HAL open science

À propos de quelques démonstrations pas très convaincantes

Gilles Dowek

▶ To cite this version:

Gilles Dowek. À propos de quelques démonstrations pas très convaincantes. 2001. hal-04045747

HAL Id: hal-04045747
https://inria.hal.science/hal-04045747v1

Preprint submitted on 25 Mar 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

À propos de quelques démonstrations pas très convaincantes

Gilles Dowek *

28 mai 2001

Je remercie Thérèse Hardin, Jean-Baptiste Joinet, Claude Kirchner, César Muñoz et Benjamin Werner pour leurs remarques sur une version antérieure de ce manuscrit.

Il y a plusieurs manières de répondre à la question "Qu'est-ce qu'une démonstration mathématique ?". Une première consiste à donner une définition, à dire, par exemple, qu'une démonstration est une suite finie de propositions telle que chacune de ces propositions soit un axiome ou découle des précédentes par une règle de déduction. Une deuxième consiste à énoncer des propriétés qu'une chose doit vérifier pour être une démonstration, à dire, par exemple, qu'une démonstration doit être convaincante, explicative, que les détours qu'elle contient peuvent être éliminés, qu'elle doit être vérifiable avec tel ou tel outil, que sa recherche peut s'organiser de telle ou telle façon, ... Répondre de cette deuxième manière ne consiste pas à donner une définition, mais à énoncer des critères qui permettent d'évaluer diverses définitions possibles.

J'ai été amené à m'intéresser à cette question des critères d'évaluation d'une définition de la notion de démonstration, car j'ai participé, à la fin du siècle dernier, à la proposition d'une "nouvelle" définition de la notion de démonstration avec un formalisme qui s'appelle la *déduction modulo* [1]. Il était donc naturel de se demander si la définition que nous proposions était acceptable, c'est-à-dire si nos

*INRIA-Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France.
`Gilles.Dowek@inria.fr`, `logical.inria.fr/~dowek`.

1. G. Dowek, Th. Hardin and C. Kirchner, Theorem proving modulo, Rapport de Recherche 3400, Institut National de Recherche en Informatique et en Automatique (1998).

démonstrations vérifiaient les propriétés habituellement attendues des démonstrations mathématiques.

Cette interrogation n'est cependant pas propre à la déduction modulo, car ce formalisme n'a pas été créé *ex nihilo* : les idées sur lesquelles il se fonde étaient déjà présentes plus ou moins explicitement dans différents formalismes antérieurs, pour lesquels les mêmes questions se posent. Cependant, la simplicité de la déduction modulo fait que ces questions se posent peut-être là, avec davantage de clarté.

La déduction modulo

Dans la tradition hilbertienne, une démonstration est une suite d'étapes de raisonnement. L'idée de la déduction modulo est qu'une démonstration est une suite non seulement d'étapes de raisonnement mais aussi d'étapes de calcul. Démontrer, ce n'est pas uniquement raisonner, c'est raisonner et calculer.

Il est banal de remarquer que démontrer la proposition *non* $\exists xy \in \mathbb{N}\ x^2/y^2 = 2$ demande de construire un raisonnement, mais que démontrer la proposition $2 \times 2 = 4$ ne demande que d'effectuer une multiplication. Bien entendu, la proposition $2 \times 2 = 4$ peut, malgré tout, se démontrer dans un cadre hilbertien, par exemple dans l'arithmétique ou dans la théorie des ensembles. Mais dans cette démonstration, chaque étape de l'algorithme de la multiplication est simulée par une étape de raisonnement, typiquement en recourant aux "axiomes" de l'addition et de la multiplication. Ces axiomes ne sont qu'une reformulation des règles de calcul des algorithmes de l'addition et de la multiplication, mais dans cette reformulation, leur caractère opératoire a été oublié.

Dans un cadre hilbertien, une théorie est un ensemble d'axiomes. En déduction modulo, c'est un ensemble d'axiomes et de règles de calcul. On peut, par exemple, formuler l'arithmétique en déduction modulo avec des règles de calcul qui remplacent les habituels axiomes de l'addition et de la multiplication. Dans cette théorie, on peut démontrer la proposition "le nombre 4 est pair" $\exists x\ 2 \times x = 4$. La démonstration débute comme la démonstration hilbertienne : on donne le témoin, 2, et on se ramène à démontrer la proposition $2 \times 2 = 4$. Les deux démonstrations diffèrent alors. Dans un cadre hilbertien, on doit démontrer cette proposition en utilisant les axiomes de l'addition et de la multiplication. En déduction modulo, on calcule l'expression 2×2 et on obtient la proposition $4 = 4$ qui se démontre avec l'axiome d'identité $\forall x\ x = x$. Autrement dit, en déduction modulo, comme les règles de style traditionnelles de la rédaction mathématique l'imposent, les dé-

monstrations sont expurgées des fastidieux arguments calculatoires qui n'éclairent pas l'argumentation et que le lecteur peut reconstruire s'il le désire : les calculs s'effectuent sans laisser de trace dans les démonstrations.

En déduction modulo, comme on vient de le voir, il est possible, à chaque étape d'une démonstration, de transformer les propositions, en appliquant les règles de calcul. Les règles de déduction doivent donc être reformulées pour tenir compte de cette possibilité de calcul. Ainsi, le *modus ponens* ne se formule pas de la manière traditionnelle

$$\frac{A \Rightarrow B \quad A}{B}$$

mais il se formule de la manière suivante

$$\frac{C \quad A}{B} \text{ si } C \equiv (A \Rightarrow B)$$

La condition $C \equiv (A \Rightarrow B)$ signifie que les propositions C et $A \Rightarrow B$ doivent être équivalentes, c'est-à-dire ne doivent différer que par l'exécution d'un calcul. Typiquement, les propositions $2 \times 2 = 4$ et $4 = 4$ sont équivalentes. Cette relation d'équivalence doit être décidable, car c'est cela qui garantit qu'on supprime des démonstrations des étapes de calcul et non des étapes de raisonnement.

Une autre manière de dire les choses est qu'en déduction modulo, on ne raisonne pas directement avec des propositions mais avec des classes de propositions modulo la relation d'équivalence définie par les règles de calcul. Pour conserver le caractère syntaxique des démonstrations — c'est-à-dire pour qu'une démonstration reste une suite finie de symboles —, à chaque occurrence d'une classe dans une démonstration, on choisit l'un de ses éléments comme représentant.

Les origines de la déduction modulo

Je ne veux pas décrire trop en détails les motivations qui nous ont amenés, Th. Hardin, C. Kirchner et moi, à proposer et à étudier la déduction modulo. Puisque la déduction modulo met au premier plan la notion de calcul, il y a bien entendu des motivations à chercher du côté de l'informatique. En particulier, cette distinction entre raisonnement et calcul est essentielle quand on cherche à concevoir des programmes de recherche de démonstrations. Il est en effet important quand on se trouve dans la situation de devoir démontrer la proposition $2 \times 2 = 4$, de savoir simplement effectuer le calcul et non chercher une démonstration de cette proposition en utilisant potentiellement tous les axiomes des mathématiques.

Cette remarque, due à G. Plotkin [2] est à l'origine de nombreux travaux en démonstration automatique, centrés autour de la notion d'unification équationnelle. La déduction modulo a essentiellement été développée comme pendant logique de ces travaux.

Mais, la déduction modulo s'est également révélée un cadre unificateur pour étudier des problèmes de théorie de la démonstration comme les problèmes d'élimination des coupures : nous avons démontré, avec B. Werner, un théorème d'élimination des coupures relativement général, dans la tradition de W.W. Tait et J.-Y. Girard, dont plusieurs théorèmes connus sont des corollaires, plus ou moins immédiats [3]. Ce qui constitue *a posteriori* une autre motivation.

Enfin, la motivation *a posteriori*, peut-être la plus importante, est qu'une fois qu'on a formulé cette idée qu'une démonstration articule des étapes de raisonnement et des étapes de calcul, on s'aperçoit qu'elle était déjà présente, parfois explicitement dans certaines théories particulières. On peut au moins faire remonter cette idée aux premières formulations de la théorie des types de Russell, par exemple dans les *Principia Mathematica*. En effet, la substitution d'une variable dans la théorie des types n'est pas son simple remplacement par un terme, mais demande d'exécuter un algorithme assez complexe. La simplification de cet algorithme a été l'un des soucis majeurs des continuateurs de A.N. Whitehead et B. Russell. H.B. Curry, A. Church, L. Henkin et D. Prawitz, par exemple, ont montré qu'on pouvait se ramener a un algorithme de substitution plus simple, si on acceptait d'ajouter des axiomes ou des règles de déduction à la théorie : les axiomes de la logique combinatoire pour Curry [4], le schéma de conversion pour Church [5], le schéma de compréhension pour Henkin [6], les règles d'introduction et d'élimination du symbole λ pour Prawitz [7]. Ces axiomes sont ensuite devenus des règles de calcul, au moins dans le cas du schéma de conversion et dans celui des axiomes de la logique combinatoire. Dans certaines extensions de la logique du

2. G. Plotkin, Building-in equational theories, *Machine Intelligence*, 7 (1972), pp. 73-90.

3. G. Dowek and B. Werner, Proof normalization modulo, *Types for Proofs and Programs* 98, T. Altenkirch, W. Naraschewski, B. Rues (eds.), Lecture Notes in Computer Science 1657, Springer-Verlag (1999) pp. 62-77.

4. H.B. Curry, An analysis of the logical substitution, *American Journal of Mathematics*, LI (1929) pp. 263-384.

5. A. Church, A formulation of the simple theory of types, *The Journal of Symbolic Logic*, 5,1 (1940) pp. 56-68.

6. L. Henkin, Banishing the rule of substitution for functional variables, *The Journal of Symbolic Logic*, 18, 3 (1953) pp. 201-208.

7. D. Prawitz. *Natural deduction, a proof-theoretical study*, Almqvist & Wiksell (1965).

second ordre, comme l'*Arithmétique fonctionnelle du second ordre* [8] le remplacement des égaux par les égaux se fait également sans laisser de trace dans les démonstrations.

L'idée que l'application d'une règle de déduction puisse demander un certain calcul est aussi présente dans les formulations des règles de déduction adaptées à la recherche de démonstrations, comme la règle de résolution [9] dont l'application demande l'exécution de l'algorithme d'unification.

On peut aussi trouver les origines de la déduction modulo dans les travaux de N.G. De Bruijn, et en particulier dans le formalisme qu'il a proposé avec le système *Automath* [10]. Dans ce formalisme, en effet, le remplacement d'un symbole défini par le corps de sa définition se fait sans laisser de trace dans la démonstration. De plus, le terme défini pouvant être fonctionnel, il se pose, comme dans la théorie des types, le problème du statut de la conversion et le choix est que la conversion se fait également sans laisser de trace dans les démonstrations. De Bruijn a entrevu la possibilité d'étendre ce principe à d'autres opérations, pour lui tourner immédiatement le dos : il évoque la difficulté de démontrer formellement des propositions comme $2 \times 2 = 4$, et remarque qu'on pourrait se dispenser de les faire si on effectuait simplement la multiplication — ou si, dans le cadre d'un système informatisé, on laissait l'ordinateur l'effectuer —, mais que ce serait "contraire aux règles du jeu".

On peut aussi trouver les origines de la déduction modulo dans certaines formalisations des mathématiques constructives, et en particulier dans la théorie des types intuitionniste de P. Martin-Löf [11]. Suivant une tradition, due à L.E.J. Brouwer, A. Heyting et A. Kolmogorov, une démonstration constructive est un algorithme et, en particulier, une démonstration constructive d'existence est un algorithme qui calcule un témoin de cette existence, entre autres choses. Cela amène à définir une notion algorithmique de fonction et des règles de calcul pour ces fonctions. C'est cela qui donne naissance à la notion d'égalité définitionnelle et la notion de règle de réduction dans la théorie des types intuitionniste et dans des formalismes apparentés comme le Calcul des Constructions [12] et le Calcul des

8. J.L. Krivine and M. Parigot, Programming with proofs, *J. Inf. Process. Cybern. EIK* 26 (1990), pp. 149-167.

9. J.A. Robinson, A Machine-oriented logic based on the resolution principle, *Journal of the Association for Computing Machinery*, 12, 1 (1965), pp. 23-41.

10. R.P. Nederpelt, J.H. Geuvers and R.C. de Vrijer (eds.), *Selected papers on Automath*, Studies in Logic and the Foundations of Mathematics, 133, North-Holland (1994).

11. P. Martin-Löf, Intuitionistic type theory, *Bibliopolis* (1984).

12. Th. Coquand, G. Huet, The calculus of constructions, *Information and Computation*, 76

Constructions Inductives [13].

Enfin, une dernière motivation est que la déduction modulo peut apparaître comme la résurrection de la partie raisonnable du programme de Hilbert. Un des aspects de ce programme visait à abolir la notion hilbertienne de démonstration, suite d'étapes de raisonnement, et à la remplacer par une notion où une démonstration aurait été une suite d'étapes de calcul. Comme on le sait, un théorème démontré par Church en 1936, montre que cela n'est pas possible. Mais si le théorème de Church montre qu'on ne peut pas remplacer toutes les étapes de raisonnement par des étapes de calcul, il n'indique pas jusqu'où on peut aller dans cette direction. C'est typiquement le genre de question que permet de poser la déduction modulo.

Quand on exprime une théorie en déduction modulo, on cherche, si on le peut, à remplacer tous les axiomes par des règles de calcul, toute l'indécidabilité venant alors des règles de déduction. En remplaçant ainsi les axiomes par des règles de calcul on réalise une part du programme de Hilbert, qui visait à remplacer par des règles de calcul, non seulement les axiomes, mais aussi les règles de déduction.

La théorie intentionnelle des types simples peut se définir comme une théorie modulo sans axiome, mais l'axiome d'extensionnalité pose des difficultés. De même les *Fondations nouvelles* de W.V.O. Quine peuvent se définir comme une théorie modulo sans axiome, à condition d'abandonner, ici aussi, l'axiome d'extensionnalité. Une question centrale est naturellement de savoir si on peut faire la même chose pour la théorie des ensembles. Le principal problème, avec cette théorie, est celui de la décidabilité de la relation d'équivalence définie par les règles de calcul, qui est à ma connaissance, une question ouverte. De plus, ici aussi, se pose un problème avec l'extensionnalité. Cependant, des travaux récents de J.-L. Krivine et de G. Gonthier, qui étendent des travaux plus anciens de H. Friedman, montrent qu'on peut recoder la théorie des ensembles extentionnelle dans la théorie des ensembles intentionnelle. Il y a là une piste à explorer pour présenter la théorie des ensembles comme une théorie modulo.

La déduction modulo dans la vie quotidienne

Une manière plus concrète d'aborder cette question de la part du calcul dans les démonstrations mathématiques est de s'interroger sur le rôle qu'il joue dans les

(1988) pp. 95-120.

13. Ch. Paulin-Mohring. Inductive definitions in the system Coq - Rules and properties. M. Bezem and J.-F. Groote (eds.), *Typed Lambda Calculi and Applications*, Lecture Notes in Computer Science 664 (1993).

démonstrations que les mathématiciens construisent quotidiennement. Le calcul est présent sous plusieurs formes dans ces démonstrations.

Tout d'abord, on peut dire que tous les mathématiciens font des calculs dans leurs démonstrations même s'ils n'en ont pas toujours conscience, de même qu'ils utilisent les axiomes de la théorie des ensembles sans toujours être pleinement conscients de quel axiome est utilisé dans quelle démonstration. Par exemple, l'un des axiomes de la théorie des ensembles pose que si x et y sont deux objets, il existe un ensemble qui contient ces deux objets. Si on note $\{x, y\}$ cet ensemble, l'axiome se formule $z \in \{x, y\} \Leftrightarrow (z = x \textit{ ou } z = y)$. Dans certaines formulations de la théorie des ensembles en déduction modulo, la transformation de la proposition $z \in \{x, y\}$ en $z = x \textit{ ou } z = y$ se fait non à l'aide d'un axiome, mais à l'aide d'une règle de calcul. On n'a donc pas toujours pleinement conscience d'utiliser un axiome ou une règle de calcul quand on utilise la définition de la notion de paire, et pourtant on le fait. En théorie des ensembles, ce processus de calcul n'est pas absolument trivial, et en particulier, comme je l'ai déjà mentionné, la décidabilité de la relation d'équivalence définie par ces règles de calcul est à ma connaissance un problème ouvert.

Dans l'inventaire des algorithmes utilisés quotidiennement par les mathématiciens, on peut ensuite mentionner tous ceux utilisés pour dériver des fonctions construites à partir des fonctions élémentaires, pour en chercher des primitives, pour transformer des équations différentielles en des problèmes variationnels, ... Si des mathématiciens de nombreuses époques ont laissé leur nom à des algorithmes — l'algorithme d'Euclide, les algorithmes d'al Khwarizmi, la méthode de Cardan, le triangle de Pascal, la méthode de Newton, le pivot de Gauss, ... — , c'est sans doute qu'une de leurs préoccupations était de découvrir des solutions algorithmiques aux problèmes sur lesquels ils travaillaient et que ces algorithmes étaient ensuite utilisés pour résoudre d'autres problèmes. Les mathématiciens contemporains utilisent ces algorithmes à la main et parfois dans des systèmes de calcul formel.

Il y a ensuite certains domaines des mathématiques où les démonstrations font appel au calcul massif, en particulier dans les mathématiques développées pour les autres sciences et pour la technologie. On dit parfois des mathématiciens du *Courant Institute* qu'ils font des mathématiques sans démontrer de théorèmes. Il me semble que cette formulation n'est pas correcte, et qu'elle est contradictoire. Quand on établit que le plus court chemin pour parcourir tous les nœuds d'un graphe donné est celui-ci ou celui-là, quand on établit que les orbitales d'un atome donné ont telle ou telle forme, ou quand on établit que tel ou tel grand nombre est premier ou non, on fait une démonstration. On peut dire que cette dé-

monstration, du fait de sa faible généralité, n'est pas noble ou qu'elle n'est pas intéressante ou qu'elle n'est pas belle ou ce qu'on voudra, mais on ne peut pas nier, me semble-t-il, le fait que ce soit une démonstration et qu'elle démontre un théorème. Les démonstrations de ce type, en particulier celles qui portent sur des objets particuliers de grande taille, demandent souvent une quantité importante de calculs.

Enfin, on peut s'interroger sur le rôle du calcul massif dans les démonstrations de théorèmes généraux, fermant des conjectures anciennes. Ici, il faut sans doute être plus prudent. Par exemple, il ne semble pas que la démonstration du théorème de Wiles ait demandé beaucoup de force de calcul. Cependant, il y a un exemple, célèbre pour avoir demandé une force de calcul importante, c'est le théorème des quatre couleurs [14], dont la démonstration procède à une étude de cas qui n'a pu être réalisée qu'après qu'on a eu des ordinateurs suffisamment puissants. Une question importante est de savoir si on peut formuler cette démonstration en déduction modulo, ou dans un formalisme apparenté, de façon à ce que cette étude de cas soit l'exécution d'un calcul. Des travaux en cours de V. Danos, G. Gonthier et B. Werner cherchent à formaliser cette démonstration dans le Calcul des Constructions Inductives.

Va-t-on finir par trouver un jour une démonstration du théorème des quatre couleurs qui évite ce recours au calcul massif, ou cette démonstration est-elle destinée à rester telle quelle dans les mathématiques ? Et dans cette seconde hypothèse, est-elle destinée à rester singulière, ou les années à venir vont-elles voir se multiplier les démonstrations qui font appel au calcul massif ? Il est difficile de donner, à ces questions, des réponses autres que spéculatives. Cependant, on peut noter que depuis quelques mois, la démonstration du théorème des quatre couleurs n'est déjà plus la seule de ce type. En août 1998, T. Hales a annoncé qu'il avait démontré la conjecture de Kepler sur la façon optimale d'empiler des sphères dans l'espace [15]. Sa démonstration, comme celle du théorème des quatre couleurs repose sur une étude de plusieurs centaines de cas. En fait, dès 1953, F. Tóth avait réduit la conjecture de Kepler à un calcul gigantesque, et donc infaisable en pratique, mais fini. Comme ces deux théorèmes appartiennent à la même branche des mathématiques, il n'est pas absurde de penser que le recours au calcul massif soit en train de devenir l'une des méthodes des mathématiques discrètes.

14. K. Appel and W. Haken, Every planar map is four colorable. Part I. Discharging, *Illinois J. Math.* 21 (1977), 429-490. K. Appel, W. Haken and J. Koch, Every planar map is four colorable. Part II. Reducibility, *Illinois J. Math.* 21 (1977), 491-567.

15. Voir `www.math.lsa.umich.edu/~hales/kepler.html`, et aussi J.-P. Delahaye, La conjecture de Kepler est-elle résolue ?, *Pour la Science (février 2001).*

L'acte de lecture

Une démonstration en déduction modulo est plus courte qu'une démonstration hilbertienne, puisqu'elle est expurgée des arguments calculatoires que le lecteur peut reconstruire. La contrepartie est qu'en lisant une démonstration, le lecteur qui veut se convaincre de sa correction doit reconstruire ces arguments. Pour se convaincre de la correction d'une démonstration modulo, le lecteur ne peut pas se contenter d'une simple vérification élémentaire à chaque étape, comme dans le cas d'une démonstration hilbertienne, mais il doit fournir un certain travail. Ce travail consiste à vérifier que des propositions sont équivalentes modulo les règles de calcul. Dans certaines formulations de la déduction modulo, ce travail peut même consister à vérifier qu'une proposition a une instance équivalente à une autre proposition, c'est ce qu'on appelle le problème du *filtrage équationnel*.

L'idée que le lecteur d'un texte ne se contente pas de le recevoir passivement, mais en fait quelque chose, est devenu une banalité en analyse littéraire. Cependant, il me semble que c'est une banalité plus grande encore pour qui a déjà compris un texte mathématique, fût-il élémentaire. Il n'y a donc rien de choquant à ce que la vérification d'une démonstration modulo sollicite le lecteur. Ici encore, la déduction modulo semble plus proche de la pratique mathématique quotidienne que la déduction hilbertienne.

On peut cependant remarquer que même la lecture d'une démonstration hilbertienne n'est pas un acte totalement dénué de coût, puisqu'il faut toujours faire au moins l'effort de l'analyse lexicale et syntaxique du texte. Cet effort est sans doute assez important car le langage courant et le langage mathématique disposent de nombreuses stratégies pour l'alléger, en raccourcissant les messages. Dans le langage mathématique, on dispose de la possibilité de lier des variables par le mécanisme des définitions. Par exemple, au lieu de répéter la formule "un ensemble muni d'une loi interne associative possédant un élément neutre et tel que tout élément ait un symétrique" on peut commencer un texte mathématique par une définition de la notion de groupe et utiliser ce terme ensuite. On peut de même décider de donner un nom au nombre $(1+\sqrt{\pi})/(1-\sqrt{\pi})$ si cette expression revient souvent dans le texte.

Cette possibilité est très difficile à utiliser dans le langage courant. Sauf dans des cas très rares — par exemple dans certains textes juridiques, mais est-ce encore le langage courant ? —, on ne commence pas un roman par la phrase : "Dans ce roman, j'appellerai X le facteur qui dépose le courrier dans ma boîte aux lettres tous les matins. Ce matin là ..." : on utilise l'expression complète à sa première occurrence et on utilise ensuite des anaphores. Ce mécanisme, contrairement à

celui utilisé par le langage mathématique, introduit de nombreuses ambiguïtés que le lecteur doit résoudre au moment de la lecture. Cette résolution demande des connaissances et des raisonnements souvent assez complexes, comme dans l'exemple des groupes nominaux "le grand-père de Max qui entre en sixième" et "le petit-fils de Max qui entre en sixième". Cependant, le fait que ces constructions existent dans le langage semble indiquer que l'économie en analyse lexicale et syntaxique due à l'introduction d'anaphores est supérieure au coût en raisonnement et calcul de la résolution des ambiguïtés. Cette intuition est corroborée par certaines observations faites en informatique : on gagne souvent en supprimant des informations redondantes d'un texte et en les reconstruisant juste après l'analyse syntaxique.

On peut donc penser, de même, que vérifier une démonstration modulo est dans certains cas plus rapide que vérifier une démonstration hilbertienne, car le coût en calcul est compensé par l'économie en analyse lexicale et syntaxique. Un exemple typique est celui où on veut vérifier qu'un nombre entier est composé. Il est plus facile de lire deux facteurs et de vérifier soi-même que leur produit est bien le nombre attendu, que de lire la multiplication et de vérifier, étape par étape, qu'elle est correcte.

La vérification et la conviction

Dans d'autres cas, en revanche, le coût de la vérification d'une démonstration modulo est certainement supérieur au coût de la vérification d'une démonstration hilbertienne. Si on doit vérifier, par exemple, qu'un nombre est composé, il est, sans aucun doute, plus facile de vérifier une démonstration qui indique explicitement deux facteurs, ou au moins un facteur, que d'appliquer un algorithme de factorisation.

Quand l'effort demandé au lecteur devient trop important, celui-ci peut se trouver en pratique dans l'impossibilité de vérifier la correction d'une démonstration, et on peut se demander, de ce fait, si le terme "démonstration" reste approprié pour désigner un tel argument [16].

Prenons un exemple. Un théorème démontré en 1936 par A. Tarski montre que la géométrie élémentaire est décidable, c'est-à-dire qu'il y a un algorithme qui prend en argument une proposition et indique si elle est démontrable à partir des axiomes de la géométrie ou non. De ce fait, la relation d'équivalence sur les

16. Je dois à P. Martin-Löf d'avoir attiré mon attention sur ce point.

propositions de la géométrie qui relie deux propositions si celles-ci sont toutes les deux démontrables ou toutes les deux non démontrables est décidable. Cette relation d'équivalence permet de construire une présentation de la géométrie en déduction modulo dans laquelle les théorèmes sont tous équivalents entre eux.

Dans cette formulation de la géométrie, pour démontrer n'importe quel théorème, par exemple que les médiatrices d'un triangle sont concourantes, il suffit simplement d'invoquer n'importe quel axiome, par exemple celui selon lequel par deux points il passe une et une seule droite. Si le lecteur veut vérifier cette démonstration, il lui suffit de vérifier que les deux propositions "les médiatrices d'un triangle sont concourantes" et "par deux points il passe une et une seule droite" sont équivalentes. Pour cela il suffit d'appliquer l'algorithme de Tarski à ces deux propositions et de vérifier qu'il répond la même chose.

Tous ceux qui se souviennent de l'impression que cette démonstration a produit sur eux la première fois qu'ils l'ont comprise se demandent certainement si en la vidant de toute sa substance, on n'a pas poussé le souci de concision un peu trop loin. Cette objection prend tout son sens quand on sait que l'algorithme de Tarski est particulièrement complexe et fastidieux, et que s'il est sans doute possible de l'appliquer à ces propositions, il est assez facile de donner des exemples de propositions qui ont des démonstrations hilbertiennes assez courtes, mais qui défient les ordinateurs les plus puissants quand on leur applique l'algorithme de Tarski.

Autrement dit, l'algorithme de Tarski permet en principe de vérifier les démonstrations dans cette formulation de la géométrie en déduction modulo, mais il ne permet pas de les vérifier en pratique. Ce qui amène la question suivante : pour garder une notion acceptable de démonstration, doit on, dans une théorie modulo, se limiter à des règles de calcul qui permettent une vérification des démonstrations en pratique, ou est-il suffisant de se limiter à des règles qui permettent une vérification en principe ?

Fort heureusement, cette opposition entre possibilité en pratique et possibilité en principe a déjà été étudiée assez en détail, car la notion de possibilité en principe joue un rôle important dans les bases philosophiques de la logique intuitionniste. Je m'appuierai ici en particulier sur l'article de Ch. Parsons *What can we do "in principle" ?* [17]. Dans cet article, Parsons analyse, entre autres choses, le rôle joué par cette notion de possibilité en principe dans la théorie de la calculabilité. Il montre qu'elle s'introduit dans l'idée que si on peut en pratique exécuter une action une fois, alors on peut en principe l'exécuter un nombre quelconque

17. M.L. Dalla Chiara et al. (eds.), *Logic and Scientific Methods*, Kluwer (1997), pp. 335-354.

de fois pourvu que ce nombre soit fini. C'est cette idée que la finitude suffise qui définit la calculabilité en principe. En suivant cette idée, puisque je peux ajouter, soustraire, multiplier ou diviser deux nombres compris entre 0 et 9, je peux répéter ces opérations un nombre arbitraire de fois, et donc tester la primalité d'un nombre d'un million de chiffres, puisqu'une méthode pour tester la primalité d'un nombre entier consiste à faire des divisions successives et que la division dans le système décimal se ramène à des opérations sur les chiffres. Le fait que le nombre d'opérations soit fini suffit ici et le fait qu'il ne me reste que 2 713 953 600 secondes à vivre — en faisant l'hypothèse que je vive cent vingt ans — n'importe pas.

Parsons remarque que cette idéalisation de la notion de possibilité est omniprésente en mathématiques. Par exemple, la notion de droite de la géométrie d'Euclide repose sur la possibilité en principe de prolonger un segment à l'infini. Si on pense, en effet, qu'on ne peut pas prolonger un segment au delà de la taille de sa règle ou de la taille de l'univers, alors une droite a beaucoup de parallèles qui passent par un même point [18].

Parsons défend la thèse que cette notion de possibilité en principe — très différente de la modalité commune de possibilité — est une notion tout à fait sensée, mais qu'il faut pour la construire déjà disposer de notions mathématiques comme celle de nombre entier, et qu'il y a de ce fait, une forme de circularité à l'utiliser dans la définition même de la notion de vérité mathématique, comme le font les intuitionnistes. Autrement dit, il n'y a pas de problème à utiliser cette idéalisation de la notion de possibilité au sein d'une théorie mathématique, comme la géométrie ou la théorie des fonctions calculables — c'est une banalité de remarquer que les objets mathématiques sont des idéalisations —, mais il faut être plus prudent quand on veut proposer une définition de la notion de vérité mathématique. On pourra remarquer que si la critique de Parsons vise les bases philosophiques de la logique intuitionniste, elle s'applique également, telle quelle, à la déduction modulo.

Pour tenter de répondre à l'argument de Parsons, on peut commencer par se demander si cette notion de possibilité en principe n'est utilisée que par la logique intuitionniste, et accessoirement par la déduction modulo, ou si elle apparaît à d'autres endroits de la logique, et en particulier de la partie de la logique dont l'objet est de définir la notion de vérité mathématique. Je vais, bien entendu, tenter de montrer que cette notion de possibilité en principe est aussi à la base de la

18. Sur la naissance de cette notion d'espace illimité, voir, par exemple, M. Serres, *Les Origines de la géométrie*, Flammarion (1993).

notion hilbertienne de démonstration.

Pour cela, je vais commencer par concéder qu'il n'est pas possible en pratique de vérifier la primalité d'un nombre d'un million de chiffres, et donc qu'il est déraisonnable de demander au lecteur de faire un tel calcul lors de la vérification d'une démonstration modulo. On va appeler n le nombre d'étapes de ce calcul.

Si on pense qu'il est déraisonnable de demander au lecteur d'effectuer un calcul de n étapes ou plus, on doit admettre également qu'il est déraisonnable de lui demander de lire une démonstration hilbertienne de n étapes ou plus, par exemple une démonstration modulo invérifiable reformulée dans un cadre hilbertien en explicitant les calculs. Ainsi, si on se donne deux axiomes

$$0 \in E$$

et

$$\forall x \, (x \in E \Rightarrow x + 1 \in E)$$

mais naturellement pas le principe de récurrence, il est impossible de démontrer que le nombre n, ni aucun nombre au delà, appartient à l'ensemble E, car toutes les démonstrations d'une telle proposition utilisent le second axiome n fois ou plus. Il n'y a donc qu'un nombre fini de nombres dont on puisse démontrer l'appartenance à E en pratique et on peut appeler m le plus grand de ces nombres. Il est donc possible de démontrer la proposition $m \in E$, et aussi la proposition $m \in E \Rightarrow m + 1 \in E$, mais il n'est pas possible de démontrer $m + 1 \in E$. Il est devenu impossible d'appliquer le *modus ponens* à ces deux propositions, car on a déjà épuisé toutes ses forces à les démontrer. Si on limite la possibilité de raisonner jusqu'à ce que le Soleil s'éteigne ou quelqu'autre événement apocalyptique qu'il est d'usage d'invoquer dans un tel contexte, cela signifie que quelques fractions de seconde avant l'extinction du Soleil, on aura démontré les propositions $m \in E$ et $m \in E \Rightarrow m + 1 \in E$, mais qu'on n'aura pas le temps de conclure que $m + 1 \in E$. Ce phénomène n'est pas propre à cette théorie. On peut montrer, comme un corollaire du théorème de Church, que dans toute théorie axiomatique cohérente qui contient l'arithmétique, il y a des propositions courtes qui ont des démonstrations longues, c'est-à-dire que la taille de la plus courte démonstration d'une proposition ne peut pas être bornée par l'exponentielle de la taille de la proposition — ni par aucune autre fonction calculable.

Cet exemple montre que la notion même de règle de déduction suppose la possibilité en principe d'appliquer une règle un nombre quelconque de fois, pourvu que ce nombre soit fini. Ici aussi, le principe est que la finitude suffise. Dès lors qu'on admet ce principe d'utilisation un nombre quelconque de fois des règles de

déduction, pourvu que ce nombre soit fini, il est difficile de refuser ce même principe pour les règles de calcul. Autrement dit, la notion hilbertienne de démonstration est tout autant une idéalisation de la notion pratique de démonstration que la notion mathématique d'algorithme est une idéalisation de la notion pratique d'algorithme. Et la notion même de déduction se trouve être la cible des critiques de Parsons.

Il est peut-être possible de donner une définition de la notion de vérité mathématique qui évite cette idéalisation des possibilités du lecteur, qui consiste à penser que ce qu'il est capable de faire une fois, il est capable de le faire un nombre quelconque de fois pourvu que ce nombre soit fini. Mais il me paraît inévitable dans ce cas, quelque soit l'approche choisie, qu'il y ait un nombre m tel que les propositions $m \in E$ et $m \in E \Rightarrow m + 1 \in E$ soient vraies selon cette définition, mais pas la proposition $m + 1 \in E$, ce qui amène à distordre la signification des symboles logiques, comme l'implication, d'une manière qui me paraît inacceptable. C'est pour cela qu'au programme visant à briser la circularité observée par Parsons en évitant cette notion de possibilité en principe, il me paraît plus raisonnable de substituer celui de donner une définition de cette notion qui évite le recours à une notion mathématique, comme celle de nombre entier.

Cela amène à penser que dans la définition d'une démonstration en déduction modulo, comme en déduction hilbertienne, c'est la condition de vérifiabilité en principe, et non en pratique, qui est importante.

Cela signifie-t-il pour autant qu'il soit souhaitable d'utiliser la présentation de la géométrie en déduction modulo décrite ci-dessus ? Non, bien entendu. Pas plus qu'il n'est souhaitable d'utiliser une présentation de la géométrie comme une théorie hilbertienne dans laquelle tous les théorèmes sont des axiomes, bien que ce soit possible, la seule contrainte imposée à une théorie axiomatique étant celle de la décidabilité de l'ensemble des axiomes. Pas plus, pour prendre un exemple plus simple encore, qu'il n'est souhaitable de donner une démonstration de mille pages d'un théorème qu'on sait démontrer en quelques lignes.

Mais cette exigence d'intelligibilité, pour importante qu'elle soit, est indépendante de la définition de la notion de vérité mathématique. Donner une démonstration de mille pages d'un théorème qu'on sait démontrer en quelques lignes, c'est mal, mais ce n'est pas faux. Cette exigence d'intelligibilité est, si on veut, davantage une question de morale que de logique. Même les démonstrations excessivement longues et fastidieuses sont des démonstrations, et leur refuser ce statut amène à distordre la signification des symboles logiques d'une manière inacceptable.

Cela amène donc à distinguer les arguments qui établissent qu'une proposition

est vraie et ceux qui convainquent qu'une proposition est vraie. La validité des arguments du premier type est régie exclusivement par les règles logiques qui définissent la notion de vérité. Celle des arguments du second type peut dépendre de la personne à laquelle on s'adresse, et en particulier de son endurance à la lecture et de ses facultés de calcul, ainsi sans doute que de ses connaissances.

Les démonstrations hilbertiennes courtes sont des arguments convaincants. C'est pour cela qu'on a l'habitude de confondre le fait d'établir et de convaincre qu'une proposition est vraie. Mais ces deux types d'arguments se révèlent finalement assez différents, et ils seront sans doute amenés à se séparer davantage dans le futur.

L'explication

Une autre propriété des démonstrations qui se trouve mise en péril avec la déduction modulo est leur caractère explicatif. La démonstration hilbertienne du théorème des médiatrices, par exemple, ne se contente pas de dire que les médiatrices d'un triangle sont concourantes, il dit aussi pourquoi elles le sont. Une critique qu'on fait souvent aux démonstrations massivement calculatoires est que si elles disent qu'un théorème est vrai, elles ne donnent pas la raison pour laquelle il est vrai.

Cet argument est parfois invoqué à propos des démonstrations de géométrie obtenues avec un système de calcul formel, qui effectuent souvent des opérations sur des polynômes démesurés qui produisent miraculeusement le polynôme nul *in fine*. Il est également invoqué à propos de la démonstration du théorème des quatre couleurs, qui procède à une analyse de plusieurs centaines de cas, qui donnent tous miraculeusement le même résultat. Ici aussi, cela peut amener certains à dénier le statut de "démonstration" à ces démonstrations. Examinons quelques uns des arguments qui sont invoqués pour dire que ces démonstrations ne sont pas explicatives.

Passons vite sur le premier argument qui est qu'une telle démonstration ne peut pas s'enseigner, ou plus précisément que l'enseigner n'apprend rien aux étudiants qui ne peuvent pas réutiliser les mêmes idées dans une autre démonstration. S'il est clair, en effet, qu'écrire des polynômes formés de milliers de monômes au tableau ou dans un livre de cours est inutile, il est clair également que savoir comment utiliser un outil pour tester l'appartenance d'un polynôme à un idéal est une forme de connaissance réutilisable.

Un argument plus sérieux, souvent invoqué à propos de la démonstration du

théorème des quatre couleurs, est qu'il est impossible que toutes les cartes soient coloriables par coïncidence ou par miracle, c'est-à-dire qu'elles soient toutes coloriables pour une raison différente. Une démonstration explicative devrait montrer la raison commune que tous ces cartes ont d'être coloriables, or la démonstration qu'on connaît ne le fait pas puisqu'en énumérant des centaines de cartes et en les vérifiant une à une, elle construit des centaines de raisons différentes les unes des autres.

Cet argument met en évidence un lien entre la notion d'explication et celle de quantification universelle : ce qui rend la démonstration susceptible d'être explicative ou non, c'est la présence de la quantification universelle — "toutes les cartes", "tous les triangles", ... — et une explication est la réduction d'un ensemble infini de raisons particulières à une raison générale unique. Cela permet en particulier de comprendre pourquoi on ne cherche pas à expliquer une proposition sans quantificateur universel. Pourquoi deux et deux font-ils quatre et non cinq ? Parce que c'est ainsi. Il n'y a rien à expliquer. En revanche pourquoi les médiatrices de tous les triangles sont-elles concourantes ? Voilà une question bien posée. Cela permet également de comprendre pourquoi on est plus réticent à accepter une démonstration calculatoire d'un théorème général comme le théorème des quatre couleurs ou le théorème de Morley que le résultat d'une opération arithmétique effectuée avec une calculatrice.

Le problème est que si on pousse cette exigence d'explication trop loin, on est amené à rejeter certaines démonstrations traditionnelles, comme celle qui montre que le carré d'un nombre entier relatif est toujours positif. La manière traditionnelle de faire cette démonstration consiste à considérer deux cas, selon que le nombre est positif ou négatif. Mais avec ce raisonnement par cas, on donne deux raisons différentes, selon le signe du nombre. On renonce donc à donner une raison unique, c'est-à-dire à donner une explication. On se contente de remarquer que dans un cas comme dans l'autre, le résultat est vrai, sans montrer la force impérieuse à laquelle tous les nombres obéissent, quelque soit leur signe. De même, pour démontrer que $sin(n\pi)$ est toujours égal à 0, on fait une démonstration par récurrence en utilisant la périodicité de la fonction sinus, mais comme la période est 2π et non π, on doit distinguer deux cas selon la parité de n. Également, plusieurs démonstrations en théorie des corps utilisent le fait que 0 est différent de 2, et bien souvent, on doit vérifier le cas de $\mathbb{Z}/2\mathbb{Z}$ indépendamment, et selon les théorèmes, ce corps vérifie ou ne vérifie pas la propriété qu'on cherche à démontrer. Plus généralement, les démonstrations par cas sont fréquentes en mathématiques, et on n'a pas l'habitude de leur dénier le statut d'explication : démontrer une proposition universelle ne revient pas à réduire un ensemble infini de raisons

particulières à une raison générale unique, mais à un nombre fini de raisons. De ce fait, pourquoi dénier le statut d'explication à la démonstration du théorème des quatre couleurs, qui elle aussi ramène une infinité de raisons à un nombre fini ?

Il reste possible de défendre l'idée qu'une démonstration qui procède à l'analyse de deux ou trois cas est une explication, alors qu'une démonstration qui procède à l'analyse d'une centaine de cas n'en est pas une. Cela amène à discuter de toutes les situations allant de quatre à quatre vingt dix neuf cas, pour s'apercevoir que six convient à certains, mais que cinq est déjà trop pour d'autres. En tentant d'expliquer pourquoi le basculement se fait ici ou là, on invoquerait des arguments selon lesquels on peut écrire, lire, se souvenir d'une démonstration qui distingue deux ou trois cas, mais pas d'une démonstration qui en distingue une centaine, ce qui amènerait, une fois de plus, à poser des contraintes liées à notre capacité de lecture et de mémorisation.

J'ai bien peur qu'il faille se résoudre à admettre que la frontière entre ce qui est une explication et ce qui n'en est pas n'est pas très bien définie, et que le mieux qu'on puisse faire est de dire qu'une démonstration est plus explicative qu'une autre, et que, par exemple, la récente démonstration du théorème des quatre couleurs qui demande l'analyse de 633 cas [19] est plus explicative que la démonstration originale qui en demandait l'analyse de 1476, même si on peut encore rêver de démonstrations plus explicatives.

On peut illustrer cette idée de progressivité dans l'explicativité par l'une des nombreuses curiosités mathématiques attribuées à Lewis Caroll. Il s'agit de la multiplication $12345679 \times 36 = 444444444$. D'un certain point de vue, comme on l'a vu tout à l'heure, il n'y a rien de plus à expliquer dans cette proposition que dans n'importe quelle autre multiplication. Le fait que dans la multiplication $15974312 \times 36 = 575075232$, le résultat se termine par un 2 est peut-être expliqué par le fait que le dernier chiffre du produit des unités des deux facteurs soit également un 2, mais épeler ainsi l'algorithme de la multiplication pour expliquer chaque chiffre n'apporte rien. S'il y a quelque chose à expliquer dans le cas de la multiplication de Lewis Caroll, c'est parce qu'il y une régularité, c'est-à-dire qu'on peut énoncer le résultat sous une forme universelle : tous les chiffres du résultat sont des 4 et — presque — tous les chiffres du premier des facteurs sont les chiffres dans l'ordre croissant, car il y a manifestement un problème avec le 8. Nous sommes vraisemblablement tous d'accord pour dire qu'on éclaire un peu

19. N. Robertson, D.P. Sanders, P.D. Seymour and R. Thomas, The four colour theorem, *J. Combin. Theory* Ser. B. 70 (1997), 2-44.
Voir aussi `http://www.math.gatech.edu/~thomas/FC/fourcolor.html`.

le mystère quand on élimine le 4 du problème en se ramenant à la proposition $12345679 \times 9 = 111111111$. Le mystère s'éclaire un peu parce qu'on peut expliquer pourquoi le second facteur est 36 : c'est parce que 36 est le produit de 4 et de 9 et que 4 est le chiffre répété dans le résultat. De manière équivalente, on peut expliquer pourquoi le chiffre répété dans le résultat est un 4 : c'est parce que 4 est le quotient de 36 par 9. On peut maintenant reformuler la proposition comme le fait que la division de 111111111 par 9 produit les chiffres dans l'ordre croissant. On peut expliquer cela par une démonstration par récurrence, en montrant simultanément que la suite des restes dans cette division est également la suite des chiffres dans l'ordre croissant : quand on a le reste n et qu'on descend le 1 on obtient $10n + 1$ soit, $9n + (n + 1)$. Le chiffre posé suivant est donc n et le reste suivant $n + 1$. C.Q.F.D. Naturellement, il faut une autre hypothèse pour que cela marche : il faut que $n + 1$ soit inférieur à 9. C'est pour cela qu'à la fin du calcul le chiffre posé est 9 et non 8 et le reste 0 et non 9, ce qui permet de s'arrêter ici si on a prévu le bon nombre de 1.

Cette explication est plus satisfaisante que l'opération, et c'est parce que cette explication existe que Lewis Caroll s'amuse à taquiner notre curiosité. Le désir que nous avons de trouver une explication, c'est-à-dire une raison commune à la présence des neuf quatre montre notre soif d'uniformité et notre peu de goût pour les cas particuliers. Néanmoins comme on l'a vu, il y a un spectre d'arguments plus ou moins explicatifs, dont le dernier reste imparfait, à cause du raisonnement par cas qui amène à distinguer le cas du 8. Il est donc très difficile dans un exemple comme celui-ci de tracer une frontière très nette entre ce qui est une explication et ce qui n'en est pas une.

De plus, même si tout le monde préfère la démonstration la plus explicative, il ne viendrait à l'idée de personne de dire que cette démonstration plus explicative que l'opération est impérative pour établir que cette proposition est vraie. En particulier parce qu'une explication similaire n'existe pas pour la multiplication $15974312 \times 36 = 575075232$.

De même, bien que les démonstrations de Ch. Hermite et de F. Lindeman de la transcendance de e et π paraissent très *ad hoc*, ce que je ressens comme tout le monde, mais que j'ai du mal à formuler précisément, et bien que tout le monde souhaiterait découvrir des démonstrations plus explicatives, personne ne conteste le fait que e et π soient transcendants, ni que ces arguments soient des démonstrations.

Je voudrais donc suggérer que l'explicativité, non plus, n'a rien a voir avec la notion de démonstration, même si, comme tout le monde, je préfère les démonstrations les plus explicatives.

Les outils

Après cette première partie qui concernait les particularités de la définition de la notion de démonstration en déduction modulo et la distance prise par rapport aux notions de conviction et d'explication, je voudrais en venir à la seconde partie de cet exposé qui concerne l'utilisation d'outils, et en particulier d'ordinateurs, en mathématiques. La vérification d'une démonstration modulo demande, en effet, parfois des calculs pénibles que seul un ordinateur peut effectuer. Il est donc parfois nécessaire, pour "lire" ces démonstrations d'utiliser un outil.

On peut raisonnablement dire que jusqu'au milieu du siècle dernier, les mathématiciens n'utilisaient pas d'autres outils que du papier et des crayons, quoiqu'il ne faille pas négliger l'importance de la règle et du compas, par exemple, mais ce n'est pas le propos ici. Cette situation des mathématiques était assez singulière : l'astronomie, la biologie ou la physique des particules utilisent des lunettes, des microscopes ou des chambres à bulles depuis bien longtemps.

D'un certain point de vue, il n'y a pas de différence radicale entre le fait d'utiliser un outil et de ne pas en utiliser. L'observation des satellites de Jupiter avec la lunette de Galilée a beaucoup de points communs avec l'observation de la Lune à l'œil nu. La vérification d'une démonstration modulo avec un ordinateur a également beaucoup de points communs avec la vérification d'une démonstration hilbertienne "à l'œil nu". Le changement que constitue l'introduction d'un outil est davantage un changement quantitatif que qualitatif : la lunette de Galilée permet simplement d'observer davantage de choses que l'œil nu, mais ce simple changement quantitatif a, malgré tout, été à l'origine de la révolution que l'on sait.

Les lunettes, les microscopes, les chambres à bulles sont des outils d'observation qui prolongent les capacités de nos cinq sens, en fait surtout de la vue. Nous n'aurions pas besoin de lunette si notre œil était capable de distinguer, à cette distance, des objets aussi petits que les satellites de Jupiter. Le fait que nos capacités sensorielles soient sollicitées dans la pratique des sciences du monde physique, avec ou sans instruments, n'est pas surprenant, car le but de ces sciences est de décrire une réalité extérieure, ou au moins la manière dont cette réalité nous apparaît à travers un certain nombre de phénomènes. Il n'y a aucune nécessité pour que les planètes décrivent des ellipses autour du Soleil. Il n'y a rien de contradictoire à imaginer que les forces de gravitation au lieu d'être en $1/r^2$ suivent une autre loi et que les orbites des planètes aient une autre forme géométrique. Pour proposer la théorie selon laquelle ces orbites sont des ellipses et que les forces de gravitation sont en $1/r^2$, J. Kepler et I. Newton se sont appuyés sur des observations du mouvement de ces planètes, en particulier sur les milliers d'observations

faites par T. Brahé et pour faire ces observations T. Brahé a utilisé des instruments. Même quand un phénomène du monde physique est nécessaire — certains avancent, par exemple, que la forme hélicoïdale de l'ADN est nécessaire car c'est la seule qui permet sa réplication —, il est souvent plus facile d'établir un fait expérimentalement que d'établir sa nécessité *a priori*. De plus la nécessité de la forme hélicoïdale de l'ADN, pour continuer sur cet exemple, est toute relative, car il n'y a aucune nécessité à ce que l'ADN se réplique, ni même que quoi que ce soit se réplique dans le monde physique.

L'utilisation d'outils dans les sciences du monde physique est donc une conséquence de la nécessité d'observer les phénomènes du monde physique dans ces sciences, elle-même conséquence de la contingence des lois du monde physique.

En suivant cette analyse, on comprend pourquoi les sciences du monde physique ont recours à l'expérimentation et à l'instrumentation. Mais pourquoi est-ce également le cas des mathématiques ? L'observation du monde physique ne devrait être ni nécessaire ni suffisante pour établir la vérité en mathématiques, car celle-ci est purement analytique et elle n'est donc pas relative au monde physique. On constate, pourtant, que certains outils du monde physique, comme des ordinateurs, peuvent être utilisés pour établir la vérité mathématique de certaines propositions. On peut appeler "expériences mathématiques" ces manipulations et observations d'objets du monde physique, qui permettent d'établir des vérités mathématiques.

Le mot "analytique" étant à l'origine de bien des malentendus, je vais tenter de préciser le sens que je lui donne ici. Dans ce texte une proposition sera dite analytique, ou tautologique, si elle peut être établie exclusivement par une démonstration à partir d'axiomes et de règles de calcul qui définissent la signification des mots présents dans cette proposition. Selon cette définition, la proposition "un triangle a trois angles", mais aussi la proposition "la somme de la mesure de ces trois angles est égale à π" est analytique, car ces propositions peuvent se démontrer à partir des axiomes de la géométrie qui définissent la signification des notions de point, droite, angle, triangle, ... utilisées en géométrie. Il est bien clair que "analytique", compris dans ce sens, n'est pas synonyme de "immédiat", "vide" ou "inintéressant". Tout d'abord, la définition de ce mot exclut tout jugement de valeur. Ensuite, comme le montre le théorème de Church, le fait d'être analytique, loin d'être "immédiat" n'est pas même décidable.

Pour essayer de comprendre la nature de ces expériences mathématiques, on peut prendre un exemple simple qui permet d'établir la vérité de la proposition $2+2=4$. Cette expérience consiste à mettre deux balles de ping-pong dans une boîte, puis deux autres et à compter ensuite le nombre de balles présentes dans la boîte. On peut si on préfère, utiliser un boulier, ou plus simplement, compter sur ses

doigts. Le fait qu'il y ait quatre balles dans la boîte est une observation du monde physique. On peut dire qu'il y a quatre balles dans la boîte ici et maintenant, et à première vue rien n'assure qu'on obtiendrait le même résultat si on refaisait l'expérience ailleurs, à un autre moment, si la température et la pression étaient différentes, en mettant les balles dans la boîte avec une vitesse différente, ou dans un univers dans lequel la vitesse de la lumière, ou la constante de la gravitation seraient différentes. Qu'on compare cette expérience à celle qui consiste à lancer une pièce en l'air et à observer le côté sur lequel elle retombe : dans ce cas le résultat dépend clairement de la vitesse à laquelle la pièce est lancée et de la valeur de la constante de la gravitation.

Puisqu'on parle d'expériences et d'observations du monde physique, on doit parler de la vérité d'une proposition dans le monde physique. Par exemple, on dira que la proposition "L'eau bout à $100°C$" est vraie dans le monde physique, ou encore qu'elle est synthétique. Si a, b, c et d sont ces quatre balles, on dira aussi que la proposition $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$ est vraie dans le monde physique, comme le révèle l'expérience qu'on vient de faire. J'éviterai en revanche de parler de vérité dans le monde physique de propositions comme l'axiome du choix ou l'hypothèse du continu dont la signification dans le monde physique n'est pas clairement définie. J'appellerai "proposition concrète" une proposition dont on peut évoquer la vérité dans le monde physique. La limite exacte entre les propositions concrètes et celles qui ne le sont pas n'est pas elle-même très bien définie, mais ce n'est pas le propos ici. Je tenterai donc de me limiter à des propositions concrètes au dessus de tout soupçon.

Les propositions concrètes et analytiques sont vraies dans le monde physique. C'est, par exemple, le cas de la proposition "Si l'eau bout à $100°C$ alors l'eau bout à $100°C$" ainsi que de la proposition "Si l'eau bout à $0°C$ alors l'eau bout à $0°C$". Les propositions concrètes et analytiques sont donc également synthétiques. On exprime parfois cela en disant que les propositions concrètes et analytiques sont vraies dans tous les mondes possibles. Si elles sont vraies dans tous les mondes possibles, elles sont *a fortiori* vraies dans le monde physique. On réserve parfois le nom de "proposition synthétique" pour les propositions vraies dans le monde physique mais pas dans tous les mondes possibles, et bien que toutes les conventions linguistiques soient possibles, cela me paraît aussi peu pratique que de définir les nombres rationnels en se débrouillant pour exclure les nombres entiers.

Il n'y a donc rien de surprenant au fait que savoir si une proposition est synthétique ou non puisse donner des renseignements sur le fait qu'elle soit analytique ou non. Par exemple, la proposition "Si l'eau bout à $100°C$ alors (l'eau bout à $100°C$ et la vitesse de la lumière est $100ms^{-1}$)", est fausse dans le monde physique. De

ce fait, on peut en déduire qu'elle n'est pas analytique.

Le fait que les propositions concrètes et analytiques soient synthétiques, implique bien entendu que les propositions concrètes qui ne sont pas synthétiques ne sont *a fortiori* pas analytiques. Une expérience peut donc réfuter le fait qu'une proposition soit analytique. On peut faire ici un parallèle avec le fait qu'une expérience permette de réfuter une loi physique, mais jamais de l'établir. La similarité vient du fait que les propositions analytiques sont universelles — vraies dans tous les mondes possibles — comme les lois physiques — vraies à chaque occurrence expérimentale.

Mais l'expérience qu'on a faite tout à l'heure avait permis d'établir, et non de réfuter, que la proposition $2 + 2 = 4$ était analytique. Comment cela est-il possible ? Il y a ici un tour de passe-passe qui a permis de transformer une information négative en une information positive. Pour tenter de le comprendre, on peut comparer cette expérience à la véritable manière d'établir que $2 + 2 = 4$, c'est-à-dire à la démonstration.

Cette démonstration peut se faire dans plusieurs théories, en particulier dans l'arithmétique et dans la théorie des ensembles. Pour tenter d'établir un lien avec l'expérience, je vais me concentrer sur la démonstration en théorie des ensembles. Le lien avec la démonstration en arithmétique me semble beaucoup plus compliqué. Cette démonstration utilise les axiomes de la théorie des ensembles qui définissent les notions primitives de cette théorie — les notions d'ensemble, d'égalité et d'appartenance — ainsi que les définitions de la notion de nombre, du nombre 2, du nombre 4 et de l'addition en théorie des ensembles. Commençons par la notion de nombre entier. Ici encore, je vais me concentrer sur une définition possible, parmi d'autres, celle de G. Cantor, révisée par Whitehead et Russell. Les axiomes de la théorie des ensembles posent l'existence d'un ensemble infini, qu'on peut appeler A. Ces axiomes permettent ensuite de construire l'ensemble $\wp(A)$ des parties de A et la relation d'équipotence sur $\wp(A)$ puis l'ensemble quotient C de $\wp(A)$ par cette relation. On peut appeler "cardinaux" les éléments de C. L'un des cardinaux contient l'ensemble vide, on l'appelle 0, un autre contient les singletons contenant un élément de A on l'appelle 1, un autre contient les paires d'éléments de A, on l'appelle 2, ... On peut également construire un sous-ensemble $\mathbb{N}$ de C qui ne contient que les cardinaux finis, mais ce n'est pas essentiel ici.

Si n et p sont deux cardinaux, la somme de n et p se définit comme l'ensemble contenant $x \cup y$ à chaque fois que x est un élément de n, y un élément de p et x et y sont disjoints. Montrer que $2 + 2 = 4$ consiste donc à montrer que l'ensemble obtenu est le cardinal 4, dans le cas où n et p sont le cardinal 2, autrement dit, que chaque fois qu'on prend deux paires disjointes d'éléments de A, leur réunion

est un ensemble de quatre éléments, et également que n'importe quel ensemble de quatre éléments de A peut être obtenu ainsi.

En regardant les choses un peu naïvement, il faudrait donc tester tous les couples de paires disjointes d'éléments de A et vérifier que leur réunion contient bien quatre éléments. La démonstration de la proposition $2+2 = 4$ est une manière générique de faire cette vérification sans énumérer tous les couples. Avec l'expérience mathématique qu'on a faite tout à l'heure, on s'est approché de cette vérification. Mais l'expérience et la vérification diffèrent au moins sur trois points :

— le choix de A : la vérification devait porter sur les éléments de A sur lesquels on ne sait rien et qui n'ont aucune raison d'être des balles de ping-pong,

— le nombre de vérifications : la vérification devrait porter sur tous les couples de paires d'éléments de A et on n'a vérifié la propriété que dans un seul cas,

— la nature de la vérification : on devait établir que la proposition $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$ était analytique, et on a uniquement établi qu'elle était synthétique.

Commençons par le deuxième point : pourquoi suffit-il de vérifier l'un des cas pour se convaincre que dans tous les autres, le résultat serait identique ? Simplement parce qu'on peut démontrer que quand on ajoute deux cardinaux, on obtient un cardinal. De ce fait, pour déterminer le cardinal obtenu, il suffit d'observer un seul de ses éléments. En effet, les cardinaux formant une partition de l'ensemble $\wp(A)$, il suffit de savoir qu'un cardinal contient un ensemble de quatre éléments pour connaître ce cardinal en entier. Le premier point se résout de la même manière. Là encore on peut démontrer que si on remplace l'ensemble infini A par un autre ensemble infini A', le résultat est identique. Il suffit donc, encore une fois, de vérifier un seul ensemble A. Dans ce cas, pourquoi ne pas choisir pour A un ensemble qui contient ces balles de ping-pong.

Le dernier point est le plus important. Pour le résoudre, il faut utiliser le fait que la théorie des ensembles est une théorie complète pour les propositions de ce type, et donc qu'elle démontre ou bien la proposition $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$ ou bien la proposition $\{a, b\} \cup \{c, d\} \neq \{a, b, c, d\}$. Or si la proposition $\{a, b\} \cup \{c, d\} \neq \{a, b, c, d\}$ était démontrable, elle serait analytique et donc synthétique. La proposition $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$ serait donc fausse dans le monde physique, et l'expérience qu'on vient de faire a montré que ce n'était pas le cas. Donc, du fait de la complétude de la théorie des ensembles pour des propositions de ce type, on peut déduire que la proposition $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$ est analytique parce qu'elle est synthétique. C'est cette notion de complétude qui

permet la transmutation d'une réfutation en une affirmation.

Je voudrais faire une courte digression pour comparer la manière dont on interprète le résultat de cette expérience avec la manière dont on interprète certaines propositions qu'on entend dans sa vie quotidienne. En temps normal, quand on entend une proposition, on reconnaît des mots dont on connaît la catégorie grammaticale, ce qui permet d'analyser la structure de la proposition et d'en déduire le sens. Le lexique et la grammaire étant ce qu'ils sont, il peut arriver qu'il y ait plusieurs analyses et plusieurs sens possibles et dans ce cas, on peut utiliser le contexte d'énonciation pour réduire les ambiguïtés. Souvent la connaissance complète du contexte d'énonciation n'est pas nécessaire et quelques indices suffisent à lever les ambiguïtés.

Pourtant, il y a des situations d'énonciation dans lesquelles on peut utiliser une méthode beaucoup plus simple : ce sont toutes les situations où on sait *a priori* que seuls deux ou trois messages peuvent être énoncés. Par exemple, quand on fait cuire une côte de bœuf, on demande parfois à la personne qui va la manger la cuisson qu'elle préfère. On sait *a priori* que la réponse se situera dans un ensemble prédéterminé de trois énoncés possibles. Quand on l'entend, au lieu d'utiliser la méthode habituelle d'analyse, on peut se contenter de la comparer, à un niveau phonologique rudimentaire, aux trois énoncés possibles et à retenir le plus proche. Le contexte d'énonciation ne sert pas ici à désambiguïser le message, c'est quasiment le message qui sert à désambiguïser l'information présente dans le contexte. De ce fait, un indice sur le message suffit en général à être compris, et la communication peut s'établir même dans un environnement très bruyant, comme dans un restaurant : il suffit par exemple d'entendre le son "an", pour connaître la réponse en entier. Ce principe est utilisé par certains systèmes informatiques qui interagissent "en langue naturelle" avec leurs utilisateurs et qui au lieu d'effectuer une analyse lexicale et syntaxique du message entré par l'utilisateur se contentent de rechercher des mots-clés.

Dans un cas comme dans l'autre, il y a une construction qui procède par élimination : le fait que le message contienne le son "an" indique que ce n'est ni "à point" ni "bien cuit", ce qui permet de déduire le message en entier. De la même manière, dans l'expérience qu'on vient de faire, c'est parce qu'on sait que la proposition $\{a, b\} \cup \{c, d\} \neq \{a, b, c, d\}$ n'est pas analytique qu'on en déduit que la proposition $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$ l'est. Ensuite, dans un cas comme dans l'autre, c'est parce qu'on sait *a priori* ce qu'on cherche qu'on peut faire cette construction par élimination : c'est la condition d'énonciation qui indique qu'il n'y a que trois réponses possibles, de même, c'est la connaissance *a priori* que le choix de l'ensemble A est indifférent, que le résultat de l'enquête doit être un

cardinal et que la théorie des ensembles est complète pour les énoncés de ce type qui permet d'interpréter le résultat.

Des souffleries, comme calculateurs analogiques

On peut se demander si ces expériences mathématiques ont un caractère exceptionnel, ou si elles sont, au contraire, fréquemment utilisées. On a déjà évoqué deux exemples : l'utilisation d'abaques pour compter — sur ses doigts, avec un boulier, ... — et l'utilisation d'ordinateurs pour vérifier la correction de démonstrations en déduction modulo. On peut ajouter un troisième exemple, qui montre que ce type d'expérience est peut-être assez fréquent. Il s'agit des "essais en soufflerie" pratiqués en aéronautique.

Je voudrais surtout insister sur le fait que ces essais en soufflerie ont très peu à voir avec les expériences qu'on fait dans les sciences du monde physique, par exemple avec l'expérience de Michelson et Morley, mais sont beaucoup plus proches des expériences mathématiques comme celles qu'on vient de faire avec les balles de ping-pong.

Quand on construit un nouveau type d'avion, on veut connaître la forme de l'écoulement de l'air autour de cet avion quand il est en mouvement, de façon à savoir s'il peut voler, s'il optimise la consommation de carburant, ... Pour cela, il suffit de résoudre une équation aux dérivées partielles simple, mais aux conditions de bord compliquées, puisqu'elles dépendent de la forme de l'avion. Comme on ne peut pas, en général, calculer explicitement la solution de cette équation, on fabrique une maquette, on la met dans une soufflerie et on observe la manière dont l'air s'écoule autour de cette maquette.

En quoi un tel essai diffère-t-il de l'expérience de Michelson et Morley ? Dans les deux cas, on a une théorie : d'une part l'aérodynamique, qui décrit la manière dont l'air s'écoule autour d'un objet, d'autre part la mécanique newtonienne à laquelle on ajoute l'hypothèse d'un référentiel absolu pour la lumière. Dans les deux cas, on fait une expérience : la théorie prévoit un résultat et on observe un résultat. Dans le cas de l'expérience de Michelson et Morley, et dans les cas des expériences qu'on mène dans les sciences du monde physique en général, on compare ces deux résultats, de façon à voir si les faits corroborent, ou au contraire réfutent, la théorie. Pour que cela soit possible, il faut connaître explicitement le résultat prévu par la théorie. Or, dans le cas des essais en soufflerie, on ne connaît pas le résultat prévu par la théorie, et c'est précisément pour cela qu'on fait l'essai. On ne cherche donc pas dans ce type d'essais à éprouver les lois de

l'aérodynamique et si on le cherchait, il faudrait remplacer l'avion par une forme plus simple, comme une sphère ou un cylindre, afin de pouvoir calculer le résultat prévu par la théorie et le comparer au résultat de l'expérience.

Si on ne cherche pas à éprouver la théorie, que cherche-t-on ? On cherche simplement à connaître la forme de l'écoulement de l'air autour de l'avion. L'essai en soufflerie, la résolution exacte de l'équation quand elle est possible et la simulation numérique — c'est-à-dire la résolution approchée de l'équation à grands renforts de calculs — servent à la même chose : à trouver la forme de l'écoulement de l'air autour de l'avion, c'est-à-dire la solution de l'équation.

On peut objecter que l'essai en soufflerie présente l'avantage sur la résolution de l'équation et la simulation numérique, que si les lois de l'aérodynamique venaient à être réfutées un jour, le résultat de l'essai en soufflerie resterait valable, mais pas celui de la résolution, exacte ou approchée, de l'équation. Certes l'essai en soufflerie, la résolution exacte de l'équation et la simulation numérique partagent le même but : connaître la forme des écoulements, mais ils ne partagent pas la même méthode, car la résolution exacte de l'équation et la simulation numérique calculent le résultat prédit par la théorie, alors que l'essai en soufflerie observe le résultat dans le monde physique, sans référence à la théorie.

Cette objection est parfois pertinente, mais pour cela il faut que l'essai en soufflerie reproduise exactement les conditions d'utilisation réelle de l'avion. Or, c'est rarement le cas. Par exemple, quand on teste une maquette d'avion réduite au dixième, il n'est pas immédiat de savoir si on doit conserver la vitesse du vent relatif identique à celle des conditions réelles, ou si on doit elle aussi la réduire au dixième, ou au centième, ... Pour le savoir on doit utiliser la théorie. De manière plus visuelle, la lave d'un volcan est quasiment solide à l'échelle de quelques centimètres, mais très liquide à l'échelle de quelques kilomètres. Quand on étudie la dynamique de l'écoulement de la lave sur une maquette de volcan de quelques centimètres, on doit utiliser un liquide beaucoup moins visqueux que la lave pour que l'expérience soit pertinente. Pour choisir le coefficient de viscosité du substitut, on doit utiliser la théorie. Autrement dit, il est peut-être hasardeux de prétendre que la pertinence d'un essai d'écoulement de lave sur une maquette de volcan, ou d'un essai en soufflerie est complètement indépendante de la théorie générale de la mécanique des fluides. De ce fait, les essais en soufflerie se rapprochent de la résolution de l'équation, non seulement dans leur but — connaître la forme de l'écoulement de l'air —, mais aussi dans leurs moyens — le recours à la théorie. La véritable opposition n'est pas que les essais en soufflerie contrairement aux expériences des sciences du monde physique sont indépendantes de toute forme de théorisation, mais le fait que l'essai permet d'obtenir un résultat inconnu alors

que l'expérience permet de tester un résultat connu.

Les essais en soufflerie, comme la simulation numérique, sont des manipulations d'un objet du monde physique qui permettent de trouver la solution d'une équation aux dérivées partielles, c'est-à-dire d'établir un résultat mathématique. Si on veut le formuler ainsi, on peut dire que la soufflerie est un calculateur analogique.

La construction des outils

Pour construire une lunette, un ordinateur, une soufflerie, un thermomètre, ... il faut avoir quelques connaissances sur le monde physique. De ce fait, la correction des observations faites avec un outil — dans les sciences du monde physique comme en mathématiques — est conditionnée par la correction des théories du monde physique qui ont servi à construire cet outil. C'est sur ce point que l'utilisation d'outils en mathématiques introduit la rupture peut-être la plus radicale.

Pour étudier expérimentalement la loi de dilatation d'un gaz avec la température, on doit utiliser un thermomètre, par exemple un thermomètre à mercure. Sur ce thermomètre, on ne lit pas directement une température, mais le volume pris par le mercure. Quand on lit que la température est de $100°C$, même en supposant qu'on ne fasse pas d'erreur de lecture, on peut en déduire que la température est effectivement de $100°C$, pourvu que la loi de la dilatation du mercure qui a servi à fabriquer le thermomètre soit correcte. De ce fait la loi de dilatation du gaz qu'on établit n'est vraie que si celle de dilatation du mercure qui a servi à fabriquer le thermomètre l'est également. Et le résultat est encore plus hypothétique quand on utilise un thermomètre à mercure pour étudier la loi de dilatation du mercure.

Naturellement, une objection possible est de dire qu'on utilise uniquement des lois du monde physique bien établies pour fabriquer des outils, et qu'on utilise ces outils pour tester des lois plus conjecturales. Il est vrai que c'est parfois le cas. Par exemple, dans l'expérience qu'on a faite avec les balles de ping-pong, on utilise le fait que deux balles de ping-pong ne peuvent pas s'annihiler en émettant une paire de photons, ce qui est une loi du monde physique relativement bien établie. De même, comme on connaît les lois de la réfraction de la lumière, on sait que quand on observe avec une lunette un astre rouge en haut et indigo en bas en passant successivement par toutes les couleurs de l'arc-en-ciel, cela est plus vraisemblablement une aberration qu'une propriété de l'astre observé.

Mais, il n'est pas absolument certain que les lois de l'optique qui servent à fabriquer une lunette — et qui portent le nom de "lois de Descartes" — étaient

si bien établies au moment où Galilée a observé les satellites de Jupiter et il n'est donc pas absurde de penser que les observations de Galilée auraient pu être inexactes à cause d'une mauvaise conception ou d'une mauvaise utilisation de sa lunette dont il n'aurait pas pleinement eu conscience. Pour fabriquer des instruments, on utilise souvent les découvertes scientifiques les plus récentes, comme dans le cas de la lunette de Galilée ou du microscope à effet tunnel, et cette objection n'est donc pas toujours pertinente.

Naturellement, dans les sciences du monde physique, ce problème se résout de lui même, si on pense que les observations ne servent pas à établir les théories physiques, mais à les réfuter. De ce fait, quand on étudie par exemple la dilatation d'un gaz avec la température pour éprouver une loi supposée, si jamais l'expérience ne produit pas le résultat prévu par la théorie, on sait qu'il y a une réfutation, que ce soit de la loi de dilatation du gaz testée ou de la loi de dilatation du mercure utilisée pour fabriquer le thermomètre. C'est banalité que de remarquer que le processus expérimental n'éprouve pas les lois physiques individuellement, mais dans leur ensemble, et qu'une réfutation par l'expérience n'indique jamais quelle loi est réfutée, mais uniquement qu'une des lois au moins parmi l'ensemble des lois testées est erronée. C'est pour cela qu'il y a toujours plusieurs façons d'interpréter le résultat négatif d'une expérience, l'une d'elles étant que les outils qu'on utilise sont conçus sur des lois erronées.

Autrement dit, dans les sciences du monde physique, il ne faut pas trop opposer le processus expérimental aux instruments de mesure. L'ensemble forme un système, dont la théorie prévoit l'état et qu'on observe à l'œil nu. Le fait que le processus de mesure soit décrit par les lois ordinaires de la théorie est un principe fondamental, auquel on devrait accorder, me semble-t-il, autant d'importance que la concordance avec l'expérience et la réfutabilité dans la définition de la scientificité d'une théorie du monde physique. Dire que l'observation d'un phénomène physique est elle même un phénomène physique susceptible d'être observé et décrit par la théorie me semble une thèse réaliste que les positivistes pourraient adopter et aussi une thèse positiviste que les réalistes pourraient adopter.

Une seule théorie a prétendu déroger à cette règle et singulariser l'acte d'observation, c'est la mécanique quantique dans l'interprétation de Copenhague, selon laquelle la mesure produit un effet sur un système — sa mise dans un état propre — qui n'est pas conséquence de l'équation de Schödinger. Ce principe est, de loin, beaucoup plus déroutant que l'absence de déterminisme [20] ou la non lo-

20. selon laquelle la théorie ne peut pas prévoir l'état d'un système dans le futur mais seulement des probabilités, que ce soit à cause d'une imprévisibilité intrinsèque du monde physique, ou à

calité [21]. C'est cette singularisation de la mesure qui crée des paradoxes comme celui du chat de Schrödinger, et en particulier la question de savoir si l'observation du chat est suffisante à mettre le système dans un état propre où si seule l'observation du physicien est susceptible d'opérer cette transformation. C'est aussi cette singularisation de la mesure qui rend la mécanique quantique dans l'interprétation de Copenhague compatible uniquement avec le positivisme, mais pas avec le réalisme, et en fait donc la seule théorie du monde physique non métaphysiquement neutre. Cependant, il est assez raisonnable de dire que cette formulation de la mécanique quantique est en passe d'être abandonnée depuis les travaux sur la décohérence [22] qui font dériver de principes plus fondamentaux l'évolution du système en un état propre lors d'une mesure, mais plus généralement lors de son interaction avec un objet de grande taille.

Le problème de la dépendance des faits établis par rapport aux hypothèses ayant servi à la construction de l'outil se résout donc de lui même du fait de la nature conjecturale et révisable des théories du monde physique et du rôle négatif de l'expérience. Malheureusement, le problème se résout ainsi uniquement pour les théories du monde physique, mais pas pour les mathématiques.

Quand on fait une multiplication à la main ou mentalement, et qu'on obtient un résultat différent de celui fourni par une calculatrice, il se peut que ce soit parce que la théorie des semi-conducteurs qui a permis de construire la calculatrice est erronée. Beaucoup de mathématiciens et d'informaticiens pensent que quand on utilise un ordinateur pour démontrer un théorème, il faut également démontrer la correction des programmes utilisés — compilateurs et systèmes d'exploitation compris —, et aussi celle des circuits logiques de l'ordinateur. Mais toutes ces démonstrations n'empêcheront jamais le fait qu'en utilisant un objet du monde physique, on fait reposer la vérité du théorème démontré sur des connaissances révisables.

On arrive alors à une forme de paradoxe. En principe, comme on vient de le voir, l'utilisation d'un ordinateur ou d'un autre outil pour établir la vérité d'une proposition mathématique introduit une certaine possibilité d'erreur. En revanche, on s'aperçoit que, dans les faits, la vérification d'une démonstration mathématique avec un ordinateur augmente en général la confiance qu'on a dans cette démonstration.

---

cause d'une incomplétude de la théorie, à laquelle il manque des "variables cachées".

21. selon laquelle, d'une part les systèmes physiques ne sont pas en un lieu déterminé, mais sont décrits par une fonction d'onde étalée sur l'univers entier, et d'autre part, si le le non déterminisme est dû à la présence de variables cachées, celles-ci sont également étalées sur l'univers entier.

22. Voir, par exemple, R. Omnès, *Philosophie de la science contemporaine*, Gallimard (1994).

Par exemple, refaire les calculs de la théorie des mouvements de la lune de Ch. Delaunay à l'aide d'un système de calcul formel a permis d'y trouver une petite erreur [23]. De même vérifier des démonstrations de Newton à l'aide d'un système informatique à aussi permis d'y trouver une petite erreur [24]. De plus, quand on propose de nouveaux algorithmes critiques pour l'aéronautique, l'informatique médicale ou les télécommunications, la tendance des organismes de certification est de plus en plus de demander que les démonstrations de correction de ces algorithmes aient été vérifiées à l'aide d'ordinateurs. Certains pensent, également, que cette vérification sera un moyen a relativement court terme d'éviter l'annonce et la publication de résultats faux en mathématiques. Qu'on pense, par exemple, aux dizaines de démonstrations fausses de la quadrature du cercle, ou du théorème de Fermat, qui ne sont pas toutes l'œuvre d'illuminés, mais aussi, pour certaines, de mathématiciens sérieux. Plus simplement, enfin, quand on fait une multiplication à la main ou mentalement, et qu'on obtient un résultat différent de celui fourni par une calculatrice, la première idée est qu'on a fait une erreur et non que la théorie des semi-conducteurs qui a permis de construire la calculatrice est réfutée. D'une part, cette possibilité qu'une calculatrice puisse donner un résultat faux parce que la théorie des semi-conducteurs est erronée paraît très improbable, aussi improbable que celle qu'une démonstration écrite à la main soit erronée parce que l'encre utilisée est sympathique et que certains symboles ont disparu entre le moment où on les a écrits et le moment où on les a relus. D'autre part, cette possibilité qu'on ait fait une erreur de calcul n'a rien d'improbable.

Ce paradoxe n'existe donc que parce que nous pensons, peut-être hâtivement, que nos connaissances mathématiques, qui ne reposent que sur la démonstration, sont dures comme du roc, alors que nous nous trompons parfois. Il faut reconnaître, pour expliquer ce paradoxe apparent, qu'une certaine tradition philosophique qui fait du *cogito* le point de départ de toute forme de connaissance nous a amené avec raison à nous méfier de nos perceptions sensorielles et des généralisations hâtives que nous faisons à partir de nos observations — c'est cela, entre autres choses, qui nous amène à penser les théories du monde physique comme conjecturales et révisables —, mais que cette tradition, qui place la conscience au sommet, nous met très rarement en garde contre les défaillances de notre entendement. Cette confiance absolue dans l'entendement est rappelée dès les pre-

23. Voir, par exemple, D. Barton and J.P. Fitch, Applications of algebraic manipulation programs in physics,*Reports on Progress in Physics*, 35 (1972) pp. 235-314.

24. J.D. Fleuriot and L.C. Paulson, Proving Newton's Propositio Kepleriana using geometry and nonstandard analysis in Isabelle, X.-S. Gao, D. Wang and L. Yang (eds.) *Automated Deduction in Geometry*, Lecture Notes in Artificial Intelligence 1669, Springer-Verlag (1999).

mières lignes du *Discours de la méthode*. Et c'est tout naturellement que nous en déduisons que les théories mathématiques, contrairement aux théories du monde physique ne peuvent pas être erronées puisqu'elles ne sont le fruit que de cet entendement si parfait. Il faudra pourtant sans doute admettre un jour que cet entendement également est faillible, si nous voulons comprendre pourquoi utiliser un outil pour effectuer une opération permet d'augmenter la confiance que nous avons dans son résultat, alors qu'en théorie, cela est au contraire, potentiellement une source d'erreurs.

Il ne s'agit pas ici, de confondre les démonstrations mathématiques erronées avec les théories du monde physique réfutées, et encore moins d'assimiler les connaissances mathématiques à des connaissances expérimentales et revisables. Ces deux formes de connaissances sont naturellement très différentes. Il s'agit, beaucoup plus simplement, de reconnaître que nous faisons tous parfois des erreurs dans nos démonstrations et qu'utiliser des outils peut remédier à ces défaillances de notre entendement, même si cela rend nos connaissances mathématiques dépendantes, en théorie, des connaissances révisables sur le monde physique qui ont servi à la construction de ces outils.