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 $\mathscr{L}_0 = \{⓪, Ⓢ, \oplus, \otimes\}$ où

- ▷ ⓪ 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 ⓪, 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. $\forall x\ \neg(Ⓢ x = ⓪)$

A2. $\forall x\ \exists y\ \big(\neg(x = ⓪) \to x = Ⓢ y\big)$

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

Deux axiomes pour l'addition :

A4. $\forall x\ (x \oplus ⓪ = x)$

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

Deux axiomes pour la multiplication :

A6. $\forall x\ (x \otimes ⓪ = ⓪)$

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 $x_0, \ldots, x_n$,

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

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

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

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,

$$T' \subseteq \mathscr{P} \cup \{\neg(c = ⓝ_1), \neg(c = ⓝ_2), \ldots, (c = ⓝ_k)\},$$

et $n_k \geq n_1, \ldots, n_{k-1}$. 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 $n \in \mathbb{N}$, $\mathscr{M} \models \neg(c = ⓝ)$. Or, on ne peut pas avoir $\mathbb{N} \models \neg(\gamma = ⓝ)$ 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 $\times$:

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

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 $\mathscr{P} \vdash F(y,x) \to F(\circledS y, x)$ car : si $\circledS(x \oplus y) = (\circledS x) \oplus y$, alors

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

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

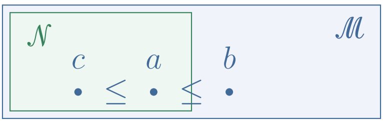
□

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



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 $\le$ 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 $\mathscr{P}_0 \vdash \underline{n+1} = \mathbf{S}\,\underline{n}$.
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
$$\mathscr{P}_0 \vdash \forall x \left(x \le \underline{n} \to (x = \underline{0} \vee x = \underline{1} \vee \cdots \vee x = \underline{n})\right).$$
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 $F(x_0, x_1) := x_0 = \textcircled{0}$.
- 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 $\pi_p^i : \mathbb{N}^p \to \mathbb{N}, (x_1, \dots, x_p) \mapsto x_i$ 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 $F(x_0, x_1) := x_0 = (\textcircled{S} x_1)$.
- 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 $F(x_0, x_1, x_2) := x_0 = x_1 \otimes x_2$.

Théorème 4. Toute fonction récursive totale est représentable.