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 $x_0, \dots, x_n$,

$$\forall x_1 \cdots \forall x_n \Big(\big(F(⓪,\dots,x_1,\dots,x_n) \land \forall x\,(F(x,x_1,\dots,x_n) \to F(Ⓢ x,x_1,\dots,x_n))\big) \to \forall x\, F(x,x_1,\dots,x_n)\Big).$$

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

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

Le SI avec hypothèse forte est :

$$\forall x_1 \cdots \forall x_n \Big(\big(F(⓪,\dots,x_1,\dots,x_n) \land \forall x\,\big((\forall y \le x\; F(y,x_1,\dots,x_n)) \to F(Ⓢ x,x_1,\dots,x_n)\big)\big) \to \forall x\, F(x,x_1,\dots,x_n)\Big)$$

▷ 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 :

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

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

Notation. On note ⓝ le terme $\underbrace{Ⓢ \cdots Ⓢ}_{n \text{ fois}}⓪$ 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 ⓝ 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 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

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

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,

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

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 $n \in \mathbb{N}$, $\mathscr{M} \models \neg(c = \textcircled{n})$. Or, on ne peut pas avoir $\mathbb{N} \models \neg(\textcircled{\gamma} = \textcircled{n})$ 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 :

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

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

     $$\forall x\, \big((⓪ \oplus x = x) \to (⓪ \oplus (Ⓢ\, x) = Ⓢ\, x)\big).$$

     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 $\mathscr{P} \vdash \forall x \forall y\, Ⓢ(x \oplus y) = (Ⓢ\, x) \oplus y$. On veut utiliser le schéma d'induction avec $F(x, y) := Ⓢ(x \oplus y) = (Ⓢ\, x) \oplus y$. Mais ça ne marche pas...(Pourquoi ?)

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

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

     Ceci est vrai car

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

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

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

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

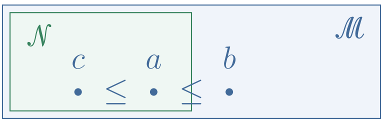
□

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 $\mathscr{M}$ suivant 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 $\mathscr{P}_0 \vdash \underline{n+1} = \mathsf{S}\,\underline{n}$.
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
$$\mathscr{P}_0 \vdash \forall x \left(x \le \underline{n} \to (x = \underline{0} \vee x = \underline{1} \vee \cdots \vee x = \underline{n})\right).$$
7. Pour tout x, on a $\mathscr{P}_0 \vdash \forall x\, (x \le \underline{n} \vee \underline{n} \le x)$.

□

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 $F(x_0, x_1) := x_0 = ⓪$.
- ▷ Les fonctions constantes $f : \mathbb{N} \to \mathbb{N}, x \mapsto n$ sont représentables par $F(x_0, x_1) := x_0 = ⓝ$, où $n \in \mathbb{N}$.
- ▷ Les projections $\pi_p^i : \mathbb{N}^p \to \mathbb{N}, (x_1, \dots, x_p) \mapsto x_i$ sont représentables par $F(x_0, x_1, \dots, x_p) := x_0 = x_i$.
- ▷ La fonction successeur $f : \mathbb{N} \to \mathbb{N}, x \mapsto x + 1$ est représentable par $F(x_0, x_1) := x_0 = (Ⓢ\, x_1)$.
- ▷ 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 $f(x_1, \ldots x_{p+1})$ une fonction partielle. Soit

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

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

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

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

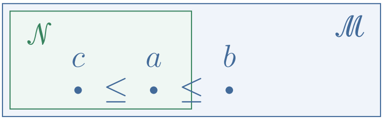
sont récursives primitives.

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 $F(x_0, \ldots, x_p)$ de $\mathscr{L}_0$ su pour tout p-uplet d'entiers $(n_1, \ldots, n_p)$ on a :

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

- *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 $n_1, \dots, n_{\max(p,n)}$:

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

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

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

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

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

$\square$

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

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

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

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

Considérons la formule

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

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

est vrai. Montrons que $b := f(n_1, \ldots, n_p)$ est le seul élément à satisfaire $F(y, n_1, \ldots, n_p)$. On a bien $G(0, b, n_1, \ldots, n_p)$ par définition de f et pour tout entier $z < b$, on a $\neg G(0, z, n_1, \ldots, n_p)$. 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, $F(b, n_1, \ldots, n_p)$. Montrons que b est le seul. Soit y tel que $F(y, n_1, \ldots, n_p)$. 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, $g(y, x_1, \ldots, x_p) = 0$ et $b < y$ avec $g(b, x_1, \ldots, x_p) = 0$. Ainsi, $\forall z < y \neg G(0, z, x_1, \ldots, x_p)$ est fausse, et donc $F(y, n_1, \ldots, n_p)$ est fausse.

□

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

Preuve. Soient f, g, h telles que

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

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

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

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 $(n_0, \ldots, n_p) \in \mathbb{N}^{p+1}$, il existe des entiers a et b tels que pour tout $0 \le i \le p$, on ait $\beta(i, a, b) = n_i$.

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

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

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

Preuve. Soient f, g, h telles que

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

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

- ▷ $z_0 = g(x_1, \ldots, x_p)$
- ▷ $z_1 = h(0, z_0, x_1, \ldots, x_p)$
- ▷ $z_2 = h(1, z_1, x_1, \ldots, x_p)$
- ▷ $\vdots$

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

ssi

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

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 $f(n_0, \ldots, n_p)$ 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 $\mathscr{M} \models F(d, n_0, \ldots, n_p)$ alors il existe a, b, z_0 tels que $B'(z_0, 0, a, b)$ 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 $d = f(n_0, \ldots, n_p)$.

$\square$

Ceci conclut la preuve du théorème 4.

Maintenant que l'on a transformé les fonctions en formules, on va faire l'opposé. Notre but est de montrer le théorème suivant : soit T une théorie consistante contenant $\mathscr{P}_0$ alors T est indécidable. La « partie technique » de l'indécidabilité de Gödel est la preuve par diagonalisation.

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

On va coder :

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

Lemme 5 (Récursion)**.** Soient $p, n \in \mathbb{N}$ et

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

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

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

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

□

Lemme 6 (Définition par cas)**.** Soient $P_1, \dots, P_n$ des ensembles récursifs primitifs (*resp.* récursifs) disjoints de $\mathbb{N}^m$ et $f_1, \dots, f_{n+1}$ des fonctions récursives primitives (*resp.* récursives) $\mathbb{N}^m \to \mathbb{N}$

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

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

□

Lemme 7 (Définition par cas et récursion). Soient $p, n, m \in \mathbb{N}$, et

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

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

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

et

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

□

4.1 Codage des suites d'entiers.

Proposition 1. Pour tout entier non nul p il existe des fonctions récursives primitives bijectives $\alpha_p : \mathbb{N}^p \to \mathbb{N}$ et $\beta_p^1, \dots, \beta_p^p : \mathbb{N} \to \mathbb{N}$ telles que la réciproque de α_p est $(\beta_p^1, \dots, \beta_p^p)$ et, de plus, si

$x > 1$ et $p \geq 2$ alors $\beta_p^i(x) < x$.

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

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

et on pose

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

Ainsi,

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

□

4.2 Les termes.

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

Définition 6. Le nombre de Gödel d'un terme t sur $\mathscr{L}$, noté $\sharp t$, est défini par :

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

Lemme 8. Le codage est injectif.

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

Lemme 9. L'ensemble $\mathrm{Term} := \{\sharp t \mid t \text{ est un terme de } \mathscr{L}_0\}$ est récursif primitif.

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

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

□

4.3 Les formules.

Définition 7. On étend $\sharp\cdot$ aux formules :

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

Lemme 10. Le codage ci-dessus est injectif. □

Lemme 11. L'ensemble $\mathrm{Form} := \{\sharp F \mid F \text{ formule de } \mathscr{L}_0\}$ est récursif primitif. □

4.4 Opérations sur les formules.

Lemme 12. Les ensembles suivants sont récursifs primitifs :

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

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

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

□

Lemme 13 (Substitutions). Il existe des fonctions récursives primitives $\mathrm{Subst}_\mathrm{t}$ et $\mathrm{Subst}_\mathrm{f}$ à trois variables telles que, si t t u sont des termes, et si G est une formule, alors pour tout entier n,

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

Preuve. On définit $\mathrm{Subst}_\mathrm{t}$ par cas/récursion. Pour (n, y, x), on a :

- ▷ si $\beta_3^3(x) = 0$ alors

  - si $\beta_3^1(x) = n+1$ alors $\mathrm{Subst}_\mathrm{t}(n,y,x) := y$,
  - sinon $\mathrm{Subst}_\mathrm{t}(n,y,x) := x$;
- si $\beta_3^3(x) = 1$ alors $\mathrm{Subst}_\mathrm{t}(n,y,x) := \alpha_3(\mathrm{Subst}_\mathrm{t}(n,y,\beta_3^1(x)),0,1)$;
- si $\beta_3^3(x) = 1$ alors
  $\mathrm{Subst}_\mathrm{t}(n,y,x) := \alpha_3(\mathrm{Subst}_\mathrm{t}(n,y,\beta_3^1(x)), \mathrm{Subst}_\mathrm{t}(n,y,\beta_3^2(x)), \beta_3^3(x))$;
- sinon $\mathrm{Subst}_\mathrm{t}(n,y,x) := 0$.

Puis, on définit $\mathrm{Subst}_\mathrm{f}$ par :

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

□

4.5 Codage des preuves.

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

Définition 8. On définit le codage par :

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

Lemme 14. Le décodage est unique. □

Lemme 15. La substitution d'une formule dans un contexte est récursif primitif. Tester si une variable est libre (*resp.* liée) dans un contexte est récursif primitif. □

4.6 Codage des preuves en déduction naturelle.

Remarque 6. Le contexte de la conclusion et des prémisses est le même sauf pour

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

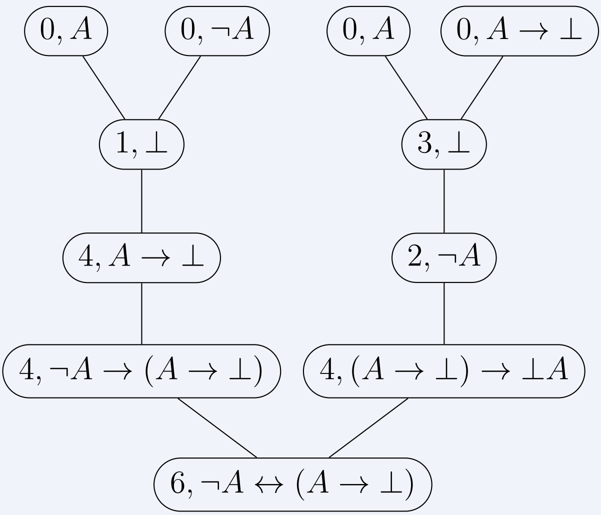
$$\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_{\mathsf{c}} \qquad \dfrac{}{\Gamma \vdash A}\ \mathsf{ax}.$$

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

Exemple 3. La preuve

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

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



Définition 9. On numérote

- $\sharp\mathsf{ax} := 0$
- $\sharp\neg_{\mathsf{e}} := 1$
- $\sharp\neg_{\mathsf{i}} := 2$
- $\sharp \to_{\mathsf{e}} := 3$
- $\sharp \to_{\mathsf{i}} := 4$
- $\sharp\wedge_{\mathsf{e}} := 5$
- $\sharp\wedge_{\mathsf{i}} := 6$
- *etc.*

Définition 10 (Nombre de Gödel des preuves).

- Si $D^\star$ est un arbre de preuve à un seul nœud étiqueté par la formule F et la règle n alors $\sharp D^\star := \alpha_3(n, \sharp F, 0)$.
- Si $D^\star$ est un arbre de preuve dont la racine est étiquetée par la formule F et la règle n à k prémisses avec les sous arbres $D_1^\star, \ldots, D_k^\star$

$$\dfrac{D_1^\star \qquad \cdots \qquad D_k^\star}{F}\ \text{règle } n$$

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

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

Lemme 16. C'est un code injectif.

Lemme 17. L'ensemble $\mathrm{Preuve} := \{\sharp D \mid D \text{ est une preuve}\}$ est récursif primitif.

4.7 Qu'est ce qu'une bonne théorie ?

Définition 11. Un ensemble A de formules est un ensemble d'*axiomes* de la théorie T si $A \vdash T$ et $T \vdash A$.

Définition 12. Une théorie T sur $\mathscr{L}_0$ a un ensemble d'axiomes Ax_T récursif si l'ensemble des numéros de formules de Ax_T est récursif.

Remarque 7. Si Ax_T est fini, alors il est récursif (exemple : $\mathscr{P}_0$).

Lemme 18. L'ensemble des axiomes de Peano $\mathscr{P}$ est récursif.

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

$$A_F := \forall x_1 \cdots \forall x_n \Big(\big(F(0, x_1, \ldots, x_n) \land \forall x_0 \left(F(x_0, \ldots, x_n) \to F(Ⓢ x_0, x_1, \ldots, x_n) \right) \big) \to \forall x_0\, F(x_0, \ldots, x_n) \Big).$$

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

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

$\square$