L'arithmétique de Peano.

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

La formalisation de l'arithmétique engendre deux questions :

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

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

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

On a donné plusieurs formalisations des algorithmes :

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

On démontre que les trois modèles sont équivalents.

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

1 Les axiomes.

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

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

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

Remarque 1 (Convention). La structure $\mathbb{N}$ représente la $\mathscr{L}_0$-structure dans laquelle on interprète les symboles de manière habituelle :

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

Les axiomes de Peano.

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

Trois axiomes pour le successeur :

A1. $\forall x\, \neg(Ⓢ x = Ⓞ)$

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

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

Deux axiomes pour l'addition :

A4. $\forall x\, (x \oplus Ⓞ = x)$

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

Deux axiomes pour la multiplication :

A6. $\forall x\, (x \otimes Ⓞ = Ⓞ)$

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

Et le schéma d'induction :

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

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

Remarque 2. ▷ Le schéma est le SI avec hypothèse faible, qui permet de montrer le SI avec hypothèse forte. On adopte la notation $\forall y \leq x \; F(y, x_1, \ldots, x_n)$ pour

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

Le SI avec hypothèse forte est :

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

▷ L'ensemble $\mathscr{P}$ est non-contradictoire car $\mathbb{N}$ est un modèle, appelé *modèle standard*.

▷ On peur remplacer le SI par une nouvelle règle de démonstration :

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

Exercice 1. Montrer l'équivalence entre SI et la nouvelle règle rec, *i.e.* on peut démontrer les mêmes théorèmes.

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

Définition 1. Dans une $\mathscr{L}_0$-structure, on dit qu'un élément est *standard* s'il est l'interprétation d'un terme $\textcircled{n}$ avec $n \in \mathbb{N}$.

Remarque 3. Dans $\mathbb{N}$ (le modèle standard), tout élément est standard.

Théorème 1. Il existe des modèles de $\mathscr{P}$ non isomorphes à $\mathbb{N}$.

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

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

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

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

$$T' \subseteq \mathscr{P} \cup \{\neg(c = \underline{n_1}), \neg(c = \underline{n_2}), \dots, (c = \underline{n_k})\},$$

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

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

□

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

Théorème 2. Dans tout modèle $\mathscr{M}$ de $\mathscr{P}$,

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

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

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

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

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

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

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

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

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

     On peut le montrer par A5.

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

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

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

     Ceci est vrai car

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

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

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

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

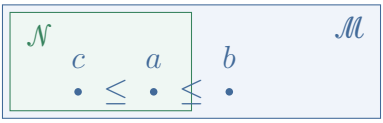
□

Exercice 2. Finir la preuve du théorème.

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

Définition 2. Si $\mathscr{M} \models \mathscr{P}_0$ et $\mathscr{N} \models \mathscr{P}_0$ et $\mathscr{N}$ une sous-interprétation de $\mathscr{M}$, on dit que $\mathscr{N}$ est un segment initial de $\mathscr{M}$, ou que $\mathscr{M}$ est une extension finale de $\mathscr{N}$, si pour tous $a, b, c \in |\mathscr{M}|$ avec $a \in |\mathscr{N}|$ on a :

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



Remarque 4.
▷ Les points peuvent être incomparables et dans $\mathscr{M}$.
▷ L'ensemble $\mathscr{P}_0$ est très faible, on ne montre même pas que $\oplus$ commute ou que $\leq$ est une relation d'ordre (*c.f.* TD).

Théorème 3. Soit $\mathscr{M} \models \mathscr{P}_0$. Alors, le sous-ensemble de $\mathscr{M}$ sui-

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

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

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

□

3 Les fonctions représentables.

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

Définition 3. Soit $f : \mathbb{N}^p \to \mathbb{N}$ une fonction totale et $F(x_0, \ldots, x_p)$ une formule de $\mathscr{L}_0$. On dit que F *représente* f si, pour tout p-uplet d'entiers $(n_1, \ldots, n_p)$ on a :

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

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

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

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

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

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

Exercice 3. Montrer qu'un ensemble est représentable ssi sa fonction indicatrice l'est.

Exemple 1 (Les briques de base des fonctions récursives).

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

On introduit trois nouvelles opérations.

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

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

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

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

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

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

Définition 4. L'ensemble des fonctions récursives primitives (*resp.* récursives) est le plus petit ensemble des fonctions contenant les briques de base et stable par composition et récurrence (*resp.* par composition, récurrence et schéma μ).

Exemple 2. Les fonctions

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

et

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

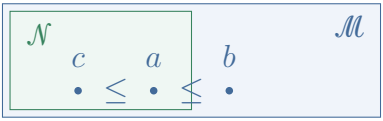
sont récursives primitives.

Définition 5. Une fonction récursive *totale* est une fonction récursive définie partout.

Remarque 5.
- ▷ Une fonction récursive primitive est totale.
- ▷ Une fonction récursive primitive peut se fabriquer avec un seul schéma μ à la fin (*c.f.* cours de FDI).
- ▷ *Rappel.* Une fonction $f : \mathbb{N}^p \to \mathbb{N}$ totale est représentée par la formule $F(x_0, \dots, x_p)$ de $\mathscr{L}_0$ su pour tout p-uplet d'entiers $(n_1, \dots, n_p)$ on a :

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

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



Théorème 4. Toute fonction récursive totale est représentable.

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

Lemme 1. L'ensemble des fonctions représentables est clos par composition.

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

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

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

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

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

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

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

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

□

Lemme 2. Si, à partir d'une fonction représentable totale, on obtient par schéma μ une fonction totale, alors cette fonction est représentable.

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

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

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

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

Considérons la formule

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

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

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

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

□

Lemme 3. L'ensemble des fonctions totales est stable par définition par récurrence.

Preuve. Soient f, g, h telles que

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

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

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

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

Lemme 4 (Fonction β de Gödel)**.** Il existe une fonction β à trois variables, récursive primitive et représentable, tel que pour tout $p \in \mathbb{N}$ et toute suite $(n_0, \dots, n_p) \in \mathbb{N}^{p+1}$, il existe des entiers a et b tels que pour tout $0 \leq i \leq p$, on ait $\beta(i, a, b) = n_i$.

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

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

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

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

Preuve. Soient f, g, h telles que

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

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

- $z_0 = g(x_1, \dots, x_p)$
- $z_1 = h(0, z_0, x_1, \dots, x_p)$
- $z_2 = h(1, z_1, x_1, \dots, x_p)$
- ⋮

- ▷ $z_{x_0} = h(x_0 - 1, z_{x_0-1}, x_1, \ldots, x_p)$
- ▷ $y = z_{x_0}$

ssi

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

est vraie. Montrons que F représente f.

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

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

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

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

□

Ceci conclut la preuve du théorème 4.