Les théorèmes dits « d'incomplétude » de Kurt Gödel

Mathématiques souterraines n°1

(21–22 décembre 2019)

« Vrai » ; « faux » ; « démontrable » ; « réfutable ». « Faux », c'est quand la négation est vraie. « Réfutable », c'est quand la négation est démontrable.

Il semblerait qu'on ait tout dit ; et pourtant non, car il manquait « non démontrable », pour quoi nos langues n'ont même pas de mot. Il paraît bien que ce cas n'était pas prévu par la pensée mathématique. Souvent l'absence de nom signale une obscurité. Je propose d'aller au cœur de ces ténèbres conceptuelles.

Je ne parlerai pas d'épistémologie ni d'histoire : ceci est un exposé de mathématiques. Contraint par le cadre à éluder les points techniques, je tenterai pourtant de faire passer des idées rigoureuses et précises.

---

1. Introduction

Platonisme

Mais d'abord je veux annoncer le point de vue adopté dans la suite : l'*algébrisme est un réalisme.* Les objets mathématiques existent et nous tentons de les décrire. Quand on débute en mathématiques et qu'on découvre le pouvoir du formalisme, on s'éprend des fondements ; on croit qu'on « construit » $\mathbb{R}$. Puis on vieillit et peut-être le platonisme est-il une attitude acceptable. C'est du moins la mienne. Le rôle du mathématicien n'est pas d'enchaîner les jeux formels, et le critère ultime en faveur de son activité n'est pas la cohérence interne, mais bien la pertinence, c'est-à-dire son pouvoir explicatif et prédictif. Car les mathématiques sont, aussi, une science.

Admettez donc le temps de cet exposé ou le restant de votre vie que la réalité mathématique existe ; inaccessible aux sens elle l'est à l'entendement. La réalité ultimement nous échappe, mais nous en captons des fragments. En mathématiques l'essence paraît précéder : et l'objet intemporel est trivialement antérieur à nos descriptions humaines et partielles. Et quel meilleur endroit qu'ici pour évoquer l'allégorie de la Caverne ?

Le rôle de l'axiomatique

Il existe une Vérité, par instants perçue par l'intuition. Les mathématiques, disait Vladimir Arnold, forment la branche de la physique où les expériences ne coûtent guère. Ce sont des expériences mentales, mais qui forment pourtant la base de notre pratique ; en cela les mathématiques ne se distinguent pas des autres sciences.

Mais comment se convaincre soi-même et les autres de la justesse de ces expériences mentales ? Par la démonstration, qui bien conduite en garantit la reproductibilité, seul critère de validité comme en les autres sciences. Je laisse ici de côté ces démonstrations qui « n'expliquent rien » :

celles-là convainquent de la seule solidité de l'énoncé, sans valeur élucidatrice. La bonne démonstration sert de support à l'intuition, et la guide à travers les paysages conceptuels parcourus par d'autres, ou par soi, pour l'amener au but.

Axiomatiser un objet mathématique n'est donc pas inventer l'arbitraire d'un jeu d'énoncés ; c'est en peignant d'après nature tenter d'en dégager des traits pertinents, qui serviront dans les démonstrations.

But de l'exposé

J'entends ainsi dans ce exposé montrer quelques relations entre des concepts apparemment non-mathématiques, comme « démontrable » et « vrai ». Pour que ces liens soient rigoureux, déjà faut-il que les notions le soient. Je vais donc proposer des définitions mathématiques de la vérité, et de la démontrabilité.

Pour le serein platonisme, la définition mathématique est descriptive et non prescriptive : les réels n'ont pas besoin d'être « construits » mais observés, car ils existent et nous importent. Ainsi desdits concepts. Et j'en profite pour maudire ici les promoteurs du mot « méta-mathématique », dont la fortune doit tout à ses balancements sonores.

2. Le concept de modèle

Les liens entre « démontrable » et « vrai » ne sont pas si naïfs. Un légitime espoir est que tout ce qui se démontre, soit vrai.

Caractère relatif de la vérité

> Voici un premier exemple. Si $x^2 = -1$, alors $x = \pm i$. En effet factorisons $x^2 + 1$ en $(x + i)(x - i)$; comme $\mathbb{C}$ est intègre, on a $x = i$ ou $x = -i$.
>
> Cette démonstration d'un énoncé vrai est rigoureuse. Et pourtant soit x un quaternion unitaire imaginaire, par exemple $x = j$; alors $x^2 = -1$.

Les nombres complexes vérifient un certain énoncé, que les quaternions ne vérifient pas. Ceci montre que le concept de vérité est *relatif* à un objet mathématique donné. La formalisation de la vérité fut effectuée par Alfred Tarski dans les années 20–30 seulement. Cette vérité « locale » est longtemps restée inaperçue en raison de son évidence même.

La définition précise *décrit* les liens entre ce que nous pensons, et ce qui est : la théorie de la vérité est une théorie de l'adéquation entre la réalité et nos opinions.

> On dit que $a \cdot b = c$ est vraie si le résultat de a multiplié par b vaut c. On dit que non-P est vraie si P n'est pas vraie. On dit que P et Q est vraie si P et Q sont vraies. On dit que $\exists x\ P$ est vraie s'il existe x tel que P soit vraie.
>
> Les autres cas (ou, implique, pour tout) sont à l'avenant ; c'est donc une simple récurrence sur la structure des énoncés.
>
> Notez que le rôle des quantificateurs explique le caractère relatif de la chose : ainsi $\mathbb{R}$ ne vérifie *pas* qu'il existe une racine carrée à -1, alors que $\mathbb{C}$ le vérifie.

Je reviendrai plus tard sur une restriction fondamentale, mais veux d'abord illustrer la force de ce point de vue.

Les parallèles

Considérons les axiomes d'Euclide pour le plan, dont j'ai oublié la liste. Peut-on démontrer le postulat des parallèles ? En voici un équivalent moderne :

> Un point et une droite étant donnés sans incidence, il existe passant par le point au plus une droite évitant la première.

La question de la redondance fut envisagée par des esprits brillants ; on ne saurait prendre à la légère les efforts d'Adrien-Marie Legendre.

Et pourtant le plan hyperbolique $\mathbb{H}$ pourvu de ses géodésiques vérifie les premiers axiomes d'Euclide, mais pas le postulat des parallèles. Or si le postulat était démontrable à partir des autres axiomes, $\mathbb{H}$ le vérifierait : ce qui n'est pas.

C'était votre première preuve d'indépendance. La terminologie du XX^{e} siècle dira que les axiomes sont *incomplets*. Celle du XXI^{e} retiendra que le demi-plan de Poincaré est un *modèle* des axiomes d'Euclide sans le postulat incriminé. C'est un concept central pour la suite.

> Une structure $\mathbb{S}$ est *modèle* d'un ensemble d'énoncés E_i s'il vérifie chacun d'eux.

3. La notion de preuve

J'ai admis lors de parler du plan hyperbolique, que si un énoncé se démontre, alors il est vrai. Je vais à présent rendre précis ce principe.

Arbres de preuve

La notion de vérité est celle de Tarski ; celle de preuve a été formalisée dans les années 30 par Gerhard Gentzen. Dans son formalisme une preuve est un arbre ; aux feuilles on met les axiomes ; aux nœuds on respecte des règles de construction données ; la racine de l'arbre est alors démontrée. L'écriture humaine est linéaire par accident ; intrinsèquement la preuve est arborescente.

> La mention d'un axiome est une preuve. Pour prouver P et Q on prouve P et Q. Pour prouver non-P on montre que P donne une contradiction. Pour prouver P implique Q on suppose P et l'on montre Q. Pour prouver $\exists x\ P$ on produit un x pour lequel P est prouvée.
>
> La négation est un point délicat. Si l'on a prouvé non-non-P, on a prouvé P : ce qui reflète le comportement de la valeur de vérité. L'effet de cette *démonstration par l'absurde* sur l'existentiel est qu'on peut aussi montrer $\exists x\ P$ en montrant non-$\forall x$-non-P ; la preuve n'est alors pas constructive par opposition à la stratégie première, et peut-être à l'intuition naïve de ce qu'est une preuve.
>
> (Certaines hérésies contestent ce dogme et mènent à d'autres notions de preuve. Pareil à l'historien des religions dans son étude, le logicien ne doit statuer ni choisir, mais bien considérer les *relations* qu'entretiennent ces diverses notions.)

Noter que la prouvabilité d'un énoncé est toujours relative à un jeu d'axiomes. Une analogie triviale et vive est de comparer les règles de preuve aux recettes, et les axiomes aux ingrédients.

On a bien formalisé la notion de preuve par simple récurrence sur des arbres finis. Cette formalisation est ainsi mécanisable, mais sa complexité interdit de l'employer *pour trouver du nouveau.*

Correction

À présent que vérité et démontrabilité sont des notions précises, toutes deux définies par une récurrence naïve, nous pouvons énoncer le théorème employé lors de la discussion géométrique.

> Si une structure $\mathbb{S}$ vérifie les axiomes A_i et que l'énoncé E est prouvable à partir des A_i, alors $\mathbb{S}$ vérifie E.

Et cela se démontre, par récurrence sur l'arbre de preuve.

Intermède

En vue d'élucider les liens entre « démontrable » et « vrai », nous avons formalisé les deux notions, nous en avons donné une description entrant dans le cadre de la définition mathématique. La preuve est un certain type d'arbre, bâti sur des axiomes. La vérité est toujours relative à une structure. Ce qui se démontre est vrai, dans un sens rendu précis. Tout jusqu'ici n'était que trivialité.

---

4. Complétude

Question mal, puis bien posée

La question de la réciproque est naturelle.

> Si la structure $\mathbb{S}$ vérifie les axiomes A_i et l'énoncé E, peut-on démontrer E à partir des A_i ?

La question est évidemment mal formulée. On a pu oublier les A_i. Par exemple le plan euclidien vérifie que tout point est un point, et le postulat des parallèles, mais on ne saurait en établir une preuve à partir d'une tautologie.

Il manque en fait dans la question un parfum de *nécessité*, l'idée que les A_i *ne peuvent pas se produire sans* E. C'est en fait une quantification sur $\mathbb{S}$: et nous amendons la question.

> Si *toute* structure $\mathbb{S}$ qui vérifie les axiomes A_i vérifie aussi l'énoncé E, peut-on démontrer E à partir des A_i ?

Le premier fait d'armes de Kurt Gödel est d'avoir établi la réponse positive.

Deux notions de conséquence

Ce théorème dit « de complétude » parfait l'équivalence entre preuve et de vérité. On n'oubliera pourtant pas le besoin de quantifier sur les structures. Deux notions rivales de conséquence étaient en jeu :

— la conséquence *de facto* : chaque fois qu'on a les A_i, on doit avoir E ;

— la conséquence *de jure* : en partant des A_i on peut démontrer E.

Ces deux notions n'en font qu'une. Je reformule ainsi le théorème.

> L'énoncé E est prouvable à partir des axiomes A_i si et seulement si tout modèle des A_i est également modèle de E.

Mais ici je vous dois une précision d'importance.

5. La logique élémentaire

J'ai mentionné en § 2 une restriction fondamentale sur la classe des énoncés pris en compte. Ils seront dits *élémentaires* car ils ne porteront que sur les éléments. Quand j'ai défini précédemment la vérité (relative) d'un énoncé, je vous devais une élucidation du concept même d'énoncé : la voici.

> *On ne permet pas la quantification ensembliste.*
>
> Les expressions de base comme $a \cdot b = c$ sont des énoncés élémentaires. Si P est un énoncé élémentaire, non-P aussi. Si P et Q sont des énoncés élémentaires, P et Q aussi. Si P est un énoncé élémentaire, $\exists x\ P$ aussi.
>
> Mais notez que la quantification $\exists x$ ne peut faire référence qu'à un élément de la structure en jeu, jamais à un sous-ensemble. La classe d'énoncés tire son nom de cette restriction. On parle aussi de « logique du premier ordre ».

Si l'on voulait quantifier sur les ensembles, il faudrait à leur tour considérer les ensembles comme les éléments d'une autre structure, étudiée par la théorie des ensembles. Mais tel n'est pas mon propos car les phénomènes d'incomplétude prennent place dès une théorie en apparence inoffensive : la théorie des nombres. C'est là que va notre exposé.

D'ailleurs pour les entiers, l'énoncé « il existe un ensemble infini de nombres vérifiant P » revient à « pour tout nombre, il en existe un supérieur vérifiant P ». Le prudent génie grec l'avait déjà noté, qui ne maniait pas l'infini actuel.

6. L'arithmétique

Je vais dans la suite considérer les nombres entiers $\mathbb{N}$ équipés de l'addition et de la multiplication. Cette structure est avec la géométrie l'autre divine inspiratrice du génie grec. La seconde moitié du XIX^{e} fut un néo-classicisme mathématique, avec les premiers efforts raisonnés d'axiomatiser cette structure, c'est-à-dire de la décrire aux fins de démonstrations.

Arithmétique immodérée

On entend affirmer que la première tentative raisonnée d'axiomatiser les entiers est due à Peano. Voici son inspiration.

> Toute partie non-vide des entiers possède un minimum.

On peut aussi l'énoncer sous la forme du principe de récurrence. J'appellerai cet énoncé l'arithmétique *immodérée.*

> Si A est une partie des entiers contenant 0 et stable par $n \mapsto n + 1$, alors A est l'ensemble des entiers.

Les deux énoncés sont équivalents sitôt que $0, <, +1$ ont un sens. En faveur de cette axiomatique est son incomparable force. Car elle caractérise à isomorphisme près les entiers ; et c'est une simple récurrence.

> Soit $\mathbb{P}$ vérifiant l'arithmétique immodérée. Il possède un plus petit élément $0_{\mathbb{P}}$; au 0 de $\mathbb{N}$ associons celui de $\mathbb{P}$. Puis au plus petit entier après 0 (qui est 1), associons le plus élément de $\mathbb{P}$ après $0_{\mathbb{P}}$, que nous appelons $1_{\mathbb{P}}$. Puis 2 sur $2_{\mathbb{P}}$. On continue ; la fonction définie est une injection. Mais son image A contient $0_{\mathbb{P}}$ et est stable sous $p \mapsto p + 1$ par construction ; si bien que d'après l'arithmétique immodérée dans $\mathbb{P}$ appliquée au sous-ensemble A, on trouve $A = \mathbb{P}$, donc f est surjective. C'est même un isomorphisme.

Mais contre cette axiomatique immodérée plaide son caractère hautement non-élémentaire, puisqu'elle appelle une quantification ensembliste. Or à moins de préciser ce que sont les ensembles, cela n'est que vague au mieux, en tout cas ne tombe pas sous les lumières de la logique.

Arithmétique élémentaire

Nous allons donc, chose non prévue par Peano, *modérer* le principe de récurrence.

> Soit $E(x)$ un énoncé *élémentaire* sur les entiers. On suppose qu'est vérifié $E(0)$, et que si $E(n)$ est vérifié, alors $E(n+1)$ l'est aussi. Alors tous les points vérifient E.

On note que j'évite ainsi la quantification ensembliste, mais que je dois faire autant d'axiomes qu'il y a d'énoncés élémentaires. Et je ne peux pas (a priori) quantifier sur les énoncés ; on parle de *schéma d'axiome* de récurrence.

Ce schéma d'axiomes, avec quelques propriétés élémentaires de base régissant l'addition et la multiplication, forme l'arithmétique élémentaire. On l'appelle communément « arithmétique de Peano du premier ordre » ; en forme courte PA_1. Retenez ce nom pour la suite.

Intermède

La méthode axiomatique est entièrement validée par le théorème de complétude de Kurt Gödel, qui affirme l'équivalence entre deux notions de conséquence. Cette méthode axiomatique est pourtant intrinsèquement limitée aux énoncés *élémentaires*, sans quantification ensembliste. Je rappelle le phénomène.

> L'énoncé élémentaire E est démontrable à partir des axiomes élémentaires A_i si et seulement si tout modèle des axiomes A_i est modèle de E.

Et dans la suite je m'intéresse à l'axiomatique dite « de Peano restreinte » PA_1, qui décrit certaines propriétés de base des entiers avec somme et produit, et le schéma de récurrence. Cette axiomatique est infinie mais élémentaire.

---

7. Modèles de l'arithmétique

Modèles non standards

Paradoxalement, la découverte par Thoralf Skolem d'autres modèles de PA_1 que le modèle standard $\mathbb{N}$, est postérieure de trois ans aux travaux de Gödel. Mais elle les éclaire immensément. C'est un fait qu'hors cas vraiment triviaux, *aucune* axiomatique élémentaire ne possède un modèle unique. Il existe ainsi d'autres modèles de PA_1 que $\mathbb{N}$, un peu comme $\overline{\mathbb{Q}}$ et $\mathbb{C}$ sont deux modèles de l'axiomatique des corps algébriquement clos.

On les appelle *non-standards*. Vous n'en avez jamais entendu parler parce qu'ils ne sont pas naturels comme $\mathbb{N}$; ils n'ont pas sa pertinence. Au fond ce sont des artefacts indésirés de la méthode axiomatique. Mais en donner serait fort simple. Ils ne vérifient pas le principe immodéré de récurrence (nous avons vu qu'à isomorphisme près celui-ci caractérise $\mathbb{N}$), mais sa version élémentaire. J'en rappelle le sens ; soit $\mathbb{P}$ un tel objet. Pour chaque instance du schéma de récurrence, i.e. chaque énoncé élémentaire $E(x)$, si $\mathbb{P}$ vérifie $E(0)$ et que pour tout p, $\mathbb{P}$ vérifie « $E(p)$ implique $E(p+1)$ », alors tout p de $\mathbb{P}$ vérifie E. Un tel $\mathbb{P}$ a des entiers infiniment grands par rapport aux entiers naturels, comme en analyse existent des infinitésimaux qui ne sont pas des nombres réels.

À la croisée des chemins

On peut envisager deux cas.

1. Cas favorable. L'arithmétique élémentaire permet de démontrer *tous* les énoncés vrais dans $\mathbb{N}$. Cela entraîne notamment que si $\mathbb{P}$ est un modèle quelconque de PA_1, tout énoncé vérifié par $\mathbb{N}$ l'est aussi par $\mathbb{P}$. En effet $\mathbb{P}$ vérifie PA_1 donc tout ce qu'on démontre avec.

   Dans ce cas favorable l'axiomatique remplit entièrement son rôle : ce qui est vrai dans le modèle standard $\mathbb{N}$, l'est dans tout autre modèle. Tous les modèles de PA_1, bien que non-isomorphes, ont les mêmes propriétés élémentaires, les mêmes propriétés « observables ».
2. Cas défavorable. L'arithmétique élémentaire ne permet *pas* de démontrer tout ce qui est vrai dans $\mathbb{N}$. Mais alors, par l'équivalence des deux notions de conséquence, il doit exister des modèles non-standards $\mathbb{P}$ de PA_1 qui n'ont pas les mêmes propriétés observables, qui sont en désaccord avec $\mathbb{N}$ sur certains énoncés élémentaires.

Au fond, la question est de décrire *tous* les modèles de PA_1, de les classifier non pas à isomorphisme près mais *selon leurs propriétés élémentaires.* Existe-t-il à PA_1 des modèles qui n'ont *pas* les mêmes propriétés que $\mathbb{N}$, comme la géométrie d'Euclide a des modèles en profond désaccord avec le plan ? Par exemple existe-t-il des modèles de l'arithmétique élémentaire où le théorème de Fermat serait faux ? (La question est ouverte ; elle l'est même pour le *petit* théorème de Fermat.) Bien sûr il ne s'agirait pas des vrais entiers, pour lesquels la chose est connue, mais cela nous éclaire sur les limitations de notre axiomatique. Car le sort est défavorable.

8. Le premier théorème d'incomplétude

Énoncé

Un avatar du « premier théorème d'incomplétude » est le résultat suivant.

> Il existe des modèles de PA_1 qui ne vérifient pas les mêmes énoncés que $\mathbb{N}$.

Si vous repensez au plan euclidien, ce n'est pas si choquant. D'après la notion de conséquence, on peut aussi le formuler en termes de preuves.

> Il existe des énoncés vrais dans $\mathbb{N}$ qui ne sont pas démontrables dans PA_1.

Il y a même là quelque chose de plus profond : *aucune* axiomatique ne convient.

> Si (A_i) est une axiomatique élémentaire *effective* pour $\mathbb{N}$, alors il y a des énoncés vrais dans $\mathbb{N}$ qui ne sont pas démontrables à partir des A_i.

« Effective » signifie qu'on peut faire une liste, éventuellement infinie par schéma, mais bien construite, énumératrice, des axiomes A_i. Cette contrainte est mise pour disqualifier l'axiomatique « tous les énoncés vrais dans $\mathbb{N}$ ». Certes, cela conviendrait en théorie. Mais on ne saurait fonder la méthode axiomatique ou la communication mathématique sur la tautologie « ce qui est vrai, est vrai ».

PA_1 n'est qu'un exemple. C'est notre meilleure candidate en l'état actuel de nos connaissances, mais le théorème stipule qu'*aucune* axiomatique raisonnable n'épuisera la vérité de $\mathbb{N}$.

Idée de preuve

Je voudrais donner quelques mots de preuve pour ce premier théorème.

> À la surprise générale, $\mathbb{N}$ permet de coder la combinatoire finie : c'est le cœur de la découverte de Gödel. Cela signifie que toute opération combinatoire finie est émulable en termes d'entiers.
>
> Le plus étonnant est la quasi-trivialité de la preuve : c'est une simple application de l'isomorphisme $\mathbb{Z}/(mn\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, pour m et n premiers entre eux. Mais c'est trivial au sens où le système RSA est trivial : le principe mathématique est bas de gamme, et pourtant je dois me le faire réexpliquer à chaque fois car il est fort ingénieux.
>
> On peut donc coder à l'intérieur des entiers toute opération de type traitement de texte, données finies ou effectives, ou copier-coller d'arbres. Notamment la notion d'arbre de preuve est codable. Supposons donnée une axiomatique élémentaire et effective (A_i). Alors l'ensemble de ses conséquences est effectif aussi : il suffit d'écrire qu'il existe un arbre de preuve aux feuilles parmi les A_i.
>
> Mais par ailleurs en adaptant le lemme diagonal de Cantor, Tarski a montré (Gödel l'avait fait avant lui mais cela semble indépendant) que l'ensemble des énoncés vérifiés dans $\mathbb{N}$ ne peut *pas* être effectif. En supposant que c'est le cas, il a construit un énoncé disant essentiellement « je ne suis pas vrai » : ce qui mène à une contradiction. Ici les détails demanderaient sans doute un tableau.
>
> Ainsi d'une part l'ensemble des conséquences des A_i est effectif, d'autre part celui des vérités de $\mathbb{N}$ ne l'est pas : ces deux ensembles diffèrent, ce qui montre le premier théorème.

Je répète qu'il ne faut pas être surpris outre mesure. La structure des entiers est trop complexe pour être décrite de façon élémentaire et effective. Mais cela suggère que la classe des modèles de PA_1 peut manifester des comportements excentriques.

9. Le second théorème

Tout cela va bien plus loin.

La cohérence

La suggestion diabolique est de considérer l'énoncé de cohérence : « PA_1 ne prouve pas que $0 = 1$ ».

Dans l'argument précédent nous avons vu que si les axiomes sont effectifs, alors leurs conséquences aussi ; cette partie n'était pas établie par l'absurde, mais simplement en remarquant que la notion d'arbre de preuve est élémentaire. Il suit que comme toute affirmation d'existence ou d'inexistence de preuve, l'énoncé de cohérence est lui-même élémentaire, et rentre dans notre cadre logique.

Et cet énoncé est vrai dans $\mathbb{N}$, car il n'existe pas de démonstration de $0 = 1$ dans PA_1 : sans quoi $\mathbb{N}$ vérifierait $0 = 1$, ce qui n'est pas.

La cohérence est donc élémentaire et vraie dans le modèle standard. On peut se demander si elle est conséquence de PA_1.

La question n'est pas gratuite. En effet PA_1 permet la combinatoire finie ; comme la syntaxe et la notion de preuve se formalisent par de simples récurrences finies, on peut exprimer (je n'ai pas dit : « affirmer ») la cohérence de n'importe quelle théorie mathématique effective T en son sein : que T mentionne l'infini ou non, les *preuves* de T restent des objets finis représentables dans PA_1. Si l'on pouvait prouver la cohérence de T dans PA_1, la cohérence de PA_1 serait alors un gage épistémologique suffisant pour T. On ramène ainsi la question de la fiabilité d'une théorie T de cohérence prouvable, à la question-mère de la prouvabilité dans PA_1 de la cohérence de PA_1.

Cela permettrait d'asseoir la *cohérence* des mathématiques de l'infini actuel (p.ex. ensemblistes) sur celle des mathématiques de l'infini potentiel (p.ex. la théorie des nombres). Ce fut un important enjeu historique, a posteriori nommé « programme de Hilbert ». Ceci motive la question : la cohérence est-elle prouvable dans PA_1 ?

Second théorème pour l'arithmétique élémentaire

Voici le second théorème.

> La cohérence n'est pas démontrable dans PA_1.

Le trait de génie de Gödel est d'avoir noté (sans le faire pourtant lui-même : Paul Bernays et David Hilbert furent les premiers rédacteurs de la preuve en ses moindres et laborieux détails) que quasiment tout cet exposé prend place à l'intérieur de PA_1. C'est ensuite un artifice technique que d'obtenir, comme corollaire, que la cohérence n'est pas démontrable. Ici bien sûr j'élude à peu près tout, qui nous emmènerait trop loin.

Il existe en particulier des modèles non-standards de PA_1 qui vérifient la non-cohérence. Ils détiennent ainsi un arbre de preuve de $1 = 0$. Mais cet arbre est non-standard, infiniment grand : et ne correspond plus à notre intuition première de la preuve.

En théorie des ensembles

Tout ce qui précède est d'ailleurs encore vrai dans la théorie ZF, la candidate la plus consensuelle pour décrire le comportement des ensembles. On peut former l'énoncé de cohérence de ZF. Il est beaucoup plus simple de refaire tout l'exposé dans ZF et d'arriver aux mêmes phénomènes. Gödel nous laisse avec l'amer savoir que si ZF démontre sa cohérence, alors elle démontre son incohérence.

Mais autant pour PA_1 nous avions le sentiment profond de l'existence du modèle standard $\mathbb{N}$ (ce qui nous convainquait de la cohérence de l'axiomatique PA_1), autant le concept de modèle standard de la théorie des ensembles est plus incertain. Et comme le critère actuel de validité d'une preuve est la possibilité de la conduire dans ZF, nous perdons ici nos repères platoniciens : on ne dispose d'aucun moyen mathématique consensuel d'établir la cohérence de ZF.

Discussion finale

Roland Fraïssé avait une expression magnifique, *le complexe de Descartes*, pour désigner l'espoir de bâtir un réseau de certitudes à partir de peu ou pas de données admises. On s'étonne que près d'un siècle après la découverte des phénomènes d'incomplétude, cette attitude survive dans certaines expositions des mathématiques. Toute formalisation des entiers repose sur une observation de la nature mathématique ; nos justifications a posteriori sont insuffisantes à rendre compte du primat de l'expérience intuitive.