

xix^e siècle que l'on saura reprendre son précieux travail sur ces sujets et les mettre parfaitement en ordre.

Nous ne reviendrons pas sur le cas d'Augustin Cauchy et de son célèbre énoncé affirmant à tort qu'une limite de fonctions continues est aussi une fonction continue (<http://fredrickey.info/hm/CalcNotes/CauchyWrgPr.pdf>), ni sur Henri Poincaré et son mémoire faux qui lui valut le prix en l'honneur du roi Oscar de Suède (<https://journals.openedition.org/lettre-cdf/1103>) et qu'il fit réimprimer à ses frais après correction.

David Hilbert, lui aussi considéré comme l'un des plus grands mathématiciens et logiciens, a laissé un grand nombre de petites erreurs dans ses articles. Lorsqu'on décida, pour publier ses œuvres complètes, de les nettoyer de tout ce qui devait être remis sur pied, trois ans furent nécessaires à Olga Taussky-Todd pour réaliser le travail. Hilbert se trompa aussi une fois gravement en proposant une démonstration erronée de l'« hypothèse du continu », selon laquelle il n'y a pas d'infini intermédiaire entre celui des entiers et celui des nombres réels.

ÉCRIRE LES DÉMONSTRATIONS DANS LE LANGAGE DE LA LOGIQUE

Le développement de la logique a abouti au début du xx^e siècle à l'idée qu'une démonstration mathématique correcte peut être contrôlée mécaniquement, à condition de l'écrire dans un langage dont les premières esquisses furent proposées par Alfred Whitehead et Bertrand Russell dans les trois volumes des *Principia Mathematica* (1910-1913). En complétant légèrement la méthode des *Principia* dont la syntaxe de base n'est pas totalement fixée, on aboutit à la notion de « système formel » aujourd'hui au cœur de la logique mathématique. C'est elle qui donne son sens plein aux célèbres théorèmes d'incomplétude de Kurt Gödel, affirmant qu'aucun système formel ne sera jamais assez puissant pour toutes les mathématiques et qu'il sera donc toujours nécessaire de rechercher de nouveaux axiomes.

La précision absolue rendue possible par les systèmes formels aurait dû mettre fin aux erreurs en mathématiques. Ce n'était qu'illusion, car il est très difficile en pratique d'écrire ces textes mécaniquement vérifiables et qui fournissent d'absolues certitudes. Aujourd'hui, on a conçu des programmes informatiques, des « assistants de preuve », qui mettent au point ces preuves. Ces systèmes ne trouvent pas seuls de nouvelles démonstrations, mais aident les mathématiciens à écrire des démonstrations incontestables.

Grâce à eux, on a formalisé une part importante des mathématiques de base, ce qui >

4

LES ASSISTANTS DE PREUVE CORRIGENT LES ERREURS

Les systèmes informatiques dénommés « assistants de preuve » permettent aux mathématiciens d'écrire des démonstrations formelles, donc parfaitement complètes sans qu'aucune erreur ne puisse subsister. Ces logiciels ont-ils permis de corriger des erreurs passées inaperçues ? Dans certains cas oui (voir le cas de la preuve ontologique de Gödel dans le texte de l'article). Manuel Eberl est un expert qui travaille depuis des années à écrire des démonstrations en utilisant l'assistant de preuves Isabelle/HOL. Il témoigne de son travail :

« Normalement, il faut une compréhension très approfondie d'une preuve sur papier pour la formaliser et il faut réfléchir à la façon de s'y prendre pour la formaliser. [...] Si vous formalisez une démonstration particulière comme celle du théorème des nombres premiers [...], vous ne découvrirez probablement pas que tout est faux et que tout s'effondre, mais vous rencontrerez des petits problèmes.

J'ai trouvé des "erreurs" dans de nombreuses démonstrations, y compris quand elles étaient publiées dans des manuels scolaires ou des articles. La plupart de ces erreurs sont faciles à corriger et la plupart des mathématiciens les considéreraient probablement comme sans gravité. Certaines sont identifiées en quelques jours, d'autres nécessitent en fait de changer les définitions, d'ajouter des hypothèses ou de modifier l'énoncé du théorème. La plupart des "erreurs" entrent dans les catégories suivantes.

- Des arguments étonnamment non triviaux sont déclarés faciles et sans importance. [...]
- Des cas sont omis.

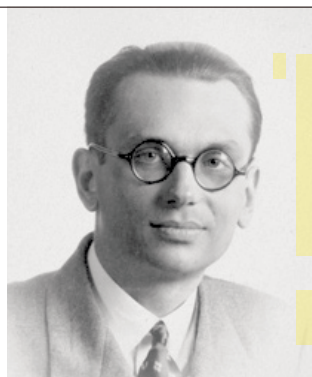
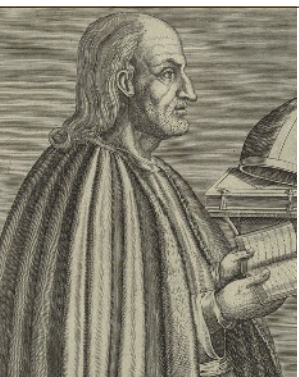
- Des erreurs arithmétiques sont commises, comme multiplier les deux côtés d'une inégalité par une constante dont on ne vérifie pas qu'elle est positive.
- Des hypothèses non indiquées sont utilisées subrepticement.

Je suis conscient que les mathématiciens ont souvent un point de vue indulgent. [...] Les types d'erreurs que je mentionne sont en général jugés insignifiants, et on pense que quelqu'un les aurait corrigées même en l'absence d'un système informatique, et donc que finalement les théorèmes et démonstrations incriminés sont corrects en un sens, puisque les problèmes identifiés sont mineurs.

Cependant, je ne suis pas d'accord avec cela. Je veux que mes démonstrations soient aussi rigoureuses que possible. Je veux être certain de n'avoir manqué aucune hypothèse. » (Pour le texte complet de Manuel Eberl, voir : <https://mathoverflow.net/questions/291158/proofs-assistant/312661>)



Manuel Eberl est chercheur à l'université technique de Munich, en Allemagne.



LA PREUVE ONTOLOGIQUE

5

Saint Anselme de Cantorbéry (1033-1109) (ci-dessus à gauche), puis Gottfried Leibniz (1646-1716) (au milieu), puis le logicien autrichien Kurt Gödel (1906-1978) (à droite) ont chacun à leur tour proposé des raisonnements utilisant uniquement des considérations logiques pour conclure que Dieu existe.

Le raisonnement ontologique d'Anselme dans sa version grossière est : « Dieu possède toutes les qualités, donc la qualité d'existence, donc Dieu existe. » Un peu plus précisément : « Dieu, par définition, est ce dont on ne peut rien concevoir de plus grand. Dieu existe dans l'entendement humain. Si Dieu existe dans l'entendement humain, nous pouvons l'imaginer plus grand, considérant qu'il existe aussi dans la réalité. Par conséquent, Dieu existe. »

Une version plus élaborée a été donnée par Leibniz et c'est elle que Gödel a tenté encore de perfectionner. Ces versions sont plus complexes et utilisent des notions de logique modale (comme « il est nécessaire », « il est possible », etc.), logiques dont des versions formelles ont été proposées et étudiées dès 1918 par Clarence Lewis, puis approfondies tout au long du xx^e siècle.

La validité de ces raisonnements repose sur l'acceptation individuelle des axiomes et définitions de départ qu'on peut

discuter à l'infini. Elle dépend aussi de la validité des raisonnements quand on a admis les axiomes et définitions. Cette validité est contrôlable grâce aux outils informatiques dont on dispose aujourd'hui. Cependant, même si on accepte individuellement les axiomes et que le raisonnement est jugé correct, il se peut encore que les axiomes soient globalement insatisfaisants parce que conduisant à des absurdités manifestes. C'est ce qui s'est produit pour le raisonnement proposé par Gödel.

En février 1970, pensant qu'il était mourant, Gödel a autorisé le mathématicien Dana Scott (né en 1932) à copier la dernière version de son raisonnement. Un peu plus tard, Gödel a affirmé à son ami le mathématicien et économiste Oskar Morgenstern (1902-1977) qu'il était satisfait de sa preuve, en précisant qu'il ne voulait pas la publier parce qu'il avait peur qu'on en déduise qu'il croyait en Dieu, alors qu'il était seulement engagé dans une exploration logique.

Récemment, Christoph Benz Müller, de l'université libre de Berlin, et Bruno Woltzenlogel Paleo, de l'université nationale australienne, ont montré, en utilisant des assistants de preuve, que le système utilisé par Gödel était absurde (voir leur article cité dans la bibliographie).

> confirme que nous ne devons avoir aucune inquiétude concernant la partie centrale des mathématiques. Pour les théorèmes les plus difficiles, dont les démonstrations sont très longues ou mettent en œuvre des concepts abstraits et délicats, on ne dispose pas encore de ces versions formalisées.

DES ÉNONCÉS PROUVÉS FORMELLEMENT...

Parmi les énoncés dont les preuves ont été contrôlées ainsi, on a par exemple :

- Il existe exactement cinq solides platoniciens (polyèdres réguliers convexes).
- Impossibilité de la trisection d'un angle à la règle et au compas.
- Indépendance du postulat des parallèles vis-à-vis des autres axiomes de la géométrie de base du plan.
- Théorème fondamental de l'algèbre sur les racines des polynômes.
- Théorème des valeurs intermédiaires concernant les fonctions continues de l'ensemble des nombres réels dans lui-même.
- Théorème des deux carrés: un entier est somme de deux carrés si et seulement si chacun de ses facteurs premiers, de la forme $4k+3$, intervient avec un exposant pair.
- Théorème fondamental de l'analyse: la dérivée par rapport à x de l'intégrale de la fonction f , prise entre une constante a et x , est égale à $f(x)$.
- Théorème de Liouville: le nombre $1/10^{11} + 1/10^{21} + 1/10^{31} + \dots$ est transcendant.
- Les nombres e et π sont transcendants.
- Théorème des nombres premiers: la densité des nombres premiers autour de n est $1/\log(n)$.
- Procédé diagonal de Cantor: les nombres réels ne peuvent se mettre en bijection avec les nombres entiers.
- Premier théorème d'incomplétude de Gödel.
- Théorème des quatre couleurs: toute carte géographique dessinée sur un plan peut être coloriée avec quatre couleurs de façon que deux pays voisins soient de couleurs différentes.
- Conjecture de Kepler sur l'empilement le plus dense de sphères dans l'espace.

... ET D'AUTRES NON

Les résultats suivants n'ont pas été contrôlés par des assistants de preuve, mais pour les deux premiers, les spécialistes sont d'accord pour considérer que la démonstration informelle disponible est satisfaisante.

- Le théorème de Fermat qui indique que l'équation $a^n + b^n = c^n$ n'a pas de solutions en nombres entiers positifs si $n > 2$.
- Le théorème géant concernant la classification des groupes finis simples, dont la démonstration actuelle occupe des dizaines de milliers de pages dispersées dans plus de cinq cents articles. On tente d'écrire une