A propos de l'intuition en mathématiques

Jean-Louis Krivine

krivine@irif.fr

13 février 2018

Je prends comme principe que le cerveau, humain ou autre, contient une masse de programmes qui forment un système d'exploitation et qui en font un « serveur », dont le « client » est le monde extérieur à l'organisme qu'il contrôle. Ce monde extérieur envoie des signaux, qui sont reçus par les capteurs correspondants et gérés suivant divers protocoles (visuels, auditifs, olfactifs, etc.).
Le mathématicien parvient à examiner certains de ces programmes dans son propre cerveau et à les transcrire sous forme de textes qui sont les « démonstrations ».
Il joue donc le rôle de « désassembleur », qui transforme le code binaire en un programme commenté écrit dans un langage de programmation évolué.
Première question : on sait comment récupérer un programme à partir d'une démonstration (correspondance preuves-programmes) mais il y a alors perte d'information. Pourquoi n'obtient-on pas directement des programmes ? Noter que l'information supplémentaire contenue dans la preuve constitue un « label de qualité » du programme sous-jacent.
Deuxième question : peut-on dire quelque chose du processus qui nous permet d'écrire ces démonstrations ? Noter qu'on n'écrit jamais de démonstrations formelles (celles qu'on peut directement transformer en programmes). D'ailleurs, la notion même de démonstration formelle est récente. On a toujours écrit les preuves sous forme intuitive. Ces appels à l'intuition servent la plupart du temps à masquer, consciemment ou non, des appels à des axiomes.
Or, la correspondance preuves-programmes est, en fait, constituée de deux parties :
la déduction formelle, c'est-à-dire l'application des règles logiques d'une part
et les axiomes d'autre part.
La correspondance de Curry-Howard permet de transformer mécaniquement l'application des règles de déduction en programme écrit dans un langage de programmation convenable (essentiellement le λ-calcul ou la logique combinatoire). Mais que faire des axiomes ? il faudrait leur associer des instructions dans ce langage, de façon à obtenir un ensemble cohérent, c'est-à-dire des programmes qui fonctionnent. Est-ce seulement possible ? Si l'on pense véritablement que les démonstrations mathématiques correspondent à des programmes déjà écrits dans le cerveau, la réponse est oui. Et, de fait,on y parvient pour la plupart des axiomes usuels des mathématiques (la théorie des ensembles) en se guidant à l'aide d'outils comme la *théorie de la réalisabilité* initiée par S.C. Kleene.

Or, les axiomes de la théorie des ensembles ont émergé, difficilement, avec essais et

erreurs, au début du 20ème siècle, en se basant essentiellement sur l'*intuition*, sur la *notion intuitive d'ensemble*. On considère comme intuitif que les parties d'un ensemble forment un ensemble (axiome des parties) ; que les éléments d'un ensemble qui ont une certaine propriété forment un ensemble (axiome de compréhension), etc.
Mais on a été obligé d'éliminer l'axiome plus général, pourtant assez intuitif : les ensembles qui ont une certaine propriété forment un ensemble. Pourquoi ? pour cause de contradiction (paradoxe de Russell) et donc, en fin de compte, d'impossibilité absolue de lui associer un programme.
Il est tout à fait étonnant que la théorie des ensembles de Zermelo-Frænkel, à laquelle a finalement abouti ce long processus basé sur l'intuition, se soit prêtée de si bonne grâce à la correspondance preuves-programmes. Cela en dit long sur la nature de l'intuition en mathématiques. J'en conclus que lorsqu'une notion mathématique me semble intuitive, c'est le signe que je suis capable de lire dans mon cerveau le programme correspondant ; ce qui ne veut pas dire que je suis capable de l'écrire. Mais il faut aussi que cette notion soit intuitive pour d'autres individus, il faut que l'intuition soit partagée. Dans ce cas, je peux avoir confiance que le programme correspondant à cette notion existe réellement dans le cerveau humain et que cette intuition n'est pas un mirage. On peut alors essayer d'appliquer tout ce qu'on sait, et de creuser tout ce qu'on ne sait pas, sur la correspondance preuves-programmes pour trouver cet objet mystérieux qui se cache derrière l'intuition.

Il y a un grand nombre d'exemples de ce type, où l'intuition précède l'axiomatisation, qui sont bien connus : on a une intuition de la droite réelle, de la géométrie, de la notion de probabilité, etc. On n'a pas attendu l'axiomatisation pour raisonner avec ces notions, les démonstrations faisant appel à des axiomes non formulés. Les théorèmes obtenus ainsi permettent néanmoins de faire des calculs utilisables, ce qui veut dire que, sans même connaître les axiomes, on avait deviné les programmes qui leur sont associés.

Il y a une autre façon d'utiliser l'intuition, qui est très intéressante et absolument universelle : c'est la capacité du mathématicien de lire et d'écrire des démonstrations non formalisées (alors qu'il nous est impossible de manipuler des preuves formelles). Pour cela, on s'appuie sur le raisonnement sémantique, c'est-à-dire qu'on pense en termes de *modèles*. Cela permet d'éliminer énormément de pas de démonstration formalisée. Il s'agit bien d'intuition partagée, car personne ne pense une seconde à essayer de rétablir les chaînons formels qui manquent et néanmoins tout le monde (mathématique) comprend la preuve. C'est cette forme d'intuition qui rend possible la communication entre mathématiciens.
Or l'équivalence entre les notions de conséquence syntaxique et sémantique est l'objet d'un théorème essentiel de logique : le *théorème de complétude* qui affirme qu'une formule vraie dans tout modèle est formellement démontrable (la réciproque étant triviale).
Ce n'est pas qu'il soit très difficile à démontrer, mais il est quand même très surprenant. En effet, il nous donne l'intime conviction que les règles de la logique formelle sont complètes. Autrement dit, malgré l'extrême variété des méthodes de démonstration utilisées dans tous les domaines des mathématiques, et de toutes celles qu'on pourra imaginer dans le futur, il n'y aura jamais besoin d'ajouter quoi que ce soit aux quatre

ou cinq malheureuses règles énoncées dans ce théorème pour pouvoir tout formaliser. Comment se fait-il même qu'on puisse *démontrer* une chose pareille ?

La compréhension intuitive qu'on a de ce théorème me paraît être l'exemple fondamental de l'intuition mathématique. Plus généralement, c'est l'intuition qui nous permet de *comprendre* une démonstration sans avoir à écrire une preuve formelle que, d'ailleurs, on ne pourrait jamais lire. En effet, ce théorème fait le lien entre la *sémantique* et la *syntaxe*. En général, la sémantique s'occupe de la signification des formules, de leur sens. Mais ici, plus précisément, elle parle de *modèles*.
Quand je cherche à montrer ou seulement à comprendre un théorème dans une théorie (par exemple la théorie des corps réels clos, ou la théorie des ensembles) je ne vois pas les axiomes et les règles de déduction mais j'imagine un modèle (un corps réel clos ou un modèle de ZF). En fin de compte, le cerveau produira une démonstration formelle, mais on ne la voit pas ; de même qu'ayant écrit un programme en langage évolué, on ne voit (presque) jamais le résultat de la compilation.
Le problème de l'intuition est donc celui du rapport *sémantique / syntaxe* ou encore, par la correspondance de Curry-Howard, *langage évolué / langage machine*.

Notre intuition pour la notion d'*ensemble* provient vraisemblablement du réseau qui est à la base du fonctionnement du cerveau. Je vais me référer à Internet car il se développe très probablement en imitation (inconsciente) de ce réseau.
En théorie des ensembles, il y a une relation d'équivalence fondamentale : *l'extensionnalité*. Deux ensembles sont équivalents si (et seulement si) ils ont les mêmes éléments. Je pense que cette équivalence correspond à la mise en relation de deux nœuds du réseau : toute information située dans l'un est connue de l'autre.
Les programmes provenant des preuves mathématiques usuelles, en théorie des ensembles, sont valables sous cette condition. Par exemple, la théorie des ondelettes va me donner un programme de compression d'image. On a besoin d'appliquer ce programme à un fichier video qui est dispersé en morceaux sur plusieurs sites. Pour cela, on doit supposer que ces sites sont reliés entre eux par le réseau, c'est-à-dire sont extensionnellement équivalents. Le programme n'est applicable qu'à cette condition et ne se préoccupe pas de savoir comment réaliser ces connexions. Voilà pourquoi l'axiome d'extensionnalité est nécessaire en analyse, par exemple.
Mais les programmes qui permettent d'effectuer la mise en relation de deux sites correspondent, bien sûr, à des démonstrations dans une théorie où *il n'y a pas d'extensionnalité*. On a donc été naturellement (mais toujours inconsciemment) amené à généraliser et à considérer une théorie des ensembles sans axiome d'extensionnalité. Analogie avec l'introduction des géométries non euclidiennes.
On peut aussi remarquer que la distinction entre *ensembles* et *classes* est très apparente dans le réseau Internet. Un ensemble est un groupe de sites que l'on peut relier à un même nœud du réseau, au cours d'une session de communication par exemple, ou pour effectuer un calcul, ou une attaque par déni de service. C'est évidemment hors de question pour l'ensemble de tous les sites, qui est beaucoup trop gros pour cela et n'existe donc pas comme ensemble mais comme classe. C'est la traduction concrète du paradoxe de Russell.