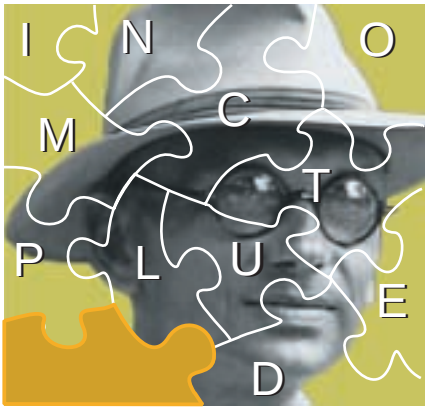


Les propositions indécidables

JEAN-PAUL DELAHAYE

L'incomplétude gödélienne concerne-t-elle d'autres domaines que les mathématiques?

En 1931, le logicien Kurt Gödel prouvait un théorème révolutionnaire qui démontrait que les mathématiques sont plus profondes que les mathématiciens ne l'imaginaient. Toute tentative pour définir de qu'est une preuve échoue nécessairement à cause des propositions dites indécidables (on ne peut déterminer ni leur vérité, ni leur fausseté) qui se glissent dans tout système.

Imaginez l'émoi que ce résultat aurait dû susciter : assez paradoxalement toutefois, l'incomplétude et l'indécidabilité gödélienne engendrent un intérêt considérable chez nombre de ceux qu'elles ne concernent pas vraiment (ou seulement à titre de vagues métaphores) et une indifférence aveugle chez les mathématiciens, qui devraient en être troublés. Nous allons examiner le théorème de Gödel et l'importance qu'il devrait avoir.

L'AXIOME DES PARALLÈLES

L'exemple le plus simple d'une situation d'incomplétude et d'indécidabilité est ancienne : c'est la géométrie qui découle de l'axiome des parallèles. L'affaire remonte aux *Éléments* d'Euclide, qui furent écrits vers 300 avant J.-C. et qui rapportaient des résultats mathématiques plus anciens encore. Euclide y développe une conception axiomatique de la géométrie : il énumère les propriétés primitives des objets points, droites, plans, etc., qu'il accepte sans démonstration (ce sont les axiomes et postulats). Toute la géométrie n'est plus alors qu'une question de raisonnement pur, de déduction logique.

La présentation d'Euclide ne décrit pas les règles de raisonnement autorisées (elles n'ont été comprises qu'au cours du XIX^{e} siècle). Euclide ignore les notations qui, aujourd'hui, facilitent l'exposé des démonstrations et leurs vérifications ; pour rendre plus aisée la lecture, l'axiomatisation de la géométrie que nous évoquons ici prend en compte les progrès faits par la méthode axiomatique.

Parmi les propriétés posées par Euclide, la pierre d'achoppement est l'axiome des parallèles (ou cinquième postulat d'Euclide), qui énonce :

Si P *est un point donné et si* D *est une droite ne contenant pas* P, *alors dans le plan déterminé par* P *et* D *il existe une droite unique* D' *contenant* P *et ne rencontrant pas* D (la droite *D'* est dénommée la parallèle à *D* passant par *P*).

La question s'est posée très tôt : pouvait-on déduire cet axiome des autres axiomes, en apparence plus naturels? On a longtemps pensé que cela devait être possible. Hélas, toutes les tentatives échouèrent pour prouver l'axiome des parallèles à partir des autres axiomes. Avec la maturité des méthodes logiques, on a fini par démontrer en 1868 que l'énoncé des parallèles ne se déduisait pas des autres axiomes : aujourd'hui, il est donc inutile d'essayer de le «prouver»!

Il s'agit bien là d'une situation d'incomplétude et d'indécidabilité : la géométrie euclidienne sans l'axiome des parallèles, dénommée *géométrie absolue*, est incomplète. Quelle que soit la longueur des raisonnements qu'on fasse, on ne peut déduire de la géométrie absolue, ni l'axiome des parallèles ni sa négation (c'est-à-dire l'affirmation qu'il n'est pas vérifié). Vis-à-vis de la géométrie absolue, l'axiome des parallèles est indécidable.

Même si la preuve de cette indécidabilité a joué un rôle important dans la compréhension de la nature de l'espace physique, la conclusion qu'on en tire n'est pas très grave sur le plan mathématique. On la formule ainsi : la géométrie absolue n'est pas la théorie de l'espace, car la géométrie absolue n'est que le socle

1. ON N'ÉCHAPPE PAS AU THÉORÈME DE GÖDEL

Si un système formel permet de faire de l'arithmétique et qu'il est consistant (c'est-à-dire qu'il ne se contredit pas), alors il existe des énoncés *I* dont *S* ne peut démontrer ni qu'ils sont vrais, ni qu'ils sont faux (on les appelle des indécidables de *S*).

Le théorème de Gödel permet de construire explicitement un tel indécidable *I* (sa démonstration est fondée sur l'écriture d'un énoncé codant dans *S* l'affirmation : "je ne suis pas démontrable dans *S*").

Une idée naturelle vient à l'esprit : partant d'un système S_1, on construit un tel indécidable I_1 et on l'ajoute à S_1 comme nouvel axiome, ce qui donne un nouveau système S_2 dans lequel bien sûr I_1 n'est plus indécidable.

Puisque le théorème de Gödel appliqué à S_1 nous permet d'obtenir un autre indécidable I_2 on l'ajoute aux axiomes de S_1, ce qui conduit à un nouveau système S_2. Etc.

Les systèmes emboîtés S_1, S_2, S_3, etc., sont de plus en plus puissants (ils comportent de moins en moins d'indécidables). À l'infini, ils fournissent un nouveau système formel S_∞. Malheureusement, ce système comporte encore des indécidables! On n'échappe pas si facilement au théorème de Gödel.

commun à plusieurs géométries possibles que l'on définit en ajoutant à la géométrie absolue, soit l'axiome des parallèles, soit un autre axiome. Parmi les différentes géométries possibles obtenues en complétant la géométrie absolue, c'est aux physiciens de dire celle qui leur convient le mieux pour représenter l'espace.

Être incomplet, pour un système formel (comme celui de la géométrie euclidienne), c'est laisser certaines propositions en suspens : un système incomplet est un système où l'on ne peut prouver ni la vérité ni la fausseté d'énoncés qu'il permet pourtant de formuler. Un indécidable d'un système incomplet, c'est un énoncé pour lequel le système ne sait rien dire.

L'incomplétude de la géométrie absolue traduit simplement un oubli dans les axiomes : depuis des siècles, de nombreux mathématiciens croyaient que l'axiome des parallèles pouvait se déduire des autres, ils se trompaient. En voilà une affaire !

Bien des problèmes restent ouverts concernant l'indécidabilité de problèmes simples, y compris lorsqu'ils ont été résolus dans un cadre particulier. Par exemple, la démonstration du grand théorème de Fermat par Andrew Wiles en 1994 s'est faite dans le cadre de la théorie des ensembles – ce théorème n'est pas un indécidable de la théorie des ensembles, mais savoir s'il s'agit d'un indécidable de l'arithmétique est une question difficile et non résolue dont nous verrons la pertinence.

En attendant Gödel...

Les phénomènes d'indécidabilité et d'incomplétude (même si, dans le passé, les mathématiciens n'utilisaient pas ces termes) sont présents dans les mathématiques depuis toujours. Ce qui a changé en 1931, avec les fameux résultats de Kurt Gödel, c'est qu'il est aujourd'hui prouvé que ces phénomènes – contrairement à ce qu'on pensait – sont universels : toute théorie d'un certain niveau y est assujettie. D'aucuns ont cru déduire de cette universalité que l'indécidabilité était inquiétante. D'autres, sans contester la justesse des résultats de Gödel, soutiennent à l'opposé qu'on ne doit pas s'en préoccuper, et donc, en quelque sorte, que la situation des mathématiques est désespérée, mais pas grave.

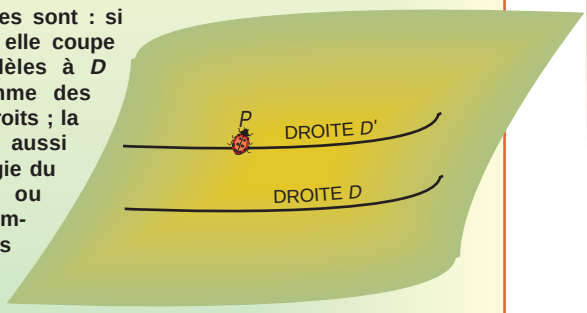
Un exemple simplissime de système formel est indiqué dans l'encadré 3. Les logiciens affirment qu'un système formel est consistant (ou cohérent, ou non contradictoire) quand il est impossible d'y démontrer une proposition et sa négation (autrement dit, le système ne se contredit pas). Dans le

2. L'AXIOME DES PARALLÈLES EST INDÉCIDABLE

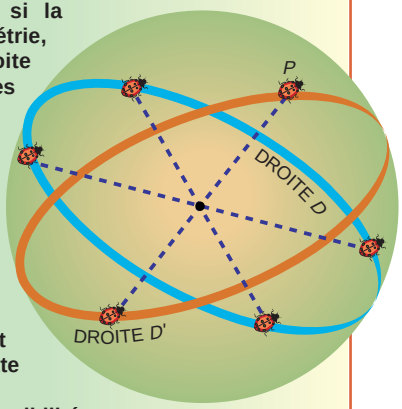
Si *P* est un point donné et si *D* est une droite ne contenant pas *P*, alors dans le plan déterminé par *P* et *D* il existe une droite unique *D'*, contenant *P* et ne rencontrant pas *D*.

Cette formulation de l'axiome des parallèles n'est pas exactement celle d'Euclide. Il utilisait l'énoncé équivalent : si deux droites, coupées par une sécante, forment des angles intérieurs d'un même côté dont la somme est inférieure à deux droits, ces droites se coupent.

D'autres formulations équivalentes sont : si une droite *D* coupe une droite, elle coupe aussi toutes les droites parallèles à *D* (axiome de Proclus) ; la somme des angles d'un triangle vaut deux droits ; la surface d'un triangle peut être aussi grande qu'on veut. La terminologie du *cinquième postulat d'Euclide* ou *postulat des parallèles,* est trompeuse, car chez Euclide certaines définitions cachent des axiomes. Dans la présentation moderne de l'axiomatisation de la géométrie – étudiée par David Hilbert –, il y a bien plus de cinq postulats-axiomes fondamentaux.

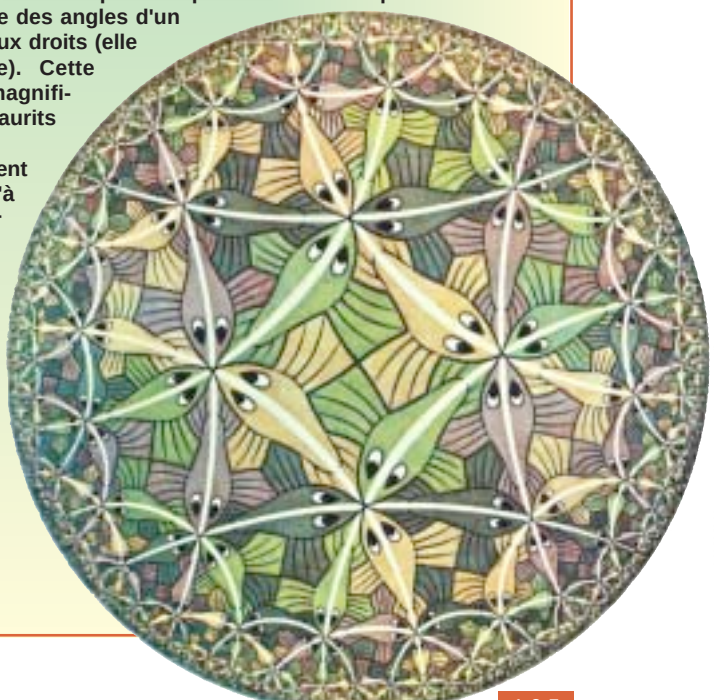


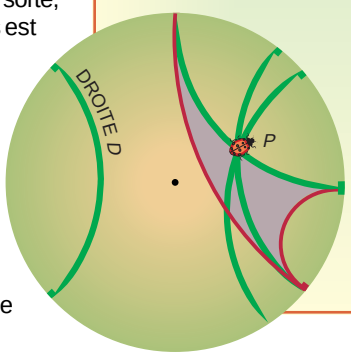
La première démonstration que l'axiome des parallèles est indécidable dans la géométrie absolue est due à Eugenio Beltrani en 1868. Il prouva que la géométrie elliptique (ou de Riemann) est consistante si la géométrie euclidienne l'est. Dans cette géométrie, par un point ne passe pas forcément de droite parallèle à une droite donnée, et la somme des angles d'un triangle est supérieure à deux droits. Il appelle point un couple de points diamétralement opposés et droite un cercle sur la sphère de diamètre maximum. Avec ce vocabulaire redéfini, il constate que les axiomes de la géométrie sont vérifiés. Par exemple : par deux points (au sens nouveau) distincts passe une droite (au sens nouveau) unique. Le seul axiome qui n'est pas satisfait est celui des parallèles : une droite *D* étant donnée, ainsi qu'un point *P* à l'extérieur de cette droite, toute droite *D'* passant par *P* coupe *D*.



Une autre version de la démonstration de l'impossibilité de déduire l'axiome des parallèles des autres axiomes est due au grand mathématicien français Henri Poincaré. On prend un disque (sans sa circonférence) et on appelle droite les arcs de cercle situés dans ce disque qui coupent orthogonalement le bord du disque. Dans cette géométrie hyperbolique (ou de Lobachevski), par un point donné passent plusieurs droites parallèles à une droite donnée, et la somme des angles d'un triangle est inférieure à deux droits (elle est éventuellement nulle). Cette géométrie a inspiré de magnifiques œuvres au graveur Maurits Escher.

Les mathématiciens utilisent aujourd'hui des dessins "à la Escher" pour visualiser les propriétés de la géométrie hyperbolique.





cadre de la logique usuelle, dès qu'un système peut démontrer *P* et non-*P* (une proposition et sa négation), alors il peut tout démontrer. C'est pourquoi l'inconsistance est crainte et bannie.

Le résultat de Kurt Gödel de 1931, qui universalise l'incomplétude déjà connue pour la géométrie absolue, se décompose en deux parties. La première indique que tout système formel permettant de faire de l'arithmétique (la théorie élémentaire des nombres entiers) est soit inconsistant (donc inintéressant, puisque tout y est vrai et faux à la fois), soit incomplet (donc insatisfaisant, puisque le système laisse en suspens certains énoncés).

Autrement dit : tout système formel, à la fois assez puissant pour l'arithmétique élémentaire et consistant contient des indécidables. La seconde partie des résultats de 1931 (ou second théorème de Gödel) indique que justement l'énoncé qui affirme qu'un système est consistant est l'un des indécidables de ce système, ce que l'on traduit simplement en disant qu'un système consistant ne peut savoir qu'il l'est. Une démonstration de ce théorème due à Georges Boolos est présentée sur le site Internet de *Pour la Science*.

Insistons sur le fait que ces résultats n'indiquent pas qu'il existe des indécidables absolus (c'est-à-dire définitivement indémontrables dans tout système formel), mais indique que, pour chaque système formel particulier (assez puissant et consistant), il y a au moins un indécidable *I*.

Si vous repérez un indécidable pour un système *S* auquel vous ajoutez le nouvel axiome *I*, vous créez un système *S'* où *I* n'est plus indécidable. Fort bien, mais avez-vous par là véritablement progressé? Hélas, guère : le théorème de Gödel s'applique alors au nouveau système *S'*, et donc il existe au moins un indécidable *I'* de *S'* (*I'* est bien sûr aussi un indécidable de *S*). Si vous ajoutez *I'* aux axiomes de *S'*, vous obtenez un système *S"* qui contiendra un indécidable *I"*, etc.

Ceux qui interprètent le phénomène de l'indécidabilité comme établissant que les mathématiques sont incomplètes se trompent : un système particulier qui n'accède pas à une certaine vérité mathématique peut toujours être complété pour y accéder.

Un piège existe, piège que nous allons détailler pour assimiler le sens du théorème de Gödel. Le mathématicien n'est jamais effrayé par l'infini et, devant les systèmes *S, S', S"*, etc., il se dit qu'il suffit d'ajouter jusqu'à l'infini les indécidables qu'on trouve et qu'on obtiendra alors un système complet.

UNE MÉTHODE DE COMPLÉTION INEFFICACE

Si ce mathématicien s'y prend trop naïvement, il ne réussira pas car, même après avoir ajouté *I, I', I"*, etc. jusqu'à l'infini, le système obtenu contiendra encore des indécidables (on sait le démontrer). L'impossibilité est analogue avec les tentatives d'énumération des nombres entiers : ce n'est pas parce que vous prenez une infinité d'entiers (par exemple, les entiers pairs, 2, 4, 6, 8, ...) que vous prenez tous les entiers. Similairement, ce n'est pas parce que vous ajoutez une infinité d'indécidables à *S* qu'il n'y en n'a plus.

Après un moment de réflexion, le mathématicien propose une autre idée un peu plus subtile. Il dit :

– Je numérote toutes les formules ayant un sens dans mon système $S = S_0$: f_0, f_1, f_2, f_3, f_4, ... (une telle numérotation est possible pour des formules).

– Je les prends une à une en ajoutant comme nouveaux axiomes celles qui sont encore indécidables au moment où je les considère : à l'étape *n* du processus de complétion, j'arrive à un certain système S_n, je regarde f_n ; si c'est un indécidable de S_n, j'ajoute f_n à S_n pour obtenir S_{n+1}, sinon je conserve le même S_n : $S_{n+1} = S_n$.

3. UN EXEMPLE DE SYSTÈME FORMEL

Dans un système formel (ou système de démonstrations), on détaille successivement ce que sont les formules, les axiomes, les règles d'inférence. Examinons un exemple de système formel, dont la signification sera donnée par la suite.

Formules : des bâtons | suivis du symbole 🐞, puis à nouveau des bâtons, puis le symbole =, puis encore des bâtons, ou la même chose précédée de un ou plusieurs NON.

Exemples : |||||| 🐞 |||||||| = ||||| ; NON |||||| 🐞 |||||||| = |||||

Axiomes : Toutes les formules sans NON où le nombre de bâtons des trois paquets est le même.

Exemple : |||||| 🐞 |||||| = ||||||

Règles d'inférence :

– règle *A* : on permute les deux paquets devant le =.

Exemple : de |||||| 🐞 || = |||, on déduit || 🐞 |||||| = |||

– règle *B* : on ajoute au paquet entre 🐞 et = le nombre de bâtons qu'il y a dans le paquet à gauche de 🐞 .

Exemple : de ||| 🐞 ||| = |||, on déduit ||| 🐞 |||||| = |||

– règle *C* : on ajoute ou on soustrait au moins un des bâtons du paquet derrière = et on fait précéder le tout de NON.

Exemple : de ||| 🐞 |||||| = |||, on déduit : NON ||| 🐞 |||||| = ||

– règle *D* : on ajoute deux fois NON devant une formule déjà obtenue.

Exemple : de ||| 🐞 |||||| = |||, on déduit : NON NON ||| 🐞 |||||| = |||

Une déduction (ou démonstration) dans le système 🐞 est une suite de formules telle que chacune est soit un axiome, soit provient de l'utilisation d'une des règles *A, B, C* ou *D* sur des formules précédemment déduites.

Les axiomes et les règles d'inférence doivent être suffisamment simples pour que la vérification qu'une suite de formules est une déduction correcte puisse se faire mécaniquement (c'est-à-dire par algorithme).

Exemple de déduction dans le système 🐞 :

| 🐞 | = | (c'est un axiome)

| 🐞 || = | (règle *B* appliquée à la formule précédente).

|| 🐞 | = | (règle *A* appliquée à la formule précédente)

|| 🐞 |||= | (règle *B* appliquée à la formule précédente)

|| 🐞 ||||| = | (règle *B* aplliquée à la formule précédente)

NON || 🐞 ||||| = || (règle *C* appliquée à la formule précédente)

Interprétation du système formel 🐞

Ce système formel permet de démontrer *(i)* toutes les propriétés vraies concernant le plus grand commun diviseur de deux nombres entiers du type : le pgcd de 6 et 4 est 2 (ce qui, avec nos notations, s'écrit |||||| 🐞 |||| = ||) ;

***(ii)* toutes les formules de ce type précédées d'un nombre quelconque de NON.**

Le fait que nous ayons réussi à établir || 🐞 ||||| = | signifie en particulier que le pgcd de 2 et 5 est 1, autrement dit que 2 et 5 sont premiers entre eux. Ayant établi que NON || 🐞 ||||| = ||, nous avons démontré que le pgcd de 2 et 5 n'est pas 2.

Les propriétés de ce système sont :

– correction vis-à-vis du domaine mathématique visé : tout ce qu'on démontre en suivant le système est juste ;

– adéquation vis-à-vis du domaine mathématique visé : tout ce qu'on peut formuler avec les formules du système et qui est vrai est démontrable ;

– consistance (résulte de l'adéquation) : jamais on ne prouve une formule et son contraire (la même formule précédée de NON) ;

– complétude : pour toute formule F du système, on peut démontrer F ou NON-F.

Ce système capte complètement le domaine mathématique visé, et son étude peut être menée entièrement (c'est rarement le cas). Il ne contient pas d'indécidables, mais, si on omettait un seul axiome (par exemple || 🐞 || = ||), certains énoncés vrais (exemple : |||| 🐞 |||||| = ||) deviendraient indécidables. Le système modifié serait alors incomplet.

– 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 inconsistant.

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)*}?

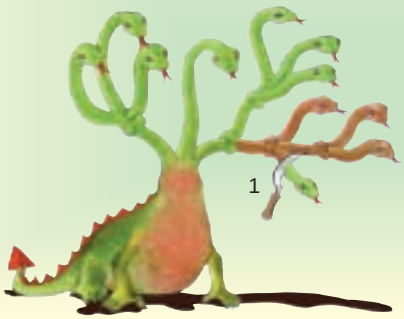
(Réponses : oui, oui, non)

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.

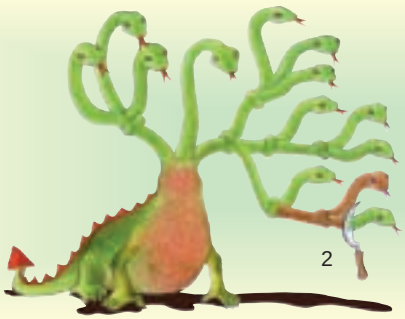
Le résultat de Gödel de 1929 répond à cette question : il existe des systèmes formels qui démontrent toutes les formules justes du calcul des prédicats du premier

4. HERCULE CONTRE L'HYDRE

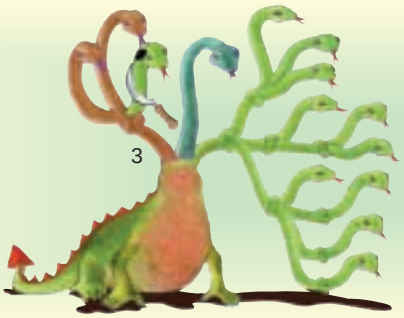
Une hydre possède une multitude de têtes reliées à son corps et organisées selon un réseau de cous reliés par des nœuds, le tout formant un arbre. Hercule doit tuer l'hydre en coupant toutes les têtes.



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.

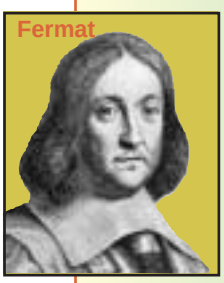
Hercule doit tuer l'hydre en ne coupant qu'une tête à la fois et en tranchant la dernière partie du cou située avant la tête coupée. Lorsqu'il coupe une tête et un cou, une multitude de nouveaux cous et têtes apparaissent : lorsqu'il vient de couper la *n*-ième tête et son cou, le cou en dessous de la 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.

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'Hadamard 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).

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-gödélienne), 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 énoncés 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 Indépendance 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.