Brouwer et Gödel : deux frères ennemis

Mark van Atten

Leurs conceptions philosophiques les opposaient, mais tous deux s'appuyèrent sur elles pour fonder une logique et des mathématiques modernes.

À l'aube du XX^e siècle, les travaux de Luitzen Brouwer et de Kurt Gödel ont marqué, pour la logique et les mathématiques, deux révolutions. En introduisant de nouvelles techniques, Gödel a inauguré l'approche mathématique de la logique telle qu'on la pratique aujourd'hui. En ce sens, il fut le premier logicien moderne. Brouwer a développé le premier système mathématique, à la fois cohérent et incompatible avec les mathématiques classiques (voir L'intuitionnisme, par Alexandre Miquel, dans ce dossier). Cependant Brouwer et Gödel édifiaient leurs mathématiques sur des convictions philosophiques personnelles, aussi contestées à leur époque qu'elles le sont aujourd'hui.

Les mathématiques ont-elles besoin de fondements philosophiques ? Les philosophes américains Willard Quine et Hilary Putnam, entre autres, prétendent le contraire depuis les années 1960, et leur opinion reste encore la plus partagée. Pourtant Brouwer, Gödel et la plupart de leurs contemporains ont tenu à poser de tels fondements.

Brouwer et Gödel ont forgé l'essentiel de leurs conceptions philosophiques alors qu'ils étaient encore de jeunes étudiants, et y sont restés fidèles durant toute leur carrière mathématique. Ces conceptions opposaient les deux hommes de leur vivant. Aujourd'hui toutefois, avec le recul du temps, on reconnaît leurs points communs, et l'on comprend mieux comment le travail de Brouwer inspira à Gödel son théorème d'incomplétude.

Le programme formaliste

Nous ne pouvons raconter les carrières de Brouwer et de Gödel sans évoquer le programme de David Hilbert, mathématicien allemand de la génération précédant celle de Brouwer. Selon Hilbert, les mathématiques se rapportent à des manipulations de signes et de formules qui n'ont pas de signification intrinsèque. Les mathématiques traitent d'objets qui n'existent pas en dehors des formules : ainsi pourrait-on remplacer les termes "point", "droite" et "plan" par "chope à bière", "chaise" et "table".

Les tenants de cette approche affirment que les mathématiques peuvent être complètement reconstruites sur la base de systèmes formels. En d'autres termes, les mathématiques peuvent être formalisées.

Avec le temps, Brouwer a convaincu Hilbert (comme Henri Poincaré l'avait déjà indiqué) qu'une théorie des systèmes formels doit inclure au moins l'arithmétique des nombres naturels et l'induction complète pour permettre la démonstration rigoureuse des propriétés importantes.

En effet, à cette condition, la preuve de la validité d'une loi pour tous les nombres comporte deux étapes : d'abord, on montre que cette loi est valide pour le nombre 0, puis on montre que, si elle

Articles extraits du magazine Pour la Science d'octobre-décembre 2005

est valide pour un nombre quelconque, alors elle l'est aussi pour le nombre suivant. En outre, il semblait préférable qu'un système formel comporte deux propriétés particulières : la cohérence et la complétude. La première assure que toute formule que le système est capable de montrer peut être interprétée comme une proposition mathématique vraie. La deuxième assure que tout énoncé valide admet une démonstration formelle dans ce système.

Suivant ces préceptes, Hilbert proposait de commencer à formaliser une petite partie des mathématiques simple et dénuée de problème philosophique. À partir de cette partie, on serait ensuite passé à des fragments de plus en plus grands des mathématiques, pour lesquels on aurait établi la complétude et la cohérence de systèmes formels. Finalement, en un nombre fini d'étapes, toutes les mathématiques classiques auraient été formalisées d'une façon cohérente et complète. Ce projet, que l'illustre mathématicien allemand proposa en 1900 lors du Congrès international des mathématiques de Paris, constitue ce que nous appelons "le programme de Hilbert" ; il occupa de nombreux mathématiciens des deux générations suivantes.

Des constructions mentales et intuitives

Nous l'avons vu, Brouwer a influencé le programme de Hilbert. Né en 1881 à Overschie, aujourd'hui faubourg de Rotterdam, aux Pays-Bas, Brouwer appartient à la génération de la mère de Gödel et d'Albert Einstein, futur ami intime de Gödel. À 17 ans, il écrit une déclaration de foi protestante, qui comporte déjà les grandes lignes de sa philosophie : seuls existent le moi et ses expériences, et il n'existe aucune réalité qui n'en dépende (Dieu est l'origine du moi). En 1905, dans un petit livre intitulé *La vie, l'art, et le mysticisme*, il développe cette idée et présente la vision du monde qui en découle.

En 1907, à l'Université d'Amsterdam, il soutient sa thèse de doctorat où il projette de fonder les mathématiques sur sa philosophie. L'"intuition pure" que l'on a du temps, concept inspiré de la philosophie d'Emmanuel Kant, y joue un rôle crucial. (En revanche, Brouwer rejette la notion kantienne d'une intuition pure de l'espace, à cause de la découverte de la géométrie non euclidienne.) Pour cette raison, Brouwer nomme "intuitionnisme" son programme fondateur.

Selon lui, l'esprit construit les objets mathématiques à partir de l'intuition pure ; aucun objet mathématique n'existe indépendamment de l'esprit, et rien en dehors des actes de pensée ne détermine la vérité mathématique. Ainsi les constructions mentales donnent aux mathématiques leur contenu propre ; les mathématiques sont intuitives et ne peuvent pas être purement hypothético-déductives comme le prétendent Hilbert et les formalistes. De surcroît, on ne peut réduire ces constructions à une simple langue, ainsi que souhaite faire Hilbert. L'intuitionnisme s'oppose d'emblée au formalisme, terme introduit dans le débat par Brouwer.

Pourtant, dans sa thèse, Brouwer admet la possibilité d'étudier le langage des mathématiques en faisant abstraction de son interprétation. Bien plus : il envisage la possibilité d'analyser mathématiquement ce langage en tant que tel (possibilité qu'il n'a pourtant jamais explorée). Il introduit alors la distinction entre mathématiques et métamathématiques lesquelles consistent en l'étude mathématique des mathématiques, ainsi que la distinction entre langage et métalangage. Brouwer communique ces vues à Hilbert lors d'un séjour commun sur la plage de Scheveningen, aux

Pays-Bas, en 1909. Plus tard, dans son programme pour fonder les mathématiques, Hilbert prêtera de l'importance à ces distinctions. L'investigation métamathématique jouera un rôle essentiel dans les théorèmes de Gödel.

De 1909 à 1913, Brouwer se ménage une pause dans son projet intuitionniste. Il crée la topologie moderne, branche des mathématiques qui étudie les déformations continues dans l'espace. C'est pour ce travail que la plupart des mathématiciens d'aujourd'hui le connaissent. Brouwer fournit la première définition correcte de la notion de dimension d'un espace, et démontre son théorème du point fixe (selon lequel la déformation continue d'une boule laisse toujours au moins un point inchangé).

Grâce à ces brillants résultats, Brouwer obtient en 1913 une chaire à Amsterdam. Il peut alors retourner, pour le reste de sa vie, à son intuitionnisme. Plusieurs années plus tard, il refusera des postes dans les deux principaux départements de mathématiques de l'époque, Göttingen et Berlin : "Je préfère vivre au milieu d'amis néerlandais que j'apprécie, et d'ennemis néerlandais dont je sais percer le jeu, que vivre loin d'ici parmi des étrangers." En 1920, Brouwer devient un acteur important de la Grundlagenstreit, la polémique publique qui oppose, principalement, formalistes et intuitionnistes.

Une existence objective

Un quart de siècle après Brouwer, en 1906, Gödel naît à Brno, en actuelle République tchèque, en tant que citoyen de l'Empire austro-hongrois. Il devient autrichien après la Première Guerre mondiale, et déménage à Vienne en 1924 pour entreprendre des études de physique. Il abandonne vite la physique pour les mathématiques, et se pique d'intérêt pour la philosophie.

Ainsi qu'il le racontera plus tard, Gödel devient platonicien vers 1925 : comme Platon, il pense que les objets des mathématiques existent en soi, indépendamment de l'esprit et des constructions mentales. Alors que selon Brouwer les vérités mathématiques sont construites, selon Gödel elles sont découvertes : le monde des idées serait une caverne d'Ali Baba, qui ne demanderait qu'à être découverte.

Cependant les deux hommes se rejoignent sur un point : ils soutiennent, l'un comme l'autre, que les mathématiques et ses objets ne sont pas de nature linguistique. Ici Gödel se trouve en désaccord non seulement avec Hilbert, mais aussi avec le Cercle de Vienne, dont il assiste aux réunions à partir de 1926.

Le Cercle de Vienne rassemble, entre autres, trois professeurs de Gödel, Rudolf Carnap, Moritz Schlick et Hans Hahn, qui se définissent comme des positivistes logiques : pour eux, la logique et les mathématiques sont des langages sans signification indépendante, des outils servant à organiser les sciences de la nature. À cause de son platonisme, Gödel partage rarement les opinions du positivisme logique qui règne à Vienne. Plus tard, il expliquera qu'il appréciait ces réunions parce qu'elles le familiarisaient avec les problèmes et les articles philosophiques d'alors.

Le premier résultat obtenu par Gödel, présenté dans sa thèse de doctorat de 1929, est le théorème de complétude pour la logique du premier ordre, c'est-à-dire une logique qui s'applique à des objets, et non aux relations entre ces objets (qui serait une logique du deuxième ordre). Ce théorème peut s'énoncer ainsi : tout énoncé valide de la logique du premier ordre admet une démonstration formelle dans un système qui formalise cette logique. En termes informatiques d'aujourd'hui, si un énoncé de cette logique est vrai, on peut commander à un logiciel de produire une preuve formelle de cet énoncé, alors que ce logiciel ignore totalement le sens de cet énoncé.

La méthode qu'emploie Gödel pour montrer ce théorème illustre sa modernité. Non seulement il sait distinguer les systèmes formels et leurs interprétations mathématiques - distinction bien connue depuis quelques décennies - , mais il sait aussi étudier les systèmes formels eux-mêmes par des méthodes de la théorie classique des ensembles, en utilisant librement, lorsque nécessaire, des techniques non constructives, telles que le raisonnement par l'absurde. Cela le distingue de Hilbert ainsi que d'autres contemporains, dont le Français Jacques Herbrand, qui a pressenti la possibilité de montrer le même théorème de complétude que Gödel, sans y parvenir parce qu'il refusait les méthodes non constructives dans les métamathématiques.

Le théorème de complétude de Gödel est une avancée dans le programme de Hilbert. En 1930 toutefois, au moment de la publication de ce théorème dans une revue de mathématique, l'esprit de Gödel comporte déjà en germe son célèbre théorème d'incomplétude, qui ruinera définitivement les espoirs de Hilbert (voir l'encadré) : "Pour tout système cohérent qui inclut l'arithmétique, il existe des énoncés que ce système ne pourra ni montrer ni réfuter." Et ce germe, c'est Brouwer qui l'y a semé.

En mars 1928, dans la tourmente de la Grundlagenstreit, Gödel assiste aux deux conférences que Brouwer donne à Vienne sur les fondements intuitionnistes des mathématiques et l'analyse intuitionniste. (L'éminent et influent Ludwig Wittgenstein est aussi présent, au moins à la première conférence ; on dit que celle-ci l'a fait retourner à la philosophie...)

Un an et demi plus tard, le 12 décembre 1929, Gödel rencontre Carnap chez un de ces pâtissiers de Vienne et, comme le rapporte Carnap dans son journal, lui explique que les mathématiques sont inépuisables. Carnap ajoute : "[Gödel] a été incité à cette idée par la conférence de Brouwer à Vienne. On ne peut pas complètement formaliser les mathématiques. Il semble qu'il ait raison."

La suite du rapport de Carnap montre que Gödel avait en tête un argument de la seconde conférence de Brouwer. En premier lieu, le continu nous est donné par l'intuition a priori du temps (on reconnaît la philosophie de Brouwer). En second lieu, le continu ne se laisse appréhender par aucun langage qui ne contiendrait qu'une quantité dénombrable d'expressions (parce que les nombres réels sont indénombrables).

Pour cette raison, aucune formalisation ne pourra saisir toutes les mathématiques. Au contraire, toute formalisation ratera des vérités sur le continu, vérités que seules de nouvelles intuitions pourront atteindre.

Pour accepter cet argument, on doit admettre qu'il existe dans les fondements des mathématiques un élément non formel ou, ce qui revient au même, non linguistique. Cette idée ne représente un obstacle ni pour Brouwer, qui comprenait les mathématiques comme des constructions non linguistiques et fondées sur l'intuition du temps, ni pour Gödel, qui comprenait les mathématiques comme une description d'un domaine platonicien, à l'existence indépendante de l'esprit humain et de ses créations (comme le langage).

Notons que le théorème d'incomplétude signale l'échec du programme de Hilbert, ce qui prouve qu'un résultat purement technique suffit parfois à réfuter une position philosophique.

Les oppositions

Nous avons vu que les idées de Brouwer, que Gödel découvre à Vienne, étaient dans sa thèse de 1907. Aussi Brouwer n'est-il pas surpris outre mesure, une vingtaine d'années plus tard, par le théorème d'incomplétude. Mais il aurait dû l'être, car Gödel montre bien plus que ce que Brouwer a prévu.

Dans une lettre de 1931 au mathématicien allemand Ernst Zermelo, Gödel précise (cette fois sans faire référence aux conférences de Brouwer) : "L'essentiel de mon résultat n'est pas qu'on puisse, d'une manière ou d'une autre, dépasser tout système formel (cela découle déjà de la "méthode de la diagonale" [par laquelle Cantor prouve que les nombres réels ne sont pas dénombrables] ; l'essentiel est que, pour tout système des mathématiques, il existe des énoncés exprimables dans ce système, mais indécidables à partir des axiomes de ce système, et que ces énoncés sont assez simples, puisqu'ils appartiennent à la théorie des nombres entiers positifs".

Brouwer et Gödel s'accordent sur l'idée que les progrès des mathématiques font toujours appel à l'intuition, mais ils divergent sur la nature exacte de ce que nous donne cette intuition : ils divergent sur la nature des objets mathématiques.

On pourrait penser qu'une telle divergence reste d'ordre philosophique, et concerne peu les mathématiques. En effet, plus que la nature des objets, ce sont les relations entre ces objets qui comptent dans les mathématiques. Après tout, $2 + 2 = 4$ reste vrai, que l'on considère les objets 2, 4, la fonction d'addition et le prédicat d'égalité comme des constructions mentales, comme des objets platoniques, ou comme n'importe quoi d'autre.

Pourtant la nature des objets mathématiques peut déterminer leur existence même. Dans un domaine platonicien, les objets mathématiques existent en dehors de ce que l'esprit est capable de construire, même en supposant illimités notre capacité de mémoire et notre temps disponible. Un exemple est donné par l'ensemble des nombres réels, dont l'infini est supérieur à l'infini dénombrable de l'ensemble des nombres entiers. L'existence de tels objets est justement permise par l'indépendance du monde platonicien vis-à-vis de nos esprits.

Inversement, selon Brouwer, il existe des constructions mentales qui ne correspondent à aucun objet du monde platonicien. Par exemple, quand un individu effectue des choix dans le temps, il engendre des suites de choix (à ne pas confondre avec la problématique de l'axiome de choix, dont il sera question plus loin). L'intuitionnisme produira des théorèmes qui ne sont pas valables en mathématiques classiques et qui concernent précisément les suites de choix.

Cette opinion sur la nature des objets mathématiques influe aussi sur les manières de raisonner. Brouwer n'accorde pas le statut de loi universelle au principe du tiers exclu, qui affirme que soit une proposition est vraie, soit sa négation l'est. En conséquence, des trois célèbres théorèmes de Gödel (complétude, incomplétude et indépendance de l'axiome du choix), seul le théorème d'incomplétude a un sens d'après les principes intuitionnistes, car les deux autres utilisent des modes de raisonnement que les intuitionnistes n'acceptent pas.

Ainsi des vues philosophiques différentes conduisent à des mathématiques différentes. La conception gödelienne des objets mathématiques est compatible avec les mathématiques classiques et notamment avec la théorie des ensembles, fondée par l'Allemand Georg Cantor, autre platonicien. La conception de Brouwer ne l'est pas. Dès qu'on accepte l'intuitionnisme, on est obligé de renoncer à plusieurs parties des mathématiques classiques, et on doit reconstruire ces parties sur de nouveaux fondements. D'un autre côté, la conception brouwerienne permet l'élaboration de théories mathématiques qui seraient impossibles du point de vue classique.

Retours à la philosophie

Quand Gödel publie son théorème d'incomplétude (1931), la carrière de Brouwer s'est déjà arrêtée. Des conflits titanesques ont mis à mal ses forces mentales et émotionnelles à la fin des années 1920, dont deux avec Hilbert concernant un congrès et la rédaction d'une revue, et un avec le mathématicien autrichien Karl Menger qui lui disputait la priorité quant à la définition correcte de la notion de dimension. En outre, en 1929, Brouwer se fait voler son carnet mathématique dans le tramway de Bruxelles, et il est au désespoir de reconstruire son contenu. Il avouera plus tard que cette perte le détermina à reporter son intérêt des mathématiques vers la philosophie.

Ce n'est qu'après la Seconde Guerre mondiale qu'il reprend ses recherches mathématiques et écrit une série d'articles plus radicaux que jamais. Les temps ont changé, car ces articles n'attirent plus autant l'attention que durant les années 1920. Ironie de l'histoire : si l'intuitionnisme exerce aujourd'hui une influence considérable dans certains domaines des mathématiques et de l'informatique, cette influence réside non pas dans les mathématiques elles-mêmes, mais dans la logique, que Brouwer considérait comme moins intéressante.

Après l'incomplétude, le premier grand résultat de Gödel concerne la théorie des ensembles, dont la version la plus élaborée, dite "théorie ZF", est due aux deux mathématiciens Ernst Zermelo et Adolf Fraenkel. À la fin des années 1930, le logicien autrichien montre qu'un axiome contesté, l'axiome du choix (voir la figure 4), ainsi que l'hypothèse du continu (selon laquelle il n'existe pas d'infini plus grand que celui des entiers naturels et plus petit que celui des réels), sont tous les deux cohérents avec les axiomes de la théorie ZF.

Gödel cherche à démontrer l'"indépendance" de ces propositions par rapport à ZF, c'est-à-dire l'impossibilité de déduire de ZF ni ces propositions ni leurs négations. Son but est de montrer que la théorie ZF serait trop faible pour décider ces propositions. Comme il a déjà montré leur cohérence avec ZF, il lui reste donc à prouver la cohérence de leurs négations avec ZF. Mais il n'y parvient pas. Aux alentours de 1942, frustré par ses échecs successifs, Gödel décide, comme

Brouwer une décennie plus tôt, de quitter la logique mathématique pour la philosophie. Il s'attache notamment à l'Allemand Gottfried Leibniz, rationaliste et initiateur de la logique symbolique, et surtout (il y consacrera 20 ans) à l'Autrichien Edmund Husserl, fondateur de la phénoménologie.

Les théorèmes d'indépendance que cherchait Gödel sont établis en 1963 par l'Américain Paul Cohen. Pour certains théoriciens des ensembles, cette indépendance suggère qu'il n'existe pas une vérité absolue dans la théorie des ensembles : qu'on choisisse d'accepter l'axiome du choix ou sa négation, ZF n'est pas contredit. Pour Gödel, en revanche, cette indépendance indique qu'il faut trouver une théorie des ensembles capable de décrire le monde platonicien en plus grand détail que ne le fait ZF. Il suggère alors de chercher de nouveaux axiomes à ajouter à ZF.

Dans les années 1960 et 1970, bien qu'il consacre la plupart de son temps à la philosophie, Gödel poursuit une dernière fois ce but mathématique, en cherchant à déterminer si l'hypothèse du continu est vraie ou fausse. Il n'y est pas parvenu, mais des progrès ont été récemment accomplis dans ce programme.

Rencontres peu amicales

En 1940, Gödel et sa femme émigrent aux États-Unis, puis se font naturaliser américains quelques années plus tard. Gödel travaille à l'Institute for Advanced Study (IAS) à Princeton, où il devient l'ami intime d'Einstein. Restée à Vienne, la mère de Gödel est fière de l'amitié de son fils avec le célèbre physicien et demande souvent de ses nouvelles dans ses lettres.

En 1953, Brouwer donne une série de conférences au Canada et aux États-Unis, qui comporte un arrêt à Princeton. Gödel l'invite à deux reprises, pour le déjeuner et pour le thé. D'après sa correspondance avec sa mère, il n'a pas beaucoup apprécié Brouwer, ce que confirment ses amis. Quand Gödel raconte que les conférences de Brouwer n'ont pas remporté un franc succès, il ajoute : "à juste titre". Cependant, les idées de Brouwer et Gödel se rejoignent sur plusieurs points : fièrement en désaccord avec l'esprit du temps (Zeitgeist), intransigeants, ils ont souligné l'importance de l'intuition, sont restés sceptiques quant au pouvoir du langage, et ont rejeté les philosophies naturaliste, matérialiste et mécaniste. Enfin ils ont tous les deux partagé un intérêt pour le mysticisme.

Nous l'avons vu, les travaux techniques de Brouwer et de Gödel ont été motivés par leurs positions philosophiques, tout aussi contestées l'une que l'autre. Cependant, à la différence de Brouwer, Gödel était en faveur de la tradition des mathématiques classiques. C'est pourquoi les résultats qu'il a obtenus, bien qu'en grande partie motivés par ses idées platoniciennes, sont acceptés par la majorité des mathématiciens, y compris ceux qui ne partagent pas ses vues platoniciennes, et y compris ceux qui pensent que la philosophie n'est pas capable de fonder les mathématiques.

Les mathématiques intuitionnistes, au contraire, s'opposent à la tradition et semblent avoir besoin d'une motivation philosophique. Accepter l'intuitionnisme, c'est abandonner les pratiques traditionnelles, et cette circonstance a longtemps été un obstacle au développement de l'intuitionnisme.

D'un autre côté, Brouwer a intégré sa philosophie à son travail technique, bien mieux que ne l'a fait Gödel. Ce dernier a développé une vision fondamentale du monde, à partir de Leibniz, mais il n'a jamais noué de liens aussi solides que Brouwer entre ses conceptions et ses mathématiques.

On peut douter que les idées philosophiques de quelqu'un puissent résulter de sa psychologie, mais on peut remarquer que certaine constitution psychologique s'accorde avec certaine position philosophique. L'intuitionniste Brouwer cherchait la vérité en son for intérieur, puis l'appliquait au monde extérieur ; le platonicien Gödel cherchait la vérité en dehors de lui-même, puis subordonnait sa vie à ce qu'il découvrait. De fait, Brouwer s'est engagé dans le monde bien plus énergiquement que Gödel : il a pris part à un grand nombre de conflits scientifiques et politiques, et il a beaucoup voyagé. De son côté, Gödel a évité les voyages et l'engagement politique ; il a toujours respecté la loi et les autorités, parfois jusqu'à l'irrationalité, et a fui les discussions en public.

Tous les deux connurent une fin tragique. Un soir de 1966, en traversant la rue, Brouwer fut renversé par une voiture et écrasé par plusieurs autres. En 1978, après des années de troubles mentaux allant s'aggravant, Gödel se laissa mourir de faim.

Le théorème d'incomplétude

"Pour tout système formel qui est cohérent et qui inclut l'arithmétique, il existe des énoncés que ce système ne pourra ni montrer ni réfuter." (S'il n'est pas cohérent, un système est capable de montrer tout énoncé exprimable dans son langage et est donc inutile.) Comment Gödel a-t-il démontré son théorème d'incomplétude ?

Dans un premier temps, il constate que la formalisation d'une théorie, menée jusqu'au bout, lui permet de codifier les éléments et la structure d'une preuve formelle en nombres entiers. Ainsi il attribue un nombre à chaque symbole de l'arithmétique et de la logique. Par exemple, le chiffre 0 est codé par 1, le quantificateur universel par 9, la parenthèse ouvrante par 11. Une formule de l'arithmétique, qui n'est qu'une suite de symboles, est donc transposée en une suite de nombres.

Cette suite est à son tour transformée en un nombre unique, tel que sa décomposition en nombres premiers admet pour puissances successives les nombres qui codifient les différents symboles. Grâce à l'unicité de cette décomposition, cette transformation est réversible : la décomposition permet de retrouver la suite de nombres (puis de symboles) d'origine.

Ce codage autorise un traitement strictement mathématique des systèmes formels. Ainsi on comprend pourquoi un système doit contenir l'arithmétique pour que la preuve de Gödel fonctionne : le codage et le décodage utilisent des opérations arithmétiques, telles que la décomposition en nombres premiers.

Étant donné un système formel, Gödel indique comment construire l'ensemble des nombres qui codifient tous les énoncés démontrables par les règles formelles de ce système. Notons que cet ensemble contient aussi les nombres qui codifient les négations des énoncés que le système est capable de réfuter.

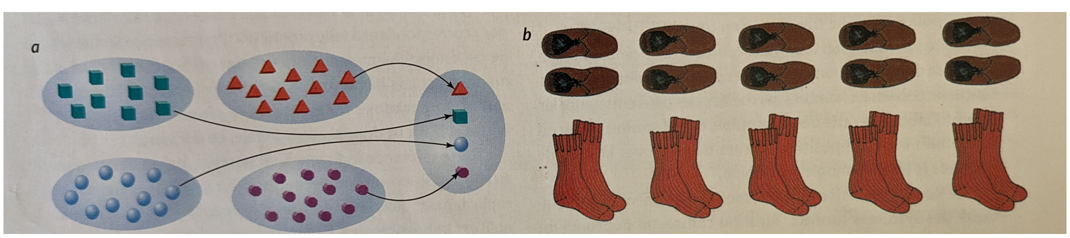
Enfin Gödel construit un nombre qui codifie un énoncé de ce système mais n'appartient pas à cet ensemble. Ce nombre correspond donc à un énoncé qui est indécidable dans le système. Il est toujours possible de décider cet énoncé dans un système un peu plus complexe, mais pour ce système-là on construira par les mêmes méthodes des énoncés indécidables propres.

Un énoncé indécidable est le suivant : “L’énoncé codifié par le nombre correspondant à telle propriété n’admet ni preuve ni réfutation dans ce système.” L’astuce est de s’assurer que, par construction, le nombre auquel cet énoncé fait référence par “correspondant à telle propriété” n’est autre que le nombre de cet énoncé lui-même. Alors en effet cet énoncé dit que lui-même n’est pas démontrable. Cela rappelle, sans y être équivalent, le paradoxe du menteur : la phrase “Je mens” est fausse si je mens donc si elle est vraie, et vice versa.

Cette référence indirecte à un nombre, par sa description au lieu de son expression, est nécessaire, car on ne peut nommer explicitement dans un énoncé le nombre qui le codifie, de même qu’il est impossible de citer intégralement dans une phrase en français cette phrase elle-même. Par exemple, on peut écrire : “La phrase que j’écris ici est en français”, mais on ne peut remplacer la description “que j’écris ici” par une citation explicite, au risque de se heurter à une régression infinie : “La phrase “La phrase “La phrase...

Notes

1. Luitzen Brouwer (1881-1966) fut, comme le témoigna le philosophe allemand Edmund Husserl après leur rencontre, “un homme absolument original, radicalement sincère, authentique, complètement moderne”.
2. Kurt Gödel (1906-1978) suivit les conférences que Brouwer donna en 1928 à Vienne sur l’intuitionnisme, et s’en inspira. Des conférences ultérieures de Brouwer, il rapporta qu’elles eurent peu de succès, “à juste titre”. Les deux hommes ne s’appréciaient guère.
3. David Hilbert (1862-1943) propose de formaliser les mathématiques, partant de l’idée que seules comptent les définitions des propriétés des objets.
4. Selon l’axiome du choix, étant donné une collection d’ensembles (disjoints et non vides), il existe un ensemble qui contient (qui a choisi) exactement un élément de chaque (a). Les intuitionnistes refusent cet axiome comme principe général. En effet, on peut définir une collection d’ensembles dont on sait qu’ils sont disjoints et non vides, mais dont on ne connaît pas (ou pas encore) une méthode pour construire les éléments. Dans ce cas, on ne peut choisir des éléments parmi eux, si bien qu’on ne peut dire si l’ensemble des éléments choisis existe. Bertrand Russell avait soulevé un problème semblable (b) : pour la collection infinie de paires de chaussures, la loi “choisir la chaussure droite de chaque paire” définit un ensemble d’éléments. En revanche, il n’existe pas de telle loi pour la collection infinie de paires de chaussettes (les chaussettes droites et gauches étant identiques).



5. Platon et Aristote, ainsi représentés par Raphaël, pourraient symboliser Gödel et Brouwer : pour l’un, les idées préexistent dans un monde supérieur, pour l’autre, les idées sont conçues ici-bas.

Mark van Atten est chargé de recherche (CNRS) à l’Institut d’histoire et de philosophie des sciences et techniques, Paris.

Références

[1] Mark van Atten, On Brouwer, Belmont, Wadsworth, 2004.
[2] Pierre Cassou-Nogues, Gödel, Paris, Les Belles Lettres, 2004.
[3] Dirk van Dalen, Mystic, Geometer, and intuitionist, 2 tomes, Oxford, Clarendon Press, 1999 et 2005.
[4] Glanbruno Guererio, Gödel, logique à la folie. Pour la Science, Collec. Les génies de la science n° 20, août 2004.
[5] Palle Yourgrau, Einstein/Gödel. Quand deux génies refont le monde, Paris, Dunod, 2005.

L'intuitionnisme : où l'on construit une preuve

Alexandre Miquel

Le raisonnement par l'absurde n'est pas constructif ! La logique intuitionniste, au contraire, relie preuve construite et calcul.

À partir de la fin du XIX[e] siècle, le développement considérable des mathématiques conduit de nombreux chercheurs de cette discipline à s'interroger sur la nature du raisonnement mathématique. L'introduction de nouveaux objets toujours plus complexes et l'utilisation de méthodes de raisonnement toujours plus abstraites (comme l'axiome du choix, dont l'introduction par Ernst Zermelo fut suivie de débats houleux) nécessite bien plus qu'une simple remise à plat des principes mathématiques.

Il ne suffit pas de spécifier les axiomes que l'on se donne et les règles de raisonnement que l'on s'autorise encore faut-il savoir pourquoi on considère tel ou tel axiome, et pourquoi on raisonne de telle ou telle manière.

Dans ce contexte, le jeune mathématicien hollandais Luitzen Brouwer bâtit à partir de 1907 une critique philosophique originale du raisonnement mathématique classique, auquel il reproche ses méthodes non constructives (on démontre qu'un être mathématique existe, mais on n'en construit pas d'exemple). En remplacement, il propose une méthode de raisonnement centrée sur la notion de "construction intuitive", qu'il dénomme finalement "intuitionnisme".

De cette démarche, la plupart des contemporains de Brouwer - et encore aujourd'hui la majorité des mathématiciens - ont retenu qu'elle consistait à rejeter des principes logiques élémentaires, tels que le principe du tiers exclu ("ou A ou non-A") et, ce qui revient au même, le raisonnement par l'absurde. Pourtant, loin d'amputer les mathématiques, l'intuitionnisme donne au contraire un caractère plus tangible aux objets mathématiques et renforce la notion de preuve.

Exclu, le tiers exclu !

Pour saisir la démarche de Brouwer, examinons pourquoi la logique classique n'est pas constructive : du point de vue de la prouvabilité, le comportement des connecteurs logiques tels que la conjonction "et", notée $\wedge$, et la disjonction "ou" notée $\vee$, est révélateur.

Traitons d'abord la conjonction. À partir d'une preuve d'une proposition A et d'une preuve d'une autre proposition B, il est possible, par simple assemblage, de constituer une preuve de la proposition $A \wedge B$ (A et B sont vraies) : c'est la signification même de la conjonction. Réciproquement, à partir de toute preuve de la proposition $A \wedge B$, on peut déduire une preuve de A (puisque A est une conséquence logique de $A \wedge B$), ainsi qu'une preuve de B (par le raisonnement symétrique). En d'autres termes, la proposition $A \wedge B$ est prouvable si et seulement si A est prouvable et B est prouvable.

Cette propriété est loin d'être anecdotique : elle exprime que les règles de démonstration qui régissent le comportement du connecteur $\wedge$ se conforment à l'utilisation qu'on souhaite en faire. Il semble qu'une logique qui ne vérifierait pas cette propriété serait bonne à jeter.

Passons à la disjonction. À partir d'une preuve de la proposition A, on démontre la proposition $A \vee B$ (A ou B est vraie), puisque $A \vee B$ est une conséquence logique de A. De même on démontre la proposition $A \vee B$ à partir d'une preuve de la proposition B. Le simple fait de disposer ou bien d'une preuve de A ou bien d'une preuve de B suffit à construire une preuve de $A \vee B$.

Qu'en est-il de la réciproque ?

Est-il possible, à partir d'une preuve de la proposition $A \vee B$, de retrouver ou bien une preuve de A, ou bien une preuve de B ?

Étonnamment la réciproque est fausse en logique classique. Le principe du tiers exclu permet en effet de prouver certaines propositions de la forme $A \vee B$ sans pour autant prouver ni A ni B. Pour nous en convaincre, examinons une proposition A qui est indécidable dans le formalisme, c'est-à-dire telle que ni A ni sa négation $\neg A$ ne sont prouvables dans le système considéré (le théorème de Gödel permet de construire une telle proposition dans n'importe quelle théorie contenant l'arithmétique). Bien qu'aucune des deux propositions A et $\neg A$ ne soit prouvable, leur disjonction $A \vee \neg A$ est néanmoins prouvable... d'après le principe du tiers exclu ! L'encadré A fournit un exemple d'une telle preuve.

Le même problème surgit avec la quantification existentielle, notée $\exists$. Considérons une proposition de la forme "Il existe un objet x qui possède la propriété A", ce que l'on écrit en logique formelle $\exists x\ A(x)$. S'il existe un terme t, dit "témoin", pour lequel la proposition $A(t)$ est prouvable, alors on détient une preuve de la proposition $\exists x\ A(x)$.

Réciproquement, on serait en droit d'attendre que pour chaque proposition prouvable de la forme $\exists x\ A(x)$, il soit possible de trouver un terme t pour lequel la proposition $A(t)$ est prouvable. Hélas il n'en est rien, car le tiers exclu permet de construire des formules $A(x)$ pour lesquelles la proposition $\exists x\ A(x)$ est prouvable, sans pour autant qu'il soit possible d'exhiber un objet t pour lequel la proposition $A(t)$ est prouvable : l'encadré B en donne un exemple.

Ce comportement surprenant, en logique classique, de la disjonction et de la quantification existentielle incite les mathématiciens intuitionnistes à rejeter le tiers exclu. Pour les intuitionnistes, non seulement les objets mathématiques doivent conserver un caractère concret, mais aussi et surtout toute preuve de $A \vee B$ doit contenir, au moins implicitement, une preuve de A ou une preuve de B. de même que toute preuve de $\exists x\ A(x)$ doit contenir, au moins implicitement, un témoin t de cette existence accompagné d'une preuve de la proposition $A(t)$.

Avec une telle exigence sur le contenu des preuves, l'intuitionnisme est loin d'affaiblir la logique !

Des objets construits

On touche ici à une différence essentielle entre la conception classique et celle que prône Brouwer. La conception classique des mathématiques est essentiellement réaliste : elle considère implicitement que chaque énoncé mathématique réfère à une réalité extérieure, indépendante du mathématicien. Si cette conception se justifie aisement pour des énoncés simples, qui ne portent que sur des objets élémentaires, elle devient plus hasardeuse dès que les énoncés et les objets manipulés gagnent en complexité. Car enfin, à quelle réalité extérieure peuvent bien référer des objets aussi abstraits qu'un espace de dimension infinie ou l'ensemble des parties de l'ensemble des parties de la droite réelle ?

Sans doute parce qu'ils manipulent fréquemment de tels objets, de nombreux mathématiciens se réclament de l'école néo-platonicienne, qui accorde une existence objective aux entités mathématiques les plus abstraites ; c'était aussi le cas du logicien Kurt Gödel (voir *Brouwer et Gödel, deux frères ennemis*, par Mark van Atten, dans ce dossier).

Brouwer refuse le recours à des arguments de nature métaphysique pour justifier le raisonnement mathématique. Selon lui, le raisonnement est avant tout une construction du mathématicien, une activité du sujet créateur. Les énoncés mathématiques réfèrent non pas à une quelconque réalité extérieure, mais aux constructions de l'esprit du mathématicien. En particulier, la démarche intuitionniste ne sépare pas le caractère constructif des objets mathématiques du caractère constructif des preuves, ce qui explique sans doute que Brouwer ne se soit jamais intéressé à la partie purement logique de l'intuitionnisme.

La question de l'infini

L'intuitionnisme rejette non pas la notion d'infini, mais la notion d'infini réalisé, ou infini actuel, c'est-à-dire l'idée qu'il existe un ensemble infini dont tous les éléments sont donnés a priori. L'intuitionniste ne reconnaît que l'infini potentiel, engendré à partir d'un nombre fini de règles de constructions élémentaires. Par exemple, la notion d'entier naturel est définie à partir d'un objet - le zéro - et d'une méthode permettant de construite un nouvel entier à partir de chaque entier - la construction successeur.

Le mathématicien italien Giuseppe Peano, en 1889, avait déjà reconstruit l'arithmétique des entiers naturels sur de tels principes. Le Hollandais Arend Heyting, étudiant de Brouwer, reformulera cette arithmétique dans le cadre intuitionniste. L'ensemble des entiers naturels, pour les intuitionnistes, n'est rien d'autre que l'ensemble des objets qu'il est possible de construire à l'aide de ces deux méthodes de construction, le zéro et le successeur. Pour raisonner sur les entiers, il n'est pas nécessaire de supposer que tous ceux-ci aient été déjà construits.

Ce point explique que le tiers exclu soit valide dans certaines circonstances et pas dans d'autres. Par exemple, l'énoncé “quels que soient les entiers naturels x et y, ou $x = y$ ou $x \neq y$”, noté $\forall x \in \mathbb{N}\ \forall y \in \mathbb{N}\ (x = y \vee x \neq y)$, prend bien la forme du tiers exclu et reste vrai pour les intuitionnistes : une procédure simple permet de comparer deux entiers et de decider s'ils sont égaux ou non (*voir la figure 2*).

En revanche, dès qu'on passe aux nombres réels, la proposition $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ (x = y \vee x \neq y)$ n'est plus démontrable. Pour les intuitionnistes en effet, un nombre réel se ramène à un processus de production d'une suite de décimales. Or. pour décider si deux suites de chiffres désignent le même nombre réel ou non, il faudrait être capable de les inspecter à l'infini : cela interdit toute possibilité de donner une preuve constructive à la proposition précédente.

Dans la mesure où l'intuitionnisme conçoit le raisonnement mathématique comme une activité subjective, il n'est pas étonnant que de subtiles différences d'appréciation aient surgi au sein de l'école constructiviste, et subsistent encore. En revanche, la partie purement logique de l'intuitionnisme, c'est-à-dire le calcul propositionnel intuitionniste et le calcul des prédicats intuitionniste, est définie sans ambiguïté. Comme la logique classique, elle admet diverses formalisations, qui sont toutes équivalentes.

Négation et double négation

L'abandon du tiers exclu a des répercussions considérables, parfois déroutantes, sur la structure de la logique. En premier lieu, la disparition de la dualité vrai/faux, qui n'est que l'expression idéalisée du tiers exclu, rend caduque la notion de table de vérité ! Comme les règles de déduction intuitionnistes sont toutes valides en logique classique, la logique intuitionniste n'établit que des formules tautologiques au sens des tables de vérité.

La réciproque est loin d'être vraie... En logique intuitionniste en effet, une proposition A n'est en général pas équivalente à sa double négation $\neg\neg A$. L'implication $A \implies \neg\neg A$ reste démontrable, mais sa réciproque ne l'est pas en général. Intuitivement, on peut considérer la formule $\neg\neg A$ comme une forme affaiblie de A, qui exprime littéralement que “A n'est pas contradictoire”. En revanche, la triple négation $\neg\neg\neg A$ reste équivalente à la simple négation $\neg A$.

Les lois de Morgan sont quant à elles altérées. Le logicien britannique Auguste De Morgan fut l'un des premiers, avec George Boole, à formaliser la logique au XIX$^{\text{e}}$ siècle. Il s'est notamment intéressé à l'effet cumulé de la négation et des connecteurs logiques, et a établi les équivalences duales suivantes : la négation de la disjonction de deux propositions équivaut à la conjonction des négations de ces propositions, ce que l'on écrit $\neg(A \vee B) \iff \neg A \wedge \neg B$; et la négation d'une conjonction équivaut à la disjonction des négations, soit $\neg(A \wedge B) \iff \neg A \vee \neg B$.

En logique intuitionniste, la première de ces équivalences subsiste tandis que sa duale disparaît. À la place, on doit se contenter de l'implication $\neg A \vee \neg B \implies \neg(A \wedge B)$. Ainsi la proposition $\neg(A \wedge B)$ peut être considérée comme une disjonction affaiblie, qui indique que les propositions A et B ne peuvent être toutes les deux vraies sans pour autant préciser laquelle des deux est fausse. (L'encadré A donne un exemple d'une telle disjonction.)

Disjonction et conjonction, qui ne peuvent plus être définies l'une à partir de l'autre par double négation, acquièrent ainsi leur indépendance.

Qu'en est-il des quantificateurs existentiel et universel ? De Morgan énonça aussi des équivalences sur ces quantificateurs : la non-existence d'un x tel que $A(x)$ équivaut à la négation de $A(x)$ pour tout x, ce que l'on écrit $\neg\exists x\ A(x) \iff \forall x\ \neg A(x)$; et la négation de $A(x)$ pour tout x équivaut à l'existence d'un x tel que non-$A(x)$: $\neg\forall x\ A(x) \iff \exists x\ \neg A(x)$.

L'intuitionniste conserve la première équivalence mais remplace la seconde par la simple implication $\exists x\ \neg A(x) \implies \neg\forall x\ A(x)$. Autrement dit, la proposition $\neg\forall x\ A(x)$ n'est plus qu'une forme affaiblie de $\exists x\ \neg A(x)$.

Enfin l'implication $A \implies B$ n'est plus équivalente à la proposition $\neg A \vee B$. (Cette dernière proposition, qui est plus forte, est parfois qualifiée d'implication "matérielle".) L'implication $A \implies B$ acquiert toute son autonomie pour devenir le connecteur principal de la logique intuitionniste.

Ainsi, en logique intuitionniste, la double négation d'une proposition A, $\neg\neg A$, tend à affaiblir le sens de la proposition A : cela revient à remplacer "A est vraie" par "A est non contradictoire". Comme d'autre part l'intuitionnisme renforce la disjonction, les tenants de cette démarche ont tôt remarqué que la disjonction affaiblie $\neg\neg(A \vee B)$ se comporte exactement comme une disjonction classique.

De la même manière, la quantification existentielle affaiblie $\neg\neg\exists x\ A(x)$ se comporte comme une quantification existentielle classique. Intuitivement cette dernière proposition exprime qu'il n'existe pas forcément (au sens constructif) un objet x satisfaisant la propriété A, mais qu'il n'est pas contradictoire de la supposer...

À partir de cette constatation, Gödel a démontré qu'en insérant des doubles négations dans une formule à certains endroits stratégiques (notamment devant des disjonctions et des quantifications existentielles), toute formule démontrable en logique classique devient démontrable en logique intuitionniste. Cette transformation des formules, qu'on appelle une "non-non-traduction", est fondamentale pour comprendre les liens qui unissent les deux logiques. Avec elle en effet, ce n'est plus la logique intuitionniste qui s'insère dans la logique classique, mais c'est la logique classique elle-même qui peut être étudiée comme un fragment de la logique intuitionniste.

Brouwer conçoit l'intuitionnisme comme une démarche de nature philosophique et délibérément informelle. Cette volonté de tenir l'intuitionnisme à l'écart de tout formalisme a sans doute handicapé les intuitionnistes face aux tenants de l'approche formaliste prônée par le mathématicien David Hilbert. De fait, l'intuitionnisme n'avait pas à ses débuts les outils mathématiques pour préciser ce qu'il fallait entendre par "construction" ou par "méthode effective".

Construire, c'est calculer !

Dans les années 1930 et 1940, les liens entre la prouvabilité en logique intuitionniste et la calculabilité en mathématiques se sont resserrés. À cette époque, on comprend mieux les notions mathématiques de fonction calculable, de programme et d'algorithme. Trois approches proposent des définitions équivalentes de la notion de fonction calculable, et engendreront trois familles de langages de programmation.

D'abord, en 1932, le mathématicien américain Alonzo Church introduit le lambda-calcul, un langage de programmation universel, fondé sur la seule notion de fonction (*voir l'encadré C page 35*).

Indépendamment, en 1936, le mathématicien anglais Alan Turing conçoit une machine capable de calculer à partir d'une suite d'instructions mécaniques. Enfin, à la fin des années 1940, le logicien américain Stephen Kleene, un étudiant de Church, fournit la définition moderne des fonctions récursives - les fonctions calculables des entiers dans les entiers - à partir d'un petit nombre de règles de construction très simples.

Cette clarification du concept de fonction calculable permet alors à Kleene d'établir un premier lien formel entre la prouvabilité intuitionniste et la calculabilité, à l'aide d'une technique qu'il appelle la "réalisabilité". L'idée de Kleene consiste à associer à chaque proposition A un ensemble de fonctions récursives (ou de programmes) qui la "réalisent", c'est-à-dire qui reflètent le contenu calculatoire d'une preuve constructive de A. En particulier, les programmes qui réalisent une disjonction $A \vee B$ choisissent effectivement l'un des deux membres A ou B, et les programmes qui réalisent une quantification existentielle $\exists x\ A(x)$ calculent effectivement un témoin de l'existence.

Kleene montre alors qu'à toute proposition A prouvable en logique intuitionniste, on peut associer un programme qui la réalise, ce qui lui permet d'établir quelques résultats fondamentaux concernant l'arithmétique de Heyting. Par exemple, à partir d'une preuve intuitionniste d'une proposition de la forme "pour tout x, il existe un y qui vérifie telle relation R avec x", ce qu'on écrit $\forall x\ \exists y\ R(x, y)$, il montre qu'on peut extraire un programme qui calcule effectivement y en fonction de x. Un corollaire de ce résultat est que la logique intuitionniste interdit toute possibilité de définir une fonction non calculable !

Il est important de comprendre que le programme n'est pas deviné à partir de la formule, mais qu'il est bel est bien construit à partir de la démonstration, dont il suit fidèlement la structure. En particulier, tout changement dans la démonstration peut avoir des répercussions importantes sur le programme qui en est extrait.

Le constructivisme quitte le terrain philosophique pour rejoindre celui des mathématiques et de l'informatique...

Une correspondance bien fructueuse

La réalisabilité de Kleene établit un pont entre les preuves de la logique intuitionniste et les programmes de calcul. Il faudra attendre les années 1960 pour que cette correspondance soit comprise. Ce que nous appelons aujourd'hui la correspondance de Curry-Howard (du nom des mathématiciens américains Haskell Curry, un étudiant de Hilbert, et William Howard, qui ont été les premiers à la remarquer) repose sur la notion de "type" : un type est un ensemble de données, de structures ou de fonctions qu'il est possible de manipuler de manière uniforme, à travers un certain nombre d'opérations communes. Par exemple, les entiers forment un type, et les fonctions des entiers dans les entiers forment un autre type. La correspondance de Curry-Howard associe à chaque proposition un type de données, et à chaque preuve d'une proposition un objet du type de données correspondant.

Pour comprendre en quoi consiste cette correspondance, rappelons qu'en logique intuitionniste, la valeur d'une proposition A est donnée, non pas par sa valeur de vérité, mais par l'ensemble de ses "preuves", c'est-à-dire par l'ensemble des constructions qui entraînent la conviction que A est vraie. Pour fixer les idées, désignons par $\Phi(A)$ l'ensemble des preuves de A, et examinons la structure de cet ensemble pour chacun des connecteurs $\wedge, \vee$ et $\implies$.

Commençons par la conjonction. Pour prouver la proposition $A \wedge B$, il faut être en mesure de prouver à la fois la proposition A et la proposition B. Par conséquent, une preuve de la proposition $A \wedge B$, en tant que construction, est un couple (x, y) constitué d'une preuve x de la proposition A et d'une preuve y de la proposition B. L'ensemble $\Phi(A \wedge B)$ des preuves de $A \wedge B$ est donc donné par le produit cartésien des deux ensembles de preuves $\Phi(A)$ et $\Phi(B)$ formé par l'ensemble de tous les couples (x, y) constitués d'une preuve x de A et d'une preuve y de B. Ainsi $\Phi(A \wedge B) = \Phi(A) \times \Phi(B)$, où $\times$ désigne le produit cartésien sur les ensembles.

Passons à la disjonction. Pour prouver la proposition $A \vee B$ en logique intuitionniste, il faut apporter soit une preuve de A, soit une preuve de B. Une preuve de $A \vee B$, en tant que construction, est donc soit de la forme x, où x est une preuve de la proposition A accompagnée d'une marque (l'indice "g") indiquantqu'on a prouvé le membre gauche de la disjonction, soit de la forme y, où y est une preuve de la proposition B accompagnée d'une marque (l'indice "d") indiquant que l'on a prouvé le membre droit de cette disjonction.

L'ensemble $\Phi(A \vee B)$ des preuves de $A \vee B$ est alors donné par l'union disjointe des ensembles de preuves $\Phi(A)$ et $\Phi(B)$ (l'union disjointe est une forme d'union dans laquelle on marque les éléments des membres gauche et droit avec des symboles différents de manière à ne jamais les confondre). En notant $+$ l'union disjointe, $\Phi(A \vee B) = \Phi(A) + \Phi(B)$. À travers la correspondance de Curry-Howard, la disjonction n'est donc rien d'autre que l'union disjointe.

Pour terminer, considérons le cas de l'implication, sans doute le plus important. Pour prouver la proposition $A \implies B$, il faut être en mesure de fournir un procédé permettant de transformer n'importe quelle preuve de A en une preuve de B. Une preuve de $A \implies B$, en tant que construction, est donc une fonction qui transforme n'importe quelle preuve de A en une preuve de B : c'est une fonction de l'ensemble $\Phi(A)$ vers l'ensemble $\Phi(B)$. L'ensemble $\Phi(A \implies B)$ des constructions qui prouvent $A \implies B$ est alors donné par $\Phi(A \implies B) = \Phi(A) \rightarrow \Phi(B)$ où $\Phi(A) \rightarrow \Phi(B)$ désigne l'ensemble des fonctions de $\Phi(A)$ dans $\Phi(B)$.

Voyons comment cette correspondance fonctionne sur un exemple, celui de la proposition $A \wedge B \implies B \wedge A$ qui exprime la symétrie de la conjonction. D'après la correspondance de Curry-Howard, cette proposition se transpose à l'ensemble des fonctions $\Phi(A) \times \Phi(B) \rightarrow \Phi(B) \times \Phi(A)$. Une preuve constructive de cette proposition est donnée par n'importe quel élément de cet ensemble, dont la fonction $(x, y) \rightarrow (y, x)$ qui échange les composantes du couple donné en argument. CQFD

Cette correspondance concerne toutes les constructions de la logique intuitionniste, en particulier les quantifications universelle et existentielle. On montre alors qu'à chaque règle de raisonnement intuitionniste correspond un mécanisme de construction de programme dans les types de données correspondants. Cette correspondance entre propositions et types, entre preuves et programmes, permet de relier nombre d'intuitions mathématiques à des intuitions informatiques.

De la mathématisation au traitement informatique

On le devine, la correspondance de Curry-Howard ouvre la voie à la programmation des preuves par l'informatique. En 1970, le mathématicien français Jean-Yves Girard définit un langage de programmation fondé sur le lambda-calcul, qu'il appelle le système F, et qui garantit la terminaison des programmes (à l'inverse de la machine de Turing). Il montre alors que toute fonction dont l'existence est prouvable en analyse intuitionniste peut être exprimée comme un programme bien typé (qui respecte les types des données qu'il manipule) dans le système F, et vice versa.

Dans les années 1970, le mathématicien suédois Per Martin-Löf propose un langage de programmation pour exprimer les mathématiques constructives : la théorie des types. Son point de départ est le suivant : si on définit un langage de programmation dont le système de types est suffisamment riche pour pouvoir exprimer toutes les constructions de la correspondance de Curry-Howard, alors ce langage de programmation permet également d'exprimer toutes les propositions et les démonstrations de la logique intuitionniste, à condition d'identifier les propositions aux types de données, et les preuves aux programmes.

Au-delà de l'immense simplification conceptuelle opérée par une telle identification, le bénéfice de cette approche tient à ce qu'elle ramène le problème épineux de la vérification de preuve à un simple exercice de vérification de type : il suffit de s'assurer que le programme donné (qui représente une preuve) a bien le type attendu (c'est-à-dire prouve la proposition voulue).

Dans la deuxième moitié des années 1980, de nombreux assistants à la démonstration mathématique sont construits sur le principe de la théorie des types. C'est le cas notamment du système *Coq* développé à l'Institut National de Recherche en Informatique et Automatique (Inria). Ce système repose sur le calcul des constructions, une variante de la théorie des types introduite par Thierry Coquand en 1985. Le noyau d'un assistant à la démonstration tel que *Coq* est essentiellement un vérificateur de types, qui fait également office de vérificateur de démonstrations. Autour de ce noyau est bâti un système de "tactiques" qui automatise certaines parties de la démonstration. Ce processus de construction est caché derrière une interface de logique traditionnelle, familière au mathématicien utilisateur.

Récemment le système *Coq* a ainsi vérifié la correction formelle de la preuve du théorème des quatre couleurs, selon lequel il est possible de colorier n'importe quelle carte à l'aide de seulement quatre couleurs, sans jamais assigner la même couleur à deux pays voisins. La démonstration de ce théorème repose sur un grand nombre de calculs, effectués par des programmes auxiliaires et, à cause de cette complexité, elle n'avait jamais complètement convaincu les mathématiciens. Les dernières incertitudes quant à la validité du théorème des quatre couleurs ont disparu quand il est devenu possible d'exprimer dans un même système formel tous les éléments de la preuve - qu'il s'agisse des programmes auxiliaires, de leur preuve de correction, ou de la preuve que la bonne exécution de ces programmes entraîne le théorème.

Le retour de la logique classique

La correspondance de Curry-Howard s'est étendue à toutes les mathématiques constructives, et même au-delà. Au début des années 1990, les informaticiens Matthias Felleisen et Timothy Griffin reconnaissent dans l'opérateur "call-cc", une instruction de traitement des erreurs dans un langage dérivé du lambda-calcul, le type correspondant à la loi de Peirce $((A \implies B) \implies A) \implies A$, variante du principe de raisonnement par l'absurde : dans le cas où B est la proposition absurde, cette loi exprime que s'il est possible de démontrer une proposition A à partir de l'hypothèse selon laquelle A est absurde, alors la proposition A est vraie.

Or cette loi, énoncée à la fin du XIX^e^ siècle par le logicien américain Charles Sanders Peirce, implique de manière intuitionniste le principe du tiers exclu. Il ne reste donc qu'un pas à franchir pour étendre la correspondance de Curry-Howard à la logique classique...

Il semble extraordinaire de conférer un contenu calculatoire à toutes les preuves de la logique classique, y compris aux preuves non constructives que nous avons mentionnées au début de cet article. Un tel miracle est possible grâce à un mécanisme, basé sur la notion de "continuation", qui permet aux programmes d'effectuer des retours en arrière au cours de leur exécution, et donc de revenir sur certains de leurs choix. Ainsi, au cours d'une preuve constructive, on peut "bluffer" en empruntant temporairement une piste de démonstration fausse (quitte à donner un témoin factice pour justifier une quantification existentielle), avant de revenir en arrière en cas de contradiction. Grâce aux continuations, les preuves constructives acquièrent la possibilité de "prêcher le faux pour découvrir le vrai", le principe même du raisonnement par l'absurde.

La boucle est bouclée : l'intuitionnisme permet de revenir à la logique classique, ce qui expliquerait que l'immense majorité des mathématiques repose encore sur la logique classique sans que cela ne pose le moindre problème. Cependant l'intuitionnisme a permis d'explorer des pistes nouvelles et fécondes en logique, et a engendré de nombreux sous-produits, aussi bien en logique, en informatique théorique que dans d'autres secteurs des mathématiques.

En logique, l'intuitionnisme a permis l'essor de la théorie de la démonstration dans la deuxième moitié du XX^e^ siècle, notamment à travers la réalisabilité, puis la correspondance de Curry-Howard. La constructivité en logique et sa difficulté à cohabiter avec la logique classique ont amené Jean-Yves Girard à découvrir la logique linéaire à la fin des années 1980. Les applications informatiques restent prometteuses.

L'intuitionnisme a aussi inspiré d'autres domaines des mathématiques, tels que la théorie des catégories ou la théorie des domaines. Enfin la logique intuitionniste a bouleversé notre compréhension même du raisonnement mathématique, en le ramenant à une construction de programme.

Il reste beaucoup à tirer de la correspondance entre preuves et programmes, dont la simple existence lève une partie du mystère de la "déraisonnable efficacité des mathématiques"

A. Une disjonction sans alternative

Théorème : *Ou bien $e + \pi$ est transcendant, ou bien $e\pi$ est transcendant.*

Rappelons qu'un nombre a est algébrique s'il existe un polynome $P(x)$ non nul à coefficients entiers tel que $P(a) = 0$, et qu'il est transcendant s'il n'existe pas de tel polynome. Par exemple, les nombres e et π sont tous les deux transcendants.

Preuve : On raisonne par l'absurde, en supposant que les deux nombres $S = e + \pi$ et $P = e\pi$ sont tous deux algébriques. Les deux nombres e et π peuvent être retrouvés à partir de leur somme S et de leur produit P comme les solutions de l'équation du second degré

$$x^2 - Sx + P = 0$$

dont les coefficients S et P sont algébriques.

Puisque toute solution d'une équation polynomiale à coefficients algébriques est elle-même algébrique, les nombres e et π sont tous les deux algébriques, ce qui est absurde. Donc S ou P est transcendant. CQFD

Cette preuve n'est pas constructive, car elle n'indique pas lequel des deux nombres $S = e + \pi$ ou $P = e\pi$ est transcendant. Ici le caractère non constructif provient de l'utilisation du raisonnement par l'absurde, qui permet entre autres d'établir un énoncé de la forme "A ou B" à partir du fait que sa négation est contradictoire, sans jamais décider pour autant qui, de A ou de B, est démontré.

B. Une existence sans témoin

Théorème : *Il existe deux nombres irrationnels a et b tels que a^b est rationnel.*

On rappelle qu'un nombre a est rationnel lorsqu'il peut s'écrire sous la forme du quotient de deux entiers, et qu'il est irrationnel sinon. Le nombre $\sqrt{2}$ est un exemple d'irrationnel.

Preuve. On applique le principe du tiers exclu à la proposition "Le nombre $\sqrt{2}^{\sqrt{2}}$ est rationnel" : soit $\sqrt{2}^{\sqrt{2}}$ est rationnel, soit il est irrationnel. Puis on raisonne sur chacun des cas.

1. Dans le cas où $\sqrt{2}^{\sqrt{2}}$ est rationnel, il suffit de prendre $a = b = \sqrt{2}$, et le théorème est démontré.

2. Dans le cas où $\sqrt{2}^{\sqrt{2}}$ est irrationnel, il suffit de prendre $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$. On vérifie alors que $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\left(\sqrt{2}^{\sqrt{2}}\right)} = \sqrt{2}^2 = 2$. Le théorème est démontré.

Cette preuve n'est pas constructive, car elle ne produit aucun couple (a, b) de nombres irrationnels tel que a^b soit rationnel. Chacun des deux cas propose bien un couple différent, mais l'instance du tiers exclu, qui est à la base de la disjonction de cas ci-dessus, ne permet pas de décider lequel des deux couples proposés répond à la question.

Notons que ce n'est pas l'énoncé du théorème ci-dessus qui est à incriminer, mais la preuve qui en est donnée. Le théorème est en réalité démontrable constructivement, à condition d'utiliser un raisonnement différent. Par exemple, en montrant d'abord de manière constructive que les nombres $\sqrt{2}$ et $\ln_2 3$ (le logarithme de 3 en base 2) sont irrationnels, puis en posant $a = \sqrt{2}$ et $b = 2 \ln_2 3$ (car $a^b = 3$).

C. Le lambda-calcul

Le λ-calcul est un langage qui exprime des fonctions et permet de les manipuler de manière purement symbolique. Comme la machine de Turing, il permet de représenter tous les entiers naturels et toutes les fonctions calculables.

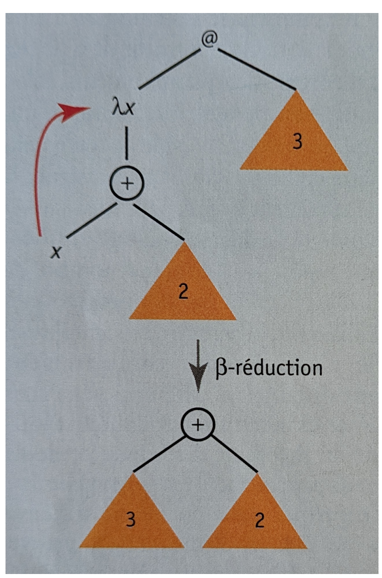
Une expression du λ-calcul est une expression formelle, faisant intervenir des variables, et construite à l'aide de deux mécanismes : la λ-abstraction et l'application.

Une λ-abstraction représente une fonction qui à tout objet désigné par une variable x associe un autre objet désigné par une λ-expression M dépendant de x ; on l'écrit $\lambda x.M$. Par exemple, l'expression $\lambda x.x+2$ représente la fonction qui à tout x associe $x+2$. L'abstraction rend la variable x muette. Ainsi les expressions $\lambda x.x+2$ et $\lambda y.y+2$ désignent la même fonction.

Une application, notée MN et symbolisée @ ci-dessous, désigne l'application de la fonction M à l'argument N (ce qu'on note plutôt $M(N)$ en mathématiques). Par exemple, l'expression $(\lambda\, x.x+2)3$ désigne l'application de la fonction $\lambda x.x+2$ à l'argument 3.

La seule règle de calcul, appelée β-réduction, consiste à remplacer, pour chaque application de fonction, la variable abstraite x par l'objet appliqué (dans notre exemple, 3). L'expression $(\lambda x.x+2)3$ se β-réduit à l'expression $3+2$.

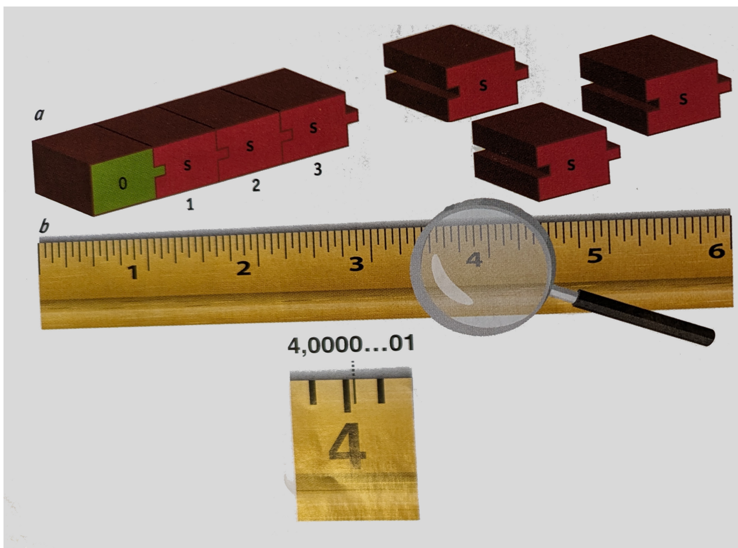
On poursuit le calcul en réduisant $3+2$ à 5 par une suite de β-réductions, avec un codage approprié.



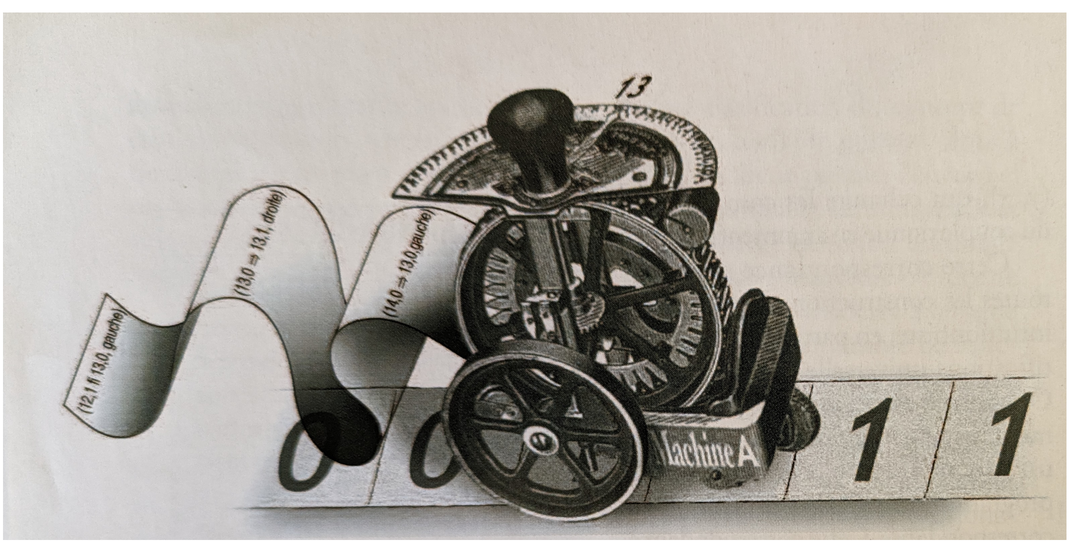
Notes

1. Le théorème des quatre couleurs affirme qu'il suffit de quatre couleurs pour colorier n'importe quelle carte de façon que deux pays ayant une frontière commune aient des couleurs différentes. Pour démonter ce théorème, Kenneth Appel et Wolfgang Haken eurent recours, en 1976, à des programmes informatiques, mais leur démonstration ne convainquit pas entièrement la communauté des mathématiciens. En 2004, le logiciel assistant de preuve *Coq* de l'INRIA a vérifié cette démonstration, créant un précédent dans la vérification automatique des preuves mathématiques. *Coq* repose sur la logique intuitionniste.

2. L'ensemble des entiers est construit (a) à partir du zéro (brique 0) et du successeur (brique s). Un algorithme récursif permet de tester si deux entiers sont égaux ou non ; il prouve de manière constructive que le tiers exclu est valide pour l'égalité des entiers. En revanche, dans l'ensemble des réels (b), on ne peut décider si deux éléments sont égaux ou non, car il faudrait pour cela explorer leurs décimales à l'infini : même si un grand nombre de décimales sont égales, il se peut que les décimales suivantes diffèrent.



3. La machine de Turing comporte une liste d'instructions qu'un mécanisme exécute sous la forme d'opérations de lecture ou d'écriture sur un ruban, à raison d'un signe par cellule. Après chaque opération, le ruban se décale d'une cellule, vers la droite ou vers la gauche. Cette machine rudimentaire n'en est pas moins extraordinairement puissante : elle est capable de calculer toute fonction effectivement calculable.



Alexandre Miquel est maître de conférences en informatique à l'Université Paris 7, au Laboratoire "Preuves, programmes et systèmes".

Références

[1] J.-Y. Girard, Y. Laffont et P. Taylor, Proofs and Types ; Cambridge University Press, 1989.

[2] A. Heyting, Intuitionism : An Introduction, North-Holland, Amsterdam, 1956.

[3] S. Kleene, Logique mathématique, Reprint J. Gabay, 2004.