# Le programme de Hilbert et les mathématiques constructives

Henri LOMBARDI
IREM de Besançon, Université de Franche-Comté.

Septembre 2002.
Article pour la revue Repères IREM

**Résumé**

Nous discutons le programme de Hilbert. Nous soutenons que seule sa version la plus primitive a été mise en échec par le théorème d'incomplétude de Gödel. Nous expliquons en quoi on peut considérer qu'il a été réalisé pour l'arithmétique élémentaire (décrite par le système formel appelé arithmétique de Peano). Pour ce qui concerne le corpus mathématique de base, nous défendons l'idée que les mathématiques constructives sont les mieux à même de réaliser le programme de Hilbert, et donc de lever les doutes quant à la validité des mathématiques classiques.

## Posons le problème

Nous commençons par une tentative consistant à énoncer le programme de Hilbert de la manière la plus générale et la plus informelle possible.

### Programme de travail

(1) *Lorsqu'un résultat concret est démontré en mathématiques par des méthodes douteuses, certifier ce résultat par des méthodes sûres.*

(2) *Réaliser ce travail de manière aussi systématique (voire automatique) que possible.*

Lorsque Hilbert développe ce genre d'idées, la théorie des ensembles traverse une crise. On a trouvé des paradoxes assez inquiétants dont on n'est pas sûr de savoir se débarrasser.

Une première difficulté concerne l'univers $U$ formé de tous les ensembles (ceux de la théorie mathématique). Normalement ce devrait être un ensemble (de la théorie mathématique), mais cela conduit à plusieurs paradoxes.
– Le premier est que l'ensemble $\mathcal{P}(U)$ doit être à la fois contenu dans $U$ et de cardinal strictement plus grand que $U$ (et pour tout ensemble $X$, une application surjective $X \to \mathcal{P}(X)$ est impossible en vertu de l'argument diagonal de Cantor).
– Le deuxième, en fait une simple variante du premier, est que la considération de la partie $V$ de $U$ définie par $V := \{x \in U \mid x \notin x\}$ conduit à la contradiction suivante :

$$V \in V \iff V \notin V$$

par simple application des définitions.

D'autres questions difficiles sont soulevées par la théorie des ordinaux de Cantor. Selon Cantor, tout ensemble devrait pouvoir être *bien ordonné* (une relation de *bon ordre* est un ordre total pour lequel toute partie admet un plus petit élément). Mais personne n'est arrivé à construire un bon ordre sur $\mathbb{R}$.

Néanmoins, Hilbert ne veut en aucun cas « être chassé du paradis que Cantor a construit pour nous ».

Face aux arguments adverses difficiles à contrer, il propose d'admettre qu'on n'est pas certain de l'existence des objets mathématiques construits par Cantor. La considération et l'utilisation de ces objets est donc à répertorier parmi les méthodes douteuses. Si ce qui arrive à la fin d'un raisonnement utilisant de telles méthodes est un résultat de nature très concrète, on n'est pas vraiment certain du résultat.

Hilbert argumente que, au fond, cela n'a pas d'importance que les ensembles infinis de Cantor n'existent nulle part, si toutefois on peut considérer ces objets comme de pures idéalités (qui nous aident à réfléchir, à développer une certaine intuition) et si on est capable de montrer qu'ils ne conduisent à aucune contradiction.

Il propose de traiter les infinis de Cantor, (et de manière générale tous les raisonnements qui impliquent en théorie une infinité de vérifications concrètes pour être assurés,) exactement comme dans le passé on a fait avec les nombres négatifs puis avec les nombres imaginaires : on a fini par s'y habituer d'une part, et on leur a trouvé ensuite une justification concrète très simple. Raisonner avec des « nombres réels avec signes » c'est comme raisonner avec la différence idéale de deux nombres réels sans signe. Raisonner avec les nombres complexes, c'est comme raisonner avec des couples de nombres réels (la partie réelle et la partie imaginaire du nombre complexe). Finalement, les procédures de calcul sont entièrement justifiées, au niveau des nombres complexes, par les procédures de calcul sur les nombres réels sans signe.

En outre on s'est rendu compte que la géométrie, pour laquelle on avait longtemps pensé que les axiomes avaient force d'évidence, ne peut pas se justifier par elle-même. Pour démontrer qu'elle ne conduit à aucune contradiction le mieux est de considérer un « modèle abstrait » dans lequel les points de l'espace géométrique sont remplacés par des triplets de nombres réels : c'est Descartes qui justifie in fine Euclide et non le contraire.

Quant aux nombres réels, ils peuvent être sujets à suspicion à cause de leur utilisation dans la théorie des ensembles infinis de Cantor, mais en même temps ils semblent garantis dans leur existence par les constructions qu'en ont fait Dedekind (via les coupures) et Cantor (via les suites de Cauchy de nombres rationnels).

Le premier des 23 problèmes de Hilbert de 1900 (voir par exemple [17]) demandait qu'on prouve ou infirme la possibilité de construire une relation de bon ordre sur $\mathbb{R}$, et qu'on prouve ou infirme l'hypothèse du continu, qui se formule comme suit : *tout sous-ensemble infini de* $\mathbb{R}$ *peut être mis en bijection, soit avec* $\mathbb{N}$*, soit avec* $\mathbb{R}$([1]).

Il est écrit sur la tombe de Hilbert : « Nous devons savoir. Nous saurons ».

« Nous aurions bien voulu savoir, et il est probable que nous ne saurons jamais » dirions-nous sur ces deux sujets aujourd'hui. En effet, on a démontré depuis que sur la

[1] Hilbert pensait à la suite de Cantor que la deuxième affirmation serait une conséquence de la première.

base d'une axiomatique « raisonnable » de la théorie des ensembles (et en supposant que cette axiomatique ne contienne pas de contradictions cachées), les deux affirmations sont indécidables et sans rapport l'une avec l'autre.

## L'échec du premier programme de Hilbert

Au départ (disons, en 1900, au moment des célèbres 23 problèmes, où l'urgence de lever les paradoxes de la théorie des ensembles 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.

Fort heureusement ce rêve quelque peu mégalomaniaque était impossible à réaliser : on sait depuis les années 30, avec les grands théorèmes d'indécidabilité, qu'il restera du travail pour les mathématiciens jusqu'à la fin des siècles. Mais à l'époque, il était permis de rêver le contraire.

Le deuxième problème demandait qu'on prouve par des moyens élémentaires la cohérence de l'arithmétique[2]. C'était une première formulation de ce qui deviendra *le programme de Hilbert*. En 1900, cette formulation était encore bien floue, car il fallait définir précisément ce qu'est une méthode élémentaire et quelle axiomatique on proposait pour l'arithmétique.

Á l'époque on croyait par exemple que la construction des réels comme (classes d'équivalence de) suites de Cauchy de rationnels impliquait que la cohérence de « l'analyse » (la théorie des nombres et fonctions réelles) pouvait facilement se déduire 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 d'une description formelle complète non seulement de $\mathbb{N}$, mais de la vérité dans $\mathbb{N}$. En conséquence, une formalisation adéquate de l'axiomatique informelle de Peano suivie d'une preuve élémentaire de la cohérence du système formel obtenu pouvait sembler la baguette magique absolue, qui permettrait à la fois de mécaniser entièrement les preuves et de traiter de manière sûre, sans paradoxes, toute l'analyse réelle.

En 1900, quand Hilbert pose son deuxième problème, les systèmes formels ne sont pas encore complètement au point, mais le problème est pertinent. Il débouche justement dans les années qui suivent sur la mise au point des systèmes formels qui permettent à Hilbert de préciser son programme (voir [18]).

Dans les années 20, Hilbert propose de démontrer, par des moyens élémentaires, la cohérence de systèmes formels dans lesquels on veut décrire non seulement l'arithmétique et l'analyse, mais la théorie des ensembles elle-même. Il précise ce qu'il entend par *méthodes élémentaires* (il dit *méthodes finitistes*) : ce sont des méthodes de preuve qui relèvent du raisonnement par récurrence lorsque celui-ci porte sur des propriétés de nature très simples (voir [19]).

[2] Encore plus audacieux, le 10ème problème demandait une méthode algorithmique pour résoudre une fois pour toutes tous les problèmes diophantiens : décider si un polynôme de $\mathbb{Z}[x_1, \ldots, x_n]$ admet ou non un zéro dans $\mathbb{Z}^n$.

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 une encyclopédie de mathématiques, et elle a alors un caractère fini et discret, donc elle est par nature opposée à l'intuition que nous avons du continu. Ainsi le système formel $\mathcal{ZF}$ (axiomatique de Zermelo-Frankel) ne décrit aucunement l'univers de la théorie des ensembles de Cantor mais seulement une activité mécanisable des mathématicien(ne)s au sujet de cet univers hypothétique.

La théorie *formelle* $\mathcal{ZF}$ est structurellement analogue à $\mathbb{N}$ mais pas à $\mathbb{R}$, et encore moins à l'univers cantorien de la théorie des ensembles. 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 : il est d'ailleurs fort heureux que le théorème d'incomplétude de Gödel qui produit ce flop interdise par la même occasion à n'importe quelle machine de simuler convenablement les capacités inventives d'Homo Sapiens.

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 profonde ignorance de la nature réelle de cet univers. 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.

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 : c'est l'arithmétique elle-même, et plus précisément n'importe quel système formel $S$ ayant pour ambition de décrire de manière suffisamment précise les entiers naturels, qui ne peut pas être prouvé cohérent par des moyens élémentaires. Plus précisément, si on s'est mis d'accord sur ce qu'on peut qualifier de *méthodes élémentaires* et si on a les a incluses dans le système $S$, alors elles seront incapables de démontrer la cohérence de $S$ puisque le théorème d'incomplétude de Gödel dit que $S$ ne peut pas prouver l'énoncé formel qui signifie que $S$ est cohérent (plus précisément, si $S$ prouve cet énoncé, alors $S$ est incohérent[3]).

## La nécessité d'une reformulation du programme de Hilbert

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 outrancier de Bourbaki), et comme une certaine dose d'infini à l'état au moins potentiel est nécessaire aux mathématiques, le programme de Hilbert, en tant que réflexion, par des moyens sûrs, au sujet des mathématiques pratiquées, reste une tâche permanente. À défaut de pouvoir maîtriser l'infini par en bas une fois pour toutes, ce qui était trop ambitieux, il reste nécessaire d'analyser la pratique mathématique de l'infini.

De manière 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

[3] Ceci constitue le deuxième théorème d'incomplétude de Gödel. Le premier théorème d'incomplétude affirme, après un raffinement apporté par Rosser que si $S$ est cohérent, alors il est incomplet. Plus précisément, on peut expliciter une fonction primitive récursive $f : \mathbb{N} \to \mathbb{N}$ telle que l'énoncé « $\forall n \in \mathbb{N},\ f(n) = 0$ » est vrai mais n'a pas de preuve dans $S$.

de l'étude d'un jeu très concret, très compliqué et sans signification profonde, par exemple le jeu que Bourbaki appelle LA mathématique.

Comme exemple a contrario, qui montre que les mathématicien(ne)s sont au premier chef intéressé(e)s par la *signification* des théorèmes *et* de leurs preuves, on peut signaler que l'activité de recherche en mathématiques est consacrée en bonne partie à la *simplification des preuves*. 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 du programme de Hilbert (révisé à la baisse) est réalisé.

Prenons un exemple célèbre. Une conjecture mathématique due à Mordell affirme que toute courbe algébrique rationnelle plane de genre $\geq 2$ ([4]) n'a qu'un nombre fini de points rationnels. Cette conjecture a été démontrée par une belle méthode très abstraite en 1983 par G. Faltings. Immédiatement une activité intense de simplification et d'explicitation de la preuve s'est mise en route. Et les mathématicien(ne)s ne seront pas satisfait(e)s tant qu'ils (elles) n'auront pas réussi à rendre beaucoup plus précise l'affirmation concernant le « nombre fini de points » : trouver une méthode générale qui permette de calculer pour chaque courbe de la famille en question une majoration explicite de ce nombre fini, ou mieux de borner la taille des nombres rationnels que sont les coordonnées des points en question. En d'autres termes les mathématicien(ne)s ne seront pas satisfait(e)s tant qu'ils (elles) n'auront pas soumis le beau théorème abstrait aux préceptes du programme de Hilbert.

Il y a donc un contraste saisissant entre l'opinion commune selon laquelle le programme de Hilbert est illusoire, opinion basée sur l'échec qu'il a subi dans sa forme primitive, et la volonté concrète de réaliser ce programme, de manière non systématique il est vrai, chaque fois qu'un beau théorème n'est pas complètement validé.

Depuis une quarantaine d'années cependant se sont accumulés des résultats qui vont dans le sens d'un traitement vraiment systématique du programme de Hilbert. La fin de cet article essaie de décrire quelques uns de ces résultats et plaide en faveur des mathématiques constructives en tant qu'elles constituent la manière la plus pratique de réaliser le programme de Hilbert, parce que la plus naturelle, la plus intuitive, la moins encombrée de formalisme et de techniques relevant de la logique mathématique.

## Le Principe du Tiers Exclu comme principe litigieux fondamental

On pense souvent que le principe litigieux le plus important en mathématiques classiques est l'axiome du choix.

Certes l'axiome du choix conduit à des constructions fort peu crédibles, comme une base de $\mathbb{R}$ en tant que $\mathbb{Q}$-espace vectoriel, ou la multiplication des boules de $\mathbb{R}^3$ non pas selon les miracles de l'Évangile, mais selon le théorème de Banach-Tarski (voir l'encadré sur ce sujet).

[4] Par définition une courbe algébrique plane est rationnelle si l'équation qui la définit est un polynome irréductible à coefficients entiers. Le genre d'une courbe algébrique est une notion délicate, mais très importante. Les courbes rationnelles de genre 0 qui possèdent au moins un point rationnel admettent une paramétrisation par des fractions rationnelles à coefficients rationnels. Les courbes rationnelles de genre 1 sont également assez bien connues et certaines admettent une infinité de points rationnels.

En fait, le mal est plus profond que l'axiome du choix, et la plupart des « constructions » à l'oeuvre dans la théorie de Cantor ont une signification très obscure, à commencer par la considération de l'ensemble des parties d'un ensemble infini. Poincaré pensait que de telles méthodes présentent inévitablement des cercles vicieux.

### Les critiques de Poincaré contre l'infini actuel

Le livre « Dernières pensées » ([26] 1913) regroupe divers articles et conférences que Henri Poincaré (mort en 1912) destinait à former le 4ème volume de ses ouvrages de philosophie scientifique. Dans les deux articles « La logique de l'infini » et « Les mathématiques et la logique » il attaque vigoureusement la théorie des ensembles et les axiomatiques qui en ont été proposées. Le fond de son argumentation est que l'infini n'existe qu'à l'état potentiel et que donc une axiomatique prétendant décrire l'infini comme un donné achevé n'est fondée sur aucune évidence intuitive et renferme inévitablement des cercles vicieux. Voici un court extrait du résumé qui conclut le premier de ces articles.

« M. Zermelo a voulu construire un système impeccable d'axiomes ; mais ces axiomes ne peuvent être regardés comme des décrets arbitraires, puisqu'il faudrait montrer que ces décrets ne sont pas contradictoires, et qu'ayant fait entièrement table rase on n'a plus rien sur quoi l'on puisse appuyer une semblable démonstration. Il faut donc que ces axiomes soient évidents par eux-mêmes. or quel est le mécanisme par lequel on les a construits ? on a pris des axiomes qui sont vrais des collections finies ; on ne pouvait les étendre tous aux collections infinies, on n'a fait cette extension que pour un certain nombre d'entre eux, choisis plus ou moins arbitrairement. A mon sens d'ailleurs [...] aucune proposition concernant les collections infinies ne peut être évidente par définition. [...]

Quant à moi je proposerais de s'en tenir aux règles suivantes :

1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots ;
2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini ;
3. Éviter les classifications et les définitions non prédicatives.

[...] On se propose d'enseigner les mathématiques à un élève qui ne sait pas encore la différence qu'il y a entre l'infini et le fini ; on ne se hâte pas de lui apprendre en quoi consiste cette différence ; on commence par lui montrer tout ce qu'on peut savoir de l'infini sans se préoccuper de cette distinction ; puis dans une région écartée du champ qu'on lui a fait parcourir, on lui découvre un petit coin où se cachent les nombres finis. Cela me paraît psychologiquement faux. ... »

En 1918, développant les idées de Poincaré et prenant le contre-pied de Hilbert, Hermann Weyl a montré dans le livre *Das Kontinuum* comment on pouvait se passer, pour fonder l'analyse classique, de la théorie des ensembles à la Cantor. Pour lui, la seule base solide des mathématiques est constituée par les entiers naturels. Comme Poincaré et contrairement à Hilbert, il ne cherche aucune preuve « élémentaire » pour la cohérence du système des entiers naturels. Par contre il ne prend ce système que comme un infini potentiel et refuse absolument de considérer l'ensemble de toutes les parties de $\mathbb{N}$ comme un objet bien défini. Il explique comment on peut très bien s'en passer sans pour autant renoncer aux nombres réels, aux fonctions continues, aux espaces de Hilbert usuels et à beaucoup d'autres notions de base.

Il montre qu'on peut baser les mathématiques usuellement pratiquées, celles par exemple qui ont des conséquences intéressantes pour la physique, d'une part sur des objets de même complexité que les entiers naturels (par exemple les nombres rationnels), et sur les suites infinies de tels objets d'autre part (par exemple les nombres réels, ou les espaces métriques complets à base dénombrable, peuvent être compris de cette manière).

Le Modern Algebra de van der Waerden est de fait écrit selon ce même point de vue.

Ce point de vue est également mis en pratique par ceux qui implémentent les mathématiques sur ordinateur.

La position d'Hermann Weyl a été poursuivie et développée au 20ème siècle par des logiciens, au premier rang desquels il faut citer Solomon Feferman. Une synthèse des idées de Feferman se trouve dans son livre *In the light of logic* [12], que nous commenterons à la fin de l'article.

## Le théorème de Banach-Tarski

Dans le système axiomatique $\mathcal{ZFC}$ qui se veut une description de l'Univers cantorien ensembliste, le théorème de Banach-Tarski est l'enoncé suivant :

*On peut décomposer la boule unité dans $\mathbb{R}^3$ en une partition finie, de telle sorte que les morceaux de cette partition, réarrangés spatialement via des* isométries *de $\mathbb{R}^3$ forment maintenant les partitions de deux boules unités l'une à coté de l'autre.*

Le peu d'espoir de voir se réaliser la duplication des lingots d'or en application de ce théorème n'a pas découragé la plupart des mathématicien(ne)s, qui se contentent d'oublier le théorème dans la minute qui suit son énoncé.
Contrairement à la solution de la conjecture de Mordell par Faltings (voir page 5), ce théorème n'a fait l'objet d'aucune investigation supplémentaire visant à le rendre « explicite », car aucun espoir ne semble permis dans cette direction. Cela signifie bien que les mathématicien(ne)s n'accordent pas le même degré de réalité à la théorie des nombres et à la théorie des ensembles.

En fait comme l'a fait remarquer Brouwer, qui était le principal contestataire de Hilbert au début du vingtième siècle, c'est dans le principe du tiers exclu, appliqué sans discernement à des situations par essence infinies, que se situe le principal obstacle quand on essaie d'attribuer une signification claire aux preuves et aux énoncés des mathématiques classiques. Hermann Weyl a d'ailleurs apporté son appui sur le fond à la position de Brouwer (cf. dans le livre de Feferman [12] l'article « Infinity in Mathematics : Is Cantor necessary ? »).

On appelle *principe d'omniscience* un principe qui, bien qu'accepté comme une évidence en mathématiques classiques, pose manifestement problème, car il suppose une connaissance a priori de ce qui se passe dans une situation essentiellement infinie. Le mot omniscience vaut donc ici pour « prescience de l'infini ».

En appliquant les méthodes de Hermann Weyl pour limiter drastiquement l'usage des infinis en mathématiques, la majeure partie de l'analyse classique devient non problématique si on veut bien admettre un *Petit Principe d'Omniscience*, que nous décrivons maintenant.

Soit $\alpha = (\alpha_n)$ une *suite binaire*, i.e., une construction qui pour chaque entier naturel (pris en entrée) donne en sortie un élément de $\{0, 1\}$ (on dit encore : *un booléen*). Considérons les assertions suivantes :

$$\begin{array}{rcl} P(\alpha) & : & \alpha_n = 1 \text{ pour un } n, \\ \neg P(\alpha) & : & \alpha_n = 0 \text{ pour tout } n, \\ P(\alpha) \vee \neg P(\alpha) & : & P(\alpha) \text{ ou } \neg P(\alpha), \\ \forall \alpha \ \ (P(\alpha) \vee \neg P(\alpha)) & : & \text{pour toute suite binaire } \alpha, \ P(\alpha) \text{ ou } \neg P(\alpha). \end{array}$$

Une preuve *constructive* de $P(\alpha) \vee \neg P(\alpha)$, c'est-à-dire une preuve qui rend parfaitement claire l'affirmation correspondante, doit fonctionner avec la signification du « ou » et du « il existe » sous leur forme explicite. En conséquence, un sous-produit de cette preuve serait un algorithme qui décide si $\alpha_n = 0$ pour tout $n$, et dans le cas contraire calcule un entier naturel $n$ tel que $\alpha_n = 1$. Cet algorithme serait un algorithme général qui s'appliquerait à n'importe quelle suite binaire bien définie d'un point de vue constructif.

Un tel algorithme est beaucoup trop performant, car il permettrait de résoudre de manière automatique, sans effort d'imagination, la plupart de conjectures mathématiques importantes.

En fait nous savons que si un tel algorithme existe, il n'est certainement pas « mécaniquement calculable ». Un programme qui tourne sur machine ne peut sûrement pas accomplir un tel travail même lorsqu'on impose une limitation sévère sur l'entrée $\alpha$ : qu'elle soit une suite binaire *primitive récursive* [5] explicite.

C'est un théorème fondamental de la théorie du calcul mécanisable, qu'on peut exprimer comme suit :

**Théorème de la halte des programmes** (On ne peut pas tout savoir)
*Sous trois formes immédiatement équivalentes :*

- *Le débuggage ne peut pas être automatisé*[6] *: il n'existe pas de programme $T$ qui puisse tester si un programme arbitraire $P$ finira par aboutir à l'instruction Stop.*
- *Il n'existe pas de programme qui puisse tester si une suite primitive récursive arbitraire est identiquement nulle.*
- *Il n'existe pas de programme $U$ qui prenne en entrée deux entiers, donne en sortie un booléen, et qui énumère toutes les suites binaires programmables (la suite $n \mapsto U(m, n)$ est la $m$-ème suite énumérée par $U$).*

[5] Une suite est primitive récursive si elle se laisse calculer par un programme de nature élémentaire, voir l'encadré à part sur ce sujet.

[6] En particulier, l'ex-ministre de l'Éducation Nationale C. Allègre se trompait dans ses déclarations sur le remplacement des mathématiciens par des machines : celles-ci ne remplaceront jamais l'intelligence humaine pour ce qui concerne nos besoins de connaissance abstraite mathématique, et notamment pour obtenir un fonctionnement correct des machines elles-mêmes.

Non seulement ce théorème , sous sa dernière formulation, ressemble au théorème de Cantor qui affirme qu'on ne peut pas énumérer l'ensemble des suites binaires, mais la preuve, très simple, est essentiellement la même.

Bien que le théorème précédent n'interdise pas a priori l'existence d'une procédure effective mais non mécanisable pour résoudre de manière systématique ce type de problèmes, il confirme l'idée intuitive selon laquelle il faudra toujours faire preuve de nouvelle inventitivité pour progresser dans notre connaissance du monde mathématique.

Aussi, d'un point de vue constructif, nous rejetons le *Petit Principe d'Omniscience (Limited Principle of Omniscience)* :

– (**LPO**) : Si $(\alpha_n)$ est une suite binaire, alors ou bien il existe un $n$ tel que $\alpha_n = 1$, ou bien $\alpha_n = 0$ pour tout $n$.

Ce refus semble souvent exagéré : l'interlocuteur a tendance à exiger sur le champ un contre-exemple précis, une suite $\alpha$ qui refuse absolument de se plier au tiers exclu. Ce que ne fournit pas le théorème de la halte des programmes.

## Les fonctions primitives récursives

Une fonction primitive récursive est une fonction $\mathbb{N}^k \to \mathbb{N}$ qui peut être définie par composition ou par récurrence ordinaire à partir de fonctions primitives récursives déjà définies. Au départ on a par exemple la fonction $+$ et les constantes $0, 1$. En fait du point de vue des nombres entiers codés en binaire, les fonctions de base seraient plutôt : $n \mapsto 2\,n,\ n \mapsto 2\,n+1,\ n \mapsto n \operatorname{div} 2,\ n \mapsto n \bmod 2$.

On peut également définir une fonction primitive récursive $\mathbb{N}^k \to \mathbb{N}$ comme une fonction qui peut être calculée par un programme obéissant aux spécifications suivantes. Il utilise uniquement des variables entières et booléennes, et il n'autorise qu'un nombre limité d'instructions :

– un certain nombre d'affectations élémentaires :
  l'addition des entiers, les fonctions booléennes usuelles,
  le test d'égalité à 0 pour un entier,
  la définition cas par cas : si $b$ alors $x \leftarrow y$ sinon $x \leftarrow z$, (ici $b$ est un booléen)

– les boucles pour.

Une fois fixée la syntaxe du langage de programmation correspondant, chaque programme bien écrit possède un *nombre de Gödel*, qui est simplement *le texte du programme* interprété comme un nombre entier écrit en base $b$ où $b$ est le nombre d'éléments dans l'alphabet utilisé par le langage de programmation.

Il s'ensuit par exemple qu'on peut énumérer toutes les fonctions primitives récursives à une seule variable. Si $f_n$ est la fonction primitive récursive numérotée $n$, la fonction $n \mapsto f_n(n) + 1$ n'est sûrement pas primitive récursive, selon l'argument diagonal de Cantor.

L'immense majorité des mathématiques couramment pratiquées admet un codage primitif récursif. Par exemple, les décimales de $\pi$ ou de $\sin(2)$ forment des suites primitives récursives.

En fait, sans prendre parti sur la possibilité qu'existe ou non un tel contre-exemple, ce qui à notre avis ne peut être tranché ni dans un sens ni dans l'autre de manière « objective », il faut plutôt considérer que le refus de **LPO** est indispensable si on veut que les preuves d'existence en mathématiques soient des preuves d'existence effective.

Toute personne qui a essayé un jour de programmer le calcul du rang d'une matrice réelle sait qu'il n'y a pas de solution raisonnable. La réponse à la question est fondamentalement instable (sauf au voisinage des matrices de rang maximum), et aucun algorithme sérieux ne sera jamais produit en analyse numérique pour résoudre ce problème. Ce problème est tout simplement mal posé, car il dépend de manière incontournable du test d'égalité à 0 pour les nombres réels, ce qui est une des formes équivalentes de **LPO**.

Si on veut donc éviter d'avoir des théorèmes mathématiques d'existence (ici l'existence du rang d'une matrice) sans aucun espoir d'existence explicite, c'est-à-dire sans aucun espoir d'une signification claire du mot « exister », il faut se passer de **LPO**.

Cela peut sembler bien douloureux, mais c'est surtout un problème de culture. Quand on acquiert une culture constructive, l'acceptation de **LPO** semble un acte de surdité ou d'ignorance.

Le principe **LPO** a de nombreuses formes équivalentes, e.g. :

1. $\forall x \in \mathbb{R}$, $(\ x \neq 0\ \vee\ x = 0\ )$.
2. $\forall x \in \mathbb{R}$, $(\ x > 0\ \vee\ x = 0\ \vee\ x < 0\ )$.
3. Toute suite décroissante dans $\mathbb{N}$ est constante à partir d'un certain rang.
4. Toute suite dans $\mathbb{N}$ admet un plus petit élément.
5. D'une suite bornée dans $\mathbb{N}$ on peut extraire une sous-suite infinie constante.
6. Toute suite dans $\mathbb{N}$ est ou bien bornée, ou bien non bornée.
7. Toute suite bornée monotone dans $\mathbb{R}$ converge.
8. Toute suite minorée de $\mathbb{R}$ admet une borne inférieure.
9. D'une suite bornée dans $\mathbb{R}$ on peut extraire une sous-suite convergente.
10. Tout nombre réel est ou bien rationnel ou bien irrationnel.
11. Tout sous-espace de vectoriel de type fini de $\mathbb{R}^n$ admet une base.
12. Tout espace de Hilbert séparable admet ou bien une base hilbertienne finie ou bien une base hilbertienne dénombrable.
13. Tout sous-groupe détachable[7] de $\mathbb{Z}$ est un sous groupe $a\mathbb{Z}$.
14. Tout sous-groupe de $\mathbb{Z}^p$ engendré par une suite $(u_n)_{n\in\mathbb{N}}$ dans $\mathbb{Z}^p$ est de type fini.

En outre, **LPO** admet comme conséquences d'autres théorèmes incontournables en mathématiques classiques. Ces théorèmes n'impliquent pas **LPO** mais ils sont équivalents à un principe d'omniscience un peu plus faible, appelé **LLPO**, dont voici quelques formes équivalentes.

1. $\forall x \in \mathbb{R}\quad (\ x \leq 0\ \vee\ x \geq 0\ )$
   (ceci permet de faire de nombreuses preuves par dichotomie avec les nombres réels.)

[7] Une partie $A$ d'un ensemble $B$ est dite détachable si on sait tester l'appartenance d'un élément de $B$ à $A$. Sous forme symbolique c'est une partie $A$ qui vérifie le principe de tiers exclu suivant : $\forall x \in B\ \ (x \in A \vee x \notin A)$. Par exemple tout sous groupe de type fini de $\mathbb{Z}^p$ est détachable, ou, beaucoup plus remarquable, tout idéal de type fini de $\mathbb{Z}[X_1, \ldots, X_n]$ est détachable.

2. $\forall x, y \in \mathbb{R} \quad ( \; xy = 0 \; \Rightarrow \; ( \; x = 0 \; \vee \; y = 0 \; ) \; )$.
3. L'image d'un intervalle $[a, b] \subset \mathbb{R}$ par une fonction réelle uniformément continue est un intervalle $[c, d]$.
4. Une fonction réelle uniformémént continue sur un espace métrique compact atteint ses bornes.
5. (une des versions du lemme de König) Tout arbre infini explicite à embranchements finis possède une branche infinie.

Naturellement **LPO** n'est qu'une forme très particulière et extrêmement limitée du grand principe général d'omniscience (de prescience de l'infini) qu'est le *principe général du tiers exclu*.

## L'arithmétique avec et sans le Principe du Tiers Exclu

Une formalisation de nombreuses méthodes constructives concernant les entiers naturels est donnée par un système formel appelé Arithmétique de Heyting, avec pour acronyme $\mathcal{HA}$.

Une version plus faible de ce système formel est appelée Arithmétique primitive récursive, avec pour acronyme $\mathcal{PRA}$.

Dans ces systèmes formels nous travaillons avec $\mathbb{N}$ vu comme une sorte de structure algébrique. Nous avons des constantes, des fonctions et des prédicats représentés par des symboles, avec au moins $+, \times, =, 0, 1$. Les variables représentent toutes des entiers naturels. Nous ajoutons aussi un symbole pour chaque *fonction primitive récursive*.

Dans les axiomes de la théorie $\mathcal{PRA}$ on met les formules qui correspondent aux définitions des fonctions primitives récursives (par substitution et par récurrence).

Les *formules atomiques* sont les formules $t = t'$ où $t$ et $t'$ sont des termes bien écrits (nous pouvons voir $t$ et $t'$ comme deux fonctions primitives récursives des variables qui y figurent).

Dans $\mathcal{PRA}$ on n'utilise pas d'autres formules que ces formules atomiques, donc pas de connecteurs logiques ni de quantificateurs. Les seuls théorèmes sont de la forme $t = t'$ avec la quantification universelle implicite sur les variables qui y figurent. Les deux seules méthodes de preuve sont :

– primo : la substitution d'égaux produit des égaux
– secundo : la preuve par récurrence.

Un exposé remarquable mais un peu technique du système $\mathcal{PRA}$ se trouve dans le livre de Goodstein [15][8]. La force du système est surprenante. On a pu mettre en évidence qu'un très grand nombre de théorèmes concrets peuvent se démontrer à l'intérieur de ce système (voir par exemple [21]).

Des logiciens ont argumenté de façon assez convaincante pour dire que les méthodes finitistes admises par Hilbert ([19]) recouvraient exactement ce qui est prouvable dans $\mathcal{PRA}$ (voir par exemple Tait [30]).

Dans $\mathcal{HA}$ nous autorisons les *formules du premier ordre*, i.e., les formules construites à partir des formules atomiques en utilisant les connecteurs logiques et les quantificateurs.

[8] En fait Goodstein admet des récurrences multiples, qui permettent de construire des fonctions plus compliquées que les seules fonctions primitives récursives.

Nous avons aussi un « schéma de preuve par récurrence » qui dit pour toute formule qu'elle peut être prouvée par récurrence sur l'une des variables libres qui y est présente.

Finalement nous avons des axiomes logiques et des règles de déduction conformes aux raisonnements utilisés dans les mathématiques constructives.

Toute formule sans quantificateur de $\mathcal{HA}$ est équivalente (à l'intérieur du système formel $\mathcal{HA}$) à une formule $f(n_1, \ldots, n_k) = 0$ où $f$ est une fonction primitive récursive et les $n_j$ sont les variables apparaissant dans la formule.

### Formes équivalentes de **LPO** (un exemple)

Nous montrons ici deux équivalences annoncées page 10. Cela peut être instructif pour voir fonctionner des preuves constructives. Rappelons qu'en mathématiques classiques le principe **LPO** est trivial. Ce principe ne prend sa signification que lorsqu'on décide de lire les « ou » et « il existe » avec leur signification intuitive usuelle[a] explicite.

3. $\Rightarrow$ 4. Soit $(u_n)$ une suite dans $\mathbb{N}$. On considère la suite $(v_n)$ définie par $v_n = \inf(u_k; 0 \leq k \leq n)$. Montrer que $(u_n)$ admet un plus petit élément revient à montrer que $(v_n)$, qui est une suite décroissante, est constante à partir d'un certain rang.

**LPO** $\Rightarrow$ 3. Etant donnée une suite décroissante $(v_n)$ on considère la suite double binaire $(w_{n,m})$ définie par $w_{n,m} = 0$ si $v_{n+m} = v_n$, $w_{n,m} = 1$ sinon. Pour chaque valeur de $n$, en application de **LPO**, la suite $m \mapsto w_{n,m}$ est ou bien identiquement nulle, ou bien non identiquement nulle de manière explicite. On définit alors les entiers successifs $n_0 < n_1 < \cdots$ de proche en proche comme suit :

– $n_0 = 0$

– si $n_k$ est défini, ou bien la suite $m \mapsto w_{n_k,m}$ est identiquement nulle et on arrête la suite à $n_k$, ou bien ce n'est pas le cas et on prend pour $n_{k+1}$ le plus petit entier $n_k + m$ tel que $w_{n_k,m} = 1$, c'est-à-dire le plus petit entier $n > n_k$ tel que $v_n < v_{n_k}$.

Par construction on a $v_0 = v_{n_0} > v_{n_1} > \cdots$ si bien que la suite $n_k$ s'arrête en au plus $v_0$ étapes. On a en fait donné un algorithme qui prend en entrée la suite décroissante $(v_n)$ et donne en sortie le rang $n_k$ à partir duquel cette suite est stationnaire. Pour cela on a eu besoin de consulter (au plus $v_0$ fois) un « oracle » d'omniscience de type **LPO**.

4. $\Rightarrow$ **LPO** Si $(a_n)$ est une suite binaire considérons la suite $n \mapsto 1 - a_n$. Si sa plus petite valeur est obtenue pour $n = k$, ou bien cette plus petite valeur est $0$ et la suite $(a_n)$ n'est pas identiquement nulle, précisément $a_k = 1$, ou bien cette valeur est $1$ et la suite $(a_n)$ est identiquement nulle.

[a] Ce que je veux savoir ce n'est pas que le bébé est un garçon ou une fille, merci je ne suis pas débile, mais si c'est un garçon ou une fille

Nous considérons aussi le système formel appelé Arithmétique de Peano qui a pour acronyme $\mathcal{PA}$. Ce système est obtenu à partir de $\mathcal{HA}$ en ajoutant l'axiome $P \vee \neg P$ pour toute formule bien écrite de $\mathcal{HA}$.

Concernant la portée et la signification de ce principe de tiers exclu, dans cette situation arithmétique précise, on peut montrer qu'il est moins fort que **LPO**. En fait, dans $\mathcal{PA}$

l'utilisation de la logique classique correspond à une version affaiblie de **LPO** dans laquelle n'interviennent que les suites d'entiers définissables[9] dans le langage de $\mathcal{PA}$, c'est à dire ce que les logiciens appellent les *suites arithmétiques* : autrement dit, $\mathcal{PA} = \mathcal{HA} + \mathbf{LPO}_{arith}$.

Le système formel $\mathcal{PA}$ prouve plus de « théorèmes » que $\mathcal{HA}$ : par exemple, on construit assez facilement une fonction[10] primitive récursive $f(n,m)$ telle que la formule

$$\forall n \;\; (\forall m \; f(n,m) = 0 \;\text{ ou }\; \exists m \; f(n,m) \neq 0)$$

est évidemment vraie dans $\mathcal{PA}$ alors qu'elle n'est pas prouvable dans $\mathcal{HA}$, parce qu'elle correspond à une version affaiblie de **LPO** qui est impossible à réaliser concrétement par un programme (le test sur $n$ pour savoir dans quelle branche de l'alternative on tombe n'est pas calculable par un programme).

Néanmoins, il a été prouvé constructivement le résultat très significatif suivant : *tant qu'on n'a pas de divergence d'interprétation entre le point de vue constructif et le point de vue classique concernant un énoncé, $\mathcal{PA}$ ne prouve rien de plus que $\mathcal{HA}$*, précisément (voir par exemple [13]) :

**Théorème** *Si $f : \mathbb{N}^2 \to \mathbb{N}$ est une fonction primitive récursive arbitraire alors la formule $\forall n \, \exists m \;\; f(n,m) \neq 0$ est prouvable dans $\mathcal{PA}$ si et seulement si elle est prouvable dans $\mathcal{HA}$.*

Ceci signifie que les facilités données par **LPO** ne posent pas problème quand elles servent à prouver avec les moyens (limités) de $\mathcal{PA}$ des formules qui ne sont pas trop compliquées. Ce théorème assure un contenu constructif pour une grande quantité de mathématiques classiques, en particulier pour celles qui peuvent être développées selon les préceptes d'Hermann Weyl dans [33].

Ce genre de résultat en logique doit être considéré comme donnant *une réponse positive partielle* au programme de Hilbert.

## Le programme de Hilbert revisité

Au vu de ce succès obtenu pour l'arithmétique de Peano nous proposons pour le programme de Hilbert une version plausible mais parfaitement raisonnable, qui, nous le croyons, en respecte la signification la plus profonde. Nous remplaçons seulement le mot *finitiste* par le mot *constructif*.

### Programme de travail

(1) *Lorsqu'un résultat concret est démontré en mathématiques par des méthodes douteuses, certifier ce résultat par des méthodes constructives.*

(2) *Réaliser ce travail de manière aussi systématique (voire automatique) que possible.*

Le théorème d'incomplétude de Gödel ne peut pas mettre hors jeu cette version (raisonnable) du programme de Hilbert. Pour la simple raison que nous ne donnons pas de

[9] D'un point de vue classique.

[10] Cette fonction est celle qui intervient dans le théorème de la halte des programmes, $f(n,m) = 0$ signifie que le programme n°$n$ s'est arrêté au bout de $m$ étapes élémentaires.

définition restrictive a priori de ce que c'est qu'une preuve constructive. Et cela n'enlève évidemment rien à notre profonde admiration pour le théorème d'incomplétude de Gödel.

Sous cette forme le programme de Hilbert a été réalisé pour l'arithmétique de Peano, grâce au théorème cité ci-dessus. Malheureusement, les mathématiques classiques usuelles ne sont pas *facilement* formalisables dans $\mathcal{PA}$([11]).

## Les mathématiques constructives comme réalisation partielle du programme de Hilbert

Quand Erret Bishop publie en 1967 un livre, *Foundations of Constructive Analysis* [4], où il interprête en termes constructifs les bases de l'analyse moderne, il réalise un morceau substantiel du programme de Hilbert tel que nous venons de l'énoncer.

Dans le livre de Bishop tous les théorèmes d'analyse ont la signification d'algorithmes qui calculent des objets concrets à partir d'autres objets concrets, conformément à certaines spécifications requises, et ces algorithmes sont *prouvés par des méthodes sûres* : en particulier personne ne conteste qu'ils aboutissent certainement en un temps fini au résultat souhaité. Ainsi les bases de l'analyse sont ramenées à un degré de certitude comparable à ce qui règne en théorie élémentaire des entiers naturels.

Bishop va bien au delà de ce qu'avait pu faire auparavant un logicien remarquable comme Goodstein dans [16] : non seulement sont traités une quantité incomparablement plus grande de résultats, mais encore, le style d'exposition est direct, sans autre différence sensible avec le style mathématique usuel qu'une attention scrupuleuse accordée aux aspects effectifs.

On pourra lire à ce sujet l'article de D. Knuth [20] dans lequel il analyse quelques « page n°100 » dans différents livres de mathématiques, dont celui de Bishop, du point de vue la pensée algorithmique.

Non seulement, le programme de Hilbert (revisité) n'est pas utopique, mais il a de bonnes chances de pouvoir être développé sur une grande ampleur après un tel coup de maître.

Mais au lieu d'être acclamé comme le travail d'un bienfaiteur des mathématiques, *Foundations of Constructive Analysis* a été accueilli par une quasi-indifférence des professionnels. Ceci ne s'explique que par le poids de la routine (qu'est-ce que c'est que ce type qui prétend faire changer nos standards ?) et par le manque presque total de questionnement des *professionnels* concernant la *signification* de leur activité scientifique. L'épistémologie des mathématiques n'est pas à l'ordre du jour, elle ne fait pas partie du cursus normal : elle n'est presque pas enseignée, et quand elle l'est c'est en général uniquement à titre de spécialité.

Le livre de Bishop a été rapidement épuisé (pas à cause des ventes en France, rassurez-vous M. Bourbaki) et a fait l'objet d'études approfondies chez les logiciens (citons notam-

[11] Ce travail donne des résultats spectaculaires et trop peu connus. Une énorme quantité de résultats concrets obtenus en mathématiques classiques peuvent être formulés dans $\mathcal{PA}$ et beaucoup de preuves classiques peuvent, avec un certain effort, être transformées en preuves dans $\mathcal{PA}$. En fait on ne travaille en général pas directement dans $\mathcal{PA}$ mais dans des extensions conservatives de $\mathcal{PA}$. Voir notamment [12] et [21].

ment M. Beeson [2, 3]). Une nouvelle édition [5], dans laquelle la théorie de l'intégrale de Lebesgue a été simplifiée, est parue en 1985.

En algèbre, le point de vue algorithmique a toujours eu des défenseurs. Il y a de quoi, puisque le mot *algèbre* est tiré de *Al Djabr*, extrait du titre d'un livre écrit il y a fort longtemps par un auteur arabe qui s'appelait *M. Algorithme* (Al Kwarismi).

Il faut bien évidemment souligner la tradition de Gauss et Kronecker, entièrement dans le style algorithmique.

Bien que les méthodes abstraites soient ensuite devenues quelque peu hégémoniques sous l'influence de Hilbert puis de Bourbaki, il est encore permis d'enseigner et de publier des algorithmes. Signalons entre autres les travaux de Seidenberg (par exemple [28, 29]).

En 1985 le merveilleux petit livre de Mines, Richman et Ruitenburg [25] a fait pour les bases de l'algèbre moderne ce qu'avait fait le livre de Bishop pour celles de l'analyse.

La nouvelle discipline du Calcul Formel (calculs symboliques et algébriques sur machine [8, 9]) se rattache de facto à cette tradition, même si les auteurs ne comprennent pas toujours la différence entre preuve constructive et algorithme : un algorithme qui met en oeuvre un théorème d'algèbre est parfois prouvé par des méthodes abstraites non constructives, auquel cas le programme de Hilbert n'est réalisé que très imparfaitement pour le théorème en question.

## Deux ou trois commentaires sur la bibliographie en guise de conclusion

Malheureusement, vous trouverez ci-dessous dans la bibliographie surtout des livres ou des articles écrits en anglais.

C'est le résultat entre autres de la politique désastreuse de non traduction en français des grands ouvrages étrangers par les éditeurs français, y compris les éditeurs institutionnels. A titre de comparaison, la plupart des ouvrages importants dans n'importe quelle langue sont traduits en anglais, et on trouve plus de traductions italiennes et espagnoles que de traductions françaises d'ouvrages importants.

Les bases des mathématiques constructives sont dans [5] et [25]. Le livre [6] est une très bonne introduction aux différentes variantes des mathématiques constructives. Le livre de Aberth [1] est une présentation simple de la variante récursiviste russe (dans laquelle tous les objets sont supposés « récursifs »).

Le livre de David, Nour et Raffali [10] est un livre d'enseignement universitaire. Il doit être salué comme le premier livre de ce type (à notre connaissance) écrit en français et qui accorde la place qu'elle mérite à la logique intuitionniste (la logique des mathématiques constructives). Cependant il est écrit du point de vue des mathématiques classiques, ce qui est paradoxal quand on veut traiter sérieusement la question des fondements (il est vrai que ce n'est pas l'objet essentiel de l'ouvrage).

Le livre de Gilles Dowek [11] est par ailleurs un excellent petit texte de présentation de la logique, mais écrit pour un public large, donc sans description précise des outils de la logique mathématique.

Le livre [22] de Jean-Louis Krivine, d'une clarté remarquable, doit être lu par tout(e) mathématicien(ne) qui veut comprendre ce qu'est la théorie *formelle* des ensembles :

l'étude d'une structure particulière, non pas celle d'anneau commutatif, ni celle de treillis distributif, mais celle d'univers, c'est-à-dire la structure des ensembles (naïfs) munis d'une relation, notée « $\in$ » vérifiant des axiomes convenables[12].

En informatique les auteurs clairvoyants ne cachent pas que la seule logique qui vaille pour l'informatique théorique est la logique intuitionniste. Voir par exemple le beau livre de Lalement [24].

Le livre de Lakatos [23] reste une source importante de réflexion sur les fondements. Notamment, la place centrale qui est accordée aux preuves par rapport aux théorèmes est en accord profond avec le dicton constructif : ce qui est vrai est ce qui peut être prouvé. De manière similaire, et dans la mesure où on prend le programme de Hilbert au sérieux, ce seront les preuves plus que les théorèmes des mathématiques classiques qui doivent être considérées comme contenant la part de vérité objective présente en mathématiques classiques.

L'article d'Abraham Robinson [27], le fondateur de l'analyse non standard, montre à quel point ce visionnaire des infinitésimaux doute de la réalité de l'infini cantorien.

Le livre [14] donne une traduction française de l'article original de Gödel où il établit ses théorèmes d'incomplétude. Il contient aussi la traduction française d'un livre de Nagel et Newman exposant de manière simple les idées à l'oeuvre dans l'article de Gödel. Enfin on trouve un commentaire de J.-Y. Girard dans lequel il assassine avec brio un certain nombre de positions adverses, dont celle de Hilbert.

Le livre [31] est un recueil d'articles, en français, italien et anglais, de physiciens, de logiciens, de philosophes et d'historiens des sciences sur le problème de l'infini dans les sciences. Sa lecture pourrait aider les mathématicien(ne)s à sortir de leur bulle et à jeter un regard critique sur ce qui leur semble évident par habitude professionnelle.

Le livre [12] reprend une série d'articles importants de Feferman concernant les fondements des mathématiques. Tout son livre tend à la conclusion que pour faire des mathématiques, la théorie des ensembles « ne sert à rien ». Elle sert évidemment à faire des théorèmes[13] ou à développer des intuitions fructueuses, mais, sur le fond, elle n'apporte aucun outil que ne nous apporterait pas la théorie des entiers naturels. Gödel pensait par exemple que des axiomes qu'on rajouterait à $\mathcal{ZF}$, affirmant l'existence de grands cardinaux, pourraient aider à décider des choses mystérieuses comme l'hypothèse du continu[14], ou à donner des bases plus solides à la théorie des entiers naturels. Feferman montre que tous les efforts dans ce sens (et ils ont été nombreux, car personne ne prend à la légère les intuitions de quelqu'un comme Kurt Gödel) ont abouti à des échecs. Le point de vue personnel de Feferman sembe être essentiellement un développement de la position défendue par Hermann Weyl dans *Das Kontinuum* [33]. En très bref :

---

[12] Convenables pour celui qui, à la suite de Gödel, croit à la validité intrinsèque de l'univers cantorien, mais extrêmement farfelus pour Poincaré, Weyl ou Brouwer : bien évidemment, on ne connaît aucun modèle raisonnable d'univers. Mais ce n'est surtout pas l'objet du livre de discuter cette question.

[13] Comme celui de Banach-Tarski, qu'on aurait préféré éviter !

[14] Pour qui croit à l'univers cantorien, cette question doit avoir une réponse objective. Pour un mathématicien constructif, il s'agit seulement d'une question sans signification réelle. La trancher dans un sens relèverait de l'arbitraire et ne saurait aider en quoi que ce soit à résoudre des questions pertinentes qui se osent par ailleurs.

Le seul fondement complètement assuré pour les mathématiques est donné par les entiers naturels, lesquels sont une base de départ incontournable, qu'on ne saurait fonder sur une base plus primitive. Par ailleurs, Hermann Weyl accepte la logique classique concernant les énoncés « simples » sur les entiers naturels. On peut interpréter cette position en disant que le système formel $\mathcal{PA}$ constitue la vraie base de travail des mathématiques. C'est aussi une reprise des arguments de Poincaré, de manière plus systématique et plus formelle. Concernant les nombres réels, ils sont introduits par leurs coupures de Dedekind, mais en se limitant à des définitions « non circulaires ». En fait dans Das Kontinuum, Hermann Weyl n'a accès de manière explicite qu'aux nombres réels dont la coupure de Dedekind est une partie arithmétique[15] de $\mathbb{Q}$. On ne considèrera pas comme légitime une définition faisant intervenir un quantificateur du type « pour tout nombre réel ... ». Une conséquence est la suivante : bien que *toute suite* majorée de nombres réels admette une borne supérieure (la lectrice peut ici se rappeler qu'il s'agit d'une variante de **LPO**), on ne peut affirmer pour autant que *tout ensemble* majoré de nombres réels admette une borne supérieure. Feferman a développé différents systèmes formels qui rendent compte soit des mathématiques constructives à la Bishop, soit des mathématiques dans le style de Hermann Weyl. Un achèvement remarquable de ce travail est la construction d'un système formel $\mathcal{W}$ dans lequel on peut écrire de manière (presque) naturelle toutes les mathématiques utiles pour la physique, en respectant les présupposés d'Hermann Weyl sur les fondements. En outre ce système formel est une extension conservative de $\mathcal{PA}$, c'est-à-dire ne démontre rien de plus que $\mathcal{PA}$ pour ce qui concerne les propriétés formulables dans $\mathcal{PA}$.

Tous les articles qui constituent ce livre sont remarquables. Je recommanderais particulièrement le chapitre II (articles 3 : *The logic of mathematical discovery versus the logical structure of mathematics*, sur Lakatos ; 4 : *Foundational ways* ; 5 : *Working foundations*) ; les deux articles *Infinity in mathematics, is Cantor necessary ?* (articles 2 et 12) ; l'article 9 : *What does logic have to tell us about mathematical proofs ?* ; l'article 11 : *Gödel's Dialectica interpretation and its two way stretch* ; et l'article 13 : *Weyl vindicated, Das Kontinuum seventy years later.*

# Références


[1] Aberth O. *Computable analysis.* McGraw-Hill (1980). 15

[2] Beeson M. *Foundations of Constructive Mathematics.* Springer-Verlag (1985). 15

[3] Beeson M. *Some theories conservative over intuitionistic arithmetic.* 1–15, dans : Logic and computation (Pittsburgh, PA, 1987), Contemporary Mathematics, No 106, Amer. Math. Soc., Providence, RI, (1990). 15

[4] Bishop E. *Foundations of Constructive Analysis.* McGraw Hill (1967). 14

[5] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag (1985). 15

[6] Bridges D., Richman F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987). 15

[7] Brouwer L. *Brouwer's Cambridge Lectures on Intuitionism.* (Van Dalen ed.) Cambridge University Press (1981).


[15] Une partie arithmétique de $\mathbb{Q}$ est une partie qui, via un codage naturel de $\mathbb{Q}$ dans $\mathbb{N}$ devient une partie définissable dans le langage de $\mathcal{PA}$.

[8] Cohen A., Cuypers H., Sterk H. (eds) *Some Tapas of Computer Algebra*, Springer Verlag (1999). 15

[9] Cox Q., Little J, O'Shea D. *Ideals, Varieties, and Algorithms*, (2nd edition) Springer Verlag UTM (1998). 15

[10] David R., Nour K., Raffali C. *Introduction à la logique*, Dunod (2001). 15

[11] Dowek G. *La logique*, Flammarion. Collection Dominos (1995). 15

[12] Feferman, S. *In the Light of Logic*. Oxford University Press, (1998). 7, 14, 16

[13] Friedman H. *Classically and intuitionistically provably recursive functions in Peano*, dans : Higher Set Theory. Lecture Notes in Mathematics n°669, 21–27, Springer (1978). 13

[14] Gödel, Nagel, Newman, Girard. *Le théorème de Gödel*. (1997). Le Seuil 16

[15] Goodstein R. *Recursive number theory*. Amsterdam, North-Holland, (1957). 11

[16] Goodstein R. *Recursive Analysis*. Amsterdam, North-Holland, (1961). 14

[17] Hilbert D. *Les problèmes de Hilbert*. Encyclopedia Universalis. Tome 11. 412–418. 2

[18] Hilbert D. *Über die Grundlagen der Logik und der Arithmetik*. dans Verhandlungen des dritten internationalen Mathematiker-Congresses in Heidelberg vom 8. bis 13. August 1904 (Teubner, Leipzig) 174–185. (Sur les fondements de la logique et de l'arithmétique) traduction anglaise dans [32] 129-138. 3

[19] Hilbert D. *Über das Unendliche*. Math. Annalen **95** (1926) 161–19O. (Sur l'infini) traduction anglaise dans [32] 367-392. 3, 11

[20] Knuth D. *Algorithmic thinking and mathematical thinking.* American Math. Monthly **92** n°3 (1985) 170–181. 14

[21] Kohlenbach U. *Things that can and things that cannot be done in PRA.* Annals of Pure and Applied Logic **102** (2000) 223–245. 11, 14

[22] Krivine J.-L. *Théorie des ensembles.* Cassini (1998). 15

[23] Lakatos I. *Preuves et réfutations*, Version française, Hermann (1984). 16

[24] Lalement R. *Logique, réduction, résolution*, Masson (1990). 16

[25] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 15

[26] Poincaré H. *Dernières pensées*, Flammarion (1913). 6

[27] Robinson A. *Formalism 64.* pp. 228–246 dans : Logic, Methodology and Philos. Sci. (Proc. 1964 Internat. Congr.) North-Holland, Amsterdam (1965) 16

[28] Seidenberg A. *Constructions in Algebra*. Trans. Amer. Math Soc. **197** (1974), 273–313. 15

[29] Seidenberg A. *What is Noetherian ?* Rend. Sem. Mat. e Fis. di Milano **44** (1974), 55–61. 15

[30] Tait W., *Finitism.* Journal of Philosophy **78** (1981) 524–546. 11

[31] Toraldo di Francia G. (ed.), *L'infinito nella scienza*, Istituto della Enciclopedia Italiana, Rome, (1987). 16

[32] van Heijenoort J. (ed.), *Frome Frege to Gödel : a source book in mathematical logic*, Harvard University Press, Cambridge, Massachussets (1967). 18

[33] Weyl H., *Das Kontinuum, Kritische Untersuchungen über die Grundlagen der Analysis.* Veit, Leipzig (1918). Traduction italienne *Il Continuo. Indagine critiche sui fondamenti dell' Analisi.* par A. B. Veit Riccioli, Bibliopolis, Naples (1977). Traduction anglaise *The Continuum. A critical examination of the foundations of Analysis.* par S. Polard et T. Bole. Thomas Jefferson Press, University Press of America (1987). 13, 16