$. D'après le lemme 3.5, pour montrer que les opérations et relations de $\mathcal{M}$ induisent une structure bien définie $\mathcal{M}_\bullet$ de domaine $\mathbb{N}_\bullet$, il suffit de vérifier que $\mathbb{N}_\bullet$ est clos par toutes les opérations de $\Sigma_{\mathrm{arith}^+}$, donc de Σ_{arith}. C'est le cas pour le symbole de constante $\mathbf{0}$, puisque $\mathbf{0}^{\mathcal{M}}$ est dans $\mathbb{N}_\bullet$ par hypothèse ; c'est le cas pour $\boldsymbol{S}$, puisque, par construction, on a $\boldsymbol{S}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0}) = \boldsymbol{S}^{\mathsf{p}+1}\mathbf{0}$, donc $\boldsymbol{S}^{\mathcal{M}}((\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}) = (\boldsymbol{S}^{\mathsf{p}+1}\mathbf{0})^{\mathcal{M}}$; c'est le cas pour $+$ et $\cdot$, puisque, par (3.2) et (3.3), on a $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} +^{\mathcal{M}} (\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}} = (\boldsymbol{S}^{\mathsf{p}+\mathsf{q}}\mathbf{0})^{\mathcal{M}}$ et $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}} \cdot^{\mathcal{M}} (\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}} = (\boldsymbol{S}^{\mathsf{p}\mathsf{q}}\mathbf{0})^{\mathcal{M}}$.

Ensuite, l'application $f : \mathsf{n} \mapsto (\boldsymbol{S}^{\mathsf{n}}\mathbf{0})^{\mathcal{M}}$ est une surjection de $\mathbb{N}$ sur $\mathbb{N}_\bullet$, et elle est injective en vertu de (3.1). Donc f est une bijection. Par construction, on a $f(0) = \mathbf{0}^{\mathcal{M}}$, et $f(S(\mathsf{n})) = \boldsymbol{S}^{\mathcal{M}}(f(\mathsf{n}))$. Puis, par (3.2) et (3.3) à nouveau, $f(\mathsf{p}+\mathsf{q}) = f(\mathsf{p}) +^{\mathcal{M}} f(\mathsf{q})$ et $f(\mathsf{p}\cdot\mathsf{q}) = f(\mathsf{p}) \cdot^{\mathcal{M}} f(\mathsf{q})$. Enfin, par (3.5), $\mathsf{p} \leqslant \mathsf{q}$ équivaut à $f(\mathsf{p}) \leqslant^{\mathcal{M}} f(\mathsf{q})$. Donc la bijection f établit un isomorphisme entre les structures $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ et $\mathcal{M}_\bullet$.

Enfin soit a un élément de $\mathbb{N}_\bullet$, disons $a = (\boldsymbol{S}^{\mathsf{n}}\mathbf{0})^{\mathcal{M}}$, et b un élément quelconque du domaine de $\mathcal{M}$. Par (3.8), on a $a \leqslant b$ ou $b \leqslant a$. Alors, par (3.7), $b \leqslant a$ entraîne qu'il existe un entier $\mathsf{p} \leqslant \mathsf{n}$ tel que b soit $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$, donc appartienne à $\mathbb{N}_\bullet$: c'est dire que $\mathcal{M}$ est extension $\leqslant$-finale de $\mathcal{M}_\bullet$. □

▷ *Noter que le résultat ainsi établi étend le résultat démontré au chapitre VII pour les modèles de l'arithmétique. Il est naturel que la proposition 3.6 s'applique à tous les modèles de l'arithmétique puisqu'une telle structure est modèle de* $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, donc, par hypothèse, de* PA_1*, et a fortiori de* $\mathsf{PA}_{\mathrm{faible}}$ *puisque ce dernier est inclus dans* PA_1*, à l'ajout près de la définition de* $\leqslant$*, laquelle ne change rien aux modèles puisque tout modèle sans* $\leqslant$ *peut être étendu par définition. Par contre, étant donné que* $\mathsf{PA}_{\mathrm{faible}}$ *est beaucoup plus faible que* PA_1 *et, a fortiori, que* $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *— tout au moins de façon conjecturale pour le moment — il existe des*

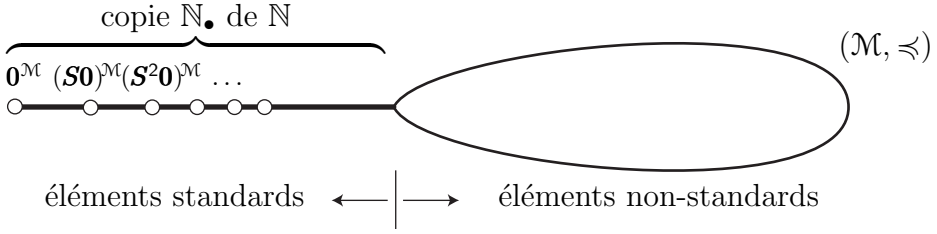

FIGURE 1. Modèle de $\mathsf{PA}_{\text{faible}}$: Une copie de $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ suivie d'éventuels éléments non-standards ; à la différence du cas particulier des modèles de l'arithmétique de la figure VII.2, la relation $\leqslant^{\mathcal{M}}$ n'a aucune raison en général d'être un ordre sur les éléments non-standards.

quantités de modèles de $\mathsf{PA}_{\text{faible}}$ *qui ne sont pas modèles de* PA_1*, et des quantités de modèles de* PA_1 *qui ne sont pas modèles de l'arithmétique, c'est-à-dire qui ne sont pas élémentairement équivalents à* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*. Le résultat précédent montre que, malgré tout, aussi exotiques soient ces modèles de* $\mathsf{PA}_{\text{faible}}$*, néanmoins ils ont tous en commun de commencer par une copie des entiers.* ◁

3.2. Absoluité des formules Σ_1.

▶ On montre que toute formule dont les quantifications non bornées sont exclusivement existentielles est préservée par extension finale. ◀

▷ *Deux modèles quelconques du système* $\mathsf{PA}_{\text{faible}}$ *n'ont aucune raison de satisfaire les mêmes formules du premier ordre : par exemple, on a mentionné qu'il existe des modèles de* $\mathsf{PA}_{\text{faible}}$ *où l'addition n'est pas commutative, ce qui signifie qu'il existe des modèles de* $\mathsf{PA}_{\text{faible}}$ *où la formule* $\forall \boldsymbol{x}, \boldsymbol{y}(\boldsymbol{x}+\boldsymbol{y} = \boldsymbol{y}+\boldsymbol{x})$ *est satisfaite, comme* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, et d'autres où elle est fausse (cf. exercice 3). On va montrer ici que ce type de situation ne peut se produire pour certaines formules syntaxiquement simples, dites de complexité* Σ_1*. La raison est que les formules de complexité* Σ_1 *vraies dans une structure* $\mathcal{M}_\bullet$ *restent automatiquement vraies dans toute extension finale de* $\mathcal{M}_\bullet$ *: comme on sait que tout modèle de* $\mathsf{PA}_{\text{faible}}$ *est extension finale de* $(\mathbb{N}, 0, S, +, \cdot)$*, on en déduit que les formules de complexité* Σ_1 *vraies dans* $(\mathbb{N}, 0, S, +, \cdot)$ *doivent être vraies dans tout modèle de* $\mathsf{PA}_{\text{faible}}$*. De là, par complétude, on pourra déduire que toute formule* Σ_1 *vraie dans* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *est prouvable à partir de* $\mathsf{PA}_{\text{faible}}$*.*

On commence avec le cas d'une extension quelconque et les formules sans quantificateurs, puis on considère celui des extensions finales vis-à-vis des formules dites à quantifications bornées. ◁

LEMME 3.7. *Supposons* $\mathcal{M}$ *extension de* $\mathcal{M}_\bullet$*. Alors, pour toute formule* $\mathsf{F}(\vec{\boldsymbol{x}})$ *sans quantificateur et tous* $\vec{a}$ *dans le domaine de* $\mathcal{M}_\bullet$*,*

$$\mathcal{M}_\bullet \models \mathsf{F}(\vec{a}) \text{ équivaut à } \mathcal{M} \models \mathsf{F}(\vec{a}). \tag{3.9}$$

En particulier, $\mathcal{M}_\bullet$ *et* $\mathcal{M}$ *satisfont les mêmes formules closes sans quantificateur.*

DÉMONSTRATION. Une induction montre d'abord $\mathsf{t}(\vec{a})^{\mathcal{M}_\bullet} = \mathsf{t}(\vec{a})^{\mathcal{M}}$ pour tout terme $\mathsf{t}(\vec{\boldsymbol{x}})$ et tous $\vec{a}$ dans le domaine de $\mathcal{M}_\bullet$. On en déduit l'équivalence (3.9) pour les formules atomiques, puis, inductivement, pour toutes les formules sans quantificateur, c'est-à-dire pour les combinaisons booléennes de formules atomiques. □

On rappelle que, suivant la convention VII.1.11, $\exists \boldsymbol{x} \leqslant \boldsymbol{y}(...)$ signifie $\exists \boldsymbol{x}(\boldsymbol{x} \leqslant \boldsymbol{y} \wedge ...)$, et $\forall \boldsymbol{x} \leqslant \boldsymbol{y}(...)$ signifie $\forall \boldsymbol{x}(\boldsymbol{x} \leqslant \boldsymbol{y} \Rightarrow ...)$.

DÉFINITION 3.8. (formules Δ_0 et Σ_1) On dit qu'une formule F de $\mathcal{L}_{\text{arith}^+}$ est *de complexité* Δ_0 — ou simplement est une formule Δ_0 — si les seules quantifications figurant dans F sont des quantifications bornées $\exists \boldsymbol{x} \leqslant \mathsf{t}$ ou $\forall \boldsymbol{x} \leqslant \mathsf{t}$ avec t terme sans occurrence de $\boldsymbol{x}$. On dit que F est *de complexité* Σ_1 si les seules quantifications universelles figurant dans F sont des quantifications bornées $\forall \boldsymbol{x} \leqslant \mathsf{t}$ et si, dans l'arbre représentant F, il n'y a aucun symbole $\neg$, $\Rightarrow$, $\Leftrightarrow$ au-dessus d'une quantification existentielle.

De façon équivalente, la famille des formules de complexité Σ_1 est la plus petite famille contenant toutes les formules sans quantificateur et close par conjonction, disjonction, quantification universelle bornée, et quantification existentielle. En particulier, toute formule du type $\exists \boldsymbol{x}_1, ..., \boldsymbol{x}_\mathsf{k}(\mathsf{G})$ avec G de complexité Δ_0 est de complexité Σ_1.

▷ *On parle d'absoluité pour exprimer que la valeur « vrai » ou « faux » d'une formule ne change pas entre une structure et une autre. Le résultat suivant exprime que les formules closes Δ_0 sont absolues et les formules closes Σ_1 semi-absolues vers le haut vis-à-vis des extensions finales.* ◁

PROPOSITION 3.9. (absoluité) *Supposons $\mathcal{M}$ extension finale de $\mathcal{M}_\bullet$. Alors pour toute formule $\mathsf{F}(\vec{\boldsymbol{x}})$ de complexité Δ_0 et tous $\vec{a}$ dans le domaine de $\mathcal{M}_\bullet$,*

$$\mathcal{M}_\bullet \models \mathsf{F}(\vec{a}) \text{ équivaut à } \mathcal{M} \models \mathsf{F}(\vec{a}). \tag{3.10}$$

En particulier, $\mathcal{M}_\bullet$ et $\mathcal{M}$ satisfont les mêmes formules closes de complexité Δ_0.

Pour toute formule $\mathsf{F}(\vec{\boldsymbol{x}})$ de complexité Σ_1 et tous $\vec{a}$ dans le domaine de $\mathcal{M}_\bullet$,

$$\mathcal{M}_\bullet \models \mathsf{F}(\vec{a}) \text{ entraîne } \mathcal{M} \models \mathsf{F}(\vec{a}). \tag{3.11}$$

En particulier, tout formule close de complexité Σ_1 vraie dans $\mathcal{M}_\bullet$ est aussi vraie dans $\mathcal{M}$.

DÉMONSTRATION. On montre l'équivalence (3.10) par induction sur F. D'après le lemme 3.7, l'équivalence est vraie pour les formules atomiques puisque $\mathcal{M}$ est extension de $\mathcal{M}_\bullet$, et elle est préservée par négation, conjonction, disjonction, implication et équivalence. Il reste à voir que (3.10) est aussi préservée par quantification bornée. On considère le cas d'une quantification universelle. Supposons que $\mathsf{F}(\vec{\boldsymbol{x}})$ est $\forall \boldsymbol{y} \leqslant \mathsf{t}(\vec{\boldsymbol{x}})(\mathsf{G}(\vec{\boldsymbol{x}}, \boldsymbol{y}))$ et que $\vec{a}$ est une suite d'éléments dans le domaine de $\mathcal{M}_\bullet$. On cherche le lien entre la satisfaction de $\forall \boldsymbol{y} \leqslant \mathsf{t}(\vec{a})(\mathsf{G}(\vec{a}, \boldsymbol{y}))$ dans $\mathcal{M}_\bullet$ et sa satisfaction dans $\mathcal{M}$. Or, soit b un élément de $\mathcal{M}$ vérifiant $b \leqslant \mathsf{t}(\vec{a})^{\mathcal{M}}$. Comme $\mathcal{M}$ est extension de $\mathcal{M}_\bullet$, on a $\mathsf{t}(\vec{a})^{\mathcal{M}} = \mathsf{t}(\vec{a})^{\mathcal{M}_\bullet}$, et, comme $\mathcal{M}$ est extension finale de $\mathcal{M}_\bullet$ et que $\mathsf{t}(\vec{a})^{\mathcal{M}_\bullet}$ est dans $\mathrm{Dom}(\mathcal{M}_\bullet)$, la relation $b \leqslant \mathsf{t}(\vec{a})^{\mathcal{M}}$ entraîne que b est dans $\mathrm{Dom}(\mathcal{M}_\bullet)$. Par conséquent, les éléments vérifiant $b \leqslant \mathsf{t}(\vec{a})$ dans $\mathcal{M}_\bullet$ et $\mathcal{M}$ coïncident. Par hypothèse d'induction, pour tout tel élément b, les relations $\mathcal{M}_\bullet \models \mathsf{G}(\vec{a}, b)$ et $\mathcal{M} \models \mathsf{G}(\vec{a}, b)$ sont équivalentes, et, par conséquent, il en est de même de $\mathcal{M}_\bullet \models \mathsf{F}(\vec{a})$ et $\mathcal{M} \models \mathsf{F}(\vec{a})$. Le cas du quantificateur $\exists$ est similaire.

On procède de même pour l'implication (3.11). Par (3.10), celle-ci est vraie pour toutes les formules sans quantificateur. Le passage à la conjonction et à la disjonction est facile. L'argument pour les quantifications universelles bornées est le même que ci-dessus. Enfin, pour une quantification existentielle, supposons que $\mathsf{F}(\vec{\boldsymbol{x}})$ est $\exists \boldsymbol{y}(\mathsf{G}(\vec{\boldsymbol{x}}, \boldsymbol{y}))$ avec $\mathsf{G}(\vec{\boldsymbol{x}}, \boldsymbol{y})$ de complexité Σ_1. Supposons $\mathcal{M}_\bullet \models \mathsf{F}(\vec{a})$. On a donc $\mathcal{M}_\bullet \models \mathsf{G}(\vec{a}, b)$ pour un certain b dans le domaine de $\mathcal{M}_\bullet$. Par hypothèse d'induction, on déduit $\mathcal{M} \models \mathsf{G}(\vec{a}, b)$, d'où $\mathcal{M} \models \exists \boldsymbol{y}(\mathsf{G}(\vec{a}, \boldsymbol{y}))$, et par conséquent $\mathcal{M} \models \mathsf{F}(\vec{a})$. □

▷ *Noter que, pour ce qui est de l'implication* (3.11)*, il n'y a a priori aucune chance que l'implication réciproque soit vraie : si* $\mathcal{M}$ *satisfait* $\mathsf{F}(\vec{a})$*, il existe un élément* b *dans le domaine de* $\mathcal{M}$ *vérifiant* $\mathsf{G}(\vec{a}, b)$*, mais, faute de borne sur la quantification, rien ne permet d'affirmer que cet élément appartient au domaine de* $\mathcal{M}_\bullet$*.*

On déduit de ce qui précède un résultat de complétude faible affirmant que toute formule suffisamment simple vraie dans les entiers est prouvable dans le système de Robinson. On verra dans la suite que ce résultat ne s'étend absolument pas à des formules plus compliquées : c'est précisément ce qu'affirme le premier théorème d'incomplétude de Gödel. ◁

PROPOSITION 3.10. (prouvabilité) *Toute formule close de complexité* Σ_1 *vraie dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *est prouvable à partir des axiomes de Robinson* $\mathsf{PA}_{\text{faible}}$*.*

DÉMONSTRATION. Soit F une formule close de complexité Σ_1 de $\mathcal{L}_{\text{arith}^+}$ vraie dans la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$. Par la proposition 3.10, F est vraie dans toute extension finale de $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, donc, par la proposition 3.6, dans tout modèle de $\mathsf{PA}_{\text{faible}}$. Par le théorème de complétude, cela implique que F est prouvable à partir de $\mathsf{PA}_{\text{faible}}$. □

COROLLAIRE 3.11. *Si* F *est une formule arithmétique close de complexité* Δ_0*, alors* $\mathsf{PA}_{\text{faible}}$ *prouve l'une au moins des formules* F *ou* $\neg\mathsf{F}$*.*

DÉMONSTRATION. Si F est Δ_0, alors à la fois F et $\neg\mathsf{F}$ sont Δ_0, donc *a fortiori* Σ_1, et l'une des deux est satisfaite dans la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$. On applique alors la proposition 3.10. □

▷ *En d'autres termes, le système* $\mathsf{PA}_{\text{faible}}$ *est complet pour les formules arithmétiques* Δ_0*, c'est-à-dire les formules dont toutes les quantifications sont bornées.* ◁

3.3. Représentabilité.

► On montre que toute fonction récursive f sur $\mathbb{N}^{\mathsf{p}}$ est représentable dans le système $\mathsf{PA}_{\text{faible}}$, ceci signifiant que $\mathsf{PA}_{\text{faible}}$ prouve, en un sens convenable, la valeur de $f(\vec{\mathsf{n}})$. ◄

▷ *On en vient ici à la mise en relation des fonctions récursives et du système* $\mathsf{PA}_{\text{faible}}$*. Il s'agit de montrer que, si* f *est une fonction récursive, alors* $\mathsf{PA}_{\text{faible}}$ *calcule en un certain sens la valeur de* f*. On a déjà rencontré la notion de fonction définissable : si* $\mathcal{M}$ *est une structure, une fonction* f *de* $\mathrm{Dom}(\mathcal{M})^{\mathsf{p}}$ *dans* $\mathrm{Dom}(\mathcal{M})$ *est dite définissable dans* $\mathcal{M}$ *s'il existe une formule* $\mathsf{F}(\vec{\boldsymbol{x}}, \boldsymbol{y})$ *telle que* $b = f(\vec{a})$ *est vrai dans* $\mathcal{M}$ *si et seulement* $\mathcal{M}$ *satisfait* $\mathsf{F}(\vec{a}, b)$*. De fait, on peut effectivement montrer que toute fonction récursive sur* $\mathbb{N}^{\mathsf{p}}$ *est définissable dans la structure* $(\mathbb{N}, 0, S, +, \cdot)$ *(exercice 4). Mais ce n'est pas cette notion qui est adaptée ici, puisqu'on ne vise pas des résultats relatifs à la satisfaction dans une structure particulière, mais des résultats de prouvabilité à partir d'un système d'axiomes, ici* $\mathsf{PA}_{\text{faible}}$*. Le problème est qu'alors parler des entiers ne fait pas sens, puisque* $\mathsf{PA}_{\text{faible}}$ *ne connaît que leur contre-partie formelle, à savoir les termes* $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$*. Du coup, ce à quoi on s'intéresse pour une fonction donnée* f *de* $\mathbb{N}^{\mathsf{p}}$ *dans* $\mathbb{N}$ *est l'existence d'une formule* $\mathsf{F}(\vec{\boldsymbol{x}}, \boldsymbol{y})$ *telle que, quand on a* $f(\mathsf{n}_1, ..., \mathsf{n}_{\mathsf{p}}) = \mathsf{n}$*, alors* $\mathsf{PA}_{\text{faible}}$ *prouve* $\mathsf{F}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0}, ..., \boldsymbol{S}^{\mathsf{n}_{\mathsf{p}}}\mathbf{0}, \boldsymbol{S}^{\mathsf{n}}\mathbf{0})$*. De plus, comme un modèle de* $\mathsf{PA}_{\text{faible}}$ *peut contenir bien d'autres éléments que les interprétations des termes* $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$*, on demande explicitement que* $\mathsf{PA}_{\text{faible}}$ *prouve la formule* $\forall \boldsymbol{y} \neq \boldsymbol{S}^{\mathsf{n}}\mathbf{0}\, (\neg\mathsf{F}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0}, ..., \boldsymbol{S}^{\mathsf{n}_{\mathsf{p}}}\mathbf{0}, \boldsymbol{y}))$*. Noter que cette condition, qui affirme le caractère fonctionnel de* F *aux valeurs standards des arguments, est plus faible que la condition qui coinsisterait à affirmer que* F *est fonctionnelle partout.* ◁

DÉFINITION 3.12. (représentable) Soit T une théorie de $\mathcal{L}_\Sigma$, avec Σ incluant Σ_{arith}. On dit qu'une formule $\mathsf{F}(\boldsymbol{x}_1, ..., \boldsymbol{x}_{\mathsf{p}}, \boldsymbol{y})$ de $\mathcal{L}_\Sigma$ *représente* dans T une fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ partout définie si, pour tous n_1, ... , n_{p}, n dans $\mathbb{N}$ vérifiant $f(\mathsf{n}_1, \ldots, \mathsf{n}_{\mathsf{p}}) = \mathsf{n}$,

- T prouve $\mathsf{F}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0}, \ldots, \boldsymbol{S}^{\mathsf{n}_\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{n}}\mathbf{0})$, et
- T prouve $\forall \boldsymbol{y} \neq \boldsymbol{S}^{\mathsf{n}}\mathbf{0}\, (\neg \mathsf{F}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0}, \ldots, \boldsymbol{S}^{\mathsf{n}_\mathsf{p}}\mathbf{0}, \boldsymbol{y}))$.

Le résultat principal de cette section est le théorème suivant :

PROPOSITION 3.13. (représentabilité) *Toute fonction récursive totale peut être représentée dans* $\mathsf{PA}_{\text{faible}}$ *par une formule de complexité* Σ_1.

▷ *A un point spécifique près, la démonstration de ce résultat n'est pas difficile : elle consiste naturellement à vérifier que les fonctions récursives de base sont représentables, puis que l'ensemble des fonctions représentables est clos par les opérations de composition, récursion, et minimalisation.* ◁

Dans toute la suite, on dit « Σ_1-représentable » pour « représentable par une formule de complexité Σ_1 ». Par ailleurs, dans tout modèle $\mathcal{M}$ de $\mathsf{PA}_{\text{faible}}$, les éléments de la forme $(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})^{\mathcal{M}}$ seront dits standards : ce sont eux qui correspondent aux entiers usuels, par opposition à tous les éventuels éléments dits non-standards qui ne correspondent à aucun entier naturel.

LEMME 3.14. *Les fonctions* $\mathtt{zero}$, $\mathtt{succ}$ *et* $\mathtt{proj}_{\mathsf{p},\mathsf{i}}$ *pour chaque* p, i *sont* Σ_1*-représentables dans* $\mathsf{PA}_{\text{faible}}$.

DÉMONSTRATION. Soit $\mathsf{F}(\boldsymbol{y})$ la formule $\boldsymbol{y} = \mathbf{0}$. Alors la formule $\mathsf{F}(\mathbf{0})$, c'est-à-dire $\mathbf{0} = \mathbf{0}$, est valide, donc prouvable à partir des seuls axiomes de $\mathcal{L}_{\text{arith}^+}$. Il en est de même de la formule $\forall \boldsymbol{y} \neq \mathbf{0}(\boldsymbol{y} \neq \mathbf{0})$. Donc, par définition, la formule $\mathsf{F}(\boldsymbol{y})$ représente dans $\mathsf{PA}_{\text{faible}}$ la fonction (à zéro argument) $\mathtt{zero}$. De même, $\boldsymbol{y} = \boldsymbol{S}(\boldsymbol{x})$ représente dans $\mathsf{PA}_{\text{faible}}$ la fonction $\mathtt{succ}$, et $\boldsymbol{y} = \boldsymbol{x}_\mathsf{i}$ représente $\mathtt{proj}_{\mathsf{p},\mathsf{i}}$. Les formules précédentes sont sans quantificateur, donc certainement de complexité Σ_1. □

LEMME 3.15. *Les fonctions* Σ_1*-représentables dans* $\mathsf{PA}_{\text{faible}}$ *sont closes par composition.*

DÉMONSTRATION. Supposons $f = \mathtt{comp}(g, f_1, \ldots, f_\mathsf{q})$. Supposons que F_i représente f_i pour $1 \leqslant \mathsf{i} \leqslant \mathsf{q}$, et que G représente g dans $\mathsf{PA}_{\text{faible}}$. Soit $\mathsf{F}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\mathsf{p}, \boldsymbol{y})$ la formule

$$\exists \boldsymbol{y}_1, ..., \boldsymbol{y}_\mathsf{q}(\mathsf{F}_1(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\mathsf{p}, \boldsymbol{y}_1) \wedge \cdots \wedge \mathsf{F}_\mathsf{q}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\mathsf{p}, \boldsymbol{y}_\mathsf{q}) \wedge \mathsf{G}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_\mathsf{q}, \boldsymbol{y})).$$

Alors F représente f dans $\mathsf{PA}_{\text{faible}}$. En effet, soit $\mathcal{M}$ un modèle quelconque de $\mathsf{PA}_{\text{faible}}$. Pour chaque i, et pour chaque choix d'entiers n_1, ... , n_p, il existe exactement un élément b_i du domaine de $\mathcal{M}$ vérifiant $\mathsf{F}_\mathsf{i}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0}, \ldots, \boldsymbol{S}^{\mathsf{n}_\mathsf{p}}\mathbf{0}, b_\mathsf{i})$, à savoir $(\boldsymbol{S}^{\mathsf{m}_\mathsf{i}}\mathbf{0})^{\mathcal{M}}$ avec $\mathsf{m}_\mathsf{i} = f_\mathsf{i}(\mathsf{n}_1, \ldots, \mathsf{n}_\mathsf{p})$. Ensuite, il existe exactement un élément a du domaine de $\mathcal{M}$ vérifiant $\mathsf{F}(\boldsymbol{S}^{\mathsf{m}_1}\mathbf{0}, \ldots, \boldsymbol{S}^{\mathsf{m}_\mathsf{q}}\mathbf{0}, a)$, à savoir $(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})^{\mathcal{M}}$ avec $\mathsf{n} = g(\mathsf{m}_1, \ldots, \mathsf{m}_\mathsf{q})$, soit $\mathsf{n} = f(\mathsf{n}_1, \ldots, \mathsf{n}_\mathsf{p})$. Par ailleurs, si chacune des formules F_1, ... , F_q, G est de complexité Σ_1, il en est de même de F. □

▷ *Avant d'en venir aux définitions par récursion, qui sont la partie délicate de la construction, on considère maintenant les définitions par minimalisation. On sait que, même si* g *est une fonction totale, la fonction* $\mathtt{min}(g)$ *n'est pas nécessairement totale, puisque, pour un choix* $\vec{\mathsf{n}}$ *donné, il n'existe pas nécessairement d'entier* k *pour lequel on ait* $g(\vec{\mathsf{n}}, \mathsf{k}) = 0$. *On dira ici que* f *est définie par minimalisation totale à partir de* g *si* f *est définie par minimalisation à partir de* g, *et* f *et* g *sont totales.* ◁

LEMME 3.16. *La famille des fonctions récursives totales est la clôture des fonctions de base par composition, récursion, et minimalisation totale.*

DÉMONSTRATION. Il est clair que toute fonction obtenue à partir des fonctions de base par composition, récursion, et minimalisation totale est une fonction récursive totale. Le problème est qu'inversement, il se pourrait que, dans la définition d'une fonction récursive totale, on utilise à des étapes intermédiaires des fonctions partielles. La question est donc de montrer qu'on peut l'éviter, c'est-à-dire que toute fonction récursive totale peut être construite en n'utilisant que des minimalisations totales : ceci résulte du corollaire 1.22 qui affirme qu'on peut toujours se contenter d'une unique minimalisation finale. □

LEMME 3.17. *Les fonctions Σ_1-représentables dans $\mathsf{PA}_{\text{faible}}$ sont closes par minimalisation totale.*

DÉMONSTRATION. Supposons que f est obtenue par minimalisation totale à partir de g, et que $\mathsf{G}(\vec{\boldsymbol{x}},\boldsymbol{y},\boldsymbol{z})$ est une formule de complexité Σ_1 représentant g dans $\mathsf{PA}_{\text{faible}}$. Soit $\mathsf{F}(\vec{\boldsymbol{x}},\boldsymbol{y})$ la formule

$$\mathsf{G}(\vec{\boldsymbol{x}},\boldsymbol{y},\mathbf{0}) \wedge \forall \boldsymbol{y}'{<}\boldsymbol{y}\ \exists \boldsymbol{z}{\neq}\mathbf{0}\ (\mathsf{G}(\vec{\boldsymbol{x}},\boldsymbol{y}',\boldsymbol{z})).$$

La formule F est elle aussi Σ_1 puisqu'obtenue à partir d'instances de G par conjonction, quantification universelle bornée et quantification existentielle. On va montrer que F représente f dans $\mathsf{PA}_{\text{faible}}$. Soit $\mathcal{M}$ un modèle quelconque de $\mathsf{PA}_{\text{faible}}$, et soient $\vec{\mathsf{n}}$ des entiers naturels. Soient $\mathsf{m} := f(\vec{\mathsf{n}})$, qui existe puisque, par hypothèse, f est une fonction totale, et, pour chaque $\mathsf{k} < \mathsf{m}$, soit $\mathsf{m}_\mathsf{k} := g(\vec{\mathsf{n}},\mathsf{k})$. Par hypothèse, on a $g(\vec{\mathsf{n}},\mathsf{m}) = 0$ et $g(\vec{\mathsf{n}},\mathsf{k}) = \mathsf{m}_\mathsf{k} \neq 0$ pour $\mathsf{k} < \mathsf{m}$. Puisque G représente g, on a $\mathcal{M} \models \mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}}\mathbf{0}, \mathbf{0})$. Par ailleurs, par (3.7), $\mathcal{M} \models b < \boldsymbol{S}^{\mathsf{m}}\mathbf{0}$ entraîne $b = \mathbf{0} \vee b = \boldsymbol{S}\mathbf{0} \vee \ldots \vee b = \boldsymbol{S}^{\mathsf{m}-1}\mathbf{0}$, donc, comme $\mathcal{M}$ satisfait $\mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, \boldsymbol{S}^{\mathsf{k}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}_\mathsf{k}}\mathbf{0})$, on a

$$\mathcal{M} \models \forall \boldsymbol{y}'{<}\boldsymbol{S}^{\mathsf{m}}\mathbf{0}\ \exists \boldsymbol{z}{\neq}\mathbf{0}\ (\mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, \boldsymbol{y}', \boldsymbol{z})),$$

donc $\mathcal{M} \models \mathsf{F}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}}\mathbf{0})$.

Par ailleurs, supposons $\mathcal{M} \models \mathsf{F}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, b)$. *A priori*, on ne sait pas que b doit être standard. Mais, par (3.8), on a $\mathcal{M} \models b \leqslant \boldsymbol{S}^{\mathsf{m}}\mathbf{0} \vee \boldsymbol{S}^{\mathsf{m}}\mathbf{0} < b$. Or $\mathcal{M} \models \boldsymbol{S}^{\mathsf{m}}\mathbf{0} < b$ est impossible : en effet, par définition, on aurait alors $\mathcal{M} \models \exists \boldsymbol{z}{\neq}\mathbf{0}(\mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}}\mathbf{0}, \boldsymbol{z}))$, alors que l'hypothèse que G représente g et qu'on a $g(\vec{\mathsf{n}},\mathsf{m}) = 0$ implique $\mathcal{M} \models \forall \boldsymbol{z}{\neq}\,\mathbf{0}(\neg\mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}}\mathbf{0}, \mathbf{0}))$. On a donc$\mathcal{M} \models b \leqslant \boldsymbol{S}^{\mathsf{m}}\mathbf{0}$, c'est-à-dire que b est standard, et, alors, il est clair que la seule valeur possible est $b = (\boldsymbol{S}^{\mathsf{m}}\mathbf{0})^{\mathcal{M}}$. Par conséquent, F représente f dans $\mathsf{PA}_{\text{faible}}$. □

▷ *On en vient à la clôture de la famille des fonction représentables dans $\mathsf{PA}_{\text{faible}}$ vis-à-vis des définitions par récursion. La construction est plus délicate, parce qu'il faut être capable de parler d'une suite de valeurs de longueur quelconque. C'est ici qu'on utilise la fonction* `frag` *du lemme 1.12 : comme annoncé dans la section 1, cette fonction permet de remplacer une quantification du type « il existe une suite d'entiers telle que… » par une unique quantification « il existe un entier tel que… ».* ◁

LEMME 3.18. *La fonction* `beta` *est Σ_1-représentable dans $\mathsf{PA}_{\text{faible}}$ par une formule $\mathsf{B}'(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3,\boldsymbol{y})$ pour laquelle $\mathsf{PA}_{\text{faible}}$ prouve*

$$\mathsf{B}'(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3,\boldsymbol{S}^{\mathsf{m}}\mathbf{0}) \Rightarrow \forall \boldsymbol{y}{\neq}\boldsymbol{S}^{\mathsf{m}}\mathbf{0}\ (\neg\mathsf{B}'(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3,\boldsymbol{y})). \tag{3.12}$$

DÉMONSTRATION. On utilise $\boldsymbol{x} < \boldsymbol{y}$ comme un raccourci pour $\boldsymbol{x} \leqslant \boldsymbol{y} \wedge \boldsymbol{x} \neq \boldsymbol{y}$, où $\boldsymbol{x} \neq \boldsymbol{y}$ est lui-même un racourci pour $\neg(\boldsymbol{x} = \boldsymbol{y})$. Soit $\mathsf{F}(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)$ la formule de complexité Δ_0

$$(\boldsymbol{x}_2 = \mathbf{0} \wedge \boldsymbol{x}_3 = \mathbf{0}) \vee (\boldsymbol{x}_2 \neq \mathbf{0} \wedge \exists \boldsymbol{x}_4{\leqslant}\boldsymbol{x}_1(\boldsymbol{x}_1 = \boldsymbol{x}_2 \cdot \boldsymbol{x}_4 + \boldsymbol{x}_3 \wedge \boldsymbol{x}_3 < \boldsymbol{x}_2)).$$

Alors F représente la fonction « reste de la division euclidienne ». En effet, si n, p sont des entiers et que r est le reste de la division euclidienne de n par p, alors, en notant q le quotient, on a $\mathsf{n} = \mathsf{p}\cdot\mathsf{q} + \mathsf{r}$ et $\mathsf{r} \leqslant \mathsf{p}$ et $\mathsf{r} \neq \mathsf{p}$, donc $\mathsf{PA}_{\text{faible}}$ prouve $\boldsymbol{S}^{\mathsf{n}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} \cdot \boldsymbol{S}^{\mathsf{q}}\mathbf{0} + \boldsymbol{S}^{\mathsf{r}}\mathbf{0}$, et $\boldsymbol{S}^{\mathsf{r}}\mathbf{0} \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ et $\boldsymbol{S}^{\mathsf{r}}\mathbf{0} \neq \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$, donc $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{F}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{r}}\mathbf{0})$. Par ailleurs, soit $\mathcal{M}$ un modèle quelconque

de $\mathsf{PA}_{\text{faible}}$. Supposons $\mathcal{M} \models \mathsf{F}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, a)$ avec $\mathsf{p} \geqslant 1$. Alors il existe b dans le domaine de $\mathcal{M}$ tel que $\mathcal{M}$ satisfait à la fois $b \leqslant \boldsymbol{S}^{\mathsf{n}}\mathbf{0}$, $\boldsymbol{S}^{\mathsf{n}}\mathbf{0} = \boldsymbol{S}^{\mathsf{p}}\mathbf{0} \cdot b + a$, $a \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$, et $a \neq \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$. Si a et b sont standards, les seules valeurs possibles sont $a = (\boldsymbol{S}^{\mathsf{r}}\mathbf{0})^{\mathcal{M}}$ et $b = (\boldsymbol{S}^{\mathsf{q}}\mathbf{0})^{\mathcal{M}}$. Or, par (3.7), $\mathcal{M} \models a \leqslant \boldsymbol{S}^{\mathsf{p}}\mathbf{0}$ entraîne que a est standard, et, de même, $\mathcal{M} \models b \leqslant \boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ entraîne que b est standard.

Soit $\mathsf{B}(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{y})$ la formule $\mathsf{F}(\boldsymbol{x}_1, \boldsymbol{S}(\boldsymbol{S}(\boldsymbol{x}_3) \cdot \boldsymbol{x}_2), \boldsymbol{y})$. Alors B est une formule Δ_0, tout comme F, et le fait que F représente la fonction « `reste` » implique que B représente `beta`.

Soit alors $\mathsf{B}'(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{y})$ la formule $\mathsf{B}(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{y}) \wedge \forall \boldsymbol{y}' < \boldsymbol{y}(\neg \mathsf{B}(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{y}'))$. Alors B', qui est encore une formule Δ_0, et donc *a fortiori* Σ_1, représente aussi `beta`. En effet, soient $\mathsf{n}, \mathsf{p}, \mathsf{i}$ des entiers, et soit $\mathsf{m} = \mathtt{beta}(\mathsf{n}, \mathsf{p}, \mathsf{i})$. Puisque B représente `beta`, la théorie $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{B}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{i}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}}\mathbf{0})$. Par (3.7), $\mathsf{PA}_{\text{faible}}$ prouve $\boldsymbol{y}' < \boldsymbol{S}^{\mathsf{m}}\mathbf{0} \Rightarrow (\boldsymbol{y}' = \mathbf{0} \vee \ldots \vee \boldsymbol{y}' = \boldsymbol{S}^{\mathsf{m}-1}\mathbf{0})$, et d'autre part $\neg \mathsf{B}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{i}}\mathbf{0}, \boldsymbol{S}^{\mathsf{j}}\mathbf{0})$ pour $\mathsf{j} = 0, 1, \ldots, \mathsf{m} - 1$. Par conséquent, $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{B}'(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{i}}\mathbf{0}, \boldsymbol{S}^{\mathsf{m}}\mathbf{0})$. Par ailleurs, puisque B représente `beta`, la théorie $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{B}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{i}}\mathbf{0}, \boldsymbol{y}) \Rightarrow \boldsymbol{y} = \boldsymbol{S}^{\mathsf{m}}\mathbf{0}$, donc, *a fortiori*, $\mathsf{PA}_{\text{faible}} \vdash \mathsf{B}'(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0}, \boldsymbol{S}^{\mathsf{i}}\mathbf{0}, \boldsymbol{y}) \Rightarrow \boldsymbol{y} = \boldsymbol{S}^{\mathsf{m}}\mathbf{0}$, et on conclut que B' représente `beta`.

Or soit $\mathcal{M}$ un modèle quelconque de $\mathsf{PA}_{\text{faible}}$, et supposons $\mathcal{M} \models \mathsf{B}'(a, b, c, \boldsymbol{S}^{\mathsf{m}}\mathbf{0})$. Soit d un élément du domaine de $\mathcal{M}$ distinct de $(\boldsymbol{S}^{\mathsf{m}}\mathbf{0})^{\mathcal{M}}$. Par (3.7), on a $\mathcal{M} \models d < \boldsymbol{S}^{\mathsf{m}}\mathbf{0}$ ou $\mathcal{M} \models \boldsymbol{S}^{\mathsf{m}}\mathbf{0} < d$. Dans le premier cas, l'hypothèse $\mathcal{M} \models \mathsf{B}'(a, b, c, \boldsymbol{S}^{\mathsf{m}}\mathbf{0})$ entraîne $\mathcal{M} \not\models \mathsf{B}'(a, b, c, d)$. Dans le second cas, si on avait $\mathcal{M} \models \mathsf{B}'(a, b, c, d)$, on déduirait $\mathcal{M} \not\models \mathsf{B}'(a, b, c, \boldsymbol{S}^{\mathsf{m}}\mathbf{0})$, contrairement à l'hypothèse. Par conséquent, on a nécessairement $\mathcal{M} \not\models \mathsf{B}'(a, b, c, d)$ et donc $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{B}'(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{S}^{\mathsf{m}}\mathbf{0}) \Rightarrow \forall \boldsymbol{y} \neq \boldsymbol{S}^{\mathsf{m}}\mathbf{0}(\neg \mathsf{B}'(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{y}))$. □

LEMME 3.19. *Les fonctions Σ_1-représentables dans $\mathsf{PA}_{\text{faible}}$ sont closes par récursion.*

DÉMONSTRATION. Supposons que g et h sont des fonctions respectivement de $\mathbb{N}^{\mathsf{p}}$ et $\mathbb{N}^{\mathsf{p}+2}$ dans $\mathbb{N}$ représentées dans $\mathsf{PA}_{\text{faible}}$ par les formules $\mathsf{G}(\vec{\boldsymbol{x}}, \boldsymbol{y})$ et $\mathsf{H}(\vec{\boldsymbol{x}}, \boldsymbol{x}_{\mathsf{p}+1}, \boldsymbol{x}_{\mathsf{p}+2}, \boldsymbol{y})$ de complexité Σ_1, et que f est la fonction $\mathtt{rec}(g, h)$. Dire qu'on a $f(\vec{\mathsf{n}}, \mathsf{k}) = \mathsf{m}$ dans $\mathbb{N}$, c'est dire qu'il existe des entiers m_0, m_1, … , m_{k} vérifiant

$$\mathsf{m}_0 = g(\vec{\mathsf{n}}) \wedge \mathsf{m}_1 = h(\vec{\mathsf{n}}, 1, \mathsf{m}_0) \wedge \cdots \wedge \mathsf{m}_{\mathsf{k}} = h(\vec{\mathsf{n}}, \mathsf{k}, \mathsf{m}_{\mathsf{k}-1}) \wedge \mathsf{m} = \mathsf{m}_{\mathsf{k}}. \tag{3.13}$$

En vertu du lemme 1.12, cette condition est vérifiée si et seulement si il existe deux entiers s, t vérifiant

$$\begin{aligned}&\mathtt{beta}(\mathsf{s}, \mathsf{t}, 0) = g(\vec{\mathsf{n}})\\ &\quad \wedge \mathtt{beta}(\mathsf{s}, \mathsf{t}, 1) = h(\vec{\mathsf{n}}, 1, \mathtt{frag}(s, 0)) \wedge \cdots \wedge \mathtt{beta}(\mathsf{s}, \mathsf{t}, \mathsf{k}) = h(\vec{\mathsf{n}}, \mathsf{k}, \mathtt{frag}(s, \mathsf{k} - 1))\\ &\quad \wedge \mathsf{m} = \mathtt{beta}(\mathsf{s}, \mathsf{t}, \mathsf{k}),\end{aligned}$$

donc

$$\begin{aligned}&\mathtt{beta}(\mathsf{s}, \mathsf{t}, 0) = g(\vec{\mathsf{n}})\\ &\quad \wedge \forall \mathsf{i} < \mathsf{k}(\mathtt{beta}(\mathsf{s}, \mathsf{t}, \mathsf{i} + 1) = h(\vec{\mathsf{n}}, \mathsf{i} + 1, \mathtt{beta}(\mathsf{s}, \mathsf{t}, \mathsf{i})))\\ &\quad \wedge \mathsf{m} = \mathtt{beta}(\mathsf{s}, \mathsf{t}, \mathsf{k}),\end{aligned}$$

donc si et seulement si il existe deux entiers s, t vérifiant

$$\begin{aligned}&\exists \boldsymbol{x}_1(\mathtt{beta}(\mathsf{s}, \mathsf{t}, 0) = \boldsymbol{x}_1 \text{ et } g(\vec{\mathsf{n}}) = \boldsymbol{x}_1)\\ &\quad \wedge \forall \boldsymbol{x}_2 < \mathsf{k}\ \exists \boldsymbol{x}_3\ \exists \boldsymbol{x}_4(\mathtt{beta}(\mathsf{s}, \mathsf{t}, \boldsymbol{x}_2) = \boldsymbol{x}_3 \wedge \mathtt{beta}(\mathsf{s}, \mathsf{t}, \boldsymbol{S}(\boldsymbol{x}_2)) = \boldsymbol{x}_4 \wedge h(\vec{\mathsf{n}}, \boldsymbol{S}(\boldsymbol{x}_2), \boldsymbol{x}_3) = \boldsymbol{x}_4))\\ &\quad \wedge \mathtt{beta}(\mathsf{s}, \mathsf{t}, \mathsf{k}) = \mathsf{m}).\end{aligned}$$

Soit alors $\mathsf{F}(\boldsymbol{s}, \boldsymbol{t}, \vec{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z})$ la formule

$$\begin{aligned}&\exists \boldsymbol{x}_1(\mathsf{B}'(\boldsymbol{s}, \boldsymbol{t}, \mathbf{0}, \boldsymbol{x}_1) \wedge \mathsf{G}(\vec{\boldsymbol{x}}, \boldsymbol{x}_1))\\ &\quad \wedge \forall \boldsymbol{x}_2 < \boldsymbol{y}\ \exists \boldsymbol{x}_3\ \exists \boldsymbol{x}_4(\mathsf{B}'(\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{x}_2, \boldsymbol{x}_3) \wedge \mathsf{B}'(\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{S}(\boldsymbol{x}_2), \boldsymbol{x}_4) \wedge \mathsf{H}(\vec{\boldsymbol{x}}, \boldsymbol{S}(\boldsymbol{x}_2), \boldsymbol{x}_2, \boldsymbol{x}_4))\\ &\quad \wedge \mathsf{B}'(\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{y}, \boldsymbol{z})\end{aligned}$$

obtenue à partir de la précédente en substituant des variables aux entiers et en remplaçant les fonctions g, h et $\mathtt{beta}$ par les formules F, H et B' qui, par hypothèse, les représentent dans $\mathsf{PA}_{\text{faible}}$. On va montrer que $\exists \boldsymbol{s},\boldsymbol{t}(\mathsf{F})$, qui, par construction, est une formule Σ_1, représente f dans $\mathsf{PA}_{\text{faible}}$. Pour cela, soient $\vec{\mathsf{n}}$ et k des entiers naturels, et $\mathcal{M}$ un modèle quelconque de $\mathsf{PA}_{\text{faible}}$. Il s'agit de montrer que

- $\mathcal{M}$ satisfait $\exists \boldsymbol{s},\boldsymbol{t}(\mathsf{F}(\boldsymbol{s},\boldsymbol{t},\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{k}}\mathbf{0},a))$ pour au plus un élément a de $\mathrm{Dom}(\mathcal{M})$, et
- $\mathcal{M}$ satisfait $\exists \boldsymbol{s},\boldsymbol{t}(\mathsf{F}(\boldsymbol{s},\boldsymbol{t},\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{k}}\mathbf{0},\boldsymbol{S}^{\mathsf{m}}\mathbf{0}))$ pour $\mathsf{m}=f(\vec{\mathsf{n}},\mathsf{k})$.

Supposons $\mathcal{M}\models\exists \boldsymbol{s},\boldsymbol{t}(\mathsf{F}(\boldsymbol{s},\boldsymbol{t},\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{k}}\mathbf{0},a)$. Il existe donc s,t et a_0 dans $\mathrm{Dom}(\mathcal{M})$ tel que $\mathcal{M}$ satisfasse

$$\begin{aligned}&(\mathsf{B}'(s,t,\mathbf{0},a_0)\text{ et }\mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},a_0))\\&\quad\wedge\forall \boldsymbol{x}_2{<}\,\boldsymbol{S}^{\mathsf{k}}\mathbf{0}\;\exists \boldsymbol{x}_3,\boldsymbol{x}_4\;(\mathsf{B}'(s,t,\boldsymbol{x}_2,\boldsymbol{x}_3)\wedge\mathsf{B}'(s,t,\boldsymbol{S}(\boldsymbol{x}_2),\boldsymbol{x}_4)\wedge\mathsf{H}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}(\boldsymbol{x}_2),\boldsymbol{x}_3,\boldsymbol{x}_4))\\&\quad\wedge\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{k}}\mathbf{0},\boldsymbol{z}).\end{aligned}$$

On montre par induction sur i que $\mathcal{M}$ satisfait $\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}}\mathbf{0},\boldsymbol{S}^{\mathsf{m_i}}\mathbf{0})$, où $\mathsf{m_i}$ est l'entier défini par (3.13). Pour $\mathsf{i}=0$, puisque $\mathcal{M}$ satisfait $\mathsf{G}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},a_0)$ et que G représente g, on doit avoir $a_0=(\boldsymbol{S}^{\mathsf{m}_0}\mathbf{0})^{\mathcal{M}}$ avec $\mathsf{m}_0=g(\vec{\mathsf{n}})$. Ensuite, pour chaque entier i entre 0 et $\mathsf{k}-1$, le système $\mathsf{PA}_{\text{faible}}$ prouve, donc le modèle $\mathcal{M}$ satisfait, $\boldsymbol{S}^{\mathsf{i}}\mathbf{0}{<}\boldsymbol{S}^{\mathsf{k}}\mathbf{0}$, et l'hypothèse que $\mathcal{M}$ satisfait le fragment central de la formule implique que, pour tout tel i, le modèle $\mathcal{M}$ satisfait

$$\exists \boldsymbol{x}\;\exists \boldsymbol{x}'\;(\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}}\mathbf{0},\boldsymbol{x})\wedge\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},\boldsymbol{x}')\wedge\mathsf{H}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},\boldsymbol{x},\boldsymbol{x}')).$$

Soient a,a' tels que $\mathcal{M}$ satisfait $\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}}\mathbf{0},a)$, $\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},a')$, et $\mathsf{H}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},a,a')$. Comme, par hypothèse d'induction, on a $\mathcal{M}\models\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}}\mathbf{0},\boldsymbol{S}^{\mathsf{m_i}}\mathbf{0})$, l'hypothèse additionnelle sur la formule B' établie dans le lemme 1.12 garantit $a=(\boldsymbol{S}^{\mathsf{m_i}}\mathbf{0})^{\mathcal{M}}$ [6]. Mais alors, $\mathsf{H}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},a,a')$, c'est-à-dire $\mathsf{H}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},\boldsymbol{S}^{\mathsf{m_i}}\mathbf{0},a')$, entraîne $a'=(\boldsymbol{S}^{\mathsf{m_{i+1}}}\mathbf{0})^{\mathcal{M}}$, et donc $\mathcal{M}\models\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}+1}\mathbf{0},\boldsymbol{S}^{\mathsf{m_{i+1}}}\mathbf{0})$, et la récurrence continue. A la fin, on obtient que a est nécessairement $(\boldsymbol{S}^{\mathsf{m}}\mathbf{0})^{\mathcal{M}}$, avec $\mathsf{m}=f(\vec{\mathsf{n}},\mathsf{k})$.

Le second point est facile. Toujours avec les mêmes notations, en choisissant deux entiers s,t vérifiant $\mathtt{beta}(\mathsf{s},\mathsf{t},\mathsf{i})=\mathsf{m_i}$ pour $0\leqslant\mathsf{i}\leqslant\mathsf{k}$, on obtient $\mathcal{M}\models\mathsf{F}(\boldsymbol{S}^{\mathsf{s}}\mathbf{0},\boldsymbol{S}^{\mathsf{t}}\mathbf{0},\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^{\mathsf{k}}\mathbf{0},\boldsymbol{S}^{\mathsf{m}}\mathbf{0})$. Le seul point à noter est l'utilisation de (3.7) pour passer de $(\boldsymbol{x}_2=\mathbf{0}\vee\ldots\vee\boldsymbol{x}_2=\boldsymbol{S}^{\mathsf{k}-1}\mathbf{0})\Rightarrow\ldots$ à $(\boldsymbol{x}_2<\boldsymbol{S}^{\mathsf{k}}\mathbf{0})\Rightarrow\ldots$. □

La démonstration de la proposition 3.13 est donc complète. On déduit un résultat analogue de représentabilité des relations récursives.

DÉFINITION 3.20. (représentable) On dit qu'une formule $\mathsf{F}(\boldsymbol{x}_1,...,\boldsymbol{x}_\mathsf{p})$ *représente* une relation R de $\mathbb{N}^\mathsf{p}$ dans une théorie T si, pour tous $\mathsf{n}_1,\ldots,\mathsf{n}_\mathsf{p}$ dans $\mathbb{N}$,

- T prouve $\mathsf{F}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0},...,\boldsymbol{S}^{\mathsf{n}_\mathsf{p}}\mathbf{0})$ lorsque $R(\mathsf{n}_1,...,\mathsf{n}_\mathsf{p})$ est vraie, et
- T prouve $\neg\mathsf{F}(\boldsymbol{S}^{\mathsf{n}_1}\mathbf{0},...,\boldsymbol{S}^{\mathsf{n}_\mathsf{p}}\mathbf{0})$ lorsque $R(\mathsf{n}_1,...,\mathsf{n}_\mathsf{p})$ est fausse.

COROLLAIRE 3.21. *Toute relation récursive sur $\mathbb{N}^\mathsf{p}$ est représentable dans le système $\mathsf{PA}_{\text{faible}}$ par une formule Σ_1.*

DÉMONSTRATION. Supposons que R est une relation récursive sur $\mathbb{N}^\mathsf{p}$. Alors la fonction indicatrice de R est une fonction récursive totale. Il existe donc une formule $\mathsf{F}(\vec{\boldsymbol{x}},\boldsymbol{y})$ de complexité Σ_1 représentant $\mathbf{1}_R$ dans $\mathsf{PA}_{\text{faible}}$. Soit $\mathsf{F}'(\vec{\boldsymbol{x}})$ la formule $\mathsf{F}(\vec{\boldsymbol{x}},\boldsymbol{S}^1\mathbf{0})$, et soit $\vec{\mathsf{n}}$ une suite d'entiers quelconque. Si $R(\vec{\mathsf{n}})$ est vraie, alors $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{F}(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0},\boldsymbol{S}^1\mathbf{0})$, donc $\mathsf{F}'(\boldsymbol{S}^{\vec{\mathsf{n}}}\mathbf{0})$. Si $R(\vec{\mathsf{n}})$

[6] Rien ne permet d'affirmer que s,t sont des éléments standards de $\mathcal{M}$: on ne peut donc pas affirmer que $\mathsf{B}'(s,t,\boldsymbol{S}^{\mathsf{i}}\mathbf{0},a)$ est satisfait pour un a au plus en général. Comme on ne peut pas introduire une suite de variables de longueur k puisque k est variable, et qu'on doit se contenter d'une sous-formule locale reliant les valeurs en i et en $\mathsf{i}+1$, l'unicité de la valeur en i est essentielle.

est fausse, alors $\mathsf{PA}_{\text{faible}}$ prouve $\mathsf{F}(\boldsymbol{S}^{\bar{n}}\mathbf{0}, \mathbf{0})$, et donc $\neg\mathsf{F}(\boldsymbol{S}^{\bar{n}}\mathbf{0}, \boldsymbol{S}^{1}\mathbf{0})$, soit $\neg\mathsf{F}'(\boldsymbol{S}^{\bar{n}}\mathbf{0})$, par définition de la représentabilité d'une fonction. □

4. Indécidabilité et incomplétude

▶ On démontre les théorèmes de limitation. D'abord, on établit une forme générique de l'argument diagonal appelée lemme diagonal mettant en jeu une formule d'arithmétique quelconque. Ensuite, en appliquant le lemme diagonal à trois formules convenablement choisies, on déduit successivement le théorème de Church sur l'indécidabilité de l'ensemble des formules valides, puis le théorème de Tarski sur la non-définissabilité de la vérité arithmétique, et enfin les théorèmes d'incomplétude de Gödel, le second ici sous une forme non optimale puisque démontré seulement pour les théories au moins aussi fortes que la théorie des ensembles, alors que l'arithmétique de Peano serait suffisante. ◀

▷ *Ayant fait provision de résultats préparatoires — en l'occurrence le seul résultat crucial est l'existence d'une numérotation des formules telle que la fonction de substitution associée soit représentable dans le système* $\mathsf{PA}_{\text{faible}}$ *par une formule* Σ_1 *— on en vient (enfin!) aux théorèmes de limitation qui constituent l'objet principal de ce chapitre. Ces théorèmes s'énoncent comme des résultats négatifs exprimant des limitations inhérentes à la logique du premier ordre, sur le modèle des célèbres théorèmes d'incomplétude de Gödel affirmant l'existence de formules vraies mais non prouvables. On constatera que les arguments techniques sont assez brefs, tous basés sur l'unique argument diagonal.* ◁

4.1. L'argument diagonal.

▶ On dégage ici sous le nom de lemme diagonal l'argument générique qui servira ensuite à établir tous les résultats ultérieurs du chapitre. ◀

▷ *Le lemme diagonal est une variation sur l'argument du même nom, et, comme toujours, il combine autoréférence et négation. L'autoréférence vient ici de la possibilité d'appliquer une formule de la logique* $\mathcal{L}_{\text{arith}}$ *à une (autre) formule via l'arithmétisation de la syntaxe : a priori, les formules d'arithmétique s'appliquent aux entiers, mais, une fois les formules numérotées par des entiers, rien n'empêche d'appliquer une formule au numéro d'une autre formule, et même — et c'est là que l'autoréférence arrive — à son propre numéro.*

Le principe est le suivant. Grâce à l'arithmétisation, on peut faire comme si les formules s'appliquaient aux formules, ou encore les entiers aux entiers. Soit $\mathsf{F}(\boldsymbol{x})$ *une formule d'arithmétique quelconque. Si on pose* $\mathsf{F}'(\boldsymbol{x}) := \mathsf{F}(\boldsymbol{x}(\boldsymbol{x}))$*, et* $\Delta := \neg\mathsf{F}'(\neg\mathsf{F}')$*, alors on a l'« égalité »*

$$\mathsf{F}(\Delta) = \mathsf{F}(\neg\mathsf{F}'(\neg\mathsf{F}')) = \mathsf{F}'(\neg\mathsf{F}') = \neg\Delta.$$

De la sorte, Δ *est une formule qui, vis-à-vis de* F*, est (équivalente à) sa propre négation. En particulier, si* $\mathsf{F}(\boldsymbol{x})$ *signifie «* $\boldsymbol{x}$ *est vrai », alors* $\mathsf{F}'(\boldsymbol{x})$ *signifie quelque chose comme «* $\boldsymbol{x}$ *est vraiment vrai », et* Δ *affirme sa propre fausseté, et, de ce fait, ne peut être ni vraie, ni fausse, sur le modèle du paradoxe du menteur qui constate qu'on ne peut attribuer raisonnablement de valeur de vérité à la phrase « Je mens ». De même, si* $\mathsf{F}(\boldsymbol{x})$ *signifie «* $\boldsymbol{x}$ *est prouvable », alors* $\mathsf{F}'(\boldsymbol{x})$ *signifie quelque chose comme «* $\boldsymbol{x}$ *est prouvablement prouvable », et* Δ *affirme sa propre non-prouvabilité.* ◁

Dans toute la suite, l'expression formule d'arithmétique réfère à une formule de la logique $\mathcal{L}_{\text{arith}^+}$, c'est-à-dire une formule du premier ordre vis-à-vis de la signature $(\mathbf{0}, \boldsymbol{S}, +, \cdot, \leqslant)$.

PROPOSITION 4.1. (lemme diagonal) *Soit* $\mathsf{G}(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})$ *une formule* Σ_1 *de* $\mathcal{L}_{\text{arith}^+}$ *représentant la fonction* `subst` *dans* $\mathsf{PA}_{\text{faible}}$. *Pour toute formule* $\mathsf{F}(\boldsymbol{x}_1)$ *de* $\mathcal{L}_{\max}$ *à une variable libre, soit* $\text{Diag}(\mathsf{F})$ *la formule close* $\neg\mathsf{H}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})$, *où* $\mathsf{H}(\boldsymbol{x})$ *est la formule* $\exists\boldsymbol{z}(\mathsf{G}(\boldsymbol{x},\boldsymbol{x},\boldsymbol{z})\wedge\mathsf{F}(\boldsymbol{z}))$ *et où* n *est l'entier* $\ulcorner\neg\mathsf{H}(\boldsymbol{x})\urcorner$. *Alors, pour toute* F, *on a*

$$\mathsf{PA}_{\text{faible}}\vdash\mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})\Leftrightarrow\neg\Delta, \tag{4.1}$$

où Δ *est* $\text{Diag}(\mathsf{F})$. *De plus, si* $\mathsf{F}(\boldsymbol{x}_1)$ *est une formule* Σ_1, *alors* $\text{Diag}(\mathsf{F})$ *est la négation d'une formule* Σ_1.

DÉMONSTRATION. La fonction G existe d'après le corollaire 2.5 et la proposition 3.13. Soit $\mathsf{F}(\boldsymbol{x}_1)$ une formule de $\mathcal{L}_{\max}$ à une variable libre. Ecrivant Δ pour $\text{Diag}(\mathsf{F})$, on a par définition

$$\Delta=\neg\,\exists\boldsymbol{z}\,(\mathsf{G}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{z})\wedge\mathsf{F}(\boldsymbol{z})),$$

ce qui montre que, si F est de complexité Σ_1, alors Δ est la négation d'une formule Σ_1. Par le théorème de complétude, il suffit pour établir l'équivalence (4.1) de montrer que tout modèle de $\mathsf{PA}_{\text{faible}}$ satisfaisant $\mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$ satisfait $\neg\Delta$, et que tout modèle de $\mathsf{PA}_{\text{faible}}$ satisfaisant $\neg\Delta$ satisfait $\mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$.

Par construction, on a $\ulcorner\Delta\urcorner=\ulcorner\neg\mathsf{H}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})\urcorner=\mathtt{subst}(\mathsf{n},\mathsf{n})$, et, par conséquent, puisque la formule G représente la fonction `subst` dans $\mathsf{PA}_{\text{faible}}$, on a

$$\mathsf{PA}_{\text{faible}}\vdash\mathsf{G}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0}), \tag{4.2}$$

$$\mathsf{PA}_{\text{faible}}\vdash\forall\boldsymbol{z}(\mathsf{G}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{z})\Rightarrow\boldsymbol{z}=\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0}). \tag{4.3}$$

Supposons que $\mathcal{M}$ est modèle de $\mathsf{PA}_{\text{faible}}$ et satisfait $\mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$. Par (4.2), $\mathcal{M}$ satisfait aussi $\mathsf{G}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$, donc il existe c, à savoir $(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})^{\mathcal{M}}$, tel que $\mathcal{M}$ satisfait $\mathsf{G}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\mathsf{n}}\mathbf{0},c)\wedge\mathsf{F}(c)$. Donc $\mathcal{M}$ satisfait $\neg\Delta$.

Inversement, supposons que $\mathcal{M}$ est modèle de $\mathsf{PA}_{\text{faible}}$ et satisfait $\neg\Delta$. Il existe donc dans le domaine de $\mathcal{M}$ un élément c satisfaisant $\mathsf{G}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0},\boldsymbol{S}^{\mathsf{n}}\mathbf{0},c)$ et $\mathsf{F}(c)$. D'après (4.3), l'élément c est forcément $(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})^{\mathcal{M}}$, et l'hypothèse que $\mathcal{M}$ satisfait $\mathsf{F}(c)$ signifie que $\mathcal{M}$ satisfait $\mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$. □

4.2. Le théorème de non-définissabilité de la vérité de Tarski.

▶ Une première application, très simple, du lemme diagonal est le théorème de Tarski qui affirme l'impossibilité de définir de façon interne la vérité dans toute structure qui est modèle de $\mathsf{PA}_{\text{faible}}$, donc en particulier dans la structure $(\mathbb{N},0,S,+,\cdot,\leqslant)$. On en déduit une forme faible du mremier théorème d'incomplétude, ainsi que l'inexistence de toute notion de preuve donnant lieu à un théorème de complétude pour la logique du second ordre. ◀

▷ *On pourra noter que le théorème de Tarski apporte une réfutation forte au paradoxe de Richard-Berry, en montrant qu'on ne saurait, de l'intérieur de la structure* $(\mathbb{N},0,S,+,\cdot,\leqslant)$, *parler de ce qui y est vrai, donc en particulier de ce qui y est définissable.* ◁

PROPOSITION 4.2. (non-définissabilité de la vérité) *Supposons que* Σ *est une signature finie ou dénombrable incluant* Σ_{arith^+} *et que* $\mathcal{M}$ *est une structure de type* Σ *qui est modèle de* $\mathsf{PA}_{\text{faible}}$. *Alors l'ensemble des numéros des formules de* $\mathcal{L}_\Sigma$

vraies dans $\mathcal{M}$ n'est pas définissable dans $\mathcal{M}$: il n'existe pas de formule $\mathrm{Sat}_{\mathcal{M}}(\boldsymbol{x})$ *de* $\mathcal{L}_\Sigma$ *telle que, pour toute formule close* F *de* $\mathcal{L}_\Sigma$*, on ait*

$$\mathcal{M} \models \mathsf{F} \quad \Leftrightarrow \quad \mathcal{M} \models \mathrm{Sat}_{\mathcal{M}}(\boldsymbol{S}^{\ulcorner \mathsf{F} \urcorner}\mathbf{0}). \tag{4.4}$$

Démonstration. Sans perte de généralité, on peut supposer $\Sigma \subseteq \Sigma_{\max}$. Supposons que $\mathrm{Sat}_{\mathcal{M}}(\boldsymbol{x})$ satisfait l'équivalence (4.4). Soit $\Delta = \mathrm{Diag}(\mathrm{Sat}_{\mathcal{M}})$. On a donc par hypothèse

$$\mathsf{PA}_{\text{faible}} \vdash \mathrm{Sat}_{\mathcal{M}}(\boldsymbol{S}^{\ulcorner \Delta \urcorner}\mathbf{0}) \Leftrightarrow \neg\Delta,$$

donc, puisque $\mathcal{M}$ est modèle de $\mathsf{PA}_{\text{faible}}$,

$$\mathcal{M} \models \mathrm{Sat}_{\mathcal{M}}(\boldsymbol{S}^{\ulcorner \Delta \urcorner}\mathbf{0}) \Leftrightarrow \neg\Delta. \tag{4.5}$$

Par construction, la formule close Δ est soit vraie, soit fausse dans $\mathcal{M}$. Or, de façon évidente, les équivalences (4.4) et (4.5) se contredisent. En effet, Si Δ est vraie, (4.5) implique $\mathcal{M} \not\models \mathrm{Sat}_{\mathcal{M}}(\boldsymbol{S}^{\ulcorner \Delta \urcorner}\mathbf{0})$, d'où $\mathcal{M} \not\models \Delta$ par (4.4), ce qui contredit l'hypothèse. Si Δ est fausse,(4.5) implique $\mathcal{M} \models \mathrm{Sat}_{\mathcal{M}}(\boldsymbol{S}^{\ulcorner \Delta \urcorner}\mathbf{0})$, d'où $\mathcal{M} \models \Delta$ par (4.4), à nouveau une contradiction. C'est donc que l'hypothèse de l'existence de la formule $\mathrm{Sat}_{\mathcal{M}}$ est intenable. □

Corollaire 4.3. *Il n'existe pas de formule* $\mathrm{Sat}_{\mathbb{N}}(\boldsymbol{x})$ *de* $\mathcal{L}_{\mathrm{arith}^+}$ *telle que, pour toute formule close* F *de* $\mathcal{L}_{\mathrm{arith}^+}$*, on ait*

$$(\mathbb{N}, 0, S, +, \cdot, \leqslant) \models \mathsf{F} \quad \Leftrightarrow \quad (\mathbb{N}, 0, S, +, \cdot, \leqslant) \models \mathrm{Sat}_{\mathbb{N}}(\ulcorner \mathsf{F} \urcorner). \tag{4.6}$$

Démonstration. Dans le cas particulier de la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, l'interprétation du terme $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ est, par définition, l'entier n lui-même. □

On déduit du théorème de Tarski plusieurs applications. La première est que la théorie du premier ordre de $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ est un ensemble compliqué, au sens où il ne saurait être récursif, ni même semi-récursif

Lemme 4.4. (semi-récursif) *Tout sous-ensemble semi-récursif de* $\mathbb{N}^{\mathsf{p}}$ *dont le complémentaire est semi-récursif est récursif.*

Démonstration. On suppose que S est la projection sur $\mathbb{N}^{\mathsf{p}}$ d'un ensemble récursif R_+ de $\mathbb{N}^{\mathsf{q}}$, et que $\mathbb{N}^{\mathsf{p}} \setminus S$ est la projection d'un ensemble récursif R_- de $\mathbb{N}^{\mathsf{r}}$. Quitte à remplacer R_+ ou R_- par son produit avec une puissance convenable de $\mathbb{N}$, on peut supposer $\mathsf{r} = \mathsf{q}$. La fonction $\mathbf{1}_{R_+} + \mathbf{1}_{R_-}$ est récursive totale, et il en est de même de la fonction f qui à $\vec{\mathsf{n}}$ associe le plus petit m tel que $\mathbf{1}_{R_+}(\vec{\mathsf{n}}, \mathsf{m}) + \mathbf{1}_{R_-}(\vec{\mathsf{n}}, \mathsf{m})$ vaut 1 : la fonction f est récursive puisqu'elle se définit comme $\mathtt{min}(\mathtt{comp}(\mathbf{1}_{\{1\}}, \mathtt{comp}(\mathtt{add}, \mathbf{1}_{R_+}, \mathbf{1}_{R_-})))$, et elle est totale puisque la réunion des projections de R_+ et R_- est $\mathbb{N}^{\mathsf{p}}$. On a alors $\mathbf{1}_S(\vec{\mathsf{n}}) = \mathbf{1}_{R_+}(\vec{\mathsf{n}}, f(\vec{\mathsf{n}}))$, ce qui montre que $\mathbf{1}_S$ est une fonction récursive, et donc que S est récursif. □

Proposition 4.5. (indécidabilité) *L'ensemble* $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *n'est pas semi-récursif.*

Démonstration. Supposons que $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ est semi-récursif. Par construction, $\mathsf{F} \notin \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ équivaut à $\neg\mathsf{F} \in \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, donc le complémentaire dans $\mathbb{N}$ de $\ulcorner \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant) \urcorner$ est également semi-récursif. Par le lemme 4.4, il en résulte que l'ensemble $\ulcorner \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant) \urcorner$ est récursif, donc, par le corollaire 3.21, représentable dans $\mathsf{PA}_{\text{faible}}$ par une formule $\mathsf{G}(\boldsymbol{x})$. Ceci signifie que, pour toute formule F close, $(\mathbb{N}, 0, S, +, \cdot, \leqslant) \models \mathsf{F}$, c'est-à-dire $\ulcorner \mathsf{F} \urcorner \in \ulcorner \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant) \urcorner$, équivaut à $(\mathbb{N}, 0, S, +, \cdot, \leqslant) \models \mathsf{G}(\ulcorner \mathsf{F} \urcorner)$. C'est dire que G satisfait à l'équivalence (4.4), ce qui contredit le théorème de Tarski. □

La seconde application est une forme faible du premier théorème d'incomplétude de Gödel dans laquelle on n'exhibe pas de formule non prouvable explicite.

PROPOSITION 4.6. (premier théorème d'incomplétude, forme faible) *Supposons que* T *est une théorie récursive incluse dans* $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$. *Alors il existe une formule vraie dans* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *mais non prouvable à partir de* T.

DÉMONSTRATION. Soit $\widehat{\mathsf{T}}$ l'ensemble des formules closes prouvables à partir de T. Toute formule close de $\widehat{\mathsf{T}}$ est satisfaite dans $(\mathbb{N}, 0, S, +, \cdot)$, donc on a $\widehat{\mathsf{T}} \subseteq \mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$. Par le lemme 2.11, $\widehat{\mathsf{T}}$ est semi-récursif. Comme $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$ n'est pas semi-récursif, l'inclusion de $\widehat{\mathsf{T}}$ dans $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot)$ doit être stricte, ce qui signifie qu'il existe une formule close F vraie dans $(\mathbb{N}, 0, S, +, \cdot)$ et non prouvable à partir de T. □

Noter que le résultat s'applique en particulier au système de Peano PA_1, puisque ce dernier est un ensemble (primitif) récursif, ainsi qu'on l'a vu dans l'exemple 2.9 (*cf.* corollaire 4.15 ci-dessous). Une autre application est qu'il ne peut exister de notion satisfaisante de prouvabilité pour la logique du second ordre.

PROPOSITION 4.7. (second ordre) *Il ne peut pas exister de notion de preuve en logique du second ordre telle que l'ensemble des numéros des formules prouvables forme un ensemble semi-récursif et telle que toute formule valide soit prouvable.*

DÉMONSTRATION. Le système PA complété de $\mathsf{Def}_{\leqslant}$ est équivalent à l'unique formule du second ordre H qui est la conjonction des sept formules de la définition III.1.8 et de $\mathsf{Def}_{\leqslant}$. D'après la proposition VII.4.5, le seul modèle de H est la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, et donc dire qu'une formule close F est vraie dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ équivaut à dire que la formule $\mathsf{H}\Rightarrow\mathsf{F}$ est valide. S'il existait une notion de preuve vérifiant les conditions de la proposition, ceci équivaudrait à dire que $\mathsf{H}\Rightarrow\mathsf{F}$ est prouvable, et il en résulterait que $\mathrm{Th}_2(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ serait semi-récursif, puis *a fortiori* que $\mathrm{Th}_1(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ le serait, contredisant la proposition 4.5. □

▷ *Le résultat précédent explique l'intérêt spécifique de la logique du premier ordre comparée à celle du second ordre. En logique du premier ordre, il existe une notion de preuve suffisamment simple pour que les formules prouvables forment une famille explicitement énumérable, et en même temps suffisamment riche pour que toutes les formules valides soient prouvables. En logique du second ordre, il ne peut exister de notion de preuve réunissant ces deux vertus antagonistes : si une notion de preuve était suffisamment riche pour qu'il y ait complétude, alors elle devrait être trop compliquée pour que l'ensemble des formules prouvables puisse être énuméré effectivement. Autrement dit, il ne peut exister de bonne notion de preuve en logique du second ordre.* ◁

4.3. Le théorème d'indécidabilité de Church.

► Une autre application du lemme diagonal est le théorème d'indécidabilité de Church affirmant que l'ensemble des formules d'arithmétique prouvables à partir de $\mathsf{PA}_{\text{faible}}$, ainsi que l'ensemble des formules d'arithmétique valides, sont des ensembles non récursifs. ◄

▷ *Moyennant la thèse de Church–Turing, le théorème de Church signifie qu'il n'existe pas de moyen algorithmique permettant de décider si une formule d'arithmétique est ou non prouvable à partir de* $\mathsf{PA}_{\text{faible}}$*, ou encore soit valide, c'est-à-dire prouvable à partir des seuls axiomes de la logique* $\mathcal{L}_{\text{arith}^+}$. *On notera que le théorème ne dit* rien *quant à une formule particulière : ce qu'il affirme, c'est qu'il ne saurait exister de méthode uniforme permettant de décider, pour* toute

formule d'arithmétique F*, si* F *est ou non valide, autrement dit, il n'existe pas de recette miracle marchant pour toutes les formules à la fois.* ◁

On rappelle qu'un ensemble de formules T est dit récursif si l'ensemble des numéros des formules appartenant à T est un ensemble récursif d'entiers.

PROPOSITION 4.8. (indécidabilité) *Supposons que* T *est un ensemble consistant de formules d'arithmétique incluant* $\mathsf{PA}_{\text{faible}}$*. Alors l'ensemble des formules prouvables à partir de* T *n'est pas récursif.*

DÉMONSTRATION. Soit $\widehat{\mathsf{T}}$ l'ensemble de toutes les formules de $\mathcal{L}_{\text{arith}^+}$ prouvables à partir de T. Supposons $\widehat{\mathsf{T}}$ récursif. Par le corollaire 3.21, il existe une formule $\mathsf{F}(\boldsymbol{x})$ représentant $\ulcorner\widehat{\mathsf{T}}\urcorner$ (vue comme relation unaire) dans $\mathsf{PA}_{\text{faible}}$. Soit $\Delta = \text{Diag}(\mathsf{F})$. Par construction on a donc

$$\mathsf{PA}_{\text{faible}} \vdash \mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0}) \Leftrightarrow \neg\Delta. \tag{4.7}$$

On se demande si Δ est ou non prouvable à partir de T.

Supposons $\mathsf{T} \vdash \Delta$. Cela signifie que $\ulcorner\Delta\urcorner$ est dans $\ulcorner\widehat{\mathsf{T}}\urcorner$, et l'hypothèse que F représente $\ulcorner\widehat{\mathsf{T}}\urcorner$ dans $\mathsf{PA}_{\text{faible}}$ implique $\mathsf{PA}_{\text{faible}} \vdash \mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$. En utilisant (4.7) et une coupure, on déduit $\mathsf{PA}_{\text{faible}} \vdash \neg\Delta$, et donc *a fortiori* $\mathsf{T} \vdash \neg\Delta$, ce qui contredit la consistance de T.

Supposons maintenant $\mathsf{T} \nvdash \Delta$. Alors $\ulcorner\Delta\urcorner$ n'est pas dans $\ulcorner\widehat{\mathsf{T}}\urcorner$, et l'hypothèse que F représente $\ulcorner\widehat{\mathsf{T}}\urcorner$ dans $\mathsf{PA}_{\text{faible}}$ implique $\mathsf{PA}_{\text{faible}} \vdash \neg\mathsf{F}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$. Par (4.7), on déduit $\mathsf{PA}_{\text{faible}} \vdash \Delta$, donc $\mathsf{T} \vdash \Delta$, ce qui contredit l'hypothèse $\mathsf{T} \nvdash \Delta$. L'hypothèse que $\widehat{\mathsf{T}}$ est récursif — et même plus généralement l'hypothèse que $\ulcorner\widehat{\mathsf{T}}\urcorner$ est représentable dans $\mathsf{PA}_{\text{faible}}$ — est donc contradictoire. □

COROLLAIRE 4.9. *Si* T *est un ensemble récursif et consistant de formules d'arithmétique incluant* $\mathsf{PA}_{\text{faible}}$*, alors l'ensemble des formules prouvables à partir* T *est un ensemble semi-récursif non récursif.*

DÉMONSTRATION. Comme ci-dessus, soit $\widehat{\mathsf{T}}$ l'ensemble des formules prouvables à partir de T. Alors, par le corollaire 2.11, $\widehat{\mathsf{T}}$ est semi-récursif, et, par la proposition 4.8, il est non récursif. □

Une seconde application est l'impossibilité d'un algorithme permettant de reconnaître les formules de $\mathcal{L}_{\text{arith}^+}$ qui sont valides :

COROLLAIRE 4.10. *L'ensemble des formules de* $\mathcal{L}_{\text{arith}^+}$ *qui sont valides — c'est-à-dire satisfaites dans toute réalisation — est semi-récursif et non récursif.*

DÉMONSTRATION. D'après le théorème de complétude, une formule de $\mathcal{L}_{\text{arith}^+}$ est valide si et seulement si elle est prouvable à partir d'un ensemble vide d'hypothèses. Avec les notations précédentes, l'ensemble des formules valides est donc $\widehat{\emptyset}$ et, par le corollaire 2.11, cet ensemble est semi-récursif puisque l'ensemble vide l'est.

Notons alors H la formule de $\mathcal{L}_{\text{arith}^+}$ qui est la conjonction des axiomes constituant $\mathsf{PA}_{\text{faible}}$. D'après le théorème de la déduction, il y a équivalence, pour toute formule F de $\mathcal{L}_{\text{arith}^+}$, entre $\mathsf{PA}_{\text{faible}} \vdash \mathsf{F}$, c'est-à-dire $\{\mathsf{H}\} \vdash \mathsf{F}$, et $\vdash \mathsf{H}\Rightarrow\mathsf{F}$, c'est-à-dire l'appartenance de $\mathsf{H}\Rightarrow\mathsf{F}$ à $\widehat{\emptyset}$. Soit f la fonction primitive récursive définie par $f(\mathsf{n}) := \langle\ulcorner\Rightarrow\urcorner, \ulcorner\mathsf{H}\urcorner, \mathsf{n}\rangle$. Pour toute formule F, on a $f(\ulcorner\mathsf{F}\urcorner) = \ulcorner\mathsf{H}\Rightarrow\mathsf{F}\urcorner$, et donc $\mathsf{n} \in \ulcorner\widehat{\mathsf{PA}_{\text{faible}}}\urcorner$ équivaut à $f(\mathsf{n}) \in \ulcorner\widehat{\emptyset}\urcorner$. Donc, si l'ensemble $\widehat{\emptyset}$ était récursif, il en serait de même de l'ensemble $\widehat{\mathsf{PA}_{\text{faible}}}$, ce qui contredit la proposition 4.8. □

▷ *Le résultat précédent exprime formellement que la logique du premier ordre n'est pas triviale. Si les formules valides se limitaient à des évidences du genre* $\boldsymbol{x} = \boldsymbol{y} \Rightarrow \boldsymbol{y} = \boldsymbol{x}$*, on s'attendrait*

à ce qu'elles puissent être décrites simplement, et donc à ce que l'ensemble des numéros des formules valides soit simple, donc en particulier récursif.

On peut noter que le caractère récursif ou non de l'ensemble des numéros des formules valides d'une logique $\mathcal{L}_\Sigma$ dépend du pouvoir d'expression de $\mathcal{L}_\Sigma$, et donc de la signature Σ. On vient de voir que, si Σ est la signature Σ_{arith^+} de l'arithmétique, alors l'ensemble des numéros des formules valides est non récursif. Avec un peu de travail supplémentaire, on peut éliminer les symboles d'opération et obtenir le même résultat dès que la signature contient au moins un symbole de relation binaire. Par contre que, si une signature Σ ne contient que des symboles de relation unaire et pas de symbole d'opération, alors le pouvoir d'expression de $\mathcal{L}_\Sigma$ est faible et, dans ce cas, l'ensemble des numéros des formules valides de $\mathcal{L}_\Sigma$ est récursif. ◁

4.4. Le premier théorème d'incomplétude de Gödel.

► On établit le premier théorème d'incomplétude en appliquant le lemme diagonal non plus à la notion sémantique de satisfaction, mais à la notion syntaxique de prouvabilité. ◄

Si T est une théorie récursive, alors, par la proposition 2.8, la relation $\mathtt{Preuve}_\mathsf{T}$ est récursive, et donc, par le corollaire 3.21, elle est représentable dans $\mathsf{PA}_{\text{faible}}$ par une formule de complexité Σ_1.

Définition 4.11. (prouvabilité) Supposons que T est une théorie récursive de $\mathcal{L}_{\max}$. On fixe une formule $\mathrm{Pr}_\mathsf{T}(\boldsymbol{x},\boldsymbol{y})$ de complexité Σ_1 représentant la relation $\mathtt{Preuve}_\mathsf{T}(\mathsf{n},\mathsf{m})$ dans $\mathsf{PA}_{\text{faible}}$, et on note $\Box_\mathsf{T}(\boldsymbol{x})$ la formule $\exists\boldsymbol{y}(\mathrm{Pr}_\mathsf{T}(\boldsymbol{x},\boldsymbol{y}))$.

▷ *La formule $\Box_\mathsf{T}(\boldsymbol{x})$ code la prouvabilité de $\boldsymbol{x}$ à partir de T. Par construction, dans la structure $(\mathbb{N},0,S,+,\cdot,\leqslant)$, la formule $\Box_\mathsf{T}$ correspond à la notion de prouvabilité à partir de T : pour toute formule close F, il y a équivalence entre $\mathsf{T}\vdash\mathsf{F}$ et $\mathbb{N}\models\Box_\mathsf{T}(\ulcorner\mathsf{F}\urcorner)$ — voir néanmoins la note **??** ci-dessous. Par contre, dans un modèle non-standard de $\mathsf{PA}_{\text{faible}}$, la situation peut être différente : les éléments non-standards peuvent coder des preuves ne correspondant à aucune preuve standard, et on ne peut rien conclure en général.* ◁

Définition 4.12. (formule de Gödel) Pour toute théorie récursive T incluant $\mathsf{PA}_{\text{faible}}$, on pose $\Delta_\mathsf{T} := \mathrm{Diag}(\Box_\mathsf{T})$, et on appelle Δ_T la *formule de Gödel* associée à T.

▷ *On va établir une nouvelle version du premier théorème d'incomplétude de Gödel, qui se distingue de la proposition 4.6 en ce que, cette fois, on exhibe pour chaque système T une formule vraie dans $(\mathbb{N},0,S,+,\cdot,\leqslant)$ mais non prouvable à partir de T. Afin de donner l'énoncé sous une forme complète, on va introduire le contexte de la ω-logique, qui est le renforcement de la logique du premier ordre obtenu en ajoutant une nouvelle règle de déduction appelée ω-règle.* ◁

Définition 4.13. (ω-logique) Soit Σ une signature incluant Σ_{arith}. On appelle *ω-règle* l'opération (infinitaire) consistant à déduire $\forall\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$ de la conjonction des formules $\mathsf{F}(\mathbf{0})$, $\mathsf{F}(\boldsymbol{S}\mathbf{0})$, $\mathsf{F}(\boldsymbol{S}^2\mathbf{0})$... On note $\vdash_\omega$ la relation de prouvabilité obtenue en ajoutant la ω-règle aux règles de la logique du premier ordre. Une théorie T est dite ω-consistante s'il n'existe pas de formule F telle qu'on ait à la fois $\mathsf{T}\vdash_\omega\mathsf{F}$ et $\mathsf{T}\vdash_\omega\neg\mathsf{F}$.

PROPOSITION 4.14. (premier théorème d'incomplétude de Gödel) *Soit* T *une théorie récursive consistante incluant* $\mathsf{PA}_{\text{faible}}$. *Alors :*

(*i*) *La formule* Δ_{T} *est satisfaite dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$;

(*ii*) *La théorie* T *ne prouve pas* Δ_{T} ;

(*iii*) *De plus, si* T *est* ω*-consistante, alors* T *ne prouve pas non plus* $\neg\Delta_{\mathsf{T}}$.

DÉMONSTRATION. Dans toute la suite, on écrit Δ pour Δ_{T}, et on pose $\mathsf{n} := \ulcorner\Delta\urcorner$. Par hypothèse on a

$$\mathsf{PA}_{\text{faible}} \vdash \Box_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}) \Leftrightarrow \neg\Delta. \tag{4.8}$$

(*i*) Supposons $(\mathbb{N}, 0, S, +, \cdot, \leqslant) \not\models \Delta$. Alors, par (4.8), $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ satisfait $\Box_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})$, et il existe un entier p tel que $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ satisfait la formule $\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \mathsf{p})$. Par construction, cet entier p est le numéro d'une preuve de Δ à partir de T, et on a donc $\mathsf{T} \vdash \Delta$, d'où $(\mathbb{N}, 0, S, +, \cdot, \leqslant) \models \Delta$, contredisant l'hypothèse. Par conséquent, la seule possibilité est que $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ satisfasse Δ.

(*ii*) Supposons $\mathsf{T} \vdash \Delta$. Soit p le numéro d'une preuve de Δ à partir de T. Alors la relation $\mathtt{Preuve}_{\mathsf{T}}(\ulcorner\Delta\urcorner, \mathsf{p})$ est vraie dans $\mathbb{N}$, donc, puisque la formule Pr_{T} représente la relation $\mathtt{Preuve}_{\mathsf{T}}$ dans $\mathsf{PA}_{\text{faible}}$, le système $\mathsf{PA}_{\text{faible}}$ prouve $\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0})$, donc, *a fortiori*, $\exists\boldsymbol{y}(\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{y}))$, c'est-à-dire $\Box_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})$. Par (4.8), on en déduit que $\mathsf{PA}_{\text{faible}}$, donc *a fortiori* T, prouvent $\neg\Delta$, et, de là, que T prouve à la fois Δ et $\neg\Delta$, donc n'est pas consistante.

(*iii*) Supposons $\mathsf{T} \vdash \neg\Delta$. Toujours par (4.8), on en déduit que T prouve $\Box_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})$, c'est-à-dire $\exists\boldsymbol{y}(\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{y}))$. En vertu de (*ii*), T ne prouve pas Δ, et, par conséquent, il ne peut exister aucun entier naturel p tel que p soit le numéro d'une preuve de Δ à partir de T. Donc, pour chaque entier naturel p, la relation $\mathtt{Preuve}_{\mathsf{T}}(\mathsf{n}, \mathsf{p})$ est fausse, et, de là, par définition de la représentabilité, $\mathsf{PA}_{\text{faible}}$ prouve $\neg\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0})$. Par la ω-règle, on en déduit que $\mathsf{PA}_{\text{faible}}$ prouve la formule $\forall\boldsymbol{y}(\neg\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{y}))$, et, de là par les règles usuelles de la logique du premier ordre, que $\mathsf{PA}_{\text{faible}}$, et *a fortiori* T, prouvent la formule équivalente $\neg\,\exists\boldsymbol{y}\,(\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0}, \boldsymbol{y}))$, qui est $\neg\Box_{\mathsf{T}}(\boldsymbol{S}^{\mathsf{n}}\mathbf{0})$, puis, par (4.8), Δ. Au total, on a donc établi la relation $\mathsf{T} \vdash_{\omega} \Delta$. Par ailleurs, l'hypothèse $\mathsf{T} \vdash \neg\Delta$ implique, *a fortiori*, $\mathsf{T} \vdash_{\omega} \neg\Delta$, et on conclut que T n'est pas ω-consistante. □

▷ *J.B. Rosser a montré comment passer — par une astuce voisine de celle utilisée pour passer de* B *à* B' *dans la démonstration du lemme 3.18 — de* $\Box_{\mathsf{T}}$ *à une formule* $\Box'_{\mathsf{T}}$ *telle que, si* Δ'_{T} *est la formule qu'on en déduit par le lemme diagonal, alors* T *ne prouve ni* Δ'_{T}, *ni* $\neg\Delta'_{\mathsf{T}}$ *sous l'hypothèse que* T *est simplement consistante, et non nécessairement* ω*-consistante.*

Dans le cas présent, la dissymétrie entre Δ *et sa négation provient de l'impossibilité de passer automatiquement de* $\mathsf{T} \vdash \Box_{\mathsf{T}}(\ulcorner\mathsf{F}\urcorner)$ *à* $\mathsf{T} \vdash \mathsf{F}$, *et c'est là qu'on utilise l'hypothèse, a priori plus forte, que* T *est* ω*-consistante, et pas seulement consistante. Le problème est le suivant. S'il existe un entier (standard)* p *tel que* $\mathsf{PA}_{\text{faible}}$ *prouve* $\mathrm{Pr}_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\mathsf{F}\urcorner}\mathbf{0}, \boldsymbol{S}^{\mathsf{p}}\mathbf{0})$, *alors on peut déduire que* $\mathsf{PA}_{\text{faible}}$ *prouve* F, *mais, d'une façon générale,* $\mathsf{PA}_{\text{faible}} \vdash \exists\boldsymbol{y}(\mathsf{F}(\boldsymbol{y}))$ *n'a aucune raison de garantir l'existence d'un entier* p *vérifiant* $\mathsf{PA}_{\text{faible}} \vdash \mathsf{F}(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})$ *: si* $\mathcal{M}$ *est un modèle de* $\mathsf{PA}_{\text{faible}}$ *vérifiant* $\mathsf{PA}_{\text{faible}} \vdash \exists\boldsymbol{y}(\mathsf{F}(\boldsymbol{y}))$, *il doit bien exister un élément* b *du domaine de* $\mathcal{M}$ *tel que* $\mathcal{M}$ *vérifie* $\mathsf{F}(b)$, *mais* b *peut être non-standard, c'est-à-dire distinct de* $(\boldsymbol{S}^{\mathsf{p}}\mathbf{0})^{\mathcal{M}}$ *pour tout entier* p.

Un point peut paraître paradoxal. Dans le point (*i*) *de la proposition 4.14, on affirme que la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *satisfait la formule* Δ_{T}. *Il pourrait sembler alors évident que cela implique que* T *ne prouve pas* $\neg\Delta_{\mathsf{T}}$, *puisqu'une formule prouvable doit être satisfaite dans toute structure. L'argument est correct, mais il repose sur le fait que* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *est un modèle de l'arithmétique, et, plus exactement, sur le fait qu'il existe un modèle de l'arithmétique tel que tous les éléments du domaine soient de la forme* $\boldsymbol{S}^{\mathsf{n}}\mathbf{0}$ — *autrement dit sur l'existence d'un modèle standard pour* $\mathsf{PA}_{\text{faible}}$, *que ne réclame pas la démonstration de* (*i*) *par exemple. Pour clarifier ce point, on peut recourir au formalisme de la section VII.4 qui réfère explicitement au cadre métamathématique. Si* $(\mathsf{T}^{\star}, \vdash^{\star})$ *est le cadre métamathématique formel, alors, par définition,*

établir une relation $(\mathbb{N},0,S,+,\cdot,\leqslant)\models\forall\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))$ *revient à montrer la relation* $(\mathbb{N},0,S,+,\cdot,\leqslant)\models\mathsf{F}(\mathsf{p})$ *pour chaque entier naturel* p*, donc, formellement, à établir la relation*

$$\mathsf{T}^\star\vdash^\star\ \forall\mathsf{p}\ (\text{« }(\mathbb{N},0,S,+,\cdot,\leqslant)\models\mathsf{F}(\mathsf{p})\text{ »}). \tag{4.9}$$

La question est de savoir si cette condition est suffisante pour en déduire

$$\mathsf{T}^\star\vdash^\star\text{« }(\mathbb{N},0,S,+,\cdot,\leqslant)\models\forall\boldsymbol{x}(\mathsf{F}(\boldsymbol{x}))\text{ ».} \tag{4.10}$$

Si la notion de prouvabilité ambiante inclut la ω*-règle, c'est-à-dire si* $\vdash^\star$ *est* $\vdash_\omega$ *ou une extension de celle-ci, alors il est légitime de passer de* (4.9) *à* (4.10)*. Sinon, le passage est a priori impossible. En termes de prouvabilité, cela signifie qu'on peut passer de* $\mathsf{T}^\star\vdash\text{« }\mathsf{PA}_{\text{faible}}\vdash\Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\mathsf{F}\urcorner}\mathbf{0})\text{ »}$ *à* $\mathsf{T}^\star\vdash_\omega\text{« }\mathsf{T}\vdash\mathsf{F}\text{ »}$*, mais a priori pas à* $\mathsf{T}^\star\vdash\text{« }\mathsf{T}\vdash\mathsf{F}\text{ »}$*. Comme on préfère s'en tenir à un cadre métamathématique formalisable en logique du premier ordre, on préfère s'abstenir d'utiliser la* ω*-règle, c'est-à-dire s'abstenir d'utiliser le principe, inexprimable en logique du premier ordre, que l'univers de référence est standard. C'est exactement ce qu'on a fait depuis le chapître III en renonçant à définir l'ordinal* ω *comme la borne supérieure des ordinaux* $\underline{\mathsf{n}}$ *pour* n *entier, une définition typique de* ω*-logique, et en le définissant à la place comme le plus petit des ordinaux récurrents : ce faisant, on s'est assuré de rester dans un cadre métamathématique formalisable par la logique du premier ordre, avec tous les bénéfices afférents, en particulier l'usage du théorème de complétude et la possibilité d'arguments sémantiques.* ◁

4.5. Les limites imposées par le premier théorème d'incomplétude.

► On résume informellement et on discute les limites que le premier théorème d'incomplétude de Gödel impose à toute axiomatisation. ◄

En montrant qu'aucune théorie récursive et consistante ne prouve la formule de Gödel associée, le premier théorème d'incomplétude apporte une réponse négative aux questions VII.3.18 et VII.3.19 :

Corollaire 4.15. *Toute théorie arithmétique récursive et consistante incluant* $\mathsf{PA}_{\text{faible}}$ *est incomplète. En particulier, si le système* PA_1 *est consistant, la formule de Gödel* Δ_{PA_1} *est une formule d'arithmétique vraie dans* $(\mathbb{N},0,S,+,\cdot,\leqslant)$ *mais non prouvable à partir de* PA_1*.*

▷ *La conviction que le système de Peano décrit les entiers de façon complète, voire celle que le système de Zermelo–Fraenkel décrit les ensembles de façon complète, est souvent considérée comme intuitive dans la communauté des mathématiciens. Le premier théorème d'incomplétude contredit cette intuition de manière incontournable : aucun système explicite exprimable dans un langage du premier ordre ne peut axiomatiser l'arithmétique ou la théorie des ensembles de façon complète. Noter ici l'importance de chaque qualificatif : explicite réfère à l'hypothèse de récursivité qui écarte un système stupidement complet tel que* $\mathrm{Th}_1(\mathbb{N},0,S,+,\cdot,\leqslant)$*, exprimable au premier ordre est essentiel pour que la notion-même de prouvabilité ait un sens. Mais, dans le cadre ainsi défini, les limites induites par le théorème d'incomplétude sont infranchissables, et toute tentative de contournement serait vaine.*

En particulier, on notera ci-dessous que le passage de l'arithmétique de Peano à la théorie des ensembles de Zermelo–Fraenkel renforce strictement le cadre axiomatique : le système ZF *prouve davantage d'énoncés d'arithmétique que le système* PA_1*. Du coup, on pourrait penser que le système* ZF *donne une description complète des nombres entiers, et que sa propre incomplétude ne se manifeste qu'à un niveau ultérieur, nombres réels ou objets plus compliqués. Ce n'est* ***pas*** *le cas puisqu'en appliquant le premier théorème d'incomplétude à* ZF*, on obtient :* ◁

Corollaire 4.16. *Si le système* ZF *est consistant, la formule de Gödel* Δ_{ZF} *est une formule d'arithmétique vraie dans* $(\mathbb{N},0,S,+,\cdot,\leqslant)$ *mais non prouvable à partir de* ZF*.*

▷ *Ainsi, même au niveau des nombres entiers, la description du monde mathématique fournie par le système* ZFC*, et, de même, par tout autre système axiomatique, est incomplète. L'appellation de théorème d'incomplétude est donc naturelle et légitime. Comme cette appellation s'oppose directement à celle du théorème de complétude établi au chapitre VII, il peut être utile de préciser les rapports entre les deux énoncés, l'un et l'autre rigoureusement démontrés : dans le théorème de complétude, on affirme que toute formule qui est satisfaite dans tout modèle d'une théorie* T *est prouvable à partir de* T *; dans le théorème d'incomplétude, on affirme l'existence d'une formule qui est satisfaite dans un modèle particulier d'une théorie* T*, mais n'est pas prouvable à partir de* T*. Il n'y a aucune contradiction : la formule de Gödel* Δ_{T}*, dont le théorème d'incomplétude affirme qu'elle n'est pas prouvable à partir de* T*, est certes satisfaite dans le modèle* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *de* T*, mais il existe d'autres modèles de* T *dans lesquels elle n'est pas satisfaite, et rien ne contredit le théorème de complétude.*

Par ailleurs, deux remarques peuvent être ajoutées, qui tempèrent légèrement les limites imposées par le théorème d'incomplétude. La première concerne le caractère peu intuitif — et de ce fait un peu décevant — des formules de Gödel, ces formules vraies mais non prouvables fournies par le théorème d'incomplétude. Pour chaque théorie T*, la formule de Gödel associée est parfaitement effective au sens où, avec (beaucoup) de courage, on pourrait l'écrire explicitement, mais il faut reconnaître que cette formule est éloignée des énoncés usuellement considérés en dehors de la logique : en particulier, la formule de Gödel associée à l'arithmétique de Peano est une formule d'arithmétique bien absconse. On peut signaler qu'on connaît aujourd'hui des résultats analogues pour des énoncés où n'apparaît aucun codage de formules logiques et autres ingrédients ejusdem farinæ. En particulier, L. Kirby et J. Paris ont démontré en 1981 que le théorème de Goodstein (proposition II.4.6) n'est pas prouvable à partir de* PA_1*. Exprimé sous la forme*

$$\forall \mathsf{k}\ \exists \mathsf{n}\ (\text{« } \textit{la suite partant de } \mathsf{k} \textit{ atteint la valeur } 0 \textit{ après } \mathsf{n} \textit{ étapes} \text{ »}),$$

le résultat peut être traduit en une formule de $\mathcal{L}_{\mathrm{arith}}$ *car l'exponentielle, puis la fonction « écrire en base* p *itérée et remplacer* p *par* q *», sont récursives, donc définissables dans* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *(cf. exercice 4). On a donc là un exemple plus naturel de formule d'arithmétique vraie dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *mais non prouvable à partir du système de Peano du premier ordre* PA_1*.*

Malgré cela, des résultats comme le théorème de Goodstein restent marginaux en arithmétique, et d'un type très particulier, sinon suspect : le fait que la fonction de Goodstein donnant l'indice où la valeur 0 *est atteinte prenne pour* $\mathsf{n} = 4$ *une valeur énorme, puis pour* $\mathsf{n} \geqslant 5$ *des valeurs tellement grandes qu'elles échappent à toute possibilité de détermination pratique peut donner le sentiment que la propriété des nombres entiers exprimée par le théorème de Goodstein n'est pas du même type que les énoncés arithmétiques plus conventionnels. Du coup, se repose la question d'une possible complétude empirique du système de Peano vis-à-vis des propriétés usuelles : à l'exception des inévitables mais peu concrètes formules de Gödel et de bizarreries telles que le théorème de Goodstein, se pourrait-il que le système de Peano, ou telle ou telle extension de celui-ci, par exemple une théorie des ensembles, se comporte comme un système complet, typiquement lorsqu'on envisage des propriétés suffisamment simples ? La question (qui est informelle) n'est pas tranchée, mais une réponse positive n'est pas exclue a priori.* ◁

4.6. Le second théorème d'incomplétude de Gödel.

► On démontre le second théorème d'incomplétude pour les systèmes incluant le système de Zermelo. ◄

Pour pouvoir énoncer le résultat, on a d'abord besoin d'arithmétiser la notion de consistance d'une théorie T.

DÉFINITION 4.17. (consistance) Ayant fixé une formule $\mathsf{O}(\boldsymbol{x}, \boldsymbol{x}')$ de complexité Σ_1 représentant dans $\mathsf{PA}_{\text{faible}}$ la relation $\mathtt{Oppose}$ telle que $\mathtt{Oppose}(\mathsf{p}, \mathsf{p}')$ est vraie s'il existe une formule close F vérifiant $\mathsf{p} = \ulcorner \mathsf{F} \urcorner$ et $\mathsf{p}' = \ulcorner \neg \mathsf{F} \urcorner$, on définit, pour toute théorie récursive T, la formule close $\mathrm{Cons}_{\mathsf{T}}$ comme étant

$$\neg\, \exists \boldsymbol{x}, \boldsymbol{x}'\ (\Box_{\mathsf{T}}(\boldsymbol{x}) \wedge \Box_{\mathsf{T}}(\boldsymbol{x}') \wedge \mathsf{O}(\boldsymbol{x}, \boldsymbol{x}')). \tag{4.11}$$

▷ *La formule* $\mathrm{Cons}_{\mathsf{T}}$ *exprime qu'on ne peut pas prouver à partir de* T *à la fois une chose et son contraire, et elle est donc la contre-partie formelle de la notion de consistance. Précisément, la formule* $\mathrm{Cons}_{\mathsf{T}}$ *est satisfaite dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *si et seulement si* T *est consistante donc, en* ω*-logique, démontrer qu'une théorie* T *est consistante est synonyme de montrer que le système ambiant prouve la formule* $\mathrm{Cons}_{\mathsf{T}}$*. En logique du premier ordre, on peut seulement affirmer que, si* $\mathrm{Cons}_{\mathsf{T}}$ *est prouvable, alors* T *est consistante, car il se pourrait que* T *soit consistante mais qu'il existe des entiers non standards codant la preuve d'une contradiction dans* T*.*

Pour énoncer le second théorème d'incomplétude, on a besoin d'une dernière notion. D'après la proposition 3.10, on sait que, si une formule close F *de complexité* Σ_1 *est vraie dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, alors* F *est prouvable dans* $\mathsf{PA}_{\text{faible}}$*. Il en résulte alors que la formule* $\Box_{\mathsf{PA}_{\text{faible}}}(\ulcorner\mathsf{F}\urcorner)$ *est à son tour vraie dans* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, de même a fortiori que* $\Box_{\mathsf{T}}(\ulcorner\mathsf{F}\urcorner)$ *dès que* T *inclut* $\mathsf{PA}_{\text{faible}}$*. Par conséquent, la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *satisfait l'implication*

$$\mathsf{F} \Rightarrow \Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\mathsf{F}\urcorner}\mathbf{0}) \tag{4.12}$$

dès que F *est une formule* Σ_1*.* ◁

Définition 4.18. (absoluité) On dit qu'une théorie T de $\mathcal{L}_{\max}$ *prouve l'absoluité des formules* Σ_1 si T prouve l'implication (4.12) pour chaque formule close F de complexité Σ_1.

Proposition 4.19. (second théorème d'incomplétude de Gödel) *Si* T *est une théorie récursive consistante incluant* $\mathsf{PA}_{\text{faible}}$ *et prouvant l'absoluité des formules* Σ_1*, alors* T *ne prouve pas* $\mathrm{Cons}_{\mathsf{T}}$*.*

Démonstration. Comme dans la démonstration du premier théorème d'incomplétude (proposition 4.14), soit Δ la formule de Gödel associée à T, c'est-à-dire la formule $\mathrm{Diag}(\Box_{\mathsf{T}})$ associée à $\Box_{\mathsf{T}}$ par le lemme diagonal. On sait que, par construction, la formule Δ est la négation d'une certaine formule Δ' de complexité Σ_1.

D'après le premier théorème d'incomplétude, T ne prouve pas Δ, donc, pour montrer que T ne prouve pas une formule F, il suffit de montrer que T prouve $\mathsf{F}\Rightarrow\Delta$, ou encore de montrer que T prouve $\Delta' \Rightarrow \neg\mathsf{F}$. On va appliquer ceci à $\mathsf{F} = \mathrm{Cons}_{\mathsf{T}}$, en montrant que T prouve que Δ' implique la T-prouvabilité de deux numéros de formule opposés, à savoir $\ulcorner\Delta'\urcorner$ et $\ulcorner\Delta\urcorner$.

D'un côté, puisque Δ' est une formule Σ_1, l'hypothèse que T prouve l'absoluité des formules Σ_1 entraîne, par définition,

$$\mathsf{T} \vdash \Delta' \Rightarrow \Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\Delta'\urcorner}\mathbf{0}). \tag{4.13}$$

D'un autre côté, par le lemme diagonal, on a la relation (4.8), donc $\mathsf{PA}_{\text{faible}}$, et *a fortiori* T, prouvent $\neg\Delta\Rightarrow\Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$, d'où, puisque Δ est $\neg\Delta'$,

$$\mathsf{T} \vdash \Delta' \Rightarrow \Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0}). \tag{4.14}$$

Enfin, par construction, les formules Δ' et Δ sont opposées, donc la relation $\mathtt{Oppose}(\ulcorner\Delta'\urcorner, \ulcorner\Delta\urcorner)$ est vraie dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$, et, puisque la formule $\mathsf{O}(\boldsymbol{x}, \boldsymbol{y})$ représente $\mathtt{Oppose}$ dans $\mathsf{PA}_{\text{faible}}$ donc dans T, on a $\mathsf{PA}_{\text{faible}} \vdash \mathsf{O}(\boldsymbol{S}^{\ulcorner\Delta'\urcorner}\mathbf{0}, \boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})$, d'où, *a fortiori*,

$$\mathsf{T} \vdash \mathsf{O}(\boldsymbol{S}^{\ulcorner\Delta'\urcorner}\mathbf{0}, \boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0}). \tag{4.15}$$

En rapprochant (4.13),(4.14), et (4.15), on obtient

$$\mathsf{T} \vdash \Delta' \Rightarrow (\Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\Delta'\urcorner}\mathbf{0}) \wedge \Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0}) \wedge \mathsf{O}(\boldsymbol{S}^{\ulcorner\Delta'\urcorner}\mathbf{0}, \boldsymbol{S}^{\ulcorner\Delta\urcorner}\mathbf{0})),$$

d'où $\mathsf{T} \vdash \Delta' \Rightarrow \neg\mathrm{Cons}_{\mathsf{T}}$, qui, on l'a vu, entraîne $\mathsf{T} \nvdash \mathrm{Cons}_{\mathsf{T}}$. □

▷ *L'argument précédent est très simple une fois acquise la non-prouvabilité de la formule de Gödel* Δ_{T}*, c'est-à-dire le premier théorème d'incomplétude. Le seul élément supplémentaire nécessaire pour obtenir le second théorème est ici fourni automatiquement par l'hypothèse sur l'absoluité des formules* Σ_1*, et on peut soupçonner que la véritable difficulté va consister à établir que telle ou telle théorie* T *prouve l'absoluité des formules* Σ_1*.*

Dans ce texte, on va considérer le cas où T *est une théorie des ensembles, typiquement* Z *ou* ZF*, et la démonstration est alors facile. On mentionnera ensuite sans démonstration le cas où* T *est l'arithmétique de Peano* PA_1*, pour lequel la démonstration est beaucoup plus malaisée.* ◁

Proposition 4.20. (absoluité) *Le système de Zermelo* Z *et, a fortiori, le système de Zermelo–Fraenkel* ZF*, prouvent l'absoluité des formules* Σ_1*.*

Démonstration. La proposition 3.10 affirme que toute formule close Σ_1 vraie dans la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ est prouvable à partir de $\mathsf{PA}_{\text{faible}}$. Dire qu'une théorie T prouve l'absoluité Σ_1, c'est dire qu'on peut construire une démonstration de ce résultat à partir des axiomes de T. On a montré au chapitre III que les entiers et les ensembles d'entiers pouvaient être construits dans tout modèle d'une théorie des ensembles comme Z, et la question est de vérifier que la démonstration de la proposition 3.10 peut être entièrement formalisée dans le cadre de Z. Or les ingrédients de cette démonstration sont, d'une part, le fait que les formules closes Σ_1 vraies dans $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ sont vraies dans tous les modèles de $\mathsf{PA}_{\text{faible}}$, et, d'autre part, le théorème de complétude qui permet de déduire du fait qu'une formule close est vraie dans tous les modèles de $\mathsf{PA}_{\text{faible}}$ le fait que cette formule est prouvable à partir de $\mathsf{PA}_{\text{faible}}$. Chacune des deux démonstrations se formalise sans problème dans le cadre de Z (et en particulier sans faire appel à la ω-règle) : pour le démontrer, il suffit de relire la démonstration du théorème de complétude au chapitre VII en vérifiant qu'on n'introduit aucun ensemble dont l'existence ne soit garantie par Z. On notera que, la signature $\Sigma_{\max}$ et les formules associées ayant été numérotées, il n'y a pas de problème de choix pour construire le modèle requis pour le théorème de complétude. □

Corollaire 4.21. *S'il est consistant, le système* Z *ne prouve pas la formule* $\mathrm{Cons}_{\mathsf{Z}}$*, et, s'il est consistant, le système* ZF *ne prouve pas la formule* $\mathrm{Cons}_{\mathsf{ZF}}$*. Plus généralement, pour tout système* T *récursif incluant* ZF*, si* T *est consistant, il ne prouve pas* $\mathrm{Cons}_{\mathsf{T}}$*.*

On mentionne sans démonstration :

Proposition 4.22. (absoluité) *Le système de Peano* PA_1 *prouve l'absoluité des formules* Σ_1*.*

▷ *La démonstration de ce résultat est délicate. Il s'agit de montrer à l'intérieur de tout modèle de* PA_1 *une version du théorème de complétude ; il est ici essentiel de disposer des axiomes d'induction, donc du système* PA_1 *et pas seulement de* $\mathsf{PA}_{\text{faible}}$*, mais, même avec cet outil, il reste à développer des arguments de codage délicats et sans commune mesure avec ce qu'on fait dans le contexte de* Z*, où il s'agit d'une simple transcription de la démonstration du théorème de complétude.* ◁

Corollaire 4.23. *S'il est consistant, le système* PA_1 *ne prouve pas la formule* $\mathrm{Cons}_{\mathsf{PA}_1}$*.*

4.7. Retour sur les questions de fondement.

► Le second théorème d'incomplétude ruine les espoirs de démontrer formellement la cohérence de l'édifice mathématique. ◄

▷ *Au chapitre III, on a souligné l'intérêt de la représentation des objets mathématiques les plus divers par des ensembles purs en termes de fondements des mathématiques : dès lors que toutes les théories mathématiques peuvent être vues comme incluses dans l'unique théorie des ensembles, il suffit, pour établir la cohérence de l'édifice entier, d'établir la cohérence de l'unique théorie des ensembles. Et, puisqu'il apparaît raisonnable de développer cette dernière comme une théorie du premier ordre basée sur les axiomes de* ZF *ou, plus généralement, sur un système d'axiomes* T *incluant* ZF*, la question de la cohérénce de la théorie des ensembles devient celle de l'impossibilité de prouver une contradiction à partir des axiomes de* T*. De façon précise, on a la suite d'équivalences* $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$*, avec*

(i) *On peut démontrer une contradictoire à partir des axiomes de* T*;*

(ii) *Il existe une formule close* F *telle qu'on ait à la fois* $\mathsf{T} \vdash \mathsf{F}$ *et* $\mathsf{T} \vdash \neg\mathsf{F}$*;*

(iii) *La formule* $\neg\mathrm{Cons}_{\mathsf{T}}$ *est satisfaite dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*.*

L'équivalence de (i) *et* (ii) *reflète l'exhaustivité des règles de la logique du premier ordre comme modélisation du raisonnement mathématique — et l'implication* $(i) \Rightarrow (ii)$ *est donc objet de consensus mais non de démonstration ; celle de* (ii) *et* (iii) *reflète la possibilité d'arithmétiser la syntaxe de la logique du premier ordre — et elle est donc objet de démonstration.*

Etablir la cohérence d'un système T *comme base des mathématiques signifierait donc établir que la formule* $\mathrm{Cons}_{\mathsf{T}}$ *est satisfaite dans la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$*, et la seule façon envisageable de le faire consisterait à la démontrer à partir des axiomes retenus, donc, utilisant à nouveau une équivalence entre démonstration et preuve, à démontrer que* T *prouve* $\mathrm{Cons}_{\mathsf{T}}$*. Et c'est précisément ce que le second théorème d'incomplétude affirme être impossible. La situation ainsi créée peut se résumer dans l'énoncé suivant :* ◁

« Proposition » 4.24. (fondement) *Quel que soit le cadre axiomatique* $\mathfrak{T}$*, dès lors que* $\mathfrak{T}$ *est formalisable dans une logique du premier ordre par un système récursif consistant incluant le système de Peano* PA_1 [7]*, il est impossible de démontrer dans le cadre de* $\mathfrak{T}$ *que les mathématiques sont non contradictoires.*

▷ *On notera que le second théorème d'incomplétude n'empêche pas toute démonstration de non-contradiction : rien interdit de montrer* $\mathrm{Cons}_{\mathsf{T}}$ *dans une théorie* T' *plus forte que* T *— à commencer par* $\mathsf{T}' = \mathsf{T} + \mathrm{Cons}_{\mathsf{T}}$*. Ce qu'interdit le théorème de Gödel, c'est de trouver le point fixe d'une théorie prouvant sa propre non-contradiction.*

On notera que la consistance du système PA *ou du système* ZF *ne saurait être justifiée par l'existence des entiers ou des ensembles, c'est-à-dire par le fait que la structure* $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$ *soit un modèle de* PA*, ou que* $(\mathbf{V}, \in)$ *soit un modèle de* ZF *: quand bien même on tiendrait pour acquise l'existence des nombres entiers ou des ensembles, le fait que ces objets satisfassent aux axiomes de Peano ou de Zermelo–Fraenkel est une opinion qui ne peut faire l'objet d'une démonstration, et ne peut donc être alléguée comme argument d'une quelconque démonstration ultérieure — par contre, elle peut l'être pour justifier l'opportunité d'étudier les systèmes* PA *ou* ZF*.*

Du point de vue des fondements, le théorème de Gödel tend à relativiser l'intérêt de la représentation des objets mathématiques par des ensembles — ou par tout autre type privilégié. On a bien ramené la question de la cohérénce de l'édifice à l'unique question de l'absence de contradiction dans le système ZF *ou une extension de celui-ci, mais on sait désormais qu'il n'y a aucun espoir de résoudre positivement cette dernière question, et le gain n'est donc pas si considérable. Au contraire, l'impossibilité de montrer la cohérence globale de l'édifice, redonne de l'intérêt à considérer séparément des fragments plus modestes dont la cohérence, au moins relative, peut être établie directement. Sans remettre en cause l'unité profonde des mathématiques, on peut souligner que l'approche du traité de Bourbaki fondée sur la théorie des ensembles*

[7] ou, pour s'en tenir à ce qui a été démontré ici, le système de Zermelo Z

comme base axiomatique unique et absolue des mathématiques — et de surcroît sur une identification du monde des ensembles et de celui des formules, c'est-à-dire du niveau mathématique et du niveau métamathématique — procède d'une vision pré-gödélienne aujourd'hui dépassée. ◁

Exercices

EXERCICE 1. (fonctions récursives) Soit F l'ensemble des fonctions pouvant s'obtenir par un nombre fini de compositions et de récursions à partir des fonctions constantes $\mathtt{const}_{\mathsf{p},\mathsf{m}}$ et des projections $\mathtt{proj}_{\mathsf{p},\mathsf{i}}$. Montrer que toute fonction dans F est primitive récursive. Montrer que, pour toute fonction f de $\mathbb{N}^{\mathsf{p}}$ dans $\mathbb{N}$ qui est dans F, il existe une constante C_f telle que, pour tous $\mathsf{n}_1, \ldots, \mathsf{n}_{\mathsf{p}}$ dans $\mathbb{N}$, on a $f(\mathsf{n}_1, \ldots, \mathsf{n}_{\mathsf{p}}) \leq \sup(C_f, \mathsf{n}_1, \ldots, \mathsf{n}_{\mathsf{p}})$. En déduire que F est un sous-ensemble strict de l'ensemble des fonctions primitives récursives.

EXERCICE 2. (semi-récursif) Montrer que, pour toute relation S sur $\mathbb{N}^{\mathsf{p}}$, il y a équivalence entre : (*i*) La relation S est semi-récursive ; (*ii*) La relation S est MT-semi-décidable, au sens où il existe une machine de Turing déterministe M dont le calcul à partir de l'entrée $\vec{\mathsf{n}}$ est acceptant quand $R(\vec{\mathsf{n}})$ est vrai et ne se termine pas quand $R(\vec{\mathsf{n}})$ est faux ; (*iii*) La relation S est la projection d'une relation primitive récursive sur $\mathbb{N}^{\mathsf{p}+1}$; (*iv*) Il existe une fonction récursive f dont le domaine est S.

EXERCICE 3. (Peano) (*i*) Montrer que PA_1 prouve $\forall \boldsymbol{x}, \boldsymbol{y}(\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x})$, (*ii*) En déduire en utilisant une induction sur $\boldsymbol{x}$ que PA_1 prouve l'existence de la division euclidienne sous la forme

$$(*) \qquad \forall \boldsymbol{x}, \boldsymbol{y}\ \exists \boldsymbol{q}, \boldsymbol{r}, \boldsymbol{s}\ (\boldsymbol{x} = \boldsymbol{S}(\boldsymbol{y}) \cdot \boldsymbol{q} + \boldsymbol{r} \wedge \boldsymbol{s} + \boldsymbol{r} = \boldsymbol{y}).$$

(*iii*) Montrer que la structure $\mathcal{M}$ formée par les polynômes de $\mathbb{Z}[X]$ à coefficient dominant positif munis des opérations usuelles est un modèle de $\mathsf{PA}_{\text{faible}}$. Peut-on diviser X par 2 dans $\mathcal{M}$? Qu'en déduit-on pour (*) ?

EXERCICE 4. (définissabilité) Si $\mathcal{M}$ est une structure de type Σ, une fonction f de $\mathrm{Dom}(\mathcal{M})^{\mathsf{p}}$ dans $\mathrm{Dom}(\mathcal{M})$ est dite *définissable* dans $\mathcal{M}$ s'il existe une formule $\mathsf{F}(\vec{\boldsymbol{x}}, \boldsymbol{y})$ de $\mathcal{L}_\Sigma$ telle que, pour tous $\vec{a}, b$ dans $\mathrm{Dom}(\mathcal{M})$, la relation $f(\vec{a}) = b$ est vraie si et seulement si $\mathcal{M}$ satisfait $\mathsf{F}(\vec{a}, b)$. Montrer que toute fonction récursive est définissable dans la structure $(\mathbb{N}, 0, S, +, \cdot, \leqslant)$. [Suivre le même schéma que pour montrer que toute fonction récursive totale est représentable.]

EXERCICE 5. (couplage) (*i*) Montrer que la bijection $\mathtt{coupl}$ de $\mathbb{N}^2$ dans $\mathbb{N}$ définie par $\mathtt{coupl}(\mathsf{n}_1, \mathsf{n}_2) := (\mathsf{n}_1 + \mathsf{n}_2)(\mathsf{n}_1 + \mathsf{n}_2 + 1)/2 + \mathsf{n}_1$ est primitive récursive, de même que chacune des deux composantes $\mathtt{coord}_1$, $\mathtt{coord}_2$ de la bijection réciproque.
(*ii*) En déduire l'existence d'une fonction primitive récursive $\mathtt{frag}$ de $\mathbb{N}^2$ dans $\mathbb{N}$ telle que, pour toute suite finie d'entiers $(\mathsf{n}_0, ..., \mathsf{n}_{\mathsf{k}})$, il existe un entier n tel qu'on ait $\mathtt{frag}(\mathsf{n}, \mathsf{i}) = \mathsf{n}_{\mathsf{i}}$ pour $\mathsf{i} = 0, ..., \mathsf{k}$. [Utiliser la fonction $\mathtt{beta}$, et la fonction $\mathtt{coupl}$ pour contracter les deux premiers arguments de $\mathtt{beta}$ en un seul.]

EXERCICE 6. (récursion simultanée) Soient g_1, g_2, h_1, h_2 des fonctions primitives récursives respectivement de $\mathbb{N}^{\mathsf{p}}$, $\mathbb{N}^{\mathsf{p}}$, $\mathbb{N}^{\mathsf{p}+3}$, et $\mathbb{N}^{\mathsf{p}+3}$ dans $\mathbb{N}$. Montrer les fonctions f_1, f_2 de $\mathbb{N}^{\mathsf{p}+1}$ dans $\mathbb{N}$ définies pour $\mathsf{i} = 1, 2$ par

$$f_{\mathsf{i}}(\vec{\mathsf{n}}, \mathsf{k}) := \begin{cases} g_{\mathsf{i}}(\vec{\mathsf{n}}) & \text{pour } \mathsf{k} = 0, \\ h_{\mathsf{i}}(\vec{\mathsf{n}}, \mathsf{k}, f_1(\vec{\mathsf{n}}, \mathsf{k}-1), f_2(\vec{\mathsf{n}}, \mathsf{k}-1)) & \text{pour } \mathsf{k} > 0 \end{cases}$$

sont primitives récursives.

EXERCICE 7. (consistance) (*i*) Montrer que, si ZFC est consistant, alors il en est de même de la théorie $\mathsf{ZFC} + \neg\mathrm{Cons}_{\mathsf{ZFC}}$ [Utiliser le second théorème d'incomplétude].
(*ii*) Montrer que la théorie $\mathsf{ZFC} + \neg\mathrm{Cons}_{\mathsf{ZFC}}$ ne possède pas de modèle standard, c'est-à-dire tel que ω soit le sup des ordinaux $\underline{\mathsf{n}}$ pour n entier naturel [Remarquer que, dans un modèle standard, la satisfaction de $\Box_{\mathsf{T}}(\boldsymbol{S}^{\ulcorner \mathsf{F} \urcorner}\mathbf{0})$ entraîne la prouvabilité de F].
(*iii*) Peut-on raffiner le théorème de complétude en un énoncé affirmant l'existence d'un modèle standard pour chaque théorie consistante ?