peuvent espérer ne jamais rencontrer les monstruosités dont Gödel dit qu'elles les menacent. Toutefois, les développements de la théorie du calcul par K. Gödel, A. Turing, E. Post et S. Kleene, à partir des années 1930 et qui se poursuivent aujourd'hui, donnent de nouveaux arguments aux logiciens.

La théorie du calcul répand l'indécidabilité

En tentant de généraliser le théorème de Gödel, et peut-être parce que ces problèmes étaient dans l'air des années 1930 (on commençait à s'intéresser aux calculateurs qui deviendront les ordinateurs), les logiciens proposèrent une théorie du calcul ; celle-ci allait fournir quelques munitions pour ébranler les mathématiciens.

La théorie du calcul consiste à détailler mathématiquement ce qu'est un algorithme. Pour ce faire, plusieurs voies sont possibles, dont celle, très élégante, que proposa A. Turing : elle consiste à définir une machine à calcul prototypique d'une simplicité parfaite (appelée aujourd'hui machine de Turing), dont le pouvoir théorique de calcul est aussi grand que le plus puissant des ordinateurs passés ou à venir. Cette théorie précise ce qu'est un système formel et fait, grâce à cela, émerger deux grands progrès.

D'une part, on peut formuler des versions générales des théorèmes d'incomplétude de Gödel. L'article de 1931 de Gödel ne concernait que le système formel des *Principia* de B. Russell et A. Withehead, et quelques systèmes apparentés. La portée des méthodes qu'il utilisait était à identifier, ce que fit la théorie du calcul en précisant ce qu'est un mécanisme de preuve dans un système formel.

D'autre part, la théorie du calcul conduisit à formuler dans chaque système formel une multitude de propositions indécidables ayant un sens proche des préoccupations des mathématiciens, et certainement plus troublantes pour un mathématicien que les énoncés proposés initialement par Gödel.

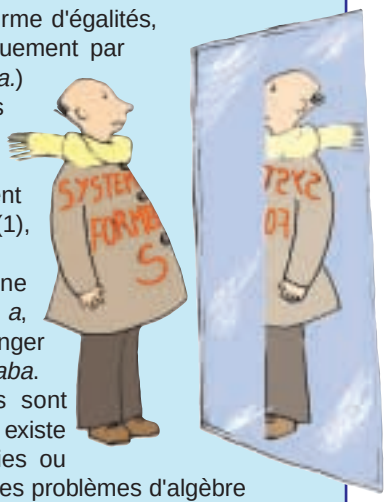
Bourbaki concerné?

Donnons quelques exemples d'indécidables parmi les centaines provenant de cette théorie du calcul. Nous nous fixons un système formel S (par exemple, celui de la théorie des ensembles que Bourbaki utilise, mais ce pourrait être celui de l'arithmétique de Peano, ou un autre encore) dont nous supposons qu'il est consistant (lorsque S est inconsistant, tout est vrai et faux à la fois, et donc rien d'intéressant ne se produit dans S).

1. EXEMPLE D'ALGÈBRE INDÉCIDABLE

En algèbre, on utilise des structures (qu'on appelle des semis-groupes) qui sont définis par la donnée de symboles, ici trois, a, b et c, et par des lois qui sont des égalités, ici également au nombre de trois : *(1)* $ab = bc$, *(2)* $b = ccc$, *(3)* $bb = b$. Ce sont les tables de la loi.

Quelles sont les autres lois, exprimées sous forme d'égalités, que nous pouvons obtenir en procédant uniquement par substitution? (Attention, ab n'est pas égale à ba.) Peut-on, par exemple, en utilisant les égalités ci-dessus et aucune autre arriver à la nouvelle égalité : $aaab = b$?



La réponse est oui : en utilisant successivement les égalités 1, 2 et 3, on obtient, en partant de (1), $aaab = aabc = abcc = bccc = bb = b$.

On démontre, avec ces égalités, que l'on ne trouvera jamais $aba = a$. En effet, partant de a, aucune des trois équations ne permet de changer quoi que ce soit, et l'on ne parviendra jamais à aba.

Ainsi, on démontre que certaines équations sont vraies et que d'autres sont fausses, mais il en existe dont on ne peut démontrer qu'elles sont vraies ou fausses : aussi élémentaires qu'ils paraissent, ces problèmes d'algèbre engendrent l'indécidabilité. Pour tout système formel donné, il existe un ensemble fini E_S d'équations et une équation e_S telle que E_S ne permet pas de déduire e_S. Pourtant, les lois régissant S ne permettent pas de démontrer la proposition "E_S ne permet pas de déduire e_S".

2. L'INDÉCIDABILITÉ AVEC DES JEUX

On appelle jeu diophantien un jeu du type suivant : une équation est fixée, par exemple : $7(b_1 + a_2) + 3 + a_1 + a_3 = (b_2 + 2)(b_3 + 2) + a_1 + a_3$.

Le joueur A choisit un nombre entier positif pour a_1.
Le joueur B choisit un nombre entier positif pour b_1.
Le joueur A choisit un nombre entier positif pour a_2.
Le joueur B choisit un nombre entier positif pour b_2.
Le joueur A choisit un nombre entier positif pour a_3.
Le joueur B choisit un nombre entier positif pour b_3.
La partie est alors terminée.

Si l'équation est vérifiée, B a gagné ; si elle ne l'est pas, A a gagné.

En analysant le jeu correspondant à l'équation indiquée, on voit que A gagnera toujours. Justification. Le premier choix de A est sans importance, car a_1 se simplifie. Le joueur B propose ensuite un nombre b_1. Le joueur A doit choisir alors un nombre a_2 tel que $7(b_1 + a_2) + 3$ soit un nombre premier. C'est toujours possible, puisqu'il existe une infinité de nombres premiers de la forme $7n + 3$. À partir de là, B ne pourra plus s'arranger pour que l'égalité soit vérifiée, car si l'égalité était vérifiée, après simplification de a_1 et a_3 elle donnerait une décomposition de $7(b_1 + a_2) + 3$ en deux facteurs >1, ce qui est impossible puisque $7(b_1 + a_2) + 3$ est premier. Le joueur A a donc gagné.

À chaque équation correspond un jeu. Dans un tel jeu à information complète, on sait qu'il existe pour chaque équation une stratégie gagnante pour l'un des deux joueurs : soit A possède la possibilité de toujours gagner, soit c'est B.

Bien que le nombre d'échanges soit fini et connu à l'avance, ces jeux diophantiens sont difficiles à analyser. En fait, d'après un résultat d'indécidabilité de Matiiassevitch, aucune méthode générale ne permet de mener l'analyse de tous ces jeux : à chaque système formel S correspond au moins un jeu diophantien dont l'analyse est infaisable dans S. Précisément : à chaque système formel S, on peut associer une équation gagnante pour B, et un premier coup pour le joueur A tel que la formule indiquant ce que B doit jouer en réponse à ce premier coup est une proposition indécidable de S.

– On peut écrire un programme *pro* (ou une machine de Turing) qui ne s'arrête pas, mais tel que l'énoncé de *S* qui exprime «*pro* ne s'arrête pas» est indécidable dans *S*. Dit en bref dans le cas particulier du système formel de Bourbaki : Bourbaki n'est pas assez puissant pour comprendre le comportement du programme *pro*.

– On peut construire un ensemble fini de formes géométriques simples *ens* (chaque forme a un bord polygonal, possède des sommets à coordonnées entières et est disponible en quantité illimitée) avec lesquelles on peut paver le plan sans interstice ni chevauchement, et pourtant l'énoncé qui exprime l'existence de ce pavage n'est pas démontrable dans *S* : Bourbaki ne voit pas qu'avec les formes de *ens* on pave le plan.

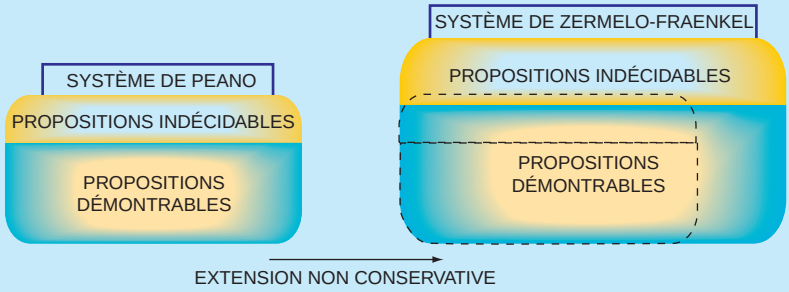
– On peut définir un jeu à information complète *jic* (le jeu de dame ou le jeu d'échecs sont de tels jeux) tel que le second joueur possède une stratégie gagnante, mais telle aussi que *S* soit incapable de voir comment répliquer correctement à certains coups initiaux du premier joueur. Bourbaki, même s'il continue à développer son traité pendant plus de 1 000 ans, ne connaîtra jamais la stratégie gagnante au jeu *jic*... alors qu'elle existe.

– Certaines égalités algébriques ne sont pas vraies, mais *S* ne sait pas le démontrer. En bref, les méthodes de preuves qu'utilise le traité de Bourbaki, même lorsqu'il s'intéresse à des problèmes algébriques simples, sont parfois aveugles.

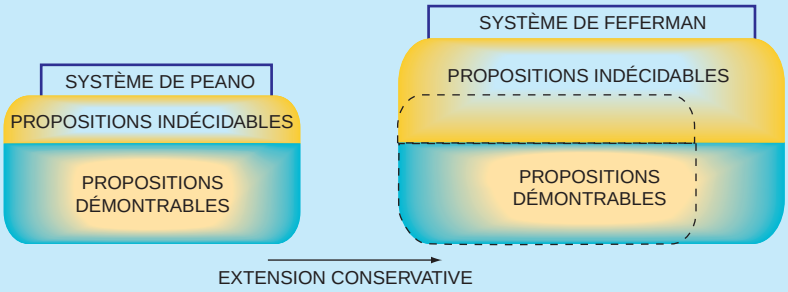
– Certaines propriétés élémentaires concernant des produits de matrices sont indécidables dans *S* (il s'agit d'un résultat récent de V. Blondel et J. Tsitsiklis).

Même dans des parties élémentaires des mathématiques, Bourbaki ne pourra jamais démontrer tout ce qui est vrai.

3. CONSERVER LES MÊMES INDÉCIDABLES



Quand on passe de l'arithmétique de Peano (PA) à la théorie des ensembles de Zermelo-Fraenkel (ZF), on étend le domaine des objets que l'on peut traiter. On augmente alors le nombre de formules d'arithmétique que la théorie peut démontrer, et il y a donc moins de formules arithmétiques indécidables. Hélas, ce faisant, on risque de démontrer des formules absurdes telles que 0 = 1, ce qui signifierait que le nouveau système est inconsistant. L'augmentation du pouvoir de preuve que donne une telle extension dite non conservative s'accompagne d'une prise de risque.



En revanche, quand on passe de l'arithmétique de Peano (PA) à une extension conservative du type de celles proposées par S. Feferman ou S. Simpson, on étend le domaine d'objets que l'on peut traiter (ce qui permet, par exemple, de développer l'analyse classique), mais cette fois sans augmenter le nombre de formules arithmétiques que la théorie peut démontrer (les formules arithmétiques indécidables restent donc les mêmes). Cette attitude prudente empêche d'introduire une inconsistance (si le nouveau système était inconsistant, on y démontrerait la formule 0 = 1, ce qui signifierait que PA le démontre aussi : donc si PA est consistant, le nouveau système aussi). La découverte qu'on pouvait mener l'essentiel des mathématiques utiles aux sciences de la nature dans de telles extensions prudentes conduit à s'interroger sur le sens des autres extensions : en plus d'être dangereuses, ne sont-elles pas illusoires ?

LA COMPLEXITÉ EST INDÉCIDABLE

D'autres avancées de la théorie du calcul ont conduit depuis 1965 au développement de la théorie de la complexité de Kolmogorov, où l'on définit la complexité d'une séquence *s* composée uniquement de 0 et de 1, par la taille *K(s)* du plus court programme qui engendre *s*.

Cette théorie, pourtant importante sur le plan pratique (car c'est la théorie mathématique de la compression de données qui, on le sait, concerne toutes les technologies de l'information), est un remarquable nid d'indécidabilité. Certaines situations sont même profondément troublantes, comme celle-ci. Il existe une infinité de propositions du type «la séquence *s* possède la complexité *n*», certaines sont exactes et d'autres fausses. Non seulement un système formel donné passe à côté de certaines formules vraies de ce type, mais il ne peut en démontrer qu'un nombre fini (ces résultats ont été établis pas N. Kolmogorov et G. Chaitin). La complexité de Kolmogorov échappe gravement à tout système formel qui, par nature, n'en connaîtra qu'une partie finie.

En particulier, en exploitant au mieux les ressources que donne le traité de Bourbaki, il arrivera un moment où il aura déduit tout ce qu'il pouvait sur la complexité des séquences *s* : il aura réussi à identifier quelle était la complexité *K(s)* pour certaines suites *s* en nombre fini, par exemple $K(010101) = 3$, $K(01101001110) = 12$, mais il ne pourra pas prouver un seul résultat de plus de ce type. Récemment, certains travaux de G. Chaitin conduisent à évaluer que Zermelo-Fraenkel (donc cela s'applique à Bourbaki) ne pourrait jamais démontrer qu'aucune séquence *s* ne possède une complexité de Kolmogorov supérieure à 100 000. Notons pourtant que Zermelo-Fraenkel permet de montrer l'énoncé «il existe une infinité de *s* ayant une complexité supérieure à 100 000».

La situation n'est pas la marque d'une contradiction dans Zermelo-Fraenkel, mais celle de l'incomplétude.

EFFROYABLE ÉQUATION

Un autre domaine où l'indécidabilité a été explicitée par la théorie du calcul est celui des équations arithmétiques. Citons le résultat de G. Chaitin, qui a construit explicitement et a fait imprimer pour de vrai (j'en ai une copie que je garde