Le point de vue constructif

Une introduction

LOMBARDI Henri
Maître de Conférences
Université de Franche-Comté, Besançon
henri.lombardi@univ-fcomte.fr

Notes de Cours. 2005

Table des matières

1 Un premier exemple : les groupes abéliens de type fini **3**
- 1.1 Les théorèmes doivent avoir un contenu calculatoire . . . 3
- 1.2 Le théorème de la base adaptée avec un sous-groupe de type fini . . . 3
- 1.3 Cohérence . . . 5
- 1.4 Noetherianité . . . 6
- 1.5 Le Théorème de la Base de Hilbert . . . 8

2 Logique Constructive **9**
- 2.1 Objets de base, Ensembles, Fonctions . . . 9
- 2.2 Affirmer signifie prouver . . . 12
- 2.3 Connecteurs et quantificateurs . . . 13
- 2.4 Calculs mécaniques . . . 14
- 2.5 Principes d'omniscience . . . 15
- 2.6 Principes problématiques 18

3 Nombres réels et fonctions continues **21**
- 3.1 Construction des nombres réels . . . 21
- 3.2 Fonctions réelles . . . 24
- 3.3 Algèbre réelle . . . 24
- 3.4 **LPO** implique le principe de continuité uniforme . . . 26

4 Le programme de Hilbert **29**
- 4.1 Echecs et succès du programme de Hilbert . . . 29
- 4.2 Du bon usage des objets abstraits . . . 31
- 4.3 Objets abstraits purement idéaux et principes d'omniscience . . . 36

Corrigés d'exercices **39**

Références **41**

Résumé

Nous exposons quelques traits marquants des mathématiques constructives à la Bishop.

Deux références de base sont : *A Course in Constructive Algebra* ([MRR] Mines R., Richman F., Ruitenburg W.) et *Constructive Analysis* ([BB] Bishop E., Bridges D.).

Le livre de D. Bridges et F. Richman *Varieties of Constructive Mathematics* [BR] est très utile pour comprendre les autres sortes de mathématiques constructives. Voyez aussi le livre de M. Beeson *Foundations of Constructive Mathematics* [Be] pour une étude approfondie du point de vue de la logique mathématique.

Nous considérons les mathématiques de Bishop comme une base pour les autres mathématiques.

En ajoutant le principe du tiers exclu et l'axiome du choix, vous obtenez les mathématiques classiques. En ajoutant la thèse de Church et le principe de Markov vous obtenez les constructivisme russe (voir [Ab, BR, Ku], [21]). En ajoutant d'autres axiomes vous obtenez l'intuitionnisme de Brouwer (voir [BR, Bro, He, Du, TD]).

Le chapitre 1 analyse l'exemple des sous-groupes de $\mathbb{Z}^n$, ce qui nous amène à discuter le traitement constructif de la noethérianité. Le chapitre 2 donne quelques commentaires sur la logique. Le chapitre 3 donne un premier aperçu sur les nombres réels. Le chapitre 4 aborde les relations entre le programme de Hilbert et les mathématiques constructives.

Nous avons mis en *digressions carrément philosophiques* des discussions qui, bien qu'elles nous semblent importantes, ne semblent pas pouvoir avoir de conséquences purement mathématiques.

On ne doit pas s'attendre à lire dans ce qui suit un exposé complètement linéaire. Dans la mesure où on parle sérieusement de questions de fondements, il est inévitable d'avancer des arguments ainsi que des définitions plus ou moins circulaires.

1. Un premier exemple : les groupes abéliens de type fini

1.1 Les théorèmes doivent avoir un contenu calculatoire

Un principe de base général du constructivisme est le suivant : *en mathématiques les théorèmes doivent avoir un contenu calculatoire.* En particulier lorsqu'un théorème affirme l'existence d'un objet mathématique sa preuve doit montrer comment construire cet objet. On ne peut pas se contenter d'une existence purement idéale de l'objet : la vérité en mathématiques doit avoir contenu calculatoire.

Un premier mini contre exemple est donné par la plaisanterie suivante.

Question : Trouver deux nombres irrationnels a et b tels que a^b soit un nombre rationnel.
Réponse : Soit $\alpha = \sqrt{3}$, $\beta = \sqrt{2}$, $\gamma = \alpha^\beta$. Si γ est rationnel, prendre $a = \alpha$, $b = \beta$. Sinon prendre $a = \gamma$, $b = \beta$.

On voit qu'il y a un « malaise ». Si nous n'avons pas moyen de répondre, au moins en principe, à la question « γ est-il un nombre rationnel ? », alors nous n'avons pas donné une réponse concrète à la question de départ. Le nombre γ est bien défini en tant que nombre réel à la Cauchy : on peut le calculer avec une précision arbitraire. Mais il est nettement plus difficile de décider s'il est rationnel ou irrationnel.

Nous étudions maintenant un exemple plus sérieux. Le théorème de la base adaptée pour les sous-groupes de $\mathbb{Z}^n$.

Théorème 1.1 (Théorème de la base adaptée). *Si G est un sous-groupe de $(\mathbb{Z}^n, +)$ alors il existe une $\mathbb{Z}$-base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$, un entier r $(0 \leq r \leq n)$, et des entiers positifs $a_1, \ldots, a_r$ qui vérifient :*

- *a_i divise a_{i+1} $(1 \leq i < r)$*
- *$(a_1 e_1, \ldots, a_r e_r)$ est une $\mathbb{Z}$-base de G.*

Dans ces conditions, la liste des entiers a_i est déterminée de manière unique. En outre le sous-groupe $\widetilde{G} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$ de $\mathbb{Z}^n$ ne dépend que de G : c'est l'ensemble des x tels qu'il existe $k > 0$ avec $kx \in G$. Enfin on a $(\widetilde{G} : G) = a_1 \cdots a_r$.

Nous allons faire une analyse assez complète du contenu constructif de ce théorème.

Le contenu concret du théorème dépend de la réponse à la question « comment G nous est-il donné ? »

1.2 Le théorème de la base adaptée avec un sous-groupe de type fini

Lorsque G est donné comme sous-groupe de type fini de $\mathbb{Z}^n$, le théorème de la base adaptée a un contenu extrêmement concret. En fait le théorème suivant donne des renseignements plus précis.

Théorème 1.2 (Théorème de réduction de Smith pour $\mathbb{Z}$) *Soit M une matrice $\in \mathbb{Z}^{n\times m}$, alors elle admet une* réduction de Smith *: il existe deux matrices inversibles $C \in \mathbb{Z}^{m\times m}$ et $L \in \mathbb{Z}^{n\times n}$ telles que la matrice $D = LMC$ est sous* forme de Smith*, i.e., toutes les entrées $d_{i,j}$ avec $i \neq j$ sont nulles, et $d_{i,i}$ divise $d_{i+1,i+1}$ $(1 \leq i \leq \min(m,n)-1)$.*
En outre si on choisit les $d_{i,i}$ positifs ou nuls, ils sont déterminés de manière unique par M. (en fait le produit $d_{1,1}\cdots d_{k,k}$ est égal au pgcd des mineurs $k \times k$ de M).

Preuve Dans une matrice, une *manipulation élémentaire* de lignes (resp. de colonnes) consiste à rajouter à une ligne (resp. une colonne) un multiple d'une autre ligne (resp. d'une autre colonne). Une telle manipulation revient à multiplier la matrice à gauche (resp. à droite) par une *matrice élémentaire* (une matrice avec des 1 sur la diagonale et seulement un terme non nul en dehors). Une succession simple de manipulations élémentaires de lignes permet d'échanger deux lignes, en multipliant l'une d'entre elles par -1. On peut aussi remplacer un coefficient de la matrice par le reste de sa division par un autre coefficient situé sur la même ligne ou sur la même colonne. Comme le pgcd de deux entiers non nuls peut être calculé par divisions successives, on peut rendre le coefficient en position $(1,1)$ égal au pgcd de tous les coefficients de sa ligne et de sa colonne (le processus s'arrête parce qu'un entier ne peut diminuer qu'un nombre fini de fois pour la divisibilité). On utilise alors ce coefficient comme pivot pour annuler toutes les autres entrées dans la première ligne et la première colonne. Si dans la partie restante de la matrice, il y a un coefficient non multiple du pivot, on rajoute sa ligne à la première et on recommence. Le processus s'arrête parce qu'un entier ne peut diminuer qu'un nombre fini de fois pour la divisibilité. Par manipulations élémentaires de lignes et de colonnes, on a donc fait apparaître en position $(1,1)$ un entier qui est le pgcd des entrées de la matrice. Précisément on obtient :

$$L_1 M C_1 = \begin{pmatrix} d & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & d\cdot M_1 & \\ 0 & & & \end{pmatrix}$$

où L_1 et C_1 sont produits de matrices élémentaires. Il reste à recommencer avec M_1. On peut donc obtenir dans le théorème les matrices C et L comme produits de matrices élémentaires([1]).
□

Corollaire 1.2.1 *Soit $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ une application $\mathbb{Z}$-linéaire (c'est-à-dire un homomorphisme de groupes). Alors le théorème de la base adaptée s'applique à* $\mathrm{Ker}\varphi$ *et* $\mathrm{Im}\varphi$*. En outre $\mathbb{Z}^m = \mathrm{Ker}\varphi \oplus N$ avec N libre.*

Une autre conséquence du théorème 1.2 est que les systèmes d'équations linéaires avec coefficients et inconnues dans $\mathbb{Z}$ peuvent être résolus et discutés d'une manière simple et systématique. Le « second membre » doit vérifier certaines équations et congruences. Quand ces conditions de compatiblité sont vérifiées, une solution particulière est facile à calculer, et la solution générale est obtenue en rajoutant une combinaison $\mathbb{Z}$-linéaire d'une famille finie explicite de vecteurs $\mathbb{Z}$-indépendants.

Kaplansky a étudié dans [12] quels sont les anneaux pour lesquels le théorème de réduction de Smith s'applique. Nous pouvons donner certains de ses résultats sous la forme suivante.

Définition 1.2.2 *Nous disons qu'un anneau commutatif $\mathbf{A}$ est un* anneau de Bezout strict *si pour tout $A = (a,b) \in \mathbf{A}^{1\times 2}$ il existe une matrice inversible $C \in \mathbf{A}^{2\times 2}$ telle que $AC = (g,0)$. Nous disons qu'un anneau commutatif $\mathbf{A}$ est un* anneau de Smith *si c'est un anneau de Bezout strict et si pour toute matrice triangulaire $T \in \mathbf{A}^{2\times 2}$ il existe des matrices inversibles $C \in \mathbf{A}^{2\times 2}$ et $L \in \mathbf{A}^{2\times 2}$ telles que la matrice LTC soit diagonale.*

[1] Néanmoins, si M est une matrice carrée non singulière de déterminant < 0, puisque le produit par des matrices élémentaires ne change pas le déterminant, on peut seulement obtenir de cette manière tous les $d_{i,i} > 0$ sauf un.

Proposition 1.2.3 *Les matrices M dans un anneau $\mathbf{A}$ admettent une réduction de Smith $D = LMC$ si et seulement si $\mathbf{A}$ est un anneau de Smith. Si en outre l'anneau $\mathbf{A}$ est intègre les $d_{i,i}$ sont déterminés de manière unique, à des unités près, par M.*

Il semble qu'on ignore toujours s'il existe des anneaux de Bezout stricts qui ne soient pas des anneaux de Smith.

Exercice 1.2.4

1. Prouver la proposition précédente.
2. Deux éléments u, v dans un anneau $\mathbf{A}$ sont dits *étrangers* si ils engendrent l'idéal $\mathbf{A}$. Montrer qu'un anneau de Bezout strict $\mathbf{A}$ est un anneau de Smith si et seulement si pour tous a, b, c dans $\mathbf{A}$, on peut trouver u, v étrangers et u', v' étrangers tels que $uu'a+vu'c+vv'b$ divise a, b et c.
3. Montrer qu'un anneau intègre est un anneau de Bezout strict si et seulement si tout idéal engendré par deux éléments est principal.

1.3 Cohérence

Une autre manière de décrire en termes finis un sous-groupe de $\mathbb{Z}^n$ est de le donner comme intersection finie de sous-groupes de type fini de $\mathbb{Z}^n$.

Théorème 1.3 *Le théorème de la base adaptée est valable pour toute intersection finie de sous-groupes de type fini de $\mathbb{Z}^n$.*

Preuve Si $G_1 = \mathrm{Im}(\varphi_1)$ et $G_2 = \mathrm{Im}(\varphi_2)$ avec $\varphi_j : \mathbb{Z}^{m_j} \to \mathbb{Z}^n$ définissons $\varphi : \mathbb{Z}^{m_1+m_2} \to \mathbb{Z}^n$ par $\varphi(x_1, x_2) = \varphi_1(x_1) - \varphi_2(x_2)$. Notons $\pi_1 : \mathbb{Z}^{m_1+m_2} \to \mathbb{Z}^{m_1}$ la projection canonique. On voit facilement que

$$G_1 \cap G_2 = \varphi_1(\pi_1(\mathrm{Ker}(\varphi))).$$

Nous obtenons donc le résultat en appliquant le corollaire 1.2.1. □

La méthode précédente pour calculer une intersection marche dans des situations beaucoup plus générales. Cela conduit à la notion d'anneau cohérent.

Définition 1.3.1 *Soit $\mathbf{A}$ un anneau commutatif. Un $\mathbf{A}$-module M est dit* de présentation finie *si il existe une application linéaire surjective $\varphi : \mathbf{A}^m \to M$ dont le noyau est un $\mathbf{A}$-module de type fini. Ce noyau est appelé le module des relations (ou des syzygies) entre les générateurs $\varphi(e_i)$ (où les e_i forment la base canonique de $\mathbf{A}^n$.*

Nous laissons en exercice le fait suivant :

Fait 1.3.2 *Si M est un $\mathbf{A}$-module de présentation finie, pour tout système générateur $(x_1, \ldots, x_\ell)$ de M le module des relations entre les x_i est de type fini.*

Ceci légitime la définition suivante.

Définition 1.3.3 *Un anneau $\mathbf{A}$ est dit* cohérent *si tout idéal de type fini est de présentation finie. Il revient au même de dire que toute forme linéaire $\alpha : \mathbf{A}^n \to \mathbf{A}$ a pour noyau un sous $\mathbf{A}$-module de type fini de $\mathbf{A}^n$.*
Un $\mathbf{A}$-module M est dit cohérent *si tout sous-module de type fini est de présentation finie. Il revient au même de dire que toute application linéaire $\varphi : \mathbf{A}^n \to M$ a pour noyau un sous $\mathbf{A}$-module de type fini de $\mathbf{A}^n$.*

Il est clair que $\mathbb{Z}$ est un anneau cohérent.
Nous avons les résultats généraux suivants (voir par exemple [MRR]).

Proposition 1.3.4 *Un anneau commutatif $\mathbf{A}$ est cohérent si et seulement si il vérifie les deux propriétés suivantes :*

– *l'intersection de deux idéaux de type fini est de type fini.*

– *l'annulateur* $(0 : a) = \{x \in \mathbf{A} \ ; \ ax = 0\}$ *de tout élément* $a \in \mathbf{A}$ *est de type fini.*

Proposition 1.3.5 *Si l'anneau* $\mathbf{A}$ *est cohérent, tout* $\mathbf{A}$*-module de présentation finie* M *est cohérent.*

Exercice 1.3.6 Montrer le fait 1.3.2.

Exercice 1.3.7 En vous inspirant de la preuve du théorème 1.3 montrez que si M est cohérent alors l'intersection de deux sous-modules de type fini est un sous-module de type fini.

1.4 Noetherianité

Le théorème de la base adaptée peut être décomposé en deux morceaux :

– Tout sous-groupe de type fini de $\mathbb{Z}^n$ admet une base adaptée (corollaire 1.2.1).

– Tout sous-groupe de $\mathbb{Z}^n$ est de type fini.

Pour analyser constructivement la seconde assertion considérons les cinq propriétés suivantes pour un $\mathbf{A}$-module M.

N1 : Tout sous-module de M est de type fini.

N2 : Toute suite croissante de sous-modules de M ($M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$) est constante après un certain rang.

N3 : Toute suite croissante de sous-modules de type fini de M est constante après un certain rang.

N4 : Toute suite croissante de sous-modules de type fini de M a deux termes consecutifs égaux.

N5 : Une suite strictement croissante de sous-modules de type fini de M est impossible.

Les implications suivantes sont directes et constructives :

$$\text{N1} \ \Rightarrow \ \text{N2} \ \Rightarrow \ \text{N3} \ \Rightarrow \ \text{N4} \ \Rightarrow \ \text{N5}$$

Par contre l'implication N5 $\Rightarrow$ N1 n'est pas prouvable d'un point de vue constructif. En fait aucune des implications réciproques de celles écrites ci-dessus n'a de preuve constructive.

Considérons par exemple l'implication N4 $\Rightarrow$ N3 pour le $\mathbb{Z}$-module $\mathbb{Z}$. Tout sous module de type fini de $\mathbb{Z}$ est de la forme $u\mathbb{Z}$ pour un entier $u \geq 0$. Donner une suite croissante de sous modules de type fini revient donc à donner une suite (u_n) d'entiers ≥ 0 telle que u_{n+1} divise u_n pour tout n. Si on prend $u_n = 2^{k_n}$ on a donc une suite décroissante d'entiers $k_n \geq 0$. Mais il est impossible de prouver constructivement que toute suite décroissante d'entiers ≥ 0 est constante après un certain rang. Car pour donner le résultat de manière explicite, il faudrait expliquer comment il est possible de calculer le rang en question à partir de la donnée : « une suite décroissante d'entiers arbitraire ».

Pour mieux comprendre pourquoi N1 ne peut pas être démontré constructivement pour $\mathbf{A} = M = \mathbb{Z}$ nous donnons deux exemples.

Tout d'abord nous définissons $G_1 \subset \mathbb{Z}$ comme le sous-groupe engendré par les contre exemples à la Conjecture de Golbach. Plus précisément, G_1 est est donné comme engendré par une suite infinie (g_n) dans $\mathbb{Z}$: pour un $n \in \mathbb{N}$ nous testons si $2n + 4$ est la somme de deux nombres premiers, si la réponse est oui, alors $g_n = 0$, si la réponse est non, alors $g_n = n$. Tant que nous ne disposons pas d'informations suffisamment précises sur la Conjecture de Golbach, nous sommes incapables de savoir si $m \in G_1$, pour n'importe quel $m \neq 0$ dans $\mathbb{N}$. Ainsi G_1 est un objet plutôt étrange. Il est bien défini en ce sens qu'il est engendré par une suite infinie explicite, mais il n'est pas *détachable* : on n'a pas de test pour « $m \in G_1$? » A fortiori nous ne pouvons pas trouver un système fini de générateurs pour G_1.

Ensuite nous définissons $G_2 \subset \mathbb{Z}$ comme le sous-groupe engendré par « le premier contre exemple » à la Conjecture de Golbach. Plus précisément, G_2 est donné comme engendré par la suite infinie (h_n) dans $\mathbb{Z}$, avec $h_m = 0$ sauf si g_m est le premier terme non nul de la suite

(g_n). Dans ce cas $h_m := g_m$. Ici il est facile de voir que G_2 est un sous-groupe détachable. Mais donner explicitement un ensemble fini de générateurs pour G_2 revient à résoudre la Conjecture de Golbach.

La notion N4 est la bonne notion d'un point de vue constructif. Nous *définissons* la noethérianité d'un $\mathbf{A}$-module M comme signifiant N4 :

Définition 1.4.1 (anneaux noethériens)

- *(en mathématiques classiques) Un anneau est dit noethérien lorsqu'il vérifie les conditions équivalentes N1, ..., N5.*
- *(en mathématiques constructives) Un anneau est dit noethérien lorsqu'il vérifie N4.*

Montrons que $\mathbb{Z}^k$ est un $\mathbb{Z}$-module noethérien au sens de N4.

Théorème 1.4 *$\mathbb{Z}^k$ est un $\mathbb{Z}$-module noethérien au sens constructif : toute suite croissante de sous-groupes de type fini de $\mathbb{Z}^k$ a deux termes consécutifs égaux.*

Preuve Si $G \subset H \subset \mathbb{Z}^n$ sont de type fini, nous appliquons le Théorème de réduction de Smith. Les sous-groupes G et H ont des formes réduites de Smith D_G et D_H avec respectivement $g_1, \ldots, g_r, 0, \ldots, 0$ et $h_1, \ldots, h_s, 0, \ldots, 0$ sur la diagonale. Nous laissons le soin au lecteur de démontrer les quatre propriétés suivantes :
— $r \leq s$,
— $r = s = 0$ implique $G = H = 0$,
— si $r = s > 0$ alors $h_1 \cdots h_r$ divise $g_1 \cdots g_r$ ($\widetilde{G} = \widetilde{H} \simeq \mathbb{Z}^r$ cf. théorème 1.1),
— si $r = s > 0$ et $h_1 \cdots h_r = g_1 \cdots g_r$ alors $G = H$.
Nous notons r_G le rang r de G et j_G le produit $g_1 \cdots g_r$ qui est égal à l'ordre du groupe fini $\widetilde{G}/G$. Remarquons que si $r_G = 0$ alors $j_G = 1$.
Si $G_1 \subset G_2 \subset \cdots \subset G_n \subset \cdots$ sont des sous-groupes de type fini de $\mathbb{Z}^k$, nous posons $r_n = r_{G_n}$ et $j_n = j_{G_n}$. Ainsi nous avons :
— $r_n \leq r_{n+1}$ et
— si $r_n = r_{n+1}$ alors j_n divise j_{n+1}
— si $r_n = r_{n+1}$ et $j_n = j_{n+1}$ alors $G_n = G_{n+1}$
Ainsi il est plus ou moins clair que N5 est vrai. Mais nous voulons une preuve constructive de N4. On peut la faire comme suit. Définissons par récurrence une suite croissante infinie (u_n) dans $\mathbb{N}$. Nous posons $u_1 = 1$. A partir de u_n nous définissons u_{n+1} en considérant

$$(r_{u_n}, j_{u_n}), (r_{1+u_n}, j_{1+u_n}), \ldots, (r_{t+u_n}, j_{t+u_n})$$

et en arrêtant la première fois que deux paires consécutives

$$(r_{t-1+u_n}, j_{t-1+u_n}) \text{ et } (r_{t+u_n}, j_{t+u_n}) \ (t \geq 1)$$

sont égales ou bien ont leurs premières coordonnées différentes. Ceci arrive après au plus $\log_2(j_{u_n})$ étapes. Nous notons t_n la valeur de t correspondante et nous posons $u_{n+1} = t_n + u_n$. Ainsi r_{u_n} est une suite croissante infinie dans $\{0, \ldots, k\}$. Deux termes consecutifs sont égaux (au plus tard aux pas $k+1$ et $k+2$). Les sous-groupes correspondants G_{u_n} et $G_{u_{n+1}}$ sont égaux. A fortiori $G_{u_n} = G_{1+u_n} = \ldots = G_{u_{n+1}}$. □

Remarquons que nous avons fait une analyse constructive assez détaillée du théorème de la base adaptée, mais que l'histoire n'est pas terminée. En fait, chaque fois que ce théorème est appliqué en mathématiques classiques, nous avons à chercher un contenu constructif pour le résultat obtenu. Et il n'est pas sûr a priori que le théorème 1.2, le corollaire 1.2.1 et les théorèmes 1.3 et 1.4 donnent toujours la solution.

Exercice 1.4.2 Démontrez en mathématiques classiques que N5 implique N1.

1.5 Le Théorème de la Base de Hilbert

Classiquement, quand un anneau $\mathbf{A}$ est noethérien, il est cohérent. Mais ce résultat n'admet pas de preuve constructive. Le Théorème de la Base de Hilbert affirme que si $\mathbf{A}$ est noethérien, alors $\mathbf{A}[X]$ également.

Analyser le contenu constructif du Théorème de la Base de Hilbert est une tâche assez ardue. Des réponses satisfaisantes ont été données en 1974 par Richman et Seidenberg avec le théorème suivant (notez les deux versions).

Théorème 1.5

1. *Si* $\mathbf{A}$ *est un anneau noethérien cohérent, alors* $\mathbf{A}[X]$ *également.*
2. *Si* $\mathbf{A}$ *est un anneau noethérien cohérent dont les idéaux de type fini sont détachables, alors* $\mathbf{A}[X]$ *également.*

Voir [MRR], [24] et [28]. Le résultat constructif suivant est aussi très important.

Théorème 1.6

1. *Si* $\mathbf{A}$ *est un anneau noethérien cohérent et* M *est un* $\mathbf{A}$*-module de présentation finie, alors* M *est un* $\mathbf{A}$*-module noethérien cohérent.*
2. *Si* $\mathbf{A}$ *est un anneau noethérien cohérent dont les idéaux de type fini sont détachables et* M *est un* $\mathbf{A}$*-module de présentation finie, alors* M *est un* $\mathbf{A}$*-module noethérien cohérent et ses sous-modules de type fini sont détachables.*

En particulier pour un corps discret $\mathbf{K}$ l'anneau des polynomes $\mathbf{K}[X_1, \ldots, X_n]$ est noethérien cohérent.

Les calculs avec les idéaux de type fini de l'anneau $\mathbf{K}[X_1, \ldots, X_n]$ lorsque $\mathbf{K}$ est un *corps discret*([2]) peuvent se faire en utilisant les bases de Gröbner (cf. [2, 3, 10], [CLS]). La théorie des bases de Gröbner peut être rendue entièrement constructive en utilisant les méthodes de Richman et Seidenberg (cf. [19]). Indépendamment de la théorie des bases de Gröbner, les méthodes explicites en géométrie algébrique ont été développées par Greta Hermann et A. Seidenberg (cf. [16, 27, 29]).

D'autres versions constructives de la noethérianité, plus fortes (du point de vue constructif) que la définition 1.4.1 à la Richman-Seidenberg, s'avèrent parfois utile (cf. [6, 22]). Trois tests importants que doit subir toute définition constructive intéressante de la noethérianité sont les suivants :

– la définition doit être équivalente en mathématiques classiques à la définition 1.4.1,
– $\mathbb{Z}$ et tout corps discret doivent vérifier la définition au sens constructif,
– un théorème de la base de Hilbert similaire au théorème 1.5 doit pouvoir être démontré constructivement.

[2] Nous disons qu'un ensemble X est *discret* quand on peut tester explicitement l'égalité de deux éléments de X (donnés conformément à la définition de X.) Pour plus de précisions voir page 10.

2. Logique Constructive

Ce chapitre est consacré à l'exposition de quelques concepts de base des mathématiques constructives dans le style de Bishop.

Par logique constructive, nous entendons la logique des mathématiques constructives.

2.1 Objets de base, Ensembles, Fonctions

Entiers naturels et constructions sont deux notions primitives. Elles ne peuvent pas être définies.

D'autres notions primitives sont liées au langage usuel et difficiles à situer précisément. Par exemple l'égalité du nombre 2 en deux occurrences distinctes.

La formalisation d'un morceau de mathématiques peut être utilisée pour mieux comprendre ce qu'on est en train d'y faire. Mais pour parler à propos d'un formalisme il faut comprendre beaucoup de choses qui sont du même genre de complexité que les entiers naturels. Ainsi le formalisme est seulement un outil et il ne peut pas remplacer les intuitions et les expériences de base (par exemple les entiers naturels, les constructions) : si puissant que soit un ordinateur, il ne comprendra jamais « ce qu'il fait », ou encore, comme le disait René Thom « Tout ce qui est rigoureux est insignifiant ».

Ensembles

Un *ensemble* $(X, =_X, \neq_X)$ est défini en disant :

— comment on peut construire un élément de l'ensemble (nous disons que nous avons défini un *préensemble* X)

— quelle est la signification de l'*égalité* pour deux éléments de l'ensemble (nous avons à montrer que c'est bien une relation d'équivalence)

— quelle est la signification de la *distinction*[1] pour deux éléments de l'ensemble (on dit alors que les éléments sont *discernables* ou *distincts*). Nous avons à montrer les propriétés suivantes :

- $(x \neq_X y \ \wedge \ x =_X x' \ \wedge \ y =_X y') \ \Rightarrow \ x' \neq_X y'$
- $x \neq_X x$ est impossible
- $x \neq_X y \ \Rightarrow \ y \neq_X x$

Ordinairement, on laisse tomber l'indice X pour les symboles $=$ et $\neq$. Si la distinction n'est pas précisée, elle est implicitement définie comme signifiant l'absurdité de l'égalité.

Une relation de distinction est une relation de *séparation* si elle vérifie la propriété de *co-transitivité* suivante (pour trois éléments x, y, z de X arbitraires) :

- $x \neq_X y \ \Rightarrow \ (x \neq_X z \ \vee \ y \neq_X z)$

Une relation de séparation $\neq_X$ est dite *étroite* si $x =_X y$ équivaut à l'absurdité de $x \neq_X y$. Dans un ensemble avec une séparation étroite, la distinction est souvent plus importante que l'égalité.

[1] Cette terminologie *n'est pas* un hommage à Pierre Bourdieu. Tous comptes faits, nous préférons *distinction* à *non-égalité*, qui présente l'inconvénient d'une connotation négative, et à *inégalité* qui est plutot utilisé dans le cadre des relations d'ordre. Pour les nombres réels par exemple, c'est l'égalité et non la distinction qui est une assertion négative.

Un ensemble $(X, =_X, \neq_X)$ est dit *discret* si on a

$$\forall x, y \in X \ (x =_X y \vee x \neq_X y).$$

Dans ce cas la distinction est une séparation étroite et elle équivaut à l'absurdité de l'égalité.

Les entiers naturels
L'ensemble $\mathbb{N}$ est considéré comme bien défini a priori. Notez cependant que constructivement il s'agit d'un *infini potentiel* et pas d'un *infini actuel*. On entend par l'idée d'infini potentiel que l'infinitude de $\mathbb{N}$ est appréhendée comme une notion essentiellement négative : on n'a jamais fini d'épuiser les entiers naturels. Au contraire, la sémantique de $\mathbb{N}$ en mathématiques classiques est celle d'un infini achevé, qui existe « quelque part » au moins de manière purement idéale.

Un entier naturel peut être codé d'une manière usuelle. La comparaison de deux entiers donnés sous forme codée peut être faite de manière sûre. En bref, l'ensemble des entiers naturels est un ensemble discret et la relation d'ordre est *décidable* :

$$\forall n, m \in \mathbb{N} \quad (n < m \quad \vee \quad n = m \quad \vee \quad n > m)$$

Ensembles de couples
Quand deux ensembles sont définis leur *produit cartésien* est également défini, de manière naturelle : la fabrication des couples d'objets est une construction élémentaire. L'égalité et la distinction sur un produit cartésien sont définis de manière naturelle.

Fonctions
L'ensemble $\mathbb{N}^{\mathbb{N}}$ des suites d'entiers naturels dépend de la notion primitive de construction. Un élément de $\mathbb{N}^{\mathbb{N}}$ est une construction qui prend en entrée un élément de $\mathbb{N}$ et donne en sortie un élément de $\mathbb{N}$. L'égalité de deux éléments dans $\mathbb{N}^{\mathbb{N}}$ est l'*égalité extensionnelle* :

$$(u_n) =_{\mathbb{N}^{\mathbb{N}}} (v_n) \quad \text{signifie} \quad \forall n \in \mathbb{N} \ \ u_n = v_n$$

Ainsi, l'égalité entre deux éléments de $\mathbb{N}^{\mathbb{N}}$ demande a priori une infinité de « calculs élémentaires », en fait l'égalité réclame une preuve.
La distinction de deux éléments de $\mathbb{N}^{\mathbb{N}}$ est la relation de *distinction extensionnelle* :

$$(u_n) \neq_{\mathbb{N}^{\mathbb{N}}} (v_n) \quad \overset{\text{def}}{\iff} \quad \exists n \in \mathbb{N} \ \ u_n \neq v_n$$

Ainsi, la distinction de deux éléments de $\mathbb{N}^{\mathbb{N}}$ peut être constatée par un simple calcul.

L'argument diagonal de Cantor est constructif. Il montre que $\mathbb{N}^{\mathbb{N}}$ est *beaucoup plus compliqué* que $\mathbb{N}$. D'un point de vue constructif, $\mathbb{N}$ et $\mathbb{N}^{\mathbb{N}}$ sont seulement des infinis potentiels : cela n'a pas de signification de dire qu'un infini potentiel est *plus grand* qu'un autre.

Quand vous dites « Je vous donne une suite d'entiers naturels », vous devez prouver que la construction $n \mapsto u_n$ que vous proposez marche pour n'importe quelle entrée n. Par ailleurs, quand vous dites « Soit (u_n) une suite arbitraire de nombres naturels », la seule chose que vous savez avec certitude est que pour tout $n \in \mathbb{N}$ vous avez $u_n \in \mathbb{N}$, et que cet u_n est non ambigu : vous pouvez concevoir la suite comme donnée par un oracle. En fait, vous pourriez a priori demander, de manière symétrique, une preuve que la construction $n \mapsto u_n$ marche pour toute entrée n.

Mais, dans le constructivisme à la Bishop, on ne fait aucune hypothèse précise concernant « ce que sont les constructions légitimes de $\mathbb{N}$ vers $\mathbb{N}$ » ni non plus sur « qu'est-ce précisément qu'une preuve qu'une construction marche ? ». Ainsi nous sommes dans une situation disymétrique.

Cette disymétrie a la conséquence suivante. Tout ce que vous prouvez a un contenu calculatoire. Mais tout ce que vous prouvez est également valide d'un point de vue classique. Les mathématiques classiques pourraient voir les mathématiques constructives comme parlant

seulement d'objets constructifs. Et les mathématiques constructives de Bishop sont certainement intéressées au premier chef par les objets constructifs (cf. [1]). Mais en fait les mathématiques constructives à la Bishop font des preuves constructives qui marchent pour n'importe quel type d'objets mathématiques. Les théorèmes que l'on trouve dans [BB] et [MRR] sont valables en mathématiques classiques, mais ils supportent aussi l'interprétation constructive russe (dans laquelle tous les objets mathématiques sont des mots d'un langage formel qu'on pourrait fixer une fois pour toutes) ou encore la philosophie intuitionniste de Brouwer, qui a une composante nettement idéaliste.

Après cette digression revenons à nos moutons : les fonctions. De manière générale, une *fonction* $f : X \to Y$ est une construction qui prend en entrée un $x \in X$ et une preuve que $x \in X$ et donne en sortie un $y \in Y$ et une preuve que $y \in Y$. En outre cette construction doit être *extensionnelle* :

$$x =_X x' \Rightarrow f(x) =_Y f(x') \qquad \text{et} \qquad f(x) \neq_Y f(x') \Rightarrow x \neq_X x'$$

Quand X et Y sont des ensembles bien définis, on considére (dans les mathématiques constructives à la Bishop) que l'ensemble $\mathcal{F}(X, Y)$ des fonctions $f : X \to Y$ est aussi bien défini. Pour l'égalité et la distinction on prend les définitions extensionnelles usuelles.

Une fonction $f : X \to Y$ est *injective* si elle vérifie

$$f(x) =_Y f(x') \Rightarrow x =_X x' \qquad \text{et} \qquad x \neq_X x' \Rightarrow f(x) \neq_Y f(x')$$

Ensembles finis, bornés, énumérables et dénombrables

Nous donnons maintenant un certain nombre de définitions constructivement pertinentes en relation avec les concepts d'ensembles finis, infinis et dénombrables en mathématiques classiques.

- Un préensemble X est dit *énumérable* si on a donné un moyen de l'énumérer en lui laissant la possibilité d'être vide, ce qui se passe en pratique comme suit : on donne un $\alpha \in \{0,1\}^{\mathbb{N}}$ et une opération φ qui vérifient
  - si $\alpha(n) = 1$ alors φ construit à partir de l'entrée n un élément de X
  - tout élément de X est construit de cette façon.
- Un ensemble X *finiment énumérable* est défini de manière analogue, en remplaçant $\mathbb{N}$ par un segment $[0, n]$ de $\mathbb{N}$.
- Un ensemble est dit *dénombrable* s'il est énumérable (en tant que préensemble) et discret.
- Un ensemble est *fini* s'il y a une bijection entre cet ensemble et l'ensemble des entiers $< n$ (pour un certain entier n).
- Si n est un entier non nul, on dit qu'un ensemble *possède au plus n éléments* si pour toute famille $(a_i)_{i=0,\ldots,n}$ dans l'ensemble il existe des entiers h et k $(0 \leq h < k \leq n)$ tels que $a_h = a_k$.
- Un ensemble X est *borné en nombre* (*borné* tout court s'il n'y a pas d'ambiguité) s'il existe un entier n non nul tel que X ait au plus n éléments.
- Un ensemble X est *faiblement fini* si pour toute suite $(u_n)_{n\in\mathbb{N}}$ dans X il existe m et $p > m$ tels que $u_m = u_p$.
- Un ensemble X est *infini* s'il existe une application injective $\mathbb{N} \to X$.
- Un ensemble X est *non infini* s'il est absurde qu'il soit infini.

Exercice 2.1.1 Montrer qu'un ensemble infini et dénombrable peut être mis en bijection avec $\mathbb{N}$.

Parties d'un ensemble

Une partie d'un ensemble $(X, =_X, \neq_X)$ est définie par une propriété $P(x)$ *portant sur les éléments de* X, c.-à-d. vérifiant

$$\forall x, y \in X \ (\ (\ x = y \ \wedge \ P(x)) \ \Longrightarrow \ P(y)\ )$$

Un élément de la partie $\{x \in X\ ;\ P(x)\}$ est donné par un couple (x, p) où x est un élément de X et p est une preuve que $P(x)$([2]). Deux propriétés concernant les éléments de X définissent la même partie lorsqu'elles sont équivalentes.

On peut aussi présenter les choses de la manière suivante, qui, bien que revenant au même, fait un peu moins mal à la tête au nouvel arrivant. Une partie de X est donnée par un couple (Y, φ) où Y est un ensemble et φ est une fonction injective de Y dans X([3]). Deux couples (Y, φ) et (Y', φ') définissent la même partie de X si on a

$$\forall y \in Y\ \exists y' \in Y'\ \varphi(y) = \varphi'(y') \qquad \text{et} \qquad \forall y' \in Y'\ \exists y \in Y\ \varphi(y) = \varphi'(y').$$

On tâche en général en mathématiques constructives d'éviter de considérer l'ensemble des parties de X, qui n'a pas clairement le statut d'un ensemble (au sens donné ci-dessus).

Une partie Y de X est dite *détachable* lorsqu'on a un test pour « $x \in Y$? » lorsque $x \in X$. Les parties détachables de X forment un ensemble qui s'identifie à $\{0,1\}^X$.

Constructivement, on ne connaît aucune partie détachable de $\mathbb{R}$, hormis $\emptyset$ et $\mathbb{R}$: *il n'y a pas de trou dans le continu sans la logique du tiers exclu.*

Une variante constructivement intéressante pour une partie Y_1 de X est obtenue en considérant un couple (Y_1, Y_2) de parties de X qui vérifient les deux propriétés suivantes

$$\forall x_1 \in Y_1\ \forall x_2 \in Y_2\ \ x_1 \neq_X x_2 \qquad \text{et} \qquad \forall x \in X\ \neg(x \notin Y_1\ \wedge\ x \notin Y_2)$$

Le *complémentaire* est alors donné par le couple (Y_2, Y_1), ce qui rétablit une certaine symétrie.

L'ensemble des parties d'un ensemble ?
Si on admet l'ensemble des parties de X, qu'on note $\mathcal{P}(X)$ alors il y a une bijection naturelle entre $\mathcal{P}(X)$ et $\mathcal{F}(X, \mathcal{P}(\{0\})) = \mathcal{P}(\{0\})^X$. En fait toute la difficulté avec l'ensemble des parties est concentrée sur l'ensemble $\mathcal{P}(\{0\})$, c'est-à-dire sur l'ensemble des *valeurs de vérité*. En mathématiques classiques, on admet le *principe du tiers exclu* **PTE** :

$$\mathcal{P}(\{0\}) = \{\{0\}, \emptyset\}$$

(ce qui revient à dire que l'ensemble des valeurs de vérité est égal à $\{\mathsf{Vrai}, \mathsf{Faux}\}$) et on n'a évidemment plus aucun problème avec $\mathcal{P}(X)$. En fait il s'agit plutot de l'art de l'esquive : cachez ce problème que je ne saurais voir.

Il ne semble pas qu'on connaisse un seul théorème mathématique pertinent de mathématiques classiques dont l'étude du point de vue constructif nécessite le recours à l'ensemble $\mathcal{P}(\{0\})$.

2.2 Affirmer signifie prouver

En mathématiques constructives la vérité est aussi le résultat d'une construction. Si P est une assertion mathématique, nous écrirons « $\vdash P$ » pour « nous avons une preuve de P ».

Les assertions élémentaires peuvent être testées par des calculs simples. E.g., la comparaison de deux entiers naturels. Quand une assertion signifie une infinité d'assertions élémentaires (e.g., la conjecture de Golbach), les mathématiques constructives considèrent qu'elle n'est pas a priori « vraie ou fausse ». A fortiori, les assertions ayant une complexité logique encore plus grande ne sont pas considérées (d'un point de vue constructif) comme ayant une valeur de vérité absolue.

Ceci ne doit pas être nécessairement considéré comme une position philosophique concernant la vérité. Mais c'est sûrement une position mathématique concernant les assertions mathématiques. En fait, cette position est nécessaire pour avoir une signification calculatoire pour tous les théorèmes qui sont prouvés de manière constructive.

[2] Par exemple, un nombre réel ≥ 0 est *un peu plus qu*'un nombre réel.

[3] Par exemple on peut définir les nombres réels ≥ 0 comme ceux qui sont donnés par des suites de Cauchy de rationnels ≥ 0.

Digression carrément philosophique. Cette position est également à distinguer de la position qui consiste à dire qu'il y a certainement différents univers mathématiques possibles, par exemple l'un dans lequel l'hypothèse du continu[4] est vraie, un autre dans lequel elle est fausse. Cette position est naturellement parfaitement défendable (Cantor, et sans doute Gödel, l'auraient refusée au nom d'un réalisme platonicien des Idées), mais elle intéresse peu les mathématiques constructives à la Bishop qui ont pour objet d'étude une abstraction de l'univers concret des calculs finis, avec l'idée que cette abstraction doit correspondre d'aussi près que possible à la réalité qu'elle veut décrire. Ainsi, l'hypothèse du continu est plutot dans ce cadre considérée comme vide de signification, car il est absurde de vouloir comparer des infinis potentiels selon leur taille. Si on désire les comparer selon leur complexité, on s'aperçoit bien vite qu'il n'y a aucun espoir de mettre une vraie relation d'ordre total dans ce fouillis. En conséquence, l'hypothèse du continu ne semble rien d'autre aujourd'hui qu'un jeu des spécialistes de la théorie formelle ZF. Mais chacun et chacune est bien libre de croire Platon, ou même Cantor, ou Zermelo-Frankel, ou encore, pourquoi pas, de croire en la multiplicité des mondes. Personne ne pourra jamais lui prouver qu'il a tort. Et rien ne dit par ailleurs que le jeu ZF ne s'avèrera pas un jour vraiment utile, par exemple pour comprendre certains points subtils des mathématiques qui ont une signification concrète. □

2.3 Connecteurs et quantificateurs

Ici nous donnons l'explication « Brouwer-Heyting-Kolmogorov » pour la signification constructive des symboles logiques usuels. Ce sont seulement des explications, pas des définitions. Concernant le point de vue de Kolmogorov plus précisément on pourra consulter [5, 14].

Conjonction : $\vdash P \wedge Q$ signifie $\vdash P$ et $\vdash Q$ (comme pour la logique classique). En d'autres termes : une preuve de $P \wedge Q$ est un couple (p, q) où p est une preuve de P et q une preuve de Q.

Disjonction : $\vdash P \vee Q$ signifie $\vdash P$ ou $\vdash Q$ (ce qui ne marche pas avec la logique classique). En d'autres termes : une preuve de $P \vee Q$ est un couple (n, r) avec $n \in \{0, 1\}$. Si $n = 0$, r doit être une preuve de P, si $n = 1$, r doit être une preuve de Q.

Implication : $\vdash P \Rightarrow Q$ a la signification suivante : une preuve de $P \Rightarrow Q$ est une construction $p \mapsto q$ qui transforme toute preuve p de P en une preuve q de Q.

Négation : $\vdash \neg P$ signifie $\vdash P \Rightarrow 0 = 1$.

Quantificateur universel : (similaire à l'implication). Une quantification est toujours une quantification sur les objets d'un ensemble défini au préalable. Soit $P(x)$ une propriété concernant les objets x d'un ensemble X, alors $\vdash \forall x \in X \ P(x)$ signifie : nous avons une construction $(x, q) \mapsto p(x, q)$ qui prend en entrée un $x \in X$ et une preuve q que $x \in X$ et donne en sortie une preuve $p(x, q)$ de l'assertion $P(x)$.

Pour une quantification sur $\mathbb{N}$ on estime que la donnée d'un enteir x (sous-entendu, sous forme standard) suffit à prouver que $x \in \mathbb{N}$: la partie q dans le couple (x, q) ci dessus peut être omise. Par exemple supposons que P et Q dépendent d'une variable $x \in \mathbb{N}$, alors une preuve de $\forall x \in \mathbb{N} \ (P(x) \vee Q(x))$ est une construction $\mathbb{N} \ni x \mapsto (n(x), r(x))$ avec $n(x) \in \{0, 1\}$. Si $n(x) = 0$, $r(x)$ doit être une preuve de $P(x)$. Si $n(x) = 1$, $r(x)$ doit être une preuve de $Q(x)$.

Quantificateur existentiel : (similaire à la disjonction) Une quantification est toujours une quantification sur les objets d'un ensemble défini au préalable. Soit $P(x)$ une propriété concernant les objets x d'un ensemble X, alors une preuve de $\vdash \exists x \in X \ P(x)$ est un triplet (x, p, q) où x est un objet, p est une preuve de $x \in X$ et et q une preuve de l'assertion $P(x)$.

[4] L'hypothèse du continu est, dans la théorie des ensembles classiques, l'affirmation qu'il n'y a pas de cardinal strictement compris entre celui de $\mathbb{N}$ et celui de $\mathbb{R}$, autrement dit, que toute partie infinie de $\mathbb{R}$ est équipotente à $\mathbb{N}$ ou à $\mathbb{R}$.

Exercice 2.3.1 Soit $P(x, y)$ une propriété concernant les entiers naturels. Montrer que

$$\vdash \forall x \in \mathbb{N}\ \ \exists y \in \mathbb{N}\ \ P(x, y)$$

signifie : voici une construction $u : x \mapsto y$ de $\mathbb{N}$ vers $\mathbb{N}$ et une preuve de $\vdash \forall x \in \mathbb{N}\, P(x, u(x))$.

Exercice 2.3.2 Soient $A,\ B,\ C$ des propriétés mathématiques. Montrer les équivalences suivantes :

- $((A \Rightarrow C)\ \wedge\ (B \Rightarrow C))\ \iff\ ((A\ \vee\ B)\ \Rightarrow\ C)$
- $\neg(A\ \vee B\ )\ \iff\ (\neg A \wedge \neg B)$
- $(A \Rightarrow (B \Rightarrow C))\ \iff\ ((A\ \wedge\ B)\ \Rightarrow\ C)$
- $(A \Rightarrow B)\ \implies\ (\neg B\ \Rightarrow\ \neg A)$
- $\neg\neg\neg A\ \iff\ \neg A$

Montrer que si en outre on a $A\ \vee \neg A$, $B\ \vee \neg B$ alors on a :

- $\neg\neg A\ \iff\ A$
- $\neg(A\ \wedge B\ )\ \iff\ (\neg A \vee \neg B)$
- $(A \Rightarrow B)\ \iff\ (\neg A \vee B)$

Remarque. Puisque $\neg\neg\neg A \Leftrightarrow \neg A$, une propriété C est équivalente à une propriété $\neg B$ (pour une certaine propriété B non encore précisée) si et seulement si $\neg\neg C \Rightarrow C$. Ainsi, on peut définir en mathématiques constructives le concept de *propriété négative*. En mathématiques classiques, le concept n'a pas d'intérêt puisque toute propriété est négative. En mathématiques constructives il faut prendre garde que Vrai est aussi une propriété négative : puisque Faux $\Rightarrow$ Faux, $\neg$Faux est vrai.

Exercice 2.3.3 Montrer que la distinction de $\mathbb{N}^{\mathbb{N}}$ est une relation de séparation étroite.

2.4 Calculs mécaniques

Nous discutons ici un point qui est souvent difficile à comprendre pour les mathématiciens classiques. Une fonction de $\mathbb{N}$ vers $\mathbb{N}$ est donnée par une construction. Les constructions usuelles correspondent à des programmes algorithmiques qui peuvent tourner sur un ordinateur « idéal »[5]. Ceci conduit à la notion de *calculs mécaniques*. Une fonction $f \in \mathbb{N}^{\mathbb{N}}$ obtenue par un tel calcul mécanique est appelée une *fonction récursive*. Le sous-ensemble $\mathbf{Rec} \subset \mathbb{N}^{\mathbb{N}}$ formé par les fonctions récursives peut être décrit de manière plus formelle comme nous l'expliquons maintenant.

Rappelons qu'une *fonction primitive récursive* est une fonction $\mathbb{N}^k \to \mathbb{N}$ qui peut être définie par composition ou par récurrence simple à partir de fonctions primitives récursives déjà définies (nous commençons avec les fonctions constantes et l'addition $+$). Appelons $\mathbf{Prim}_2$ l'ensemble des fonctions primitives récursives $\mathbb{N}^2 \to \mathbb{N}$. On vérifie sans peine que $\mathbf{Prim}_2$ est un ensemble énumérable. Une fonction $\beta \in \mathbf{Prim}_2$ est pensée comme simulant l'exécution d'un programme. Pour une entrée n nous calculons $\beta(n, m)$ pour $m = 0, 1, \ldots$ jusqu'à ce que nous trouvions l'instruction Stop, qui signifie $\beta(n, m) \neq 0$. La fonction $\alpha \in \mathbf{Rec}$ calculée par le « programme » $\beta \in \mathbf{Prim}_2$ est : $f : n \mapsto \beta(n, m_n) - 1$ où m_n est la première valeur de m telle que $\beta(n, m) \neq 0$.

Ainsi nous obtenons une application surjective d'un sous-ensemble *Rec* de $\mathbf{Prim}_2$ sur $\mathbf{Rec}$, et $\mathbf{Rec}$ peut être identifié au préensemble *Rec* muni de l'égalité et de la distinction convenables. Cela signifie que $\mathbf{Rec}$ est défini comme un « quotient »([6]) d'un sous-ensemble d'un ensemble énumérable. Les éléments de la partie *Rec* de $\mathbf{Prim}_2$ sont définis par la condition suivante :

$$\beta \in Rec \overset{\text{def}}{\iff} (*)\ :\ (\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}\ \ \beta(n, m) \neq 0)$$

[5] Un ordinateur disposant de tout l'espace et de tout le temps nécessaire au calcul envisagé.

[6] Puisque $\mathbf{Rec}$ est l'image de *Rec* par une application surjective.

D'un point de vue classique, pour n'importe quel $\beta \in \mathbf{Prim}_2$, l'assertion $(*)$ ci-dessus est vraie ou fausse dans l'absolu, en référence à la logique du tiers exclu (ou, si on préfère, à l'infinité actuelle de $\mathbb{N}$) : la notion de calcul mécanique peut ainsi être définie sans référence aucune à une notion primitive de construction.

D'un point de vue constructif par contre, l'assertion $(*)$ doit être prouvée, et une telle preuve est elle-même une construction. Ainsi *la notion de calcul mécanique dépend de la notion de construction, qui ne peut pas être définie.*

Signalons pour terminer ce paragraphe que le constructivisme russe à la Markov admet comme principe fondamental l'égalité $\mathbf{Rec} = \mathbb{N}^{\mathbb{N}}$, principe parfois appelé **Fausse Thèse de Church**. Voir [Be, BR] et [25]. La vraie Thèse de Church est qu'aucun système de calcul automatique ne pourra jamais calculer d'autres fonctions que les fonctions récursives : on pourra améliorer les performances des ordinateurs, mais aucun système de calcul automatique ne pourra dépasser ce qu'ils savent calculer « en principe » si on leur donne le temps et l'espace nécessaire. La vraie Thèse de Church est extrêmement vraisemblable, mais elle n'est évidemment suceptible d'aucune preuve.

2.5 Principes d'omniscience

On appelle *principe d'omniscience* un principe qui, bien que vrai en mathématiques classiques, pose manifestement problème en mathématiques constructives, car il suppose une connaissance a priori de ce qui se passe avec un infini potentiel. Le mot omniscience vaut donc ici pour « prescience de l'infini potentiel ». Les principes d'omniscience ont en général des contre-exemples durs dans les mathématiques constructives russes. Ils ne peuvent cependant pas être démontrés faux dans les mathématiques constructives à la Bishop, qui sont compatibles avec les mathématiques classiques.

Le Petit Principe d'Omniscience
Soit $\alpha = (\alpha_n) \in \{0,1\}^{\mathbb{N}}$ une *suite binaire*, i.e., une construction qui donne pour chaque entier naturel (en entrée) un élément de $\{0,1\}$ (en sortie). Considérons les assertions suivantes :

$$\begin{array}{rcl} P(\alpha) & : & \alpha_n = 1 \text{ pour un } n, \\ \neg P(\alpha) & : & \alpha_n = 0 \text{ pour tout } n, \\ P(\alpha) \vee \neg P(\alpha) & : & P(\alpha) \text{ ou } \neg P(\alpha), \\ \forall \alpha \ \ (P(\alpha) \vee \neg P(\alpha)) & : & \text{pour toute suite binaire } \alpha,\ P(\alpha) \text{ ou } \neg P(\alpha). \end{array}$$

Une preuve constructive de $P(\alpha) \vee \neg P(\alpha)$ devrait fournir un algorithme qui ou bien montre que $\alpha_n = 0$ pour tout n, ou bien calcule un entier naturel n tel que $\alpha_n = 1$.

Un tel algorithme est beaucoup trop performant, car il permettrait de résoudre de manière automatique un grand nombre de conjectures importantes. En fait nous savons que si un tel algorithme existe, il n'est certainement pas « mécaniquement calculable » : un programme qui tourne sur machine ne peut sûrement pas accomplir un tel travail même lorsqu'on impose la limitation sur l'entrée α qu'elle soit une suite binaire primitive récursive explicite. Cette impossibilité est un grand théorème d'informatique théorique, souvent indiqué sous l'appelation « théorème de la halte des programmes ».

Théorème de la halte des programmes (On ne peut pas tout savoir)
Sous trois formes immédiatement équivalentes :

- *Le débuggage ne peut pas être automatisé : il n'existe pas de programme T qui puisse tester si un programme arbitraire P finira par aboutir à l'instruction Stop.*
- *Il n'existe pas de programme qui puisse tester si une suite primitive récursive arbitraire est identiquement nulle.*

– *Il n'existe pas de programme U qui prenne en entrée deux entiers, donne en sortie un booléen, et qui énumère toutes les suites binaires programmables (la suite $n \mapsto U(m,n)$ est la m-ème suite énumérée par U).*

Non seulement ce théorème, sous sa dernière formulation, ressemble au théorème de Cantor qui affirme qu'on ne peut pas énumérer l'ensemble des suites binaires, mais la preuve, très simple, est essentiellement la même.

Bien que le théorème précédent n'interdise pas a priori l'existence d'une procédure effective mais non mécanisable pour résoudre de manière systématique ce type de problèmes, il confirme l'idée intuitive selon laquelle il faudra toujours faire preuve de nouvelle inventitivité pour progresser dans notre connaissance du monde mathématique.

Ainsi, d'un point de vue constructif, nous rejetons le *Limited Principle of Omniscience* :

– **LPO** : Si (α_n) est une suite binaire, alors ou bien il existe un n tel que $\alpha_n = 1$, ou bien $\alpha_n = 0$ pour tout n.

Le principe **LPO** a de nombreuses formes équivalentes, e.g. :

1. Si A est une propriété *élémentaire*, i.e., équivalente à $\exists n\ \alpha(n) \neq 0$ pour un certain $\alpha \in \mathbb{N}^{\mathbb{N}}$, on a $A \vee \neg A$. Autrement dit :
$$\forall \alpha \in \mathbb{N}^{\mathbb{N}},\ \ (\alpha \neq 0 \vee \alpha = 0)$$
2. Toute suite dans $\mathbb{N}$ est ou bien bornée, ou bien non bornée.
3. Toute suite décroissante dans $\mathbb{N}$ est constante à partir d'un certain rang.
4. D'une suite bornée dans $\mathbb{N}$ on peut extraire une sous-suite infinie constante.
5. Toute partie énumérable de $\mathbb{N}$ est détachable.
6. Toute partie énumérable de $\mathbb{N}$ est ou bien finie, ou bien infinie.
7. Pour toute suite double d'entiers $\beta : \mathbb{N}^2 \to \mathbb{N}$ on a :
$$\forall n\ \exists m\ \ \beta(n,m) = 0 \quad \vee \quad \exists n\ \forall m\ \ \beta(n,m) \neq 0$$
8. Tout sous-groupe détachable de $\mathbb{Z}$ est engendré par un seul élément.
9. Tout sous-groupe de $\mathbb{Z}^p$ engendré par une suite infinie est de type fini.
10. $\forall x \in \mathbb{R}$, ($x \neq 0\ \vee\ x = 0$).
11. $\forall x \in \mathbb{R}$, ($x > 0\ \vee\ x = 0\ \vee\ x < 0$).
12. Toute suite bornée monotone dans $\mathbb{R}$ converge.
13. D'une suite bornée dans $\mathbb{R}$ on peut extraire une sous-suite convergente.
14. Tout nombre réel est ou bien rationnel ou bien irrationnel.
15. Tout sous-espace de vectoriel de type fini de $\mathbb{R}^n$ admet une base.
16. Tout espace de Hilbert séparable admet ou bien une base hilbertienne finie ou bien une base hilbertienne dénombrable.

Le Mini Principe d'Omniscience

Un autre principe d'omniscience, plus faible, **LLPO** (Lesser Limited Principle of Omniscience) est le suivant :

– Si A et B sont deux propriétés élémentaires on a
$$\neg(A\ \wedge\ B) \quad \Longrightarrow \quad (\neg A\ \vee\ \neg B)$$

Ce principe **LLPO** a de nombreuses formes équivalentes, e.g. :

1. $\forall \alpha, \beta$ suites croissantes $\in \mathbb{N}^{\mathbb{N}}$, si $\forall n\ \alpha(n)\beta(n) = 0$ alors $\alpha = 0$ ou $\beta = 0$.

2. $\forall \alpha, \beta \in \mathbb{N}^{\mathbb{N}}$, si $\forall n, m \in \mathbb{N}\ \ \alpha(n) \neq \beta(m)$ alors $\exists \gamma \in \mathbb{N}^{\mathbb{N}}$ tel que
$$\forall n, m \in \mathbb{N} \quad (\gamma(\alpha(n)) = 0 \ \wedge\ \gamma(\beta(m)) = 1)$$
3. $\forall \alpha \in \mathbb{N}^{\mathbb{N}}$, $\exists k \in \{0,1\}$, ($\exists n\ \alpha(n) = 0\ \Rightarrow\ \exists m\ \alpha(2m+k) = 0$).
4. $\forall x \in \mathbb{R}\quad (\ x \leq 0\ \vee\ x \geq 0\ )$ (ceci permet de faire de nombreuses preuves par dichotomie avec les nombres réels.)
5. $\forall x, y \in \mathbb{R}\quad (\ xy = 0\ \Rightarrow\ (\ x = 0\ \vee\ y = 0\ )\ )$.
6. L'image d'un intervalle $[a, b] \subset \mathbb{R}$ par une fonction réelle uniformément continue est un intervalle $[c, d]$.
7. Une fonction réelle uniformémént continue sur un espace métrique compact atteint ses bornes.
8. $\mathbf{KL}_1$ (une des versions du lemme de König) Tout arbre infini explicite à embranchements finis possède une branche infinie.

Il est connu que si un algorithme existe pour le troisième item il ne peut pas être « mécaniquement calculable » (i.e., récursif) : on peut construire α et β mécaniquement calculables vérifiant l'hypothèse, mais pour lesquels aucun γ mécaniquement calculable ne vérifie la conclusion. De même, l'arbre singulier de Kleene est un arbre récursif dénombrable infini à embranchements finis qui ne possède aucune branche infinie récursive. Ceci donne un « contre-exemple récursif » pour $\mathbf{KL}_1$.

Nous allons montrer maintenant l'équivalence $\mathbf{KL}_1 \Leftrightarrow \mathbf{LLPO}$.

Un arbre infini explicite à embranchements finis peut être décrit par un ensemble $A \subset \mathbf{Lst}(\mathbb{N})$ de listes d'entiers vérifiant les propriétés suivantes (les quatre premières correspondant à la notion d'arbre explicite à embranchements finis) :

- La liste vide [ ] représente la racine de l'arbre, elle appartient à A,
- un $a = [a_1, \ldots, a_n] \in A$ représente à la fois un noeud de l'arbre et le chemin qui mène de la racine jusqu'au noeud,
- si $[a_1, \ldots, a_n] \in A$ et $n \geq 0$, alors $[a_1, \ldots, a_{n-1}] \in A$,
- si $a = [a_1, \ldots, a_n] \in A$ alors les $x \in \mathbb{N}$ tels que $[a_1, \ldots, a_n, x] \in A$ forment un segment $\{x \in \mathbb{N}\ ;\ x < \mu(a)\}$ où $\mu(a)$ est donné explicitement en fonction de a : les branches issues de a sont numérotées $0, \ldots, \mu(a) - 1$.
- Pour tout $n \in \mathbb{N}$ il y a au moins un $[a_1, \ldots, a_n] \in A$ (l'arbre est explicitement infini).

Ainsi la partie A de $\mathbf{Lst}(\mathbb{N})$ est détachable (c'est en fin de compte ce que signifie ici le mot « explicite »). Et A est dénombrable.

Preuve de $\mathbf{KL}_1 \Leftrightarrow \mathbf{LLPO}$.
Nous prenons pour **LLPO** la varaiante donnée dans l'item 1.
Supposons $\mathbf{KL}_1$. Soit $\alpha, \beta \in \mathbb{N}^{\mathbb{N}}$ comme dans l'item 1. Considérons l'arbre suivant. Après la racine on ouvre deux branches qui se poursuivent indéfiniment sans jamais créer de nouveaux embranchements, jusqu'à ce que $\alpha(n) \neq 0$ ou $\beta(n) \neq 0$ (si jamais cela se produit). Si cela se produit avec $\alpha(n) \neq 0$, on arrête la branche de gauche et on continue celle de droite. Si c'est avec $\beta(n) = 0$, on fait le contraire. Donner explicitement une branche infinie dans cet arbre revient à certifier d'avance que $\alpha = 0$ ou $\beta = 0$.

Inversement supposons **LLPO**. Considérons un arbre infini explicite à embranchements finis. Supposons sans perte de généralité que l'arbre est binaire : au delà d'un noeud il y a au plus deux branches. Nous prouvons par récurrence que nous pouvons sélectionner jusqu'à la profondeur n un chemin qui aboutit à un noeud K_n en dessous duquel l'arbre est infini. Ceci est vrai pour $n = 0$ par hypothèse. Si cela est vrai pour n, il y a au moins une branche en dessous du noeud K_n sélectionné. S'il y en a deux, considérons les suites α_n et $\beta_n \in \mathbb{N}^{\mathbb{N}}$ définies comme suit :
— $\alpha_n(m) = 0$ si il y a au moins une branche de longueur m en dessous de K_n partant sur la droite, sinon $\alpha_n(m) = 1$

— $\beta_n(m) = 0$ si il y a au moins une branche de longueur m en dessous de K_n partant sur la gauche, sinon $\beta_n(m) = 1$.
Par hypothèse de récurrence α_n et β_n sont des suites croissantes dont le produit est nul. On applique l'item 1 : l'une des deux suites est nulle et cela nous donne le moyen de sélectionner le chemin vers la droite ou celui vers la gauche. □

Le Principe du Tiers Exclu
Le Principe du Tiers Exclu (**PTE**) affirme que $P \vee \neg P$ est vrai pour toute proposition P. Ce principe d'omniscience extrêmement fort implique **LPO**. Il suppose de manière implicite que des ensembles tels que $\mathbb{N}$ ou $\mathbb{N}^{\mathbb{N}}$ ou même nettement plus compliqués, sont des *infinis actuels*. Il implique également qu'un ensemble X est discret dès que $\neg(x \neq_X y) \Rightarrow x =_X y$ ou que $\neg(x =_X y) \Rightarrow x \neq_X y$ (donc en particulier si on définit $x \neq_X y$ comme signifiant $\neg(x =_X y)$).

Exercices

Exercice 2.5.1 Expliquez pourquoi les notions d'ensemble fini, finiment énumérable, borné en nombre, faiblement fini, énumérable et borné en nombre, énumérable et non infini, non infini, ne peuvent pas être identifiées en mathématiques constructives. Expliquez pourquoi ces notions coïncident si on admet le principe du tiers exclu.

Exercice 2.5.2 Démontrer quelques unes des équivalences signalées pour **LPO**.

Exercice 2.5.3 Démontrer quelques unes des équivalences signalées pour **LLPO**.

2.6 Principes problématiques en mathématiques constructives

Nous entendons par principes problématiques des principes qui, quoique vérifiés en pratique si on fait des mathématiques constructives dans le style de Bishop, sont indémontrables constructivement. En mathématiques classiques, ils peuvent être connus comme vrais ou connus comme faux. Par exemple, en pratique, chaque fois qu'un $\alpha \in \mathbb{N}^{\mathbb{N}}$ est bien défini constructivement, il peut être calculé par un programme. Autrement dit, en pratique, la fausse Thèse de Church, écrite sous forme $\mathbf{Rec} = \mathbb{N}^{\mathbb{N}}$, est vérifiée en mathématiques constructives. Il s'agit d'un principe faux en mathématiques classiques. Par contre, les mathématiques constructives russes le prennent comme un axiome fondamental.

Le livre [Be] fait un étude systématique de nombreux principes problématiques en mathématiques constructives.

Nous allons ici examiner (brièvement) seulement deux principes problématiques, tous deux vrais en mathématiques classiques.

Le Principe de Markov
Le *Principe de Markov*, **MP**, est le suivant :

$$\forall x \in \mathbb{R} \quad (\neg x = 0 \Rightarrow x \neq 0)$$

Affirmer **MP** revient à dire : pour toute suite binaire α, s'il est impossible que tous ses termes soient nuls, alors il doit y avoir un terme non nul.

C.-à-d. encore : si A est une propriété élémentaire alors $\neg\neg A \Rightarrow A$. L'école constructive russe admet **MP**. En fait, pour un $\alpha \in \mathbb{N}^{\mathbb{N}}$, il semble impossible de donner une preuve constructive de $\neg(\alpha = 0)$ sans trouver un n tel que $\alpha(n) \neq 0$. Ainsi **MP** est valide d'un point de vue pratique dans le constructivisme à la Bishop. Remarquons aussi que **LPO** implique clairement **MP**.

Principes de continuité uniforme

Le principe de continuité uniforme affirme que toute fonction ponctuellement continue sur un espace métrique compact est uniformément continue. Il est équivalent à la même affirmation dans un cas particulier, qui est elle-même très proche de l'une des formes classiques du lemme de König. Les principes problématiques suivants semblent intéressants à étudier dans leurs relations mutuelles, d'autant plus qu'ils apparaissent très souvent en analyse classique (cf. la section 3.4.)

UC$^+$ Toute fonction ponctuellement continue $f : X \to Y$, avec X espace métrique compact et Y espace métrique, est uniformément continue.

UC Toute fonction ponctuellement continue $f : \{0,1\}^{\mathbb{N}} \to \mathbb{N}$ est uniformément continue.

Min Toute fonction réelle > 0 uniformément continue sur un espace métrique compact est minorée par un réel > 0.

Min$^-$ Toute fonction réelle > 0 uniformément continue sur un intervalle compact $[a, b]$ est minorée par un réel > 0.

Min$^+$ Toute fonction réelle > 0 ponctuellement continue sur un espace métrique compact est minorée par un réel > 0.

KL$_2$ Un arbre binaire explicite A qui ne possède pas de branche infinie (i.e., $\forall \alpha \in \{0,1\}^{\mathbb{N}}\ \exists m \in \mathbb{N}\ \alpha|^m \notin A$.) est fini.

KL$_2^+$ Un arbre binaire énumérable qui ne possède pas de branche infinie a une profondeur bornée[7].

Dans la formulation **KL$_2$**, on voit que ce principe est apparemment voisin de **LLPO** (voir **KL$_1$** la dernière forme équivalente citée ci-dessus). En fait, on peut montrer qu'il est une conséquence de **LPO** (voir la section 3.4). Mais il ne s'agit pas d'un principe d'omniscience. D'ailleurs il n'implique pas **LLPO**. En fait **LLPO** est manifestement faux en pratique (en mathématiques constructives) tandis que **KL$_2$** est vérifié en pratique : chaque fois qu'on sait prouver constructivement qu'un arbre à embranchements finis n'a pas de branche infinie, on sait également prouver qu'il est fini.

Le principe **KL$_2$** a à voir avec le « Fan Theorem » des mathématiques intuitionnistes à la Brouwer. Pour une discussion sur ce sujet voir [4].

[7] Il revient au même de dire qu'il est borné en nombre.

3. Nombres réels et fonctions continues

Une grande quantité d'analyse constructive paraît en 1967, dans le livre de E. Bishop [Bi]. Cela a été une grande surprise pour les mathématiciens[1]. Faire de l'analyse sans **LPO** semblait un tour de force. En fait il y avait eu des travaux précédents avec la même saveur, mais dans une mise en forme « logicienne » et avec moins de résultats, voir par exemple [Go2]. Le livre de Bishop a été rapidement épuisé. Une nouvelle version ([BB]) est parue en 1985, avec quelques résultats nouveaux, et une autre présentation constructive de l'intégrale de Lebesgue.

Le livre de Bishop peut être considéré comme réalisant le Programme de Hilbert pour ce qui concerne les fondements de l'Analyse[2].

3.1 Construction des nombres réels

Les constructions usuelles de $\mathbb{Z}$ et $\mathbb{Q}$ à partir de $\mathbb{N}$ sont tout à fait explicites.
Rappelons qu'un ensemble $(X, =_X, \neq_X)$ est *discret* quand

$$\forall x, y \in X \qquad (x =_X y \ \vee x \neq_X y)$$

Par exemple $\mathbb{Q}$ est un corps discret, mais l'ensemble de nombres réels *n'est pas* discret[3] : cela impliquerait **LPO**.

Constructivement, un nombre réel est connu lorsqu'on connaît des approximations rationnelles arbitrairement proches. Cela revient à dire[4] qu'un nombre réel est donné par une suite de Cauchy de nombres rationnels, avec la signification précise que la suite doit être de Cauchy de manière explicite.

Par exemple considérons une certaine « vitesse de convergence » $\mu : \mathbb{N} \to \mathbb{Q}$, i.e., une suite décroissante de rationnels > 0 qui tend explicitement vers 0. Par exemple $\mu(n) = 2^{-n}$. Nous disons qu'une suite (r_n) de nombres rationnels est μ-Cauchy si nous avons

$$\forall n, m \in \mathbb{N} \quad |r_n - r_m| \leq \mu(n) + \mu(m).$$

Une telle suite définit un nombre réel. Pour deux telles suites $r = (r_n)$ et $s = (s_n)$ nous définissons :

$$\begin{aligned}
r =_{\mathbb{R}} s &\overset{\text{def}}{\iff} \forall n \ \ |r_n - s_n| \leq 2\mu(n) \\
r \neq_{\mathbb{R}} s &\overset{\text{def}}{\iff} \exists n \ \ |r_n - s_n| > 2\mu(n) \\
r < s &\overset{\text{def}}{\iff} \exists n \ \ r_n + 2\mu(n) < s_n \\
r \geq s &\overset{\text{def}}{\iff} \forall n \ \ r_n + 2\mu(n) \geq s_n \\
(\max(r,s))_n &\overset{\text{def}}{=} \max(r_n, s_n)
\end{aligned}$$

[1] En France, le livre de Bishop a été accueilli par un silence abyssal et une indifférence très appuyée.
[2] Voir le chapitre 4 concernant le Programme de Hilbert.
[3] Nous mettons la négation en italique pour indiquer que le fait correspondant, bien que vrai classiquement, est impossible à prouver constructivement.
[4] Nous admettons ici comme non problématique l'axiome du choix dénombrable, comme dans l'exercice 2.3.1.

Ainsi nous avons

$$\neg(r \neq_{\mathbb{R}} s) \quad \Longleftrightarrow \quad r =_{\mathbb{R}} s$$

et

$$\neg(r < s) \quad \Longleftrightarrow \quad r \geq s.$$

La distinction de deux réels est une relation de séparation étroite. La définition des fonctions réelles les plus élémentaires sur $\mathbb{R}^2$ est directe. Par exemple, avec $\mu(n) = 2^{-n}$, $(r + s)_n = r_{n+1} + s_{n+1}$. Nous avons aussi

$$r \neq_{\mathbb{R}} 0 \quad \Longleftrightarrow \quad r \text{ est inversible}$$

Nous avons le résultat suivant : pour toute vitesse de convergence ν toute suite ν-Cauchy de nombres réels est convergente. Ainsi, différents choix pour la vitesse de convergence μ donnent « le même » ensemble de nombres réels.

Complexité de l'ensemble de nombres réels

Les nombres réels peuvent aussi être définis via les *développements en base b ambigus*. Par exemple considérons la base 4 avec les chiffres $-2, -1, 0, 1, 2$, alors les nombres réels peuvent être écrits sous la forme

$$x = a + \sum_{n \in \mathbb{N}^+} x_n / 4^n$$

Ainsi nous obtenons une application de $\mathbb{Z} \times \{-2, -1, 0, 1, 2\}^{\mathbb{N}^+}$ sur $\mathbb{R}$. Cela montre que, en tant que préensemble, $\mathbb{R}$ a la même complexité que $\mathbb{N} \times \{0, 1\}^{\mathbb{N}}$. En tant qu'ensemble cependant, $\mathbb{R}$ devrait être considéré comme un peu plus compliqué que $\mathbb{N} \times \{0, 1\}^{\mathbb{N}}$: alors qu'il est possible d'envoyer injectivement ou surjectivement $\mathbb{N} \times \{0, 1\}^{\mathbb{N}}$ dans $\mathbb{R}$, il est par contre impossible d'envoyer (constructivement) $\mathbb{R}$ injectivement ou surjectivement dans $\mathbb{N} \times \{0, 1\}^{\mathbb{N}}$. Ces étrangetés (du point de vue classique) ont leurs contreparties dans la théorie de la complexité algorithmique des nombres réels.

Digression carrément philosophique. Lorsqu'on dit qu'un nombre réel est donné par un développement en base 4 ambigu, qui est un élément de $\mathbb{Z} \times \{-2, -1, 0, 1, 2\}^{\mathbb{N}^+}$, on ne voit plus guère de différence entre un nombre réel vu par une mathématicienne classique et un nombre réel vu par un mathématicien constructif. Le mathématicien classique pourrait croire que les réels constructifs sont tous récursifs (c.-à-d. possédant un développement en base 4 ambigu qui est récursif) et se dire : ces mathématiciens constructifs ne considèrent qu'une petite partie de l'ensemble des nombres réels. En fait, ce n'est pas du tout le cas, l'ensemble $\{-2, -1, 0, 1, 2\}^{\mathbb{N}^+}$ dépend seulement du concept de construction, qui est un concept primitif non défini. On peut donc considérer que la croyance en des réels de nature différente, les classiques et les constructifs, est aujourd'hui purement un effet de sidération produit par le dépaysement radical de l'approche constructive. Cet effet de sidération est subi par tout un chacun, y compris la mathématicienne constructive contemporaine, qui a été au départ une mathématicienne classique. En fait, la vraie différence entre les mathématiques constructives et les mathématiques classiques tient essentiellement à ceci : les mathématiques classiques s'autorisent dans leurs raisonnements le principe du tiers exclu. Ce ne sont donc pas les mathématiques constructives qui explorent une petite partie de l'univers mathématique classique (mathématiques constructives et mathématiques classiques explorent le même univers mathématique), mais les mathématiques classiques qui explorent une petite partie des théorèmes de mathématiques constructives, les théorèmes T' qui sont de la forme $\mathbf{PTE} \Rightarrow T$. C'est en tout cas la thèse défendue par Fred Richman, par exemple dans [26].

Du point de vue défendu par Fred Richman, il n'y a pas lieu de distinguer l'infini actuel et l'infini potentiel sinon dans un but pédagogique. Les mathématiques classiques et les mathématiques constructives ont *les mêmes infinis* ($\mathbb{N}$, $\mathbb{N}^{\mathbb{N}}$, $\mathbb{R}$, $\mathrm{L}^2(\mathbb{R})$ etc...), mais parler d'infini actuel revient à dire qu'on explore seulement les conséquences de **PTE** tandis que parler d'infini

potentiel revient à parler d'infini sans restriction aucune. Prenons un exemple concret. Si en mathématiques classiques on montre que toute suite croissante bornée de nombres réels tend vers un nombre réel, alors que la preuve est impossible en mathématiques constructives, cela ne signifie pas qu'il y a des nombres réels classiques qui ne sont pas constructifs, cela signifie qu'il y a certains objets mathématiques, les *limites idéales de suites croissantes bornées de nombres réels* qui peuvent être identifiés avec les nombres réels usuels si et seulement si on admet **LPO**. Cette identification sous l'hypothèse **LPO** est un théorème aussi bien de mathématiques constructives que de mathématiques classiques. Le résultat des courses est primo que les mathématiques classiques passent à coté d'une généralisation de la notion de nombre réel, secundo qu'elles ignorent que **LPO** suffit là où elles utilisent **PTE**.

Sous ensembles de la droite réelle
Nous traitons dans ce paragraphe trois exemples instructifs.

Premier exemple.

Question : Quel est l'ensemble des zéros réels de $(X-a)(X-b)$?

Réponse : C'est l'adhérence de $\{a,b\}$. Cette partie de $\mathbb{R}$ contient $\max(a,b)$ et $\min(a,b)$. Mais l'assertion

$$\forall a,b\in\mathbb{R}\quad \{a,b\}=\{\min(a,b),\max(a,b)\}$$

est la même chose que **LLPO**.

Deuxième exemple, l'inclusion $\mathbb{Q}\subset\mathbb{R}$. Voici un contre exemple récursif instructif concernant cette inclusion : soit $\alpha:\mathbb{N}\to\mathbb{N}$ une fonction injective primitive récursive telle que le test

$$\text{« } m \text{ est-il dans l'image de } \alpha \text{ ? »}$$

n'est pas récursif[5]. Définissons $\delta(n,m)=1$ si $n=m$ et $\delta(n,m)=0$ sinon. Le nombre réel $x_m=\sum_n \delta(\alpha(n),m)/2^n$ est bien défini. La suite (x_m) est une suite bien définie de nombres réels. C'est une *suite récursive (mécaniquement calculable) de nombres réels* pour la définition naturelle de cette notion. Classiquement, chaque x_m est dans $\mathbb{Q}$ puisqu'il est égal à 0 ou à un rationnel $1/2^n$. Néanmoins, il est facile de voir que si (x_m) est une suite dans $\mathbb{Q}$ alors c'est une suite non récursive dans $\mathbb{Q}$. Ceci correspond au fait que *constructivement* (x_m) est une suite dans $\mathbb{R}$ mais elle *n'est pas* une suite dans $\mathbb{Q}$. Si nous donnons une définition positive de l'ensemble **Irr** des nombres irrationnels[6], nous pouvons prouver constructivement pour tout m qu'il est impossible que x_m soit irrationnel. Ceci n'est pas suffisant pour prouver que x_m est rationnel : constructivement, $\mathbb{R}$ est beaucoup plus que la réunion de $\mathbb{Q}$ et **Irr**.

Troisième exemple : on lira avec intérêt dans [23] la preuve de l'équivalence suivante :

$$\forall x\in\mathbb{R}\ \ (\mathbb{R}x \text{ est fermé } \iff\ (x=0\ \vee\ x\neq 0))$$

Exercice 3.1.1 Développer les trois exemples instructifs cités dans ce paragraphe.

Espaces métriques séparables complets
L'ensemble $\mathcal{F}(\mathbb{N},\mathbb{R})=\mathbb{R}^{\mathbb{N}}$ des suites de nombres réels s'identifie à une partie S de l'ensemble des suites doubles de rationnels, $\mathbb{Q}^{\mathbb{N}\times\mathbb{N}}$. Une suite double $(r_{n,m})$ est dans S si et seulement si elle vérifie

$$\forall n,m,p\in\mathbb{N}\quad |r_{n,m}-r_{n,p}|\leq\mu(m)+\mu(p)$$

où μ définit une vitesse de convergence (par exemple $\mu(m)=1/2^m$). À cet élément de S est associée la suite de nombres réels $(x_n)_{n\in\mathbb{N}}$ où $x_n=\lim_{m\to\infty} r_{n,m}$. Il faut naturellement définir $=_{\mathbb{R}^{\mathbb{N}}}$ et $\neq_{\mathbb{R}^{\mathbb{N}}}$ de façon extensionnelle.

[5] L'image de α est appelée une partie récursivement énumérable mais non récursive de $\mathbb{N}$.
[6] I.e., un nombre réel x est irrationnel si, pour tout $r\in\mathbb{Q}$ on a $x\neq r$.

Les espaces métriques séparables complets peuvent être construits de manière analogue à $\mathbb{R}$, ils ont en tant que préensembles une complexité « majorée » par celle de $\mathbb{N}^{\mathbb{N}}$.

Voici comment cela se passe. Si (X, d) est un espace métrique complet dont on connaît une partie énumérable dense $\{x_n\,;\, n \in \mathbb{N}\}$, on peut définir un écart $\delta : \mathbb{N} \times \mathbb{N} \to \mathbb{R}^{\geq 0}$ par $\delta(n, m) = d(x_n, x_m)$ et X s'identifie au séparé complété de $(\mathbb{N}, \delta)$, c'est-à-dire à l'ensemble suites μ-Cauchy dans $(\mathbb{N}, \delta)$, avec par exemple $\mu(n) = 1/2^n$, muni de la distance qui se déduit de δ.

L'espace métrique obtenu est *compact* s'il est précompact c'est-à-dire si on donne une suite d'entiers (a_n) avec la preuve que

$$\forall m \in \mathbb{N}\ \exists q \leq a_n\ \delta(m, q) \leq 1/2^n$$

3.2 Fonctions réelles

On a le résultat expérimental suivant : seules les fonctions continues sont constructivement partout bien définies. Par exemple considérons la fonction *signe*

$$\mathit{signe}\ \left\{\begin{array}{ccc}]-\infty, 0] \cup \{0\} \cup [0, \infty[& \longrightarrow & \{-1, 0, 1\} \\ x < 0 & \longmapsto & -1 \\ 0 & \longmapsto & 0 \\ x > 0 & \longmapsto & 1 \end{array}\right.$$

C'est une fonction définie sur $]-\infty, 0] \cup \{0\} \cup [0, \infty[$. Mais l'égalité $]-\infty, 0] \cup \{0\} \cup [0, \infty[= \mathbb{R}$ signifie **LPO**.

Une *fonction continue* $f : [a, b] \to \mathbb{R}$ est définie comme un couple (f, ν) où f est une fonction $[a, b] \to \mathbb{R}$ et $\nu : \mathbb{N} \to \mathbb{N}$ est un *module de continuité uniforme*[7] c'est-à-dire que ν vérifie la propriété suivante :

$$\forall x, x' \in [a, b] \quad \Big(\big|x - x'\big| < 1/2^{\nu(n)} \ \Rightarrow\ \big|f(x) - f(x')\big| \leq 1/2^n\Big)$$

Il semble important de signaler que les mathématiques constructives russes à la Markov, parce qu'elles interdisent a priori les nombres réels ou les fonctions réelles non récursives[8], autorisent des contre-théorèmes aux mathématiques classiques. Par exemple, elles *prouvent* qu'une fonction réelle partout définie est continue en tout point, et elles donnent des exemples de fonctions réelles continues en tout point mais non majorées sur l'intervalle $[0, 1]$.

C'est par contre un résultat d'expérience que seules les fonctions uniformément continues (sur $[a, b]$) sont constructivement « continues en tout point » lorsqu'on se place dans le cadre des mathématiques constructives à la Bishop[9].

Une *fonction continue* $f :]0, \infty[\to \mathbb{R}$ est définie comme une fonction qui est continue sur tous les intervalles fermés $[a, b] \subset]0, \infty[$. Une telle fonction est donnée par un couple (f, ν) où f est une fonction $[a, b] \to \mathbb{R}$ et $\nu : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ est un *module de continuité uniforme sur tous les intervalles fermés* :

$$\begin{array}{ll} \forall m \in \mathbb{N} & \forall x, x' \in [1/2^m, 2^m] \\ & \big(|x - x'| < 1/2^{\nu(m,n)} \implies |f(x) - f(x')| \leq 1/2^n\big) \end{array}$$

[7] En fait, on doit aussi avoir une preuve que la construction f définit bien une fonction $[a, b] \to \mathbb{R}$ et la preuve que ν est bien un module de continuité uniforme pour la fonction f.

[8] Accord de genre avec le plus proche cité, avouez que cela sonne mieux.

[9] Dans la mesure où les mathématiques constructives à la Bishop sont compatibles aussi bien avec les mathématiques classiques qu'avec le constructivisme russe, on est assuré que le théorème de continuité uniforme ne peut y être ni prouvé ni infirmé.

3.3 Algèbre réelle

Algèbre linéaire réelle
L'algèbre linéaire réelle constructive est presque la même chose que la (bonne) analyse numérique matricielle. Par exemple il est impossible de travailler constructivement avec l'espace image d'une matrice réelle si son rang n'est pas connu.

Dans un espace réel normé nous pouvons définir trois notions d'indépendance linéaire pour une famille $(x_1, \ldots, x_k)$.

La famille est *faiblement indépendante* quand nous avons l'implication

$$\left\|\sum_i \lambda_i x_i\right\| = 0 \;\Rightarrow\; \sum_i |\lambda_i| = 0$$

La famille est *indépendante* quand nous avons l'implication

$$\sum_i |\lambda_i| \neq 0 \;\Rightarrow\; \left\|\sum_i \lambda_i x_i\right\| \neq 0$$

La famille est *numériquement indépendante* quand nous avons une *constante d'indépendance numérique* $c > 0$, i.e., un $c > 0$ tel que

$$\left\|\sum_i \lambda_i x_i\right\| \;\geq\; c \sum_i |\lambda_i|$$

La troisième notion est de loin la plus utile.

Explicitons ces trois notions lorsque l'espace est muni d'un produit scalaire $\langle x, y\rangle$.

Notons $G = (\langle x_i, x_j\rangle)_{1\leq i,j\leq k}$ et $g = \det(G)$ la matrice et le déterminant de Gram du système $(x_1, \ldots, x_k)$. Pour $V = {}^{\mathrm{t}}(\lambda_1, \ldots, \lambda_k)$ on a $\|\sum_i \lambda_i x_i\|^2 = {}^{\mathrm{t}}V\,G\,V$, et

$$\left\|\sum_i \lambda_i x_i\right\| = 0 \;\Leftrightarrow\; \sum_i \lambda_i x_i = 0 \;\Leftrightarrow\; G\,V = 0 \;\Leftrightarrow\; {}^{\mathrm{t}}V\,G\,V = 0$$

On en déduit que l'indépendance faible équivaut à l'affirmation :

$$\forall \alpha \in \mathbb{R} \quad (g\,\alpha = 0 \;\Rightarrow\; \alpha = 0)$$

Elle-même équivaut à $\neg(g = 0)$.

De même on a

$$\left\|\sum_i \lambda_i x_i\right\| > 0 \;\Leftrightarrow\; {}^{\mathrm{t}}V\,G\,V > 0$$

et l'indépendance équivaut à

$$\forall \alpha \in \mathbb{R} \quad (\alpha \neq 0 \;\Rightarrow\; g\,\alpha \neq 0)$$

donc aussi à $g > 0$.

Enfin l'indépendance numérique équivaut à $\exists c\; g \geq c$.

Ainsi indépendance et indépendance numérique sont équivalentes : elles signifient la même chose que « le déterminant de Gram g est > 0 ». Dans ce cas (espace avec produit sclaire), l'indépendance numérique peut être vue comme l'explicitation de l'indépendance : $g > 0$ est remplacé par $g \geq c$ avec un $c > 0$ donné.

Enfin « L'indépendance faible implique l'indépendance » signifie « $\neg(g = 0) \;\Rightarrow\; g > 0$ » ce qui est le principe de Markov **MP**, appliqué avec le réel $g \geq 0$.

Par ailleurs, on ne connait pas d'exemple où on sache certifier constructivement l'indépendance faible autrement qu'en prouvant l'indépendance numérique, sauf évidemment à mettre directement sous forme cachée l'indépendance faible dans l'hypothèse.

Exercice 3.3.1 Donner les détails des preuves des affirmations ci-dessus.

Algèbre polynomiale avec les nombres réels
La géométrie algébrique réelle classique est pour l'essentiel constructive quand on traite des *corps réels clos discrets*[10], par exemple les nombres réels algébriques (cf. [BCR]). Dans ce cadre, de nombreux résultats qui ont une preuve non constructive dans le livre [BCR] peuvent être rendus constructifs (cf. par exemple [20, 18]).

Développer l'algèbre constructive avec les polynomes réels (au sens des nombres réels à la Cauchy) est une tâche beaucoup plus difficile. Aujourd'hui, la question de savoir quelles sont les propriétés algébriques des nombres réels n'a pas encore reçu de réponse entièrement satisfaisante en mathématiques constructives. En fait beaucoup de sous-corps non discrets de $\mathbb{R}$, tel que le corps des nombres réels définis par des suites primitives récursives μ-Cauchy de nombres rationnels (avec $\mu(n) = 1/2^n$), ont de bonnes propriétés algébriques, les mêmes semble-t-il que le corps $\mathbb{R}$. Il serait donc intéressant de mettre au point un bon formalisme pour les *corps réels clos non discrets*.

Un point délicat est de traiter constructivement les racines réelles des polynomes réels. Il y a des discontinuités lorsque les racines disparaissent dans le plan complexe, et ceci est une difficulté majeure. Peut-être une bonne manière d'appréhender la question est d'introduire les *racines réelles virtuelles* des polynomes réels unitaires comme dans [7, 11]. Ce sont des fonctions continues des coefficients et elles recouvrent toutes les racines réelles. Quand une paire de racines réelles disparaît dans le plan complexe les racines virtuelles correspondantes sont des racines (réelles ou virtuelles) de la dérivée.

Une autre voie à explorer est de considérer les systèmes d'équations polynomiales réelles comme des points réels à la Cauchy de « bonnes familles » définies sur $\mathbb{Q}$. Si la famille a de bonnes propriétés uniformes, ces propriétés s'appliqueront aussi pour ses « points réels à la Cauchy ». C'est ce qui se passe par exemple pour la réponse positive au 17-ème problème de Hilbert[11] (cf. [8]).

3.4 LPO implique le principe de continuité uniforme

Nous faisons dans cette section une brève étude partielle des relations entre **LPO** d'une part, différents principes de continuité uniforme d'autre part. Introduisons quelques notations.

Notation 3.4.1

- si $\alpha \in \mathbb{N}^{\mathbb{N}}$ et $n \in \mathbb{N}$ on désigne par $\alpha|^n$ la liste $[\alpha_0, \ldots, \alpha_{n-1}]$.
- si $\lambda \in \mathbf{Lst}(\{0,1\})$ est une liste finie $[\lambda_0, \ldots, \lambda_{k-1}]$ d'éléments de $\{0,1\}$ nous notons $\widetilde{\lambda}$ l'élément de $\{0,1\}^{\mathbb{N}}$ défini par : si $n < k$, $\widetilde{\lambda}(n) = \lambda_n$, sinon $\widetilde{\lambda}(n) = 0$.

Théorème 3.1 *Les propriétés suivantes sont une conséquence de* **LPO**.

UC$^+$ *Toute fonction ponctuellement continue $f : X \to Y$, avec X espace métrique compact et Y espace métrique, est uniformément continue.*

UC *Toute fonction ponctuellement continue $f : \{0,1\}^{\mathbb{N}} \to \mathbb{N}$ est uniformément continue.*

Min *Toute fonction réelle > 0 uniformément continue sur un espace métrique compact est minorée par un réel > 0.*

Min$^-$ *Toute fonction réelle > 0 uniformément continue sur un intervalle compact $[a, b]$ est minorée par un réel > 0.*

Min$^+$ *Toute fonction réelle > 0 ponctuellement continue sur un espace métrique compact est minorée par un réel > 0.*

[10] Un corps réel clos discret est un corps ordonné pour lequel on a : un polynome qui change de signe sur un intervalle admet une racine sur cet intervalle. On demande aussi d'avoir constructivement la disjonction $\forall x\ (x > 0 \vee x = 0 \vee x < 0)$.

[11] Écrire un polynome partout positif ou nul comme somme de carrés de fractions rationnelles.

KL$_2$ *Un arbre binaire explicite A qui ne possède pas de branche infinie (i.e., $\forall \alpha \in \{0,1\}^{\mathbb{N}}\ \exists m \in \mathbb{N}\ \alpha|^m \notin A$.) est fini.*

KL$_2^+$ *Un arbre binaire énumérable qui ne possède pas de branche infinie a une profondeur bornée.*

Plus précisément on a :

$$\boldsymbol{LPO} \Rightarrow \boldsymbol{KL}_2^+ \Rightarrow \boldsymbol{KL}_2\ , \quad \boldsymbol{KL}_2^+ \Leftrightarrow \boldsymbol{UC}^+ \Leftrightarrow \boldsymbol{UC} \quad \textit{et}$$
$$\boldsymbol{UC}^+ \Rightarrow \boldsymbol{Min}^+ \Rightarrow \boldsymbol{Min} \Rightarrow \boldsymbol{Min}^-$$

Preuve
Nous montrerons seulement $\mathbf{KL}_2^+ \Rightarrow \mathbf{UC}$, $\mathbf{UC} \Rightarrow \mathbf{KL}_2$, $\mathbf{UC}^+ \Rightarrow \mathbf{Min}^+ \Rightarrow \mathbf{Min} \Rightarrow \mathbf{Min}^-$ et $\mathbf{LPO} \Rightarrow \mathbf{KL}_2^+$.

Soit $F \in \mathcal{F}(\{0,1\}^{\mathbb{N}}, \mathbb{N})$ et supposons que F est continue en tout point.
Si $\lambda \in \mathbf{Lst}(\{0,1\})$ nous dirons que F *refuse* λ s'il existe $\alpha \in \{0,1\}^{\mathbb{N}}$ et $k \in \mathbb{N}$ avec $\alpha|^k = \lambda$ mais $F(\alpha) \neq F(\widetilde{\lambda})$. Si tel est le cas, puisque F est continue au point α il existe un entier $m > k$ tel que $\lambda' = \alpha|^m$ vérifie $F(\widetilde{\lambda'}) = F(\alpha)$, donc $F(\widetilde{\lambda'}) \neq F(\widetilde{\lambda})$. On en déduit que les λ refusés par F forment un arbre A_F binaire énumérable : énumérer les couples (λ, λ') où λ' prolonge λ et retenir tous les λ pour lesquels se présente un λ' tel que $F(\widetilde{\lambda}) \neq F(\widetilde{\lambda'})$.
Puisque F est continue, cet arbre ne possède pas de branche infinie.

Montrons $\mathbf{KL}_2^+ \Rightarrow \mathbf{UC}$. Si on suppose $\mathbf{KL}_2^+$ l'arbre A_F est borné en profondeur. Ceci implique la continuité uniforme de F.

Inversement tout arbre binaire explicite T sans branche infinie permet de définir une fonction F_T ponctuellement continue telle $A_{F_T} = T$ de la manière suivante : pour $\alpha \in \{0,1\}^{\mathbb{N}}$ on considère le plus petit entier n tel que $\alpha|^n \notin T$, on pose $F_T(\alpha) = n$. Si on suppose **UC**, la continuité uniforme de F_T implique que l'arbre T est borné. Donc $\mathbf{UC} \Rightarrow \mathbf{KL}_2$.

Les implications $\mathbf{Min}^+ \Rightarrow \mathbf{Min} \Rightarrow \mathbf{Min}^-$ sont immédiates.

Voyons $\mathbf{UC}^+ \Rightarrow \mathbf{Min}^+$. Si $f : X \to \mathbb{R}$ est continue ponctuellement et partout > 0, il en va de même pour $x \mapsto 1/f(x)$. Puisqu'on suppose $\mathbf{UC}^+$, $1/f$ est uniformément continue, donc majorée.

Supposons maintenant **LPO**. Soit T un arbre binaire énumérable. Puisque $\mathbf{Lst}(\{0,1\})$ est un ensemble dénombrable et T une partie énumérable, **LPO** implique que T est détachable et qu'en outre on a

$$(*) \qquad T \text{ est fini } \vee\ T \text{ est infini}$$

Mais puisqu'on suppose **LPO** on a a fortiori **LLPO**, donc $\mathbf{KL}_1$. Donc si T est infini, il possède une branche infinie. Par hypothèse, ceci est absurde, et vue la disjonction $(*)$, T est fini. Ceci démontre $\mathbf{KL}_2^+$.
□

4. Le programme de Hilbert

4.1 Echecs et succès du programme de Hilbert

Nous commençons ce chapitre par une tentative consistant à énoncer le programme de Hilbert de la manière la plus générale et la plus informelle possible.

Programme de travail

(1) *Lorsqu'un résultat concret est démontré en mathématiques par des méthodes douteuses, certifier ce résultat par des méthodes sûres.*

(2) *Réaliser ce travail de manière aussi systématique (voire automatique) que possible.*

Ce programme a été imaginé pour faire face aux problèmes d'interprétations que pose la théorie des ensembles infinis de Cantor.

Pour Hilbert les « méthodes sûres » étaient finitistes et devaient relever de l'arithmétique élémentaire. Cependant Gödel a démontré avec son théorème d'incomplétude que n'importe quel système formel S ayant pour ambition de décrire de manière suffisamment précise les entiers naturels, ne peut pas être prouvé cohérent par de tels moyens élémentaires.

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 outrancier de Bourbaki), et comme une certaine dose d'infini à l'état au moins potentiel est nécessaire aux mathématiques, le programme de Hilbert, en tant que réflexion, par des moyens sûrs, au sujet des mathématiques pratiquées, reste une tâche permanente. À défaut de pouvoir maîtriser l'infini par en bas une fois pour toutes, ce qui était trop ambitieux, il reste nécessaire d'analyser la pratique mathématique de l'infini.

L'arithmétique avec et sans le Principe du Tiers Exclu

Nous allons voir qu'en un certain sens, le programme de Hilbert a été réalisé pour l'arithmétique.

Une formalisation de nombreuses méthodes constructives concernant les entiers naturels est donnée par un système formel appelé Arithmétique de Heyting, avec pour acronyme HA.

Une version plus faible de ce système formel est appelée Arithmétique primitive récursive, avec pour acronyme PRA.

Dans ces systèmes formels nous travaillons avec $\mathbb{N}$ vu comme une sorte de structure algébrique. Nous avons des constantes, des fonctions et des prédicats représentés par des symboles, avec au moins $+, \times, =, 0, 1$. Les variables représentent toutes des entiers naturels. Nous ajoutons aussi un symbole pour chaque *fonction primitive récursive*.

Dans les axiomes de la théorie PRA on met les formules qui correspondent aux définitions des fonctions primitives récursives (par substitution et par récurrence).

Les *formules atomiques* sont les formules $t = t'$ où t et t' sont des termes bien écrits (nous pouvons voir t et t' comme deux fonctions primitives récursives des variables qui y figurent).

Dans PRA on n'utilise pas d'autres formules que ces formules atomiques, donc pas de connecteurs logiques ni de quantificateurs. Les seuls théorèmes sont de la forme $t = t'$ avec la quantification universelle implicite sur les variables qui y figurent.

Les deux seules méthodes de preuve sont :

– primo : la substitution d'égaux produit des égaux

– secundo : la preuve par récurrence.

Un exposé remarquable mais un peu technique du système PRA se trouve dans le livre de Goodstein [Go][1]. La force du système est surprenante. On a pu mettre en évidence qu'un très grand nombre de théorèmes concrets peuvent se démontrer à l'intérieur de ce système (voir par exemple [13]).

Des logiciens ont argumenté de façon assez convaincante pour dire que les méthodes finitistes admises par Hilbert ([15]) recouvraient exactement ce qui est prouvable dans PRA (voir par exemple Tait [30]).

Dans HA nous autorisons les *formules du premier ordre*, i.e., les formules construites à partir des formules atomiques en utilisant les connecteurs logiques et les quantificateurs. Nous avons aussi un « schéma de preuve par récurrence » qui dit pour toute formule qu'elle peut être prouvée par récurrence sur l'une des variables libres qui y est présente.

Finalement nous avons des axiomes logiques et des règles de déduction conformes aux raisonnements utilisés dans les mathématiques constructives.

Toute formule sans quantificateur de HA est équivalente (à l'intérieur du système formel HA) à une formule $f(n_1, \ldots, n_k) = 0$ où f est une fonction primitive récursive et les n_j sont les variables apparaissant dans la formule.

Nous considérons aussi le système formel appelé Arithmétique de Peano qui a pour acronyme PA. Ce système est obtenu à partir de HA en ajoutant l'axiome $P \vee \neg P$ pour toute formule bien écrite de HA.

Concernant la portée et la signification de ce principe de tiers exclu, dans cette situation arithmétique précise, on peut montrer qu'il est moins fort que **LPO**. En fait, dans PA l'utilisation de la logique classique correspond à une version affaiblie de **LPO** dans laquelle n'interviennent que les suites d'entiers définissables[2] dans le langage de PA, c'est à dire ce que les logiciens appellent les *suites arithmétiques* : autrement dit, $\mathsf{PA} = \mathsf{HA} + \mathbf{LPO}_{arith}$.

Le système formel PA prouve plus de « théorèmes » que HA : par exemple, on construit assez facilement une fonction[3] primitive récursive $f(n, m)$ telle que la formule

$$\forall n \ \ (\forall m \ f(n, m) = 0 \ \text{ ou } \ \exists m \ f(n, m) \neq 0)$$

est évidemment vraie dans PA alors qu'elle n'est pas prouvable dans HA, parce qu'elle correspond à une version affaiblie de **LPO** qui est impossible à réaliser concrétement par un programme (le test sur n pour savoir dans quelle branche de l'alternative on tombe n'est pas calculable par un programme).

Néanmoins, il a été prouvé constructivement le résultat très significatif suivant : *tant qu'on n'a pas de divergence d'interprétation entre le point de vue constructif et le point de vue classique concernant un énoncé, PA ne prouve rien de plus que HA*, précisément (voir par exemple [9]) :

Théorème *Si* $f : \mathbb{N}^2 \to \mathbb{N}$ *est une fonction primitive récursive arbitraire alors la formule* $\forall n \ \exists m \ \ f(n, m) \neq 0$ *est prouvable dans PA si et seulement si elle est prouvable dans HA.*

Ceci signifie que les facilités données par **LPO** ne posent pas problème quand elles servent à prouver avec les moyens (limités) de PA des formules qui ne sont pas trop compliquées. Ce théorème assure un contenu constructif pour une grande quantité de mathématiques classiques,.

Ce genre de résultat en logique doit être considéré comme donnant *une réponse positive partielle* au programme de Hilbert.

[1] En fait Goodstein admet des récurrences multiples, qui permettent de construire des fonctions plus compliquées que les seules fonctions primitives récursives.

[2] D'un point de vue classique.

[3] Cette fonction est celle qui intervient dans le théorème de la halte des programmes, $f(n, m) = 0$ signifie que le programme n°n s'est arrêté au bout de m étapes élémentaires.

Le programme de Hilbert revisité
Au vu de ce succès obtenu pour l'arithmétique de Peano nous proposons pour le programme de Hilbert une version plausible mais parfaitement raisonnable, qui, nous le croyons, en respecte la signification la plus profonde. Nous remplaçons seulement le mot *finitiste* par le mot *constructif*.

Programme de travail

(1) *Lorsqu'un résultat concret est démontré en mathématiques par des méthodes douteuses, certifier ce résultat par des méthodes constructives.*

(2) *Réaliser ce travail de manière aussi systématique (voire automatique) que possible.*

Le théorème d'incomplétude de Gödel ne peut pas mettre hors jeu cette version (raisonnable) du programme de Hilbert. Pour la simple raison que nous ne donnons pas de définition restrictive a priori de ce que c'est qu'une preuve constructive. Et cela n'enlève évidemment rien à notre profonde admiration pour le théorème d'incomplétude de Gödel.

Sous cette forme le programme de Hilbert a été réalisé pour l'arithmétique de Peano, grâce au théorème cité ci-dessus.

Quand Erret Bishop publie en 1967 le livre *Foundations of Constructive Analysis* [Bi] où il interprête en termes constructifs les bases de l'analyse moderne, il réalise un morceau substantiel du programme de Hilbert tel que nous venons de l'énoncer.

Dans le livre de Bishop tous les théorèmes d'analyse ont la signification d'algorithmes qui calculent des objets concrets à partir d'autres objets concrets, conformément à certaines spécifications requises, et ces algorithmes sont *prouvés par des méthodes sûres* : en particulier personne ne conteste qu'ils aboutissent certainement en un temps fini au résultat souhaité. Ainsi les bases de l'analyse sont ramenées à un degré de certitude comparable à ce qui règne en théorie élémentaire des entiers naturels.

Bishop va bien au delà de ce qu'avait pu faire auparavant un logicien remarquable comme Goodstein dans [Go2] : non seulement sont traités une quantité incomparablement plus grande de résultats, mais encore, le style d'exposition est direct, sans autre différence sensible avec le style mathématique usuel qu'une attention scrupuleuse accordée aux aspects effectifs.

On pourra lire à ce sujet l'article de D. Knuth [17] dans lequel il analyse quelques « page n°100 » dans différents livres de mathématiques, dont celui de Bishop, du point de vue la pensée algorithmique.

En 1985 le livre de Mines, Richman et Ruitenburg [MRR] a fait pour les bases de l'algèbre moderne ce qu'avait fait le livre de Bishop pour celles de l'analyse.

Enfin notons que la nouvelle discipline du Calcul Formel (calculs symboliques et algébriques sur machine [CCS, CLS]) se rattache de facto à cette tradition.

4.2 Du bon usage des objets abstraits

Les mathématiques modernes abstraites utilisent systématiquement des « constructions » d'objets basées sur le lemme de Zorn. Nous proposons dans cette section une manière constructive de comprendre un grand nombre de ces « constructions ». Notre but est ici de montrer que les mathématiques classiques sont plus constructives qu'on ne le pense en général. Au fond, nous pensons que lorsqu'on a une preuve classique d'un résultat concret P, on a en fait, dans 90% des cas, beaucoup mieux que $\mathbf{PTE} \Rightarrow P$.

En bref, nous essayons d'indiquer une voie pour une réalisation possible du programme de Hilbert pour une bonne partie des mathématiques classiques.

Les idéaux premiers comme objets idéaux en algèbre commutative
Prenons l'énoncé classique : *Tout idéal strict d'un anneau est contenu dans un idéal premier.* Pour les anneaux énumérables, cet énoncé, sous la forme « *Tout idéal détachable strict d'un*

anneau est contenu dans un idéal premier détachable », équivaut à **LLPO** (cf. théorème 4.3 section 4.3). Pour des anneaux plus compliqués, l'énoncé est encore moins acceptable constructivement. Cependant, à quoi sert en mathématiques classiques ce théorème ? A-t-on vraiment besoin d'un idéal premier précis $\mathfrak{p}$? Ou seulement d'une sorte d'existence purement idéale d'un tel objet : en effet, on n'est pas spécifiquement intéressé par un idéal premier $\mathfrak{p}$ particulier mais bien plutôt par tous les $\mathfrak{p}$ possibles. Quels sont alors les calculs concrets mis en jeu en mathématiques classiques à travers ces objets idéaux ?

Souvent, un théorème de mathématiques classiques va demander d'aller voir ce qui se passe dans tous les localisés de l'anneau $\mathbf{A}$ en ses idéaux premiers $\mathfrak{p}$, ceci en vue de réaliser un certain but précis B.

Une interprétation possible de l'utilisation de ces objets « purement idéaux » est la suivante : l'anneau $\mathbf{A}$ est considéré comme un projet d'anneau local $\mathbf{A}_\mathfrak{p}$, incomplètement spécifié. C'est en quelque sorte une *présentation* d'anneau local (au sens où on parle d'une présentation d'un groupe ou d'un anneau). Mais à cause de l'axiome des anneau locaux :

$$\forall x \ (x \text{ est inversible } \vee \ (1-x) \text{ est inversible}) \qquad (*)$$

calculer dans $\mathbf{A}$ comme si c'était un anneau local implique une discussion cas par cas chaque fois que l'on veut réaliser la disjonction $(*)$. D'où un calcul arborescent. À un moment donné du calcul, chaque branche correspond à un système de conditions « x_i inversible $(i \in I)$, $(1-x_j)$ inversible $(j \in J)$ » : dans chaque branche, le projet d'anneau local $\mathbf{A}_\mathfrak{p}$ a été précisé en indiquant un certain nombre d'éléments qui sont extérieurs à l'idéal premier $\mathfrak{p}$.

D'un point de vue constructif, on peut se contenter de considérer les calculs arborescents finis en tant que tels. La preuve classique doit sans doute cacher quelque part l'argument constructif qui dit qu'avec un certain arbre fini, chaque branche est « adéquate pour le but précis B ».

Quelle est alors la contrepartie constructive du théorème d'existence des idéaux premiers ? C'est la chose suivante : si on part avec un anneau où $1 \neq 0$, et si on déclare morte toute branche où a été prouvé $1 = 0$ (branche qui ne peut plus représenter un projet d'anneau local), alors l'arbre ne meurt jamais tout entier[4]. Dit d'une autre manière, plus positive (mais à préciser) : si on a démontré un résultat à chaque feuille de l'arbre alors il est aussi vrai à la racine de l'arbre (en particulier $1 = 0$ ne peut être vrai à toutes les feuilles que lorsqu'il est vrai à la racine).

En guise de premières précisions nous donnons des faits simples et utiles qui expliquent en bonne partie comment fonctionne la méthode de calcul arborescent esquissée ci-dessus.

Rappelons que des éléments d'un anneau sont dit *comaximaux* lorsque l'idéal qu'ils engendrent contient 1.

Fait 4.2.1 *Soit $x_1, \ldots, x_m$ des éléments comaximaux dans $\mathbf{A}$, alors pour tous $k_i > 0$, $x_1^{k_1}, \ldots, x_m^{k_m}$ sont comaximaux.*

Preuve Élever $\sum_i x_i a_i = 1$ à une puissance suffisante. □

Notons que lorsqu'on a un anneau $\mathbf{A}$ et qu'on considère un embranchement avec les deux anneaux $\mathbf{A}[1/x]$ et $\mathbf{A}[1/(1-x)]$ en vue de réaliser dans chaque branche une alternative de la disjonction $(*)$ les deux éléments x et $1-x$ sont comaximaux. Le fait suivant explique comment ce phénomène se maintient dans un calcul arborescent.

Fait 4.2.2 *Soit $x, x_1, \ldots, x_m$ des éléments comaximaux dans $\mathbf{A}$. Dans $\mathbf{A}[1/x]$ considérons deux éléments dont la somme est égale à 1, $y = a/x^k$ et $z = 1 - y = (x^k - a)/x^k$, alors on a :*

- $\mathbf{A}[1/x][1/y] = \mathbf{A}[1/ax]$,
- $\mathbf{A}[1/x][1/z] = \mathbf{A}[1/a(x^k - a)]$,
- *les éléments $ax, x(x^k - a), x_1, \ldots, x_m$ sont des éléments comaximaux dans $\mathbf{A}$.*

Preuve On a $ax + x(x^k - a) = x^{k+1}$ et $x^{k+1}, x_1, \ldots, x_m$ sont comaximaux. □

[4] En mathématiques classiques, par application du lemme de König, on en déduit l'existence de l'idéal premier.

Fait 4.2.3 *Soit $x_1, \ldots, x_m$ des éléments comaximaux dans $\mathbf{A}$. Considérons un système linéaire sur $\mathbf{A}$ écrit sous forme matricielle $AX = B$. Alors le système admet une solution dans $\mathbf{A}$ si et seulement si il admet une solution dans chacun des $\mathbf{A}[1/s_i]$. En particulier un élément de $\mathbf{A}$ est nul, régulier ou inversible si et seulement si il est nul, régulier ou inversible dans chacun des $\mathbf{A}[1/s_i]$.*

Preuve Il suffit de montrer la première affirmation. La solution dans $\mathbf{A}[1/x_i]$ donne des exposants k_i, ℓ_i et un vecteur colonne X_i tel que $x_i^{k_i} AX_i = x_i^{\ell_i} B$. Comme les $x_i^{\ell_i}$ sont comaximaux on a des c_i tels que $\sum_i c_i x_i^{\ell_i} = 1$ et cela donne dans $\mathbf{A}$ la solution $X = \sum_i c_i x_i^{k_i} X_i$. □

Un exemple précis

Nous prenons un exemple simple tiré de la théorie des modules projectifs de type fini. Pour ne pas faire trop de théorie nous donnons les énoncés en termes de matrices. Une matrice $F \in \mathbf{A}^{n\times n}$ est dite idempotente, ou encore est appelée une *matrice de projection*, lorsque $F^2 = F$. Nous allons examiner deux théorèmes concernant de telles matrices.

On appelle matrice de projection standard une matrice de la forme :

$$\mathrm{I}_{r,n,n} = \begin{bmatrix} \mathrm{I}_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r} \end{bmatrix}$$

En langage abstrait le premier théorème dit qu'un module projectif devient libre après localisation en des éléments comaximaux (i.e., qui engendrent l'idéal $\mathbf{A}$).

Théorème 4.1 *Si $F \in \mathbf{A}^{n\times n}$ est une matrice de projection il existe une famille finie $s_1, \ldots, s_k \in \mathbf{A}$ telle que $\langle s_1, \ldots, s_k\rangle = \mathbf{A}$, des entiers $r_i \leq n$ et des matrices $P_i \in \mathbf{A}[1/s_i]^{n\times n}$ telles que :*

- *P_i est inversible dans $\mathbf{A}[1/s_i]$,*
- *$P_i F P_i^{-1} = \mathrm{I}_{r_i,n,n}$*

Preuve en mathématiques classiques Considérons un idéal premier arbitraire $\mathfrak{p}$ de $\mathbf{A}$. On sait (voir lemme 4.2.4) que sur $\mathbf{A}_\mathfrak{p}$, qui est un anneau local, la matrice F est semblable à une matrice $\mathrm{I}_{r_\mathfrak{p},n,n}$. Notons $R_\mathfrak{p}$ la matrice de passage. On a donc $R_\mathfrak{p} F = \mathrm{I}_{r_\mathfrak{p},n,n} R_\mathfrak{p}$ sur l'anneau $\mathbf{A}_\mathfrak{p}$, avec $\det R_\mathfrak{p}$ inversible dans cet anneau. En chassant les dénominateurs, et en tenant compte de ce que signifie l'égalité dans $\mathbf{A}_\mathfrak{p}$ on obtient une matrice $P_\mathfrak{p} \in \mathbf{A}^{n\times n}$ qui vérifie :

- $\det P_\mathfrak{p} \notin \mathfrak{p}$,
- $P_\mathfrak{p} F = \mathrm{I}_{r_\mathfrak{p},n,n} P_\mathfrak{p}$ sur l'anneau $\mathbf{A}$.

Posons $s_\mathfrak{p} = \det P_\mathfrak{p}$. On a donc $\det P_\mathfrak{p}$ inversible dans $\mathbf{A}[1/s_\mathfrak{p}]$ et $P_\mathfrak{p} F = \mathrm{I}_{r_\mathfrak{p},n,n} P_\mathfrak{p}$ sur l'anneau $\mathbf{A}[1/s_\mathfrak{p}]$.
La famille (infinie) des $s_\mathfrak{p}$ engendre un idéal $\mathfrak{a}$ qui contient un élément à l'extérieur de chaque idéal premier $\mathfrak{p}$. En conséquence $\mathfrak{a} = \mathbf{A}$ puisque tout idéal strict est contenu dans un idéal premier. Mais si 1 est dans $\mathfrak{a}$ il est combinaison linéaire d'un nombre fini des générateurs de $\mathfrak{a}$. Ceci donne les s_i, les r_i et les matrices P_i dont le théorème affirme l'existence. □

Commentaire. On notera à quel point l'idéal premier intervient de manière purement idéale dans la preuve, et la façon aussi dont le résultat final est tiré du chapeau du magicien, sans que soit visible d'où sort exactement la famille finie. Evidemment, il n'y a pas de miracle en mathématiques et la famille finie ne peut sortir que du double fond du chapeau : la matrice F d'une part et la preuve du lemme 4.2.4 d'autre part, les deux seuls ingrédients concrets à notre disposition. Pendant que le magicien détournait notre regard loin de la matrice F et loin de la preuve du lemme 4.2.4, il les mettait en oeuvre activement dans l'ombre, pour mieux éblouir le spectateur qui ne voyait que le mouvement gracieux des mains autour du chapeau : « ... en conséquence $\mathfrak{a} = \mathbf{A}$ puisque tout idéal strict est contenu dans un idéal premier, mais si 1 est dans $\mathfrak{a}$ il est combinaison linéaire d'un nombre fini des générateurs de $\mathfrak{a}$ ... ».

Lemme 4.2.4 (Lemme de la liberté locale) *Sur un anneau local $\mathbf{B}$ toute matrice de projection est semblable à une matrice de projection standard.*

Première preuve. *(preuve classique usuelle)*
Nous notons $x \mapsto \overline{x}$ la passage au corps résiduel. Si $M \subseteq \mathbf{B}^n$ est l'image d'une matrice de projection F et si $\mathbf{k}$ est le corps résiduel on considère une base de $\mathbf{k}^n$ qui commence par des colonnes de $\overline{F}$ ($\operatorname{Im}\overline{F}$ est un sous espace vectoriel de dimension r) et se termine par des colonnes de $\mathrm{I}_n - \overline{F}$ ($\operatorname{Im}(\mathrm{I}_n - \overline{F}) = \operatorname{Ker}\overline{F}$). En considérant des colonnes correspondantes de $\operatorname{Im} F$ et $\operatorname{Im}(\mathrm{I}_n - F) = \operatorname{Ker} F$ on obtient un relèvement de la base résiduelle en une matrice dont le déterminant est résiduellement inversible, donc inversible. Les colonnes de cette matrice forment donc une base de $\mathbf{B}^n$ et sur cette base il est clair que la projection admet pour matrice $\mathrm{I}_{r,n,n}$.
Notez que dans cette preuve on extrait une base parmi les colonnes d'une matrice à coefficients dans un corps. Cela se fait usuellement par la méthode du pivot de Gauss. Cela réclame donc que le corps résiduel soit discret. □

Deuxième preuve. *(preuve par Azumaya)*
Contrairement à la précédente cette preuve ne suppose pas que l'anneau local soit résiduellement discret. Elle est extraite de la preuve du théorème d'Azumaya III.6.2 dans [MRR], pour le cas qui nous occupe ici. Autrement dit, nous donnons le contenu « matriciel » de la preuve du lemme de la liberté locale dans [MRR]. Nous allons diagonaliser la matrice F. Appelons f_1 le vecteur colonne $F_{1..n,1}$ de la matrice F, $e_1, \ldots, e_n$ la base canonique de $\mathbf{B}^n$ et φ l'application linéaire représentée par F.
– Premier cas, $f_{1,1}$ est inversible. Alors $f_1, e_2, \ldots, e_n$ est une base de $\mathbf{B}^n$. Par rapport à cette base, l'application linéaire φ a une matrice :

$$G = \begin{bmatrix} 1 & L \\ 0_{n-1,1} & F_1 \end{bmatrix}$$

En écrivant $G^2 = G$ on obtient $F_1^2 = F_1$ et $LF_1 = 0$. On a alors en posant $P = \begin{bmatrix} 1 & L \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{bmatrix}$:

$$\begin{aligned} PGP^{-1} &= \begin{bmatrix} 1 & L \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{bmatrix} \begin{bmatrix} 1 & L \\ 0_{n-1,1} & F_1 \end{bmatrix} \begin{bmatrix} 1 & -L \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{bmatrix} \end{aligned}$$

– Deuxième cas, $1 - f_{1,1}$ est inversible. Alors $e_1 - f_1, e_2, \ldots, e_n$ est une base de $\mathbf{B}^n$. Par rapport à cette base, $\mathrm{Id}_n - \varphi$ a une matrice :

$$G := \begin{bmatrix} 1 & L \\ 0_{n-1,1} & F_1 \end{bmatrix}$$

avec $G^2 = G$. Avec le même calcul que dans le cas précédent, $\mathrm{I}_n - F$ est donc semblable à une matrice :

$$\begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{bmatrix}$$

avec $F_1^2 = F_1$, ce qui signifie que F est semblable à une matrice :

$$\begin{bmatrix} 0 & 0_{1,n-1} \\ 0_{n-1,1} & H_1 \end{bmatrix}$$

avec $H_1^2 = H_1$.
On termine la preuve par récurrence sur n. □

Preuve constructive du théorème 4.1
Reprenons la preuve du lemme de la liberté locale « par Azumaya » avec un anneau arbitraire et ouvrons deux branches chaque fois que l'algorithme utilise une disjonction « x ou $(1-x)$ inversible ». On voit se déployer un arbre de calcul avec 2^n feuilles. En vertu du fait 4.2.2, à chacune des feuilles de l'arbre se trouve un anneau $\mathbf{A}[1/s_i]$, les éléments s_i étant comaximaux. En outre à chacune des feuilles de l'arbre le calcul a produit dans l'anneau $\mathbf{A}[1/s_i]$ une diagonalisation $F = P_i^{-1}\mathrm{I}_{r_i,n,n}P_i$. □

Commentaires. On voit que la preuve constructive n'a rien fait d'autre que mettre à jour le double fond du chapeau du magicien. En contrepartie, les objets purement idéaux « $\mathfrak{p}$ » ont complètement disparu de la preuve.
On aurait pu utiliser aussi la preuve classique du lemme de la liberté locale. Implicitement cette preuve utilise tous les mineurs de la matrice F (en nombre bien plus grand que 2^n) en vue de déterminer le rang de F (sur le corps résiduel) ainsi que des colonnes engendrant l'image de F : dit autrement, la méthode du pivot de Gauss pour extraire des colonnes qui engendrent l'image de F comporte beaucoup plus que 2^n possibilités de calcul. En outre comme la preuve classique utilise la disjonction

« x est inversible ou x est dans l'idéal maximal »

il faudrait avoir recours à des localisations plus compliquées que celles que nous avons utilisées : dans une branche on force l'inversibilité de x tandis que dans l'autre on force x à rentrer dans le radical de Jacobson. Ceci peut se faire en utilisant des monoïdes du style

$$\mathcal{S}(a_1,\dots,a_k;u_1,\dots,u_\ell)=\Big\{x\ ;\ \exists m\in\mathbb{N}\,\exists c_1,\dots,c_k\in\mathbf{C}\ x=(u_1\cdots u_\ell)^m+\sum\nolimits_i a_ic_i\Big\}$$

Et il faut établir un lemme analogue au fait 4.2.2 pour des localisations successives utilisant ce type de monoïdes.

Nous examinons maintenant un deuxième théorème qui analyse plus précisément la structure des matrices de projection.

Théorème 4.2 *Soit $F\in\mathbf{A}^{n\times n}$ une matrice de projection. Définissons le polynome $R_F(X)=\sum_{k=0,n}e_kX^k$ par l'égalité $R_F(1+X)=\det(\mathrm{I}_n+XF)$. Alors on a :*

- *les e_k forment un système fondamental d'idempotents orthogonaux : $e_k^2=e_k$, $\sum_k e_k=1$ et $e_ke_\ell=0$ pour $k\neq\ell$,*
- *si s est un mineur d'ordre $r+1$ de F on a $se_r=0$,*
- *si u est un mineur diagonal d'ordre r de F, F est semblable à $\mathrm{I}_{r,n,n}$ sur l'anneau $\mathbf{A}[1/(e_ru)]$,*
- *si F est semblable à $\mathrm{I}_{r,n,n}$ sur un localisé $\mathbf{A}_S$, tous les e_j pour $j\neq r$ sont nuls dans $\mathbf{A}_S$, et si $\mathbf{A}_S$ n'est pas réduit à 0, e_r est le seul des e_j qui divise un élément de S.*

NB : les éléments e_ku comme ci-dessus, lorsque u parcourt tous les mineurs diagonaux d'ordre k et k parcourt $\{0,\dots,n\}$ ont pour somme 1. Ceci donne donc une version plus précise du théorème 4.1. Dans les deux cas on obtient 2^n localisations en des éléments comaximaux mais le résultat est formulé de façon plus explicite dans le second théorème.

Preuve en mathématiques classiques des deux premiers items.
Si on localise en un idéal premier arbitraire, F est semblable à une matrice $\mathrm{I}_{r_\mathfrak{p},n,n}$ sur l'anneau $\mathbf{A}_\mathfrak{p}$. On a alors

$$R_F(1+X)=\det(\mathrm{I}_n+XF)=\det(\mathrm{I}_n+X\mathrm{I}_{r_\mathfrak{p},n,n})=\det\begin{bmatrix}(1+X)\mathrm{I}_{r_\mathfrak{p}} & 0\\ 0 & \mathrm{I}_{n-r_\mathfrak{p}}\end{bmatrix}=(1+X)^{r_\mathfrak{p}}$$

sur $\mathbf{A}_\mathfrak{p}$, c'est-à-dire $e_{r_\mathfrak{p}}=1$ et $e_j=0$ pour $j\neq r_\mathfrak{p}$. Toutes les égalités dans le premier et le second item sont donc vérifiées après localisation en $\mathfrak{p}$. Comme $\mathfrak{p}$ est arbitraire, ces égalités sont vraies sur $\mathbf{A}$. □

Commentaire. On va voir que la preuve constructive des deux premiers items est presque identique à la preuve classique : on remplace la localisation en tous les idéaux premiers par les localisations $\mathbf{A}[1/s_i]$ obtenues dans le théorème 4.1.

Preuve constructive.
Considérons la famille $(s_i)_{i=1,\dots,2^n}$ d'éléments comaximaux donnés par le théorème 4.1. On a (comme pour la localisation en un idéal premier dans la preuve classique) $e_{r_i}=1$ et $e_j=0$ pour $j\neq r_i$ dans l'anneau $\mathbf{A}[1/s_i]$. Toutes les égalités dans le premier et le second item sont donc

vérifiées dans chaque $\mathbf{A}[1/s_i]$, et par le fait 4.2.3, elles sont vraies dans $\mathbf{A}$.
Pour le troisième item on peut supposer que le mineur diagonal d'ordre r est celui dans le coin supérieur gauche. On écrit

$$F = \begin{bmatrix} F_{1,1} & F_{1,2} \\ F_{2,1} & F_{2,2} \end{bmatrix}$$

avec $F_{1,1}$ inversible dans $\mathbf{A}[1/(e_r u)]$. On a donc une matrice $H \in (\mathbf{A}[1/(e_r u)])^{r\times n-r}$ telle que en posant

$$P = \begin{bmatrix} \mathrm{I}_r & H \\ 0 & \mathrm{I}_{n-r} \end{bmatrix}$$

on ait $FP = \begin{bmatrix} F_{1,1} & 0 \\ F_{2,1} & C \end{bmatrix}$ sur $\mathbf{A}[1/(e_r u)]$. Sur cet anneau puisque tout mineur d'ordre $r+1$ de F est nul, il en va de même pour les mineurs d'ordre $r+1$ de la matrice FP. Donc, puisque $F_{1,1}$ est inversible, $C = 0$. Alors $QFP = \mathrm{I}_{r,n,n}$ pour deux matrices inversibles P et Q. Ainsi $\mathrm{Ker}F$ et $\mathrm{Im}F$ (qui sont en somme directe dans $\mathbf{A}^n$) sont deux modules libres de rang $n-r$ et r. Et F, qui représente la projection sur $\mathrm{Im}F$ parallèlement à $\mathrm{Ker}F$ est semblable à $\mathrm{I}_{r,n,n}$.
Pour le dernier point, on a $e_r = 1$ dans $\mathbf{A}_S$, donc tous les autres e_j sont nuls, ce qui leur interdit d'être inversible si $\mathbf{A}_S \neq 0$. □

4.3 Objets abstraits purement idéaux et principes d'omniscience

Dans le cas de structures algébriques dénombrables le lemme de Zorn n'est pas nécessaire pour construire les objets idéaux familiers de l'algèbre moderne (par exemple un idéal maximal dans un anneau commutatif). En effet pour construire ces objets abstraits, il suffit en mathématiques classiques de l'axiome dit « axiome du choix dénombrable » ou d'une version un peu plus forte dite « axiome du choix dépendant »([5]).

Ce genre de principe n'est pas vraiment problématique en mathématiques constructives. Et nous avons souvent implicitement utilisé l'axiome du choix dépendant sans le mentionner lorsque nous avons envisagé des constructions par récurrence.

C'est par réticence à l'égard du lemme de Zorn, qui permet de construire des objets idéaux dans le cas non dénombrable, par une « récurrence transfinie » le long d'un ordinal non dénombrable, que van der Waerden [vdW] limite les structures algébriques qu'il considère aux structures dénombrables.

Nous allons voir qu'en fait, ce qui est non constructif, c'est surtout l'usage de principes d'omniscience du style tiers exclu.

Définition 4.3.1 *Une structure algébrique, comprenant un nombre fini de lois de composition et de prédicats, est dite* énumérable *si les conditions suivantes sont vérifiées :*

1. *le préensemble X correspondant est énumérable,*
2. *les lois de composition de la structure sont explicites,*
3. *les constantes de la structure sont énumérables,*
4. *le diagramme positif de la structure*[6] *est énumérable.*

NB : Lorsqu'on ne spécifie aucun prédicat dans la structure, il y a cependant toujours l'égalité qui doit être considérée comme un prédicat de la structure. Par contre, si on le précise pas, l'inégalité ne fait pas partie des prédicats de la structure.

[5] L'axiome du choix dépendant dit que si $R(x,y)$ est une relation binaire définie sur un ensemble X et si elle vérifie $\forall x \in X \quad \exists y \in X \quad R(x,y)$, et si $a \in X$ alors il existe une suite (x_n) dans X telle que $x_0 = a$ et $\forall n \in \mathbb{N}\ R(x_n, x_{n+1})$.

[6] Un élément du diagramme positif de la structure est défini comme un couple (P,x) où P est un prédicat de la structure (disons d'arité k), x un k-tuple dans X, avec $P(x)$ est vrai dans la structure.

On a les deux théorèmes importants suivants.

Théorème 4.3 *Le principe d'omniscience* **LLPO** *et les trois propriétés suivantes sont équivalentes :*

(1) *Tout anneau énumérable non trivial possède un idéal premier détachable.*

(2) *Pour tout entier n, tout idéal énumérable strict de* $\mathbb{Z}[X_1, \ldots, X_n]$ *est contenu dans un idéal premier détachable.*

(3) *Tout idéal énumérable strict de* $\mathbf{A} = \mathbb{Z}/15\mathbb{Z}$ *est contenu dans l'un des deux idéaux* $\overline{3}\mathbf{A}$ *ou* $\overline{5}\mathbf{A}$.

Preuve Supposons **LLPO** et montrons (1). Soit $\mathbf{A}$ un anneau énumérable où $1 \neq 0$. Soit $(x_n)_{n\in\mathbb{N}}$ une énumération de $\mathbf{A}$. On pose $I_0 = \{0\}$, $M_0 = \{1\}$. On construit par récurrence. un idéal I_n de $\mathbf{A}$ et un monoïde multiplicatif M_n dans $\mathbf{A}$, avec :
– $I_{n-1} \subset I_n,\ M_{n-1} \subset M_n$
– $I_n \cap M_n = \emptyset$
– $\forall j < n\ (x_j \in I_n \vee x_j \in M_n)$
– I_n (resp. M_n) est engendré par les $x_j \in I_n$ (resp. $x_j \in M_n$) avec $j < n$.
On doit décider si on prend $x_n \in I_{n+1}$ ($I_{n+1} = I_n + x_n\mathbf{A}$) ou $x_n \in M_{n+1}$ ($M_{n+1} = \cup_{r\in\mathbb{N}} x_n^r M_n$). Puisque $\mathbf{A}$ est énumérable, que I_n et M_n sont de type fini et que l'égalité est énumérable dans $\mathbf{A}^2$, chacune des deux propriétés
– $(I_n + x_n\mathbf{A}) \cap M_n \neq \emptyset$
– $I_n \cap (\cup_r x_n^r M_n) \neq \emptyset$
est une propriété élémentaire.
Elles ne peuvent pas être simultanément vraies : si on avait $i_1 + x_n a = s_1$ et $i_2 = x_n^r s_2$ avec $a \in \mathbf{A}$, $i_1, i_2 \in I_n$, $s_1, s_2 \in M_n$, alors

$$i_4 = a^r i_2 = a^r(x_n^r s_2) = s_2(x_n a)^r = s_2(s_1 - i_1)^r = s_3 + i_3$$

avec $i_3, i_4 \in I_n$, $s_3 \in M_n$, et cela impliquerait $I_n \cap M_n \neq \emptyset$.
Par **LLPO** on en déduit que $(I_n + x_n\mathbf{A}) \cap M_n = \emptyset$ ou $I_n \cap (\cup_r x_n^r M_n) = \emptyset$. Dans le premier cas on pose $x_n \in I_{n+1}$, dans le deuxième cas, on pose $x_n \in M_{n+1}$. Les propriétés requises sont bien vérifiées par I_{n+1} et M_{n+1}. Finalement on prend $I = \cup_n I_n$, $M = \cup_n M_n$.

(2) est un cas particulier de (1) (considérer l'anneau quotient).

Montrons que (2) implique (3). On a un idéal énumérable I de $\mathbb{Z}$ qui contient $15\mathbb{Z}$ et on considère l'anneau quotient. D'après (2) cet idéal est contenu dans un idéal premier détachable P. On a $15 \in P$ donc $3 \in P$ ou $5 \in P$. Si $3 \in P$ alors $P = 3\mathbb{Z}$, si $5 \in P$ alors $P = 5\mathbb{Z}$.

Supposons maintenant (3) : tout idéal énumérable strict de $\mathbf{A} = \mathbb{Z}/15\mathbb{Z}$ est contenu dans l'un des deux idéaux $\overline{3}\mathbf{A}$ et $\overline{5}\mathbf{A}$, et montrons **LLPO** . Soient α, β deux suites croissantes $\in \mathbb{N}^{\mathbb{N}}$ avec $\forall n\ \alpha(n)\beta(n) = 0$. On veut montrer que l'une des deux suites est nulle. On considère l'idéal de $\mathbb{Z}/15\mathbb{Z}$ engendré par la suite x_n ainsi définie : si $\alpha(n) > 0$ on pose $x_n = \overline{3}$ (la classe de 3 modulo 15), si $\beta(n) > 0$ on pose $x_n = \overline{5}$, sinon on pose $x_n = 0$. Cet idéal I est clairement énumérable. En outre il est strict : $\overline{3} \in I$ signifie que la suite α est non nulle (donc la suite β est nulle et $I = \overline{3}\mathbf{A}$), tandis que $\overline{5} \in I$ signifie que la suite β est non nulle (donc la suite α est nulle). Si I est contenu dans $\overline{5}\mathbf{A}$ alors $\overline{3} \notin I$ donc $\alpha = 0$. Si I est contenu dans $\overline{3}\mathbf{A}$ alors $\overline{5} \notin I$ donc $\beta = 0$.
□

Remarque 4.3.2 On peut aussi montrer que **LLPO** est équivalent à l'une des possibilités de constructions classiques suivantes

– Tout corps énumérable réel (c'est-à-dire dans lequel -1 n'est pas une somme de carrés) peut être ordonné (c'est-à-dire muni d'une relation d'ordre total compatible avec la structure de corps).

– Tout sous-anneau local énumérable $\mathbf{A}$ d'un corps énumérable $\mathbf{K}$ est dominé par un anneau de valuation du corps.

Théorème 4.4 *Le principe d'omniscience **LPO** et les propriétés suivantes sont équivalentes :*

(1) *Tout anneau énumérable non trivial possède un idéal maximal détachable.*

(2) *Pour tout entier s, tout idéal énumérable strict de $\mathbb{Z}[X_1, \ldots, X_s]$ est contenu dans un idéal maximal détachable.*

(3) *Tout idéal énumérable strict de $\mathbb{Z}$ est contenu dans un idéal maximal détachable.*

(4) *Pour tout entier s, tout idéal énumérable de $\mathbb{Z}[X_1, \ldots, X_s]$ est un idéal de type fini.*

Preuve Supposons **LPO** et montrons (1). Soit $\mathbf{A}$ un anneau énumérable où $1 \neq 0$. Soit $(x_n)_{n\in\mathbb{N}}$ une énumération de $\mathbf{A}$. On pose $I_0 = \{0\}$. On construit par récurrence un idéal énumérable I_n ne contenant pas 1. Supposons I_n construit. D'après **LPO** on a

$$\forall y \exists z\ (1 + x_n y)z = 1 \bmod I_n \quad \vee \quad \exists y \forall z\ (1 + x_n y)z \neq 1 \bmod I_n$$

Dans le premier cas, on pose $I_{n+1} = I_n + x_n\mathbf{A}$ (donc $x_n = 0 \bmod I_{n+1}$ et $1 \notin I_{n+1}$), dans le second cas on pose $I_{n+1} = I_n + (1 + x_n y_n)\mathbf{A}$, où y_n vérifie $\forall z\ (1 + x_n y_n)z \neq 1 \bmod I_n$ (donc x_n est inversible mod I_{n+1} et $1 \notin I_{n+1}$.) Finalement $I = \cup_n I_n$ est un idéal maximal détachable de $\mathbf{A}$.

(3) est un cas particulier de (2) qui est un cas particulier de (1).

Montrons que (3) implique **LPO**. Soit p_n le n-ème nombre premier ($p_0 = 2$, $p_1 = 3, \ldots$). Soit α une suite d'entiers *fugitive* (elle prend au plus une fois une valeur $\neq 0$, et dans ce cas c'est la valeur 1). On veut montrer $\alpha = 0 \vee \alpha \neq 0$.
Soit I l'idéal de $\mathbb{Z}$ engendré par la suite $\alpha(n)p_n$ et soit P un idéal maximal détachable contenant I. Si $2 \in P$ et $\alpha(0) \neq 1$, alors $\alpha = 0$. Si $2 \notin P$ soit $u \in \mathbb{Z}$ l'inverse de 2 modulo P. Comme $2u - 1 \in P$ l'un des diviseurs premiers de $2u - 1$ est dans P, par exemple p_k puisque P est détachable. Donc ou bien $\alpha(k) = 1$, ou bien $\alpha = 0$.

Il est clair que (4) implique (3). En fait la théorie des idéaux de type fini de $\mathbb{Z}[X_1, \ldots, X_s]$ montre que tout idéal strict de type fini est détachable et contenu dans un idéal maximal de type fini détachable (cf. [MRR]).

Montrons enfin que **LPO** implique (4). Soit $(u_n)_{n\in\mathbb{N}}$ une énumération de $\mathbf{A} = \mathbb{Z}[X_1, \ldots, X_s]$ et I un idéal énumérable. Soit $I_0 = \{0\}$. On construit par récurrence une suite croissante (I_n) d'idéaux de type fini contenus dans I. Supposons avoir construit I_n. Par **LPO**, puisque I est énumérable, pour tout m ou bien $u_m \in I$ ou bien $u_m \notin I$. De même, ou bien $u_m \in I_n$ ou bien $u_m \notin I_n$. Posons $\alpha_n(m) = 1$ si $u_m \in I$ mais $u_m \notin I_n$, $\alpha_n(m) = 0$ sinon. Par **LPO** ou bien $\exists m\ \alpha_n(m) = 1$ ou bien $\forall m\ \alpha_n(m) = 0$. Dans le premier cas, soit m_n le premier indice tel que $\alpha_n(m_n) = 1$, on pose $I_{n+1} = I_n + u_{m_n}\mathbf{A}$. Dans le deuxième cas on pose $I_{n+1} = I_n$. La suite I_n est croissante, et dès qu'il y a deux termes consécutifs égaux, on a $I_n = I_{n+1} = I$. En utilisant le théorème 1.5 on obtient que la suite a deux termes consécutifs égaux. □

Corrigés d'exercices

Références

[Ab] Aberth O. *Computable analysis.* McGraw-Hill (1980). 1

[Be] Beeson M. *Foundations of Constructive Mathematics.* Springer-Verlag (1985). 1, 15, 18

[Bi] Bishop E. *Foundations of Constructive Analysis.* McGraw Hill (1967). 21, 31

[BB] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag (1985). 1, 11, 21

[BCR] Bochnak J., Coste M., Roy M.-F. *Géométrie algébrique réelle.* Springer-Verlag (1987). 26

[BR] Bridges D., Richman F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987). 1, 15

[Bro] Brouwer L. *Brouwer's Cambridge Lectures on Intuitionism* (Van Dalen ed.) (1981) Cambridge University Press. 1

[CCS] Cohen A., Cuypers H., Sterk H. (eds) *Some Tapas of Computer Algebra*, Springer Verlag (1999). 31

[CLS] Cox Q., Little J, O'Shea D. *Ideals, Varieties, and Algorithms*, (2nd edition) Springer Verlag UTM (1998). 8, 31

[Du] Dummett M. *Elements of Intuitionism.* Oxford University Press, (1977). 1

[Go] Goodstein R. *Recursive Number Theory.* Amsterdam, North-Holland, (1957). 30

[Go2] Goodstein R. *Recursive Analysis.* Amsterdam, North-Holland, (1961). 21, 31

[He] Heyting A. *Intuitionism, an Introduction.* Amsterdam, North-Holland, (1956). 1

[Ku] Kushner B. A. *Lectures on constructive mathematical analysis.* AMS Translations de Mathematical monographs n°60 (1984) (la version russe est de 1973) 1

[MRR] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 1, 5, 8, 11, 31, 34, 38

[TD] Troelstra A. S., van Dalen D. *Constructivism in Mathematics.* Vol I et II. Amsterdam, North-Holland, (1988). 1

[vdW] van der Waerden : *Moderne Algebra.* Vol I et II. Springer Verlag, (1930). Nombreuses éditions anglaises *Modern Algebra* à partir de 1936, Springer Verlag, Berlin, Frederik Ubgar Pub., New York.

Articles

36

[1] Bishop, E. *Mathematics as a numerical language*, in Intuitionism and Proof Theory. Eds. Myhill, Kino, and Vesley, North- Holland, Amsterdam, (1970) 11

[2] Buchberger B. *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal* (en Allemand). PhD Thesis. University of Innsbruck, Institute for Mathematics. (1965) 8

[3] Buchberger B. *An algorithmic method in polynomial ideal theory*, in Multidimensional systems theory, ed. by N.K. Bose. D Reidel. Publishing Company, Dordrecht, (1985), 184–232. 8

[4] Coquand T. *About Brouwer's fan theorem* Revue internationale de philosophie, **230** (2004), 483–489. 19

[5] Coquand T. *La contribultion de Kolmogorov en logique intuitionniste*. p. 31–53 dans L'héritage de Kolmogorov en mathématiques. Charpentier E., Lesne A., Nikolski N. (eds). Belin, Paris (2004). 13

[6] Coquand T., Persson *Gröbner bases in type theory*. in Proceeding of Types 1998, LNCS 1657, (1999). 8

[7] Coste M., Lajous T., Lombardi H., Roy M.-F. *Generalized Budan-Fourier theorem and virtual roots*. Journal of Complexity **21** (2005), 479–486. 26

[8] Delzell C., González-Vega L., Lombardi H. *A continuous and rational solution to Hilbert's 17-th problem and several Positivstellensatz cases*, in Computational Algebraic Geometry. Eds. Eyssette F., Galligo A.. Birkhäuser Progress in Math. n°109 (1993), 61–76. 26

[9] Friedman H. *Classically and intuitionistically provably recursive functions in Peano*, in Higher Set Theory. Lecture Notes in Mathematics n°669, 21–27 (1978). (Springer) 30

[10] Galligo A. *Algorithmes de calcul de Bases Standard*. Technical Report. Université de Nice. (1983) 8

[11] González-Vega L., Lombardi H., Mahé L. *Virtual roots of real polynomials.* Journal of Pure and Applied Algebra **124** (1998), 147–166. 26

[12] Kaplansky I. *Elementary divisors and modules.* Transactions of the AMS **66** (1949), 464–491. 4

[13] Kohlenbach U. *Things that can and things that cannot be done in PRA.* Annals of Pure and Applied Logic **102** (2000) 223–245. 30

[14] Kolmogorov *Sur le principe du tiers exclu* (en russe), Matematicheski Sbornik **32** (1925), 646-647. Traduction anglaise dans [31]. 13

[15] Hilbert D. *Über das Unendliche*. Math. Annalen **95** (1926) 161–19O. (Sur l'infini) traduction anglaise dans [31] 367-392. 30

[16] Hermann G. *Der Frage der endlich vielen Schritte in der Theorie der Polynomideale.* Math. Ann. **95** (1926), 736–788 8

[17] D. E. Knuth : *Algorithmic thinking and mathematical thinking* American Math. Monthly **92** (3), (mars 1985) 170–181 31

[18] Lombardi H. *Effective real nullstellensatz and variants*, in Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C.. Birkhäuser. Progress in Math n°94 (1991), 263–288. 26

[19] Lombardi H., Perdry H. *The Buchberger Algorithm as a Tool for Ideal Theory of Polynomials Rings in Constructive Mathematics*, in Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases), Cambridge University Press, London Mathematical Society Lecture Notes Series, n°251, 1998, 393– 407. 8

[20] Lombardi H., Roy M.-F. *Constructive elementary theory of ordered fields*, in Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C.. Birkhäuser 1991. Progress in Math. n°94 (MEGA 90 Castiglioncello, Italy) 249–262. 26

[21] Margenstern M. *L'école constructive de Markov.* Revue d'Histoire des Mathématiques, **1** (2) (1995), 271–305. 1

[22] Perdry H. *Strongly Noetherian rings and constructive ideal theory.* J. Symb. Comput. **37** (4) (2004), 511–535. 8

[23] Richman F. *Meaning and Information in Constructive Mathematics.* Amer. Math. Monthly, **89** (1982), 385–388. 23

[24] Richman F. *Constructive aspects of Noetherian rings.* Proc. Amer. Mat. Soc. **44** (1974), 436–441. 8

[25] Richman F. *Church Thesis without tears.* Journal of Symbolic Logic, **48** (3) (1983), 797–803. 15

[26] Richman F. *Interview with a constructive mathematician.* Modern Logic, **6** (1996), 247–271. 22

[27] Seidenberg A. *Constructions in Algebra*, Trans. Amer. Math Soc. **197** (1974), 273–313. 8

[28] Seidenberg A. *What is Noetherian ?* Rend. Sem. Mat. e Fis. di Milano **44** (1974), 55–61. 8

[29] Seidenberg A. *Construction of the integral closure of a finite integral domain.* Proc. Amer. Math Soc. **52** (1975), 368–372. 8

[30] Tait W. *Finitism.* Journal of Philosophy **78** (1981) 524–546. 30

[31] van Heijenoort J. (ed.), *Frome Frege to Gödel : a source book in mathematical logic*, Harvard University Press, Cambridge, Massachussets (1967). (troisième réimpression en 2002). 42