Les Métamorphoses du calcul

Gilles DOWEK
2007

éd° Le Pommier

20 Abstraire du concret

La grande révolution du V^e^ siècle avant notre ère consiste donc en la distance mise entre les objets mathématiques, qui sont abstraits, et les objets concrets de la nature, même quand les objets mathématiques sont construits à partir des objets concrets.

22 Naissance de la mathématique

Qu'est-ce qui fait que le problème des pythagoriciens ne peut pas être résolu par un calcul ? […] Ce problème ne concerne […] pas un triangle particulier mais, potentiellement tous les triangles possibles. En outre, comme il n'existe pas de limite à la taille d'un triangle, le problème concerne simultanément une infinité de triangles. Ce changement dans la nature des objets mathématiques s'accompagne donc d'une irruption de l'infini dans les mathématiques : c'est cette irruption qui a rendu un changement de méthode nécessaire et a demandé de substituer le raisonnement au calcul. […]

Ce passage du calcul au raisonnement a été retenu comme l'acte de naissance des mathématiques, en Grèce, au V^e^ siècle avant notre ère.

25 Mathématiciens grecs et logiques

La logique des stoïciens […] est une conception très pauvre du langage dans laquelle il n'y a que deux catégories grammaticales : les propositions atomiques et les conjonctions. Elle ne prend pas en compte le fait qu'une proposition atomique – comme « Socrate est mortel » – se décompose en un sujet – Socrate – et un prédicat ou attribut – mortel.

La logique d'Aristote, contrairement à la logique des stoïciens, donne une place à la notion de prédicat […]. En revanche, [elle] ne comporte pas de « noms propres », c'est-à-dire de symboles pour désigner des individus ou des objets, comme « Socrate », car, pour Aristote, la science ne concerne pas les individus particulier, comme Socrate, mais uniquement les notions générales comme « homme », « mortel »… […] la logique d'Aristote reste trop frustre pour exprimer certains énoncé mathématiques : […] il n'y a pas de moyen de former la proposition « 4 est inférieur à 5 » […], il n'est pas possible de former la proposition « la droite D passe par le point A ».

On comprend pourquoi les mathématiciens grecs n'ont pas utilisé les logiques proposées par les philosophes de leur époque pour formuler les raisonnements de l'arithmétique et de la géométrie naissante : parce ces logiques n'étaient pas assez riches pour le permettre.

28 Table rase du calcul

On pourrait penser que les mathématiciens grecs, découvrant avec la méthode axiomatique une nouvelle sorte de mathématiques, ont cherché à comprendre comment cette nouvelle sorte de mathématiques prolongeait les mathématiques plus anciennes des Mésopotamiens et des Égyptiens. S'ils l'avaient fait, cela les aurait certainement amenés à chercher à comprendre comment articuler le calcul et le raisonnement. Mais ce n'est pas ce qu'ils ont cherché à faire : au contraire, ils ont fait table rase du passé et abandonné le calcul pour le remplacer pour le raisonnement.

De ce fait, après les Grecs, le calcul a à peine eu une petite place dans l'édifice mathématique.

57-8 Logique de Frege

Frege […] a réussi la synthèse des logiques d'Aristote et des stoïciens, et proposé une logique plus expressive que celle des philosophes de l'Antiquité.

[…] on peut définir, dans la logique de Frege, à peu près toutes les notions que l'on veut et y démontrer à peu près tous les théorèmes que l'on connaît. La logique de Frege a donc un double visage. D'un côté, elle ne fait qu'un énoncer les règles du raisonnement et des axiomes concernant des notions générales, comme la notion d'ensemble ou de concept. De ce point de vue, elle se situe dans la tradition des logiques d'Aristote et des stoïciens, et l'on peut définir l'adjectif « logique » en disant qu'un raisonnement est logique s'il peut se formuler dans la logique de Frege. D'un autre côté, elle permet de formuler tous les raisonnements mathématiques : elle se situe donc dans la tradition de la géométrie d'Euclide et l'on peut définir l'adjectif « mathématique » en disant qu'un raisonnement est mathématique s'il peut se formuler dans la logique de Frege. La logique de Frege fait donc apparaître une synonymie entre les adjectifs « logique » et « mathématique ». Il n'y a pas de spécificité du raisonnement mathématique : tout raisonnement logique peut être qualifié de « mathématique ». Des lors, il n'y a plus lieu de définir les mathématiques par les objets dont elles parlent : les nombres, les figures géométriques… On peut les définir par la manière dont elles en parlent : en faisant des démonstrations logiques. La spécificité des mathématiques, qui était de parler avec des nombres et des figures géométriques, s'efface et les mathématiques apparaissent universelles.

Au début du XX[e] siècle, Bertrand Russell a souligné l'importance de cette découverte, par Frege, de l'universalité des mathématiques. C'est une chose dont devraient se souvenir ceux qui dénient toute pertinence aux mathématiques dans le champ des sciences humaines.

59 Du paradoxe de Russell à la théorie des types

Un premier paradoxe dans la logique de Frege a été trouvé en 1897 par Cesare Burali-Forti. Il a ensuite été simplifié et popularisé par Russell en 1902. […]

Russell a été le premier à proposer, en 1903, une correction de la logique de Frege : la théorie des types, qu'il a développée dans les années qui ont suivi avec Alfred North Whitehead. La théorie des types de Russell et Whitehead classe les objets selon leur type : les objets qui ne sont pas des ensembles (les atomes) reçoivent le type 0, les ensembles d'objets de type 0 (les ensembles d'atomes) le type 1, les ensembles d'objets de type 1 (les ensembles d'ensembles d'atomes) le type 2… et la proposition « *x* est un éléments de *y* » ne peut être formée que quand le type de *y* est égal au type de *x* plus un. En conséquence, il n'y a pas d'ensemble de tous les ensembles, car on ne peut mettre ensemble les ensembles d'atomes et les ensembles d'ensembles d'atomes, pas non plus d'ensemble des ensembles qui ne sont pas éléments d'eux-mêmes, et pas de paradoxe de Russell.

60 De la théorie des types à la logique prédicative

Traditionnellement, on oppose les règles de déduction valables indépendamment des objets sur lesquels on raisonne, aux axiomes, spécifiques à une théorie particulière. Cette neutralité des règles de déduction par rapport aux objets sur lesquels on raisonne porte un nom savant : la neutralité ontologique de la logique. La logique de Frege, et après elle celle de Russell, comportait le défaut d'avoir des règles de déduction spécifiques à la notion de concept ou d'ensemble. Et si la notion d'ensemble ou de concept paraissait générale à l'époque de Frege, après le paradoxe de Russell, elle est apparue comme une notion comme les autres, en particulier, comme une notion qui demandait ses propres axiomes. La théorie des types de Russell a donc été à nouveau simplifiée dans les années vingt par David Hilbert, qui y a supprimé tout ce qui était spécifique à la notion d'ensemble, pour aboutir à la constitution de la « logique des prédicats », qui reste aujourd'hui le cadre de référence en logique. Les axiomes propres à la notion d'ensemble, énoncés en 1908 par Ernst Zermelo, forment, depuis cette époque, une théorie parmi d'autres : la théorie des ensembles.

61 Neutralité ontologique de la théorie des ensembles

un théorème démontré en 1930 par Kurt Gödel – mais qui n'est pas le célèbre « théorème de Gödel » montre que n'importe quelle théorie peut se traduire en théorie des ensembles : par exemple, la géométrique d'Euclide, qui est *a priori* un ensemble d'axiomes que la théorie des ensembles, peut se traduire en théorie des ensembles. Ce théorème restaure la thèse de Russell en donnant une universalité et une neutralité ontologique à la théorie des ensembles elle-même.

64 Sens d'une proposition, d'un axiome

C'est ainsi que les philosophes définissent la signification du mot « signification » : la signification d'un mot est l'ensemble des propositions vraies qui contiennent ce mot. De ce fait, il n'est pas possible de définir la signification d'un mot isolé, comme le laissent croire les dictionnaires. La signification de tous les mots est simultanément définie par l'ensemble des propositions vraies du langage. La vérité de la proposition « un oiseau vole dans le ciel » participe à la fois à la définition du mot « oiseau », du mot « ciel » et du mot « voler ». Pour être tout à fait exact, ce n'est pas l'ensemble des propositions vraies qui définit la signification des mots du langage, car cet ensemble est infini et assez compliqué : ce sont les critères qui permettent d'établir qu'une proposition est vraie, c'est-à-dire, dans le cas du langage mathématique, les axiomes et les règles de déduction.

[…] Depuis Poincaré, nous comprenons que cet axiome n'est pas une proposition qui nous apparaît miraculeusement évidente, parce que nous connaissons la signification de ces mots, mais que nous la tenons pour vraie parce qu'elle fait partie de leur définition.

69-70 / 74 / 77 Le problème de la décision : arithmétique, géométrie, prédicats

En 1929, Mojzesz Presburger a proposé un algorithme pour décider toutes les propositions de l'« arithmétique linéaire », c'est-à-dire du fragment de la théorie des nombres entiers, dans lequel on garde l'addition mais on supprime la multiplication. […] En 1930, Thoralf Skolem a, à l'inverse, proposé un algorithme pour décider la démontrabilité de toutes les propositions de la théorie des nombres entiers dans lesquelles figure la multiplication, mais pas l'addition. En 1930 encore, Alfred Tarski a proposé un algorithme pour décider toutes les propositions de la théorie des nombres réels dans lesquelles figurent à la fois l'addition et la multiplication.

[…] Une conséquence de l'existence de l'algorithme de Tarski est que tous [les problèmes de la géométrie d'Euclide] peuvent se résoudre par le calcul. Alors que les Grecs avaient introduits le raisonnement pour résoudre des problèmes, en particulier de géométrie, qu'ils n'arrivaient pas à résoudre par le calcul, Tarski montrait, au moins dans le cas de la géométrie, que ce passage du calcul au raisonnement n'était rétrospectivement pas nécessaire, puisqu'un algorithme, que les Grecs n'avaient pas entrevu, pouvait se substituer au raisonnement.

[…]

Une question s'est alors naturellement posée : qu'en était-il du langage mathématique en entier ? […] Le problème de trouver un algorithme pour décider si une proposition est démontrable ou non dans la logique des prédicats a été formulée par Hilbert dans les années vingt sous le nom de « problème de la décision ». […] La solution au problème de la décision a été apportée indépendamment, en 1936, par Alonzo Church et Alan Turing, et elle est négative : il n'existe pas d'algorithme de décision pour la logique des prédicats. Il existe donc une différence de nature entre le raisonnement et le calcul, et le programme de Hilbert de remplacer le raisonnement par le calcul était voué à l'échec. […]

La question de Hilbert n'était […] pas de savoir si l'on pouvait remplacer le raisonnement par le calcul, car la réponse, positive, est assez évidente, puisqu'il suffit de reformuler chaque règle de déduction comme une règle de calcul, mais si l'on pouvait le remplacer par un algorithme, c'est-à-dire par un processus qui termine toujours et répond négativement quand la proposition n'est pas démontrable.

78-79 Le problème de l'arrêt (par argument diagonal)

Il s'agit d'une tentative de concevoir un algorithme *A* qui […] s'applique à deux objets *a* et *b*, où *a* est un ensemble de règles de calcul, et indique si la méthode formée des règles *a* termine ou non quand on l'applique à la valeur *b*. Appliquer *A* à *a* et *b* donnerait donc le résultat 1, si la méthode formée des règles *a* termine quand on l'applique à *b*, et 0 sinon.

Or […] Turing et, indépendamment, Church et Kleene ont construit en 1936 une démonstration par l'absurde qui consiste à montrer que l'hypothèse de [l'existence de l'algorithme *A*] a des conséquences contradictoires et, donc qu'elle est fausse. Tout d'abord, si un tel algorithme existait, il ne serait pas difficile de l'utiliser pour construire une méthode *B* qui, comme l'algorithme *A*, s'applique à deux objets *a* et *b*, teste si *a* est une méthode qui termine quand on l'applique à la valeur *b*, se lance dans un calcul qui ne termine pas si c'est le cas et termine dans le cas contraire. Si une telle méthode *B* existait, on pourrait l'utiliser pour construire une troisième méthode *C* qui s'appliquerait à un objet unique *a* et appliquerait *B* à *a* et *a*. On pourrait alors appliquer *C* à *C* ? Ce calcul se terminerait-il ou non ?

Par définition de *C*, appliquer *C* à C revient à appliquer *B* à *C* et *C*. Or la méthode *B* termine quand on l'applique à *C* et *C* si *C* ne se termine pas quand on l'appliquer à *C*. Donc, appliquer *C* à *C* donnerait un calcul qui termine s'il ne termine pas, ce qui est contradictoire.

83-84 La thèse de Church

préciser ce qu'[est] un algorithme et […] en proposer plusieurs définitions : les équations de Herbrand et Gödel, le lambda-calcul de Church, les machines de Turing, les fonctions récursives de Kleene, la réécriture… Ces définitions proposent chacune un langage dans lequel exprimer un algorithme : on dirait aujourd'hui que chacune définit un « langage de programmation ».

Ces définitions se sont révélées équivalentes *a posteriori* : si un algorithme peut être défini dans l'un de ces langages, on peut traduire cette définition dans n'importe quel autre. Cette équivalence des définitions est l'un des succès de la théorie de la calculabilité : elle est le signe que l'on a atteint un concept absolu de calcul, indépendamment des formes accidentelles que prendre tel ou tel langage d'expressions des algorithmes.

Une question n'a, cependant, pas manqué de se poser aux mathématiciens des années trente : cette notion de calcul est-elle « la » notion de calcul, ou est-il possible que, dans le futur, d'autres mathématiciens proposent d'autres langages, dans lesquels puissent s'exprimer davantage d'algorithmes ? La plupart des mathématiciens des années trente ont pensé que ce n'était pas le cas, donc que la notion de calcul définie par les machines de Turing, le lambda-calcul… était la bonne notion de calcul. Cette thèse est appelée la « thèse de Church » bien que, encore une fois, plusieurs mathématiciens, en particulier Turing, aient proposé des thèses similaires.

Commentaire : une question similaire mériterait à nos yeux d'être posée : la mathématique est-elle « la » voie vers la connaissance ? À noter que le problème de l'équivalence des différentes « mathématiques » n'est même pas encore résolu : quelle logique (classique, intuitionniste, linéaire, ludique, séquentielle…), quelle théorie (ensembles, catégories, fonctions, arithmétique…), quels axiomes (parties, remplacement, choix, grands cardinaux…).

106 PUISSANCE DU LAMBDA-CALCUL

La puissance calculatoire insoupçonnée du lambda-calcul vient […] du fait que rien n'interdit, dans ce langage, d'appliquer une fonction à elle-même.

113/115/119 TIERS EXCLU, CONSTRUCTIVISME, INTUITIONNISME

C'est […] le tiers exclu qui permet de construire des démonstrations d'existence qui ne donnent pas de témoin. C'est pour cela qu'on a décidé d'appeler « démonstration constructive » une démonstration qui n'utilise pas le tiers exclu.

[…] à cette querelle du tiers exclu se sont mêlées d'autres querelles. Par exemple, Brouwer défendait le point de vue selon lequel notre intuition des objets mathématiques est plus importante que la connaissance que nous en avons par la démonstration. De là vient le nom d' « intuitionnisme ». […]

La dernière étape pour réconcilier les mathématiques constructives et non constructives consistait à proposer une variante de la logique des prédicats qui comprenne deux locutions « il existe » et des règles de déduction qui expriment la signification de ces deux locutions. Une telle logique a été proposée par Gödel, en 1933, sous le nom de « traduction négative ». Les détails de cette logique sont moins importants que le fait qu'elle montre que les mathématiques constructives et non constructives peuvent coexister pacifiquement, contrairement à ce que pensaient aussi bien Brouwer que Hilbert.

124/126/127 ALGORITHMES, FONCTIONS & DÉMONSTRATIONS CONSTRUCTIVES

La notion d'algorithme trouve […] une nouvelle définition, plus abstraite : un algorithme est une fonction que l'on peut définir de manière constructive.

[…] Finalement, en fondant toues leurs mathématiques sur la notion d'algorithme, le Mésopotamiens avaient, sans le savoir, commencé par la notion la plus fondamentale. Ce sont les Grecs qui, en fondant les leurs sur la notion de démonstration, en ont donné une image déformée.

[…]

Pour conclure, le lien entre les notions de démonstration constructive et d'algorithme est, finalement, assez simple : les démonstrations constructives sont les algorithmes.

136-137 JUGEMENTS ANALYTIQUES & SYNTHÉTIQUES

La terminologie classique qui oppose les jugements analytiques aux jugements synthétiques laisse croire qu'il existe deux types de jugement, alors qu'il en existe trois : les jugements qui s'établissent par un calcul, ceux qui s'établissent par une démonstration et ceux qui demandent une interaction avec la nature. Tout le monde est d'accord sur le fait que les jugements mathématiques appartiennent à la deuxième catégorie, mais tout le monde ne donne pas le même nom à cette catégorie.

153 DÉMONSTRATIONS AUTOMATIQUES

quelles idées ont permis aux méthodes de démonstration automatique de progresser depuis les années cinquante ? L'une de ces idées est celle de transformer des axiomes en règles de calcul, donc de prendre de la distance par rapport à la logique des prédicats et à la méthode axiomatique. Si l'on avait conservé la conception axiomatique des mathématiques, on se serait condamné à concevoir des méthodes qui cherchent à démontrer la proposition « 2 + 2 = 4 » en convoquant potentiellement tous les axiomes des mathématiques, au lieu de simplement effectuer l'addition.

177 TAILLE DES ÉNONCÉS & DES PREUVES

On peut […] se demander s'il existe un lien entre la taille d'une proposition et la taille de ses démonstrations. À cette question, la théorie de la calculabilité apporte une réponse et cette réponse est malheureusement négative. Le théorème de Church a, en effet, comme conséquence l'existence de théorème dont l'énoncé est de longueur n et dont la plus courte démonstration a pour longueur $1000n$, ou même 2^n. Encore une fois, raisonnons par l'absurde et supposons que toutes les propositions démontrables aient une démonstration de longueur inférieure à 2^n, où n est la longueur de la proposition elle-même. Dans ce cas, il existerait un algorithme pour décider si une proposition a une démonstration ou non puisque les textes de taille inférieure à 2^n sont en nombre fini.

191/201 La mathématique instrumentée

L'entrée des mathématiques dans leur ère instrumentée incite […], non à accorder une confiance excessive dans les instruments utilisés, mais à restreindre prudemment la confiance, parfois exagérée, que nous avons en nous-mêmes : nous aussi, nous pouvons faire des erreurs.

[…] De la même manière que les livres de physique décrivent aujourd'hui des expériences que le lecteur peut, plus ou moins, refaire, les livres de mathématiques du futur évoqueront peut-être des calculs effectués à l'aide d'instruments, que le lecteur pourra refaire avec ses propres instruments s'il veut se convaincre de leur correction. Et ces lecteurs seront peut-être surpris quand des notes historiques leurs apprendront que, jusqu'à la fin du XX^{e} siècle, les mathématiciens n'utilisaient pas d'instruments et résolvaient tous les problèmes à mains nues.

197 En finir avec les axiomes ?

Les axiomes empoisonnent les mathématiques depuis Hilbert, sinon depuis Euclide. Cela amène à rêver d'une nouvelle logique dans laquelle une démonstration serait construite avec des règles de déduction et des règles de calcul, mais sans axiome. Le programme de Hilbert visait à s'affranchir des axiomes et des règles de déduction. Il était trop ambitieux et a échoué. Mais s'affranchir des axiomes tout en gardant les règles de déduction serait déjà un progrès important.