Séminaire BOURBAKI Mars 2003
55e année, 2002-2003, n$^{\text{o}}$ 915, p. 147 à 172

PROGRÈS RÉCENTS SUR L'HYPOTHÈSE DU CONTINU
[d'après Woodin]

par **Patrick DEHORNOY**

Une profusion de résultats conceptuellement profonds et techniquement difficiles ont été accumulés en théorie des ensembles depuis l'introduction des méthodes de forcing et de structure fine dans les années 1960. Ce rapport est consacré aux travaux récents de Woodin, qui non seulement ont constitué des percées techniques remarquables, mais ont aussi renouvelé le cadre conceptuel en améliorant l'intelligibilité globale de la théorie et en soulignant son unité profonde. Pour la première fois apparaissent une explication autre qu'empirique de la hiérarchie des grands cardinaux et, surtout, une perspective réaliste de décider l'hypothèse du continu, en l'occurrence dans une direction négative :

Conjecture (Woodin, 1999). — *Toute théorie des ensembles compatible avec l'existence de grands cardinaux et rendant invariantes par forcing les propriétés des ensembles héréditairement de cardinal au plus $\aleph_1$ implique que l'hypothèse du continu soit fausse.*

Les travaux de Woodin arrivent très près de cette conjecture, qu'ils établissent pour une part substantielle de la hiérarchie des grands cardinaux. La question reste de savoir si cette part substantielle est en fait toute la hiérarchie des grands cardinaux. Dans tous les cas — et c'est ce qui légitime de parler de ces travaux maintenant, sans attendre une possible solution de la partie ouverte de la conjecture ci-dessus — les résultats de Woodin contribuent à montrer que le problème du continu et, plus généralement, la notion d'infini non dénombrable ne sont pas intrinsèquement vagues et inaccessibles à l'analyse, mais peuvent faire l'objet d'une véritable théorie conceptuelle allant bien au-delà de l'exploration formelle des conséquences d'axiomes plus ou moins arbitraires.

Le texte présent, qui doit beaucoup aux articles d'exposition [17, 19], s'efforce d'expliquer et de mettre en perspective les énoncés de quatre résultats de Woodin, apparaissant ici comme les théorèmes 5.10, 6.4, 6.7, et, surtout, 7.2 et son corollaire 7.6. Il semble hors de portée de donner une idée des démonstrations, dont la partie publiée occupe une bonne fraction des 900 pages de [16], et dont la partie la plus récente n'est décrite que dans [18].

Je remercie tous les théoriciens des ensembles qui m'ont apporté des commentaires et des suggestions, notamment Joan Bagaria, Matthew Foreman, Alexander Kechris, John Steel, Hugh Woodin, et, particulièrement, Stevo Todorcevic.

1. UNE AFFAIRE TERMINÉE ?

L'hypothèse du continu (**HC**) est l'affirmation « Tout sous-ensemble infini de $\mathbb{R}$ est en bijection soit avec $\mathbb{N}$, soit avec $\mathbb{R}$ », et le problème du continu est la question, soulevée par Cantor vers 1890, « L'hypothèse du continu est-elle vraie ? ». Premier de la liste de Hilbert en 1900, le problème du continu a suscité des recherches tout au long du vingtième siècle. Une fois réuni un vaste consensus sur le système de Zermelo-Fraenkel (**ZF**, ou **ZFC** quand l'axiome du choix est inclus) comme point de départ axiomatique d'une théorie des ensembles, la *première* étape dans l'étude du problème du continu est la question « **HC**, ou sa négation $\neg$**HC**, est-elle prouvable à partir de **ZFC** ? ».

La réponse tient en deux résultats, tournants majeurs de la théorie des ensembles tant par leur importance propre que par les démonstrations qui ont permis de les établir :

THÉORÈME 1.1 (Gödel, 1938). — *Si* **ZFC** *est non contradictoire, il n'existe pas de preuve de* $\neg$**HC** *à partir de* **ZFC**.

THÉORÈME 1.2 (Cohen, 1963). — *Si* **ZFC** *est non contradictoire, il n'existe pas de preuve de* **HC** *à partir de* **ZFC**.

Il peut être tentant de retenir que le problème du continu ne peut être résolu et qu'à défaut d'être fermé, il est du moins sans intérêt, tout nouvel effort étant voué à l'échec. Cette conclusion est erronée. On peut certes juger le problème inopportun si on accorde peu d'intérêt aux objets qu'il met en jeu : sous-ensembles compliqués de $\mathbb{R}$, bons ordres dont l'existence relève de l'axiome du choix(1). Par contre, on doit voir que la question, si elle n'est pas écartée *a priori*, n'est pas fermée mais ouverte par les résultats de Gödel et Cohen : ainsi que le démontre le corpus accumulé, le système **ZFC** n'épuise pas notre intuition des ensembles, et la conclusion ne doit pas être que l'hypothèse du continu n'est ni vraie, ni fausse(2), mais, simplement, que le système **ZFC** est incomplet, et qu'il s'agit de le compléter.

Des analogies sont évidentes : que l'axiome des parallèles ne soit pas conséquence des autres axiomes d'Euclide n'a pas clos la géométrie, mais, au contraire, a permis

(1) En fait, il existe aussi des versions plus effectives de **HC** ne portant que sur des objets *définissables*.
(2) voire est indécidable en quelque sens mystérieux

l'émergence des géométries non euclidiennes, et a ouvert la question de reconnaître, parmi toutes les géométries possibles, la plus pertinente pour décrire le monde physique. De même, les résultats de Gödel et de Cohen montrent que plusieurs univers sont possibles à partir de **ZFC**, et ouvrent donc l'étude des divers univers possibles — c'est-à-dire, de façon équivalente, des divers systèmes axiomatiques complétant **ZFC** — et la question de reconnaître, parmi ceux-ci, le(s) plus pertinent(s) pour décrire le monde mathématique.

Diverses questions préliminaires se posent, de ce que peut être un bon axiome, et, surtout, de ce que peut signifier *résoudre* un problème tel que le problème du continu sur la base d'axiomes additionnels(3). On reviendra sur ces questions dans la section 2 à la lueur du cas de l'arithmétique. Divers axiomes susceptibles de compléter **ZFC** interviendront dans la suite de cet exposé. Pour le moment, mentionnons simplement les axiomes de grands cardinaux, qui, intuitivement, sont les plus naturels, et dont le rôle est central. Ces axiomes affirment l'existence d'infinis d'ordre supérieur, dépassant les infinis qui les précèdent à la façon dont l'infini dépasse le fini. Ils constituent une itération du principe de départ de la théorie des ensembles qui est précisément de postuler l'existence d'ensembles infinis(4). L'une des raisons du succès des axiomes de grands cardinaux est leur efficacité pour décider un grand nombre d'énoncés non prouvables à partir de **ZFC**, *cf.* [9]. Le point important ici est qu'il semble raisonnable de tenir ces axiomes pour vrais, ou, au moins, de ne tenir pour plausibles que des axiomes **A** *compatibles* avec l'existence de grands cardinaux au sens où aucun axiome de grand cardinal ne contredit **A**.

2. ARITHMÉTIQUE, INCOMPLÉTUDE, ET FORCING

Notons V la collection de tous les ensembles(5). De même que le but ultime de l'arithmétique serait de déterminer tous les énoncés satisfaits dans la structure $(\mathbb{N}, +, \times)$, celui de la théorie des ensembles serait de déterminer tous les énoncés satisfaits dans la structure $(V, \in)$. Ce but étant inaccessible, une possibilité est de se restreindre à des structures plus simples du type $(H, \in)$, où H est un certain fragment de la collection des ensembles. La filtration par la cardinalité est alors naturelle :

(3)On se doute qu'ajouter simplement **HC** ou $\neg$**HC** aux axiomes ne serait pas une très bonne solution !
(4)Comme l'existence d'un grand cardinal entraîne toujours la non-contradiction de **ZFC**, le second théorème d'incomplétude interdit qu'une telle existence puisse être démontrée à partir de **ZFC**, et la poser comme hypothèse constitue donc toujours un axiome propre.
(5)en fait, la collection de tous les ensembles *purs*, définis comme ceux pouvant être obtenus à partir de l'ensemble vide en itérant les opérations de passage à l'ensemble des parties, à la réunion, et aux éléments. On sait que de tels ensembles suffisent à représenter tous les objets mathématiques.

Définition 2.1. — *Pour k entier, on note H_k l'ensemble de tous les ensembles A* héréditairement *de cardinal strictement plus petit que $\aleph_k$, au sens où A, les éléments de A, les élements des éléments de A, etc. sont tous de cardinal plus petit que $\aleph_k$*[6].

Considérons pour commencer la structure $(H_0, \in)$, c'est-à-dire le niveau des ensembles héréditairement finis. Notons $\mathsf{ZF}^{\text{fini}}$ le système ZF privé de l'axiome de l'infini.

Lemme 2.2. — *À partir des axiomes de $\mathsf{ZF}^{\text{fini}}$, on peut définir à l'intérieur de $(H_0, \in)$ une copie de $(\mathbb{N}, +, \times)$; inversement, à partir des axiomes de Peano, on peut définir à l'intérieur de $(\mathbb{N}, +, \times)$ une copie de $(H_0, \in)$* [7].

À un codage près, décrire $(H_0, \in)$ équivaut donc à décrire $(\mathbb{N}, +, \times)$: le niveau « héréditairement fini » de la théorie des ensembles coïncide avec l'arithmétique.

Une façon usuelle de décrire une structure S consiste à l'*axiomatiser*, c'est-à-dire à caractériser les énoncés satisfaits dans S comme ceux qui sont *prouvables* à partir d'un système d'axiomes suffisamment simple. Pour l'arithmétique, le système de Peano est bien connu, mais les théorèmes d'incomplétude de Gödel montrent que la description obtenue n'est pas complète : il existe des énoncés satisfaits dans $(\mathbb{N}, +, \times)$ mais non prouvables à partir des axiomes de Peano, et, de même, des énoncés satisfaits dans $(H_0, \in)$ mais non prouvables à partir de $\mathsf{ZF}^{\text{fini}}$.

Se placer dans le cadre de la théorie des ensembles permet de démontrer davantage d'énoncés, donc de se rapprocher d'une description complète. Dans le cas d'un énoncé φ portant sur H_0, cela signifie non plus chercher si φ est prouvable à partir de $\mathsf{ZF}^{\text{fini}}$, mais si l'énoncé « $(H_0, \in)$ satisfait φ » [8] est prouvable à partir de ZFC. De même, dans le cas d'un énoncé φ portant sur $\mathbb{N}$, il s'agit, au lieu de chercher si φ est prouvable à partir des axiomes de Peano, de chercher si « $(\mathbb{N}, +, \times)$ satisfait φ » [9] est prouvable à partir de ZFC.

---

[6] On rappelle que $\aleph_0, \aleph_1, \ldots$ est l'énumération croissante des cardinaux infinis, ceux-ci étant définis comme les ordinaux infinis qui ne sont en bijection avec aucun ordinal plus petit. Ainsi $\aleph_0$ (aussi noté ω), est le plus petit ordinal infini, donc aussi la limite supérieure des ordinaux finis, et $\aleph_1$ est le plus petit ordinal non dénombrable, donc la limite supérieure des ordinaux dénombrables. Alors $\aleph_0$ est le cardinal de $\mathbb{N}$, et, en notant 2^κ le cardinal de $\mathfrak{P}(\kappa)$ comme dans le cas fini, $2^{\aleph_0}$ est celui de $\mathfrak{P}(\mathbb{N})$, donc aussi de $\mathbb{R}$, de sorte que l'hypothèse du continu s'écrit $2^{\aleph_0} = \aleph_1$.

[7] On obtient une copie $\underline{\mathbb{N}}$ de $\mathbb{N}$ à l'intérieur de H_0 en définissant récursivement une copie $\underline{i}$ de l'entier i par $\underline{0} = \varnothing$ et $\underline{i+1} = \underline{i} \cup \{\underline{i}\}$: c'est la représentation de von Neuman des entiers par des ensembles. Il est alors facile de construire des copies $\underline{+}$ et $\underline{\times}$ de $+$ et $\times$, et de montrer à partir de $\mathsf{ZF}^{\text{fini}}$ que $(\underline{\mathbb{N}}, \underline{+}, \underline{\times})$ satisfait aux axiomes de Peano. À l'inverse, suivant Ackermann, on définit à l'intérieur de $(\mathbb{N}, +, \times)$ une relation $\underline{\in}$ en déclarant $p \mathrel{\underline{\in}} q$ vraie si le p-ième chiffre du développement binaire de q est 1, et on montre à partir des axiomes de Peano que $(\mathbb{N}, \underline{\in})$ satisfait aux axiomes de $\mathsf{ZF}^{\text{fini}}$, et est isomorphe à $(H_0, \in)$.

[8] c'est-à-dire l'énoncé obtenu à partir de φ en ajoutant que toutes les variables prennent leurs valeurs dans l'ensemble définissable H_0, *cf.* note 14

[9] ou, plus exactement et avec les notations de la note 7, « $(\underline{\mathbb{N}}, \underline{+}, \underline{\times})$ satisfait φ »

Le théorème d'incomplétude s'applique derechef, et l'axiomatisation par **ZFC** ne donne toujours pas une description complète de $(H_0, \in)$ et de l'arithmétique. Pour autant, cette description est en pratique satisfaisante, en ce que la plupart des exemples d'énoncés vrais mais non prouvables sont des énoncés *ad hoc* plus ou moins directement issus de la logique(10). De plus, et surtout, les manifestations de l'incomplétude de **ZFC** au niveau de l'arithmétique diffèrent fondamentalement de ses manifestations à des niveaux ultérieurs, par exemple dans le cas de l'hypothèse du continu.

Expliquer cette différence de nature requiert d'introduire la notion de *forcing* et, d'abord, celle de *modèle de* **ZFC**. Comme **ZFC** est une famille d'axiomes portant sur l'unique relation d'appartenance, on peut considérer de façon abstraite des structures (M, E) avec E relation binaire sur M telles que chacun des axiomes de **ZFC** soit satisfait lorsque E est prise comme valeur de l'appartenance : une telle structure est appelée *modèle* de **ZFC**. La validité des axiomes de **ZFC** s'exprime alors par le fait que la structure $(V, \in)$ constituée des *vrais* ensembles et de la *vraie* appartenance est un modèle de **ZFC** (11).

C'est le cadre conceptuel fourni par la notion de modèle de **ZFC** qui permet d'établir les théorèmes 1.1 et 1.2 : pour montrer que ¬**HC** (*resp.* **HC**) n'est pas prouvable à partir de **ZFC**, il suffit de construire un modèle de **ZFC** satisfaisant **HC** (*resp.* ¬**HC**), ce qu'on fait en partant d'un modèle (quelconque) M de **ZFC**, et en en construisant respectivement un sous-modèle L satisfaisant **HC** avec Gödel, et une extension $M[G]$ satisfaisant ¬**HC** avec Cohen(12). La méthode de Cohen, ou méthode du *forcing*, consiste à ajouter à M un ensemble G dont les propriétés sont définies (« forcées ») depuis l'intérieur de M par un ensemble ordonné $\mathbb{P}$, dit de *forcing*, qui décrit les éléments de $M[G]$ (13). Un modèle du type $M[G]$ est appelé extension *générique* de M.

L'existence du forcing introduit une variabilité essentielle dans la théorie des ensembles. Étant donné un modèle M, et un énoncé φ tel que ni φ, ni $\neg\varphi$ ne soient prouvables à partir de **ZFC**, il est fréquent qu'on puisse construire, à l'aide d'un premier ensemble de forcing $\mathbb{P}_1$, une extension générique $M[G_1]$ dans laquelle φ est satisfait, et, à l'aide d'un second ensemble de forcing $\mathbb{P}_2$, une autre extension générique $M[G_2]$ dans laquelle $\neg\varphi$ est satisfait, de sorte que privilégier φ ou $\neg\varphi$ semble

(10) Noter néanmoins les propriétés combinatoires isolées par H. Friedman [6], ou les résultats de Y. Matiyasevich sur l'existence d'équations diophantiennes dont la résolubilité est indémontrable [11].

(11) Cette description adopte un vocabulaire délibérément platonicien référant à un vrai monde de vrais ensembles : plus que d'une option philosophique, il s'agit d'une commodité de présentation, consistant à fixer un modèle de référence et à distinguer les modèles partageant la même relation d'appartenance.

(12) De même, pour montrer que les axiomes des groupes n'entraînent pas, disons, la commutativité, on pourrait partir d'un groupe G quelconque, et en construire respectivement un sous-groupe commutatif et une extension non commutative. La construction est plus délicate dans le second cas, car, rien n'excluant de partir avec $G = \{1\}$ ou $M = L$, le passage à une sous-structure ne saurait suffire.

(13) comme une extension de corps dont les éléments sont décrits par des polynômes du corps de base