

7239

IBC96006.PDF :

Irem de Besançon

IREM de LYON

BIBLIOTHEQUE

Université Claude Bernard -LYON I

43, Bd du 11 Novembre 1918

69622 VILLEURBANNE Cedex

~~EXCLU~~

Mathématiques Constructives

Hier et Demain

À propos du théorème des accroissements finis

De la difficulté d'être omniscient

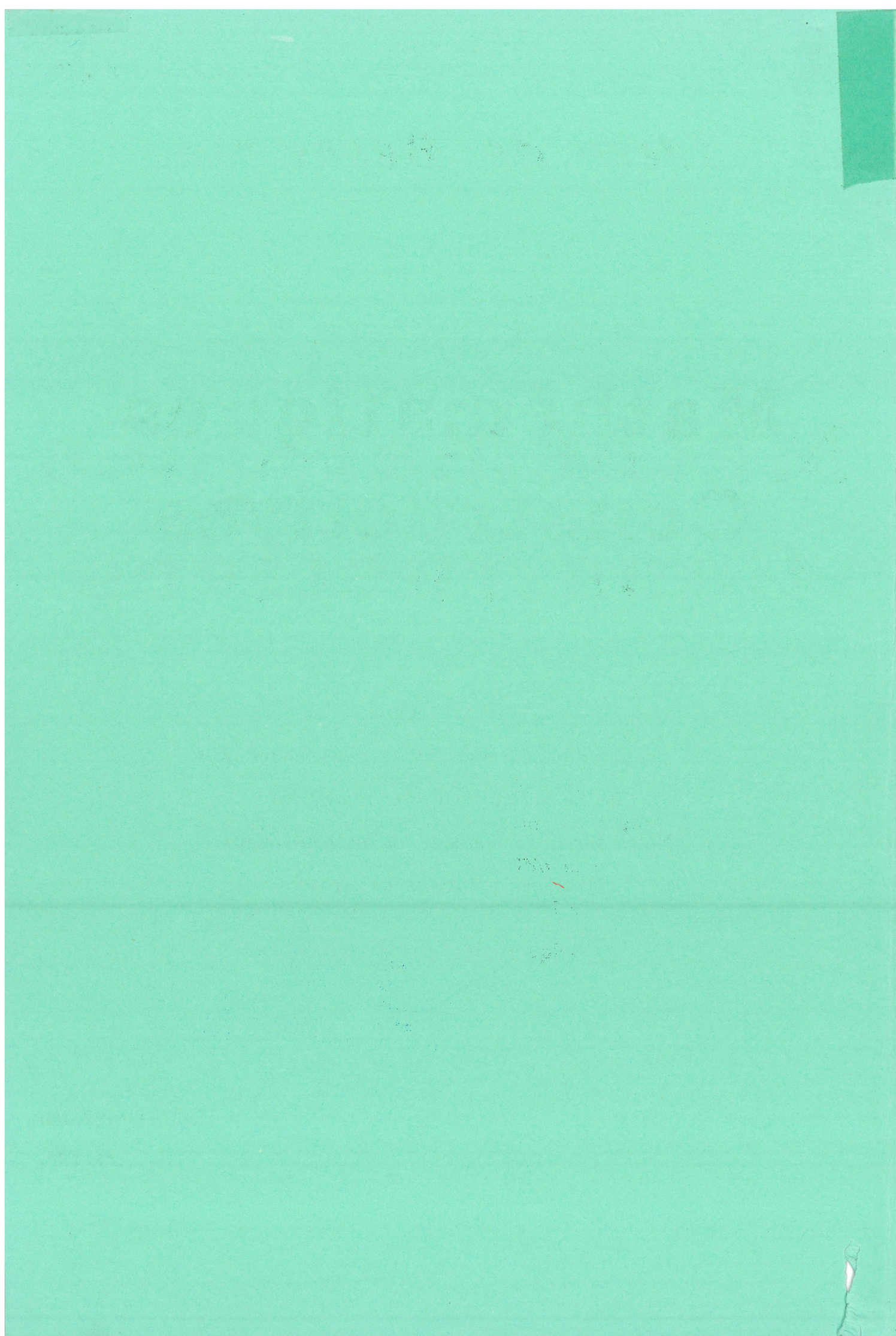
Notes sur le formalisme en mathématiques

Quelques principes de travail

Henri LOMBARDI

ISBN 2-909963-70-5

Mai 1994



Irem de Besançon

Mathématiques Constructives

Hier et Demain

À propos du théorème des accroissements finis

De la difficulté d'être omniscient

Notes sur le formalisme en mathématiques

Quelques principes de travail

IREM de LYON
BIBLIOTHEQUE
Université Claude Bernard - LYON I
43, Bd du 11 Novembre 1918
69622 VILLEURBANNE Cedex

Henri LOMBARDI

Mai 1994

Présentation

Cette brochure rassemble différents textes parus de manière éparse.

Mathématiques constructives Hier et Demain : texte présenté au Colloque Inter Irem "Les démonstrations mathématiques dans l'Histoire" tenu en 1989 à Besançon

À propos du théorème des accroissements finis : texte, remanié, provenant du bulletin IREM de Besançon n°35 (nov. 87)

De la difficulté d'être omniscient : texte présenté au Colloque Inter Irem "Histoires d'infinis" tenu en 1992 à Brest

Notes sur le formalisme en mathématiques : texte, remanié, provenant de la brochure du Groupe d'Épistémologie de Besançon, parue en 1982.

Mathématiques constructives, quelques principes de travail : texte paru dans les bulletins IREM de Besançon n°53 et 54 (mars et mai 94).

Ces différents chapitres sont écrits de manière à pouvoir être lus indépendamment les uns des autres. Aussi la lectrice ne s'étonnera pas de voir certains leitmotivs réapparaître régulièrement.

Je remercie d'avance les lectrices et lecteurs qui me feront part de leurs remarques et critiques.

Henri Lombardi

Mathématiques constructives

Hier et Demain

Introduction

Nous sommes arrivés dans une période où le goût des “grandes abstractions” est un peu retombé en mathématiques.

Cela tient en partie au développement des méthodes numériques efficaces dû à l'explosion informatique.

Par ailleurs, les ordinateurs, gros et moins gros, savent désormais manipuler des expressions formelles compliquées, calculer des intégrales sous forme littérale explicite

Cela a augmenté l'intérêt général pour les méthodes algorithmiques, et pas seulement dans le cadre de l'analyse numérique.

Enfin, la communauté mathématique a toujours été intéressée à rendre effectifs des résultats d'existence “abstraits”. Une preuve d'existence qui donne un moyen algorithmique de construire l'objet (dont on affirme qu'il existe) est considérée par tout le monde comme supérieure à une preuve d'existence purement abstraite.

En 1967, le livre de Bishop “Foundations of Constructive Analysis” a créé une certaine surprise: ce livre démontrait dans la pratique que les résultats de base de l'analyse classique pouvaient être rendus “effectifs”, “algorithmiques”.

Autrement dit, les méthodes algorithmiques ne sont pas seulement praticables en algèbre pour des structures énumérées, mais dans tout le domaine mathématique.

Ce livre est cependant passé pratiquement inaperçu en France. Et alors que tous les mathématiciens sentent spontanément la différence entre une méthode abstraite et une méthode constructive, l'opposition radicale des deux méthodologies n'est pas clairement identifiée.

Trois exemples d'opposition entre les méthodologies cantorienne et constructives

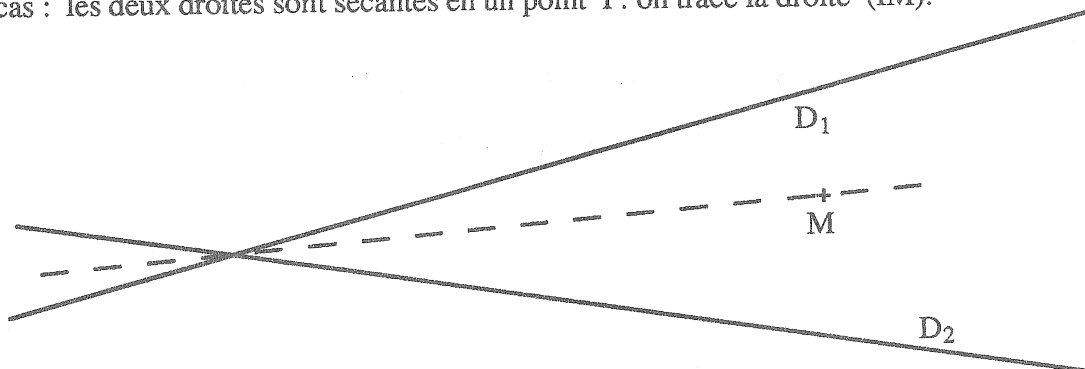
Constructions ... géométriques

On donne deux droites distinctes D_1 , D_2 , et un point M extérieur à ces deux droites. Construire une droite D_3 passant par M et telle que les trois droites soient “en faisceau”.

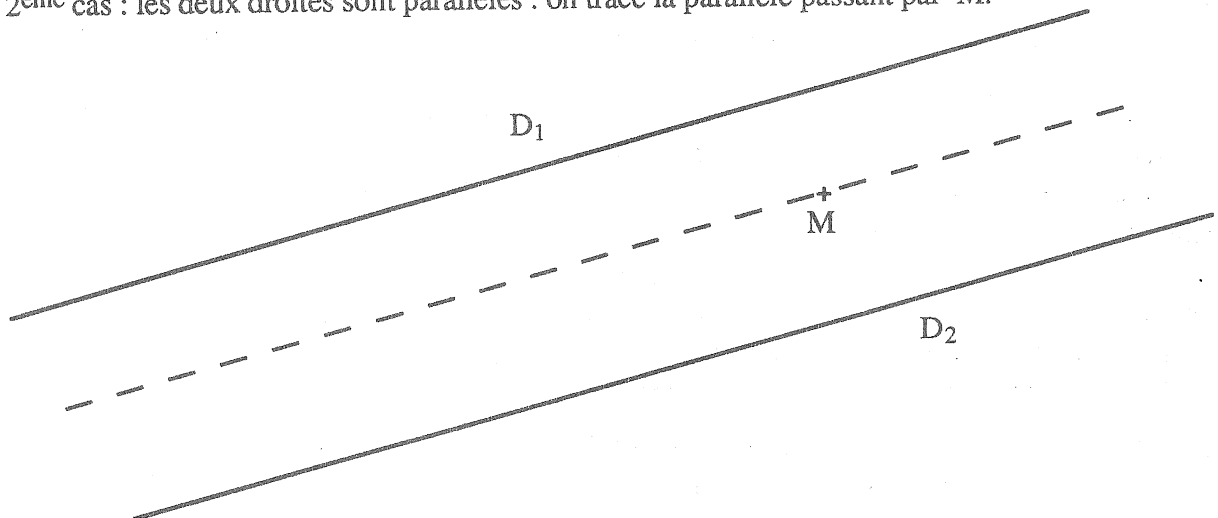
Du point de vue cantorien abstrait habituel

Il n'y a pas à proprement parler de problème de construction. On dira:

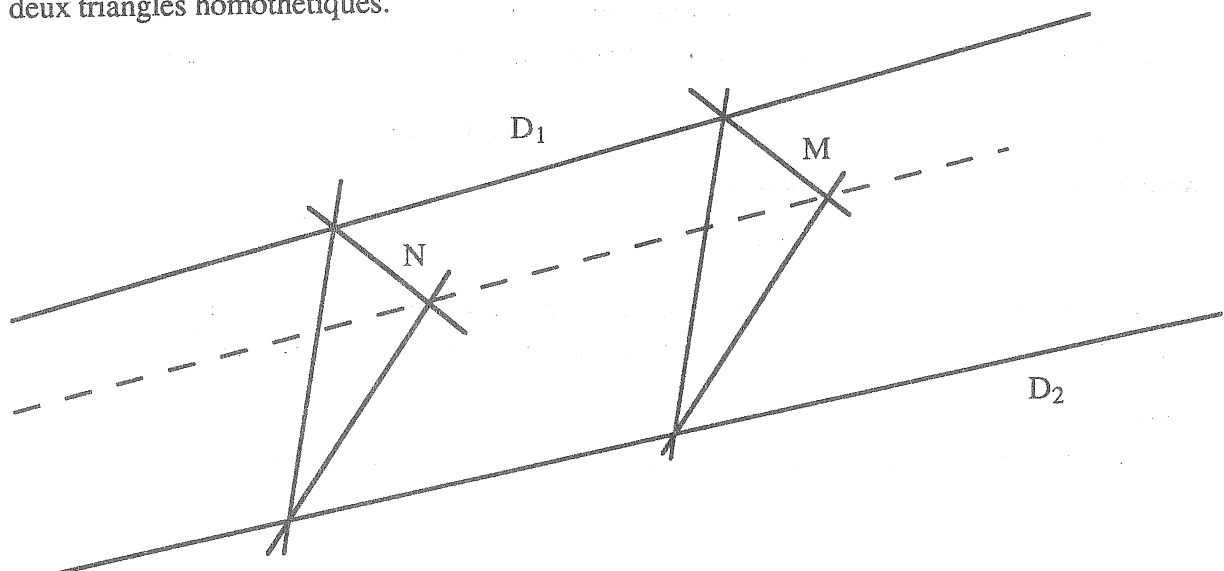
1^{er} cas : les deux droites sont sécantes en un point I : on trace la droite (IM) .



2^{ème} cas : les deux droites sont parallèles : on trace la parallèle passant par M .



Du point de vue du dessinateur qui dispose d'une feuille de papier fini sur laquelle sont tracées les deux droites et le point si les deux droites se coupent en dehors de la feuille de papier, on résout le problème par une construction de 3^{ème} concourante, faisant par exemple intervenir deux triangles homothétiques.



Il est à noter que cette construction donne aussi le bon résultat lorsque les deux droites sont parallèles.

Du point de vue des mathématiques constructives

On considère qu'on dispose d'une feuille de papier fini, mais arbitrairement grande. On n'a

donc aucune méthode *générale* pour décider si deux droites qui *semblent* parallèles sont sécantes ou non. La construction du dessinateur nous sauve cependant la mise. Il y a donc un concept constructif de 3^{ème} concourante, qui recouvre le cas de la 3^{ème} concourante lorsque les deux droites de départ sont sécantes et celui de la 3^{ème} parallèle lorsque les deux droites de départ sont parallèles. (par exemple, on peut définir trois droites “en faisceau”, en disant que le produit des trois symétries par rapport à ces droites doit être une symétrie)

A noter cependant que, pour que la construction fonctionne bien, les deux droites de départ doivent être clairement distinctes.

Ainsi le point de vue constructif apparaît comme une abstraction “raisonnable” de celui du dessinateur, tandis que le point de vue cantorien, qui accepte le plan euclidien comme une totalité préexistante, est une abstraction “purement idéale”.

Remarques

Le dessinateur est confronté à d'autres limitations que celle due à la taille finie, fixée a priori, de sa feuille de papier. Pour lui, en effet :

- deux points distincts mais “trop proches” ne définissent pas une droite
- deux droites sécantes mais “faisant un angle trop petit” ne définissent pas un point d'intersection
- un cercle de rayon trop petit ne peut pas être tracé
- le point de contact entre un cercle et une droite tangente doit être construit (alors qu'il est parfaitement défini comme unique point commun au cercle et à la droite).

En mathématiques constructives, on a des limitations tout à fait analogues:

- on ne peut pas dire “soit D une droite passant par A et B ” sauf si on est assuré que les deux points sont clairement distincts, ou qu'ils sont confondus.
- etc...

Une preuve en arithmétique

On considère le théorème d'existence du PGCD de 2 nombres entiers positifs.

$$\forall a, b \in \mathbb{N}^+ \quad \exists c \in \mathbb{N}^+ \quad \forall d \in \mathbb{N}^+ : \\ d \text{ divise } c \Leftrightarrow d \text{ divise } a \text{ et } b$$

Preuve constructive

- 1) on décrit l'algorithme d'Euclide (divisions successives)
- 2) on démontre qu'il se termine en moins de étapes
- 3) on prouve que le dernier reste obtenu, c est PGCD de a et b
- 4) on améliore un tout petit peu l'algorithme, de manière à ce qu'il fournisse en outre la relation de Bezout $u.a + v.b = c$ (avec u et v dans $\mathbb{Z}$).

Preuve cantorienne

- 1) on démontre le résultat général suivant :
toute partie non vide de $\mathbb{N}^+$ possède un plus petit élément
- 2) on considère la partie I de $\mathbb{N}^+$ définie par

$$I := \{ x \in \mathbb{N}^+ ; \exists u, v \in \mathbb{Z}, u.a + v.b = x \}$$

on considère le plus petit élément c de I , et on démontre facilement que c est PGCD de a et b .

Le théorème est prouvé, et sans effort supplémentaire, on obtient l'existence "abstraite" d'une relation de Bezout.

Commentaires

La preuve cantorienne est plus élégante. Sans doute même éclaire-t-elle mieux le problème.

Cependant, elle ne fournit aucun moyen de construire le PGCD ou la relation de Bezout.

Si on veut rendre constructive la démonstration cantorienne, on procédera comme suit :

- le résultat (1) est vrai constructivement sous la forme suivante :

Si on sait tester l'appartenance d'un entier à une partie explicitement non vide de $\mathbb{N}^+$, alors on sait construire le plus petit élément de cette partie

- pour utiliser le résultat (1) dans la deuxième partie du raisonnement, il faut donc montrer qu'il existe un test d'appartenance pour la partie I considérée.

C'est faisable, au prix de la perte de l'élégance de la démonstration.

En outre, on se rendra facilement compte du fait que l'algorithme sous-jacent à cette démonstration est beaucoup moins performant que l'algorithme d'Euclide : si a et b sont de l'ordre de 1 million, l'algorithme d'Euclide va demander une trentaine d'étapes et l'autre algorithme en moyenne 500 mille étapes.

Un théorème d'analyse

On considère le théorème des valeurs intermédiaires.

Soit $f : [a, b] \rightarrow \mathbb{R}$ une fonction continue avec
 $f(a) < 0 < f(b)$
 alors $\exists c \in]a, b[$ tel que $f(c) = 0$

Les premières démonstrations de ce théorème remontent à Bolzano et à Cauchy.

Bolzano donne une démonstration du type "borne supérieure des x où $f(x) \leq 0$ ". Pour lui, il s'agit de parachever les démonstrations par Gauss du théorème fondamental de l'algèbre. Bolzano remarque que les différentes démonstrations proposées utilisent toutes des arguments du genre "théorème des valeurs intermédiaires".

Or, dit Bolzano, en toute rigueur, l'évidence géométrique ne doit pas être utilisée pour démontrer un résultat dans un domaine où la géométrie n'a rien à voir.

Pour Cauchy, l'évidence géométrique du théorème est suffisamment forte (dans son cours à l'École Polytechnique) mais il prend quand même la peine de donner en annexe une démonstration par dichotomie pour ceux qui veulent une preuve relevant purement de l'analyse.

Nous allons voir qu'en fait, le théorème des valeurs intermédiaires, sous sa forme la plus générale, n'est pas démontrable constructivement. Ainsi, Bolzano, qui pensait avoir achevé la preuve de Gauss, n'avait fait que la moitié du travail. C'est Brouwer, au début du XX^{ème} siècle, qui donnera la première preuve constructive du théorème fondamental de l'algèbre.

Nous allons d'abord présenter l'algorithme classique par dichotomie, avant de le critiquer et de proposer quelques substituts au théorème "abstrait" des valeurs intermédiaires.

*L'algorithme par dichotomie classique***Algorithme Zéro Dichotomie Exacte**Description des variables utilisées

nombres rationnels

a, b : bornes de l'intervalle

u, v : approximation par défaut et par excès de la racine

w : $(u+v)/2$

epsilon : majoration de l'erreur souhaitée

z : valeur approchée de la racine

Signes: (+1, -1 ou 0)

Su, Sv, Sw : signes de la fonction aux points u, v, w

fonction continue sur $[a, b]$:

f : la fonction dont on cherche un zéro

Cet algorithme traite les entrées a, b, epsilon, f et donne en sortie une valeur approchée (à epsilon près) z d'une racine c de f sur $[a, b]$, la racine c ne dépendant pas de epsilon. La fonction f doit changer de signe aux bornes de l'intervalle de départ. L'algorithme donne un résultat sûrement correct si le calcul du signe de $f(x)$ est effectif.

Algorithme détaillé**Module ZÉRO DICHOTOMIE EXACTE****Variables**

entrées : a, b, f, epsilon

retournées : z

locales : u, v, w, Su, Sv, Sw

Débutu $\leftarrow$ a; v $\leftarrow$ b;Su $\leftarrow$ Signe(f(u)); Sv $\leftarrow$ Signe(f(v)) ;**Si** Su.Sv < 0 **alors****Début****Répéter**w $\leftarrow$ (u+v)/2;Sw $\leftarrow$ Signe(f(w));**Si** Sw = 0 **alors début** u $\leftarrow$ w; v $\leftarrow$ w **fin****sinon si** Su.Sw > 0 **alors** u $\leftarrow$ w **sinon** v $\leftarrow$ w;**jusqu'à ce que** $|u - v| < 2 \cdot \text{epsilon}$;z $\leftarrow$ (u+v)/2**fin****sinon** signaler "intervalle mal choisi"**fin***Commentaire*

L'algorithme ne tourne en pratique que si on sait déterminer les signes successifs de $f(w)$. Donc, si f est donnée, de manière absolument générale en tant que fonction uniformément continue sur l'intervalle considéré, l'algorithme ne tourne pas à tout coup: il peut très bien échouer à tester le signe de $f(w)$ pour une certaine valeur de w.

D'ailleurs, cet algorithme fournit un zéro (calculé avec une précision arbitraire) qui ne dépend que de la fonction f. Mais une méthode algorithmique générale traitant en entrée une fonction continue définie sur $[a, b]$ (avec $f(a)$ et $f(b)$ fixés par exemple) et qui fonctionne de

manière *extensionnelle*⁽¹⁾ donne obligatoirement un résultat qui dépend continûment de la donnée f . Ceci parce qu'un algorithme n'a accès qu'à un nombre fini d'informations au cours de son calcul.

Or, manifestement, le calcul du zéro d'une fonction f strictement croissante (pour ne considérer que ce cas) ne peut pas être prolongé *continûment* aux fonctions croissantes "tout court".

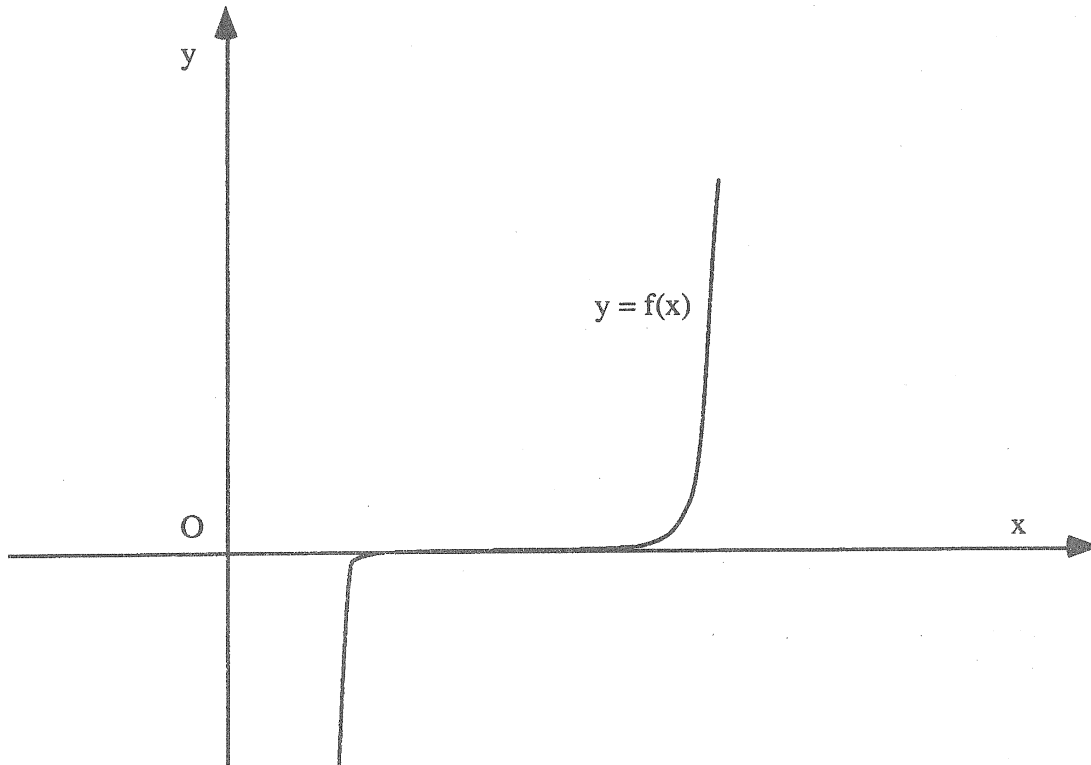


figure 3 : une fonction très voisine de f (pour la norme uniforme) peut avoir un zéro unique très éloigné de celui de f

Quelles sortes d'objets sont un nombre réel, une fonction continue, d'un point de vue algorithmique, constructif ?

Un nombre réel x est connu lorsqu'on connaît, pour chaque entier n un nombre rationnel qui approche x à $1/2^n$.

Une fonction $f : [a, b] \rightarrow \mathbb{R}$ est connue en tant que fonction continue lorsqu'on connaît, pour chaque entier n une approximation rationnelle de f avec la précision $1/2^n$, pour la norme uniforme. Par "approximation rationnelle" on entendra par exemple une fonction linéaire par morceaux rationnels.

Remarque : on traite de la même manière tous les espaces métriques complets séparables.

On voit que de ce point de vue, un nombre réel ou une fonction continue peuvent très bien être considérés comme une entrée ou une sortie d'un algorithme.

Nous sommes fondamentalement dans la même situation que celle décrite pour le plan euclidien: nous avons accès à une partie finie, mais arbitrairement grande, de l'information contenue dans l'objet considéré.

¹ c'est à dire que le résultat ne dépend que de la donnée f en tant que fonction, et non de la manière dont cette donnée est présentée

Le lecteur se demande sans doute ici s'il est bien sérieux d'envisager de faire de l'analyse sans le théorème des valeurs intermédiaires. Nous allons expliquer comment la difficulté peut être tournée.

Trois théorèmes constructifs qui explicitent les significations réelles du théorème des valeurs intermédiaires

Hypothèse : soit $f : [a, b] \rightarrow \mathbb{R}$ une fonction continue avec
 $f(a) < 0 < f(b)$

Théorème 1 (le théorème pour les physiciens)

$$\forall \varepsilon > 0 \exists c \in [a, b] : |f(c)| \leq \varepsilon$$

L'algorithme se déduit aisément de l'algorithme de dichotomie classique: on calcule un rationnel approchant $f(w)$ à $\varepsilon/2$, ce qui permet de situer $f(w)$ sur un intervalle rationnel de longueur $\leq \varepsilon$. On en déduit : $f(w) < 0$ ou $f(w) > 0$ ou $|f(w)| \leq \varepsilon$. On montre que l'algorithme termine en un temps fini en utilisant la continuité uniforme de la fonction f (continuité uniforme qui est connue de manière explicite).

Théorème 2 (le théorème pour les pinailleurs)

Si $f(x)$ est clairement distinct de 0 pour tout $x \in \mathbb{Q} \cap [a, b]$,
 alors $\exists c \in [a, b] : f(c) = 0$

En particulier, il est absurde de supposer que pour tout $x \in [a, b]$, $f(x)$ soit clairement distinct de 0.

En effet, sous l'hypothèse énoncée, l'algorithme par dichotomie classique "tourne": quand un nombre est supposé clairement distinct de 0, il suffit de le calculer avec une précision suffisante pour connaître son signe.

La deuxième affirmation du théorème explicite le contenu constructif du théorème des valeurs intermédiaires classique. On voit que cela présente un intérêt relativement limité.

La première affirmation du théorème permet par exemple de démontrer le théorème de la valeur intermédiaire classique pour une fonction polynôme à coefficients rationnels. Cela ne suffit pas pour traiter tous les polynômes à coefficients réels.

Néanmoins, on peut démontrer le théorème suivant:

Théorème 3 (pour les fonctions analytiques réelles)

Si $x \mapsto f(x)$ est une fonction analytique réelle, alors $\exists c \in [a, b] : f(c) = 0$

La démonstration de ce théorème est relativement difficile, et il faut bien expliciter le contenu algorithmique de l'affirmation "la fonction réelle f est une fonction analytique". Si le but est de démontrer le théorème fondamental de l'algèbre, on pourra se limiter aux fonctions polynômes à coefficients réels, pour lesquelles une preuve relativement simple peut être donnée.

Il faut noter cependant qu'il existe des preuves du théorème fondamental de l'algèbre reposant sur une évidence géométrique : par exemple on pose $z = r e^{i\theta}$, et on regarde comment évolue la courbe fermée obtenue pour r fixé et θ variable, lorsque r varie de 0 à ∞ . C'est sûrement une démonstration beaucoup plus éclairante du théorème, même si elle manque de rigueur dans la mesure où il est difficile d'en déduire un algorithme de calcul d'une racine du polynôme.

Points de repère historiques concernant le débat philosophique

On aura remarqué que la différence entre les deux méthodologies (constructive et cantorienne) repose sur une différence d'attitude à l'égard de l'infini.

Le point de vue constructif tient l'infini pour une abstraction de caractère "négatif" (l'ensemble des nombres entiers n'est jamais épuisé), et se rattache à la tradition grecque de l'infini potentiel.

Le point de vue cantorien estime l'existence d'ensembles infinis "en acte" comme assurée, au moins dans un univers mathématique idéal. En conséquence, on peut raisonner avec les ensembles infinis de la même manière qu'avec les ensembles finis, sans précautions supplémentaires.

Les points de repère qui suivent se veulent tout sauf exhaustifs et objectifs. Ils sont écrits d'un point de vue constructif (parmi d'autres).

L'infini chez les grecs

Chez Euclide, une droite n'existe jamais "en entier". Il y a seulement des segments de droites, qu'on peut prolonger "à volonté".

Le nombre $\sqrt{2}$ ne peut pas être nommé, il n'a pas le statut d'un nombre parce qu'il ne possède pas de description arithmétique finie (ce n'est pas une fraction).

Une théorie de la comparaison des rapports de grandeurs est développée, qui permet de parler des nombres réels sans jamais les nommer comme "infinis actuels". Comme en mathématiques constructives, l'égalité est de nature négative (double réduction à l'absurde), alors que les inégalités strictes ont un caractère positif.

Cette distinction entre énoncés de caractère positif et énoncés de caractère négatif disparaît si l'on admet que "deux négations valent une affirmation".

Le paradoxe de Zénon nous parle aussi de l'infini. Il peut être interprété comme une réfutation de la possibilité d'existence de l'infini actuel.

La crise des infinitésimaux

L'efficacité du calcul différentiel et de la méthode des infinitésimaux prépare le terrain pour la reconnaissance d'un statut "ordinaire" accordé à l'infini. C'est en raisonnant sur des infiniment grands et infiniment petits *comme si* c'était des quantités finies, c'est à dire en se débarrassant des scrupules imposés par la tradition grecque, qu'on obtient, par des méthodes uniformes et extraordinairement efficaces, des résultats qui auparavant étaient inaccessibles ou dans le meilleur des cas demandaient une ingéniosité toujours renouvelée.

Les notions de nombre réel et de fonction s'avèrent des notions fondamentales.

Cependant, on ne trouve pas de justification convaincante pour ces objets qui sont des sortes d'infinis en acte.

La crise sera résolue en chassant les infinitésimaux au profit de la notion de limite, mais en accordant un statut à part entière aux nombres réels en tant qu'infinis actuels.

Il faudra attendre l'analyse non standard d'A. Robinson dans les années 60 pour s'apercevoir que les infinitésimaux ne sont ni plus ni moins sulfureux que les nombres réels. Dans sa version Internal Set Theory, l'analyse non standard peut aujourd'hui être considérée comme une meilleure heuristique de l'analyse constructive que l'analyse classique.

La crise des géométries non euclidiennes

L'existence des géométries non euclidiennes, tout aussi cohérentes que la géométrie euclidienne, introduit un bouleversement conceptuel concernant la notion de vérité, et la place des mathématiques.

Avant les géométries non euclidiennes, on pouvait croire à l'existence d'une vérité géométrique "absolue", que l'esprit humain, par la seule force de son raisonnement, arrivait à maîtriser.

Après, tout change. L'esprit humain ne fait plus que proposer des modèles mathématiques imparfaits pour une description proprement humaine d'une réalité extérieure fuyante et insaisissable dans sa totalité. Il va maintenant falloir mesurer la somme des angles de très grands triangles et regarder des étoiles cachées derrière le soleil pour savoir dans quel univers on vit. La vérité perd son caractère absolu pour devenir une construction proprement humaine et donc très relative. A tous points de vue, nous ne sommes plus au centre du monde, mais bel et bien perdus dans un coin de galaxie.

Cette notion de vérité mathématique construite par l'esprit humain est au coeur de la problématique intuitionniste de Brouwer.

Cantor et l'avènement de l'infini actuel

On a du mal à imaginer à quel point Cantor heurtait de front les conceptions établies en introduisant la théorie des ensembles infinis "actuels". C'était à l'époque un véritable acte de foi. Ses articles étaient systématiquement refusés par Kronecker. Des affirmations telles que « l'ensemble $\mathbb{N}$ est strictement plus petit que l'ensemble $\mathbb{R}$ » semblaient relever de la folie. Et Cantor lui-même avait du mal à admettre que $\mathbb{R}$ et $\mathbb{R}^2$ ont le même cardinal.

Cependant, c'est bien grâce aux infinis actuels de Cantor qu'on a pu donner une "construction" de l'ensemble des nombres réels, ou la définition générale de la notion de fonction.

Les paradoxes de la théorie des ensembles et les avatars de l'hypothèse du continu

Les constructions d'infinis autorisés par la théorie des ensembles de Cantor sont a priori aberrantes: imaginez par exemple que vous mettez une relation de bon ordre sur $\mathbb{R}$, puis que par récurrence transfinie sur ce bon ordre vous construisez à chaque étape l'ensemble des parties de la réunion des ensembles précédemment construits, en ayant démarré avec l'ensemble $\mathbb{N}$ au bout du compte vous obtenez quelque chose de vraiment très très très **gros**, et dont l'utilité mathématique est tout à fait contestable.

Certains ensembles infinis s'avèrent de toute manière trop grands, trop infinis: par exemple

$$X = \{ x ; x \text{ est un ensemble tel que } x \notin x \}$$

Ensemble pour lequel on a $X \in X \Leftrightarrow X \notin X$.

On se tirera d'affaire en décrétant que les ensembles trop infinis ne sont pas des ensembles, mais des classes⁽²⁾. La théorie formelle correspondante n'a depuis donné lieu à aucune contradiction logique.

Par ailleurs Brouwer développe une réfutation systématique de la notion d'infini actuel et met en pratique des mathématiques où le principe du tiers exclu n'est plus admis pour les affir-

² Un ensemble peut être élément d'une classe, mais les classes "trop infinies" ne sont éléments d'aucun ensemble

mations correspondant à une infinité de vérifications. La logique sous-jacente sera formalisée par Heyting, sous le nom de logique intuitionniste.

Enfin, la comparaison des infinis selon leur taille va réserver quelques surprises.

Cantor passera la fin de sa vie à essayer, sans succès, de démontrer “l’hypothèse du continu” : il n’y a pas de cardinal strictement compris entre celui de $\mathbb{N}$ et celui de $\mathbb{R}$.

Skolem démontrera que toute théorie mathématique formelle cohérente possède un modèle dont le cardinal est celui de $\mathbb{N}$: dans un tel modèle, $\mathbb{R}$ n’admet pas “plus” d’éléments que $\mathbb{N}$, et il existe une bijection entre $\mathbb{N}$ et $\mathbb{R}$... mais elle ne fait pas partie du modèle.

Plus tard K. Gödel et P. Cohen démontreront que l’hypothèse du continu est indépendante des axiomes communément admis pour la théorie des ensembles.

Face à ce genre de résultats, deux attitudes opposées sont développées.

Les uns, comme Skolem, estiment que la comparaison des cardinaux a un caractère très relatif. Pour eux, l’infini ne correspond à aucune réalité et est simplement une manière de parler.

Les autres, comme Gödel, s’en tiennent à un point de vue “réaliste” : un univers mathématique cantorien existe bel et bien, et dans cet univers, l’hypothèse du continu est nécessairement vraie ou fausse. En conséquence, ils estiment que de nouveaux axiomes raisonnables doivent être cherchés, qui décideront vraie ou fausse l’hypothèse du continu.

Du point de vue constructif, $\mathbb{R}$ est un infini potentiel *plus compliqué (et non pas plus grand)* que $\mathbb{N}$. Mais il y a aussi des parties de $\mathbb{N}$ qui sont plus compliquées que $\mathbb{N}$, et en particulier il n’est pas absurde de supposer que l’infini potentiel $\mathbb{R}$ est isomorphe à une partie compliquée de l’infini potentiel simple $\mathbb{N}$ (cette hypothèse est admise comme vraie par l’école constructive russe héritière de Markov).

Le programme de Hilbert

Hilbert tient les critiques de Brouwer pour sérieuses. Mais ce qui lui importe, c’est avant tout de faire des mathématiques. Or les mathématiques sont plus faciles à faire dans le paradis de Cantor que dans l’enfer de Brouwer.

Hilbert tient le langage suivant : finalement peu nous importe de savoir si les infinis actuels existent ou non, si l’hypothèse du continu est vraie ou fausse, si elle a un sens ou si elle n’en a pas ; ce qui nous importe, c’est de savoir si, en utilisant la théorie des ensembles infinis, on est assuré de ne jamais démontrer des énoncés qui ont du sens mais qui seraient faux. C’est exactement la même attitude que vis à vis des nombres imaginaires qui servent à trouver la racine réelle d’une équation du troisième degré : l’important est avant tout que, une fois le calcul terminé, et les nombres imaginaires évaporés, le résultat soit juste.

Autrement dit, si on pouvait réduire l’infini mathématique à n’être qu’une manière de parler, on serait pleinement satisfaits.

Pour cela, il faut considérer une théorie purement formelle, dans laquelle on puisse librement utiliser les infinis de Cantor d’une part, et dans laquelle on puisse écrire les énoncés mathématiques qui “ont sûrement du sens”, d’autre part.

Ensuite, il faut, par des méthodes constructives, démontrer que tout énoncé “ayant du sens” et démontré comme vrai dans la théorie formelle, est vrai dans la réalité.

La première théorie à tester est une théorie très simple (la théorie formelle dite *de Peano*) où on peut tout juste écrire quelques énoncés concernant les entiers naturels, mais où la logique du tiers exclu est admise, même pour des énoncés correspondant à une infinité de vérifications. Ensuite, il faudra passer à des théories plus sophistiquées, en espérant un jour traiter la théorie des ensembles elle-même.

Gödel apportera deux réponses contradictoires au problème posé.

La première réponse est que, pour de qui concerne la théorie de Peano, la logique *avec tiers exclu* n'introduit aucune contradiction. En particulier, comme la théorie de Peano sans tiers exclu (l'arithmétique de Heyting) est admise comme consistante par tout le monde, on peut être assuré que la théorie de Peano est non contradictoire (Hilbert gagne donc par un point à zéro). Gödel ira plus loin et proposera de donner un sens constructif aux énoncés et aux preuves de la théorie de Peano (Hilbert gagne par deux points à zéro).

Néanmoins, on n'a pas réussi pour le moment à faire le travail analogue pour des théories formelles plus sophistiquées que celle de Peano; et cette dernière est bien trop pauvre pour pouvoir être prise comme base du travail mathématique ordinaire.

La deuxième réponse est que, pour toute théorie formelle qui prétend décrire au moins $\mathbb{N}$, la cohérence de la théorie ne peut pas être démontrée avec les seuls moyens formalisés dans la théorie.

A fortiori, la théorie des ensembles semble bien ne jamais pouvoir être prouvée consistante dans la mesure où on a incorporé dans son formalisme toutes les méthodes de démonstrations connues, mêmes celles qui sont le plus douteuses (deux points à un).

En fait, le théorème d'incomplétude de Gödel milite en faveur d'une vérité mathématique non préétablie, mais en état de construction permanente.

Une réponse d'une toute autre nature est apportée par Bishop en 1967 avec son livre d'analyse constructive: Cantor n'est pas le paradis, et Brouwer n'est pas l'enfer. En ne mettant en oeuvre que les idées les plus incontestables de Brouwer, on fait une mathématique, certes un peu plus difficile, mais où tous les énoncés ont du sens, où tous les théorèmes sont incontestables (par toutes les écoles de pensée), et où, simplement, on regarde un peu plus en détail la signification algorithmique réelle des énoncés classiques. (deux points partout).

Le point de vue formaliste

Il s'agit d'une attitude repli frileux, bizarrement adoptée par Bourbaki dans son introduction, et qui n'a en réalité que bien peu d'adeptes³. On peut la résumer par "courage, fuyons!", fuyons la question du sens puisqu'elle nous embête. Vous croyiez naïvement faire *des* mathématiques dans le but de construire des modèles abstraits pour le mouvement des planètes, la propagation de la chaleur où les éruptions volcaniques. Vous vous trompiez, vous êtes en train de jouer à un nouveau jeu, fort intelligent, très sophistiqué, qui s'appelle *la* mathématique, et dont les règles ont été édictées, 4000 ans a posteriori mais pour l'éternité à venir, par quelques très grands savants dans leur infinie sagesse, très grands savants qui, comble de modestie, ne donnent même par leur nom sur la couverture. Les situations (parfois encore appelées énoncés) gagnantes de ce jeu subtil s'appellent "théorèmes". Amusez-vous bien. Plus les théorèmes démontrés auront l'air d'avoir du sens et plus ce sera amusant. Mais gardez vous bien de croire qu'ils aient réellement du sens.

Et demain ?

La situation actuelle est dominée par la pragmatisme. Dans la mesure où les résultats de nature effective sont de plus en plus recherchés, on peut penser que la méthodologie constructive va finir par s'imposer comme la méthodologie normale. Néanmoins, les facilités offertes par le tiers exclu et l'axiome du choix sont grandes, et les fabricants de théorèmes ne sont pas prêts à

³ La majorité des mathématiciens, y compris sans nul doute les rédacteurs de Bourbaki, est sur une position proche de celle de Gödel.

lâcher la proie pour l'ombre. En fait le programme de Hilbert reste à réaliser : démontrer que, si on délimite convenablement le cadre de travail, l'analyse et l'algèbre classiques, ou mieux, non standards, ne conduiront jamais à des résultats faux sur les énoncés qui ont du sens.

Quelques conclusions

Ce que ne sont pas les mathématiques constructives :

- une entreprise de déstabilisation de l'éducation nationale
- la volonté d'être encore plus rigoureux que Bourbaki, et encore plus difficile à comprendre
- un rejet des mathématiques classiques

Ce que sont les mathématiques constructives :

- une volonté de donner du sens aux énoncés mathématiques
- une bonne heuristique pour la recherche d'algorithmes performants
- l'adoption des résultats classiques (cantoriens) à titre d'heuristique pour la recherche de résultats ayant sûrement du sens
- une conception algorithmique des êtres mathématiques et de la vérité (pour les énoncés concernant ces êtres mathématiques)

Petit tableau comparatif des méthodologies cantorienne et constructives

point de vue cantorien	point de vue constructif
utiliser des méthodes abstraites et puissantes pour obtenir de nombreux résultats, même très abstraits	donner des algorithmes pour résoudre des problèmes concrets, ou, du moins, idéalement concrets
un univers mathématique cantorien idéal existe: les êtres mathématiques y sont préexistants la vérité est préexistante dans cet univers, le but des mathématiques est de la découvrir	les êtres mathématiques sont des constructions humaines la vérité concernant ces êtres est elle-même l'objet d'une construction
acceptation de l'infini actuel	refus de l'infini actuel, acceptation de l'infini potentiel
raisonnement par l'absurde pour démontrer un théorème d'existence	toute démonstration d'existence fournit, en filigrane, un algorithme pour construire l'objet
refus du tiers cas : par exemple $\forall x \in \mathbb{R} (x = 0 \text{ ou } x \neq 0)$ est un théorème des mathématiques cantorienne, alors même qu'aucun algorithme connu ne permet de le réaliser	acceptation du pouvoir limité du raisonnement humain, qui est de nature finie, algorithmique: le théorème en face n'est pas démontrable constructivement on peut tout juste démontrer le théorème suivant (sans intérêt) $\neg \exists x \in \mathbb{R} (x = 0 \text{ et } x \neq 0)$
une preuve constructive est toujours acceptable par un cantorien, mais elle semble souvent inutilement compliquée	il est souvent bien difficile d'attribuer une signification constructive à une preuve classique
la notion d'ensemble est la notion de base, prémathématique, non définie	les notions de base, non définies, sont celles de construction et d'entier naturel
$\forall x \exists y$ a un sens purement abstrait	$\forall x \exists y$ a le sens d'une construction

À propos du théorème des accroissements finis

Introduction

Sans doute avez-vous un cousin qui ne fait pas de mathématiques mais qui conduit une voiture. La prochaine fois que vous le voyez demandez lui à brûle pourpoint :

« Suppose que tu roules pendant une heure entre 30 et 40 km /h, combien penses-tu que tu auras fait de kilomètres ? ». (1)

La réponse sera sans doute

« Eh, tu me prends pour un imbécile ? »

ou bien

« Je ne vois pas ce qu'il y a de drôle. »

Dans le premier cas, faites vous tout petit (il serait absurde de se fâcher avec son cousin pour si peu).

Dans le deuxième cas, vous pouvez enchaîner

« Ce qu'il y a de drôle, c'est qu'on le démontre en mathématiques, qu'on a fait entre 30 et 40 kilomètres ».

Et vous aurez peut-être fait faire un grand progrès au développement de l'esprit mathématique dans toutes les couches de la société.

Si vous indiquez en outre qu'il s'agit d'un théorème assez difficile à démontrer, vous aurez sans doute créé un nouvel adepte des démonstrations rigoureuses. Si vous êtes enseignant en mathématiques⁽¹⁾ en terminales vous aurez la joie d'avoir à démontrer l'évidence (1) ci-dessus au moyen de l'évidence (2) suivante:

« Suppose que tu n'avances à aucun moment, est-ce que tu penses que tu as une chance d'avoir reculé ? » (2).

Bref, vous l'avez compris, il s'agit de faire quitter à vos élèves la planète terre pour les emmener dans la planète "mathématiques formelles".

Et si vos élèves n'y pigent que couic, et ne recherchent que des recettes, demandez-vous si par hasard, la nécessité de démonstrations convaincantes ne devrait pas être illustrée sur des exemples pour lesquels le résultat n'est pas a priori évident.

En fait la "démonstration" du théorème des accroissements finis, démontre, non pas la réponse à l'évidente question (1), mais l'adéquation du modèle "nombres réels, fonctions dérivables" pour la réalité "voiture qui roule avec un compteur de vitesse".

Cette adéquation, on le sait, n'est d'ailleurs que partielle et approximative (il est douteux que $\mathbb{R}$ modélise parfaitement l'écoulement du temps, ou l'espace sur une ligne).

Bref d'une part, il est absurde de vouloir démontrer le théorème des accroissements finis en terminales, d'autre part, on ne devrait jamais l'enseigner (en DEUG par exemple) en tant que preuve d'une chose évidente, mais en tant que "vérification de l'adéquation d'un modèle mathématique à la réalité qu'il veut représenter".

¹ c'était en l'année 1987 où a été écrit cet article

Première discussion

Plaçons nous au niveau du DEUG, et supposons que nous ayons déjà fait sentir suffisamment en quoi la structure $\mathbb{R}$ est un assez bon modèle pour certaines choses, et en quoi une fonction réelle uniformément continue sur un intervalle $[t_0, t_1]$ est un assez bon modèle pour la description du mouvement d'un mobile sur une ligne.

Nous en arrivons au chapitre "dérivée comme modélisation de la notion de vitesse".

Nous parlons de la vitesse moyenne, et nous arrivons au point : qu'il serait agréable d'avoir une fonction "vitesse instantanée".

Si nous utilisons le réflexe de Pavlov, nous aurons tendance à débiter ce qu'on nous a enseigné quand nous étions jeunes, c'est-à-dire en fait ce qu'une certaine école mathématique nous a enseigné comme étant "la vérité".

Dans ce cas nous définirons, sans plus nous poser de problème, la vitesse instantanée comme limite de la vitesse moyenne au sens de la définition usuelle.

Si nous prenons un tout petit peu de recul, et si nous nous débarrassons de cet autre réflexe de vouloir toujours rechercher des hypothèses minimales (même quand, dans la pratique mathématique, les problèmes ne se présentent jamais avec ces seules hypothèses minimales), nous serons amenés à nous demander si la définition minimale est, après tout, bien "réaliste". En classe de physique (seconde ou après), la vitesse à l'instant t_0 est mesurée expérimentalement comme étant:

$$(f(t_0 + \Delta t) - f(t_0 - \Delta t)) / 2 \Delta t$$

avec Δt petit. Ceci suggérerait une aussi bonne définition minimale, de la "dérivée de la fonction f au point t_0 " qui serait:

$$f'(t_0) = \lim_{h \rightarrow 0} \frac{f(t_0 + h) - f(t_0 - h)}{2h} \quad (3)$$

Avec cette nouvelle définition, certaines fonctions qui étaient non dérivables en t_0 , deviennent dérivables, comme par exemple la fonction $f(t) = |t|$ (qui devient dérivable en 0 avec $f'(0) = 0$).

Évidemment, vous sentez bien que cette définition est peut-être "un peu trop" minimale⁽²⁾. Mais pourquoi alors la définition usuellement donnée en classe de mathématiques serait-elle "juste assez minimale mais pas trop"? Si on ne veut pas utiliser des arguments purement esthétiques ("c'est plus élégant", "ça donne de plus jolis théorèmes", "ça me plaît mieux", "si vous remettez tout en cause, vous risquez de recevoir votre poing dans la figure par vos élèves à la sortie, près du sous-bois⁽³⁾" etc...) on est bien obligé de se fatiguer un peu et d'ouvrir une discussion qui, ordinairement, est renvoyée dans les "notes historiques", mais qui, du point de vue de la formation mathématique, devrait être partie intégrante du cours.

Si la 2^{ème} définition est "trop" minimale, la 1^{ère} l'est aussi, nécessairement, et pour la même raison: le fait de fixer, arbitrairement, un accroissement égal de chaque côté, est déplaisant pour une raison de fond (et pas seulement esthétique). De même, le fait de fixer, arbitrairement, un

² Avec cette définition le "théorème de Rolle" devient faux, et cela a de quoi chagriner bien des gens

³ cf. une déclaration de Jacques Médecin sur "les instituteurs marxistes" qui les menaçait en ces termes, ... depuis, il a d'autres chats à fouetter

accroissement égal à h d'un côté et à 0 de l'autre, est encore plus déplaisant. Nous en arriverons donc à la définition un peu moins minimale suivante (f étant supposée continue):

la dérivée de f au point t_0 est la limite suivante, si elle existe

$$\lim_{h,k \rightarrow 0, h \neq k} \frac{f(t_0 + h) - f(t_0 + k)}{h - k} \quad (4) \quad (4)$$

Une démarche plus systématique

Jusqu'à présent, nous avons raisonné, par jeu, en digression à partir de la définition "standard".

Mais nous avons en quelque sorte continué à jouer le même jeu, en ce sens que nous n'avons pas procédé systématiquement, ce qui nécessite de commencer par préciser les propriétés que nous voulons voir vérifier par le modèle mathématique.

Personnellement, il me semble que la propriété que nous voulons voir vérifier à la fonction dérivée est la propriété (1). Celle justement que votre cousin, qui ne fait pas de mathématique, trouverait absolument aberrant qu'elle ne soit pas vérifiée.

En langage mathématique formalisé, nous obtenons la traduction (5) de la propriété (1)

La fonction $g : [t_0, t_1] \rightarrow \mathbb{R}$, uniformément continue, sera dite fonction dérivée de la fonction $f : [t_0, t_1] \rightarrow \mathbb{R}$ si on a :

$$\forall a, b \in [t_0, t_1] \quad \forall m, M \in \mathbb{R} \quad \text{avec } a < b \text{ et } m < M$$

$$g([a, b]) \subset [m, M] \Rightarrow \frac{f(b) - f(a)}{b - a} \in [m, M]$$

Insistons sur le fait que (5) est **exactement la traduction de (1)**, avec l'a priori de modéliser au moyen de fonctions uniformément continues de $[t_0, t_1]$ vers $\mathbb{R}$. (5)

Notons que la définition (5) implique que g est la dérivée au sens "usuel" (preuve donnée un peu plus loin).

Expliquons ici la suite de l'article:

- tout d'abord nous montrons que la définition (5) implique une propriété (6) "locale au sens uniforme", qui est la définition de la dérivabilité en mathématiques constructives;
- ensuite nous montrons que (6) implique (5);
- ensuite nous vérifions que (6) est une version très agréable, pour laquelle les "théorèmes classiques" se démontrent très facilement;
- une conclusion est que les fonctions usuelles vérifient bien "le théorème des accroissements finis" c'est-à-dire (5), et que ceci a été démontré par une preuve simple, et constructive (contrairement à la preuve que subissent les étudiants);

⁴ l'appellation officielle pour cette propriété est : f est strictement dérivable en t_0

⁵ Le "réflexe minimaliste" inciterait à ne pas demander la continuité uniforme, au moins pour la fonction g . Sans vouloir discuter cette question en tant que telle, je signalerai que, dans la mesure où on modélise au moyen de fonctions, il est à peu près inévitable de s'en tenir aux fonctions uniformément continues (pour un segment borné) ceci parce que:

- (a) la continuité est "dans la nature de la modélisation" (les mesures en physique sont toujours "approchées", sauf lorsque la variable est dans un ensemble discret),
- (b) l'uniforme continuité est la forme manipulable de la continuité.

- nous comparerons enfin avec la démonstration usuelle de (5) donnée en général avec des hypothèses minimales.

Équivalence de la définition "globale" avec une définition "locale uniforme"

La définition (5) peut être qualifiée de globale. Elle implique la propriété (6) suivante, "locale au sens uniforme", qui est la définition de la dérivabilité donnée en mathématiques constructives.

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x, y \in [t_0, t_1] : \\ |y - x| \leq \delta \Rightarrow |f(y) - f(x) - g(x)(y - x)| \leq \varepsilon |x - y| \quad (6)$$

En effet si on a $|x - y| \leq \delta \Rightarrow |g(y) - g(x)| \leq \varepsilon$
alors "en fixant x " on obtient :

$$|x - y| \leq \delta \Rightarrow g(y) \in [g(x) - \varepsilon, g(x) + \varepsilon]$$

et en appliquant (5) pour l'intervalle $[x - \delta, x + \delta] \cap [t_0, t_1]$ on obtient (6).

On notera que (6) implique que $g(x)$ est la dérivée de f au point x "au sens usuel" mais aussi au sens de la stricte dérivabilité (définition (4)).⁽⁶⁾

Avant de démontrer $(6) \Rightarrow (5)$ notons que (6) admet la formulation équivalente suivante :

la fonction $z \mapsto g(z)$ est limite uniforme, lorsque y et x distincts tendent vers z ,
de la fonction "taux d'accroissement de f "⁽⁷⁾

$$h(x, y) := (f(y) - f(x)) / (y - x) \quad (7)$$

Or cette définition peut être lue comme suit :

la fonction "dérivée" est la limite de la "fonction vitesse moyenne" lorsque l'intervalle de temps tend vers 0.

Autrement dit, du point de vue strictement mathématique, la phrase "la vitesse instantanée est la limite de la vitesse moyenne" recèle un flou suffisamment important pour laisser ouvertes une foultitude d'interprétations très diverses, aussi bien celle correspondant à la définition usuelle que celle correspondant à la définition constructive.

Passons à la preuve que $(6) \Rightarrow (5)$.

Supposons (6), et, avec $a, b \in [t_0, t_1]$, supposons $g([a, b]) \subset [m, M]$. On veut montrer que le taux d'accroissement de la fonction f sur l'intervalle $[a, b]$ est compris entre m et M . Soit $\varepsilon > 0$, il suffira de montrer que le taux d'accroissement est inférieur à $M + \varepsilon$ (la même démonstration prouverait qu'il est supérieur à $m - \varepsilon$).

Considérons un δ convenant à ε dans (6), et découpons l'intervalle $[a, b]$ en intervalles $[x_i, x_{i+1}]$ de longueur $\leq \delta$.

On a alors

$$|f(x_{i+1}) - f(x_i) - g(x_i)(x_{i+1} - x_i)| \leq \varepsilon |x_{i+1} - x_i|$$

d'où

$$(f(x_{i+1}) - f(x_i)) / (x_{i+1} - x_i) \in [m - \varepsilon, M + \varepsilon]$$

⁶ On peut montrer, qu'une fonction qui admet une dérivée "au sens usuel" uniformément continue, est dérivable au sens (6). On peut aussi montrer (au moins en mathématiques classiques) qu'une fonction qui est partout strictement dérivable est dérivable au sens (6)

⁷ On peut donc écrire (modulo une petite modification en t_1) que g est limite uniforme de la suite de fonctions : $h_n(x) := n(f(x + 1/n) - f(x))$. Cela montre que l'hypothèse "g uniformément continue", nécessaire dans (5), est superflue dans (6)

en particulier

$$f(x_{i+1}) - f(x_i) \leq (M + \varepsilon) (x_{i+1} - x_i)$$

et enfin

$$f(b) - f(a) \leq (M + \varepsilon) (b - a)$$

Il est bon de signaler que cette preuve est essentiellement celle que Cauchy donne pour le théorème des accroissements finis. C'est en fait une preuve simple et naturelle, celle qui va de soi lorsqu'on a formalisé la notion de limite et qu'on cherche à en vérifier l'efficacité. Que cette preuve de Cauchy soit réputée fautive est à vrai dire un grand sujet d'étonnement, car la définition qu'il donne de la fonction dérivée (il ne donne pas celle de la dérivée en un point) est trop imprécise pour qu'on puisse trancher entre l'interprétation maintenant usuelle et l'interprétation (6).

Efficacité de la définition "locale uniforme"

La définition (6) "locale uniforme" est celle donnée en mathématiques constructives (cf. [BB]). C'est une définition "très efficace" parce qu'elle permet de donner des démonstrations constructives des théorèmes essentiels sur les fonctions dérivées.

Nous laissons à la lectrice le soin de vérifier que les preuves classiques concernant la dérivabilité d'une somme, d'un produit ou d'un quotient, ou celle qui donne l'existence d'une primitive pour une fonction uniformément continue, fonctionnent pratiquement sans aucun changement avec la définition (6), et sont des démonstrations entièrement constructives.

Ici il faut que nous expliquions un peu en quoi une preuve peut être déclarée constructive. Par exemple avec le théorème des accroissements finis lui-même.

Nous le prenons sous la forme équivalente suivante :

$$(TAF1) \quad \text{Si la fonction } f \text{ est dérivable au sens (6) et si } f' \geq 0 \text{ sur } [a, b] \text{ alors } f(b) \geq f(a)$$

Si nous examinons en détail la démonstration que nous avons donnée, elle donne en fait un résultat qui a une signification algorithmique plus forte.

$$(TAF2) \quad \text{Si } f \text{ est dérivable au sens (6) et si } f(b) < f(a), \text{ alors on peut expliciter en un temps fini un } x \text{ dans } [a, b] \text{ tels que } f'(x) < 0$$

Plus précisément cette démonstration fournit le plan d'un algorithme qui traite les données f , a , b , (la fonction f étant dérivable au sens (6)) et fournit en sortie un rationnel $r \in [0, 1]$ tel que $f'(a + r(b - a)) < 0$.⁽⁸⁾

À partir de la définition "usuelle" de dérivée, il est également possible de fournir une preuve algorithmique de (TAF1), mais nettement moins intuitive et dont le caractère algorithmique est

⁸ Un problème qui se pose est "comment un algorithme traite-t-il une fonction uniformément continue en tant que donnée ?". C'est-à-dire encore: quelle est la forme "manipulable" (algorithmique) prise par une fonction continue $[a, b] \rightarrow \mathbb{R}$? Une possibilité est la suivante.

Nous avons besoin de 2 choses : d'une part, le module de continuité uniforme de f , qui est une fonction $m_c : \mathbb{N} \rightarrow \mathbb{N}$ vérifiant : $(|x - y| \leq m_c(n)) \Rightarrow (|f(x) - f(y)| \leq 1/2^n)$. Et d'autre part, pour chaque $n \in \mathbb{N}$ et chaque nombre rationnel $t \in [a, b]$, nous devons connaître un rationnel z vérifiant $|f(t) - z| \leq 1/2^n$.

Ainsi, un algorithme qui traite "une donnée qui est une fonction uniformément continue f " peut être conçu comme un algorithme utilisant 2 "oracles" :

le premier répond $m_c(n)$ lorsqu'on lui pose la question "module de continuité pour l'écart $1/2^n$?", le deuxième répond z (rationnel) lorsqu'on lui pose la question "valeur de f au rationnel t avec la précision $1/2^n$?" ($t \in \mathbb{Q} \cap [a, b]$, $n \in \mathbb{N}$).

moins convaincant. En effet, cette preuve ne fournit pas (TAF2) mais une version un peu plus faible (TAF3), qui implique aussi (TAF1), mais dans laquelle le réel x cherché n'est pas explicité en un temps fini; c'est seulement le n -ème terme d'une suite de rationnels convergeant vers x (de manière géométrique) qui est explicité en temps fini :

(TAF3) Si f est dérivable au sens usuel sur l'intervalle $[a, b]$ et si $f(b) < f(a)$, alors on peut expliciter un $x \in [a, b]$ tel que $f'(x) < 0$.

Voici cette preuve, qui fonctionne par dichotomie (quelques détails techniques supplémentaires devraient être rajoutés, mais l'essence de la preuve est donnée).

On note $t = (f(b) - f(a))/(b - a)$. On considère $\varepsilon > 0$, $\varepsilon_n = \varepsilon/2^n$. A l'étape numéro n on détermine un intervalle $[a_n, b_n]$ de longueur $(b - a)/2^n$ sur lequel le taux d'accroissement de la fonction f est $\geq t - \varepsilon + \varepsilon_n$, les intervalles successifs étant emboîtés. L'initialisation avec $n = 0$ et l'intervalle $[a, b]$ est claire. Ensuite on remarque que lorsqu'on divise un intervalle en deux intervalles égaux, le taux d'accroissement global T est la moyenne des deux taux d'accroissements T' et T'' sur les intervalles de longueur moitié. Il suffit alors de calculer chacun des deux réels T' et T'' avec une précision suffisante, pour être sûr que l'un des deux au moins est supérieur $T - \delta$ où δ est un rationnel strictement positif arbitraire. Enfin, la limite commune des deux suites (a_n) et (b_n) est un réel x de $[a, b]$ en lequel le nombre dérivé (supposé exister) est $\geq t - \varepsilon$.

Si nous comparons le contenu algorithmique des deux preuves, nous voyons que la première fournit un rationnel r convenable en un nombre fini d'étapes, tandis que la seconde fournit un réel x comme limite d'une suite de Cauchy (explicite et explicitement convergente).

Mais surtout, bien que nous venions de faire fonctionner la définition usuelle à l'intérieur d'une preuve de nature algorithmique, la définition usuelle de la dérivabilité en tout point n'a pas de signification algorithmique connue. Plus précisément, personne n'a la moindre idée de comment on pourrait rendre la définition usuelle de la dérivabilité d'une fonction en tout point d'un intervalle, entièrement explicite. En effet, on ne sait pas expliciter le fait que "le nombre dérivé existe en tout point de l'intervalle" autrement qu'en exprimant ce nombre dérivé comme fonction uniformément continue de la variable x et en donnant un "module de convergence", uniforme par rapport à x , qui explicite la manière dont le taux d'accroissement tend vers le nombre dérivé en x . Mais alors on tombe sur la définition (6) et non sur la définition usuelle.

Signalons en outre que, puisque les théorèmes essentiels sur les fonctions dérivées sont démontrables constructivement avec la définition (6), nous obtenons une preuve complètement explicite du théorème (TAF2) lorsque la fonction f est une fonction polynôme, ou une fraction rationnelle dont le dénominateur reste $\geq m > 0$ sur un intervalle $[a, b]$.

Ceci nous amène à poser la question suivante : le théorème des accroissements finis (sous la forme (TAF2)) est-il un théorème d'algèbre ? (f est un polynôme ou une fraction rationnelle dont le dénominateur est supposé $\geq m > 0$ sur l'intervalle considéré, et le corps des réels est remplacé par un corps ordonné arbitraire).

La réponse est sûrement oui lorsque l'on considère un corps ordonné $K \subset \mathbb{R}$, puisque la preuve "complètement explicite" de (TAF2) n'utilise aucun passage à la limite⁹ mais seulement des minoration et des majoration. Il existe également une preuve "purement algébrique" dans le cas général d'un corps ordonné, mais seulement avec une fonction polynôme, nous la donnons en annexe.

⁹ Contrairement à celle donnée pour (TAF3)

Mais revenons pour terminer à un autre aspect de la discussion générale sur le caractère plus ou moins constructif, algorithmique, des preuves en analyse. Et ceci, à partir de l'exemple du "théorème de Rolle".

Le théorème de Rolle : un théorème non algorithmique

Donnons tout d'abord la version constructive du théorème de Rolle:

(R1) Si la fonction f est dérivable au sens (6) et si $f(a) = f(b)$, alors
 $\inf \{ |f'(t)| ; t \in [a, b] \} = 0$

Preuve algorithmique : soit un rationnel $\varepsilon > 0$ et découpons $[a, b]$ en intervalles $[x_i, x_{i+1}]$ de longueur $\leq \delta$ sur chacun desquels la fonction f' varie de moins que $\varepsilon/4$. Pour chaque i , on calcule $f'(x_i)$ avec une précision meilleure que $\varepsilon/4$, ce qui permet d'affirmer au moins une des 2 éventualités:

$$|f'(x_i)| \geq \varepsilon/2 \quad \text{ou} \quad |f'(x_i)| \leq \varepsilon$$

Si on avait $|f'(x_i)| \geq \varepsilon/2$ pour chaque i , alors $f'(x_i)$ resterait de signe constant (car $|f'(x_{i+1}) - f'(x_i)| \leq \varepsilon/4$), par exemple > 0 , et on aurait, par (5)

$$f(b) \geq f(a) + \varepsilon/4 (b - a)$$

Cette preuve algorithmique nous donne le moyen de trouver, pour chaque entier n , en un nombre fini d'étapes, majoré a priori, un rationnel x_i tel que

$$|f'(x_i)| \leq 1/2^n$$

Elle ne nous donne cependant pas le moyen de construire un nombre réel x (c'est-à-dire : une suite de Cauchy de rationnels) pour lequel $f'(x) = 0$.

En outre, il semble difficile de modifier convenablement cette preuve pour la rendre explicite dans le cas où la fonction f est seulement supposée dérivable au sens usuel.

Quant à la preuve "usuelle" du théorème de Rolle, elle est basée sur le fait que la fonction f atteint son maximum sur l'intervalle $[a, b]$. Mais ce "théorème" d'analyse est fortement non algorithmique : en effet, on peut construire une fonction f uniformément continue sur un intervalle $[a, b]$, de manière complètement explicite, et telle que cependant f n'atteigne son maximum en aucun point "mécaniquement calculable" de l'intervalle $[a, b]$. En conséquence, aucun algorithme ne peut fournir, à partir d'une fonction uniformément continue arbitraire explicite f , un point x où cette fonction atteindrait son maximum. Même dans l'hypothèse où f est supposée dérivable au sens (6), il est impossible de réaliser le théorème de Rolle par un algorithme général, parce que cet algorithme général serait capable de réaliser le théorème de la valeur intermédiaire pour la fonction dérivée⁽¹⁰⁾.

Conclusion

Une préoccupation de réalisme nous a tout d'abord incité à changer le statut du théorème des accroissements finis : il démontre, non pas "une vérité", mais l'adéquation d'un modèle à une réalité qu'il voulait représenter.

Cette même préoccupation de réalisme nous a ensuite conduit à proposer une définition alternative pour la notion de "fonction dérivable".

Sans machiavélisme prémédité, nous avons abouti à une formulation équivalente à celle donnée par les mathématiques constructives. Cette définition alternative de fonction dérivable s'avère en

¹⁰ Voir le chapitre « Hier et Demain » pour une discussion sur le théorème de la valeur intermédiaire.

fin de compte très efficace du point de vue algorithmique, et fournit par exemple une preuve “purement algébrique” du théorème des accroissements finis dans le cas d’une fraction rationnelle à dénominateur $\geq m > 0$ et à coefficients rationnels.

Pour passer de la formulation usuelle “vitesse instantanée = limite de la vitesse moyenne” à la formulation constructive alternative, il suffit de lire le mot “limite” au sens uniforme.

Ceci n’est pas sans rappeler une mésaventure qui arriva à Cauchy, célèbre pour avoir introduit la rigueur en analyse. Cauchy, (qui passait parfois pour un dangereux faiseur de contre-exemples irréalistes), proposa une définition de la continuité (c’était la continuité en tout point, formulée dans son langage) et, comme il ne prétendait pas “démontrer des vérités”, mais “vérifier l’adéquation d’un modèle”, il s’attaqua à un “théorème” qui, à l’époque, avait quasiment le statut d’une évidence: “si une suite de fonctions continues admet une limite, sa limite est une fonction continue”.

Ce théorème n’est ni vrai, ni faux. Tout dépend du contexte, du sens précis qu’on attribue au mot limite. Cauchy donna en 1821 une démonstration “fausse”. On connut rapidement des contre-exemples. Mais l’erreur dans la démonstration ne fut découverte que 26 ans plus tard. C’est Seidel qui mit clairement à jour le point faible dans le modèle: la notion de limite d’une suite de fonctions devait être prise “au sens uniforme” et non au sens “point par point”, le premier qui venait à l’esprit. Pour plus de détails sur ce sujet, on lira “Preuves et réfutations” de Imre Lakatos, p. 165-182.

Annexe : le théorème algébrique des accroissements finis

Il affirme que le taux d'accroissement d'un polynôme de degré fixé sur un intervalle est une moyenne, pondérée par des coefficients positifs, de valeurs de la dérivée en des points connus de l'intervalle, indépendants du polynôme.

Exemple : Pour tout polynôme de degré ≤ 4 on a l'identité:

$$P(a) - P(b) = (a - b) \left(P'(a/6 + 5b/6)/3 + P'(a/3 + 2b/3)/6 + P'(2a/3 + b/3)/6 + P'(5a/6 + b/6)/3 \right)$$

Plus généralement on a les résultats suivants :

Lemme : Il existe deux suites $(\lambda_{i,j})_{1 \leq i \leq j; j=1,2,\dots,n,\dots}$ et $(r_{i,j})_{1 \leq i \leq j; j=1,2,\dots,n,\dots}$ de rationnels $\in]0, 1[$ telles que, pour tout polynôme $P \in \mathbb{Q}[X]$ de degré $\leq n$, on ait :

$$P(a) - P(b) = (a - b) \times \sum_{i=1}^n r_{i,n} \cdot P'(a + \lambda_{i,n}(b - a))$$

Théorème 1 : (théorème algébrique des accroissements finis pour les polynômes)

Il existe deux suites $(\lambda_{i,j})_{1 \leq i \leq j; j=1,2,\dots,n,\dots}$ et $(r_{i,j})_{1 \leq i \leq j; j=1,2,\dots,n,\dots}$ de rationnels $\in]0, 1[$ telles que, pour tout corps ordonné K et tout polynôme $P \in K[X]$ de degré $\leq n$, on ait :

$$P(a) - P(b) = (a - b) \times \sum_{i=1}^n r_{i,n} \cdot P'(a + \lambda_{i,n}(b - a))$$

En particulier, si P' est de signe positif sur un intervalle, la fonction polynôme est croissante sur tout l'intervalle, et si le taux d'accroissement de P est < 0 entre a et b la dérivée de P est < 0 en l'un au moins des points $a + \lambda_{i,n}(b - a)$

preuve Le théorème est une conséquence immédiate du lemme: ce dernier fournit en effet des identités algébriques concernant les variables “ a , b , et les coefficients du polynôme ” qui s'appliquent alors dans tout anneau commutatif qui est une $\mathbb{Q}$ -algèbre, et en particulier dans les corps ordonnés.

Démontrons le lemme.

Par changement de variable affine, on se ramène au cas où $a = -1$ et $b = 1$. Considérons le degré n fixé. L'application $P \mapsto P(1) - P(-1)$ est une forme linéaire ne faisant pas intervenir le coefficient constant. Les formes linéaires ne faisant pas intervenir le coefficient constant forment un espace de dimension n . Pour tout choix de n rationnels $\lambda_{i,n}$, les formes linéaires $P \mapsto P'(\lambda_{i,n})$ sont indépendantes et ne font pas intervenir le coefficient constant. Il correspond donc à ce choix des rationnels $r_{i,n}$ qui rendent la formule vraie. La difficulté consiste à déterminer des $\lambda_{i,n} \in]0, 1[$ tels que les $r_{i,n}$ correspondants soient également dans $]0, 1[$. Les formules de quadrature de Gauss correspondent à un tel choix, mais avec des réels alors que nous voulons des rationnels. Il suffit alors de choisir des $\lambda_{i,n}$ rationnels suffisamment voisins des $\lambda_{i,n}$ de Gauss (zéros des polynômes de Legendre) pour que les $r_{i,n}$ correspondants restent positifs. $\square$

De la difficulté d'être omniscient

Le moyen fait partie de la recherche de la vérité, aussi bien que le résultat.

Il faut que la recherche de la vérité soit elle-même vraie; la recherche vraie, c'est la vérité déployée, dont les membres épars se réunissent dans le résultat.

Karl Marx, cité par Georges Perec dans Les Choses

Résumé

Depuis les résultats de consistance relative de l'axiome de choix et de sa négation, de l'hypothèse du continu et de sa négation, il est difficile d'accorder foi au réalisme platonicien selon lequel un Univers Mathématique Cantorien (ou plutôt Zermelo-Frankelien) existe de manière idéale quelque part, garant du sens des énoncés mathématiques cantorien usuels. Pour Gödel, par exemple, qui défend ce point de vue, on doit un jour trouver des axiomes raisonnables qui permettront de décider l'hypothèse du continu. Mais est-ce vraiment un programme raisonnable ?

La contradiction entre l'axiome du choix et l'axiome de détermination pose un problème plus délicat encore, celui de l'impossibilité d'être omniscient en ce qui concerne l'infini actuel, s'il existe. On peut interpréter ce paradoxe en disant qu'il est impossible de vouloir extrapoler du fini à l'infini tout ce qui semble raisonnable dans le domaine fini.

Dans l'article, après avoir situé les problèmes soulevés, on essaiera de montrer comment une problématique d'infini potentiel relativise ces problèmes et change l'interprétation même du vocabulaire ensembliste.

Introduction

Les affirmations du langage courant se prêtent très mal à la logique du Vrai et du Faux. Lorsqu'on dit par exemple : «Ceci est une grosse pomme» la limite entre Vrai et Faux est entourée d'une zone de flou importante. Tout d'abord concernant la partie "ceci est une pomme" (s'il manque la queue ? si elle est coupée en deux, si on a enlevé les pépins, etc...) et aussi concernant l'affirmation que la pomme est "grosse".

En un certain sens on peut dire que l'homme a inventé des êtres mathématiques abstraits tels que "les nombres" ou "le plan euclidien" de manière à pouvoir raisonner "sans ambiguïté de sens", c'est-à-dire de manière à pouvoir raisonner avec une logique du Vrai et du Faux. Une fois définies les opérations élémentaires sur les nombres entiers une affirmation telle que :

si p est un nombre premier et si r est un entier $< p$, alors
le nombre $r^{p-1} - 1$ est divisible par p "

est vraie, et on peut en donner une démonstration parfaitement convaincante.

Cependant l'introduction par Cantor des ensembles infinis dans les mathématiques a jeté une certaine confusion au sujet de la notion de Vrai et Faux. La question du Vrai et du Faux se pose en effet de manière différente selon qu'un énoncé mathématique est testable par un processus fini ou par un processus infini, ou encore par une infinité en cascade de processus infinis, ou même par des processus encore plus "mystérieux".

On pourrait croire que l'infini en mathématiques existait bien avant Cantor, dès que la notion de nombre entier fut mise au point. La collection des entiers naturels, en effet, a la particularité de n'être "jamais finie".

En fait, avant Cantor, personne n'avait eu l'audace de considérer "l'ensemble de tous les entiers naturels" comme une totalité donnée, actuelle. L'esprit humain, en effet, ne peut appréhender qu'un nombre fini d'objets, les uns après les autres.

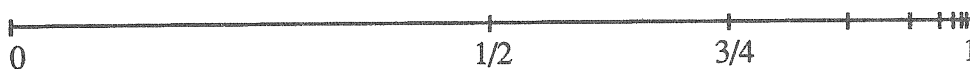
Avant Cantor donc, la collection des entiers naturels était seulement un infini en puissance, un infini "potentiel" et non "actuel". Lorsqu'on parle d'infini potentiel, ce que l'on a clairement en tête, c'est *le processus* qui permet de passer de l'entier n à l'entier $n + 1$, processus qui fait que la collection des entiers n'est jamais finie.

La croyance en un infini actuel équivaut en fait de manière quasiment logique à la croyance en un "Dieu mathématicien" capable, lui, d'appréhender "d'un seul coup" l'ensemble de tous les entiers naturels. C'est ce que nous essayerons d'illustrer dans cet article.

Les philosophes grecs ne croyaient pas en l'infini actuel, ou tout au moins s'en interdisaient l'usage en mathématiques.

Zénon d'Elée, à sa manière et à juste titre, avait soulevé la contradiction existant entre l'homme et "Dieu" puisque "Dieu" est capable de diviser en un temps fini (en une seconde !) l'intervalle de temps constitué par 1 seconde en une infinité de subdivisions, alors que l'homme n'arrive *jamais* au bout de la description complète de cette "subdivision à l'infini", ni en une seconde, ni en un siècle.

Un paradoxe de Zénon



Y a-t-il VRAIMENT une infinité d'instants "en acte" entre l'instant 0 et l'instant 1 ?

La solution proposée par les Grecs et acceptée jusqu'à Cantor :

Seul l'infini potentiel est autorisé en mathématiques.

De même Euclide, dans ses *Éléments*, ne considère pas "un espace infini à 3 dimensions" mais seulement "un espace à 3 dimensions qui n'est jamais fini". Il ne considère pas "l'ensemble de tous les entiers naturels" mais seulement "des entiers naturels" (collection ouverte, jamais finie). Il ne considère pas "l'ensemble des nombres réels" mais se contente de comparer entre eux des rapports de grandeurs homogènes qui viennent se présenter à lui dans sa quête géométrique. Interprétation en langage moderne : deux rapports sont égaux selon Eudoxe⁽¹⁾ si et seulement si ils définissent des coupures égales selon Dedekind. Mais Euclide se refuse à considérer la coupure en tant que telle, elle représenterait un infini actuel. A fortiori refuse-t-il de considérer l'infini actuel de telles coupures.

¹ On attribue à Eudoxe la théorie des proportions mise au point par les Grecs pour faire face aux problèmes des grandeurs "sans commune mesure" comme le côté et la diagonale d'un carré.

La notion d'infini mathématique actuel s'est avérée extrêmement "pratique" et a été adoptée par la majorité des mathématiciens.

Cependant, le prix à payer est en fin de compte assez cher. En effet, les notions logiques de base, qui ne posent pas problème lorsqu'elles sont utilisées pour des propriétés bien définies portant sur des collections finies d'objets mathématiques, ne peuvent s'appliquer aux propriétés concernant des ensembles infinis qu'au prix d'une extrapolation douteuse.

La question du tiers exclu pour des énoncés du type de la conjecture de Goldbach

La conjecture de Goldbach est la suivante :

Tout entier pair supérieur à 4 est somme de 2 nombres premiers.

Nous sommes tellement habitués à raisonner avec l'infini actuel comme avec le fini, que si vous lisez :

La conjecture de Goldbach est forcément vraie ou fausse.

Vous avez l'impression de lire une trivialité.

Or ce n'est pas du tout une trivialité.

Dire que la conjecture est fausse c'est dire qu'on peut trouver un entier pair supérieur à 4 qui n'est pas somme de 2 nombres premiers. Donc il suffit d'une vérification pour montrer que la conjecture est fausse.

Par contre dire que la conjecture est vraie c'est signifier, ou bien qu'on en possède une démonstration convaincante, ou bien qu'il faut faire une infinité de vérifications. Or non seulement l'homme ne sait pas faire une infinité de vérifications, mais on peut penser qu'une infinité de vérifications est a priori hors des "capacités de calcul de l'univers". Autrement dit, une "machine à calculer infinie" semble inconcevable. Même si l'univers avait une durée de vie infinie et si une machine à calculer pouvait être construite qui dispose de l'éternité du temps à venir, la conjecture de Goldbach ne serait pourtant "jamais vérifiée en entier".

Maintenant supposez que la situation concrète soit la suivante

- l'homme ne trouvera jamais de démonstration convaincante de la conjecture,
- l'homme ne trouvera jamais de contre-exemple prouvant que la conjecture est fausse.
- il ne peut exister de machine à calculer infinie

Alors dans ce cas, seul un "Dieu mathématicien" (s'il existe) peut dire que la conjecture est forcément vraie ou fausse.

Vous direz sans doute que je coupe des cheveux en quatre. En fait je souligne seulement qu'il n'est pas du tout trivial de considérer que la loi du tiers exclu s'applique aux ensembles infinis, même dans le cas d'un énoncé dont la structure est extrêmement simple.

Le coup de génie de Cantor a été de transformer la fameuse démonstration d'impossibilité «l'infini actuel ne peut exister en mathématiques puisque le tout doit toujours être supérieur à la partie» en une définition a contrario «j'appelle infini un tout qui est en bijection avec l'une de ses parties». Cet acte fondateur est le refus d'admettre comme définitive une évidence qui a lieu dans le domaine du fini. Mais d'autres évidences qui ont lieu dans le domaine du fini, comme le tiers exclu, sont alors ipso facto elles-mêmes sujettes à caution et à discussion. Si j'appelle distribution la dérivée d'une fonction continue non dérivable, je dois bien évidemment m'atten-

dre à ne pas pouvoir faire avec les distributions tout ce que j'avais le droit de faire avec les fonctions continues. Et celui qui ne prendrait pas de précautions de peur de se faire accuser de couper les cheveux en quatre serait sûrement accusé de laxisme.

Reprenons en le détaillant, ce genre d'extrapolation, du fini à l'infini, qui se cache derrière la phrase : «La conjecture de Goldbach est forcément vraie ou fausse»

Notons « $A(n)$ » pour « $2n + 4$ est somme de 2 nombres premiers»

L'affirmation $A(n)$ peut être testée pour tout entier n . En effet l'affirmation $A(n)$ est parfaitement décidable puisqu'on dispose d'un processus effectif qui permet de calculer tous les nombres premiers inférieurs à $2n + 4$. On est donc assuré que $A(n)$ est «Vrai ou Faux» en un sens fort⁽²⁾, pour chaque entier n . Cela s'écrit en langage formalisé constructif :

$$(1) \quad \forall n \in \mathbb{N} \quad (A(n) \text{ ou } \text{non } A(n))$$

Dire que la conjecture de Goldbach est forcément vraie ou fausse consiste à affirmer :

$$(2) \quad \forall n \in \mathbb{N} \quad A(n) \text{ ou } \exists n \in \mathbb{N} \quad \text{non } A(n)$$

Le fait qu'un énoncé du type (1) implique l'énoncé correspondant du type (2) est, du point de vue de l'interprétation constructive de la vérité, un *principe d'omniscience*. Dans la littérature constructive, on l'appelle «le petit principe d'omniscience»⁽³⁾.

Ce principe est couramment admis par les mathématiciens actuels, en général au nom du réalisme platonicien : il y aurait, quelque part, au moins de manière idéale, un ensemble infini actuel des entiers naturels, pour lequel la logique du tiers exclu s'applique tout comme dans les ensembles finis.

C'était en tout cas le point de vue de Gödel, qui étendait d'ailleurs le réalisme platonicien à toute la hiérarchie cumulative des ensembles.

Le réalisme platonicien

Un ensemble infini "en acte" $\mathbb{N}$ existe, au moins de manière idéale, et, dans cet ensemble, la logique du "Vrai ou Faux", valable pour les ensembles finis, s'applique tout aussi bien.

² Il est vrai que pour un entier dépassant 10^{100} chiffres, la possibilité de vérifier $A(n)$ semble excéder à jamais en pratique nos capacités de calcul. Néanmoins, on peut considérer que cette possibilité n'est pas exclue en principe mais seulement en pratique. Admettre qu'un énoncé du type $A(n)$ peut, au moins en principe, être testé vrai ou faux pour tout entier n relève de l'"extrapolation du potentiellement réalisable". Dans ce genre d'extrapolation, on extrapole un résultat vrai depuis le fini raisonnable jusqu'au fini même déraisonnable, mais on reste dans un cadre fini.

³ Ce principe d'omniscience peut être compris et discuté sans recours à aucun système formel. Dans les systèmes formels classiques, on admet le principe du tiers exclu, qui est une sorte de méga principe d'omniscience. Dans de tels systèmes formels, aussi bien les énoncés du type (1) que les énoncés du type (2) sont des théorèmes, et donc a fortiori les énoncés du type $(1) \Rightarrow (2)$. Dans un système formel constructif, il n'y a pas de preuve générale des énoncés $(1) \Rightarrow (2)$. Néanmoins, si on rajoute le schéma d'axiome $(1) \Rightarrow (2)$, on obtient un système formel où le tiers exclu n'est pas pour autant valable. D'autres principes d'omniscience, plus faibles ou plus forts que le «le petit principe d'omniscience» peuvent être discutés. Le degré de non-effectivité des théorèmes usuels de mathématiques classiques peut être analysé en référence à un nombre relativement restreints de tels principes d'omniscience.

Ce réalisme platonicien semble difficile à distinguer de la croyance en un "Dieu mathématicien connaissant la vérité de tous les énoncés sensés concernant les entiers naturels".

Une autre approche était celle de Hilbert, qui pensait pouvoir réduire le recours aux ensembles infinis à une simple "manière de parler", un peu comme lorsqu'on dit « $\sqrt{-3}$ est un nombre» ou encore «toute fonction continue est dérivable (au sens des distributions)». En ce sens l'énoncé (2) peut évidemment être décrété «Vrai de manière purement conventionnelle», mais alors le mot «Vrai» est privé de sa signification habituelle.

Le problème est alors de démontrer, (au sens de : emporter la conviction intime), que les preuves purement formelles qu'on déroule n'aboutissent jamais à affirmer vraies des propositions douées d'une signification concrète précise et cependant fausses dans la réalité.

La solution formaliste (Hilbert)

On introduit $\mathbb{N}$ comme "manière de parler", (exactement comme $\sqrt{-3}$), on raisonne avec la logique du "Vrai ou Faux" valable pour les ensembles finis.

On prouve, par une argumentation séparée, qu'un théorème démontré "idéalement vrai" n'est jamais "concrètement faux".

Le programme de Hilbert sous sa forme la plus stricte (Hilbert demandait que la preuve de consistance du système formel considéré soit d'un type particulièrement élémentaire) a été ruiné par le théorème d'incomplétude de Gödel. Néanmoins, on peut considérer qu'il a été réalisé pour l'essentiel, sous une forme légèrement affaiblie, pour la théorie formelle «arithmétique de Peano», notée PA, qui se limite à décrire les entiers naturels à un niveau assez élémentaire.

Par contre, le programme de Hilbert n'a jamais été réalisé pour la théorie des ensembles infinis actuels de Cantor, formalisée aujourd'hui dans le système axiomatique noté ZF⁽⁴⁾, ni même pour ce qui concerne des théories, beaucoup moins puissantes que ZF, qui cherchent à décrire ne serait-ce que l'ensemble des parties de $\mathbb{N}$.

⁴ Le système proposé par Zermelo, noté Z, permet la construction de tous les $\mathcal{P}(\mathcal{P}(\dots\mathcal{P}(\mathbb{N})))$. Le système ZF, qui est le précédent "amélioré" par Frankel, permet d'itérer de manière infinie la construction précédente. Dans ZFC, on rajoute l'axiome du choix. Les mathématiques usuelles ne dépassent pas $\mathcal{P}(\mathcal{P}(\mathbb{N}))$.

Les variables de cet énoncé ont “seulement” pour domaine $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, ou $\mathbb{N}$, ou $\mathcal{P}(\mathbb{N})$ ⁽⁵⁾. Pour un réaliste platonicien à la Gödel qui pense que $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ existe quelque part, au moins de manière idéale, et que les énoncés qui ne font référence qu'à ce “petit” infini sont forcément Vrais ou Faux “en réalité”, l'hypothèse du continu admet certainement une réponse positive ou négative.

Pourtant Gödel et Cohen ont démontré les deux résultats selon lesquels l'hypothèse du continu ne peut ni être prouvée fausse, ni être prouvée vraie dans le système formel ZFC, qui semble pourtant intégrer tous les ingrédients raisonnables de la théorie cantorienne.

Beaucoup de logiciens et de mathématiciens s'accordent à interpréter ces résultats de la manière suivante : l'homme ne saura jamais démontrer si l'hypothèse du continu est vraie ou fausse.

Certains autres, à la suite de Gödel, pensent qu'on finira par découvrir un axiome raisonnable qui prouvera que l'hypothèse du continu est fausse (ou, plus improbableement, vraie).

On voit donc que l'introduction des trois infinis actuels $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$ et $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ suffit à produire des problèmes sans doute à jamais insolubles pour l'homme, même en utilisant des preuves hautement abstraites et absolument pas constructives. Voici qui jette un flou considérable sur la notion de “Vérité” appliquée dans l'ensemble $\mathcal{P}(\mathcal{P}(\mathbb{N}))$!

En fait, l'attitude qui semble la plus naturelle, au vu des résultats de consistance relative de Gödel et Cohen, serait de déclarer que l'hypothèse du continu est insoluble pour la bonne raison qu'elle n'a pas de signification réelle précise, mais seulement une signification purement conventionnelle. A savoir la signification d'une «règle du jeu» qu'on décide d'introduire ou non dans la théorie des ensembles infinis actuels. C'était par exemple le point de vue d'A. Robinson, le créateur de l'Analyse non standard (cf. son texte “Formalisme 64”). Cette attitude trouve un autre argument en sa faveur dans le théorème de Lowenheim-Skolem :

la théorie des ensembles infinis, une fois formalisée, par exemple dans le système axiomatique ZFC, admet des modèles dénombrables

Dans un tel modèle, la vraie cardinalité de $\mathcal{P}(\mathbb{N})$ est le dénombrable, mais aucune des bijections existant entre $\mathbb{N}$ et $\mathcal{P}(\mathbb{N})$ n'est dans le modèle.

La majorité des réalistes platoniciens adopte sur ces questions une position de repli confortable : tout ceci n'est pas bien grave puisque l'hypothèse du continu n'a aucune conséquence importante pour les mathématiques couramment pratiquées.

Peut-on imaginer un jeu sans partie nulle mais sans stratégie gagnante pour aucun des deux joueurs ?

Un des axiomes de la théorie des ensembles qui a fait couler beaucoup d'encre est l'*axiome du choix*, qui est en fait un axiome de choix infini uniforme. Combiné avec le principe du tiers exclu, cet axiome permet de démontrer l'existence d'objets idéaux (par exemple : une clôture algébrique d'un corps arbitraire, ou une fonction réelle non Lebesgue-mesurable) pour lesquels aucune construction explicite n'est possible. Donnons un énoncé parmi d'autres pour cet axiome du choix.

$\forall g : X \longrightarrow Y$ surjective, $\exists h : Y \longrightarrow X$ telle que $\forall y \in Y \quad g(h(y)) = y$

⁵ Des variables quantifiées sont cachées dans les morceaux de phrases en français : «représente une bijection».

Si l'ensemble X est fini ou si c'est l'ensemble des entiers naturels, l'axiome est évidemment "vrai dans la réalité": on prend pour $h(y)$ le premier x de X qui vérifie $g(x) = y$. Le problème avec l'axiome du choix est donc un problème d'extrapoler un énoncé depuis l'infini dénombrable jusqu'à des infinis de structure arbitraire.

Je vais maintenant montrer une autre extrapolation à l'infini qui semble a priori tout aussi légitime et qui, en réalité, ne l'est pas du tout (pour les adeptes de Cantor eux-mêmes).

Il s'agit de considérer un jeu où deux adversaires s'affrontent sans intervention du hasard. Ce jeu, par exemple le jeu d'échec, est d'abord supposé de nature finie, c'est-à-dire que le nombre de coups dans une partie est limité a priori (par exemple à 1000) et que dans chaque situation le joueur ne peut choisir qu'entre un nombre fini de possibilités (mettons par exemple 200). La partie peut alors grosso modo être décrite de manière formalisée comme suit : le premier joueur choisit un nombre entre 1 et 200 : x_1 , le deuxième joueur choisit à son tour un nombre entre 1 et 200 : x_2 etc...

Au bout de 1000 coups la partie s'arrête (si elle est terminée avant, on peut convenir, pour simplifier notre description formalisée, que tous les coups de la fin sont d'un type donné, réservé à cet effet).

La partie ainsi complètement décrite est une suite $(x_n)_{n \in \{1, \dots, 1000\}}$ de 1000 nombres entiers compris entre 1 et 200. Si j'appelle $\mathcal{A}$ l'ensemble de toutes les suites de 1000 nombres entiers $\in C := \{1, \dots, 200\}$ (l'ensemble $\mathcal{A}$ possède 200^{1000} éléments), la "règle du jeu" peut être considérée comme donnée par un sous-ensemble B de $\mathcal{A}$ pour lequel on a :

- si $(x_n)_{n \in \{1, \dots, 1000\}} \in B$, c'est le joueur 1 qui a gagné
- si $(x_n)_{n \in \{1, \dots, 1000\}} \notin B$, c'est le joueur 2 qui a gagné

Comme 200^{1000} est un nombre hors d'atteinte des ordinateurs les plus puissants, il est possible que le jeu en question (si le sous-ensemble B est suffisamment compliqué) reste à jamais un mystère pour l'homme. C'est peut être le cas du jeu d'échec par exemple. Néanmoins, on peut affirmer⁽⁶⁾

- ou bien le premier joueur dispose d'une stratégie gagnante
- ou bien le deuxième joueur dispose d'une stratégie gagnante.

En effet, la première affirmation peut s'écrire :

(*) $\exists x_1 \in C \forall x_2 \in C \exists x_3 \in C \dots \exists x_{199} \in C \forall x_{200} \in C$ la liste $[x_1, \dots, x_{1000}] \in B$
et la deuxième affirmation est simplement la négation de la première :

(**) $\forall x_1 \in C \exists x_2 \in C \forall x_3 \in C \dots \forall x_{199} \in C \exists x_{200} \in C$ la liste $[x_1, \dots, x_{1000}] \notin B$

En admettant l'extrapolation du potentiellement réalisable, une et une seule ces 2 affirmations est forcément vraie, car ceci est vérifiable en *un nombre fini* d'opérations purement mécaniques (cela pourrait faire l'objet d'un programme d'ordinateur).

Passons maintenant au problème de "l'extrapolation à l'infini" de cette affirmation («ou bien le premier joueur dispose d'une stratégie gagnante, ou bien c'est le deuxième»). On se trouve face à la question d'interpréter la signification d'une écriture

$$\exists x_1 \in C \forall x_2 \in C \exists x_3 \in C \dots$$

ou on trouverait une infinité de quantificateurs en cascade.

⁶ Si on admet l'extrapolation du potentiellement réalisable : c'est à dire l'extrapolation du fini "raisonnable" au fini "déraisonnable"

Il faut pour cela donner une formulation équivalente à cette écriture dans le cas "fini" et pour laquelle "l'extrapolation à l'infini" soit plus facile à écrire.

Pour cela, notons L l'ensemble des listes finies d'éléments de C , limitées à 1000 éléments, y compris la liste vide.

Voici alors une formulation équivalente à (*)

$$(\#) \quad \exists f : L \rightarrow C \quad \forall x_2, x_4, \dots, x_{1000} \in C, \\ \text{la liste } [f(\square), x_2, f([x_2]), x_4, f([x_2, x_4]), x_6, \dots, f([x_2, x_4, \dots, x_{998}]), x_{1000}] \in B$$

Un examen un peu attentif convaincra le lecteur que la formulation (#) est équivalente à (*) : en effet le " $\exists f$ " dans (#) signifie que le premier joueur a le moyen de riposter à tous les choix faits par le deuxième joueur.

De même on obtient une formulation équivalente à (**)

$$(\#\#) \quad \exists f : L \rightarrow C \quad \forall x_1, x_3, \dots, x_{999} \in C, \\ \text{la liste } [x_1, f([x_1]), x_3, f([x_1, x_3]), x_5, \dots, x_{999}, f([x_1, x_3, \dots, x_{999}])] \notin B$$

Nous sommes maintenant en mesure de donner une signification à la phrase "le premier joueur dispose d'une stratégie gagnante" lorsqu'on "extrapole à l'infini" c.-à-d. lorsqu'on remplace les ensembles finis $C = \{1, 2, \dots, 200\}$ et $\{1, 2, \dots, 1000\}$ par $\mathbb{N}$.

Prenons en effet pour $\mathcal{A}$ l'ensemble $\mathbb{N}^{\mathbb{N}}$ de toutes les suites infinies de nombres entiers. Si nous notons x un élément de $\mathcal{A}$ nous noterons x_n le $n^{\text{ème}}$ terme de la suite x . Prenons pour B un sous-ensemble arbitraire de $\mathcal{A}$. Notons L l'ensemble des listes finies d'éléments de $\mathbb{N}$, sans limitation du nombre d'éléments. L'énoncé ($\approx$) qui signifie "le premier joueur a une stratégie gagnante pour le jeu B " est le suivant :

$$(\approx) \quad \exists f : L \rightarrow C \quad \forall x \in \mathbb{N}^{\mathbb{N}}, \\ \text{la suite infinie } (f(\square), x_1, f([x_1]), x_2, f([x_1, x_2]), x_3, \dots) \in B$$

De la même manière, on a l'énoncé ($\approx\approx$) qui signifie "le deuxième joueur a une stratégie gagnante pour le jeu B ".

$$(\approx\approx) \quad \exists f : L \rightarrow C \quad \forall x \in \mathbb{N}^{\mathbb{N}}, \\ \text{la suite infinie } (x_1, f([x_1]), x_2, f([x_1, x_2]), x_3, \dots) \notin B$$

On s'attend alors, en extrapolant la forme particulière de tiers exclu⁽⁷⁾ examinée, à l'infini, à avoir le résultat suivant :

Pour tout jeu infini $B \subset \mathbb{N}^{\mathbb{N}}$ ou bien le premier joueur dispose d'une stratégie gagnante, ou bien le deuxième joueur dispose d'une stratégie gagnante.

Disons plutôt : on s'attend à ce que ce résultat soit vrai (ou au moins que son contraire ne soit pas un théorème) dans la théorie des ensembles couramment pratiquée. Eh bien, surprise! ce résultat est *démontré FAUX* dans la théorie des ensembles infinis actuels habituelle, formalisée dans le système ZFC (fonctionnant selon les règles de la logique "classique", donc admettant la version ordinaire du tiers exclu).

Des logiciens ont proposé de modifier la théorie ZFC en supprimant l'axiome du choix et en introduisant comme nouvel axiome "de tiers exclu", l'énoncé ci-dessus en italique, rebaptisé **axiome de détermination**.

Mais cette solution, qui sauve le tiers exclu dans le cas des "jeux infinis", ne sauve nullement le principe général d'extrapolation à l'infini.

⁷ Il ne s'agit pas du "tiers exclu" au sens ordinaire de la logique classique, il s'agit néanmoins d'une forme "intuitive" de tiers exclu, apparemment parfaitement raisonnable, ni plus ni moins "contestable" que la forme ordinaire du tiers exclu.

En effet, l'axiome du choix est "évidemment vrai" dans le cas d'ensembles finis, et il n'y a aucune raison de refuser son extrapolation à l'infini pour un mathématicien classique.

Gödel a d'ailleurs démontré que l'axiome du choix était "non contradictoire avec les autres axiomes de ZF". Plus précisément, "s'il existe" un "univers mathématique" où les axiomes de ZF sont vérifiés, alors on peut décrire en son sein un autre "univers mathématique" où tous les axiomes de ZFC (ZF avec l'axiome du choix) sont vérifiés.

L'enseignement que je tirerai de cet exemple est que, d'un point de vue cantorien, toutes les extrapolations à l'infini "raisonnables" ne sont pas compatibles entre elles. C'est le témoignage d'une *fragilité interne certaine* du système de pensée cantorien. Pour les réalistes platoniciens de la hiérarchie cumulative des ensembles, ce devrait être un sacré coup dur⁽⁸⁾. Non seulement cette "réalité existante idéale" nous cache ses secrets (comme l'hypothèse du continu), mais elle nous tend des pièges carrément méchants, comme celui d'avoir à choisir, en toute ignorance de cause, entre deux axiomes parfaitement raisonnables mais cependant contradictoires, celui du choix infini uniforme et celui de la détermination des jeux infinis.

Au risque de se faire condamner par un Ayatollah, par l'Inquisition ou par l'Opus Dei, on peut désormais avancer la "preuve d'inexistence" suivante :

si l'infini existe il ne saurait être infiniment savant

en effet, ou bien il est savant au point de savoir choisir simultanément un élément dans chaque ensemble d'une collection infinie arbitraire, ou bien il est savant au point de savoir élaborer une stratégie gagnante pour un des deux partenaires de n'importe quel jeu infini; mais il ne peut être savant au point de savoir faire les deux choses à la fois.

Que les croyants se rassurent, ce n'est ni le premier ni le dernier sophisme au sujet de l'infini en acte⁽⁹⁾.

D'ailleurs, puisque nous avons commencé par une citation de Marx, en voici une autre, qui nous conseille de nous méfier de l'omniscience en politique :

La doctrine matérialiste qui veut que les hommes soient des produits des circonstances et de l'éducation, que, par conséquent, des hommes transformés soient des produits d'autres circonstances et d'une éducation modifiée, oublie que ce sont précisément les hommes qui transforment les circonstances et que l'éducateur a lui-même besoin d'être éduqué. C'est pourquoi elle tend inévitablement à diviser la société en deux parties dont l'une est au-dessus de la société
(Thèses sur Feuerbach)

La question de la comparaison des cardinaux en mathématiques constructives

Revenons à la question de l'hypothèse du continu.

On peut remarquer que l'homme ne pourra, quant à lui, jamais définir qu'une quantité "dénombrable" de nombres réels : un nombre réel défini par un homme sera toujours en fin de

⁸ Mais en matière de philosophie, les coups durs ne sont jamais mortels.

⁹ Le plus célèbre est bien évidemment le pari de Pascal. Mais dans son calcul d'espérance mathématico-religieuse, Pascal a oublié de compter comme non nulle la probabilité de l'existence d'un dieu "non conforme", qui assurerait le paradis post mortem aux seules femmes et hommes qui ne le considéreraient pas comme tout puissant, combattraient l'aspect obscurantiste de toutes les religions et refuseraient de se soumettre aux diktats de n'importe quel dogme irrationnel.

compte défini par une phrase imprimée dans un livre. Donc l'homme ne dispose que d'un infini "potentiel" de parties de $\mathbb{N}$, pas plus gros que l'infini "potentiel" des nombres entiers. L'affirmation selon laquelle «l'ensemble $\mathbb{R}$ a un cardinal strictement plus grand que l'ensemble $\mathbb{N}$ » est donc une vérité moins "absolue" que $2 + 2 = 4$; elle est entachée d'un certain flou ; elle nécessite certainement "les nombres réels que l'homme ne pourra jamais définir, même à l'état potentiel".

Si on examine en détail la preuve diagonale de Cantor selon laquelle l'infini $\mathbb{N}$ des entiers naturels est de cardinalité strictement plus petite que l'infini $\mathbb{R}$ des nombres réels, on est frappé par le caractère constructif de cette preuve. Par exemple, à partir d'une énumération explicite des nombres réels algébriques, la preuve de Cantor fournit un procédé explicite pour construire des nombres réels transcendants, c.-à-d. non algébriques. En fait, la preuve de Cantor peut être affinée et rendue entièrement constructive et fournit alors le théorème suivant (cf. [BB] théorème 2.19 p.27) :

étant donnés une suite $(x_n)_{n \in \mathbb{N}}$ de nombres réels, et deux réels a, b avec $a < b$, on peut construire un réel c clairement distinct de tous les x_i et compris entre a et b

Il s'agit d'une version précise du théorème selon lequel $\mathbb{R}$ n'est pas dénombrable. C'est une affirmation de caractère positif (on peut construire ...) susceptible de fournir un programme qui "exécute" le théorème.

Quelle doit donc être l'interprétation constructive de cet énoncé en termes de cardinaux ? La notion de cardinal a été élaborée par Cantor pour comparer entre eux des infinis actuels. L'idée était de les comparer selon leur taille.

Constructivement, la question de comparer entre eux des infinis potentiels tels que $\mathbb{N}$ et $\mathbb{R}$ est également légitime. Mais en tant qu'infinis potentiels, ils n'ont pas réellement de taille, et il serait sans doute impossible d'attribuer une signification à l'affirmation qu'un infini potentiel est **plus gros** qu'un autre, ne serait-ce qu'en raison de l'argument avancé au tout début de cette section. Ce que dit la preuve du théorème de Cantor, c'est que les nombres réels ne peuvent pas être générés de manière automatique comme les nombres entiers, selon un processus clairement défini une fois pour toutes. Chaque fois qu'on aura défini un processus de manière claire, il produira une suite de nombres réels, et il manquera tout plein de nombres réels dans cette suite. En deux mots :

L'infini $\mathbb{R}$ est plus compliqué que l'infini $\mathbb{N}$

Si on adopte le point de vue des constructivistes russes selon lequel tout nombre réel doit pouvoir être calculé de manière purement mécanique⁽¹⁰⁾, on peut produire une preuve que l'ensemble $\mathbb{R}$ peut être mis en bijection avec le quotient (par une relation d'équivalence) d'un sous-ensemble R de $\mathbb{N}$. Cela ne contredit pas l'interprétation constructive du théorème de Cantor, en effet :

"La partie" R est nettement plus compliquée que "le tout" $\mathbb{N}$.

Cela contredit par contre les mathématiques classiques.

Le point de vue constructif minimal développé par Bishop (cf. [BB] et [MRR]) ne prétend pas donner de définition du mot «effectif», qui est pris comme une notion primitive. En conséquence, tous les théorèmes obtenus avec ce point de vue sont vrais pour à peu près tous

¹⁰ En mots de tous les jours : tout procédé effectif doit pouvoir être mécanisé de manière automatique.

les mathématiciens⁽¹¹⁾. En outre, ils ont toujours un contenu algorithmique et constituent en quelque sorte des schémas de programmes informatiques.

Il est intéressant d'analyser l'hypothèse du continu quand on se place du point de vue constructif minimal. La première chose que l'on constate, c'est que des tas d'énoncés équivalents à HC en mathématiques classiques, ne peuvent plus être prouvés équivalents en mathématiques constructives, ce qui fournit autant d'hypothèses du continu distinctes, n'ayant pas la même signification intuitive. Si nous comparons deux infinis selon le point de vue des applications injectives de l'un vers l'autre, alors l'hypothèse du continu s'avère plutôt fausse, et certainement indémontrable⁽¹²⁾. En effet l'infini $\mathbb{N}$ peut être injecté dans l'infini $2^{\mathbb{N}}$ qui peut lui-même être injecté dans l'infini $\mathbb{R}$, (cf. l'ensemble triadique de Cantor), mais l'infini $\mathbb{R}$ ne sera (sans doute) jamais injecté de manière constructive dans $2^{\mathbb{N}}$: cette impossibilité est un théorème des constructivistes russes, et ce théorème "russe" empêche qu'on puisse construire l'injection au moyen d'un procédé purement mécanique.

Conclusion

Face aux problèmes posés par la "signification réelle" des énoncés mathématiques de la théorie des ensembles infinis actuels⁽¹³⁾ d'une part, et par la "validité réelle" des résultats obtenus dans cette théorie (problème de validité qui se pose lorsque ces résultats ont une signification concrète évidente), la tentation est grande de se rabattre sur un système formel du genre "théorie axiomatique des ensembles ZFC".

C'est pourtant une option bien contestable, car quel intérêt porter à une théorie formelle dont les "théorèmes" ne prétendent plus énoncer des Vérités ?

Le point de vue "constructif" en mathématiques est le point de vue "réaliste concret" qui, à propos de chaque énoncé mathématique, pose le problème de sa "signification algorithmique". Le point de vue "constructif" demande que toute affirmation mathématique ait *un sens*. Cela ne revient pas à jeter bas toutes les mathématiques "classiques" mais à les aborder d'un autre point de vue.

E. Bishop, auteur de "Fondements de l'analyse constructive", fait à ce sujet la remarque suivante :

*« Le point de vue constructif ne signifie pas que les mathématiques classiques sont "sans valeur". Ce serait aussi stupide que de dire que, d'un point de vue "classique" les mathématiques "non rigoureuses" seraient "sans valeur".
Tout théorème de mathématiques classiques pose un défi au mathématicien constructif
– soit en trouver une démonstration constructive
– soit en donner une version constructive. »*

Je terminerai en remarquant que dans les applications "concrètes" des mathématiques (en physique théorique, en astronomie...) il s'agit toujours en fin de compte de décrire des

¹¹ Il y a des mathématiciens qui n'admettent pas l'extrapolation du potentiellement réalisable, et qui donc ne sont pas satisfaits par les mathématiques constructives à la Bishop.

¹² L'affirmation peut paraître un peu présomptueuse. Il faudrait préciser "indémontrable dans tous les systèmes formels constructifs connus". Une caractéristique des systèmes formels constructifs actuels est que toute preuve d'existence "contient en filigrane" une preuve d'existence explicitée par des procédés purement mécaniques.

¹³ Ce qu'on appelle ordinairement la "théorie des ensembles" est en fait une "théorie des ensembles infinis actuels".

processus de calcul qui, à partir de certaines données numériques, permettent d'obtenir des résultats sous forme numérique, à vérifier ou infirmer par l'expérience. Ainsi seule la partie "constructive" des mathématiques s'avérera en définitive un jour ou l'autre "utile" et "vérifiable"⁽¹⁴⁾. La partie non constructive, elle, consiste essentiellement en un *discours* concernant des êtres mathématiques dont l'existence réelle est tout sauf évidente. Et personne (sauf à croire en un Dieu mathématicien) ne peut être sûr que ce discours n'est pas en grande partie "vide de sens".

¹⁴ Il ne faut pas prendre cette affirmation pour la défense d'un point de vue "utilitaire". Même la partie constructive d'une théorie mathématique donnée n'est pas forcément directement ou immédiatement "utilisable" en physique théorique par exemple (son utilité peut n'apparaître que bien longtemps après sa construction comme théorie mathématique : cf. la théorie des groupes). Cependant, toute mathématique constructive est toujours "immédiatement utile" en tant que partie de la "théorie générale des processus" : ce qui revient à dire : tout énoncé de mathématiques constructives démontré constructivement a bien un sens.

Notes sur le formalisme en mathématiques

II

La question de savoir s'il y a lieu de reconnaître à la pensée humaine une vérité objective n'est pas une question théorique, mais une question pratique. C'est dans la pratique qu'il faut que l'homme prouve la vérité, c'est-à-dire la réalité, et la puissance de sa pensée, dans ce monde et pour notre temps. La discussion sur la réalité ou l'irréalité d'une pensée qui s'isole de la pratique, est purement scolastique.

VIII

Toute vie sociale est essentiellement pratique. Tous les mystères qui détournent la théorie vers le mysticisme trouvent leur solution rationnelle dans la pratique humaine et dans la compréhension de cette pratique.

Marx : thèses sur Feuerbach

Introduction

Le formalisme en mathématiques a été inventé en grande partie pour faire face aux nombreux paradoxes qui sont apparus avec l'avènement de la théorie des ensembles.

Un autre but du formalisme était une tentative de réduire le raisonnement mathématique à des calculs "automatiques" sur des symboles. Rêve qu'avait déjà caressé Leibniz.

La mise au point des géométries non euclidiennes avait, de plus, jeté un doute sur la notion de vérité absolue. Auparavant les mathématiciens pensaient plus ou moins soumettre à leur étude des objets existant réellement, tel l'espace euclidien à 3 dimensions. Et les vérités concernant ces objets réels semblaient indiscutables.

Quand il apparut que l'axiome des parallèles n'était pas indiscutable, on put se demander qu'est ce qui était vraiment indiscutable en mathématiques.

La logique formelle et la formalisation des théories mathématiques avaient pour but également d'aboutir à préciser la partie vraiment indiscutable de la logique et des mathématiques.

Le but du formalisme tel que le définissait Hilbert était donc de trouver une base solide et universelle aux mathématiques :

- *solide* parce qu'entièrement basée sur des procédés de démonstration prédéfinis portant sur des énoncés finis et ne faisant appel à aucune propriété douteuse de l'infini,
- *universelle* parce qu'on espérait que toutes les mathématiques passées et à venir pourraient entrer dans le cadre de ce formalisme.

Après l'échec du projet formaliste, ces espoirs démesurés peuvent sembler bien naïfs. Il faut pourtant voir qu'à l'époque, la théorie des ensembles semblait être un cadre de référence dans lequel toutes les mathématiques trouvaient leur place. Aujourd'hui encore c'est le point de vue de la plupart des mathématiciens.

La théorie des ensembles se serait-elle avérée formalisable au sens où l'espérait Hilbert, alors l'ensemble de son projet se serait révélé valide.

Pour expliquer les limites du formalisme, il est nécessaire d'avoir une idée un peu précise de ce qu'est :

- un *langage mathématique du premier ordre* (cf. A1),
- une *interprétation* (ou réalisation) de ce langage (cf. A2),
- un *modèle* d'un système d'axiomes de ce langage (cf. A3).

Il est en particulier nécessaire d'introduire la notion de *vérité sémantique* d'un énoncé du premier ordre interprété dans un modèle.

Il faut noter que tant la description d'un langage que la description de la notion de modèle utilisent une "théorie naïve" des ensembles. Par exemple, un langage est "un ensemble de mots". Les notions "d'objets" (tels que les lettres d'un alphabet ou les objets d'un modèle) et de "collection d'objets" sont donc admises a priori et ne peuvent être discutées qu'à un autre niveau. Néanmoins, les collections d'objets qu'on utilise (mots d'un langage ou objets d'un modèle) ont en général le mérite d'être "vraiment bien définies" (ceci est d'ailleurs plus vrai pour les mots d'un langage que pour les objets de certains modèles).

Remarquons enfin que d'autres tentatives de "formalisation de la vérité" en mathématiques sont possibles en se basant sur d'autres langages que les langages du premier ordre. Sans entrer dans le détail de ces autres langages, j'essaye en A4 d'expliquer quelles limitations a priori résultent de l'utilisation exclusive de "langages du premier ordre".

Je vous propose donc de suivre le plan suivant :

- A Exposition d'un langage formel (celui de l'arithmétique) d'un système d'axiome (celui de Peano), de l'un de ses modèles (l'ensemble des entiers naturels).
- B Première discussion sur la notion de vérité en mathématiques à travers l'exemple précédent. Théorème de complétude de Gödel.
- C Les problèmes posés par la théorie des ensembles et par sa formalisation.
- D L'insuffisance fondamentale des systèmes formels à travers le théorème d'incomplétude de Gödel et de le théorème de "non définissabilité de la vérité" de Tarski.
- E Remarques sur le programme de Hilbert.
- F Quelques conclusions.

A Le langage de l'arithmétique, les axiomes de Peano, le modèle standard

A1 Le langage de l'arithmétique

Le langage de l'arithmétique est un ensemble de "mots bien formés" à partir d'un alphabet qu'on va définir et de règles de formation des mots (qu'on n'explicitera que par des exemples).

Nous noterons par la suite $\mathcal{La}$ le langage de l'arithmétique.

Ce sera donc un "ensemble intuitif" ou "collection" de mots.

L'alphabet est le suivant¹ :

deux symboles de constante	:	1	et	0
deux symboles fonctionnels	:	+	et	$\times$
deux symboles relationnels	:	<	et	=
des symboles de variables	:	x, x', x'', x'''	etc.	
les connecteurs logiques	:	$\neg$	$\wedge$	$\vee$ $\Rightarrow$ et $\Leftrightarrow$
les quantificateurs	:	$\forall$	et	$\exists$
les parenthèses	:	)	et	(

L'alphabet qu'on vient de définir contient une infinité de symboles de variables, mais on peut se ramener à un alphabet fini en introduisant la barre verticale "|" et les symboles de variables sont alors écrits $x, x|, x||$ etc...

Venons en maintenant à la définition des *termes* du langage $\mathcal{La}$, puis des *énoncés* du langage $\mathcal{La}$.

Un *terme* (d'arithmétique) est alors un mot construit à l'aide des symboles de fonction, des symboles de constante, des symboles de variable, et des parenthèses, selon des règles qu'il serait fastidieux d'expliciter. Donnons plutôt des exemples de termes, nous les encadrerons pour souligner le fait que nous les considérons comme de pures écritures, destinées à être étudiées pour elles-mêmes (voir A2) :

$$\boxed{(((1+1)+x) \times x) \times x'}$$

est un terme.

$$\boxed{(((1+1)+1)+1) \times ((x \times x) \times x) \times (x'+1)}$$

est un terme.

Dans la pratique on utilise des notations abrégées usuelles. Le premier terme écrit ci-dessus se note alors $\boxed{(2+x)xx'}$, et le deuxième terme écrit ci-dessus se note $\boxed{4x^3(x'+1)}$.

Dans la suite, nous désignerons par $\mathcal{Ta}$ la collection des *termes d'arithmétique* (bien écrits).

Un *énoncé atomique* est alors un mot de la forme :

$$\boxed{t = u}$$

ou

$$\boxed{t < u}$$

où t et u désignent deux termes.

¹ En ce qui concerne les connecteurs logiques, ils sont ici considérés comme lettres de l'alphabet $\mathcal{La}$ et, lorsqu'ils seront "interprétés", ils prendront leur sens habituel, mais je m'efforcerai de les écrire alors en français ordinaire.

Un *énoncé d'arithmétique* (ou “une formule d'arithmétique”) est alors soit un énoncé atomique, soit un mot construit à partir d'énoncés atomiques en utilisant les connecteurs logiques et les quantificateurs.

Exemples d'énoncés d'arithmétique

Nous noterons $R(x)$ l'énoncé d'arithmétique suivant :

$$\exists a \exists b \exists c \exists d \quad x = a^2 + b^2 + c^2 + d^2$$

Dans l'énoncé (ou formule) $R(x)$ la variable x est dite libre tandis que les autres variables a, b, c, d sont dites liées (ou “sous quantificateur”)(2).

Remarquons que nous avons écrit en fait une notation abrégée pour l'énoncé suivant

$$\exists a \exists b \exists c \exists d \quad x = (a \times a) + (b \times b) + (c \times c) + (d \times d)$$

Nous noterons $S(x)$ l'énoncé suivant(3) :

$$\begin{aligned} & \exists a \exists b \forall z \forall t : \\ & (zt=a \Rightarrow (z=1 \vee t=1)) \wedge (zt=b \Rightarrow (z=1 \vee t=1)) \\ & \wedge (x+x+4 = a+b) \wedge 1 < a \wedge 1 < b . \end{aligned}$$

Dans cet énoncé, la variable x est libre et les autres variables sont liées.

On a utilisé les abréviations zt pour $z \times t$ et 4 pour $((((1+1)+1)+1))$ et on a supprimé quelques parenthèses.

Anticipons sur le paragraphe qui suit : l'interprétation de l'énoncé $R(x)$ dans le modèle standard de l'arithmétique sera « x est une somme de 4 carrés ». Quant à l'interprétation de l'énoncé $S(x)$ dans le modèle standard, ce sera « $2x + 4$ est la somme de deux nombres premiers ».

Le langage de l'arithmétique est donc, pour récapituler, la collection des énoncés d'arithmétique bien écrits. Cette collection, nous la notons $\mathcal{La}$.

A2 Une interprétation (ou réalisation) du langage $\mathcal{La}$

Elle est définie par la donnée de :

- un ensemble intuitif (ou collection) N (4),
- deux éléments de N , notés 0 et 1 ,
- deux lois de composition interne sur N , notées $+$ et $\times$,
- une relation binaire sur N , notée $<$.

Par “loi de composition interne sur N ”, on entend une application de $N \times N$ dans N , et par “relation binaire sur N ” une application de $N \times N$ dans $\{\text{Vrai}, \text{Faux}\}$.

2 Nous utilisons la notation $R(x)$ avec un caractère gras pour indiquer que $R(x)$ désigne un énoncé d'arithmétique (mais ce n'en est pas un en tant qu'écriture).

3 Certains pièges doivent être évités dans les manipulations de quantificateurs. Dans une formule donnée, les variables liées peuvent a priori changer de nom sans que l'interprétation de la formule en soit affectée, mais certains renommages ont des effets désastreux. Par exemple dans l'énoncé $\exists x \quad x \neq y$ on peut renommer à peu près comme on veut la variable x mais le renommage y n'est évidemment pas autorisé.

4 N est parfois appelé la “collection des objets de l'interprétation” ou, dans le cas des modèles, “la collection sous-jacente du modèle”

Une réalisation du langage $\mathcal{La}$ étant donnée, tout *terme d'arithmétique* peut être interprété comme un élément de N une fois qu'on a attribué à chaque symbole de variable figurant dans le terme une valeur comme élément de N . (pour interpréter un terme, il faut donc également interpréter les symboles de variables qui figurent dans le terme).

Toujours en considérant donnée une réalisation du langage $\mathcal{La}$, tout énoncé d'arithmétique est alors interprété comme Vrai ou Faux selon les valeurs attribuées aux variables libres qui figurent dans l'énoncé.

Il faut naturellement donner aux connecteurs logiques et quantificateurs leur interprétation habituelle :

$A \wedge B$	est Vrai	si et seulement si	A et B sont Vrais
$A \vee B$	est Faux	si et seulement si	A et B sont Faux
$A \Rightarrow B$	est Faux	si et seulement si	A est Vrai et B est Faux
$\neg A$	est Vrai	si et seulement si	A est Faux
$\forall x \, U(x)$	est Vrai	si et seulement si	$U(x)$ est Vrai pour toute interprétation du symbole de variable x
$\exists x \, U(x)$	est Vrai	si et seulement si	$U(x)$ est Vrai pour au moins une interprétation de x

Enfin, le signe $=$ doit être interprété par la relation d'égalité.

La *réalisation standard* de $\mathcal{La}$ consiste à prendre pour N la collection $\mathbb{N}$ des entiers naturels et, pour 0 , 1 , $+$, $\times$ et $<$, l'interprétation habituelle.

A3 Les axiomes et les modèles du système formel *Peano*

On va donner un système d'axiomes assez intuitifs pour décrire des propriétés vérifiées par la réalisation standard $\mathbb{N}$ du langage de l'arithmétique $\mathcal{La}$. Ce système d'axiomes est une formalisation possible des axiomes qui avaient été proposés (de manière informelle) par Peano.

Le système formel *Peano* est donné par le langage $\mathcal{La}$ et la collection de ces axiomes.

Les axiomes du système formel *Peano* sont des énoncés d'arithmétique, ils forment une sous collection de $\mathcal{La}$. On ne va pas ici les écrire tous explicitement car ce serait un peu long et moins parlant.

Ce sont donc les énoncés suivants :

- 0 - Les énoncés exprimant la commutativité et l'associativité de $+$ et $\times$, le fait que 0 et 1 sont des neutres pour l'addition et la multiplication, ainsi que la distributivité de $+$ par rapport à $\times$. Par exemple :

$$(x + y) \times z = (x \times z) + (y \times z).$$

1 - $z + x = z + y \Rightarrow x = y$

3 - $\neg (1 + x = 0)$ (en abrégé : $1 + x \neq 0$)

4 - $(x < y) \vee (x = y) \vee (y < x)$

5 - $x < y \Leftrightarrow \exists z \, x + z + 1 = y$

- 6 - Le schéma d'axiomes, dit *schéma de récurrence*, qui, étant donné une relation $U(x)$ contenant x comme variable non quantifiée⁽⁵⁾, fournit l'énoncé suivant :

⁵ la formule $U(x)$ peut contenir d'autres variables libres que x

$$(U(0) \wedge (\forall x (U(x) \Rightarrow U(x+1)))) \Rightarrow \forall x U(x)) .$$

Un *modèle de Peano* est (par définition) une interprétation du langage $\mathcal{L}_a$ dans laquelle les axiomes de *Peano* sont interprétés comme Vrais (pour toute interprétation des variables libres qui y figurent).

Le *modèle standard* du système formel *Peano* est l'interprétation standard qui est définie au paragraphe précédent.

On sait démontrer que l'énoncé $\forall x R(x)$ (défini en fin de A1 et qu'on interprète dans le modèle standard par "tout entier est somme de 4 carrés") est interprété Vrai dans tout modèle de *Peano*.

Par contre, l'énoncé $\forall x S(x)$ (où $S(x)$ est défini en fin de A1 et qu'on interprète dans le modèle standard par "tout entier pair ≥ 4 est somme de deux nombres premiers") pose problème. Pour tout entier pair qu'on a voulu essayer, on a trouvé deux nombres premiers dont il est la somme :

$$12 = 7 + 5, 14 = 7 + 7, 28 = 17 + 11, \text{ etc ...}$$

Mais on ne sait pas s'il est interprété Vrai dans le modèle standard, et on ne sait pas non plus s'il est possible qu'il soit interprété Vrai dans le modèle standard et Faux dans un autre.

A4 Utilité et limites du langage $\mathcal{L}_a$ pour étudier les propriétés des entiers naturels

Aux yeux des mathématiciens, le principal mérite d'un langage tel que $\mathcal{L}_a$ est avant tout qu'il permet d'écrire de manière extrêmement précise des textes concernant les entiers naturels.

La rançon de cette "clarté et précision" des propriétés qu'on peut écrire au moyen d'énoncés d'arithmétique (c'est-à-dire d'énoncés appartenant au langage $\mathcal{L}_a$, c'est que le langage $\mathcal{L}_a$ ne permet pas d'écrire toutes les propriétés a priori intéressantes pour l'étude des entiers naturels.

Une propriété telle que "toute partie de $\mathbb{N}$ admet un plus petit élément" ne peut pas être écrite dans le langage $\mathcal{L}_a$. C'est-à-dire, précisément : il n'existe aucun énoncé d'arithmétique dont l'interprétation dans le modèle standard soit la propriété énoncée ci-dessus. Pour quelle raison ? tout simplement parce que les parties de $\mathbb{N}$ qui peuvent être décrites comme "ensemble des entiers n vérifiant un énoncé d'arithmétique $U(x)$ " ne sont pas toutes les parties de $\mathbb{N}$.

Donc, ce que l'on gagne en "clarification de la formulation des propriétés" on le perd sous forme de "restriction quant aux propriétés étudiées".

Mais, magie de la dialectique, cette "perte" est néanmoins source d'enrichissement car, désormais, une classification des propriétés concernant $\mathbb{N}$ est apparue : parmi les propriétés concernant $\mathbb{N}$, il y a celles qui sont les interprétations (standard) d'énoncés d'arithmétique et on les appelle les *propriétés arithmétiques* de $\mathbb{N}$. Les autres propriétés sont "plus complexes" et seront plus difficiles à étudier. Mais c'est déjà un bon renseignement que de savoir qu'une propriété est de nature arithmétique !⁽⁶⁾

⁶ Jusqu'à ce jour, on peut ranger les grandes conjectures mathématiques en deux groupes. Le premier groupe, formé des conjectures "sérieuses" est formé de problèmes concernant les mathématiques usuelles. Toutes ces conjectures sont prouvées équivalentes à des propriétés arithmétiques de $\mathbb{N}$. Le deuxième groupe est formé de conjectures concernant la théorie des ensembles. Dans ce dernier cas, ou bien on interprète ces conjectures en termes de systèmes formels, et elles sont ipso facto transformées en propriétés arithmétiques de $\mathbb{N}$ (par exemple, il y a des théorèmes d'arithmétique qui signifient que la théorie formelle des ensembles n'est pas

En particulier, on adoptera la définition suivante :

une partie de $\mathbb{N}$ est dite arithmétique si elle est la collection des entiers n qui vérifient (dans l'interprétation standard) un certain énoncé d'arithmétique $\mathcal{U}(x)$ à une seule variable libre. (la variable x est interprétée par l'entier intuitif n)

De même, on définira :

une relation liant deux éléments de $\mathbb{N}$ est dite arithmétique s'il existe un énoncé d'arithmétique $\mathcal{V}(x, y)$ tel que pour deux entiers naturels n, m arbitraires, n et m sont liés par la relation si et seulement si $\mathcal{V}(x, y)$ s'interprète Vrai dans le modèle standard lorsqu'on donne à x et y les valeurs n et m .

B Première discussion sur la notion de vérité en mathématiques, à travers l'exemple des entiers naturels

V

Feuerbach, qui ne satisfait pas la pensée abstraite en appelle à l'intuition sensible mais il ne considère pas le monde sensible en tant qu'activité pratique concrète de l'homme.

Marx : thèses sur Feuerbach

B1 Objection intuitionniste

Pour définir la valeur "Vrai" ou "Faux" d'un énoncé d'arithmétique lorsqu'il est interprété au moyen d'une interprétation de $\mathcal{L}_A$ (par exemple lorsqu'il est interprété dans le modèle standard de *Peano*), nous avons fait comme si cela ne posait a priori aucun problème.

Autrement dit, nous avons implicitement admis comme évidente la notion de *vérité sémantique* d'un énoncé d'arithmétique une fois qu'il est interprété dans un modèle.

Regardons pourtant ce que signifie la phrase :

L'énoncé d'arithmétique $\forall x \mathcal{S}(x)$ est interprété Vrai dans le modèle standard

où $\mathcal{S}(x)$ est l'énoncé défini en fin de A1.

Cette phrase signifie :

Tout nombre entier pair ≥ 4 est somme de deux nombres premiers.

Pour infirmer ce résultat : "il suffit" d'une vérification : trouver un entier pair $n \geq 4$. Établir la liste des nombres premiers inférieurs à n , et vérifier que la somme de deux d'entre eux n'est jamais égale à n .

Pour confirmer ce résultat : il faut, soit une démonstration convaincante, soit (si on n'en trouve pas) une infinité de vérifications : pour tout entier pair ≥ 4 , il faut trouver deux nombres premiers dont il est la somme.

Or, Homo Sapiens ne sait pas, et ne saura jamais, faire une infinité de vérifications en un temps fini. Penser qu'a priori l'énoncé $\forall x \mathcal{S}(x)$ est nécessairement interprété Vrai ou Faux dans le modèle standard réclame donc de croire en un "dieu de $\mathbb{N}$ " qui soit capable de faire, lui,

plus contradictoire avec l'axiome du choix ou avec sa négation, avec l'hypothèse du continu ou avec sa négation, etc..., ce qui a d'une certaine manière "résolu" les conjectures de l'axiome du choix et de l'hypothèse du continu), ou bien on interprète ces conjectures dans un hypothétique univers cantorien, et personne ne peut dire à l'heure actuelle que ce sont des conjectures ayant la moindre signification mathématique. Surement les logiciens ont du mettre au point des conjectures sérieuses concernant des propriétés non arithmétiques de $\mathbb{N}$ mais cela n'a pas "percé" dans la communauté des mathématiciens non spécialistes de logique.

l'infinité de vérifications nécessaires. C'est croire que "la vérité dans $\mathbb{N}$ " existe indépendamment de la pratique d'Homo Sapiens.

Si on introduit des formules plus compliquées que $\forall x \ S(x)$, avec des quantificateurs en cascade, du type :

$$\forall x \ \exists y \ \forall z \ W(x, y, z)$$

on s'apercevra qu'en général (c'est-à-dire lorsqu'on ne dispose pas de démonstration convaincante) il faudra une infinité de vérifications aussi bien pour infirmer que pour confirmer la vérité d'un énoncé d'arithmétique une fois qu'il est interprété dans le modèle standard, et même des infinités emboîtées de vérifications ...

B2 Pour contourner cette objection des intuitionnistes, il peut exister deux attitudes possibles

Ou bien on pense que l'objection n'est pas fondée car de toute manière "ou bien tout nombre pair est somme de deux nombres premiers, ou bien ce n'est pas vrai" et ainsi de suite pour tous les énoncés d'arithmétique (c'est-à-dire rappelons-le, les énoncés de $\mathcal{L}_A$) interprétés dans le modèle standard.

Ou bien on ignore le problème de l'interprétation du langage, on ignore le problème de la vérité sémantique et on fait comme si on n'étudiait que les propriétés du langage pour lui-même. C'est le point de vue formaliste poussé à l'extrême, tel qu'il est exposé dans l'introduction de Bourbaki. Mais ce un point de vue, en apparence confortable, est complètement débilitant et réduit l'activité des mathématiciens à l'étude d'un *jeu* particulier : celui du "langage de la théorie mathématique" dans lequel on cherche les combinaisons gagnantes (théorème R) et les combinaisons perdantes (théorème $\neg R$); les combinaisons indéterminées (ni R , ni $\neg R$ n'est un théorème) ne faisant d'ailleurs même pas partie de l'étude du jeu tel que la définit Bourbaki.

Dans la suite de ce texte, j'adopterai la terminologie suivante :

Le point de vue intuitionniste (pour $\mathbb{N}$ et $\mathcal{L}_A$) est l'attitude qui consiste à n'admettre pour "Vrai" ou "Faux" a priori dans le modèle standard que les énoncés d'arithmétique pour lesquels on dispose d'une démonstration convaincante (par exemple un processus de vérification aboutissant en un temps fini). Cette attitude implique qu'on refuse la loi du Tiers Exclu dans les "démonstrations convaincantes" dont il est question.

Le point de vue classique (pour $\mathbb{N}$ et $\mathcal{L}_A$) est l'attitude qui consiste à admettre que tout énoncé d'arithmétique est forcément Vrai ou Faux une fois qu'il est interprété dans le modèle standard.

Le point de vue formaliste (pour $\mathcal{L}_A$ et les axiomes de *Peano*) consiste à ignorer le modèle standard $\mathbb{N}$, à refuser de se poser la question de la vérité sémantique dans l'interprétation standard, et à étudier la théorie formelle *Peano* basée sur le langage $\mathcal{L}_A$ pour elle-même.

Ce dernier point de vue n'est cependant pas aussi absurde que ce qu'il peut paraître au premier abord. Pour le comprendre, il faut qu'il soit expliqué un peu plus en détail. C'est ce qui est fait dans le paragraphe qui suit.

B3 Description rapide (et informelle) de la théorie formelle “arithmétique de Peano”

Au lieu de rechercher quels sont les énoncés d'arithmétique qui sont interprétés “Vrai” dans le modèle standard, on recherche quels sont tous les énoncés d'arithmétique “qu'on peut déduire des axiomes de *Peano* au moyen de règles de déduction logique répertoriées et considérées valables d'un point de vue classique”.

Ces “règles de déduction logique répertoriées considérées valables d'un point de vue classique” constituent ce qu'on appelle la *logique formelle* (classique) des langages du premier ordre (c'est-à-dire des langages semblables à $\mathcal{L}_a$).

La collection des énoncés d'arithmétique ainsi obtenus est appelée la “collection des théorèmes formels du système formel *Peano*”. (on dit souvent “arithmétique de Peano” au lieu de “système formel *Peano*”)

Si on note $\mathcal{P}_1$ le système d'axiomes de *Peano*, on note alors $\text{Tf}(\mathcal{L}_a, \mathcal{P}_1)$, ou $\text{Tf}(\text{Peano})$ la collection des théorèmes formels de l'arithmétique de *Peano*.

On voit qu'ici, on a une double limitation a priori :

- La limitation dont on a déjà parlé en A4 : on ne s'intéresse qu'aux “énoncés d'arithmétique” lesquels, une fois interprétés dans $\mathbb{N}$, ne traduisent que certaines des propriétés de $\mathbb{N}$.
- On ne s'intéresse qu'aux énoncés “qui peuvent se déduire d'un nombre fini d'axiomes”, ou du moins d'axiomes parfaitement bien définis a priori.

Si on se place d'un point de vue classique, tous les “théorèmes de l'arithmétique de Peano” sont “vrais” lorsqu'interprétés dans $\mathbb{N}$ parce que la logique formelle utilisée (c'est-à-dire les règles de déduction logique répertoriées utilisées) sont valables du point de vue classique et que les axiomes eux-mêmes sont vrais dans $\mathbb{N}$.

Si on se place d'un point de vue intuitionniste, certains “théorèmes de l'arithmétique formelle de *Peano*” ne sont pas forcément interprétés “Vrai” dans $\mathbb{N}$, parce que la logique formelle utilisée n'est pas valable (les axiomes, eux, ne posent pas problème).

Le point de vue formaliste “à outrance” ignore tout simplement le débat sur la nature de la vérité sémantique.

Le *programme de Hilbert* pour l'arithmétique peut être rephrasé comme suit. Dans sa version la plus forte (un peu folle), le programme de Hilbert demande une méthode mécanique capable de décider la vérité ou la fausseté de n'importe quel énoncé d'arithmétique de structure suffisamment simple⁽⁷⁾. Dans sa version raisonnable, le programme de Hilbert demande qu'un système mécanique capable de produire beaucoup de théorèmes en arithmétique (par exemple le système formel *Peano*) puisse être prouvé efficace (c.-à-d. ne jamais se tromper de manière flagrante) en utilisant uniquement des arguments d'une nature extrêmement simple⁽⁸⁾.

⁷ Nous tâcherons de sortir de ce flou dans la dernière partie, consacrée au programme de Hilbert.

⁸ Il semble difficile de préciser mieux le programme de Hilbert sans donner des définitions techniques un peu dures à digérer. Néanmoins, lorsque nous parlerons du théorème d'incomplétude de Gödel en D2, il sera clair, sans besoin d'aucune définition technique, que ce théorème ruine définitivement le programme de Hilbert pour l'arithmétique. Dans la partie E, nous essaierons de montrer qu'une version légèrement affaiblie de ce programme reste d'une très grande pertinence.

B4 Les règles de la logique formelle (pour un langage du premier ordre) sont “entièrement satisfaisantes” du point de vue classique (théorème de complétude de Gödel)

Cette affirmation, que je vais essayer d'expliquer, est évidemment d'un grand soulagement pour les formalistes à outrance, car ça leur permet de garder dans un coin de leur tête (mais sans le dire) que tout ce qui se fait en mathématiques formelles a quelque chose à voir avec “le sens” et la “réalité”.

Rappelons ici qu'un langage du premier ordre est un langage $\mathcal{L}$ du même type que $\mathcal{L}_A$ mais où on s'autorise à prendre d'autres symboles de fonction, d'autres symboles relationnels et d'autres symboles de constante que ceux de $\mathcal{L}_A$.

Rappelons aussi que la *logique formelle classique* est un ensemble de règles de manipulations d'énoncés de $\mathcal{L}$ qui, lorsque ces énoncés sont “interprétés”, constituent des règles de déduction logique valables d'un point de vue classique.

Du point de vue formel, ces règles sont de simples manipulations d'énoncés. Par exemple, une de ces règles est la suivante : si $A \Rightarrow B$ et si A font partie de la collection des théorèmes formels, alors, par la règle dite Modus Ponens, B fait également partie de la collection des théorèmes formels.

Dans ce cadre, le théorème de Gödel (de complétude) établit une *adéquation parfaite* entre, d'une part :

- (1) les énoncés du langage $\mathcal{L}$ du premier ordre démontrables au moyen de la logique formelle classique

et, d'autre part :

- (2) les énoncés prenant la valeur Vrai dans toute interprétation du langage du premier ordre considéré.

Évidemment, l'adéquation parfaite démontrée dans le théorème de Gödel est démontrée, dans le sens (1) implique (2), au moyen de raisonnements sur les modèles faisant appel à des principes de déduction logiques valables d'un point de vue classique uniquement. En ce qui concerne le sens (2) implique (1), la preuve du théorème de Gödel utilise un principe de construction d'ensembles basé sur un usage systématique du principe du Tiers Exclu concernant des énoncés d'arithmétique a priori non décidables. Bref, l'adéquation parfaite n'est parfaite que du point de vue des mathématiques classiques, et elle nécessite une réinterprétation constructive⁽⁹⁾.

Néanmoins, il est important de noter que la phrase

“énoncé prenant la valeur Vrai dans toute interprétation du langage considéré”

peut être comprise dans un sens relativement faible, qui est précisé maintenant :

on peut se limiter aux interprétations où la collection des objets est, ou bien finie, ou bien est la collection des entiers naturels $\mathbb{N}$ et, dans le cas où la collection des objets est $\mathbb{N}$, on peut se limiter aux interprétations où les symboles relationnels et les symboles fonctionnels peuvent être définis arithmétiquement (voir A4 par exemple pour la définition d'une relation binaire arithmétique dans $\mathbb{N}$).

Autrement dit et plus précisément :

si un énoncé $\mathcal{E}$ d'un langage $\mathcal{L}$ (du premier ordre) n'est pas un théorème de logique formelle classique, on peut trouver une “interprétation arithmétique” des symboles (de

⁹ Du moins si on est convaincu de la pertinence du point de vue constructif

constante, de fonction, de relation) figurant dans le langage $\mathcal{L}$, tel que l'énoncé $\mathcal{E}$ soit interprété Faux.

À ce résultat de complétude (d'entière satisfaction) de la logique formelle du premier ordre, il faut opposer trois faits importants :

- ce résultat n'est établi que pour les langages du premier ordre, lesquels introduisent a priori une limitation dans l'étude des propriétés d'un objet mathématique (tel que $\mathbb{N}$ par exemple),
- la logique formelle utilisée dans le système formel, et la logique concrète mise en oeuvre dans la preuve du théorème de complétude ne sont pas acceptables d'un point de vue intuitionniste, cela signifie que le théorème de complétude de Gödel nécessite une relecture complète du point de vue constructif
- du point de vue classique comme du point de vue constructif, aucun système d'axiome raisonnable ne permet de décrire entièrement les propriétés arithmétiques de $\mathbb{N}$ (c'est le théorème d'incomplétude de Gödel, qui sera discuté plus loin).

C Les problèmes posés par la formalisation de la théorie des ensembles et par la théorie des ensembles elle-même

C1 Deux actes de foi de la théorie des ensembles

Nous avons déjà remarqué dans l'introduction qu'un minimum de théorie naïve des ensembles est nécessaire pour développer toute théorie mathématique.

On a besoin de la notion d'objets distincts, on a besoin de savoir repérer que deux signes d'un alphabet sont “les mêmes” alors qu'ils sont écrits en deux endroits distincts de la page, on a aussi besoin de la notion de “collection potentiellement infinie” aussi bien pour définir un objet d'études mathématiques (par exemple : la collection potentiellement infinie des entiers naturels) que pour développer une théorie formelle (la collection potentiellement infinie des mots d'un langage du premier ordre).

Avec l'avènement de la théorie des ensembles, il s'est agi de tout autre chose et Cantor avait bien raison (de son point de vue) de remercier Dieu d'avoir créé un “univers mathématique” infini dans lequel on peut sans scrupule :

- considérer un ensemble infini tel que $\mathbb{N}$ comme un infini “actuel” (et non potentiel),
- considérer, une fois qu'un ensemble “existe” que toute partie de cet ensemble “existe” également, pour elle-même, en dehors du fait qu'elle puisse être pensable ou non par un homme, et même :
- construire, pour tout ensemble donné A , l'ensemble de toutes les parties de cet ensemble (“beaucoup plus gros” que A),

Avec l'univers mathématique de Cantor (ou plutôt celui de Zermelo-Frankel qui a permis d'éliminer tous les paradoxes apparus à ce jour dans celui de Cantor) nous voici dans le royaume de la vérité sémantique absolue.

Les mathématiques sont désormais l'étude de cet univers à la fois monstrueux et admirable, dont certaines des propriétés resteront à tout jamais cachées aux Homo Sapiens, mais qu'importe.

Et, chose remarquable, si un tel univers existe et peut être soumis aux investigations par les méthodes relevant de la logique classique (répertoriées dans la logique formelle), alors on peut

définir en son sein d'autres Univers qui ont les mêmes propriétés de base (que celles énoncées précédemment) et qui, en outre, vérifient d'autres propriétés particulièrement commodes pour les raisonnements mathématiques.

Par exemple, l'axiome du choix, un temps controversé, est devenu un vulgaire "axiome des parallèles d'Euclide" : aucun danger à considérer qu'il est vrai puisque, si un univers mathématique existe *sans* axiome du choix, on pourra construire avec lui un autre univers mathématique *avec* axiome du choix (de la même manière que l'existence d'une géométrie euclidienne garantit l'existence d'une géométrie non euclidienne et vice versa).

Il y a pourtant une différence de taille entre la géométrie euclidienne et la théorie des ensembles.

La différence est la suivante :

- tout mathématicien qui croit en le modèle standard de l'arithmétique croit du même coup en la géométrie euclidienne car on peut construire sur la collection $\mathbb{N}$ une géométrie euclidienne (certains éléments de $\mathbb{N}$ étant appelés "points", d'autres "droites", d'autres "plans", d'autres "cercles", d'autres "sphères", et étant définis entre eux les relations "le point est sur la droite", "la droite est dans le plan" etc... , le tout vérifiant les axiomes d'une géométrie euclidienne⁽¹⁰⁾). De plus, cette construction sera parfaitement explicite, y compris la vérification des axiomes de la géométrie euclidienne dans le modèle : il s'agit donc d'une géométrie euclidienne satisfaisante d'un point de vue intuitionniste.
- mais tout mathématicien qui croit en le modèle standard de l'arithmétique ne croit pas forcément pour autant à l'univers mathématique de Zermelo-Frankel .

A cela deux ordres de raison :

- Dans la croyance en l'existence d'un univers mathématique à la Zermelo-Frankel, il y a véritablement deux "actes de foi" qui surpassent de loin "l'acte de foi en l'arithmétique", ce sont :
 - l'acte de foi de l'infini actuel,
 - l'acte de foi de l'ensemble des parties d'un ensemble.

Comme l'univers mathématique de Zermelo-Frankel, s'il existe, contient des ensembles infinis non dénombrables (c'est-à-dire, pour le mathématicien classique, "strictement plus gros que $\mathbb{N}$ ") un mathématicien classique ne peut espérer disposer un jour d'une construction analogue à celle de la géométrie euclidienne, pour un univers mathématique au sein de $\mathbb{N}$.

- si, au lieu de considérer comme possible, de manière purement abstraite, l'existence d'un univers mathématique à la Zermelo-Frankel, on considère seulement comme très probable le fait que les axiomes de Zermelo-Frankel sont non contradictoires, on peut alors construire (à l'aide du théorème de complétude de Gödel, qui a pour conséquence que tout système d'axiomes "bien défini"⁽¹¹⁾ et non contradictoire possède un modèle, et même un modèle arithmétique) un "modèle réduit" d'univers mathématique construit dans $\mathbb{N}$, pour lequel tous les axiomes de $\mathcal{ZF}$ sont interprétés "Vrai". Dans ce cas, on se trouve néanmoins confronté à trois problèmes d'importance :
 - le fait que le "modèle réduit" d'univers mathématique n'est vraiment que le pâle reflet de l'univers mathématique "réel" puisque tous les "ensembles dans le modèle", s'ils

¹⁰ Par exemple si on choisit comme axiomes un système décrivant les propriétés d'un plan "euclidien" construit sur un corps "réel clos", où un corps réel clos est défini comme un corps ordonné dans lequel les fonctions polynômes vérifient le théorème de la valeur intermédiaire. Ce genre de cadre est le cadre le plus simple où on puisse réaliser le programme de Descartes d'algébrisation des théorèmes de géométrie.

¹¹ Par exemple un système d'axiomes fini, ou un système d'axiomes infini mais engendré par un processus parfaitement explicite.

ne sont pas “dénombrables dans le modèle”, sont néanmoins “dénombrables hors du modèle” (en effet, ces “ensembles dans le modèle” peuvent tous être définis comme des parties arithmétiques de $\mathbb{N}$)

- le fait que le “modèle réduit” d'univers mathématique possède des propriétés de type pathologique (voir les résultats de Rabin paragraphe suivant),
- le fait enfin que la construction du modèle réduit n'est possible que si les axiomes de $\mathcal{ZF}$ sont non contradictoires, or Homo Sapiens ne sait pas, et ne saura sans doute jamais, si les axiomes de $\mathcal{ZF}$ sont non contradictoires (voir D).

C2 À propos des modèles réduits arithmétiques de l'Univers à la Cantor-Zermelo-Fraenkel

Ces résultats de M.O. Rabin concernent les “modèles réduits” dénombrables d'univers mathématique ou, si l'on préfère, les “modèles ayant comme collection d'objets les entiers naturels”.

Le système d'axiomes utilisé n'est pas $\mathcal{ZF}$ mais une version affaiblie du système $\mathcal{GB}$ ($\mathcal{GB}$ comme : Gödel Bernays). Je vais décrire rapidement et informellement ce système d'axiomes affaibli que je noterai $\mathcal{GB}^-$, mais précisons tout de suite que $\mathcal{ZF}$ et $\mathcal{GB}$ sont fondamentalement équivalents (au même sens que géométrie euclidienne et non euclidienne sont fondamentalement équivalentes).

Décrivons tout d'abord le langage utilisé (qui est le même pour $\mathcal{ZF}$ ou $\mathcal{GB}$) :

- il y a un seul symbole de constante : $\emptyset$
- il n'y a pas de symbole de fonction
- il y a deux symboles de relation : $=$ et $\in$
- il y a enfin les symboles logiques communs à tous les langages du premier ordre.

On notera $\mathcal{L}_e$ ce “langage de la théorie des ensembles”.

Les axiomes de $\mathcal{GB}$ décrivent un univers mathématique hypothétique $\mathcal{U}$ où il y a deux types d'objets : d'une part les ensembles, d'autre part les classes. Tout ensemble est une classe (donc tout objet est une classe), toute classe est entièrement définie par les ensembles qui lui appartiennent, mais certaines classes sont “trop grosses” pour être des ensembles (par exemple la classe de tous les ensembles).

Dans un univers mathématique de $\mathcal{GB}$, l'énoncé :

$$\exists x \quad y \in x$$

s'interprète donc dans $\mathcal{U}$: y est un ensemble

et l'énoncé :

$$\forall x \quad \neg (y \in x)$$

s'interprète dans $\mathcal{U}$: y est une classe propre (une classe qui n'est pas un ensemble).

Voici donc les axiomes de $\mathcal{GB}^-$ (cf. annexe pour leur écriture sous forme d'énoncés de $\mathcal{L}_e$) :

- pour les classes (classes propres ou ensembles) :
 - il existe une classe contenant tous les ensembles : W
 - il existe une classe contenant tous les couples d'ensembles (x, y) tels que $x \in y$
 - si deux classes A et B existent alors $A \cap B$, $A \cup B$, $A \times B$, $W - A$ existent également,
 - deux classes qui ont les mêmes éléments sont égales
 - si une classe A existe, alors la classe : $\text{Dom}(A) = \{ x \mid \exists y (x, y) \in A \}$ existe également

- quatre axiomes annexes introduits pour des raisons techniques (et qui ne posent pas réellement problème)
- pour les ensembles (du modèle) :
 - les axiomes habituels de $\mathcal{ZF}$, sans l'axiome de l'ensemble infini ni l'axiome du choix, et en remplaçant un schéma d'axiome dit “schéma de substitution” par un seul axiome, grâce au recours des classes.

Notez que le système d'axiomes est fini et peut donc être remplacé par un axiome unique.

Dans les modèles de $\mathcal{GB}^-$, on n'a pas besoin d'ensemble infini, mais on a une classe de tous les ensembles finis. Ce système formel est donc une manière d'accepter le premier acte de foi, l'existence d'un infini actuel, en omettant le second, l'existence de l'ensemble des parties d'un ensemble infini.

Décrivons maintenant un “modèle naturel” de $\mathcal{GB}^-$, plus crédible qu'un univers de $\mathcal{GB}$ (dans lequel il y a nécessairement non seulement des classes infinies, mais aussi des “ensembles” infinis). Pour décrire ce “modèle naturel”, nous nous plaçons d'un point de vue “théorie naïve des ensembles finis”. Nous considérons alors toutes les collections finies qui peuvent être “écrites à la main” en utilisant les symboles $\emptyset$, $\{$, et $\}$. Par exemple :

$$\emptyset; \{\emptyset\}; \{\emptyset, \{\emptyset\}\}; \{\emptyset, \{\{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}\}.$$

Toutes ces collections finies peuvent être obtenues comme éléments des collections finies $\mathbb{V}_n$, construites par récurrence comme suit :

$$\begin{aligned} \mathbb{V}_0 &= \emptyset & \mathbb{V}_1 &= \mathcal{P}(\mathbb{V}_0) = \{\emptyset, \{\emptyset\}\} \\ \mathbb{V}_2 &= \mathcal{P}(\mathbb{V}_1) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \\ \mathbb{V}_{n+1} &= \mathcal{P}(\mathbb{V}_n) & (\mathcal{P}(A) \text{ est la collection des parties de } A) \end{aligned}$$

Pour construire notre “modèle naturel”, nous posons tout d'abord :

$$\mathbb{V}_\omega = \bigcup_{n \in \mathbb{N}} \mathbb{V}_n$$

puis

$$\mathbb{W} = \mathcal{P}(\mathbb{V}_\omega).$$

Enfin nous considérons $\mathbb{W}$ comme collection des objets du “modèle naturel”, et nous interprétons $\boxed{\in}$ par $\in$ dans $\mathbb{W}$. Je dis qu'on obtient un modèle de $\mathcal{GB}^-$.

En effet, on démontre par récurrence que $\mathbb{V}_n \subset \mathbb{V}_{n+1}$, puis que toute partie finie de $\mathbb{V}_\omega$ est un élément de $\mathbb{V}_\omega$.

Par ailleurs, tout élément de $\mathbb{V}_\omega$ est une partie finie de $\mathbb{V}_\omega$. Donc $\mathbb{V}_\omega \subset \mathbb{W}$ et on a :

- tout objet du modèle est une partie de $\mathbb{V}_\omega$.
- les parties finies de $\mathbb{V}_\omega$ sont les “ensembles” du modèle, .
- les parties infinies de $\mathbb{V}_\omega$ sont les “classes propres” du modèle.

On vérifie facilement que les axiomes de $\mathcal{GB}^-$ sont vérifiés dans ce “modèle naturel”.

Ce “modèle naturel” $\mathbb{W}$ et ce système d'axiomes $\mathcal{GB}^-$ constituent en quelque sorte le degré zéro de la théorie des ensembles infinis de Cantor, le point précis où l'on décolle du point de vue purement “naïf” (“intuitif”). En fait, structurellement le triplet $(\mathbb{V}_\omega, \mathbb{W}, \in)$ est “isomorphe”⁽¹²⁾ au triplet $((\mathbb{N}, +, \times, 0, 1, <), \mathcal{P}(\mathbb{N}), \in)$

Pour tout mathématicien qui croit en $\mathbb{W}$ et qui croit en la logique formelle classique lorsqu'elle est interprétée dans $\mathbb{W}$, le système d'axiome $\mathcal{GB}^-$ est manifestement non contradictoire (de la même manière qu'un mathématicien qui croit en $\mathbb{N}$ et en la logique formelle lorsqu'elle est interprétée dans $\mathbb{N}$ pense du même coup que le système d'axiome de *Peano* est non

¹² Représente le même degré de complexité logique

contradictoire).

Par ailleurs, si un mathématicien classique considère le modèle $(\mathbb{V}_\omega, \mathbb{W}, \in)$ comme un modèle extrêmement naturel de $\mathcal{GB}^-$, c'est parce qu'il pense que $\mathcal{P}(\mathbb{V}_\omega)$ n'est absolument pas problématique. Pour un mathématicien qui pense que $\mathcal{P}(\mathbb{V}_\omega)$ est, tout comme $\mathcal{P}(\mathbb{N})$, un objet bien mystérieux et sans doute problématique, le système formel peut être vu, soit comme un "mauvais système d'axiomes" ne correspondant à aucune réalité mathématique, soit comme un moyen d'investigation d'une réalité mathématique sensiblement distincte du $\mathcal{P}(\mathbb{V}_\omega)$ des mathématiciens classiques.

Les deux résultats de Rabin concernent les "modèles réduits" du système d'axiomes $\mathcal{GB}^-$. Si ce système est non contradictoire, il admet, d'après une conséquence du théorème de complétude de Gödel, un modèle dénombrable et même un modèle arithmétique (c'est-à-dire, rappelons-le, un modèle où la collection des objets est $\mathbb{N}$ et où la relation $\underline{\in}$ (qui interprète le symbole $\in$) est une relation arithmétique).

Premier résultat :

Il est impossible de trouver une fonction $n \mapsto (x_n, y_n)$ parfaitement explicite de $\mathbb{N}$ dans $\mathbb{N} \times \mathbb{N}$, telle que la collection des couples (x_n, y_n) soit la collection des couples vérifiant $x_n \underline{\in} y_n$, où " $\underline{\in}$ " est une relation binaire sur $\mathbb{N}$ qui vérifie les axiomes de $\mathcal{GB}^-$.

Autrement dit : il n'y a pas de modèle réduit "simple" pour $\mathcal{GB}^-$.⁽¹³⁾

Si maintenant on considère des modèles structurellement plus compliqués, on a :

Deuxième résultat :

Considérons sur $\mathbb{N}$ une relation binaire arithmétique, que nous notons $\underline{\in}$, qui fasse de $(\mathbb{N}, \underline{\in})$ un modèle arithmétique de $\mathcal{GB}^-$. Alors ce modèle est "non standard pour les entiers", c'est-à-dire :

ce qui, dans ce modèle, joue le rôle de la "classe propre des entiers naturels" contient non seulement les analogues de 0, 1, 2, 3 etc... mais encore des tas d'autres éléments, appelés "entiers non standard".

Autrement dit : si on se place sur une position où on admet comme crédibles les "parties de $\mathbb{N}$ définies de manière arithmétique", mais pas d'autres collections plus compliquées, alors $\mathcal{GB}^-$ n'admet pas non plus de modèle "satisfaisant".

En fait ce résultat n'est pas si surprenant. La théorie formelle $\mathcal{GB}^-$ est assez puissante pour traduire *Peano* et elle permet donc de définir une classe pour toute partie arithmétique de $\mathbb{N}$. Ce qui, avec *Peano* relevait du métalangage, relève maintenant du langage lui-même. En conséquence le procédé diagonal de Cantor produit, dans le métalangage, des parties de $\mathbb{N}$ plus compliquées que n'importe quelle partie arithmétique (ce qui n'était pas le cas avec *Peano*). C'est cela qui fait que, si on se limite aux modèles arithmétiques, (notez que la question des modèles relève du métalangage), des comportements pathologiques apparaissent inévitablement.

Un mathématicien classique peut relire le deuxième résultat de Rabin sous la forme positive suivante : si on désire un modèle $(\mathbb{N}, \underline{\in})$ pour $\mathcal{GB}^-$ dans lequel les "entiers du modèle" sont tous standards, il faut que la relation $\underline{\in}$ sur $\mathbb{N}$ soit plus compliquée qu'une relation arithmétique.

¹³ En langage plus savant: il n'existe pas de modèle énuméré pour lequel la relation d'appartenance soit récursivement énumérable

Signalons en conclusion que la situation sera évidemment encore diablement plus compliquée si on considère les modèles de la théorie $\mathcal{GB}$ avec axiome de l'infini.

D L'insuffisance fondamentale des systèmes formels

Dans le premier paragraphe, j'explique en quoi la recherche des théorèmes d'une théorie formelle (pour un langage du premier ordre donné et pour un système d'axiomes bien défini de ce langage) est équivalente à l'étude d'une fonction bien définie de $\mathbb{N}$ dans $\mathbb{N}$.

Ce simple fait inciterait déjà fortement à douter de la capacité d'une théorie formelle à être la traduction de la notion de vérité en mathématiques.

Dans le deuxième paragraphe, j'essaie d'expliquer ce que signifie le théorème d'incomplétude de Gödel : ce théorème précise de manière très frappante un point où réside cette "incapacité" d'une théorie formelle. Elle réside dans l'incapacité à démontrer "sa propre non contradiction".

Dans le troisième paragraphe, j'explique en quoi ce résultat absolument remarquable de Gödel peut être interprété pour apporter de l'eau au moulin des intuitionnistes.

Dans le quatrième paragraphe, j'essaie d'expliquer ce que signifie le théorème de "non-définissabilité de la vérité" de Tarski. Ce théorème se situe sur un terrain légèrement différent du théorème d'incomplétude de Gödel, il ne s'attaque pas à la notion de théorie formelle mais seulement à la notion de langage formel et il affirme qu'un langage formel est incapable de décrire "sa propre vérité sémantique" dans une interprétation donnée.

D1 Arithmétisation d'une théorie formelle du premier ordre

Nous considérons donc un langage du premier ordre $\mathcal{L}$ analogue à $\mathcal{La}$ (c'est-à-dire avec les mêmes symboles logiques, mais avec des symboles de fonction, de constante et de relation différents) et un système $\mathcal{A}$ d'axiomes bien définis écrits dans $\mathcal{L}$. Autrement dit $\mathcal{A}$ est une sous-collection explicite de la collection des énoncés de $\mathcal{L}$.

La théorie formelle de $(\mathcal{L}, \mathcal{A})$ est définie de la même manière que la théorie formelle *Peano* de l'arithmétique. Cela signifie que les théorèmes formels de $(\mathcal{L}, \mathcal{A})$ forment la collection des énoncés de $\mathcal{L}$ qui peuvent être déduits des énoncés de $\mathcal{A}$ au moyen des règles de la logique formelle classique. Rappelons que nous notons $\text{Tf}(\mathcal{L}, \mathcal{A})$ la collection des théorèmes (formels) de cette théorie formelle.

Nous commençons par numéroter les énoncés de $\mathcal{L}$ (c'est-à-dire attribuer un numéro, qui est un entier naturel ordinaire, à chaque énoncé de $\mathcal{L}$). Voici comment cela fonctionne :

- tout d'abord on range dans un certain ordre les symboles de l'alphabet de $\mathcal{L}$ (on supposera pour simplifier cet alphabet fini),
- ensuite, on remarque que si un mot est écrit au moyen de cet alphabet, on peut déterminer par un processus explicite si ce mot est un énoncé (bien écrit) de $\mathcal{L}$ ou non,
- enfin on remarque que les énoncés bien écrits qui ont une longueur déterminée n sont en nombre fini et peuvent donc être rangés par ordre alphabétique,
- alors, pour obtenir le numéro d'un énoncé de $\mathcal{L}$, on compte d'une part tous les énoncés qui ont une longueur plus petite et d'autre part tous les énoncés qui ont même longueur mais qui le précèdent dans l'ordre alphabétique. La somme des deux nombres obtenus est le numéro de notre énoncé. Par exemple, l'énoncé le plus court et le premier par ordre alphabétique (parmi les énoncés de même longueur) a pour numéro 0,
- on voit que ce processus permet d'établir une correspondance entre $\mathbb{N}$ et $\mathcal{L}$ telle qu'à tout nombre soit associé un et un seul énoncé (qui ait ce nombre pour numéro).

On peut alors énoncer le théorème d'arithmétisation comme suit :

Théorème d'arithmétisation d'une théorie formelle

Soit $\mathcal{L}$ un langage du premier ordre et soit $\mathcal{A}$ un système d'axiomes bien défini de $\mathcal{L}$ (par exemple un système d'axiomes fini).

Soit $n \mapsto E_n$ une numérotation explicite des énoncés de $\mathcal{L}$.

Il existe une fonction parfaitement explicite : $f : n \mapsto f(n)$

de $\mathbb{N}$ dans $\mathbb{N}$, telle que la collection des nombres $m = f(n)$ soit exactement la collection des numéros des théorèmes formels du système formel $(\mathcal{L}, \mathcal{A})$.

NB : L'expression "fonction parfaitement explicite de $\mathbb{N}$ dans $\mathbb{N}$ " est justifiable d'une définition qui précise le sens intuitif qu'on lui attribue. Ici on peut fournir un processus explicite qui, à partir du numéro n permet de calculer le numéro $f(n)$. Ce processus est décrit informellement dans la preuve qui suit.

Le théorème d'arithmétisation n'est pas très difficile à démontrer mais demanderait quelques détails techniques. Disons que comme la collection $\mathcal{A}$ est bien définie et comme les règles de la logique formelle sont elles aussi bien définies, on peut définir de manière explicite ce qu'est une "démonstration formelle", et on peut numéroter les "démonstrations formelles" (de la même manière à peu près qu'on a numéroté $\mathcal{L}$). Enfin, un "théorème formel" est un énoncé pour lequel il existe une démonstration formelle. La fonction f est donc la fonction qui, à un entier naturel n , fait correspondre le numéro (pour la numérotation de $\mathcal{L}$) du dernier énoncé de la démonstration formelle qui a pour numéro n (pour la numérotation de la collection des démonstrations formelles de $(\mathcal{L}, \mathcal{A})$).

Si on regarde de près le travail d'arithmétisation de la théorie formelle de $(\mathcal{L}, \mathcal{A})$, on voit qu'apparaît constamment la notion de processus parfaitement bien défini (ou parfaitement explicite). En fait, tous ces processus parfaitement explicites sont "primitifs récursifs" (définition ci-après) et ils admettent une traduction formelle dans le langage $\mathcal{La}$, langage qui joue ainsi un rôle central dans les théories formelles⁽¹⁴⁾.

Voici la définition des processus primitifs récursifs, et le résultat disant que ces processus peuvent être traduits dans $\mathcal{La}$, énoncés précisément :

Définition des processus primitifs récursifs

On appelle fonction primitive récursive toute fonction de $\mathbb{N}^k$ vers $\mathbb{N}$ qui peut être obtenue, à partir des fonctions coordonnées, des fonctions constantes, de l'addition et de la multiplication, en appliquant un nombre fini de fois le procédé de composition des fonctions et le procédé de définition par récurrence simple⁽¹⁵⁾.

¹⁴ En fait, l'important est qu'on puisse "traduire" suffisamment de raisonnements élémentaires, comme ceux que nous avons esquissés, dans la théorie formelle *Peano*. En conséquence cette théorie n'occupe un rôle central que pour des raisons historiques. A posteriori, on se demande bien pourquoi avoir choisi un langage aussi pauvre pour décrire les entiers naturels. Il serait infiniment plus confortable de disposer dans le langage formel de beaucoup plus de symboles de fonctions que seulement l'addition et la multiplication. Cette pauvreté du langage $\mathcal{La}$ rend la preuve du théorème d'adéquation ci-après et celle du théorème d'incomplétude de Gödel (qui en découle) inutilement compliquées : une accumulation de lemmes techniques s'avère nécessaire pour vérifier qu'on est bien capable de "traduire" les fonctions primitives récursives dans *Peano*.

¹⁵ Les suites d'entiers usuelles des mathématiques sont primitives récursives, par exemple la n -ème décimale de π ou le n -ème nombre premier sont des suites primitives récursives.

Comme l'ensemble des mots écrits sur un alphabet fini peut être codé par des entiers naturels⁽¹⁶⁾ on peut également définir des processus primitifs récursifs qui, par exemple, prennent en entrée un entier naturel et donnent en sortie un mot sur un alphabet fini fixé. Alors, dans le théorème d'arithmétisation, tous les processus décrits sont primitifs récursifs. En outre les procédés primitifs récursifs peuvent être traduits dans *Peano* :

Théorème d'adéquation de *La* et *Peano* à la description des fonctions primitives récursives

Soit $n \mapsto f(n)$ une fonction primitive récursive de $\mathbb{N}$ dans $\mathbb{N}$.

Il existe un énoncé arithmétique $U_f(x, y)$ à deux variables libres x et y tel que l'on ait :

- pour tout entier naturel n , il existe un et un seul entier naturel m tel que :

$U_f(n, m)$ est interprété Vrai dans l'interprétation standard $\mathbb{N}$ de *La*, et la valeur m ainsi définie est égale à $f(n)$

- soit n un entier naturel et $m = f(n)$, n et m des écritures représentant n et m dans le langage *La*, alors l'énoncé

$$\boxed{U_f(n, m)}$$

est un théorème de *Peano*.

- l'énoncé

$$\boxed{\forall x \exists ! y \quad U_f(x, y)}$$

est un théorème de *Peano*.

Commentaires :

1. Ainsi, la théorie formelle de $\mathcal{ZF}$ (système d'axiomes mis au point pour décrire un univers mathématique complètement "énorme"), toute la théorie formelle de $\mathcal{ZF}$, se réduit à l'étude d'une seule fonction explicite de $\mathbb{N}$ dans $\mathbb{N}$, fonction qui peut être "écrite dans *La* et prouvée dans *Peano*",

2. Ceci est vrai pour toute théorie formelle : cela justifie qu'on ait depuis le début attaché une importance particulière à " $\mathbb{N}$ et *La*"⁽¹⁷⁾

D2 Le théorème d'incomplétude de Gödel

C'est ce théorème qui a ruiné les espoirs du projet formaliste de Hilbert.

Une fois arithmétisée la théorie formelle de $(\mathcal{L}, \mathcal{A})$, le problème de la *consistance* (ou "non contradiction") de cette théorie formelle, admet une nouvelle formulation :

La théorie formelle $(\mathcal{L}, \mathcal{A})$ est dite non contradictoire (ou consistante, ou encore cohérente) si la collection des théorèmes ne contient pas de contradiction.

En fait, vu les règles de la logique formelle, si une théorie formelle $\text{Tf}(\mathcal{L}, \mathcal{A})$ sur un langage $\mathcal{L}$ contient une contradiction, alors $\text{Tf}(\mathcal{L}, \mathcal{A})$ est la collection $\mathcal{L}$ toute entière ("tout" peut être démontré formellement à partir d'une contradiction).

¹⁶ Par exemple, si l'alphabet possède neuf lettres, qu'on nomme 0, 1, ..., 8 tout mot w peut être codé par le nombre qui, écrit en base 10, commence par 9 et se poursuit par le mot w

¹⁷ Comme disait Kronecker en langage imagé : «Dieu nous a donné les entiers naturels, tout le reste n'est que l'invention des hommes». Cantor, quant à lui, remerciait Dieu d'avoir créé l'univers mathématique des ensembles infinis actuels de tailles extraordinaires. Le fait qu'une réflexion sur les fondements des mathématiques, à travers le formalisme, ait abouti, beaucoup plus tard, à ce rôle central de l'arithmétique élémentaire peut être considéré comme un résultat en faveur de cette philosophie de Kronecker, et en défaveur de la philosophie «réaliste idéaliste» des infinis actuels à la Cantor.

Soit donc n_0 le numéro de l'énoncé « $\forall x \quad x \neq x$ ». On voit que $(L, \mathcal{A})$ est contradictoire si et seulement si l'énoncé F ayant pour numéro n_0 fait partie des théorèmes de la théorie formelle.

Si $f: \mathbb{N} \rightarrow \mathbb{N}$ est la fonction explicite de $\mathbb{N}$ dans $\mathbb{N}$ décrite dans le théorème d'arithmétisation, on a donc :

La théorie formelle $(L, \mathcal{A})$ est non contradictoire si et seulement si
pour tout entier naturel n , $f(n) \neq n_0$

Si $U_f(x, y)$ est l'énoncé d'arithmétique correspondant à la fonction primitive récursive f décrit dans le théorème d'adéquation, on a donc l'énoncé d'arithmétique,

$$\forall x \quad \neg U_f(x, n_0)$$

noté $\text{Consis } \mathcal{A}$ ⁽¹⁸⁾, avec l'équivalence :

“La théorie formelle $(L, \mathcal{A})$ est non contradictoire” si et seulement si
l'énoncé $\text{Consis } \mathcal{A}$ est Vrai dans l'interprétation standard $\mathbb{N}$ de $L\mathcal{A}$.

Ceci nous amène à la formulation du théorème d'incomplétude de Gödel.

Théorème d'incomplétude Gödel

1. $\text{Consis } \textit{Peano}$ n'est pas un théorème de *Peano*, à moins que *Peano* soit contradictoire.
2. $\text{Consis } Z\mathcal{F}$ peut être “traduit” dans le langage Le de la théorie des ensembles. Notons alors $\text{CONSIS } Z\mathcal{F}$ la traduction de $\text{Consis } Z\mathcal{F}$ dans Le . Alors $\text{CONSIS } Z\mathcal{F}$ n'est pas un théorème de $Z\mathcal{F}$, à moins que $Z\mathcal{F}$ soit contradictoire.
3. Soit, de manière plus générale, un système d'axiome $\mathcal{A}$ explicite sur un langage du premier ordre L . Supposons que ce système d'axiome soit assez fort pour permettre une traduction dans L de l'arithmétique de *Peano*. Supposons enfin que $(L, \mathcal{A})$ soit non contradictoire. Soit enfin $\text{CONSIS } (L, \mathcal{A})$ la traduction de $\text{Consis } (L, \mathcal{A})$ dans la langage L . Alors $\text{CONSIS } (L, \mathcal{A})$ n'est pas un théorème formel de $(L, \mathcal{A})$.

Ce théorème reste imprécis pour la lectrice dans la mesure où je n'ai pas expliqué la notion de traduction (un exemple est donné en annexe).

Voici cependant quelques commentaires en un langage que j'espère compréhensible.

Commentaires :

1. Il est facile de comprendre pourquoi le théorème d'incomplétude de Gödel ruine le programme de Hilbert sous la forme où il était énoncé au départ, c.-à-d. un programme tendant à maîtriser par le biais de processus de nature extrêmement élémentaires l'utilisation de l'infini en mathématiques. Le système formel *Peano* est la traduction d'une partie relativement modeste de l'utilisation de procédés infinis par les mathématiciens (essentiellement *Peano* décrit les preuves par récurrence simple portant sur des propriétés arithmétiques). Pourtant, la preuve de la cohérence de cette théorie formelle relève de procédés nécessairement plus complexes que ceux formalisés dans *Peano*. On ne pourra jamais maîtriser un infini en se situant à un niveau plus élémentaire que cet infini.
2. La théorie des ensembles et les méthodes de démonstration qu'elle autorisait semblait, à son apparition, et semble encore aujourd'hui à beaucoup de mathématiciens le cadre dans lequel s'inscrivent toutes les mathématiques. Pourtant, si $Z\mathcal{F}$ est non contradictoire, il y a un énoncé d'arithmétique, $\text{Consis } Z\mathcal{F}$, qui, interprété dans le modèle standard $\mathbb{N}$, est Vrai, mais

¹⁸ n_0 est ici une abréviation pour: $(\dots((1+1)+\dots+1)+1)$ (n_0 fois)

indémontrable au moyen de ZF . Donc la théorie des ensembles, dès qu'on en a choisi une formulation axiomatique telle que ZF , est insuffisante à démontrer des énoncés arithmétiques *simples* : En effet, $\text{Consis } ZF$ exprime “seulement” qu'une certaine fonction $f_{ZF} : n \mapsto f_{ZF}(n)$ de $\mathbb{N}$ vers $\mathbb{N}$, bien définie, ne prend pas une valeur n_0 bien définie.

3. Appelons $\mathcal{P}_1$ le système d'axiomes de *Peano*.

Si nous nous plaçons d'un point de vue classique pour $\mathbb{N}$ et $\mathcal{L}_a$, ce système est manifestement non contradictoire (il admet en effet un modèle explicite : c'est le modèle standard $\mathbb{N}$ et toute contradiction dans la théorie formelle de *Peano* impliquerait une contradiction dans le modèle explicite, ce qui est impossible⁽¹⁹⁾).

Donc, $\text{Consis } \mathcal{P}_1$ est Vrai lorsqu'on l'interprète dans le modèle standard.

Mais, comme $\text{Consis } \mathcal{P}_1 \notin \text{Tf}(\mathcal{P}_1)$, on obtiendra une meilleure description de $(\mathbb{N}, +, \times, 0, 1, <)$ avec un système d'axiomes $\mathcal{P}_2$ formé en prenant les axiomes de $\mathcal{P}_1$ et l'axiome supplémentaire $\text{Consis } \mathcal{P}_1$.

Mais, de nouveau, $\text{Consis } \mathcal{P}_2$ est à la fois Vrai dans le modèle standard et indémontrable formellement à partir de $\mathcal{P}_2$ (c'est-à-dire $\text{Consis } \mathcal{P}_2 \notin \text{Tf}(\mathcal{P}_2)$). Donc on obtiendra une meilleure description de $(\mathbb{N}, +, \times, 0, 1, <)$ avec le système d'axiomes $\mathcal{P}_3$ formé en prenant les axiomes de $\mathcal{P}_2$ et l'axiome supplémentaire $\text{Consis } \mathcal{P}_2$.

Et ainsi de suite⁽²⁰⁾.

De manière plus générale : il n'existe aucun système d'axiomes $\mathcal{P}$, défini de manière explicite sur $\mathcal{L}_a$, pour lequel $\text{Tf}(\mathcal{P})$ soit la collection de tous les énoncés d'arithmétiques interprétés Vrai dans le modèle standard. Ou encore, (il ne faut pas avoir peur de se répéter), la vérité sémantique dans $\mathbb{N}$ (pour des propriétés qui sont les interprétations d'énoncés de $\mathcal{L}_a$) ne pourra jamais être enfermée dans un système d'axiomes bien défini a priori.

Dans la discussion précédente nous avons démontré la Vérité dans $\mathbb{N}$ d'énoncés tels que $\text{Consis } \mathcal{P}_1$, $\text{Consis } \mathcal{P}_2$ etc ... Mais, pour ce faire, nous avons dû faire des aller-retour entre théories formelles et modèle standard $\mathbb{N}$. C'est seulement dans ces aller-retour entre réalité mathématique et formalisation que peut se situer l'intérêt profond des théories formelles⁽²¹⁾.

D3 Propriétés arithmétiques qu'on ne démontrera jamais ?

Rappelons que nous avons appelé propriété arithmétique une propriété (concernant les entiers naturels) qui est l'interprétation standard d'un énoncé d'arithmétique (c'est-à-dire un énoncé de $\mathcal{L}_a$). Considérons alors la propriété arithmétique suivante :

“la théorie formelle ZF est consistante”

(c'est l'interprétation de l'énoncé sans variable libre $\text{Consis } ZF$), et supposons qu'elle soit vraie.

La démontrer reviendrait (d'après le théorème d'incomplétude de Gödel) à utiliser des méthodes de preuve plus fortes que celles formalisées dans ZF .

¹⁹ En fait il existe également des preuves de la cohérence de *Peano* qui sont convaincantes d'un point de vue intuitionniste. cf. E2

²⁰ Cela pourrait aller assez loin. La lectrice connaissant les ordinaux pourra par exemple s'entraîner à décrire explicitement un système d'axiome $\mathcal{P}_\alpha$ pour chaque ordinal dénombrable α qu'elle est capable de décrire de manière suffisamment explicite.

²¹ Par exemple, l'analyse non standard utilise, pour étudier les propriétés de fonctions standard de $\mathbb{R}$ dans $\mathbb{R}$, le comportement de ces fonctions standard par rapport à des réels non standard, “infinitésimaux”, c'est-à-dire infiniment petits par rapport aux nombres réels standard.

Il semble donc bien que : “la théorie formelle $Z\mathcal{F}$ est consistante” est le type même de propriété arithmétique qui, si elle est vraie, est indémontrable à tout jamais par Homo Sapiens (mais là, je crois que je m'avance quand même un peu).

Ainsi serait levée une objection possible des “classiques pour $\mathbb{N}$ et $\mathcal{L}\mathcal{A}$ ” aux “intuitionnistes pour $\mathbb{N}$ et $\mathcal{L}\mathcal{A}$ ” qui dit que tout énoncé d'arithmétique aujourd'hui indécis sera forcément un jour démontré Vrai ou Faux (dans $\mathbb{N}$) et donc qu'on peut lui appliquer la loi du tiers exclu.

D4 Non définissabilité de la vérité (d'un langage par ce langage)

Plaçons-nous d'un point de vue classique.

Considérons un langage du premier ordre $\mathcal{L}$ et une interprétation M de ce langage. Il s'agit, rappelons-le, d'une collection d'objets M , et pour chaque symbole de fonction, de constante ou de relation de $\mathcal{L}$, d'avoir une fonction, un objet, une relation qui lui est associée dans l'interprétation.

Puisqu'on se place d'un point de vue classique, tout énoncé de $\mathcal{L}$, une fois interprété dans M , est forcément vrai ou faux.

Notons alors $Ts(\mathcal{L}, M)$ la collection des énoncés de $\mathcal{L}$ qui sont Vrais lorsqu'on les interprète dans M (je note Ts comme “théorème sémantique” de la même manière que plus haut j'ai noté Tf comme “théorème formel”).

Le théorème de “non définissabilité de la vérité” de Tarski affirme que la collection $Ts(\mathcal{L}, M)$ ne peut pas être définie avec “les seuls moyens du bord” que sont M et $\mathcal{L}$.

Cela reste un peu imprécis, je vais donc donner le théorème dans les cas de $(\mathcal{L}\mathcal{A}, \mathcal{P}_1, (\mathbb{N}, +, \times, 0, 1, <))$ et dans le cas de $(Z\mathcal{F}, (U, \in))$ où $(U, \in)$ est un modèle de $Z\mathcal{F}$.

Remarquons cependant tout de suite que ce théorème achève de ruiner tout espoir de formalisation de la vérité. Alors que le théorème de Gödel est un théorème de “non démontrabilité de la vérité par des moyens purement formels”, celui de Tarski va d'une certaine manière plus loin : la vérité sémantique échappe non seulement à la *démonstration* par des moyens purement formels, mais elle échappe également à la *description* (ou définition) par des moyens purement formels⁽²²⁾.

Théorème de non définissabilité en arithmétique

Soit $E_0, E_1, E_2, \dots, E_n, \dots$ une numérotation explicite d'énoncés d'arithmétique sans variable libre. Considérons la collection des entiers n tels que E_n s'interprète Vrai dans le modèle standard $(\mathbb{N}, +, \times, 0, 1, <)$ de *Peano*. Alors cette collection n'est pas une partie arithmétique de $\mathbb{N}$.

Théorème de non définissabilité de la vérité dans $Z\mathcal{F}$:

Étant donné un modèle U de $Z\mathcal{F}$, il n'existe aucun énoncé $R(x)$ du langage $\mathcal{L}\mathcal{E}$, à une seule variable libre x , vérifiant la propriété suivante : pour chaque énoncé E sans variable libre

$$E \Leftrightarrow R(|E|) \text{ est Vrai dans } U.$$

Ici $|E|$ est le numéro de E (pour une numérotation effective de $\mathcal{L}\mathcal{E}$) traduit dans U :

²² Le théorème d'incomplétude est cependant “plus fort”, plus subtil, et plus difficile à démontrer, à cause de sa précision diabolique concernant la vérité indémontrable. Le théorème “sémantique” de Tarski serait plutôt l'analogue d'un théorème d'incomplétude plus faible, relativement facile à démontrer en utilisant le procédé diagonal de Cantor, qui affirme seulement qu'il existe des propositions vraies mais indémontrables dans *Peano*.

dans U on peut définir des objets qu'on note $0, 1, \dots, n, \dots$ et qui font fonction d'entiers naturels standard. Par exemple on peut prendre : $0 = \emptyset$ (c.-à-d. l'interprétation du symbole de constante $\emptyset$ dans U), puis de proche en proche $n+1 = n \cup \{n\}$ (où $\cup$ est l'interprétation de la réunion dans l'univers U).

E Remarques sur le programme de Hilbert

E1 Évolution du programme de Hilbert

Il est écrit sur la tombe de Hilbert : «Nous devons savoir. Nous saurons».

Au départ (disons, en 1900, au moment des célèbres 23 problèmes, où l'urgence de lever les paradoxes de l'infini actuel se faisait pressante), il semble que Hilbert pensait que l'on disposerait un jour prochain d'une méthode systématique et purement mécanique d'investigation de la vérité mathématique.

Rappelons que le premier des problèmes de Hilbert demandait qu'on prouve la possibilité d'un bon ordre sur $\mathbb{R}$ et l'hypothèse du continu. «Nous aurions bien voulu savoir, et il est probable que nous ne saurons jamais» dirions nous sur ces sujets aujourd'hui.

Autre exemple, le 10^{ème} problème de Hilbert est la requête d'une méthode mécanique capable de décider si un polynôme multivariable à coefficients entiers s'annule en au moins un point à coordonnées entières. La preuve qu'une telle méthode mécanique ne peut exister est relativement récente (Matiasevitch 1970).

Si on élargit la classe des problèmes à résoudre sous la forme suivante :

«décider si une fonction primitive récursive de $\mathbb{N}$ vers $\mathbb{N}$
prend au moins une fois la valeur 0 »,

alors la preuve d'impossibilité d'une procédure mécanique est très simple (c'est essentiellement le procédé diagonal de Cantor, génial mais très simple), et il semble aujourd'hui bizarre que Hilbert ait pu jamais espérer une réponse positive.

Mais, en 1900, quand Hilbert pose son 2^{ème} problème, qui demande qu'on prouve par des moyens très élémentaires la cohérence de l'arithmétique, les systèmes formels ne sont pas encore complètement au point, et les fonctions explicites mécaniques (récursives) ne seront définies que 30 ans plus tard.

À l'époque on croyait par exemple que la construction des réels comme (classes d'équivalence de) suites de Cauchy de rationnels impliquerait que la cohérence de "l'analyse" (la théorie des nombres et fonctions réelles) se déduirait facilement de la cohérence de l'arithmétique.

On croyait également que le système des axiomes informels de Peano (dans lequel l'axiome de récurrence est énoncé informellement pour "toute" partie de $\mathbb{N}$), dans la mesure où il "caractérisait" $\mathbb{N}$ de manière univoque, fournirait la base formelle d'une description complète de $\mathbb{N}$.

En conséquence, une preuve élémentaire de la cohérence de l'arithmétique ajoutée à une formalisation adéquate de l'axiomatique informelle de Peano pouvait sembler la baguette magique absolue, qui permettrait à la fois de résoudre les paradoxes et de mécaniser entièrement les preuves.

La mise en oeuvre du programme de Hilbert nécessitait la description la plus objective possible de l'activité mathématique. Mais l'activité mathématique, décrite objectivement, ressemble diablement à un bouquin de mathématiques, et elle a alors un caractère fini et discret, c.-à-d. est par nature opposée à l'intuition que nous avons du continu. Ainsi le système formel ZF ne décrit aucunement les univers ensemblistes hypothétiques à la Cantor, mais seulement une

activité mécanisable des mathématicien(ne)s au sujet de ces univers. La théorie formelle ZF est structurellement analogue à $\mathbb{N}$ et non à $\mathbb{R}$, et encore moins à l'univers cantorien. Cette contradiction entre l'objet supposé de l'étude mathématique et les moyens bien limités dont dispose tout procédé de démonstration automatique s'est résolue dans un flop retentissant du programme de Hilbert initial⁽²³⁾. Cela peut sembler après coup comme une évidence bien simple. Soit que l'on croie à l'univers cantorien, mais alors il faut se résigner à une très probable profonde ignorance. Soit que l'on n'y croie pas, et l'échec était prévisible comme l'éclatement de la grenouille qui veut se faire plus grosse qu'un boeuf (en l'occurrence un boeuf tellement énorme qu'il n'existe même pas). Ce qui n'était sans doute pas prévisible, c'est l'endroit où ça a fait flop, qui est relativement bas dans le degré d'abstraction.

Néanmoins, comme l'activité mathématique va bien au delà de l'étude d'un système formel particulier (contrairement à ce que laisse entendre le formalisme), et comme une certaine dose d'infini à l'état au moins potentiel est nécessaire à la réflexion mathématique, le programme de Hilbert, en tant que réflexion au sujet des mathématiques pratiquées, par des moyens de nature mathématique, reste une tâche permanente. À défaut de pouvoir maîtriser l'infini par en dessous, on doit essayer d'analyser les formalisations de l'infini (lesquelles ne sont structurellement pas des infinis bien compliqués) depuis pas trop haut. De manière plus générale, il semble indispensable d'analyser l'activité mathématique la plus abstraite en termes d'une signification concrète de cette activité qui ne soit pas seulement formaliste (car alors il ne s'agirait pas de l'analyse d'une activité abstraite, mais seulement de l'étude d'un jeu très concret, très compliqué et sans signification profonde). C'est ce qu'on pourrait appeler un programme de Hilbert revu à la baisse.

L'activité de recherche en mathématiques est consacrée en grande partie à la simplification des preuves. Il n'y a sûrement pas consensus sur ce qu'est une preuve simple. Mais une des manières de "simplifier" une preuve est souvent de la rendre plus concrète et plus explicite. Chaque fois que la simplification est faite de cette manière, on peut considérer qu'un petit morceau de ce programme de Hilbert (révisé à la baisse) est réalisé. Quand Bishop publie en 1967 un livre où il interprète en termes constructifs les bases de l'analyse moderne, il réalise un morceau substantiel de ce programme de Hilbert. Quant une conjecture mathématique qui affirme que toutes les courbes algébriques planes d'une très vaste famille n'ont qu'un nombre fini de points rationnels est démontrée par une belle méthode très abstraite, immédiatement une activité intense de simplification et d'explicitation de la preuve se met en route. Et les mathématicien(ne)s ne seront pas satisfait(e)s tant qu'ils (elles) n'auront pas réussi à rendre beaucoup plus précise l'affirmation concernant le "nombre fini de points". C.-à-d. tant qu'ils n'auront pas soumis le beau théorème au programme de Hilbert.

E2 Le programme de Hilbert pour l'arithmétique de Peano

À défaut de pouvoir prouver la cohérence de *Peano* par des moyens élémentaires, on peut essayer d'analyser la complexité des preuves contenues dans ce système formel. La première chose à faire semble être de répondre aux objections des intuitionnistes concernant l'usage abusif du tiers exclu en matière d'infini. Une logique formelle répondant à la compréhension constructive de l'activité mathématique a été mise au point par Heyting. La théorie formelle basée sur les axiomes de Peano mais avec la logique formelle intuitionniste a été baptisée *Heyting*.

²³ Il est par ailleurs fort heureux que le théorème d'incomplétude de Gödel interdise à n'importe quelle activité purement mécanique de simuler convenablement les capacités inventives d'Homo Sapiens.

Gödel a montré que le système formel *Peano* n'est pas plus incohérent que le système formel *Heyting*. C'est une preuve très élémentaire, qui consiste essentiellement à interpréter une affirmation classique comme une affirmation constructive dont la signification est nettement plus faible. Parmi tous les énoncés classiquement équivalents à un énoncé d'arithmétique donné, on choisit celui dont la signification constructive est la plus faible. La preuve classique de l'énoncé dans le système *Peano* se transforme alors automatiquement en une preuve de l'énoncé affaibli dans *Heyting*. Si une contradiction (qui est un énoncé faible) est prouvée par *Peano* elle est alors automatiquement prouvée par *Heyting*.

Cette analyse de la cohérence de *Peano* a été améliorée de plusieurs façons, dont plusieurs essentielles. Par exemple :

- Gentzen a donné une analyse de la cohérence de *Peano* en termes d'ordinaux : il revient au même de pratiquer des raisonnements par récurrence simple sur des énoncés d'arithmétiques arbitraires (qui sont des énoncés relativement compliqués), ou de pratiquer des raisonnements par récurrence le long d'un ordinal assez grand, mais pas trop, sur des énoncés d'arithmétiques tout à fait élémentaires.
- Gödel a donné une analyse de la cohérence de *Heyting* en montrant que celle-ci équivaut à accepter des définitions par récurrence simple portant sur des objets de structure assez compliquée, mais pas trop, les fonctionnelles récursives.
- Dragalin et Friedman ont montré que les fonctions mécaniquement calculables prouvées exister dans *Peano* peuvent également être prouvées exister dans *Heyting*.

E3 Vérité des résultats d'arithmétique établis au moyen des axiomes de $\mathcal{ZF}$?

Si les mathématiciens utilisent la théorie des ensembles et la “logique formelle classique” (pour des propriétés interprétant des énoncés écrits en un langage du premier ordre), c'est pour des raisons de simplicité et de facilité des démonstrations dans ce cadre.

Dans ce cadre, ils sont amenés à utiliser des objets mathématiques assez incroyables. Par exemple, on définit au moyen d'énoncés explicites des ensembles dont on ne sait définir explicitement aucun élément isolé et dont on démontre qu'ils sont infinis. Un peu comme si on savait définir l'ensemble des nombres réels mais qu'on ne sache définir aucun de ces nombres isolément.

Il n'y a pas besoin d'être intuitionniste pur et dur pour mettre en doute “le sens réel” de résultats concernant de tels objets. Mais, les mathématiciens “classiques” ne sont pas masochistes : s'ils utilisent des objets “complètement farfelus” et “pas du tout crédibles” c'est comme intermédiaires dans des démonstrations concernant des objets tout à fait ordinaires et crédibles, tels que les entiers naturels. On voit immédiatement que se pose le problème de la validité de résultats concernant les entiers naturels, mais obtenus au prix de détours dans l'univers mathématique de Zermelo-Frankel.

Le programme de Hilbert pour $\mathcal{ZF}$ aurait réclamé dans sa version initiale une preuve, par des moyens élémentaires, que tout théorème d'arithmétique de structure suffisamment simple⁽²⁴⁾ prouvé au moyen de $\mathcal{ZF}$ soit Vrai dans la réalité de $\mathbb{N}$. Comme la cohérence de $\mathcal{ZF}$ (c.-à-d. l'impossibilité de prouver l'affirmation $0 = 1$, manifestement fausse dans la réalité) est hors de portée des méthodes élémentaires, ce programme ne peut être réalisé. Néanmoins,

²⁴ Plus précisément, tout théorème d'arithmétique de la forme « $\forall n \ f(n) = 0$ » où f est une fonction primitive récursive. Ce genre de théorème d'arithmétique a une structure très simple et sa signification n'est pas sujette à trop de contestation.

on doit se poser la question de savoir quel type de garantie on peut espérer concernant les résultats d'arithmétique prouvés au moyen de $\mathcal{ZF}$. (par exemple, est-on absolument certain que le beau théorème auquel il est fait allusion à la fin du paragraphe E1 corresponde à une vérité dans le monde réel des entiers naturels, dès que sa preuve est formellement correcte dans $\mathcal{ZF}$?).

Le point de vue formaliste a "l'avantage" d'ignorer ce problème puisque le mathématicien formaliste joue au jeu "langage de la théorie des ensembles, axiomes de $\mathcal{ZF}$ et règles de la logique formelle" et ne prétend jamais que les énoncés qu'il appelle "théorèmes" s'interprètent en une réalité Vraie. Même s'il démontre au moyen de $\mathcal{ZF}$ l'énoncé de $\mathcal{Le}$ qui s'interprète par "tout nombre pair ≥ 4 est somme de deux nombres premiers", le mathématicien formaliste ne prétend pas avoir démontré que tout nombre pair ≥ 4 soit somme de deux nombres premiers. Si, par la suite, quelqu'un trouve un nombre pair qui ne soit pas somme de deux nombres premiers, le mathématicien formaliste dira : les axiomes de $\mathcal{ZF}$ sont donc contradictoires et mon jeu est sans intérêt, je vais essayer de jouer à autre chose.

Pour le mathématicien qui admet le point de vue classique (pour $\mathbb{N}$ et $\mathcal{La}$) mais qui admet difficilement l'existence d'un univers mathématique aussi "monstrueux" que celui de $\mathcal{ZF}$, quelle est la validité des "résultats d'arithmétique" obtenus au moyen de $\mathcal{ZF}$ au moins si nous supposons que la théorie formelle de $\mathcal{ZF}$ est non contradictoire ?

J'avoue que j'ai bien du mal à répondre à cette question, pourtant pertinente. Mais il me semble que la réponse est à l'heure actuelle incertaine.

Cette réponse semble dépendre de la structure de l'énoncé d'arithmétique démontré dans $\mathcal{ZF}$. Considérons tout d'abord un énoncé d'arithmétique simple du type : « $\forall n \quad f(n)=0$ » où f est une fonction primitive récursive. Si la preuve a été donnée dans $\mathcal{ZF}$ et que l'énoncé soit faux dans la réalité, il existe un entier m tel que $f(m) \neq 0$ et le calcul de $f(m)$ peut être prouvé dans $\mathcal{ZF}$, ce qui permettrait d'établir une contradiction dans $\mathcal{ZF}$, contrairement à l'hypothèse.

Considérons ensuite un énoncé d'arithmétique du type : « $\exists n \quad f(n)=0$ » où f est une fonction primitive récursive. Une preuve dans $\mathcal{ZF}$ d'un tel énoncé ne permet pas a priori d'exhiber un entier usuel n tel que $f(n)=0$. Et le fait que l'énoncé soit faux avec les entiers usuels (standards) ne permet pas non plus a priori d'induire une contradiction dans $\mathcal{ZF}$. Bien au contraire, le fait que tout modèle suffisamment simple de $\mathcal{ZF}$ contienne inévitablement des entiers non standards (résultat de Rabin) peut nous inciter à penser que les entiers n que $\mathcal{ZF}$ affirme annuler f pourraient après tout être tous non standards.

Si maintenant nous analysons la structure du beau théorème cité en fin de E1 nous voyons que l'énoncé est a priori du type, pas vraiment simple, suivant :

$$\ll \forall p \exists n \forall m > n \quad g(p, m) = 0 \gg \quad (25)$$

où g est une fonction primitive récursive. Ici, nous sommes dans un cas bien pire que le précédent. Et la vérité de l'énoncé dans $\mathbb{N}$ semble encore nettement plus difficile à établir à partir de la seule preuve dans $\mathcal{ZF}$ (et de l'hypothèse Consis $\mathcal{ZF}$).⁽²⁶⁾

²⁵ Pour toute courbe C_p de la famille considérée (qui peut être énumérée en une suite) il existe un entier qui majore le numéro de tout point rationnel P_m de la courbe (pour une numérotation des points rationnels du plan). Le calcul de $g(p, m)$ donne 1 si le point P_m est sur la courbe C_p et 0 sinon.

²⁶ Plaçons nous un moment du point de vue constructif. Même si le théorème est établi dans *Peano* nous pouvons avoir des doutes sur sa vérité. L'explicitation complète du théorème, à laquelle travaillent pas mal de gens, demande en effet qu'on calcule n en fonction de p . Mais pour p fixé, on n'a pas a priori de test concernant n qui puisse certifier que $\forall m > n \quad g(p, m) = 0$. En conséquence on n'est même pas a priori garanti que la dépendance de n par rapport à p puisse être explicitée par une fonction mécaniquement

Pour me résumer, il me semble qu'il faut admettre *plus* que la logique formelle classique lorsqu'elle est appliquée $\mathcal{L}_a$ et $\mathbb{N}$, pour être convaincu qu'un énoncé d'arithmétique démontré formellement dans $\mathcal{ZF}$ soit Vrai dans $(\mathbb{N}, +, \times, 0, 1, <)$ (en supposant évidemment $\mathcal{ZF}$ non contradictoire). Ou encore : les mathématiques couramment pratiquées n'ont de "sens" que si elles permettent de démontrer uniquement des énoncés d'arithmétique Vrais dans le modèle standard $(\mathbb{N}, +, \times, 0, 1, <)$. Or, pour être assuré de cela *il ne suffit pas* de supposer que $\mathcal{ZF}$ est non contradictoire, il faut *en plus* supposer que $\mathcal{ZF}$ est non contradictoire avec tout énoncé d'arithmétique Vrai dans le modèle standard (et traduit dans $\mathcal{L}_e$).

Ordinairement, en fait, les mathématicien(ne)s admettent que $\mathcal{ZF}$ possède un modèle dans lequel "l'ensemble des entiers" est standard pour l'arithmétique, mais "l'acte de foi" de la croyance en un tel modèle est a priori plus fort que l'acte de foi en la consistance de $\mathcal{ZF}$. Il semble à vrai dire presque aussi fort que celui de la croyance en l'univers cantorien abstrait dont une pâle description est donnée par $\mathcal{ZF}$.

F Quelques conclusions

1 – La formalisation de la logique pour les énoncés écrivables en un langage du premier ordre a un intérêt théorique remarquable en ce qu'elle permet une clarification du débat quant aux méthodes de raisonnements acceptables.

Ces méthodes de raisonnements "acceptables" ne le sont justement pas toutes par tous les mathématiciens. Le débat reste donc ouvert et, semble-t-il, restera ouvert longtemps encore.

2 – L'étude d'objets mathématiques tels que "les entiers naturels", "les groupes finis", "les nombres réels", "les ensembles" etc ... est susceptible d'une formalisation dans des langages du premier ordre, mais au prix de "pertes sèches" importantes.

- Au lieu de s'intéresser alors à toutes les propriétés imaginables de ces objets (à supposer qu'on soit convaincu de leur existence), on ne s'intéresse alors qu'aux propriétés qui peuvent être écrites dans un langage du premier ordre donné et, parmi ces propriétés, seulement à celles qui sont démontrables à partir d'un système d'axiomes préalablement choisis.
- Mais alors, de plus :
 - si l'objet est "peu puissant" (un groupe fini particulier par exemple), sa théorie formelle n'apporte rien de plus que sa théorie naïve,
 - si l'objet est "assez puissant" (par exemple il contient une partie identifiable à $\mathbb{N}$) aucune formalisation n'épuisera jamais la notion intuitive de vérité dans cet objet (quel que soit le point de vue qu'on adopte quant à la notion intuitive de vérité d'ailleurs),
 - si l'objet est "trop puissant" (par exemple un univers mathématique de Zermelo Frankel : objet de l'existence duquel on peut douter fortement et dont on ne connaît pas de "copie modèle réduit" convaincante), alors le recours à une théorie formelle du premier ordre semble d'un bien faible secours pour valider l'utilisation de cet objet (des obstacles considérables semblent se présenter à la réalisation d'un programme de Hilbert, même fortement révisé à la baisse, pour de tels types d'objets)

3 – L'étude d'un objet mathématique, une fois réduite à l'étude d'une théorie formelle de cet objet (après choix d'un système d'axiomes écrits dans un langage du premier ordre), est ramenée à l'étude de l'ensemble des valeurs $f(n)$ d'une fonction f de $\mathbb{N}$ dans $\mathbb{N}$ parfaite-

calculable. Or une preuve constructive de cette dépendance fournirait à coup sûr un algorithme de calcul mécanisable.

ment explicite. Aucun mathématicien ne peut croire que les mathématiques pourraient se réduire à l'étude *d'une seule* fonction explicite de $\mathbb{N}$ dans $\mathbb{N}$, si complexe soit elle.

Annexe 1 Les axiomes de $\mathcal{GB}$

Par convention, les lettres latines minuscules désigneront les “ensembles” du modèle, tandis que les lettres majuscules désigneront indistinctement “ensembles” ou “classes”.

Autrement dit encore un énoncé $\forall x R(x)$ est une abréviation pour :

$$\forall X ((\exists Y X \in Y) \Rightarrow R(X))$$

et un énoncé $\exists x R(x)$ est une abréviation pour :

$$\exists X ((\exists Y X \in Y) \wedge R(X))$$

Les axiomes de $\mathcal{GB}$ sont alors les suivants :

1) Extensionnalité : deux classes qui ont les mêmes éléments sont égales

$$\forall X \forall Y (\forall z (z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y)$$

2) Ensemble vide : $\forall x x \notin \emptyset$, $\exists Y \emptyset \in Y$

3) Ensemble à un ou deux éléments : $\forall x \forall y \exists z \forall t (t \in z \Leftrightarrow (t=x \vee t=y))$.

4) Ensemble réunion des éléments de y :

$$\forall y \exists z \forall u (u \in z \Leftrightarrow (\exists t (u \in t \wedge t \in y)))$$

5) Ensemble infini : $\exists x (\emptyset \in x \wedge \forall y (y \in x \Rightarrow y \cup \{y\} \in x))$.

Dans cet énoncé, $y \cup \{y\}$ désigne l'unique ensemble qui a pour éléments y et les éléments de y ; l'existence de cet ensemble unique est assurée par les axiomes 3 et 4.

6) Ensemble des parties d'un ensemble : $\forall x \exists y \forall u (u \in y \Leftrightarrow u \subset x)$

où $u \subset x$ est une abréviation pour : $\forall t (t \in u \Rightarrow t \in x)$.

7) Axiome de substitution : on définit le couple $\langle x, y \rangle$ comme étant égal à $\{\{x, y\}, \{x\}\}$.

On a alors $\langle x, y \rangle = \langle z, t \rangle$ si et seulement si $x = z$ et $y = t$.

L'axiome de substitution s'écrit alors :

$$\forall X \forall u [(\forall x \exists! y \langle x, y \rangle \in X) \Rightarrow \exists v \forall y (y \in v \Leftrightarrow \exists x (x \in u \wedge \langle x, y \rangle \in X))]$$

En gros : l'ensemble v est l'image de l'ensemble u par la classe X qui joue le rôle d'une fonction.

Comme conséquence de l'axiome 7 on a notamment : toute classe contenue dans un ensemble est un ensemble.

L'écriture $\exists! y$ est une abréviation, et elle signifie “il existe un et un seul y ”.

8) Axiome du choix fort :

$$\exists C \forall x (x \neq \emptyset \Rightarrow \exists! y (y \in x \wedge \langle x, y \rangle \in C))$$

(La classe C “choisit” dans chaque ensemble x un élément y).

9) $\exists A \forall a (a \in A \Leftrightarrow \exists x \exists y (a = \langle x, y \rangle \wedge x \in y))$

(Il existe une classe A dont les éléments sont les couples d'ensembles tels que $x \in y$).

10) Réunion de deux classes : $\forall Y \forall Z \exists X \forall a (a \in X \Leftrightarrow (a \in Y \vee a \in Z))$.

11) Complémentaire d'une classe : $\forall Y \exists Z \forall a (a \notin Y \Leftrightarrow a \in Z)$.

12) Domaine d'une relation entre ensembles :

$$\forall R \exists D \forall a (a \in D \Leftrightarrow \exists x \langle a, x \rangle \in R)$$

13) Classe des couples $\langle x, y \rangle$ où $x \in X$:

$$\forall X \exists Y \forall a (a \in Y \Leftrightarrow \exists x \exists y (x \in X \wedge a = \langle x, y \rangle))$$

14) Permutations entre éléments d'un triplet ou d'un couple :

$$\begin{aligned} \forall x \exists y \forall x \forall y & \quad (\langle x, y \rangle \in Y \Leftrightarrow \langle y, x \rangle \in X) \\ \forall x \exists z \forall x \forall y \forall z & \quad (\langle x, y, z \rangle \in Z \Leftrightarrow \langle y, z, x \rangle \in X) \\ \forall x \exists t \forall x \forall y \forall z & \quad (\langle x, y, z \rangle \in T \Leftrightarrow \langle x, z, y \rangle \in X) \end{aligned}$$

15) Fondation (facultatif)

$$\forall x (x \neq \emptyset \Rightarrow \exists u (u \in x \wedge \forall y (y \in x \Rightarrow y \in u)))$$

(Toute classe contient un ensemble "minimal" pour la relation $\in$).

$$\forall a \exists c \forall x [(x \neq \emptyset \wedge x \in a) \Rightarrow \exists ! y (y \in x \wedge \langle x, y \rangle \in c)]$$

Pour la théorie ZF on utilise un seul type de variable. Les axiomes sont les axiomes 1, 2, 3, 4, 5, 6, 15. Les axiomes 9 à 14 sont supprimés.

L'axiome 7 est remplacé par :

7*) Schéma de substitution: on réécrit l'axiome 7) en remplaçant

$$\langle x, y \rangle \in X \quad \text{par} \quad R(x, y)$$

où R désigne un énoncé écrit dans $\mathcal{L}$.

Il y a donc un axiome pour chaque énoncé $R(x, y)$. On dit que 7*) est un schéma d'axiomes.

L'axiome 8 est remplacé par :

8*) Axiome du choix :

$$\forall a \exists c \forall x [(x \neq \emptyset \wedge x \in a) \Rightarrow \exists ! y (y \in x \wedge \langle x, y \rangle \in c)]$$

(Pour tout ensemble a il y a un ensemble c qui permet le choix simultané d'un objet $y(x)$ dans chaque élément x non vide de l'ensemble a)

Pour tout modèle M de $\mathcal{GB}$, les "ensembles" du modèle M forment un modèle pour ZF .

À partir de tout modèle M de ZF , on peut construire ("mécaniquement") un modèle de $\mathcal{GB}$.

Annexe 2 Traduction de l'arithmétique de Peano dans le langage $\mathcal{L}_e$ de la théorie des ensembles

Considérons un "Univers de Zermelo Frankel" c'est-à-dire un modèle U du système d'axiomes $\mathcal{ZF}$ (du langage $\mathcal{L}_e$).

Pour tout entier naturel n , on définit un objet bien déterminé de l'univers U , objet qu'on notera par exemple $\underline{n}$.

Cet objet est défini par récurrence (c.-à-d. de proche en proche), en posant :

$$\underline{0} = \emptyset, \text{ et } \underline{n+1} = \underline{n} \cup \{\underline{n}\}$$

On peut aussi donner pour chaque n un énoncé $F_n(x)$ de $\mathcal{L}_e$ tel que $\mathcal{ZF}$ prouve l'existence et l'unicité d'un x vérifiant $F_n(x)$ et tel que dans le modèle U l'interprétation de $F_n(x)$ soit vraie si on interprète x par $\underline{n}$.

Modulo cette traduction, on démontre un schéma de théorèmes de $\mathcal{ZF}$ qui affirment que pour des entiers n et m distincts, $\underline{n}$ et $\underline{m}$ sont des objets distincts de l'univers U (il y a un théorème distinct pour chaque couple d'entiers naturels distincts).

Qu'est-ce qui joue alors "le rôle de $\mathbb{N}$ " dans l'univers U ?

Les axiomes de $\mathcal{ZF}$ permettent de montrer qu'il existe un unique élément ω de la collection U , qui vérifie :

$$\begin{aligned} & \emptyset \in \omega \wedge (\forall x \in \omega \quad x \cup \{x\} \in \omega) \\ & \wedge \forall X \quad [(\emptyset \in X \wedge (\forall x \in X \quad x \cup \{x\} \in X)) \Rightarrow \omega \subset X] \end{aligned}$$

c'est-à-dire : ω est le plus petit ensemble qui contienne $\emptyset$ et qui soit stable pour l'opération qui à un élément x de ω associe l'élément $x \cup \{x\}$.

On constate que pour tout entier naturel n , l'objet $\underline{n}$ de U vérifie : $\underline{n} \in \omega$.

Par contre, il n'y a aucun énoncé *écrivable dans $\mathcal{L}_e$* qui puisse traduire l'idée "pourtant simple" que ω ne doit pas avoir d'autres éléments que les objets $\underline{n}$ (et d'ailleurs, si $\mathcal{ZF}$ est non contradictoire, il y a des modèles de $\mathcal{ZF}$ pour lesquels ω contient des entiers non standard). On démontre ensuite, en tant que théorèmes formels de $\mathcal{ZF}$ l'existence de "lois de composition" $\pm$ et $\times$ définies sur ω et vérifiant les axiomes de *Peano*.

Remarque :

Pour traduire *Peano* dans $\mathcal{ZF}$, on a été aidé par le fait que les axiomes de $\mathcal{ZF}$ permettent de définir un objet ω qui joue le rôle de "collection de tous les entiers".

En fait, on peut se débrouiller sans cet "infini actuel". C'est l'objet de l'explication plus générale qui suit.

Annexe 3 Traduction de l'arithmétique de Peano dans une autre théorie formelle

On considère une théorie formelle définie par un système d'axiomes $\mathcal{A}$ écrits dans un langage du premier ordre $\mathcal{L}$.

Une traduction de $(\mathcal{L}_a, \text{Peano})$ dans $(\mathcal{L}, \mathcal{A})$ est fournie par cinq énoncés de $\mathcal{L}$.

- Un énoncé $\mathbf{N}(x)$ à une seule variable libre x (qu'on lira : x est un entier).
- Un énoncé $\mathbf{I}(x, y)$ à deux variables libres x, y (qu'on lira : x et y sont entiers et $x < y$).
- Un énoncé $\mathbf{S}(x, y, z)$ à trois variables libres x, y, z (qu'on lira : z est l'entier somme des entiers x et y).
- Un énoncé $\mathbf{P}(x, y, z)$ correspondant au produit.
- Un énoncé $\mathbf{E}_0(x)$, un énoncé $\mathbf{E}_1(x)$, (qu'on lira $x = 0$ et $x = 1$).

Tout ceci doit "vérifier les axiomes de *Peano*" au sens suivant :

La théorie formelle $(\mathcal{L}, \mathcal{A})$ contient les théorèmes qui "traduisent" les axiomes de *Peano*, c'est-à-dire précisons :

- $\exists x \forall y ((\mathbf{N}(x) \wedge \mathbf{E}_0(x) \wedge (\mathbf{E}_0(y) \Rightarrow y=x)) :$
($\mathbf{E}_0$ définit un entier unique)
- $\exists x \forall y ((\mathbf{N}(x) \wedge \mathbf{E}_1(x) \wedge (\mathbf{E}_1(y) \Rightarrow y=x)) :$ (idem avec $\mathbf{E}_1$)
- $\forall x \forall y ((\mathbf{I}(x, y) \Rightarrow (\mathbf{N}(x) \wedge \mathbf{N}(y))) :$
(la relation $\mathbf{I}(x, y)$ concerne des entiers)
- $\forall x \forall y \forall z ((\mathbf{S}(x, y, z) \Rightarrow (\mathbf{N}(x) \wedge \mathbf{N}(y) \wedge \mathbf{N}(z))) :$ (idem avec $\mathbf{S}$)
- $\forall x \forall y \forall z ((\mathbf{P}(x, y, z) \Rightarrow (\mathbf{N}(x) \wedge \mathbf{N}(y) \wedge \mathbf{N}(z))) :$ (idem avec $\mathbf{P}$)
- $\forall x \forall y \exists z \forall t ((\mathbf{N}(x) \wedge \mathbf{N}(y)) \Rightarrow (\mathbf{S}(x, y, z) \wedge (\mathbf{S}(x, y, t) \Rightarrow t=z))$
(c'est-à-dire $\mathbf{S}(x, y, z)$ définit l'entier z en fonction des entiers y et x)
- $\forall x \forall y \exists z \forall t ((\mathbf{N}(x) \wedge \mathbf{N}(y)) \Rightarrow (\mathbf{P}(x, y, z) \wedge (\mathbf{P}(x, y, t) \Rightarrow t=z))$
(même chose avec $\mathbf{P}(x, y, z)$)
- la traduction des axiomes de *Peano* : donnons juste un exemple
l'axiome $z + x = z + y \Rightarrow x = y$ est traduit par
 $\forall x \forall y \forall z \forall t ((\mathbf{S}(z, x, t) \wedge (\mathbf{S}(z, y, t)) \Rightarrow x = y)$

Annexe 4 Un autre modèle remarquable de $\mathcal{GB}^-$

On considère l'ensemble V_ω construit comme en C2, puis, au lieu de prendre $\mathbb{W} = \mathcal{P}(V_\omega)$, on prend :

$\mathbb{W}' =$ ensemble des parties de V_ω définies par un énoncé de $\mathcal{L}_e$.

Une partie A de V_ω est dite "définie par un énoncé $R(x)$ de $\mathcal{L}_e$ " si $R(x)$ est un énoncé de $\mathcal{L}_e$ à une seule variable libre x et si on a, pour tout x de V_ω

$x \in A$ si et seulement si $R(x)$ est vrai dans V_ω

Ces parties de V_ω définies par un énoncé de $\mathcal{L}_e$ sont appelées les parties "arithmétiques" de V_ω parce que, pour une numérotation naturelle de V_ω , elles correspondent exactement aux parties arithmétiques de $\mathbb{N}$.

Enfin, on interprète le symbole $\boxed{\in}$ par la relation $\in$ dans $\mathbb{W}'$.

On obtient de nouveau un modèle de $\mathcal{GB}^-$, mais cette fois-ci dénombrable (puisque l'on peut numéroter les énoncés à une variable libre de $\mathcal{L}_e$). Les "ensembles" de ce modèle sont de nouveau les parties finies de V_ω et les "classes" de ce modèle sont maintenant les parties arithmétiques de V_ω .

Ce modèle $(\mathbb{W}', \in)$ de $\mathcal{GB}^-$ est déjà nettement plus crédible que le modèle $(\mathbb{W}, \in)$ défini en C2, ne serait-ce que parce qu'il est dénombrable. Remarquons que la croyance en l'existence de $(\mathbb{W}', \in)$ comme infini actuel revient sur le fond à adopter un point de vue classique pour $\mathbb{N}$ et $\mathcal{L}_a$. Admettre que chaque énoncé à une variable libre de $\mathcal{L}_e$ définit "actuellement" une partie de V_ω revient à admettre que chaque énoncé à une variable libre de $\mathcal{L}_a$ définit comme infini actuel une partie de $\mathbb{N}$. C'est-à-dire que cela revient à admettre une vérité absolue pour $\mathbb{N}$ et $\mathcal{L}_a$.

On pourra remarquer également que dans ce modèle $(\mathbb{W}', \in)$ les "entiers" sont tous standards (cette affirmation a un sens parce que l'"ensemble des entiers" est définissable par un énoncé de $\mathcal{L}_e$, comme expliqué dans l'annexe 2). Donc le résultat de Rabin montre qu'il n'existe pas de numérotation de $\mathbb{W}'$ qui fasse de l'appartenance une relation arithmétique. Mais ceci ne saurait nous surprendre vu le théorème de non-définissabilité de la vérité en arithmétique.

Enfin, pour conclure, il ne faudrait pas croire que "l'existence" de ce modèle quasi-naturel de $\mathcal{GB}^-$ implique "l'existence" de modèles tout aussi naturels de $\mathcal{ZF}$ car, si $\mathcal{GB}^-$ contient un axiome d'existence d'une classe infinie (par exemple : l'axiome 11 en prenant la classe complémentaire de la classe vide), $\mathcal{ZF}$ contient quant à lui la combinaison de l'axiome d'existence d'un ensemble infini, de l'axiome de l'ensemble des parties d'un ensemble et du schéma de substitution, combinaison aboutissant à des ensembles de "grosesseur" véritablement "inimaginable".

Mathématiques constructives, quelques principes de travail

Introduction

Dans les chapitres précédents (cf. par exemple «De la difficulté d'être omniscient» et «Mathématiques constructives : hier et demain»), nous avons critiqué le point de vue cantorien en mathématiques, qui assimile l'infini à une notion positive, et raisonne avec les objets infinis par pure extrapolation des raisonnements concernant les objets finis, sans analyse critique de la situation ainsi créée.

Le point de vue opposé selon lequel l'infini est une notion purement négative⁽¹⁾, et qui est basé sur un contenu constructif des mathématiques, peut très bien être défendu et développé, même s'il est pour le moment relativement minoritaire (plus au niveau philosophique qu'au niveau pratique, d'ailleurs).

Nous essayons dans ce chapitre d'expliquer sur quels principes de travail se fondent les mathématiques constructives. Il y a naturellement beaucoup d'opinions diverses et de nuances d'interprétation chez les mathématiciens constructifs. Néanmoins, nous nous en tenons à des explications couramment admises. En particulier, l'interprétation de la logique constructive (sa justification heuristique, qui conduit aux règles de la logique intuitionniste formalisée par Heyting) que nous donnons ici est (avec des nuances inévitables) l'interprétation BHK (Brouwer-Heyting-Kolmogorov).

L'abondance particulière des notes de bas de page dans ce chapitre tient à ce que nous avons voulu, pour une première lecture sur un sujet certainement déroutant pour le profane⁽²⁾, ne pas entrer systématiquement dans trop de détails, de nuances et de polémiques ... toutes choses renvoyées systématiquement en bas de page

Le but des mathématiques est l'étude des propriétés de certains objets abstraits appelés "objets mathématiques" (les nombres entiers, les nombres réels, les fonctions continues, les espaces géométriques etc.).

Pour les mathématiques constructives, tout objet doit pouvoir être clairement défini par une construction, et seules les propriétés ayant une signification objective claire sont considérées et étudiées.

¹ L'infini est alors simplement le non fini, ou ce qui revient au même, l'infini potentiel à la manière des mathématiques depuis Euclide jusqu'à Gauss, c.-à-d. avant la révolution cantorienne.

² Le profane des mathématiques constructives peut très bien être un initié des mathématiques classiques, qui en général n'aura pas perçu comme tels les rites d'initiation (par exemple : veuillez faire un raisonnement par récurrence propre plutôt que de dire « et ainsi de suite » sinon ce n'est pas rigoureux et vous passez pour un attardé du 17^{ème} siècle). La connotation religieuse, voire sectaire, des mots «profanes» et «initiés», outre sa fonction provocatrice qui peut être parfois salutaire, est en réalité surtout imposée par la pauvreté du langage usuel qui assimile toute controverse ou critique à un désordre. La vérité absolue a de plus en plus seule droit de cité, à l'image des (dés)informations télévisées de la grand-messe du 20 heures.

En général, une propriété concerne un ou plusieurs objets indéterminés, qu'on appelle des variables. En mathématiques constructives, on demande que chaque variable soit d'un type bien déterminé, clairement défini.

La discussion va donc porter sur les problèmes suivants :

- quelles sont les constructions d'objets mathématiques qui sont légitimes ?
- à quels types peuvent appartenir les “variables” ?
- quelles sont les propriétés qui ont une signification objective claire ?

1) Tous les objets doivent être construits

Ce principe, en général facile à vérifier dans la pratique, est très flou dans son énoncé général.

En fait il s'agit d'un commentaire et non d'une définition.

Le principe se mord d'ailleurs la queue, dans la mesure où une construction est elle-même un objet mathématique. En outre les objets compliqués sont construits à partir d'objets simples, qui ne peuvent recevoir une définition purement mathématique.

Pour donner vie au principe «Tous les objets doivent être construits» il faut préciser ce que sont les objets de départ et ce que sont les constructions autorisées, légitimes. Comme nous ne sommes pas prophètes, nous ne pouvons que préciser les “constructions” *aujourd'hui* légitimes. Le développement des mathématiques ayant depuis longtemps réservé des surprises, il est probable que certaines constructions, non encore inventées, auront un jour une signification très claire.

1a) Les entiers naturels

Les mathématiques commencent *après* l'invention des entiers naturels. Concernant les entiers naturels, on peut faire des commentaires pertinents, mais on ne peut pas les définir.

Toute description des entiers naturels utilise le langage, qui est quelque chose d'une grande complexité. Une théorie formelle des entiers naturels utilise quant à elle un langage formel. Mais dans un langage formel, il y a au moins autant de présupposés mathématiques que dans les entiers naturels. Aussi les mathématiciens ou mathématiciennes qui pensent en toute bonne foi définir les entiers naturels grâce à une construction formelle ne font que tourner en rond. Il semble en tout cas bien étrange que ceci ait échappé aux mathématiciens du groupe Bourbaki.

Préalable à l'invention des entiers naturels, il y a le langage, et dans le langage il y a la notion d'objets identifiables, jouissant d'une certaine permanence, et distinguables les uns des autres. Le procédé consistant à construire le successeur de l'entier n est intimement lié à cette notion d'objets repérables et distinguables.

Dans la pratique, un entier naturel est repérable par une écriture⁽³⁾. Néanmoins, on peut imaginer des entiers naturels si grands qu'aucune écriture ne puisse les repérer (en supposant que l'Univers est fini).

Les mathématiques constructives ne tiennent pas compte de cette limitation concrète. Elles sont basées sur des entiers “potentiellement réalisables” et non sur les seuls entiers “concrètement réalisables”.

³ L'école constructiviste russe héritière de Markov considère que tout objet mathématique *est* une écriture dans un alphabet donné.

On écrit " $n \in \mathbb{N}$ " comme abréviation pour " n est un entier naturel". Cela ne sous-entend pas, contrairement à l'acception "classique"⁽⁴⁾, que les entiers naturels existent déjà une fois pour toutes, rangés entièrement dans la collection $\mathbb{N}$.

Au vu de cette première discussion sur les entiers naturels, le principe «tous les objets doivent être construits» doit donc être reformulé plus précisément comme suit «tous les objets doivent être potentiellement constructibles».

En outre, on admet, ou plutôt on constate, que les entiers naturels sont les objets d'une construction légitime fondatrice des mathématiques.

Remarque: on généralise la notation $n \in \mathbb{N}$. Si on considère comme clairement défini un certain type d'objets, on pourra écrire « x est un objet de type A » sous forme abrégée « $x \in A$ ».

1a') Autres types élémentaires

Le type "entier naturel" pourrait être considéré comme le seul type *élémentaire* des mathématiques, en ce sens qu'il n'y en a pas besoin d'autres de manière impérative pour développer l'édifice mathématique. Les autres types élémentaires peuvent être en effet codés dans les entiers naturels. Néanmoins les procédures de codage ont toujours un caractère arbitraire et déplaisant.

Il est donc naturel d'admettre d'autres types élémentaires

- les types finis explicites : un tel type est explicité par la liste des objets qui le composent.
- le type "mots sur un alphabet fini explicite". Ce type est engendré à partir des mots à une lettre (ou le mot vide, si on l'autorise, mais il faut alors le noter autrement que par lui-même) au moyen des opérations "ajout d'une lettre à la fin du mot".

Ceci est tout à fait analogue à la construction des entiers naturels à partir de 0 par l'opération "successeur".

Il y a, outre les objets fondamentaux que sont les entiers naturels, plusieurs méthodes de construction couramment utilisées. En voici trois d'entre elles.

1b) Couples d'objets

La notion de «couple d'objets» est elle aussi une notion prémathématique, du même type que la notion d'objets clairement identifiables.

Si on a donné un sens à " $x \in A$ " et à " $y \in B$ ", on définit un objet z comme étant de type $A \times B$, en disant que z est un couple ordonné formé par un objet x de type A et un objet y de type B . On écrit $z = (x, y)$, et aussi " $z \in A \times B$ ". Il faut évidemment considérer que chaque "coordonnée" du couple z peut être calculée à partir de z ⁽⁵⁾.

⁴ Classique depuis Cantor ! considérer que l'ensemble $\mathbb{N}$ "existe" est une attitude d'esprit conforme à l'idée d'un infini actuel, à caractère positif.

⁵ Notez qu'en théorie des ensembles classique, on définit (x, y) comme égal à $\{x, \{x, y\}\}$, ce qui est tout à fait arbitraire et contraire à l'intuition. En fait, il semble que la notion de paire non ordonnée vienne inévitablement après la notion de paire ordonnée: une paire non ordonnée est donnée par une paire ordonnée, et deux paires non ordonnées sont égales si et seulement si les paires ordonnées qui les donnent sont les mêmes ou si la seconde s'obtient par permutation des coordonnées de la première. Dans le même genre d'idée, on voit souvent définir 0 comme étant l'ensemble vide $\emptyset$ et $n+1$ comme étant l'ensemble des entiers qui le précèdent $\{0, 1, \dots, n\}$. Ce genre de crime contre l'intuition et le bon sens est une invention relativement récente, due à Von Neuman. Au départ, la théorie des ensembles admettait des objets initiaux non définis, des atomes, les entiers naturels, qui n'avaient pas le statut d'ensembles. C'est à partir des atomes «entiers

1c) Opérations de A vers B

Si on a donné un sens à “ $x \in A$ ” et à “ $x \in B$ ”, on dit qu'un objet F est une opération de A vers B, si F est une “méthode de calcul explicite” qui, à partir d'un objet x de type A, fournit, en un temps fini, un objet y de type B. On écrit $y = Fx$, ou $y = F(x)$.

On abrège la “définition” précédente, sous la forme

$$F \in (A \rightarrow B)$$

ou encore sous la forme

$$F \in B^A.$$

J'ai mis “définition” entre guillemets parce qu'il ne s'agit pas d'une définition, mais d'une paraphrase. Les définitions en mathématiques ne pourront venir *qu'après* ... après qu'on ait précisé les principes de départ, qui sont susceptibles de commentaires et discussions seulement.⁽⁶⁾

Le fait qu'on considère comme “clair” ce que signifie “ F est une méthode de calcul explicite, aboutissant en un temps fini, et qui, à partir d'un objet de type A, fournit un objet de type B” est plutôt une constatation d'un fait d'expérience : lorsqu'une mathématicienne déclare avoir trouvé une méthode explicite pour résoudre tel ou tel type de problème, les autres mathématiciens tombent assez rapidement d'accord pour affirmer, soit qu'elle a raison, soit qu'elle s'est trompée à tel endroit précis.

Et nul besoin pour cela d'être un mathématicien rallié aux thèses constructivistes. Le fait qu'un résultat est “effectif” n'est pas “formulable” en mathématiques classiques, mais tout le monde tombe néanmoins rapidement d'accord sur ce que ça *signifie* (du moins si on oublie le désaccord entre “potentiellement réalisable” et “concrètement réalisable”).

Reprenons la discussion : considérer comme “clair” ce que signifie “ F est une opération de A vers B” ne sous entend pas qu'on sache définir *a priori* de quelle forme précise sont toutes les opérations de A vers B.

Par exemple toute opération de $\mathbb{N}$ vers $\mathbb{N}$ peut elle être ramenée à la forme d'un programme machine ?

Et si c'est le cas, est-ce que le passage de l'opération F au programme machine correspondant est toujours parfaitement clair dès la donnée de l'opération F ?

Cette discussion est reliée à ce qu'on appelle la “Thèse de Church”.

La thèse de Church est que toute opération de $\mathbb{N}$ vers $\mathbb{N}$ qui peut être mécanisée peut l'être à travers un programme machine. Si l'expérience accumulée semble donner raison à Church, cela ne règle pas pour autant la question, différente, de savoir si toute procédure effective peut être mécanisée, et si oui, celle de savoir dans quelle mesure cette mécanisation est elle même automatique ou si elle réserve une place à l'invention.

Par ailleurs, même en ce qui concerne un programme machine censé calculer une fonction de $\mathbb{N}$ vers $\mathbb{N}$, reste posé le problème suivant : est-ce que l'exécution du programme aboutit bien

naturels» qu'étaient construits les ensembles. Un jour, quelques légiférateurs dogmatiques se sont aperçus que les atomes initiaux étaient autant d'objets “vides” (sans éléments) et pourtant deux à deux distincts, et distincts de l'ensemble vide, et ils ont décidé de réparer cette offense à l'unité des mathématiques. Une aimable plaisanterie de Von Neuman, qui introduisait d'ailleurs certaines facilités dans la théorie des ordinaux fut érigée en principe intangible. Cachez ces atomes que je ne saurais voir !

⁶ De manière générale, presque tout ce texte contient plutôt des “définitions-commentaires” que des définitions proprement dites.

en un temps fini à l'instruction d'arrêt pour chaque valeur de l'entrée n , ou bien le programme ne risque-t-il pas de tourner indéfiniment en rond pour certaines valeurs de l'entrée ?

Cette difficile question, considérée comme portant sur tous les programmes, ne comporte pas de réponse mécanisable. En d'autres termes, il n'existe pas de programme qui, acceptant comme entrée un texte arbitraire de programme, décide sans jamais se tromper si le programme examiné aboutit à l'instruction d'arrêt.

Dans la pratique, il y a donc les programmes pour lesquels on sait démontrer qu'ils aboutissent à l'instruction d'arrêt pour toute valeur (potentielle) de la variable n , il y a ceux pour lesquels on connaît une valeur de la variable n pour laquelle on sait démontrer que le programme tourne indéfiniment en rond, et il y a *les autres*.

Ainsi, bien que l'affirmation "ce programme aboutit à l'instruction d'arrêt pour toute valeur de la variable n " ait *un sens clair*, il n'y a pas de méthode générale pour décider si elle est "vraie" ou "fausse".

La discussion sur "les objets de type $(A \rightarrow B)$ " n'est pas close. Les considérations précédentes pour le cas où A et B sont tous deux le type $\mathbb{N}$ n'éclairent que partiellement le problème de fond posé dans le cas général. Nous y reviendrons dans la suite.

Notez que les constructions précédemment décrites sont suffisantes pour créer des types relativement compliqués. Les nombres rationnels peuvent être vus comme des couples d'entiers naturels munis d'un signe. Les nombres réels peuvent être vus comme formant une partie de $\mathbb{Q}^{\mathbb{N}}$ (la partie formée des suites de Cauchy). Pour que cette dernière construction devienne claire, il nous faudra préciser quelle est la signification constructive d'une phrase comme "telle suite de rationnels est une suite de Cauchy".

1d) Objets d'un certain type vérifiant une certaine propriété

Il s'agit ici de discuter la légitimité de la définition d'un type d'objet comme le type des nombres réels : objets d'un certain type déjà défini et qui vérifient en outre une propriété précisée.

Pour que cette méthode de définition soit vraiment une méthode de *construction*, il faut que la propriété ait un sens clair, ce qui signifie que la "vérité" de cette propriété pour tel objet déjà défini doit résulter elle-même d'une construction.

Pour revenir à notre exemple du type des nombres réels, la phrase

« Soit un nombre réel x »

doit prendre le sens d'une construction. Ca sera à peu près cela :

voici une construction qui à partir d'un entier naturel n doit aboutir à un nombre rationnel u_n

voici également une preuve qui montre que la construction précédente aboutit bien en un temps fini pour toute valeur de l'entrée n

voici enfin une preuve du fait que la suite de rationnels vérifie la propriété de Cauchy de manière tout à fait explicite

Tout ceci est une construction dans la mesure où une preuve est elle-même une construction.

Dans l'acception classique "être une suite de Cauchy" est une chose "vraie en soi" ou "fausse en soi", de toute éternité, et pour les siècles à venir⁽⁷⁾.

En mathématiques constructives, comme on ne veut pas avoir affaire à des êtres purement idéaux sans aucune garantie sur leur existence, on est obligé de donner un sens constructif à la vérité, c.-à-d. aussi de relativiser la vérité.

⁷ Amen !

Nous arrivons là au problème crucial de “construction de la vérité”, qui sera discuté plus en détail dans le paragraphe 2 : “affirmer c'est démontrer.”

Mais d'abord quelques réflexions préliminaires sur la notion de “propriété ayant une signification claire”.

Une telle propriété doit concerner des objets d'un type préalablement défini. Par exemple “ x est un objet” ne saurait être considéré comme une propriété : son champ d'application est trop vaste. Ou alors il faudrait admettre que tous les types d'objets mathématiques possibles pourraient être définis a priori et une fois pour toutes.

Par ailleurs, toute propriété ayant un sens clair est susceptible d'être décrite dans un langage suffisamment précis. Elle peut donc être considérée elle-même comme un objet mathématique construit. Lorsqu'on “fige” un corps de mathématiques à l'intérieur d'un système formel, les objets et les propriétés envisagés sont définis “une fois pour toutes”, de même que les méthodes de démonstration autorisées⁽⁸⁾.

Malgré l'intérêt que présentent de tels systèmes formels pour “prendre du recul” par rapport à un corps de mathématiques concrètement pratiquées (en discuter la force, l'intérêt, la cohérence), on sait (par expérience, et par le théorème d'incomplétude de Gödel) que de tels systèmes formels sont un cadre trop étroit pour développer les mathématiques : de nouvelles méthodes de démonstrations peuvent être découvertes, de nouveaux types d'objets inventés.

Ainsi, bien que toute propriété considérée dans la pratique doive être “un être mathématique construit”, il semble très hasardeux de considérer que l'on pourrait définir un nouveau *type d'objet* qui serait : “les propriétés se rapportant aux objets de type A ”.

Et le tour de magie (qui était aussi un tour de force, il faut le reconnaître, à l'époque de Cantor) consistant à considérer que “l'ensemble des parties de $\mathbb{N}$ est bien défini” a été un escamotage du problème et non sa solution⁽⁹⁾.

L'objet du paragraphe (2) qui suit est une discussion d'ordre général sur “construire la vérité” et a pour but d'en préciser la problématique pour les propriétés les plus couramment utilisées en mathématiques.

2) Affirmer, c'est démontrer

Dans le paragraphe précédent, on a vu que l'exigence «tous les objets doivent être construits», implique, si on veut pouvoir faire suffisamment de mathématiques, l'exigence: «il faut donner un sens constructif à la vérité». En fait, cette deuxième exigence s'impose de manière autonome, dès qu'on réfléchit sur la notion de vérité et qu'on veut donner aux mathématiques une signification concrète, objective.

⁸ La construction de la vérité prend alors un caractère quelque peu automatique et relativement déplaisant (car nous espérons tous qu'une place reste réservée à l'invention, l'humour, l'extravagance)

⁹ Cette phrase n'a jamais été justifiée autrement que de manière purement proclamatoire. Il est par contre intéressant de savoir que Dedekind pensait *démontrer* l'existence de l'infini actuel par la considération du caractère a priori non fini de ses pensées (par exemple, le fait de penser à la pensée précédente ne saurait être considéré que comme une pensée radicalement distincte de la précédente). Pourquoi diable ne déclarait-il pas tout de go: «considérons l'ensemble infini des entiers naturels (certainement plus clair que l'ensemble fini de ses propres pensées, passées, présentes et à venir), nous le voyons clairement en pensée, donc il existe bien en acte». Au moins, cette attitude discutable était elle celle d'un pionnier, et d'un très grand mathématicien. Que penser des rédacteurs d'un bouquin de premier cycle qui écrivent sans vergogne «on démontre en théorie des ensembles qu'il existe un ensemble infini», sinon que l'inculture est la chose la mieux partagée dans les milieux savants.

Certaines propriétés demandent pour être vérifiées un simple calcul machine. D'autres, comme la conjecture de Goldbach (tout nombre pair est somme de deux nombres premiers) demandent a priori une infinité de vérifications, ce qui excède les possibilités d'Homo Sapiens.

Les mathématiques "classiques" qui affirment que la conjecture de Goldbach est forcément vraie ou fausse, admettent donc implicitement :

- ou bien l'existence d'un dieu mathématicien capable de faire une infinité de vérifications en un temps fini
- ou bien l'"omniscience" de Homo Sapiens : il serait capable de trouver un jour ou l'autre des réponses et démonstrations convaincantes pour tout problème mathématique clairement posé.

Les mathématiques constructives ne font aucune de ces deux hypothèses hasardeuses. Elles considèrent donc que seules sont "vraies" les affirmations démontrées de manière convaincante. Les affirmations non encore démontrées seront peut-être "vraies" un jour prochain. En attendant le jour de leur démonstration, elles restent dans un no man's land inconfortable mais inévitable. Il y a donc des vérités actuelles, et des vérités potentielles, mais pas de vérité absolue indépendante d'Homo Sapiens. On peut, si on le désire, considérer que les vérités potentielles forment une sorte de "vérité absolue", mais cela ne légitimera pas pour autant toutes les méthodes des mathématiques classiques pour ce qui concerne les affirmations qui sous-entendent une infinité de vérifications.

Par ailleurs, même si on est "croyant", la notion de "vérité humaine potentielle" présente au moins autant d'intérêt que la notion de "vérité absolue constatable par un dieu mathématicien", et mérite qu'on s'y attarde un peu.

C'est ce que nous allons faire en examinant la signification constructive de la vérité pour les propriétés les plus couramment considérées en mathématiques.

De la discussion précédente, on voit que la notion de base avec lequel travaille le mathématicien constructif n'est pas exactement : "La propriété P est vraie", mais plutôt "Voici une démonstration de la propriété P". Comprendre le deuxième énoncé lorsqu'on entend le premier, c'est appliquer le principe : «affirmer c'est démontrer».

On utilisera l'écriture " $\vdash P$ " pour : "voici une démonstration de P". Il s'agit d'une démonstration convaincante, pour un mathématicien constructif, une telle démonstration est nécessairement constructive, mais il n'y a pas de catalogue définitif de ce que sont les démonstrations constructives. En bref et au risque de nous répéter, la notion de "construction" est une notion première, prémathématique, qui sous-tend les mathématiques constructives, un peu de la même manière que l'idée d'un univers ensembliste cantorien avec vérité absolue et tiers exclu est une idée prémathématique qui sous-tend les mathématiques classiques.

2a) Propriétés dont la vérité résulte d'un constat

Pour les types élémentaires, on considère aussi que l'égalité ou la séparation de deux objets donnés (de même type) est elle-même immédiatement constatable⁽¹⁰⁾. La séparation est considérée comme une constatation positive au même titre que l'égalité⁽¹¹⁾. Évidemment, cela ne

¹⁰ Cela pourrait susciter une discussion prémathématique sur la possibilité de constater sans ambiguïté l'"égalité" de deux objets "non identiques" (écrits en des endroits différents d'une feuille de papier par exemple). Comme nous l'avons déjà remarqué, les mathématiques commencent *après* la solution de ce genre de questions.

¹¹ Du point de vue "prémathématique" on pourrait même sans doute considérer que la question de la séparation est plus claire, et préexiste à la question de l'égalité, qui est toujours une égalité "sous certains aspects"

s'applique que lorsqu'il s'agit d'objets donnés (au départ d'un raisonnement, d'une construction).

De la "définition" 1c) de la notion de fonction, il résulte alors que si F et G sont deux fonctions de $\mathbb{N}$ dans $\mathbb{N}$, et n et m deux entiers naturels, les propriétés : " $F(n) = G(m)$ ", ou : " $F(n) \neq G(m)$ " sont elles mêmes constatables après un simple calcul. Autrement dit, une opération conserve le caractère "d'objet clairement défini" que possède implicitement un objet apparaissant au début d'une phrase du style : soit n un entier naturel, On voit donc que la notion d'opération donnée en mathématiques constructives est très différente de la notion de fonction donnée en mathématiques classiques. Par exemple un mathématicien classique, devant une série de conjectures difficiles P_n peut inventer la fonction de $\mathbb{N}$ vers $\mathbb{N}$ égale à 1 pour chaque entier n tel que P_n est vraie, et égale à 0 sinon. Bien que cette phrase définisse un ensemble de couples (n, m) , ensemble inclus dans $\mathbb{N} \times \{0, 1\}$ (même pour un mathématicien constructif) il est clair que la valeur m (0 ou 1) correspondant à n ne résulte pas d'une construction, et ne définit donc pas une opération (ce qui revient à dire qu'on ne peut pas prouver constructivement que le graphe considéré est celui d'une opération).

2b) Les connecteurs "Et" et "Ou"

Étant données deux propriétés P et Q , on accorde la signification suivante à la propriété : $(P \text{ et } Q)$:

– $\vdash (P \text{ et } Q)$ signifie : $\vdash P$ et $\vdash Q$

En d'autres termes, pour donner une démonstration de $(P \text{ et } Q)$ il faut donner une démonstration de P et une démonstration de Q .

De même la signification constructive du connecteur ou est donnée par :

– $\vdash (P \text{ ou } Q)$ signifie : $\vdash P$ ou $\vdash Q$

Une démonstration de $(P \text{ ou } Q)$ doit contenir de manière explicite une démonstration de P ou une démonstration de Q .

L'intérêt du "ou" constructif, apparaît clairement lorsque les propriétés P et Q concernent un objet variable (de type précisé). Pour certaines valeurs de la variable, la démonstration de $(P \text{ ou } Q)$ fournira une démonstration de P , pour les autres valeurs la démonstration de $(P \text{ ou } Q)$ fournira une démonstration de Q .

Les commentaires précédents sur les connecteurs "ou" et "et" ne sont pas des plaisanteries. D'une part, ils confirment que le langage a une priorité historique par rapport aux mathématiques. C'est seulement à l'être humain qui a appris à parler, qu'on peut commencer à parler de mathématiques. D'autre part, derrière leur apparence d'évidence pour Mr. de Lapalisse, ils cachent bien des mystères. Par exemple les systèmes formels modélisant les mathématiques constructives possèdent bien les deux propriétés énoncées lorsqu'on lit « $\vdash P$ » comme «la propriété P est prouvable dans le système formel considéré», tandis que les systèmes formels modélisant les mathématiques idéalistes (dites classiques) ont un comportement correct par rapport au "et" mais incorrect par rapport au "ou". Dans de tels systèmes formels, on peut très bien démontrer " $P \text{ ou } Q$ " sans pouvoir démontrer ni P ni Q ¹².

¹² Par exemple la théorie formelle classique des ensembles, si elle est consistante, ne peut pas prouver qu'elle est consistante, très probablement, elle ne peut pas non plus prouver qu'elle est inconsistante, mais elle peut facilement prouver qu'elle est consistante ou inconsistante.

Dans un commentaire précédent, nous avons vu que si n et m sont des objets d'un même type élémentaire, leur égalité ou leur séparation est considérée comme constatable par un calcul élémentaire. Cela donne donc par exemple pour le type des entiers naturels, l'axiome suivant :
Si m et n sont des entiers donnés, on a : $(m = n)$ ou $(m \neq n)$

2c) "Il existe un objet de type A vérifiant la propriété P "

On considère une propriété P concernant (peut-être et entre autres) un objet de type A . On appelle x cet objet (qui dans l'écriture de P apparaît comme une variable de type A). Pour chaque valeur précise a de la variable x , on obtient une propriété particulière notée $P(a)$.

On accorde alors la signification intuitive suivante à la propriété :

"Il existe un objet x de type A tel que $P(x)$ " :

- Voici un objet a , voici une démonstration du fait que a est de type A , et voici une démonstration de $P(a)$.

En abrégé : $\vdash \exists x \in A, P(x)$ signifie : Voici un a , et $\vdash a \in A$, et $\vdash P(a)$.

Concernant la signification constructive du "il existe", on voit que la différence, de taille, avec la signification classique est la nécessaire explicitation de l'objet a . Cette exigence est d'ailleurs proche de la signification intuitive usuelle. Les systèmes formels modélisant les mathématiques constructives possèdent cette propriété, que lorsqu'on a réussi à démontrer l'existence d'un objet vérifiant une formule, alors on peut extraire de la preuve, par un procédé purement automatique, une construction de l'objet en question. Par contre, dans les systèmes formels modélisant les mathématiques classiques, on peut très bien arriver à démontrer qu'un objet existe, sans qu'aucune explicitation de cet objet soit possible.

Par exemple, considérons une fonction f de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$. Dans un système formel classique on démontre l'existence de la fonction g de $\mathbb{N}$ vers $\mathbb{N}$ vérifiant la propriété suivante :

- pour tout $n \in \mathbb{N}$, $g(n)$ est la plus petite des valeurs $f(n,m)$ lorsqu'on fait varier m

Cela est basé sur l'existence d'une valeur minimum parmi tous les $f(n,m)$. Mais la preuve de cette existence n'est pas constructive. Plus précisément il y a des exemples où la fonction f est tout à fait explicite (calculable au moyen d'une procédure simple), tandis que la fonction g ne l'est pas (elle n'est calculable par aucune procédure mécanique).

Naturellement, dans le système formel constructif correspondant, la fonction g ne peut tout bonnement pas être définie, puisqu'un obstacle apparemment infranchissable est posé à son explicitation : il semble peu probable, (quoique a priori pas complètement impossible) qu'on puisse un jour expliciter une fonction non récursive de $\mathbb{N}$ vers $\mathbb{N}$.

2d) "Pour tout entier n la propriété P est vraie"

La signification constructive de : $\vdash \forall n \in \mathbb{N}, P(n)$

est la suivante :

- voici une construction qui transforme l'entier n en une démonstration de $P(n)$
ou encore :
- voici une construction qui, à partir de n , fournit une démonstration de $P(n)$.

Une définition analogue peut être prise pour la quantification universelle d'une variable d'un autre type élémentaire que les entiers naturels (par exemple le type des mots sur un alphabet fini donné).

Notez que le quantificateur universel $\forall n \in \mathbb{N}$ est en fait sous entendu lorsqu'on demande la démonstration d'une propriété $P(n)$ concernant un entier n donné sur lequel on ne fait aucune hypothèse particulière. En d'autres termes, il revient au même de démontrer $P(n)$, sachant seulement que n est un entier, ou de démontrer $\forall n \in \mathbb{N} P(n)$.

L'exemple de propriété, démontrable classiquement mais non constructivement, donné à la fin du 2c) peut s'écrire, sans faire appel directement à la "fonction g ", sous la forme suivante :

$$- \quad \forall n \in \mathbb{N} \quad \exists m \in \mathbb{N} \quad \forall p \in \mathbb{N} \quad f(n,m) \leq f(n,p) \quad (*)$$

En outre, la proposition :

$$- \quad \exists n \in \mathbb{N} \quad \forall m \in \mathbb{N} \quad \exists p \in \mathbb{N} \quad f(n,m) > f(n,p) \quad (**)$$

est facilement prouvée absurde.

En fait, ce genre de propriété (*) est typiquement un "tiers cas non exclu" en mathématiques constructives. Car si la preuve classique de (*) ne fonctionne pas constructivement⁽¹³⁾, cet échec ne constitue pas la base d'un contre exemple fort de (*) que serait la preuve constructive de la proposition (**)⁽¹⁴⁾. De même, le fait que la fonction g n'est pas calculable mécaniquement n'implique pas pour autant de manière certaine sa non existence constructive⁽¹⁵⁾.

Avant de passer à la quantification universelle sur des types plus compliqués, nous devons expliciter la signification constructive de l'implication.

2e) "La propriété P implique la propriété Q "

La signification constructive de $\vdash (P \Rightarrow Q)$ est la suivante :

- Voici une construction qui transforme une démonstration de P en une démonstration de Q .

Cette définition correspond tout à fait à la pratique intuitive des mathématiques, une fois qu'on a interprété "la propriété P est vraie" par "voici une démonstration de P ".

Lorsque P et Q comportent des variables communes, il faut comprendre que ces variables "prennent la même valeur" lors de la construction qui transforme une démonstration de P en une démonstration de Q , et que la démonstration de P peut très bien dépendre directement des valeurs prises par les variables.

Supposons qu'on ait une preuve constructive de l'implication $(P \Rightarrow Q)$. Pour les valeurs précisées des variables communes où on sait démontrer P , on saura donc aussi démontrer Q . Pour des valeurs précisées des variables communes où P est absurde (cf. paragraphe qui suit) la démonstration de $P \Rightarrow Q$ ne nous apprendra rien sur Q . Et pour des valeurs précisées des variables communes pour lesquelles on ne sait pas grand chose de la propriété P , l'implication $\vdash P \Rightarrow Q$ nous apprend néanmoins quelque chose : un certain lien entre P et Q .

Ce lien entre P et Q (qui, pour tout mathématicien, constitue la signification *profonde* de l'implication) est complètement déformé dans la logique classique, où $\vdash (P \Rightarrow Q)$ équivaut à $\vdash (\neg P \text{ ou } Q)$.

¹³ Elle démontre seulement que (**) est absurde

¹⁴ Une interprétation constructive possible des preuves classiques (due à Kreisel) est de dire que la preuve classique d'un théorème donne la preuve constructive de l'absurdité de l'existence d'un contre-exemple fort au théorème. Ceci au moins lorsque les objets apparaissant dans le théorème ont une signification constructive. De ce point de vue, et lorsque la dernière restriction est valable, les mathématiques constructives sont un raffinement des mathématiques classiques.

¹⁵ Sauf si on admet que toute fonction explicite de $\mathbb{N}$ vers $\mathbb{N}$ est récursive, mécanisable.

En fait, constructivement $(\neg P \text{ ou } Q)$ est nettement plus fort (plus difficile à démontrer) que $(P \Rightarrow Q)$.

2f) La négation : “La propriété P est absurde”

La vérité d'une propriété en mathématiques constructives doit être “construite” au moyen d'une démonstration. Par conséquent la notion de “faux” absolu n'existe pas plus que la notion de “vrai” absolu. Par ailleurs la “négation intuitive” de l'affirmation : “la propriété P peut être démontrée” ne peut pas être “construite”. Si la propriété P est suffisamment mystérieuse, il faudrait être un dieu mathématicien pour savoir avec certitude qu'aucune démonstration convaincante n'existe pour la propriété P .

La négation constructive n'aura donc pas la signification intuitive “ P n'est pas vraie”, mais la signification “ P est absurde”, ou encore “ P implique une absurdité”. C'est donc une signification intuitive plus forte que “ P n'est pas vraie”.

En prenant comme propriété absurde la propriété : “ $0 = 1$ ”, on obtient donc la définition-commentaire suivante : l'affirmation “ P est absurde” signifie “ P implique $0 = 1$ ”

Ce qui peut s'écrire de manière abrégée en symboles :

– $\vdash \neg P$, signifie : $\vdash (P \Rightarrow (0 = 1))$.

Arrivé à ce point, la lectrice comprendra que, via l'interprétation donnée des notions de : « Vrai, Absurde, Ou », le principe du tiers exclu signifierait : “toute propriété P peut être ou bien démontrée, ou bien réduite à l'absurde”, c.-à-d. : un principe d'omniscience d'Homo Sapiens ajouté à un principe d'existence d'une vérité absolue. Ce qui est quand même beaucoup.

Et le refus du tiers exclu du point de vue constructif n'est nullement une provocation visant à embêter les mathématiciens classiques, mais un simple constat : dès que l'on accorde une signification constructive à la vérité et que l'on considère l'infinité (potentielle ou actuelle, peu importe) des entiers naturels, on perd le principe du tiers exclu. Ce principe ne serait pas problématique si on ne considérait que des propriétés portant sur un ensemble fini et fixé d'objets.

Le choix de $0 = 1$ pour désigner l'absurde est une question annexe⁽¹⁶⁾.

On admet en tout cas l'existence d'une propriété Faux répondant au schéma d'axiome suivant : pour n'importe quelle propriété P , on a :

$$\vdash \text{Faux} \Rightarrow P.$$

¹⁶ Personnellement, j'aime bien penser “sans négation”. Je considère donc que lorsque je fais des mathématiques, j'ai toujours au moins deux modèles en tête. Le modèle intuitif usuel (où les entiers sont les entiers intuitifs etc...), et un deuxième modèle qui résulte d'un collapsus général : il y a un unique objet :

$0 = 1 = \pi = \dots = \mathbb{N} = \mathbb{R}$ = l'ensemble des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ etc.

et cet objet vérifie toutes les propriétés. Par exemple $2 \neq 2$ puisque $0 = 1 \Rightarrow (2 = 2 \Rightarrow 0 = 1)$. Ainsi lorsqu'on démontre qu'une propriété est absurde, on démontre seulement que si on tient absolument à avoir cette propriété, il faut choisir le second modèle, où tout s'est effondré.

2g) Pour tout objet x de type A , la propriété $P(x)$ est vraie

Si nous jetons un regard rétrospectif sur les types d'objets que nous avons admis, nous voyons que tout "type d'objets" A peut être défini de la manière suivante : donner un objet x de type A revient à faire deux choses :

- primo, effectuer une certaine construction X (d'où découle en particulier l'objet x)
- secundo, démontrer une certaine propriété $Q(X)$ concernant la construction X ⁽¹⁷⁾

Alors l'affirmation : "pour tout objet x de type A , la propriété $P(x)$ est vraie" aura la signification constructive suivante :

- voici une construction qui, à partir de la construction X et de la démonstration que X vérifie la propriété $Q(X)$, fournit une démonstration de $P(x)$.

Pour paraphraser et se référer aux autres définitions-commentaires déjà données, nous pourrions dire ceci :

Lorsque le type A est défini par :

$\vdash x \in A$ signifie: $\vdash (x \in B \text{ et } Q(x))$

où la signification de $x \in B$ est "plus simple" que celle de $x \in A$

Alors $\vdash \forall x \in A P(x)$ signifie : $\vdash \forall x \in B (Q(x) \Rightarrow P(x))$

2h) Conclusion provisoire sur ce qu'est une propriété :

En mathématiques constructives, une "propriété" (ou "assertion" ou "affirmation", ou "relation") est donc donnée par :

- primo : une déclaration de types
- secundo : une déclaration de variables (dans des types déclarés)
- tertio : une déclaration de constantes (c.-à-d., on donne des objets effectivement construits, dans des types déclarés)
- quarto : la propriété proprement dite, qui concerne les variables et les constantes : elle doit être "construite" à partir de propriétés considérées comme élémentaires (c.-à-d. dont la vérification résulte d'un constat) au moyen de règles précises. Les connecteurs logiques et les quantifications font partie de ces règles. (on pourra en définir d'autres, à condition de leur attribuer une "signification" claire en précisant ce qu'il faut faire pour démontrer la nouvelle propriété ainsi construite).

2i) Exercices de raisonnements constructifs

Nous commençons par des règles du "calcul des propositions", c.-à-d. lorsqu'on ne parle pas de quantificateurs.

Nous proposons à titre d'exercice à la lectrice de "démontrer" les théorèmes constructifs suivants, en s'appuyant sur l'interprétation donnée des connecteurs logiques, lorsque P , Q et

¹⁷ Ici, on pourra remarquer la très vieille problématique de la définition par "genre" (genre = génération = construction) et "différence" (différence = propriété particulière vérifiée). On pourra aussi se demander si les constructions de type évoquées au paragraphe 1 vérifient toujours cette "définition" par genre et différence. En fait c'est seulement dans la mise en pratique des maths constructives que l'on pourra faire cette discussion en détail : le fond de la question tourne autour de la notion de "construction". Une démonstration est sans nul doute elle-même une construction : cela suffira je pense à justifier le fait qu'il n'y a pas et ne peut y avoir de "définition a priori" de ce que sont les "constructions". Par suite, la discussion sur "les principes de travail" ne peut être faite une fois pour toutes, et doit sans cesse être reprise, poursuivie, étendue : au même rythme que les mathématiques elles-mêmes.

R sont des propriétés. L'équivalence est définie comme la conjonction des deux implications, directe et réciproque.

- $\vdash (P \Rightarrow (Q \Rightarrow R)) \Leftrightarrow ((P \text{ et } Q) \Rightarrow R)$
- $\vdash ((P \text{ ou } Q) \Rightarrow R) \Leftrightarrow ((P \Rightarrow R) \text{ et } (Q \Rightarrow R))$
- $\vdash (R \text{ et } (P \text{ ou } Q)) \Leftrightarrow ((R \text{ et } P) \text{ ou } (R \text{ et } Q))$
- $\vdash (R \text{ ou } (P \text{ et } Q)) \Leftrightarrow ((R \text{ ou } P) \text{ et } (R \text{ ou } Q))$
- $\vdash \neg(P \text{ et } \neg P)$
- $\vdash \neg P \Rightarrow (P \Rightarrow Q)$
- $\vdash \neg(P \text{ et } Q) \Leftrightarrow (P \Rightarrow \neg Q)$
- $\vdash (P \Rightarrow \neg Q) \Leftrightarrow (Q \Rightarrow \neg P)$
- $\vdash \neg(P \text{ ou } Q) \Leftrightarrow (\neg P \text{ et } \neg Q)$
- $\vdash (P \text{ ou } Q) \Rightarrow \neg(\neg P \text{ et } \neg Q)$
- $\vdash (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$
- $\vdash P \Rightarrow \neg \neg P$
- $\vdash \neg P \Leftrightarrow \neg \neg \neg P$
- $\vdash \neg \neg (P \Rightarrow Q) \Leftrightarrow \neg (P \text{ et } \neg Q) \Leftrightarrow (P \Rightarrow \neg \neg Q) \Leftrightarrow (\neg \neg P \Rightarrow \neg \neg Q)$

Nous passons maintenant à la logique des prédicats, où apparaissent explicitement les quantificateurs. De nouveau nous proposons en exercice de "démontrer" quelques règles valides constructivement, en s'appuyant sur l'interprétation donnée des connecteurs logiques et des quantificateurs.

Précisons quelques conventions. Tout d'abord, implicitement, toute variable est d'un type bien défini. Appelons A un prédicat. Si un quantificateur portant sur α apparaît dans la formule, nous notons alors $A(\alpha)$ si α figure dans A et nous notons A si α ne figure pas dans A (mais d'autres variables peuvent figurer dans A). On note t un terme.

- $\vdash A(t) \Rightarrow \exists \alpha A(\alpha)$
- $\vdash \forall \alpha A(\alpha) \Rightarrow A(t)$
- $\vdash \forall \alpha A \Leftrightarrow A$
- $\vdash \exists \alpha A \Leftrightarrow A$
- $\vdash \forall \alpha \forall \beta A(\alpha, \beta) \Leftrightarrow \forall \beta \forall \alpha A(\alpha, \beta)$
- $\vdash \exists \alpha \exists \beta A(\alpha, \beta) \Leftrightarrow \exists \beta \exists \alpha A(\alpha, \beta)$
- $\vdash \exists \alpha \forall \beta A(\alpha, \beta) \Rightarrow \forall \beta \exists \alpha A(\alpha, \beta)$
- $\vdash \forall \alpha (A(\alpha) \text{ et } B(\alpha)) \Leftrightarrow (\forall \alpha A(\alpha) \text{ et } \forall \alpha B(\alpha))$
- $\vdash \exists \alpha (A(\alpha) \text{ ou } B(\alpha)) \Leftrightarrow (\exists \alpha A(\alpha) \text{ ou } \exists \alpha B(\alpha))$
- $\vdash \neg \exists \alpha A(\alpha) \Leftrightarrow \forall \alpha \neg A(\alpha)$
- $\vdash \exists \alpha \neg A(\alpha) \Rightarrow \neg \forall \alpha A(\alpha)$
- $\vdash \forall \alpha (A \Rightarrow B(\alpha)) \Leftrightarrow (A \Rightarrow \forall \alpha B(\alpha))$
- $\vdash \forall \alpha (A(\alpha) \Rightarrow B) \Leftrightarrow (\exists \alpha A(\alpha) \Rightarrow B)$
- $\vdash \exists \alpha (A \Rightarrow B(\alpha)) \Rightarrow (A \Rightarrow \exists \alpha B(\alpha))$
- $\vdash \exists \alpha (A(\alpha) \Rightarrow B) \Rightarrow (\forall \alpha A(\alpha) \Rightarrow B)$
- $\vdash \exists \alpha (A(\alpha) \Rightarrow B(\alpha)) \Rightarrow (\forall \alpha A(\alpha) \Rightarrow \exists \alpha B(\alpha))$
- $\vdash \forall \alpha (A(\alpha) \Rightarrow B(\alpha)) \Rightarrow (\forall \alpha A(\alpha) \Rightarrow \forall \alpha B(\alpha))$

3) Exemples caractéristiques de divergences entre logique classique et logique constructive

Lorsqu'on se trouve confronté au besoin de changer les règles de la logique, pour passer de la logique classique à la logique constructive, on subit un dépaysement qui fait qu'on n'a plus au

départ d'intuition sûre sur ce qui est acceptable et ce qui ne l'est pas. Le retour systématique à l'explication de la signification constructive des connecteurs et des quantificateurs est en un premier temps nécessaire. Quand un énoncé vrai d'un point de vue classique ne semble pas clair d'un point de vue constructif, on peut essayer des "contre-exemples". Ces contre-exemples montrent que l'assertion douteuse implique un principe qui n'est pas acceptable d'un point de vue constructif. Ces principes peuvent en général être classés dans la rubrique des principes d'omniscience, dans la mesure où leur acceptation ne serait compatible avec le sens constructif des énoncés que si Homo Sapiens était doué de capacités d'omniscience du type : appréhender d'un seul coup l'ensemble des valeurs d'une suite infinie arbitraire d'entiers naturels.

Nous allons nous livrer dans cette section 3 au petit jeu qui consiste à débusquer des principes d'omniscience derrière des affirmations d'apparence anodine. Nous commençons par décrire quelques uns de ces principes.

3a) Principes d'omniscience

Considérons un nombre réel x défini par une suite de Cauchy de rationnels (x_n) vérifiant

$$\forall n \quad |x_n - x_{n+1}| < 1/2^{n+1}$$

de sorte que nous savons que x_n approche x avec un écart $< 1/2^n$. La propriété $x > 0$ équivaut à $\exists n \quad x_n > 1/2^n$. La négation de $x > 0$ est notée $x \leq 0$ et équivaut à $\forall n \quad x_n \leq 1/2^n$. La négation de $x \leq 0$ signifie que l'on sait réduire à l'absurde l'hypothèse $\forall n \quad x_n \leq 1/2^n$. Le prédicat $x = 0$ est défini comme équivalent à $(x \geq 0 \text{ et } x \leq 0)$ et le prédicat $x \neq 0$ comme équivalent à $(x > 0 \text{ ou } x < 0)$.

Pour donner nos contre-exemples intuitifs aux règles classiques, nous utiliserons des propriétés du style $x > 0$ (pour un nombre réel x).

Nous avons déjà expliqué en quoi le tiers exclu $(P \text{ ou } \neg P)$ ne peut être valable constructivement. En particulier, un cas crucial et simple de tiers exclu non valide constructivement est pour un réel x arbitraire :

$$(x > 0 \text{ ou } x \leq 0)$$

Presque toutes les grandes conjectures mathématiques peuvent être ramenées à la forme $x \leq 0$ pour des valeurs particulières de x . Si on avait constructivement $(x > 0 \text{ ou } x \leq 0)$ cela signifierait qu'on dispose d'une méthode générale, qui pourrait décider au moins en principe toutes ces conjectures mathématiques.

Le principe classique, non valide constructivement :

$$\forall x \in \mathbb{R} \quad (x > 0 \text{ ou } x \leq 0)$$

est appelé par Bishop le «petit principe d'omniscience» (PPO).

Il peut être formulé aussi sous la forme : $\forall x \in \mathbb{R} \quad (x = 0 \text{ ou } x \neq 0)$

Ce principe revient à affirmer que, étant donnée une suite d'entiers arbitraire, ou bien elle est identiquement nulle, ou bien il y a un terme non nul dans la suite :

$$\forall f \in (\mathbb{N} \rightarrow \mathbb{N}) \quad ((\forall n \in \mathbb{N} \quad f(n) = 0) \text{ ou } (\exists n \in \mathbb{N} \quad f(n) \neq 0))$$

Un principe plus faible, appelé le «mini principe d'omniscience» (MPO) est le suivant :

$$\forall x \in \mathbb{R} \quad (x \geq 0 \text{ ou } x \leq 0)$$

Cela revient à dire que pour toute suite d'entiers, ou bien le premier terme non nul éventuel est de rang pair, ou bien il est de rang impair. Ceci n'est pas constructivement valide dans la

mesure où, pour une suite infinie qui a l'air identiquement nulle, on hésite indéfiniment avant de pouvoir décider l'alternative. Il est clair que PPO implique MPO⁽¹⁸⁾.

Exercice : démontrez
$$\text{PPO} \Rightarrow (\forall x \in \mathbb{R} (x \geq 0 \text{ ou } \neg x \geq 0)) \Rightarrow \text{MPO}$$

3b) Le principe de Markov

Le principe de Markov (PM) (admis en général par les constructivistes russes), peut être formulé comme suit :

$$\forall x \in \mathbb{R} (\neg x \leq 0 \Rightarrow x > 0)$$

Cela équivaut au fait de considérer que, lorsqu'on a prouvé l'absurdité qu'une suite d'entiers soit partout nulle, alors cette suite se révélera non identiquement nulle un jour ou l'autre.

Deux formulations équivalentes sont les suivantes :

$$\forall x \in \mathbb{R} (\neg x = 0 \Rightarrow x \neq 0)$$

et

$$\forall f \in (\mathbb{N} \rightarrow \mathbb{N}) (\neg (\forall n \in \mathbb{N} f(n) = 0) \Rightarrow (\exists n \in \mathbb{N} f(n) \neq 0))$$

Le principe de Markov est une instance particulièrement élémentaire du principe classique général de double négation

$$\vdash \neg \neg P \Rightarrow P$$

Plus la propriété P a une structure logique compliquée et plus le principe classique de double négation a une signification obscure.

Le principe de Markov est en général refusé selon l'argument que l'existence d'un entier (vérifiant une condition explicite) ne peut pas être considérée comme explicite si la preuve ne fournit pas une borne pour cet entier. Ce qui est en jeu, en fait, c'est le caractère automatique de la construction que signifie une implication: il est intuitivement impensable qu'on dispose jamais d'une méthode universelle qui, à partir d'une double réduction à l'absurde de «la suite d'entiers (u_n) admet un terme non nul», soit capable de borner l'entier n pour lesquels $u_n \neq 0$ ⁽¹⁹⁾.

3c) Quelques comparaisons entre la logique formelle classique et la logique formelle constructive

Nous donnons maintenant quelques commentaires sur la non validité constructive de certaines règles classiques. Nous commençons par le calcul des propositions. Nous examinerons des cas plus subtils que le principe du tiers exclu :

¹⁸ Le fait que MPO est strictement plus faible que PPO (du point de vue des preuves constructives) est sans doute un peu mystérieux. En tout cas, cela se vérifie dans les systèmes formels constructifs capables de rendre compte des suites d'entiers naturels et/ou des nombres réels à la Cauchy. La considération de principes tels que MPO et PPO est intéressante parce que de nombreux théorèmes de mathématiques classiques sont équivalents constructivement à l'un de ces principes. Un travail de logique significatif serait de classer les théorèmes de mathématiques classiques non valides constructivement selon leur équivalence avec l'un (parmi un petit nombre) des principes tels que MPO et PPO. Une affirmation comme $\text{MPO} \Rightarrow \text{PPO}$, qui n'est sans doute pas prouvable constructivement, ne présente pas d'intérêt réel, du moins tant qu'on n'a pas repéré des théorèmes classiques significatifs qui seraient constructivement équivalents à cette affirmation.

¹⁹ Par contre, dans tous les systèmes formels constructifs, on dispose d'une telle méthode : si $\neg x \leq 0$ est prouvable, alors $x > 0$ également. Mais un système formel constructif précis ne constitue qu'un tout petit morceau de mathématiques constructives. Les prétentions à l'universalité des systèmes formels a définitivement été réduite à néant par le théorème d'incomplétude de Gödel.

Variations sur les lois de Morgan

Considérons les formulations suivantes des lois de Morgan.

$$\begin{aligned} \vdash & \neg(\neg P \text{ et } \neg Q) \Rightarrow (P \text{ ou } Q) \\ \vdash & \neg(P \text{ et } Q) \Rightarrow (\neg P \text{ ou } \neg Q) \\ \vdash & \neg(\neg P \text{ et } \neg Q) \Rightarrow (\neg\neg P \text{ ou } \neg\neg Q) \end{aligned}$$

Aucune n'est valable constructivement. Pour s'en convaincre, nous donnons un contre-exemple intuitif à la troisième loi (qui est manifestement une forme plus faible que des deux autres). Considérons un réel arbitraire x et pour P et Q les propriétés $x > 0$ et $x \leq 0$. Alors $(\neg P \text{ et } \neg Q)$ signifie $(Q \text{ et } \neg Q)$ et est donc absurde. La propriété $(\neg\neg P \text{ ou } \neg\neg Q)$ signifie $(\neg x \leq 0 \text{ ou } x \leq 0)$.

Par ailleurs $(x < 0 \Rightarrow x \leq 0)$, donc par contraposition $(\neg x \leq 0 \Rightarrow x \geq 0)$.

Donc, si on avait $(\neg\neg P \text{ ou } \neg\neg Q)$ on aurait également $(x \geq 0 \text{ ou } x \leq 0)$ c.-à-d. MPO.

Notons par ailleurs que la première loi citée ci-dessus implique le principe général de tiers exclu puisqu'en prenant pour Q la propriété $\neg P$ on en déduit $(P \text{ ou } \neg P)$.

Variations sur l'implication

Considérons tout d'abord le "faux principe de contraposition", classiquement vrai :

$$\vdash (\neg P \Rightarrow \neg Q) \Rightarrow (Q \Rightarrow P)$$

On donne un premier contre exemple intuitif en prenant pour Q la propriété $\neg(x = 0)$ et pour P la propriété $x \neq 0$, avec un réel x arbitraire. Alors l'hypothèse avec les négations est facile à prouver⁽²⁰⁾ tandis que la conclusion est le principe de Markov.

Ce faux principe de contraposition implique en fait le principe général de tiers exclu : on prend pour P la propriété $(A \text{ ou } B)$ et pour Q la propriété $\neg(\neg A \text{ et } \neg B)$. Alors la premier membre de l'implication est vrai, tandis que le second membre est la première loi de Morgan citée au paragraphe précédent.

Considérons ensuite le principe classiquement vrai ⁽²¹⁾

$$\vdash ((P_1 \text{ et } P_2) \Rightarrow Q) \Rightarrow ((P_1 \Rightarrow Q) \text{ ou } (P_2 \Rightarrow Q))$$

Un contre-exemple intuitif est fourni comme suit. On considère un réel x arbitraire, la propriété P_1 signifie $x \geq 0$, la propriété P_2 signifie $x \leq 0$ et la propriété Q signifie $x = 0$. Le premier membre de l'implication est vrai par définition de l'égalité sur les réels.

La propriété $(P_1 \Rightarrow Q)$ implique $x \leq 0$ (pour le voir supposez $x > 0$ et réduisez cette hypothèse à l'absurde). De même La propriété $(P_2 \Rightarrow Q)$ implique $x \geq 0$.

Si la formule initiale était vraie on aurait donc MPO : $x \geq 0 \text{ ou } x \leq 0$.

Considérons maintenant l'autre principe classiquement vrai ⁽²²⁾

$$\vdash (P \Rightarrow (Q_1 \text{ ou } Q_2)) \Rightarrow ((P \Rightarrow Q_1) \text{ ou } (P \Rightarrow Q_2))$$

²⁰ Il suffit de réduire à l'absurde Q et $\neg P$, c.-à-d., $\neg\neg P$ et $\neg P$.

²¹ Les deux membres de l'implication ci dessous sont classiquement équivalents à $(\neg P_1 \text{ ou } \neg P_2 \text{ ou } Q)$. Cependant cette implication est bel et bien troublante pour le profane qui se posera inévitablement la question : comment se fait il que toute preuve basée sur deux hypothèses puisse toujours se réduire à une preuve basée sur une seule des deux hypothèses ? ... la réponse est simplement que l'implication classique a perdu la signification intuitive de l'implication comme preuve lorsqu'on a introduit la révélation magique du tiers exclu. Dès lors les preuves n'ont plus le statut d'être mathématiques à part entière, et seuls demeurent le Vrai et le Faux immuables dans l'éternité des siècles. La seule manière de rendre le second membre évidemment faux est de rendre à la fois Q faux et P_1 et P_2 vrais ... et ce second membre est, du point de vue classique, réputé vrai dès qu'il n'est pas évidemment faux.

²² La lectrice pourra développer pour elle-même le même genre de considérations que celles de la note précédente.

Un contre-exemple intuitif est obtenu comme suit. La propriété P signifie $x \neq 0$, la propriété Q_1 signifie $x > 0$, la propriété Q_2 signifie $x < 0$. Le premier membre de l'implication est toujours vrai. Cependant $(P \Rightarrow Q_1)$ implique $x \geq 0$ (réduire à l'absurde $x < 0$) et $(P \Rightarrow Q_2)$ implique $x \leq 0$. Donc on aurait MPO.

Le principe de double négation

On peut donner un "contre-exemple" pour le principe classique de double négation, qui convainc mêmes les adeptes du principe de Markov. On considère un réel x et on prend pour P la propriété $(x > 0 \text{ ou } x \leq 0)$. Cependant, sa double négation est équivalente à $\neg(x \leq 0 \text{ et } \neg x \leq 0)$ et est donc constructivement valide. Ainsi, si on avait $\neg \neg P \Rightarrow P$ on en déduirait le principe PPO.

De la même manière, dans un système formalisé de calcul des propositions constructifs, le principe général de double négation implique le principe du tiers exclu.

Passons maintenant à quelques théorèmes classiques non valides constructivement dans le calcul des prédicats.

Calcul des prédicats

Comme premier exemple nous choisissons :

$$\vdash \neg \forall \alpha A(\alpha) \Rightarrow \exists \alpha \neg A(\alpha)$$

Le principe de Markov est de cette forme. Mais on a aussi des contre-exemples plus forts, par exemple construits comme suit. Si on fait varier α dans l'ensemble $\{1,2\}$ la quantification universelle signifie alors la conjonction A_1 et A_2 tandis que la quantification existentielle doit être remplacée par un «ou» constructif. On obtient donc comme cas particulier le principe du calcul des propositions :

$$\vdash \neg(A_1 \text{ et } A_2) \Rightarrow (\neg A_1 \text{ ou } \neg A_2)$$

Et nous avons montré que ce principe implique MPO.

On peut de la même manière donner des contre-exemples pour les deux principes classiques suivants :

$$\vdash (A \Rightarrow \exists \alpha B(\alpha)) \Rightarrow \exists \alpha (A \Rightarrow B(\alpha))$$

$$\vdash (\forall \alpha A(\alpha) \Rightarrow B) \Rightarrow \exists \alpha (A(\alpha) \Rightarrow B)$$

4) Démonstrations et constructions par induction

Les entiers naturels peuvent être construits à partir de 0 en utilisant l'opération "successeur" (qui est une opération élémentaire de $\mathbb{N}$ dans $\mathbb{N}$). Cette construction est sans doute l'opération la plus "fondamentale" des mathématiques, celle qui permet d'abstraire l'idée de "potentiellement réalisable" à partir de la constatation des objets "effectivement réalisés".

4a) Construction par récurrence

Du fait que tout entier naturel peut être construit à partir de 0, on déduit facilement le principe de "construction par récurrence" suivant :

- soit A un type d'objets, x un objet de type A , et F une opération de $A \times \mathbb{N}$ dans A , alors il existe une opération G de $\mathbb{N}$ dans A , qui vérifie :
 - à partir de 0, l'opération G construit l'objet x
 - si, à partir de $n \in \mathbb{N}$, l'opération G construit l'objet $y \in A$, alors, à partir de $n+1 \in \mathbb{N}$, l'opération G construit l'objet $F(y,n)$.

Ce principe est quasiment “clair par lui-même” à partir du moment où on a compris comment se construisent les entiers naturels. Si l'opération F et l'objet x sont donnés de manière explicite, la lectrice peut voir tout de suite quelles constructions il faut faire pour calculer, par exemple $G(45)$.

On doit considérer que l'opération G résulte “mécaniquement” de la donnée de l'objet x et de l'opération F . Autrement dit, le passage du couple (x, F) à l'opération G est lui-même une opération.

Le principe de construction par récurrence est donc l'affirmation, pour chaque type d'objet A , d'une “opération” R_A de type

$$(A \times (A \times \mathbb{N}) \rightarrow A) \rightarrow (\mathbb{N} \rightarrow A)$$

avec $R_A(x, F) = G$

4b) Démonstration par récurrence

À ce principe de “construction par récurrence”, correspond un principe de “démonstration par récurrence” (qui s'en déduirait d'ailleurs si on considérait que les démonstrations d'une propriété sont des objets d'un certain type bien défini).

C'est le suivant :

- soit P une propriété portant (entre autres) sur une variable $n \in \mathbb{N}$, et notons là $P(n)$. Alors, si on a une démonstration de $P(0)$ et une démonstration de $\forall n \in \mathbb{N} (P(n) \Rightarrow P(n+1))$, on en déduit mécaniquement une démonstration de $\forall k \in \mathbb{N} P(k)$.

En symboles, cela donne, pour chaque propriété $P(n)$ portant (entre autres) sur un entier variable n , l'axiome suivant :

$$\vdash (P(0) \text{ et } \forall n \in \mathbb{N} (P(n) \Rightarrow P(n+1))) \Rightarrow \forall k \in \mathbb{N} P(k)$$

Si $\underline{n}$ est une valeur précisée de “l'entier variable” n , la démonstration de $P(\underline{n})$ sera donnée par la construction suivante :

- démontrer $P(0)$
- construire l'entier $\underline{n}$ à partir de l'entier 0 au moyen de l'opération successeur
- à chaque nouvel entier $\underline{k}+1$ ainsi obtenu, effectuer les constructions nécessaires à la démonstration de $P(\underline{k}) \Rightarrow P(\underline{k}+1)$, et en déduire la construction globale nécessaire à la démonstration de $P(\underline{k}+1)$.

4c) Induction pour d'autres types élémentaires

De manière analogue, lorsqu'un type d'objet sera défini comme :

les objets construits à partir de certains objets “initiaux” et de certaines “opérations élémentaires”

on aura de même un principe de construction et un principe de démonstration par induction correspondant à ce type d'objet. Il en est ainsi par exemple, pour le type “mots sur l'alphabet fini... (à préciser)”. Les objets initiaux sont les mots à une lettre (ou le mot vide, au choix), et les opérations élémentaires consistent à rajouter une lettre à la fin du mot.

4d) Preuves par induction pour des types construits

À partir du principe de démonstration par induction sur l'ensemble des entiers naturels, on peut établir des principes de démonstration par induction pour des ensembles ordonnés plus sophistiqués, comme par exemple : “ $\mathbb{N} \times \mathbb{N}$ muni de l'ordre lexicographique”.

- soit P une propriété portant (entre autres) sur deux variables n et $m \in \mathbb{N}$, et notons là $P(n,m)$. Alors, si on a $P(0,0)$ et si on a démontré

$$\forall (n,m) \in \mathbb{N}^2 - \{(0,0)\} \quad ((\forall (n',m') < (n,m) \ P(n',m')) \Rightarrow P(n,m))$$
alors on peut démontrer $\forall (n,m) \in \mathbb{N}^2 \ P(n,m)$.

Pour établir ce principe, on prouve par induction sur n que $P(n,m)$ est vrai pour tout m , et cette preuve elle-même se fait par induction sur m .

De même, on peut expliciter un principe de construction par induction pour cet ensemble $\mathbb{N} \times \mathbb{N}$ muni de l'ordre lexicographique.

Un ensemble ordonné avec un premier élément sur lequel on peut pratiquer les preuves par induction est appelé un ensemble bien ordonné.

Pour certains ensemble ordonnés, on pourra se trouver dans la situation intermédiaire suivante : la démonstration de la validité des principes de construction et démonstration par induction ne semble pas pouvoir être déduite à partir des principes correspondants pour les entiers naturels mais des "commentaires" (du type de celui qu'on fait pour la récurrence) et l'expérience accumulée conduisent à admettre cette validité : c'est tout le problème de l'invention de nouvelles méthodes de démonstrations qui est alors posé.

Ce phénomène peut en particulier se présenter sous la forme suivante : il existe certains ensembles ordonnés dénombrables ayant une description parfaitement explicite, et qui, en mathématiques classiques, sont prouvés être des ensembles bien ordonnés. Mais la preuve classique (du fait que l'ordre est un bon ordre) n'est pas entièrement convaincante d'un point de vue constructif. D'autre part, le fait d'admettre qu'un tel ordre est bien un bon ordre n'est pas non plus frappé d'interdit par des "contre exemples" analogues à ceux développés à la section 3.

Ce genre de discussion n'a en fait apparemment pas de conséquence sur les mathématiques usuelles, car les théorèmes fondamentaux ne sont jamais établis en utilisant des preuves par induction sur des ensembles bien ordonnés trop sophistiqués⁽²³⁾. Ce qui fait problème dans l'immense majorité des preuves classiques, c'est bien plutôt des principes d'omniscience tout à fait simples comme PPO ou MPO, ainsi que certains usages de l'axiome du choix.

4e) Constructions de type par induction

Abordons ce problème à partir d'un exemple. Pour tout entier n , on peut considérer le type A_n , défini par récurrence comme suit :

$$A_0 = \mathbb{N} \quad A_{n+1} = (A_n \rightarrow \mathbb{N}).$$

²³ Un fait d'expérience est que, chaque fois qu'un théorème classique usuel possède une version constructive, les algorithmes qui correspondent au théorème n'utilisent que des constructions par induction sur des bons ordres assez simples, le cas typique étant celui d'un "algorithme à oracles uniformément primitif récursif" : considérons par exemple le théorème élémentaire d'analyse constructive qui affirme qu'une fonction uniformément continue f sur l'intervalle $[0,1]$ admet une borne supérieure. La "variable" du théorème est la fonction uniformément continue f . Comme on ne veut pas faire d'hypothèse contraignante concernant comment une fonction uniformément continue vient à être calculée, elle est représentée par deux oracles : le premier oracle donne la précision $(1/2^n)$ avec laquelle doit être donnée x pour que soit assurée une précision $(1/2^m)$ pour $y = f(x)$ (l'oracle répond n à la question m). Le deuxième oracle donne la réponse " $f(x)$ avec une précision $1/2^m$ " lorsqu'on lui pose la question (x,m) où x est un rationnel de l'intervalle. Il n'est pas difficile de produire un algorithme qui, à l'aide de ces deux oracles, et sans aucune autre information concernant la fonction f , est capable de calculer avec une précision donnée la borne supérieure de f . La preuve constructive du théorème contient toujours en filigrane un tel algorithme à oracle (cf. [Knu]).

Enfin, on peut considérer le type $A = \prod_{n \in \mathbb{N}} A_n$ défini comme suit : un objet de type A est une construction F qui, pour chaque entier n , fournit un objet F_n de type A_n . Il n'est pas difficile de produire des objets F de type A .

Mais le type A ne peut pas être ramené à un type construit à partir $\mathbb{N}$ au moyen des autres procédés de constructions déjà légitimes.

Cette explication est-elle suffisamment claire pour qu'on puisse admettre qu'on a bien défini ainsi A comme un type d'objet légitime ?

Cela mérite sûrement une discussion. Mais en fait, comme à la section précédente 4d), cela n'a apparemment pas de conséquence sur les mathématiques usuelles.

5) Ensembles, égalités, fonctions, espaces métriques complets

5a) L'égalité doit en général être définie

Dans un texte mathématique formalisé, deux objets définis "exactement de la même manière" peuvent être considérés "identiques" (quoique définis en deux moments différents). Mais les mathématiques préexistent à leur formalisation (formalisation qui est toujours partielle, limitée, insatisfaisante, rappelons-le). Et les "objets mathématiques" ont une existence indépendante du *nom* qui leur est donné dans tel ou tel système formel.

Il semble donc difficile d'admettre a priori une relation d'"identité" définie une fois pour toutes entre objets mathématiques.

De plus, si on considère, par exemple, deux opérations F et G de $\mathbb{N}$ dans $\mathbb{N}$, la notion la plus importante à manipuler n'est pas celle de leur identité, encore appelée égalité intentionnelle (les opérations F et G sont définies par la même procédure de calcul⁽²⁴⁾), mais c'est celle d'égalité extensionnelle, à savoir :

$$\text{pour tout entier } n, F_n = G_n$$

Il se peut que F et G soient des méthodes de calcul très différentes mais qu'elles aboutissent systématiquement au même résultat. Cette notion d'égalité extensionnelle⁽²⁵⁾ est la notion la plus productive d'un point de vue mathématique.

Ceci conduit à adopter le point de vue suivant :

- l'égalité de deux objets de même type élémentaire est une relation dont la vérité résulte d'un simple calcul (voire d'un simple constat)
- l'égalité de deux objets d'un même type plus complexe X est une relation sujette à définition. Une relation d'égalité, définie sur le type X , doit évidemment être une relation d'équivalence.

Remarque : même pour les entiers naturels on peut considérer que seule la relation " $n = 0$ " résulte d'un constat, auquel cas on pourra construire par récurrence une opération E de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$ convenable, et définir l'égalité, par : $E(n, m) = 0$. Ce point de vue est

²⁴ L'identité de deux procédures de calcul est une chose quasiment impossible à définir en dehors d'un système formel d'écritures qui formalisent certaines procédures de calcul, (par exemple les calculs récursifs) selon des codifications qui ne peuvent que comporter une grande part d'arbitraire. En conséquence la notion d'égalité purement intentionnelle entre opérations de $\mathbb{N}$ vers $\mathbb{N}$ n'est pas très réaliste. Néanmoins, en face de la notion d'égalité purement extensionnelle, on peut imaginer différents degrés d'intentionnalité pour différentes relations d'égalité.

²⁵ extensionnel est dit par opposition à "intentionnel" : "deux" objets sont "intentionnellement égaux" lorsqu'ils sont donnés comme le même objet

peut-être plus proche de la pratique : la comparaison du nombre de billes dans deux boîtes ne résulte généralement pas d'un simple constat. Par ailleurs et a contrario, quand deux entiers naturels (qui peuvent résulter de calculs différents) ont été ramenés à leur forme d'entiers naturels "à l'état pur", c.-à-d. comme successeurs itérés de 0, alors leur égalité n'est rien d'autre que leur identité.

5b) Ensembles

Le slogan de Bishop (cf. [Bis] ou [BB]) est qu'un ensemble est bien défini constructivement lorsqu'on sait ce qu'il faut faire pour construire un élément arbitraire de cet ensemble, et ce qu'il faut faire pour démontrer que deux éléments de cet ensemble sont égaux.

Avec les notions que nous avons développées jusqu'à présent, cela signifie qu'un ensemble est constructivement défini par la donnée d'un type (légitime) d'objets et la définition d'une relation d'égalité.

Une conception relativement prudente, mais rassurons nous, tout à fait efficace, de la notion d'ensemble "constructif" sera donc la suivante : un ensemble E est donné par :

- un type X_E ,
- une relation binaire pour les objets de ce type, notée $x =_E y$, et
- une preuve que cette relation binaire $x =_E y$ est bien une relation d'équivalence

Cette notion d'ensemble renvoie donc aux notions de type⁽²⁶⁾ et de propriété, plus fondamentales.

Par exemple l'ensemble des nombres réels est formé à partir du type «suites de rationnels de Cauchy» et de la relation d'égalité convenablement définie.

Quant à l'ensemble des entiers naturels, il n'est pas vraiment distinct de son type sous-jacent $\mathbb{N}$ puisque la relation d'égalité entre entiers naturels est considérée comme "primitive" (au même titre que les entiers naturels).

Par rapport aux ensembles des mathématiques classiques, il y a au moins deux différences de points de vue importantes. La première est qu'un ensemble constructif est toujours⁽²⁷⁾ obtenu comme résultat d'une série de descriptions précises (qui permettent de définir le type et la relation d'égalité) et de constructions (qui permettent de prouver que la relation d'égalité est une relation d'équivalence). La deuxième est que l'appartenance d'un objet à un ensemble n'est pas un fait brut et éternel, mais est directement dépendant d'une preuve donc d'une construction.

Tout ensemble constructif arrive donc sur la scène mathématique sous forme relativement concrète : c'est un ensemble classique avec une "présentation". Dans la présentation de l'ensemble, la preuve du fait que la relation d'égalité est une relation d'équivalence est en général omise. Et deux ensembles dont les présentations ne diffèrent que sur la preuve en question sont considérés comme «les mêmes». Mais même si la preuve n'est pas mentionnée, elle doit être disponible quelque part.

Le produit cartésien de deux ensembles est une notion claire : le produit de l'ensemble $E = (X_E, =_E)$ et de l'ensemble $F = (X_F, =_F)$ est l'ensemble $G = (X_E \times X_F, =_G)$ avec la relation $(x, y) =_G (x', y')$ définie comme signifiant : $x =_E x'$ et $y =_F y'$. On notera $E \times F$ l'ensemble ainsi obtenu (malgré l'ambiguïté avec le produit cartésien de deux types).

²⁶ Bishop parle de préensemble plutôt que de type

²⁷ sauf pour les ensembles les plus élémentaires, comme l'ensemble des entiers naturels, car il est impossible de bâtir quoique ce soit sur du vide, malgré les illusions d'optique créées par la théorie des ensembles classiques dans sa forme la plus achevée «à la Zermelo-Frankel»

5c) Fonctions

Considérons un ensemble $E = (X_E, =_E)$, un ensemble $F = (X_F, =_F)$, et une opération f de X vers X_F . On dira que cette opération est extensionnelle (pour $=_E$ et $=_F$) si on a :

$$- \quad \forall x \in X_E, \forall x' \in X_E, x =_E x' \Rightarrow f(x) =_F f(x')$$

On voit donc que le type "opérations extensionnelles de E vers F " est un type bien défini.

On peut faire de ce type un ensemble $G = \mathcal{F}(E, F)$ en adoptant la définition d'égalité extensionnelle entre opérations :

$$- \quad f =_G g \text{ signifie : } \forall x \in X_E \quad f(x) =_F g(x)$$

Bien que des raffinements de la notion constructive de fonction puissent être imaginés (cf. [Bee] et la note ci-après), on peut en général s'en tenir à la convention selon laquelle toute fonction doit être définie à partir d'une opération entre les types sous-jacents, ce que nous ferons désormais. Donc l'ensemble $\mathcal{F}(E, F)$ défini ci-dessus sera considéré comme l'ensemble des fonctions de E vers F .⁽²⁸⁾

Essayons de préciser les choses avec quelques exemples.

Vu le caractère a priori de l'égalité entre entiers naturels, toute opération de $\mathbb{N}$ vers $\mathbb{N}$ est une fonction. L'ensemble $\mathcal{F}(\mathbb{N}, \mathbb{N})$ est donc formé sur le type $(\mathbb{N} \rightarrow \mathbb{N})$ avec pour relation d'égalité l'égalité extensionnelle.

Revenons à l'ensemble $\mathbb{R}$ des nombres réels. Son type sous-jacent est le type $SC(\mathbb{N}, \mathbb{Q})$ des opérations de $\mathbb{N}$ vers $\mathbb{Q}$ vérifiant le critère de Cauchy, mais sa relation d'égalité est plus grossière que l'égalité extensionnelle entre suites de rationnels⁽²⁹⁾.

A partir de l'ensemble $\mathbb{R}$ on peut définir l'ensemble des fonctions réelles $\mathcal{F}(\mathbb{R}, \mathbb{R})$. Voici comment. Le type sous-jacent est le type des opérations de $SC(\mathbb{N}, \mathbb{Q})$ vers $SC(\mathbb{N}, \mathbb{Q})$ qui sont extensionnelles pour l'égalité entre réels $=_{\mathbb{R}}$. Qu'est-ce qu'une opération de $SC(\mathbb{N}, \mathbb{Q})$ vers $SC(\mathbb{N}, \mathbb{Q})$? C'est une construction qui prend en entrée un élément de $(\mathbb{N} \rightarrow \mathbb{Q})$ et qui pour fonctionner peut utiliser le fait que la suite de rationnels considérée est de Cauchy. En sortie, cette opération fournit un élément de $SC(\mathbb{N}, \mathbb{Q})$, c.-à-d. un élément de $(\mathbb{N} \rightarrow \mathbb{Q})$ avec une preuve qu'il s'agit bien d'une suite de Cauchy.

Ici l'auteur et la lectrice (ou le lecteur) commencent à avoir mal à la tête. Aussi l'auteur tient à se rassurer lui-même et à rassurer si possible la lectrice : l'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ n'a pratiquement aucun intérêt mathématique, et aucune activité mathématique productive ne semble jamais avoir été basée sur la considération d'ensembles aussi compliqués. L'ensemble des fonctions réelles

²⁸ A strictement parler, on a plutôt défini l'ensemble des opérations extensionnelles de E vers F ; on peut imaginer en effet que la construction qui permet de passer de x à $f(x)$ dépende non seulement de l'objet x lui-même, mais aussi de la preuve que $x \in X_E$, et certaines fonctions, malgré leur caractère extensionnel, ne pourraient alors pas être définies en tant qu'opérations portant sur les types sous-jacents. Mais ce raffinement, même s'il est légitime, ne semble pas avoir de conséquence mathématique réellement significative, et nous nous en passerons.

²⁹ On peut calquer la terminologie classique et dire que $\mathbb{R}$ est un ensemble quotient de l'ensemble des suites de Cauchy de rationnels. Mais en mathématiques constructives on ne prétend pas manipuler des classes d'équivalences en tant que telles, qui sont à vrai dire des "objets" bien encombrants. Tout réel est représenté par une suite de Cauchy, et comme il est impossible de définir un représentant canonique dans la classe d'équivalence, il n'y a pas moyen en mathématiques constructives d'identifier un réel avec un objet de structure simple. Cela ne contredit pas le caractère relativement simple de l'ensemble $\mathbb{R}$. C'est uniquement le mythe de l'égalité comme identité (deux réels classiques, eux, sont bien égaux si et seulement si ils sont identiques) qui a conduit à préférer le concept d'ensemble quotient comme ensemble de classes d'équivalence, à celui d'ensemble quotient comme relâchement de la relation d'égalité, sans modification des objets. Pour Gauss, les entiers modulo p n'existaient pas comme objets distincts des entiers naturels, et l'étude des entiers modulo p n'est rien d'autre que l'étude des congruences modulo p sur les entiers naturels.

continues, l'ensemble des fonctions réelles analytiques, l'ensemble des fonctions réelles indéfiniment dérivables, ou l'espace des fonctions réelles de carré sommable, qui sont, eux, des ensembles utiles et significatifs, ont une structure beaucoup plus simple que cet extraordinaire ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ cher à Cantor. Ce sont des espaces métriques séparables complets, c.-à-d. que leur structure n'est pas plus compliquée que celle de $\mathbb{R}$ (voir infra). L'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ des mathématiques classiques est à vrai dire encore beaucoup plus compliqué et certainement plus mystérieux que celui que nous avons décrit (dans lequel les fonctions non continues ont beaucoup de mal à entrer), mais son utilité comme fourre-tout n'a-t-elle pas été détronée depuis un certain temps par l'ensemble des distributions réelles (toute fonction ne définit pas une distribution, et vice versa, mais le fourre-tout des distributions est bien plus significatif que celui des fonctions).

5d) Propriétés “concernant les objets d'un ensemble”

Étant donné un ensemble $E = (X_E, =_E)$ une propriété $P(x)$ concernant une variable x de type X_E sera dite : concerner les objets de l'ensemble E si on a :

- $\forall x \in X_E, \forall x' \in X_E, x =_E x' \Rightarrow (P(x) \Leftrightarrow P(x'))$

On dit encore que la propriété $P(x)$ définie pour les objets de type X_E est cohérente avec la relation d'égalité $=_E$. En mathématique classique on dirait que la propriété $P(x)$ passe au quotient.

Par exemple, dire qu'une opération f de X_E vers X_F est extensionnelle (paragraphe précédent) signifie que la propriété $y =_F f(x)$ concerne l'objet x de l'ensemble E .

Un exemple important est la relation d'inégalité (positive) dans l'ensemble $G = \mathcal{F}(\mathbb{N}, \mathbb{N})$. Étant données deux suites d'entiers $u = (u_n)$ et $v = (v_n)$ la relation $u \neq_G v$ signifie par définition :

- $\exists n \in \mathbb{N} \quad u_n \neq v_n$

Cette relation d'inégalité concerne bien les éléments de $\mathcal{F}(\mathbb{N}, \mathbb{N})$. En outre

- $\neq_G$ est symétrique : $x \neq_G y \Rightarrow y \neq_G x$
- $\neq_G$ est cotransitive forte : $x \neq_G y \Rightarrow (x \neq_G z \text{ ou } y \neq_G z)$
- $\neq_G$ est de caractère positif (sa vérité résulte d'un simple calcul)
- $=_G$ est équivalente à la négation de $\neq_G$

Les ensembles munis d'une relation d'inégalité vérifiant ces propriétés sont relativement agréables à utiliser d'un point de vue constructif. Parmi ceux-ci, il y a l'ensemble des réels et plus généralement les espaces métriques séparables complets.

5e) Espaces métriques séparables complets

Constructivement un espace métrique séparable complet M est donné par :

- un ensemble énumérable E_M (c.-à-d. un ensemble E_M et une fonction surjective de $\mathbb{N}$ sur E_M) qu'on peut voir comme l'ensemble des points rationnels de M
- un écart défini sur E_M c.-à-d. une fonction $d_M : E_M \times E_M \rightarrow \mathbb{R}^{\geq 0}$ vérifiant les propriétés usuelles de symétrie et d'inégalité triangulaire.

Le type sous-jacent à l'ensemble M est alors le type des suites de points rationnels

$$(x_n) \in (\mathbb{N} \rightarrow E_M) \quad (30)$$

³⁰ Comme l'ensemble E_M est énumérable, les êtres mathématiques permettant de définir les points de l'espace M peuvent être vus comme des suites d'entiers. Ainsi les objets de base des mathématiques usuelles sont basés sur le seul type $\mathbb{N}^{\mathbb{N}}$.

qui sont des suites de Cauchy. En pratique on peut se limiter à celles vérifiant un critère de convergence "géométrique" :

- $\forall n \in \mathbb{N} \quad d_M(x_n, x_{n+1}) < 1/2^n$

On définit alors une inégalité et une égalité sur M par :

- $(x_n) \neq_M (y_n)$ signifie $\exists n \, d_M(x_n, y_n) > 1/2^{n-1}$, et $x =_M y$ signifie $\neg x \neq_M y$

On montre qu'on peut prolonger par continuité l'écart d_M défini sur E_M et on obtient une distance, encore notée d_M , définie sur M .

On peut rendre compte de cette manière de la plupart des espaces manipulés en analyse et donner un contenu constructif à l'analyse enseignée à l'université.

5f) Et l'axiome du choix ?

Un énoncé équivalent à l'axiome du choix classique est le suivant :

- si on a deux ensembles X et Y et une fonction surjective f de X sur Y alors il existe une fonction g de Y vers X telle que $f \circ g = \text{Id}_Y$

Il résulte immédiatement des définitions données jusqu'à maintenant que l'axiome du choix est valable sous la forme suivante en mathématiques constructives :

- si on a deux types X et Y et une opération surjective f de X sur Y alors il existe une opération g de Y vers X telle que $f \circ g = \text{Id}_Y$

Le problème avec l'axiome du choix est lorsqu'on demande qu'une opération réalisant certains buts puisse être remplacée par une fonction, c.-à-d. qu'elle ait un caractère extensionnel. Par exemple, pour tout réel x il existe un entier naturel m tel que $x < m$. Cela signifie constructivement que, à partir d'une suite de Cauchy de rationnels (rappelons nous que le fait d'être une suite de Cauchy, puisqu'il est affirmé, est explicitable), on pourra construire un entier m strictement supérieur à sa limite. Cette opération $(x_n) \mapsto m$ n'offre aucune difficulté, mais on ne sait pas la remplacer par une fonction qui réaliserait les mêmes objectifs (car les seules fonctions de $\mathbb{R}$ vers $\mathbb{N}$ qu'on sache construire sont les fonctions constantes).

J'entends déjà des soupirs de désespoir : est-il vraiment possible de faire des mathématiques sans disposer de la fonction «partie entière» sur les réels ? La réponse est bien simplement «oui». Si on a besoin d'avoir un entier qui minore le réel x on sait le faire sans le secours de cette fonction. Et si on a besoin de la fonction elle-même (pas seulement d'une opération), en général c'est sous la forme «la fonction partie entière en tant qu'élément de tel ou tel espace fonctionnel», mais alors justement, peu importe que la fonction soit partout définie, et il est bien clair que la fonction partie entière est, constructivement, presque partout définie.

Très brève conclusion

Nous terminerons ici notre présentation des mathématiques constructives, en ayant l'espoir d'avoir suscité la curiosité de la lectrice. Si notre but est atteint nous espérons pour elle qu'elle lit bien l'anglais mathématique et qu'elle a facilement accès à des bibliothèques universitaires, ce qui lui permettra, peut être, de prendre connaissance de quelques textes de base signalés dans la bibliographie.

Signalons qu'aucun éditeur scientifique de langue française contacté à ce jour (tous conseillés par d'éminents mathématiciens, en général bourbakistes³¹) ne semble intéressé par le projet d'une édition en français du texte fondateur de Bishop.

³¹ Il ne faut quand même pas désespérer. Les éditions Hermann ont fini par accepter en 1984 de publier une traduction française de "Preuves et Réfutations" de I. Lakatos, un des socles de l'épistémologie contemporaine des mathématiques, ... mais l'épistémologie de Lakatos n'étant pas celle de Bourbaki, il a fallu patienter très très longtemps

Bibliographie

livres

- [Abe] Aberth O. : *Computable Analysis* (1980) McGraw Hill.
(c'est écrit dans l'esprit de l'école constructiviste russe)
- [Bee] Beeson M. J. : *Foundations of Constructive Mathematics* (1985) Springer
(c'est un livre de logique) . On pourra aussi consulter dans la brochure Epiphymat de Besançon (1992), la traduction légèrement abrégée, par H. Lombardi, d'un article de M. Beeson : "principes problématiques en mathématiques constructives".
- [Bis] Bishop Erret : *Foundations of Constructive Analysis* (1967) McGraw Hill (épuisé)
- [BB] Bishop E., Bridges D. : *Constructive Analysis*. (Springer-Verlag; 1985)
- [BR] Bridges D., Richman F. : *Varieties of Constructive Mathematics*. London Math. Soc. LNS 97. Cambridge University Press (1987)
(comparaison dans la pratique des trois principales tendances du constructivisme)
- [Bro] Brouwer : *Brouwer's Cambridge Lectures on Intuitionism* (Van Dalen ed.) (1981) Cambridge University Press.
- [GGNN] Girard J.-Y., Gödel K., Nagel, Newman : *Le théorème de Gödel* . Sources de savoir. Seuil. (1989)
- [Hey] Heyting A. : *Intuitionism*. 1966. Amsterdam. NorthHolland
- [K11] S. C. Kleene. *Introduction to Metamathematics* (Van Nostrand; 1952)
- [K12] S. C. Kleene. *Logique mathématique* (Dunod, 1970)
- [Kus1] Kushner B. A. *Constructive real numbers and constructive function spaces*
Translation of Mathematical Monographs (traduit du russe) American Mathematical Society Vol. 21. 1968.
- [Kus2] Kushner B. A. : *Lectures on Constructive Mathematical Analysis* (traduit du russe en 1985) dans la série: Translations of the A.M.S.
- [Kri] Krivine A. : *Théorie des Ensembles*. Collection SUP des PUF.
- [Lak] Lakatos I. : *Preuves et Réfutations* . Hermann 1984
- [MRR] Mines R., Richman F., Ruitenburg W. : *A Course in Constructive Algebra*. Springer-Verlag. Universitext. 1988.
- Collectif : *"Penser les mathématiques"* - Collection Seuil Points.
On comparera avec intérêt les articles de Dieudonné et de Apéry. Une bibliographie assez complète se trouve à la fin de l'article d'Apéry.

articles, brochures

- [Apé] Apéry R. : article à lire dans "Penser les mathématiques" (collection Seuil Points Sciences)

Notes sur le formalisme en mathématiques

Introduction	39
A Le langage de l'arithmétique, les axiomes de Peano, le modèle standard	41
A1 Le langage de l'arithmétique.....	41
A2 Une interprétation (ou réalisation) du langage $\mathcal{L}_A$	42
A3 Les axiomes et les modèles du système formel Peano.....	43
A4 Utilité et limites du langage $\mathcal{L}_A$ pour étudier les propriétés des entiers naturels.....	44
B Première discussion sur la notion de vérité en mathématiques, à travers l'exemple des entiers naturels.....	45
B1 Objection intuitionniste.....	45
B2 Pour contourner cette objection des intuitionnistes, il peut exister deux attitudes possibles	46
B3 Description rapide (et informelle) de la théorie formelle "arithmétique de Peano"	47
B4 Les règles de la logique formelle (pour un langage du premier ordre) sont "entièrement satisfaisantes" du point de vue classique (théorème de complétude de Gödel).....	48
C Les problèmes posés par la formalisation de la théorie des ensembles et par la théorie des ensembles elle-même.....	49
C1 Deux actes de foi de la théorie des ensembles.....	49
C2 À propos des modèles réduits arithmétiques de l'Univers à la Cantor-Zermelo-Fraenkel.....	51
D L'insuffisance fondamentale des systèmes formels.....	54
D1 Arithmétisation d'une théorie formelle du premier ordre.....	54
D2 Le théorème d'incomplétude de Gödel.....	56
D3 Propriétés arithmétiques qu'on ne démontrera jamais ?.....	58
D4 Non définissabilité de la vérité (d'un langage par ce langage).....	59
E Remarques sur le programme de Hilbert.....	60
E1 Évolution du programme de Hilbert.....	60
E2 Le programme de Hilbert pour l'arithmétique de Peano	61
E3 Vérité des résultats d'arithmétique établis au moyen des axiomes de ZF ?	62
F Quelques conclusions.....	64
Annexe 1 Les axiomes de $\mathcal{GB}$	66
Annexe 2 Traduction de l'arithmétique de Peano dans le langage $\mathcal{L}_E$ de la théorie des ensembles	68
Annexe 3 Traduction de l'arithmétique de Peano dans une autre théorie formelle	69
Annexe 4 Un autre modèle remarquable de $\mathcal{GB}$	70

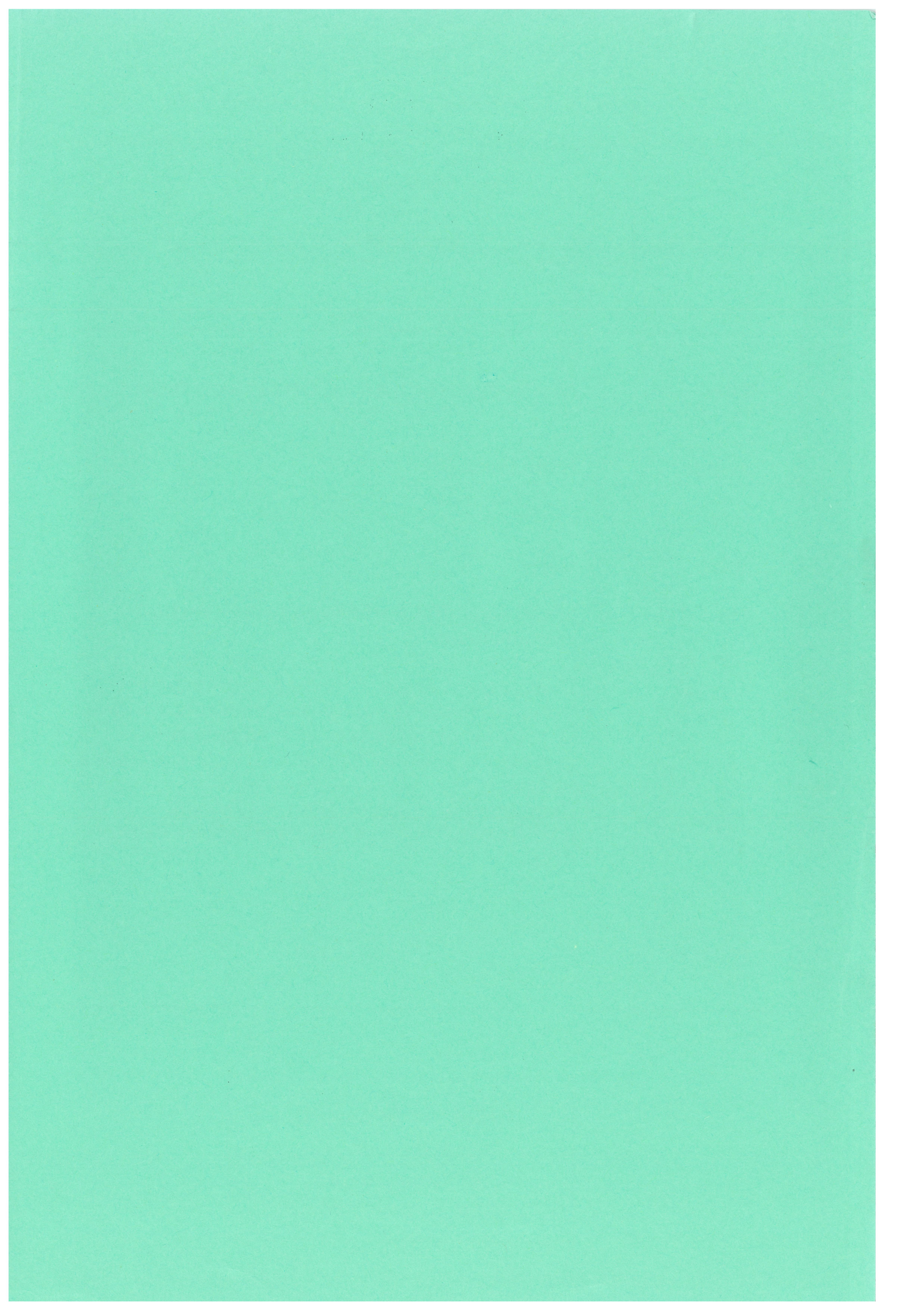
Quelques principes de travail

Introduction.....	71
1) Tous les objets doivent être construits.....	72
1a) Les entiers naturels.....	72
1a') Autres types élémentaires.....	73
1b) Couples d'objets.....	73
1c) Opérations de A vers B	74
1d) Objets d'un certain type vérifiant une certaine propriété.....	75
2) Affirmer, c'est démontrer.....	76
2a) Propriétés dont la vérité résulte d'un constat.....	77
2b) Les connecteurs "Et" et "Ou"	78
2c) "Il existe un objet de type A vérifiant la propriété P".....	79
2d) "Pour tout entier n la propriété P est vraie".....	79
2e) "La propriété P implique la propriété Q".....	80
2f) La négation : "La propriété P est absurde".....	81
2g) Pour tout objet x de type A, la propriété P(x) est vraie	82
2h) Conclusion provisoire sur ce qu'est une propriété :.....	82
2i) Exercices de raisonnements constructifs.....	82
3) Exemples caractéristiques de divergences entre logique classique et logique constructive.....	83
3a) Principes d'omniscience.....	84
3b) Le principe de Markov.....	85
3c) Quelques comparaisons entre la logique formelle classique et la logique formelle constructive.....	85
4) Démonstrations et constructions par induction	87
4a) Construction par récurrence.....	87
4b) Démonstration par récurrence.....	88
4c) Induction pour d'autres types élémentaires.....	88
4d) Preuves par induction pour des types construits.....	88
4e) Constructions de type par induction.....	89
5) Ensembles, égalités, fonctions, espaces métriques complets.....	90
5a) L'égalité doit en général être définie.....	90
5b) Ensembles.....	91
5c) Fonctions.....	92
5d) Propriétés "concernant les objets d'un ensemble".....	93
5e) Espaces métriques séparables complets.....	93
5f) Et l'axiome du choix ?.....	94
Très brève conclusion	95

Bibliographie

97

IREM de LYON
BIBLIOTHEQUE
Université Claude Bernard -LYON I
43, Bd du 11 Novembre 1918
69622 VILLEURBANNE Cedex



I.R.E.M - FACULTE DES SCIENCES -
LA BOULOIE - ROUTE DE GRAY
25030 BESANÇON CEDEX
tél 81 66 61 92
fax 81 66 61 99

Titre **Mathématiques Constructives**

Auteur **Henri Lombardi**

Public **s'intéressant aux mathématiques**

Date **mai 94**

Mots clés **effectivité, infini mathématique, tiers exclu, épistémologie**

Résumé **Dans ce texte, on présente cinq études séparées autour du thème des mathématiques constructives. Le point de vue actuellement dominant en mathématiques, celui de l'infini actuel, est soumis à la critique. La question de la signification des énoncés mathématiques occupe une place centrale dans ce débat.**

FORMAT **A4** **pages 100**

IREM de Besançon.

Dépôt légal 88-94

2^{ème} trimestre 94

ISBN 2-909963-70-5