Ensembles et preuves

Jean-Louis Krivine

Equipe de Logique mathématique, Université Paris VII, C.N.R.S.

e-mail krivine@logique.jussieu.fr

(Séminaire de logique à la Sorbonne, 18 Février 1997)

Le thème général de ce séminaire est : " Qu'est-ce qu'*une* logique ? ", mais pour cet exposé, ce sera :" Qu'est-ce que *la* logique ? ", ce qui me convient beaucoup mieux, parce que je n'en connais qu'une. Comme je suis mathématicien, cela sera même, de façon encore plus restrictive : " Qu'est-ce que la logique mathématique ? "

Qu'est-ce donc que la logique ? La motivation initiale est sans aucun doute, pour le logicien, de comprendre la nature des mathématiques. Il s'agit donc, en quelque sorte, d'un travail d'entomologiste : on observe l'activité du mathématicien, et on en fabrique un modèle, qui sera, bien sûr, un modèle mathématique. Notons tout de même qu'en l'occurrence, l'observateur et l'observé sont en général une seule et même personne.

Or, l'activité mathématique consiste visiblement à produire des démonstrations à partir d'axiomes. Ces deux objets, axiomes et preuves, sont assez indépendants, dans le sens qu'on peut changer d'axiomes en gardant les mêmes règles de démonstration, ou, au contraire, conserver les axiomes et changer les règles. C'est donc de façon naturelle que la recherche en logique s'est graduellement scindée en deux branches bien distinctes, pour tenter de répondre à ces deux questions :

• Qu'est-ce qu'une preuve mathématique ? et, pour commencer, que peut-on dire de sa structure, quelles sont les bonnes règles de déduction ? comment peut-on passer d'une preuve à une autre ?, etc. Ainsi est apparue la *théorie des démonstrations*, avec Hilbert, Gödel (théorèmes de complétude et d'incomplétude), Gentzen (élimination des coupures), Church, Curry (invention du λ-calcul), ...

• Quels axiomes faut-il poser pour qu'en utilisant ces règles de démonstration, on retrouve les raisonnements habituels du mathématicien, la vie quotidienne mathématique, en quelque sorte ? On s'est d'abord limité à l'arithmétique, et il s'agissait alors de trouver les axiomes pour les nombres entiers, ce qui a été fait par Peano. Mais on s'est aussi posé le problème en toute généralité, de trouver des axiomes pour toutes les mathématiques passées, présentes et futures, et cela a donné la *théorie des ensembles*, et divers avatars comme la théorie des types. Cantor, Frege, Russell, Zermelo, Von Neumann,... ont contribué à poser les bons axiomes et à développer la théorie. Puis Gödel et Cohen ont inventé des méthodes très puissantes pour passer d'un système d'axiomes à un autre, en théorie des ensembles. On en reparlera tout à l'heure.

Pour tenter de répondre à la question initiale : " Qu'est-ce que la logique ? ", je vais bien sûr m'appuyer sur les résultats mathématiques élaborés dans ces deux théories, et il

faut donc commencer par vous expliquer en quoi ils consistent, en évitant cependant de vous assommer en entrant dans la technique. La tâche n'est pas si facile, d'autant qu'il s'agit parfois de résultats fort récents, ou même de recherches en cours. Toutefois, cela vaut la peine d'essayer, car j'espère parvenir à vous montrer à quel point ce domaine, ces recherches, et les perspectives qu'ils ouvrent, sont passionnants.

Remarquons toutefois que des résultats mathématiques, si intéressants soient-ils, ne peuvent, par eux-mêmes, apporter une réponse à une question extra-mathématique. Il faut, de plus, interpréter ces résultats dans le monde réel ; c'est ce qu'on fait tout le temps en physique. Par exemple, si l'on se donne l'équation : $f = Kmm'/d^2$, on en déduira mathématiquement des trajectoires (des coniques, dans le cas le plus simple). Mais il faut *décider* que cette équation représente la loi de la gravitation dans le monde réel, pour pouvoir confronter ces trajectoires à celles des planètes, des fusées et des satellites. De toute évidence, cette décision, qui n'a rien de mathématique, donne un relief extraordinaire à cette équation toute simple.

La réponse à notre question s'obtiendra donc en confrontant les résultats mathématiques dont j'ai parlé, à des phénomènes réels. Mais lesquels ? Je ne le dirai pas tout de suite, car cela apparaîtra plus naturellement dans la suite de mon exposé. Il est clair, cependant, que l'informatique va jouer un grand rôle dans cette interprétation. Il me faudra donc aussi vous parler de quelques notions générales sur les systèmes informatiques.

I. Sur les preuves mathématiques

Le résultat fondamental est le *théorème de complétude* de Gödel. Son intérêt est double : d'une part, il montre que la déduction mathématique est mécanisable, c'est-à-dire réductible à un petit nombre de règles simples, qu'on peut très bien apprendre à une machine. Ce n'est nullement évident, et on a cru longtemps que seul un être humain pouvait raisonner mathématiquement, et qu'il apparaîtrait toujours des modes de raisonnement nouveaux, non réductibles aux anciens. Il est tout à fait étonnant que cette question soit définitivement réglée par un théorème.

Un exemple bien connu de règle de déduction est le *modus ponens* qui s'énonce ainsi : si, à partir d'un système d'axiomes, on a déduit les deux formules A et $A \to B$, alors on peut déduire B de ce système d'axiomes. Un autre exemple, tout à fait trivial, est que, si la formule A fait partie d'un système d'axiomes, alors on peut déduire A de ce système d'axiomes. Le théorème de complétude montre que toute déduction, à partir d'un système d'axiomes quelconque, peut s'effectuer au moyen de ces règles et quelques autres du même genre.

Le deuxième point intéressant, à propos du théorème de complétude, est, bien entendu, qu'il donne l'équivalence de la syntaxe et de la sémantique : autrement dit, une formule est conséquence d'un système d'axiomes si, et seulement si, elle est vraie dans tous les *modèles* de ce système d'axiomes, c'est-à-dire toutes les structures qui vérifient ce système d'axiomes. Nous reviendrons sur cette notion essentielle de modèle quand nous parlerons de la théorie des ensembles. Donnons un exemple simple. Le système d'axiomes pour une relation d'ordre est formé des trois formules suivantes :

$$\forall x(x \leq x);\ \forall x \forall y(x \leq y \wedge y \leq x \to x = y);\ \forall x \forall y \forall z(x \leq y \wedge y \leq z \to x \leq z).$$

Elles expriment respectivement la réflexivité, l'antisymétrie et la transitivité pour une relation binaire notée $\leq$. Alors la formule $\forall x \forall y \forall z (x \leq y \wedge y \leq z \wedge z \leq x \rightarrow x = y)$ est conséquence de ce système d'axiomes, ce qui veut dire qu'on peut la déduire au moyen des règles. Mais, au lieu de chercher une telle déduction, ce qui n'est pas facile, on peut aussi bien se contenter de prendre un modèle arbitraire des axiomes ci-dessus, c'est-à-dire un ensemble ordonné quelconque, et de montrer que la formule considérée y est satisfaite. Voila exactement ce qu'affirme le théorème de complétude.

Une deuxième découverte fondamentale de la théorie des démonstrations est ce qu'on appelle la *correspondance de Curry-Howard*. On s'est aperçu qu'à chaque démonstration, effectuée au moyen des règles de déduction dont je viens de parler, on pouvait associer un *programme* au sens informatique du terme. Cela se passe de la façon suivante : une démonstration consiste en une suite d'applications des règles de déduction, à partir des axiomes ; un programme, d'autre part, est une suite d'instructions élémentaires, adressées au processeur d'une machine. Si l'on parvient à associer une instruction à chaque règle de déduction, on aura transformé chaque preuve en une suite d'instructions, c'est-à-dire en un programme. Or, c'est exactement ce que fait la correspondance de Curry-Howard ; reprenons, comme exemple de règle, le modus ponens, qui nous permet, à partir d'une démonstration D_A de la formule A, et d'une démonstration $D_{A \rightarrow B}$ de $A \rightarrow B$, d'obtenir une démonstration D_B de B. L'instruction associée à cette règle prend les programmes P_A et $P_{A \rightarrow B}$ qui sont déjà associés aux démonstrations D_A et $D_{A \rightarrow B}$, et donne le programme $P_B = P_{A \rightarrow B}(P_A)$ obtenu en passant P_A en argument au programme $P_{A \rightarrow B}$. Autrement dit, l'instruction associée au modus ponens est ce qu'on appelle l'*application*, c'est-à-dire l'opération d'appliquer une fonction (un programme) à son argument.

On peut faire de même pour chacune des règles de déduction, et on a ainsi un moyen très simple de fabriquer un programme à partir d'une démonstration quelconque. C'est là un résultat inattendu, et bien évidemment d'une importance capitale en logique. Il est essentiel également pour la question qui nous occupe aujourd'hui : " Qu'est-ce que la logique ? ". Grâce au lien étroit qu'il établit entre logique et informatique, nous disposerons, en effet, d'un puissant outil d'analyse pour répondre à notre question. Nous allons considérer cela de plus près.

Malheureusement, il y a un problème de taille à régler d'abord. Car, si la transformation des preuves en programmes paraît établie, il y a tout de même un os ! Il faut se rappeler, en effet, que, pour construire une démonstration mathématique, il ne suffit pas de connaître les règles de déduction : il faut aussi se donner un système d'axiomes. Pour pouvoir transformer effectivement une preuve en un programme, il faut donc savoir associer un programme convenable à chaque axiome du système. Comment peut-on faire ? La correspondance de Curry-Howard, et, en général, la théorie des démonstrations, ne nous donne pas la moindre lumière sur cette question. Elle ne nous indique même pas où chercher ce système d'axiomes ; elle suppose, en effet, qu'il est donné, de façon absolument arbitraire d'ailleurs. Mais, si nous voulons faire des mathématiques, il est bien évident que nous n'allons pas prendre nos axiomes au petit bonheur la chance, mais bien au contraire, les choisir avec le plus grand soin. Qui va nous dire comment ? Cette question est, bien sûr, vitale pour mener à bonne fin notre correspondance entre preuves et programmes. La réponse va venir d'un tout autre côté, d'une autre branche de la logique, que l'on appelle *la théorie des ensembles*.

II. Sur la théorie des ensembles

Chaque fois que se développe une théorie mathématique, il vient un moment où l'on éprouve le besoin d'*axiomatiser* cette théorie, c'est-à-dire d'expliciter les hypothèses sur lesquelles s'appuie le raisonnement. Ces hypothèses, ce sont les *axiomes* de la théorie. Cela remonte très loin dans l'histoire des mathématiques ; par exemple, tout le monde connaît le système d'axiomes donné par Euclide pour la géométrie qui porte son nom. Cette nécessité d'axiomatiser, c'est tout simplement la nécessité de la rigueur, sans laquelle le raisonnement mathématique finit par s'enliser et se bloquer complètement.

Au 19ème siècle est apparue l'idée de rechercher des axiomatiques pour des théories de plus en plus générales, dans un but évident d'efficacité et d'unification. Dedekind et Peano ont cherché à axiomatiser la notion de nombre entier, car il apparaît clairement que la plupart des notions mathématiques se ramènent à celle-là. Enfin, l'unification complète des mathématiques dans une seule et même axiomatique a été réalisée avec la théorie des ensembles, due à G. Cantor, puis développée sous diverses formes par Russell, Zermelo, Von Neumann, Frænkel,... Un consensus général s'est maintenant réalisé autour du système d'axiomes dit de Zermelo-Frænkel (ZF en abrégé), pour la théorie des ensembles.

Remarque. On pourrait trouver bizarre de parler de consensus en mathématiques, puisque ce n'est pas le mode de fonctionnement habituel de cette science : un théorème est accepté, non par consensus, mais parce qu'on le démontre. Par exemple, cela fait longtemps que tous les mathématiciens sont d'accord pour penser que le théorème de Fermat ou l'hypothèse de Riemann sont vrais. Cela ne suffit pas pour qu'on les admette, et c'est toute la différence entre une conjecture et un théorème. Mais la recherche d'un système d'axiomes n'est pas, à proprement parler, un problème mathématique. Il n'est pas question de *démontrer* que la théorie de Zermelo-Frænkel est le seul système d'axiomes convenable pour développer les mathématiques, et d'ailleurs ce n'est pas vrai. On peut en imaginer une foule d'autres, et on en utilise couramment plusieurs, par exemple la théorie des types finis, l'arithmétique du second ordre, la théorie de Zermelo, celle de Von Neumann-Bernays-Gödel, etc. Simplement, les qualités de commodité et d'élégance de la théorie de Zermelo-Frænkel en ont fait, en quelque sorte, un *standard*. Cette idée de " standard " est à retenir pour la suite, quand nous chercherons à saisir ce qu'est vraiment la théorie des ensembles.

Nous savons donc maintenant pourquoi la théorie ZF a été élaborée : le but était la rigueur et l'unification ; il s'agissait de donner un système d'axiomes valable pour toute théorie mathématique, et ce but a été atteint. Est-ce que l'histoire s'arrête là ? Non, bien sûr. Au contraire, c'est ici que les choses deviennent amusantes et, disons-le, un peu surprenantes.

En effet, dorénavant, si je me pose un problème mathématique, je n'ai plus qu'à l'écrire comme une formule Φ de théorie des ensembles, et chercher à déduire Φ au moyen des axiomes de ZF et des règles de déduction logique dont nous avons déjà parlé. Mais alors l'idée vient tout naturellement d'appliquer le théorème de complétude, et le problème se ramène à montrer que Φ est vraie dans tous les modèles de ZF. Et c'est ici qu'apparaît, pour la première fois, un objet vraiment extraordinaire, la structure la plus exotique dont on ait jamais parlé en mathématiques : *un modèle de la théorie de Zermelo-Frænkel.*

Avant de vous montrer à quoi ça ressemble, il vaut mieux insister sur le fait que ces " monstres " n'ont pas été inventés de toutes pièces par un mathématicien fou, mais sont au contraire le fruit d'une recherche de longue haleine, tout à fait raisonnable et d'ailleurs réussie, dont le but était l'efficacité et l'unification des mathématiques. Le problème va donc se poser, de comprendre comment une démarche aussi sensée a pu aboutir à un résultat pareil.

Les formules de théorie des ensembles sont écrites avec, en plus des symboles logiques habituels, un seul et unique symbole $\in$, appelé symbole d'appartenance. Pour mémoire, les symboles logiques habituels sont les connecteurs propositionnels : $\vee, \wedge, \rightarrow, \neg$, les quantificateurs : $\exists, \forall$, les variables $x, y, z, \ldots$, et le symbole d'égalité $=$; mais ils sont valables pour n'importe quelle théorie, seul le symbole $\in$, qui représente une relation binaire, est spécifique à la théorie des ensembles.

Un modèle de la théorie de Zermelo-Frænkel est donc une structure définie par une relation binaire ; c'est ce qu'on appelle un *graphe orienté*. On peut en donner une représentation en considérant un ensemble de points dont certains sont reliés par des flèches. C'est un objet mathématique très courant, mais nous allons voir que le cas qui nous occupe est un peu spécial. Tout d'abord au point de vue terminologie : le graphe s'appelle *univers*, les points du graphe s'appellent naturellement *ensembles*, et s'il y a une flèche qui va du point a au point b, on dira, bien entendu que $b \in a$ (l'ensemble b est élément de, ou appartient à, l'ensemble a).

Mais, de plus, ce graphe doit vérifier les axiomes de ZF. Ceux-ci ne font qu'exprimer des propriétés " évidentes " de la notion intuitive d'ensemble, et paraissent donc tout à fait anodins et triviaux. Il est d'autant plus étonnant de constater les incroyables contorsions qu'ils imposent à notre malheureux graphe, pour qu'il parvienne à se plier à leurs directives. Voyons cela en examinant deux ou trois axiomes de ZF.

Le premier axiome, qui s'appelle *axiome d'extensionnalité*, s'énonce : deux ensembles qui ont les mêmes éléments sont égaux. Rien de plus banal. La formule correspondante s'écrit : $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$. Il impose à notre graphe d'avoir la propriété suivante : étant donnés deux points distincts quelconques, il y a une flèche issu de l'un qui n'aboutit pas à l'extrémité d'une flèche issu de l'autre. C'est déjà une condition assez forte, puisque beaucoup de graphes ne la satisfont pas (par exemple la relation binaire toujours fausse, sur un ensemble ayant au moins deux éléments), mais facile à réaliser tout de même.

Les autres axiomes de ZF nous indiquent quels sont les procédés autorisés pour fabriquer un ensemble à partir d'ensembles donnés. Par exemple, *l'axiome de la paire* nous permet, étant donnés deux ensembles, d'en construire un troisième, qui aura exactement ces deux ensembles comme éléments. Là encore, c'est intuitivement évident. Cela s'écrit en formule : $\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y)$.

Mais, en considérant le graphe, on voit que la situation se complique passablement : car l'application répétée de cet axiome nous permet de construire sans arrêt de nouveaux points, en l'appliquant à tous ceux qu'on a déjà obtenus ; et cette situation va se répéter avec les autres axiomes, en se compliquant encore puisqu'ils interagissent entre eux. Autre exemple, *l'axiome de la réunion* permet à partir d'un ensemble donné d'en construire un autre, qui a comme éléments les éléments des éléments du premier. Pourquoi pas, en effet ? La formule s'écrit : $\forall x \exists y \forall z (z \in y \leftrightarrow \exists u (u \in x \wedge z \in u))$. En regardant l'effet

produit sur le graphe, on s'aperçoit que la situation est devenue assez inextricable. Et ce n'est rien, en comparaison de ce qui va se passer avec les derniers axiomes de ZF, qui portent les jolis noms d'axiomes des parties, de l'infini, et du remplacement.

Quel est, en fin de compte, le résultat ? Un modèle de ZF se présente comme un fouillis invraisemblable de liens, dont la complexité défie l'imagination. Mais après tout, me direz-vous, les mathématiques sont faites, justement, pour apporter ordre et clarté dans les situations les plus tordues. Laissons faire les mathématiciens, et ils ne tarderont pas à découvrir la simplicité profonde qui se cache sous l'apparente complication.

Hélas, ce bel optimisme est balayé par le verdict sans appel du théorème d'incomplétude de Gödel : *il est impossible de démontrer l'existence d'un modèle de ZF !* Cela veut bien dire que la situation est grave ; en effet, de deux choses l'une :

• Ou bien il n'en existe pas, et alors la théorie des ensembles, mise au point avec tant d'efforts et de temps, s'effondre lamentablement dans la contradiction.

• Ou bien il existe un modèle de ZF, mais toute tentative d'en donner une description complète est vouée à l'échec.

Entre deux maux, il est raisonnable de choisir le moindre, c'est-à-dire le deuxième. Plutôt que de tuer les mathématiques, il vaut mieux accepter la présence de ces animaux bizarres ; les logiciens ont donc appris à vivre avec, ils ont étudié leurs mœurs, leur mode de reproduction, la diversité des espèces (Gödel et Cohen en ont découvert plusieurs), et ils ont même tenté de les apprivoiser. Bien qu'il ne s'agisse visiblement pas d'une espèce menacée, beaucoup de monde s'est occupé d'eux, et la littérature sur le sujet est maintenant très riche et fort intéressante. C'est là ce qu'on appelle aujourd'hui la théorie des ensembles.

Je voudrais maintenant revenir au problème évoqué tout à l'heure : il semblerait que ces étranges structures, qui sont pourtant apparues naturellement en mathématiques, et dont l'intérêt n'est mis en doute par personne, ne se rattachent, de près ou de loin, à aucun phénomène concret connu. Mais, après tout, cela a été souvent le cas dans l'histoire des mathématiques ; par exemple, les coniques ont été inventées et étudiées bien avant que l'on découvre que les planètes décrivent des ellipses, les comètes des hyperboles, et les boulets de canon des paraboles. Alors, de quels objets naturels nous parlent donc les modèles de ZF ? Je crois que la réponse va de soi, si l'on observe :

d'un côté, qu'ils sont apparus au moment précis où l'on a réussi à comprendre comment fonctionne le raisonnement mathématique, activité qui se déroule très vraisemblablement dans le cerveau du mathématicien ;

d'autre part, qu'il s'agit d'un réseau très complexe de connexions, qui rappelle irrésistiblement le fouillis apparent des neurones dans le cerveau. On sait, par exemple, qu'un modèle de ZF est organisé en couches successives, ce qui fait, bien entendu, penser aux couches de neurones. Cela est dû à l'un des axiomes, appelé *axiome de fondation*, et l'ordre de ces strates est d'ailleurs excessivement complexe, puisqu'il est décrit par les *ordinaux* du modèle.

Finalement, si l'on cherche un objet naturel et répandu, dont la structure soit aussi sophistiquée que celle d'un modèle de la théorie des ensembles, on aboutit forcément à la conclusion suivante : un tel modèle ne peut être qu'une représentation détaillée d'un ensemble de connexions entre neurones, dans le cerveau humain ; il s'agit, en quelque sorte, d'un schéma, un peu comme celui d'une installation électrique. De plus, cet ensemble de

neurones doit occuper une position assez stratégique, puisqu'il est sans doute responsable de l'activité raisonnée. Si c'est bien le cas, l'intérêt pour ces structures est, on l'imagine, amplement justifié.

III. Les programmes derrière les preuves

Mais revenons maintenant à nos moutons, c'est-à-dire la transformation des preuves en programmes. Nous avons vu que cette transformation sera établie si nous parvenons à savoir quels programmes il faut associer aux axiomes de la théorie des ensembles. Ceci a été résolu, il y a longtemps, pour une théorie plus faible que ZF, à savoir " l'Arithmétique du second ordre ", qui suffit d'ailleurs, pour axiomatiser une bonne partie des mathématiques (ce qu'on appelle " l'Analyse "). Les programmes obtenus sont on ne peut plus simples : il y a un seul axiome (en fait, un schéma d'axiomes, appelé *schéma de compréhension*), et le programme associé consiste à ne rien faire !

Cependant, l'Analyse, ce n'est pas toutes les mathématiques, loin de là, et la question garde tout son intérêt pour ZF. C'est seulement tout récemment qu'elle a été résolue, et l'on constate alors que les programmes obtenus pour les axiomes de ZF sont bien loin d'être triviaux, comme dans le cas précédent. En fait, leur écriture est si compliquée que, pour le moment du moins, on n'a pas la moindre idée de la tâche qu'ils accomplissent quand on les exécute.

Il est temps de faire un peu le point, après toutes ces péripéties. Le bilan est le suivant : nous savons associer des programmes aux axiomes de la théorie des ensembles, et aussi aux démonstrations faites à partir de ces axiomes. Comme toutes les mathématiques sont formalisées dans ZF, nous savons donc associer, à un théorème quel qu'il soit, un programme, et même plusieurs, puisqu'un théorème peut être démontré de diverses façons.

Nous avons donc devant nous un ensemble de programmes, issus les uns des axiomes de ZF, les autres des théorèmes, et qui, en quelque sorte, résument toute la logique (au moins la théorie des ensembles et la théorie des démonstrations). Pour répondre à notre question initiale : " Qu'est-ce que la logique ? ", il ne nous reste plus qu'à déterminer ce que peuvent bien faire ces programmes, à quoi sont-ils donc destinés ?

Qu'avons-nous donc gagné, me direz-vous, en établissant ce pont qui va de la logique vers l'informatique, puisque nous avons transformé notre question, fort difficile, en une autre, qui ne l'est sans doute pas moins ? Eh bien, un pont peut être traversé dans les deux sens, et on peut penser que beaucoup de notions et d'outils informatiques vont avoir leur contrepartie en logique, et que ce qui est mystérieux ou incompréhensible du côté logique, pourrait bien être parfaitement clair du côté informatique (et vice-versa, d'ailleurs, mais ce n'est pas notre propos aujourd'hui).

Cela se vérifie immédiatement pour le problème qui nous occupe, et il y a une notion bien connue en informatique, qui a visiblement un rapport étroit avec les questions que nous nous posons : c'est celle de *système d'exploitation*. Vous en avez sûrement déjà entendu parler, et des expressions barbares comme MS-DOS, UNIX, Windows 95, Linux, OS2, etc, vous rappellent sans doute quelque chose.

Qu'est-ce qu'un système d'exploitation ? C'est un ensemble de programmes, qui est à la base du fonctionnement d'un ordinateur, puisqu'il fait le lien entre ses différents organes (mémoire vive, mémoire de masse, clavier, console, réseau, périphériques divers,

etc) et l'utilisateur. Un ordinateur sans système d'exploitation est totalement inutilisable. Entendons-nous bien, une même machine peut fonctionner avec différents systèmes, le choix se faisant à l'initialisation (à l'allumage si vous préférez). Dans le jargon informatique, on dit qu'on boote sous UNIX, ou sous Windows, par exemple.

Un programme utilitaire (ou programme d'application, comme un éditeur, ou un tableur) est adapté à un système d'exploitation donné et un seul (on dit qu'il *tourne* sous UNIX, ou sous DOS). En fait, un tel programme est essentiellement constitué à l'aide des programmes mêmes tirés du système d'exploitation (que l'on nomme des *appels système*), combinés à l'aide d'instructions élémentaires.

Essayons de transposer ces notions en logique, en traversant notre pont en sens inverse. Le système d'exploitation devient un certain ensemble d'énoncés mathématiques, qui correspondent aux appels système, les instructions élémentaires deviennent des règles de déduction, et notre tableur devient un énoncé mathématique obtenu à l'aide de ces règles, à partir des énoncés précédents. Autrement dit :

La notion de système d'exploitation correspond à celle de système d'axiomes (tiens, tiens, c'est le même mot), la notion de programme d'application correspond à celle de théorème. Et de même qu'un programme ne peut tourner que dans un système donné, de même un théorème n'a de sens que dans un système d'axiomes donné (essayez donc d'utiliser un théorème de géométrie euclidienne dans un espace hyperbolique).

Rappelons-nous les divers systèmes d'axiomes possibles pour faire des mathématiques : arithmétique de Peano, arithmétique d'ordre supérieur, théorie de Zermelo, ZF, NBG, etc. Ils correspondent donc à autant de systèmes d'exploitation, sous lesquels notre " ordinateur personnel " va pouvoir tourner, c'est-à-dire raisonner. Et la théorie de Zermelo-Fraenkel est devenue plus ou moins un " standard ", de la même façon que parmi les systèmes d'exploitation, un ou deux d'entre eux se sont imposés comme standards (en l'occurrence UNIX et Windows) soit par leurs qualités propres, soit par la puissance commerciale.

Or, comme nous l'avons vu, on a réussi à écrire les programmes qui correspondent aux axiomes de ZF, et la question est maintenant de déterminer ce qu'ils font. Nous nous retrouvons donc dans la situation d'un programmeur, qui a devant lui un ordinateur en état de marche, qui peut lire les programmes système, mais ceux-ci ne sont pas documentés, et il voudrait bien les comprendre. Cette tâche, fort malaisée en général, est assez courante en informatique, et on l'appelle *désassemblage*. Elle nécessite beaucoup d'astuce et de flair de la part du programmeur, et ne peut en aucun cas être réalisée par un programme, ce qu'on comprendra facilement. Mais on peut se faire aider dans ce travail par un programme convenable, qui réalisera à la demande (c'est pourquoi on dit qu'il est *interactif*) une foule d'opérations de recherche et de classification systématiques et répétitives, qui permettra une exécution en pas à pas, etc. En fait, un tel programme, qui porte donc naturellement le nom de *désassembleur interactif*, est absolument indispensable pour effectuer ce genre d'opération.

Voilà bien notre chance, il nous faut réaliser un désassemblage, sans avoir de désassembleur à notre disposition, nous sommes foutus. Mais, au fait, peut-être en cherchant bien, pourrait-on en trouver un au fond d'un tiroir ? Raisonnons un peu, en repassant notre fameux pont dans le sens informatique vers logique ; puisqu'un désassembleur est un programme d'application, ce qu'il nous faut dénicher, c'est un théorème qui fasse l'affaire.

Mais lequel est-ce ? des théorèmes, il y en a quand même beaucoup ; et existe-t-il seulement, cet oiseau rare ?

Pour résoudre cette devinette, il faut chercher tout ce que l'on peut dire à propos de cet hypothétique théorème. C'est certainement un théorème important, et comme le programme associé est un désassembleur, donc proche du système d'exploitation, il s'agit probablement d'un théorème de logique. Comme tout théorème qui se respecte, il doit avoir une hypothèse et une conclusion. Or, dans la correspondance de Curry-Howard, les hypothèses, ce sont les données, et la conclusion, c'est le résultat de l'exécution du programme. Mais quel est le résultat de l'exécution d'un désassemblage ? C'est un programme documenté ; en passant par le pont Curry-Howard, cela devient la démonstration d'une formule F. Quel est donc le théorème célèbre, dont la conclusion est : " il existe une démonstration de F " ? Tous les logiciens vous le diront : c'est le théorème de complétude de Gödel ! Il s'énonce en effet : *Si tout modèle satisfait la formule F, alors il existe une démonstration de F.*

Et voilà, il ne reste plus qu'à décortiquer le programme associé à une preuve du théorème de complétude, pour s'apercevoir qu'en effet, celui-ci se comporte exactement comme un désassembleur interactif.

Il vaut la peine de s'arrêter un peu sur ce résultat, qui est intéressant à plus d'un titre. D'abord, il est plutôt inattendu, car il n'y a aucun rapport, semble-t-il, entre l'énoncé du théorème de complétude et le désassemblage (opération qui n'existait d'ailleurs pas, et pour cause, quand Gödel découvrit le théorème). Quel rapport mystérieux y a-t-il donc entre un théorème mathématique, et les programmes qui se cachent derrière ses démonstrations ? Il faut bien dire que l'on n'en sait rien, et c'est l'un des charmes de la recherche dans ce domaine, on a toujours une surprise.

Cependant l'informatique vient, encore une fois, à notre secours, pour nous faire comprendre au moins l'ampleur du problème. En effet, si une démonstration correspond à un programme, un théorème correspond, lui, à toute une famille de programmes, puisqu'il possède plusieurs preuves. Il est naturel de penser que tous ces programmes ont un comportement analogue, autrement dit, qu'ils font tous la même chose. En informatique, on dit qu'ils ont la même *spécification*. Nous sommes donc parvenus à définir rigoureusement ce qu'est une spécification, puisqu'elle correspond, en logique, à la notion de théorème. C'est un résultat vraiment inespéré, car cette notion de spécification semble particulièrement rétive à toute tentative de définition. En effet, ce n'est pas autre chose que l'intention du programmeur au début de son travail, et comment définir *l'intention* ? Il ne saurait donc y avoir, en plus, une relation évidente entre l'énoncé d'un théorème mathématique et la spécification qu'il dissimule.

Mais voici un autre point intéressant, à propos du théorème de complétude : nous avons dit qu'un désassembleur permet d'exécuter un programme en pas à pas, ce qui veut dire qu'il s'arrête après chaque instruction élémentaire pour permettre à l'utilisateur d'intervenir comme il lui plaira. Toutefois, par prudence, il omet de s'arrêter à certains endroits sensibles, où une intervention irréfléchie de l'utilisateur pourrait avoir un effet désastreux, comme de planter la machine. Il est fascinant de constater que *ce dispositif de sécurité existe bel et bien dans le désassembleur associé au théorème de complétude de Gödel*. Comment diable se fait-il qu'un théorème, démontré dans les années 30, alors qu'il n'existait pas l'ombre d'un ordinateur, puisse nous parler de la sécurité d'un système

informatique ? De quel système informatique s'agit-il donc ? Il n'y a qu'une réponse possible, il s'agit, bien sûr, de la seule marque d'ordinateur commercialisée à l'époque, et qui est d'ailleurs sur le marché depuis quelques centaines de milliers d'années. Comme me disait récemment un ami informaticien : " Ce matériel ne manque pas de qualités, mais malheureusement, le service après-vente est quelque peu déficient, il ne répond même plus au téléphone " ...

Au terme de cette excursion en théorie des ensembles et en théorie des démonstrations, il est temps, pour conclure, de revenir à la question initiale : " Qu'est-ce que la logique ? " Je donnerai, pour ma part, la réponse suivante : c'est un outil fabuleux et irremplaçable pour explorer la structure profonde du cerveau humain, et découvrir la façon dont il est programmé. D'ailleurs, quand le service après-vente est aux abonnés absents, et que le fabricant a mis la clé sous la porte, il faut bien que le client essaie de se débrouiller tout seul.