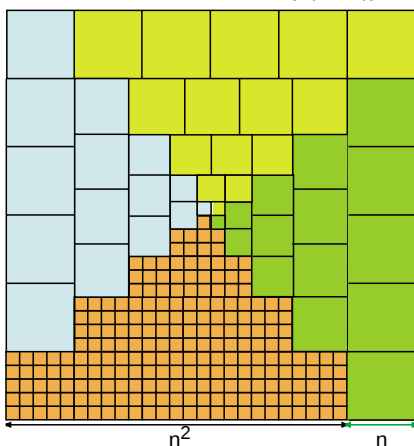


$$1^3 + 2^3 + 3^3 + \dots + n^3 = \{n(n+1)\}^2/4$$



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 sys-

tèmes 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

•52.2. $\vdash. 1 \in Cls$

Dem.

$\vdash. \bullet 52.1. \supset \vdash : \alpha \in 1. \supset. (\exists x). \alpha = t'x.$

[•51.11] $\supset. (\exists x). \alpha = 2(z=x).$

[•20.54] $\supset. (\exists x, \phi). 2(\phi!x) = 2(z=x). \alpha = 2(\phi!x).$

[•10.5] $\supset. (\exists \phi). \alpha = 2(\phi!x).$

[•20.4] $\supset. \alpha \in Cls : \supset \vdash. Prop$

•52.21. $\vdash. \Lambda \sim \epsilon 1$

Dem.

$\vdash. \bullet 52.16. \supset \vdash : \alpha \in 1. \supset. \exists ! \alpha :$

[•24.63] $\supset \vdash : \Lambda \sim \epsilon 1$

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.

2. LES ABUS DANS LES EXPOSÉS MATHÉMATIQUES...

Les raccourcis et omissions pratiqués lors d'exposés sont bien pires que ceux qu'on trouve dans les textes écrits. Des recensions humoristiques de ces abus ont plusieurs fois été proposées. En voici une, largement inspirée par celle de la revue *Plot* (APMEP Orléans-Tour, n° 86).

- Démonstration par l'évidence : «La démonstration est triviale» ; «Immédiat à partir des définitions» ; «On obtient sans peine que...» ; «On voit que...»
- Démonstration par la confiance : «Vous n'avez qu'à essayer, vous verrez, ça marche». Variante : «Je l'ai démontré hier chez moi, aucune difficulté.»
- Démonstration par consensus : «Tous ceux qui sont d'accord lèvent la main». Variante encore plus efficace : «Tous ceux qui ne sont pas d'accord lèvent la main.»
- Démonstration par commodité dénommée «nos désirs sont des réalités» : «Ce serait si beau si c'était vrai, donc...» (Redoutablement dangereuse.)
- Démonstration par nécessité : «Ça doit être vrai, sinon toutes les mathématiques s'effondreraient.» Variante : «Le cas contraire contredirait un résultat bien connu qui ne peut pas être faux.» (Peu de travail est nécessaire pour en tirer une bonne vieille preuve par l'absurde.)
- Démonstration par plausibilité : «Ça a l'air bon, donc ça doit être vrai.» (Très utilisé pour évaluer le résultat d'un long calcul ; ne pas en abuser.)
- Démonstration par intimidation : «Ne soyez pas stupide ! Bien sûr que c'est vrai.» Variantes du débutant : «Même un débutant sait ça» ; «Vous l'avez vu en sixième.» Variante du devoir pour demain : «Ceux qui en doutent feront la démonstration pour demain sur une feuille qu'ils me rendront.» Variante du tableau : «Si quelqu'un a des doutes, il passe au tableau le démontrer.»
- Démonstration par manque de temps : «Il ne me reste pas assez de temps, vous ferez la démonstration vous-même.»
- Démonstration par complexité : «La démonstration est trop compliquée pour être donnée ici.» Variantes : «Je ne peux pas vous le faire, car ça fait partie du programme de l'année prochaine.» «J'ai fait le calcul en 1985, c'est assez pénible, je n'ai pas envie de le refaire.»
- Démonstration par accident : «Tiens, tiens, qu'avons-nous



là...» (En fait, tout était calculé par avance pour obtenir le résultat prétendument inattendu.)

- Démonstration par la définition dite méthode du postulat d'Euclide : «On le définit comme vrai.» (En abuser risque de diminuer l'intérêt de votre cours.)
- Démonstration par la tautologie : «C'est vrai, parce que c'est vrai.» (Risque de vous faire perdre du crédit, mieux vaut utiliser une des autres méthodes.)
- Démonstration par référence : «Comme c'est établi à la page 289 du ...» (Là encore, si vous en abusez, vous viderez votre cours de sa substance.)
- Démonstration par perte de référence : «Je sais que j'ai vu la démonstration quelque part.» (Même si c'est du bluff, préférez la méthode précédente.)
- Démonstration par manque d'intérêt : «Y a-t-il quelqu'un qui souhaite vraiment voir la démonstration?» Variante en combinant avec la démonstration par complexité : «La démonstration est longue et pénible. Est-ce que je la fais?» Variante dite du calcul merdique : «En général, quand je me lance dans ce calcul, je me plante. On y va?»
- Démonstration par obstination : «Vous pouvez croire ce que vous voulez, moi je vous dis que c'est vrai.» Variante du contre-exemple : «Trouvez-moi un contre-exemple, en attendant je considère que c'est vrai.» (Contraire à la déontologie la charge de la preuve ne serait pas à celui qui affirme.)
- Démonstration par analogie : «C'est la même chose que...» ; «Il suffit de s'inspirer de...» «On procède comme pour...» (Moyen efficace d'obtenir des résultats faux : le procédé a coûté cher à de nombreux mathématiciens.)
- Démonstration par autorité : «Borsnuch l'a dit.» Variante dite de l'ascenseur : «J'ai rencontré Borsnuch dans l'ascenseur, et il est d'accord.»
- Démonstration par symbolisme excessif : « $\forall a > 0 \exists b > a$ $F(-A(a)) > 0 \wedge B(b)$ fi ...» Variante dite du renvoi multiple : «On conclut en combinant les lemmes 1, 3, 8 et 15 avec le théorème 12, puis en utilisant les propositions 7, 9 et 21.»
- Démonstration par appel à l'opinion publique : «Si c'était vrai ça se saurait, donc c'est faux...» (Contrairement aux apparences, ce procédé marche bien, car les résultats simples qui n'ont pas été démontrés sont généralement faux.)



J.-M. Thiriet

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 :

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

Imagine-t-on combien il serait pé

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 mathé-

matiques 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 $u \otimes v$ 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 pour-tant 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 linéaire* 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 omette, 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 sûr 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 délicate 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). Pour quoi 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.