Le mystère de la structure du continu

Lombardi Henri

12 juin 2012

Colloque *Des Nombres et des Mondes.*
En hommage à Guy Wallet,
à l'occasion de son départ en retraite.

Résumé

Dans le cadre du colloque « Des Nombres et des Mondes », et en hommage aux recherches de Guy Wallet sur la question, on évoque le mystère de la structure du continu. Pour soulever un coin du voile, on propose d'essayer de mieux comprendre l'algèbre réelle, quand les nombres réels sont vus d'un point de vue constructif.

1 L'invention de la droite réelle par Cantor et Dedekind

Les mathématiques ont longtemps été vues comme une « théorie des grandeurs ».

Le grec Eudoxe avait mis au point une théorie des « rapports de grandeur » qui évitait de nommer ces rapports comme des nombres. Deux grandeurs du même type (deux longueurs, ou deux aires par exemple) devaient pouvoir être comparées d'une part, et additionnées d'autre part.

Eudoxe disait que « A est à B comme A' est à B' » lorsque pour tous entiers m et n, si $mA > nB$ alors $mA' > nB'$, et la même chose en remplaçant le symbole $>$ par $=$ ou $<$. En outre on avait besoin d'un « axiome d'Archimède » disant que pour deux grandeurs de même nature, la plus petite, additionnée un nombre suffisant de fois à elle-même, finissait toujours par dépasser la plus grande.

En conséquence, la relation d'égalité (de deux rapports) ne pouvait que rarement être constatée, et devait en général être démontrée par « une double réduction à l'absurde ».

Avec le développement des calculs, des nombres réels « de fait » (i.e., pas « de droit » puisqu'aucune définition n'en avait été donnée) ont été utilisés de plus en plus librement. On aboutit à une simplification et algorithmisation des fabuleuses démonstrations des Grecs (on parlait du divin Archimède) par le développement du calcul infinitésimal.

Mais les infinitésimaux n'avaient pas un statut suffisamment clair et le 19^{e} siècle a essayé de s'en débarrasser. Cauchy basa son « analyse algébrique » sur la notion de suite convergente et énonça son fameux critère pour la convergence d'une série. Cela ne faisait pas une définition des nombres réels pour autant, et il n'établissait aucun lien direct entre ce critère et la formulation d'Eudoxe.

Il fallut que Cantor brise le tabou des ensembles infinis pour que l'on en vienne à oser donner une définition de ce qu'était un nombre réel.

Ce furent Cantor et Dedekind qui osèrent franchir le Rubicon, chacun avec sa défintion propre.

Dedekind procéda pour les nombres réels comme il procéda pour les (nombres) idéaux de Kummer : il remplaça une phrase par le nom de la phrase.

En termes plus savants et moins provocateurs, il remplaça un prédicat par son extension.

Dans certains « anneaux de nombres » (en particulier dans $\mathbb{Z}[\zeta_n]$, où ζ_n est une racine primitive n-ème de l'unité), Kummer, constatant que deux éléments pouvaient avoir deux décompositions distinctes en produits de facteurs irréductibles, inventa un calcul sur des « nombres idéaux », introduits comme pgcd idéaux de vrais nombres. Kummer ne pouvait pas additionner ces nombres idéaux, mais il savait les multiplier et obtenait ainsi une théorie de la divisibilité dans laquelle il retrouvait le pgcd, le ppcm, ainsi que l'existence et l'unicité de la décomposition en facteurs premiers. Une propriété caractérisant le nombre idéal « pgcd de $(x_1, \ldots, x_n)$ » était que les nombres usuels (ceux de l'anneau d'entiers) multiples de ce pgcd étaient exactement les combinaisons linéaires $\sum_i x_i y_i$ (comme dans $\mathbb{Z}$, où tous les nombres idéaux sont de vrais nombres).

Dedekind décida de remplacer le prédicat

$$\text{« } z \text{ est multiple du pgcd idéal de } (x_1, \ldots, x_n) \text{ »}$$

qui servait à caractériser le nombre idéal de Kummer, par l'extension de ce prédicat, c'est-à-dire

$$\text{« l'ensemble des } z \text{ qui sont multiples du pgcd idéal de } (x_1, \ldots, x_n). \text{ »}$$

Ce qui lui semblait une notion imparfaite devint ainsi une notion parfaite, par la magie d'avoir osé « nommer » un ensemble infini, et d'avoir décidé que les ensembles infinis sont des objets mathématiques acceptables[1].

Concernant les nombres réels, Dedekind fit avec Eudoxe (pour ses rapports de grandeurs) ce qu'il fit avec Kummer (pour ses nombres idéaux). Il explicita le concept sous-jacent à la définition d'Eudoxe et le traduisit en un ensemble infini (ou plutôt une paire d'ensembles infinis). Puisqu'un rapport de grandeur A/B est caractérisé par les nombres rationnels qui lui sont strictement supérieurs (les n/m tels que $mA < nB$) et ceux qui lui sont strictement inférieurs (les n'/m' tels que $m'A > n'B$), Dedekind remplaça la notion imparfaite de rapport de grandeurs par la notion parfaite de « coupure » qui est l'extension du prédicat d'Eudoxe.

La coupure correspondant au rapport de grandeur non nommé x chez Eudoxe, ce n'était rien d'autre que la partition correspondante l'ensemble de tous les rationnels en deux parties, la partie inférieure, et la partie supérieure

$$\big(\{\, \tfrac{n}{m} \in \mathbb{Q} \;\big|\; \tfrac{n}{m} \leqslant x \,\}, \{\, \tfrac{n}{m} \in \mathbb{Q} \;\big|\; \tfrac{n}{m} > x \,\}\big).$$

La différence avec les nombres idéaux de Kummer, c'est que ces derniers avaient été nommés par Kummer, tandis qu'Eudoxe ne nomma jamais un nombre réel. Ainsi, Dedekind faisait vraiment preuve d'invention : il inventait une définition pour tous les nombres réels. Pour tous les nombres réels, passés et à venir en quelque sorte[2].

Dans sa fierté d'avoir donné un statut plus clair aux nombres réels, Dedekind prétendit même être le premier à donner une démonstration rigoureuse de l'égalité $\sqrt{2}\,\sqrt{3} = \sqrt{6}$.

1. Un dommage collatéral fut que désormais un pgcd idéal dépendait de l'anneau de nombres où on le considérait, contrairement au pgcd idéal de Kummer.

2. C'est ce qui fait qu'aujourd'hui, la majorité des mathématiciens, ceux qui considèrent que la vérité absolue des énoncés concernant les nombres réels a un statut objectif, considèrent de la même manière qu'il existe un seul ensemble $\mathbb{R}$, « engendré non pas créé » et que l'esprit sain des mathématiques procède de manière égale du père ($\mathbb{N}$) et du fils ($\mathbb{R}$).

Égalité pourtant dont la paraphrase euclidienne (comparaison des aires de deux rectangles) n'aurait naturellement pas résisté à Archimède, expert en doubles réductions à l'absurde (dans ce cas, la double réduction à l'absurde sera une copie conforme de la démonstration de Dedekind).

Cantor proposa une définition alternative, dans laquelle un nombre réel est une classe d'équivalence de suites de Cauchy de nombres rationnels, autrement dit un ensemble infini (non dénombrable) d'ensembles infinis (dénombrables).

L'appréciation de Poincaré

Après avoir expliqué que les nombres réels ont servi à remplir les trous que l'on trouvait dans la droite rationnelle. Poincaré conclut sa description par l'appréciation suivante.

« Avant d'aller plus loin, faisons une première remarque. Le continu ainsi conçu n'est plus qu'une collection d'individus rangés dans un certain ordre, en nombre infini, il est vrai, mais *extérieurs* les uns aux autres. Ce n'est pas là la conception ordinaire, où l'on suppose entre les éléments du continu une sorte de lien intime qui en fait un tout, où le point ne préexiste pas à la ligne, mais la ligne au point. De la célèbre formule, le continu est l'unité dans la multiplicité, la multiplicité seule subsiste, l'unité a disparu. Les analystes n'en ont pas moins raison de définir leur continu comme ils le font, puisque c'est toujours sur celui-là qu'ils raisonnent depuis qu'ils se piquent de rigueur. Mais c'est assez pour nous avertir que le véritable continu mathématique est tout autre chose que celui des physiciens et celui des métaphysiciens. »

La Science et l'Hypothèse. Chapitre II. La grandeur mathématique et l'expérience.

La physique contemporaine et l'infiniment petit

Depuis la mécanique quantique, il semble difficile d'accorder foi à des grandeurs d'espace, de temps, ou de masse qui seraient trop petites, comme 10^{-50} cm. Même si le temps et l'espace ne sont pas quantifiés dans la théorie, le fait de représenter le temps et l'espace par des êtres mathématiques indéfiniment divisibles (comme le sont les segments de la droite réelle) suscite un profond scepticisme. L'intuition du continu à laquelle se réfère Poincaré est peut-être seulement une propriété de notre cerveau, de notre manière de raisonner intuitivement, et elle pourrait n'avoir aucun rapport avec la réalité physique.

Néanmoins, les réels (à la Cauchy ou à la Dedekind) sont les objets de base de l'analyse mathématique. Et l'analyse mathématique s'est révélée d'une efficacité remarquable dans la modélisation du monde physique.

C'est là sans doute un des principaux mystères du continu mathématique. Nous ne pouvons pas savoir s'il sera résolu un jour, ni deviner dans quelle direction.

Dans la suite de l'article, je me consacre uniquement aux mystères du continu mathématique en tant que tel (sans la question de son rapport avec la physique mathématique).

2 Quelques difficultés du continu mathématique dans son acception usuelle

L'analyse traitée de manière usuelle, avec la logique classique du tiers exclu, conduit à un certain nombre de faits contre-intuitifs, qui sont usuellement acceptés parce qu'on a perdu l'habitude de discuter les questions concernant les fondements.

Des théorèmes au contenu étrange, difficile à cerner

Un théorème part d'une hypothèse pour arriver à une conclusion. Il est utile dans la mesure où il nous fait découvrir une propriété qui a le caractère d'une vraie nouveauté par rapport à l'hypothèse.

Par exemple le théorème de Cayley-Hamilton prédit le résultat d'un calcul compliqué fait avec une matrice carrée à coefficients dans un anneau commutatif.

Un théorème qui décrit la répartition des nombres premiers, s'il est suffisamment précis, nous donne un encadrement a priori insoupçonnable, pour le nombre de nombres premiers inférieurs à un entier N au moyen d'une formule unique, simple, valable pour tout entier N supérieur à une valeur donnée.

En analyse, le théorème des accroissements finis, convenablement formulé, donne aussi accès à un résultat général qui, parce qu'intuitif, nous rassure quant aux choix qui ont été faits pour définir les objets de bases (nombres réels, fonctions continument dérivables).

En analyse classique, il arrive pourtant fréquemment que l'on ne sache pas certifier l'hypothèse[3] d'un théorème autrement que par sa conclusion. Un tel théorème, profondément inutile, devrait poser problème. L'hypothèse, très abstraite, semble impossible à maitriser, sauf sous la forme de la conclusion, beaucoup plus « concrète ».

Prenons par exemple le théorème suivant.

Théorème 1. *Une fonction réelle f continue en tout point d'un intervalle fermé borné $I = [a, b]$ est uniformément continue*

Nous demandons ici au lecteur de bien vouloir oublier un moment ce qui lui semble évident concernant les nombres réels et de ne plus les considérer qu'avec un certain recul, comme donnés par des suites de Cauchy de rationnels. Et pour un nombre réel arbitraire, on n'a aucune raison de connaître très précisément le comportement à l'infini de la suite de Cauchy qui le définit.

Notons pour commencer que la notion de continuité de la fonction f en un point $x \in I$ est une notion « assez compliquée » qui s'explicite au moyen de deux quantificateurs portant sur des entiers naturels, et un quantificateur portant sur les nombres réels :

$$\forall m \in \mathbb{N}, \exists n \in \mathbb{N}, \forall x' \in I, \quad |x' - x| < \tfrac{1}{2^n} \Rightarrow |f(x') - f(x)| < \tfrac{1}{2^m}.$$

Néanmoins, ce n'est « pas trop compliqué » car l'entier n doit être donné à partir de l'entier m seulement.

Maintenant, regardons l'hypothèse du théorème. Elle se formule avec un quantificateur de plus, portant sur les nombres réels, qui crée un complication terrible.

$$\forall x \in I, \forall m \in \mathbb{N}, \exists n \in \mathbb{N}, \forall x' \in I, \quad |x' - x| < \tfrac{1}{2^n} \Rightarrow |f(x') - f(x)| < \tfrac{1}{2^m}.$$

En effet, comment une telle hypothèse peut-elle être donnée et certifiée ?
Il nous faut :

- d'une part une procédure qui calcule, pour un nombre réel arbitraire de l'intervalle, disons x, son image $f(x)$,
- et d'autre part quelque chose qui nous garantit aussi la continuité de la fonction en tout point de l'intervalle.

3. Nous entendons par là que dans un contexte donné, au moment d'appliquer le théorème, il faut être certain que l'hypothèse est satisfaite. Mais comment en être certain, sinon grâce à la donnée de « quelque chose » dans le contexte qui emporte la conviction ? C'est ce que nous appelons certifier l'hypothèse. Certaines hypothèses ne posent manifestement pas de problème de certificat, par exemple lorsque l'on dit « Soient deux entiers m et n strictement positifs et premiers entre eux. ». En analyse par contre, il est souvent légitime de se poser la question de l'existence d'un certificat.

La première procédure est déjà difficile à imaginer sans l'hypothèse de continuité uniforme, car x est a priori donné par une suite de rationnels $(r_n)_{n\in\mathbb{N}}$ satisfaisant le critère de Cauchy sous la forme $|r_n - r_m| < \frac{1}{2^n} + \frac{1}{2^m}$ pour tous $m, n \in \mathbb{N}$. La valeur $f(x)$ doit être donnée sous la même forme, et le calcul doit respecter l'égalité des réels : si deux suites de Cauchy donnent le même réel x, les deux suites calculées pour $f(x)$ doivent donner le même réel y.

Avec l'hypothèse que f est ponctuellement continue, les choses sont cependant un peu plus faciles. Il suffit alors

- de donner pour chaque nombre rationnel r de l'intervalle la valeur $f(r)$, calculée avec la suite de Cauchy constante, d'une part,
- de préciser pour chaque réel x de l'intervalle la « vitesse de convergence » de $f(r_n)$ vers $f(x)$ lorsque (r_n) est une suite de Cauchy (avec $|r_n - r_m| < \frac{1}{2^n} + \frac{1}{2^m}$ pour tous m et n) qui définit x, d'autre part.

Il est vrai que l'on peut se poser les question de savoir si la fonction f que cela permet a priori de définir est d'une part « bien définie » (je crois que oui), et d'autre part « continue en tout point » (je crois que non, c'est-à-dire qu'il faut réclamer plus dans la donnée pour certifier que l'hypothèse est satisfaite).

Mais même sans s'attarder sur ce dernier point, comment diable peut-on imaginer réaliser l'hypothèse sous la forme décrite ?

Le calcul des suites de Cauchy définissant les réels $f(r)$ pour tout $r \in \mathbb{Q} \cap [a, b]$ ne pose pas de problème de principe.

La donnée d'un module de continuité ponctuelle, pour chaque x de l'intervalle est par contre difficile à imaginer. Le module de continuité est une fonction $\mu_x : \mathbb{N} \to \mathbb{N}$ qui doit vérifier :

$$\text{si } n > \mu_x(p) \text{ et } m > \mu_x(p), \text{ alors } |f(r_n) - f(r_m)| \leqslant \frac{1}{2^p} ,$$

ceci pour toute suite de rationnels (r_n) qui définit x (au sens précisé au départ).

Ainsi $(x, p) \mapsto \mu_x(p)$ est une opération $Q \times \mathbb{N} \to \mathbb{N}$, où Q est l'ensemble des suites de Cauchy de rationnels qui définissent des réels de $[a, b]$ au sens précisé au départ.

Mais « personne » n'est capable d'imaginer comment produire un tel objet sans l'hypothèse de continuité uniforme, c'est-à-dire sans supprimer la dépendance en x pour cette opération. En tout cas, pour être un peu moins affirmatif, disons que je n'ai jamais rencontré personne qui ...

Ayant bien réfléchi à ce genre de question, Brouwer introduisit des principes de continuité uniforme du style suivant : $(*)$ *toute fonction réelle sur l'intervalle* $[0, 1]$ *est uniformément continue.*

Ce faisant il se rapprochait du désir intuitif de Poincaré : « le continu est l'unité dans la multiplicité », mais de manière incompatible avec les mathématiques classiques.

Pour un mathématicien classique, il est très facile de définir des fonctions discontinues :

$$\chi(x) = 0 \text{ si } x \leqslant 1/2, \quad \text{et } \chi(x) = 1 \text{ si } x > 1/2.$$

Brouwer remarque simplement qu'en l'absence d'un test pour « $x \leqslant 1/2$? », cette fonction est mal définie. Leibniz pourrait dire que pour un réel x infiniment proche de $1/2$, on ne saura jamais quelle valeur attribuer à $\chi(x)$.

Bishop [1, 2] préféra éviter de recourir à un principe tel que $(*)$, qui est faux pour les mathématiques classiques, et difficile à justifier de manière pleinement convaincante d'un point de vue constructif.

Ne voyant pas comment on pouvait imaginer de certifier l'hypothèse du théorème ci-dessus autrement qu'en certifiant la conclusion, Bishop décida que ce théorème n'avait

aucun intérêt mathématique clairement identifiable, et utilisa une solution très simple, celle de *définir* une fonction continue sur $[0,1]$ comme étant une fonction uniformément continue. Ce faisant il se rapprochait lui aussi du désir intuitif de Poincaré. De manière moins radicale certes, mais cette fois-ci acceptable par les mathématiques classiques. Et il rejoignait également tous ceux qui font de l'analyse numérique en prenant au sérieux, dans leurs théories et leurs algorithmes, la nature infinie de chaque nombre réel.

L'immense avantage des mathématiques constructives « à la Bishop » est qu'elles fournissent un cadre de travail minimal compatible avec toutes les options concernant « ce que sont les nombres réels et les fonctions continues ». Et l'immense surprise qui ressort de son livre, c'est que les bases de l'analyse classique peuvent être entièrement développées dans un tel cadre, où tous les théorèmes ont un contenu algorithmique clair.

L'analyse constructive : une solution ?

Brouwer découvrit que l'infini des mathématiques classiques avait un grave défaut quant à la possibilité de réaliser concrètement les résultats des théorèmes, et que ce défaut pouvait être identifié comme l'acceptation inconsidérée du principe du tiers exclu lorsque les énoncés réclament a priori un infinité de vérifications. Par exemple, croire qu'un nombre réel donné par une suite de Cauchy de rationnels a forcément un signe bien déterminé est contraire à tout point de vue calculatoire.

D'ailleurs aucun programme sérieux écrit en analyse numérique n'utilise le test « $x = 0\,?$ » pour faire des branchements.

À la suite de Brouwer, un des mérites de Bishop est d'avoir clairement mis en valeur le *principe d'omniscience* suivant :

LPO : **le petit principe d'omniscience**,

qui gouverne les théorèmes étranges dont nous venons de parler (et d'autres moins étranges) en analyse classique.

LPO : Étant donnée une suite d'entiers, ou bien elle est identiquement nulle, ou bien elle a un terme non nul.

Bishop contourne la difficulté des « théorèmes étranges » en modifiant convenablement les définitions.

Néanmoins, chez lui, la droite réelle reste un ensemble de points, même s'ils ne sont plus autant extérieurs les uns aux autres qu'ils le sont en mathématiques classiques.

Le recours à l'axiome du choix dépendant[4] jette cependant un certain trouble, car il permet des énoncés moins *uniformes* qu'on ne le souhaite avec notre intuition du continu.

Prenons l'exemple du théorème fondamental de l'algèbre, soulevé par Fred Richman dans [12]. Une bonne implémentation sur machine de ce théorème ne calcule pas les zéros du polynôme de façon isolée les uns des autres. Seuls sont isolés, à une certaine étape de l'algorithme, les zéros dont on est certain qu'ils sont simples. Les zéros qui sont ou semblent multiples sont regroupés en paquets : dans ce petit disque trois zéros, dans cet autre petit disque cinq zéros et ainsi de suite.

La factorisation complète du polynôme en facteurs linéaires est obtenue par Bishop avec le secours de l'axiome du choix dépendant, mais cette factorisation complète est dans une certaine mesure contraire à notre intuition, et contraire à l'interprétation naturelle de ce que fait un algorithme de localisation des racines.

4. L'axiome du choix dépendant dit que si l'on dispose d'une relation binaire $R(x,y)$ sur un ensemble E, et si cette relation vérifie la propriété « $\forall x, \exists y,\ R(x,y)$ », alors pour tout $x_0 \in E$ on peut construire une suite infinie $(x_n)_{n\in\mathbb{N}}$ dans E qui satisfait : $\forall n \in \mathbb{N},\ R(x_n, x_{n+1})$.

La topologie sans points : une solution ?

Certainement la topologie sans points devrait ouvrir de belles perspectives.

Dans la topologie sans points on remplace la description usuelle d'un espace topologique comme ensemble de points muni d'une famille de parties « ouvertes », par la seule considération de la structure « algébrique » formée par les ouverts, lorsqu'on les munit des deux « lois » $U \cap V$ et $\bigcup_i U_i$. Les lois binaires $\cap$ et $\cup$ forment un treillis distributif, et l'on demande en outre une propriété de distributivité infinie : $V \cap \bigcup_i U_i = \bigcup_i (V \cap U_i)$. Un espace topologique sans point est souvent appelé une « locale ».

Si tout espace topologique usuel fournit une locale, la réciproque n'est pas vraie : certaines locales manquent de points.

En mathématiques constructives, on se contente souvent de définir une locale par une base d'ouverts. Un ouvert général étant une réunion arbiraire d'ouverts.

En algèbre, les espaces spectraux des mathématiques classiques ont souvent pour points des objets dont l'existence repose sur l'axiome du choix, et qui sont invisibles du point de vue constructif. Il vaut donc beaucoup mieux considérer les espaces spectraux comme des locales, dont on détermine souvent des bases d'ouverts simples à définir (voir par exemple [4] pour le spectre de Zariski).

Sans doute en analyse constructive les locales sont appelées à un avenir très prometteur car elles permettront de trouver le sens constructif caché de nombreux théorèmes qui pouvaient sembler a priori étranges.

Regardons par exemple la manière dont la topologie sans points résout le problème posé par le théorème de Heine-Borel (un autre « théorème étrange »).

La topologie de la droite réelle est définie par la base d'ouverts formée par les intervalles rationnels. On doit en outre :

- vérifer que l'intersection de deux ouverts de base est une réunion d'ouverts de base,
- donner la définition de ce que signifie : « une famille d'ouverts de base $(U_i)_{i\in I}$ recouvre un ouvert de base $]a, b[$ »

Ici le premier point est évident, car l'intersection de deux ouverts de base est un ouvert de base.

Quant au deuxième point, la définition choisie demande que pour chaque intervalle rationnel fermé $[c, d]$ contenu dans $]a, b[$, une famille finie extraite admette pour réunion un ouvert contenant $[c, d]$.

On voit que Heine-Borel est ainsi incorporé comme une partie essentielle de la définition de la topologie de la droite réelle. Laquelle, grâce à ce merveilleux subterfuge, n'a plus besoin de mentionner ses « points » dans sa définition.

Bon, mais il reste sans doute encore trop de points bien visibles sur cette belle droite, élégante et minimaliste.

L'analyse constructive non standard : une solution ?

À creuser. On se rappelle de l'heuristique constructive pour l'analyse non standard développée par Harthong et Reeb dans *Intuitionnisme 84*.

Voir également une mise en forme constructive de l'analyse non-standard par Erik Palmgren (par exemple [11])

On attend avec intérêt les développements sur ce sujet dans l'optique ou Guy Wallet.

Qu'est-ce qu'un vrai nombre réel en Calcul Formel ?

On peut a priori viser deux objectifs différents lorsque l'on cherche à implémenter sur machine les calculs qui relèvent de l'analyse.

Un objectif très intéressant a priori, certainement ambitieux, mais encore peu exploré, serait d'avoir une vision « sans points » de la droite réelle, et plus généralement des espaces topologiques. Dans ce cadre on viserait à implémenter les algorithmes sous-jacents à une théorie constructive des locales.

De manière plus modeste, on peut viser à se baser sur l'analyse constructive à la Bishop, déjà bien développée, et à en expliciter les algorithmes sous-jacents. C'est ce vers quoi tendent tous ceux qui font de l'analyse numérique en essayant de certifier les résultats obtenus.

On voit alors qu'implémenter les nombres réels comme des objets manipulables par un ordinateur relève inévitablement de l'évaluation paresseuse. Un « nombre réel arbitraire », pris en entrée d'un algorithme, n'est jamais connu "en entier", mais seulement de façon approchée.

En entrée, on peut considérer que l'on a un oracle qui donne une approximation rationnelle a du nombre réel x selon une précision requise, requise par l'algorithme, au moyen d'une instruction du type suivant :

$a \leftarrow x \pm 1/2^n$.

Donnons l'exemple d'un programme typique. Celui pour implémenter le calcul de la fonction $x \mapsto \exp(x)$

Le programme commence par poser deux requêtes :

- donnez moi x avec la précision 1 ? (mettons que la réponse soit un entier a),
- quelle est la précision requise sur $y = \exp(x)$? (mettons que la réponse soit un entier n, signifiant que l'on désire un rationnel b tel que l'intervalle $]b - \frac{1}{2^n}, b + \frac{1}{2^n}[$ contienne y)

En fonction de a, le programme calcule une constante de Lipschitz k pour la fonction exponentielle sur l'intervalle $[a-1, a+1]$ et pose une nouvelle question : veuillez me donner x avec telle précision (cette précision est obtenue à partir de k et n).

En sortie : un nombre rationnel b convenable.

Notons que pour cet exemple précis, il ne semble pas y avoir de différence significative avec ce qui devrait être programmé dans une optique de topologie sans point.

3 Étudier l'algèbre réelle constructive

Introduction

Définissons *l'algèbre réelle* comme l'étude les propriétés algébriques des nombres réels, i.e., les propriétés de $\mathbb{R}$ vis à vis de $(0,\ 1,\ +,\ -,\ \times,\ >,\ \geqslant)$.

L'*algèbre réelle constructive* n'est pas bien comprise ! L'analyse constructive ($\simeq$ les méthodes certifiées en analyse numérique) est nettement mieux étudiée.

D'un point de vue constructif, l'algèbre réelle est *assez éloignée* de la théorie usuelle classique des corps réels clos à la Artin-Tarski, dans laquelle on suppose que l'on a un *test de signe*.

La plupart des algorithmes de l'algèbre réelle classique échouent avec les nombres réels, parce qu'ils requièrent un test de signe.

Même en analyse constructive, on pourrait avoir des retombées intéressantes d'une étude plus approfondie de l'algèbre réelle. Par exemple cela permettrait de mieux comprendre comment éviter le recours à l'axiome du choix dépendant.

La compréhension de l'algèbre réelle constructive peut également être un premier pas pour une théorie constructive (et donc algorithmique) des *structures O-minimales* (cf. [6, 9]).

L'algèbre réelle peut en effet être vue comme la plus simple des structures O-minimales. La théorie classique (non algorithmique) des structures O-minimales donne en effet des pseudo-algorithmes qui fonctionneraient correctement si on avait un test de signe sur les réels. Et la théorie des structures O-minimales a a priori un champ d'application très important en analyse.

Dans ce qui suit, nous esquissons l'étude d'une *théorie axiomatique formelle du premier ordre* pour l'algèbre réelle.

Nous avons en vue les réels à la Bishop, dont l'ensemble doit former un modèle de cette théorie formelle, au sens de la théorie constructive des ensembles à la Bishop.

Mais il serait également intéressant d'envisager comment on peut parler de modèles sans points pour une théorie formelle du premier ordre.

Corps de Heyting ordonnés

Nous commençons par expliquer ce qu'est un corps ordonné au sens de Heyting. Nous utilisons aussi la terminologie développée dans l'article [8].

Un corps ordonné est une structure algébrique basée sur un ensemble $\mathbf{K}$ avec la signature suivante, dans laquelle les trois prédicats sont unaires.

$$(\mathbf{K},\ \cdot = 0,\ \cdot > 0,\ \cdot \geqslant 0,\ \cdot + \cdot,\ -\cdot,\ \cdot \times \cdot,\ \sup(\cdot,\cdot),\ 0,\ 1)$$

Abréviations

- $x = y$ signifie $x - y = 0$
- $x > y$ signifie $x - y > 0$
- $x \geqslant y$ signifie $x - y \geqslant 0$
- $x \neq y$ signifie $(x - y)^2 > 0$

Axiomes directs

1. $(\mathbf{K}, = 0, +, -, \times, 0, 1)$ est un anneau commutatif :
   machinerie calculatoire des polynômes, et 3 axiomes directs
   1a. $\vdash\ 0 = 0$, 1b. $x = 0 \vdash xy = 0$, 1c. $x = 0,\ y = 0 \vdash x + y = 0$.
2. $\vdash\ 1 > 0$
3. $x = 0 \vdash x \geqslant 0$
4. $x > 0 \vdash x \geqslant 0$
5. $\vdash\ x^2 \geqslant 0$
6. $(x > 0,\ y \geqslant 0) \vdash x + y > 0$
7. $(x > 0,\ y > 0) \vdash xy > 0$
8. $(x \geqslant 0,\ y \geqslant 0) \vdash x + y \geqslant 0$
9. $(x \geqslant 0,\ y \geqslant 0) \vdash xy \geqslant 0$
10. **Collapsus** $0 > 0 \vdash 1 = 0$

Règles de simplification

11. $x^2 \leqslant 0 \vdash x = 0$
12. $(c \geqslant 0,\ cs > 0) \vdash s > 0$
13. $(s > 0,\ cs \geqslant 0) \vdash c \geqslant 0$
14. $(c \geqslant 0,\ x(x^2 + c) \geqslant 0) \vdash x \geqslant 0$

Règles dynamiques

15. $x + y > 0 \vdash x > 0 \vee y > 0$
16. $xy > 0 \vdash x > 0 \vee -y > 0$
17. $x > 0 \vdash \exists y\, xy = 1$

En fait, on montre que les règles dynamiques, les règles directes et le collapsus (qui est une règle directe particulière) impliquent les règles de simplification.

L'axiome de Heyting.

HOF : $(-x > 0 \Rightarrow 1 = 0) \vdash x \geqslant 0$

Cet axiome traduit la définition de la relation $\geqslant$ pour les nombres réels. Mais c'est un axiome désagréable, car il ne correspond pas à une règle dynamique, et son hypothèse contient une négation (ou du moins son substitut). Or les mathématiques sont plus élégantes et plus claires sans négation.

Un corps ordonné avec un test de signe obéirait lui à l'axiome plus fort suivant, qui est une règle dynamique.

Corps ordonnés discrets.

DOF : $\vdash x \geqslant 0 \vee -x > 0$

La fonction sup

La théorie formelle précédente, avec **HOF**, *ne prouve pas* l'existence de la borne supérieure de deux éléments, i.e., la formule suivante n'est pas prouvable (voir [5]) :

$$\forall x, y \;\; \exists z \quad (z - x)(z - y) = 0,\; z \geqslant x,\; z \geqslant y$$

Il nous faut donc ajouter dans la syntaxe le symbole de fonction sup avec les axiomes suivants.

Règles pour sup

18. $\vdash \sup(x, y) = \sup(y, x)$
19. $\vdash \sup(x, y) \geqslant x$
20. $\vdash (\sup(x, y) - x)\,(\sup(x, y) - y) = 0$

On peut alors démontrer les propriétés suivantes de la fonction sup, en définissant $\inf(a, b) = -\sup(-a, -b)$ et $|a| = \sup(a, -a)$.

- $\sup(x + z, y + z) = \sup(x, y) + z$
- $\sup(x, y) + \inf(x, y) = x + y$
- $\sup(x, y) \inf(x, y) = xy$
- $\sup(x, \inf(y, z)) = \inf(\sup(x, y), \sup(x, z))$
- $|x| \sup(y, z) = \sup(|x|\, y, |x|\, z)$
- $\sup(x, y) > 0 \iff (\, x > 0 \vee y > 0\,)$
- $x = \sup(x, y) \iff y = \inf(x, y) \iff x \geqslant y$
- $\sup(x, y) < 0 \iff (x < 0 \wedge y < 0)$
- $\sup(x, y) \leqslant 0 \iff (x \leqslant 0 \wedge y \leqslant 0)$

- $\inf(|x|,|y|) = 0 \iff (xy = 0)$
- $x \neq 0 \iff |x| > 0$

Remarque. Les deux ensembles $\{a, b\}$ et $\{\inf(a, b), \sup(a, b)\}$ ont la même adhérence, qui est l'ensemble des zéros de $(T - a)(T - b)$.
Et l'on a des résultats similaires avec $(T - a_1) \cdots (T - a_n)$.

Nous proposons la définition provisoire suivante.

Défintion 2. *Un corps ordonné de Heyting est un anneau commutatif avec une loi binaire* sup *vérifiant les axiomes 1 à 20 et l'axiome* **HOF**.

Cette définition est provisoire dans la mesure où il faut sans doute introduire dans la syntaxe des fonctions analogues à la fonction sup : fonctions semialgébriques continues « rationnelles » (i.e., qui prennent toujours leurs valeurs dans le corps de leurs entrées), définies sur $\mathbb{Q}$, mais dont l'existence ne pourrait pas être prouvée à l'aide des seuls axiomes déjà introduits.

Notez que pour la structure de corps ordonné discret, on remplace simplment l'axiome **HOF** par l'axiome **DOF**.

Propriétés de clôture réelle

Usuellement, un corps réel clos est défini comme un corps ordonné pour lequel tout polynôme qui change de signe sur un intervalle admet une racine dans l'intervalle.

Pour les corps ordonnés discrets, on obtient donc la théorie formelle des corps réels clos en rajoutant, pour chaque degré, un axiome correspondant au théorème de la valeur intermédiaire.

RCF1 : Soient $a < b$. Un polynôme P tel que $P(a)P(b) < 0$ admet un zéro sur $]a, b[$.

Pour la théorie des corps réels clos discrets on recommande l'excellent [3].

Cependant les choses se compliquent pour le corps des réels $\mathbb{R}$, car ce n'est pas un corps ordonné discret (on n'a pas de test de signe).

En outre la propriété **RCF1** ne semble pas démontrable pour le corps des nombres réels à la Bishop sans recours à l'axiome du choix dépendant.

La propriété suivante est par contre constructivement valide pour $\mathbb{R}$ même sans axiome du choix dépendant.

RCF2 : Soient $a < b$. Un polynôme P tel que $P(a)P(b) < 0$ et $P' > 0$ sur (a, b), admet un zéro sur $]a, b[$.

Néanmoins cet axiome est loin de décrire toutes les propriétés des réels qui relèvent du thème des corps réels clos.

Exemples de sous-corps de $\mathbb{R}$ intéressants pour les applications

Citons par exemple les trois suivants, qui satisfont **RCF2** (c'est moins clair pour **RCF1**). Les deux premiers sont récursivement énumérables.

- Le corps des nombres réels primitifs récursifs.
- Le corps des nombres réels calculables en temps polynomial.
- Le corps des nombres réels « récursifs », c'est-à-dire calculables au sens de Turing.

Un outil qui pourrait s'avérer utile : les racines virtuelles

La définition des racines virtuelles d'un polynôme unitaire (ou en tous cas un polynôme de degré bien défini) est basée sur le lemme suivant, qui admet une démonstration constructive[5].

NB : pour plus de précisions concernant les racines virtuelles, voir [10, 7].

Lemme 3. *Une fonction réelle f uniformément continue et strictement croissante sur un intervalle $[a, b]$ ($a \leqslant b$) atteint son (unique) minimum en valeur absolue.*

Corollaire 4. *On peut définir par récurrence sur d, sur l'espace des polynômes réels unitaires de degré d, d* fonctions "racines virtuelles" *$\rho_{d,k} : \mathbb{R}^d \to \mathbb{R}$ ($k = 1, \ldots, d$). On définit d'abord formellement $\rho_{d,0}(f) = -\infty$, $\rho_{d,d+1}(f) = +\infty$, et l'on pose $f(-\infty) = (-1)^d \infty$, $f(+\infty) = +\infty$. On demande alors que soient vérifiées les propriétés suivantes.*

RV1 : $\rho_{1,1}(f) = a$, *si* $f = X - a$.

Si $1 \leqslant k \leqslant d = \deg(f) \geqslant 2$, *les deux axiomes :*

RV2$_d$: $\rho_{d-1,k-1}(f'/d) \leqslant \rho_{d,k}(f) \leqslant \rho_{d-1,k}(f'/d)$.

RV3$_d$: $\rho_{d-1,k-1}(f'/d) \leqslant x \leqslant \rho_{d-1,k}(f'/d) \;\Rightarrow\; |f(\rho_{d,k}(f))| \leqslant |f(x)|$.

Quelques propriétés importantes des racines virtuelles sont les suivantes.

Dans un corps ordonné de Heyting, elles peuvent être déduites constructivement des seules propriétés **RV1**, **RV2$_d$** et **RV3$_d$**.

1. Si $\rho_{d,k}(f) < x < \rho_{d,k+1}(f)$, alors $(-1)^{d+k} f(x) > 0$ (pour $0 \leqslant k \leqslant d$).
2. Si $\deg(f) = d$ et $f(x) = 0$, alors $\prod_{i=1}^{d}(x - \rho_{d,i}(f)) = 0$ (les racines virtuelles « recouvrent » les racines du polynôme).
3. Si $f(T) = (T - a)(T - b)$, alors $\rho_{2,1}(f) = \inf(a, b)$ et $\rho_{2,2}(f) = \sup(a, b)$.
4. Une version constructive de l'axiome **RCF1** :
   si $\deg(f) = d$, $a < b$ et $f(a)f(b) < 0$, alors $\prod_{i=1}^{d} f(\mu_{d,i}(f)) = 0$,
   où $\mu_{d,i}(f) = \inf(b, \sup(a, \rho_{d,i}(f)))$.
5. Chaque $\rho_{d,k} : \mathbb{R}^d \to \mathbb{R}$ est une fonction localement uniformément continue, et $\rho_{d,k}(f)$ est un zéro du produit
   $$f \cdot f' \cdots f^{(j)} \cdots f^{(d-1)}.$$
6. Pour $a < b$ et P un polynôme, on a
   $$\inf\{\, P(x) \mid x \in [a, b] \,\} = \inf\{P(a), P(b), \inf(b, \sup(a, P(\zeta_k)))\}$$
   où les ζ_k sont les zéros virtuels de P'.
7. Les racines virtuelles sont comptées par la méthode de **Descartes-Budan-Fourier**. En particulier elles sont « faciles à calculer », en fait, en un sens convenable, calculables en temps polynomial.

Enfin, si un corps ordonné de Heyting possède des fonctions racines virtuelles vérifiant les axiomes **RV1**, **RV2$_d$** et **RV3$_d$**, alors il vérifie l'axiome **RCF2**.

5. Toute la suite est écrite d'un point de vue constructif. En particulier, la théorie formelle considérée utilise la logique intuitionniste

Ue théorie formelle à étudier

On pourrait alors proposer pour les corps réels clos dans le cas non discret la théorie formelle suivante. On rajoute des symboles de fonctions pour les fonctions racines virtuelles des polynômes unitaires. On prend les axiomes des corps ordonnés de Heyting et on rajoute les axiomes **RV1**, **RV2**$_d$ et **RV3**$_d$.

Dans ce cadre il est intéressant de savoir si l'axiome désagréable **HOF** a la moindre utilité, ou si l'on peut s'en passer.

Un résultat à la Pierce-Birkhoff

Théorème 5.
Soit $f : \mathbb{R}^n \to \mathbb{R}$ une fonction semialgébrique continue définie sur $\mathbb{Q}$ et entière sur le sous-anneau des fonctions polynômes, identifié à $\mathbb{Q}[X_1, \ldots, X_n]$. Alors f peut s'exprimer comme combinaison de fonctions racines virtuelles et de polynômes à coefficients dans $\mathbb{Q}$.

Remarque. Dans le théorème précédent on peut remplacer $\mathbb{Q}$ par un sous-corps discret de $\mathbb{R}$.

Question 1. Est-il possible de remplacer $\mathbb{Q}$ par $\mathbb{R}$ dans le théorème 5 ? La signification exacte de l'hypothèse doit alors être éclaircie.

Autrement dit, nous avons besoin d'une bonne définition pour « $f : \mathbb{R}^n \to \mathbb{R}$ est une fonction semialgébrique continue. » ! Si possible d'une définition qui n'utilise que le langage de la théorie formelle proposée dans le paragraphe précédent.

Il faut aussi étendre une telle définition aux fonctions semialgébriques continues ayant pour domaine de définition un ensemble semialgébrique localement fermé « raisonnable ».

Question 2. Toutes les fonctions semialgébriques continues définies sur $\mathbb{Q}$, avec pour domaine de définition un ensemble semialgébrique localement fermé défini sur $\mathbb{Q}$, peuvent-elles être démontrées exister dans la théorie formelle évoquée au paragraphe précédent. Si ce n'est pas le cas, quels axiomes serait-il raisonnable d'ajouter ?

Un cas important à étudier serait la fonction distance à un fermé smialgébrique.

Question 3. Dans toutes ces questions, est-ce que l'on peut se passer de l'axiome **HOF** ?

Références

[1] Bishop E. *Foundations of Constructive Analysis.* McGraw Hill, (1967). 5

[2] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag (1985). 5

[3] Bochnak J., Coste M., Roy M.-F. *Géométrie algébrique réelle.* Springer Verlag, (1987). 11

[4] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*, p. 477–499 dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker, (2002). 7

[5] Coquand T., Lombardi H. *A note on the axiomatisation of real numbers.* Math. Logic Quarterly. **54** (3), (2008), 224–228. 10

[6] Coste M. *An introduction to O-minimal Geometry.* Dip. Mat. Univ. Pisa, Dottorato di Ricerca in Matematica, Istituti Editoriali e Poligrafici Internazionali, Pisa (2000). 9

[7] Coste M., Lajous T., Lombardi H., Roy M.-F. *Generalized Budan-Fourier theorem and virtual roots* Journal of Complexity **21** (2005), 479–486. 12

[8] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256. 9

[9] van den Dries L. *Tame Topology and O-minimal Structures.* London Math. Soc. Lecture Note 248. Cambridge Univ. Press 1998 9

[10] Gonzalez-Vega L., Lombardi H., Mahé L. *Virtual roots of real polynomials.* Journal of Pure and Applied Algebra **124**, (1998) 147–166. 12

[11] Palmgren E. *Developments in constructive nonstandard analysis.* Bulletin of Symbolic Logic, **4** (1998), 233–272. 7

[12] Richman F. *The fundamental theorem of algebra : a constructive development without choice.* Pacific Journal of Mathematics, **196** (2000), 213–230. 6