

– À l'infini, je dispose d'un système S_{infini} qui possède peut-être une infinité d'axiomes, mais qui est complet.

Ce système semble contredire le théorème de Gödel. Où est la faille de ce raisonnement?

Il est bien vrai qu'il n'y a plus d'indécidable pour S_{infini} : par construction, il ne peut y en avoir. Si au départ S était consistant, S_{infini} l'est aussi. En revanche, et c'est ce qui ne va pas, le prétendu système S_{infini} n'en est pas vraiment un, car il n'existe aucun moyen algorithmique de savoir si une formule donnée est un axiome ou n'en est pas un. Or pour qu'un système formel soit envisageable en mathématiques, il faut bien sûr qu'on sache en reconnaître les axiomes (on dit que le système doit être effectif). La prétendue méthode pour passer de S_n à S_{n+1} aboutit à une abstraction mathématique qui n'est pas utilisable comme système formel.

L'énoncé du premier théorème de Gödel en faisant apparaître cette précision (qu'on omet souvent pour simplifier l'exposé ou parce qu'on sous-entend le mot effectif dans la définition de système formel) est donc : tout système formel effectif permettant de faire de l'arithmétique est soit incomplet, soit inconsistent.

COMPLÉTUDE DE LA LOGIQUE

Mettons en parallèle le résultat d'incomplétude de Gödel avec un autre résultat de Gödel, de deux ans plus ancien et qui, lui, est positif. Il s'agit de la complétude de la logique. Ce résultat intéresse moins les philosophes, alors que pourtant c'est la comparaison des résultats de complétude et d'incomplétude qui contient les enseignements les plus précieux, et fait entrevoir les mystères les plus profonds sur la nature des mathématiques.

Au lieu de s'intéresser à ce qui est vrai des nombres entiers, on cherche à savoir ce qui est vrai sur le plan de la logique pure. On se pose des questions comme :

- est-il vrai que si $\{a$ implique $b\}$ alors $\{non-b$ implique $non-a\}$?
- est-il vrai que si $\{pour\ tout\ x, y : P(x,y)\}$ alors $\{pour\ tout\ z : P(z,z)\}$?
- est-il vrai que si $\{pour\ tout\ x, il\ existe\ y\ tel\ que : Q(x,y)\}$ alors $\{il\ existe\ y\ tel\ que\ pour\ tout\ x : Q(x,y)\}$?

(Réponses : oui, oui, non)

Nous cherchons ici un système formel pour ce que nous dénommons le calcul des prédicats du premier ordre qui est la logique générale où tout raisonnement mathématique peut s'exprimer.

Le résultat de Gödel de 1929 répond à cette question : il existe des systèmes formels qui démontrent toutes les formules justes du calcul des prédicats du premier

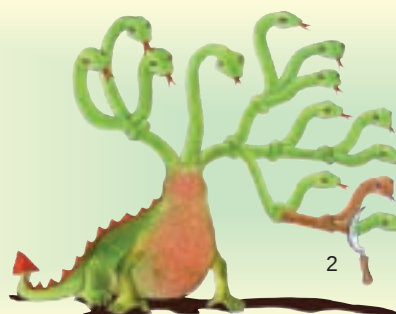
4. HERCULE CONTRE L'HYDRE

Une hydre possède une multitude de têtes reliées à son corps et organisées selon un réseau de cous reliés par des nœuds, le tout formant un arbre. Hercule doit tuer l'hydre en coupant toutes les têtes.



PREMIÈRE COUPURE

En brun, la partie excitée de l'hydre. La partie excitée est dupliquée.



DEUXIÈME COUPURE

En brun, la partie excitée par la deuxième coupure. La partie excitée est ajoutée deux fois.



TROISIÈME COUPURE

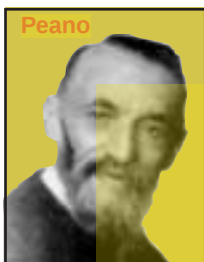
En brun, la partie excitée par la troisième coupure. La partie excitée est ajoutée trois fois. S'il coupe la tête bleue reliée directement au corps de l'hydre, elle ne repousse pas.



Coupera-t-on toutes les têtes de l'hydre? Cette affirmation, démontrable avec des théories puissantes, est un indécidable de l'arithmétique.

Hercule doit tuer l'hydre en ne coupant qu'une tête à la fois et en tranchant la dernière partie du cou située avant la tête coupée. Lorsqu'il coupe une tête et un cou, une multitude de nouveaux cous et têtes apparaissent : lorsqu'il vient de couper la n -ième tête et son cou, le cou en dessous de la partie qu'il vient de couper et tout l'ensemble des nœuds, cous et têtes au-dessus de ce nœud ("le bout excité de l'hydre") se reproduit en n exemplaires qui poussent à côté du bout excité. Toutefois, lorsque Hercule coupe un cou directement lié au corps de l'hydre, les têtes ne repoussent plus.

Hercule peut-il vaincre l'hydre en éliminant toutes les têtes? L'opération de coupe augmente beaucoup le nombre des têtes, mais diminue aussi le nombre de têtes associées à un cou relié au corps. Aussi espère-t-on arriver au moment où toutes les têtes sont directement liées au corps et où l'on peut les couper sans déclencher de reproduction. On démontre, avec des théories plus puissantes que l'arithmétique de Peano, que Hercule, avec n'importe quelle stratégie de choix de tête à couper, vient à bout de l'hydre en un temps fini, mais aussi que ce résultat est un indécidable de l'arithmétique de Peano.



Peano

5. PEANO, FERMAT ET GÖDEL

L'arithmétique de Peano est le système formel dans lequel on démontre les propriétés des nombres entiers comme «13 est un nombre premier», «l'équation $x^2 + y^2 = z^2$ possède une infinité de solutions», ou «tout nombre entier est la somme de quatre carrés». On définit l'arithmétique de Peano en indiquant les propriétés du nombre 0, de l'opération "est le successeur de", de l'addition, de la multiplication et, surtout, en précisant qu'on peut raisonner par récurrence pour toute formule arithmétique $P(n)$ (si

$P(0)$ est vrai et que pour toute valeur de n , $P(n)$ vrai implique $P(n+1)$ vrai, alors $P(n)$ est vrai pour tout n).

Le philosophe Daniel Isaacson soutient que toutes les propriétés purement arithmétiques sont démontrables dans le système de Peano qui, en un certain sens, serait donc complet. L'incomplétude (établie par les théorèmes de Gödel)

ne serait en mesure que de faire apparaître des indécidables non purement arithmétiques obtenus soit par codage (comme les indécidables donnés par la démonstration de Gödel), soit artificiellement parce que provenant de concepts de haut niveau (de type ensembliste, par exemple).

Cette analyse est soutenue par les résultats des logiciens français P. Cegielski et O. Sudac, qui ont obtenu, pour certains résultats d'arithmétique pure, comme le théorème d'Hadarnard et de La Vallée Poussin, des démonstrations ne mettant en jeu que le système de Peano.

D'autres résultats (voir le problème d'Hercule et de l'hydre, illustré sur la figure 4) sont plus difficiles à concilier avec l'analyse de

D. Isaacson. Aujourd'hui on ne sait pas ce qu'il en est du théorème de Fermat (démontré par Wiles en 1994), théorème qui est incontestablement un énoncé d'arithmétique pure et qu'on ne sait actuellement démontrer que dans des systèmes plus forts que l'arithmétique de Peano.

La réponse à cette question est importante pour comprendre en quel sens l'arithmétique de Peano est complète et garantirait la preuve d'Andrew Wiles. Elle ne reposerait plus implicitement, comme c'est le cas aujourd'hui, sur l'hypothèse de consistance de la théorie des ensembles (hypothèse jugée forte par beaucoup de mathématiciens et improuvable de manière satisfaisante, comme l'établit le second théorème d'incomplétude de Gödel).



Fermat



Gödel

ordre et uniquement elles (et on sait construire de tels systèmes). Nombre de logiciens jugent ce résultat aussi important que le résultat d'incomplétude. C'est l'un des triomphes de la logique moderne et il a étonné bien des philosophes qui croyaient impossible de cerner toute la logique et considéraient que l'opération de vérification des raisonnements mathématiques ne pouvait pas être pas mécanisée (possibilité qui est une conséquence du théorème de complétude).

La mise en parallèle des résultats positifs et négatifs de Gödel étonne : le domaine des vérités logiques abstraites est formalisable, alors que celui des vérités concernant les entiers ne l'est pas. Le domaine du raisonnement est accessible, celui des nombres ne l'est jamais entièrement : l'abstrait le plus pur et le plus général serait à notre portée, alors que le concret des nombres entiers serait par nature inépuisable et impossible à cerner, à moins, comme le soutiennent certains philosophes, que l'impression de clarté que nous avons concernant les entiers ne soit qu'une illusion, l'incomplétude étant un symptôme de l'irréalité de l'infini et

une mise en garde contre les utilisations imprudentes qu'on en fait.

Il ne fait aucun doute : les mathématiques sont concernées par l'incomplétude et l'indécidabilité. Toute la réflexion sur les mathématiques est hantée par les résultats de Kurt Gödel, comme l'ouvrage récent *The Philosophy of Mathematics* de W. Hart (Oxford University Press, 1996) l'illustre avec finesse. Savoir si d'autres domaines doivent en tenir compte est plus délicat et l'on peut en douter tant le manque de sérieux est la règle dans l'usage pratiqué hors des mathématiques des théorèmes d'incomplétude (qu'on préfère aux théorèmes de complétude, le plus souvent ignorés).

L'USAGE PHILOSOPHIQUE DE L'INCOMPLÉTUDE

Le texte suivant du philosophe Jacques Bouveresse, que je me permets de citer longuement, commente avec intelligence et justesse la situation.

«Lorsqu'un philosophe se met à parler de l'indécidabilité et du théorème de Gödel dans le cadre d'une réflexion sur le problème de la littérature et de l'analyse

de textes littéraires, on pourrait évidemment s'attendre à ce que ce soit pour introduire, si possible, un peu plus de précision dans la discussion de questions qui sont par nature imprécises. Mais c'est en réalité exactement l'inverse qui se passe, puisque le flou et l'imprécision de l'usage littéraire ont plutôt tendance à remonter immédiatement jusqu'aux notions techniques telles qu'elles se présentent initialement dans leur contexte d'origine, au point que l'on finit tout simplement par ne plus rien comprendre à ce qu'elles signifient. Le résultat le plus évident me semble être que rien d'intéressant n'a été ajouté par l'invocation du théorème de Gödel à ce que l'on peut dire sans lui à propos d'une question comme celle de l'indécidabilité dans le domaine de la littérature, de la métaphysique ou de la religion, mais que l'on a, en revanche, perdu toute chance d'avoir encore une idée précise de ce que Gödel a démontré exactement et des conséquences qui en résultent. [...] On peut remarquer que le théorème ne représente pas seulement, comme il se dit généralement, un échec, mais également un succès pour le formalisme lui-même, dont Gödel maîtrise et exploite toutes les ressources. Mais de cela, bien entendu, la plupart des philosophes qui cherchent à utiliser pour leurs propres fins le résultat de Gödel ne croient pas utile de savoir quoi que ce soit. [...] La recommandation que l'on peut formuler à l'usage de ceux qui ont des ambitions de cette sorte est la suivante : 1) Ne regardez surtout jamais la démonstration du théorème, ce qui serait pourtant le meilleur moyen de savoir ce qu'elle démontre au juste. Comme dit Wittgenstein, si vous voulez savoir ce qu'une démonstration démontre, regardez la démonstration. 2) Ne lisez aucun des nombreux commentaires sérieux et informés (mais il est vrai, malheureusement assez techniques) qui ont été écrits sur le genre de signification philosophique que l'on peut ou ne peut pas attribuer au théorème de Gödel. Car si vous le faisiez, vous risqueriez de découvrir immédiatement qu'il est impossible de l'utiliser de la façon à laquelle vous songiez et qui a l'avantage d'être considérée comme particulièrement philosophique. 3) Évitez aussi de regarder ce que Gödel a dit lui-même de la signification philosophique de son résultat et des extensions que l'on pourrait éventuellement songer à lui donner. [...] Une véritable mise en parallèle de la situation en logique et en sociologie par exemple consisterait à rechercher les emboîtements de systèmes, mais le plus souvent les utilisateurs de l'incomplétude ne peuvent faire cette mise en parallèle précise car ils croient faussement que les indécidables le sont absolument, ce qui est le contresens le plus grand qu'on puisse faire (mais aussi le plus

courant). [...] Même comme métaphore vague (qu'on pourrait remplacer par celle, géométrique et accessible à chacun, mais ce ne serait pas drôle, de sommets montagneux de plus en plus hauts) l'incomplétude des systèmes formels n'est pas comprise. On ne retient de Gödel que l'idée (fausse et passablement religieuse) de vérités qui échappent à la vue de ceux qui sont situés en un point théorique donné et qui par principe leur échapperont toujours, car le théorème dit qu'il en est ainsi ! L'idée que celui qui évoque le théorème réalise un dépassement de tout cela est souvent implicite et produit sans doute l'effet (recherché) qu'il est au-dessus de la mêlée (pré-gödelienne), hors de portée d'une certaine façon des effets du théorème de Gödel (car comme en psychanalyse peut-être le fait de savoir est déjà le début de la guérison !)» (Jacques Bouveresse, *Qu'appelle-t-il penser ?* Les cahiers rationalistes, septembre 1998 et novembre 1998).

LE THÉORÈME DE FERMAT EST-IL DÉMONTRÉ ?

À l'inverse, l'importance au quotidien en mathématiques de l'incomplétude n'est pas toujours clairement perçue. Illustrons-la à propos du grand théorème de Fermat. Ce théorème est l'affirmation qu'il n'existe aucun quadruplet de nombres entiers x , y , z et n avec x , y et z positifs, et n supérieur à 2 tel que $x^n + y^n = z^n$. Il s'agit donc d'un énoncé d'arithmétique et l'on s'attend, s'il est vrai, à ce qu'il soit démontrable dans le système formel naturel de l'arithmétique, qui est l'arithmétique de Peano. Or la démonstration d'Andrew Wiles de 1994 utilise des moyens bien plus puissants et fait usage de la théorie des ensembles nommée théorie de Zermelo-Fraenkel. La question se pose donc : le théorème de Fermat peut-il être démontré dans l'arithmétique de Peano ou nécessite-t-il vraiment l'usage de toute la puissance de Zermelo-Fraenkel ? Autrement dit, ce théorème est-il un indécidable de l'arithmétique de Peano ?

Personne ne sait répondre aujourd'hui, mais des équipes de chercheurs s'occupent de cette question, en particulier en France où Patrick Cegielski et Olivier Sudac ont déjà obtenu des résultats très intéressants. Ils ont montré que le théorème de Dirichlet (qui indique que, dans toute progression arithmétique $an+b$, a et b premiers entre eux, il y a une infinité de nombres premiers) et le théorème de répartition des nombres premiers d'Hadamard et de La Vallée-Poussin (qui indique qu'il y a environ $n/\ln(n)$ nombres premiers inférieurs à n) étaient démontrables dans l'arithmétique de Peano. De tels résultats sur la décidabilité des énon-

cés d'arithmétique dans la théorie de Peano sont importants pour le mathématicien, car ils rendent plus sûres les démonstrations obtenues dans Zermelo-Fraenkel et les libèrent d'hypothèses implicites sur la réalité des ensembles.

En effet, la notion d'ensemble est beaucoup plus délicate que celle de nombre entier (la première permet d'ailleurs de retrouver la seconde), et l'assurance que nous avons que ces entités que nous appelons ensembles existent est bien moins grande que celle que nous avons que les entiers existent. D'ailleurs, face aux nombreux problèmes de la théorie des ensembles, des mathématiciens de très grand renom comme Brouwer, Borel, Lebesgue, Weil ou Poincaré ont exprimé des doutes concernant les ensembles ou même les ont complètement rejetés.

Pour eux, la preuve de Wiles ne serait pas complètement satisfaisante (ce qui ne signifie pas qu'ils la jugeraient inintéressante !). Une preuve du théorème de Fermat n'utilisant que l'arithmétique de Peano serait un soulagement, et si l'on devait découvrir qu'une telle preuve n'existe pas – que le théorème de Fermat est un indécidable de l'arithmétique de Peano –, ce serait une découverte encore plus importante, qui amènerait à reconsidérer l'arithmétique de Peano qu'on juge (sans preuve) comme suffisante pour tous les résultats d'arithmétique classique.

Un résultat de logique indique que, si l'on ajoute à l'arithmétique de Peano l'axiome affirmant que «la théorie des ensembles est consistante», alors, avec la preuve du théorème de Fermat de Wiles, on pourra en construire une dans l'arithmétique de Peano. Pour penser que le théorème de Fermat est vraiment démontré, il n'est donc pas nécessaire de croire à l'existence des ensembles, mais seulement à la consistance de la théorie Zermelo-Fraenkel, ce qui est beaucoup plus faible. Aujourd'hui, concernant le théorème de Fermat, trois attitudes sont donc possibles.

(a) Soit on fait confiance à l'évidence des ensembles (ils existent, et ce qu'on démontre avec eux est vrai sans qu'on ait rien à craindre), et alors la démonstration de Wiles prouve définitivement le théorème de Fermat.

(b) Soit on fait confiance seulement à la consistance du système formel Zermelo-Fraenkel, et alors la démonstration de Wiles est garantie par le fait qu'il existe une preuve du théorème de Fermat dans l'arithmétique de Peano qui utilise l'hypothèse de cette consistance. Croire en la consistance de Zermelo-Fraenkel sans croire aux ensembles peut se justifier en disant que, depuis bientôt un siècle qu'on utilise ZF, personne n'y

a trouvé de contradiction. Bien des mathématiciens sont tentés par cette position, qui leur évite l'engagement ontologique de croire aux ensembles, mais ils doivent se rendre compte que c'est là une position contraire à celle qu'on prend habituellement concernant les conjectures non démontrées : quand aucun contre-exemple n'a été découvert concernant une conjecture, on ne la considère pas pour autant comme vraie ; pourquoi alors considérer que Zermelo-Fraenkel ne donne jamais de contradiction du seul fait qu'on n'en a pas trouvé jusqu'à maintenant ! L'indécidabilité des preuves de consistance que le second théorème de Gödel énonce ne signifie pas que tous les systèmes auxquels on s'intéresse sont consistants !

(c) Soit on considère qu'il reste des doutes concernant la consistance de Zermelo-Fraenkel, et alors on doit aussi douter du théorème de Fermat, et donc en rechercher une preuve dans des systèmes plus faibles que Zermelo-Fraenkel, ou démontrer qu'il s'agit d'un indécidable de l'arithmétique.

Le nombre premier de deux millions de chiffres évoqué dans le dernier article ne valait pas 50 000 \$ mais rien du tout. En effet une malheureuse erreur typographique, qui, par les vertus du copier-coller, s'est répandue en quatre exemplaires dans l'article, a changé un "6" en "8". Le nombre premier gagnant a l'exposant 6 972 593 et non pas 8 972 593. Nous présentons toutes nos excuses aux lecteurs que cette erreur a pu gêner.

Patrick CEGIELSKI, Quelques contributions à l'étude des arithmétiques faibles, Thèse de doctorat d'État, Université de Paris VII, 1990.

J.-P. DELAHAYE, Arguments et indices dans le débat sur le réalisme mathématique, in L'Objectivité mathématique, Platonisme et structures formelles, pp. 23-48, Masson, 1995.

L. KIRBY et J. PARIS, Accessible Independence Results for Peano Arithmetics, in Bull. London Math. Soc., vol. 14, pp. 285-293, 1982.

R. SMULLYAN, Les théorèmes d'incomplétude de Gödel, Masson, 1993.

O. SUDAC, Étude de la prouvabilité de certains résultats classiques dans l'arithmétique primitive récursive et l'arithmétique de Peano, Thèse de doctorat, 1998.

D. VALLEMAN, Fermat's Last Theorem and Hilbert Program, in The Mathematical Intelligencer, vol. 19, n° 1, pp. 64-67, 1997.