HAL
open science

Five Conferences on Undecidability

Nicolas Bouleau, Jean-Yves Girard, Alain Louveau

To cite this version:

Nicolas Bouleau, Jean-Yves Girard, Alain Louveau. Five Conferences on Undecidability. N. Bouleau. Presses de l'Ecole Nationale des Ponts et Chaussées, pp.57, 1983. hal-00192557

HAL Id: hal-00192557

https://hal.science/hal-00192557v1

Submitted on 28 Nov 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

cinq conférences sur l'indécidabilité

organisées en 1982 à l'Ecole Nationale des Ponts et Chaussées
dans le cadre du programme
Sciences, Techniques et Société

Nicolas Bouleau, JeanYves Girard, Alain Louveau

hal-00192557, version 1 - 28 Nov 2007

Sommaire

	Pages
Introduction	3
La formalisation des mathématiques, Nicolas Bouleau	6
Sur le théorème d'incomplétude de Gödel	
- jusqu'à Gödel	15
- après Gödel, Jean-Yves Girard	24
Indécidabilité de l'hypothèse du continu, Alain Louveau	35
Sur la calculabilité effective, exemples, Nicolas Bouleau	43
Bibliographie	55

Introduction

Entre les scientifiques purs, chercheurs et universitaires, et l'habitant de nos cités dans sa vie quotidienne, existe une catégorie de personnes qui utilisent la science sous diverses formes et la relient à la vie sociale. Appelons ceux-ci les ingénieurs, ce sont eux qui font que les trains circulent, que les ponts tiennent, que les avions sont guidés. Un tel ingénieur possède un savoir efficace, une théorie pertinente qui permet de déboucher effectivement sur les actions à entreprendre : conception, dimensionnement, vérification. Que cette théorie ne soit qu'une approximation, l'ingénieur le sait, il n'a pas pris en compte la structure fine de la matière et ses contrôles ne sont que statistiques, mais il maîtrise les ordres de grandeurs et néglige ce qui est négligeable.

Y aurait-il des questions indécidables ? Notre ingénieur aura tendance à considérer que ce sont là des élucubrations purement spéculatives sans incidences sur la vie réelle qu'il connaît et qui est bien décrite par les méthodes qu'il utilise.

Il n'a raison qu'à demi. Dès qu'on pense aux enjeux, à l'intérêt général et à celui de chacun, plusieurs lectures de la réalité apparaissent. Ces conférences sur l'indécidabilité, peuvent le concerner par analogie entre sa situation et celle des mathématiciens.

En effet, le plus souvent, le mathématicien reste installé dans son cadre conceptuel habituel qui est aujourdhui celui de la théorie des ensembles et ne voit pas l'intérêt d'en sortir. Jean Dieudonné écrit à propos des logiciens "Nous, les mathématiciens, comment voyons-nous leur travail ? Eh bien, d'une part, ils explorent les possibilités de notre système logique celui avec lequel nous travaillons, Zermelo-Fraenkel, d'un autre côté - et cela nous intéresse beaucoup moins - ils élaborent et explorent des quantités d'autres systèmes logiques. Alors, quand on vient nous parler de la logique du premier et du deuxième ordre, de fonctions récursives et de modèles, théories très gentilles et très belles qui ont obtenu des résultats remarquables, nous, mathématiciens, nous ne voyons aucune objection

à ce qu'on s'en occupe, mais cela nous laisse entièrement froids"[1]. Cette attitude sereine semble être une position pertinente. Cependant, lorsqu'un mathématicien a rencontré dans la poursuite naturelle de ses recherches un problème difficile, et que ce problème après des tentatives infructueuses de démonstration et de réfutation s'avère indécidable, alors il est convaincu qu'on ne peut laisser la logique de côté avec ses fonctions récursives et ses modèles, il change de camp, s'intéresse à des systèmes syntaxiques ou sémantiques différents (comme celui de l'analyse non standard qui trouve maintenant des applications en mécanique, en physique et en calcul stochastique) comme à autant d'outils possibles.

De même l'ingénieur ne peut me semble-t-il aujourdhui, ne pas se préoccuper du contexte de son activité, des approches différentes, du caractère relatif de sa modélisation favorite.

Quelques mots, en outre, doivent être dits sur l'intérêt intrinsèque du sujet. Ce que dit A.Shenitzer à propos des étudiants en mathématiques "Speaking of the deductive method, it is a sad reflexion on the intellectual level of mathematical education that, unless he takes courses in logic, the mathematics student may get his degree without having heard about Gödel or about his monumental discovery of the intrinsic limitations of deductive method, a discovery widely regarded as one of the greatest intellectual accomplishements of the 20th century"[2] s'applique aussi bien à l'élève-ingénieur. C'est tout le problème de la vulgarisation qui se pose alors. La logique mathématique est un domaine très ésotérique. Que font les logiciens ? Je peux apporter un modeste témoignage, je suis allé me promener par là-bas et je puis dire qu'ils font des choses difficiles mais passionnantes, certainement pas anodines, des questions centrales sont abordées, les méthodes et les concepts sont forts et éclairants, à tel point qu'une certaine philosophie de la représentation paraît bien vaine à côté. C'est d'ailleurs ce qui explique que les logiciens répugnent à vulgariser leurs travaux. Même si leur démarche est très abstraite, ils ont le sentiment de tenir en main du réel bien plus que certains verbiages philosophiques et que les enjeux

[1] *Penser les mathmatiques*, Seuil 1982.

[2] "Teaching mathematics" in *Mathematics tomorrow* L.A. Steen , editor Springer 1981.

des difficultés qu'ils surmontent apparaîtront un jour ou l'autre.

La question de la vulgarisation se pose avec d'autant plus de force. Je pense que les lecteurs trouveront de l'intérêt à lire dans les exposés de Jean-Yves GIRARD et Alain LOUVEAU une sorte de philosophie vivante des mathématiques qui est simplement la vision fraîche de chercheurs de haut niveau dans leur propre champ.

Nicolas Bouleau

La formalisation des mathématiques

Nicolas Bouleau

Cette séance a pour but de vous présenter quelques notions introductives vous permettant de suivre plus aisément les prochaines conférences.

Au cours de cet exposé je n'ai pas l'intention de faire des mathématiques, je ne ferai aucune démonstration, mais simplement de parler sur les mathématiques. Or, il y a beaucoup de façons d'envisager les mathématiques, en raison des différentes écoles de la philosophie des sciences, et également des sous-variétés propres à la philosophie des mathématiques (logicisme, formalisme, intuitionnisme, platonisme, etc...). Dès lors il est bon que je vous prévienne que ce que je vais dire a plutôt tendance à orienter les choses vers le point de vue formaliste. Gardez seulement à l'esprit que ce point de vue est loin de mettre un point final à la question *Que sont les mathématiques?*

I. Les mathématiques naturelles

Dans l'antiquité et jusque vers la fin du 18e siècle, les mathématiques étaient considérées comme l'expression des lois de la nature. La chose était d'ailleurs si évidente que les auteurs n'abordent pas cette question en elle-même mais plutôt (comme Aristote ou Galilée) la question de savoir si tous les phénomènes naturels relèvent des mathématiques ou une partie seulement. Le sens des symboles mathématiques était unique et clair. Pascal écrira vers 1660 [qu'on ne puisse tout définir et tout prouver] "c'est ce que la géométrie enseigne parfaitement. Elle ne définit aucune de ces choses espace, temps, mouvement, nombre, égalité, ni les semblables qui sont en grand nombre, parce que ces termes-là désignent si naturellement les choses qu'ils signifient, à ceux qui entendent la langue, que l'éclaircissement qu'on voudrait faire apporterait plus d'obscurité que d'instruction. Car il n'y a rien de plus faible que le discours de ceux qui veulent définir ces mots primitifs". Ainsi, si Pascal considère qu'il est mauvais de chercher à définir les notions primitives des mathématiques, c'est simplement parce qu'il estime que ces notions sont claires. Il n'envisage pas que le sens de ces notions primitives puisse n'avoir que peu d'importance pour les mathématiques elles-mêmes. Le premier penseur qui s'est rendu compte que le fait que les mathématiques nous apprenaient quelque chose sur la nature

faisait problème si on le rapprochait du caractère rigoureux du raisonnement mathématique, est incontestablement Kant. La solution qu'il propose pour résoudre cette difficulté à savoir l'introduction de la célèbre catégorie des *jugements synthétiques a priori*, nous apparaît aujourd'hui un peu comme une clause *ad hoc*, mais c'est qu'il était impossible d'imaginer à cette époque une mathématique qui ne soit pas naturelle. Depuis l'antiquité la géométrie était la branche maîtresse des mathématiques et c'est précisément dans le domaine de la géométrie que vont naître de nouvelles idées qui vont se développer tout au long du 19e siècle et aboutir à une modification radicale de la conception des mathématiques. C'est seulement à partir du 19e siècle, que l'on trouve, en réaction à ces nouvelles idées, des mathématiciens partisans des mathématiques naturelles. Si Hermite écrit vers 1870 "Je crois que les nombres et les fonctions de l'Analyse ne sont pas le produit arbitraire de notre esprit, je pense qu'ils existent en dehors de nous avec le même caractère de nécessité que les choses de la réalité objective, et nous les rencontrons et les étudions comme les physiciens, les chimistes et les zoologistes", c'est que ceci n'est plus complètement évident. Que s'est-il produit ? L'apparition des géométries non-euclidiennes.

II. Naissance du formalisme

Dans les Eléments d'Euclide (3e siècle avant J.C.) l'axiome des parallèles est ainsi formulé "Si une ligne droite qui en rencontre deux autres forme d'un même côté avec les droites des angles internes dont la somme est moindre que deux droits, les deux premières droites se rencontrent ou leurs prolongements du côté où la somme est inférieure à deux droits". Après de nombreuses tentatives souvent ingénieuses durant des siècles pour démontrer ce postulat à partir des autres axiomes, au début du 19e siècle quelques mathématiciens (Bolyai, Gauss, Lobachevski) en étaient arrivés à la conviction que les autres axiomes ne tranchaient pas entre cette hypothèse et son contraire et certains d'entre eux affirmaient même qu'on pouvait à partir d'autres postulats et développer tout un ensemble de conséquences "Une étrange géométrie, tout à fait différente de la nôtre, entièrement cohérente en elle-même" dira Gauss vers 1820-1830. Les géométries non-euclidiennes étaient nées, on ne pouvait plus considérer la géométrie classique que comme une parmi d'autres possibles et Riemann montrera en 1854 que certaines de ces différentes

géométries planes peuvent se représenter dans l'espace comme la géométrie des géodésiques d'une surface, de courbure totale positive ou négative, démontrant ainsi par un raisonnement de théorie des modèles avant la lettre, que ces nouvelles géométries sont aussi fiables que l'ancienne.

Le développement de la géométrie va s'intensifier dans le courant du 19e siècle (Cayley, Plücker, Klein et le programme d'Erlangen, Pash, etc...). Progressivement émerge l'idée que la validité des raisonnements ne tient pas à la clarté du sens des notions primitives mais aux relations algébriques qu'elles entretiennent les unes avec les autres. Cayley écrira en 1859 "1) Le mot point peut signifier point et le mot droite peut signifier droite, 2) le mot point peut signifier droite et le mot droite signifier point. Nous pouvons par une telle extension comprendre les théorèmes corrélatifs sous un énoncé commun. Nous allons dans la géométrie à deux dimensions inclure la géométrie sphérique, les mots plan, point et droite signifiant à cette fin surface sphérique, arc (d'un grand cercle) et point (c'est-à-dire paire de points opposés) de cette surface sphérique". On traitait dans cet esprit d'un même coup un théorème sur les coniques et le théorème dual obtenu par transformation par polaires réciproques.

Pash écrira très clairement en 1882 dans ses leçons sur la géométrie nouvelle "Il faut en effet, pour que la géométrie devienne une science déductive, que la manière dont on tire les conséquences soit partout indépendante du sens des concepts géométriques, comme elle doit l'être des figures, seuls sont à prendre en considération les rapports entre les concepts géométriques posés par les propositions et les définitions employées". Cantor pourra dire en 1883 "La mathématique est entièrement libre dans son développement et ses concepts ne sont liés que par la nécessité d'être non contradictoires et coordonnés aux concepts antérieurement introduits par des définitions précises".

Les choses vont assez rapidement à partir de 1880, une floraison de géométries apparaît et un point culminant est atteint par Hilbert en 1899 dans ses *Fondements de la géométrie* où il étudiera quasiment toutes les géométries possibles et montrera l'indépendance des divers axiomes par le moyen d'interprétations. La rigueur de ce travail et la puissance de sa généralité (géométries non archimédiennes, non arguesiennes, etc.) a fortement impressionné les contemporains, il apparaissait difficile d'aller

plus loin.

Mais déjà la méthode axiomatique envahissait d'autres branches des mathématiques. En 1889, Peano donnait une version de ses célèbres neuf axiomes de l'arithmétique. Quelques années auparavant G. Frege proposait dans son *Begriffschrift* (1879) le premier langage complètement formalisé (dans lequel sont introduits pour la première fois les quantificateurs existentiels et universels) et s'en servait dans ses *Grundsetze der Arithmetik* (1883) pour fonder l'arithmétique sur la logique pure. Après quelques soubresauts dus à la découverte par Russell en 1901 d'une contradiction (l'antinomie de Russell) dans un système d'une aussi grande généralité que celui de Frege, Russell et Whitehead proposaient en 1910 dans leurs *Principia mathematica* un système formel qui se mettait à l'abri des paradoxes par l'élimination des définitions non prédicatives.

Alors qu'au 19e siècle les mathématiques se présentaient comme plusieurs domaines indépendants géométrie, algèbre, théorie des fonctions dont le nombre s'était accru récemment par l'apparition des géométries non-euclidiennes, de la géométrie projective et de la théorie des groupes, après la publication des Principia Mathematica l'ensemble des théories mathématiques connues, depuis la géométrie jusqu'aux nombres transfinis de Cantor, est complètement unifiée en une seule théorie, dont une forme plus commode utilisée aujourd'hui est l'axiomatique de la théorie des ensembles de Zermelo-Fraenkel (ZF).

III. Le formalisme de la théorie des Ensembles

Je vais maintenant préciser un peu le formalisme de la théorie des ensembles, afin de tenter de vous convaincre en quelques minutes de deux choses pour lesquelles on estime généralement qu'elles ne peuvent vraiment s'acquérir qu'en au moins un an de pratique personnelle. La première que j'exposerai sommairement est que le langage de la théorie des ensembles est purement formel, on peut même dire matériel assemblages formés de signes parfaitement codifiés. La seconde, que je ne ferai qu'évoquer, est que toute pensée mathématique du moins la quasi-totalité peut s'exprimer dans ce langage.

La théorie des ensembles de Zermelo-Fraenkel s'exprime dans le langage de la logique des prédicats du 1er ordre en posant un certain nombre d'axiomes spécifiques. La logique des prédicats du 1er ordre est une théorie logique dans laquelle les quantificateurs $\forall\ \exists$ ne peuvent porter que sur des variables

d'individus et non des variables de prédicats (c'est-à-dire de propriétés).

Langage du 1er ordre

a) Symboles de variables $x, y, z, x', y', z', x'', y'', z'' \ldots$

b) Symboles de fonctions

- fonctions 0-aires ou constantes,
- fonctions unaires $f(\,), g(\,) \ldots$,
- fonctions binaires $h(\,,\,) \ldots$,
- fonctions n-aires $h(\,, \ldots, \,) \ldots$,

c) Symboles de prédicats

- prédicats unaires $P(\,)$, $Q(\,) \ldots$,
- prédicats n-aires $R(\,, \ldots, \,) \ldots$,

d) Les symboles $\neg$ (non), $\vee$ (ou), $\exists$ (il existe).

e) Un prédicat binaire particulier noté $=$.

On définit alors les assemblages de signes qu'on appellera termes et ceux qu'on appellera formules.

Termes

i) une variable est un terme,

ii) si $u_1, \ldots, u_n$, sont des termes et si f est une fonction n-aire alors $f(u_1, \ldots, u_n)$ est un terme,

Formules

a) une formule atomique est un assemblage de la forme $P(a_1, \ldots, a_n)$ où les a_i sont des termes et P un prédicat n-aire.

b) i) une formule atomique est une formule

ii) si φ est une formule, $\neg\varphi$ est une formule

iii) si φ et ψ sont des formules, $\varphi \vee \psi$ est une formule,

iv) si φ est une formule, $\exists x \varphi$ est une formule et de même en remplaçant x par une autre variable.

Abréviations on note $A \Rightarrow B$ pour $\neg A \vee B$, $A \& B$ pour $\neg(A \Rightarrow \neg B)$, et enfin $\forall x A$ pour $\neg \exists x \neg A$.

Logique des prédicats du 1er ordre

On appelle ainsi une théorie formalisée utilisant le langage du 1er ordre plus un certain nombre d'axiomes et de règles d'inférence, permettant de construire des formules à partir des axiomes, formules qu'on appellera

des théorèmes.

Axiomes

Les formules suivantes sont des axiomes

1) toute formule de la forme $A \vee \neg A$ où A est une formule.

2) Si $A(x)$ est une formule ayant x comme variable libre (non dans le champ d'un quantificateur) et si a est un terme

$$A(a) \Rightarrow \exists x A(x)$$

est un axiome.

3) Si x est une variable $x = x$ est un axiome,

4) Si $x_1, \ldots, x_n, y_1, \ldots, y_n$ sont des variables et f une fonction n-aire

$$(x_1 = y_1)\&(x_2 = y_2)\& \cdots \&(x_n = y_n) \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$

est un axiome.

5) et de même si P est un prédicat n-aire

$$(x_1 = y_1)\&(x_2 = y_2)\& \cdots \&(x_n = y_n) \Rightarrow (P(x_1, \ldots, x_n) \Rightarrow P(y_1, \ldots, y_n))$$

est un axiome.

Règles d'inférence

1) de A on déduit $B \vee A$

2) de $A \vee A$ on déduit A

3) de $(A \vee B) \vee C$ on déduit $A \vee (B \vee C)$

4) de $A \vee B$ et de $\neg A \vee C$ on déduit $B \vee C$

5) Si x n'est pas une variable libre de B,
de $A \Rightarrow B$ on déduit $(\exists x A) \Rightarrow B$.

Théorie des Ensembles

Cette théorie utilise un langage du 1er ordre sans symbole de fonction.

Un seul prédicat binaire (en plus de =) noté $\in$ et un certain nombre d'axiomes pour le détail desquels je renvoie à Krivine [10].

1) Extensionalité :

$$\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow x = y$$

2) Régularité (ou fondation)

$$\exists y(y \in x) \Rightarrow \exists y(y \in x \ \& \ \neg\exists z(z \in x \& z \in y))$$

3) Axiomes de partie : quelque soit la formule A

$$\exists z \forall x(x \in z \Leftrightarrow x \in y \ \& A)$$

est un axiome dès que les variables x, y, z sont distinctes et n'interviennent pas dans A.

4) Le schéma de remplacement.
5) L'axiome de l'ensemble des parties.
6) L'axiome de l'infini.
7) (éventuellement) L'axiome du choix.

Pour ce qui est de voir comment on peut introduire à partir de cela toutes les mathématiques, nombres entiers, réels, espaces topologiques, etc... je vous renvoie au cours d'analyse de C. WAGSCHAL, en attirant seulement votre attention sur le fait que ce cours est rédigé dans le cadre de l'axiomatique de Zermelo qui est plus faible que ZF (le schéma de remplacement y est remplacé par l'axiome de compréhension), mais déjà suffisante pour faire la majeure partie de l'analyse.

IV. Formalisation et indécidabilité

Ainsi nous sommes dans la situation suivante, l'ensemble des mathématiques se présente sous la forme d'un système formel où chaque théorème n'est qu'une conséquence purement logique et étrangère à toute intuition sensible de certains axiomes. La vérité de tel énoncé n'étant que relative à ce système d'axiome, les mathématiques d'un côté se sont unifiées, de l'autre ont perdu tout caractère absolu les théories ne contiennent que ce qu'on a mis dedans. Si c'était la seule conclusion à laquelle avait mené la formalisation des mathématiques cela ne serait pas bien intéressant. Mais ceci a conduit les mathématiciens à considérer et à tenter d'étudier ces sortes de jeux que sont les systèmes formels eux-mêmes, et ont découvert des phénomènes curieux auxquels en vérité ils ne s'attendaient pas. Ce sera l'objet principal de tout ce cycle de conférences. Sans trop déflorer

les sujets des autres conférenciers, je dirai simplement ceci

A. Syntaxe

A partir du moment où toutes les mathématiques avaient été ramenées à des enchaînements de signes, il ne devait pas être bien sorcier de voir si ces enchaînements, indépendamment de toute signification attribuée aux symboles, peuvent mener a une contradiction, c'est-à-dire à $A\&\neg A$ ou non. C'est du moins ce qu'a cru Hilbert pendant un temps. Cependant certains systèmes formels en particulier ceux obtenus a partir de la formalisation des mathématiques, quoique formés d'enchaînements codifiés de suites de signes qu'on pourrait si l'on veut réaliser matériellement en bois par exemple ou faire manipuler par un ordinateur, sont d'une telle richesse combinatoire, que sur certaines de leurs propriétés plane un doute d'une nature particulière. La thèse suivante sera précisée et commentée par les prochaines conférences "Il y a des systèmes combinatoires parfaitement déterminés (le hasard en est complètement étranger) dont certaines propriétés (comme de savoir s'ils sont contradictoires ou non) sont à jamais en dehors du champ de la connaissance certaine en tout cas telle qu'elle était entendue au 19e siècle." Cet aspect syntaxique sera illustré et développé dans les conférences de J.Y. GIRARD.

B. Sémantique

La théorie des ensembles de Zermelo-Fraenkel est un système formel particulier qui a l'avantage de constituer un cadre conceptuel très large dans lequel les problèmes de signification et de modèles des systèmes formels peuvent être abordés. Un modèle d'une théorie formelle doit être compris comme "une réalité" dont la théorie serait la formalisation, c'est-à-dire comme un univers d'objets et de relations satisfaisant aux lois édictées par les théorèmes de cette théorie. Un des résultats fondamentaux de la théorie des modèles est que les systèmes formels ont le plus souvent plusieurs modèles on dit qu'ils sont non catégoriques.

Nous utilisons ces systèmes en attribuant un sens (le sens usuel) aux symboles, mais en fait d'autres significations sont possibles, d'autres objets que ceux dont on a voulu formaliser les propriétés satisfont les énoncés. Par exemple quoique l'on puisse faire toute la théorie classique

des nombres réels dans Zermelo-Fraenkel, à partir de tout modèle de Zermelo-Fraenkel on peut construire un modèle dénombrable dans lequel évidemment la relation d'appartenance et la propriété d'être dénombrable n'ont pas le sens habituel.

De même il existe des modèles de l'arithmétique de Peano dans lesquels il y a des entiers infinis, et ces modèles non-standards trouvent des applications intéressantes. La théorie des modèles a développé des concepts et des méthodes par lesquels nos connaissances de la notion de symbole s'est trouvée grandement affinée par rapport à la réflexion spéculative de l'approche intuitive.

On peut dire si l'on veut que le mathématicien traditionnel se préoccupe de savoir s'il n'a pas désigné le même objet par deux symboles différents (c'est ce qu'il fait lorsqu'il pose ou résout une équation) alors que le logicien se pose la question de savoir si d'aventure un même symbole ne désignerait pas plusieurs choses différentes.

Cet aspect sémantique sera illustré particulièrement par l'exposé de A. LOUVEAU sur l'hypothèse du continu.

Le théorème d'incomplétude de Gödel

Jean-Yves Girard

Le formalisme, c'est-à-dire la position philosophique sur les mathématiques dont le représentant le plus éminent fut Hilbert, constitue le sujet essentiel de cet exposé. Plus précisément, nous allons exposer en détail l'idéologie formaliste, dont la quintessence est le "programme de Hilbert" (en évoquant en contrepoint, une idéologie concurrente, l'intuitionnisme). Le programme de Hilbert avait ceci de particulier qu'il s'agissait d'un programme mathématique très précis, tendant à démontrer la justesse de l'ontologie formaliste (et non pas une vague succession d'intentions) c'était sûrement assez présomptueux de la part de Hilbert que de vouloir trancher une question philosophique par le biais des mathématiques, mais sans doute moins ridicule que l'inverse, à savoir décider une question scientifique au moyen de considérations "philosophiques" générales. En tout cas, on s'expose à la possibilité de réfutation, car il est bien connu que les conjectures mathématiques peuvent être démontrées (c'est ce qu'espérait Hilbert pour son programme) ou réfutées c'est ce qu'il advint. En 1931, par son théorème d'incomplétude, Gödel réfutait clairement le programme de Hilbert. Cet exposé s'arrêtera donc avec le théorème d'incomplétude. La semaine prochaine, nous nous préoccuperons de ce qu'il advint après car si le théorème d'incomplétude a montré la fausseté des vues hilbertiennes sur les mathématiques, il ne nous a pas proposé grand-chose à la place, il y a eu des travaux dans la lignée de Hilbert, et dont l'évaluation exacte reste délicate, je pense en particulier aux travaux de Gentzen.

1. La philosophie formaliste

Les succès de la formalisation (voir l'exposé précédent) ont conduit à la position philosophique suivante, qui fut celle de Hilbert, mais qui a toujours de nombreux défenseurs (notamment en France, voir les *Eléments de Mathématique* de Bourbaki) Les mathématiques doivent être analysées comme une activité dépourvue de signification, comme, disons, le jeu d'échecs. Il s'agit, au moyen de règles formelles fixées à l'avance, de construire certains assemblages de symboles (les énoncés mathématiques et leurs démonstrations).

Faut-il en conclure que le formalisme sous-entend une attitude ontologique (l'ontologie est la partie de la philosophie qui traite de l'existence) cohérente ? il n'en est rien, et nous pouvons facilement distinguer entre plusieurs positions formalistes

1 - D'abord des gens pour qui rien n'existe. Cette position me semble difficilement conciliable avec l'idée d'analyser les mathématiques comme un jeu formel, il semble en effet implicite dans cette idée que les symboles formels existent vraiment on est donc amené à reconnaître une certaine existence aux assemblages de symboles ainsi obtenus, et une certaine signification aux propriétés combinatoires (cohérence, etc...) de ces assemblages.

2 - A l'opposé se situe le monsieur qui dit au fond, toutes ces questions d'existence me passent au-dessus de la tête, je ne veux pas savoir si les objets mathématiques existent ou non en tout cas, ce qui est sûr, c'est le côté purement formel mentionné plus haut. Il ne s'agit pas vraiment d'une prise de position, mais plutôt d'une fuite...

3 - La position de Hilbert, elle, est nettement plus intéressante

Les seuls objets qui existent pour Hilbert, ce sont des objets finitistes (ou encore élémentaires) il s'agit là des êtres réels dont parlent les mathématiques. Quels sont-ils au juste ? Essentiellement les entiers, mais aussi les assemblages formels (qui peuvent être représentés par des entiers).

Parmi les propriétés mathématiques, il en est qui n'ont pas de sens (comme par exemple des propriétés qui feraient référence à des objets non finitistes), et d'autres qui ont une signification (et que l'on appellera encore "réelles", "élémentaires", "finitistes"). Ces énoncés pleins de sens, Hilbert propose de les identifier aux propriétés qui ont lieu pour toute valeur des variables.

Exemples

$$\forall x(x^2 + 2x + 1 = (x + 1)^2)$$

$$\forall x \forall y \forall z \forall n(xyz \neq 0 \ \& \ n > 2 \Longrightarrow x^n + y^n \neq z^n)$$

la conjecture de Riemann (dans ce cas, elle n'est pas directement élémentaire, mais on peut la ramener à une identité, d'ailleurs sans intérêt apparent). Parmi ces énoncés, il y a les formules de cohérence Coh(ZF) exprime que la théorie ZF (Zermelo-Fraenkel) est cohérente, c'est-à-dire

$$\forall \pi \ (\pi \text{ démonstration dans ZF} \Rightarrow \pi \text{ ne se termine pas par } 0 = 1)$$

enfin, ce ne sont pas toutes les démonstrations mathématiques (y compris quand elles ne font intervenir que des énoncés et des objets élémentaires) qui seront irréprochables, il faut que les principes utilisés dans les démonstrations soient particulièrement immédiats, on parlera alors de démonstration élémentaire (ou finitiste).

Les mathématiques (et spécialement celles du XXe siècle) sont loin de se réduire à ce noyau délimité par Hilbert, nous avons des objets abstraits (ou idéaux) (pensons aux ultrafiltres, aux espaces de... Hilbert). Pour Hilbert, ils n'existent pas, de même les propriétés abstraites (ou idéales) n'ont pas de sens, par exemple, la négation d'une identité n'a pas, pour Hilbert, de signification, de même quant aux principes abstraits qui se retrouvent dans de nombreuses démonstrations, par exemple, l'axiome du choix. Cette distinction entre "réel" et "abstrait" va nous conduire au programme de Hilbert.

2. Le programme de Hilbert

L'idée de Hilbert est de montrer qu'il est possible, en théorie du moins, de se passer des objets abstraits, des énoncés abstraits. Voilà donc le programme qu'il se proposait de réaliser.

Soit R une propriété élémentaire, établie à l'aide de méthodes abstraites, montrer que R peut être établie à l'aide de méthodes élémentaires.

Ce programme, d'énoncé simple, appelle un certain nombre de remarques

- D'abord, il se place dans une certaine tradition, rappelons-nous le théorème des nombres premiers (Hadamard, de la Vallée-Poussin), démontré au moyen de la théorie des fonctions analytiques, mais qui a été élémentarisé au XXe siècle, on a trouvé des démonstrations plus proches du résultat, c'est-à-dire n'utilisant pas de principes abstraits comme des résultats généraux sur des fonctions analytiques... Le principe de "pureté des méthodes" dit qu'il est bien, élégant... de se restreindre, lors d'une démonstration, à des principes et des énoncés en rapport avec la conclusion, une démonstration abstraite d'un énonce réel viole la pureté des méthodes, et le programme de Hilbert nous donne donc un principe de pureté des méthodes généralisé.

- Le programme de Hilbert suppose la complétude des mathématiques élémentaires, en effet, il ne fait pas de doute que toute identité vraie est démontrable par des méthodes abstraites ad hoc, et donc par le programme de Hilbert, par des méthodes élémentaires. D'ailleurs, les formalistes attardés utilisent "vrai" pour "démontrable" et "faux" pour "réfutable". Les phénomènes de complétude (c'est-à-dire l'adéquation entre vrai et "prouvable") ne sont pas si rares que cela, mentionnons quelques exemples

- la théorie des corps réels clos est complète,

- la complétude est vraie pour les énonces co-élémentaires (négations d'énoncés élémentaires) en fait tout énoncé co-élémentaire vrai est prouvable dans les mathématiques "co-élémentaires"... malheureusement, ce n'est pas à cette classe-là que Hilbert s'est intéressé pour son programme.

Une démonstration valable du programme de Hilbert ne saurait être qu'élémentaire : sinon, on ne pourrait rien conclure, puisque ce qui n'est pas élémentaire n'a pas de sens... Concrètement, la démonstration du programme de Hilbert consiste à se placer dans une théorie abstraite (par exemple ZF), et d'y considérer un énoncé élémentaire, et une démonstration abstraite T de cet énoncé R, il s'agirait alors, au moyen de transformations élémentaires sur T, d'obtenir une démonstration élémentaire T' du même énoncé R. Ce genre de résultat (dans un autre contexte) n'a rien d'utopique on sait par exemple (à l'aide des résultats de Gödel sur l'hypothèse du continu) transformer, au moyen d'un procédé tout ce qu'il y a d'élémentaire, toute démonstration dans ZF+AC+GCH d'un énoncé élémentaire, en une démonstration dans ZF (mais la démonstration n'est pas élémentaire, et l'analogie s'arrête là...). L'école de Hilbert se fit d'abord les dents sur de tout petits systèmes (fragments de l'arithmétique), en attendant d'être à même de démontrer le résultat pour la théorie des ensembles. Mais Gödel donna un coup d'arrêt brutal au programme...

3. Démonstration de cohérence

Une formulation équivalente du programme de Hilbert, est la recherche de démonstrations de cohérence élémentaires :

(i) si le programme de Hilbert est réalisé, supposons que par exemple, ZF soit contradictoire, c'est-à-dire démontre $0 = 1$, qui est un énoncé élémentaire, par le programme de Hilbert, cet énoncé peut donc être démontré

par des méthodes élémentaires mais ces méthodes ne sont dites "élémentaires" que parce que nous n'avons aucun doute en ce qui les concerne, en particulier elles ne sauraient mener à une absurdité du genre de 0 = 1. Nous venons ainsi d'obtenir une démonstration élémentaire de cohérence pour ZF (la démonstration élémentaire du programme de Hilbert pour ZF, et l'évidence élémentaire de la cohérence des mathématiques élémentaires (si la cohérence des mathématiques élémentaires n'est pas établie de manière élémentaire, ici encore, une application du programme de Hilbert rendra notre démonstration élémentaire))

ii) réciproquement, si la théorie ZF est cohérente, prenons un énoncé élémentaire, disons le théorème de Fermat, et supposons l'y avoir prouvé; si par ailleurs, les entiers $a, b, c, \neq 0$ et $n > 2$ sont tels que $a^n + b^n = c^n$ par exemple si $17^{101}+23^{101} = 24^{101}$, alors l'équation $a^n+b^n = c^n$ serait prouvable en théorie des ensembles ZF, ce qui donnerait une contradiction dans ZF. Nous venons de donner informellement une démonstration élémentaire du programme de Hilbert (dans le cas du théorème de Fermat), en donnant un procédé élémentaire pour transformer une démonstration non-élémentaire de Fermat dans ZF en une démonstration élémentaire, au moyen d'une démonstration élémentaire de cohérence de ZF...

4. L'intuitionnisme

On comprendra mieux le formalisme en parlant de son frère ennemi, l'intuitionnisme, dont le champion fut Brouwer. Les deux théories se rejoignaient dans un même refus du réalisme (c'est-à-dire de la philosophie "naïve" des mathématiques, pour laquelle les énoncés mathématiques parlent d'objets réels dans un univers idéal à préciser...). Par contre, les deux théories divergeaient radicalement pour ce qui est de l'analyse de l'activité mathématique.

- Pour Hilbert, l'activité mathématique est mécanique, pour lui le mathématicien idéal serait un robot, essayant systématiquement toutes les démonstrations élémentaires possibles. Tout ce que nous appelons "intuition" n'est rien d'autre que ce qui permet au mathématicien de se hausser au niveau de ce mathématicien idéal...

- au contraire, pour Brouwer, l'activité mathématique est un acte créateur de l'esprit, qui ne saurait en aucune façon être mécanisé, en particulier, pour lui, les mathématiques étaient par essence non formalisables.

Le système intuitionniste se développe par des principes logiques totalement différents des principes classiques, notamment le refus du principe du tiers exclu, tout cela se justifie, suivant Brouwer, en faisant référence à un "sujet pensant" qui produit des résultats mathématiques. Une discussion approfondie de l'intuitionnisme serait ici hors de propos contentons-nous de remarquer que cette théorie, bien qu'extravagante par certains côtés, présente une vision de l'activité mathématique moins désolante que celle de Hilbert, malheureusement, l'intuitionnisme n'a pas tenu ses promesses...

5. Réfutation du programme de Hilbert (1931)

Le premier théorème d'incomplétude de Gödel associe à toute théorie cohérente T satisfaisant des conditions très générales, un énoncé élémentaire C, ayant les propriétés suivantes

- C est vrai
- C n'est pas démontrable dans T.

Ceci détruit le programme de Hilbert, car si on prend pour théorie T une théorie cohérente contenant toutes les mathématiques élémentaires, (par exemple, on pourrait prendre pour T l'arithmétique de Peano AP), l'énoncé de Gödel C est élémentaire, démontré par le théorème de Gödel (puisque le théorème dit qu'il est vrai) et la cohérence de T, mais sans démonstration dans T, donc sans démonstration élémentaire.

On trouve plus souvent la référence au deuxième théorème d'incomplétude, qui dit la chose suivante : sous des conditions presque aussi générales que celles du premier théorème, l'énoncé élémentaire qui exprime la cohérence de T n'est pas démontrable dans T. Ce deuxième théorème détruit le programme sous sa forme "cohérence" mais il n'est pas nécessaire (sa démonstration est plus difficile que celle du premier) à la réfutation du programme de Hilbert le premier théorème suffit.

Le programme de Hilbert est donc réfuté en 1931, mais, par un phénomène psychologique bien compréhensible, le formalisme a gardé une grande partie de ses adeptes : en effet le formalisme présente une vision assez simple des mathématiques (le mécanisme, la complétude, les objets abstraits comme des façons de parler, mais n'existant pas...), et on sait bien que les visions simplistes, réductrices, du monde ont toujours un impact sans commune mesure avec leur succès réel. Tout aurait été bien différent si au lieu

de démolir le programme de Hilbert sans rien mettre à sa place qui ait les mêmes vertus d'attraction, Gödel avait trouvé une caractérisation simple de la prouvabilité en termes de vérité, ou le contraire... Nous allons maintenant voir d'un peu plus près ces théorèmes d'incomplétude.

6. Le premier théorème d'incomplétude

Nous allons nous intéresser ici uniquement à l'arithmétique de Peano AP. La première chose est de représenter les données syntaxiques de AP au moyen d'entiers. Cela ne présente théoriquement aucune difficulté, vu que le langage, et les constructions qui gravitent autour, forment des ensembles dénombrables. La bijection que l'on établit entre énoncés et $\mathbb{N}$ s'appelle numérotation de Gödel. Rappelons que le langage de l'arithmétique est basé sur $0, S, +, ., =, <$ à chacun de ces symboles, ainsi qu'aux connecteurs, aux quantificateurs et aux variables, on attribue un entier son <u>nombre de</u> <u>Gödel</u> : $\ulcorner 0 \urcorner = 1$; $\ulcorner S \urcorner = 3$; $\ulcorner + \urcorner = 5$; $\ulcorner . \urcorner = 7$; $\ulcorner = \urcorner = 9$; $\ulcorner < \urcorner = 11$; $\ulcorner \neg \urcorner = 13$; $\ulcorner \vee \urcorner = 15$; $\ulcorner \& \urcorner = 17$; $\ulcorner \Rightarrow \urcorner = 19$; $\ulcorner \exists \urcorner = 21$; $\ulcorner \forall \urcorner = 23$; $\ulcorner x_n \urcorner = 25 + 2n$.
Les nombres de Gödel ne sont en rien remarquables ; on pourrait imaginer beaucoup d'autres manières de numéroter les symboles du langage. Il ne s'agit pas d'entiers qui auraient des relations cachées avec les symboles qu'ils représentent, je dis cela à cause de l'association qu'on peut être amené à faire avec d'autres "nombres de" (Bernoulli par exemple). Si $a_0, \ldots, a_{n-1}$ est une suite d'entiers de longueur n, on introduit un entier $\ulcorner a_0, \ldots, a_{n-1} \urcorner = p_1^{a_0+1} \cdots p_n^{a_{n-1}+1}$ où p_n désigne le n-ime nombre premier, alors $\ulcorner a_0, \ldots, a_{n-1} \urcorner$ détermine n uniquement, ainsi que les entiers $a_0, \ldots, a_{n-1}$.

On sait qu'il est possible, en utilisant la "notation polonaise", c'est-à-dire en écrivant $\vee AB$ à la place de $A \vee B$, $\& AB$ à la place de $A \& B$,... d'éliminer les parenthèses, et tout énoncé du langage apparaît comme une suite finie de symboles $0, S, \ldots, x_n, \ldots$ dans un certain ordre. Si A est un tel énoncé, on peut donc écrire $A = s_0 \ldots s_m$ où $s_0 \ldots s_m$ sont des symboles $0, S, \ldots, x_n, \ldots$ et on posera donc $\ulcorner A \urcorner = \ulcorner \ulcorner s_0 \urcorner, \ldots, \ulcorner s_m \urcorner \urcorner$. Une démonstration de A dans AP, c'est une suite $A_0, \ldots, A_p$ d'énoncés, telle que $A_p = A$, et la suite est bâtie en respectant les règles d'inférence du calcul des prédicats, et les axiomes de Peano (dont l'énoncé précis ne joue aucun rôle ici). On peut donc associer a une démonstration $A_0, \ldots, A_p$ un nombre

de Gödel $\ulcorner A \urcorner = \ulcorner\ulcorner A_0 \urcorner, \ldots, \ulcorner A_p \urcorner\urcorner$.

On considère la propriété $Dem(d,a)$: d est le nombre de Gödel d'une démonstration de l'énoncé dont le nombre de Gödel est a. Nous allons énoncer quelques évidences (techniquement, cela demande des notions de récursivité, et ce n'est pas du tout évident)

- $Dem(d,a)$ est une formule de l'arithmétique (on voit bien que les règles syntaxiques de formation des énoncés et des démonstrations vont être expressibles, au moyen du nombre de Gödel, par des propriétés arithmétiques)

- surtout dès que $Dem(d,a)$ est vrai, il est démontrable dans AP, cela peut se voir ainsi : une démonstration est une suite finie de symboles, qui vérifie un certain nombre de critères combinatoires que l'on peut vérifier mécaniquement ; or tout ce qui est mécanique est du ressort de la démonstrabilité (je n'ai pas dit que l'on peut décider mécaniquement la démonstrabilité dans AP), c'est-à-dire que le processus mécanique de vérification qu'un assemblage de symboles est une démonstration peut être confié à une théorie formelle comme AP. En fait les énoncés, qui comme Dem(d,a) sont prouvables dès qu'ils sont vrais, sont les co-élémentaires. (On dit plus souvent Σ_1^0)

L'étape suivante consiste à reproduire le fameux <u>paradoxe du menteur</u>, connu depuis l'Antiquité : "je mens" ; à proprement parler, le paradoxe du menteur donnerait "je ne suis pas vrai" ; ici nous allons considérer "je ne suis pas prouvable", à savoir un énoncé A équivalent à $\forall d \neg Dem(d, \ulcorner A \urcorner)$ en fait on a mieux que l'équivalence A et $\forall d \neg Dem(d, \ulcorner A \urcorner)$ sont le même énoncé. Un tel énoncé A se construit facilement avec un peu plus de technique que ce que nous avons introduit... Remarquons que A est par construction un énoncé élémentaire (on dit encore Π_1^0).

A n'est pas prouvable dans AP : en effet, si A était prouvable dans AP, on y prouverait A et donc $Dem(d, \ulcorner A \urcorner)$ pour un certain d ; mais comme A est $\forall d \neg Dem(d, \ulcorner A \urcorner)$, on obtiendrait une contradiction dans AP donc si AP est cohérente, l'énoncé A n'est pas démontrable dans AP. Mais comme A est équivalent à sa non-prouvabilité dans AP, et que nous venons de voir que A n'est pas démontrable dans AP, il s'ensuit que A est vrai, mais non démontrable. Remarquons que rien n'exclut que $\neg A$ soit démontrable dans AP (sinon notre intuition que les théorèmes de AP sont vrais). Par une amélioration due à Rosser (1936), on peut construire A vrai et élémentaire

tel que ni A ni $\neg A$ ne soient démontrables dans AP.

Une autre remarque est le résultat suivant, dû à Tarski, on ne peut pas trouver de prédicat de vérité dans AP, à savoir d'énoncé V tel que $V(\ulcorner B \urcorner) \Leftrightarrow (B$ soit démontrable dans AP) pour tout B il suffit de refaire la construction de Gödel en remplaçant $\exists d\, Dem(d, \ulcorner B \urcorner)$ par $V(\ulcorner B \urcorner)$.

7. Deuxième théorème d'incomplétude

$Coh(\mathrm{AP})$ est l'énoncé $\forall d \neg Dem(d, \ulcorner 0 = S0 \urcorner)$, qui exprime que AP est cohérente ; il est extrêmement pénible de démontrer le premier théorème d'incomplétude formellement dans AP, mais on y arrive : si AP est cohérente, A est vrai : l'énoncé $Coh(\mathrm{AP}) \Rightarrow A$ est donc démontrable dans AP, et comme A n'est pas démontrable dans AP, $Coh(\mathrm{AP})$ ne peut pas être démontrable dans AP, si AP est cohérente. L'idée est simple, mais la mise en oeuvre mathématique est très lourde...

8. Signification des théorèmes d'incomplétude

Le résultat de Gödel est extrêmement célèbre, d'ailleurs surtout hors des milieux mathématiques. Nous avons déjà eu l'occasion de dire que ce théorème n'avait pas affecté de façon sensible la conception des mathématiques du mathématicien moyen. La renommée de ce résultat dans des cercles non mathématiques vient surtout d'une mécompréhension : on retient l'imitation du paradoxe du menteur, et cela donne quelque chose comme (si on parle du deuxième théorème, qui a de loin le plus de succès) "une théorie ne peut pas se penser elle-même", ou pire, en extrapolant "la science ne peut pas se penser elle-même". Ce qui est certain, c'est qu'un résultat comme le théorème de Gödel appelle naturellement de nombreux commentaires et des extrapolations variées : c'est qu'on a l'impression que son importance dépasse de loin le strict cadre technique où il se place... Ceci dit, ce n'est pas une raison pour dire n'importe quoi.

- Quand on dit qu'une théorie ne peut pas se penser elle-même on fait un contresens sur la signification du théorème, les énoncés qui expriment dans AP les propriétés de AP, telle la formule $Coh(\mathrm{AP})$, montrent bien que AP peut "se penser elle-même" ; si on veut dire par là qu'il y a des énoncés sur AP qui ne sont pas démontrables dans AP elle-même, il conviendra de remarquer qu'il y a aussi des énoncés vrais qui ne parlent pas de AP, et

qui ne sont pas démontrables dans AP, ainsi que des propriétés vraies de AP qui sont démontrables dans AP : l'accent mis sur la cohérence est arbitraire...

- Quand l'extrapolation va plus loin que les théories formelles, à savoir quand on veut faire dire au théorème d'incomplétude quelque chose sur la pensée en général, on passe loin de la signification profonde du résultat, en effet le théorème d'incomplétude est avant tout un résultat sur la pensée mécanique (une théorie formelle) et s'il semble honnête d'extrapoler les résultats d'incomplétude au domaine de la pensée mécanique (ordinateurs, jeux...), appliquer le théorème d'incomplétude à l'activité humaine est hautement farfelu, d'ailleurs, quand je dis appliquer, c'est un bien grand mot : on cite Gödel à la place où naguère on aurait cité, disons... Mallarmé, dont les vers énigmatiques renferment, on le sait, tout ce qu'il faut pour ce genre de situation : il importe seulement de ne pas mélanger les genres et de ne pas utiliser les résultats scientifiques sous une forme tellement métaphoriques qu'ils en sont devenus méconnaissables.

Pour résumer, si nous devons dire en une phrase quelle est la signification de la réfutation par Gödel du programme de Hilbert, c'est :

"il y a des choses qui ne sont pas du ressort du mécanisme."

Voilà ce que disent les théorèmes d'incomplétude, et ce message est répété sous de nombreuses formes techniques, je pense aux théorèmes d'indécidabilité (voir 5ème conférence). S'il y a des choses qui ne sont pas du ressort du mécanisme, cela veut dire qu'il y a quelque chose de non mécanique dans, disons, la pensée mathématique par exemple, la production de nouveaux axiomes est nécessairement chaotique (vue du point de vue d'un robot) il s'agit de parier à chaque étape sur l'étape suivante : il n'est pas question de produire des axiomes par une méthode régulière.

9. Démonstrations de cohérence relative([3])

Après le résultat de Gödel, il devenait impossible de penser à raisonner sur la cohérence d'une manière qui soit épistémologiquement absolument convaincante. Comment penser un instant qu'une démonstration de cohérence, qui utilise plus que l'arithmétique, a une réelle valeur, au niveau de la philosophie des mathématiques... En fait ceci ne concerne que les démons-

[3]Ce qui suit constitue la 2e conférence de J.Y. GIRARD

trations de cohérence, dans ce qu'elles ont de plus prétentieux : les démonstrations de cohérence absolue. Par contre, il est une autre catégorie de démonstrations de cohérence, les démonstrations de cohérence relative, c'est-à-dire des énoncés de la forme

$$Coh(\mathtt{T}) \Rightarrow Coh(\mathtt{U})$$

(si T est cohérente, alors U l'est). La valeur épistémologique de tels résultats est plus limitée, mais par contre, vu que de telles démonstrations se font toujours dans les mathématiques élémentaires chères à Hilbert, cette valeur épistémologique est incontestable ; par exemple, le résultat de 1939 de Gödel : $Coh(\mathtt{ZF}) \Rightarrow Coh(\mathtt{ZF} + \mathtt{AC} + \mathtt{GCH})$ (cohérence relative de l'axiome du choix et de l'hypothèse du continu par rapport à ZF) montre que l'axiome du choix et l'hypothèse du continu ne sont pas plus "risquées" que la théorie des ensembles ; nous avons ici une vraie réduction... De la même manière, les résultats de Cohen (cohérence relative de la négation de l'axiome du choix, de la négation de l'hypothèse du continu), montrent que l'on peut aussi faire des choix opposés qui ne sont pas plus risqués. Mais ne déflorons pas trop le sujet de la conférence d'A. LOUVEAU.

10. Signification des démonstrations de cohérence

Un mot de Kreisel "les doutes quant à la cohérence sont plus douteux que la cohérence elle-même". Au fond, personne ne doute vraiment de la cohérence de l'arithmétique ; s'il existe un problème lié aux théorèmes de Gödel, il importe de ne pas dramatiser à l'excès, et de ne pas appliquer à ces situations délicates des considérations trop brutales.

Un des résultats les plus remarquables de Gentzen est son introduction, dans les années 30 du calcul des séquents, et la démonstration pour le calcul des séquents, du Hauptsatz (qui est un véritable principe de pureté des méthodes pour le calcul des prédicats, c'est-à-dire la logique pure) n'est pas sans conséquences pour les questions de cohérence. Avant de parler du calcul des séquents, expliquons comment on peut par exemple utiliser le Hauptsatz pour établir, en un sens presque satisfaisant, la cohérence des mathématiques élémentaires.

(ARP) l'arithmétique récursive primitive est une bonne formulation des mathématiques élémentaires ; ce système est formé ainsi

- il y a un grand nombre (une infinité) de lettres de fonctions, pour représenter des fonctions combinatoires élémentaires (fonctions récursives primitives) comme $+, ., \exp$, etc..., et pour chacune de ces fonctions, on écrit des axiomes de définition, par exemple
$2^0 = 1$
$2^{Sx} = 2^x + 2^x$

- on permet l'induction (récurrence) sur les énoncés de la forme $t = u$, où t et u sont des <u>termes</u>, c'est-à-dire sont construits en utilisant les lettres de fonction mentionnées plus haut, et des variables.

Ce système est une bonne formalisation des mathématiques élémentaires ; mais est-il cohérent ? Il y a une démonstration "naïve" de la cohérence de ARP, qui consiste seulement à remarquer que tout théorème de ARP est vrai, par exemple, à montrer que si $\forall x \exists y\, t[x, y] = 0$ est démontrable dans ARP, alors, pour tout x, on peut trouver un y tel que $t[x, y]$ soit égal à 0. Malheureusement, on voit bien que dans la définition de la vérité, on utilise des quantificateurs qui nous font sortir de la classe des énoncés élémentaires typiquement, le "on peut trouver y" est un quantificateur indésirable... Heureusement, le Hauptsatz peut ici être utilisé, on remarque d'abord que tous les axiomes de ARP sont de la forme $t = u$, y compris l'axiome (les axiomes en fait) d'induction. Le Hauptsatz nous dit alors (c'est un principe de pureté des méthodes) qu'une démonstration de $0 = S0$ se place dans la partie purement équationnelle de ARP, c'est-à-dire qu'à partir des équations qui nous servent d'axiomes, utilisant la transitivité et la symétrie de l'égalité, on a déduit $0 = S0$!. Cette réduction (qui utilise le Hauptsatz) de ARP à sa partie équationnelle est faite par des moyens purement élémentaires. Par contre, il faut démontrer la cohérence de la partie purement équationnelle (sans logique) de ARP, et pour cela, nous avons une fonction de valuation, qui à tout terme clos (sans variable) de ARP, associe sa valeur ; bien entendu, cette fonction de valuation ne saurait être parmi les fonctions de ARP. Cette partie de la démonstration de cohérence de ARP n'est donc pas, conformément au théorème de Gödel, formalisable dans ARP. La fin de la démonstration est simple, on démontre que, si t et u sont des termes clos tels que l'équation $t = u$ soit démontrable dans la partie équationnelle de ARP, alors $V(t) = V(u)$; pour les axiomes c'est immédiat, et la transitivité, la symétrie de l'égalité, préservent

cette propriété... En particulier, comme $V(0) = 0 \neq 1 = V(S0)$, $0 = S0$ n'est pas démontrable dans le calcul équationnel, et donc pas démontrable tout court dans ARP.

Nous voyons ici que la partie problématique de la cohérence (tout ce qui touche aux quantificateurs) est démontrée de manière élémentaire, tandis que le théorème de Gödel ne s'applique vraiment qu'à la partie purement équationnelle de ARP, pour laquelle nous n'avons pas de doute sérieux.

11. Le calcul des séquents

Il est difficile ici de ne pas évoquer la mémoire de Jacques Herbrand, mort prématurément en 1931, et dont les travaux (le théorème de Herbrand) préfigurent les résultats de Gentzen...

Pour obtenir son principe de pureté des méthodes, Gentzen modifie les notions de base de la logique : la notion essentielle n'est plus le concept d'énoncé, mais celui de séquent, Gentzen appelle séquent une expression formelle $\Gamma \Rrightarrow \Delta$, où Γ et Δ sont des suites finies d'énoncés. La signification intuitive de $A_1, \ldots, A_n \Rrightarrow B_1, \ldots, B_m$ c'est que si tous les A_i sont vrais, alors un des B_j l'est :

$$A_1 \& \ldots \& A_n \Rightarrow B_1 \vee \ldots B_m$$

(En particulier, $\Rrightarrow A$ veut dire A, et $A \Rrightarrow$ veut dire $\neg A$, et puis le séquent vide $\Rrightarrow$ veut dire l'absurdité, c'est-à-dire $0 = S0$). Les règles du calcul des séquents sont tout à fait remarquables ; on les divise en quatre groupes

(I) AXIOMES

$$A \Rrightarrow A \quad (A \text{ énoncé quelconque})$$

(Il) REGLES STRUCTURELLES

Affaiblissement

$$\frac{\Gamma \Rrightarrow \Delta}{\Gamma \Rrightarrow A, \Delta} \; dA \qquad \frac{\Gamma \Rrightarrow \Delta}{\Gamma, A \Rrightarrow \Delta} \; gA$$

Echange

$$\frac{\Gamma \Rrightarrow \Delta', A, B, \Delta''}{\Gamma \Rrightarrow \Delta', B, A, \Delta''} \; dE \qquad \frac{\Gamma', A, B, \Gamma'' \Rrightarrow \Delta}{\Gamma', B, A, \Gamma'' \Rrightarrow \Delta} \; gE$$

Contraction

$$\frac{\Gamma \Vdash A, A, \Delta}{\Gamma \Vdash A, \Delta}\ dC \qquad \frac{\Gamma, A, A \Vdash \Delta}{\Gamma, A \Vdash \Delta}\ gC$$

(III) REGLES LOGIQUES

Règles du &

$$\frac{\Gamma \Vdash A, \Delta \quad \Gamma' \Vdash B, \Delta'}{\Gamma, \Gamma' \Vdash A\&B, \Delta, \Delta'}\ d\& \qquad \frac{\Gamma, A \Vdash \Delta}{\Gamma, A\&B \Vdash \Delta}\ g1\& \qquad \frac{\Gamma, B \Vdash \Delta}{\Gamma, A\&B \Vdash \Delta}\ g2\&$$

Règles du $\vee$

$$\frac{\Gamma \Vdash A, \Delta}{\Gamma \Vdash A \vee B, \Delta}\ d1\vee \qquad \frac{\Gamma \Vdash B, \Delta}{\Gamma \Vdash A \vee B, \Delta}\ d2\vee \qquad \frac{\Gamma, A \Vdash \Delta \quad \Gamma', B \Vdash \Delta'}{\Gamma, \Gamma', A \vee B \Vdash \Delta, \Delta'}\ g\vee$$

Règles du $\Rightarrow$

$$\frac{\Gamma, A \Vdash B, \Delta}{\Gamma \Vdash A \Rightarrow B, \Delta}\ d\Rightarrow \qquad \frac{\Gamma \Vdash A, \Delta \quad \Gamma', B \Vdash \Delta'}{\Gamma, \Gamma', A \Rightarrow B \Vdash \Delta, \Delta'}\ g\Rightarrow$$

Règles du $\neg$

$$\frac{\Gamma, A \Vdash \Delta}{\Gamma \Vdash \neg A, \Delta}\ d\neg \qquad \frac{\Gamma \Vdash A, \Delta}{\Gamma, \neg A \Vdash \Delta}\ g\neg$$

Règles du $\forall$

$$\frac{\Gamma \Vdash A, \Delta}{\Gamma \Vdash \forall x A, \Delta}\ d\forall(^*) \qquad \frac{\Gamma, A[t] \Vdash \Delta}{\Gamma, \forall x A \Vdash \Delta}\ g\forall$$

Règles du $\exists$

$$\frac{\Gamma \Vdash A[t], \Delta}{\Gamma \Vdash \exists x A, \Delta}\ d\exists \qquad \frac{\Gamma, A \Vdash \Delta}{\Gamma, \exists x A \Vdash \Delta}\ g\exists(^*)$$

(*) règles restreintes au cas où x n'est pas libre dans $\Gamma \Vdash \Delta$.

(IV) COUPURE

$$\frac{\Gamma \Vdash A, \Delta \qquad \Gamma', A \Vdash \delta'}{\Gamma, \Gamma' \Vdash \Delta, \Delta'}\ \mathtt{C}$$

une démonstration dans le calcul des séquents LK, c'est une suite de séquents (disposée en forme d'arbre) construite à partir des axiomes, au moyen des règles (II), (III), (IV) . Un mot sur les règles

(II) les règles structurelles sont des règles assez anodines : elles permettent de faire quelques manipulations combinatoires simples (permutation, augmentation, identification d'énoncés du même côté du signe $\Rrightarrow$) ; il importe cependant de ne pas mépriser le pouvoir de la règle de contraction,

(III) les règles logiques démarquent la genèse des énoncés ; on parle encore de règles génétiques pour la partie (I) (II) (III) de LK (calcul sans coupures), pour cette raison. C'est une réussite indéniable de Gentzen que d'avoir isolé, au moyen des séquents de tels principes "purs" de démonstration.

(IV) la règle de coupure exprime quant à elle la <u>transitivité</u> de la notion de conséquence logique ; c'est une règle qui correspond à la pratique mathématique chaque fois que dans un raisonnement mathématique, vous utilisez un résultat général, vous effectuez une coupure ; je donne un exemple simple :

si on vous demande de calculer 499^2 , il est peu vraisemblable que vous effectuiez le calcul il est tellement mieux de faire

$$499^2 = 500^2 - 2 \times 500 + 1$$

Pour cela, vous utilisez un résultat général $\forall x\ (x-1)^2 = x^2 - 2x + 1$ que vous appliquer au cas particulier de 499 ; ce processus se traduit par une coupure : soit π la démonstration classique de l'identité susmentionnée, alors, on peut obtenir $499 = 500 - 2.500 + 1$ ainsi

$$\dfrac{\begin{array}{c}\pi\\ \vdots\\ \Rrightarrow \forall x\ (x-1)^2 = x^2 - 2x + 1\end{array} \qquad \dfrac{(500-1)^2=500^2-2.500+1 \Rrightarrow (500-1)^2=500^2-2.500+1}{\forall x\ (x-1)^2=x^2-2x+1 \Rrightarrow (500-1)^2=500^2-2.500+1}\,g\forall}{\Rrightarrow (500-1)^2 = 500^2 - 2.500 + 1}\ \mathtt{C}$$

Les résultats sur le calcul LK sont les suivants :

1/ Un résultat attendu, LK est une bonne formulation de la logique, autrement dit A est démontrable dans le calcul des prédicats (encore : A est vrai dans tout modèle) si et seulement si $\Rrightarrow A$ est démontrable dans LK.

2/ Le Hauptsatz : si un séquent est démontrable dans LK il est aussi démontrable sans coupures, autrement dit la règle de coupure est redondante.

Le corollaire le plus connu du Hauptsatz, c'est la <u>propriété</u> de la <u>sous-formule</u>. Gentzen appelle sous-formule de A, A lui-même et

- si A est $\neg B$, les sous-formules de B,
- si A est $B\&C$, $B \vee C$, $B \Rightarrow C$, les sous-formules de B et/ou de C,
- si A est $\forall x B[x]$, $\exists x B[x]$, les sous-formules des $B[t]$, où t est un terme.

On voit qu'il y a toujours (dès que A contient un quantificateur), une infinité de sous-formules distinctes pour A. On a la propriété

Dans une démonstration sans coupures de $\Gamma \Rrightarrow \Delta$, tous les énoncés utilisés sont des sous-formules d'énoncés apparaissant dans Γ ou dans A.

Ce résultat est une conséquence des deux remarques suivantes
- dans les règles (II) et (III), tous les énoncés utilisés dans une quelconque prémisse de la règle, sont des sous-formules d'énoncés apparaissant dans la conclusion,
- la notion de sous-formule est transitive.

Ce principe, qui est un authentique principe de pureté des méthodes pour le calcul des prédicats (à un détail près il y a des substitutions arbitraires de termes pour fabriquer les sous-formules, mais on se rappellera que l'on peut se ramener à des calculs sans lettres de fonctions, où les seuls termes sont donc des variables), nous a permis d'"éliminer les quantificateurs" dans ARP.

Le théorème de Gentzen est élémentaire, c'est-à-dire que Gentzen donne un procédé effectif pour éliminer les coupures. (Il est à remarquer que ce procédé, quoique effectif, dépasse de loin, les capacités théoriques des ordinateurs !). En particulier, on peut se demander ce que donne une démonstration sans coupures du résultat donné plus haut (sur 499^2) : c'est tout simplement effectuer le calcul on voit que les démonstrations sans coupures ont tendance à devenir longues et bêtes, c'est la règle de coupure qui concentre l'intelligibilité des démonstrations, et c'est pourquoi elle correspond à la pratique ; les règles sans coupures, correspondent elles, à l'étude abstraite du raisonnement. Elles sont commodes à étudier, mais pas à manier.

Un mot sur la <u>sémantique</u> des règles sans coupures : c'est une sémantique à trois valeurs (vrai, faux, indéterminé) ; les règles (I) (Il) (III) sont valides pour l'interprétation : si $A_1, \ldots, A_n$ sont vrais, alors un des

énoncés $B_1, \ldots, B_m$ n'est pas faux. Pour ce type d'interprétation, la règle de coupure n'est pas valide, puisque cela exigerait que A non faux implique A vrai, autrement dit la règle de coupure caractérise la sémantique binaire, où tout est vrai ou faux...

La postérité de Gentzen est impressionnante en théorie de la démonstration les théorèmes d'élimination des coupures continuent à fournir une grande partie de l'inspiration et de la problématique du sujet...

12. Démonstrations de cohérence pour l'arithmétique

Gentzen a aussi donné des démonstrations de cohérence pour l'arithmétique ; ces démonstrations reposent sur un principe additionnel, qui est un principe d'induction (récurrence) transfinie. Considérons les polynômes exponentiels, construits, à partir de 0, de la somme, et de l'exponentiation $x^{P(x)}$; on peut comparer deux tels polynômes par

$$P < Q \Leftrightarrow \exists n(\forall m > n\ (P(m) > Q(m))).$$

On obtient un ordre linéaire qui est un bon ordre (pas de suite infinie décroissante), et que l'on note ε_0. Gentzen démontre la cohérence de AP (l'arithmétique de Peano) par induction transfinie jusqu'à ε_0. L'idée de la démonstration est de répéter ce que nous avons fait pour ARP, c'est-à-dire de se ramener à la partie purement équationnelle de AP, qui est trivialement cohérente ; pour cela, il nous suffirait d'un principe de pureté des méthodes, c'est-à-dire d'une généralisation du Hauptsatz à l'arithmétique. Mais le Hauptsatz n'est vrai que pour des systèmes sans axiomes (ou des axiomes de complexité très simple comme ARP) ; l'idée est de se ramener à cette situation en faisant apparaître le principe d'induction comme quelque chose de purement logique[4]

On écrit donc les règles

$$\frac{\cdots \Gamma \Vdash A[n], \Delta \cdots}{\Gamma \Vdash \forall x A[x], \Delta}\ d\forall\omega \qquad\qquad \frac{\Gamma, A[n_0] \Vdash \Delta}{\Gamma, \forall x A[x] \Vdash \Delta}\ g\forall\omega$$

[4]Ceci est à rapprocher de la manière dont Bourbaki écrit l'axiome du choix : par un tour de passe-passe, cet axiome devient une conséquence purement logique des autres ; l'avantage est que cela permet (?) de couper court à des discussions sur le choix des axiomes qui obligeraient à mettre 'mathématique' au pluriel...

et

$$\frac{\Gamma \Vdash A[n_0], \Delta}{\Gamma \Vdash \exists A[x], \Delta}\, d\exists\omega \qquad\qquad \frac{\cdots \Gamma, A[n] \Vdash \Delta \cdots}{\Gamma, \exists x A(x) \Vdash \Delta}\, g\exists\omega$$

à la place des règles logiques écrites plus haut pour $\forall$ et $\exists$; observer que $d\forall\omega$ et $g\exists\omega$ sont des règles infinies : les démonstrations sont donc des arbres bien fondés, et on a affaire à une généralisation de la notion habituelle de démonstration, qui n'a rien à voir avec la notion de démonstration formelle. (Schütte, à qui on doit cette formulation, parle de système "semi-formel"). Rappelez-vous la justification du principe d'induction comme on a pu vous l'apprendre il y a quelques années : si $A[0]$ et $\forall x(A[x] \Rightarrow A[Sx])$, alors $A[0] \Rightarrow A[S0]$, donc $A[S0]$, puis $A[S0] \Rightarrow A[SS0]$; donc $A[SS0]$ etc..., autrement dit les séquents $A[0], \forall x(A[x] \Rightarrow A[Sx]) \Vdash A[n]$ sont prouvables pour tout n, et par la règle $(d\forall\omega)$, $A[0], \forall x(A[x] \Rightarrow A[Sx]) \Vdash \forall x A[x]$ est démontrable ce qui donne bien une démonstration purement logique du principe d'induction usuelle. Mais le calcul semi-formel mentionné plus haut vérifie l'élimination des coupures, et de plus, si on part d'une démonstration (finie) dans l'arithmétique, on obtient finalement une démonstration sans coupures du même séquent, et de <u>hauteur</u> bornée par ε_0 ; en particulier, en prenant le séquent $\Vdash$, on voit immédiatement qu'une démonstration sans coupures de ce séquent (qui se placerait dans la partie équationnelle de AP) ne saurait exister ; mais ici, on utilise un principe extérieur à AP l'induction transfinie jusqu'à ε_0, c'est le tribut qu'il faut payer au deuxième théorème d'incomplétude.

13. Signification des démonstrations de cohérence

Un mathématicien français a dit : "Gentzen, c'est le type qui a démontré la cohérence de l'arithmétique, c'est-à-dire de l'induction transfinie jusqu'à ω, au moyen de l'induction transfinie jusqu'à ε_0". Cette plaisanterie exprime très bien le malaise que l'on ressent devant le résultat de Gentzen : qu'est-ce que ces résultats veulent bien dire ?

1/ A y regarder de plus près, le travail de Gentzen n'est pas si ridicule que cela ; en effet, l'arithmétique, c'est l'induction jusqu'à ω sur des énoncés arbitraires, alors que dans le travail de Gentzen, comme l'a fait remarquer Kreisel, l'induction jusqu'à ε_0 n'est utilisée que sur des énoncés sans quantificateurs, c'est-à-dire qu'il s'agit d'une induction élémentaire.

Avec cette remarque, le travail de Gentzen peut tout à fait être accepté comme une généralisation légitime du programme de Hilbert, mais il n'en reste pas moins que la valeur épistémologique en reste limitée, si on se borne à la question des démonstrations de cohérence absolue ; après tout, l'induction jusqu'à ω sur des énoncés quelconques est plus près de notre intuition que l'induction (même élémentaire) jusqu'à ε_0 !

2/ Comme il n'est donc pas possible de considérer les résultats de Gentzen comme des démonstrations absolument irréfutables de la cohérence, Kreisel a proposé de leur trouver un contenu positif (indépendant de considérations oiseuses), c'est-à-dire des corollaires mathématiques indiscutables. Par exemple des propriétés de pureté des méthodes généralisées, telles :

Si A est démontrable dans AP, il est démontrable en utilisant l'induction transfinie jusqu'à un ordinal $< \varepsilon_0$ et sur un énoncé de complexité moindre que A : ce résultat est une application directe du résultat d'élimination des coupures pour la ω-logique.

3/ Peut-on quand même essayer de faire plus que de trouver de simples "contenus positifs" aux résultats de Gentzen ? Il semble que oui : si α est un ordinal, on peut définir[5] l'exponentielle 2^α , par :

$2^0 = 1$

$2^{\alpha+1} = 2^\alpha + 2^\alpha$

$2^\lambda = \sup_{\mu<\lambda} 2^\mu \qquad (\lambda \text{ limite })$

La "philosophie" du travail de Oentzen, c'est que

un quantificateur = une exponentielle

autrement dit on peut éliminer des quantificateurs au moyen d'exponentielles ordinales, ou le contraire. D'ailleurs, ε_0 n'est rien d'autre que le premier $\alpha \neq \omega$ tel que $\alpha = 2^\alpha$, c'est-à-dire le résultat de ω exponentiations...

Tout cela peut être rendu plus explicite par le résultat suivant : les deux principes suivants sont équivalents dans les mathématiques élémentaires

(1) le fait que tout sous-ensemble de $\mathbb{N}^2$ a une projection sur $\mathbb{N}$.

(2) le fait que si α est un bon ordre, 2^α est un bon ordre.

L'intérêt de cette équivalence est que, dans (1), l'opération de projection n'est pas élémentaire ; étant donné $X \subset \mathbb{N}^2$, comment déterminer les éléments de $pr_1(X)$ et de son complémentaire sans utiliser d'opérations infinies ?

[5] Ne pas confondre cette exponentielle ordinale avec l'exponentiation cardinale qui elle, est reliée à la notation A^B pour désigner l'ensemble des applications de B dans A.

Par contre, si on connaît α, on connaît ipso facto 2^α : ce qui fait problème, c'est alors le fait que l'exponentielle préserve le côté bien ordonné des ordres linéaires. On a donc une mise en relation entre deux approches : d'une part une approche "réaliste" où il y a des objets, et surtout des constructions infinies, et qui correspond à notre pratique mathématique, d'autre part, une approche "élémentaire", où seules un certain type de construction est autorisé ; certaines propriétés non-élémentaires des constructions (ici être bien ordonné) permettent de rendre compte des opérations non élémentaires de l'univers "réaliste".

Tout cela nous engage fortement à chercher une autre ontologie pour les mathématiques, c'est-à-dire à chercher les "vrais" objets de la pratique mathématique ailleurs que dans notre intuition première. L'erreur de Hilbert semble être d'avoir voulu faire des énoncés, des propriétés élémentaires quelque chose de mécanique, alors qu'il apparaît clairement que de nouveaux principes élémentaires (comme l'induction jusqu'à ε_0 sur des équations) sont sans arrêt nécessités pour rendre compte de la complexité logique croissante des mathématiques. Oui, l'univers mathématique se ramène certainement à un sous-univers élémentaire ; mais ce dernier n'est pas plus simple que l'univers tout entier.

Indécidabilité de l'hypothèse du continu

Alain Louveau

1. L'hypothèse du continu

Dans ce troisième volet sur l'indécidabilité en mathématiques, je vais parler de l'indécidabilité en théorie des ensembles. Le théorème d'incomplétude de Gödel, appliqué à cette théorie, nous assure l'existence d'énoncés ni prouvables ni réfutables dans cette théorie. Le second théorème donne un exemple de tel énoncé celui qui affirme la cohérence de la théorie elle-même. Ces résultats sont certainement très importants du point de vue théorique, mais d'un effet très faible sur la pratique mathématique. Tant que dans sa propre pratique, un mathématicien n'a pas rencontré un énoncé qu'il cherchait à démontrer et qui s'avère indécidabie, les résultats d'indécidabilité restent sans effets. Mais les dernières vingt années ont vu fleurir, dans diverses branches des mathématiques, des résultats d'indépendance. Et c'est de l'histoire de l'un d'entre eux - le plus célèbre - que je vais parler : l'hypothèse du continu.

A la fin du 19e siècle, le mathématicien Georg Cantor fonde la théorie des ensembles par ses travaux sur la notion de cardinalité : deux ensembles ont la même cardinalité si leurs éléments peuvent être mis en correspondance biunivoque; C'est la notion naturelle de taille pour les ensembles finis. L'extension aux ensembles infinis a des propriétés un peu plus étranges par exemple l'ensemble des entiers, celui des entiers pairs et l'ensemble $\mathbb{Q}$ des rationnels ont la même cardinalité (la plus petite pour les ensembles infinis, et qui est notée $\aleph_0$). Un résultat fondamental de Cantor assure qu'un ensemble A n'a jamais la même cardinalité que l'ensemble $\mathcal{P}(A)$ de toutes ses parties. En itérant l'opération des parties, on construit donc des ensembles de cardinalités de plus en plus grandes. Ainsi la cardinalité de $\mathcal{P}(\mathbb{N})$, notée $2^{\aleph_0}$, et qui est la même que celle de l'ensemble $\mathbb{R}$ des nombres réels, est plus grande que $\aleph_0$, etc... Il est naturel de se demander s'il y a des cardinalités intermédiaires, en particulier s'il existe une partie de $\mathbb{R}$ n'ayant ni la cardinalité $\aleph_0$ de $\mathbb{N}$, ni celle de $\mathbb{R}$. Cantor ne put construire de tel ensemble, et conjectura que cela devait être impossible. C'est cet énoncé "Il n'y a pas de partie de $\mathbb{R}$ de cardinalité intermédiaire entre$\aleph_0$ et $2^{\aleph_0}$, qui est connu sous le nom d'hypothèse du continu (la droite

réelle, dans les textes anciens, est aussi appelée continu).

Ce problème donna lieu à un grand nombre de recherches, avant 1938, année où K. Gödel apporta une demi-réponse : il n'est pas possible de réfuter l'hypothèse du continu dans la théorie ZFC[6]. Le résultat est un résultat de cohérence relative : s'il est possible de trouver une contradiction à partir de la théorie des ensembles augmentée de l'hypothèse du continu, alors la théorie des ensembles, à elle seule, est déjà contradictoire. L'hypothèse du continu peut donc être considérée comme un axiome supplémentaire "sûr". Mais est-ce vraiment un axiome supplémentaire (et non pas un théorème) ? La réponse attendit vingt-cinq ans. En 1963, P. Cohen prouva que pas plus qu'elle n'est réfutable, l'hypothèse du continu n'est démontrable nous sommes bien en présence d'un énoncé indécidable.

Les démonstrations de Gödel et Cohen sont nécessairement techniques. Je vais cependant essayer d'en donner les idées principales, en commençant par dégager le principe des démonstrations d'indépendance : la construction de modèles.

2. Syntaxe et sémantique

Pour illustrer ce qui va suivre, prenons une théorie plus simple, par exemple la théorie des corps. Le langage de cette théorie comprend des symboles pour $+, \times, 0$ et 1. Et les axiomes sont ceux des corps. Considérons l'énoncé E de ce langage "$1 + 1 = 0$". Cet énoncé est-il démontrable ou réfutable à partir des axiomes de la théorie des corps ? Il s'agit d'un problème combinatoire portant sur des assemblages de symboles. Pourtant une première réponse, de nature très différente, vient à l'esprit. Si "$1+1 = 0$" était démontrable à partir des axiomes, il serait sûrement vrai dans le corps $\mathbb{R}$, ce qui n'est pas le cas. E ne doit donc pas être démontrable. En disant cela, on est passé de l'aspect syntaxique à l'aspect sémantique des théories formelles. Etant donnée une théorie T dans un certain langage, on appelle modèle de T un ensemble, muni des relations et fonctions idoines, spécifiées par le langage, et qui satisfait les axiomes de la théorie T. Par exemple un modèle de la théorie des corps est un corps. Une fois que l'on possède cette notion sémantique, on introduit naturellement,

[6]ZFC est la théorie des ensembles de Zermelo-Fraenkel avec axiome du choix c'est la théorie axiomatique usuelle de la pratique mathématique.

à côté de la notion de conséquence syntaxique (existence d'une démonstration), une notion de conséquence sémantique un énoncé du langage est conséquence sémantique des axiomes de T s'il est satisfait par tous les modèles de T. Le fait que ces deux notions de conséquence coïncident est un autre remarquable résultat de K. Gödel, appelé le théorème de complétude. Il a comme conséquence qu'une théorie formelle est cohérente si et seulement si elle admet un modèle. Par suite, pour revenir à notre énoncé E du langage de la théorie des corps, il suffit, pour prouver l'indécidabilité de E, de produire deux corps l'un, comme $\mathbb{R}$, dans lequel la négation de E est satisfaite, et l'autre, par exemple $\mathbb{Z}/2$ dans lequel l'énoncé E est satisfait.

La technique utilisée pour l'indépendance de l'hypothèse du continu va être la même : produire deux modèles de ZFC, l'un satisfaisant l'hypothèse du continu, l'autre sa négation. Avec une difficulté, nous n'allons pas construire ces modèles à partir de rien, car ce n'est pas possible en effet, ces modèles seraient en particulier modèles de la théorie des ensembles, et par le théorème de complétude la construction fournirait alors une preuve de la cohérence de cette théorie, ce qui n'est pas possible par des arguments formalisables dans la théorie des ensembles (ce sont les seuls que nous allons employer), par le théorème d'incomplétude. Ce n'est pas non plus ce que nous cherchons nous voulons établir une cohérence relative à celle de la théorie des ensembles. Nous allons donc partir d'un modèle arbitraire de la théorie des ensembles, supposé exister, et construire à partir de lui les deux modèles cherchés. Bien entendu, ces constructions dépendent d'une certaine connaissance générale des modèles de la théorie des ensembles.

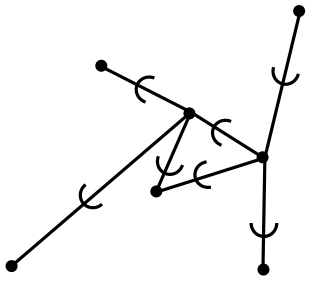
3. A quoi ressemble un univers ?

La théorie des ensembles va intervenir à deux niveaux dans ce qui suit d'une part les constructions effectuées vont être (au moins théoriquement) formalisables dans cette théorie. D'autre part, les objets construits seront (on l'espère) des modèles de la théorie des ensembles.

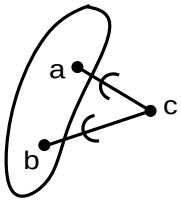
Il faut donc bien séparer ces deux niveaux, en particulier en ce qui concerne la terminologie. Dans le premier cas, nous parlerons d'ensembles intuitifs. Par exemple, un modèle de la théorie des ensembles, que nous appellerons un univers, est un ensemble intuitif, comme tout modèle d'une théorie. Et le langage de la théorie des ensembles spécifiant une relation

binaire, l'univers U est muni d'une telle relation, que nous noterons $\in^U$ peut donc être représenté comme un graphe du type suivant, où

représente la relation $\in^U$.



Nous appellerons ensembles les éléments (intuitifs) de U. Pour illustrer la distinction entre ensembles et ensembles intuitifs, considérons le fragment suivant de l'univers U



Dans ce dessin, l'élément c de U est l'ensemble $\{a, b\}^{\mathrm{U}}$. Il a exactement pour éléments, au sens de U , les ensembles a et b. Par contre la "patate" dessinée est la paire intuitive $\{a, b\}$. Il y a là un phénomène général à chaque élément x de U, on peut associer un ensemble intuitif $\{y : y \in x\}$. Cette application est même injective, par l'axiome d'extentionalité que U doit satisfaire. Mais on n'a pas de surjectivité. A un ensemble intuitif de points de U ne correspond pas nécessairement un point de U qui soit relié par $\in^{\mathrm{U}}$ très exactement aux points de cet ensemble intuitif.

Un univers U est caractérisé par deux choses d'une part ses ordinaux, qui donnent sa hauteur, d'autre part l'opération $\mathcal{P}$ de prise des parties, qui fournit l'épaisseur de U.

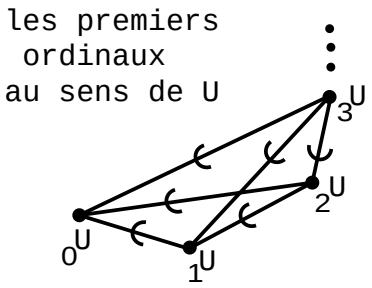
Un ordinal est un ensemble a tel que si $x \in y \in a$, alors $x \in a$, et si $x \in a$ et $y \in a$, alors ou bien $x \in y$, ou bien $x = y$, ou bien $y \in x$. La relation $\in$ est donc un ordre total sur a, qui est un bon-ordre, c'est-à-dire est tel que tout sous-ensemble non vide a un plus petit élément pour l'ordre. On obtient, à partir de l'ensemble vide (qui est un ordinal) tous les ordinaux par les opérations suivantes :

Si a est un ordinal, $a \cup \{a\}$ est un ordinal, appelé le successeur de a,

Si X est un ensemble d'ordinaux, $a = \bigcup_{x \in X} x$ est un ordinal.

Par exemple, les premiers ordinaux sont $\emptyset$ (noté aussi 0), puis son successeur $\{\emptyset\}$, noté aussi 1, puis $\{\emptyset, \{\emptyset\}\} = 2$, etc... Le premier ordinal autre que $\emptyset$ qui n'est pas successeur, et qui existe par l'axiome de l'infini, est l'ensemble, noté ω , des entiers $\omega = \{0, 1, 2, \ldots\}$.

Ces notions ont un sens dans U (qui est modèle de la théorie des ensembles).



A chaque entier correspond un entier $n^{\mathtt{U}}$. Que dire de l'ensemble intuitif $\{0^{\mathtt{U}}, 1^{\mathtt{U}}, 2^{\mathtt{U}}, \ldots\}$? On s'attendrait qu'il corresponde à l'ordinal $\omega^{\mathtt{U}}$. Pourtant il n'en est rien en général cet ensemble intuitif peut très bien ne correspondre à rien dans U, et l'ensemble $\omega^{\mathtt{U}}$ être relié à d'autres objets de U (qu'on appelle alors entiers non standards de U).

Une fois que les ordinaux de U sont connus, on définit pour chaque ordinal α de U un élément $\mathtt{U}_\alpha$ de U par les clauses

$$\mathtt{U}_0 = \emptyset^{\mathtt{U}}$$
$$\mathtt{U}_\alpha = [\mathcal{P}(\textstyle\bigcup_{\beta \in \alpha} \mathtt{U}_\beta)]^{\mathtt{U}}$$

i.e. on obtient $\mathtt{U}_\alpha$ en prenant,au sens de U, la réunion des $\mathtt{U}_\beta$ déjà construits, puis l'ensemble des parties de cette réunion. Qu'une telle définition

par récurrence soit possible est une propriété fondamentale des ordinaux. Et on peut montrer qu'on obtient ainsi tout l'univers U, au sens suivant : un élément de U apparaît comme élément (au sens de U) de l'un des U_α.

4. La construction de Gödel

Reprenons l'exemple de la théorie des corps et du modèle $\mathbb{R}$. Comment, à partir de ce modèle, en construire un autre ? A priori, nous devons choisir une addition et une multiplication. Mais si on veut travailler à l'économie, on peut essayer de garder ces opérations, et ne changer que l'ensemble de base. Et notre souci d'économie nous amène à construire le corps $\mathbb{Q}$. (En effet un sous-corps de $\mathbb{R}$ doit contenir 0 et 1 donc les entiers, donc les entiers relatifs et leurs inverses, donc tous les rationnels.)

Essayons la même idée avec notre univers U. Nous n'allons pas changer la relation d'appartenance $\in^{\mathrm{U}}$ (et donc mettre dans U', avec un élément x, tous ses éléments au sens de $\in^{\mathrm{U}}$). Les ordinaux de U étant définis de façon très intrinsèque à partir de $\in^{\mathrm{U}}$, décidons aussi de conserver les ordinaux. Par contre, nous allons essayer de jouer sur l'opération $\mathcal{P}$ pour diminuer au maximum l'"épaisseur" de l'univers.

Le problème est donc soit x un élément de U que nous avons décidé de conserver dans U' . Quelles parties de x (au sens de U) devons-nous également conserver ? La réponse est fournie par les axiomes de compréhension : nous devons mettre dans U' toutes les sous-parties de x qui sont définies par des formules (avec paramètres mis dans U').

Ceci donne l'idée d'imiter la construction inductive des U_α - qui fournit U - mais en définissant maintenant des L_α avec

$$\begin{aligned} L_{\alpha+1} = \ & \{y \subset^{\mathrm{U}} L_\alpha \mid y = \{z \in^{\mathrm{U}} L_\alpha \ \&\ \varphi(z, a_1, \ldots, a_n)\}^{\mathrm{U}}, \\ & \quad \text{pour une formule } \varphi \text{ et des paramètres } a_1, \ldots, a_n \in^{\mathrm{U}} L_\alpha\}. \end{aligned}$$

La définition qui précède est incorrecte : l'ensemble défini est intuitif, et doit être remplacé par un élément de U, ce qui est possible mais délicat, une définition précise des L_α peut être trouvée dans le livre de J.L. Krivine [10]. Mais l'idée de la construction de Gödel est bien celle que nous venons d'indiquer. Et il se trouve que l'ensemble intuitif, noté généralement L^{U} , obtenu en conservant tous les éléments des L_α est bien

un univers de la théorie des ensembles, appelé univers des ensembles constructibles de U. De plus, par sa construction, L^{U} est le plus petit possible parmi les univers ayant même relation d'appartenance et mêmes ordinaux. Et la construction des constructibles, refaite dans L^{U} , fournit de nouveau L^{U}.

La construction de Gödel permet donc de démontrer la cohérence relative d'un énoncé de la Théorie des Ensembles, l'énoncé V = L. Et par la même occasion, de toutes les conséquences de cet énoncé. Mais on peut prouver que parmi les conséquences de V = L figure l'hypothèse du continu même généralisée en "il n'y a pas de cardinalité intermédiaire entre celle d'un ensemble A et celle de $\mathcal{P}(A)$", ainsi qu'un autre énoncé mathématique très discuté en son temps, l'axiome du choix.

5. La construction de Cohen

Pour construire un modèle de la négation de l'hypothèse du continu, il faut déjà savoir construire un modèle de V $\neq$ L, et par ce qui précède, une diminution de l'univers est inefficace. La méthode de Cohen consiste à l'augmenter, mais là encore, à l'économie partant d'un univers U (que nous pouvons supposer satisfaire V = L), nous allons adjoindre un objet extérieur x, pour fabriquer un nouvel univers U', mais de façon que la relation $\in^{\mathrm{U}'}$, restreinte aux éléments de U, soit la relation $\in^{\mathrm{U}}$ de U (un peu de la même façon que l'on passe de $\mathbb{R}$ à $\mathbb{C}$). Décidons par exemple de rajouter une nouvelle partie de x de ω^{U} . Nous allons certainement devoir mettre dans U' d'autres objets, par exemple $\mathcal{P}(x)$. Comment s'assurer que la plus petite collection U' ainsi obtenue est un modèle de la théorie des ensembles ? L'idée de Cohen est de choisir x de façon à perturber U le moins possible on va essayer de donner à x un minimum de propriétés "particulières" si une propriété des parties de ω^{U} est vraie dans U de "presque toutes" les parties de ω^{U} , alors elle sera vraie dans U' de x. La mise en forme mathématique de cette idée est délicate, mais fournit un modèle U' dans lequel x n'est pas constructible : on prouve ainsi la cohérence relative de V $\neq$ L. La construction de Cohen a l'avantage de pouvoir être appliquée pour fournir un grand nombre de modèles différents. Par exemple, en ajoutant beaucoup de nouvelles parties de ω^{U} à U, on peut obtenir un modèle U' dans lequel $\mathcal{P}(\omega^{\mathrm{U}})^{\mathrm{U}}$ a une cardinalité intermédiaire entre celle de ω^{U} et celle de $\mathcal{P}(\omega^{\mathrm{U}})^{\mathrm{U}'}$, c'est-à- dire un modèle dans lequel

la négation de l'hypothèse du continu est satisfaite. L'étude des modèles qui sont produits par la méthode de Cohen a permis, durant ces vingt dernières années, de montrer qu'un grand nombre d'énoncés mathématiques sont indécidables, touchant (de manière très inégale) de nombreuses branches des mathématiques.

6. Et l'hypothèse du continu ?

La réponse apportée par Gödel et Cohen au problème de Cantor est définitive. Mais elle n'est pas nécessairement convaincante. Gödel lui-même n'en était pas du tout satisfait cette réponse indique en effet plutôt les limites de la formalisation, et une réponse par vrai ou faux est envisageable, à condition d'augmenter les axiomes de la théorie des ensembles. On pourrait bien sûr ajouter comme axiome l'hypothèse du continu elle-même, ou sa négation. Mais que choisir ? Une autre possibilité serait de prendre comme nouvel axiome l'énoncé de Gödel V = L. C'est un énoncé qui a de nombreuses conséquences intéressantes, mais il a le défaut de "diminuer" l'univers d'etude, ce qui, ne serait-ce que d'un point de vue méthodologique, n'est pas du tout satisfaisant. On peut imaginer que l'on propose un jour un nouvel axiome, à la fois naturel et intuitivement vrai, qui résolve l'hypothèse du continu, et que la pratique mathématique d'alors en fasse l'une des "réalités mathématiques" indiscutées. En attendant, on se trouve place devant une pluralité de choix (et ce, pas seulement pour l'hypothèse du continu), avec laquelle nous devons bien vivre.

Sur la calculabilité effective, exemples

Nicolas Bouleau

I. Systèmes formels

Le système formel le plus simple est le "système des allumettes". il est constitué d'un seul signe I et ses assemblages sont des groupes finis de ce signe répété I, II, III, IIII, IIIII,...

L'arithmétique des entiers naturels décrit des lois de ce système formel, elle-même formalisée suivant un système formel : l'arithmétique de Peano.

C'est une théorie du 1er ordre (cf. 1er exposé).

Langage du 1er ordre

a) constante 0

b) fonction unaire S (successeur), fonctions binaires + et .

c) prédicat binaire <

Axiomes.

P1. $Sx \neq 0$

P2. $Sx = Sy \Rightarrow x = y$

P3. $x + 0 = x$

P4. $x + Sy = S(x + y)$

P5. $x.0 = 0$

P6. $x.Sy = (x.y) + x$

P7. $\neg(x < 0)$

P8. $x < Sy \Leftrightarrow x < y \vee x = y$

et le schéma d'axiomes suivant

P9. Si $A(x)$ est une formule admettant x pour variable libre

$A(0)\ \&\ \forall y(A(y) \Rightarrow A(S(y)) \Rightarrow \forall x A(x)$

Est-ce que les théorèmes de cette théorie sont vrais ? Si l'on regarde ce que signifie tel théorème pour notre système des allumettes et si on effectue sur ces dernières les opérations indiquées on constate que ça marche. Par ses conséquences dans toutes les mathématiques, dans la physique et en informatique on peut dire que cette théorie est de loin celle qui a été le plus sévèrement testée.

Une fois convaincu de cela il reste cependant deux questions importantes

1^0) A-t-on en recueillant tous les théorèmes de cette théorie, toutes les propriétés vraies des allumettes qui peuvent s'exprimer dans le langage

utilisé ?

2^0) Existe-t-il un moyen mécanique de savoir si une propriété des allumettes exprimée en ce langage est conséquence des axiomes ou non ?

Je vais tenter de faire comprendre intuitivement comment dans les années trente, les logiciens (Turing, Gödel, Church, Kleene, etc.) ont pu répondre à ces questions.

Prenons un système formel tel que celui de Peano ou celui de Zermelo-Fraenkel. Bien que nous ayons plusieurs règles de déduction à notre disposition, il est possible pour écrire nos théorèmes, de procéder de façon systématique.

En effet, on peut numéroter les symboles de notre langage puis numéroter les termes et les formules et enfin puisque les démonstrations sont des suites finies de formules, chacune reliée aux précédentes par un nombre fini de règles, on peut numéroter les démonstrations[7].

Alors si nous prenons les démonstrations par ordre de numéros croissants, nous passons ainsi en revue tous les théorèmes de notre système.

La chose importante à comprendre est que si nous procédons de cette manière systématique, les théorèmes que nous obtenons successivement sont des énoncés de longueur très variable. Nous n'obtenons pas les théorèmes par ordre de numéros croissants, il se peut en effet qu'une démonstration très longue mène à un théorème assez court pour lequel il n'y ait pas de démonstration plus courte. De telle sorte que si, à l'inverse, nous nous donnons un énoncé a priori et si nous cherchons à savoir si c'est un théorème de notre théorie, il n'y a pas de borne supérieure à la longueur des démonstrations à investiguer pour savoir si notre énoncé est déductible ou non de nos axiomes.

Les logiciens ont alors démontré les résultats suivants

Si le système formel est suffisamment riche (grosso-modo s'il est au moins aussi riche que l'arithmétique de Peano), et s'il n'est pas contradictoire (c'est-à-dire s'il existe des énoncés qui ne sont pas conséquences des axiomes) alors

1) Il n'existe aucun algorithme (c'est-à-dire de méthode programmable sur un ordinateur même de mémoire de capacité infinie) permettant de dire en un temps fini si un énoncé est un théorème ou non.

[7] Voir les exposés de J.-Y. Girard.

2) Il existe même des énoncés tels que ni eux ni leur négation ne sont des théorèmes.

La première propriété s'exprime en logique par le fait que l'ensemble des théorèmes est un ensemble recursivement énumérable non récursif, ou encore en disant que pour un énoncé, le fait d'être un théorème est une propriété semi-définie positive.

Pour faire comprendre cela intuitivement prenons une analogie et considérons un ouvrier chargé d'examiner un lot infini de pommes passant devant lui sur un tapis roulant. Si d'aventure il rencontre une pomme véreuse alors il est sûr qu'il y a des pommes véreuses dans le lot, mais si nous imaginons que l'ouvrier ne rencontre jamais de pommes véreuses alors l'ouvrier ne saura jamais s'il y a des pommes véreuses ou non dans le lot. C'est moins trivial qu'il n'y paraît si l'on pose maintenant la question existe-t-il un groupe de 10 zéros à la suite dans les décimales de $\sqrt{2}$? Si l'on découvre une telle suite, la réponse est positive, si on n'en trouve pas on ne sait pas répondre à la question.

A moins que l'on ne dispose par bonheur d'une theorie dont un des théorèmes dit justement "Il existe dans les décimales de $\sqrt{2}$ un groupe de 10 zéros à la suite". On ne connaît pas actuellement de tel théorème et on est donc obligé de passer en revue les théorèmes et si l'on ne trouve jamais de tel théorème on est dans la même situation qu'avant.

Ce type de réflexion se rattache historiquement à l'intuitionisme que je ne puis aborder maintenant.

La deuxième propriété s'énonce en disant que le système est incomplet. Historiquement le premier énoncé d'arithmétique ni prouvable ni réfutable fut découvert par Rosser améliorant un travail préalable de Gödel. A noter que quoique formellement indécidable cet énoncé est intuitivement vrai. Il en est de même pour la traduction dans le langage de l'arithmétique de l'assertion "L'arithmétique est non contradictoire". Cet énoncé n'étant pas réfutable on peut évidemment l'ajouter comme nouvel axiome sans risque nouveau de contradiction. Cependant la nouvelle théorie obtenue aura les mêmes tares d'indécidabilité et d'incomplétude que l'ancienne.

II. Fonctions récursives

On peut démontrer dans ZF le théorème suivant

Théorème. *Pour presque tout réel $\theta > 1$ pour la mesure de Lebesgue, la suite $a_n =$ reste de θ^n modulo 1, est équirépartie sur $[0,1]$,*
C'est-à-dire si $[a,b] \subset [0,1]$

$$\lim_{N\uparrow\infty} \frac{\textit{nombre des } a_n \in [a,b] \textit{ pour } n \leq N}{N} = b - a.$$

Ce qui est chagrinant par ailleurs c'est qu'on ne sait citer concrètement aucun nombre $\theta > 1$ qui vérifie la propriété.

On a un théorème d'existence mais ce théorème ne permet pas de construire effectivement un objet dont on affirme l'existence.

Un nombre θ réel en base 2 est une application de $\mathbb{N}$ dans $\{0,1\}$, quand pourra-t-on dire qu'une application de $\mathbb{N}$ dans lui-même est effectivement calculable ? Une réponse à cette question est donnée par la théorie des fonctions récursives.

Comme la notion de fonction "effectivement calculable" est intuitive et un peu floue, les mathématiciens lui préfèrent une notion plus précise (a priori plus restreinte) de fonction recursive.

Les fonctions récursives d'entiers à valeurs entières sont définies de la façon suivante

1) les projections de $\mathbb{N}^n$ dans $\mathbb{N}$ sont récursives.

$$(a_1, \ldots, a_i, \ldots, a_n) \mapsto a_i$$

2) les fonctions de 2 variables

$$\begin{array}{c} . + . \\ . \times . \\ 1_{\{.<.\}} \end{array}$$

sont récursives[8]

3) si $G, H_1, \ldots, H_n$ sont récursives la fonction composée $G(H_1, \ldots, H_n)$ est récursive.

[8] La notation 1_A désigne la fonction indicatrice de l'ensemble A : elle vaut 1 au point x si x est dans A, zéro sinon.

4) si $G(a_0, a_1, \ldots, a_n)$ est récursive et si G vérifie

$$\forall a_1, \ldots, \forall a_n, \exists a : G(a, a_1, \ldots, a_n) = 0$$

la fonction

$$F(a_1, \ldots, a_n) = \text{ le plus petit } a \text{ tel que } G(a, a_1, \ldots, a_n) = 0$$

est recursive.

Je vous renvoie aux livres sur la calculabilité effective où sont développés de proche en proche des exemples de fonctions récursives pour vous convaincre de ce qu'on appelle la thèse de Church, c'est-à-dire du fait que les fonctions effectivement calculables sont exactement les fonctions récursives.

Nous dirons qu'un sous-ensemble de $\mathbb{N}$ est récursif si sa fonction indicatrice est récursive.

Il est clair que par application successives des règles 1) 2) 3) 4) on obtient un ensemble dénombrable de fonctions : l'ensemble des fonctions récursives est dénombrable. Au demeurant la numérotation des fonctions récursives ne peut elle-même être récursive, par un argument diagonal simple : s'il existe une fonction récursive $h(m, n)$ telle que lorsque m varie les fonctions $n \mapsto h(m, n)$ soient toutes les fonctions récursives d'une variable, la fonction $n \mapsto h(n, n)+1$ serait récursive et ne serait pas dans la liste.

La particularité d'un ensemble non récursif A est qu'il n'existe aucun algorithme permettant de répondre à la question

$$n \in A \ ?$$

c'est-à-dire de méthode de calcul qui appliquée à n répondra en un nombre fini d'étape à la question $n \in A$?

Les fonctions récursives permettent de préciser la notion de "propriété semi-définie positive" grâce à la notion rigoureuse d'"ensemble récursivement énumérable" : si $n \mapsto f(n)$ est récursive, l'image de la fonction f, c'est-à-dire l'ensemble $\{n \mid \exists m \ f(m) = n\}$ est un ensemble récursivement énumérable. On peut montrer que c'est une classe d'ensembles plus vaste que celle des ensembles récursifs. Si A est un ensemble récursivement énumérable non récursif, alors la question $n \in A$? est semi-définie positive : si $n \in A$ un calcul effectif nous le dira en un temps fini, mais si $n \notin A$,

il faut passer en revue tous les entiers pour s'assurer qu'aucun ne donne n comme image par f.

Ainsi l'application d'un quantificateur existentiel devant une propriété récursive $P(m,n)$ donnant $\exists m P(m,n)$ conduit à des ensembles de plus grande complexité.

Le phénomène est analogue au fait que la projection sur $\mathbb{R}$ d'un borélien de $\mathbb{R}^2$ n'est pas en général un borélien (mais un ensemble analytique comme l'a montré Souslin, contrairement à ce que Lebesgue avait cru pouvoir affirmer).

En revanche, on peut montrer que si A et son complémentaire sont récursivement énumérables alors ils sont en fait récursifs.

Un des résultats les plus célèbres et lié à ce que j'évoquais au début de l'exposé est le suivant

Théorème de Church.

Considérons une numérotation effective des théorèmes d'une théorie non contradictoire qui contienne l'arithmétique alors l'ensemble des théorèmes est non récursif.

III. Exemples

Nous allons maintenant donner quelques exemples de problèmes récursivement insolubles.

a) Dixième problème de Hilbert.

Hilbert au congrès international des mathématiciens à Paris en 1900 proposait à la postérité une liste de 23 problèmes dont la solution à son avis risquait de faire avancer les mathématiques.

Le 10e problème a trait aux équations diophantiennes, c'est-à-dire la résolution en nombres entiers d'équations polynomiales à coefficients entiers par exemple du type

$$4x^2 - xy^3 + 7z^5 + 1 = 0.$$

La question posée par Hilbert était la suivante

Existe-t-il un algorithme permettant de dire si une équation diophantienne admet une solution ou non ?

Hilbert s'intéressait à ce problème et attachait de l'importance à la notion d'algorithme dès cette époque.

Il s'agit donc de trouver une méthode permettant pour tout polynôme à coefficients entiers, $P(x_1, \ldots, x_n)$ de dire s'il existe n nombres entiers $a_1, \ldots, a_n$, tels que $P(a_1, \ldots, a_n) = 0$ ou non.

La réponse a été résolue par la négative par Yu. V. Matiyassevic en 1970, prolongeant les travaux de Putnam, Davis et Julia Robinson.

La démonstration permet de montrer le résultat plus précis suivant :

Il existe un polynôme de 10 variables à coefficients entiers

$$U(a, x_1, \ldots, x_9)$$

tel qu'il n'existe aucun algorithme pour dire si les équations

$$n \textit{ fixé} \quad U(n, x_1, \ldots, x_9) = 0$$

ont des solutions entières ou non.

Et comme sous-produit de la démonstration on obtient aussi l'existence d'un polynôme de 10 variables à coefficients entiers dont l'ensemble des valeurs prises lorsque les variables parcourent les entiers est exactement l'ensemble des nombres premiers.

Enfin, en traduisant le fait qu'on peut démontrer dans ZF la non-contradiction du système de Peano, on obtient le résultat suivant :

Il existe un polynôme de plusieurs variables à coefficients entiers P (que l'on pourrait écrire explicitement) pour lequel c'est un théorème de ZF que l'équation $P = 0$ n'a aucune solution entière, mais pour lequel cette assertion n'est pas démontrable dans l'arithmétique de Peano.

La théorie ZF améliore donc notre connaissance de l'arithmétique, nous reviendrons sur ce point en conclusion.

b) Le problème des mots pour un semi-groupe.

On considère le semi-groupe libre à 2 générateurs c'est-à-dire les mots formés de 2 lettres a et b

$$a, b, aa, ab, aba, \ldots, abbabab, \ldots$$

muni de la loi de composition qui est la juxtaposition sans parenthèses donc associative.

Nous désignons les mots par des lettres majuscules. On définit alors une relation d'équivalence sur l'ensemble des mots de la façon suivante :

On prend deux mots $A = abbabab$ et $B = aaba$ par exemple et on pose

$$A \equiv B \quad \text{(c'est l'axiome)}$$

et on impose les règles suivantes entre mots

$$\begin{aligned} C \equiv C' &\Rightarrow CD \equiv C'D \\ C \equiv C' &\Rightarrow EC \equiv EC' \\ FGH \equiv FG'H &\Rightarrow G \equiv G' \end{aligned}$$

Alors on peut montrer que:

Il existe des axiomes en nombre finis

$$A_1 \equiv B_1, \ldots, A_n \equiv B_n$$

(qu'on peut écrire effectivement) tels qu'il n'existe aucun algorithme permettant de résoudre la question

$$E \equiv F \ ?$$

entre deux mots quelconques.

c) Linguistique formelle.

Je renvoie pour les détails à Davis M., "Unsolvable problems",in *Handbook of Mathematical Logic* Barwise editor North Holland 1978.

Il n'y a pas d'algorithmes pour dire si deux grammaires sans contexte permettent une phrase commune ou non.

Une grammaire est dite ambiguë si elle permet des phrases ambiguës c'est-à-dire dont la structure grammaticale peut être de deux types différents. Par exemple la phrase

"Pourquoi crois-tu que Walesa est en prison ?"

est ambiguë. Si pourquoi se rapporte au groupe "Walesa est en prison" elle recevra une réponse du type :
Réponse : parce que les autorités ont jugé qu'il était dangereux. Si pourquoi se rapporte au groupe "crois-tu" elle recevra une réponse du type
Réponse : parce que c'est ce que dit la presse.
Il n'y a pas d'algorithme permettant de dire si une grammaire formelle est ambiguë ou non.

d) Autre exemple.
Il n'y a pas d'algorithme permettant de dire si deux variétés de dimensions 4 sont homéomorphes ou non.

e) En revanche des théories plus faibles que l'arithmétique (dans lesquelles on ne peut pas faire la théorie des fonctions récursives ou celle des machines de Turing) peuvent être décidables, c'est le cas pour la théorie de l'addition de Presburger. Cette théorie a le même langage que l'arithmétique de Peano excepté la fonction binaire .×., et les mêmes axiomes exceptés P5 et P6.
Dans cette théorie l'ensemble des théorèmes est récursif. Il existe un algorithme permettant de dire en un temps fini si une formule du langage est un théorème ou non. Un énoncé est soit prouvable soit réfutable (i.e. sa négation est prouvable) : la théorie est complète. Il existe une méthode finitiste permettant de montrer que cette théorie est non contradictoire.

IV. Quelques commentaires philosophiques : l'exemple et l'argument

Il est toujours assez hasardeux de tirer des conséquences philosophiques de travaux scientifiques, d'une part ces commentaires sont parfois de peu d'utilité pour la recherche scientifique elle-même, d'autre part c'est leur nature, semble-t-il, de vieillir assez rapidement.
Si je m'y risque ici c'est pour critiquer quelque peu des conceptions philosophiques précisément fondées sur une certaine image de la science et des mathématiques en particulier.
Une question qui a fait couler beaucoup d'encre depuis le 17e siècle est de concilier la fécondité du raisonnement mathématique avec sa nature rigoureuse. Les références sont abondantes, on peut citer, par exemple,

Pascal, Kant, Poincaré, les positivistes logiques (Carnap, etc.).

La découverte de l'indécidabilité éclaire ce problème d'un jour nouveau. Il faut dire à ce sujet que si, de 1930 à la guerre, les positivistes logiques avaient bien "assimilé" la formalisation des mathématiques découverte 20 ans plus tôt, il n'en va pas de même pour les questions relatives à l'indécidabilité qui fut élucidée pour une large part par des mathématiciens (Gödel, Tarski) liés au cercle de Vienne lui-même. Des leçons de ces travaux ne seront tirés qu'après la guerre chez Putnam, Quine, voire Chomsky, etc.

A. Lorsqu'un mécanisme combinatoire est assez simple, on peut dire que tous les assemblages qu'il engendre sont "contenus" dans ses hypothèses et ses règles de formation, il ne réserve en vérité aucune surprise et une connaissance rationnelle peut l'embrasser globalement.

Au contraire lorsque le mécanisme atteint un certain niveau de complexité (caractérisé par le fait que ses "outputs" forment un ensemble non récursif) alors il n'existe aucune méthode de connaissance certaine des résultats de ces mecanismes autre que l'expérimentation du mécanisme lui-même[9].

On ne sait pas quels sont les théorèmes de l'arithmétique, on ne connaît que des exemples de tels théorèmes.

On peut dire en quelque sorte que le système quoique purement mécanique est d'une complexité suffisante pour que son développement engendre en permanence des surprises.

Dans la dualité classique entre déterminisme et hasard un troisième terme intervient qui est l'indécidable. Et pour reprendre l'image tant commentée de Laplace : on pourrait dire que, quand bien même seraient connues toutes les positions des molécules de l'univers et les champs de forces agissant sur elles que, sans qu'aucun hasard n'intervienne, leurs combinaisons ne cesseraient de nous réserver des surprises.

Plusieurs auteurs contemporains dont Edgar Morin par exemple ont vu

[9]ou d'un autre mecanisme, lié au précédent ou le contenant, Cette nuance est épistémologiquement importante dans la mesure où les systèmes formels que sont AP ou ZF sont considérés par tous les mathématiciens comme absolument fiables. Cette conviction solide ne s'appuie évidemment pas sur une preuve formelle, sur quoi se fonde-t-elle ? Il serait long de l'analyser. En tout cas ne pas croire à la cohérence de ZF risque fort d'être une attitude mathématiquement stérile. Le bon choix est de faire le pari, c'est l'argument pascalien avec cette différence qu'ici on y gagne même en ce bas monde.

l'importance de la complexité dans les problèmes épistémologiques (de la biologie surtout : ontogenèse et phylogenèse). Hélas, cette littérature est assez confuse et les liens avec les systèmes formels ne sont pas clairement dégagés de tout le fourbi thermo-dynamico-informationnel. Cependant d'importants travaux récents (Kolmogorov, Rabin, Blum, Constable, Chaitin, etc) tendent à préciser cette notion de complexité.

B. Revenons aux mathématiques, ce que nous avons dit à l'instant pourrait faire conclure qu'épistémologiquement c'est l'exemple qui est le plus fort. Cependant les choses ne sont, là encore, pas si simples. Nous ne savons pas manier les systèmes formels en eux-mêmes sans attribuer une signification aux symboles[10]. Nous réussissons mieux à faire de la théorie que de la combinatoire. C'est là que l'argument reprend sa place.

Plutôt que de chercher vainement une démonstration de telle conjecture arithmétique, on peut avec peut-être plus de succès tenter de construire une théorie mathématique plus puissante que l'arithmétique dans laquelle on a une bonne confiance et de regarder les propositions arithmétiques qu'elle permet de démontrer (cf. III in fine). C'est une des raisons qui poussent certains logiciens contemporains à rechercher des axiomes nouveaux à adjoindre à ZF, souvent ces axiomes sont d'un même type : axiomes de l'infini. Ils postulent l'existence d'un cardinal très grand. Ces axiomes permettent de démontrer des théorèmes d'arithmétique qu'on ne sait pas démontrer dans le système de Peano ni même dans ZF.

Dans cette course aux cardinaux très grands le risque évident est de viser trop haut et d'aboutir à une théorie contradictoire.

On peut dire en quelque sorte que les théories les plus fructueuses semblent être parmi celles qui prennent le plus de risques vis-à-vis du problème de non contradiction. On trouve une situation analogue à celle que décrit Popper à propos des sciences de la nature lorsqu'il dit qu'entre deux théories la plus intéressante est celle qui prend le plus de risques vis-a-vis des sanctions de l'expérience.

Mais la discussion ne s'arrête pas là. Les théories ne se laissent pas classer en ordre linéaire. Il y a des façons non comparables d'exprimer

[10] Il n'est pour s'en convaincre que d'écrire et d'essayer de démontrer sans aucune abréviation dans le langage de ZF que la limite uniforme d'une suite de fonctions réelles continues est continue.

qu'un cardinal est grand. Et de même, pour les autres sciences l'initiative revient au chercheur et c'est à lui d'assumer les risques engendrés par son activité.

Bibliographie

I - Un livre de vulgarisation sur les mathématiques et leurs problèmes historiques, philosophiques et épistémologiques
[1] R. HERSH & Ph. J. DAVIS *The Mathematical Experience*, Birkhäuser Boston 1980.

Il - Livres introductifs
[2] M. COMBES *Fondements des mathématiques*, P.U.F. coll. sup. 1971.
[3] B.C. LYNDON *Notes on logic* Von Nostrand 1964.

III - Livres généraux
[4] S.C. KLEENE *Introduction to Metamathematics*, North Holland 1952. (Le livre du même auteur *Mathematical logic*, Wiley 1967 - traduit en français chez A. Colin est moins riche).
[5] SHOENFIELD *Mathematical Logic* Addison Wesley 1967.
signalons également l'ouvrage collectif
[6] BARWISE & al., *Handbook of Mathematical Logic* North Holland 1978.
où l'on trouvera des bibliographies détaillées.

IV Grandes branches de la logique
A. Théorie de la récursivité
Les références sont très nombreuses, un classique est le livre de
[7] M. DAVIS, *Computability and unsolvability* Mc Graw Hill 1958.
voir également [5] et les bibliographies de [6].

B. Théorie des modèles
[8] CHANG & KEISLER, *Model Theory* North Holland 1973.
[9] BELL & SLOMSON, *Models and Ultraproducts, an introduction* North Holland 1974.

C. Théorie des ensembles
[10] J.L. KRIVINE, *Théorie axiomatique des Ensembles* P.U.F. 1972.

D. Théorie de la demonstration
voir [6] et [12] [13] [14] ci-dessous.

V - Références relatives aux cinq conférences

A. L'exposé sur la formalisation des mathématiques utilise abondamment l'étude historique de

[11] M. GUILLAUME "Axiomatique et logique" in *Abrégé d'histoire des mathematiques* Tome II, J. Dieudonné Hermann 1978.

B. A propos des exposés de J.Y. GIRARD on pourra consulter

[12] K. GÖDEL "Ueber formale unentscheidbare Sätze der Principia Mathematica und verwandter Systeme" Monatshefte für Math. und Physik. 38, pp 173 - 198, 1931.
[13] C. GENTZEN "Die Widerspruchfreiheits beweise der reine Zahltheorie" *Math. Ann.* 112 p 493 - 595 (1936)
[14] G. KREISEL "A survey of Proof theory" *J. of symb. logic*, vol. 33 (1968).
"A survey of Proof theory II" *Proc. of the 2d scandinavian logic symp.* Feustad ed. North Holland (1971).

C. Au sujet de l'exposé d'Alain LOUVEAU sur l'hypothèse du continu on pourra consulter les textes originaux suivants

[15] K. GÖDEL, "The consistency of the axiom of choice and the generalized continuum hypothesis". *Proc. Nat. Acad. Sci. USA*, 24, pp 556-557 (1938).
[16] P. COHEN *Set Theory and the Continuum Hypothesis* Benjamin 1966.
ainsi que les cours sur la théorie du forcing :
[17] J.L. KRIVINE *Théorie des ensembles* Cours du 3e cycle multigraphie 1970.
[18] S. GRIGORIEFF & J. STERN *Théorie et pratique du forcing* Cours du 3e cycle multigraphié Université Paris VII.

D. Sur la calculabilité effective on pourra consulter

DAVIS, MATIYASSEVITCH, J. ROBINSON *Procedings of symp. in pure math.* vol. 28 pp 323-378 (1976).
M. MARGENSTERN "Le théorème de Matiyassevitch et résultats connexes" preprint.
un aperçu des recherches récentes sur la complexité est donné dans

J.E. HOPCROFT, J.D. ULLMAN *Introduction to Automata Theory, Languages and Computation* Addison - Wesley (1979).