Notes sur le formalisme en mathématiques

II

La question de savoir s'il y a lieu de reconnaître à la pensée humaine une vérité objective n'est pas une question théorique, mais une question pratique. C'est dans la pratique qu'il faut que l'homme prouve la vérité, c'est-à-dire la réalité, et la puissance de sa pensée, dans ce monde et pour notre temps. La discussion sur la réalité ou l'irréalité d'une pensée qui s'isole de la pratique, est purement scolastique.

VIII

Toute vie sociale est essentiellement pratique. Tous les mystères qui détournent la théorie vers le mysticisme trouvent leur solution rationnelle dans la pratique humaine et dans la compréhension de cette pratique.

Marx : thèses sur Feuerbach

Introduction

Le formalisme en mathématiques a été inventé en grande partie pour faire face aux nombreux paradoxes qui sont apparus avec l'avènement de la théorie des ensembles.

Un autre but du formalisme était une tentative de réduire le raisonnement mathématique à des calculs "automatiques" sur des symboles. Rêve qu'avait déjà caressé Leibniz.

La mise au point des géométries non euclidiennes avait, de plus, jeté un doute sur la notion de vérité absolue. Auparavant les mathématiciens pensaient plus ou moins soumettre à leur étude des objets existant réellement, tel l'espace euclidien à 3 dimensions. Et les vérités concernant ces objets réels semblaient indiscutables.
Quand il apparut que l'axiome des parallèles n'était pas indiscutable, on put se demander qu'est ce qui était vraiment indiscutable en mathématiques.

La logique formelle et la formalisation des théories mathématiques avaient pour but également d'aboutir à préciser la partie vraiment indiscutable de la logique et des mathématiques.

Le but du formalisme tel que le définissait Hilbert était donc de trouver une base solide et universelle aux mathématiques :

- *solide* parce qu'entièrement basée sur des procédés de démonstration prédéfinis portant sur des énoncés finis et ne faisant appel à aucune propriété douteuse de l'infini,
- *universelle* parce qu'on espérait que toutes les mathématiques passées et à venir pourraient entrer dans le cadre de ce formalisme.

Après l'échec du projet formaliste, ces espoirs démesurés peuvent sembler bien naïfs. Il faut pourtant voir qu'à l'époque, la théorie des ensembles semblait être un cadre de référence dans lequel toutes les mathématiques trouvaient leur place. Aujourd'hui encore c'est le point de vue de la plupart des mathématiciens.

La théorie des ensembles se serait-elle avérée formalisable au sens où l'espérait Hilbert, alors l'ensemble de son projet se serait révélé valide.

Pour expliquer les limites du formalisme, il est nécessaire d'avoir une idée un peu précise de ce qu'est :

- un *langage mathématique du premier ordre* (cf. A1),
- une *interprétation* (ou réalisation) de ce langage (cf. A2),
- un *modèle* d'un système d'axiomes de ce langage (cf. A3).

Il est en particulier nécessaire d'introduire la notion de *vérité sémantique* d'un énoncé du premier ordre interprété dans un modèle.

Il faut noter que tant la description d'un langage que la description de la notion de modèle utilisent une "théorie naïve" des ensembles. Par exemple, un langage est "un ensemble de mots". Les notions "d'objets" (tels que les lettres d'un alphabet ou les objets d'un modèle) et de "collection d'objets" sont donc admises a priori et ne peuvent être discutées qu'à un autre niveau. Néanmoins, les collections d'objets qu'on utilise (mots d'un langage ou objets d'un modèle) ont en général le mérite d'être "vraiment bien définies" (ceci est d'ailleurs plus vrai pour les mots d'un langage que pour les objets de certains modèles).

Remarquons enfin que d'autres tentatives de "formalisation de la vérité" en mathématiques sont possibles en se basant sur d'autres langages que les langages du premier ordre. Sans entrer dans le détail de ces autres langages, j'essaye en A4 d'expliquer quelles limitations a priori résultent de l'utilisation exclusive de "langages du premier ordre".

Je vous propose donc de suivre le plan suivant :

A Exposition d'un langage formel (celui de l'arithmétique) d'un système d'axiome (celui de Peano), de l'un de ses modèles (l'ensemble des entiers naturels).
B Première discussion sur la notion de vérité en mathématiques à travers l'exemple précédent. Théorème de complétude de Gödel.
C Les problèmes posés par la théorie des ensembles et par sa formalisation.
D L'insuffisance fondamentale des systèmes formels à travers le théorème d'incomplétude de Gödel et de le théorème de "non définissabilité de la vérité" de Tarski.
E Remarques sur le programme de Hilbert.
F Quelques conclusions.

A Le langage de l'arithmétique, les axiomes de Peano, le modèle standard

A1 Le langage de l'arithmétique

Le langage de l'arithmétique est un ensemble de "mots bien formés" à partir d'un alphabet qu'on va définir et de règles de formation des mots (qu'on n'explicitera que par des exemples).
Nous noterons par la suite $\mathcal{L}a$ le langage de l'arithmétique.
Ce sera donc un "ensemble intuitif" ou "collection" de mots.
L'*alphabet* est le suivant[1] :

deux symboles de constante	:	1 et 0
deux symboles fonctionnels	:	+ et ×
deux symboles relationnels	:	< et =
des symboles de variables	:	x, x', x'', x''' etc.
les connecteurs logiques	:	¬ ∧ ∨ ⇒ et ⇔
les quantificateurs	:	∀ et ∃
les parenthèses	:	) et (

L'alphabet qu'on vient de définir contient une infinité de symboles de variables, mais on peut se ramener à un alphabet fini en introduisant la barre verticale "|" et les symboles de variables sont alors écrits x, x|, x|| etc...

Venons en maintenant à la définition des *termes* du langage $\mathcal{L}a$, puis des *énoncés* du langage $\mathcal{L}a$.

Un *terme* (d'arithmétique) est alors un mot construit à l'aide des symboles de fonction, des symboles de constante, des symboles de variable, et des parenthèses, selon des règles qu'il serait fastidieux d'expliciter. Donnons plutôt des exemples de termes, nous les encadrerons pour souligner le fait que nous les considérons comme de pures écritures, destinées à être étudiées pour elles-mêmes (voir A2) :

$$\boxed{((((1+1)+x) \times x) \times x')}$$

est un terme.

$$\boxed{(((1+1)+1)+1) \times ((x \times x) \times x) \times (x'+1)}$$

est un terme.

Dans la pratique on utilise des notations abrégées usuelles. Le premier terme écrit ci-dessus se note alors $\boxed{(2+x)xx'}$, et le deuxième terme écrit ci-dessus se note $\boxed{4x^3(x'+1)}$.

Dans la suite, nous désignerons par $\mathcal{T}a$ la collection des *termes d'arithmétique* (bien écrits).

Un *énoncé atomique* est alors un mot de la forme :

$$\boxed{t = u} \qquad \text{ou} \qquad \boxed{t < u}$$

où t et u désignent deux termes.

---

[1] En ce qui concerne les connecteurs logiques, ils sont ici considérés comme lettres de l'alphabet $\mathcal{L}a$ et, lorsqu'ils seront "interprétés", ils prendront leur sens habituel, mais je m'efforcerai de les écrire alors en français ordinaire.

Un *énoncé d'arithmétique* (ou "une formule d'arithmétique") est alors soit un énoncé atomique, soit un mot construit à partir d'énoncés atomiques en utilisant les connecteurs logiques et les quantificateurs.

Exemples d'énoncés d'arithmétique

Nous noterons **R**(x) l'énoncé d'arithmétique suivant :

$$\exists a \exists b \exists c \exists d \quad x = a^2 + b^2 + c^2 + d^2$$

Dans l'énoncé (ou formule) **R**(x) la variable x est dite libre tandis que les autres variables a, b, c, d sont dites liées (ou "sous quantificateur")(2).
Remarquons que nous avons écrit en fait une notation abrégée pour l'énoncé suivant

$$\exists a \ \exists b \ \exists c \ \exists d \quad x = (a \times a) + (b \times b) + (c \times c) + (d \times d)$$

Nous noterons **S**(x) l'énoncé suivant(3) :

$$\exists a \ \exists b \ \forall z \ \forall t \ :$$

$$(zt=a \Rightarrow (z=1 \vee t=1)) \wedge (zt=b \Rightarrow (z=1 \vee t=1))$$

$$\wedge (x+x+4 = a+b) \wedge 1<a \wedge 1<b \ .$$

Dans cet énoncé, la variable x est libre et les autres variables sont liées.
On a utilisé les abréviations zt pour $z \times t$ et 4 pour $(((1+1)+1)+1)$ et on a supprimé quelques parenthèses.
Anticipons sur le paragraphe qui suit : l'interprétation de l'énoncé **R**(x) dans le modèle standard de l'arithmétique sera « x est une somme de 4 carrés». Quant à l'interprétation de l'énoncé **S**(x) dans le modèle standard, ce sera « 2x + 4 est la somme de deux nombres premiers».

Le *langage de l'arithmétique* est donc, pour récapituler, la *collection* des *énoncés d'arithmétique* bien écrits. Cette collection, nous la notons $\mathcal{L}a$.

A2 Une interprétation (ou réalisation) du langage $\mathcal{L}a$

Elle est définie par la donnée de :

- un ensemble intuitif (ou collection) N (4),
- deux éléments de N, notés 0 et 1,
- deux lois de composition interne sur N, notées + et ×,
- une relation binaire sur N, notée <.

Par "loi de composition interne sur N", on entend une application de $N \times N$ dans N, et par "relation binaire sur N" une application de $N \times N$ dans {Vrai, Faux}.

---

2 Nous utilisons la notation **R**(x) avec un caractère gras pour indiquer que **R**(x) désigne un énoncé d'arithmétique (mais ce n'en est pas un en tant qu'écriture).

3 Certains pièges doivent être évités dans les manipulations de quantificateurs. Dans une formule donnée, les variables liées peuvent a priori changer de nom sans que l'interprétation de la formule en soit affectée, mais certains renommages ont des effets désastreux. Par exemple dans l'énoncé $\exists x \quad x \neq y$ on peut renommer à peu près comme on veut la variable x mais le renommage y n'est évidemment pas autorisé.

4 N est parfois appelé la "collection des objets de l'interprétation" ou, dans le cas des modèles, " la collection sous- jacente du modèle"

Une réalisation du langage $\mathcal{L}a$ étant donnée, tout *terme d'arithmétique* peut être interprété comme un élément de N une fois qu'on a attribué à chaque symbole de variable figurant dans le terme une valeur comme élément de N. (pour interpréter un terme, il faut donc également interpréter les symboles de variables qui figurent dans le terme).

Toujours en considérant donnée une réalisation du langage $\mathcal{L}a$, tout énoncé d'arithmétique est alors interprété comme Vrai ou Faux selon les valeurs attribuées aux variables libres qui figurent dans l'énoncé.

Il faut naturellement donner aux connecteurs logiques et quantificateurs leur interprétation habituelle :

$A \wedge B$	est Vrai	si et seulement si	A et B sont Vrais
$A \vee B$	est Faux	si et seulement si	A et B sont Faux
$A \Rightarrow B$	est Faux	si et seulement si	A est Vrai et B est Faux
$\neg A$	est Vrai	si et seulement si	A est Faux
$\forall x\ U(x)$	est Vrai	si et seulement si	$U(x)$ est Vrai pour toute interprétation du symbole de variable x
$\exists x\ U(x)$	est Vrai	si et seulement si	$U(x)$ est Vrai pour au moins une interprétation de x

Enfin, le signe $\boxed{=}$ doit être interprété par la relation d'égalité.

La *réalisation standard* de $\mathcal{L}a$ consiste à prendre pour N la collection $\mathbb{N}$ des entiers naturels et, pour 0, 1, +, × et <, l'interprétation habituelle.

A3 Les axiomes et les modèles du système formel *Peano*

On va donner un système d'axiomes assez intuitifs pour décrire des propriétés vérifiées par la réalisation standard $\mathbb{N}$ du langage de l'arithmétique $\mathcal{L}a$. Ce système d'axiomes est une formalisation possible des axiomes qui avaient été proposés (de manière informelle) par Peano.
Le système formel *Peano* est donné par le langage $\mathcal{L}a$ et la collection de ces axiomes.
Les axiomes du système formel *Peano* sont des énoncés d'arithmétique, ils forment une sous collection de $\mathcal{L}a$. On ne va pas ici les écrire tous explicitement car ce serait un peu long et moins parlant.
Ce sont donc les énoncés suivants :

0 - Les énoncés exprimant la commutativité et l'associativité de + et ×, le fait que 0 et 1 sont des neutres pour l'addition et la multiplication, ainsi que la distributivité de + par rapport à ×. Par exemple :
$\boxed{(x + y) \times z = (x \times z) + (y \times z)}$.

1 - $\boxed{z + x = z + y \Rightarrow x = y}$

3 - $\boxed{\neg (1+x = 0)}$ (en abrégé : $\boxed{1 + x \neq 0}$)

4 - $\boxed{(x < y) \vee (x = y) \vee (y < x)}$

5 - $\boxed{x < y \Leftrightarrow \exists z\ x + z + 1 = y}$

6 - Le schéma d'axiomes, dit *schéma de récurrence*, qui, étant donné une relation $U(x)$ contenant x comme variable non quantifiée(5), fournit l'énoncé suivant :

5 la formule $U(x)$ peut contenir d'autres variables libres que x

$$\boxed{\left(\mathtt{U}(0) \wedge \left(\forall x \ (\mathtt{U}(x) \Rightarrow \mathtt{U}(x+1)) \right) \right) \Rightarrow \forall x \ \mathtt{U}(x)}\ .$$

Un *modèle de Peano* est (par définition) une interprétation du langage *La* dans laquelle les axiomes de *Peano* sont interprétés comme Vrais (pour toute interprétation des variables libres qui y figurent).

Le *modèle standard* du système formel *Peano* est l'interprétation standard qui est définie au paragraphe précédent.

On sait démontrer que l'énoncé $\boxed{\forall x \ \mathtt{R}(x)}$ (défini en fin de A1 et qu'on interprète dans le modèle standard par "tout entier est somme de 4 carrés") est interprété Vrai dans tout modèle de *Peano*.

Par contre, l'énoncé $\boxed{\forall x \ \mathtt{S}(x)}$ (où $\mathtt{S}(x)$ est défini en fin de A1 et qu'on interprète dans le modèle standard par "tout entier pair ≥ 4 est somme de deux nombres premiers") pose problème. Pour tout entier pair qu'on a voulu essayer, on a trouvé deux nombres premiers dont il est la somme :

$$12 = 7 + 5,\ 14 = 7 + 7,\ 28 = 17 + 11,\ \text{etc} \ldots$$

Mais on ne sait pas s'il est interprété Vrai dans le modèle standard, et on ne sait pas non plus s'il est possible qu'il soit interprété Vrai dans le modèle standard et Faux dans un autre.

A4 Utilité et limites du langage *La* pour étudier les propriétés des entiers naturels

Aux yeux des mathématiciens, le principal mérite d'un langage tel que *La* est avant tout qu'il permet d'écrire de manière extrêmement précise des textes concernant les entiers naturels.

La rançon de cette "clarté et précision" des propriétés qu'on peut écrire au moyen *d'énoncés d'arithmétique* (c'est-à-dire d'énoncés appartenant au langage *La*, c'est que le langage *La ne permet pas* d'écrire toutes les propriétés a priori intéressantes pour l'étude des entiers naturels.

Une propriété telle que "toute partie de $\mathbb{N}$ admet un plus petit élément" ne peut pas être écrite dans le langage *La*. C'est-à-dire, précisément : il n'existe aucun énoncé d'arithmétique dont l'interprétation dans le modèle standard soit la propriété énoncée ci-dessus. Pour quelle raison ? tout simplement parce que les parties de $\mathbb{N}$ qui peuvent être décrites comme "ensemble des entiers n vérifiant un énoncé d'arithmétique $\mathtt{U}(x)$ " ne sont pas *toutes* les parties de $\mathbb{N}$.

Donc, ce que l'on gagne en "clarification de la formulation des propriétés" on le perd sous forme de "restriction quant aux propriétés étudiées".

Mais, magie de la dialectique, cette "perte" est néanmoins source d'enrichissement car, désormais, une classification des propriétés concernant $\mathbb{N}$ est apparue : parmi les propriétés concernant $\mathbb{N}$, il y a celles qui sont les interprétations (standard) *d'énoncés d'arithmétique* et on les appelle les *propriétés arithmétiques* de $\mathbb{N}$. Les autres propriétés sont "plus complexes" et seront plus difficiles à étudier. Mais c'est déjà un bon renseignement que de savoir qu'une propriété est de nature arithmétique !(6)

---

6 Jusqu'à ce jour, on peut ranger les grandes conjectures mathématiques en deux groupes. Le premier groupe, formé des conjectures "sérieuses" est formé de problèmes concernant les mathématiques usuelles. Toutes ces conjectures sont prouvées équivalentes à des propriétés arithmétiques de $\mathbb{N}$. Le deuxième groupe est formé de conjectures concernant la théorie des ensembles. Dans ce dernier cas, ou bien on interprète ces conjectures en termes de systèmes formels, et elles sont ipso facto transformées en propriétés arithmétiques de $\mathbb{N}$ (par exemple, il y a des théorèmes d'arithmétique qui signifient que la théorie formelle des ensembles n'est pas

En particulier, on adoptera la définition suivante :

une partie de $\mathbb{N}$ est dite arithmétique si elle est la collection des entiers n qui vérifient (dans l'interprétation standard) un certain énoncé d'arithmétique $U(x)$ à une seule variable libre. (la variable x est interprétée par l'entier intuitif n)

De même, on définira :

une relation liant deux éléments de $\mathbb{N}$ est dite arithmétique s'il existe un énoncé d'arithmétique $V(x,y)$ tel que pour deux entiers naturels n , m arbitraires, n et m sont liés par la relation si et seulement si $V(x,y)$ s'interprète Vrai dans le modèle standard lorsqu'on donne à x et y les valeurs n et m .

B Première discussion sur la notion de vérité en mathématiques, à travers l'exemple des entiers naturels

V

Feuerbach, qui ne satisfait pas la pensée abstraite en appelle à l'intuition sensible mais il ne considère pas le monde sensible en tant qu'activité pratique concrète de l'homme.

Marx : thèses sur Feuerbach

B1 Objection intuitionniste

Pour définir la valeur "Vrai" ou "Faux" d'un énoncé d'arithmétique lorsqu'il est interprété au moyen d'une interprétation de *La* (par exemple lorsqu'il est interprété dans le modèle standard de *Peano*), nous avons fait comme si cela ne posait a priori aucun problème.

Autrement dit, nous avons implicitement admis comme évidente la notion de *vérité sémantique* d'un énoncé d'arithmétique une fois qu'il est interprété dans un modèle.
Regardons pourtant ce que signifie la phrase :

L'énoncé d'arithmétique $\boxed{\forall x\ S(x)}$ est interprété Vrai dans le modèle standard où $S(x)$ est l'énoncé défini en fin de A1.
Cette phrase signifie :

Tout nombre entier pair ≥ 4 est somme de deux nombres premiers.

Pour infirmer ce résultat : "il suffit" d'une vérification : trouver un entier pair n ≥ 4 . Établir la liste des nombres premiers inférieurs à n , et vérifier que la somme de deux d'entre eux n'est jamais égale à n .
Pour confirmer ce résultat : il faut, soit une démonstration convaincante, soit (si on n'en trouve pas) une infinité de vérifications : pour tout entier pair ≥ 4, il faut trouver deux nombres premiers dont il est la somme.
Or, Homo Sapiens ne sait pas, et ne saura jamais, faire une infinité de vérifications en un temps fini. Penser qu'a priori l'énoncé $\forall x\ S(x)$ est nécessairement interprété Vrai ou Faux dans le modèle standard réclame donc de croire en un "dieu de $\mathbb{N}$ " qui soit capable de faire, lui,

---

plus contradictoire avec l'axiome du choix ou avec sa négation, avec l'hypothèse du continu ou avec sa négation, etc..., ce qui a d'une certaine manière "résolu" les conjectures de l'axiome du choix et de l'hypothèse du continu), ou bien on interprète ces conjectures dans un hypothétique univers cantorien, et personne ne peut dire à l'heure actuelle que ce sont des conjectures ayant la moindre signification mathématique. Surement les logiciens ont du mettre au point des conjectures sérieuses concernant des propriétés non arithmétiques de $\mathbb{N}$ mais cela n'a pas "percé" dans la communauté des mathématiciens non spécialistes de logique.

l'infinité de vérifications nécessaires. C'est croire que "la vérité dans $\mathbb{N}$ " existe indépendamment de la pratique d'Homo Sapiens.

Si on introduit des formules plus compliquées que $\forall x\ S(x)$, avec des quantificateurs en cascade, du type :

$$\forall x\ \exists y\ \forall z\ W(x,y,z)$$

on s'apercevra qu'en général (c'est-à-dire lorsqu'on ne dispose pas de démonstration convaincante) il faudra une infinité de vérifications aussi bien pour infirmer que pour confirmer la vérité d'un énoncé d'arithmétique une fois qu'il est interprété dans le modèle standard, et même des infinités emboîtées de vérifications ...

B2 Pour contourner cette objection des intuitionnistes, il peut exister deux attitudes possibles

Ou bien on pense que l'objection n'est pas fondée car de toute manière "ou bien tout nombre pair est somme de deux nombres premiers, ou bien ce n'est pas vrai" et ainsi de suite pour tous les énoncés d'arithmétique (c'est-à-dire rappelons-le, les énoncés de $\mathcal{L}a$) interprétés dans le modèle standard.

Ou bien on ignore le problème de l'interprétation du langage, on ignore le problème de la vérité sémantique et on fait comme si on n'étudiait que les propriétés du langage pour lui-même. C'est le point de vue formaliste poussé à l'extrême, tel qu'il est exposé dans l'introduction de Bourbaki. Mais ce un point de vue, en apparence confortable, est complètement débilitant et réduit l'activité des mathématiciens à l'étude d'un *jeu* particulier : celui du "langage de la théorie mathématique" dans lequel on cherche les combinaisons gagnantes (théorème R) et les combinaisons perdantes (théorème $\neg R$); les combinaisons indéterminées (ni R , ni $\neg R$ n'est un théorème) ne faisant d'ailleurs même pas partie de l'étude du jeu tel que la définit Bourbaki.

Dans la suite de ce texte, j'adopterai la terminologie suivante :

> Le *point de vue intuitionniste* (pour $\mathbb{N}$ et $\mathcal{L}a$) est l'attitude qui consiste à n'admettre pour "Vrai" ou "Faux" a priori dans le modèle standard que les énoncés d'arithmétique pour lesquels on dispose d'une démonstration convaincante (par exemple un processus de vérification aboutissant en un temps fini). Cette attitude implique qu'on refuse la loi du Tiers Exclu dans les "démonstrations convaincantes" dont il est question.
>
> Le *point de vue classique* (pour $\mathbb{N}$ et $\mathcal{L}a$) est l'attitude qui consiste à admettre que tout énoncé d'arithmétique est forcément Vrai ou Faux une fois qu'il est interprété dans le modèle standard.
>
> Le *point de vue formaliste* (pour $\mathcal{L}a$ et les axiomes de $\mathcal{P}eano$) consiste à ignorer le modèle standard $\mathbb{N}$, à refuser de se poser la question de la vérité sémantique dans l'interprétation standard, et à étudier la théorie formelle $\mathcal{P}eano$ basée sur le langage $\mathcal{L}a$ pour elle-même.

Ce dernier point de vue n'est cependant pas aussi absurde que ce qu'il peut paraître au premier abord. Pour le comprendre, il faut qu'il soit expliqué un peu plus en détail. C'est ce qui est fait dans le paragraphe qui suit.

B3 Description rapide (et informelle) de la théorie formelle "arithmétique de Peano"

Au lieu de rechercher quels sont les énoncés d'arithmétique qui sont interprétés "Vrai" dans le modèle standard, on recherche quels sont tous les énoncés d'arithmétique "qu'on peut déduire des axiomes de *Peano* au moyen de règles de déduction logique répertoriées et considérées valables d'un point de vue classique".

Ces "règles de déduction logique répertoriées considérées valables d'un point de vue classique" constituent ce qu'on appelle la *logique formelle* (classique) des langages du premier ordre (c'est-à-dire des langages semblables à $\mathcal{La}$).
La collection des énoncés d'arithmétique ainsi obtenus est appelée la "collection des théorèmes formels du système formel *Peano*". (on dit souvent "arithmétique de Peano" au lieu de "système formel *Peano*")
Si on note $\mathcal{P}_1$ le système d'axiomes de *Peano*, on note alors $\mathrm{Tf}(\mathcal{La},\mathcal{P}_1)$, ou $\mathrm{Tf}(\mathcal{Peano})$ la collection des théorèmes formels de l'arithmétique de *Peano*.
On voit qu'ici, on a une double limitation a priori :

- La limitation dont on a déjà parlé en A4 : on ne s'intéresse qu'aux "énoncés d'arithmétique" lesquels, une fois interprétés dans $\mathbb{N}$, ne traduisent que certaines des propriétés de $\mathbb{N}$.
- On ne s'intéresse qu'aux énoncés "qui peuvent se déduire d'un nombre fini d'axiomes", ou du moins d'axiomes parfaitement bien définis a priori.

Si on se place d'un point de vue classique, tous les "théorèmes de l'arithmétique de Peano" sont "vrais" lorsqu'interprétés dans $\mathbb{N}$ parce que la logique formelle utilisée (c'est-à-dire les règles de déduction logique répertoriées utilisées) sont valables du point de vue classique et que les axiomes eux-mêmes sont vrais dans $\mathbb{N}$.
Si on se place d'un point de vue intuitionniste, certains "théorèmes de l'arithmétique formelle de *Peano*" ne sont pas forcément interprétés "Vrai" dans $\mathbb{N}$, parce que la logique formelle utilisée n'est pas valable (les axiomes, eux, ne posent pas problème).
Le point de vue formaliste "à outrance" ignore tout simplement le débat sur la nature de la vérité sémantique.

Le *programme de Hilbert* pour l'arithmétique peut être rephrasé comme suit. Dans sa version la plus forte (un peu folle), le programme de Hilbert demande une méthode mécanique capable de décider la vérité ou la fausseté de n'importe quel d'énoncé d'arithmétique de structure suffisamment simple([7]). Dans sa version raisonnable, le programme de Hilbert demande qu'un système mécanique capable de produire beaucoup de théorèmes en arithmétique (par exemple le système formel *Peano*) puisse être prouvé efficace (c.-à-d. ne jamais se tromper de manière flagrante) en utilisant uniquement des arguments d'une nature extrêmement simple([8]).

---

7 Nous tâcherons de sortir de ce flou dans la dernière partie, consacrée au programme de Hilbert.

8 Il semble difficile de préciser mieux le programme de Hilbert sans donner des définitions techniques un peu dures à digérer. Néanmoins, lorsque nous parlerons du théorème d'incomplétude de Gödel en D2, il sera clair, sans besoin d'aucune définition technique, que ce théorème ruine définitivement le programme de Hilbert pour l'arithmétique. Dans la partie E, nous essaierons de montrer qu'une version légèrement affaiblie de ce programme reste d'une très grande pertinence.

B4 Les règles de la logique formelle (pour un langage du premier ordre) sont "entièrement satisfaisantes" du point de vue classique (théorème de complétude de Gödel)

Cette affirmation, que je vais essayer d'expliquer, est évidemment d'un grand soulagement pour les formalistes à outrance, car ça leur permet de garder dans un coin de leur tête (mais sans le dire) que tout ce qui se fait en mathématiques formelles a quelque chose à voir avec "le sens" et la "réalité".

Rappelons ici qu'un langage du premier ordre est un langage $\mathcal{L}$ du même type que $\mathcal{L}a$ mais où on s'autorise à prendre d'autres symboles de fonction, d'autres symboles relationnels et d'autres symboles de constante que ceux de $\mathcal{L}a$.
Rappelons aussi que la *logique formelle classique* est un ensemble de règles de manipulations d'énoncés de $\mathcal{L}$ qui, lorsque ces énoncés sont "interprétés", constituent des règles de déduction logique valables d'un point de vue classique.
Du point de vue formel, ces règles sont de simples manipulations d'énoncés. Par exemple, une de ces règles est la suivante : si $A \Rightarrow B$ et si A font partie de la collection des théorèmes formels, alors, par la règle dite Modus Ponens, B fait également partie de la collection des théorèmes formels.

Dans ce cadre, le théorème de Gödel (de complétude) établit une *adéquation parfaite* entre, *d'une part* :

(1) les énoncés du langage $\mathcal{L}$ du premier ordre démontrables au moyen de la logique formelle classique

et, *d'autre part* :

(2) les énoncés prenant la valeur Vrai dans toute interprétation du langage du premier ordre considéré.

Évidemment, l'adéquation parfaite démontrée dans le théorème de Gödel est démontrée, dans le sens (1) implique (2), au moyen de raisonnements sur les modèles faisant appel à des principes de déduction logiques valables d'un point de vue classique uniquement. En ce qui concerne le sens (2) implique (1), la preuve du théorème de Gödel utilise un principe de construction d'ensembles basé sur un usage systématique du principe du Tiers Exclu concernant des énoncés d'arithmétique a priori non décidables. Bref, l'adéquation parfaite n'est parfaite que du point de vue des mathématiques classiques, et elle nécessite une réinterprétation constructive(9).

Néanmoins, il est important de noter que la phrase

"énoncé prenant la valeur Vrai dans *toute* interprétation du langage considéré"

peut être comprise dans un sens relativement faible, qui est précisé maintenant :
on peut se limiter aux interprétations où la collection des objets est, ou bien finie, ou bien est la collection des entiers naturels $\mathbb{N}$ et, dans le cas où la collection des objets est $\mathbb{N}$, on peut se limiter aux interprétations où les symboles relationnels et les symboles fonctionnels peuvent être définis arithmétiquement (voir A4 par exemple pour la définition d'une relation binaire arithmétique dans $\mathbb{N}$).
Autrement dit et plus précisément :

si un énoncé $\mathbf{E}$ d'un langage $\mathcal{L}$ (du premier ordre) n'est pas un théorème de logique formelle classique, on peut trouver une "interprétation arithmétique" des symboles (de

9 Du moins si on est convaincu de la pertinence du point de vue constructif

constante, de fonction, de relation) figurant dans le langage $\mathcal{L}$, tel que l'énoncé $\mathbf{E}$ soit interprété Faux.

À ce résultat de complétude (d'entière satisfaction) de la logique formelle du premier ordre, il faut opposer trois faits importants :

- ce résultat n'est établi que pour les langages du premier ordre, lesquels introduisent a priori une limitation dans l'étude des propriétés d'un objet mathématique (tel que $\mathbb{N}$ par exemple),
- la logique formelle utilisée dans le système formel, et la logique concrète mise en oeuvre dans la preuve du théorème de complétude ne sont pas acceptables d'un point de vue intuitionniste, cela signifie que le théorème de complétude de Gödel nécessite une relecture complète du point de vue constructif
- du point de vue classique comme du point de vue constructif, aucun système d'axiome raisonnable ne permet de décrire entièrement les propriétés arithmétiques de $\mathbb{N}$ (c'est le théorème d'incomplétude de Gödel, qui sera discuté plus loin).

C Les problèmes posés par la formalisation de la théorie des ensembles et par la théorie des ensembles elle-même

C1 Deux actes de foi de la théorie des ensembles

Nous avons déjà remarqué dans l'introduction qu'un minimum de théorie naïve des ensembles est nécessaire pour développer toute théorie mathématique.
On a besoin de la notion d'objets distincts, on a besoin de savoir repérer que deux signes d'un alphabet sont "les mêmes" alors qu'ils sont écrits en deux endroits distincts de la page, on a aussi besoin de la notion de "collection potentiellement infinie" aussi bien pour définir un objet d'études mathématiques (par exemple : la collection potentiellement infinie des entiers naturels) que pour développer une théorie formelle (la collection potentiellement infinie des mots d'un langage du premier ordre).
Avec l'avènement de la théorie des ensembles, il s'est agi de tout autre chose et Cantor avait bien raison (de son point de vue) de remercier Dieu d'avoir créé un "univers mathématique" infini dans lequel on peut sans scrupule :

- considérer un ensemble infini tel que $\mathbb{N}$ comme un infini "actuel" (et non potentiel),
- considérer, une fois qu'un ensemble "existe" que toute partie de cet ensemble "existe" également, pour elle-même, en dehors du fait qu'elle puisse être pensable ou non par un homme, et même :
- construire, pour tout ensemble donné A, l'ensemble de toutes les parties de cet ensemble ("beaucoup plus gros" que A),

Avec l'univers mathématique de Cantor (ou plutôt celui de Zermelo-Frankel qui a permis d'éliminer tous les paradoxes apparus à ce jour dans celui de Cantor) nous voici dans le royaume de la vérité sémantique absolue.
Les mathématiques sont désormais l'étude de cet univers à la fois monstrueux et admirable, dont certaines des propriétés resteront à tout jamais cachées aux Homo Sapiens, mais qu'importe.

Et, chose remarquable, si un tel univers existe et peut être soumis aux investigations par les méthodes relevant de la logique classique (répertoriées dans la logique formelle), alors on peut

définir en son sein d'autres Univers qui ont les mêmes propriétés de base (que celles énoncées précédemment) et qui, en outre, vérifient d'autres propriétés particulièrement commodes pour les raisonnements mathématiques.
Par exemple, l'axiome du choix, un temps controversé, est devenu un vulgaire "axiome des parallèles d'Euclide" : aucun danger à considérer qu'il est vrai puisque, si un univers mathématique existe *sans* axiome du choix, on pourra construire avec lui un autre univers mathématique *avec* axiome du choix (de la même manière que l'existence d'une géométrie euclidienne garantit l'existence d'une géométrie non euclidienne et vice versa).
Il y a pourtant une différence de taille entre la géométrie euclidienne et la théorie des ensembles.
La différence est la suivante :

- tout mathématicien qui croit en le modèle standard de l'arithmétique croit du même coup en la géométrie euclidienne car on peut construire sur la collection $\mathbb{N}$ une géométrie euclidienne (certains éléments de $\mathbb{N}$ étant appelés "points", d'autres "droites", d'autres "plans", d'autres "cercles", d'autres "sphères", et étant définis entre eux les relations "le point est sur la droite", "la droite est dans le plan" etc... , le tout vérifiant les axiomes d'une géométrie euclidienne(10)). De plus, cette construction sera parfaitement explicite, y compris la vérification des axiomes de la géométrie euclidienne dans le modèle : il s'agit donc d'une géométrie euclidienne satisfaisante d'un point de vue intuitionniste.
- mais tout mathématicien qui croit en le modèle standard de l'arithmétique ne croit pas forcément pour autant à l'univers mathématique de Zermelo-Frankel .

A cela deux ordres de raison :

- Dans la croyance en l'existence d'un univers mathématique à la Zermelo-Frankel, il y a véritablement deux "actes de foi" qui surpassent de loin "l'acte de foi en l'arithmétique", ce sont :
  - l'acte de foi de l'infini actuel,
  - l'acte de foi de l'ensemble des parties d'un ensemble.

  Comme l'univers mathématique de Zermelo-Frankel, s'il existe, contient des ensembles infinis non dénombrables (c'est-à-dire, pour le mathématicien classique, "strictement plus gros que $\mathbb{N}$ ") un mathématicien classique ne peut espérer disposer un jour d'une construction analogue à celle de la géométrie euclidienne, pour un univers mathématique au sein de $\mathbb{N}$.
- si, au lieu de considérer comme possible, de manière purement abstraite, l'existence d'un univers mathématique à la Zermelo-Frankel, on considère seulement comme très probable le fait que les axiomes de Zermelo-Frankel sont non contradictoires, on peut alors construire (à l'aide du théorème de complétude de Gödel, qui a pour conséquence que tout système d'axiomes "bien défini"(11) et non contradictoire possède un modèle, et même un modèle arithmétique) un "modèle réduit" d'univers mathématique construit dans $\mathbb{N}$, pour lequel tous les axiomes de $\mathcal{ZF}$ sont interprétés "Vrai". Dans ce cas, on se trouve néanmoins confronté à trois problèmes d'importance :
  - le fait que le "modèle réduit" d'univers mathématique n'est vraiment que le pâle reflet de l'univers mathématique "réel" puisque tous les "ensembles dans le modèle", s'ils

---

10 Par exemple si on choisit comme axiomes un système décrivant les propriétés d'un plan "euclidien" construit sur un corps "réel clos", où un corps réel clos est défini comme un corps ordonné dans lequel les fonctions polynomes vérifient le théorème de la valeur intermédiaire. Ce genre de cadre est le cadre le plus simple où on puisse réaliser le programme de Descartes d'algébrisation des théorèmes de géométrie.

11 Par exemple un système d'axiomes fini, ou un système d'axiomes infini mais engendré par un processus parfaitement explicite.

ne sont pas "dénombrables dans le modèle", sont néanmoins "dénombrables hors du modèle" (en effet, ces "ensembles dans le modèle" peuvent tous être définis comme des parties arithmétiques de $\mathbb{N}$)

— le fait que le "modèle réduit" d'univers mathématique possède des propriétés de type pathologique (voir les résultats de Rabin paragraphe suivant),

— le fait enfin que la construction du modèle réduit n'est possible que si les axiomes de $\mathcal{ZF}$ sont non contradictoires, or Homo Sapiens ne sait pas, et ne saura sans doute jamais, si les axiomes de $\mathcal{ZF}$ sont non contradictoires (voir D).

C2 À propos des modèles réduits arithmétiques de l'Univers à la Cantor-Zermelo-Fraenkel

Ces résultats de M.O. Rabin concernent les "modèles réduits" dénombrables d'univers mathématique ou, si l'on préfère, les "modèles ayant comme collection d'objets les entiers naturels".
Le système d'axiomes utilisé n'est pas $\mathcal{ZF}$ mais une version affaiblie du système $\mathcal{GB}$ ($\mathcal{GB}$ comme : Gödel Bernays). Je vais décrire rapidement et informellement ce système d'axiomes affaibli que je noterai $\mathcal{GB}^-$, mais précisons tout de suite que $\mathcal{ZF}$ et $\mathcal{GB}$ sont fondamentalement équivalents (au même sens que géométrie euclidienne et non euclidienne sont fondamentalement équivalentes).

Décrivons tout d'abord le langage utilisé (qui est le même pour $\mathcal{ZF}$ ou $\mathcal{GB}$) :

- il y a un seul symbole de constante : $\boxed{\emptyset}$
- il n'y a pas de symbole de fonction
- il y a deux symboles de relation : $\boxed{=}$ et $\boxed{\in}$
- il y a enfin les symboles logiques communs à tous les langages du premier ordre.

On notera $\mathcal{Le}$ ce "langage de la théorie des ensembles".
Les axiomes de $\mathcal{GB}$ décrivent un univers mathématique hypothétique $\mathbb{U}$ où il y a deux types d'objets : d'une part les ensembles, d'autre part les classes. Tout ensemble est une classe (donc tout objet est une classe), toute classe est entièrement définie par les ensembles qui lui appartiennent, mais certaines classes sont "trop grosses" pour être des ensembles (par exemple la classe de tous les ensembles).
Dans un univers mathématique de $\mathcal{GB}$, l'énoncé :

$$\boxed{\exists\, x \quad y \in x}$$

s'interprète donc dans $\mathbb{U}$: y est un ensemble
et l'énoncé :

$$\boxed{\forall\, x \quad \neg\, (\, y \in x\,)}$$

s'interprète dans $\mathbb{U}$: y est une classe propre (une classe qui n'est pas un ensemble).

Voici donc les axiomes de $\mathcal{GB}^-$ (cf. annexe pour leur écriture sous forme d'énoncés de $\mathcal{Le}$) :
– pour les classes (classes propres ou ensembles) :

- il existe une classe contenant tous les ensembles : W
- il existe une classe contenant tous les couples d'ensembles (x, y) tels que $x \in y$
- si deux classes A et B existent alors $A \cap B$, $A \cup B$, $A \times B$, $W - A$ existent également,
- deux classes qui ont les mêmes éléments sont égales
- si une classe A existe, alors la classe : $\mathrm{Dom}(A) = \{\, x \mid \exists\, y \ (x,y) \in A \,\}$ existe également

- quatre axiomes annexes introduits pour des raisons techniques (et qui ne posent pas réellement problème)

– pour les ensembles (du modèle) :

- les axiomes habituels de $\mathcal{ZF}$, sans l'axiome de l'ensemble infini ni l'axiome du choix, et en remplaçant un schéma d'axiome dit "schéma de substitution" par un seul axiome, grâce au recours des classes.

Notez que le système d'axiomes est fini et peut donc être remplacé par un axiome unique.
Dans les modèles de $\mathcal{GB}^-$, on n'a pas besoin d'ensemble infini, mais on a une classe de tous les ensembles finis. Ce système formel est donc une manière d'accepter le premier acte de foi, l'existence d'un infini actuel, en omettant le second, l'existence de l'ensemble des parties d'un ensemble infini.

Décrivons maintenant un "modèle naturel" de $\mathcal{GB}^-$, plus crédible qu'un univers de $\mathcal{GB}$ (dans lequel il y a nécessairement non seulement des classes infinies, mais aussi des "ensembles" infinis). Pour décrire ce "modèle naturel ", nous nous plaçons d'un point de vue "théorie naïve des ensembles finis". Nous considérons alors toutes les collections finies qui peuvent être "écrites à la main" en utilisant les symboles $\emptyset$, { , et } . Par exemple :

$$\emptyset\ ;\ \{\emptyset\}\ ;\ \{\emptyset, \{\emptyset\}\}\ ;\ \{\emptyset, \{\{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}\}\ .$$

Toutes ces collections finies peuvent être obtenues comme éléments des collections finies $\mathbb{V}_n$, construites par récurrence comme suit :

$$\mathbb{V}_0 = \emptyset \qquad \mathbb{V}_1 = \mathcal{P}(\mathbb{V}_0) = \{\emptyset, \{\emptyset\}\}$$

$$\mathbb{V}_2 = \mathcal{P}(\mathbb{V}_1) = \{\emptyset\ ,\ \{\emptyset\}\ ,\ \{\{\emptyset\}\}\ ,\ \{\emptyset\ ,\ \{\emptyset\}\}\}$$

$$\mathbb{V}_{n+1} = \mathcal{P}(\mathbb{V}_n) \qquad (\mathcal{P}(A) \text{ est la collection des parties de A})$$

Pour construire notre "modèle naturel", nous posons tout d'abord :

$$\mathbb{V}_\omega = \bigcup_{n \in \mathbb{N}} \mathbb{V}_n$$

puis

$$\mathbb{W} = \mathcal{P}(\mathbb{V}_\omega)\ .$$

Enfin nous considérons $\mathbb{W}$ comme collection des objets du "modèle naturel", et nous interprétons $\boxed{\in}$ par $\in$ dans $\mathbb{W}$. Je dis qu'on obtient un modèle de $\mathcal{GB}^-$.
En effet, on démontre par récurrence que $\mathbb{V}_n \subset \mathbb{V}_{n+1}$, puis que toute partie finie de $\mathbb{V}_\omega$ est un élément de $\mathbb{V}_\omega$.
Par ailleurs, tout élément de $\mathbb{V}_\omega$ est une partie finie de $\mathbb{V}_\omega$. Donc $\mathbb{V}_\omega \subset \mathbb{W}$ et on a :

- tout objet du modèle est une partie de $\mathbb{V}_\omega$.
- les parties finies de $\mathbb{V}_\omega$ sont les "ensembles" du modèle, .
- les parties infinies de $\mathbb{V}_\omega$ sont les "classes propres" du modèle.

On vérifie facilement que les axiomes de $\mathcal{GB}^-$ sont vérifiés dans ce "modèle naturel".
Ce "modèle naturel" $\mathbb{W}$ et ce système d'axiomes $\mathcal{GB}^-$ constituent en quelque sorte le degré zéro de la théorie des ensembles infinis de Cantor, le point précis où I'on décolle du point de vue purement "naïf" ("intuitif"). En fait, structurellement le triplet $(\mathbb{V}_\omega, \mathbb{W}, \in)$ est "isomorphe"(12) au triplet $((\mathbb{N}, +, \times, 0, 1, <), \mathcal{P}(\mathbb{N}), \in)$
Pour tout mathématicien qui croit en $\mathbb{W}$ et qui croit en la logique formelle classique lorsqu'elle est interprétée dans $\mathbb{W}$, le système d'axiome $\mathcal{GB}^-$ est manifestement non contradictoire (de la même manière qu'un mathématicien qui croit en $\mathbb{N}$ et en la logique formelle lorsqu'elle est interprétée dans $\mathbb{N}$ pense du même coup que le système d'axiome de *Peano* est non

12 Représente le même degré de complexité logique

contradictoire).
Par ailleurs, si un mathématicien classique considère le modèle $(\mathbb{V}_\omega, \mathbb{W}, \in)$ comme un modèle extrêmement naturel de $\mathcal{GB}^-$, c'est parce qu'il pense que $\mathcal{P}(\mathbb{V}_\omega)$ n'est absolument pas problématique. Pour un mathématicien qui pense que $\mathcal{P}(\mathbb{V}_\omega)$ est, tout comme $\mathcal{P}(\mathbb{N})$, un objet bien mystérieux et sans doute problématique, le système formel peut être vu, soit comme un "mauvais système d'axiomes" ne correspondant à aucune réalité mathématique, soit comme un moyen d'investigation d'une réalité mathématique sensiblement distincte du $\mathcal{P}(\mathbb{V}_\omega)$ des mathématiciens classiques.

Les deux résultats de Rabin concernent les "modèles réduits" du système d'axiomes $\mathcal{GB}^-$. Si ce système est non contradictoire, il admet, d'après une conséquence du théorème de complétude de Gödel, un modèle dénombrable et même un modèle arithmétique (c'est-à-dire, rappelons-le, un modèle où la collection des objets est $\mathbb{N}$ et où la relation $\subseteq$ (qui interprète le symbole $\boxed{\in}$ est une relation arithmétique).

Premier résultat :

> Il est impossible de trouver une fonction $n \longmapsto (x_n, y_n)$ parfaitement explicite de $\mathbb{N}$ dans $\mathbb{N} \times \mathbb{N}$, telle que la collection des couples (x_n, y_n) soit la collection des couples vérifiant $x_n \subseteq y_n$, où "$\subseteq$" est une relation binaire sur $\mathbb{N}$ qui vérifie les axiomes de $\mathcal{GB}^-$.

Autrement dit : il n'y a pas de modèle réduit "simple" pour $\mathcal{GB}^-$.(13)
Si maintenant on considère des modèles structurellement plus compliqués, on a :

Deuxième résultat :

> Considérons sur $\mathbb{N}$ une relation binaire arithmétique, que nous notons $\subseteq$, qui fasse de $(\mathbb{N}, \subseteq)$ un modèle arithmétique de $\mathcal{GB}^-$. Alors ce modèle est "non standard pour les entiers", c'est-à-dire :
> ce qui, dans ce modèle, joue le rôle de la "classe propre des entiers naturels" contient non seulement les analogues de 0, 1, 2, 3 etc . . . mais encore des tas d'autres éléments, appelés "entiers non standard".

Autrement dit : si on se place sur une position où on admet comme crédibles les "parties de $\mathbb{N}$ définies de manière arithmétique", mais pas d'autres collections plus compliquées, alors $\mathcal{GB}^-$ n'admet pas non plus de modèle "satisfaisant".
En fait ce résultat n'est pas si surprenant. La théorie formelle $\mathcal{GB}^-$ est assez puissante pour traduire *Peano* et elle permet donc de définir une classe pour toute partie arithmétique de $\mathbb{N}$. Ce qui, avec *Peano* relevait du métalangage, relève maintenant du langage lui-même. En conséquence le procédé diagonal de Cantor produit, dans le métalangage, des parties de $\mathbb{N}$ plus compliquées que n'importe quelle partie arithmétique (ce qui n'était pas le cas avec *Peano*). C'est cela qui fait que, si on se limite aux modèles arithmétiques, (notez que la question des modèles relève du métalangage), des comportements pathologiques apparaissent inévitablement.
Un mathématicien classique peut relire le deuxième résultat de Rabin sous la forme positive suivante : si on désire un modèle $(\mathbb{N}, \subseteq)$ pour $\mathcal{GB}^-$ dans lequel les "entiers du modèle" sont tous standards, il faut que la relation $\subseteq$ sur $\mathbb{N}$ soit plus compliquée qu'une relation arithmétique.

---

13 En langage plus savant: il n'existe pas de modèle énuméré pour lequel la relation d'appartenance soit récursivement énumérable

Signalons en conclusion que la situation sera évidemment encore diablement plus compliquée si on considère les modèles de la théorie $\mathcal{GB}$ avec axiome de l'infini.

D L'insuffisance fondamentale des systèmes formels

Dans le premier paragraphe, j'explique en quoi la recherche des théorèmes d'une théorie formelle (pour un langage du premier ordre donné et pour un système d'axiomes bien défini de ce langage) est équivalente à l'étude *d'une* fonction bien définie de $\mathbb{N}$ dans $\mathbb{N}$.
Ce simple fait inciterait déjà fortement à douter de la capacité d'une théorie formelle à être la traduction de la notion de vérité en mathématiques.
Dans le deuxième paragraphe, j'essaie d'expliquer ce que signifie le théorème d'incomplétude de Gödel : ce théorème précise de manière très frappante un point où réside cette "incapacité" d'une théorie formelle. Elle réside dans l'incapacité à démontrer "sa propre non contradiction".
Dans le troisième paragraphe, j'explique en quoi ce résultat absolument remarquable de Gödel peut être interprété pour apporter de l'eau au moulin des intuitionnistes.
Dans le quatrième paragraphe, j'essaie d'expliquer ce que signifie le théorème de "non-définissabilité de la vérité" de Tarski. Ce théorème se situe sur un terrain légèrement différent du théorème d'incomplétude de Gödel, il ne s'attaque pas à la notion de théorie formelle mais seulement à la notion de langage formel et il affirme qu'un langage formel est incapable de décrire "sa propre vérité sémantique" dans une interprétation donnée.

D1 Arithmétisation d'une théorie formelle du premier ordre

Nous considérons donc un langage du premier ordre $\mathcal{L}$ analogue à $\mathcal{L}a$ (c'est-à-dire avec les mêmes symboles logiques, mais avec des symboles de fonction, de constante et de relation différents) et un système $\mathcal{A}$ d'axiomes bien définis écrits dans $\mathcal{L}$. Autrement dit $\mathcal{A}$ est une sous-collection explicite de la collection des énoncés de $\mathcal{L}$.

La théorie formelle de $(\mathcal{L},\mathcal{A})$ est définie de la même manière que la théorie formelle *Peano* de l'arithmétique. Cela signifie que les théorèmes formels de $(\mathcal{L},\mathcal{A})$ forment la collection des énoncés de $\mathcal{L}$ qui peuvent être déduits des énoncés de $\mathcal{A}$ au moyen des règles de la logique formelle classique. Rappelons que nous notons $\mathrm{Tf}(\mathcal{L},\mathcal{A})$ la collection des théorèmes (formels) de cette théorie formelle.

Nous commençons par numéroter les énoncés de $\mathcal{L}$ (c'est-à-dire attribuer un numéro, qui est un entier naturel ordinaire, à chaque énoncé de $\mathcal{L}$). Voici comment cela fonctionne :

- tout d'abord on range dans un certain ordre les symboles de l'alphabet de $\mathcal{L}$ (on supposera pour simplifier cet alphabet fini),
- ensuite, on remarque que si un mot est écrit au moyen de cet alphabet, on peut déterminer par un processus explicite si ce mot est un énoncé (bien écrit) de $\mathcal{L}$ ou non,
- enfin on remarque que les énoncés bien écrits qui ont une longueur déterminée n sont en nombre fini et peuvent donc être rangés par ordre alphabétique,
- alors, pour obtenir le numéro d'un énoncé de $\mathcal{L}$, on compte d'une part tous les énoncés qui ont une longueur plus petite et d'autre part tous les énoncés qui ont même longueur mais qui le précèdent dans l'ordre alphabétique. La somme des deux nombres obtenus est le numéro de notre énoncé. Par exemple, l'énoncé le plus court et le premier par ordre alphabétique (parmi les énoncés de même longueur) a pour numéro 0,
- on voit que ce processus permet d'établir une correspondance entre $\mathbb{N}$ et $\mathcal{L}$ telle qu'à tout nombre soit associé un et un seul énoncé (qui ait ce nombre pour numéro).

On peut alors énoncer le théorème d'arithmétisation comme suit :

Théorème d'arithmétisation d'une théorie formelle

Soit $\mathcal{L}$ un langage du premier ordre et soit $\mathcal{A}$ un système d'axiomes bien défini de $\mathcal{L}$ (par exemple un système d'axiomes fini).
Soit $n \longmapsto \mathbb{E}_n$ une numérotation explicite des énoncés de $\mathcal{L}$.
Il existe une fonction parfaitement explicite : $f : n \longmapsto f(n)$
de $\mathbb{N}$ dans $\mathbb{N}$, telle que la collection des nombres $m = f(n)$ soit exactement la collection des numéros des théorèmes formels du système formel $(\mathcal{L}, \mathcal{A})$.

NB : L'expression "fonction parfaitement explicite de $\mathbb{N}$ dans $\mathbb{N}$" est justifiable d'une définition qui précise le sens intuitif qu'on lui attribue. Ici on peut fournir un processus explicite qui, à partir du numéro n permet de calculer le numéro $f(n)$. Ce processus est décrit informellement dans la preuve qui suit.

Le théorème d'arithmétisation n'est pas très difficile à démontrer mais demanderait quelques détails techniques. Disons que comme la collection $\mathcal{A}$ est bien définie et comme les règles de la logique formelle sont elles aussi bien définies, on peut définir de manière explicite ce qu'est une "démonstration formelle", et on peut numéroter les "démonstrations formelles" (de la même manière à peu près qu'on a numéroté $\mathcal{L}$). Enfin, un "théorème formel" est un énoncé pour lequel il existe une démonstration formelle. La fonction f est donc la fonction qui, à un entier naturel n, fait correspondre le numéro (pour la numérotation de $\mathcal{L}$) du dernier énoncé de la démonstration formelle qui a pour numéro n (pour la numérotation de la collection des démonstrations formelles de $(\mathcal{L}, \mathcal{A})$).

Si on regarde de près le travail d'arithmétisation de la théorie formelle de $(\mathcal{L},\mathcal{A})$, on voit qu'apparaît constamment la notion de processus parfaitement bien défini (ou parfaitement explicite). En fait, tous ces processus parfaitement explicites sont "primitifs récursifs" (définition ci-après) et ils admettent une traduction formelle dans le langage $\mathcal{L}a$, langage qui joue ainsi un rôle central dans les théories formelles(14).
Voici la définition des processus primitifs récursifs, et le résultat disant que ces processus peuvent être traduits dans $\mathcal{L}a$, énoncés précisément :

Définition des processus primitifs récursifs

On appelle fonction primitive récursive toute fonction de $\mathbb{N}^k$ vers $\mathbb{N}$ qui peut être obtenue, à partir des fonctions coordonnées, des fonctions constantes, de l'addition et de la multiplication, en appliquant un nombre fini de fois le procédé de composition des fonctions et le procédé de définition par récurrence simple(15).

---

14 En fait, l'important est qu'on puisse "traduire" suffisamment de raisonnements élémentaires, comme ceux que nous avons esquissés, dans la théorie formelle *Peano*. En conséquence cette théorie n'occupe un role central que pour des raisons historiques. A posteriori, on se demande bien pourquoi avoir choisi un langage aussi pauvre pour décrire les entiers naturels. Il serait infiniment plus confortable de disposer dans le langage formel de beaucoup plus de symboles de fonctions que seulement l'addition et la multiplication. Cette pauvreté du langage $\mathcal{L}a$ rend la preuve du théorème d'adéquation ci-après et celle du théorème d'incomplétude de Gödel (qui en découle) inutilement compliquées : une accumulation de lemmes techniques s'avère nécessaire pour vérifier qu'on est bien capable de "traduire" les fonctions primitives récursives dans *Peano*.

15 Les suites d'entiers usuelles des mathématiques sont primitives récursives, par exemple la n-ème décimale de π ou le n-ème nombre premier sont des suites primitives récursives.

Comme l'ensemble des mots écrits sur un alphabet fini peut être codé par des entiers naturels([16]) on peut également définir des processus primitifs récursifs qui, par exemple, prennent en entrée un entier naturel et donnent en sortie un mot sur un alphabet fini fixé. Alors, dans le théorème d'arithmétisation, tous les processus décrits sont primitifs récursifs. En outre les procédés primitifs récursifs peuvent être traduits dans *Peano* :

Théorème d'adéquation de *La* et *Peano* à la description des fonctions primitives récursives

Soit $n \longmapsto f(n)$ une fonction primitive récursive de $\mathbb{N}$ dans $\mathbb{N}$.

Il existe un énoncé arithmétique $\mathtt{U}_f(x,y)$ à deux variables libres x et y tel que l'on ait :

- pour tout entier naturel n, il existe un et un seul entier naturel m tel que :
  $\mathtt{U}_f(n,m)$ est interprété Vrai dans l'interprétation standard $\mathbb{N}$ de *La*,
  et la valeur m ainsi définie est égale à $f(n)$
- soit n un entier naturel et $m = f(n)$, n et m des écritures représentant n et m dans le langage *La*, alors l'énoncé
  $$\boxed{\mathtt{U}_f(n,m)}$$
  est un théorème de *Peano*.
- l'énoncé
  $$\boxed{\forall x \; \exists\, !y \quad \mathtt{U}_f(x,y)}$$
  est un théorème de *Peano*.

Commentaires :

1. Ainsi, la théorie formelle de *ZF* (système d'axiomes mis au point pour décrire un univers mathématique complètement "énorme"), *toute* la théorie formelle de *ZF*, se réduit à l'étude *d'une seule* fonction explicite de $\mathbb{N}$ dans $\mathbb{N}$, fonction qui peut être "écrite dans *La* et prouvée dans *Peano*",

2. Ceci est vrai pour toute théorie formelle : cela justifie qu'on ait depuis le début attaché une importance particulière à " $\mathbb{N}$ *et* *La*"([17])

D2 Le théorème d'incomplétude de Gödel

C'est ce théorème qui a ruiné les espoirs du projet formaliste de Hilbert.

Une fois arithmétisée la théorie formelle de $(\mathcal{L},\mathcal{A})$, le problème de la *consistance* (ou "non contradiction") de cette théorie formelle, admet une nouvelle formulation :
La théorie formelle $(\mathcal{L},\mathcal{A})$ est dite non contradictoire (ou consistante, ou encore cohérente) si la collection des théorèmes ne contient pas de contradiction.
En fait, vu les règles de la logique formelle, si une théorie formelle $\mathrm{Tf}(\mathcal{L},\mathcal{A})$ sur un langage $\mathcal{L}$ contient une contradiction, alors $\mathrm{Tf}(\mathcal{L},\mathcal{A})$ est la collection $\mathcal{L}$ toute entière ("tout" peut être démontré formellement à partir d'une contradiction).

---

16 Par exemple, si l'alphabet possède neuf lettres, qu'on nomme 0, 1, ..., 8 tout mot w peut être codé par le nombre qui, écrit en base 10, commence par 9 et se poursuit par le mot w

17 Comme disait Kronecker en langage imagé : «Dieu nous a donné les entiers naturels, tout le reste n'est que l'invention des hommes». Cantor, quant à lui, remerciait Dieu d'avoir créé l'univers mathématique des ensembles infinis actuels de tailles extraordinaires. Le fait qu'une réflexion sur les fondements des mathématiques, à travers le formalisme, ait abouti, beaucoup plus tard, à ce role central de l'arithmétique élémentaire peut être considéré comme un résultat en faveur de cette philosophie de Kronecker, et en défaveur de la philosophie «réaliste idéaliste» des infinis actuels à la Cantor.

Soit donc n_0 le numéro de l'énoncé « $\forall x \quad x \neq x$ ». On voit que $(\mathcal{L},\mathcal{A})$ est contradictoire si et seulement si l'énoncé F ayant pour numéro n_0 fait partie des théorèmes de la théorie formelle.
Si $f : \mathbb{N} \longrightarrow \mathbb{N}$ est la fonction explicite de $\mathbb{N}$ dans $\mathbb{N}$ décrite dans le théorème d'arithmétisation, on a donc :

> La théorie formelle $(\mathcal{L},\mathcal{A})$ est non contradictoire si et seulement si
> pour tout entier naturel n, $f(n) \neq n_0$

Si $\upsilon_f(x,y)$ est l'énoncé d'arithmétique correspondant à la fonction primitive récursive f décrit dans le théorème d'adéquation, on a donc l'énoncé d'arithmétique,

$$\boxed{\forall x \ \neg \upsilon_f(x,n_0)}$$

noté $\mathtt{Consis}\ \mathcal{A}$ [18], avec l'équivalence :

> "La théorie formelle $(\mathcal{L},\mathcal{A})$ est non contradictoire" si et seulement si
> l'énoncé $\mathtt{Consis}\ \mathcal{A}$ est Vrai dans l'interprétation standard $\mathbb{N}$ de $\mathcal{L}a$.

Ceci nous amène à la formulation du théorème d'incomplétude de Gödel.

Théorème d'incomplétude Gödel

1. $\mathtt{Consis}\ \mathcal{P}eano$ n'est pas un théorème de $\mathcal{P}eano$, à moins que $\mathcal{P}eano$ soit contradictoire.
2. $\mathtt{Consis}\ \mathcal{ZF}$ peut être "traduit" dans le langage $\mathcal{L}e$ de la théorie des ensembles. Notons alors $\mathtt{CONSIS}\ \mathcal{ZF}$ la traduction de $\mathtt{Consis}\ \mathcal{ZF}$ dans $\mathcal{L}e$. Alors $\mathtt{CONSIS}\ \mathcal{ZF}$ n'est pas un théorème de $\mathcal{ZF}$, à moins que $\mathcal{ZF}$ soit contradictoire.
3. Soit, de manière plus générale, un système d'axiome $\mathcal{A}$ explicite sur un langage du premier ordre $\mathcal{L}$. Supposons que ce système d'axiome soit assez fort pour permettre une traduction dans $\mathcal{L}$ de l'arithmétique de $\mathcal{P}eano$. Supposons enfin que $(\mathcal{L},\mathcal{A})$ soit non contradictoire. Soit enfin $\mathtt{CONSIS}\ (\mathcal{L},\mathcal{A})$ la traduction de $\mathtt{Consis}\ (\mathcal{L},\mathcal{A})$ dans la langage $\mathcal{L}$. Alors $\mathtt{CONSIS}\ (\mathcal{L},\mathcal{A})$ n'est pas un théorème formel de $(\mathcal{L},\mathcal{A})$.

Ce théorème reste imprécis pour la lectrice dans la mesure où je n'ai pas expliqué la notion de traduction (un exemple est donné en annexe).

Voici cependant quelques commentaires en un langage que j'espère compréhensible.

Commentaires :

1. Il est facile de comprendre pourquoi le théorème d'incomplétude de Gödel ruine le programme de Hilbert sous la forme où il était énoncé au départ, c.-à-d. un programme tendant à maîtriser par le biais de processus de nature extrêmement élémentaires l'utilisation de l'infini en mathématiques. Le système formel $\mathcal{P}eano$ est la traduction d'une partie relativement modeste de l'utilisation de procédés infinis par les mathématiciens (essentiellement $\mathcal{P}eano$ décrit les preuves par récurrence simple portant sur des propriétés arithmétiques). Pourtant, le preuve de la cohérence de cette théorie formelle relève de procédés nécessairement plus complexes que ceux formalisés dans $\mathcal{P}eano$. On ne pourra jamais maîtriser un infini en se situant à un niveau plus élémentaire que cet infini.

2. La théorie des ensembles et les méthodes de démonstration qu'elle autorisait semblait, à son apparition, et semble encore aujourd'hui à beaucoup de mathématiciens le cadre dans lequel s'inscrivent toutes les mathématiques. Pourtant, si $\mathcal{ZF}$ est non contradictoire, il y a un énoncé d'arithmétique, $\mathtt{Consis}\ \mathcal{ZF}$, qui, interprété dans le modèle standard $\mathbb{N}$, est Vrai, mais

---

[18] n_0 est ici une abréviation pour: (. . ((1 + 1) + . . . + 1) + 1) (n_0 fois))

indémontrable au moyen de $\mathcal{ZF}$. Donc la théorie des ensembles, dès qu'on en a choisi une formulation axiomatique telle que $\mathcal{ZF}$, est insuffisante à démontrer des énoncés arithmétiques *simples* : En effet, Consis $\mathcal{ZF}$ exprime "seulement" qu'une certaine fonction $f_{\mathcal{ZF}}$: $n \longmapsto f_{\mathcal{ZF}}(n)$ de $\mathbb{N}$ vers $\mathbb{N}$, bien définie, ne prend pas une valeur n_0 bien définie.

3. Appelons $\mathcal{P}_1$ le système d'axiomes de *Peano*.
Si nous nous plaçons d'un point de vue classique pour $\mathbb{N}$ et $\mathcal{L}a$, ce système est manifestement non contradictoire (il admet en effet un modèle explicite : c'est le modèle standard $\mathbb{N}$ et toute contradiction dans la théorie formelle de *Peano* impliquerait une contradiction dans le modèle explicite, ce qui est impossible(19)).
Donc, Consis $\mathcal{P}_1$ est Vrai lorsqu'on l'interprète dans le modèle standard.
Mais, comme Consis $\mathcal{P}_1 \notin \mathrm{Tf}(\mathcal{P}_1)$, on obtiendra une meilleure description de $(\mathbb{N},+,\times,0,1,<)$ avec un système d'axiomes $\mathcal{P}_2$ formé en prenant les axiomes de $\mathcal{P}_1$ et l'axiome supplémentaire Consis $\mathcal{P}_1$.
Mais, de nouveau, Consis $\mathcal{P}_2$ est à la fois Vrai dans le modèle standard et indémontrable formellement à partir de $\mathcal{P}_2$ (c'est-à-dire Consis $\mathcal{P}_2 \notin \mathrm{Tf}(\mathcal{P}_2)$). Donc on obtiendra une meilleure description de $(\mathbb{N},+,\times,0,1,<)$ avec le système d'axiomes $\mathcal{P}_3$ formé en prenant les axiomes de $\mathcal{P}_2$ et l'axiome supplémentaire Consis $\mathcal{P}_2$.
Et ainsi de suite(20).
De manière plus générale : il n'existe aucun système d'axiomes $\mathcal{P}$, défini de manière explicite sur $\mathcal{L}a$, pour lequel $\mathrm{Tf}(\mathcal{P})$ soit la collection de tous les énoncés d'arithmétiques interprétés Vrai dans le modèle standard. Ou encore, (il ne faut pas avoir peur de se répéter), la vérité sémantique dans $\mathbb{N}$ (pour des propriétés qui sont les interprétations d'énoncés de $\mathcal{L}a$) ne pourra jamais être enfermée dans un système d'axiomes bien défini a priori.

Dans la discussion précédente nous avons démontré la Vérité dans $\mathbb{N}$ d'énoncés tels que Consis $\mathcal{P}_1$, Consis $\mathcal{P}_2$ etc .. . Mais, pour ce faire, nous avons dû faire des aller-retour entre théories formelles et modèle standard $\mathbb{N}$. C'est seulement dans ces aller-retour entre réalité mathématique et formalisation que peut se situer l'intérêt profond des théories formelles(21).

D3 Propriétés arithmétiques qu'on ne démontrera jamais ?

Rappelons que nous avons appelé propriété arithmétique une propriété (concernant les entiers naturels) qui est l'interprétation standard d'un énoncé d'arithmétique (c'est-à-dire un énoncé de $\mathcal{L}a$). Considérons alors la propriété arithmétique suivante :

"la théorie formelle $\mathcal{ZF}$ est consistante"

(c'est l'interprétation de l'énoncé sans variable libre Consis $\mathcal{ZF}$), et supposons qu'elle soit vraie.
La démontrer reviendrait (d'après le théorème d'incomplétude de Gödel) à utiliser des méthodes de preuve plus fortes que celles formalisées dans $\mathcal{ZF}$.

---

19 En fait il existe également des preuves de la cohérence de *Peano* qui sont convaincantes d'un point de vue intuitionniste. cf. E2

20 Cela pourrait aller assez loin. La lectrice connaissant les ordinaux pourra par exemple s'entraîner à décrire explicitement un système d'axiome $\mathcal{P}_\alpha$ pour chaque ordinal dénombrable α qu'elle est capable de décrire de manière suffisamment explicite.

21 Par exemple, l'analyse non standard utilise, pour étudier les propriétés de fonctions standard de $\mathbb{R}$ dans $\mathbb{R}$, le comportement de ces fonctions standard par rapport à des réels non standard, "infinitésimaux", c'est-à-dire infiniment petits par rapport aux nombres réels standard.

Il semble donc bien que : "la théorie formelle $\mathcal{ZF}$ est consistante" est le type même de propriété arithmétique qui, si elle est vraie, est indémontrable à tout jamais par Homo Sapiens (mais là, je crois que je m'avance quand même un peu).
Ainsi serait levée une objection possible des "classiques pour $\mathbb{N}$ et $\mathcal{La}$" aux "intuitionnistes pour $\mathbb{N}$ et $\mathcal{La}$" qui dit que tout énoncé d'arithmétique aujourd'hui indécis sera forcément un jour démontré Vrai ou Faux (dans $\mathbb{N}$) et donc qu'on peut lui appliquer la loi du tiers exclu.

D4 Non définissabilité de la vérité (d'un langage par ce langage)

Plaçons-nous d'un point de vue classique.
Considérons un langage du premier ordre $\mathcal{L}$ et une interprétation M de ce langage. Il s'agit, rappelons-le, d'une collection d'objets M, et pour chaque symbole de fonction, de constante ou de relation de $\mathcal{L}$, d'avoir une fonction, un objet, une relation qui lui est associée dans l'interprétation.
Puisqu'on se place d'un point de vue classique, tout énoncé de $\mathcal{L}$, une fois interprété dans M, est forcément vrai ou faux.
Notons alors Ts($\mathcal{L}$,M) la collection des énoncés de $\mathcal{L}$ qui sont Vrais lorsqu'on les interprète dans M (je note Ts comme "théorème sémantique" de la même manière que plus haut j'ai noté Tf comme "théorème formel")..
Le théorème de "non définissabilité de la vérité" de Tarski affirme que la collection Ts($\mathcal{L}$,M) ne peut pas être définie avec "les seuls moyens du bord" que sont M et $\mathcal{L}$.
Cela reste un peu imprécis, je vais donc donner le théorème dans les cas de ($\mathcal{La}$,$\mathcal{P}_1$,($\mathbb{N}$,+,×,0,1,<)) et dans le cas de ($\mathcal{ZF}$, (U, ∈)) où (U, ∈) est un modèle de $\mathcal{ZF}$.

Remarquons cependant tout de suite que ce théorème achève de ruiner tout espoir de formalisation de la vérité. Alors que le théorème de Gödel est un théorème de "non démontrabilité de la vérité par des moyens purement formels", celui de Tarski va d'une certaine manière plus loin : la vérité sémantique échappe non seulement à la *démonstration* par des moyens purement formels, mais elle échappe également à la *description* (ou définition) par des moyens purement formels(22).

Théorème de non définissabilité en arithmétique

Soit $\mathbf{E}_0$, $\mathbf{E}_1$, $\mathbf{E}_2$, . . ., $\mathbf{E}_n$, . . . une numérotation explicite d'énoncés d'arithmétique sans variable libre. Considérons la collection des entiers n tels que $\mathbf{E}_n$ s'interprète Vrai dans le modèle standard ($\mathbb{N}$,+,×,0,1,<) de *Peano*. Alors cette collection n'est pas une partie arithmétique de $\mathbb{N}$

Théorème de non définissabilité de la vérité dans $\mathcal{ZF}$:

Étant donné un modèle U de $\mathcal{ZF}$, il n'existe aucun énoncé $\mathbf{R}(x)$ du langage $\mathcal{Le}$, à une seule variable libre x, vérifiant la propriété suivante : pour chaque énoncé $\mathbf{E}$ sans variable libre

$$\mathbf{E} \Leftrightarrow \mathbf{R}(\,|\mathbf{E}|\,) \text{ est Vrai dans U .}$$

Ici $|\mathbf{E}|$ est le numéro de $\mathbf{E}$ (pour une numérotation effective de $\mathcal{Le}$) traduit dans U :

---

22 Le théorème d'incomplétude est cependant "plus fort", plus subtil, et plus difficile à démontrer, à cause de sa précision diabolique concernant la vérité indémontrable. Le théorème "sémantique" de Tarski serait plutôt l'analogue d'une théorème d'incomplétude plus faible, relativement facile à démontrer en utilisant le procédé diagonal de Cantor, qui affirme seulement qu'il existe des propositions vraies mais indémontrables dans *Peano*.

dans U on peut définir des objets qu'on note $\underline{0}, \underline{1}, ..., \underline{n}, ...$ et qui font fonction d'entiers naturels standard. Par exemple on peut prendre : $\underline{0} = \emptyset$ (c.-à-d. l'interprétation du symbole de constante $\emptyset$ dans U), puis de proche en proche $\underline{n+1} = \underline{n} \cup \{\underline{n}\}$ (où $\cup$ est l'interprétation de la réunion dans l'univers U).

E Remarques sur le programme de Hilbert

E1 Évolution du programme de Hilbert

Il est écrit sur la tombe de Hilbert : «Nous devons savoir. Nous saurons».
Au départ (disons, en 1900, au moment des célèbres 23 problèmes, où l'urgence de lever les paradoxes de l'infini actuel se faisait pressante), il semble que Hilbert pensait que l'on disposerait un jour prochain d'une méthode systématique et purement mécanique d'investigation de la vérité mathématique.
Rappelons que le premier des problèmes de Hilbert demandait qu'on prouve la possibilité d'un bon ordre sur $\mathbb{R}$ et l'hypothèse du continu. «Nous aurions bien voulu savoir, et il est probable que nous ne saurons jamais» dirions nous sur ces sujets aujourd'hui.
Autre exemple, le $10^{\text{ème}}$ problème de Hilbert est la requête d'une méthode mécanique capable de décider si un polynome multivariable à coefficients entiers s'annule en au moins un point à coordonnées entières. La preuve qu'une telle méthode mécanique ne peut exister est relativement récente (Matiassevitch 1970).
Si on élargit la classe des problèmes à résoudre sous la forme suivante :

«décider si une fonction primitive récursive de $\mathbb{N}$ vers $\mathbb{N}$
prend au moins une fois la valeur 0 »,

alors la preuve d'impossibilité d'une procédure mécanique est très simple (c'est essentiellement le procédé diagonal de Cantor, génial mais très simple), et il semble aujourd'hui bizarre que Hilbert ait pu jamais espérer une réponse positive.
Mais, en 1900, quand Hilbert pose son $2^{\text{ème}}$ problème, qui demande qu'on prouve par des moyens très élémentaires la cohérence de l'arithmétique, les systèmes formels ne sont pas encore complètement au point, et les fonctions explicites mécaniques (récursives) ne seront définies que 30 ans plus tard.
À l'époque on croyait par exemple que la construction des réels comme (classes d'équivalence de) suites de Cauchy de rationnels impliquerait que la cohérence de "l'analyse" (la théorie des nombres et fonctions réelles) se déduirait facilement de la cohérence de l'arithmétique.
On croyait également que le système des axiomes informels de Peano (dans lequel l'axiome de récurrence est énoncé informellement pour "toute" partie de $\mathbb{N}$), dans la mesure où il "caractérisait" $\mathbb{N}$ de manière univoque, fournirait la base formelle d'une description complète de $\mathbb{N}$.
En conséquence, une preuve élémentaire de la cohérence de l'arithmétique ajoutée à une formalisation adéquate de l'axiomatique informelle de Peano pouvait sembler la baguette magique absolue, qui permettrait à la fois de résoudre les paradoxes et de mécaniser entièrement les preuves.
La mise en oeuvre du programme de Hilbert nécessitait la description la plus objective possible de l'activité mathématique. Mais l'activité mathématique, décrite objectivement, ressemble diablement à un bouquin de mathématiques, et elle a alors un caractère fini et discret, c.-à-d. est par nature opposée à l'intuition que nous avons du continu. Ainsi le système formel $\mathcal{ZF}$ ne décrit aucunement les univers ensemblistes hypothétiques à la Cantor, mais seulement une

activité mécanisable des mathématicien(ne)s au sujet de ces univers. La théorie formelle $\mathcal{ZF}$ est structurellement analogue à $\mathbb{N}$ et non à $\mathbb{R}$, et encore moins à l'univers cantorien. Cette contradiction entre l'objet supposé de l'étude mathématique et les moyens bien limités dont dispose tout procédé de démonstration automatique s'est résolue dans un flop retentissant du programme de Hilbert initial(23). Cela peut sembler après coup comme une évidence bien simple. Soit que l'on croie à l'univers cantorien, mais alors il faut se résigner à une très probable profonde ignorance. Soit que l'on n'y croie pas, et l'échec était prévisible comme l'éclatement de la grenouille qui veut se faire plus grosse qu'un boeuf (en l'occurrence un boeuf tellement énorme qu'il n'existe même pas). Ce qui n'était sans doute pas prévisible, c'est l'endroit où ça a fait flop, qui est relativement bas dans le degré d'abstraction.
Néanmoins, comme l'activité mathématique va bien au delà de l'étude d'un système formel particulier (contrairement à ce que laisse entendre le formalisme), et comme une certaine dose d'infini à l'état au moins potentiel est nécessaire à la réflexion mathématique, le programme de Hilbert, en tant que réflexion au sujet des mathématiques pratiquées, par des moyens de nature mathématique, reste une tâche permanente. À défaut de pouvoir maîtriser l'infini par en dessous, on doit essayer d'analyser les formalisations de l'infini (lesquelles ne sont structurellement pas des infinis bien compliqués) depuis pas trop haut. De manière plus générale, il semble indispensable d'analyser l'activité mathématique la plus abstraite en termes d'une signification concrète de cette activité qui ne soit pas seulement formaliste (car alors il ne s'agirait pas de l'analyse d'une activité abstraite, mais seulement de l'étude d'un jeu très concret, très compliqué et sans signification profonde). C'est ce qu'on pourrait appeler un programme de Hilbert revu à la baisse.
L'activité de recherche en mathématiques est consacrée en grande partie à la simplification des preuves. Il n'y a surement pas consensus sur ce qu'est une preuve simple. Mais une des manières de "simplifier" une preuve est souvent de la rendre plus concrète et plus explicite. Chaque fois que la simplification est faite de cette manière, on peut considérer qu'un petit morceau de ce programme de Hilbert (révisé à la baisse) est réalisé. Quand Bishop publie en 1967 un livre où il interprête en termes constructifs les bases de l'analyse moderne, il réalise un morceau substantiel de ce programme de Hilbert. Quant une conjecture mathématique qui affirme que toutes les courbes algébriques planes d'une très vaste famille n'ont qu'un nombre fini de points rationnels est démontrée par une belle méthode très abstraite, immédiatement une activité intense de simplification et d'explicitation de la preuve se met en route. Et les mathématicien(ne)s ne seront pas satisfait(e)s tant qu'ils (elles) n'aurant pas réussi à rendre beaucoup plus précise l'affirmation concernant le "nombre fini de points". C.-à-d. tant qu'ils n'auront pas soumis le beau théorème au programme de Hilbert.

E2 Le programme de Hilbert pour l'arithmétique de Peano

À défaut de pouvoir prouver la cohérence de *Peano* par des moyens élémentaires, on peut essayer d'analyser la complexité des preuves contenues dans ce système formel. La première chose à faire semble être de répondre aux objections des intuitionnistes concernant l'usage abusif du tiers exclu en matière d'infini. Une logique formelle répondant à la compréhension constructive de l'activité mathématique a été mise au point par Heyting. La théorie formelle basée sur les axiomes de Peano mais avec la logique formelle intuitionniste a été baptisée *Heyting*.

---

23 Il est par ailleurs fort heureux que le théorème d'incomplétude de Gödel interdise à n'importe quelle activité purement mécanique de simuler convenablement les capacités inventives d'Homo Sapiens.

Gödel a montré que le système formel *Peano* n'est pas plus incohérent que le système formel *Heyting*. C'est une preuve très élémentaire, qui consiste essentiellement à interpréter une affirmation classique comme une affirmation constructive dont la signification est nettement plus faible. Parmi tous les énoncés classiquement équivalents à un énoncé d'arithmétique donné, on choisit celui dont la signification constructive est la plus faible. La preuve classique de l'énoncé dans le système *Peano* se transforme alors automatiquement en une preuve de l'énoncé affaibli dans *Heyting*. Si une contradiction (qui est un énoncé faible) est prouvée par *Peano* elle est alors automatiquement prouvée par *Heyting*.
Cette analyse de la cohérence de *Peano* a été améliorée de plusieurs façons, dont plusieurs essentielles. Par exemple :

- Gentzen a donné une analyse de la cohérence de *Peano* en termes d'ordinaux : il revient au même de pratiquer des raisonnements par récurrence simple sur des énoncés d'arithmétiques arbitraires (qui sont des énoncés relativement compliqués), ou de pratiquer des raisonnements par récurrence le long d'un ordinal assez grand, mais pas trop, sur des énoncés d'arithmétiques tout à fait élémentaires.
- Gödel a donné une analyse de la cohérence de *Heyting* en montrant que celle-ci équivaut à accepter des définitions par récurrence simple portant sur des objets de structure assez compliquée, mais pas trop, les fonctionnelles récursives.
- Dragalin et Friedman ont montré que les fonctions mécaniquement calculables prouvées exister dans *Peano* peuvent également être prouvées exister dans *Heyting*.

E3 Vérité des résultats d'arithmétique établis au moyen des axiomes de $\mathcal{ZF}$?

Si les mathématiciens utilisent la théorie des ensembles et la "logique formelle classique" (pour des propriétés interprétant des énoncés écrits en un langage du premier ordre), c'est pour des raisons de simplicité et de facilité des démonstrations dans ce cadre.
Dans ce cadre, ils sont amenés à utiliser des objets mathématiques assez incroyables. Par exemple, on définit au moyen d'énoncés explicites des ensembles dont on ne sait définir explicitement aucun élément isolé et dont on démontre qu'ils sont infinis. Un peu comme si on savait définir l'ensemble des nombres réels mais qu'on ne sache définir aucun de ces nombres isolément.
Il n'y a pas besoin d'être intuitionniste pur et dur pour mettre en doute "le sens réel" de résultats concernant de tels objets. Mais, les mathématiciens "classiques" ne sont pas masochistes : s'ils utilisent des objets "complètement farfelus" et "pas du tout crédibles" c'est comme intermédiaires dans des démonstrations concernant des objets tout à fait ordinaires et crédibles, tels que les entiers naturels. On voit immédiatement que se pose le problème de la validité de résultats concernant les entiers naturels, mais obtenus au prix de détours dans l'univers mathématique de Zermelo-Frankel.
Le programme de Hilbert pour $\mathcal{ZF}$ aurait réclamé dans sa version initiale une preuve, par des moyens élémentaires, que tout théorème d'arithmétique de structure suffisamment simple[24] prouvé au moyen de $\mathcal{ZF}$ soit Vrai dans la réalité de $\mathbb{N}$. Comme la cohérence de $\mathcal{ZF}$ (c.-à-d. l'impossibilité de prouver l'affirmation $0 = 1$, manifestement fausse dans la réalité) est hors de portée des méthodes élémentaires, ce programme ne peut être réalisé. Néanmoins,

---

24 Plus précisément, tout théorème d'arithmétique de la forme « $\forall n \; f(n)=0$ » où f est une fonction primitive récursive. Ce genre de théorème d'arithmétique a une structure très simple et sa signification n'est pas sujette à trop de contestation.

on doit se poser la question de savoir quel type de garantie on peut espérer concernant les résultats d'arithmétique prouvés au moyen de $\mathcal{ZF}$. (par exemple, est-on absolument certain que le beau théorème auquel il est fait allusion à la fin du paragraphe E1 corresponde à une vérité dans le monde réel des entiers naturels, dès que sa preuve est formellement correcte dans $\mathcal{ZF}$?).

Le point de vue formaliste a "l'avantage" d'ignorer ce problème puisque le mathématicien formaliste joue au jeu "langage de la théorie des ensembles, axiomes de $\mathcal{ZF}$ et règles de la logique formelle" et ne prétend jamais que les énoncés qu'il appelle "théorèmes" s'interprètent en une réalité Vraie. Même s'il démontre au moyen de $\mathcal{ZF}$ l'énoncé de $\mathcal{Le}$ qui s'interprète par "tout nombre pair ≥ 4 est somme de deux nombres premiers", le mathématicien formaliste ne prétend pas avoir démontré que tout nombre pair ≥ 4 soit somme de deux nombres premiers. Si, par la suite, quelqu'un trouve un nombre pair qui ne soit pas somme de deux nombres premiers, le mathématicien formaliste dira : les axiomes de $\mathcal{ZF}$ sont donc contradictoires et mon jeu est sans intérêt, je vais essayer de jouer à autre chose.

Pour le mathématicien qui admet le point de vue classique (pour $\mathbb{N}$ et $\mathcal{La}$) mais qui admet difficilement l'existence d'un univers mathématique aussi "monstrueux" que celui de $\mathcal{ZF}$, quelle est la validité des "résultats d'arithmétique" obtenus au moyen de $\mathcal{ZF}$ *au moins si nous supposons que la théorie formelle de* $\mathcal{ZF}$ *est non contradictoire* ?
J'avoue que j'ai bien du mal à répondre à cette question, pourtant pertinente. Mais il me semble que la réponse est à l'heure actuelle incertaine.
Cette réponse semble dépendre de la structure de l'énoncé d'arithmétique démontré dans $\mathcal{ZF}$.
Considérons tout d'abord un énoncé d'arithmétique simple du type : « $\forall$ n f(n)=0 » où f est une fonction primitive récursive. Si la preuve a été donnée dans $\mathcal{ZF}$ et que l'énoncé soit faux dans la réalité, il existe un entier m tel que $f(m) \neq 0$ et le calcul de f(m) peut être prouvé dans $\mathcal{ZF}$, ce qui permettrait d'établir une contradiction dans $\mathcal{ZF}$, contrairement à l'hypothèse.
Considérons ensuite un énoncé d'arithmétique du type : « $\exists$ n f(n)=0 » où f est une fonction primitive récursive. Une preuve dans $\mathcal{ZF}$ d'un tel énoncé ne permet pas a priori d'exhiber un entier usuel n tel que $f(n) = 0$. Et le fait que l'énoncé soit faux avec les entiers usuels (standards) ne permet pas non plus a priori d'induire une contradiction dans $\mathcal{ZF}$. Bien au contraire, le fait que tout modèle suffisamment simple de $\mathcal{ZF}$ contienne inévitablement des entiers non standards (résultat de Rabin) peut nous inciter à penser que les entiers n que $\mathcal{ZF}$ affirme annuler f pourraient après tout être tous non standards.
Si maintenant nous analysons la structure du beau théorème cité en fin de E1 nous voyons que l'énoncé est a priori du type, pas vraiment simple, suivant :

« $\forall$ p $\exists$ n $\forall$ m>n g(p,m)=0 » (25)

où g est une fonction primitive récursive. Ici, nous sommes dans un cas bien pire que le précédent. Et la vérité de l'énoncé dans $\mathbb{N}$ semble encore nettement plus difficile à établir à partir de la seule preuve dans $\mathcal{ZF}$ (et de l'hypothèse Consis $\mathcal{ZF}$).(26)

---

25 Pour toute courbe C_p de la famille considérée (qui peut être énumérée en une suite) il existe un entier qui majore le numéro de tout point rationnel P_m de la courbe (pour une numérotation des points rationnels du plan). Le calcul de g(p,m) donne 1 si le point P_m est sur la courbe C_p et 0 sinon.

26 Plaçons nous un moment du point de vue constructif. Même si le théorème est établi dans $\mathcal{Peano}$ nous pouvons avoir des doutes sur sa vérité. L'explicitation complète du théorème, à laquelle travaillent pas mal de gens, demande en effet qu'on calcule n en fonction de p. Mais pour p fixé, on n'a pas a priori de test concernant n qui puisse certifier que $\forall$ m>n g(p,m)=0. En conséquence on n'est même pas a priori garanti que la dépendance de n par rapport à p puisse être explicitée par une fonction mécaniquement

Pour me résumer, il me semble qu'il faut admettre *plus* que la logique formelle classique lorsqu'elle est appliquée $\mathcal{L}a$ et $\mathbb{N}$, pour être convaincu qu'un énoncé d'arithmétique démontré formellement dans $\mathcal{ZF}$ soit Vrai dans $(\mathbb{N},+,\times,0,1,<)$ (en supposant évidemment $\mathcal{ZF}$ non contradictoire). Ou encore : les mathématiques couramment pratiquées n'ont de "sens" que si elles permettent de démontrer uniquement des énoncés d'arithmétique Vrais dans le modèle standard $(\mathbb{N},+,\times,0,1,<)$. Or, pour être assuré de cela *il ne suffit pas* de supposer que $\mathcal{ZF}$ est non contradictoire, il faut *en plus* supposer que $\mathcal{ZF}$ est non contradictoire avec tout énoncé d'arithmétique Vrai dans le modèle standard (et traduit dans $\mathcal{L}e$).
Ordinairement, en fait, les mathématicien(ne)s admettent que $\mathcal{ZF}$ possède un modèle dans lequel "l'ensemble des entiers" est standard pour l'arithmétique, mais "l'acte de foi" de la croyance en un tel modèle est a priori plus fort que l'acte de foi en la consistance de $\mathcal{ZF}$. Il semble à vrai dire presque aussi fort que celui de la croyance en l'univers cantorien abstrait dont une pâle description est donnée par $\mathcal{ZF}$.

F Quelques conclusions

1 – La formalisation de la logique pour les énoncés écrivables en un langage du premier ordre a un intérêt théorique remarquable en ce qu'elle permet une clarification du débat quant aux méthodes de raisonnements acceptables.
Ces méthodes de raisonnements "acceptables"' ne le sont justement pas toutes par tous les mathématiciens. Le débat reste donc ouvert et, semble-t-il, restera ouvert longtemps encore.

2 – L'étude d'objets mathématiques tels que "les entiers naturels", "les groupes finis", "les nombres réels", "les ensembles" etc ... est susceptible d'une formalisation dans des langages du premier ordre, mais au prix de "pertes sèches" importantes.

- Au lieu de s'intéresser alors à toutes les propriétés imaginables de ces objets (à supposer qu'on soit convaincu de leur existence), on ne s'intéresse alors qu'aux propriétés qui peuvent être écrites dans un langage du premier ordre donné et, parmi ces propriétés, seulement à celles qui sont démontrables à partir d'un système d'axiomes préalablement choisis.
- Mais alors, de plus :

- si l'objet est "peu puissant" (un groupe fini particulier par exemple), sa théorie formelle n'apporte rien de plus que sa théorie naïve,
- si l'objet est "assez puissant" (par exemple il contient une partie identifiable à $\mathbb{N}$) aucune formalisation n'épuisera jamais la notion intuitive de vérité dans cet objet (quel que soit le point de vue qu'on adopte quant à la notion intuitive de vérité d'ailleurs),
- si l'objet est "trop puissant" (par exemple un univers mathématique de Zermelo Frankel : objet de l'existence duquel on peut douter fortement et dont on ne connaît pas de "copie modèle réduit" convaincante), alors le recours à une théorie formelle du premier ordre semble d'un bien faible secours pour valider l'utilisation de cet objet (des obstacles considérables semblent se présenter à la réalisation d'un programme de Hilbert, même fortement révisé à la baisse, pour de tels types d'objets)

3 – L'étude d'un objet mathématique, une fois réduite à l'étude d'une théorie formelle de cet objet (après choix d'un système d'axiomes écrits dans un langage du premier ordre), est ramenée à l'étude de l'ensemble des valeurs f(n) *d'une* fonction f de $\mathbb{N}$ dans $\mathbb{N}$ parfaite-

---

calculable. Or une preuve constructive de cette dépendance fournirait à coup sûr un algorithme de calcul mécanisable.

ment explicite. Aucun mathématicien ne peut croire que les mathématiques pourraient se réduire à l'étude *d'une seule* fonction explicite de $\mathbb{N}$ dans $\mathbb{N}$, si complexe soit elle.

Annexe 1 Les axiomes de $\mathcal{GB}$

Par convention, les lettres latines minuscules désigneront les "ensembles" du modèle, tandis que les lettres majuscules désigneront indistinctement "ensembles" ou "classes ".

Autrement dit encore un énoncé $\forall x\ \mathbf{R}(x)$ est une abréviation pour :

$\forall X\ (\ (\exists Y\ X \in Y) \Rightarrow \mathbf{R}(X)\ )$

et un énoncé $\exists x\ \mathbf{R}(x)$ est une abréviation pour :

$\exists X\ (\ (\exists Y\ X \in Y) \wedge \mathbf{R}(X)\ )$

Les axiomes de $\mathcal{GB}$ sont alors les suivants :

1) Extensionalité : deux classes qui ont les mêmes éléments sont égales

$\forall X\ \forall Y\ (\ \forall z\ (\ z \in X \Leftrightarrow z \in Y\ )\ \Rightarrow X = Y\ )$

2) Ensemble vide : $\forall x\ \ x \notin \emptyset\ ,\ \ \exists Y\ \emptyset \in Y$

3) Ensemble à un ou deux éléments : $\forall x\ \forall y\ \exists z\ \forall t\ (\ t \in z \Leftrightarrow (t=x \vee t=y)\ ).$

4) Ensemble réunion des éléments de y :

$\forall y\ \exists z\ \forall u\ (\ u \in z \Leftrightarrow (\exists t\ (u \in t \wedge t \in y)\ )\ ).$

5) Ensemble infini : $\exists x\ (\ \emptyset \in x\ \wedge \forall y\ (\ y \in x \Rightarrow y \cup \{y\} \in x\ )\ ).$
Dans cet énoncé, $y \cup \{y\}$ désigne l'unique ensemble qui a pour éléments y et les éléments de y ; l'existence de cet ensemble unique est assurée par les axiomes 3 et 4.

6) Ensemble des parties d'un enesmble : $\forall x\ \exists y\ \forall u\ (\ u \in y \Leftrightarrow u \subset x\ )$
où $u \subset x$ est une abréviation pour : $\forall t\ (\ t \in u \Rightarrow t \in x)\ ).$

7) Axiome de substitution : on définit le couple $\langle x,y \rangle$ comme étant égal à $\{\{x,y\},\{x\}\}$.
On a alors $\langle x,y \rangle = \langle z,t \rangle$ si et seulement si $x = z$ et $y = t$.
L'axiome de substitution s'écrit alors :
$\forall X\ \forall u\ [\ (\forall x\ \exists!y\ \langle x,y \rangle \in X) \Rightarrow \exists v\ \forall y\ (y \in v \Leftrightarrow \exists x(x \in u \wedge \langle x,y \rangle \in X))\ ]$
En gros : l'ensemble v est l'image de l'ensemble u par la classe X qui joue le rôle d'une fonction.

Comme conséquence de l'axiome 7 on a notamment : toute classe contenue dans un ensemble est un ensemble.
L'écriture $\exists!\ y$ est une abréviation, et elle signifie "il existe un et un seul y ".

8) Axiome du choix fort :

$\exists C\ \forall x\ (\ x \neq \emptyset\ \Rightarrow\ \exists!\ y\ (y \in x\ \wedge \langle x,y \rangle \in C)\ )$

(La classe C "choisit" dans chaque ensemble x un élément y.).

9) $\exists A\ \forall a\ (\ a \in A\ \ \Leftrightarrow\ \ \exists x\ \exists y\ (\ a = \langle x,y \rangle\ \wedge\ x \in y\ )\ )$
(Il existe une classe A dont les éléments sont les couples d'ensembles tels que $x \in y$).

10) Réunion de deux classes : $\forall Y\ \forall Z\ \exists X\ \forall a\ (\ a \in X \Leftrightarrow (a \in Y\ \vee\ a \in Z)\ ).$

11) Complémentaire d'une classe : $\forall Y\ \exists Z\ \forall a\ (\ a \notin Y\ \Leftrightarrow\ a \in Z\ ).$

12) Domaine d'une relation entre ensembles :

$\forall R\ \exists D\ \forall a\ (a \in D\ \Leftrightarrow\ \exists x\ \langle a,x \rangle \in R\ ).$

13) Classe des couples $\langle x,y \rangle$ où $x \in X$:

$\forall X\ \exists Y\ \forall a\ (\ a \in Y\ \Leftrightarrow\ \exists x\ \exists y\ (x \in X\ \wedge\ a = \langle x,y \rangle)\ ).$

14) Permutations entre éléments d'un triplet ou d'un couple :

$\forall X\ \exists Y\ \forall x\ \forall y \quad (\ \langle x, y\rangle \in Y \Leftrightarrow \langle y,x\rangle \in X\ )$

$\forall X\ \exists Z\ \forall x\ \forall y\ \forall z \quad (\ \langle x,y,z\rangle \in Z \Leftrightarrow \langle y,z,x\rangle \in X\ )$

$\forall X\ \exists T\ \forall x\ \forall y\ \forall z \quad (\ \langle x,y,z\rangle \in T \Leftrightarrow \langle x,z,y\rangle \in X\ )$

15) Fondation (facultatif)

$\forall X\ (\ X \neq \emptyset \Rightarrow \exists u\ (u \in X \wedge \forall y\ (y \in X \Rightarrow y \in u)\ )\ )$

(Toute classe contient un ensemble "minimal" pour la relation $\in$).

$\forall a\ \exists c\ \forall x\ [(x \neq \emptyset \wedge x \in a) \Rightarrow \exists! y\ (y \in x \wedge \langle x,y\rangle \in c)\ ]$

Pour la théorie $\mathcal{ZF}$ on utilise un seul type de variable. Les axiomes sont les axiomes 1, 2, 3, 4, 5, 6, 15. Les axiomes 9 à 14 sont supprimés.

L'axiome 7 est remplacé par :

7*) Schéma de substitution: on réécrit l'axiome 7) en remplaçant

$\langle x,y\rangle \in X$ par $R(x,y)$

où R désigne un énoncé écrit dans $\mathcal{L}e$.

Il y a donc un axiome pour chaque énoncé $R(x,y)$. On dit que 7*) est un schéma d'axiomes.

L'axiome 8 est remplacé par :

8*) Axiome du choix :

$\forall a\ \exists c\ \forall x\ [(x \neq \emptyset \wedge x \in a) \Rightarrow \exists! y\ (y \in x \wedge \langle x,y\rangle \in c)\ ]$

(Pour tout ensemble a il y a un ensemble c qui permet le choix simultané d'un objet y(x) dans chaque élément x non vide de l'ensemble a)

Pour tout modèle M de $\mathcal{GB}$, les "ensembles" du modèle M forment un modèle pour $\mathcal{ZF}$. À partir de tout modèle M de $\mathcal{ZF}$, on peut construire ("mécaniquement") un modèle de $\mathcal{GB}$.

Annexe 2 Traduction de l'arithmétique de Peano dans le langage $\mathcal{L}e$ de la théorie des ensembles

Considérons un "Univers de Zermelo Frankel" c'est-à-dire un modèle U du système d'axiomes $\mathcal{ZF}$ (du langage $\mathcal{L}e$).

Pour tout entier naturel n, on définit un objet bien déterminé de l'univers U, objet qu'on notera par exemple $\underline{n}$.
Cet objet est défini par récurrence (c.-à-d. de proche en proche), en posant :

$$\underline{0} = \emptyset \text{, et } \underline{n+1} = \underline{n} \cup \{\underline{n}\}$$

On peut aussi donner pour chaque n un énoncé $F_n(x)$ de $\mathcal{L}e$ tel que $\mathcal{ZF}$ prouve l'existence et l'unicité d'un x vérifiant $F_n(x)$ et tel que dans le modèle U l'interprétation de $F_n(x)$ soit vraie si on interprère x par $\underline{n}$.
Modulo cette traduction, on démontre un schéma de théorèmes de $\mathcal{ZF}$ qui affirment que pour des entiers n et m distincts, $\underline{n}$ et $\underline{m}$ sont des objets distincts de l'univers U (il y a un théorème distinct pour chaque couple d'entiers naturels distincts).
Qu'est-ce qui joue alors "le rôle de $\mathbb{N}$" dans l'univers U ?
Les axiomes de $\mathcal{ZF}$ permettent de montrer qu'il existe un unique élément $\underline{\omega}$ de la collection U, qui vérifie :

$$\emptyset \in \omega \ \wedge \ (\ \forall x \in \omega \quad x \cup \{x\} \in \omega \ )$$
$$\wedge \quad \forall X \quad [(\emptyset \in X \ \wedge \ (\forall x \in X \ x \cup \{x\} \in X) \ ) \ \Rightarrow \ \omega \subset X \ ]$$

c'est-à-dire : $\underline{\omega}$ est le plus petit ensemble qui contienne $\emptyset$ et qui soit stable pour l'opération qui à un élément x de $\underline{\omega}$ associe l'élément $x \cup \{x\}$.

On constate que pour tout entier naturel n, l'objet $\underline{n}$ de U vérifie : $\underline{n} \in \underline{\omega}$.

Par contre, il n'y a aucun énoncé *écrivable dans* $\mathcal{L}e$ qui puisse traduire l'idée "pourtant simple" que $\underline{\omega}$ ne doit pas avoir d'autres éléments que les objets $\underline{n}$ (et d'ailleurs, si $\mathcal{ZF}$ est non contradictoire, il y a des modèles de $\mathcal{ZF}$ pour lesquels $\underline{\omega}$ contient des entiers non standard).
On démontre ensuite, en tant que théorèmes formels de $\mathcal{ZF}$ l'existence de "lois de composition" $\underline{+}$ et $\underline{\times}$ définies sur $\underline{\omega}$ et vérifiant les axiomes de *Peano*.

Remarque :
Pour traduire *Peano* dans $\mathcal{ZF}$, on a été aidé par le fait que les axiomes de $\mathcal{ZF}$ permettent de définir un objet $\underline{\omega}$ qui joue le rôle de "collection de tous les entiers".
En fait, on peut se débrouiller sans cet "infini actuel". C'est l'objet de l'explication plus générale qui suit.

Annexe 3 Traduction de l'arithmétique de Peano dans une autre théorie formelle

On considère une théorie formelle définie par un système d'axiomes $\mathcal{A}$ écrits dans un langage du premier ordre $\mathcal{L}$.
Une traduction de ($\mathcal{L}a$, *Peano*) dans ($\mathcal{L}$, $\mathcal{A}$) est fournie par cinq énoncés de $\mathcal{L}$.

- Un énoncé $\mathbf{N}(x)$ à un seule variable libre x (qu'on lira : x est un entier).
- Un énoncé $\mathbf{I}(x,y)$ à deux variables libres x, y (qu'on lira : x et y sont entiers et $x<y$).
- Un énoncé $\mathbf{S}(x,y,z)$ à trois variables libres x, y, z (qu'on lira : z est l'entier somme des entiers x et y).
- Un énoncé $\mathbf{P}(x,y,z)$ correspondant au produit.
- Un énoncé $\mathbf{E}_0(x)$, un énoncé $\mathbf{E}_1(x)$, (qu'on lira $x = 0$ et $x = 1$).

Tout ceci doit "vérifier les axiomes de *Peano*" au sens suivant :

La théorie formelle ($\mathcal{L}$, $\mathcal{A}$) contient les théorèmes qui "traduisent" les axiomes de *Peano*, c'est-à-dire précisons :

- $\exists x\ \forall y\ ((\mathbf{N}(x) \wedge \mathbf{E}_0(x) \wedge (\mathbf{E}_0(y) \Rightarrow y=x))$:
  ($\mathbf{E}_0$ définit un entier unique)
- $\exists x\ \forall y\ ((\mathbf{N}(x) \wedge \mathbf{E}_1(x) \wedge (\mathbf{E}_1(y) \Rightarrow y=x))$: (idem avec $\mathbf{E}_1$)
- $\forall x\ \forall y\ ((\mathbf{I}(x,y) \Rightarrow (\mathbf{N}(x) \wedge \mathbf{N}(y))$:
  (la relation $\mathbf{I}(x,y)$ concerne des entiers)
- $\forall x\ \forall y\ \forall z\ ((\mathbf{S}(x,y,z) \Rightarrow (\mathbf{N}(x) \wedge \mathbf{N}(y) \wedge \mathbf{N}(z))$: (idem avec $\mathbf{S}$)
- $\forall x\ \forall y\ \forall z\ ((\mathbf{P}(x,y,z) \Rightarrow (\mathbf{N}(x) \wedge \mathbf{N}(y) \wedge \mathbf{N}(z))$: (idem avec $\mathbf{P}$)
- $\forall x\ \forall y\ \exists z\ \forall t\ ((\mathbf{N}(x) \wedge \mathbf{N}(y)) \Rightarrow (\mathbf{S}(x,y,z) \wedge (\mathbf{S}(x,y,t) \Rightarrow t=z))$
  (c'est-à-dire $\mathbf{S}(x,y,z)$ définit l'entier z en fonction des entiers y et x)
- $\forall x\ \forall y\ \exists z\ \forall t\ ((\mathbf{N}(x) \wedge \mathbf{N}(y)) \Rightarrow (\mathbf{P}(x,y,z) \wedge (\mathbf{P}(x,y,t) \Rightarrow t=z))$
  (même chose avec $\mathbf{P}(x,y,z)$)
- la traduction des axiomes de *Peano* : donnons juste un exemple

l'axiome	$z + x = z + y \Rightarrow x = y$	est traduit par
$\forall x\ \forall y\ \forall z\ \forall t$	$((\mathbf{S}(z,x,t) \wedge (\mathbf{S}(z,y,t)) \Rightarrow x = y)$	

Annexe 4 Un autre modèle remarquable de $\mathcal{GB}^-$

On considère l'ensemble V_ω construit comme en C2, puis, au lieu de prendre $\mathbb{W} = \mathcal{P}(\mathbb{V}_\omega)$, on prend :

$\mathbb{W}'$ = ensemble des parties de $\mathbb{V}_\omega$ définies par un énoncé de $\mathcal{L}e$.

Une partie A de $\mathbb{V}_\omega$ est dite "définie par un énoncé R(x) de $\mathcal{L}e$" si R(x) est un énoncé de $\mathcal{L}e$ à une seule variable libre x et si on a, pour tout x de $\mathbb{V}_\omega$

$x \in A$ si et seulement si R(x) est vrai dans $\mathbb{V}_\omega$

Ces parties de $\mathbb{V}_\omega$ définies par un énoncé de $\mathcal{L}e$ sont appelées les parties "arithmétiques" de $\mathbb{V}_\omega$ parce que, pour une numérotation naturelle de $\mathbb{V}_\omega$, elles correspondent exactement aux parties arithmétiques de $\mathbb{N}$.

Enfin, on interprète le symbole $\boxed{\in}$ par la relation $\in$ dans $\mathbb{W}'$.

On obtient de nouveau un modèle de $\mathcal{GB}^-$, mais cette fois-ci dénombrable (puisqu'on peut numéroter les énoncés à une variable libre de $\mathcal{L}e$). Les "ensembles" de ce modèle sont de nouveau les parties finies de $\mathbb{V}_\omega$ et les "classes" de ce modèle sont maintenant les parties arithmétiques de $\mathbb{V}_\omega$.

Ce modèle $(\mathbb{W}', \in)$ de $\mathcal{GB}^-$ est déjà nettement plus crédible que le modèle $(\mathbb{W}, \in)$ défini en C2, ne serait-ce que parce qu'il est dénombrable. Remarquons que la croyance en l'existence de $(\mathbb{W}', \in)$ comme infini actuel revient sur le fond à adopter un point de vue classique pour $\mathbb{N}$ et $\mathcal{L}a$. Admettre que chaque énoncé a une variable libre de $\mathcal{L}e$ définit "actuellement" une partie de $\mathbb{V}_\omega$ revient à admettre que chaque énoncé à une variable libre de $\mathcal{L}a$ définit comme infini actuel une partie de $\mathbb{N}$. C'est-à-dire que cela revient à admettre une vérité absolue pour $\mathbb{N}$ et $\mathcal{L}a$.

On pourra remarquer également que dans ce modèle $(\mathbb{W}', \in)$ les "entiers" sont tous standards (cette affirmation a un sens parce que l'"ensemble des entiers" est définissable par un énoncé de $\mathcal{L}e$, comme expliqué dans l'annexe 2). Donc le résultat de Rabin montre qu'il n'existe pas de numérotation de $\mathbb{W}'$ qui fasse de l'appartenance une relation arithmétique. Mais ceci ne saurait nous surprendre vu le théorème de non-définissabilité de la vérité en arithmétique.

Enfin, pour conclure, il ne faudrait pas croire que "l'existence" de ce modèle quasi-naturel de $\mathcal{GB}^-$ implique "l'existence" de modèles tout aussi naturels de $\mathcal{ZF}$ car, si $\mathcal{GB}^-$ contient un axiome d'existence d'une classe infinie (par exemple : l'axiome 11 en prenant la classe complémentaire de la classe vide), $\mathcal{ZF}$ contient quant à lui la combinaison de l'axiome d'existence d'un ensemble infini, de l'axiome de l'ensemble des parties d'un ensemble et du schéma de substitution, combinaison aboutissant à des ensembles de "grosseur" véritablement "inimaginable".