3. LE VIDE ET LES ENTIERS DE VON NEUMANN

Un exemple remarquable de situation où un formalisme élégant conduit à des notations impraticables si on ne les accompagne pas de notations raccourcies est celui des entiers de von Neumann, qui permettent en théorie des ensembles de construire les nombres à partir de l'ensemble vide. Ceux-ci sont définis en posant 0={} (l'ensemble vide), $n+1 = n \cup \{n\}$, ce qui donne :

0 = {}
1 = {{}}
2 = {{}, {{}}}
3 = {{}, {{}}, {{}, {{}}}}
4 = {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}
5 = {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}
6 = {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}}
7 = {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}, {{}, {{}}, {{}, {{}}}, {{}, {{}}, {{}, {{}}}}}}}}

Imagine-t-on combien il serait pénible d'écrire les tables de multiplication dans ce formalisme !

de place, il note a^7 à la place de $a\times a\times a\times a\times a\times a\times a$, ou $sin^{(5)}(x)$ à la place de $sin(sin(sin(sin(sin(x)))))$; les parenthèses autour du 5 évitent la confusion entre $sin^{(5)}(x)$ et $sin^5(x)$.

Si seules de telles abréviations étaient utilisées, il serait facile de traduire une preuve humaine en preuve formelle (et donc de la vérifier mécaniquement). On demanderait à l'ordinateur de remplacer systématiquement chaque notation abrégée par sa version complète et, même si cette pratique allonge le texte, ce ne serait pas une gêne sérieuse pour l'ordinateur chargé de le contrôler.

LES RACCOURCIS ET LES ABRÉVIATIONS

Malheureusement la plupart des abréviations sont ambiguës, et seul le contexte permet d'en déterminer la signification. La notation *dx*, par exemple, peut représenter le produit de la variable *d* par la variable *x*, ou bien la différentielle de *x* utilisée en calcul intégral. Le mathématicien Littlewood cite l'anecdote où un professeur qui écrivait le polynôme $ax^4+bx^3+cx^2+dx+e$ commentait la formule en disant : «*e* n'est pas nécessairement, mais peut l'être, la base des logarithmes naturels.» Le signe + désigne l'addition entre entiers ou celle entre matrices ou toutes sortes d'autres opérations (il n'est pas rare que, dans un même texte mathématique, plusieurs signes + soient utilisés, chacun se référant à un concept différent). La notation *i*, selon le texte, désignera un entier naturel, ou le nombre complexe dont le carré vaut –1, ou autre chose encore.

On trouve aussi fréquemment des indications qui introduisent une ambiguïté : «Le paramètre *k* sera fixé dans le reste du paragraphe, et à la place de $f_k(x)$ nous écrirons $f(x)$.» Les textes mathématiques sont remplis de ces raccourcis qui rendent difficile la traduction dans un langage formel. Les mathématiciens en sont conscients, comme cette citation de Nicolas Bourbaki (*Algèbre linéaire*, Chapitre II, p. 53) l'atteste : «La notation u⊗v pourra donc prêter à confusion, et il sera nécessaire que le contexte indique s'il s'agit d'un produit tensoriel ou d'une application linéaire.» Mille autres exemples pourraient être donnés.

PARTOUT DES MANQUES

Toutes ces abréviations, après un travail attentif et minutieux, pourraient être traquées et supprimées du texte d'une démonstration, alors qu'en revanche les abréviations dans la structure même des démonstrations sont bien plus graves. Les textes mathématiques en sont pourtant truffés.

On comprend ce que signifie «le lecteur vérifiera sans peine que le chiffre des unités de 2^{100} est 6» ou «quand on développe $(x + 4x^5)^{12}$, le coefficient de x^{20} est 1056» ; en prenant une feuille de papier, le lecteur (supposé patient) s'assurera de la justesse de ce qui est affirmé, et le bout de démonstration qui manque – un calcul – sera ainsi reconstitué.

Parfois le calcul qui permettrait la vérification est impossible à faire sans l'utilisation d'ordinateurs munis de programmes particuliers. Imaginez ce que vous devriez faire pour vous assurer de l'affirmation «il y a 9,98 % de '7' parmi le premier million de décimales du nombre π» (ce qui est un énoncé vrai qu'on trouve dans certains ouvrages). On doit faire confiance à l'auteur qui affirme cela, ou travailler des heures, voire des jours, pour le vérifier.

Lorsqu'il ne s'agit que de calculs, combler le trou présent dans la preuve humaine ne semble pas totalement insurmontable. En revanche, comment ne pas être inquiet quand le mathématicien, après avoir donné la démonstration du théorème dans le cas *b* positif, écrit : «le cas *b* négatif se traite facilement» ou «est analogue»? Va-t-on y arriver? Comment ne pas devenir franchement anxieux quand, dans le texte d'une démonstration, on découvre le laconique et pourtant très fréquent «Laissé en exercice au lecteur»?

Voici quelques exemples de ce type, tirés du livre d'*Algèbre linaire* du traité Bourbaki. D'abord le classique : «On vérifie facilement que...» (chapitre I, p. 107). Une telle phrase ne semble pourtant pas pouvoir guider le lecteur. Pas plus d'ailleurs que celle-ci qui, si vous rencontrez un obstacle dans la démonstration omise, risque de vous faire désespérer de vous-même : «La démonstration est encore plus simple pour...» (Chapitre II, p. 85).

L'inévitable «on voit que...» fait bien sûr partie de l'arsenal démonstratif du traité (Chapitre III, p. 158). Lorsque des précisions sont données, elles ne sont pas nécessairement parlantes, et l'on n'est pas certain de pouvoir s'en sortir avec celles, cryptiques, de la démonstration de la proposition 3 du Chapitre II, p. 39, qui se termine par : «La conclusion résulte donc de la déf. 1 et de II, p. 10, prop. 5(ii).» Plus délicieuse encore est l'étonnante démonstration en une ligne d'un énoncé qui en occupe quatre : «Cela résulte de E, III, p. 29, prop.12, et E,.III, p. 42, cor.1» (Chapitre III, p. 87).

ON PEUT MÊME OMETTRE LES THÉORÈMES!

Les non-mathématiciens seront étonnés, mais les raccourcis, même dans les meilleurs traités, peuvent s'étendre au-delà des démonstrations. Ainsi, parfois, les définitions et les énoncés eux-mêmes sont omis. Toujours dans le traité de N. Bourbaki, on trouvera l'admirable : «Nous laissons au lecteur le soin de formuler les définitions et remarques analogues pour les systèmes d'équations linéaires à gauche» (Chapitre II, p. 146), et aussi : «On laisse au lecteur le soin de définir un système projectif d'anneaux... et de vérifier que...» (Chapitre II, p. 146). Pourquoi ne pas confier au lecteur le soin d'écrire le chapitre suivant tout seul?

Ces omissions ne sont pas sans danger, et beaucoup de mathématiciens vous diront que, même si elles paraissent inévitables, elles restent périlleuses. Il est fréquent en effet que des erreurs se produisent dans les textes mathématiques, précisément en ces endroits incomplètement détaillés par un mathématicien pressé et sincèrement persuadé que la démonstration est possible à partir des indications succinctes qu'il propose à titre d'argument.

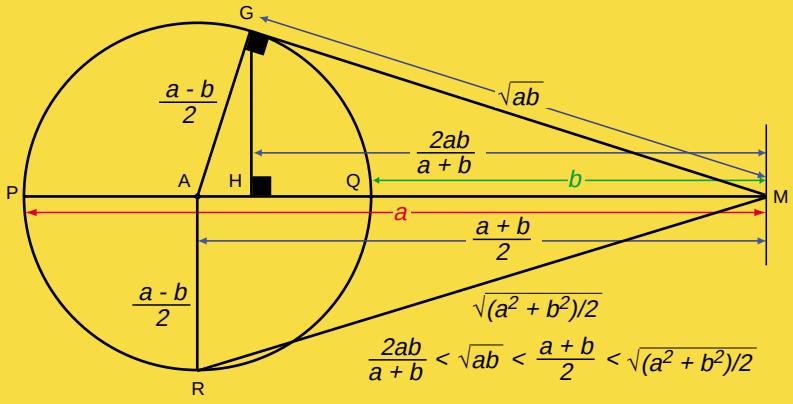
Ces facilités autorisées par les «laissés au lecteur», et autres «à titre d'exemple, démontrons le cas numéro 5», sont dangereuses, car tous ceux qui écrivent des textes mathématiques savent que bien souvent ils n'ont pas détaillé pour eux-mêmes sur une feuille à part ces parties manquantes qu'ils suggèrent au lecteur de reconstituer seuls. Ils y ont réfléchi, ils sont intimement convaincus que «ça passe», mais est-ce suffisant ? Pourtant comment pourrait-on s'interdire ces facilités, puisque Bourbaki lui-même reconnaît que, dans les textes mathématiques, «l'emploi des ressources de la rhétorique est nécessaire» (Bourbaki, Introduction, p. 7)?

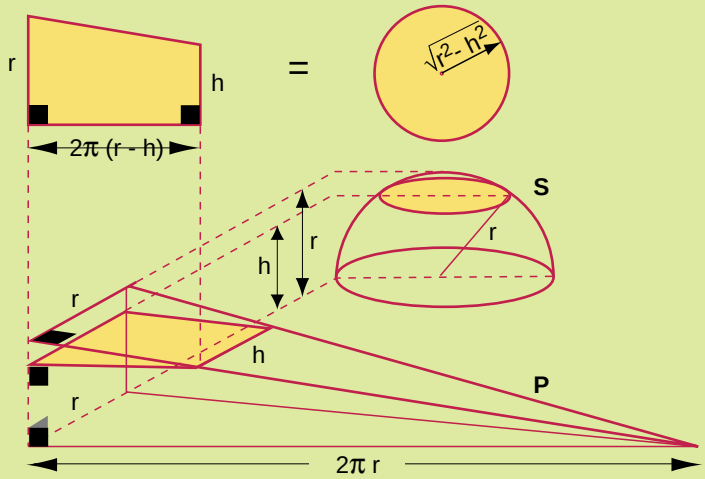
Encouragé par le plaisir de l'économie et l'élégance de la concision, soucieux aussi de ne pas passer pour un imbécile en donnant des détails sur un passage vraiment facile, tout mathématicien écourte ses démonstrations, et cela d'autant plus qu'il s'adresse à des mathématiciens de haut niveau. Assez étrangement donc, les risques sont maximaux dans les textes présentant des résultats de recherches. Dans un cours destiné à des étudiants, le mathématicien essaiera de contenir son penchant pour les brèves esquisses de preuves, sans toutefois résister à la tentation d'un «le cas 1 est trivial» et surtout au coup de l'exercice. Ces laconiques pirouettes font le désespoir des étudiants moyens, incapables de boucher ces trous prétendument aisés, et donnent un sentiment de culpabilité au lecteur trop pressé qui se dispense des travaux suggérés, dont pourtant, dans l'introduction, l'auteur a indiqué, avec perfidie, qu'il était important de les traiter soigneusement pour s'assurer de la bonne assimilation du cours.

Un trou fameux

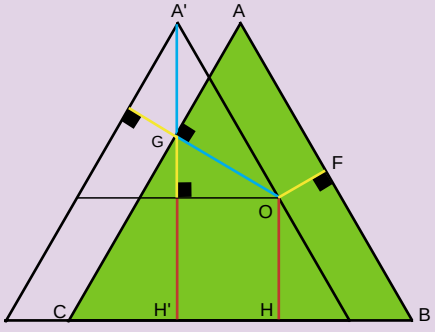
Un des plus fameux trous dans une preuve mathématique provient d'un de ces raccourcis imprudents. On sait que, le mercredi 23 juin 1993, à l'issue de trois jours de conférence Andrew Wiles concluait en public une présentation de la preuve du Grand Théorème de Fermat (qu'il démontrait comme cas particulier de résultats plus généraux). Personne sur le coup ne put vérifier la démonstration bien trop complexe, dont seules les grandes lignes avaient été expliquées oralement. La démonstration, d'environ deux cents pages, fut soumise à un comité d'experts composé de six spécialistes qui travaillèrent des mois durant. De nombreuses fois, ils durent interroger A. Wiles pour obtenir des explications leur permettant de saisir le sens de ce qui était écrit. Face à une preuve formelle, les experts mathématiciens n'au-

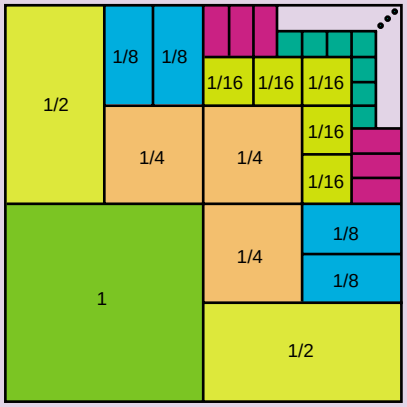
4. PREUVES SANS MOTS





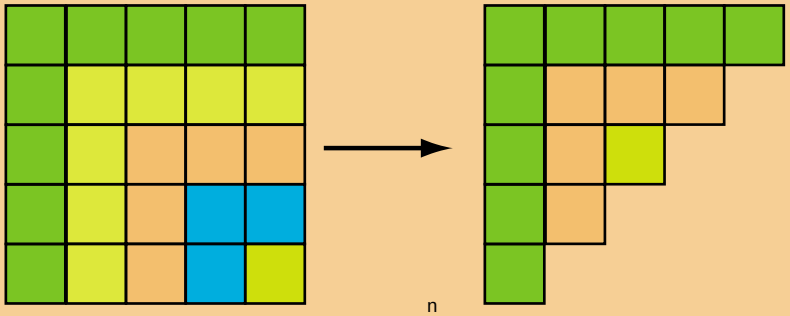
$V_S = V_P = 2\pi r^3/3$





LE THÉORÈME DE VIVIANI : OF + OH + OG = A'H'

1 + 2(1/2) + 3(1/4) + 4(1/8) + ... = 4



$$n^2 - (n-1)^2 + \ldots\ldots + (-1)^{n-1}(1)^2 = \sum_{k=0}^{n} (-1)^k (n-k)^2 = n(n+1)/2$$

5. PREUVE HEURISTIQUE IMPOSSIBLE (AUJOURD'HUI) À TRANSFORMER EN PREUVE FORMELLE

On considère la suite des nombres entiers définie par :
$x_1 = 2$,
x_2 = [le plus petit facteur premier de x_1+1]=3,
x_3 = [le plus petit facteur premier de x_1x_2+1]=7, ...,
x_{n+1}= [le plus petit facteur premier de $x_1x_2...x_n$ + 1], ...
Le début est 2, 3 , 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, ...

Cette suite d'Euclide-Mullin n'énumère que des nombres premiers différents. En effet, $y_n = x_1x_2...x_n + 1$ n'est pas divisible par x_1 (sinon 1 le serait comme différence de deux nombres divisibles par x_1). Le nombre y_n n'est pas divisible par x_2 (sinon 1 le serait), etc. Puisque y_n n'est divisible par aucun des nombres premiers, x_1, ..., x_n, x_{n+1} est un nouveau nombre premier, et donc tous les x_i sont des nombres premiers distincts. La question est de savoir si cette suite énumère tous les nombres premiers sans en oublier (bien sûr, ce sera dans le désordre). On pense que oui et l'on propose la preuve heuristique suivante.

Supposons que la suite ne contienne pas tous les nombres premiers. Soit p le plus petit nombre premier qui n'est pas dans la suite. À partir d'un certain N, tous les nombres premiers inférieurs à p seront parmi les nombres x_1, ..., x_N. Si n est un entier quelconque plus grand que N, le nombre $y_n = x_1x_2...x_n + 1$ peut être considéré comme un nombre quelconque vis-à-vis de p, et donc ce nombre a une chance sur p d'être un multiple de p (car un entier sur p est multiple de p). Le nombre y_n a donc une probabilité de $(1-1/p)$ de n'être pas multiple de p, qui est aussi la probabilité que x_{n+1} soit différent de p. La probabilité pour que ni $x_N + 1$ ni x_{N+2} ...x_{N+k} ne soient égaux à p est donc $(1–1/p)^k$ qui tend vers 0 à l'infini. Autrement dit, la probabilité pour que p n'apparaisse pas dans la suite x_n est nulle. Donc p apparaît dans la suite, ce qui contredit sa définition. Donc, tout nombre premier p apparaît dans la suite x_n, qui n'est pas autre chose que la liste des nombres premiers, sans répétition et écrite dans le désordre.

Un tel raisonnement est presque bon, mais il suppose que y_n est tiré au hasard, ce qui n'est pas le cas, et donc, sans un complément (que personne n'a réussi à découvrir et qui semble hors de portée des méthodes mathématiques actuelles), la preuve heuristique n'est pas une preuve acceptable.

raient pas eu à contacter A. Wiles ! A. Wiles lui-même prétendait avoir vérifié chaque étape de la démonstration deux fois avant de la confier à ses collègues. À chaque question des experts, il proposait d'ailleurs une réponse qui levait la difficulté soulevée. Petit à petit, A. Wiles rendait compréhensible son document, qui, si les mathématiques se conformaient à la description idéalisée évoquée au début de cet article, aurait dû l'être dès le départ.

On avançait lentement vers une validation totale, jusqu'au jour où une réponse ne contenta pas totalement un expert, ni le complément de réponse du jour suivant : il y avait un trou dans la démonstration, que, malgré tout le soin pris par A. Wiles, ce dernier n'avait pas vu. Le «bogue» provenait de l'utilisation, hors des conditions précises où il avait été démontré, d'un procédé que A. Wiles, dans une généralisation hâtive, avait utilisé sans faire dans ce cas tous les contrôles exigés.

On connaît la suite : plus de deux ans furent nécessaires pour corriger l'erreur et arriver, en empruntant un chemin différent de celui proposé en 1993, à une démonstration complète et acceptée des experts. Notons, pour rassurer les inquiets, qu'une fois cet accord des experts obtenu, la preuve fut confirmée par d'autres experts. Plus aucun doute ne persiste aujourd'hui sur sa validité, c'est-à-dire sur la possibilité d'écrire une preuve formelle du théorème de Fermat. La longueur de la preuve interdit, pour l'instant, cette transcription formelle complète, mais il n'y a aucune controverse sur son existence. La difficulté évoquée dans la rubrique de novembre concernant la transcription de la preuve de A. Wiles dans le formalisme de l'arithmétique élémentaire de Peano (plus limité que celui de la théorie des ensembles qui sert de référence implicite aujourd'hui) n'entache en rien l'unanimité qui règne sur la validité de la preuve de A. Wiles, et, sauf à imaginer que la théorie des ensembles est contradictoire, la victoire est définitive.

LES CONTROVERSES

Aujourd'hui, lorsqu'il y a une controverse en mathématiques sur la validité d'une démonstration, il est donc vrai en définitive qu'elle ne dure jamais longtemps, et cela à cause de la possibilité de s'approcher de plus en plus de ce que serait la preuve formelle complète du résultat.

Le rapport entre *preuves formelles* et *preuves réelles* peut donc se résumer en disant : les preuves formelles ne sont que très rarement écrites par les mathématiciens parce qu'elles sont très longues, mais ce sont quand même elles qui servent de recours ultime dans l'évaluation d'une *preuve réelle* dont la validité est douteuse. C'est, en effet, en cherchant à s'approcher pas à pas de ce que serait la *preuve formelle* du résultat discuté qu'on obtient l'accord définitif : ou bien on ne rencontre pas d'obstacles sur le chemin qui y conduit (et qu'on emprunte rarement jusqu'au bout) et la *preuve réelle* est considérée juste, ou bien un trou insurmontable apparaît et la preuve est insuffisante, donc inexistante...

La suppression des controverses en mathématiques est relativement nouvelle, car, avant les progrès logiques du début du siècle, il s'en présentait régulièrement et de graves incertitudes divisaient les esprits, même en mathématiques. Ce fut le cas à la fin du XVII^{e} siècle quand le calcul différentiel fut découvert et que la notion de limite n'était qu'imparfaitement maîtrisée (elle le fut par A. Cauchy, 1789-1857, et par K. Weierstrass, 1815-1897). Au moment de la mise au point de la topologie, d'autres controverses prolongées eurent lieu, comme celle que le philosophe Imre Lakatos détaille dans son livre à propos de la formule d'Euler $s–a+f = 2$ (a est le nombre d'arêtes d'un polyèdre ; s le nombre de sommets ; f le nombre des faces) dont il fut difficile de préciser exactement le domaine de validité.

Au début du siècle, une des dernières grandes controverses en mathématiques fut celle concernant les fondements mais elle ne porta pas sur l'exactitude ou l'inexactitude de preuves précises, ce fut une discussion sur les modes de raisonnement qu'on pouvait légitimement mettre en œuvre (notions ensemblistes, axiome du choix, raisonnements non constructifs, etc.). Aujourd'hui, grâce aux systèmes formels, la controverse sur les fondements des mathématiques s'est éteinte et n'est plus qu'un problème pour philosophes dont peu de mathématiciens se soucient. Sur toute question importante, un accord unanime s'établit, ce qui fait véritablement des mathématiques une science à part.

Des doutes concernant le théorème de Gödel exprimés juste après sa parution par quelques mathématiciens et les incompréhensions graves qui font douter des amateurs de tel ou tel résultat

(par exemple, la non-dénombrabilité des nombres réels ou l'impossibilité de la quadrature du cercle) ne doivent pas être pris plus au sérieux que les tentatives de réaliser un mouvement perpétuel qui obsède les inventeurs du dimanche. Oui, en mathématiques aujourd'hui, l'unanimité existe concernant la justesse, et aucune controverse véritable n'a plus cours.

Progrès dans la formalisation

Bien que peu de mathématiciens se soucient au quotidien de la formalisation complète de leurs preuves, les progrès faits sur ces questions ne sont pourtant pas négligeables.

Poincaré se moquait du fait que, pour écrire 1 dans le formalisme du système des *Principia* de Russell et Whitehead (le premier système formel complet permettant l'écriture d'un volume important de mathématiques), il fallait un grand nombre de symboles, ce qu'il trouvait absurde. Passionné par le traité de *Mathématiques* de N. Bourbaki, dont les premières pages sont constituées par la description détaillée du système formel sur lequel le traité s'appuie ensuite, un ami s'était amusé à écrire explicitement la suite des symboles représentant l'ensemble des parties d'un ensemble sans utiliser aucune abréviation. Le tout, une fois transcrit sur un rouleau de papier, avait une longueur de trois mètres.

Les systèmes formels d'aujourd'hui ne présentent pas tous ces défauts ridicules, car, dans le but de les manipuler, on a conçu avec des ordinateurs des notations plus efficaces. On a d'ailleurs, grâce à cela, pu écrire des preuves de résultats assez avancés de mathématiques. Les techniques mises au point à cette occasion servent aussi à prouver la validité de programmes informatiques, et c'est là tout un domaine de recherche actif où la logique vient en aide à l'informatique.

Les infiniment petits formalisés

D'autres progrès logiques ont étonné les mathématiciens. On désespérait de justifier par un formalisme précis les méthodes de calcul qui fonctionnent pourtant bien et qui se fondent sur la manipulation des infiniment petits. L'analyse des XVIII^{e} et XIX^{e} siècles avait d'ailleurs débarrassé les mathématiques de ces troublants infinis qui paraissaient indomptables. Le système formel de l'Analyse non standard de A. Robinson, dans les années 1960, a réussi l'exploit de proposer un usage réglé des infiniment petits. Celui qui souhaite profiter de son intuition de physicien pour calculer dispose maintenant d'un formalisme qui pourra valider ses calculs, jusque-là considérés comme non rigoureux. Les résultats logiques connus concernant l'Analyse non standard sont remarquables, et l'un d'eux indique que toute propriété ne mentionnant pas les infiniment petits démontrés dans le cadre formalisé de l'Analyse non standard peut aussi être démontrée sans utiliser les infiniment petits dans le formalisme ensembliste usuel. Ce résultat justifie *a posteriori* le choix fait historiquement par les mathématiciens de se passer des infiniment petits, mais, le connaissant, il permet aujourd'hui à celui qui trouve commode de les utiliser de laisser libre cours à son goût.

Preuves heuristiques et «presque preuves»

À côté de la notion de preuve formelle qui sert à mettre tout le monde d'accord pour savoir ce qui est vraiment démontré, il existe une multitude de preuves non formelles et résolument non formalisables (du moins avec les systèmes connus aujourd'hui) qui fournissent des presque-certitudes. Ces preuves heuristiques, c'est ainsi qu'on les appelle, sont étranges, car quand on les suit, elles persuadent de la vérité des propositions visées. Pourtant, comme pour les preuves démontrées autrefois par les infiniment petits, les mathématiciens les refusent. Bien qu'elles «fassent voir que c'est vrai», tant qu'on ne disposera pas de bons systèmes formels (analogues à celui de A. Robinson pour l'Analyse non standard), il sera impossible de les transformer en preuves formelles, ce qui signifie tout simplement qu'aux yeux des mathématiciens elles ne démontrent rien !

Un exemple de preuve heuristique difficile à transformer en preuve formelle est indiqué sur la figure 5.

Presque, mais pas vraiment

Un autre exemple de résultat presque prouvé est celui qui concerne les nombres parfaits impairs, résultat qui résiste à une démonstration depuis 20 siècles. Un nombre parfait est un nombre qui est égal à la somme de ses diviseurs différents de lui-même. Le nombre 6 qui est divisible par 1, 2, 3 est un nombre parfait, car 6 = 1+2+3. C'est le plus petit nombre parfait, et les trois suivants sont 28, 496, 8128. Existe-t-il des nombres parfaits impairs ? La question est posée depuis plus de deux millénaires. Personne n'en a jamais trouvé, mais personne n'a démontré qu'il n'en existait pas. Malgré cette absence de démonstration, tout le monde est persuadé aujourd'hui qu'il n'existe pas de nombre parfait impair, car on a démontré (rigoureusement) une grande quantité de propriétés que devrait posséder un tel nombre parfait impair *N*, s'il en existe.

– Un nombre parfait impair *N*, s'il en existe, possède au moins 8 facteurs premiers différents et, s'il est multiple de 3, il doit en posséder au moins 11 (P. Hagis, 1983).

– Un nombre parfait impair *N*, s'il en existe, est tel que la somme des inverses de ses facteurs premiers est située entre 0,596 et 0,694 (D. Suryanarayan, P. Hagis, 1970).

– La plus grande puissance d'un nombre premier qui divise un nombre parfait impair *N*, s'il en existe, est plus grande que 10^{20} (G. L. Cohen, 1988).

– Un nombre parfait impair *N*, s'il en existe, est plus grand que 10^{300} (R. Brent, G.L. Cohen, H. te Riele, 1989).

– Un des facteurs premiers d'un nombre parfait impair *N*, s'il en existe, dépasse 10^{6} (P. Hagis. G.L. Cohen, 1998), un autre dépasse 10^{4}, et un autre encore dépasse 10^{3} (1999, D. Iannucci).

Remarquez que certains résultats ont été démontrés il y a seulement quelques mois. Il semble qu'aucun nombre ne puisse vérifier toutes ces conditions à la fois (mais ce n'est pas rigoureusement établi), et donc on croit plus fortement que jamais qu'il n'existe aucun nombre parfait impair. Ce sentiment et l'idée qu'on est arrivé à quelques millimètres du résultat final ne constituent pas une preuve mathématique formalisable, et donc, comme c'est toujours le cas, aucune controverse n'a cours sur ce point : aussi fort que soit notre sentiment qu'on a qu'il n'existe pas de nombres parfaits impairs, personne ne prétend que c'est prouvé.

Nicolas Bourbaki, *Éléments de mathématique,* Paris.

Imre Lakatos, *Preuves et réfutations*, Éditions Hermann, Paris 1984.

Roger Nelsen, *Proofs Without Words : Exercices in Visual Thinking, The Mathematical Association of America*, 1993, ISBN 0-88385-700-6.

J. Dieudonné, *Pour l'honneur de l'esprit humain*, Hachette, 1987.

Jean-Michel Salanskis, *Le constructivisme non standard*, Presse universitaires du Septentrion, ISBN 2-85939-604-7, 1999. (À propos de l'Analyse non standard).

Simon Singh, *Le dernier théorème de Fermat*, Éditions J.-C. Lattès, 1998.