Postface du traducteur

L'algèbre dans le style de Bishop : quelques points essentiels du livre *A course in constructive algebra*

Introduction

Le livre qui précède, que nous citerons sous la forme [CCA], est une mise à jour des bases de l'algèbre classique dans un style proche des mathématiques constructives à la Bishop. Les versions constructives des théorèmes classiques leur donnent une nouvelle saveur et sont beaucoup plus précises. D'une manière qui peut sembler à priori étonnante, les démonstrations sont souvent plus simples et plus élégantes que celles que l'on trouve dans les textes usuels en mathématiques classiques. Cela tient au fait que, n'ayant plus aucune baguette magique du style « principe du tiers exclu » à sa disposition, on est forcé d'aller plus au fond des choses, et de mieux comprendre les mathématiques. Les raccourcis apparents qu'autorisent les mathématiques classiques introduisent ainsi souvent des détours inutiles : il n'est pas toujours bon d'être très (trop ?) savant pour traiter les problèmes de nature élémentaire, ou difficiles.

1 La réception de l'ouvrage

Après la postface se trouve un chapitre final sur la réception de [CCA]. La lectrice y trouvera une liste bibliographique des travaux qui ont cité le livre depuis sa parution. Cette liste est conséquente, mais la réception de l'ouvrage par la communauté mathématique est plutôt décevante eu égard à son caractère profondément novateur.

La réception de l'ouvrage en France est encore plus confidentielle que celle du livre de Bishop [2]. Je n'ai pratiquement jamais rencontré un ou une mathématicienne française qui ait seulement entendu parler de l'existence de l'ouvrage.

On pourrait s'attendre à ce que la communauté du Calcul Formel soit un peu plus au fait puisque les théorèmes du livre ont tous un contenu calculatoire direct qui leur permet, en principe, d'être implémentés dans les logiciels de calcul formel usuel.

Il m'est arrivé de soumettre un article d'algèbre constructive à la section « Computer Algebra » du *Journal of Algebra*, section dont les recommandations aux auteurs indiquent explicitement l'intérêt de la revue pour les mathématiques constructives. Quelle ne fut pas ma surprise lorsque le rapporteur me demanda d'expliquer ce que signifiait « ou » en mathématiques constructives, car il était dérouté et ne comprenait pas certains arguments. L'article fut finalement rejeté de cette section du *Journal of Algebra*, apparemment par impossibilité de trouver un rapporteur compétent.

J'ai cependant découvert récemment l'article *A constructive approach to Freyd categories* de Sebastian Posur, `https://arxiv.org/abs/1712.03492v1`. J'extrais un morceau de la section 2, « Constructive category theory ». Cet article me semble opérer un tournant salutaire et espéré.

> To present our algorithmic approach to Freyd categories, we chose the language of constructive mathematics (see, e.g., [MRR88]). We did that for the following reasons : the language of constructive mathematics
>
> 1. reveals the algorithmic content of the theory of Freyd categories,
> 2. is perfectly suited for describing generic algorithms, i.e., constructions not depending on particular choices of data structures,
> 3. allows us to express our algorithmic ideas without choosing some particular model of computation (like Turing machines),
> 4. encompasses classical mathematics, i.e., all results stated in constructive mathematics are also valid classically,
> 5. does not differ very much from the classical language in our particular setup.
>
> In constructive mathematics the notions of data types and algorithms (or operations) are taken as primitives and every property must have an algorithmic interpretation. For example, given an additive category **A** we interpret the property
>
> **A** has kernels
>
> as follows : we have algorithms that compute for given

- $A, B \in \mathrm{Obj}_{\mathbf{A}}$, $\alpha \in \mathrm{Hom}_{\mathbf{A}}(A, B)$, an object $\ker(\alpha) \in \mathrm{Obj}_{\mathbf{A}}$ and a morphism

$$\mathrm{KernelEmbedding}(\alpha) \in \mathrm{Hom}_{\mathbf{A}}(\ker(\alpha), A)$$

for which $\mathrm{KernelEmbedding}(\alpha) \cdot \alpha = 0$,
- $A, B, T \in \mathrm{Obj}_{\mathbf{A}}$, $\alpha \in \mathrm{Hom}_{\mathbf{A}}(A, B)$, $\tau \in \mathrm{Hom}_{\mathbf{A}}(T, A)$ such that $\tau \cdot \alpha = 0$, a morphism $u \in \mathrm{Hom}_{\mathbf{A}}(T, \ker(\alpha))$ such that

$$u \cdot \mathrm{KernelEmbedding}(\alpha) = \tau,$$

where u is uniquely determined (up to $=$) by this property.

Another important example is given by *decidable equality*, where we interpret the property that for all objects $A, B \in \mathbf{A}$, we have

$$\forall \alpha, \beta \in \mathrm{Hom}_{\mathbf{A}}(A, B) : (\alpha = \beta) \vee (\alpha \neq \beta)$$

as follows : we are given an algorithm that decides or disproves equality of a given pair of morphisms...

On the other hand, we allow ourselves to work classically whenever we interpret Freyd categories in terms of finitely presented functors. The reason for this is pragmatic : we want to demonstrate the usefulness of having Freyd categories computationally available, and we believe that this can be done by interpreting Freyd categories in terms of other categories that classical mathematicians care about.

2 Une théorie des ensembles revisitée

Dans [CCA], les auteurs introduisent une philosophie des mathématiques qui diffère légèrement de celle de [2, Bishop, 1967]. Ce point de vue se trouve sans doute exprimé de manière plus directe dans les articles [9, 10] et dans le livre [3].

Tout d'abord, comme chez Bishop, le point de vue n'est pas celui d'une mathématique formalisée, mais celui d'une mathématique ouverte à des développements imprévisibles, et pour laquelle le seul critère de vérité est la conviction qu'emporte une démonstration. L'univers mathématique n'est donc pas préexistant, il est bien au contraire une construction proprement humaine, à l'usage de la communauté humaine.

Un point original est cependant le suivant. L'attitude générale dans [CCA] est de considérer que toutes les mathématiques, aussi bien classiques que constructives, explorent un même univers d'objets idéaux, mais avec des outils différents.

Les mathématiques constructives sont une généralisation des mathématiques classiques en ce qu'elles ne supposent ni le principe du tiers exclu ni l'axiome du choix, exactement comme la théorie des groupes est une généralisation de la théorie des groupes commutatifs en ce qu'elle ne suppose plus valide la règle de commutativité.

Commençons par un premier extrait de [CCA].

> Notre notion de ce qu'est un **ensemble** est une notion plutôt libérale.
>
> **Définition I.2.1.** Un ensemble S est défini lorsque nous décrivons comment construire ses éléments à partir d'objets qui peuvent avoir été déjà construits, ou peut-être pas, avant S lui-même, et lorsque nous expliquons ce que signifie pour deux éléments de S qu'ils sont égaux.
>
> À la suite de Bishop nous regardons la **relation d'égalité** sur un ensemble comme conventionnelle : quelque chose à préciser lorsque l'ensemble est défini, et qui est soumis à la seule contrainte d'être une relation d'équivalence.
>
> . . . . . .
>
> Une relation unaire P sur S définit un **sous-ensemble** $A = \{\, x \in S : P(x) \,\}$ de S : un élément de A est un élément de S qui satisfait la propriété P, et deux éléments de A sont égaux si, et seulement si, ils sont égaux comme éléments de S. Si A et B sont des sous-ensembles de S, et si chaque élément de A est un élément de B, nous disons que A est **contenu** dans B, et nous écrivons $A \subseteq B$. Deux sous-ensembles A et B d'un ensemble S sont **égaux** si $A \subseteq B$ et $B \subseteq A$; ceci est clairement une relation d'équivalence sur les sous-ensembles de S. Nous avons décrit comment construire un sous-ensemble de S, et ce que cela signifie d'être égaux pour deux sous-ensembles de S. Donc nous avons défini l'ensemble de tous les sous-ensembles, encore appelé l'**ensemble des parties** de S.

Les lecteurs de Bishop sont ici très étonnés. Les auteurs pensent en effet que la notion de « relation unaire sur un ensemble donné » est suffisamment claire pour que l'on puisse considérer l'ensemble de toutes ces relations unaires. C'est-à-dire considérer que l'on sait les construire, comme par exemple on sait construire un entier naturel, un nombre réel ou une fonction réelle. Or cela semble problématique car nul ne prétend connaitre un langage universel pour les mathématiques, dans lequel on pourrait codifier ces relations unaires. En particulier, si l'ensemble Ω des parties du singleton $\{0\}$ existe, cela signifie que les valeurs de vérité forment un ensemble et non pas une classe. La difficulté est que l'on semble faire ici comme si l'on savait d'avance comment on pourra reconnaitre ce que seront les valeurs de vérité possibles dans l'avenir.

En fait, il semble que chaque fois qu'un « ensemble des parties de . . . » est

implicite ou explicite dans le livre, c'est dans un cadre où n'interviennent pas *toutes* les parties, mais seulement certaines parties, qui peuvent être regroupées dans un ensemble au sens plus strict adopté par Bishop ; ou alors la quantification sur l'ensemble des parties n'est pas nécessaire à la clarté du texte [1].

J'illustre ceci par un théorème assez extraordinaire, à la démonstration incroyablement simple et élégante [2].

La décomposition obtenue dans le théorème V.2.3 est essentiellement unique sur n'importe quel anneau commutatif.

Théorème V.2.4. *Soient R un anneau commutatif, $m \leqslant n$ des entiers > 0, et $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ et $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_n$ des idéaux de R. Supposons qu'un R-module M soit isomorphe à $\bigoplus_{i=1}^{m} R/I_i$ et à $\bigoplus_{j=1}^{n} R/J_j$. Alors*

(a) $J_1 = J_2 = \cdots = J_{n-m} = R$.

(b) $I_i = J_{n-m+i}$ pour $i = 1, \ldots, m$.

Ici, on ne fait aucune hypothèse sur les idéaux I_i et J_j. D'un point de vue d'une formalisation du discours, il semble donc qu'il faudrait quantifier sur l'ensemble de tous les idéaux de l'anneau R, ensemble tout aussi problématique que l'ensemble des parties de R. Mais on voit bien que c'est uniquement dans le cadre d'une formalisation mal maitrisée du discours que la nécessité de « l'ensemble des idéaux de R » se fait sentir. Pareillement, on n'a pas besoin de quantifier sur la classe des anneaux commutatifs lorsque l'on écrit : « Soit R un anneau commutatif ». Voir à ce sujet l'article [7, Dependent sums and dependent products in Bishop's set theory] de Iosif Petrakis pour un système formel utilisant la quantification sur des classes.

Signalons cependant le passage suivant qui traite de la catégorie des ensembles, et où l'ensemble Ω des parties de $\{0\}$ joue bien un rôle crucial. Notons que le joli théorème démontré ici ne semble pas avoir d'autre utilité qu'esthétique, dans le cadre de la théorie des catégories. Voir [18] pour une analyse de ce théorème dans le cadre de la théorie des types de Martin-Löf.

[...] La propriété catégorique qui correspond au fait qu'une fonction f est injective est la suivante : si g et h sont des flèches depuis n'importe quel

1. L'exception la plus importante se trouve dans la définition des ensembles bien fondés et des ordinaux, voir plus loin page 361.

2. On ne trouve pas ce théorème dans les grands traités d'algèbre en mathématiques classiques actuels. Par exemple Bourbaki (*Algèbre*, Chapitre VII, paragraphe 4, section 1), qui est un des meilleurs pour ce problème, ne donne le théorème que pour le cas où $m = n$, $I_1 \neq R$ et $J_1 \neq R$. Et la démonstration est moins belle que celle de [CCA].

ensemble C vers A et si $fg = fh$, alors $g = h$; c'est-à-dire f est **simplifiable à gauche** (on dit aussi **régulier à gauche**). Le fait qu'une fonction f est injective si, et seulement si, elle est simplifiable à gauche, est une démonstration purement routinière.

Une fonction f de A vers B est surjective si pour chaque $b \in B$ il existe un $a \in A$ tel que $f(a) = b$. La propriété catégorique correspondante est que f est **simplifiable à droite**, c'est-à-dire que si g et h sont des flèches de B vers n'importe quel ensemble C et si $gf = hf$, alors $g = h$. Le fait qu'une fonction f est surjective si, et seulement si, elle est simplifiable à droite, est une démonstration moins routinière que la démonstration du résultat correspondant pour les flèches simplifiables à la gauche.

Théorème I.4.1. *Une fonction est simplifiable à droite dans la catégorie des ensembles si, et seulement si, elle est surjective.*

Démonstration. Supposons que $f\colon A \to B$ est surjective et que $gf = hf$. Pour tout $b \in B$ il existe un $a \in A$ tel que $f(a) = b$. Donc $g(b) = g(f(a)) = h(f(a)) = h(b)$, et $g = h$. Réciproquement supposons que $f\colon A \to B$ est simplifiable à droite, et soit Ω l'ensemble des sous-ensembles de $\{0\}$. Définissons $g\colon B \to \Omega$ par $g(b) = \{0\}$ pour tout b, et définissons $h\colon B \to \Omega$ par

$$h(b) = \{\, x \in \{0\} : b = f(a) \text{ pour un } a \,\}.$$

Donc $h(b)$ est le sous-ensemble de $\{0\}$ tel que $0 \in h(b)$ si, et seulement si, il existe un a tel que $b = f(a)$. Clairement $gf = hf$ est la fonction qui fait correspondre à tout élément de A le sous-ensemble $\{0\}$. Donc $g = h$, et par suite $0 \in h(b)$, ce qui signifie que $b = f(a)$ pour un a. □

En fait, un trait original de [CCA] est la considération d'une notion de catégories en tant qu'objets mathématiques à part entière et non comme une simple « manière de parler » :

Nous travaillons avec deux types de collections d'objets mathématiques, les ensembles et les catégories.

. . . . . .

Étant donnés deux groupes, ou deux ensembles, il est en général incorrect de demander s'ils sont égaux ; la question pertinente est de savoir s'ils sont ou ne sont pas isomorphes, ou plus généralement quels sont les morphismes entre eux.

Une **catégorie** est une collection d'objets (comme l'est un ensemble).

Une relation d'égalité sur un ensemble construit, pour deux objets a et b de cet ensemble, une *proposition* « $a = b$ ». Pour spécifier une catégorie $\mathcal{C}$, nous devons montrer comment construire, pour deux objets A et B de $\mathcal{C}$, un *ensemble* $\mathcal{C}(A, B)$.

Un intérêt primordial des catégories est de permettre de généraliser la notion de famille d'objets (indexée par un ensemble). Pour la catégorie des ensembles, Bishop ne considère dans [2] que des familles de sous-ensembles d'un même ensemble. Mais dans les mathématiques usuelles, et particulièrement en algèbre, on a parfois besoin d'une notion plus générale, qui correspond à la notion de types dépendants en théorie constructive des types.

En utilisant la notion de foncteur nous pouvons étendre notre définition d'une famille d'éléments dans un ensemble à celle d'une famille d'objets dans une catégorie $\mathcal{C}$. Soit I un ensemble. Une **famille A d'objets de $\mathcal{C}$ indexée par I** est un foncteur depuis I, vu comme une catégorie, vers la catégorie $\mathcal{C}$. Nous notons souvent une telle famille par $\{A_i\}_{i\in I}$. Si $i = j$, la flèche de A_i vers A_j est notée A^i_j, et c'est un isomorphisme.

Avec cela comme outil, il est possible de construire certains objets cruciaux, comme

— les limites et colimites (en particulier les produits et les sommes directes de familles) dans certaines catégories,
— certaines structures algébriques librement engendrées par un ensemble S qui n'est pas nécessairement discret,
— de nombreuses opérations usuelles en mathématiques classiques sur les ordinaux (voir la définition des ordinaux dans [CCA] plus loin).

Par exemple on démontre qu'un module librement engendré par un ensemble S est plat ; mais il n'est pas nécessairement projectif (exercice IV.4.9). Le théorème classique selon lequel tout module est quotient d'un module libre reste valable ; la conséquence efficace n'est pas qu'il est quotient d'un module projectif, mais plutôt quotient d'un module plat. Ainsi, en forçant les ensembles à être discrets (selon le principe du tiers exclu), les mathématiques classiques simplifient à outrance la notion de module libre et aboutissent à des conclusions impossibles à satisfaire de manière algorithmique.

Une notion naturelle d'ordinal [1] est également introduite dans le chapitre I de [CCA], et elle est utilisée dans les problèmes de classification des groupes abéliens (au chapitre XI).

1. Cette notion est différente de celle que l'on peut trouver chez Brouwer ou Martin-Löf. Voir aussi [4, A constructive theory of ordinals].

Remarquons que la notion d'ensemble bien fondé définie ci-dessous utilise la quantification sur toutes les parties de W.

Soit W un ensemble muni d'une relation $a < b$. Un sous-ensemble S de W est dit **héréditaire** si $w \in S$ chaque fois que $w' \in S$ pour tout $w' < w$. L'ensemble W, ou la relation $a < b$, est dite **bien fondée** si tout sous-ensemble héréditaire de W est égal à W. Un ensemble ordonné discret est dit bien fondé si la relation $a < b$ (i.e. $a \leqslant b$ et $a \neq b$) est bien fondée. Un **ordinal**, ou **ensemble bien ordonné**, est un ensemble totalement ordonné discret et bien fondé.

Les ensembles bien ordonnés fournissent l'environnement pour les arguments par induction généraux.

. . . . . .

Pour des ordinaux λ et μ on définit un **plongement** de λ dans μ comme une fonction ρ de λ vers μ telle que si $a < b$ alors $\rho a < \rho b$, et si $c < \rho b$, alors on a un $a \in \lambda$ tel que $\rho a = c$. [. . .]

Théorème I.6.5. *Si λ et μ sont des ordinaux et si ρ et σ sont des plongements de λ dans μ, alors $\rho = \sigma$.*

. . . . . .

Lorsque l'on a un plongement de l'ordinal λ dans l'ordinal μ, nous écrivons $\lambda \leqslant \mu$. Clairement, une composition de plongements est un plongement, donc cette relation est transitive. Le théorème 6.5 implique que si $\lambda \leqslant \mu$ et $\mu \leqslant \lambda$, alors λ et μ sont isomorphes, i.e. il y a une bijection de λ vers μ qui préserve et réfléchit l'ordre. Il est naturel de dire que deux ordinaux isomorphes sont **égaux**. [. . .]

On se retrouve ainsi dans un cadre voisin de la théorie constructive des types dépendants, où tous les types sont créés par des définitions inductives généralisées.

Dans les sections suivantes, nous donnons quelques exemples significatifs de théorèmes classiques auxquels la reformulation constructive apporte un éclairage nouveau et des renseignements supplémentaires précis.

Nous indiquons aussi quelques exemples de théorèmes triviaux en mathématiques classiques et pourtant très importants du point de vue algorithmique.

3 L'exemple des anneaux principaux et des modules de type fini sur ces anneaux

Un anneau principal est en mathématiques classiques un anneau intègre dans lequel tout idéal est de type fini. D'un point de vue constructif, même le corps à deux éléments ne satisfait pas cette définition : on considère l'idéal engendré par une suite binaire ; fournir un générateur de cet idéal revient à décider si la suite est identiquement nulle, ce qui est LPO (voir page 4).

Une définition algorithmiquement pertinente, et classiquement équivalente à la définition classique, est celle d'un anneau de Bézout intègre discret qui satisfait une condition de noethérianité convenablement formulée.

Un **monoïde à pgcd** est un monoïde commutatif régulier dans lequel toute paire d'éléments possède un plus grand commun diviseur. Un **anneau intègre à pgcd** est un anneau intègre discret dont les éléments non nuls forment un monoïde à pgcd.

. . . . . .

Un **idéal principal** d'un monoïde commutatif M est un sous-ensemble I de M tel que $I = Ma = \{\, ma : m \in M \,\}$ pour un $a \in M$. Nous disons que le monoïde M **satisfait la condition de chaine des diviseurs** si pour chaque chaine ascendante $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ d'idéaux principaux, il y a un n tel que $I_n = I_{n+1}$.

On dit qu'un anneau intègre discret satisfait la condition de chaine des diviseurs si le monoïde des éléments non nuls la satisfait.

Définition IV.2.7. Un **anneau de Bézout intègre**, ou **domaine de Bézout** est un anneau intègre discret tel que pour tous éléments a, b on a deux éléments s, t tels que $sa + tb$ divise a et b. Un **anneau principal** est un domaine de Bézout qui satisfait la condition de chaine des diviseurs.

Le théorème de structure classique dit qu'un module de type fini sur un anneau principal est la somme directe d'un sous-module libre de rang fini et du sous-module de torsion, lui même égal à une somme directe de modules $R/(a_i)$ avec les a_i non nuls mis dans un ordre où chaque a_i divise le suivant.

La forme algorithmique la plus pure de ce théorème est le théorème de réduction d'une matrice en forme normale de Smith.

Une matrice $A = (a_{ij})$ est en **forme normale de Smith** si elle est diagonale et si $a_{ii} | a_{i+1,i+1}$ pour tout i.

Théorème V.1.2. *Toute matrice sur un anneau principal est équivalente à une matrice en forme normale de Smith.*

Théorème V.1.4. *Deux matrices en forme normale de Smith sur un anneau intègre à pgcd sont équivalentes si, et seulement si, les éléments diagonaux correspondants sont associés.*

Le théorème de structure pour les modules de présentation finie est une conséquence directe du théorème V.1.2.

Théorème V.2.3 (théorème de structure)**.** *Soit M un module de présentation finie sur un anneau principal R. Alors il existe des idéaux principaux $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ tels que M est isomorphe à la somme directe $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$.*

Puisque l'anneau est discret par définition, on peut séparer la somme en deux morceaux : le début, pour les indices de 1 à k disons, est alors le sous-module de torsion, avec $I_k = (a_k) \neq 0$, et le deuxième morceau, pour les $j > k$ avec les a_j nuls, est un module libre de rang $n - k$. Par contre, pour savoir quels I_j (pour les premiers indices j) sont égaux à R (et donc pourraient être supprimés sans dommage), il faut disposer d'un test pour l'inversibilité d'un élément, ce qui est la même chose ici que disposer d'un test de divisibilité entre deux éléments.

En mathématiques classiques, le théorème V.2.3 est énoncé pour les modules de type fini. D'un point de vue classique, les modules de type fini sur un anneau principal sont de présentation finie, tandis que d'un point de vue constructif il est clairement impossible d'avoir un algorithme pour réaliser cette implication, même dans le cas simple d'un $\mathbb{Z}$-module $\mathbb{Z}/I$ avec I de type dénombrable (par exemple engendré par une suite binaire).

La manière dont Bourbaki (*Algèbre*, chapitre VII) traite ces théorèmes mérite la comparaison. Le théorème de structure est donné avant le théorème de réduction de Smith pour les matrices. Et les démonstrations, qui utilisent trop le principe du tiers exclu, échouent à produire des algorithmes pour expliciter les théorèmes.

4 Les problèmes de factorisation

Le théorème IV.4.7(i) ci-après est usuellement démontré pour les anneaux factoriels, mais la condition noethérienne sous-jacente est en fait inutile.

Théorème IV.4.7. *Soit R un anneau intègre discret.*
(i) *Si R est un anneau à pgcd, alors il en va de même pour $R[X]$.*

On invite le lecteur à apprécier l'élégance de la démonstration que l'on trouve dans [CCA].

Le théorème classique de décomposition en facteurs premiers dans un monoïde à pgcd qui satisfait la condition de chaine des diviseurs est inaccessible d'un point de vue algorithmique. Il est remplacé en mathématiques constructives par un théorème un peu plus subtil qui rend en pratique les mêmes services que le théorème classique.

Théorème IV.1.8 (factorisation partielle)**.** *Soient $x_1, \ldots, x_k$ des éléments d'un monoïde à pgcd M qui satisfait la condition de chaine des diviseurs. Alors on peut construire une famille P d'éléments de M deux à deux premiers entre eux telle que chaque x_i est associé à un produit d'éléments de P.*

Soit M un monoïde régulier. Un élément $a \in M$ est dit **borné par l'entier naturel** n si chaque fois que $a = a_0 \cdots a_n$ avec des $a_i \in M$, alors l'un des a_i est inversible. Un élément de M est **borné** s'il est borné par un entier naturel ; le monoïde M est **à décomposition bornée** si tous ses éléments sont bornés. Un anneau intègre discret est **à factorisation bornée** si ses éléments non nuls forment un monoïde à décomposition bornée.

Un anneau intègre à pgcd qui satisfait la condition de chaine des diviseurs est appelé un **quasi-AFU**, où AFU est un acronyme pour « anneau à factorisation unique (en facteurs premiers) ».

Les anneaux quasi-AFU et les anneaux à pgcd à factorisation bornée sont deux versions constructives non équivalentes (constructivement) de la notion classique d'anneau factoriel. En fait, on trouve dans [CCA] encore trois autres versions constructives de cette notion classique.

Définition IV.2.1. Un anneau intègre discret R est appelé un **anneau à factorisation unique**, ou un **AFU**, si tout élément r non nul de l'anneau est inversible ou admet une factorisation essentiellement unique en produit d'éléments irréductibles, i.e. si $r = p_1 \cdots p_m$ et $r = q_1 \cdots q_n$ sont deux factorisations de r en produit d'éléments irréductibles, alors $m = n$ et on

peut réindexer les facteurs de façon à ce que $p_i \sim q_i$ pour chaque i. Nous disons que R est **factoriel** si $R[X]$ est un anneau à factorisation unique.

Un corps discret k est dit **pleinement factoriel** si tout corps extension de dimension finie de k est factoriel.

Les cinq versions constructives sont en mathématiques classiques équivalentes à la notion classique, mais elles introduisent des distinctions pertinentes du point de vue algorithmique, totalement invisibles en mathématiques classiques, par la faute de l'utilisation du principe du tiers exclu, qui écrase ces distinctions pertinentes. Dans le théorème IV.4.7 les points (ii) (joint au point (i)) et (vi) (i.e. (i) et (v)) sont deux versions distinctes, inéquivalentes, d'un même théorème de mathématiques classiques sur les anneaux factoriels.

Théorème IV.4.7. *Soit R un anneau intègre discret.*

(i) *Si R est un anneau à pgcd, alors il en va de même pour $R[X]$.*

(ii) *Si R est à factorisation bornée, alors il en va de même pour $R[X]$.*

(iii) *Si R a ses unités détachables, alors il en va de même pour $R[X]$.*

(iv) *Si la divisibilité est décidable dans R, alors il en va de même pour $R[X]$.*

(v) *Si R satisfait la condition de chaine des diviseurs, alors il en va de même pour $R[X]$.*

(vi) *Si R est un quasi-AFU, alors il en va de même pour $R[X]$.*

Concernant les problèmes de factorisation des polynômes sur un corps discret, la situation algorithmique n'est pas décrite correctement par les mathématiques classiques. Par exemple, le problème de factorisation dans $k[X]$ n'est pas trivial, contrairement à ce qu'affirme le théorème des mathématiques classiques.

Le chapitre VII de [CCA] explore cette situation en grands détails.

Le théorème constructif de base sur ce sujet est donné dans le chapitre VI. Comme il arrive que la caractéristique d'un corps ou d'un anneau ne soit pas connue d'avance, mais puisse être révélée au cours d'une construction, certaines précautions sont nécessaires dans les énoncés, comme ci-dessous dans le point (i). Notez que si l'on découvre un nombre premier p non nul dans un anneau k, il est nécessairement unique (sauf si l'anneau est trivial).

Lorsque k est un corps discret, on laisse simplement tomber l'alternative « k contient un élément non nul non inversible » dans le théorème. Mais il arrive que dans [CCA] le théorème soit utilisé sous la forme précise donnée ici, par exemple dans le chapitre IX sur la structure des algèbres de dimension finie.

Théorème VI.6.3. *Soient k un anneau commutatif discret avec unités détachables, et S un ensemble fini de polynômes unitaires de $k[X]$. Alors, ou bien k contient un élément non nul non inversible, ou bien nous pouvons construire un ensemble fini T de polynômes unitaires de $k[X]$ tel que :*

(i) *tout élément de T est de la forme $f(X^q)$ avec f séparable et q égal à 1 ou à une puissance d'un nombre premier nul dans k,*

(ii) *les éléments de T sont deux à deux étrangers,*

(iii) *tout polynôme de S est un produit de polynômes de T.*

Lorsque k est un corps discret, on obtient ainsi, en partant d'une famille donnée de polynômes univariés, une famille de polynômes unitaires séparables deux à deux étrangers qui fournit une version plus précise du théorème général de factorisation partielle IV.1.8 (lequel s'applique aux anneaux intègres à pgcd qui satisfont la condition de chaine des diviseurs).

5 Les anneaux noethériens, les décompositions primaires et le théorème de l'idéal principal de Krull

Un R-module est dit **fortement discret** si tout sous-module de type fini est détachable. Il est dit **cohérent** si tout sous-module de type fini est de présentation finie. La notion d'anneau cohérent fortement discret est fondamentale du point de vue algorithmique en algèbre commutative, en particulier pour la raison suivante : sur un anneau cohérent fortement discret, les systèmes linéaires sont parfaitement compris et maitrisés [1].

Dans les traités usuels en mathématiques classiques, cette notion est rarement mise en avant parce que l'on préfère la notion d'anneau *noethérien*. En mathématiques classiques, tout anneau noethérien A est cohérent parce que tous les sous-modules de A^n sont de type fini, et tout module de type fini est cohérent pour la même raison. En outre, on a le théorème de Hilbert qui dit que *si A est noethérien, toute A-algèbre de présentation finie est également un anneau noethérien*, tandis que la même affirmation est en défaut si l'on remplace « noethérien » par « cohérent » (voir [17, Soublin, 1970]).

D'un point de vue algorithmique cependant, il semble impossible de trouver une formulation constructive satisfaisante de la noethérianité qui implique la cohérence. Et la cohérence est souvent la propriété la plus importante du point de vue algorithmique. Comme conséquence, la cohérence doit être ajoutée (d'un

1. Dans l'article de Posur cité précédemment, ces anneaux sont appelés « calculables ».

point de vue constructif) lorsque l'on utilise la notion d'anneau ou de module noethérien.

La définition adoptée pour **module noethérien** dans [CCA] est : module dans lequel toute suite croissante de sous-modules de type fini admet deux termes consécutifs égaux. Il s'agit d'une définition constructivement acceptable, équivalente en mathématiques classiques à la définition usuelle.

Le théorème classique disant que sur un anneau noethérien tout A-module de type fini est noethérien est avantageusement remplacé par les théorèmes constructifs suivants (voir dans [CCA] le corolaire III.2.6, le théorème III.2.7 et le corolaire III.2.8).

Sur un anneau cohérent (resp. cohérent fortement discret), tout A-module de présentation finie est cohérent (resp. cohérent fortement discret).

Sur un anneau cohérent noethérien (resp. cohérent noethérien fortement discret), tout A-module de présentation finie est cohérent noethérien (resp. cohérent noethérien fortement discret).

Deux résultats classiques importants sur les anneaux noethériens ont des démonstrations constructives dans le cadre fixé par [CCA].

Théorème VIII.2.7 (Artin-Rees)**.** *Soit I un idéal de type fini d'un anneau commutatif cohérent noethérien R. Soit N un sous-module de type fini d'un R-module de présentation finie M. Alors il existe un entier k tel que pour tout $n \geqslant k$ on a*

$$I^{n-k}(I^k M \cap N) = I^n M \cap N.$$

Théorème VIII.2.8 (théorème d'intersection de Krull)**.** *Soient M un module de présentation finie sur un anneau commutatif cohérent noethérien R et I un idéal de type fini de R. Notons $A = \bigcap_n I^n M$. Alors $a \in Ia$ pour tout $a \in A$, et donc $IA = A$.*

Le théorème de la base de Hilbert

Quels sont les anneaux cohérents R pour lesquels les anneaux $R[X_1, \ldots, X_n]$ sont également cohérents ? D'un point de vue constructif, on connait deux classes d'anneaux qui satisfont cette propriété : les anneaux cohérents noethériens (voir ci-après) et les domaines de Prüfer (voir [19, Yengui, 2015, Chapter 4]).

Le théorème de la base de Hilbert pour la définition de noethérianité donnée dans [CCA] est le suivant. Les démonstrations remontent à 1974 ([8, Richman, 1974] et [13, Seidenberg, 1974], voir aussi [11, Seidenberg, 1971] et [12, Seidenberg,

1973] pour le cas des anneaux de polynômes sur un corps discret). Elles sont exposées de manière limpide dans [CCA].

Théorème VIII.1.5 (théorème de la base de Hilbert)**.** *Si R est un anneau cohérent noethérien (à gauche), alors il en va de même pour $R[X]$. Si en outre R est fortement discret (à gauche), alors il en va de même pour $R[X]$.*

Une version de ce théorème en calcul formel (voir [1, 1994, Théorème 4.2.8]) dit que pour un anneau cohérent noethérien fortement discret R, on peut donner un algorithme du type « base de Gröbner » pour calculer l'idéal de tête d'un idéal de type fini dans $R[\underline{X}] = R[X_1, \ldots, X_n]$ pour un ordre monomial donné. On en déduit assez facilement le théorème VIII.1.5. De la sorte, les deux théorèmes peuvent être considérés comme essentiellement équivalents.

Cependant, les algorithmes sous-jacents aux deux démonstrations sont assez différents. On doit aussi remarquer d'une part que les auteurs de 1994 semblent ignorer que le problème a été essentiellement résolu en 1974, et d'autre part que les algorithmes dans [1] ne sont pas certifiés de manière constructive (en particulier, en se basant sur la démonstration classique, aucune borne ne peut être calculée pour le nombre d'étapes de l'algorithme en fonction des données).

Le théorème de décomposition primaire

L'exposé de [CCA] sur le cadre constructif convenable pour les décompositions primaires est fondé sur les travaux de Seidenberg [14, 1978] et [15, 1984]. Il s'agit dans [CCA] d'une réélaboration de ce travail, de manière simplifiée et synthétique.

Soit R un anneau commutatif. Un idéal Q de R est dit **primaire** si $xy \in Q$ implique $x \in Q$ ou $y^n \in Q$ pour un n. On voit alors que $\sqrt{Q}$ est un idéal premier P.

Voici maintenant une légère variation par rapport à la terminologie classique, sans réelle importance dans le cas noethérien : les idéaux concernés sont tous de type fini [1].

Une **décomposition primaire** d'un idéal I d'un anneau commutatif est une famille finie d'idéaux primaires de type fini $Q_1, \ldots, Q_n$ telle que $I = \bigcap_i Q_i$ avec les $\sqrt{Q_i}$ de type fini. On dit aussi dans ce cas que l'idéal I est **décomposable**. En mathématiques classiques, tout idéal d'un anneau noethérien admet une décomposition primaire.

Dans le cadre constructif, pour un anneau cohérent noethérien fortement discret, que doit-on ajouter comme hypothèses constructivement acceptables pour avoir les décompositions primaires ?

1. Sauf I lui-même, mais dans le cadre des anneaux cohérents noethériens, I est nécessairement de type fini.

Voici une réponse possible, donnée dans [CCA].

> Un **anneau de Lasker-Noether** est un anneau commutatif cohérent noethérien fortement discret tel que le radical de tout idéal de type fini est l'intersection d'un nombre fini d'idéaux premiers de type fini.

Cette définition est constructivement acceptable parce que les anneaux $\mathbb{Z}$, $\mathbb{Q}[X]$, et $k[X]$ lorsque k est corps discret algébriquement clos, satisfont ces hypothèses de manière immédiate. De nombreux anneaux usuels, noethériens en mathématiques classiques, satisfont également ces hypothèses, comme expliqué plus loin.

En fait, on voit facilement que lorsque k est un corps discret, $k[X]$ est un anneau de Lasker-Noether si, et seulement si, le corps k est factoriel. Cette équivalence précise est impossible à énoncer en mathématiques classiques car tous les corps sont factoriels. On pourrait cependant énoncer un résultat analogue en se restreignant au cadre des algorithmes mécanisables à la Turing.

Les premières propriétés importantes des anneaux de Lasker-Noether sont résumées dans les trois théorèmes qui suivent. Le premier énoncé semble presque trop précis, par souci de généralité, voir le commentaire qui suit.

> **Théorème VIII.8.1.** *Soit S un sous-monoïde multiplicatif d'un anneau de Lasker-Noether R tel que $I \cap S$ est vide ou non vide pour tout idéal de type fini I de R. Alors $S^{-1}R$ est un anneau de Lasker-Noether.*

Si $S = R \setminus P$ pour un idéal premier P, la condition « $I \cap S$ est vide ou non vide » signifie « I est ou n'est pas contenu dans P ». Comme I est de type fini, le test est effectif si, et seulement si, P est détachable. Une conséquence du théorème VIII.8.1 est donc que pour tout idéal premier détachable, et en particulier pour tout idéal premier de type fini, le localisé R_P est un anneau de Lasker-Noether.

> **Théorème VIII.8.2.** *Soient R un anneau de Lasker-Noether et I un idéal de type fini de R. Alors R/I est un anneau de Lasker-Noether.*
>
> **Théorème VIII.8.5** (théorème de décomposition primaire)**.** *Soit R un anneau de Lasker-Noether. Alors tout idéal de type fini de R est décomposable.*

Le théorème de l'idéal principal de Krull

Une propriété plus élaborée des anneaux de Lasker-Noether est le fameux théorème de l'idéal principal de Krull, et le fait que tout idéal premier de type fini a une hauteur bien définie.

Théorème VIII.10.4 (théorème de l'idéal principal généralisé)**.** *Soient R un anneau de Lasker-Noether et $I = (a_1, \ldots, a_n)$. Alors tout idéal premier minimal au-dessus de I est de hauteur au plus n.*

Théorème VIII.10.5. *Soit P un idéal premier de type fini propre d'un anneau de Lasker-Noether R. Alors il existe un m tel que P est de hauteur m et est un idéal premier minimal au-dessus d'un idéal engendré par m éléments.*

Anneaux pleinement Lasker-Noether

Enfin, il faut répondre à la question : quelles hypothèses supplémentaires faut-il ajouter à la définition d'un anneau de Lasker-Noether R pour que les anneaux $R[X_1, \ldots, X_n]$ soient également de Lasker-Noether ? Voici une réponse donnée dans [CCA] :

On dit qu'un anneau R est **pleinement Lasker-Noether** si c'est un anneau de Lasker-Noether et si pour chaque idéal premier de type fini P de R, le corps de fractions de R/P est pleinement factoriel. Notez que l'anneau des entiers $\mathbb{Z}$ est pleinement Lasker-Noether, de même que tout corps pleinement factoriel.

Les trois théorèmes suivants (avec les théorèmes précédents sur les anneaux de Lasker-Noether) montrent alors que dans ce cadre (c'est-à-dire avec cette définition constructivement acceptable, équivalente en mathématiques classiques à la définition d'anneau noethérien), un très grand nombre de théorèmes classiques concernant les anneaux noethériens ont désormais une démonstration constructive et une signification claire. Cela semble un « miracle » de la même sorte que celui qu'a représenté la parution du livre de Bishop.

Théorème VIII.9.1. *Soit I un idéal de type fini d'un anneau pleinement Lasker-Noether R. Alors R/I est un anneau pleinement Lasker-Noether.*

Théorème VIII.9.2. *Si P est un idéal premier détachable d'un anneau pleinement Lasker-Noether R, le localisé R_P est un anneau pleinement*

Lasker-Noether.

Théorème VIII.9.6. *Si R est un anneau pleinement Lasker-Noether, il en va de même pour $R[X]$.*

Note. L'article [6, Perdry, 2004] définit une notion de noethérianité constructivement plus forte que celle de [CCA]. Les exemples usuels d'anneaux noethériens sont noethériens en ce sens. Avec cette notion, la définition d'un anneau de Lasker-Noether devient plus naturelle : c'est un anneau noethérien cohérent fortement discret qui possède un test de primalité pour les idéaux de type fini. L'article développe une théorie agréable des anneaux pleinement Lasker-Noether dans ce contexte.

Note. Le calcul de la décomposition primaire dans les anneaux de polynômes sur un corps discret ou sur $\mathbb{Z}$ est un sujet de recherche actif en Calcul Formel. L'article fondateur de Seidenberg est parfois cité, mais, à ma connaissance, le livre [CCA] ne l'est jamais.

6 Le théorème de structure de Wedderburn pour les k-algèbres de dimension finie

On parle ici de k-algèbres unitaires et associatives qui sont des k-espaces vectoriels de dimension finie sur un corps discret k. Autrement dit, ce sont des algèbres isomorphes à une sous-algèbre de type fini d'une algèbre de matrices $\mathrm{E}_k(k^n)$ (algèbre des k-endomorphismes de l'espace vectoriel k^n). On abrège la terminologie en parlant de « k-algèbre de dimension finie ».

Dans un anneau A non nécessairement commutatif, le **radical de Jacobson** de A est l'ensemble I des éléments x tels que $1 + xA \subseteq A^\times$. C'est un idéal (bilatère), et le quotient A/I a son radical de Jacobson nul.

Lorsque A est une k-algèbre de dimension finie, ce radical peut aussi être défini comme « radical nilpotent » : $\mathrm{rad}(A)$ est l'ensemble des éléments x tels que l'idéal (à gauche) xA est nilpotent, i.e. il existe un entier n tel que tout produit $xa_1 \cdots xa_n$ est nul.

Soit A une k-algèbre de dimension finie. On peut calculer une base du centre de A ainsi que le polynôme minimal sur k d'un élément arbitraire de A. On peut aussi calculer une base de l'idéal à gauche et une autre de l'idéal bilatère engendrés par une partie finie de A. Mais il peut être difficile de calculer une base du radical, et l'on ne peut pas affirmer en général que le radical est de dimension finie (sur k).

Néanmoins, on sait calculer des objets qui sont triviaux en mathématiques classiques (à condition qu'on ne cherche pas à les calculer !). Par exemple, comme

alternative au calcul du radical, on a le théorème suivant.

Théorème IX.3.3. *Soit A une k-algèbre de dimension finie et soit L un idéal (à gauche) de A de dimension finie. Alors, ou bien $L \cap \operatorname{rad} A \neq 0$, ou bien $A = L \oplus N$ pour un idéal (à gauche) N.*

Un module M est dit **réductible** s'il a un sous-module propre non nul ; sinon, il est dit **simple**.

Une k-algèbre est dite **simple** si tout idéal bilatère est trivial. Lorsque l'anneau est discret, comme dans le cas présent, la définition revient à dire que si un élément est non nul, l'idéal (bilatère) qu'il engendre contient 1.

La première partie du théorème de Wedderburn affirme qu'une k-algèbre de dimension finie de radical nul est un produit de k-algèbres simples. Voici la reformulation constructive que l'on trouve dans [CCA]. Un corps k est dit **séparablement factoriel** si les polynômes séparables dans $k[X]$ sont décomposables en facteurs premiers.

Nous caractérisons maintenant les corps séparablement factoriels en termes de décomposition d'algèbres en produit d'algèbres simples. Cela constitue la première partie du théorème de Wedderburn.

Théorème IX.4.3 (théorème de Wedderburn, première partie)**.** *Un corps discret k est séparablement factoriel si, et seulement si, toute k-algèbre de dimension finie de radical nul est un produit d'algèbres simples.*

Une précision concernant la capacité à calculer une base du radical est donnée dans le corolaire suivant.

Corolaire IX.4.5. *Un corps discret k est pleinement factoriel si, et seulement si, toute k-algèbre de dimension finie contient un idéal nilpotent de dimension finie I tel que A/I est un produit de k-algèbres simples.*

La seconde partie du **théorème de structure de Wedderburn** pour les algèbres semi-simples dit qu'une algèbre simple de dimension finie est isomorphe à un anneau total de matrices carrées sur une algèbre à division (un corps gauche).

La version constructive de ce théorème donnée dans [CCA] élucide d'une manière surprenante le contenu calculatoire de ce théorème classique.

Théorème IX.5.1 (théorème de structure de Wedderburn)**.**
Soit A une k-algèbre de dimension finie qui contient un idéal à gauche non trivial. L'une des propriétés suivantes est satisfaite.

(i) *Le radical de A est non nul.*

(ii) *A est un produit de k-algèbres de dimension finie (de dimensions plus petites que A).*

(iii) *Il existe un entier $n > 1$ tel que A est isomorphe à l'anneau des matrices carrées $n \times n$ sur une k-algèbre de dimension inférieure à celle de A.*

. . . . . .

Le problème fondamental et de savoir reconnaitre si une k-algèbre de dimension finie est une algèbre à division ou pas, à savoir, être capable d'affirmer que c'est une algèbre à division ou alors de construire un idéal à gauche non trivial. Si nous sommes capables de faire cela, alors le théorème 5.1 implique que toute k-algèbre de dimension finie a un radical de dimension finie, et que modulo ce radical elle est un produit d'anneaux de matrices carrées $n \times n$ sur des algèbres à division. Cette condition est équivalente à la capacité de reconnaitre si une représentation de dimension finie arbitraire d'une k-algèbre de dimension finie est réductible.

Théorème IX.5.2. *Les propriétés suivantes pour un corps discret k sont équivalentes.*

(i) *Toute k-algèbre de dimension finie est une algèbre à division ou sinon contient un idéal à gauche non trivial.*

(ii) *Tout k-module à gauche de dimension finie M sur une k-algèbre de dimension finie A est réductible ou irréductible.*

(iii) *Toute k-algèbre de dimension finie A a un radical de dimension finie, et $A/\operatorname{rad} A$ est un produit d'anneaux complets de matrices sur des algèbres à division.*

Et nous restons un peu sur notre faim avec ces interrogations à la fin du chapitre IX.

Pour quels corps k les conditions du théorème 5.2 sont-elles satisfaites ? Les corps finis et les corps algébriquement clos fournissent des exemples faciles. Le corps des nombres réels algébriques $\mathbb{R}^a$ admet seulement trois algèbres à division, et une démonstration constructive de cette assertion montre que ce corps satisfait les conditions du théorème 5.2.

Théorème IX.5.3. *Soient k un sous-corps discret du corps des nombres réels $\mathbb{R}$, algébriquement clos dans $\mathbb{R}$, $H = k(i, j)$ l'algèbre des quaternions sur k, et A une k-algèbre de dimension finie. Ou bien A contient un diviseur de zéro, ou bien A est isomorphe à l'une des algèbres k, $k(i)$, ou H.*

Est-ce que le corps $\mathbb{Q}$ des nombres rationnels satisfait les conditions du théorème 5.2 ? Nous n'allons certainement pas produire un contre-exemple brouwerien avec $k = \mathbb{Q}$. Une analyse détaillée de la théorie classique des algèbres à division sur $\mathbb{Q}$, en analogie avec le théorème 5.3, donnera probablement une démonstration.

7 Les domaines de Dedekind

Bien que la théorie algébrique des nombres est généralement ressentie comme essentiellement constructive dans sa forme classique, même les auteurs qui attachent une attention particulière aux aspects constructifs de la théorie emploient des techniques hautement non constructives qui annulent leurs efforts. Par exemple, dans l'ouvrage [Borevich et Shafarevich 1966], les auteurs supposent que tout polynôme peut être décomposé en un produit de facteurs irréductibles (tout corps est factoriel), et qu'étant donné un sous-ensemble non vide des entiers naturels, on peut trouver son plus petit élément.

La théorie constructive des domaines de Dedekind dans [CCA] permet de donner une version explicite des exposés classiques de théorie des nombres et de géométrie algébrique concernant les corps locaux, par exemple le livre de J.-P. Serre [16]. Elle donne aussi les hypothèses convenables pour rendre compte des résultats classiques de la théorie des anneaux de Dedekind telle qu'on la trouve par exemple dans Bourbaki.

Cela nécessite de donner des définitions suffisamment précises et contraignantes, en commençant par celles de la théorie des valeurs absolues.

Citons à titre d'exemple les définitions concernant les domaines de Dedekind.

Définition XIII.1.1. Un ensemble discret non vide S de valeurs absolues discrètes non triviales (voir page 292) sur un corps de Heyting k est appelé un **ensemble de Dedekind** lorsque les propriétés suivantes sont satisfaites.

(i) Pour tout $x \in k$, il existe un sous-ensemble fini T de S tel que $|x|_p \leqslant 1$ pour les $p \in S \setminus T$.

(ii) Si $|\ \ |_q$ et $|\ \ |_{q'}$ sont des valeurs absolues distinctes dans S, et si $\varepsilon > 0$, il existe un $x \in k$ tel que $|x|_p \leqslant 1$ pour toute $p \in S$, $|x-1|_q < \varepsilon$, et $|x|_{q'} < \varepsilon$. Par suite, des valeurs absolues distinctes dans S sont inéquivalentes.

Soit S un ensemble de Dedekind de valeurs absolues sur un corps de Heyting k. Si $p \in S$, alors, comme p est ultramétrique, l'ensemble $R(p) = \{\, x \in k : |x|_p \leqslant 1 \,\}$ est un anneau, qui est local parce que p est discrète. L'anneau $R(p)$ est appelé l'**anneau local en** p. Les éléments de l'anneau $\bigcap_{p\in S} R(p)$ sont appelés les éléments **entiers de** S. Un anneau est appelé un **domaine de Dedekind** si c'est l'anneau des entiers d'un ensemble de Dedekind de valeurs absolues sur un corps de Heyting.

Si le point fort est de rendre compte constructivement de l'essentiel des théorèmes classiques, un point faible est que par exemple un anneau principal intègre n'est un domaine de Dedekind que dans le cas où l'on dispose d'algorithmes de factorisation des idéaux principaux en produit d'idéaux premiers. On pourra comparer par exemple avec l'exposé dans l'ouvrage [5], avec une définition constructivement plus faible mais plus proche de la définition classique usuelle (voir la définition XII-7.7 et le théorème XII-7.9). Dans [5], les domaines de Dedekind admettent une factorisation partielle pour les ensembles finis d'idéaux de type fini, et les domaines de Dedekind à factorisation totale correspondent aux domaines de Dedekind de [CCA].

Références

[1] William W. Adams et Philippe Loustaunau : *An introduction to Gröbner bases.* American Mathematical Society, Providence, 1994.

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

[3] Douglas Bridges et Fred Richman : *Varieties of constructive mathematics.* London Mathematical Society Lecture Note Series, 97. Cambridge university press, Cambridge, 1987.

[4] Thierry Coquand, Henri Lombardi et Stefan Neuwirth : A constructive theory of ordinals. En préparation, `http://hlombardi.free.fr/ConstructiveOrdinals.pdf`, 2017.

[5] Henri Lombardi et Claude Quitté : *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices.* Calvage & Mounet, Paris, 2011. Traduction en anglais (version révisée et étendue par les auteurs) par Tania K. Roblot : *Commutative algebra : constructive methods. Finite projective modules.* Springer, Dordrecht, 2015.

[6] Hervé Perdry : Strongly Noetherian rings and constructive ideal theory. *J. Symbolic Comput.*, 37(4):511–535, 2004.

[7] Iosif Petrakis : Dependent sums and dependent products in Bishop's set theory. Rapport technique, Hausdorff Research Institute for Mathematics, 2018. `http://www.hcm.uni-bonn.de/fileadmin/him/Preprints/Types18.pdf`.

[8] Fred Richman : Constructive aspects of Noetherian rings. *Proc. Amer. Math. Soc.*, 44:436–441, 1974.

[9] Fred Richman : Confessions of a formalist, Platonist intuitionist. `http://math.fau.edu/Richman/html/Confess.htm`, 1994.

[10] Fred Richman : Interview with a constructive mathematician. *Modern Logic*, 6(3):247–271, 1996.

[11] A. Seidenberg : On the length of a Hilbert ascending chain. *Proc. Amer. Math. Soc.*, 29:443–450, 1971.

[12] A. Seidenberg : Constructive proof of Hilbert's theorem on ascending chains. *Trans. Amer. Math. Soc.*, 174:305–312, 1973.

[13] A. Seidenberg : What is Noetherian ? *Rend. Semin. Mat. Fis. Milano*, 44:55–61, 1975.

[14] A. Seidenberg : Constructions in a polynomial ring over the ring of integers. *Amer. J. Math.*, 100:685–706, 1978.

[15] A. Seidenberg : On the Lasker-Noether decomposition theorem. *Amer. J. Math.*, 106:611–638, 1984.

[16] Jean-Pierre Serre : *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, VIII.

[17] Jean-Pierre Soublin : Anneaux et modules cohérents. *J. Algebra*, 15:455–472, 1970.

[18] Olov Wilander : Setoids and universes. *Math. Structures Comput. Sci.*, 20(4): 563–576, 2010.

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