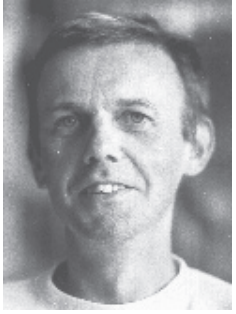

Gérard HUET

Gérard Huet, né en 1947, docteur ès sciences (1976), est directeur de recherche à l'Institut national de recherche en informatique et automatique (INRIA).

Il a fait progresser l'informatique sur le plan conceptuel et a participé à d'importantes réalisations logicielles. Spécialiste de démonstration automatique, il a fait plusieurs contributions aux fondements théoriques de cette discipline, notamment dans les domaines de logique d'ordre supérieur, de la logique équationnelle et de la théorie des types. Il a montré comment l'algorithme d'unification de Herbrand-Robinson pouvait s'étendre au lambda-calcul typé, permettant la mécanisation de la théorie des types de Church, et l'extension du langage PROLOG à la logique d'ordre supérieur. Il s'est intéressé ensuite à l'automatisation des raisonnements équationnels par réécriture canonique, ainsi qu'à l'implémentation efficace de programmes équationnels séquentiels. Les travaux de Gérard Huet, obtenus en collaboration avec Jean-Marie Hullot et Jean-Jacques Levy, sont à la source de l'école française

Vérité mathématique, cohérence logique et vérification informatique

de réécriture. Au milieu des années 80, Gérard Huet a travaillé à la définition d'une théorie des types, le calcul des constructions, dont le grand pouvoir d'expression permet de représenter des raisonnements mathématiques sophistiqués, mais aussi d'exprimer les spécifications d'algorithmes informatiques. Les preuves formelles de réalisabilité de ces spécifications sont compilables en un programme exécutable, ouvrant la voie d'une méthodologie rigoureuse de conception de logiciels certifiés. Le système d'assistance à la preuve Coq issu de ces travaux a donné lieu à de nombreuses collaborations industrielles, notamment avec les sociétés Dassault Aviation, Bull, France Télécom et Trusted Logic.
En parallèle avec ces travaux de nature fondamentale, Gérard Huet a poursuivi des recherches d'un caractère plus appliqué. En collaboration avec Gilles Kahn, il a participé à la conception et à la réalisation d'un éditeur de structures hiérarchiques appelé Mentor. Ces travaux, précurseurs sur la syntaxe abstraite, ont ouvert la voie à des environnements de programmation, tels que Centaur, et à des formats d'échange structurés tels que XML.
Dans les années 80, Gérard Huet a dirigé le projet Formel, dont le but était de définir et d'implémenter des systèmes de manipulation d'objets mathématiques, et de les appliquer aux outils de base du génie logiciel. Reprenant comme langage de programmation le langage ML, il a dirigé l'effort de conception et d'implémentation d'un langage fonctionnel puissant appelé CAML. L'environnement de programmation «Objective CAML» est utilisé par une large communauté pour l'enseignement de la programmation et l'implémentation de logiciels sûrs.

Depuis quelques années, Gérard Huet s'est tourné vers la modélisation mathématique et informatique des langues, et développe des outils efficaces de linguistique computationnelle. Il est l'auteur du premier dictionnaire informatisé sanscrit-français.
Membre de l'Academia Europaea (1989), Prix Herbrand de la «Conference on automated deduction» (1998).

La vérité dans les sciences est un problème philosophique posé depuis la nuit des temps, à savoir : quels sont les moyens de connaissance justes ?

Ces discussions portent souvent sur le discours de la méthode expérimentale, la possibilité de reproduire le résultat des expériences, etc. et il semble bizarre qu'on examine les mathématiques, puisqu'on ne sait même pas si c'est une science : c'est plutôt une sorte de firmament au-dessus des sciences.

Dans le langage courant, lorsqu'on a une certitude absolue, on dit : *« C'est mathématique »*, donc comment mettre en doute la notion de vérité mathématique ? Cela paraît difficile mais peut-être y a-t-il des problèmes cachés sous le tapis dans les mathématiques ? Il est significatif qu'on n'ait pas trouvé de mathématicien pour faire cet exposé.

En dépit de mon doctorat de mathématiques, je suis un informaticien avant d'être un mathématicien. Les mathématiciens se sont peut-être défaussés sur un informaticien pour discuter de la vérité mathématique, avec l'idée que si je dis quelque chose de non politiquement correct, ils pourront toujours me récuser comme incompétent !

Exemples de preuves mathématiques

Nous allons examiner quelques moyens de connaissance. Il y a d'abord les moyens de perception directe : *« Je l'ai vu de mes propres yeux »* et c'est donc là-dessus qu'est basée toute la vérification de la physique, c'est la méthode expérimentale. Ce n'est pas forcément vos yeux, c'est peut-être à travers un instrument. Mais l'idée est là : vous avez une perception directe du phénomène qui agit sur vous indépendamment de votre volonté. Et puis, parmi les autres moyens de connaissance, il y a la logique, notamment le raisonnement et d'autres encore. Il y a toutes sortes de classifications dans différentes traditions : l'induction, l'analogie, etc.. Les bouddhistes admettent même un moyen de connaissance disant que si on n'a pas d'appréhension du phénomène, il n'existe pas. Si le chien n'aboie pas, il n'existe pas, en quelque sorte.

Nous allons donc déjà examiner la méthode expérimentale et le problème de sa possible utilisation pour valider un raisonnement mathématique. La réponse est surprenante, car dans une grande mesure, c'est possible. On peut vérifier, par l'expérience,

le résultat d'une preuve mathématique. Je vais vous donner un exemple simple : j'ai deux bâtons dans chaque main, et maintenant, et vidant mes mains sur la table, je fais la somme de tous les bâtons : 2 + 2 = 4 ; vous pouvez le constater de vos yeux, il y a quatre bâtons. C'est une preuve tout à fait matérielle qui ne peut pas être mise en doute. Donc peut-on extrapoler et réduire toutes les preuves mathématiques à une espèce de démonstration physique complètement convaincante et existante de l'objet mathématique ? Dans une certaine mesure, oui.

Je vais maintenant faire un raisonnement mathématique plus compliqué. Je vais vous montrer qu'il existe un nombre infini de nombres premiers. Comment procède la preuve ? On raisonne ainsi : imaginons que nous ayons un nombre premier qui soit maximum, je vais vous donner un procédé pour en construire un encore plus grand, comme cela, il y en a une infinité. Le procédé est simple, il marche pour tout entier : vous prenez cet entier, vous le multipliez par tous ses prédécesseurs (n – 1, etc.), donc vous fabriquez « factorielle n » et vous lui ajoutez 1. Vous regardez donc ce grand nombre : par qui est-il divisible ? Il ne l'est ni par 1, ni par 2, ni par n. Donc soit il est lui-même premier, soit ses diviseurs sont des nombres premiers qui vont être plus grands que n. Vous avez donc réussi à exhiber un nombre premier plus grand que le nombre qui était donné comme défi. Vous voyez, c'est une démonstration moins directe ; dans ce cas, je n'ai pas de bâtons, je ne vais pas exhiber un grand nombre premier, cela ne servirait pas, mais je vous ai donné un procédé qui, si vous me donnez un nombre arbitraire, permet alors de calculer un premier plus grand. C'est un procédé de calcul mécanique, finitiste et c'est de la même essence. Tout simplement, au lieu d'exhiber directement le résultat, j'ai fabriqué un jeu à deux joueurs et je vous renvoie donc la question d'une certaine manière, en disant : *« Vous prétendez qu'il y a un nombre fini de nombres premiers, alors donnez-moi le plus grand. »* Vous le donnez, et à ce moment-là, je calcule le nombre premier. Cela revient donc au même. C'est une démonstration complètement effective et exempte de doute. Vous vous demandiez : *« Que va-t-il faire ? Il va nous amener un grand sac plein de nombres premiers et nous dire : Regardez, il y en a une infinité. »* Je n'aurais pas pu faire cela. Je n'aurais pas pu construire un sac infini de nombres premiers et vous auriez été bien en peine, si je l'avais fait, de montrer qu'il était infini. Donc en fait, j'ai fait une paraphrase sur la notion d'infini et je l'ai tournée en ce jeu qui ré-exprime la notion d'infini, de manière à pouvoir construire la preuve de manière entièrement finitiste.

Il existe de nombreux procédés de preuve en mathématiques. Par exemple, ce que nous avons fait à l'instant est de l'arithmétique, mais nous pouvons également faire de l'algèbre. Par exemple, concernant l'addition, je vous ai montré que 2 + 2 = 4, mais ceci est un cas particulier d'un résultat beaucoup

plus général qui est que n + m = m + n. On dit que l'addition est commutative. Alors pour tout m et pour tout n, vous pouvez me donner m et n et je vais vous calculer n + m et m + n et nous allons voir que c'est la même chose. Mais vous me demandez un procédé qui va montrer d'un seul coup toutes ces égalités. C'est donc à cela que sert l'algèbre : pouvoir exprimer des propriétés universelles ; pour tout n et pour tout m, n + m = m + n. Ceci est quelque chose qu'on prouve par récurrence. Le procédé de récurrence vous dit que si une propriété est vraie de 0 et si étant vraie pour n, elle est vraie pour n + 1, alors la propriété est vraie de tous les entiers. Donc un raisonnement par récurrence est une sorte de processus itérateur qui vous donne le moyen de connaître une propriété (ici des nombres entiers) par un procédé itératif. Et ainsi là, la commutativité de l'addition va se prouver par une récurrence ou plus exactement, par deux récurrences emboîtées.

L'autre jour, je zappais sur mon téléviseur et je suis tombé sur *« Questions pour un champion ».* Il s'agissait d'une question de mathématiques. Je me suis demandé ce qu'ils pouvaient bien poser comme question de mathématiques, alors que dans cette émission, on vous demande qui a gagné Wimbledon en 1937 ou de donner trois capitales de pays commençant par K et toutes sortes de savoirs encyclopédiques farfelus ; Je me demandais s'ils allaient demander si tel grand nombre est premier ou quelle était la vingtième décimale de pi, et la question était : *« Prenez les cinq premiers nombres impairs, additionnez-les et multipliez par 0, quel est le résultat ? »* J'étais atterré du niveau de connaissances mathématiques moyen de la population estimé par les meneurs du jeu *« Questions pour un champion »* et cela doit donc quelque part refléter une grave carence de notre société. Imaginer qu'il faille être un champion en mathématiques pour savoir que zéro annule, cela met la barre assez bas. J'étais un peu déprimé et je n'y ai plus repensé. Ensuite, en préparant mon exposé, je me suis dit : mais au fond, cette question était assez maligne, parce que ceux qui ont voulu faire le calcul ont compté 1 + 3 + 5 + 7… Ils ont perdu du temps, par rapport à ceux qui étaient plus malins, qui ont attendu la fin de la question et qui ont tout de suite répondu : « 0 », parce qu'ils ont employé l'algèbre, ils n'ont pas fait le calcul, ils ont employé la règle algébrique : x*0 = 0. La question aurait été totalement triviale, si on avait demandé 0*x, par la définition de la multiplication, alors que là, cela demandait justement de connaître cette égalité algébrique. Il y avait donc une utilisation de l'algèbre comme étant un raccourci calculatoire, par rapport à la méthode « bébête » qui consistait à faire tout le calcul. Si je vous pose le problème de la valeur de: *« $(2^{14} + 2^{17})* 0$ »*, là il n'est plus question de faire le calcul, il faut le faire nécessairement par l'algèbre. Le problème était plus malin qu'on pensait.

Je vais vous donner un dernier exemple de preuve mathématique un peu plus com-

pliquée mais toujours sur les nombres premiers : je vous ai convaincus qu'il y a un nombre infini de nombres premiers ; pour un nombre premier, il y en a toujours un qui est plus loin. Mais c'est loin « factoriel n », donc n'y en a-t-il pas un plus près ? Par exemple, pour un nombre premier donné, existe-t-il toujours un nombre premier plus grand que lui mais inférieur à son double ? On peut se poser ce problème-là et essayer déjà si c'est vrai pour les petits premiers. Vous regardez : 3*2 = 6, oui, il y a 5. Là c'est bon. 5*2 = 10, oui il y a 7. C'est bon et vous pouvez aller plus loin pour vous en convaincre mais là, le procédé qui dit : *« J'ai essayé avec les cent premiers nombres premiers et cela marche, donc c'est bon »*. Mais ce n'est pas bon, parce que vous n'avez pas employé un procédé de récurrence rigoureux ; c'est ce qu'on appelle « l'induction », ce n'est pas un procédé mathématique ou logique fiable et il peut toujours y avoir un contre-exemple caché plus loin. Il faut donc une vraie preuve. Mais si on essaye de pouver cette propriété par une récurrence rigoureuse, on n'y arrive pas, ça n'est pas si simple. Juste pour sonder la salle, pensez-vous que ce soit vrai ? Oui, c'est vrai. Mais comment est-ce que cela s'appelle ? Cela s'appelle : *« Le postulat de Bertrand »*. Pourquoi est-ce que cela s'appelle comme ça ? Pour des raisons historiques. Bertrand avait conjecturé ce fait en 1845, mais c'était resté à l'état de postulat, jusqu'à ce que Chebyshev en trouve une preuve assez complexe. Ce n'est qu'en 1934 que Paul Erdös en donna une preuve élémentaire.

Les mathématiques recouvrent de nombreux procédés, et les interrelations entre les différents domaines des mathématiques forment un tout. C'est en fait un tissu conceptuel très complexe. En particulier, deux remarques : d'abord la taille de la preuve d'une vérité mathématique n'a rien à voir avec la taille de la conjecture – des conjectures peuvent s'énoncer en une ligne et demandent des milliers de pages de démonstration – et ensuite il n'y a pas de méthode systématique de preuve. Vous l'avez vu : pour n*0, soit on peut faire le calcul, soit utiliser l'algèbre, ou autre chose. On a plus d'un tour dans son sac. Il n'y a donc pas une seule manière, sinon les mathématiques seraient tellement triviales que n'importe quel ordinateur pourrait faire des mathématiques. Il y a un choix et celui-ci est guidé par des critères complexes.

Remarquons en passant que tout théorème n'est pas intéressant. Le fait qu'on puisse mater aux échecs avec un fou et un cavalier est un théorème de combinatoire qui n'a qu'un intérêt sociologique, celui de fournir une stratégie gagnante dans une finale théorique qui n'arrive quasiment jamais dans une partie d'échecs. On pourrait engager des armées de mathématiciens pour étudier les finales de jeux improbables sur des damiers de tailles arbitraires, sans pour autant faire avancer d'un iota nos connaissances mathématiques profondes, et donc sans bénéfice appréciable pour l'humanité. Inversement, un mathématicien ne peut parier que ces travaux, aussi abstraits soient

ils, ne soient un jour utilisés pour construire une diablerie technologique. Paul Hardy se croyait à l'abri en faisant de la théorie des nombres, et maintenant la cryptographie y trouve son miel.

Erreurs et paradoxes

Il n'y a pas que des vérités premières en mathématiques mais aussi des énoncés erronés, des preuves apparemment correctes mais fautives dans un détail indécelé par les relecteurs, menant à des erreurs qui peuvent se propager en épidémies par le jeu des publications. Il y a aussi ce qu'on appelle des paradoxes. Ce sont des énoncés manifestement erronés mais qu'on arrive à démontrer par un procédé qui n'est pas toujours réfutable de manière évidente. Je vais vous montrer que 1 = 2, par exemple. C'est très simple : 1 est le numérateur de ½ et 2 est le numérateur de 2/4, similairement. Or chacun sait que 1/2 = 2/4, il suffit de diviser par 2. Les numérateurs de mêmes fractions étant les mêmes, 1 = 2. C'est direct. Il n'y a pas besoin de savoir des tas de choses en mathématiques pour comprendre ce paradoxe. J'aime bien raconter cela à des mathématiciens de passage, car la réaction est toujours la même : cela les rend furieux. Ils me sautent à la gorge, ne prennent pas le temps de réfléchir et éructent un énoncé catégorique. Le plus surprenant, c'est qu'ils ne disent pas tous la même chose. J'ai tout entendu et son contraire. Comme j'ai appris qu'il ne fallait pas moucher les gens, parce qu'on s'en faisait des ennemis, quelque soit la réponse, je dis : *« Bien sûr, mais toi, tu es un mathématicien, tu as tout de suite vu le truc. »* J'aurais dû faire un bêtisier de toutes les réponses, ce serait très instructif.

Pourquoi 1 n'est-il pas égal à 2, malgré ce raisonnement qui semble sans faille ? C'est un petit peu subtil mais les gens qui ont fait de la linguistique connaissent très bien cela : il ne faut pas confondre, comme dirait De Saussure, *« le signifiant et le signifié ».* Les fractions et les rationnels ne vivent pas dans le même monde. Une autre manière de dire cela, serait de dire : *« Il y a un quotient caché et les quotients et l'égalité, ce n'est pas tout à fait la même chose. »* Et ceci est un grand problème : en mathématiques, qu'est-ce que l'égalité ? On pourrait penser que l'égalité est quelque chose de trivial mais en fait, il y a de nombreuses sortes d'égalités (l'égalité de Leibniz, l'égalité extensionnelle, l'égalité structurelle, la congruence induite d'un quotient, l'égalité axiomatique, l'égalité définitionnelle, etc.) et suivant le cas, vous avez le droit d'utiliser le remplacement d'égale par égale*,* mais ici, vous n'en n'avez pas le droit, parce que vous êtes en train de confondre des notions extensionnelles avec des notions intentionnelles. Je peux dire : *« Pierre ne sait pas que l'étoile du matin et l'étoile du soir sont le même corps céleste ».* Peut-être que Pierre ne connaît-il pas ce fait d'astronomie. Mais le fait que vous sachiez que l'étoile du ma-

tin est la même que l'étoile du soir ne vous autorise pas à faire la substitution dans ma phrase. Parce que si je vous dis : *« Pierre ne sait pas que l'étoile du matin et l'étoile du matin sont le même corps céleste »*, c'est idiot. Pierre a toujours su cette trivialité. Ces considérations linguistiques sont donc pertinentes par rapport au discours mathématique, parce que le discours mathématique est d'abord un discours ; on fait des phrases et on se convainc avec ces phrases et quelquefois une raison linguistique subtile fait qu'on a, en fait, fait une erreur de raisonnement, par le biais d'une confusion linguistique.

Je vais vous donner un autre paradoxe, qui m'a été communiqué par Bob Boyer : tout à l'heure, nous avons montré qu'il y avait beaucoup de nombres premiers, puisqu'il y a a toujours un plus petit que le double d'un nombre premier donné, mais peut-être y en a-t-il beaucoup plus ? Peut-être que tout nombre est premier ? Je vais vous le démontrer. Ceci est une application d'un principe logique a toutes épreuves : « P implique P ». C'est le schéma logique exprimant : « si je sais P, alors je sais P ». Si cet argument n'était pas évident, quels seraient les raisonnements logiques admissibles ? Je vais maintenant vous faire la preuve que tout nombre est premier, en anglais. Vous allez me demander : *« Pourquoi l'anglais est-il mieux adapté pour faire passer certaines preuves mathématiques que d'autres langues ? »* Vous allez voir. En anglais, je vais instancier P avec l'assertion *« any number is prime »* et le théorème est donc: *« If any number is prime then any number is prime. »* Tous les gens qui connaissent l'anglais comprennent qu'on vient de prouver que tous les nombres sont premiers, puisqu'il suffit, pour faire cette preuve, de remplir la condition : *« If any number is prime. »* Prenez n'importe lequel, 2 par exemple. La conclusion, c'est *« Any number is prime. »* Tous les nombres sont premiers. Vous vous rendez compte ! 4 en particulier est premier, alors que tout à l'heure vous avez vu de vos yeux que 4=2*2. Alors comment repérer la faille ? Vous me direz : *« Oui mais votre exemple est spécieux, vous avez pris l'anglais, vous avez utilisé « any », c'est quelque chose de bizarre, c'est une quantification universelle dans un contexte co-variant, qui devient existentielle dans un contexte contra-variant. »* Oui mais je n'y peux rien, c'est comme ça. S'ils n'ont pas le droit d'utiliser les mots du langage, comment les mathématiciens vont-ils discuter entre eux de leurs travaux ? Comment vont-ils raconter leurs résultats dans des revues s'ils n'ont pas la langue ? Donc éliminer les difficultés de langue n'est pas toujours aussi facile que cela.

Il y a mille et mille difficultés dans la notation mathématique. Par exemple, on vous apprend à l'école qu'il ne faut jamais écrire : *« 1 divisé par 0. »* Surtout ne le faites pas, ce n'est pas bien ! Mais on nous autorise à écrire 1 sur une grande expression qui peut contenir de nombreux paramètres et pour certaines valeurs de ceux-ci, peut-être que cette expression va être nulle. Que va-t-il se

passer à ce moment-là ? Est-ce que la formule va exploser ? Non, pas du tout. Cela va simplement ouvrir la faille à une erreur de raisonnement. Vous allez introduire un nombre superflu qui va faire qu'un théorème ne va plus être vrai, etc. On voit cela tous les jours avec les systèmes de calculs formels. Ces derniers ne tiennent pas trop compte des conditions auxiliaires d'emploi de leurs formules, ils font donc des simplifications. On espère que tout se passe bien et au bout du compte, cela peut donner des résultats complètement faux. Il faut donc bien tenir compte des conditions du contexte. C'est bien connu en linguistique. Dans la langue, vous avez un discours logique derrière le discours en langue naturelle et ce que vous dites directement dans une phrase est appelé : *« le posé »*. Mais il y a également des conditions d'emploi des tournures linguistiques qui vous introduisent d'autres conditions logiques. Et ceci s'appelle : *« le présupposé ».* Par exemple, si je vous dis : *« Pierre a arrêté de boire. »* Le posé est que Pierre ne boit pas maintenant, mais le présupposé est qu'il buvait avant. Vous ne diriez pas : *« Pierre a arrêté de boire »* s'il n'a jamais bu, ce serait une calomnie. Et c'est très subtil. Comment gérez-vous le posé, le présupposé, le sous-entendu, toutes ces choses compliquées, alors qu'on nous fait croire qu'en mathématiques, la logique tient compte du fil du raisonnement logique et qu'il n'y a pas de problème ? Alors que suivant la tournure que vous allez prendre, il va alors y avoir des présuppositions, comme lorsque vous écrivez : *« 1 sur x »*, il y la présupposition que « x » n'est pas nul. Vous devez donc garder cela très précieusement en tête et puis accumuler toutes ces présuppositions dans un contexte. Est-ce que cela est fait soigneusement dans tous les textes mathématiques ? Est-ce qu'on comprend une manière absolument sans faille de gérer ces conditions ? Y a t il un consensus sur la bonne pratique dans l'usage des notations ? On peut en douter.

Regardons par exemple la notation même d'ensemble : { x | P(x) } dénote l'ensemble des x vérifiant la propriété P; qu'est-ce que cela peut bien vouloir dire ? Or c'est pourtant le langage standard des mathématiques contemporaines. Mais son utilisation naïve conduit directement à des paradoxes. Prenez par exemple pour P(x) la propriété « $x \notin x$ ». On définit ainsi l'ensemble des ensembles qui ne se contiennent pas eux-mêmes. C'est un ensemble qui, s'il se contient lui-même, alors il ne se contient pas lui-même et réciproquement. Alors avec ça, que faites-vous ? On ne va pas bien loin ou plus exactement, on peut tout prouver. Il y a donc beaucoup de paradoxes liés à des notations qui, en fait, sont d'un emploi très subtil. Vous voyez, pour la notation ensembliste, il faut considérer les axiomes de la théorie des ensembles, notamment les axiomes de compréhension utilisables, ou bien distinguer les ensembles et les classes, comme dans la présentation de Gödel-Bernays. Vous avez tout un « fourbi » qui vient se mettre dans votre notation au milieu d'une formule si vous voulez expliciter les

conditions d'emploi d'une formule ensembliste, alors on ne les écrit pas. La plupart des paradoxes se rapprochent du « *paradoxe du menteur* », inventé par Epimenides, philosophe crétois du 5ème siècle avant Jésus Christ. Il disait : « *Je suis un menteur.* » Vous avez donc là un paradoxe immédiat. Vous êtes en train de dire que vous êtes en train de mentir. Donc comme vous mentez, vous dites la vérité. Cette idée de construction paradoxale se décompose en deux idées : une idée de réflexion, c'est « je », je parle de moi et l'idée de mentir, c'est d'avoir une fonction qui n'a pas de point fixe. Donc en gros, c'est un procédé diagonal que vous pouvez utiliser dans diverses circonstances. Beaucoup de constructions mathématiques utilisent cette idée-là, nous allons le voir.

Il y a également le problème du nommage des choses. Quelle est la valeur de Pi ? Qui peut me donner la valeur de Pi à 1 % près ? J'entends : « 3.1415… ». En fait, je vais vous montrer que Pi= 2. C'est très facile ! Soit Pi = 2, alors Pi = 2. En effet, qu'est-ce qui m'empêche d'utiliser Pi comme variable mathématique ? Tout à l'heure, j'ai utilisé x, y, z, n ou m, pourquoi pas Pi ? Si on ne pouvait pas utiliser Pi comme nom, comment pourrions-nous parler de Pi ? On ne veut pas mettre la notation Pi dans le langage initial, on veut pouvoir faire de l'arithmétique sans avoir à connaître les réels au départ. Nous pouvons donc bien utiliser Pi, et même c'est nécessaire pour pouvoir définir cette constante. Mais Pi c'est quoi, au juste, dans le discours ? C'est P majuscule suivi de i minuscule pour faire l'identificateur « Pi » ? Ou bien est-ce la lettre grecque ? La discussion est sans fin. Imaginez un papier que je soumette à la Société Mathématique de France, avec deux définitions de Pi. Une sera Pi en fonte maigre avec telle définition et l'autre sera **Pi** en fonte grasse avec une autre définition. Je vais bien montrer que les deux sont équivalentes, ce qui justifie la notation. Est-ce que mon papier doit être refusé ? Ou sinon, sommes-nous obligés de distinguer les Pi maigres et les **Pi** gras ? Nous allons donc rentrer dans la typographie. Oh là là ! Mais où s'arrête ce genre de problème ? On n'a pas fini ! Si on essaye le tournevis fin, on va en trouver des problèmes de notation !

L'incertaine mathématisation de la logique

Alors c'est un peu pour tous ces phénomèmes de paradoxes, etc., qui sont arrivés avec la théorie des ensembles au début du vingtième siècle, que les mathématiciens se sont posé le problème d'utiliser la logique d'une manière un peu plus rigoureuse et ils ont donc commencé une mathématisation de la logique, de manière à pouvoir expliquer les preuves mathématiques d'une manière qui soit mathématiquement satisfaisante. Donc Frege, Russell et un certain nombre de mathématiciens, au début du vingtième siècle, ont jeté les bases de ce que nous appelons

maintenant : *« la logique mathématique »*, qui est une manière d'expliquer comment faire des raisonnements ; qu'est-ce qu'un théorème ? En gros, c'est le résultat d'une suite de règles d'inférence, c'est ce qu'on appelle une démonstration formelle. Vous prenez donc des axiomes et vous les combinez par des règles d'inférence, qui sont des règles logiques en nombre fini, et qui expriment des jugements élémentaires incontestables, comme : si A implique B, alors si vous avez A, vous en déduisez B. C'est un exemple d'inférence. Vous voyez que c'est tout à fait élémentaire, presque trop évident pour mériter même d'être identifié comme étape de raisonnement. On peut analyser ces raisonnements et donc réduire un raisonnement à un objet combinatoire, à un arbre dont les feuilles seront les axiomes, les branches exprimant les règles d'inférence et à la racine, vous aurez l'opérateur principal de la structure de preuve, qui démontre un certain résultat mathématique. Les propositions logiques sont donc des espèces d'annotations dans cette structure-là. Vous pouvez mathématiser cela, l'arithmétiser. Gödel a transformé tout cela en un grand entier, etc. On sait donc réduire l'inférence à un calcul arithmétique.

Cela a donc amené les mathématiciens à se poser le problème de savoir si on ne peut pas aller jusqu'au bout, faire le grand *bootstrap* des mathématiques, c'est-à-dire, partir de procédés complètement élémentaires et construire le système d'inférences progressif dans lequel on va faire des mathématiques plus compliquées et prouver un résultat mathématique qui va être bêtement un résultat d'arithmétique qui va vous dire : *« Voilà, on ne peut pas montrer faux. On ne peut montrer que des choses vraies. »* Préservation de la vérité par ses preuves. C'est ce qu'on appelle : *« la cohérence du système logique. »* Cela paraissait être un but certes ambitieux mais atteignable et Hilbert, le premier mathématicien de son époque, en 1900, au grand congrès international des mathématiques, a posé à ses collègues le problème d'arriver à construire le fondement des mathématiques de manière complètement interne.

Les logiciens se sont mis au travail et Gödel a poussé les symboles sur ces idées d'arithmétisation, et il a fini par axiomatiser le paradoxe d'Epimenides : *« Je suis en train de mentir. »* Simplement, ce n'est pas un théorème qui va dire : *« Je suis en train de mentir »* mais : *« Je ne suis pas démontrable dans le système formel. »* Il le dit vraiment et sa construction est exacte, c'est-à-dire qu'il n'est vraiment pas démontrable, donc il est vrai. Voilà une formule vraie d'arithmétique qui n'est pas démontrable. Ceci est le premier théorème d'incomplétude de Gödel, donc déjà, cela jette un certain froid sur l'adéquation de la notion de preuve à celle de vérité. Et en poussant les symboles un peu plus loin, Gödel est arrivé à la conclusion finale : non seulement ce n'est pas un fait isolé, - vous diriez : *« Gödel exhibe une formule vraie qui n'est pas un théorème, qu'à cela ne tienne, il n'y*

a qu'à le rajouter comme axiome et comme ça nous l'aurons. - mais ce faisant on change le système formel, et le même argument s'applique ; derrière lui il y en aura un autre, par la même construction. En fait, la plupart des formules arithmétiques vraies ne sont pas démontrables en arithmétique axiomatique. C'est donc plus grave que cela. Le plus grave, c'est que le théorème qui exprime l'incohérence de l'arithmétique est de cette sorte-là, il est non démontrable. C'est un résultat des années 1930, qui a été un grand choc chez les mathématiciens. Gödel en est devenu fou et s'est développé tout un courant de travaux de logique pour essayer de contourner la difficulté avec une notion de cohérence relative. Les mathématiciens sont restés relativement sereins. Ils ont regardé la preuve de Gödel en détail et ont dit : *« Oui, cette preuve est correcte, il n'y a pas de problème. Il faut vivre avec, mais c'est « business as usual ». »* Il y a donc le théorème de Gödel.

On a fait raconter n'importe quoi à ce malheureux théorème, qui est devenu un poncif des récréations mathématiques, mais le problème demeure. C'est une plaie au cœur des mathématiques qui est là pour toujours. Les mathématiciens ne s'en font pas plus que cela et ne considèrent pas que toutes ces préoccupations de fondement des mathématiques sont au cœur du métier. Ils considèrent que c'est plutôt auxiliaire, que c'est un peu gloser sur des histoires qui ne sont qu'à moitié intéressantes. La logique mathématique n'est pas la première spécialité mathématique. Si vous voulez vous couvrir de gloire en tant que mathématicien, ne faites pas de la logique mathématique. C'est considéré comme quelque chose d'arrière-boutique, comparé à la théorie des nombres ou à la géométrie algébrique qui sont de grands domaines prestigieux. Par exemple, un fameux mathématicien, Paul Cohen, a dit un jour : *« Donnez-moi la conjecture logique la plus importante. »* La conjecture à la mode était l'hypothèse du continu. Tout à l'heure, nous parlions d'infinité et en fait, dans la théorie des ensembles, il y a plusieurs notions d'infinité ; il y a des infinis plus ou moins gros. Par exemple, les entiers sont infinis, mais il existe des ensembles infinis beaucoup plus gros, comme les réels par exemple. On ne peut pas numéroter les réels, les mettre en correspondance avec les entiers. Comment est-ce que cela se prouve ? Toujours par le paradoxe d'Epimenides. C'est une espèce de recette de cuisine. Imaginez que vous énumériez tous les réels entre 0 et 1 en notation binaire, c'est-à-dire comme suite de zéros et de uns. Maintenant, je vais tirer un réel qui n'est pas dans l'énumération, je vais tirer la diagonale du grand tableau formé par la liste présumée de tous les réels, et sur celle-ci, je vais changer les 0 en 1 et les 1 en 0. Voilà, j'ai construit un réel et ce réel menteur par construction dit : *« Je ne suis pas dans l'énumération. »* En effet, s'il apparaissait au rang n, alors sa nième décimale serait le chiffre opposé au sien. C'est un procédé complètement général, la réflexivité avec la négation. Ceci montre que les réels ne sont pas dénombrables.

Autrement dit, il y a beaucoup plus de réels que d'entiers.

Il y a donc de plus gros infinis. Il y a ainsi une notion de cardinalité en théorie des ensembles. Ils sont notés par la lettre de l'alphabet Hébreu ℵ indicée par un ordinal ℵ 0, ce sont les entiers. Moins infini que les entiers, on ne sait pas faire. Par contre, les réels sont plus gros, comme nous avons vu. C'est ℵ combien ? On ne sait pas. La conjecture portait sur ce problème. Ces deux constructions mathématiques, les entiers et les réels, sont les deux mamelles des mathématiques. Ce sont vraiment les deux objets de choix d'étude des mathématiciens. L'un est plus gros que l'autre, on pourrait donc se demander s'il y a des ensembles de taille intermédiaire entre les deux. Ce sont peut-être des ensembles intéressants. ℵ 1, l'ensemble des ordinaux dénombrables, peut être vu comme un espace de processus. Est-il en correspondance de bijection avec les réels ? C'est plausible. D'ailleurs, Gödel avait montré que l'hypothèse du continu (c'est-à-dire que la cardinalité des réels – aussi appelée la puissance du continu - vaut ℵ 1 et donc qu'il n'y a pas d'intermédiaire entre les entiers et les réels) était cohérente avec la théorie des ensembles, on pouvait l'ajouter comme axiome. Cela ne montrait pas que la théorie des ensembles était cohérente, bien sûr, mais seulement que, si la théorie des ensembles était cohérente, alors en ajoutant cet axiome-là, on n'empirait pas les choses. On savait déjà cela mais pas si l'hypothèse du continu était effectivement une conséquence des axiomes usuels ou pas. C'est quand même un problème important, non ? Si on essaye d'avoir une espèce de vue intuitive des ensembles comme étant des nuages de points et de faire des raisonnements qui tiennent, on aimerait savoir les choses fondamentales sur, par exemple, l'existence d'un ensemble intermédiaire entre les entiers et les réels. Paul Cohen a regardé cela, il a dit : *« Tout cela est trivial. »* Il a fabriqué un procédé général qu'il s'appelle : *« le forcing »* et il a montré que l'hypothèse du continu était indépendante des axiomes de Zermelo-Fraenkel. Problème résolu.

Effectivement, cela a résolu le problème de l'hypothèse du continu mais d'une manière qui n'est pas très satisfaisante. C'est-à-dire que l'hypothèse du continu est quelque chose qui n'est ni vraie ni fausse, c'est un peu : *« Si cela vous plaît, vous le prenez, si cela ne vous plaît pas, vous ne le prenez pas. »* Alors vous dites : *« Mais attendez, que se passe-t-il ? Des mathématiciens vont utiliser cela, vont prouver des théorèmes et d'autres vont prendre le contraire et nous prouver d'autres théorèmes. Comment est-ce que cela va se recoller ? On n'est pas du tout sûr que cela va être cohérent et qu'on va recoller les mathématiques des uns et des autres. Que va-t-il y avoir ? La secte de ceux qui croient à l'hypothèse de continu, et ceux qui croient à l'axiome du choix, ceux qui ne croient pas au tiers exclu, etc. »* La grande beauté de la mathématique s'évanouit donc dans une espèce de discours confus où vous

utilisez à votre gré tous ces axiomes plus ou moins indépendants, sans avoir de doctrine globale unanimement admise.

La logique de premier ordre

Tout cela n'est donc pas extrêmement satisfaisant. Alors tout de même, je vais arriver vers les conclusions plus positives : déjà, il y a un procédé logique, à peu près standard, c'est la logique de premier ordre. Ceci est à peu près admis par les mathématiciens comme étant le cadre logique un peu standard, dans lequel on pourrait théoriquement exprimer formellement les mathématiques usuelles. Je vais vous donner un exemple de théorème de la logique de premier ordre dû à Smullyan, c'est celui du bar. Dans tout bar, il y a une personne telle que, si elle boit, alors tout le monde boit. Pourquoi est-ce vrai ? Alors vous pensez : *« Il y a le barman. »* Souvent le barman ne boit pas dans un bar, donc s'il ne boit pas, c'est bon, puisque le théorème est conditionné au fait qu'il boive. Donc l'assertion est vérifiée pour le barman, si celui-ci ne boit pas. Mais peut-être que le barman boit et trinque avec les clients, donc ce n'est pas suffisant. Mais ce raisonnement s'applique à toute personne qui ne boit pas, on n'a pas besoin de savoir si c'est le barman ou pas. Si quelqu'un ne boit pas dans le bar, c'est bon, sinon tout le monde boit, donc c'est bon aussi. Terminé. On a prouvé le théorème du bar.

Mais n'y a t il pas une difficulté cachée. On a examiné le cas où quelqu'un ne boit pas. On a examiné le cas où tout le monde boit. Le théorème est vrai dans les deux cas, mais pourquoi ces cas sont ils exhaustifs ?

… *« Ah, c'est à cause de l'axiome du tiers exclu : P ou non P. Tiens ! C'était caché là ! C'était caché dans le raisonnement, nous ne l'avions pas vu. P ou non P, c'est toujours vrai ? »* Tout à l'heure, nous avons prouvé qu'il y avait des propositions indécidables, cela veut dire qu'elles ne sont pas prouvables, ni leur contraire. Donc attention, une proposition indécidable, avec le tiers exclu, cela veut dire que cela ne va pas être quelque chose qu'on va pouvoir décider par une sorte de calcul. Il doit a y avoir une sorte d'oracle qui va nous dire pourquoi c'est vrai ou pas. Donc, on peut avoir un certain doute sur l'effectivité de ce raisonnement, mais surtout on est étonné que cette difficulté soit cachée dans le raisonnement, sans qu'on l'ait vue. Il était tellement naturel de faire ce raisonnement ! Ceci renvoie à la notion de règle d'inférence élémentaire indéniable. L'emploi du tiers exclu est-il de cette sorte ?

Après cet exercice vous finissez par vous coucher, vous vous endormez et puis vous vous réveillez en sursaut avec des sueurs froides, vous avez fait un cauchemar ; c'est la nuit, le bar est fermé, il n'y a personne dans le bar, alors que vous avez prouvé dans la journée qu'il existait une personne dans ce bar, qui avait une certaine propriété. Où

est-elle ? Le bar est fermé, il est vide. Vous retrouvez vos papiers, vous compulsez le bouquin de logique mathématique, le raisonnement classique de premier ordre : tout est bon, tout est correct, comment est-ce possible qu'on ait prouvé quelque chose qui soit bien évidemment faux par le sens commun ? Le bar est fermé, il n'y a personne.

Ceci est une conséquence d'une espèce de bizarrerie de la logique de premier ordre, une chose un peu cachée sous le tapis, qu'on ne vous explique qu'à moitié. Les domaines d'interprétation de la logique de premier ordre sont des ensembles non vides. Il fallait le savoir ! Donc dès que vous parlez d'un bar, il est non vide. C'est comme ça, c'est le domaine d'interprétation. Tout cela parce que cela facilite les règles de raisonnement, donc les quantificateurs, en particulier. J'aime bien dire à un mathématicien : *« Savez-vous que si P(x) est vrai pour tout x, alors il existe un x tel que P(x) ? »* Soit le mathématicien ne va pas m'écouter parce qu'il ne voit pas pourquoi je lui dirais des choses intéressantes parce qu'après tout, je ne suis qu'un informaticien, soit il va m'écouter et dire : *« Ecoutez, bien sûr que c'est faux, avec l'ensemble vide. » Pour tout x* P(x) va être vrai, parce qu'il n'y a rien à montrer en l'absence d'éléments, alors qu'il n'existe justement pas de x, vérifiant P(x) ou quoi que ce soit d'ailleurs. J'insiste donc en disant : *« mais vous savez, en logique de premier ordre, ceci est vrai. »* . Le mathématicien est alors convaincu que je lui fait perdre son temps avec des arguties logiques oiseuses, ou plus simplement que je suis malcomprenant.

Ce sont des détails un peu anodins à première vue, et peu connus ou plutôt non intellectualisés consciemment, mais ces bizarreries peuvent poser des problèmes au recollement de disciplines mathématiques. Par exemple la notion de semi-groupe n'est pas la même en algèbre et en logique. L'ensemble vide est un semi-groupe en algèbre, il n'y a pas de problème ; toutefois ce n'est pas un modèle de la théorie de premier ordre des semi-groupes, puisqu'il doit être non vide. On a donc des notions fondamentales de mathématiques, qui ne sont pas tout à fait les mêmes de chaque côté. C'est comme si vous aviez des gens qui font de l'arithmétique en commençant à zéro et d'autres à partir de un. Ils ont tous leurs théorèmes qui se ressemblent un peu, mais qui ne sont pas tout à fait les mêmes. Comment va-t-on recoller tous ces morceaux-là ? C'est inquiétant !

L'informatique au secours des mathématiques par la théorie des types

Alors l'informatique est arrivée. Le tableau présenté jusqu'ici est un peu noir ; il a insisté sur les difficultés linguistiques, notationnelles, sur les difficultés à bien comprendre l'interférence de différents systèmes d'axiomes, à bien intégrer le fait qu'il n'y ait pas de mathématiques dans l'absolu mais que celles-ci sont relatives à un certain contexte de faits qui sont, soit des hypothèses, soit des axiomes et qu'il faut surveiller tout cela d'assez près. Il faut une bureaucratie très tâtillonne pour traquer la faute. D'autant plus que maintenant on arrive à des preuves absolument gigantesques. Prenons la classification des groupes simples : ce sont des théorèmes monstrueux sur des milliers de pages, alors comment va-t-on réussir à vérifier ces mathématiques ? L'informatique arrive donc au secours, dans la mesure où on comprend comment automatiser les développements mathématiques, la notation mathématique, les preuves, d'une manière qui n'utilise pas ces formalismes intermédiaires, comme la logique de premier ordre utilisée traditionnellement mais une notation inspirée d'un formalisme de nature informatique appelé : *« le lambda calcul ».* Ce dernier est une notation fonctionnelle. Derrière ces preuves se cachent des fonctions. Tout à l'heure, dans mon exemple sur les nombres premiers, je vous ai dit : « *Pour tout x, il existe un y* » et je vous ai apporté cette preuve, en vous donnant un algorithme : *« Quand vous me donnez le x, alors je vais calculer le y. »* C'est donc un argument fonctionnel. Le lambda calcul est une notation qui permet d'exprimer des fonctionnelles et d'une certaine manière, c'est un mécanisme de calcul universel. C'est une sorte de soubassement à tous les langages de programmation et une notation suffisamment simple pour qu'on puisse facilement raisonner avec.

Je ne vais pas vous faire un cours sur le lambda calcul. En gros, ce sont les entiers qui sont les atomes – les variables de la notation. Il y a un constructeur binaire : l'application ; on peut appliquer une fonction à son argument, on peut écrire f appliqué à x. Finalement, on a une notation pour créer une fonction à partir d'une expression, en identifiant une variable – donc ici, représentée par un entier –, privilégiée comme étant l'argument formel. C'est la lambda notation. Elle est munie d'une seule règle de calcul, qui dit que le résultat de l'application de « lambda x f(x) » à « X » est « f(X) ». C'est un simple procédé de substitution : à partir d'une expression, vous pouvez la transformer en une expression qui va être un petit peu plus explicite, en effectuant des calculs de fonctions intermédiaires. Avec ce lambda calcul, vous pouvez tout faire, faire tous les calculs possibles et imaginables, non seulement sur les entiers, mais aussi sur toutes les structures.

En plus, il y a une manière de décorer ce lambda calcul par des assertions qui limitent les possibiltiés de combinaison en explicitant une stratification par un systèmes de types fonctionnels, une sorte de généralisation du calcul de dimension en physiques. Donc vous avez un procédé administratif qui va un peu limiter la puissance du formalisme, pour vous obliger à n'écrire que des fonctions totales, et vous allez avoir un procédé de calcul qui va terminer et c'est la base de l'utilisation de ce formalisme, pour une notation de logique appropriée à décrire, de manière complètement formelle, les raisonnements mathématiques, l'utilisation de notations, etc. En particulier , un statut très clair est affecté à la notion de définition. Si vous voulez définir la notion x associée à sa définition X, il suffit de se placer dans le contexte indiqué par les crochets dans l'expression (lambda x [])(X). Ceci équivaut exactement à la notation « Soit x=X dans … ». Ceci est en programmation la base du langage ML, qui est à la pointe de la programmation fonctionnelle. Mais pour la formalisation des mathématiques il faut un système administratif plus souple, avec une notion de type dépendant, qui en fait exprime que le langage de type est un langage logique de premier ordre. C'est la base du système Automath de Nicolas de Bruijn. Surtout, c'est la reconnaissance d'un principe très général, qui est que les preuves peuvent être exprimées par des notations fonctionnelles bien typées – les types sont les formules de la logique, et les valeurs sont des représentations concrètes d'objets fonctionnels – des algorithmes. Cette correspondance fondamentale est née des travaux de Curry, Howard, et de Bruijn.

Le lambda calcul était en fait connu avant la 2ème guerre mondiale par Church, qui l'avait utilisé dans des considérations de récursivité – on étudiait la puissance des différents procédés finitistes de faire des calculs – ; c'était un peu tombé dans l'oubli et cela a été repris par les informaticiens dans les années 1970. Church a aussi essayé de l'utiliser sans décorations pour fonder les mathématiques, mais le menteur guettait avec le combinateur d'auto-négation, et il a du se résoudre à développer un formalisme logique avec une stratification de types simples, peu utilisable pour exprimer des mathématiques sophistiquées de manière modulaire. La première tentative sérieuse d'utiliser le lambda calcul pour développer les mathématiques, c'est le système Automath du au mathématicien N. de Bruijn qui était un précurseur. Je me souviens que Michel Demazure l'avait invité à Orsay en 1976 et à l'époque, son travail était complètement mécompris. De Bruijn était un spécialiste de combinatoire mondialement connu, mais quand il s'est mis à travailler à ces fondements des mathématiques, à un langage qui permettait d'exprimer formellement des mathématiques sophistiquées appelées *« Automath »*, cet effort a été complètement mécompris, et longtemps méconnu. Ce n'est que dans les années 1980 et 1990 qu'on a utilisé cette notation ou des notations analogues, pour développer ce qu'on

appelle maintenant *« la théorie des types »*, à partir d'autres idées, en particulier, celles du philosophe suédois Per Martin Löf qui a fait une théorie constructive des types, et de travaux d'un logicien français, Jean-Yves Girard, qui a fait un lambda calcul polymorphe. On a donc mis tout cela ensemble et on a construit des lambda calculs appropriés à la représentation des mathématiques, d'une manière complètement formelle, mécanisable et modulaire. C'est-à-dire qu'on va pouvoir développer de manière indépendante de grandes preuves mathématiques et les recoller pour faire d'encore plus grandes preuves mathématiques. Tout ça sans expansion non linéaire de la taille des démonstrations formalisées.

C'est un mouvement qui maintenant arrive à maturité ; nous avons des systèmes qui permettent de faire des preuves mathématiques de très grande taille et donc, par exemple, sur un système que nous avons développé dans mon groupe de recherche à l'INRIA appelé *« Coq »*, deux chercheurs ont réussi à complètement faire la preuve formelle du théorème des 4 couleurs, (toute carte de géographie peut être coloriée avec seulement 4 couleurs, sans avoir de frontières communes entre régions de même couleur). C'est un résultat de topologie et théorie des graphes, qui est très complexe et dont la preuve mathématique était très controversée ; la première preuve a été faite dans les années 1970, avec un mélange de raisonnement mathématique et de calculs par un programme qui calculait des configurations de graphes. Du point de vue de la communauté mathématique, ce n'était pas probant comme preuve mathématique. Ce n'était pas entièrement exprimable dans un langage logique satisfaisant. Il y a donc eu plusieurs itérations à ce théorème et il fallut le raffiner, trouver des raffinements d'expression de la preuve, utiliser des techniques fines d'informatique. De plus en plus, on mélange ce procédé de construction de preuve, à un procédé de mise au point de programmes, et donc les environnements de construction de preuves, qui vont servir aux futurs mathématiciens à développer des preuves ambitieuses et vérifiées par machines, utilisent des procédés informatiques sophistiqués de construction d'algorithmes. Il y a donc tout un courant qui est en train de rebâtir un peu l'informatique, comme une forme de mathématiques constructives et d'appliquer cela en grand, à la vérification de preuves mathématiques ; vérification qui n'est pas juste une sorte de spéculation sur la connaissance, car il y a aussi un intérêt économique fort à faire les preuves, en particulier de correction de logiciels, de sécurité de protocoles réseaux, de certification de logiciels de transport, etc.. Elles vont prouver que vous allez pouvoir faire des transactions sécurisées avec votre banque, que vos données personnelles ne vont pas être trouvées par un espion, etc... Ceci génère donc une activité de spécification de processus et, ultimement, de vérification des mathématiques tout à fait conséquente.

Les mathématiques deviennent donc une connaissance dont l'extraction est une donnée économique sérieuse. Pour exactement expliquer l'état de l'art, dans une semaine, nous allons ouvrir à Orsay, un laboratoire commun avec la société Microsoft, dont l'un des axes de recherche est un axe de recherche à long terme sur le développement de mathématiques modulaires de très grande taille. Et en particulier les chercheurs qui collaborent à ce groupe et qui sont justement ceux qui ont déjà fait cet exploit du théorème des 4 couleurs, travaillent à la classification des groupes simples, mais aussi au problème de Kepler sur la façon optimale de ranger des oranges dans des caisses. Ou des boulets de canon, comme dans l'application d'origine ! Je vous remercie.

Gérard HUET
Directeur de recherche INRIA
Membre de l'Académie des Sciences