Mathématiques constructives et Évaluation paresseuse

Henri Lombardi*

17 novembre 2025

Séminaire Philosophie et Mathématiques.
École Normale Supérieure, 45 rue d'Ulm, Paris
Yves André, Joël Merker, [Jean Petitot,] Dominique Pradelle,
Victor Rabiet, Jean-Jacques Szczeciniarz
En collaboration avec l'Association des Amis de Jean Cavaillès
et avec les Archives Husserl

Table des matières

*Laboratoire de Mathématiques de Besançn, UMR CNRS 6623, UFR des Sciences et Techniques, Université Marie et Louis Pasteur, 25030 BESANCON CEDEX, FRANCE, henri.lombardi@umlp.fr

1 Introduction

Ce texte présente deux contributions remarquables aux mathématiques intuitives non formalisées.

La première contribution que nous décrivons est un article révolutionnaire de deux pages (Della Dora, Dicrescenzo, et Duval 1985) qui explique comment calculer dans la clôture algébrique d'un corps explicite quand bien même on ne sait pas construire cette clôture algébrique en tant que corps explicite. Cet article relève du Calcul Formel et de l'Informatique Théorique. Cette approche fournit une sémantique constructive pour cette clôture algébrique, au prix d'un trait de modestie que l'on peut résumer comme suit : rien ne sert de vouloir connaitre «toute la vérité» quand une partie de cette vérité est suffisante pour poursuivre les calculs. C'est la méthode de l'évaluation paresseuse bien connue des informaticiennes [1].

La seconde contribution, plus fondamentale, est le livre de Bishop (1967, Foundations of Constructive Analysis) qui explique comment échapper au formalisme dominant de l'époque pour revenir aux mathématiques intuitives traditionnelles. Pour que les théorèmes d'existence aient un contenu concret indiscutable, il est nécessaire d'admettre uniquement les démonstrations qui manipulent des objets finis de manière algorithmique. Un certain nombre de prérequis communs à la communauté des mathématiciens ne sont pas susceptibles de définition mais peuvent seulement être discutés, au cas par cas, si une contestation raisonnable est présentée. Ces prérequis sont d'une part les nombres entiers et d'autre part la notion de construction. Notons qu'aucune formalisation ne peut décrire complètement les nombres entiers intuitifs (voir Dehornoy (2017)). Notons également que la notion intuitive d'algorithme échappe à la définition par les machines de Turing adoptée en mathématiques classiques.

La plupart des définitions et résultats de mathématiques constructives donnés dans cet article sont extraits des livres Lombardi et Quitté 2021 et Díaz-Toca, Lombardi, et Quitté 2014.

2 L'évaluation paresseuse

2.1 L'article original D5

Quand on traite de manière algorithmique la théorie des nombres, la première étape est de définir le corps de nombres qui nous intéresse. Il s'agit d'une extension finie de $\mathbb{Q}$, de la forme $\mathbf{K} = \mathbb{Q}[\xi]$ où ξ est un nombre algébrique complexe, zéro d'un polynôme $P \in \mathbb{Q}[X]$. À priori le corps $\mathbb{Q}[\xi]$ est isomorphe à un quotient $\mathbb{Q}[x] = \mathbb{Q}[X]/\langle f\rangle$ où f est le polynôme minimal de ξ. Mais si le polynôme P n'est pas irréductible, le calcul de f n'est pas évident. Cette première étape a été résolue par un article fameux (Lenstra, Lenstra, et Lovász (1982)) qui donne un algorithme pour factoriser complètement les polynômes de $\mathbb{Q}[X]$.

Cependant, dès qu'il s'agit d'introduire un nouveau nombre algébrique complexe α pour résoudre une question relative à $\mathbf{K}$, les algorithmes pour décrire le corps $\mathbf{K}[\alpha]$ s'avèrent rapidement impraticables.

L'article D5 propose la solution paresseuse suivante : si nous savons qu'un $\alpha \in \mathbb{C}$ annule un polynôme unitaire $g \in \mathbf{K}[Y]$, ou si nous voulons introduire de manière formelle

1. Dans tout l'article, le lecteur est soumis à l'alternance des sexes.

un tel α dans une extension finie de $\mathbf{K}$ contentons nous de travailler dans l'algèbre quotient

$$\mathbf{L} = \mathbf{K}[Y]/\langle g(x,Y)\rangle = \mathbf{K}[y] = \mathbb{Q}[x,Y]/\langle g(x,Y)\rangle = \mathbb{Q}[X,Y]/\langle f(X,g(X,Y))\rangle$$

tant que celle-ci se comporte dans les calculs comme si g était irréductible. Notez que $\mathbf{L}$ est un $\mathbf{K}$-espace vectoriel de dimension égale au degré de g, si bien que l'on dispose d'un test d'égalité dans cette $\mathbf{K}$-algèbre.

Si $\mathbf{L}$ est un corps explicite, et si un élément $\gamma \in \mathbf{L}$ se présente dans les calculs, alors γ doit être nul ou inversible.

En fait, pour tout $\gamma \in \mathbf{L}$, comme on va le voir, on a un test qui répond à la question «γ est-il nilpotent, inversible ou ni l'un ni l'autre dans $\mathbf{L}$?».

Si γ est inversible ou nul, on peut poursuivre les calculs sans rien changer, car $\mathbf{L}$ se comporte comme un corps explicite.

Si γ est nilpotent mais pas nul, on peut le forcer à être nul en considérant le quotient $\mathbf{L}/\langle\gamma\rangle$ qui peut être décrit de manière précise sous la forme $\mathbf{K}[Y]/\langle g_1\rangle$ où g_1 est un facteur de g [2].

Si γ n'est ni nilpotent ni inversible, la situation doit être reconsidérée. Deux cas se présentent, celui où l'on force γ à être nul, et celui où l'on force γ à être inversible. Il faut donc ouvrir deux branches de calcul si l'on veut examiner toutes les situations possibles.

Nous allons démontrer que la démarche proposée, dite d'*évaluation paresseuse*, ou d'*évaluation dynamique* tient bien la route et que tous les calculs intermédiaires donnent toujours des résultats corrects.

Rappelons qu'un anneau $\mathbf{A}$ est isomorphe à un produit d'anneaux $\mathbf{A}_i$ ($i \in [\![1..r]\!]$) si, et seulement si, on a dans $\mathbf{A}$ un système fondamental d'idempotents orthogonaux [3] $(e_i)_{i\in[\![1..r]\!]}$ tel que chaque quotient $\mathbf{A}/\langle 1-e_i\rangle$ est isomorphe à $\mathbf{A}_i$.

Rappelons aussi la convention usuelle selon laquelle pour n'importe quel $x \in \mathbf{A}$, on pose $x^0 = 1$. Cela permet d'avoir $x^n x^m = x^{n+m}$ et $(xy)^n = x^n y^n$ pour tous $n, m \in \mathbb{N}$.

Lemme 2.1 (construction d'un idempotent)**.** *Dans un anneau $\mathbf{A}$ supposons qu'on ait un égalité $x^n = ax^{n+1}$, (c'est-à-dire $\langle x^n\rangle = \langle x^{n+1}\rangle$) avec $n \in \mathbb{N}$. On considère l'élément $e := (ax)^n$. Alors*

1. *e est idempotent ;*
2. *$ex^n = x^n$ et $\langle e\rangle = \langle x^n\rangle$;*
3. *$e = 1$ si, et seulement si, x est inversible ;*
4. *$e = 0$ si, et seulement si, x est nilpotent ;*
5. *x n'est ni nilpotent ni inversible si, et seulement si, $e \neq 0, 1$;*
6. *e est le seul idempotent tel que x est inversible modulo $e-1$ et nilpotent modulo e.*

Définition 2.2 (anneau zéro-dimensionnel)**.** On dira qu'un anneau est *zéro-dimensionnel* lorsqu'il vérifie l'axiome suivant :

$$\forall x \in \mathbf{A}\ \exists a \in \mathbf{A}\ \exists k \in \mathbb{N} \qquad x^k = ax^{k+1}. \tag{1}$$

En mathématiques classiques un anneau est zéro-dimensionnel si, et seulement si, tout idéal premier est maximal.

---

2. En effet, si $\gamma^m = 0$ on exprime γ comme un polynôme en y. On peut alors remplacer $g(Y)$ par le pgcd g_1 de $g(Y)$ et $\gamma(Y)$ dans $\mathbf{K}[Y]$. On remplace ainsi $\mathbf{L}$ par une sous-$\mathbf{K}$-algèbre $\mathbf{L}_0$ qui est une meilleure approximation de l'extension $\mathbf{K}[\alpha]$ convoitée (on y a forcé un nilpotent à s'annuler).

3. $\sum_i e_i = 1$ et $e_i e_j = 0$ si $i \neq j$.

En mathématiques constructives, un corps explicite avec test à zéro est appelé un *corps discret*.

Un corps discret peut-être défini comme un anneau zéro-dimensionnel réduit dont les éléments 0 et 1 sont les seuls idempotents.

Le lemme 2.1 s'applique de manière systématique dans les anneaux zéro-dimensionnels.

Un anneau intègre $\mathbf{A}$ est de dimension $\leqslant 1$ si, et seulement si, pour tout $x \neq 0$, $\mathbf{A}/\langle x\rangle$ est zéro-dimensionnel. C'est le cas de l'anneau d'entiers d'un corps de nombres.

En mathématiques classiques, un anneau arbitraire est de dimension $\leqslant 1$ si une suite strictement croissante de trois idéaux premiers est impossible. Une définition constructive (équivalente en mathématiques classiques) est la suivante :

$$\forall x, y \in \mathbf{A}\ \exists a, b \in \mathbf{A}\ \exists k, \ell \in \mathbb{N} \qquad x^k(y^\ell(1+ay)+bx) = 0.$$

Un premier exemple non trivial d'anneau zéro-dimensionnel est le suivant.

Lemme 2.3. *Si* $\mathbf{k}$ *est un corps discret, toute* $\mathbf{k}$*-algèbre* $\mathbf{A}$ *qui est un* $\mathbf{k}$*-espace vectoriel de dimension finie (explicite) est un anneau zéro-dimensionnel discret.*

Démonstration. Soit $r = \dim_{\mathbf{k}}(\mathbf{A})$. On peut regarder $\mathbf{A}$ comme une sous-$\mathbf{k}$-algèbre commutative de $\mathbb{M}_r(\mathbf{k})$ en identifiant tout élément γ de $\mathbf{A}$ à la matrice μ_γ de multiplication par γ dans le $\mathbf{k}$-espace vectoriel $\mathbf{A}$. Soit alors $z \in \mathbf{A}$ un élément non nul et M le polynôme minimal unitaire (ou le polynôme caractéristique) de μ_z : $M(Z) = a_0 + a_1 Z + \cdots + Z^s$.
On sait que a_0 est inversible si, et seulement si, z est inversible (alors $\langle z\rangle = \langle 1\rangle = \langle z^2\rangle$).
En outre z est nilpotent si, et seulement si, $M = Z^k$ pour un certain entier $k > 0$. Dans ce cas $z^k = 0 \in \langle z^{k+1}\rangle$.
Si z n'est ni inversible ni nilpotent alors considérons le plus petit $k < s$ tel que a_k est inversible. On écrit $-a_k z^k = z^{k+1}(a_{k+1} + \cdots + a_s z^{s-k-1})$, et en multipliant par l'inverse de $-a_k$ on obtient $z^k \in \langle z^{k+1}\rangle$. □

Lemme 2.4. *Sous les hypothèses du lemme 2.3, tout quotient* $\mathbf{A}/\langle z\rangle$ *est également un* $\mathbf{k}$*-espace vectoriel de dimension finie (explicite).*

Démonstration. L'idéal $\langle z\rangle$ est un sous-$\mathbf{k}$-espace vectoriel de type fini. Donc il admet une base explicite, et il possède un supplémentaire qui admet une base finie explicite. □

En fait, le lemme 2.3 est valide en remplaçant $\mathbf{k}$ par une $\mathbf{k}$-algèbre qui admet une base finie explicite. On réécrit la démonstration du lemme en scindant l'anneau en un produit de deux anneaux si a_0 n'est ni nilpotent ni inversible. Dans la composante où a_0 est inversible, la démonstration est terminée. Dans la composante où a_0 est nilpotent, on commence par forcer $a_0 = 0$ (lemme 2.4) et on traite a_1. Dans la composante où a_1 est inversible, la démonstration est terminée. Etc

On obtient précisément l'énoncé suivant.

Lemme 2.5. *Soit* $\mathbf{k}$ *un corps discret et* $\mathbf{b}$ *une* $\mathbf{k}$*-algèbre qui est un* $\mathbf{k}$*-espace vectoriel de dimension finie. Toute* $\mathbf{b}$*-algèbre qui est un* $\mathbf{b}$*-module libre de dimension finie peut être explicitée comme une* $\mathbf{k}$*-algèbre de dimension finie, à condition d'annuler certains éléments nilpotents qui se présentent au cours du calcul.*

Ceci conduit à la description suivante de ce qui se passe quand on applique la méthode D5.

Proposition 2.6. *Lorsque l'on étudie la clôture algébrique d'un corps discret* $\mathbf{k}$ *selon la méthode D5 on obtient un arbre de calcul du type suivant.*

1. *À la racine de l'arbre est implémenté le corps discret* $\mathbf{k}$ *avec la construction de ses éléments, son test à* 0*, ses lois d'anneaux et son passage à l'inverse des éléments* $\neq 0$*.*
2. *À chaque nœud* ν *de l'arbre est implémenté une* $\mathbf{k}$*-algèbre* $\mathbf{a}_\nu$ *de dimension finie.*
3. *Le passage d'un noeud* $\mathbf{a}$ *à son ou ses successeurs est de l'un des trois types suivants :*
   (a) *on introduit un zéro formel* z *d'un polynôme unitaire* $f \in \mathbf{a}[Z]$ *: on passe de* $\mathbf{a}$ *à* $\mathbf{a}[Z]/\langle f\rangle$ *;*
   (b) *à partir d'un élément* $u \in \mathbf{a}$ *qui est nilpotent mais non nul, on ajoute la contrainte* $u = 0$*, ce qui modifie* $\mathbf{a}$ *en conséquence ;*
   (c) *à partir d'un élément* $u \in \mathbf{a}$ *qui n'est ni nilpotent ni inversible on introduit deux embranchements vers des noeuds* $\mathbf{a}/\langle e\rangle$ *et* $\mathbf{a}/\langle 1-e\rangle$ *où* e *est l'idempotent de* $\mathbf{a}$ *vérifiant : modulo* e*,* u *est nilpotent, et modulo* $1-e$*,* u *est inversible.*
4. *Chaque* $\mathbf{k}$*-algèbre* $\mathbf{a}$ *implémentée à un nœud de l'arbre est isomorphe à une* $\mathbf{k}$-algèbre triangulaire $\mathbf{k}[x_1,\dots,x_r]$ *avec* $\mathbf{k}[x_1] \simeq \mathbf{k}[X_1]/\langle f_1\rangle$*,* f_1 *polynôme unitaire de* $\mathbf{k}[X_1]$*, et pour* $k>1$*,* $\mathbf{k}[(x_i)_{i\leqslant k}] \simeq \mathbf{k}[(x_i)_{i<k}][X_k]/\langle f_k\rangle$*,* f_k *polynôme unitaire de* $\mathbf{k}[(x_i)_{i<k}][X_k]$

Commentaire. La procédure de construction de l'arbre est extrêmement récursive : dans le cas *3c)* le calcul de l'idempotent $e \in \mathbf{k}[(x_i)_{i\leqslant k}]$ peut nécessiter d'affiner la connaissance de la $\mathbf{k}$-algèbre $\mathbf{k}[(x_i)_{i<k}]$ du nœud précédent et donc de la décomposer en un produit de plusieurs sous-$\mathbf{k}$-algèbres. ■

Première conclusion. L'article D5 a été écrit pour faciliter la description des corps de nombres en Calcul Formel. Sous sa forme originale telle que nous venons de l'exposer il fournit une sémantique constructive dynamique pour un objet «clôture algébrique d'un corps discret» qui n'a pas en général de sémantique constructive en tant qu'objet algébrique classique «statique».
Les performances du système D5 en termes de complexité algébrique n'ont pas vraiment tenu la promesse de ses autrices et auteur. Néanmoins, l'article van der Hoeven et Lecerf (2020), qui modifie un peu les algorithmes de départ, démontre sa pertinence également en termes de complexité algébrique. ■

2.2 Généralités sur les anneaux zéro-dimensionnels

Fait 2.7.

- *Tout anneau fini, tout corps discret est zéro-dimensionnel.*
- *Tout quotient et tout localisé d'un anneau zéro-dimensionnel est zéro-dimensionnel.*
- *Tout produit fini d'anneaux zéro-dimensionnels est un anneau zéro-dimensionnel.*
- *Une algèbre de Boole est un anneau zéro-dimensionnel.*

Le point *3* du lemme suivant généralise le lemme 2.1 en remplaçant l'idéal principal $\langle x\rangle$ par un idéal de type fini arbitraire.

Lemme 2.8. *Les propriétés suivantes sont équivalentes.*

1. $\mathbf{A}$ *est zéro-dimensionnel.*
2. $\forall x \in \mathbf{A}\ \exists e \in \mathbf{A}\ \exists h \in \mathbb{N}^*$ *tels que* $\langle x^h\rangle = \langle e\rangle$ *et* e *idempotent.*
3. *Pour tout idéal de type fini* $\mathfrak{a}$ *de* $\mathbf{A}$*, il existe* $d \in \mathbb{N}^*$ *tel que* $\mathfrak{a}^d = \langle e\rangle$ *où* e *est un idempotent. En particulier,*
   (a) $\mathfrak{a}$ *est nilpotent dans* $\mathbf{A}/\langle e\rangle$ *;*

(b) $\mathrm{Ann}(\mathfrak{a}^d) = \langle 1-e\rangle$;
(c) $\mathfrak{a}^r = \mathfrak{a}^d$ *pour* $r \geqslant d$;
(d) *en outre les générateurs de* $\mathfrak{a}$ *sont comaximaux dans* $\mathbf{A}/\langle 1-e\rangle$.

Le lemme qui suit peut être vu comme une généralisation partielle de la méthode D5.

Lemme 2.9 (lemme de scindage zéro-dimensionnel)**.** *Soit* $(z_i)_{i\in I}$ *une famille finie d'éléments dans un anneau zéro-dimensionnel* $\mathbf{A}$*. On sait construire un système fondamental d'idempotents orthogonaux* $(e_1, \ldots, e_n)$ *tel que dans chaque composante* $\mathbf{A}/\langle 1-e_j\rangle$*, chaque* z_i *est nilpotent ou inversible.*

Les anneaux zéro-dimensionnels réduits

Lemme 2.10 (anneaux zéro-dimensionnels réduits)**.**
Les propriétés suivantes sont équivalentes.

1. *L'anneau* $\mathbf{A}$ *est zéro-dimensionnel réduit.*
2. *Tout idéal principal est idempotent (i.e.* $\forall a \in \mathbf{A},\ a \in \langle a^2\rangle$*).*
3. *Tout idéal de type fini est engendré par un idempotent.*
4. *Le produit de deux idéaux de type fini est toujours égal à leur intersection.*

Fait 2.11. *Un anneau zéro-dimensionnel réduit est cohérent. Il est fortement discret*[4] *si, et seulement si, il y a un test d'égalité à zéro pour les idempotents.*

Exemple. Soit $\mathbb{P}$ l'ensemble des nombres premiers. L'anneau $\mathbf{A} = \prod_{p\in\mathbb{P}} \mathbb{Z}/\langle p\rangle$ est zéro-dimensionnel réduit mais il *n'est pas* discret. ∎

Dans les calculs, un anneau zéro-dimensionnel réduit se comporte comme un produit fini de corps discrets. Cela se concrétise sous forme dynamique par le principe de démonstration suivant.

Machinerie locale-globale élémentaire des anneaux zéro-dimensionnels réduits.
La plupart des algorithmes qui fonctionnent avec les corps discrets peuvent être modifiés de manière à fonctionner avec les anneaux zéro-dimensionnels réduits, en scindant l'anneau en deux composantes chaque fois que l'algorithme écrit pour les corps discrets utilise le test «cet élément est-il nul ou inversible ?». Dans la première composante l'élément en question est nul, dans la seconde il est inversible.

Exemple. Voici un exemple obtenu à partir du théorème qui affirme que sur un corps discret $\mathbf{k}$

1. toute matrice est équivalente à une matrice simple standard ;
2. tout $\mathbf{k}$-espace vectoriel de présentation finie est libre ;
3. tout sous-$\mathbf{k}$-espace vectoriel de type fini d'un $\mathbf{k}$-espace vectoriel de dimension finie admet un supplémentaire libre (théorème de la base incomplète).

Théorème 2.12 (le paradis des anneaux zéro-dimensionnels réduits)**.**
Soit $\mathbf{A}$ *un anneau zéro-dimensionnel réduit.*

1. *Toute matrice est équivalente à une matrice en forme de Smith avec des idempotents sur la diagonale principale.*

4. On dit qu'un anneau est fortement discret lorsqu'on a un test d'appartenance aux idéaux de type fini.

2. *Tout module de présentation finie est projectif de type fini, isomorphe à une somme directe finie d'idéaux $\langle e_i\rangle$ pour des idempotents e_i.*
3. *Tout sous-module de type fini d'un module de présentation finie est facteur direct.*

Exemple. Voici un autre exemple à propos de la mise en position de Noether d'un système polynomial.

Le théorème pour un corps discret est le suivant.

Théorème 2.13 (Nullstellensatz faible et mise en position de Noether, sans clôture algébrique)**.**
Soit $\mathbf{k}$ *un corps discret et* $(f_1,\dots,f_s)$ *un système polynomial dans l'algèbre* $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1,\dots,X_n]$ *($n \geqslant 1$). Notons* $\mathfrak{f} = \langle f_1,\dots,f_s\rangle_{\mathbf{k}[\underline{X}]}$ *et* $\mathbf{A} = \mathbf{k}[\underline{X}]/\mathfrak{f}$ *l'algèbre quotient.*

▷ (Nullstellensatz faible)

— *Ou bien* $\mathbf{A} = \{0\}$*, c'est-à-dire* $1 \in \langle f_1,\dots,f_s\rangle$*. Dans ce cas, le système* $(f_1,\dots,f_s)$ *n'admet de zéro dans aucune* $\mathbf{k}$*-algèbre non triviale.*

— *Ou bien il existe un quotient non nul de* $\mathbf{A}$ *qui est une* $\mathbf{k}$*-algèbre strictement finie.*

▷ (Position de Noether) *On a un entier* $r \in [\![-1..n]\!]$ *bien défini avec les propriétés suivantes.*

1. *Ou bien* $r = -1$ *et* $\mathbf{A} = \{0\}$*.*
2. *Ou bien* $r = 0$*, et* $\mathbf{A}$ *est une* $\mathbf{k}$*-algèbre strictement finie non nulle (en particulier, l'homomorphisme naturel* $\mathbf{k} \to \mathbf{A}$ *est injectif).*
3. *Ou bien* $r \geqslant 1$*, et il existe un changement de variables (les nouvelles variables sont notées* $Y_1,\dots,Y_n$*) qui satisfait les propriétés suivantes.*
   (a) *On a* $\mathfrak{f} \cap \mathbf{k}[Y_1,\dots,Y_r] = \{0\}$*. Autrement dit, l'anneau* $\mathbf{k}[Y_1,\dots,Y_r]$ *s'identifie à un sous-anneau du quotient* $\mathbf{k}[\underline{X}]/\mathfrak{f}$*.*
   (b) *Pour* $j \in [\![r+1..n]\!]$*,* Y_j *est entier sur* $\mathbf{k}[Y_1,\dots,Y_r]$ *modulo* $\mathfrak{f}$ *et l'anneau* $\mathbf{A}$ *est un* $\mathbf{k}[Y_1,\dots,Y_r]$*-module de présentation finie.*
   (c) *Il existe un entier* N *tel que pour chaque* $(\alpha_1,\dots,\alpha_r) \in \mathbf{k}^r$*, l'algèbre quotient* $\mathbf{A}/\langle Y_1-\alpha_1,\dots,Y_r-\alpha_r\rangle$ *est un* $\mathbf{k}$*-espace vectoriel non nul de dimension finie* $\leqslant N$*.*

Voici la version pour les anneaux zéro-dimensionnels réduits.

Théorème 2.13 bis (Nullstellensatz faible et mise en position de Noether, cas des anneaux zéro-dimensionnels réduits)
Soit $\mathbf{k}$ *un anneau zéro-dimensionnel réduit,* $(f_1,\dots,f_s)$ *un système polynomial dans l'algèbre* $\mathbf{C} = \mathbf{k}[\underline{X}] = \mathbf{k}[X_1,\dots,X_n]$ *Notons* $\mathfrak{f} = \langle f_1,\dots,f_s\rangle$ *et* $\mathbf{A} = \mathbf{k}[\underline{X}]/\mathfrak{f}$ *l'algèbre quotient. Il existe un système fondamental d'idempotents orthogonaux* $(e_{-1}, e_0,\dots,e_n)$ *de* $\mathbf{k}$ *tel que, en notant*

$$\mathbf{k}_r = \mathbf{k}/\langle 1-e_r\rangle,\ \mathbf{C}_r = \mathbf{k}_r \otimes_{\mathbf{k}} \mathbf{C} \simeq \mathbf{k}_r[\underline{X}] \text{ et } \mathbf{A}_r = \mathbf{A}/\langle 1-e_r\rangle = \mathbf{k}_r \otimes_{\mathbf{k}} \mathbf{A} \simeq \mathbf{C}_r/\mathfrak{f}\,\mathbf{C}_r,$$

on ait les résultats suivants.

1. $\mathbf{A}_{-1} = 0$*, i.e.* $1 \in \mathfrak{f}\,\mathbf{C}_{-1}$*.*
2. $\mathbf{k}_0 \cap \mathfrak{f}\,\mathbf{C}_0 = 0$ *et* $\mathbf{A}_0$ *est un* $\mathbf{k}_0$*-module projectif de type fini fidèle.*
3. *Pour* $r = 1$*, …,* n *on a un changement de variables tel que, en appelant* $Y_1,\dots,Y_n$ *les nouvelles variables,*
   (a) $\mathbf{k}_r[Y_1,\dots,Y_r] \cap \mathfrak{f}\,\mathbf{C}_r = 0$*, autrement dit l'algèbre* $\mathbf{k}_r[Y_1,\dots,Y_r]$ *peut être considérée comme une sous-*$\mathbf{k}_r$*-algèbre de* $\mathbf{A}_r$ *;*

(b) $\mathbf{A}_r$ *est un module de présentation finie sur* $\mathbf{k}_r[Y_1, \ldots, Y_r]$;

(c) *il existe un entier* N *tel que pour chaque* $(\alpha_1, \ldots, \alpha_r) \in \mathbf{k}_r^r$, *la* $\mathbf{k}_r$*-algèbre quotient* $\mathbf{A}_r/\langle Y_1 - \alpha_1, \ldots, Y_r - \alpha_r\rangle$ *est un* $\mathbf{k}_r$*-module projectif de type fini fidèle engendré par au plus* N *éléments.*

En conséquence, la $\mathbf{k}$*-algèbre* $\mathbf{A}$ *est un module de présentation finie sur la sous-algèbre «polynomiale»* $\prod_{r=0}^{n} \mathbf{k}_r[Y_1, \ldots, Y_r]$.

3 Les mathématiques constructives à la Bishop

Nous nous contenterons ici de renvoyer à l'annexe dans le livre Lombardi et Quitté (2021) et à l'article Coquand (2018) dont voici un extrait de l'introduction.

Brouwer's work on the foundation of mathematics is closely connected to his work on topology and the influences between these two research directions went both ways. While the notion of choice sequences, for instance, was clearly motivated by topological considerations, it also has been argued that the "logical ideas which he published several years before his topological work, were not only novel, but almost detailed enough to deduce rigorously some of his topological innovations from them" [25]. The links between foundation of mathematics and topology have recently been revisited by the discovery of the univalence axiom [37] and the univalent foundations program [37, 36]. From a logical point of view, one puzzling feature of this approach is the use of homotopy theory, developed in a highly non effective way [9, 22, 18], to provide a semantics of dependent type theory [12], which is usually thought of as a formal system for expressing constructive mathematics [28]. This semantics is indeed based on the notion of Kan simplicial sets, and basic properties about Kan simplicial sets used for representing spaces are inherently non constructive [3, 31]. This is surprising since one goal of this notion was precisely to provide a combinatorial account of higher homotopy groups [24]. The first part of this paper consists in an analysis of this situation from a constructive point of view. We present a basic result (Theorem 1.8) which suggests an alternative and effective formulation of basic notions of homotopy theory. The second part explains that this work has close connections with the foundation of constructive mathematics, and in particular with Bishop's notion of set [5]. This also is related to the question of how to represent collections of mathematical structures (and the notion of category) in a constructive setting [29].

---

3 M. Bezem, Th. Coquand, A Kripke model for simplicial sets, Theoret. Comput. Sci. 574 (2015) 86-91.

5 E. Bishop, Foundations of Constructive Analysis, McGraw-Hill Book Co., 1967.

9 D.-C. Cisinski, Les préfaisceaux comme modèles des types d'homotopie, Astérisqu 308 (2006).

12 N. G. de Bruijn, The Mathematical Language AUTOMATH, its Usage, and Some of its Extensions, in : Lecture Notes in Mathematics, vol. 125, Springer, Berlin, 1970, p. 29-61.

18 P. G. Goerss, J. F. Jardine, Simplicial Homotopy Theory, in : Progress in Mathematics, Birkhäuser, 2009.

22 A. Joyal, M. Tierney, Notes on simplicial homotopy theory. Preprint, 2008.

24 D. Kan, A combinatorial definition of homotopy groups, Ann. of Math. (2) 67 (1958) 282-312.

25 G. Kreisel, M. H. A. Newman, Luitzen Egbertus Jan Brouwer (1881–1966), Biogr. Mem. Fellows Roy. Soc. 15 (1969) 39-68.

28 P. Martin-Löf, An Intuitionistic Theory of Types : Predicative Part. Logic Colloquium'73, North-Holland, Amsterdam, 1975, p. 73-118.

29 R. Mines, F. Richman, W. Ruitenburg, A Course in Constructive Algebra, Springer-Verlag, 1988. Traduction française par Henri Lombardi, révisée par Stefan Neuwirth. Un cours d'algèbre constructive. Presses Universitaires de Franche-Comté. 2020.
31 E. Parmann, Case Studies in Constructive Mathematics (Ph.D.), University of Bergen, 2016.
37 V. Voevodsky, The equivalence axiom and univalent models of type theory. Talk at CMU, `https://arxiv.org/abs/1402.5556`, 2010.

4 La méthode dynamique en mathématiques constructives

4.1 L'invention de la méthode dynamique par Paul Lorenzen

La méthode dynamique est exposée pour la première fois (à notre connaissance) par Paul Lorenzen, mathématicien et philosophe allemand, dans l'article Lorenzen 1950 où il développe de manière constructive son célèbre article antérieur Lorenzen 1939.

Voir les commentaires dans Neuwirth 2021, Coquand, Lombardi, et Neuwirth 2019 et Coquand, Lombardi, et Neuwirth 2021.

Dans cet article Lorenzen explique le contenu constructif du théorème de Krull qui affirme que la clôture intégrale d'un anneau intègre $\mathbf{A}$ est l'intersection des anneaux de valuation de son corps de fractions qui contiennent $\mathbf{A}$. Il n'utilise aucun des mystérieux anneaux de valuation de Krull et remplace cette intersection infinie d'objets purement idéaux par un nombre fini de tests dans des anneaux concrets que l'on peut voir comme des approximations finies des anneaux de valuation en question.

Concernant les groupes ordonnés il explique comment construire le groupe réticulé engendré par un monoïde préordonné donné. En utilisant librement le lemme de Zorn, il en déduit toutes les manières possibles de construire un morphisme du monoïde de départ vers un groupe totalement ordonné. La méthode consiste à construire un treillis distributif aux nœuds duquel on ouvre deux branches chaque fois que se présente le problème, pour un élément x du groupe ordonné en cours de construction, de décider si $x \geqslant 0$ ou $x \leqslant 0$.

L'article Lorenzen 1953 souligne l'importance des treillis distributifs et utilise la première version connue du «théorème fondamental des relations implicatives» qu'il a démontré par ailleurs et qui a été redécouvert indépendamment par Cederquist et Coquand (2000).

Dans le même article, Lorenzen explique aussi comment construire, pour un anneau intègre et intégralement clos, un groupe réticulé «de divisibilité» qui correspond, *via* le lemme de Zorn, à tous les morphismes possibles de l'anneau vers un anneau de valuation (i.e. un anneau intègre dont le groupe de divisibilité est totalement ordonné). De manière étonnante, ce groupe, que nous appelons *le groupe de Lorenzen pour l'anneau*, est rarement mis en valeur ou même cité dans la littérature usuelle. Dans le cas d'un domaine de Prüfer, ce groupe est le groupe des idéaux fractionnaires inversibles de l'anneau.

4.2 Un article fondateur

L'article Coste, Lombardi, et Roy 2001 explique de manière générale la méthode dynamique en la mettant en relation directe avec la théorie des topos cohérents de Grothendieck. C'est plutôt un article de logique que d'algèbre constructive, mais la méthode dynamique en question permet de décrypter constructivement des résultats d'algèbre abstraite qui établissent des «certificats algébriques» (dans le style du Nullstellensatz de Hilbert)

qui donnent une explication purement algébrique de phénomènes de nature géométrique comme l'inclusion d'une variété algébrique dans une autre (une fois les scalaires étendus à un corps algébriquement clos).

Au sujet de l'utilisation de la logique en algèbre constructive voir l'article Coquand et Lombardi 2006.

4.3 Décryptage de démonstrations qui utilisent la localisation en tout idéal premier

Un argument de localisation typique fonctionne comme suit en mathématiques classiques. Lorsque l'anneau est local une certaine propriété P est vérifiée en vertu d'une démonstration assez concrète. Lorsque l'anneau n'est pas local, la même propriété est encore vraie (d'un point de vue classique non constructif) car il suffit de la vérifier localement. Ceci en vertu d'un principe local-global abstrait.

Nous examinons avec un peu d'attention la première démonstration. Nous voyons alors apparaitre certains calculs qui sont légitimes en vertu du principe suivant :

$$\forall x \in \mathbf{A} \quad x \in \mathbf{A}^{\times} \text{ ou } x \in \mathrm{Rad}(\mathbf{A}),$$

principe qui est appliqué à des éléments x provenant de la démonstration elle-même. Autrement dit, la démonstration classique donnée dans le cas local nous fournit une démonstration constructive sous l'hypothèse d'un anneau local résiduellement discret. Voici alors notre décryptage dynamique constructif. Dans le cas d'un anneau arbitraire, nous répétons la même démonstration, en remplaçant chaque disjonction «x est inversible ou x est dans le radical», par la considération des deux anneaux [5] $\mathbf{A}_{\mathcal{S}(I,x;U)}$ et $\mathbf{A}_{\mathcal{S}(I;x,U)}$, où $\mathbf{A}_{\mathcal{S}(I,U)}$ est la localisation «courante» de l'anneau $\mathbf{A}$ de départ, à l'endroit de la démonstration où l'on se trouve. Lorsque la démonstration initiale est ainsi déployée, on a construit à la fin un certain nombre, fini parce que la démonstration est finie, de localisés $\mathbf{A}_{S_i}$, pour lesquels la propriété est vraie. Et les monoïdes S_i sont comaximaux par construction.
D'un point de vue constructif, nous obtenons ainsi le résultat «quasi global» pour l'anneau $\mathbf{A}$, c'est-à-dire le résultat après localisation en des monoïdes comaximaux, en vertu du lemme 4.3. On fait alors appel à un principe local-global concret pour conclure.

Notre décryptage de la démonstration classique est rendu possible par le fait que la propriété P étudiée est de caractère fini : elle est conservée par localisation, et si elle est vraie après localisation en un monoïde S, elle est également vraie après localisation en un élément $s \in S$.

Le décryptage complet contient donc deux ingrédients essentiels. Le premier est le décryptage de la démonstration donnée dans le cas local qui permet d'obtenir un résultat quasi global (parce que la propriété est de caractère fini). Le deuxième est la démonstration constructive du principe local-global concret correspondant au principe local-global abstrait utilisé en mathématiques classiques. Dans tous les exemples que nous avons rencontrés, cette démonstration constructive n'offre aucune difficulté parce que la démonstration que nous trouvons dans la littérature classique donne déjà l'argument concret, au moins sous forme télégraphique (sauf parfois dans Bourbaki, lorsqu'il réussit à dissimuler habilement les arguments concrets).

La conclusion générale est que les démonstrations classiques «par principe local-global abstrait» sont déjà constructives, si l'on veut bien se donner la peine de les lire en détail.

5. Voir la définition 4.2.

C'est une bonne nouvelle, outre le fait que cela confirme que les mathématiques ne sont le lieu d'aucun miracle surnaturel.

Définition 4.1. On dit que *les monoïdes* $S_1, \ldots, S_n$ *de l'anneau* $\mathbf{A}$ *recouvrent le monoïde* S si S est contenu dans le saturé de chaque S_i et si un idéal de $\mathbf{A}$ qui coupe chacun des S_i coupe toujours S, autrement dit si l'on a :

$$\forall s_1 \in S_1 \ \ldots \ \forall s_n \in S_n \ \exists a_1, \ldots, a_n \in \mathbf{A} \quad \sum\nolimits_{i=1}^{n} a_i s_i \in S.$$

Des monoïdes sont comaximaux s'ils recouvrent le monoïde $\{\,1\,\}$.

Définition et notation 4.2. Soient U et I des parties de l'anneau $\mathbf{A}$. Nous notons $\mathcal{M}(U)$ le monoïde engendré par U, et $\mathcal{S}(I,U)$ est le monoïde :

$$\mathcal{S}(I,U) = \langle I \rangle_{\mathbf{A}} + \mathcal{M}(U).$$

Le couple $\mathfrak{q} = (I,U)$ est encore appelé un *idéal premier potentiel*, et l'on note (par abus) $\mathbf{A}_{\mathfrak{q}}$ pour $\mathbf{A}_{\mathcal{S}(I,U)}$. De la même manière on note :

$$\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell) = \langle a_1, \ldots, a_k \rangle_{\mathbf{A}} + \mathcal{M}(u_1, \ldots, u_\ell).$$

Nous disons qu'un tel monoïde *admet une description finie*. Le couple

$$(\{\,a_1, \ldots, a_k\,\}, \{\,u_1, \ldots, u_\ell\,\})$$

est appelé un *idéal premier potentiel fini*.

Lemme 4.3 (lemme des localisations successives)**.**
Soient U et I des parties de l'anneau $\mathbf{A}$ et $a \in \mathbf{A}$; alors les monoïdes

$$\mathcal{S}(I; U, a) \overset{\text{déf}}{=} \mathcal{S}(I, U \cup \{\,a\,\}) \ \text{ et } \ \mathcal{S}(I, a; U) \overset{\text{déf}}{=} \mathcal{S}(I \cup \{\,a\,\}, U)$$

recouvrent le monoïde $\mathcal{S}(I,U)$.
En particulier, les monoïdes $S = \mathcal{M}(a) = \mathcal{S}(0;a)$ et $S' = \mathcal{S}(a;1) = 1 + a\mathbf{A}$ sont comaximaux.

La méthode indiquée ci-dessus donne donc, comme corolaire[6] du lemme 4.3, le principe général de décryptage suivant, qui *permet d'obtenir automatiquement une version constructive globale (ou au moins quasi globale) d'un théorème à partir de sa version locale.*

Machinerie locale-globale à idéaux premiers.
Lorsque l'on relit une démonstration constructive, donnée pour le cas d'un anneau local résiduellement discret, avec un anneau $\mathbf{A}$ arbitraire, que l'on considère au départ comme $\mathbf{A} = \mathbf{A}_{\mathcal{S}(0;1)}$ et qu'à chaque disjonction (pour un élément a qui se présente au cours du calcul dans le cas local)

$$a \in \mathbf{A}^{\times} \text{ ou } \ a \in \mathrm{Rad}(\mathbf{A}),$$

on remplace l'anneau «en cours» $\mathbf{A}_{\mathcal{S}(I,U)}$ par les deux anneaux $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$ (dans chacun desquels le calcul peut se poursuivre), on obtient à la fin de la relecture une famille finie d'anneaux $\mathbf{A}_{\mathcal{S}(I_j,U_j)}$ avec les monoïdes $\mathcal{S}(I_j,U_j)$ comaximaux et I_j, U_j finis.

6. Le lecteur ou la lectrice sera sans doute surprise de l'orthographe du mot 'corolaire', avec d'autres innovations auxquelles elle n'est pas habituée, comme la suppression de certains accents circonflexes. En fait, nous avons essayé de suivre au plus près les préconisations de l'orthographe nouvelle recommandée, telle qu'elle est enseignée aujourd'hui dans les écoles en France.

Dans chacun de ces anneaux, le calcul a été poursuivi avec succès et a donné le résultat souhaité.
On obtient ainsi la version quasi globale du résultat pour l'anneau $\mathbf{A}$*, c'est-à-dire le résultat après localisation en des monoïdes comaximaux. On fait ensuite appel à un principe local-global concret pour conclure que le résultat est constructivement valide pour l'anneau* $\mathbf{A}$ *lui-même.*

On notera que si «l'anneau en cours» est $\mathbf{B} = \mathbf{A}_{\mathcal{S}(I;U)}$ et si la disjonction porte sur

$$b \in \mathbf{B}^\times \text{ ou } b \in \mathrm{Rad}(\mathbf{B}),$$

avec $b = a/(u+i)$, $a \in \mathbf{A}$, $u \in \mathcal{M}(U)$ et $i \in \langle I \rangle_{\mathbf{A}}$, alors il faut considérer les localisés $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$.

La machinerie locale-globale à idéaux premiers a été exposée dans Lombardi et Quitté 2003, Fez. Elle est utilisée depuis de manière systématique dans les articles écrits dans le style des mathématiques constructives à la Bishop.

4.4 Quotienter par tous les idéaux maximaux

Références : Outre la section XV-6 dans Lombardi et Quitté (2021) on pourra consulter l'article original Yengui 2008.

On trouve dans la littérature un certain nombre de démonstrations dans lesquelles l'auteur démontre un résultat en considérant «le passage au quotient par un idéal maximal arbitraire». L'analyse de ces démonstrations montre que le résultat peut être compris comme le fait qu'un anneau obtenu à partir de constructions plus ou moins compliquées est en fait réduit à 0. Par exemple, si l'on veut démontrer qu'un idéal $\mathfrak{a}$ de $\mathbf{A}$ contient $1_{\mathbf{A}}$, on raisonne par l'absurde, on considère un idéal maximal $\mathfrak{m}$ qui contiendrait $\mathfrak{a}$, et l'on trouve une contradiction en faisant un calcul dans le corps résiduel $\mathbf{A}/\mathfrak{m}$.

Cela revient à appliquer le principe «un anneau qui n'a pas d'idéaux maximaux est réduit à 0».

Le fait de présenter le raisonnement comme une démonstration par l'absurde est le résultat d'une déformation professionnelle. Car prouver qu'un anneau est réduit à 0 est un fait de nature concrète (on doit prouver que $1 = 0$ dans l'anneau considéré), et non pas une absurdité. Et le calcul fait dans le corps $\mathbf{A}/\mathfrak{m}$ ne conduit à une absurdité que parce que l'on a décidé un jour que dans un corps, il est interdit que $1 = 0$. Mais le calcul n'a rien à voir avec une telle interdiction. Le calcul dans un corps utilise le fait que tout élément est nul ou inversible, mais pas le fait que cette disjonction serait exclusive.

En conséquence, la relecture dynamique de la démonstration par l'absurde en une démonstration constructive est possible selon la méthode suivante. Suivons le calcul que l'on nous demande de faire comme si l'anneau $\mathbf{A}/\mathfrak{a}$ était vraiment un corps. Chaque fois que le calcul exige de savoir si un élément x_i est nul ou inversible modulo $\mathfrak{a}$, parions sur $x_i = 0$ et rajoutons cet x_i à l'idéal $\mathfrak{a}$. Au bout d'un certain temps, on trouve que $1 = 0$ modulo l'idéal construit. Au lieu de perdre courage devant une telle absurdité, voyons le bon côté des choses. Nous venons par exemple de constater que $1 \in \mathfrak{a} + \langle x_1, x_2, x_3 \rangle$. Ceci est un fait positif et non une absurdité. Nous venons en fait de calculer un inverse y_3 de x_3 dans $\mathbf{A}$ modulo $\mathfrak{a} + \langle x_1, x_2 \rangle$. Nous pouvons donc examiner le calcul que nous demande de faire la démonstration classique lorsque $x_1, x_2 \in \mathfrak{m}$ et x_3 est inversible modulo $\mathfrak{m}$. À ceci près que nous n'avons pas besoin de $\mathfrak{m}$ puisque nous venons d'établir que x_3 est inversible modulo $\mathfrak{a} + \langle x_1, x_2 \rangle$.

Contrairement à la stratégie qui correspondait à la localisation en n'importe quel idéal premier, nous n'essayons pas de déployer tout l'arbre du calcul qui semble se présenter

à nous. Nous n'utilisons que des quotients, et pour cela nous suivons systématiquement la branche «être nul» (modulo $\mathfrak{m}$) plutôt que la branche «être inversible». Ceci crée des quotients successifs de plus en plus poussés. Lorsqu'une soi-disant contradiction apparait, c'est-à-dire lorsqu'un calcul a abouti à un certain résultat de nature positive, nous revenons en arrière en profitant de l'information que nous venons de récolter : un élément a été certifié inversible dans le quotient précédent.

Résumons la discussion précédente.

Machinerie locale-globale à idéaux maximaux.
Pour relire une démonstration classique qui démontre par l'absurde qu'un anneau $\mathbf{A}$ *est trivial en supposant le contraire, puis en considérant un idéal maximal* $\mathfrak{m}$ *de cet anneau, en faisant un calcul dans le corps résiduel et en trouvant la contradiction* $1 = 0$*, procéder comme suit.*
Premièrement s'assurer que la démonstration devient une démonstration constructive que $1 = 0$ *sous l'hypothèse supplémentaire que* $\mathbf{A}$ *est un corps discret.*
Deuxièmement, supprimer l'hypothèse supplémentaire et suivre pas à pas la démonstration précédente en privilégiant la branche $x = 0$ *chaque fois que la disjonction «*$x = 0$ *ou* x *inversible» est requise pour la suite du calcul. Chaque fois que l'on prouve* $1 = 0$ *on a en fait montré que dans l'anneau quotient précédemment construit, le dernier élément à avoir subi le test était inversible, ce qui permet de remonter à ce point pour suivre la branche «*x *inversible» conformément à la démonstration proposée pour le cas inversible (qui est maintenant certifié). Si la démonstration considérée est suffisamment uniforme (l'expérience montre que c'est toujours le cas), le calcul obtenu dans son ensemble est fini et aboutit à la conclusion souhaitée.*

4.5 Localiser en tous les idéaux premiers minimaux

Références : Outre les sections XV-7 et XVI-2 dans Lombardi et Quitté (2021) on pourra consulter l'article original Coquand 2006.

La lectrice est maintenant mise à contribution pour se convaincre de la justesse de la méthode suivante, en remplaçant dans la section précédente l'addition par la multiplication et le passage au quotient par la localisation.

Machinerie locale-globale à idéaux premiers minimaux.
Pour relire une démonstration classique qui démontre par l'absurde qu'un anneau $\mathbf{A}$ *est trivial en supposant le contraire, puis en considérant un idéal premier minimal de cet anneau, en faisant un calcul dans l'anneau localisé (qui est local et zéro-dimensionnel, donc un corps dans le cas réduit) et en trouvant la contradiction* $1 = 0$*, procéder comme suit.*
Premièrement s'assurer que la démonstration devient une démonstration constructive de l'égalité $1 = 0$ *sous l'hypothèse supplémentaire que* $\mathbf{A}$ *est local et zéro-dimensionnel.*
Deuxièmement, supprimer l'hypothèse supplémentaire et suivre pas à pas la démonstration précédente en privilégiant la branche «x *inversible» chaque fois que la disjonction «*x *nilpotent ou* x *inversible» est requise pour la suite du calcul. Chaque fois que l'on prouve* $1 = 0$ *on a en fait montré que dans l'anneau localisé précédemment construit, le dernier élément à avoir subi le test était nilpotent, ce qui permet de remonter à ce point pour suivre la branche «*x *nilpotent» conformément à la démonstration proposée pour le cas nilpotent (qui est maintenant certifié). Si la démonstration considérée est suffisamment uniforme (l'expérience montre que c'est toujours le cas), le calcul obtenu dans son ensemble est fini et aboutit à la conclusion souhaitée.*

4.6 Autres utilisations de la clôture algébrique dynamique d'un corps discret

Voir par exemple l'article Coquand, Lombardi, et Neuwirth (2025) où l'on construit des $\mathbf{k}$-algèbres finies pour un corps de base $\mathbf{k}$ sur lequel est définie une algèbre centrale simple. On procède comme pour la méthode D5 mais de manière très économique : lorsqu'un élément z de la $\mathbf{k}$-algèbre de dimension finie que l'on construit (pour mimer un sous-corps de la clôture algébrique ou de la clôture séparable de $\mathbf{k}$) n'est pas inversible, on se contente d'ajouter la contrainte $z = 0$.

4.7 Autres usages de la méthode dynamique en mathématiques constructives

On peut citer le principe de recouvrement par quotients XI-2.10 dans Lombardi et Quitté 2021. Il affirme que pour démontrer une relation $a \leqslant b$ entre deux éléments d'un groupe réticulé, on peut toujours se limiter au cas où le groupe réticulé est totalement ordonné. Précisément, cela revient à dire qu'an cours du calcul visant à démontrer la relation, on peut supposer que les éléments $z_1, \ldots, z_r$ qui interviennent dans le calcul sont totalement ordonnés. De nombreux exemples de telles relations sont donnés [7] dont la preuve est identique : *dans le cas d'un groupe réticulé totalement ordonné, la relation est claire*.

Un autre exemple remarquable, dû à Ihsen Yengui, intervient dans la démonstration du théorème de Lequain-Simis : *Si* $\mathbf{A}$ *est un anneau arithmétique, tout module projectif de type fini sur* $\mathbf{A}[X_1, \ldots, X_n]$ *est étendu depuis* $\mathbf{A}$. Voir l'article Ellouz, Lombardi, et Yengui 2008 ou Lombardi et Quitté 2021, Théorème XVI-6.13.

Puisque nous parlons de Ihsen Yengui, signalons un autre tour de force (qui n'a cependant rien à voir avec le méthodes dynamiques) qui est une démonstration presque constructive du fait que pour un anneau de valuation intègre (ou un domaine de Prüfer) $\mathbf{V}$ l'anneau $\mathbf{V}[X_1, \ldots, X_n]$ est cohérent, sans hypothèse de type noethérien ou de dimension de Krull concernant $\mathbf{V}$: voir Ducos, Valibouze, et Yengui 2015.

Références

Errett Bishop : *Foundations of constructive analysis*. McGraw-Hill, New York, 1967. 2

Jan Cederquist et Thierry Coquand : Entailment relations and distributive lattices. *In Logic Colloquium '98 (Prague)*, volume 13 de *Lect. Notes Log.*, pages 127–139. Assoc. Symbol. Logic, Urbana, IL, 2000. 9

Thierry Coquand : On seminormality. *J. Algebra*, 305(1):577–584, 2006. 13

Thierry Coquand : Combinatorial topology and constructive mathematics. *Indag. Math., New Ser.*, 29:1637–1648, 2018. 8

Thierry Coquand et Henri Lombardi : A logical approach to abstract algebra. *Math. Struct. Comput. Sci.*, 16:885–900, 2006. URL `http://hlombardi.free.fr/publis/AlgebraLogicCoqLom.pdf`. 10

Thierry Coquand, Henri Lombardi et Stefan Neuwirth : Lattice-ordered groups generated by an ordered group and regular systems of ideals. *Rocky Mt. J. Math.*, 49:1449–1489, 2019. URL `https://arxiv.org/abs/1701.05115`. 9

7. Par exemple $x + y = |x - y| + 2(x \wedge y)$.

Thierry Coquand, Henri Lombardi et Stefan Neuwirth : Regular entailment relations. *In Paul Lorenzen – mathematician and logician. Contributions presented at the workshop, Konstanz, Germany, March 8–9, 2018*, pages 103–114. Cham : Springer, 2021. URL `https://arxiv.org/abs/1912.09480`. 9

Thierry Coquand, Henri Lombardi et Stefan Neuwirth : Constructive basic theory of central simple algebras. Preprint, arXiv :2102.12775 [math.RA], 2025. URL `https://arxiv.org/abs/2102.12775`. 14

Michel Coste, Henri Lombardi et Marie-Françoise Roy : Dynamical method in algebra : effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111:203–256, 2001. URL `http://arxiv.org/abs/1701.05794`. 9

Patrick Dehornoy : *La théorie des ensembles. Introduction à une théorie de l'infini et des grands cardinaux*, volume 106 de *Tableau Noir*. Paris : Calvage et Mounet, 2017. 2

Jean Della Dora, Claire Dicrescenzo et Dominique Duval : About a new method for computing in algebraic number fields. *In* Bob F. Caviness, éditeur : *EUROCAL '85. European Conference on Computer Algebra, Linz, Austria, April 1-3, 1985. Proceedings. Vol. 2 : Research contributions*, Lect. Notes Comput. Sci., 204, pages 289–290. Springer, Berlin, 1985. 2

Gema-Maria Díaz-Toca, Henri Lombardi et Claude Quitté : *Modules sur les anneaux commutatifs. Cours et exercices.* Paris : Calvage & Mounet, 2014. 2

Lionel Ducos, Annick Valibouze et Ihsen Yengui : Computing syzygies over $\mathbf{V}[X_1, \ldots, X_k]$, $\mathbf{V}$ a valuation domain. *J. Algebra*, 425:133–145, 2015. 14

Afef Ellouz, Henri Lombardi et Ihsen Yengui : A constructive comparison of the rings $R(X)$ and $R\langle X\rangle$ and application to the Lequain-Simis induction theorem. *J. Algebra*, 320:521–533, 2008. 14

A. K. Lenstra, H. W. Lenstra, Jr. et L. Lovász : Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982. 2

Henri Lombardi et Claude Quitté : Constructions cachées en algèbre abstraite : Le principe local-global. *In Commutative ring theory and applications. Proceedings of the fourth international conference, Fez, Morocco, June 7-12, 2001*, pages 461–476. New York, NY : Marcel Dekker, 2003. 12

Henri Lombardi et Claude Quitté : *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices.* Paris : Calvage & Mounet, 2021. Deuxième édition, revue et étendue, du livre paru en 2011. 2, 8, 12, 13, 14

Paul Lorenzen : Abstrakte Begründung der multiplikativen Idealtheorie. *Math. Z.*, 45:533–553, 1939. 9

Paul Lorenzen : Über halbgeordnete Gruppen. *Math. Z.*, 52:483–526, 1950. URL `http://eudml.org/doc/169131`. 9

Paul Lorenzen : Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen. *Math. Z.*, 58:15–24, 1953. URL `http://eudml.org/doc/169331`. 9

Stefan Neuwirth : Lorenzen's reshaping of Krull's Fundamentalsatz for integral domains (1938–1953). *In Paul Lorenzen – mathematician and logician. Contributions presented at the workshop, Konstanz, Germany, March 8–9, 2018*, pages 143–183. Cham : Springer, 2021. 9

Joris van der Hoeven et Grégoire Lecerf : Directed evaluation. *J. Complexity*, 60:45, 2020. 5

Ihsen Yengui : Making the use of maximal ideals constructive. *Theoret. Comput. Sci.*, 392 (1-3):174–178, 2008. 12