Le système D5, la méthode dynamique et les mathématiques constructives

Henri Lombardi*

23 avril 2026

Je ne crois pas aux miracles
Un mathématicien constructif

1 Introduction

Cette brève note consacrée à la méthode D5 qui illustre les mathématiques constructives dans le style de Bishop, introduites dans l'ouvrage révolutionnaire (Bishop 1967, Foundations of Constructive Analysis).

En mathématiques classiques les preuves d'existence sont rarement explicites. Deux obstacles essentiels apparaissent chaque fois que l'on essaie de rendre une telle preuve explicite.

Le premier obstacle est l'application du principe du tiers exclu. Par exemple, si vous considérez la preuve que tout polynôme univarié sur un corps $\mathbf{K}$ admet une décomposition en facteurs premiers, vous avez une sorte d'algorithme dont l'ingrédient essentiel est : si P est irréductible c'est bon, si P se décompose en un produit de deux facteurs de degrés $\geqslant 1$, c'est bon aussi, par hypothèse de récurrence sur le degré de P.

Malheureusement la disjonction qui sert à faire fonctionner la preuve «P est irréductible ou P se décompose en un produit de deux facteurs de degré $\geqslant 1$» n'est pas en général explicite. Autrement dit, même si un corps est défini de manière constructive, on ne peut être certain que cette disjonction puisse être explicitée par un algorithme. Nous nous trouvons ici en présence d'un cas typique où le principe du tiers exclu «pose problème», car l'existence d'un facteur irréductible ne peut pas faire l'objet d'un algorithme général.

Le deuxième obstacle est l'application du lemme de Zorn, qui permet de généraliser au cas non dénombrable les raisonnements par récurrence usuels dans le cas dénombrable.

Par exemple dans le Modern Algebra de van der Waerden le second écueil est évité en se limitant aux structures algébriques dénombrables.

Nous avons cependant deux faits d'expérience désormais bien établis.

— De nombreux résultats concrets *universels*[1] démontrés par les méthodes abstraites douteuses ci-dessus n'ont jamais été contredits. On a même très souvent réussi à en fournir des démonstrations constructives incontestables. Cela signifierait que même si les méthodes abstraites sont quelque part fautives ou contradictoires, elles ont jusqu'à présent été utilisées avec suffisamment de discernement.

*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. En particulier des résultats qui sont équivalents à un énoncé du genre : telle fonction primitive récursive de $\mathbb{N}$ vers $\{0, 1\}$ est identiquement nulle. La conjecture de Golbach par exemple est un énoncé de ce type.

— De nombreux résultats concrets *existentiels*[2] démontrés par les méthodes abstraites douteuses n'ont pas non plus été infirmés. Bien au contraire, ils ont souvent été confirmés par des algorithmes démontrés constructivement.

Face à cette situation un peu paradoxale : les méthodes abstraites sont à priori douteuses, mais elles ne nous trompent pas fondamentalement quand elles donnent un résultat de nature concrète, il y a deux réactions possibles.

Ou bien l'on croit que les méthodes abstraites sont fondamentalement justes parce qu'elles reflètent une «réalité», une sorte d'«univers cantorien idéal» dans lequel se trouve la vraie sémantique des mathématiques. C'est la position du réalisme platonicien, défendue par exemple par Gödel.

Ou bien l'on pense que les méthodes abstraites sont vraiment sujettes à caution. Mais alors, à moins de croire que les mathématiques relèvent de la magie ou du miracle, il faut expliquer pourquoi les mathématiques classiques se trompent si peu. Si l'on ne croit ni à Cantor, ni aux miracles, on est conduit à penser que les preuves abstraites de résultats concrets contiennent nécessairement des «ingrédients cachés» suffisants pour construire les preuves concrètes correspondantes.

Cette possibilité de certifier constructivement des résultats concrets obtenus par des méthodes douteuses, si l'on arrive à la réaliser de manière assez systématique, est dans le droit fil du programme de Hilbert.

La méthode dynamique en algèbre constructive est une méthode générale de décryptage des preuves abstraites des mathématiques classiques lorsqu'elles utilisent des objets «idéaux» dont l'existence repose sur des principes non constructifs : le tiers exclu et l'axiome du choix. L'ambition de cette nouvelle méthode est de «donner une sémantique constructive pour les mathématiques classiques usuellement pratiquées».

Nous remplaçons les objets abstraits des mathématiques classiques par des spécifications incomplètes mais concrètes de ces objets. C'est la contrepartie constructive des objets abstraits. Par exemple un *idéal premier potentiel fini* est donné par un nombre fini d'éléments dans l'idéal et un nombre fini d'éléments dans son complémentaire. Cela constitue une spécification incomplète mais concrète d'un idéal premier.

Plus précisément, la méthode dynamique vise à donner une interprétation systématique de preuves classiques qui utilisent des objets abstraits en les relisant comme des démonstrations constructives au sujet de contreparties constructives de ces objets abstraits.

Cela se situe dans le même esprit que certaines techniques développées en calcul formel. Nous pensons ici à l'«évaluation paresseuse», ou l'«évaluation dynamique», c'est-à-dire l'évaluation paresseuse gérée de manière arborescente, comme dans le système D5 Della Dora *et al.* (1985) qui réalise de manière très innocente ce tour de force : calculer de manière sûre dans la clôture algébrique d'un corps arbitraire, alors même que l'on sait que cet objet (la clôture algébrique) ne peut pas être construit en toute généralité.

2 Le système 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 au départ d'une extension finie de $\mathbb{Q}$, de la forme $\mathbf{K} = \mathbb{Q}[\xi]$ où ξ est un nombre algébrique complexe. 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

2. En particulier des résultats équivalents à un énonce du genre : pour tout $x \in \mathbb{N}$ il existe un $y \in \mathbb{N}$ tel que $f(x, y) = 0$, où f est fonction primitive récursive de $\mathbb{N}^2$ vers $\{0, 1\}$. La conjecture $\mathcal{P} \neq \mathcal{NP}$ en informatique théorique est un énoncé de ce type.

les calculs deviennent très compliqués lorsqu'on veut introduire une extension $\mathbb{Q}[\xi,\zeta]$ où ζ est un zéro d'un polynôme sur $\mathbb{Q}[\xi]$ dont on ne sait pas s'il est irréductible. Ou encore $\mathbb{Q}[\xi,\zeta,\alpha]$ et α est un zéro d'un polynôme sur $\mathbb{Q}[\xi,\zeta]$ dont on ne sait pas s'il est irréductible.

Plus généralement, si $\mathbf{K}$ est un corps discret arbitraire [3], on ne sait pas construire les objets qui, en mathématiques classiques, s'appellent le corps des racines d'un polynôme, ou de manière plus générale la clôture séparable, notée $\mathbf{K}^{\mathrm{sep}}$, et la clôture algébrique de $\mathbf{K}$, notée $\mathbf{K}^{\mathrm{alg}}$ [4].

L'article D5 propose la solution paresseuse suivante : on peut introduire des zéros de polynômes successifs $f, g, h, \ldots$ de manière purement formelle et calculer dans la $\mathbf{K}$-algèbre obtenue comme si c'était un corps discret. Par exemple

$$\mathbf{A} = \mathbf{K}[X,Y,Z]/\langle f(X), g(X,Y), h(X,Y,Z)\rangle = \mathbf{K}[x,y,z]\,,$$

avec $f \in \mathbf{K}[X]$ unitaire, $g \in \mathbf{K}[X,Y]$ unitaire en Y, $h \in \mathbf{K}[X,Y,Z]$ unitaire en Z. Une telle algèbre est dite *triangulaire*, c'est un $\mathbf{K}$-espace vectoriel de dimension finie égale au produit $\deg_X(f)\cdot\deg_Y(g)\cdot\deg_Z(h)$ dans lequel les calculs sont explicites.

Supposons qu'un obstacle se présente dans les calculs sous la forme d'un élément qui n'est ni nul ni inversible dans la $\mathbf{K}$-algèbre considérée $\mathbf{A}$. L'algèbre $\mathbf{A}$ est une $\mathbf{K}$-algèbre zéro-dimensionnelle : pour tout $\gamma \in \mathbf{A}$ on a un idempotent e_γ tel que γ est inversible dans $\mathbf{A}[1/e_\gamma]$ et nilpotent dans $\mathbf{A}/\langle e_\gamma\rangle$. On ouvre alors deux branches de calcul. Dans la première on ajoute l'équation $\gamma = 0$, et γ est nul dans la branche. Dans la seconde on ajoute l'équation $e_\gamma = 1$ et γ est inversible dans la branche.

De manière générale, à chaque étape du calcul, on sait construire un système fondamental d'idempotents orthogonaux tel que dans chacune des composantes $\mathbf{A}_i$ de $\mathbf{A}$, tout élément qui est intervenu au cours du calcul est ou bien nilpotent, ou bien inversible. En tuant les éléments nilpotents s'il en apparait dans les calculs, on remplace les $\mathbf{A}_i$ par des $\mathbf{K}$-algèbres quotients $\mathbf{B}_i$ dans lesquels les calculs sont plus simples. En outre chacune des $\mathbf{K}$-algèbres $\mathbf{B}_i$ est elle-même une algèbre triangulaire. C'est la partie la plus subtile de cette évaluation dynamique.

De cette manière, tous les calculs qui ont été réalisés avant l'apparition d'un obstacle restent valables dans toutes les composantes qui suivent. Ainsi on est capable de calculer dans $\mathbf{K}^{\mathrm{sep}}$ (ou dans $\mathbf{K}^{\mathrm{alg}}$) sans jamais qu'il soit nécessaire de construire l'objet en question comme une structure algébrique usuelle. Telle est la source de la méthode dynamique en mathématiques constructives, qui remonte à des travaux bien antérieurs à la parution de la méthode D5.

3 L'invention de la méthode dynamique par Paul Lorenzen

La méthode dynamique en algèbre est exposée pour la première fois (à notre connaissance) en 1951 par Paul Lorenzen, mathématicien et philosophe allemand, qui revisite sous forme dynamique un théorème abstrait qu'il avait démontré en 1939 concernant la structure de certains groupes ordonnés. Sous une certaine hypothèse, un tel groupe ordonné G peut être vu comme un sous-groupe d'un produit de groupes totalement ordonnés. La démonstration nécessitait l'utilisation du principe du tiers exclu et du lemme de Zorn pour construire ces groupes totalement ordonnés idéaux que l'on convoite.

3. Un corps est discret si l'on a un test de signe pour ses éléments.

4. En fait, la construction de tels objets ne peut pas en général être réalisée sans recours à un principe d'omniscience incompatible avec les mathématiques constructives.

Dans sa réécriture dynamique, Lorenzen utilise des approximations finies de ces groupes totalement ordonnés idéaux qui lui permettent de construire le groupe réticulé engendré par G, lequel est le substitut constructif de la famille (à priori infinie et purement idéale) des groupes totalement ordonnés en question.

Lorenzen utilise de la même manière un calcul arborescent qui est le substitut constructif d'un fameux théorème abstrait idéal de Krull qui affirme que la clôture intégrale d'un anneau intègre $\mathbf{Z}$ dans une extension $\mathbf{L}$ de son corps de fractions $\mathbf{K}$ est l'intersection des anneaux de valuation de $\mathbf{L}$ qui contiennent $\mathbf{Z}$.

4 Bibliographie commentée

On peut voir le livre (Bishop 1967, Foundations of Constructive Analysis, 1967) comme une gestion dynamique des objets fondamentaux de l'analyse via des approximations rationnelles de ces objets.

L'article D5 donne deux références «à paraitre» qui n'ont jamais été publiées. On peut cependant citer Duval (1987, D5 : Un système de calcul formel avec des nombres algébriques).

La méthode D5 a longtemps semblé d'une complexité trop élevée pour pouvoir être utilisée couramment en pratique, l'article van der Hoeven et Lecerf (2020, Directed Evaluation) a démontré récemment son efficacité en terme de complexité.

L'article Lenstra, Lenstra, et Lovász (1982, Factoring polynomials with rational coefficients) donne un algorithme en temps polynomial pour factoriser les polynômes de $\mathbb{Q}[X]$.

Les ouvrages Mines, Richman, et Ruitenburg (1988), Lombardi et Quitté (2021), Díaz-Toca, Lombardi, et Quitté (2014), Yengui (2015) et Coquand et Lombardi (2024) traitent des parties importantes de l'algèbre abstraite contemporaine dans un cadre entièrement constructif, algorithmique. Les 4 derniers utilisent la méthode dynamique.

L'article Coste, Lombardi, et Roy (2001, Dynamical method in algebra : effective Nullstellensätze) donne un exposé général de la méthode dynamique sous la forme des théories géométriques en logique. Il illustre l'efficacité de l'outil en question pour donner des formes effectives du Nullstellensatz de Hilbert et de variantes du Nullstellensatz en algèbre réelle et en algèbre valuée.

L'article (Lombardi et Quitté 2003, Constructions cachées en algèbre abstraite : Le principe local-global) utilise les idées de la méthode dynamique pour proposer une manière générale de décrypter constructivement les démonstrations en algèbre classiques basées sur la localisation en tout idéal premier.

L'article Coquand et Lombardi (2006, A logical approach to abstract algebra) traite de manière plus générale l'utilisation de la logique en algèbre constructive.

L'article Neuwirth (2021) donne un commentaire historique et philosophique des articles de Paul Lorenzen fondateurs (longtemps ignorés) de la méthode dynamique.

Les articles Coquand, Lombardi, et Neuwirth (2019, 2021) rendent compte dans un langage contemporain plus précis des articles de Lorenzen évoqués dans Neuwirth (2021).

Références

Errett Bishop : *Foundations of constructive analysis.* McGraw-Hill, New York, 1967. 1, 4

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. 4

Thierry COQUAND et Henri LOMBARDI : *Résolutions libres finies. Méthodes constructives.* Paris : Calvage & Mounet, 2024. ISBN 978-2-493230-13-3. 4

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. 4

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. 4

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. 4

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. 4

Dominique DUVAL : D5 : Un système de calcul formel avec des nombres algébriques. (D5 : A computer algebra system with algebraic numbers). Sémin. Théor. Nombres, Univ. Bordeaux I 1986-1987, Exp. No. 17, 7 p. (1987)., 1987. 4

A. K. LENSTRA, H. W. LENSTRA, Jr. et L. LOVÁSZ : Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982. 4

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. 4

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. 4

Ray MINES, Fred RICHMAN et Wim RUITENBURG : *A course in constructive algebra.* Universitext. Springer-Verlag, New York, 1988. URL https://pufc.univ-fcomte.fr/media/catalog/product/m/r/mrr-francais-avec-couverture_1.pdf. Traduction française par Henri Lombardi, révisée par Stefan Neuwirth. *Un cours d'algèbre constructive.* Presses Universitaires de Franche-Comté. 2020. 4

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. 4

Joris van der HOEVEN et Grégoire LECERF : Directed evaluation. *J. Complexity*, 60:45, 2020. ISSN 0885-064X. URL https://hal.science/hal-01966428v2. Id/No 101498. 4

Ihsen YENGUI : *Constructive commutative algebra : projective modules over polynomial rings and dynamical Gröbner bases.* Lecture Notes in Mathematics, 2138. Springer, Cham, 2015. 4

Table des matières