

précieusement) une équation terriblement indécidable (voir l'encadré 5).

L'équation est terriblement indécidable, car G. Chaitin a démontré qu'un système formel donné S ne peut jamais résoudre qu'un nombre fini de cas de l'équation, tous les autres cas étant indécidables dans S . Les moyens de preuve définis au début du traité de Bourbaki atteindront donc un jour une limite absolue face à cette équation. Même si le traité se développe pendant un milliard d'années, au-delà d'un certain point d'élucidation maximale, il ne permettra plus jamais de régler un seul cas supplémentaire de l'équation.

QUE RÉPONDEZ-VOUS DONC À ÇA ?

Quelle est la réponse des mathématiciens face à cet arsenal de résultats d'indécidabilité qui ont envahi chaque spécialité mathématique ?

Ils répondent qu'à chaque fois tout cela est construit sur du codage. Le programme qui ne s'arrête pas, le jeu à information complète que Bourbaki ne réussit pas à analyser, l'équation indécidable dont on ne peut traiter qu'un nombre fini de cas, etc., tout cela provient à chaque fois du déguisement avec les notations de divers domaines mathématiques, des indécidables originaux trouvés par Gödel et Turing. À chaque fois, les objets en cause sont complexes et longs à écrire (l'équation de Chaitin, avec ses 12 000 variables, battant tous les records). Les mathématiciens spécialistes d'équations diophantiennes ne se seraient jamais intéressés d'eux-mêmes aux équations que les logiciens aidés de la théorie du calcul leur mettent sous le nez. Les mathématiciens répondent donc : «Les indécidables que vous construisez sont artificiels et toutes vos constructions ne peuvent nous forcer à croire que nos propres problèmes, ceux que nous rencontrons dans le cours normal du développement de nos théories, risquent d'être indécidables.»

Face à cette réponse, les logiciens devaient dégager les indécidables de tout codage.

INDÉCIDABLES DE J. PARIS ET L. HARRINGTON

Cela se produisit, il y a une vingtaine d'années, quand plusieurs énoncés arithmétiques simples et dégagés de tout codage furent démontrés indécidables vis-à-vis de l'arithmétique de Peano (voir l'énoncé indécidable concernant les hydres cité dans la rubrique du mois de novembre).

Nombreux furent ceux, y compris parmi les mathématiciens, qui reconnurent alors qu'un pas important avait été franchi.

Malgré ces progrès, certains mathématiciens ont eu beau jeu de remarquer que les indécidables arithmétiques dégagés du codage inventés par les logiciens n'avaient jamais été envisagés spontanément par les mathématiciens. On parla d'énoncés «cuisinés exprès».

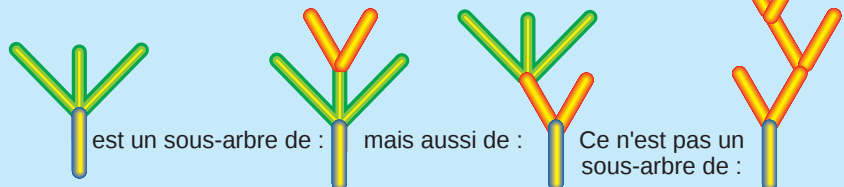
Ces énoncés sont, là encore, des constructions de logiciens. De plus, dans la grande majorité des cas, il s'agit d'indécidables de l'arithmétique de Peano décidables dans Zermelo-Fraenkel, et non pas d'indécidables de Zermelo-Fraenkel. Il manque donc encore un cas incontestable d'énoncé que les spécialistes d'arithmétique considèrent intéressant avant que les logiciens ne s'y intéressent et sur lequel ils travaillent, que les logiciens démontreraient indécidable vis-à-vis de l'arithmétique de Peano (qui

est la théorie naturelle pour écrire les raisonnements d'arithmétique) ou, mieux, indécidable avec Zermelo-Fraenkel.

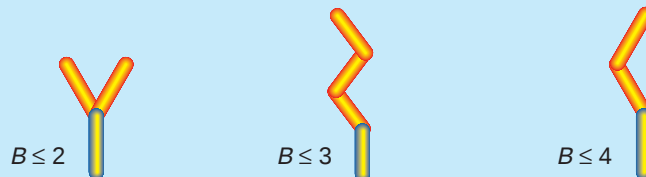
Les candidats ne manquent pas. Il y a d'une part les résultats d'arithmétique qu'on démontre avec des outils plus puissants que ceux de l'arithmétique de Peano. C'est le cas de nombreux théorèmes concernant les nombres premiers dont les premières démonstrations – qualifiées de transcendantes – utilisaient des techniques d'analyse formalisable dans la théorie Zermelo-Fraenkel, mais pas dans Peano. Pour plusieurs d'entre eux, on sait aujourd'hui que l'on peut en fait les démontrer dans l'arithmétique de Peano. Ces énoncés ne constitueront donc pas des propositions envisagées spontanément par les mathématiciens, démontrables dans Zermelo-Fraenkel, indécidables dans

4. LES ARBRES DE KRUSKAL

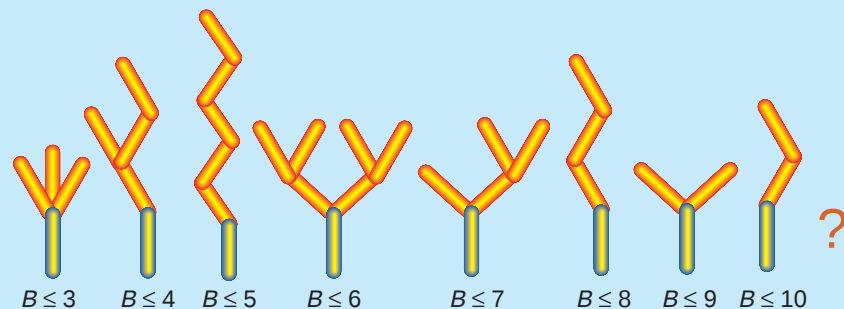
Un arbre est dit sous-arbre d'un autre si on peut retrouver la forme du premier dans le second.



On cherche à construire des séries d'arbres tels qu'aucun ne soit le sous-arbre d'un arbre placé plus loin. Une telle série d'arbres est dite correcte.



On dit qu'une série est de type 2 si le premier arbre possède deux branches au plus, le second trois branches au plus, etc. En construisant des séries correctes de type 2, on s'aperçoit qu'elles n'ont jamais plus de quatre arbres.



Une série est de type 3 si le premier arbre possède trois branches au plus, le second quatre branches au plus, etc. On s'aperçoit, là aussi, qu'on ne peut jamais prolonger indéfiniment les séries correctes de type 3.

Le théorème de Kruskal indique que, «pour tout entier n supérieur à 1, il existe une limite k à la longueur des séries correctes de type n ».

Cet énoncé ne contient aucun codage déguisé de proposition logique. C'est pourtant un énoncé indécidable de l'arithmétique de Peano. Cet énoncé est l'un de ceux qui auraient dû convaincre les mathématiciens que, même à propos de problèmes simples et naturels, l'indécidabilité peut surgir.



Gregory Chaitin

5. LES INDÉCIDABLES DE LA COMPLEXITÉ

Même le plus puissant système formel ne peut traiter qu'un nombre fini de cas de l'équation de Chaitin.

Gregory Chaitin a construit et fait imprimer une équation indécidable. L'équation est à coefficients entiers et ne fait intervenir que des additions, des multiplications et des exponentiations (une équation simple de ce type serait : $n - x^y + 3y + 2t = 0$). On ne s'intéresse qu'aux solutions en nombres entiers de l'équation. L'équation dépend d'un paramètre n et possède 12 000 variables ; on peut la résumer en écrivant : $P(n, x_1, x_2, x_3, \dots, x_{12000}) = 0$.

Pour chaque valeur de n , l'équation possède une infinité de solutions ou n'en possède qu'un nombre fini. On dit que "l'équation est résolue pour n " si on réussit à savoir dans lequel des deux cas on se trouve. G. Chaitin a démontré qu'un système formel donné S ne peut jamais résoudre qu'un nombre fini de cas de l'équation, tous les autres cas étant indécidables dans S . Pour avancer dans la résolution de cette équation, les mathématiciens seront indéfiniment obligés d'ajouter de nouveaux axiomes à leurs théories.

Peano. Pour le grand théorème de Fermat, la question est ouverte : la démonstration actuelle utilise des méthodes qui dépassent l'arithmétique de Peano, et l'on ne sait pas la retranscrire dans Peano.

Les conjectures considérées par les arithméticiens (conjectures des nombres premiers jumeaux, conjecture de Riemann, conjecture de Goldbach, etc.) sont peut-être des indécidables de l'arithmétique de Peano ou de Zermelo-Fraenkel. Personne n'a su le démontrer, et aucune piste ne semble ouverte. Force est de constater ici l'échec des logiciens : finalement aucun argument définitif n'a été fourni aux mathématiciens sceptiques, et la plupart des arithméticiens restent donc persuadés que la question de l'indécidabilité ne se pose pas vraiment pour les conjectures non démontrées. Au pire, pensent-ils, ces conjectures seront indécidables dans Peano, mais décidables dans Zermelo-Fraenkel. Le débat n'est donc pas clos.

AUTRES EXTENSIONS DE L'ARITHMÉTIQUE

Une explication de cette situation est suggérée par certains travaux récents des logiciens S. Feferman et S. Simpson qui se sont intéressés à des types nouveaux d'extension de l'arithmétique.

Lorsqu'on envisage d'étendre le pouvoir de l'arithmétique pour inclure les nombres réels, des fonctions continues et des objets complexes que l'analyse utilise, la méthode usuelle, adoptée par Bourbaki et par la quasi-totalité des mathématiciens, consiste à passer à la théorie des ensembles Zermelo-Fraenkel. La puissance de Zermelo-Fraenkel provient de l'axiome de l'infini, car on sait que si l'on prend Zermelo-Fraenkel et qu'on y remplace l'axiome «il existe un ensemble

infini» par l'axiome «il n'existe pas d'ensemble infini», on obtient alors un système équivalent à Peano.

L'extension de Peano à Zermelo-Fraenkel augmente le domaine d'objets mathématiques que le mathématicien peut traiter, mais accroît le risque de l'inconsistance dans le sens suivant : Zermelo-Fraenkel pourrait être inconsistant et Peano consistant, alors que l'inverse est impossible (car la consistance de Zermelo-Fraenkel permet de prouver celle de Peano, mais pas l'inverse).

Autrement dit, en passant de Peano à Zermelo-Fraenkel, le mathématicien enrichit les objets au prix d'un risque nouveau de contradiction. Si la situation était inévitable, ce qu'on a cru longtemps, nous accepterions ce risque sans hésitation, car nul ne souhaite renoncer aux résultats de l'analyse, qui sont si importants en physique et dans les applications des mathématiques. Cependant il existe un autre type d'extensions de l'arithmétique qui ne prend pas de risque et qui pourtant permet aussi de faire de l'analyse et de développer toutes les mathématiques nécessaires aux physiciens.

Ainsi, S. Feferman et S. Simpson ont mis à la disposition des mathématiciens des versions de l'analyse où l'on retrouve des résultats classiques (théorie classique des fonctions continues, existence de solution des systèmes différentiels, etc.) et tous les objets et méthodes utiles aux développements des mathématiques servant dans les sciences de la nature.

Ces systèmes sont un peu plus complexes à utiliser que Zermelo-Fraenkel, mais leur intérêt est immense. Ils montrent, d'une part, que d'autres voies que celle un peu brusque de la théorie des ensembles sont praticables et suffisent pour fonder et développer les mathéma-

tiques dont les sciences ont besoin. D'autre part, ils montrent que ce n'est peut-être pas par hasard si ce qui intéresse spontanément les mathématiciens quand il s'agit d'arithmétique n'a jamais été prouvé indécidable vis-à-vis de Peano.

Certaines extensions prudentes possèdent les mêmes indécidables arithmétiques que Peano, aussi s'interroge-t-on : les extensions prudentes ne sont-elles pas la voie raisonnable et réaliste d'extension de Peano ? La voie de Zermelo-Fraenkel correspondrait à une illusion infinitaire, commode, mais imprudente, voire trompeuse. Les indécidables de l'arithmétique de Peano seraient indécidables pour de bonnes raisons, et les mathématiciens ne s'intéresseraient jamais spontanément à des indécidables de Peano parce que ils resteraient dans le monde des mathématiques applicables, où les indécidables de Peano sont indécidables.

Pour faire de la physique, seules certaines parties des mathématiques sont utiles ; pour des raisons de commodité, on utilise Zermelo-Fraenkel qui est inutilement puissant. Cette puissance a pour effet (peut-être malencontreux) de diminuer le nombre des indécidables ; ne considérer que les systèmes formels juste assez puissants pour faire de la physique ne conduit pas à la suppression d'indécidables. Il y a peut-être une raison profonde, mal comprise aujourd'hui, à cette situation : il se pourrait que seuls les systèmes qui gardent les mêmes indécidables (les extensions conservatrices de Peano correspondent aux «vraies mathématiques», ce que, instinctivement, les mathématiciens avaient compris).

Tout cela est bien mystérieux et compliqué. S'astreindre à ne considérer que des systèmes qui maintiennent les mêmes indécidables plutôt que de vouloir s'en débarrasser (chose de toutes les façons impossible, on le sait) non seulement limiterait les risques d'inconsistance, mais éviterait d'entrer dans un monde abstrait irréel et peut-être insensé, et en tout cas inutile à l'applicabilité des mathématiques.

V. BLONDEL et J.N. TSITSIKLIS, *The Boundedness of All Products of a Pair of Matrice is Undecidable*, rapport de recherche de l'Université de Liège, 1999.

G. CHAITIN, *The Limits of Mathematics*, Springer-Verlag, 1997.

J.-P. DELAHAYE, *Information, complexité et hasard*, Hermès, Paris, 1994 et 1999.

J.-L. KRIVINE, *Théorie des ensembles*, Nouvelle bibliothèque mathématique, Cassini, Paris, 1998.

Y. MATHIASSEVITCH, *Le dixième problème de Hilbert et son indécidabilité*, Masson, 1995.