AKG Paris

Promenade au pays des indécidables

JEAN-PAUL DELAHAYE

Débat difficile entre logiciens et mathématiciens à propos de l'importance à accorder aux indécidables.

L'universalité de l'incomplétude, c'est-à-dire l'existence dans chaque système mathématique de propositions indécidables, dont les axiomes du système ne permettent de prouver ni la vérité ni la fausseté, est inquiétante. Depuis que ce résultat a été établi par Kurt Gödel en 1931, il a donné lieu à une multitude de commentaires *(voir l'article de cette rubrique de novembre 1999)*. Sans contester l'exactitude mathématique du résultat de Gödel, les mathématiciens y opposent une sorte de résistance passive : ils tentent de se persuader que, malgré son universalité, l'incomplétude est un phénomène marginal. Nous verrons que le débat n'est pas simple à trancher, pour des raisons profondes qui forcent à reconsidérer la nature intime des mathématiques et de son rapport avec ses applications.

La contradiction, presque un paradoxe, apparaît grande entre les logiciens qui ont, depuis 1931, construit un grand nombre d'indécidables, et les mathématiciens qui remarquent qu'aucun résultat central des mathématiques classiques, concernant par exemple l'arithmétique élémentaire, n'a été prouvé indécidable.

Le mathématicien bourbakiste Jean Dieudonné écrivait : «95 pour cent des mathématiciens se moquent éperdument de ce que peuvent faire tous les logiciens et tous les philosophes.» La vérité est-elle du côté des cinq pour cent restants?

Les indécidables s'obtiennent mécaniquement

La démonstration de K. Gödel de 1931 non seulement indique qu'il existe des indécidables pour tout système formel S consistant (c'est-à-dire non contradictoire), mais donne un moyen mécanique pour construire explicitement un indécidable I_S à partir de la description de tout système S. Grossièrement dit, cette formule est une transposition élaborée de la formule *Je mens* exprimée dans le langage de tous les jours. La méthode consiste à détailler, dans une formule de S, la description du fonctionnement de S, puis, grâce à cette description, à fabriquer une formule qui exprime *Je ne suis pas prouvable dans S* ; cette formule est indécidable dans S.

Le procédé permettant, à partir d'un système consistant S, d'obtenir l'indécidable I_S est mécanique, et donc un ordinateur peut l'élaborer.

Notons que ce point retire toute valeur aux considérations qui prétendent tirer du théorème de Gödel un argument montrant l'impossibilité logique de simuler un être humain par une machine. Cela ne signifie pas que cette simulation est possible, mais seulement que le théorème de Gödel n'apprend rien à son sujet : si l'intelligence artificielle peut exister, elle le prouvera par ses réalisations, comme celle évoquée dans cette rubrique au mois de septembre, où l'on décrivait un système informatique qui battait les humains en exploitant leur incapacité à simuler le hasard.

La construction de Gödel étant générale, c'est donc chaque système formel (assez puissant pour faire de l'arithmétique) qui est concerné. Tous les mathématiciens devraient donc se sentir menacés, y compris Nicolas Bourbaki, le mathématicien polycéphale qui, depuis plus de 50 ans, développe un traité de mathématiques qui est le plus complet jamais écrit. Toute la théorie de Bourbaki se développe dans le système formel de la théorie des ensembles de Zermelo-Fraenkel, sujette, bien sûr, à l'incomplétude. Pour suivre plus commodément l'exposé, nous caricaturerons en disant que Zermelo-Fraenkel comprend les axiomes de l'arithmétique de Peano, plus les axiomes traitant de l'infini.

Le fait que, pour tout système S consistant, l'affirmation exprimée dans S de cette consistance est un indécidable de S confirme à l'évidence que les indécidables doivent inquiéter tous les mathématiciens. En particulier, lorsqu'ils tentent de démontrer une conjecture difficile en utilisant les moyens de la théorie de Zermelo-Fraenkel, dont ils ne sortent jamais en pratique, les mathématiciens devraient se poser la question : ne sommes-nous pas en présence d'un indécidable de Zermelo-Fraenkel, et ne sommes-nous donc pas en train de perdre notre temps à vouloir prouver ce qui, avec les méthodes de Zermelo-Fraenkel, est improuvable?

Vos indécidables sont incompréhensibles

Les mathématiciens ne sont pas inquiets : une de leurs premières réponses aux logiciens consiste à dire que les énoncés indécidables construits par Gödel ne sont justement pas écrits explicitement. Gödel décrit les méthodes qu'il faut utiliser pour construire les indécidables, mais n'explicite jamais toutes les étapes de ce qu'on appelle le codage de I_S qui conduirait à mettre noir sur blanc la formule indécidable, sans raccourcis de notation ni abréviations typographiques. Jamais par exemple personne n'a vu écrit dans le formalisme utilisé par Bourbaki l'indécidable que la méthode de Gödel prétend tirer du système de Zermelo-Fraenkel utilisé par Bourbaki.

Les mathématiciens font remarquer que, si l'on menait le travail jusqu'au bout (en s'aidant de programmes, c'est concevable), on tomberait sur des propositions tellement compliquées qu'aucun mathématicien ne serait en mesure d'en percevoir le sens. Le fait est patent : sans les logiciens, personne n'aurait jamais tenté de démontrer les formules dont les logiciens disent qu'elles sont indécidables. N'étant jamais aussi complexes, il est donc possible que les énigmes sur lesquelles les mathématiciens travaillent ne soient jamais des indécidables.

Les mathématiciens marquent un point : ce que les théorèmes de Gödel leur disent être indécidable n'est pas donné explicitement par Gödel et ne correspond pas aux préoccupations authentiques des mathématiciens. Les mathématiciens 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.

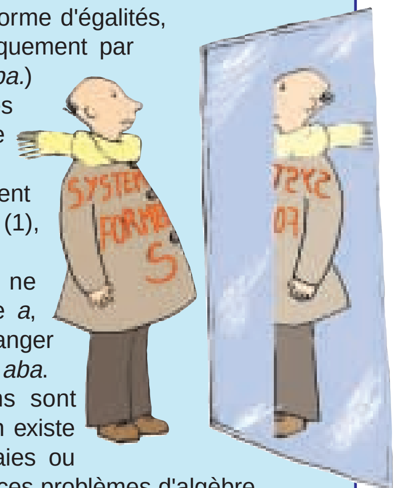
Quelles sont les autres lois, exprimées sous forme d'égalités, que nous pouvons obtenir en procédant uniquement par substitution? (Attention, ab n'est pas égale à ba.)

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 : $7(b_1 + a_2) + 3 + a_1 + a_3 = (b_2 + 2)(b_3 + 2) + a_1 + a_3$.

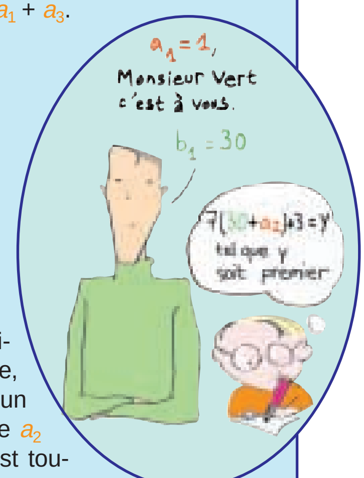
Le joueur A choisit un nombre entier positif pour a_1.
Le joueur B choisit un nombre entier positif pour b_1.
Le joueur A choisit un nombre entier positif pour a_2.
Le joueur B choisit un nombre entier positif pour b_2.
Le joueur A choisit un nombre entier positif pour a_3.
Le joueur B choisit un nombre 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*.

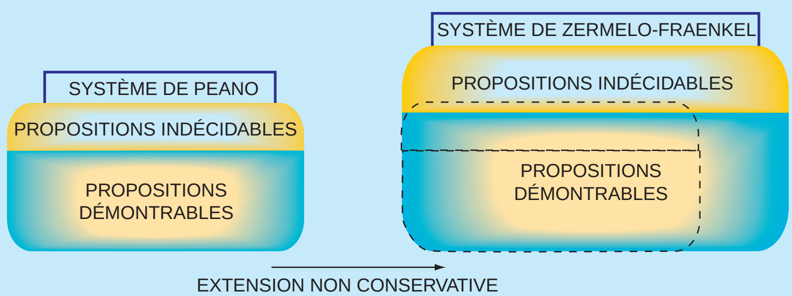
– On peut construire un ensemble fini de formes géométriques simples *ens* (chaque forme a un bord polygonal, possède des sommets à coordonnées entières et est disponible en quantité illimitée) avec lesquelles on peut paver le plan sans interstice ni chevauchement, et pourtant l'énoncé qui exprime l'existence 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.

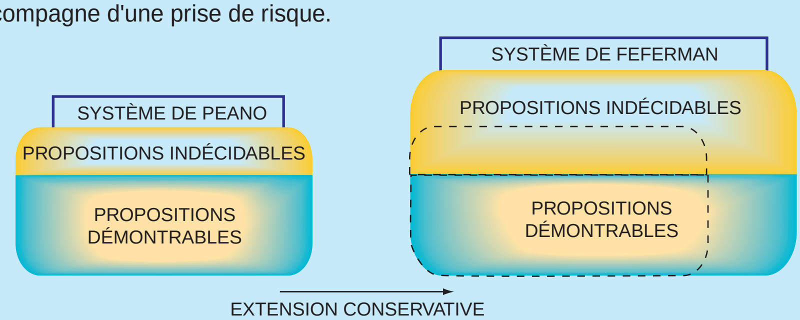
– Certaines égalités algébriques ne sont pas vraies, mais *S* ne sait pas le démontrer. En bref, les méthodes de preuves qu'utilise le traité de Bourbaki, même lorsqu'il s'intéresse à des problèmes algébriques simples, sont parfois aveugles.

– 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 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)*.

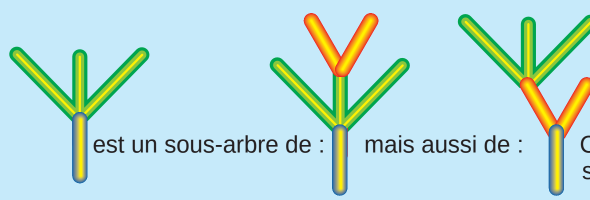
Nombreux furent ceux, y compris parmi les mathématiciens, qui reconnurent alors qu'un pas important avait été franchi. Malgré ces progrès, certains mathématiciens ont eu beau jeu de remarquer que les indécidables arithmétiques dégagés du codage inventés par les logiciens n'avaient jamais été envisagés spontanément par les mathématiciens. On parla d'énoncés «cuisinés exprès».

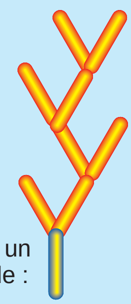
Ces énoncés sont, là encore, des constructions de logiciens. De plus, dans la grande majorité des cas, il s'agit d'indécidables de l'arithmétique de Peano décidables dans Zermelo-Fraenkel, et non pas d'indécidables de Zermelo-Fraenkel. Il manque donc encore un cas incontestable d'énoncé que les spécialistes 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

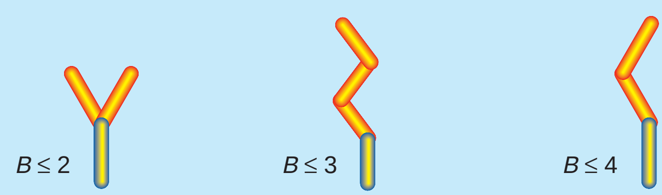
4. LES ARBRES DE KRUSKAL

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

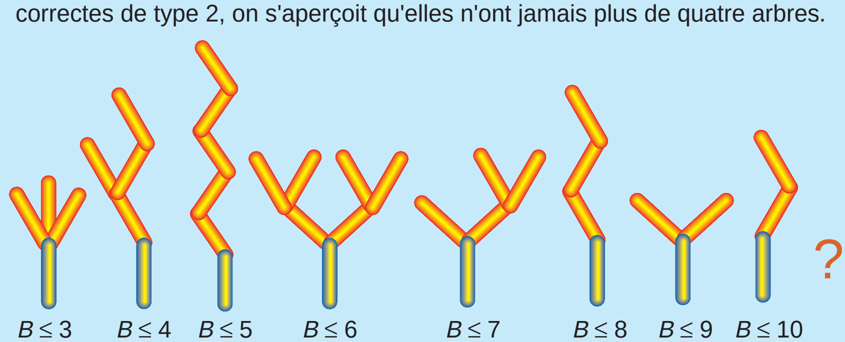




On cherche à construire des séries d'arbres tels qu'aucun ne soit le sous-arbre d'un arbre placé plus loin. Une telle série d'arbres est dite correcte.



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.

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 : $P(n, x_1, x_2, x_3, ..., x_{12000}) = 0$.

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 mathématiques 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. Matiiassevitch, *Le dixième problème de Hilbert et son indécidabilité*, Masson, 1995.