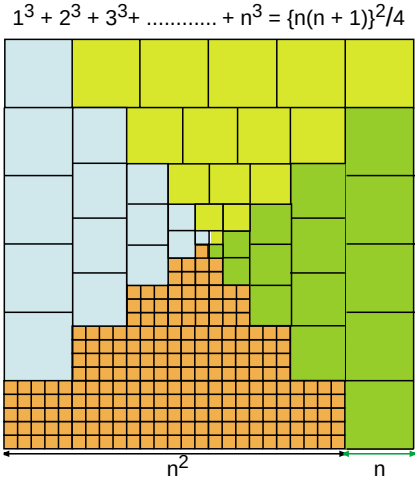

Raccourcis dans les démonstrations

JEAN-PAUL DELAHAYE

La concision risquée des preuves humaines contraste avec le bavardage impraticable des preuves formelles.

Comment savoir si une démonstration est juste ? On imagine qu'il suffit qu'un mathématicien prenne la peine de la lire soigneusement, ligne par ligne, après s'être informé des définitions et des résultats connus qui peuvent y être utilisés. Si certaines questions sont non résolues, ce qui bien sûr est le cas, nous saurions parfaitement lesquelles, et le travail des chercheurs consisterait uniquement à résoudre ces énigmes répertoriées. Partout en mathématiques régnerait la certitude.

Cette situation, si elle était vraie, opposerait catégoriquement les mathématiques à la physique où rien n'établit définitivement une théorie, laquelle n'est qu'une hypothèse susceptible d'être mise en cause par de nouvelles données. On sait ainsi qu'on ne prouve pas une loi physique, qui est un énoncé général, à partir d'observations et d'expérimentations, qui ne sont que des énoncés particuliers.

Les logiciens soutiendront la vision idéalisée des mathématiques en maintenant que, depuis le début du siècle, on dispose de systèmes codifiés pour écrire des démonstrations qu'on appelle des systèmes formels. Lorsqu'on écrit une preuve avec l'un de ces systèmes, un ordinateur peut en vérifier la justesse sans intervention humaine. La justesse d'une preuve formelle, disent les logiciens, est mécaniquement vérifiable et ne demande aucune intelligence. Or une multitude de raisons compliquent le tableau idéal et atténuent l'image trop belle d'une science mathématique sans états d'âme, sans disputes, sans erreurs où l'unanimité se ferait sur toute question et où les désaccords pourraient se régler en prenant des ordinateurs pour arbitres.

Nous allons évoquer les difficultés rencontrées pour écrire des démonstrations formelles mécaniquement vérifiables. Ces difficultés ne signifient pas que les systèmes codifiés pour l'écriture des démonstrations sont inutiles ou insatisfaisants – personne n'envisage aujourd'hui de s'en passer, et c'est à tort qu'on évoque les théorèmes d'incomplétude de Gödel comme arguments contre les formalismes *(voir les rubriques des mois de novembre et décembre 1999)*. Les difficultés signifient simplement que l'utilisation des formalismes logiques est beaucoup plus délicate qu'il n'y paraît et que le monde des mathématiques déborde d'une complexité qu'on ne sait pas, en pratique, enfermer dans les boîtes aseptisées que sont les systèmes formels des logiciens.

Dans l'introduction de son grand traité de mathématiques, Nicolas Bourbaki a exprimé très lucidement ce point de vue au cœur de la conception moderne des mathématiques : «...conservant toujours présente, comme une sorte d'horizon, la possibilité d'une formalisation totale, notre Traité vise à une rigueur parfaite. [...] Du fait que nous cherchons à nous tenir constamment aussi près d'un texte formalisé qu'il semble possible sans longueurs insupportables, la vérification, en principe, est aisée ; les erreurs (inévitables en pareille entreprise) peuvent être localisées sans excessive perte de temps, et le risque de les voir entacher de nullité un chapitre ou un Livre entier demeure très faible.»

Certaines figures de cet article reproduisent des démonstrations sans mots qui viendront compléter celles déjà proposées dans cette rubrique en février 1998. Ces démonstrations graphiques illustrent une idée forte : à côté de la présentation des démonstrations en langue vernaculaire ou formelle, une exposition silencieuse et géométrique des preuves mathématiques est parfois possible.

Les preuves réelles qu'écrivent les mathématiciens sont très différentes des preuves formelles pour une première raison : l'utilisation généralisée d'abréviations. Parmi les abréviations, il y a celles, bénignes, qui n'introduisent aucune ambiguïté. Le mathématicien indiquera par exemple que, pour gagner un peu

1. INDIGESTES SYSTÈMES FORMELS

$$\begin{aligned}
&*52{\cdot}2. \quad \vdash .\, 1 \subset \mathrm{Cls}\\
&\quad \textit{Dem.}\\
&\quad \vdash .*52{\cdot}1 . \supset \vdash : \alpha \in 1 . \supset . (\exists x) . \alpha = \iota' x .\\
&\quad [*51{\cdot}11] \qquad \supset . (\exists x) . \alpha = \hat{z}(z = x) .\\
&\quad [*20{\cdot}54] \qquad \supset . (\exists x, \phi) . \hat{z}(\phi ! z) = \hat{z}(z = x) . \alpha = \hat{z}(\phi ! z) .\\
&\quad [*10{\cdot}5] \qquad \supset . (\exists \phi) . \alpha = \hat{z}(\phi ! z) .\\
&\quad [*20{\cdot}4] \qquad \supset . \alpha \in \mathrm{Cls} : \supset \vdash . \mathrm{Prop}\\
&*52{\cdot}21. \quad \vdash . \Lambda \sim \in 1\\
&\quad \textit{Dem.}\\
&\qquad \vdash .*52{\cdot}16 . \supset \vdash : \alpha \in 1 . \supset . \exists ! \alpha :\\
&\quad [*24{\cdot}63] \quad \supset \vdash : \Lambda \sim \in 1
\end{aligned}$$

La codification des démonstrations rend celles-ci testables par ordinateur, mais pas très agréables aux humains. L'un des premiers systèmes entièrement codifiés de preuves est celui de B. Russell et A. Whitehead, qui ont essayé de rester le plus près possible du formalisme qu'ils définissaient. Voici un extrait de leur ouvrage *Principia Mathematica*, proposé ici pour en montrer l'intérêt... esthétique. On reconnaît en 52.21 un énoncé qui signifie que l'ensemble vide (le V retourné) n'est pas élément de 1 qui, par définition, dans ce système, est la classe de toutes les classes ayant un seul élément. Chaque énoncé est soigneusement justifié par sa preuve donnée juste après, qui en permet, en théorie, la vérification mécanique. Pas un mot n'apparaît.