

LOGIQUE & CALCUL

Des indécidables à portée de main

Les énoncés dont on ne peut prouver ni qu'ils sont vrais ni qu'ils sont faux semblent moins rares qu'on ne l'imaginait : de tels « indécidables », redoutés par les mathématiciens, ont été trouvés avec des problèmes portant sur de petites machines de Turing.

Jean-Paul DELAHAYE

Si un problème mathématique paraît assez simple, comme « Est-ce que, pour tout entier positif n , $4n^4 + 1$ est un nombre premier ? », le mathématicien ne doute pas qu'il saura le résoudre. Bien sûr, d'un mathématicien à l'autre, cette perception de ce qui est facile et de ce qui ne l'est pas change, et plus un mathématicien est compétent, plus nombreux sont les problèmes qu'il est capable de classer en « facile » ou « probablement difficile ».

Il se trouve cependant que même les meilleurs des mathématiciens sont impuissants à évaluer la difficulté de questions à l'apparence élémentaire. Fermat n'avait certainement pas imaginé combien il était difficile de démontrer qu'il n'y a pas de solution à l'équation $n^q + m^q = p^q$, où n , m , p désignent des entiers positifs et q un entier supérieur à 2. De graves obstacles sont dissimulés dans des énoncés d'allure innocente. Les problèmes les plus difficiles sont ceux qualifiés d'« indécidables ». Un jeu utile et délicat est de repérer les indécidables les plus simples dans le but de mieux comprendre où cette apparition d'obstacles graves risque de se produire. Identifier où se niche leur absolue difficulté fait progresser les mathématiques aussi bien que la résolution de problèmes.

Qu'est-ce que l'indécidabilité ? Un énoncé est indécidable dans une théorie donnée si celle-ci ne peut ni démontrer l'énoncé, ni démontrer sa négation. Bien sûr, pour établir que des énoncés sont

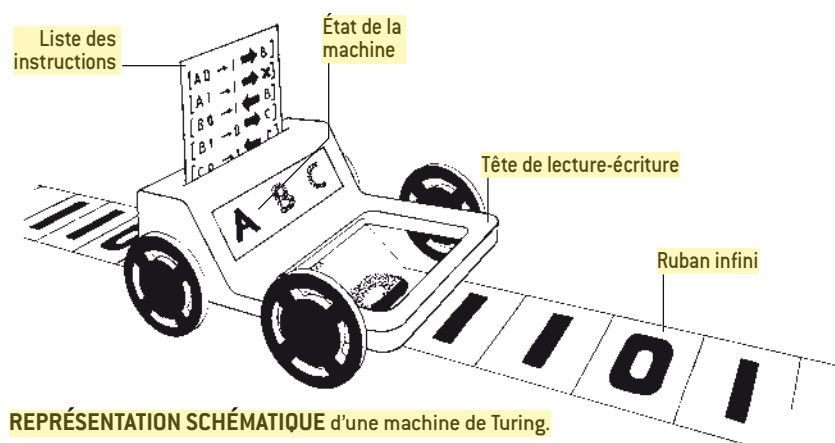
indécidables dans une théorie mathématique donnée T , il faut avoir très précisément défini cette théorie. Il faut aussi avoir acquis une maîtrise de ce qui s'y passe et, en particulier, il faut pouvoir prouver des théorèmes à propos des démonstrations !

C'est la tâche de la logique mathématique, parfois nommée métamathématique, puisqu'elle fournit une compréhension mathématique des mathématiques. Son développement aux XIX^e et XX^e siècles nous a permis de comprendre et de mesurer avec finesse le pouvoir déductif des théories.

Démontrer l'axiome des parallèles (par un point extérieur à une droite donnée D , il ne passe qu'une droite D' ne rencontrant pas D) ou sa négation à partir des autres axiomes de la géométrie du plan n'est pas possible. L'axiome des parallèles est un indécidable de la géométrie « de base », aussi

dénommée géométrie absolue, ou géométrie neutre. De même, démontrer l'« axiome du choix » et l'« hypothèse du continu » ou leur négation à partir des axiomes habituels de la théorie des ensembles est impossible. C'est un résultat obtenu en deux temps par l'Autrichien Kurt Gödel en 1938 et l'Américain Paul Cohen en 1963.

Mieux et beaucoup plus général : selon le premier théorème d'incomplétude de Gödel démontré en 1931, dès qu'une théorie mathématique T non contradictoire est capable de mener suffisamment de raisonnements arithmétiques (et c'est le cas de toutes les théories intéressantes), alors il existe des énoncés E qui ont un sens dans cette théorie et qui sont indécidables. Autrement dit, ni l'énoncé E lui-même, ni sa négation (non- E) ne sont démontrables dans T : la théorie est lacunaire, incomplète.



© P.L.S. Cassandra Vion

Plus précis, le second théorème d'incomplétude de Gödel établit que l'énoncé affirmant que la théorie T est non contradictoire est l'un des indécidables de T : une théorie n'a pas le pouvoir de démontrer d'elle-même qu'elle est non contradictoire... sauf si elle est contradictoire, auquel cas elle n'a aucun intérêt.

Ces formidables résultats de Gödel établissent que l'indécidabilité est toute proche des questions que l'on considère comme fondamentales, car la non-contradiction d'une théorie T est bien sûr la première des questions qu'on doit se poser quand on envisage cette théorie.

Cependant, ces énoncés ne sont simples que par leur sens : la non-contradiction d'une théorie est toujours assez complexe. On l'exprime souvent sous la forme : « Jamais une suite de formules obtenues en suivant les règles de raisonnement de la théorie ne conduira à la formule $0 = 1$. » Or traduire une telle affirmation en un énoncé arithmétique exige qu'on traduise d'abord les

règles de raisonnement de T , ce qui demande un travail délicat et long dénommé arithmétisation de la syntaxe et dont l'invention est due à Gödel.

Indécidabilité avec des énoncés simples ?

Pour évaluer la proximité de l'indécidabilité, les logiciens ont donc recherché des énoncés simples dont on puisse prouver l'indécidabilité. Récemment, de nouveaux résultats permettent d'évaluer le risque d'une rencontre avec un indécidable que certains mathématiciens considéraient comme improbable. Nous allons voir plus loin que l'énoncé concernant la fonction $s(n)$ de Radó, qui permettrait d'en connaître la valeur pour l'entier 1 919, est indécidable dans la puissante théorie classique des ensembles : $s(1\,919)$ est définitivement inconnaisable pour le mathématicien qui voudrait mener tout son travail avec la théorie classique des ensembles.

Pour expliquer ces nouveaux résultats, nous utiliserons les machines introduites par Alan Turing en 1936. Une machine de Turing est un automate qui peut se trouver dans un nombre fini d'états, par exemple l'état A , B ou C si ce nombre est 3. L'automate dispose d'un ruban découpé en cases. Sur le ruban, la tête de lecture-écriture de la machine lit et écrit des symboles qui viennent éventuellement effacer des symboles déjà inscrits. La machine n'a accès qu'à une seule case à la fois et déplace sa tête de lecture-écriture d'une case dans un sens ou dans l'autre. Elle parcourt ainsi le ruban pour y opérer un calcul.

Le programme de la machine est une liste finie d'instructions. Chacune est du type $[A \ 0 \rightarrow 1 \text{ droite } B]$ qui signifie : « Quand je suis dans l'état A , que je lis 0 dans la case que je suis en train d'examiner, alors j'écris 1 dans cette case, je déplace la tête de lecture-écriture d'une case vers la droite et je passe dans l'état B . »

Le castor affairé à 3 états

Un castor affairé à n états est une machine de Turing à n états qui fonctionne le plus longtemps possible (pour une machine à n états) et qui s'arrête.

Le programme du castor affairé à 3 états comporte 6 instructions. Il a été trouvé par Tibor Radó. Il écrit cinq « 1 » successifs et fonctionne 21 fois avant de s'arrêter.

Aucune machine de Turing à 3 états ne fonctionne plus de 21 fois avant de s'arrêter, sauf si elle ne s'arrête jamais.

Les 6 instructions du programme du castor affairé à 3 états sont les suivantes :

- [A $0 \rightarrow 1$ droite B],
- [A $1 \rightarrow 1$ droite ARRÊT],
- [B $0 \rightarrow 1$ gauche B],
- [B $1 \rightarrow 0$ droite C],
- [C $0 \rightarrow 1$ gauche C]
- [C $1 \rightarrow 1$ gauche A].

Voici comment il faut lire ce programme et le faire fonctionner. La machine (comme celle schématisée page ci-contre) est posée sur un ruban recouvert de 0 doublement infini (vers la droite et vers la gauche).

Supposons-la dans l'état A , et que sa tête de lecture-écriture lit un 0. L'instruction à appliquer est donc la première instruction [A $0 \rightarrow 1$ droite B] de son programme,

qui indique que le 0 lu doit être remplacé par un 1, que la tête de lecture-écriture doit se déplacer d'une case vers la droite, et que le nouvel état de la machine doit être B . On a ainsi, en supposant que la machine débute sa lecture à la quatrième case et en marquant en rouge la position de la tête de lecture-écriture :

État initial

A - 00000000000000000000000000000000...

État atteint

B - 00010000000000000000000000000000...

La machine est maintenant dans l'état B et lit un 0. Elle applique donc la 3^e instruction [B $0 \rightarrow 1$ gauche B], ce qui conduit à la situation :

B - 00011000000000000000000000000000...

Le calcul se poursuit alors. Voici l'ensemble du calcul jusqu'à l'arrêt :

```
A - 00000000000000000000000000000000...
B - 00010000000000000000000000000000...
B - 00011000000000000000000000000000...
C - 00001000000000000000000000000000...
A - 00001000000000000000000000000000...
B - 00011000000000000000000000000000...
C - 00010000000000000000000000000000...
C - 00010100000000000000000000000000...
C - 00011000000000000000000000000000...
A - 00011100000000000000000000000000...
B - 00111100000000000000000000000000...
C - 00101100000000000000000000000000...
A - 00101100000000000000000000000000...
B - 00111100000000000000000000000000...
C - 00110100000000000000000000000000...
A - 00110100000000000000000000000000...
B - 00111100000000000000000000000000...
C - 00111000000000000000000000000000...
C - 00111010000000000000000000000000...
C - 00111100000000000000000000000000...
A - 00111100000000000000000000000000...
ARRÊT - 0011111000000000000000000000...
```