Information, complexité et hasard

Jean-Paul Delahaye
Laboratoire d'Informatique Fondamentale de Lille
URA CNRS 369

HERMES

Chapitre 6

L'importance des indécidables

Résumé

Les indécidables dont les théorèmes de Gödel de 1931 démontrent l'existence et qu'ils exhibent, ont-ils une signification réelle, ou au contraire, sont-ils des énoncés pathologiques sans intérêt autre que technique ?

Cette question posée depuis longtemps (et qui peut être entendue de plusieurs façons différentes) semble recevoir des réponses contradictoires, chacune des deux thèses pouvant trouver dans les résultats de logique mathématique récents des arguments en sa faveur (ceux en faveur de l'insignifiance sont assez élaborés mais d'autant plus intéressants).

Des indécidables de la théorie de la calculabilité qui semblent concerner toutes les parties des mathématiques et qu'on découvre par dizaines, aux indécidables de Paris-Harrington et Friedman, en passant par les indécidables de l'arithmétique pure et par les indécidables de la théorie des ensembles, nous parcourons rapidement une classification des indécidables de Gödel, en nous posant à chaque fois la question de leur signification mathématique et physique.

Malgré de nombreux résultats nouveaux, rien ne semble définitivement tranché. On peut considérer évident qu'ils sont partout, et qu'on en trouve facilement qui ont du sens. De même on peut, comme Feferman, à côté des mathématiques abstraites essayer de délimiter le domaine des "mathématiques ordinaires applicables", qui pourrait être indifférent — d'une certaine façon — aux indécidables de Gödel.

6.1. Introduction

95% des mathématiciens se moquent éperdument de ce que peuvent faire tous les logiciens et tous les philosophes.

Dieudonné 1982

Le sentiment général est que le théorème de Gödel ne concerne que les logiciens.
Solovay cité par Kolata (Kolata 1985)

La proposition indécidable A décrite par Gödel paraît très artificielle, sans lien avec aucune autre partie de la théorie des nombres actuelle ; sa principale utilité était d'établir l'impossibilité d'une preuve de la non-contradiction de l'arithmétique. Parmi les nombreuses questions classiques non résolues de la théorie des nombres, on n'a pas encore à ma connaissance établi que l'une d'elles est indécidable.

Dieudonné 1987

Ce que l'on souhaiterait, c'est qu'un grand problème irrésolu des mathématiques comme le théorème de Fermat soit démontré indécidable. Cela serait vraiment remarquable.

Joël Spencer cité par Kolata (Kolata 1985)

La croyance que la théorie de la démonstration de Hilbert fait partie intégrante de la mathématique (...) ne nous paraît pas justifiée, et nous considérons que l'intervention de la métamathématique dans l'exposé de la logique peut et doit être réduite à la partie élémentaire qui traite du maniement des symboles abréviateurs et des critères déductifs.

Bourbaki 1969

6.1.1. *Importance philosophique et importance mathématique*

Les indécidables dont les théorèmes de Gödel de 1931 démontrent l'existence et qu'ils exhibent, ont-ils une signification réelle, ou au contraire sont-ils des énoncés pathologiques sans intérêt autre que technique ?

C'est cette question que nous voulons nous poser. L'intérêt logique ou philosophique des indécidables est lié à leur intérêt mathématique et c'est donc à cet aspect particulier que nous allons principalement nous intéresser. Il se trouve en effet que bien des mathématiciens considèrent les indécidables avec prudence et les jugent comme de simples curiosités ne les concernant pas vraiment. N. Bourbaki par exemple ne les mentionne que dans ses notes historiques.

Tenter de comprendre ce que peut vouloir dire : "les indécidables sont sans véritable importance pour les mathématiques" est un défi. Il semble en effet évident que ce qui est important pour la philosophie des mathématiques — et l'impossibilité aujourd'hui d'aborder la philosophie des mathématiques sans traiter des indécidables de Gödel est admise par tout le monde — l'est aussi pour les mathématiques elles-mêmes : que veulent donc dire ceux qui refusent de prêter attention aux indécidables ?

Notre méthode sera de parcourir les différentes classes d'indécidables découvertes par les logiciens depuis 1931. A propos de chacune de ces classes, nous imaginerons un dialogue contradictoire sur l'importance des indécidables. Nous envisagerons par endroits le problème de la physique. Notre conclusion sera que si soutenir l'insignifiance mathématique des indécidables est encore possible, cela se fait toujours au prix d'un réductionnisme qui possède plusieurs formes dont les deux extrêmes sont le formalisme et le finitisme. Certaines variantes du réductionnisme comme le prédicativisme de Feferman, se nourrissant des récents résultats de la théorie de la preuve, refusent de dire leur dernier mot et prétendent même faire revivre le programme de Hilbert qu'on pensait enterré justement par les théorèmes d'indécidabilité de 1931.

Nous verrons finalement que cette question de l'importance mathématique des indécidables de Gödel concentre en elle tout le problème de la philosophie des mathématiques, en un mot que l'importance mathématique des indécidables de Gödel est un problème important ... philosophiquement !

6.1.2. *Comment définir un indécidable de Gödel*

Nous commençons par proposer une définition des "indécidables de Gödel". La définition que nous donnons n'est pas mathématique, elle a simplement pour objet de préciser un usage établi qui refuse que n'importe quel énoncé indépendant de n'importe quel système formel puisse être considéré comme un "indécidable de Gödel". Plus loin nous serons d'ailleurs amenés à préciser que parmi les indécidables de Gödel il faut encore distinguer ceux qui renforcent réellement les systèmes auxquels on les ajoute (comme les énoncés de consistance) de ceux qui sont conservatifs (comme l'axiome du choix en théorie des ensembles, ou le lemme de König).

Un *indécidable de Gödel* c'est :

un énoncé mathématique vrai et non démontrable.

Plus précisément : un *indécidable de Gödel* c'est un énoncé mathématique E tel que :

(1) E n'est pas démontrable dans un système formel S1 qui permet de l'exprimer ;

(2) on peut montrer (dans un système formel S2) la non-prouvabilité de E ;

(3) on peut montrer (dans un système formel S3) que E est vrai ;

(4) le système S1 est une *axiomatisation raisonnable* d'un champ mathématique donné et reconnu comme intéressant, et on a pu penser que cette axiomatisation formalisait bien le champ en question, (comme l'arithmétique de Peano du premier ordre vis-à-vis de l'arithmétique). Cette condition est réalisée si on a cru à un moment donné que S1 est une axiomatisation complète du champ en

question. Cette condition est aussi satisfaite si certains soutiennent que tous les énoncés intéressants (dans un sens à préciser) du champ en question sont prouvables avec S1. Beaucoup de mathématiciens pensent que ZF + AC par exemple permet d'exprimer et de démontrer tout énoncé mathématique vraiment intéressant. La condition (4) sert à éviter qu'on appelle "indécidable de Gödel" n'importe quel axiome indépendant d'un système S1 clairement trop faible : l'axiome des parallèles par exemple n'est pas considéré comme un indécidable de Gödel, de même l'axiome de l'infini n'est pas un indécidable de ZF-{axiome de l'infini} ;

(5) le système S2 est un système dont on a certaines raisons de penser qu'il est consistant (par exemple ZF + AC) ;

(6) le système S3 est un système raisonnable dont on a aussi certaines raisons de penser qu'il est consistant. Dans le cas de certains axiomes des grands cardinaux en théorie des ensembles, les raisons de croire à la consistance de S3 sont assez ténues (car S3 est obtenu en ajoutant un axiome de grand cardinal à ZF + AC), il y a même des cas où la consistance de S3 est douteuse.

6.2. Classification des indécidables de Gödel

Dans ce paragraphe nous présentons une classification des indécidables de Gödel et pour chaque type d'indécidables, nous imaginons un petit dialogue entre **Monsieur Insignifiance** qui ne trouve aucun intérêt mathématique réel à ces indécidables, et **Monsieur Importance** qui lui leur trouve un sens et défend l'idée qu'ils sont d'authentiques résultats mathématiques. Les dialogues sont quelque peu naïfs, sauf à propos des derniers éléments de la classification où ils prennent un tour un peu plus technique.

6.2.1. *Les indécidables du premier théorème d'incomplétude*

Ils ont un sens simple, moyennant des considérations métamathématiques sur la prouvabilité. Ils signifient en effet :

je ne suis pas démontrable dans S1

Le système formel S1 peut être n'importe quelle extension (primitive récursive) du système Q de Robinson qui est un système plus faible que PA (l'arithmétique du premier ordre de Peano) et même que PRA (l'arithmétique primitive récursive). Voir par exemple (Boolos Jeffrey 1980) pour des définitions précises. La restriction aux extensions primitives récursives n'est pas une véritable restriction.

Ils sont démontrés exister, mais mieux que cela, ils sont produits effectivement : si S1 est donné, la démonstration de Gödel permet d'expliciter un indécidable de S1.

Pour S2 on peut prendre S1+consistance(S1). Dans la démonstration originale de Gödel S3 est plus fort que S1+consistance(S1) puisque Gödel utilisait l' -consistance de S1 (l'impossibilité dans S3 de démontrer n P(n) en même temps que nonP(0) nonP(1) etc.). C'est Rosser 1936 qui, en modifiant l'énoncé de Gödel (qui n'a alors plus un sens simple), a permis de prendre S2=S3= S1+consistance(S1).

Les formulations (données par Kleene) du premier théorème de Gödel utilisant les concepts de la théorie de la récursivité sont très intéressantes, elles s'appliquent à tout système formel, et éclairent le phénomène de l'indécidabilité qu'on peut résumer en disant :

- l'ensemble des vérités de l'arithmétique du premier ordre n'est pas récursivement énumérable,
- l'ensemble des théorèmes que peut démontrer un système formel est toujours récursivement énumérable (à cause des conditions d'effectivité qu'on impose aux systèmes formels : il faut qu'un procédé mécanique puisse vérifier si une suite donnée de formules est bien une démonstration),
- donc aucun système formel ne peut à la fois produire que des vérités de l'arithmétique du premier ordre et les produire toutes (voir chapitre 3).

Monsieur Insignifiance : Ces énoncés étranges qui affirment leur propre indémontrabilité au travers d'un codage épouvantable, sont des divertissements mathématiques amusants et non des mathématiques.

Monsieur Importance : Le paradoxe du menteur, et les paradoxes de la théorie des ensembles qui se présentent sous des formes très proches ont touché les mathématiciens du début du siècle, qui y ont vu plus que des divertissements insignifiants ; alors pourquoi refuser de considérer comme authentiquement mathématiques ces premiers indécidables. Il est dans la nature des mathématiques de s'intéresser à toutes les conséquences qu'on peut tirer des méthodes de raisonnement dont elles disposent. Ce que fait le premier théorème de Gödel, ce n'est que cela.

6.2.2. *Les indécidables du second théorème d'incomplétude*

> *Je considère Hilbert comme un mathématicien et donc son problème de consistance comme un problème de mathématiques.*
>
> *Smorynski 1982*

> *Je ne connais aucun cas où quelque chose d'un intérêt mathématique clair peut être démontré à partir de T + cons(T) alors qu'il ne peut pas l'être à partir de T seulement (à l'exception bien sûr de cons(T) lui-même)*
>
> *Drake 1985*

Les indécidables du second théorème d'incomplétude, qui sont équivalents à ceux donnés par le premier théorème (voir par exemple Smorynski 1977), ont un sens très simple et ne font pas intervenir d'autoréférence (ce qui montre que l'indécidabilité ne peut pas être évitée par l'interdiction des autoréférences).

Ils signifient en effet :

le système S1 *est consistant*

Comme précédemment ils sont produits effectivement, et donc il est parfaitement possible de créer une machine qui pour tout système consistant S produit un indécidable de S : l'aptitude que possède l'esprit humain de produire des indécidables ne prouve donc pas sa nature non mécanique comme cela a parfois été soutenu. Le système S1 peut être n'importe quelle extension (primitive récursive) du système PRA de l'arithmétique primitive récursive (Boolos Jeffrey 1980).

Comme précédemment pour S2 et S3, on peut prendre S1+consistance(S1), mais bien sûr démontrer la consistance de S1 dans un système qui contient comme axiome la consistance de S1 ne paraît pas très intéressant, aussi pour S3, il est plus naturel de penser qu'on fait appel à une théorie comme l'arithmétique du second ordre ou ZF, ou une théorie contenant un principe d'induction.

Dans le cas où S1 est ZF, pour se convaincre de consistance(ZF) on peut faire appel à des axiomes de grands cardinaux qui sont naturels et plausibles (c'est du moins ce que soutiennent certains réalistes), mais bien évidemment plus on considère des théories fortes, plus la consistance de ces théories devient problématique. Comme nous l'avons déjà indiqué, certains axiomes forts concernant les grands cardinaux sont suspectés d'être inconsistants ! Sur ces questions voir par exemple Maddy 1988.

Monsieur Insignifiance : Si on ne s'était pas intéressé à la formalisation des démonstrations, aucun mathématicien n'aurait jamais rencontré ces énoncés étranges, dont on ne peut comprendre le sens littéral, tant ils sont compliqués et tant est indéchiffrable la codification qui les lie à leur interprétation métamathématique.

Monsieur Importance : Si on peut prétendre que les indécidables produits par le premier théorème de Gödel sont d'un intérêt mathématique douteux, cela est plus difficile pour les indécidables du second : la consistance de l'arithmétique de Peano est un problème qui avait été étudié avant qu'on sache qu'elle était indécidable (pour PA). Par Hilbert lui-même ! (voir la citation de Smorynski en début de section). Le codage est désagréable certes, mais il est possible dans tout système contenant un peu d'arithmétique et c'est justement parce qu'il est possible qu'on rencontre cette difficulté. Ou bien il faut le rendre impossible (comme en calcul propositionnel ou en géométrie élémentaire), ou bien il faut en accepter les conséquences. A ce propos, notons que N. Bourbaki, qui juge par ailleurs d'intérêt mathématique secondaire la théorie de la démonstration (et donc les théorèmes de Gödel), dit de la démonstration de Gödel qu'elle est ingénieuse et que le grand nombre de signes nécessaires pour écrire les indécidables de Gödel bien que les rendant pratiquement impossibles à expliciter est sans gravité car "aucun mathématicien ne pense que cela diminue en rien la valeur de ces constructions" (Bourbaki 1969).

6.2.3. *Les indécidables de Gödel de la théorie de la récursivité*

Développée à partir de 1936, la théorie de la récursivité (c'est-à-dire de la calculabilité) a produit un grand nombre d'indécidables de Gödel, soit directement, soit indirectement.

A chaque fois qu'on démontre qu'un ensemble **A** n'est pas récursivement énumérable, cela signifie que pour tout système formel S une instance au moins de la formule "m appartient à **A**" est un indécidable de Gödel pour S. A chaque fois en particulier qu'on établit qu'un problème P(n) est indécidable, c'est-à-dire qu'il n'existe pas d'algorithme qui pour chaque donnée n produise la solution de P(n) (attention à ne pas confondre *problème indécidable* qui est une notion absolue, avec *énoncé indécidable de Gödel* qui est une notion relative à un système formel), cela implique que pour tout système formel correct S, au moins une instance du problème est un indécidable de Gödel pour S. Preuve : Soit S un système formel. Supposons que S donne tous les théorèmes "P(n) = R" et qu'il ne se trompe jamais, c'est-à-dire supposons que S est correct et complet pour toutes les instances de P(n). L'algorithme d'énumération des théorèmes de S, qui existe par définition d'un système formel, fournit alors une procédure de résolution pour P(n), ce qui contredit l'indécidabilité du problème P(n).

Le premier exemple de problème indécidable est le problème de l'arrêt des machines de Turing. Donc : pour tout système formel correct S, il existe au moins une machine de Turing bien précise (et qu'on peut expliciter) qui ne s'arrête pas et dont S ne peut pas démontrer le non-arrêt (la démonstration de l'arrêt si elle est possible est faisable dès que le système manipule assez d'arithmétique, et donc les énoncés concernant l'arrêt susceptibles d'échapper à un système intéressant sont uniquement les énoncés de non-arrêt).

De la même façon, pour tout système formel fixé correct S, il existe un couple de programmes d'ordinateurs (Pr1, Pr2) (par exemple écrits en Pascal) calculant la même fonction de N dans N, et tel que la preuve de leur équivalence échappe à S (indécidabilité de l'équivalence des programmes).

De la même façon encore, pour tout système formel correct S, il existe une configuration finie du jeu de la vie de Conway donnant lieu à une croissance indéfinie et qui échappe au pouvoir de démonstration de S (l'énoncé affirmant la croissance indéfinie de la configuration, se code facilement en un énoncé d'arithmétique et n'est pas prouvable dans S). Sur l'indécidabilité du devenir ultime d'une configuration du jeu de la vie, voir Berlekamp Conway Guy 1982. Rappelons la définition du jeu de la vie de Conway : un damier infini est donné ; certaines cases sont occupées par des pions constituant la configuration de départ qui évolue étape par étape ; pour passer d'une configuration à la configuration suivante on applique les règles : si une case est vide et possède trois voisins (parmi les huit possibles) alors elle devient occupée ; si une case est occupée et possède deux ou trois voisins elle reste occupée ; dans tous les autres cas la case est vide dans la configuration suivante.

Des résultats d'indécidabilité en algèbre, en topologie donnent aussi naissance à des indécidables de Gödel pour tout système formel. Voir par exemple Davis 1977.

Hartmanis et Hopcroft (Hartmanis Hopcroft 1976) ont tenté d'établir que le fameux problème P=?NP était indépendant des axiomes de ZF, et bien qu'ils n'aient pas réussi, ils ont montré que certaines versions relativisées P^I=?NP^I sont indépendantes de ZF. En réalité leur résultat est plus général : pour tout système formel S, ils construisent explicitement un oracle récursif I pour lequel

$P^I=NP^I$ et $P^I\neq NP^I$ *ne sont pas démontrables dans* S

Dans le même travail ils explicitent aussi la construction d'un algorithme Algo tel que :

on peut ajouter à ZF *sans introduire d'inconsistance que*

Algo *fonctionne en temps* n^2 *ou que* Algo *fonctionne en temps* 2^n

Monsieur Importance : Cette indécidabilité est concrète puisqu'on peut réaliser mécaniquement des systèmes simulant des machines de Turing, ou le jeu de la vie de Conway, etc. L'indécidabilité des énoncés sur l'arrêt des machines de Turing ou le jeu de la vie de Conway, ou la complexité des algorithmes, signifie donc qu'aucune théorie physique (formalisée) ne sera jamais en mesure de tout dire du monde mécanique, et donc *a fortiori* du monde physique : quelle que soit la théorie (formelle) qu'on proposera il existera toujours un système physique fini (simulant une machine de Turing ou le jeu de la vie, etc.) dont le devenir ne pourra être prévu par la théorie.

Monsieur Insignifiance : Il s'agit du devenir "à l'infini", or qui en physique s'intéresse au devenir de quoi que ce soit "à l'infini" ? Les énoncés indécidables produits à partir des problèmes indécidables ne nous concernent pas vraiment. Par exemple les machines de Turing dont le comportement échappe à ZF + AC sont sans intérêt pour nous et nous ne les construirons jamais, ni ne nous y intéresserons jamais.

Monsieur Importance : Pas d'accord, je peux parfaitement écrire un programme qui produise une énumération des théorèmes de ZF + AC et s'arrête s'il rencontre la démonstration de 0=1. Le non-arrêt de ce programme (si ZF+ AC est consistant) est un indécidable de Gödel (pour ZF + AC). Ce programme est-il si déraisonnable ?

Monsieur Insignifiance : Oui, car comme je viens de le dire, ce programme s'arrêtera à cause des limitations de ressource du système informatique que vous utiliserez, ou à cause de sa non-fiabilité parfaite, et donc son comportement "à l'infini" n'est pas un problème du monde physique. De toute façon il est ridicule d'écrire un programme comme celui que vous évoquez car on sait bien que les techniques de démonstration automatique (et celle que vous utilisez en particulier) sont impuissantes à produire en temps raisonnable des énoncés mathématiques ayant un véritable intérêt.

Monsieur Importance : Ce n'est pas exact, et par exemple le second théorème de Gödel a été produit pas un système de démonstration automatique (Beeson 1988).

Monsieur Insignifiance : Justement cela ne prouve rien puisque le second théorème n'a pas d'intérêt mathématique authentique !
Monsieur Importance : Il n'empêche que les résultats d'indécidabilité sont utiles en informatique : il est arrivé bien souvent qu'on découvre qu'un problème dont on cherchait la solution, était indécidable (par exemple le problème de l'utilité d'un morceau de code dans un programme) et qu'on renonce à le résoudre complètement à cause de l'indécidabilité.
Monsieur Insignifiance : C'est très exagéré, car ce qui compte en informatique c'est la possibilité de résoudre pratiquement un problème. Si on accepte d'identifier "pratiquement" avec "en temps polynomial" ce qui est communément fait (mais est discutable : Gurevich 1989) alors ce ne sont pas les questions d'indécidabilité qui sont importantes mais l'analyse des algorithmes.

6.2.4. *Les indécidables de la théorie des ensembles immunes*

6.2.4.1. "*Tous indécidables sauf un nombre fini*"

Que la famille infinie des vérités de l'arithmétique élémentaire soit telle qu'un système formel en laisse nécessairement échapper certaines, ce n'est peut-être pas très grave. Mais il est certainement gênant de penser qu'il existe des familles d'énoncés mathématiques, dont tout système formel (correct vis-à-vis d'eux, c'est-à-dire qui n'en démontre jamais de faux) ne peut en produire qu'un nombre fini. Pour de telles familles et quel que soit le système formel donné, tous les énoncés sont indécidables sauf quelques-uns.

L'existence de telles familles est liée à ce qu'on appelle les ensembles **immunes** (en termes précis : infinis et ne contenant aucun sous-ensemble infini récursivement énumérable). Les premiers exemples explicites de tels ensembles ont été découverts dans les années 1940 et 1950 par Post et les théoriciens des fonctions récursives (voir Rogers 1967). Leurs définitions ne sont pas très compliquées, mais aujourd'hui on en connaît d'autres plus simples encore provenant de la théorie algorithmique de l'information.

6.2.4.2. *Les immunes de la théorie algorithmique de l'information*

La théorie algorithmique de l'information définit la complexité d'un objet fini par la taille du plus petit programme capable de l'engendrer. Si on prend comme ordinateur de référence un ordinateur assez puissant (équivalent à une machine de Turing universelle), cette définition ne dépend du choix de l'ordinateur que par une constante (voir chapitre 3 pour plus de détails).

Un ordinateur universel U étant fixé, il est naturel de s'intéresser à la famille d'énoncés :

$$K_U(s) = n \qquad s \textit{ suite finie de } 0 \textit{ ou de } 1, n \textit{ entier}$$

Il a été établi (voir chapitre 3 et Li Vitanyi 1993) que dans tout système formel correct S, seul un nombre fini d'énoncés de cette famille pouvait être démontré. Donc pour tout système formel correct S, tous les énoncés sauf un nombre fini concernant la complexité algorithmique sont des indécidables de Gödel pour S. Jamais une théorie mathématique formalisée ne pourra dire plus qu'un nombre fini de choses sur la complexité algorithmique des objets finis. Quel que soit S, tous les énoncés de complexité, sauf un nombre fini sont des indécidables de Gödel pour S.

Sur ce sujet on pourra consulter Kolmogorov Uspenskii 1987, Chaitin 1987a 1987b, van Lambalgen 1989.

6.2.4.3. *Le nombre oméga de Chaitin*

Le nombre oméga de Chaitin (défini comme la probabilité pour qu'un ordinateur universel à programmes autodélimités s'arrête lorsqu'on lui donne un programme tiré au hasard) est un nombre réel qu'on peut écrire :

$$0,a_1\ a_2\ \ldots\ a_n\ \ldots \qquad a_i = 0 \text{ ou } 1$$

Il est tel qu'un système formel correct S ne peut fournir qu'un nombre fini de digits de oméga, ce nombre de digits étant majoré par la complexité du système formel lui-même, plus une constante (indépendante du système formel S, voir chapitre 3). Quel que soit S, tous les énoncés donnant les digits de oméga sauf un nombre fini sont des énoncés indécidables de Gödel pour S. Voir Chaitin 1987b 1987a, Bennett 1979.

Ce nombre oméga apparaît quelque peu magique puisque la connaissance de ses mille premiers digits donnerait un algorithme pour résoudre la plupart des conjectures mathématiques célèbres, et en tout cas toutes celles de la forme : dans tel système formel S tel énoncé est-il démontrable ? (par exemple : le grand théorème de Fermat est-il démontrable dans l'arithmétique de Peano ?) pourvu que la conjecture s'exprime assez brièvement, ce qui est le cas de toutes les conjectures jugées intéressantes ! (Bennett 1979).

La raison de ce pouvoir du nombre oméga provient de ce qu'il contient, sous une forme compressée, la solution du problème de l'arrêt de toutes les machines de Turing. Mais remarquons (Bennett 1988b) que même si on connaissait les mille premiers digits de oméga, le temps nécessaire pour en extraire la solution des conjectures intéressantes serait tellement grand qu'on ne pourrait pas vraiment l'exploiter (l'information est trop compressée dans oméga, le temps de décompression est donc très long).

Il semble avec ces résultats qu'on ait atteint un étonnant "concentré d'indécidabilité".

Monsieur Importance : Que la complexité d'un objet fini soit intéressante est évident et donc le résultat sur l'impuissance d'un système formel à traiter plus qu'un nombre fini de cas du problème de la détermination de complexité, donne bien des indécidables de Gödel intéressants et simples.

Monsieur Insignifiance : D'abord, l'intérêt pratique de la théorie algorithmique de l'information peut être mis en doute, à cause de la constante qui apparaît dans le théorème d'invariance et qui peut devenir aussi grande qu'on veut lorsqu'on choisit mal sa machine universelle. Ensuite, cette théorie est tellement ineffective que bien qu'elle indique qu'il y a beaucoup d'indécidables, elle n'en fournit aucun explicitement. Le théorème de Gödel, lui, est constructif et permet de produire effectivement les indécidables dont il indique l'existence. Van Lambalgen (1989 p. 1394) dit même qu'à cause de cette ineffectivité, les résultats d'indécidabilité de la théorie algorithmique de l'information constituent "une forme faible plutôt qu'une extension du premier théorème d'incomplétude".

Monsieur Importance : Le point de vue de van Lambalgen est lui-même discuté car nombreux sont ceux qui s'accordent à trouver les résultats d'indécidabilité produits par la théorie algorithmique de l'information comme de véritables aggravations des résultats d'indécidabilité de Gödel (Tymoczko 1986, Chaitin 1987a). D'ailleurs, comment prétendre que cette théorie est sans intérêt pratique alors que les physiciens se sont mis à l'utiliser pour reformuler les fondements de la thermodynamique (Bennett 1982, Zurek 1989b, Delahaye 1991fg).

D'après eux, l'entropie d'un micro-état ne peut être définie rigoureusement par les conceptions classiques, fondées sur l'entropie statistique, car celle-ci ne peut définir l'entropie que pour des ensembles d'états. La solution proposée (qui permet aussi de retirer un peu de subjectivité aux fondements de la thermodynamique) est d'utiliser la théorie algorithmique de l'information. Si cette théorie devait être adoptée, non seulement les indécidables produits par la théorie algorithmique de l'information ne pourraient plus être déclarés sans intérêt, mais ils se trouveraient recevoir un sens physique.

A propos des digits de oméga, on peut faire une remarque : si on considère que les indécidables des systèmes forts comme ZF+AC sont sans intérêt mathématique, alors les conjectures usuelles des mathématiques doivent avoir leur solution dans ZF+AC (car on peut simplement les formuler par : C ou non-C résulte-t-il de ZF+AC ?), et donc dans les premiers digits de oméga. Soutenir que les indécidables ne concernent pas vraiment les mathématiques revient donc à enfermer les mathématiques dans les premiers digits de oméga. C'est là un réductionnisme involontaire extrême.

6.2.5. *Les indécidables purifiés. Équations diophantiennes*

> *Aussi impressionnants que paraissent ces résultats [sur les indécidables de l'arithmétique], les problèmes dont ils traitent sont encore très éloignés des préoccupations quotidiennes réelles de la théorie des nombres, et cela vaut pour les 300 dernières années au moins. Le nombre de variables et la complexité*

— quelle que soit la mesure de complexité qu'on utilise — des polynômes impliqués [dans ces indécidables] sont bien plus grands que dans les problèmes des théoriciens des nombres. De plus, il n'y a pas le moindre indice que ces résultats d'indécidabilité soient reliés aux problèmes irrésolus classiques qui défient les mathématiciens depuis des générations.

Feferman 1987

6.2.5.1. *Le dixième problème de Hilbert*

Les problèmes les plus purs des mathématiques sont ceux de l'arithmétique élémentaire, et parmi eux sans doute les plus simples de tous sont ceux liés aux équations diophantiennes comme le fameux Grand Théorème de Fermat. C'est pourquoi les logiciens désireux de convaincre les mathématiciens que l'indécidabilité est bien présente au centre même des mathématiques ont recherché des problèmes indécidables exprimables en termes d'équations diophantiennes, c'est-à-dire de la forme $P(x_1, ..., x_n) = 0$ avec P polynôme à coefficients entiers, ou en termes d'équations diophantiennes exponentielles, c'est-à-dire de la forme $P(x_1, ..., x_n) = 0$ où P est une fonction n'utilisant que des entiers, des additions, des multiplications et des exponentiations (les exposants peuvent être des variables).

A la suite de la résolution par Matijasevic 1970 du dixième problème de Hilbert qui conclut à l'indécidabilité de la résolution des équations diophantiennes (c'est-à-dire à l'inexistence d'un algorithme traitant de la résolubilité de toutes les équations diophantiennes), il est devenu possible de formuler des versions "purifiées" du théorème de Gödel dont nous donnons ici un exemple tiré de Davis Matijasevic Robinson 1976 :

Théorème

Soit A *un système d'axiomes dans un langage comportant les symboles mathématiques* 0, s, +, ., < *et satisfaisant* :

(a) A *est consistant,*

(b) A *est récursivement énumérable,*

(c) A *est suffisamment puissant pour prouver tous les énoncés vrais de la forme* : a+b=c, a.b=c, a<b où a, b et c *sont l'une des séquences de symboles* 0, s0, ss0, sss0, ...

Alors il est possible de construire une équation diophantienne $F(x_1, ..., x_n) = 0$ *associée à* A *telle que* F=0 *n'ait pas de solutions en nombres entiers, mais telle que l'énoncé* : non (x_1 ... x_n $F(x_1, ..., x_n) = 0$) *ne soit pas démontrable à partir de* A.

6.2.5.2. *Un système d'équations universel*

Perfectionnant les méthodes mises au point pour le dixième problème de Hilbert on a cherché à expliciter des équations *insolubles* (c'est-à-dire dont aucun système

formel ne peut traiter tous les cas). Voici l'un des plus beaux exemples d'un tel système dû à Jones 1982.

Pour tout système formel correct S, *il existe des valeurs entières de* x z u y *telles que le système suivant n'a pas de solution et tel que* S *ne peut pas le démontrer* :

$$elg^2+A=(b-xy)q^2n \quad q=b^{560} \quad L+q^4=1+Lb^5$$
$$T+2z=b^5 \quad l=u+tT \quad e=y+mT \quad b=2^w \quad n=q^{16}$$
$$r=[g+eq^3+lq^5+(2(e-zL)(1+xb^5+g)^4+Lb^5+Lb^5q^4)q^4][n^2-n]$$
$$+[q^3-bl+l+TLq^3+(b^5-2)q^5][n^2-1] \quad Nn^2=(2r)!/(r!)^2$$

Ce système d'équations est insoluble parce que :

$$x \quad W_{z\,u\,y} \qquad \textit{le système a des solutions}$$

Ici n W_i désigne une énumération des récursivement énumérable (voir p. 69) et la notation z u y désigne un entier qui dépend bijectivement et récursivement de z u y.

Tout problème du type "F résulte-t-il du système formel S" peut être traduit dans ce système d'équations en calculant le numéro de F et le numéro de l'ensemble r.é. qui correspond à l'ensemble des théorèmes de S. On en déduit d'ailleurs que tout théorème peut être "prouvé" grâce à ce système d'équations avec quelques multiplications et additions (à l'aide d'un autre système du même genre Jones montre que toute démonstration est équivalente à au plus 100 additions et multiplications).

6.2.5.3. *Une équation dont tous les cas sauf un nombre fini sont indécidables*

La théorie algorithmique de l'information, elle aussi, a voulu formuler ses résultats sous forme spectaculaire et purifiée. Cela donne le résultat de Chaitin :

Il existe (et on peut effectivement écrire) une équation diophantienne exponentielle $P(m, x_1, ..., x_n) = 0$ *telle que tout système formel correct* S, *ne peut résoudre qu'un nombre q (q de l'ordre de la complexité algorithmique de*S*) de cas du problème* :

$$m \textit{ fixé}, P(m, x_1, ..., x_n) = 0 \textit{ a-t-il un nombre fini de solutions ?}$$

(voir Chaitin 1987b 1987c, Delahaye 1988a 1990b, van Lambalgen 1989).
Tous les cas du problème de l'équation de Chaitin sauf un nombre fini d'entre eux sont donc des indécidables de ZF + AC (ou de n'importe quel système formel fixé).

Monsieur Importance : Il me semble qu'aucun doute n'est plus possible sur la simplicité des énoncés indécidables qu'on peut rencontrer en mathématiques, et sur leur fréquence.
Monsieur Insignifiance : ... Sauf que des systèmes d'équations comme celui écrit plus haut, aucun mathématicien n'en a jamais étudié de lui-même. Ces systèmes sont toujours écrits en transformant un problème métamathématique sous

forme arithmétique : ils sont faits exprès ! ce ne sont que des problèmes métamathématiques déguisés ! Quant à l'équation de Chaitin elle présente quelques inconvénients : (i) d'abord on ne s'intéresse pas à l'existence d'une solution mais à l'existence d'une infinité de solutions (ce qui est déjà moins simple et fait quitter le fini dont justement l'arithmétique est le langage et où on aurait aimé resté pour "ces indécidables purifiés") ; mais de plus (ii) un système formel étant donné S, il est impossible de connaître d'une façon effective ne serait-ce qu'un seul cas de l'équation qui échappe à S : on sait que tous sauf un nombre fini échappent à S, mais on ne peut en connaître précisément aucun ; enfin (iii) l'équation de Chaitin une fois écrite comporte 12 000 variables et occupe 200 pages : si elle n'était la traduction arithmétique d'un autre problème, il est certain, que jamais aucun mathématicien ne s'y serait intéressé.

6.2.6. *Les indécidables de la théorie des ensembles*

> HC *[l'hypothèse du continu] est donc un exemple de problème "intéressant" concernant les ensembles qui est prouvé indépendant des axiomes de* ZFC. *[...] Les résultats [concernant les groupes abéliens], et bien d'autres trop nombreux pour être tous mentionnés, montrent que beaucoup de questions mathématiques intéressantes ne peuvent pas être résolues sur la seule base des axiomes de la théorie des ensembles de Zermelo-Fraenkel.*
>
> *Mac Lane 1986*

> *Ce système* [ZF] *correspond exactement aux besoins de tous les mathématiciens, exceptés, bien sûr, les logiciens et aussi ceux que leur attitude philosophique empêche d'accepter les prémisses d'un tel système, c'est-à-dire les mathématiciens dits intuitionnistes ou constructivistes.*
>
> *Dieudonné 1982*

On sait que le système le plus simple donnant satisfaction aux mathématiciens est ZF+AC (AC désigne l'axiome du choix qui affirme que tout produit d'ensembles non vides est non vide), et qu'il est bien sûr sujet aux théorèmes d'incomplétude de Gödel. Mais, et c'est plus intéressant, il est facile de produire directement des énoncés indécidables dans ZF+AC, et cela sans avoir recours à un codage, c'est-à-dire sans avoir à utiliser la méthode donnée dans la démonstration des théorèmes d'incomplétude de Gödel.

L'hypothèse du continu HC (qui affirme que tout ensemble infini de l'ensemble R des nombres réels peut être mis en bijection avec N ou avec R) est un tel énoncé. Mais même ZF+AC+HC peut facilement être "dépassé", par exemple avec un axiome de grand cardinal, comme l'axiome de l'existence de cardinaux inaccessibles (voir Kunen 1980).

Depuis la mise au point par Cohen de la technique du "forçage" (Cohen 1966, Kunen 1980) de nombreux énoncés ont été produits et démontrés indépendants de ZF+AC. Des hiérarchies infinies de systèmes plus forts que ZF+AC ont même été proposées par les théoriciens des ensembles. Ces résultats confirment que les

indécidables sont bien là, et que pour les rencontrer, il n'est pas nécessaire de "recourir à du codage".

Parmi ces axiomes indépendants, il faut distinguer ceux qui ont des effets arithmétiques de ceux qui n'en ont pas. Ceux qui n'ont pas d'effets arithmétiques produisent des systèmes formels qui ne sont pas plus forts, puisqu'ils ne permettront pas de montrer 0=1 si cela n'était pas possible sans eux.

Les axiomes AC, HC, V=L par exemple, n'ont pas d'effets arithmétiques (ils ne conduisent à aucun nouvel énoncé d'arithmétique qui ne peut déjà être produit par ZF ; les ajouter ne donne pas un système formel plus fort). Par contre les axiomes d'existence de grands cardinaux, eux, impliquent la consistance de ZF et donc ont des conséquences arithmétiques et même des conséquences "diophantiennes" (certaines équations diophantiennes n'ayant pas de solution et qui échappaient à ZF rentrent dans leur champ).

Ainsi que nous le verrons aussi pour les sous-systèmes de l'arithmétique du second ordre, il y a deux manières de compléter un système formel en lui ajoutant des indécidables : soit on n'en modifie pas la force arithmétique (extension conservative), soit on la modifie. Les extensions qui ne modifient pas la force arithmétique sont bénignes (la consistance du système obtenu est équivalente à celle du système qu'on avait avant l'extension), les autres prennent des risques (il se peut que le nouveau système soit inconsistant alors que l'ancien ne l'était pas).

La force d'une extension peut être mesurée par ses effets arithmétiques : ce qui établirait définitivement que "l'infini compte pour le fini" serait la démonstration d'un énoncé arithmétique intéressant (et ne résultant pas simplement d'un codage) grâce à des axiomes "risqués" comme ceux d'existence de grands cardinaux. On aurait la preuve que même lorsqu'il ne s'agit que de l'arithmétique, les indécidables ont du sens, et que se contenter des systèmes naturels (comme le système de Peano pour l'arithmétique) c'est perdre des énoncés mathématiques intéressants. Ce serait la preuve que lorsqu'il s'agit des entiers il faut réellement accepter d'utiliser plus que PA.

Ce pas, Friedman (1987) pense l'avoir franchi en montrant par l'utilisation d'un axiome d'existence de grands cardinaux (cardinaux de Mahlo), un énoncé combinatoire pur qui n'est pas la simple codification arithmétique d'un énoncé métamathématique. L'énoncé en question n'est pas suffisamment simple pour pouvoir être reproduit ici (nous verrons des énoncés combinatoires analogues mais plus simples au paragraphe suivant) et Friedman reconnaît d'ailleurs qu'il faut sans doute encore simplifier ses énoncés combinatoires.

Feferman 1987, lui, est sceptique, et se demande s'il n'y a pas une forme de cercle vicieux dans l'utilisation faite de ces énoncés par ceux qui y voient une preuve de l'importance des mathématiques de l'infini pour les mathématiques du fini : on prétend que des principes ensemblistes infinitistes forts peuvent produire des énoncés arithmétiques intéressants et vrais, mais la seule raison qu'on a de croire que ces énoncés arithmétiques sont vrais est qu'ils sont équivalents aux énoncés ensemblistes qui permettent de les produire. On se convainc donc de l'importance des

axiomes de grands cardinaux pour le fini en les supposant consistants, alors que justement ils ne sont importants que s'ils sont consistants.

Rien ne nous interdit de penser que les énoncés combinatoires que Friedman propose ne sont que le codage déguisé d'énoncés de consistance, comme les équations arithmétiques du paragraphe précédent l'étaient. Cela n'apparaît pas au premier coup d'œil (voir le système de Jones), le progrès de Friedman serait simplement d'avoir su mieux déguiser le codage.

Certains spécialistes de la théorie des ensembles recherchent des axiomes qui entraîneraient HC ou non HC. Bien que des avancées aient été réalisées ces dernières années (voir Maddy 1988) pour l'instant le problème de trouver des axiomes qui aient des conséquences sur HC (ce qui établirait que certains indécidables ont un rôle à jouer) reste non résolu. A ce propos, il faut remarquer que si vraiment les indécidables sont importants alors la recherche de nouveaux axiomes est dans l'essence des mathématiques mêmes. Le fait que très peu de mathématiciens s'adonnent à cette recherche, confirme que dans sa pratique le mathématicien ordinaire ne croit pas à la véritable portée des indécidables.

Monsieur Importance : La multitude d'énoncés indécidables proposés en théorie des ensembles montre que pour les systèmes les plus puissants le phénomène d'indécidabilité se produit facilement, et cela sans avoir recours à du codage. Dès qu'on cherche un peu on rencontre les indécidables de Gödel. C'est faire un drôle de pari que croire qu'ils ne peuvent jamais intervenir dans un vrai problème.

Monsieur Insignifiance : Les énoncés indécidables de ZF+AC n'ont jamais servi jusqu'à présent en mathématiques à résoudre de vrais problèmes, seuls les logiciens les utilisent et s'y intéressent. Et d'ailleurs les mathématiciens (à l'exception de quelques logiciens en théorie des ensembles) ne recherchent pas de nouveaux axiomes susceptibles de compléter ZF+AC. Par leur pratique ils montrent que pour eux l'indécidabilité n'a jamais à être envisagée : sans doute attendent-ils pour changer d'attitude qu'on leur montre de vrais problèmes où leurs bons vieux axiomes sont insuffisants ! La très grande énergie dépensée (depuis plus de vingt ans) à utiliser les méthodes de forçage n'a en définitive rien produit de très intéressant pour le mathématicien non logicien.

Monsieur Importance : Il faut laisser aux mathématiques le temps de se faire : les derniers résultats de Friedman s'ils n'établissent pas définitivement la preuve de l'importance mathématique des indécidables de ZF+AC, approchent très près du but. La recherche de nouveaux axiomes ayant des conséquences sur les sous-ensembles de R et en particulier sur HC progresse, les succès même partiels de ces recherches prouvent indirectement que les indécidables ont du sens et qu'il faut en tenir compte dans toutes les branches des mathématiques y compris en arithmétique.

6.2.7. *Les indécidables de Paris-Harrington et Friedman*

Une nouvelle étape dans le développement de la théorie initiée par les théorèmes de Gödel de 1931 est la découverte par Paris et Harrington en 1977 d'une question

simple et intéressante, ne dépendant pas d'un codage numérique de notions logiques, qui est indécidable.

Kleene 1986

Les instructions pour la construction de G *sont plutôt indirectes ; si elles étaient menées explicitement, le résultat en serait une très longue formule faisant intervenir un grand nombre de références à des factorisations en nombres premiers. Considérée comme une formule d'arithmétique,* G *n'est pas très intéressante. Récemment J. Paris a construit une formule vraie et intéressante de l'arithmétique de Peano qui ne peut pas être démontrée dans cette arithmétique.*

Mac Lane 1986

Jusqu'à ces dernières années, les seules arithmétiques non classiques et consistantes (si l'on suppose consistants les axiomes de Peano) étaient artificiellement obtenues au moyen des formules indécises construites par Gödel, formules atrocement compliquées et dépourvues d'intérêt mathématique, leur existence seule étant importante pour les logiciens. Depuis 1976 sont apparues des formules arithmétisant le théorème de Ramsey.

Fraïssé 1982

Quoique ce résultat de Gödel soit tout à fait extraordinaire, la critique a souvent été formulée que les exemples concrets d'indécidables combinatoires de Gödel sont mathématiquement artificiels, à cause du codage de syntaxe qu'ils contiennent. Cette critique doit être prise au sérieux, car il était tout à fait concevable que tous les théorèmes de combinatoire finie ayant du sens, soient prouvables. La situation est devenue claire à la suite du résultat de 1977 de Paris et Harrington, car cette fois leur travail aboutit à un théorème de combinatoire finie complètement transparent et non prouvable dans PA.

Simpson 1985

Il me semble que lorsqu'on passe des énoncés de Paris et Harrington, et Kirby et Paris pour PA, *à ceux donnés par Friedman pour* ATR_0 *et* $(\ ^1_1\text{-CA})_0$, *puis à ceux de Buchholz pour* $(\ ^1_1\text{-CA})+BI$ *le sens concret des énoncés devient de plus en plus ténu. Vu par un observateur non impliqué, le sentiment est que ces énoncés sont encore des énoncés "faits exprès".*

Feferman 1987

Depuis 1977 des énoncés purement combinatoires et ne résultant pas du codage direct d'énoncés métamathématiques ont été produits et démontrés être des indécidables pour PA (l'arithmétique de Peano) ou pour d'autres systèmes faibles. Ces nouveaux résultats sont unanimement considérés comme un pas en avant dans la démonstration de l'importance (de la gravité ?) de l'indécidabilité.

Nous allons en donner deux exemples. A chaque fois avant d'arriver à l'énoncé indécidable nous en présentons des formes intermédiaires.

6.2.7.1. *Le résultat de Paris-Harrington*

Théorème de Ramsey infini (1928)

Pour tout entier k *et toute partition* $C_1, C_2, ..., C_r$ *de l'ensemble* $[N]^k$ *des parties à* k *éléments de l'ensemble des entiers* N, *il existe un sous-ensemble infini* M *de* N *tel que* $[M]^k$ *est inclus dans l'un des* C_i.

Cas particulier k=r=2 : pour tout graphe infini complet dont les arcs sont rouges et verts, il existe un sous-graphe infini complet dont les arcs sont de la même couleur.

Théorème de Ramsey fini

Pour tout triplet d'entiers k, r, m *il existe un entier* n *tel que si* P *est un ensemble de* n *entiers et que* $C_1, C_2, ..., C_r$ *est une partition de* $[P]^k$ *alors il existe* M *inclus dans* P, *ayant plus de m éléments tel que* $[M]^k$ *est inclus dans l'un des* C_i.

Cas particulier k=r=2 : Pour tout m il existe un n tel que tout graphe complet de plus de n nœuds dont les arcs sont colorés en rouge ou en vert, contient un sous-graphe complet unicolore de plus de m nœuds. Exemple : tout ensemble de six personnes contient trois personnes qui, soit se connaissent deux à deux, soit sont étrangères deux à deux : pour m=3, n=6 convient. Voir Graham Spencer 1990.

Théorème de Ramsey fini de Paris et Harrington

Pour tout triplet d'entiers k, r, m *il existe un entier* n *tel que si* P *est un ensemble de n entiers et que* $C_1, C_2, ..., C_r$ *est une partition de* $[P]^k$ *alors il existe* M *inclus dans* P, *ayant plus de m éléments tel que* $[M]^k$ *est inclus dans l'un des* C_i *et tel que* :

$$\text{cardinal}(M) \geq \text{minimum}(M).$$

Ce résultat purement combinatoire ne faisant en apparence référence ni à la logique, ni à aucune notion d'algorithme a été montré indépendant des axiomes de l'arithmétique du premier ordre PA dans Paris Harrington 1977.

On peut remarquer que c'est un énoncé de la forme "pour tout n il existe m : E" avec E primitif récursif. Les indécidables arithmétiques que donne le théorème de Gödel sont de la forme "pour tout n : E" E primitif récursif. Chaque instance du Théorème de Ramsey fini de Paris et Harrington (k, r, m fixés) est prouvable dans PA. C'est la rapidité de croissance de la fonction g : (k, r, m) n, qui échappe à l'arithmétique de Peano (Smorynski 1982, Gallier 1991).

En réalité, l'énoncé de Paris-Harrington équivaut à un énoncé de consistance : celui de la théorie obtenue en ajoutant consistance(PA) à PA, puis consistance(PA + consistance(PA)), etc. jusqu'à l'ordinal $_0$ (Smorynski 1982). Sous des dehors purement arithmétiques cet énoncé est donc aussi un énoncé de logique. Il est dommage que ce ne soit pas la forme finie du Théorème de Ramsey elle-même, qui soit indécidable dans PA, mais une variante artificielle.

6.2.5.2. *Le résultat de Friedman sur le théorème de Kruskal*

Théorème de Kruskal

Si $T_1, T_2, ...$ *est une suite infinie d'arbres alors il existe* i *et* j, i<j *tels que* T_i *est homéomorphe à une partie de* T_j.
(T_i *est* homéomorphe *à une partie de* T_j *signifie qu'en enlevant des morceaux de* T_j *on peut obtenir un arbre exactement semblable à* T_i.)

Forme finie du Théorème de Kruskal de Friedman (FFF)

Pour tout entier k *il existe un entier* n *tel que si* $T_1, ..., T_n$ *est une suite d'arbres vérifiant* cardinal(T_i)≤k.i, *alors il existe deux entiers* i *et* j, i<j≤n, *tels que* T_i *est homéomorphe à une partie de* T_j.

Le théorème de Kruskal entraîne directement la forme finie. La forme finie est un énoncé d'arithmétique et Friedman a montré qu'elle était un indécidable de l'arithmétique de Peano, et même qu'elle était indécidable pour des systèmes plus forts (Simpson 1985, Smorynski 1982, Feferman 1987, Gallier 1991).

Cette fois-ci l'énoncé est encore très simple mais sa force est bien plus grande. Il équivaut à l'énoncé de consistance d'une théorie non prédicative, et certains y ont vu la réfutation de la philosophie prédicativiste des mathématiques :

> FFF *est une assertion concrète portant sur des objets finis instantanément compréhensibles par un prédicativiste, et pourtant toute preuve de* FFF *doit faire appel à des principes imprédicatifs. En bref* FFF *aurait été considéré comme ayant un sens pour Poincaré, mais il n'aurait pu en accepter ni preuve ni réfutation.*
>
> *Smorynski 1982 p. 187*

La simplicité de FFF est grande mais n'empêche pas la remarque :

> *Jusqu'à présent, aucun des énoncés [de Paris et Harrington ou* FFF*] montrés indépendants, n'a jamais été considéré pour lui-même dans des travaux de combinatoire avant son introduction par des logiciens. C'est une question de pure spéculation que de savoir s'ils auraient fini par être pris en considération dans le cours normal du développement de la combinatoire.*
>
> *Feferman 1987 p. 202*

Monsieur Importance : Cette fois-ci il n'y a plus de codage, les énoncés sont simples et ont un contenu mathématique immédiat.
Monsieur Insignifiance : Oui, c'est mieux mais il faut bien constater que ces énoncés-là, sont toujours des produits de logiciens et non pas de mathématiciens. Je me demande, comme pour les équations diophantiennes et la théorie des ensembles, si ces prétendus énoncés simples indécidables ne sont pas uniquement un progrès de la codification.

6.3. Le sens des résultats récents de la théorie de la preuve

La nécessité d'utiliser pleinement la théorie des ensembles dans les mathématiques du fini n'a pas encore été établie. [...] La théorie des ensembles semble inutile dans les mathématiques nécessaires aux applications scientifiques.

Feferman 1987

Malgré le théorème de Gödel, il est possible de fournir une réduction finitiste d'une partie substantielle des mathématiques de l'infini, incluant une grande partie des résultats les plus connus des mathématiques non constructives.

Simpson 1988

J'estime à au moins 85% *des mathématiques existantes la partie qui peut être formalisée dans* WKL_0 *ou* WKL_0^+ *ou dans des systèmes plus forts mais conservatifs par rapport à* PRA *vis-à-vis des formules* Π^0_2.

Simpson 1988

Deux types de résultats récents en théorie de la preuve conduisent à des conclusions intéressant notre propos. Pour plus de détails et des définitions précises, on se reportera à l'annexe ou à Simpson 1985 1985a 1986 1988, Friedman 1980 1986, Feferman 1987 1988, Harrington Morley Scedrov Simpson 1985.

6.3.1. *Réductibilité et extensions conservatives*

Il y a d'une part les résultats de réductibilité et d'extensions conservatives : certains systèmes formels entre PA (arithmétique du premier ordre, aussi notée Z1) et Z2 (arithmétique du second ordre) sont suffisamment forts pour contenir toutes les mathématiques ordinaires et pourtant sont des extensions conservatives vis-à-vis des formules Π^0_2 de PA ou PRA (arithmétique primitive récursive). Ces systèmes ne sont donc pas plus puissants que PA (ou PRA) et dans ces systèmes la consistance de PA (ou PRA) reste indécidable. Par contre, ils sont mathématiquement plus puissants : concernant l'infini ils donnent plus de résultats. Cela prouve qu'en un certain sens, la consistance de PA (ou de PRA) n'est pas un "vrai énoncé des mathématiques ordinaires". Ces systèmes, si on les identifie aux mathématiques "réelles", prouveraient que les indécidables (de type consistance(S)) ne concernent pas les mathématiques. On peut parfaitement soutenir que PA est un système complet pour l'arithmétique (Isaacson 1987 1992) et que ce qui lui échappe (d'après les théorèmes d'incomplétude) n'est pas authentiquement arithmétique.

Donnons quelques précisions sur les "mathématiques ordinaires".

Par mathématiques ordinaires nous voulons dire en gros, les mathématiques générales non ensemblistes, c'est-à-dire les mathématiques telles qu'elles étaient avant que la théorie abstraite des ensembles ne s'en empare (ou peut-être telles qu'elles seraient aujourd'hui si la théorie abstraite des ensembles ne s'en était pas emparée). Donc, les mathématiques ordinaires contiennent la théorie des nombres, la géométrie, le calcul et les équations différentielles, l'analyse réelle et complexe,

> *la combinatoire, l'algèbre dénombrable, les espaces de Banach séparables, la théorie de la calculabilité et la topologie des espaces métriques complets séparables. Elles ne comportent pas l'analyse fonctionnelle abstraite, l'algèbre universelle ou la topologie générale.*
>
> *Simpson 1985*

S. Feferman parle aussi de "scientifically applicable 20 th century mathematics". Son point de vue sur la possibilité de développer toutes les mathématiques ordinaires dans des systèmes formels conservatifs vis-à-vis de PA est d'ailleurs très clair :

> *Il semble alors que toute l'analyse moderne applicable peut être développée dans cette* [VT |] *extension conservative de* PA.
>
> *Feferman 1987*

La vision des mathématiques données par les résultats sur les extensions conservatives de PA est assez nouvelle : partant d'un système intuitivement clair et évident comme PA, deux grandes familles d'extensions seraient possibles :

- la famille des extensions comme Z2, ZF, ZF+{axiomes grands cardinaux}, etc. qui étendraient les énoncés élémentaires $^0_1$ de l'arithmétique qu'on peut démontrer, et qui, en particulier, décideraient (positivement bien sûr) de la consistance de PA. Avec de tels systèmes, l'indécis diminue, mais la consistance devient de plus en plus douteuse. C'est la voie des mathématiques dangereuses, des mathématiques qui prennent le double risque de l'inconsistance et de l'ontologie illusoire.
- la famille des extensions comme $^1_0$-CA_0 ou VT | qui s'élèvent aussi au-delà de PA et autorise bien plus que PA, mais conservativement vis-à-vis de PA et donc sans craindre l'inconsistance, et sans prendre d'engagement ontologique supplémentaire. Ces extensions qui d'une certaine façon refusent de croire au sérieux des indécidables, on le sait, ne redonnent pas toutes les mathématiques, mais, et c'est cela qui est nouveau et fascinant, redonnent une part tellement grande des mathématiques qu'on peut y faire toutes les mathématiques applicables. Ces réalisations partielles du programme de Hilbert (Feferman 1988, Simpson 1988, Sieg 1988) sont certainement l'une des nouveautés les plus importantes de ces dernières années en logique.

Devant cela la tentation est grande de tracer un trait entre les mathématiques de l'illusion qui se complaisent dans l'indécidable et lui attribuent du sens, et les mathématiques ordinaires qui elles s'en passent très bien. Qu'on puisse faire de l'analyse, de l'algèbre dans des extensions conservatives de PA (c'est-à-dire dans des systèmes dont la consistance est aussi assurée que celle de PA) indique entre autres choses que le continu n'oblige pas à l'engagement ontologique qu'on a cru (et auquel les physiciens n'ont jamais souscrit).

Aujourd'hui encore, on peut donc croire que les indécidables de Gödel sont sans importance pour le monde des mathématiques pures, et pour le monde physique.

6.3.2. *Le programme des "reverse mathematics"*

Il y a aussi les résultats de ce qu'on appelle les "reverses mathematics". Une étude soigneuse des sous-systèmes de l'arithmétique du second ordre Z2, montre que la plupart des grands résultats de l'analyse classique sont équivalents à des énoncés existentiels. La hiérarchie simplifiée des sous-systèmes de Z2 mise en évidence par ce programme des "reverse mathematics" distingue quelques systèmes, chacun obtenu à partir des autres par ajout d'un ou de plusieurs axiomes existentiels (Simpson 1985, Harrington Morley Scedrov Simpson 1985).

La vue donnée par ces résultats est que certains indécidables des systèmes faibles (qu'il faut justement rechercher) sont exactement les énoncés nécessaires pour passer au niveau suivant. La classification des résultats mathématiques en fonction des hypothèses existentielles qu'ils utilisent (et auxquels bien souvent ils sont équivalents) met en valeur certains indécidables qui se trouvent alors placés au centre même des mathématiques.

De la même façon qu'on considère qu'identifier précisément où sert l'axiome du choix dans les résultats qu'on démontre, et qu'on cherche en arithmétique à purifier les méthodes utilisées, on doit admettre que c'est une véritable activité mathématique que de repérer les bons systèmes et les bons indécidables qui permettent de s'élever sans brusquerie inutile (ZF + AC est trop brusque, car il donne beaucoup plus qu'il n'est nécessaire pour développer l'arithmétique ou l'analyse). La recherche des systèmes assez forts mais pas trop forts, la découverte des bons axiomes, c'est-à-dire des bons indécidables, est certainement une authentique activité mathématique.

6.3.3. *Deux sortes au moins d'indécidables de Gödel*

Les deux vues précédentes semblent se contredire complètement : l'une dénie tout sens aux indécidables, l'autre les met au centre de l'activité mathématique. Elles ne se contredisent pas si on distingue soigneusement :

- d'une part, les indécidables de consistance, ceux construits par codification de la syntaxe, ceux "construits exprès" (comme l'énoncé de Paris-Harrington ou FFF) et qui, même s'ils ressemblent aux énoncés que les mathématiciens étudient d'eux-mêmes, n'en sont jamais, et sont toujours des indécidables de consistance.
- d'autre part, certains énoncés existentiels (comme le lemme de König, le théorème que toute fonction continue sur [0,1] atteint sa borne supérieure, le théorème de complétude de Gödel, l'axiome du choix) qui produisent des extensions conservatives des systèmes auxquels on les ajoute et donc n'engagent pas plus que les systèmes auxquels on les ajoute.

Monsieur Insignifiance : Puisqu'il y a des systèmes formels qui permettent raisonnablement de faire toutes les mathématiques ordinaires et qui sont des extensions conservatives de l'arithmétique de Peano, cela signifie que les indécidables produits par les théorèmes d'incomplétude de Gödel (comme celui qui affirme la consistance de Peano) sont sans importance mathématique. De même qu'il y a des nombres transcendants de peu d'importance (ceux de Liouville) et des nombres transcendants intéressants (comme ou e) il y a des indécidables "faciles" mais sans intérêt (ceux donnés par les théorèmes de Gödel), et des indécidables profonds, respectueux des noyaux de base des mathématiques.
Monsieur Importance : Mais ce sont d'autres indécidables repérés par le programme des "reverse mathematics" qui aujourd'hui disent réellement ce qu'il en est de la pratique mathématique, et donc même s'il ne s'agit pas d'indécidables de consistance (ou de diagonalisation-codification) ce sont quand même les indécidables de Gödel qui sont au centre des mathématiques.
Monsieur Insignifiance : Les indécidables de Gödel (au sens de la définition donnée dans l'introduction) OUI, mais pas les indécidables produits par les théorèmes d'incomplétude de Gödel.
Monsieur Importance : Nous sommes d'accord, il faut distinguer deux types d'indécidables. Je reste persuadé quant à moi que les deux types sont importants ...
Monsieur Insignifiance : ... et moi que les indécidables de consistance ne le sont pas, et que les autres sont des énoncés mathématiques utiles à identifier mais qu'on ne doit pas les considérer comme des indécidables authentiques puisqu'ils ne sont pas indécidables dans les extensions conservatives les plus intéressantes de PA.

6.4. Conclusion

Les progrès en logique mathématique ces dernières années ont eu deux conséquences remarquables :

- Ils ont conduit à proposer beaucoup de nouveaux indécidables. Mais malgré tout aucun énoncé mathématique formulé pour son propre intérêt et indépendant de la logique n'a été montré indécidable, dans un système fort.
- Ils ont conduit à des réalisations partielles ou modifiées du programme de Hilbert qui permettent de croire sérieusement qu'on peut faire toutes les mathématiques ordinaires dans des extensions conservatives de systèmes faibles.

Il en résulte qu'aujourd'hui en philosophie des mathématiques :

- On peut être **réductionniste** et croire que les indécidables sont sans importance pour les mathématiques applicables (ou ordinaires). Sur ce terrain se rencontrent des mathématiciens convaincus comme l'était Dieudonné, que ZF et quelques variantes de ZF constituent un cadre suffisant et satisfaisant pour toutes les mathématiques, et des logiciens qui refusant la philosophie platonicienne considérée comme "moyen-âgeuse" (voir Feferman 1987) tentent

d'élaborer des fondements faibles des mathématiques, ou au moins, des mathématiques ordinaires. Le *réductionnisme de tranquillité* du mathématicien "qui travaille", s'accorde avec le "*réductionnisme de perplexité*" du logicien qu'effraient les ontologies débordantes et incroyables. Le premier attend toujours qu'on lui démontre que le "théorème" de Fermat ou un *vrai problème* mathématique est indécidable vis-à-vis de Peano ou de ZF+AC (si la démonstration de Wiles de 1993 est reconnue valide pour le théorème de Fermat, se pose quand même la question de sa prouvabilité dans PA ; de plus les conjectures d'arithmétique ne manquent pas pour lui succéder). Le second qui vient de mener à bien des réalisations partielles du programme de Hilbert considère qu'il prouve par là que les indécidables de Gödel ne concernent pas les mathématiques ordinaires.

- On peut aussi voir dans les théorèmes d'incomplétude et toute nouvelle occurrence d'indécidables (particulièrement celles proposées par Paris-Harrington et Friedman) la *preuve de la faillite du réductionnisme*. Sur ce terrain le platonicien et l'intuitionniste se rejoignent. Le platonicien considère que les indécidables de l'arithmétique ne sont que la manifestation d'entités de plus hauts niveaux dont ils constituent la preuve d'existence, et l'intuitionniste y voit la manifestation de l'extensibilité indéfinie des concepts d'entier et de démonstration.

Aujourd'hui c'est cet anti-réductionnisme qui prédomine largement en philosophie des mathématiques. Il a à répondre à bien des questions et une brèche est ouverte dans son assurance trop facile qui se réjouit des indécidables ("cooked-up" comme dit Feferman) de Paris-Harrington et Friedman. Cette brèche c'est la mise à jour d'extensions conservatives puissantes de PA qui permettent tout ce dont on a besoin pour la plus grande partie des mathématiques. Et cela sans prendre les engagements sur le "plus loin" et le "plus grand" que nous invitent à souscrire les anti-réductionnistes partisans du monde cantorien, mais dont on pressent qu'ils défendent un univers trop beau pour être vrai. Et cela aussi, sans avoir à se lier pieds et mains, comme les autres anti-réductionnistes nous le proposent au nom de mathématiques de l'intuition et de la construction auxquelles ils réduisent l'univers.

Note : On remarquera que le "mathématicien qui travaille", par son scepticisme vis-à-vis des indécidables n'est pas du même côté que le platonicien : c'est que le "mathématicien qui travaille" n'a pas besoin vraiment de croire aux objets qu'il manipule : le platonisme déclaré de certains mathématiciens n'est jamais sérieux, seul l'est celui des logiciens en théorie des ensembles.

Monsieur Importance en cœur avec Monsieur Anti-réductionniste : Les indécidables sont partout y compris en arithmétique et en physique. Ils sont la preuve de l'irréductibilité du monde mathématique.
Monsieur Insignifiance en cœur avec Monsieur Réductionniste : Les recherches en théorie de la preuve ont permis de repérer des systèmes formels faibles

mais suffisants pour faire toutes les mathématiques ordinaires applicables. Ces systèmes indiquent qu'il n'y a pas d'indécidables intéressants (pour les mathématiques ordinaires), et c'est sans doute ce qui explique l'échec des logiciens, qui pour l'instant n'ont jamais réussi à montrer qu'un énoncé mathématique authentique auquel les mathématiciens s'intéressent pour lui-même, est indécidable vis-à-vis de la théorie de base qui en permet l'expression.

Annexe : Quelques systèmes formels

Parmi les systèmes formels mis en avant par le programme des "reverse mathematics" et de la recherche d'extensions conservatives de PA, les systèmes suivants sont les plus importants :

(a) RCA_0 (Recursive Comprehension Axiom) = {Axiomes de semi-anneau pour N} + $^0_1$-CA + $^0_1$-IA.)

C'est un sous-système de l'arithmétique du second ordre. Il est très faible mais juste assez fort pour prouver l'existence de tous les ensembles récursifs. Il permet de développer les éléments de la théorie des fonctions continues de variables réelles. Dans RCA_0 on peut établir le théorème des intervalles emboîtés pour [0,1], ainsi que le théorème des valeurs intermédiaires.

(b) WKL_0 est une extension de RCA_0 obtenue en ajoutant le Weak König Lemma (WKL_0) qui affirme que tout sous-arbre infini de $2^<$ comporte une branche infinie. Kirby et Paris 1977 ont montré que ce système était une extension conservative de PRA vis-à-vis des $^0_2$. C'est aussi une extension conservative de RCA_0 vis-à-vis des $^1_1$. WKL_0 est un système qui permet de mener un peu plus loin la théorie des fonctions continues de variables réelles. Dans RCA_0 on a l'équivalence des propriétés suivantes :

- (i) WKL_0 ;
- (ii) Toute fonction continue sur [0,1] est uniformément continue ;
- (iii) Toute fonction continue sur [0,1] atteint sa borne supérieure ;
- (iv) Existence locale de solutions pour les équations différentielles ordinaires ;
- (v) Tout anneau commutatif dénombrable possède un idéal premier ;
- (vi) Théorème de complétude du calcul des prédicats du premier ordre de Gödel.

On voit donc qu'une part importante des *mathématiques ordinaires* peut être menée dans cette extension conservative de PRA (dont la consistance est équivalente à celle de PRA). Par ailleurs les énoncés d'analyse qui sont équivalents à WKL_0 et qui sont ce dont on a besoin pour développer les mathématiques usuelles utiles aux physiciens, ne sont pas équivalents à des indécidables de consistance.

(c) ACA_0 (Arithmetical Comprehension Axiom) est obtenu en ajoutant à RCA_0 l'axiome de compréhension pour toutes les formules Σ^1_0. Dans RCA_0 on a l'équivalence des propriétés suivantes :

- (i) Δ^0_1-CA ;
- (ii) Toute suite croissante de nombres réels possède une sous-suite convergente ;
- (iii) Toute suite de Cauchy de nombres réels est convergente ;
- (iv) Toute suite croissante de nombres réels possède une borne supérieure ;
- (iv) Toute suite monotone croissante de nombres réels est convergente ;
- (v) Tout espace vectoriel dénombrable possède une base ;
- (vi) Tout anneau commutatif dénombrable possède un idéal maximal ;

Ce système est une extension conservative de PA. L'analyse prédicative de Weyl peut y être menée. Celle-ci se trouve donc finiment fondée.

(d) ATR_0 (Arithmetical Transfinite Recursion) est obtenu en ajoutant au système précédent un axiome qui équivaut à "deux ordinaux dénombrables sont toujours comparables". La forme finie du Kruskal FFF n'y est pas démontrable, et en fait est équivalente à la 1-consistance de ATR_0. C'est un système considéré comme non prédicativiste. La forme finie du Théorème de Kruskal serait donc hors d'atteinte des mathématiques prédicativistes.

(e) Δ^1_1-CA_0 (Δ^1_1-Comprehension Axiom). FFF est prouvable dans ce système. Mais Friedman a proposé une forme étendue de FFF qui n'est pas prouvable dans Δ^1_1-CA_0. Bien que fort, ce système est réductible à des systèmes intuitionnistes, et donc — d'une certaine façon — est finiment fondé (Feferman 1987 p. 200).

Pour plus de détails sur ces systèmes voir : Feferman 1977 1987 1988, Friedman 1980, Friedman 1986, Gallier 1991, Harrington Morley Scedrov Simpson 1985, Kirby Paris 1977, Simpson 1985 1985a 1986 1988, Sieg 1988.