

# **Herbrand et le programme de Hilbert**

Thierry Coquand

15 Février 2008

## Herbrand et le programme de Hilbert

Cet exposé sera, essentiellement, un commentaire de deux papiers d'Herbrand

“Non-contradiction des axiomes d'arithmétiques”

*C.R.A.S* 188, 303-304 (1929)

“Sur la non-contradiction de l'arithmétique”

*Journal für die reine und angewandte Mathematik* 166, 1-8 (1931)

## La signification des énoncés mathématiques?

En général si on a une preuve en mathématique de l'existence d'un nombre réel satisfaisant une propriété  $E(x)$  il peut arriver que l'on n'a *aucun* moyen à partir de cette preuve de construire un tel  $x$  qui vérifie  $E(x)$

Caractère “non effectif” des mathématiques

## La signification des énoncés mathématiques?

Ceci est à comparer avec : s'il y a une erreur dans un raisonnement on peut toujours la mettre en évidence

La "signification", le "contenu" d'un énoncé peut être non effectif, mais la vérification d'un raisonnement mathématique doit l'être

Donc grande différence entre la sémantique (qui n'est pas bien définie) et la syntaxe (qui doit être précise)

## Exemple

*Si  $f : [0, 1] \rightarrow [-1, 1]$  est continue et croissante et telle que  $f(0) = -1$ ,  $f(1) = 1$  alors il existe  $x$  tel que  $f(x) = 0$  et  $f(y) < 0$  si  $0 \leq y < x$*

Il suffit de prendre pour  $x$  la borne supérieure de l'ensemble

$$\{ y \in [0, 1] \mid f(y) < 0 \}$$

## Exemple

Considérons  $f : [0, 1] \rightarrow [-1, 1]$  linéaire par morceaux (et donc calculable) telle que  $f(0) = -1$ ,  $f(1) = 1$  et

$$f(1/3) = -\epsilon, f(2/3) = +\epsilon \text{ où } \epsilon \text{ est très près de } 0$$

(Par exemple :  $\epsilon = \sum_{n>0} \frac{\epsilon_n}{2^n}$  avec  $\epsilon_k = 0$  si  $2k$  est une somme de deux nombres premiers et  $\epsilon_k = 1$  dans le cas contraire. Ce qui est important est que  $\epsilon$  est calculable : on peut en calculer des approximations arbitrairement proches)

$x$  est proche de  $1/3$  ou proche de  $1/2$

On ne peut trouver  $x$  tel que  $f(x) = 0$  et  $f(y) < 0$  si  $y < x$  ou même une approximation de  $x$  à  $1/12$  près, à partir de la preuve d' "existence" d'un tel objet (conjecture de Goldbach)

## Exemple

En algèbre (théorème de la base finie) Hilbert utilisait le fait suivant : si on a une suite d'entiers  $n_1, n_2, \dots$  il existe  $k$  tel que  $n_k$  soit minimum (on a  $n_l \geq n_k$  pour tout  $l$ ).

Peut-on calculer un tel indice  $k$  ?

## Exemple

En théorie des nombres Dirichlet a une preuve en utilisant de l'analyse qu'il y a un nombre infini de nombres premiers de la forme  $an + b$ ,  $a, b$  premiers entre eux

Peut-on extraire de cette preuve *un* tel nombre premier (étant donné  $a$  et  $b$ ) ?

(Kronecker donnait une telle extraction dans ses cours)

## Exemple

XVIIème problème de Hilbert

*Un polynome  $P$  de  $\mathbb{Q}[X_1, \dots, X_n]$  qui ne prend que des valeurs  $\geq 0$  peut s'écrire comme somme de carré de fractions rationnelles*

Artin (et Schreier) présentait une solution de ce problème en utilisant l'"existence" d'un bon ordre sur un ensemble quelconque

Si on donne  $P$  peut-on l'écrire effectivement comme une somme de carrés à partir de la preuve ? (Question posée par Artin)

## Exemple

Théorème de Quillen-Suslin (problème de Serre): *une matrice idempotente de polynomes est semblable à une matrice de projection canonique.*

La preuve de Suslin utilise l'existence d'un idéal maximal

Si on a une matrice de polynomes explicitement donnée  $M$ , peut-on calculer effectivement  $P$  tel que  $PMP^{-1}$  soit une matrice de projection canonique ?

## La signification des énoncés mathématiques?

Ceci suggère les questions suivantes :

en général on ne peut extraire de manière effective un témoin à partir d'une preuve d'existence en mathématique. Y-a-t'il certains cas où on le peut ?

quelle est la signification intuitive concrète de l'énoncé  $\exists x.E(x)$ , qui doit être plus subtile que la seule existence de  $x$  ? (question qui a été analysée par Gentzen, 1936, pour les énoncés d'arithmétique)

## Critique de Brouwer

Brouwer prend au sérieux ces problèmes de signification des énoncés mathématiques et entreprend une reconstruction des mathématiques (en particulier de l'analyse) suivant des critères plus rigoureux

rejet du tiers-exclu (sur des ensembles infinis) comme un énoncé purement formel

En particulier, rejet de

$$\neg(\forall x.A) \rightarrow \exists x.\neg A$$

qui permet de montrer indirectement l'existence d'un élément

## Le programme de Hilbert

*Si nous restons dans le domaine des propositions finitistes, comme nous le devons d'ailleurs, les relations logiques qui y règnent manquent singulièrement de perspicuité, et ce défaut s'aggrave au point de devenir insupportable lorsque "tous" et "il existe" se combinent ... il est de fait que personne, même qui parlerait le dialecte des anges, n'empêchera les hommes de nier des assertions quelconques ... et d'appliquer le tiers exclu. Que faire ?*

Hilbert, *Sur l'infini*, Math. Annal. 95, 1926, p. 161-190

## Le programme de Hilbert

remplacer “sémantique” par “syntaxe” : le calcul logique, qui est bien défini, est considéré comme un jeu formel, sans contenu

preuve de *cohérence* de ce calcul formel, en n'utilisant que des raisonnements intuitionnistes

application aux énoncés universels : *si on a une preuve de cohérence* et si on montre  $\forall x.A$  avec  $A$  décidable avec des arguments transfinis, alors l'énoncé est vrai

En effet, un contre-exemple entraînerait une contradiction

“combattre” l'intuitionnisme avec ses propres armes

## Le programme de Hilbert

Ceci suggère les autres questions :

Qu'est que l'intuitionnisme ?

Que signifie "pouvoir trouver effectivement" un témoin d'un énoncé existentiel ?

Qu'est-ce qu'un algorithme ?

## Formalisation des mathématiques

Bonne présentation dans Weyl

*Consistency in Mathematics*, 1929 *Rice Institut Pamphlet* 16, p. 245-265

Calcul propositionnel : décidable (au moins en théorie) par la méthode des tables de vérité; *sémantique* et *syntaxe*

Calcul des prédicats, on ajoute les quantifications : en général on ne peut pas calculer la valeur de vérité d'un énoncé; seulement *syntaxe*

On pourra considérer que les énoncés sans quantificateurs correspondent aux énoncés "finitistes"

## Cohérence d'une théorie

$$S x \neq 0$$

$$S(x) = S(y) \rightarrow x = y$$

Pas de modèles finis

“Naivement” ces axiomes sont vérifiés pour  $\mathbb{N}$

Mais il y a un problème (a priori) avec la signification des quantificateurs: on ne peut pas calculer la valeur de vérité de  $\forall x.A$  ou  $\exists x.A$

## Cohérence d'une théorie

$$x = x$$

$$x = y \wedge y = z \rightarrow x = z$$

$$x = y \rightarrow y = x$$

$$x = y \rightarrow S(x) = S(y)$$

$$S x \neq 0$$

$$S(x) = S(y) \rightarrow x = y$$

## Esquisse de preuve

Hilbert (1904)

Les termes sont  $0, S(0), S(S(0)), \dots$

Les axiomes  $a = a$  sont des équations vraies

Les autres axiomes peuvent être vus comme des règles d'inférences qui permettent de déduire d'autres équations à partir d'équations

On voit directement que l'on ne pourra jamais déduire que des équations vraies

## Esquisse de preuve

Par ce moyen il semble que l'on puisse montrer la cohérence d'une théorie qui n'a pas de modèle fini, à partir de raisonnement purement syntaxique.

Le même doit être possible pour la théorie des nombres réels.

*De la même manière, nous pouvons montrer que les notions fondamentales de la théorie de Cantor, en particulier les alephs, ont une existence cohérente.*

Hilbert (Heidelberg, 1904)

Existence = cohérence

## Esquisse de preuve

Problème : on peut avoir des raisonnements indirects, en passant par des lemmes qui utilisent des énoncés quantifiés compliqués

Le sens de ces énoncés quantifiés n'est pas si clair a priori (cf. les exemples au début)

Il faut donner des règles précises de déduction

Ackermann (1924), von Neumann (1927)

## Première preuve de cohérence

Herbrand montre la cohérence d'une *extension* de cette théorie où l'on ajoute les axiomes d'induction

$$\phi(\vec{x}, 0) \wedge (\forall y. \phi(\vec{x}, y) \rightarrow \phi(\vec{x}, S(y))) \rightarrow \forall y. \phi(\vec{x}, y)$$

## Première preuve de cohérence

L'argument est d'une simplicité remarquable, comparée aux preuves d'Ackermann et von Neumann

Il fournit non seulement une preuve de cohérence mais aussi une *caractérisation complète* de la théorie (procédure de décision)

Pour cette théorie très simple, on peut calculer la valeur de vérité des énoncés quantifiés

## Première preuve de cohérence

L'argument consiste à “éliminer les quantificateurs” en associant à chaque formule  $\phi(\vec{x})$  une autre formule  $\phi'(\vec{x})$  *sans quantificateurs* telle que

$$\forall \vec{x}. \phi(\vec{x}) \leftrightarrow \phi'(\vec{x})$$

est prouvable à partir des axiomes donnés

*Nous allons faire sur ce terme les opérations qui, en algèbre ordinaire, correspondent à l'élimination de  $x$  dans un système d'égalités et d'inégalités.*

## Première preuve de cohérence

(discussion de la méthode utilisée)

*La méthode employée dans ce chapitre est susceptible d'autres applications ; elle fournit toujours, en même temps que la non-contradiction de la théorie étudiée, sa résolubilité ... Il nous paraît probable qu'elle permettrait également d'arriver à la non-contradiction de la théorie des corps réels et "réellement fermés"; mais les méthodes du Chapitre suivant nous y conduiraient plus aisément*

faisant allusion à la théorie récente d'Artin et Schreier

## Première preuve de cohérence

C'est le résultat de Tarski d'élimination des quantificateurs sur la théorie des corps réels clos

Pour une analyse récente

*Dynamical method in algebra: effective Nullstellensatze*

M. Coste, H. Lombardi et M.F. Roy, *Annals of Pure and Applied Logic*, 111, 203-256 (2001)

## Deuxième preuve de cohérence

Mais cette méthode ne peut pas marcher dès que l'on ajoute l'addition et la multiplication (car elle donnerait aussi un procédé de décision)

Pressburger : on ajoute seulement l'addition

La méthode d'élimination des quantificateurs joue un rôle important en démonstration automatique

## Deuxième preuve de cohérence

Extrêmement flexible : elle marche en ajoutant des symboles de fonctions avec des axiomes qui spécifient (de manière intuitionniste) ces fonctions

Par exemple :  $x + 0 = x$ ,  $x + S(y) = S(x + y)$

$x \times 0 = 0$ ,  $x \times S(y) = x + x \times y$

Remarque : si  $P(x)$  est sans quantificateur et  $t$  est un terme clos alors soit  $P(t)$  soit  $\neg P(t)$  est prouvable (intuitivement, les formules sans quantificateurs sont décidables)

Tous les termes clos sont égaux à des termes de la forme  $0, S(0), S(S(0)), \dots$

## Deuxième preuve de cohérence

Mais aussi, on peut ajouter des définitions de la forme

$$\phi(x) \rightarrow f(x) = 0, \quad (\neg\phi(x)) \rightarrow f(x) = S(0)$$

pour  $\phi(x)$  formule sans quantificateurs

## Deuxième preuve de cohérence

On *enlève* l'axiome d'induction : il devient dérivable à partir de telles fonctions, pour les formules d'induction *sans quantificateurs*

## Théorème fondamental

La méthode marche sans avoir à décider tous les énoncés

Elle repose sur le Théorème Fondamental de Herbrand (en fait un cas particulier; on suppose que l'on a au moins un symbole de constante)

*Une théorie purement universelle, c'est-à-dire n'ayant que des axiomes de la forme  $\forall \vec{x}.\phi(\vec{x})$  où  $\phi$  est sans quantificateurs est cohérente si, et seulement si, la théorie propositionnelle qui est formée par tous les substitutions closes  $\phi(\vec{t})$  est cohérente*

On réduit (en un certain sens) le calcul des prédicats au calcul propositionnel. Ceci joue un rôle essentiel en démonstration automatique

## Théorème fondamental

On voit que ce théorème est précisément ce qui manque à l'esquisse de la preuve de Hilbert 1904 pour être conclusive

Ce théorème ne fait intervenir *que des notions syntaxiques* : dérivation dans le calcul des prédicats et dérivation en calcul propositionnel

Il n'est pas du tout évident : on doit partir d'une dérivation en calcul avec quantificateurs et la transformer progressivement en une dérivation sans quantificateurs

La preuve qu'Herbrand en donne est *fausse* ! (Très bonne discussion accessible à la page web de Peter Andrews et bonne preuve dans le livre de Shoenfield)

## Théorème fondamental, exemple

$$\forall x y z. \quad x \leq y \wedge y \leq z \rightarrow x \leq z$$

$$\forall x. \quad x \leq x$$

$$\forall x y. \quad x \leq f(x, y)$$

$$\forall x y. \quad y \leq f(x, y)$$

$$\forall x y z. \quad \neg(a \leq x \wedge b \leq y \wedge c \leq z)$$

C'est une théorie contradictoire : si on a un majorant pour deux éléments on a un majorant pour trois éléments

## Théorème fondamental, exemple

La théorie formée par toutes les instantiations closes est contradictoire puisque elle a pour conséquence (purement dans le calcul propositionnel)

$$a \leq f(a, b)$$

$$b \leq f(a, b)$$

$$f(a, b) \leq f(f(a, b), c)$$

$$c \leq f(f(a, b), c)$$

$$a \leq f(f(a, b), c) \wedge b \leq f(f(a, b), c) \wedge c \leq f(f(a, b), c)$$

## Théorème fondamental, exemple

Pour un exemple simple où la taille de la preuve peut augmenter : on ajoute un symbole de prédicat  $N(x)$  et un symbole de fonction  $2^x$  et on note  $\underline{k}$  pour  $S^k(0)$ , et en ajoutant les axiomes

$$N(0), \quad \forall x. N(x) \rightarrow N(S(x))$$

$$2^0 = S(0), \quad 2^{S(x)} = 2^x + 2^x, \quad x + (y + z) = (x + y) + z$$

On a une preuve courte en calcul des prédicats de  $N(2^{\underline{7}})$  en utilisant le prédicat  $N'$  (quantifié !)

$$N'(x) \leftrightarrow (\forall y. N(y) \rightarrow N(y + 2^x))$$

et en montrant  $N'(0)$  et  $N'(x) \rightarrow N'(S(x))$

## Théorème fondamental, exemple

On montre alors  $N'(S(0)), N'(S^2(0)), \dots, N'(S^7(0))$  et  $N'(\underline{7})$  entraîne  $N(2^{\underline{7}})$

Toute preuve purement propositionnelle de  $N(2^{\underline{7}})$  est longue (au moins 128 étapes)

## Un corollaire remarquable

*Si on montre  $\exists x.\psi(x)$  dans l'arithmétique présentée par Herbrand et  $\psi(x)$  est sans quantificateur, alors on peut calculer  $t$  tel que  $\psi(t)$  est prouvable*

En effet, la théorie universelle en ajoutant l'axiome  $\forall x.\neg\psi(x)$  est contradictoire

Donc on a (explicitement) une contradiction dans la théorie propositionnelle où l'on a ajouté toutes les instantiations  $\neg\psi(0), \neg\psi(S(0)), \dots$

Cette contradiction explicite est un objet fini qui fournit un témoin  $t$

## Un corollaire remarquable

Ceci est utilisé par Church dans “A Note on the Entscheidungsproblem”,  
Journal of Symbolic Logic 1936, Vol. 1, p. 40-41

Voir aussi “Correction to *A Note on the Entscheidungsproblem*”, p. 101-102

Par exemple on peut former  $A = \exists a b c. S(a)^3 + S(b)^3 = S(c)^3$

Si  $A$  est prouvable alors on peut trouver  $p, q, r > 0$  tels que  $p^3 + q^3 = r^3$  en utilisant le corollaire du Théorème Fondamental

## Un corollaire remarquable

Cette preuve suggère le principe (heuristique) général suivant

*Si on montre de manière classique l'existence d'un objet "concret" (entier, ou qui peut se coder comme un entier) qui vérifie une propriété décidable alors on peut extraire de cette preuve un moyen de calculer cet objet*

Ceci n'est *pas* vérifié pour les énoncés  $\exists x.\forall y.\phi(x, y)$

Exemple :  $\exists x.\forall y.g(x) \leq g(y)$

## Qu'est-ce qu'un algorithme ?

Herbrand présente l'arithmétique comme un système "ouvert"

Il est *impossible* de donner un moyen uniforme de décrire toutes les fonctions calculables (par diagonalisation)

On n'écrit que des fonctions *totales*, et on doit avoir une preuve intuitioniste de totalité

Ces réflexions contribueront à la mise au point d'une définition générale de la notion d'algorithme (par Church, Kleene et Turing)

## Qu'est-ce qu'un algorithme ?

“Herbrand-Gödel” ? La définition est vraiment due à Gödel

Herbrand n'a pas vu (ou n'a pas insisté sur) le fait que le calcul des fonctions procèdent de manière uniforme indépendamment de la preuve de totalité

## Sur le problème de la décision

L'existence de pavages du plan non périodique vient de l'analyse des formules de la forme  $\forall x.\exists y.\forall z.\phi(x, y, z)$  par rapport au problème de la décision

Deux étapes :

- (1) Si tous les pavages sont périodiques alors le problème est décidable (H. Wang)
- (2) Le problème est indécidable (R. Berger)

## Le point de vue constructif

Ce point de vue a joué un rôle crucial

(1) dans la formulation du Théorème fondamental (l'énoncé usuel du théorème de complétude étant considéré comme *non rigoureux*)

(2) dans la formulation de l'arithmétique, avec l'observation cruciale que la notion de fonction (au sens intuitionniste) est une notion "ouverte" qui ne peut se décrire de manière exhaustive

Pour Herbrand ce point de vue devait se limiter aux "métamathématiques"

## Qu'est-ce que l'intuitionnisme?

*Dans sa forme extrême, cette théorie n'autorise que des raisonnements ne portant que sur les nombres entiers (ou des objets effectivement numérotés avec des nombres entiers) et satisfaisant aux conditions suivantes : toutes les fonctions introduites devront être effectivement calculables pour toutes les valeurs de leurs arguments, par des opérations décrites entièrement d'avance . . . chaque fois que l'on sera amené à dire : "il existe un entier ayant telle propriété  $x$ ", cela voudra dire implicitement : "nous avons donné dans ce qui précède un moyen de construire un tel  $x$ ".*

(Note non signée sur la thèse de Herbrand)

## Qu'est-ce que l'intuitionnisme?

Precisé par Heyting 1930 (aussi Kolmogorov 1925). Tout à fait surprenant que l'on puisse capturer les lois intuitionnistes par un système formel (plus surprenant pour Brouwer que le théorème d'incomplétude)

Logique classique = logique intuitionnisme + tiers exclu

Analyse remarquable par Gentzen "déduction naturelle" : la logique intuitionniste correspond à la signification "naturelle" des connecteurs logique. Cette analyse sera précisée par Prawitz (1965), Martin-Löf

## Qu'est-ce que l'intuitionnisme?

Analyse des règles logiques en règles d'*introduction* (qui donnent leur signification au connecteur) et règles d'*élimination* (qui sont justifiées par les règles d'introduction)

Par exemple : prouver  $A \rightarrow B$  c'est prouver  $B$  à partir de  $A$ , prouver  $A \wedge B$  c'est prouver  $A$  et prouver  $B$

On peut alors justifier que  $B$  soit une conséquence de  $A \rightarrow B$  et de  $A$

Le tiers exclu, sous la forme  $A \vee \neg A$  ou  $(\neg\neg A) \rightarrow A$  n'a aucune telle justification (Kolmogorov, 1932)

## Qu'est-ce que l'intuitionnisme?

$\Gamma \vdash A$  si  $A$  est dans  $\Gamma$  (hypothèse)

$\Gamma \vdash A \rightarrow B$  si  $\Gamma, A \vdash B$  (introduction)

$\Gamma \vdash B$  si  $\Gamma \vdash A \rightarrow B$  et  $\Gamma \vdash A$  (élimination)

$\Gamma \vdash A \wedge B$  si  $\Gamma \vdash A$  et  $\Gamma \vdash B$  (introduction)

$\Gamma \vdash A$  et  $\Gamma \vdash B$  si  $\Gamma \vdash A \wedge B$  (élimination)

## Réduction négative

Découverte à peu près simultanée de Gödel, Gentzen, Bernays 1932 (anticipée par Kolmogorov 1925)

Réduction simple de l'arithmétique classique à l'arithmétique intuitionniste !

On explique  $\exists x.A$  par  $\neg(\forall x.\neg A)$  et  $A \vee B$  par  $\neg(\neg A \wedge \neg B)$

(Quand un mathématicien dit qu'il a montré  $\exists x.A$  c'est très souvent qu'il a déduit une contradiction à partir de l'hypothèse qu'il n'y a pas de tel  $x$ .)

## Réduction négative

Preuve surprenante de simplicité de non contradiction de l'arithmétique classique (par rapport aux mathématiques intuitionnistes)

Cet argument était esquissé dans certains écrits de Brouwer (1908)

## Preuve de cohérence

Extension à l'Analyse ? Axiome du choix dénombrable

$$(\forall x. \exists y. A(x, y)) \rightarrow \exists f. \forall x. A(x, f(x))$$

Quantification sur les *fonctions*

Grande différence entre la version intuitionniste et la version avec tiers-exclu

## Preuve de cohérence

Axiome du choix dénombrable

Spector (1961)

Berardi-Bezem-Coquand (1994)

Krivine (2003)

Plus récemment Krivine a annoncé une solution pour ZF + axiome du choix général (2005)

## Preuve de cohérence

Mais le calcul des prédicats seul réserve encore des surprises

*Formules valides, jeux et protocoles réseaux*

Jean-Louis Krivine et Yves Legrandgérard (2007)

Par exemple : signification de

$$\exists x. \forall y. (P(x) \rightarrow P(y))$$

(principe de choix pour un prédicat  $P$ )

## Mathématiques constructives

F. Richman

Ce sont les mathématiques développées en logique intuitionniste (donc sans utiliser le tiers-exclu)

Définition qui ne fait pas intervenir explicitement la notion d'algorithme !