Journées Nationales de Calcul Formel

Rencontre organisée par :
Paola Boito, Alin Bostan, Adrien Poteaux et Mohab Safey el Din

2014

Henri Lombardi

Algèbre Constructive

Vol. 4, n° 1 (2014), Cours n° III, p. 1-48.

<http://ccirm.cedram.org/item?id=CCIRM_2014__4_1_A3_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Les cours du C.I.R.M.
Vol. **4** n° 1 (2014) 1-48
Cours n° III

Algèbre Constructive

Henri Lombardi

Préface

Dans ce tutoriel, on va essayer de convaincre l'auditoire que l'Algèbre abstraite contemporaine est pour l'essentiel constructive si l'on prend la peine de « bien lire » les démonstrations usuelles.

Lorsque l'on veut examiner le contenu concret d'un théorème d'algèbre et que l'on regarde sa démonstration en détail, si celle-ci ne se laisse pas traduire en un algorithme, on se heurte usuellement à deux obstacles :

– *l'utilisation du principe du tiers exclu*, qui permet de démontrer l'existence d'un objet concret au moyen d'une preuve par l'absurde : si l'objet n'existait pas, bla bla bla, on trouverait une contradiction dans les mathématiques,

– *l'utilisation du lemme de Zorn*, qui permet de mimer le raisonnement par récurrence même dans le cas où l'ensemble considéré n'est pas dénombrable.

Par exemple, le Moderne Algebra de van der Waerden évite le deuxième obstacle en ne considérant que des structures algébriques dénombrables.

En fait, utiliser le lemme de Zorn revient la plupart du temps à agiter les mains dans le vide pour détourner l'attention du véritable problème, lequel se trouve aux étages finis de la construction, et non dans le passage à la limite. Si ce dernier n'est pas vraiment possible, cela n'affecte en rien le contenu concret du théorème. En Calcul Formel, on ne passe jamais à la limite, car on s'intéresse au contenu concret des théorèmes, en outre les ordinateurs ne peuvent pas « passer à la limite » en un temps fini.

La pratique montre que le principal obstacle pour mettre à jour la véritable signification d'un théorème, provient de l'utilisation du principe du tiers exclu.

Or *le moyen de contourner l'obstacle du tiers exclu est fourni par une pratique courante en Calcul Formel, connue sous le nom de l'évaluation paresseuse.* Le paradigme est fourni par la méthode D5 qui permet de calculer dans la clôture algébrique d'un corps explicite, sans jamais se tromper, même si aucune clôture algébrique de ce corps ne peut être construite (au sens usuel de la chose). L'existence d'un diviseur irréductible pour un polynôme donné de K[X] (K un corps explicite), laquelle se prouve en mathématiques classiques au moyen du principe du tiers exclu, y est remplacée par un calcul paresseux arborescent et sans erreur possible.

Le plan des exposés est le suivant. Dans chaque section on montre comment se débrouiller constructivement avec des notions et des théorèmes d'apparence non constructive (au premier abord).

1) Théorème de la base adaptée. Noethérianité constructive.
2) Nullstellensatz sans clôture algébrique.
3) Dimension de Krull.
4) Idéaux premiers minimaux et maximaux.

Supports de présentation

On pourra consulter les diapositives résumant ce mini-cours :
`http://hlombardi.free.fr/publis/JNCF-LectSlides1-2.pdf`
`http://hlombardi.free.fr/publis/JNCF-LectSlides3-4.pdf`

Cours professé lors de la rencontre « Journées Nationales de Calcul Formel » organisée par Paola Boito, Alin Bostan, Adrien Poteaux et Mohab Safey el Din. 3-7 novembre 2014, C.I.R.M. (Luminy).

Références

Livres

[MRR] Mines R., Richman F., Ruitenburg W.
A Course in Constructive Algebra. Universitext. Springer-Verlag, (1988).

[ACMC] Lombardi H., Quitté C.
Algèbre Commutative, Méthodes Constructives. Calvage & Mounet, (2011).

[Modules] Díaz-Toca G.-M., Lombardi H., Quitté C.
Modules sur les anneaux commutatifs. Cours et exercices. Calvage & Mounet, (2014)

Articles

[Dynamic] Coste M., Lombardi H., Roy M.-F.
Dynamical method in algebra : Effective Nullstellensätze.
Annals of Pure and Applied Logic. **111**, (2001) 203–256.
`http://hlombardi.free.fr/publis/NullstellensatzDynamic.pdf`

[Logic] Coquand T., Lombardi H.
A logical approach to abstract algebra. (survey)
Math. Struct. in Comput. Science. **16** (2006), 885–900.
`http://hlombardi.free.fr/publis/AlgebraLogicCoqLom.pdf`

[Seminormal] Coquand T. On seminormality.
Journal of Algebra, **305** (1), (2006), 585–602.
`http://www.cse.chalmers.se/~coquand/min.pdf`

[Plaidoyer] Coquand T., Lombardi H.
Plaidoyer pour l'algèbre constructive.
`http://hlombardi.free.fr/publis/Plaidoyer.pdf`

H. Lombardi,
Novembre 2014.

Table des matières

CHAPITRE 1

Théorème de la base adaptée, cohérence, noethérianité

Sommaire

Introduction

Quant à moi, je proposerais de s'en tenir aux règles suivantes :
1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots ;
2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini ;
3. Éviter les classifications et les définitions non-prédicatives.

Henri Poincaré,
dans *La logique de l'infini* (Revue de Métaphysique et de Morale, 1909).
Réédité dans *Dernières pensées*, Flammarion.

Ce tutoriel illustre la citation ci-dessus. On notera comme le point 2 semble prémonitoire du Calcul Formel : l'infini n'existe pas sur les ordinateurs.

Mais toute l'algèbre contemporaine est-elle vraiment destinée à être digérable, au moins en principe, par des calculs finis ? C'est le pari des mathématiques constructives.

Le thème de la noethérianité est particulièrement important de ce point de vue car il est réputé nous ramener sans peine dans le royaume du fini : tous les idéaux d'un anneau noethérien ne sont-ils pas réputés de type fini ?

Il y a cependant une difficulté : que signifie exactement « tous les idéaux » dans la phrase précédente. Nous allons essayer d'éclaircir ce point. Pour cela, rien ne vaut mieux qu'un exemple non trivial mais suffisamment simple. Le théorème de la base adaptée pour les sous-groupes de $\mathbb{Z}^n$ nous fournit cet exemple.

1. Les théorèmes doivent avoir un contenu calculatoire

Un principe de base général du constructivisme est le suivant :
– *en mathématiques les théorèmes doivent avoir un contenu calculatoire.*

En particulier, lorsqu'un théorème affirme l'existence d'un objet mathématique sa preuve doit montrer comment construire cet objet. On ne peut pas se contenter d'une existence purement idéale de l'objet : la vérité en mathématiques doit avoir contenu calculatoire.

On dit cela parfois sous la forme du slogan suivant.

Affirmer, c'est prouver .

Récréation. Un premier mini contre exemple est donné par la plaisanterie suivante.
Question : Trouver deux nombres irrationnels a et b tels que a^b soit un nombre rationnel.

Réponse : Considérons les nombres réels $\alpha = \sqrt{3}$, $\beta = \sqrt{2}$ et $\gamma = \alpha^\beta$. Si γ est rationnel, prendre $a = \alpha$, $b = \beta$. Sinon prendre $a = \gamma$, $b = \beta$.

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

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

1.1. Théorème*. (Théorème de la base adaptée)[1]
Soit G un sous-groupe de $(\mathbb{Z}^n, +)$. Alors il existe une $\mathbb{Z}$-base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$, un entier $r \in [\![0..n]\!]$, et des entiers $a_1, \ldots, a_r > 0$ qui vérifient :
- *a_i divise a_{i+1} $(i \in [\![1..r]\!])$,*
- *$(a_1 e_1, \ldots, a_r e_r)$ est une $\mathbb{Z}$-base de G.*

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

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

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

2. Le théorème de la base adaptée pour un sous-groupe de type fini de $\mathbb{Z}^n$

Lorsque G est donné comme sous-groupe de type fini de $\mathbb{Z}^n$, le théorème de la base adaptée a un contenu extrêmement concret. En fait le théorème suivant donne des renseignements un peu plus précis que l'énoncé 1.1.

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

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

1. Dans ce tutoriel, l'étoile indique que le théorème n'a pas de démonstration constructive.

entier qui est le pgcd des coefficients de la matrice. Précisément on obtient :

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

où L_1 et C_1 sont produits de matrices élémentaires. Si $M_1 = 0$ le calcul est terminé, sinon il reste à recommencer en remplaçant M par M_1. On peut donc obtenir dans le théorème les matrices C et L comme produits de matrices élémentaires([2]). □

2.2. Corollaire. *Soit $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ une application $\mathbb{Z}$-linéaire (c'est-à-dire un homomorphisme de groupes).*

1. *Le théorème de la base adaptée s'applique à* $\operatorname{Ker}\varphi$ *et* $\operatorname{Im}\varphi$.
2. *On a $\mathbb{Z}^m = \operatorname{Ker}\varphi \oplus N$ avec un sous-$\mathbb{Z}$-module N libre.*

Une autre conséquence du théorème 2.1 est que *les systèmes d'équations linéaires avec coefficients et inconnues dans $\mathbb{Z}$ peuvent être résolus et discutés d'une manière simple et systématique.* Le « second membre » doit vérifier certaines équations et congruences. Quand ces conditions de compatibilité sont vérifiées, une solution particulière est facile à calculer, et la solution générale est obtenue en rajoutant une combinaison $\mathbb{Z}$-linéaire d'une famille finie explicite de vecteurs $\mathbb{Z}$-indépendants.

Kaplansky a étudié dans [21] quels sont les anneaux pour lesquels le théorème de réduction de Smith s'applique. Nous pouvons donner certains de ses résultats sous la forme suivante.

2.3. Définition.

1. Un anneau commutatif $\mathbf{A}$ est appelé un ***anneau de Bezout strict*** si pour tout $A = [\,a\ b\,] \in \mathbf{A}^{1\times 2}$ il existe une matrice inversible $C \in \mathbf{A}^{2\times 2}$ telle que $AC = [\,g\ 0\,]$.
2. Un anneau commutatif $\mathbf{A}$ est appelé un ***anneau de Smith*** si toute matrice admet une réduction de Smith.

Tout anneau de Smith est un anneau de Bezout strict. Tout anneau de Bezout intègre est un anneau de Bezout strict (exercice).

2.4. Proposition. *Un anneau $\mathbf{A}$ est de Smith si, et seulement si, c'est un anneau de Bezout strict et si toute matrice triangulaire $T \in \mathbf{A}^{2\times 2}$ admet une réduction de Smith. Si en outre l'anneau $\mathbf{A}$ est intègre les $d_{i,i}$ sont déterminés de manière unique, à des unités près, par M.*

On ignore toujours s'il existe des anneaux de Bezout stricts qui ne soient pas des anneaux de Smith.

On démontre cependant qu'un anneau de Bezout intègre de dimension 1 est un anneau de Smith [Modules, proposition XVI-2.5].

Voici une définition constructivement acceptable pour la dimension $\leqslant 1$.

2.5. Définition.

1. Un anneau est dit ***zéro-dimensionnel*** lorsqu'il vérifie l'axiome suivant :

$$\forall x \in \mathbf{A}\ \exists y \in \mathbf{A}\ \exists k \in \mathbb{N} \qquad x^k = yx^{k+1}. \tag{2.1}$$

2. Un anneau intègre $\mathbf{A}$ est dit ***de dimension*** $\leqslant 1$ si, pour tout élément $a \neq 0$, le quotient $\mathbf{A}/\langle a\rangle$ est zéro-dimensionnel.

2.6. Théorème. *Tout anneau de Bezout intègre de dimension $\leqslant 1$ est un anneau de Smith.*

Ce résultat peut être vu comme la généralisation de la méthode modulaire couramment utilisée pour calculer une réduction de Smith sur $\mathbb{Z}$ en évitant l'explosion de la taille des coefficients intermédiaires.

---

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

3. Intersections de sous-groupes de type fini Cohérence

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

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

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

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

Nous obtenons donc le résultat en appliquant le corollaire 2.2. □

La méthode précédente pour calculer une intersection convient dans des situations plus générales : la démonstration montre en effet qu'il suffit que le noyau de toute matrice soit un module de type fini pour que l'intersection de deux sous-modules de type fini d'un module libre soit toujours un module de type fini. Cela conduit à la notion d'anneau cohérent.

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

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

Ceci légitime la définition suivante.

3.4. Définition.

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

Il est clair que $\mathbb{Z}$ est un anneau cohérent. Aussi : un anneau est cohérent exactement si c'est un module cohérent sur lui-même.

Remarques.
1) Bien qu'implicites dans certaines démonstrations dès le XIX$^{\text{ème}}$ siècle, les anneaux cohérents n'ont été identifés et nommés que dans les années 1950.
2) La terminologie choisie ici pour « cohérent » est la terminologie anglaise usuelle. Bourbaki dit plutôt « module pseudo-cohérent », et réserve « module cohérent » pour les modules pseudo-cohérents de présentation finie. Cela a à voir avec les faisceaux algériques cohérents de J.-P. Serre et les faisceaux de modules cohérents (sur un schéma) de Grothendieck. Chez Bourbaki, les notions n'apparaissent qu'en exercice car Bourbaki ne considère comme intéressants, pour les considérations de finitude, que les anneaux noethériens, lesquels sont, du point de vue des mathématiques classiques, automatiquement cohérents. ■

Nous avons les résultats généraux suivants ([MRR] ou [Modules]).

3.5. Proposition. *Un $\mathbf{A}$-module M est cohérent si, et seulement si, il vérifie les deux propriétés suivantes :*

- *l'intersection de deux sous-module de type fini est de type fini.*
- *l'annulateur $(0 : a) = \{\, x \in \mathbf{A} \mid ax = 0 \,\}$ de tout élément $a \in M$ est de type fini.*

3.6. Lemme.

1. *Soit M un $\mathbf{A}$-module et soit N un sous-module de type fini de M. Les propriétés suivantes sont équivalentes.*
   a. *Le module M est cohérent.*

b. Les modules N et M/N sont cohérents.

2. Le produit d'un nombre fini de $\mathbf{A}$-modules cohérents est cohérent.

3.7. Théorème. *Si l'anneau $\mathbf{A}$ est cohérent, tout $\mathbf{A}$-module de présentation finie M est cohérent. Comme cas particulier, le noyau d'une matrice sur un anneau cohérent est un module de type fini.*

La signification la plus concrète de la dernière affirmation est que sur un anneau cohérent, *on a un certain contrôle des solutions des systèmes linéaires sans second membre* : elles sont obtenues comme combinaisons linéaires d'un nombre fini d'entre elles.

À ce titre on comprend bien que la notion d'anneau cohérent est une notion capitale en algèbre commutative explicite. Alors pourquoi cette notion n'apparaît-elle presque jamais dans les traités usuels ? C'est qu'en mathématiques classiques, on se restreint souvent au cas des anneaux noethériens et que ces anneaux sont cohérents. Mais ce dernier résultat n'est pas valide d'un point de vue calculatoire, comme nous allons l'expliquer dans la section suivante.

Remarque. Des exemples parmi les plus importants d'anneaux cohérents sont les anneaux de polynômes sur les corps, sur les anneaux de Bezout intègres et sur les anneaux noethériens cohérents. Mais, sauf pour le premier cas, une démonstration constructive de ces résultats n'est pas facile. ∎

4. Sous-groupes arbitraires, Noetherianité

Le théorème de la base adaptée peut être décomposé en deux parties.

- *Tout sous-groupe* de type fini *de $\mathbb{Z}^n$ admet une base adaptée (corollaire 2.2).*
- *Tout sous-groupe de $\mathbb{Z}^n$ est de type fini.*

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

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

N2 Toute suite croissante de sous-modules de M, $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \ldots$, est constante après un certain rang.

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

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

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

Les implications suivantes sont directes et constructives :

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

En mathématiques classiques, on voit facilement que N5 implique N1. Mais il faut utiliser pour cela le principe du tiers exclu.

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

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

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

Tout d'abord nous définissons $G_1 \subseteq \mathbb{Z}$ comme le sous-groupe engendré par les contre exemples à la Conjecture de Goldbach. Plus précisément, G_1 est donné comme engendré par une suite infinie (g_n) dans $\mathbb{Z}$: pour un $n \in \mathbb{N}$ nous testons si $2n+4$ est la somme de deux nombres premiers, si la réponse est oui, alors $g_n = 0$, si la réponse est non, alors $g_n = n$. Tant que nous ne disposons pas d'informations suffisamment précises sur la Conjecture de Goldbach, nous sommes incapables de savoir si $m \in G_1$, pour n'importe quel $m \neq 0$ dans $\mathbb{N}$. Ainsi le sous-groupe G_1 est un objet plutôt

étrange. Il est bien défini en ce sens qu'il est engendré par une suite infinie explicite, mais il n'est pas *détachable* : on n'a pas de test pour «$m \in G_1$?» A fortiori nous ne pouvons pas trouver un système fini de générateurs pour G_1.

Ensuite nous définissons $G_2 \subseteq \mathbb{Z}$ comme le sous-groupe engendré par «le premier contre exemple» à la Conjecture de Goldbach. Plus précisément, G_2 est donné comme engendré par la suite infinie (h_n) dans $\mathbb{Z}$, avec $h_m = 0$ sauf si g_m est le premier terme non nul de la suite (g_n). Dans ce cas $h_m := m$. Ici il est facile de voir que G_2 est un sous-groupe détachable. Mais donner explicitement un ensemble fini de générateurs pour G_2 revient à résoudre la Conjecture de Goldbach.

Une définition constructivement acceptable. La notion N4 est la bonne notion d'un point de vue constructif. Nous *définissons* la noethérianité d'un **A**-module M comme signifiant N4 :

4.1. Définition. *(Anneaux et modules noethériens)*
– (en mathématiques classiques) Un module est dit noethérien lorsqu'il vérifie les conditions équivalentes N1, . . . , N5.
– (en mathématiques constructives) Un module est dit ***noethérien*** lorsqu'il vérifie la condition N4.

Un anneau est noethérien s'il est noethérien en tant que module sur lui-même.

Remarque. Une définition constructivement acceptable de la noethérianité a attendu 1974 : [28, Richman] et [29, Seidenberg]. Dans ces articles, les auteurs ont donné la première démonstration constructive que la notion d'anneau noethérien cohérent est stable par extension polynomiale (c'est ***le théorème de la base***, ou encore théorème de Hilbert-Noether). ∎

Le module libre $\mathbb{Z}^k$ est un $\mathbb{Z}$-module noethérien au sens de N4. C'est une conséquence des résultats plus généraux suivants.

4.2. Lemme.

1. *Soit M un **A**-module cohérent et soit N un sous-module de type fini de M. Les propriétés suivantes sont équivalentes.*
   a. *Le module M est noethérien.*
   b. *Les modules N et M/N sont noethériens.*
2. *La somme directe d'un nombre fini de **A**-modules noethériens cohérents est un module noethérien cohérent.*

Démonstration. Le point *2* résulte facilement du point *1*, dans lequel seule l'implication *1b* $\Rightarrow$ *1a* est délicate.
Soit $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_k \subseteq \ldots$ une suite croissante de sous-modules de type fini de M. Puisque M est cohérent, les $Q_i = N \cap P_i$ forment une suite croissante de sous-modules de type fini de N, et puisque N est noethérien, il y a une suite extraite $Q_{m_1} \subseteq Q_{m_2} \subseteq \cdots \subseteq Q_{m_n} \subseteq \ldots$ avec $m_1 < m_2 < \cdots < m_n < \ldots$ telle que pour chaque j,

$$Q_{m_j} = Q_{1+m_j}.$$

Par ailleurs, les modules de type fini $R_i = P_i + N$ forment une suite croissante, et puisque M/N est noethérien, il existe un indice j tel que $R_{m_j} = R_{m_{j+1}}$, et a fortiori $R_{m_j} = R_{1+m_j}$. On a donc à la fois

$$P_{m_j} \cap N = P_{1+m_j} \cap N \quad \text{et} \quad P_{m_j} + N = P_{1+m_j} + N.$$

Vu les isomorphismes canoniques

$$P_{m_j}/Q_{m_j} = P_{m_j}/(P_{m_j} \cap N) \simeq (P_{m_j} + N)/N = R_{m_j}/N \quad \text{et}$$

$$P_{1+m_j}/Q_{1+m_j} = P_{1+m_j}/(P_{1+m_j} \cap N) \simeq (P_{1+m_j} + N)/N = R_{1+m_j}/N,$$

on obtient que $P_{1+m_j}/P_{m_j} \simeq R_{1+m_j}/R_{m_j} = 0$; i.e. $P_{1+m_j} = P_{m_j}$. □

4.3. Théorème. *Un module de présentation finie sur un anneau noethérien cohérent est un module noethérien cohérent.*

Démonstration. Résulte facilement des points *1* et *2* dans le lemme 4.2. □

Les anneaux principaux. Un ***anneau principal*** est un domaine de Bezout noethérien.

Avec la définition constructive de la noethérianité on démontre que l'algorithme de réduction de Smith sur $\mathbb{Z}$ fonctionne à peu près à l'identique sur n'importe quel anneau principal.

La terminaison de l'algorithme est assurée de manière explicite par la noethérianité prise dans le sens constructif.

On démontre aussi qu'un anneau principal est de dimension de Krull $\leqslant 1$, ce qui donne accès à la variante modulaire de l'algorithme de Smith. Ainsi, comme dans beaucoup de cas, la noethérianité est seulement une condition «un peu trop forte», donc pas réellement utile, pour des résultats essentiels qui lui semblent liés.

Un autre exemple est fourni par les ***domaines de Dedekind***, dont la plupart des propriétés «ayant une signification concrète» sont déjà partagées par les anneaux ***arithmétiques*** intègres de dimension $\leqslant 1$. La définition constructive d'un anneau arithmétique est la suivante, via une égalité qui ressemble à une identité de Bezout.

Pour tous a, $b \in \mathbf{A}$, il existe s, t, v et w tels que

$$sa = vb, \quad tb = wa, \quad s + t = 1. \tag{4.1}$$

Un exemple d'un quotient «non cohérent» de l'anneau $\mathbb{Z}$. On considère dans $\mathbb{Z}$ un idéal $\mathfrak{a}$ engendré par une suite infinie d'éléments, tous nuls sauf éventuellement un, qui est alors égal à 3 (par exemple, on met un 3 la première fois, si cela arrive, qu'un zéro de la fonction zéta de Riemann n'a pas sa partie réelle égale à 1/2). Si l'on est capable de donner un système fini de générateurs pour l'annulateur de 3 dans $\mathbb{Z}/\mathfrak{a}$, on est capable de dire si la suite infinie est identiquement nulle ou pas. Cela signifierait qu'il existe une méthode sûre pour résoudre les conjectures du type de celle de Riemann. Ainsi, bien que les anneaux du type $\mathbb{Z}/\mathfrak{a}$ soient évidemment noethériens au sens de N4, on n'a pas de démonstration constructive de leur cohérence. En tout état de cause, on est capable de produire une famille $(\mathfrak{a}_n)_{n\in\mathbb{N}}$ dénombrable tout à fait explicite pour laquelle la cohérence de $\mathbb{Z}/\mathfrak{a}_n$ ne peut faire l'objet d'aucun algorithme programmable sur machine : il n'y pas de réponse programmable à la question : trouver un système générateur fini de l'idéal de Ann(3).

Commentaire. Comme toute définition constructive raisonnable de la noethérianité semble réclamer qu'un quotient d'un anneau noethérien reste noethérien, et vu le «contre-exemple» précédent, on ne peut espérer avoir une démonstration constructive du théorème de mathématiques classiques qui affirme que tout anneau noethérien est cohérent. ∎

Conclusion

Remarquons que nous avons fait une analyse constructive assez détaillée du théorème de la base adaptée, mais que l'histoire n'est pas terminée.

En effet, chaque fois que ce théorème est utilisé en mathématiques classiques, nous avons à chercher un contenu constructif pour le résultat obtenu. Et il n'est pas sûr a priori que le théorème 2.1, le corollaire 2.2 et les théorèmes 3.1 et 4.3 donnent toujours la solution.

CHAPITRE 2

Nullstellensatz sans clôture algébrique

Sommaire

Introduction

Ce chapitre donne l'interprétation constructive de l'objet « clôture algébrique d'un corps » construit en mathématiques classiques.

Bien que l'objet correspondant des mathématiques constructives soit de nature dynamique et non statique (ce qu'il est en mathématiques classiques), il rend les mêmes services (de façon améliorée, car avec un contenu algorithmique précis) que l'objet des mathématiques classiques.

Nous ne traiterons ici[3] que les corps discrets, c'est-à-dire les corps dans lesquels on dispose d'un test à zéro.

Les corps discrets sont les anneaux commutatifs qui vérifient l'axiome

CDI : tout élément est nul ou inversible.

Le corps des réels ne vérifie pas cet axiome de manière explicite, car on ne dispose pas de test à zéro pour un réel générique, c'est-à-dire défini par une suite de Cauchy de rationnels[4].

En fait, nous sommes avant tout intéressés par la construction d'un corps contenant des zéros de polynômes successifs, car la clôture algébrique peut être vue comme une limite (ressemblant à une réunion croissante) de telles extensions finies. Et tout calcul dans la clôture algébrique se réalise à un étage fini de la construction. Le système D5 ne traite que des étages finis de la construction, mais il est largement suffisant pour interpréter constructivement n'importe quelle démonstration classique qui utilise la clôture algébrique pour aboutir à un résultat concret.

Soit $\mathbf{K}$ un corps discret et soit $f \in \mathbf{K}[X]$ un polynôme unitaire séparable. Supposons que l'on dispose d'un algorithme de factorisation des polynômes séparables de $\mathbf{K}[X]$ (on dit alors que $\mathbf{K}$ est un corps ***séparablement factoriel***). Alors on peut construire, par exemple en suivant Galois, le corps de racines de f et développer constructivement la théorie de Galois de cette extension ([ACMC, théorème III-6.15], [MRR, corollaire VII-2.4 et théorème VI-8.4]).

3. Pour des corps non discrets comme $\mathbb{R}(X,Y)$ ou $\mathbb{Q}_p(X,Y)$, les choses sont moins claires. De manière purement algébrique et constructive, on doit pouvoir construire une clôture séparable, mais ce n'est pas entièrement satisfaisant. Cela est à mettre en relation avec le fait que l'on connaît mal les axiomes purement algébriques vérifiés constructivement par $\mathbb{R}$ ou $\mathbb{Q}_p$.

4. La suite de Cauchy doit avoir une convergence bien contrôlée, par exemple $|x_n - x_{n+p}| < 2^{-n}$ pour tout n.

Malheureusement, un corps discret arbitraire n'est pas séparablement factoriel[5] et dans une clôture algébrique, on demande de factoriser tous les polynômes unitaires, pas uniquement les polynômes séparables.

Construire un corps de racines d'un polynôme arbitraire demande une certaine virtuosité, développée en détail dans les chapitres VI et VII de [MRR]. Cela n'est pas possible pour un corps discret arbitraire, et même dans les cas où c'est possible, cela peut s'avérer beaucoup trop cher en temps de calcul sur machine.

Une alternattive est apparue en Calcul Formel avec le système D5 [10, (1985)], dont la simplicité est proprement époustouflante. Au lieu de construire un objet rigide, fixé, statique, «clôture algébrique du corps discret $\mathbf{K}$», on limite son ambition à «calculer sans erreur dans la clôture algébrique du corps discret $\mathbf{K}$».

Dans le logiciel `Magma`, la clôture algébrique de $\mathbb{Q}$ est implémentée d'une façon directement inspirée de D5, tout en profitant de la possibilité de calculs «modulaires» pour $\mathbb{Q}$.

Dans ce chapitre, nous n'envisageons pas les questions d'efficacité, nous cherchons seulement à comprendre en termes constructifs un objet «un peu trop idéal» des mathématiques classiques : la clôture algébrique d'un corps discret arbitraire.

1. Algorithmes de factorisation

Nous rappelons maintenant des algorithmes classiques qui remplacent souvent avantageusement les algorithmes (inexistants) de décomposition d'un polynôme en facteurs premiers.

1.1. Proposition et définition. *On dispose d'un algorithme de factorisation partielle pour les familles finies de polynômes unitaires dans $\mathbf{K}[X]$: une **factorisation partielle** pour une famille finie $(f_1,\dots,f_r)$ est donnée par une famille finie $(g_1,\dots,g_s)$ de polynômes unitaires deux à deux étrangers et par l'écriture de chaque f_i sous la forme*

$$f_i = \prod_{k=1}^{s} g_k^{m_{k,i}} \ (m_{k,i} \in \mathbb{N}).$$

*La famille $(g_1,\dots,g_s)$ s'appelle alors une **base de factorisation partielle** pour la famille $(f_1,\dots,f_r)$.*

Démonstration. Si les f_i sont deux à deux étrangers, il n'y a rien à faire. Sinon, supposons par exemple que l'on ait

$$\operatorname{pgcd}(f_1,f_2)=h_0,\ f_1=h_0h_1 \text{ et } f_2=h_0h_2 \text{ avec } \deg(h_0)\geqslant 1.$$

On remplace la famille $(f_1,\dots,f_r)$ par la famille $(h_0,h_1,h_2,f_3,\dots,f_r)$. On note que la somme des degrés a diminué. On note aussi que l'on peut supprimer dans la liste les polynômes égaux à 1, ou les occurrences multiples d'un même polynôme (tous les polynômes sont unitaires).
L'algorithme procède par étapes. Il consiste à examiner si toutes les paires dans la liste fournie à l'étape précédente sont étrangères. Si ce n'est pas le cas, on fait subir à une paire non étrangère de la liste le traitement indiqué juste avant pour la paire (f_1,f_2). Comme la somme des degrés diminue à chaque étape, l'algorithme aboutit au résultat souhaité en un nombre fini de calculs. □

1.2. Proposition et définition. (Factorisation séparable)

1. *Si $\mathbf{K}$ est un corps parfait, on dispose d'un algorithme de **factorisation séparable** des listes de polynômes unitaires de $\mathbf{K}[X]$ au sens suivant.*
   Une factorisation séparable d'une famille $(f_1,\dots,f_r)$ est donnée par :
   - *une famille $(g_1,\dots,g_s)$ de polynômes séparables deux à deux étrangers ;*
   - *l'écriture de chaque f_i sous forme $f_i=\prod_{k=1}^{s} g_k^{m_{k,i}}$ $(m_{k,i}\in\mathbb{N})$.*
2. *L'algorithme fonctionne également sans supposer le corps parfait lorsque la caractéristique du corps est supérieure aux degrés de tous les polynômes f_i de la famille de départ.*

N.B. : sur un corps parfait, on parle indifféremment de factorisation séparable ou de ***factorisation sans carré***.

5. Par exemple, on construit des corps discrets dénombrables pour lesquels le sous-ensemble des carrés n'est pas testable par un algorithme du type Turing. Variation usuelle sur le thème d'impossibilité de tester la halte des algorithmes du type Turing par un algorithme du type Turing. Il en résulte que sur un tel corps ; il n'y a pas d'algorithme de factorisation pour les polynômes de la forme X^2-a.

Démonstration. 1. On commence par calculer une base de factorisation partielle $(g_1, \ldots, g_s)$ pour la famille $(f_i)_{i\in[\![1..r]\!]}$ (voir la proposition 1.1). Il suffit d'établir ensuite le résultat suivant.

Pour un polynôme unitaire $g \in \mathbf{K}[X]$ de degré $\geqslant 1$, on peut calculer une décomposition de g comme produit de polynômes séparables.

Ce résultat s'établit par récurrence sur le degré de g. Concernant le polynôme g, trois possibilités se présentent :

- ou bien $g' = 0$, on l'écrit sous forme $g = h(X^p) = h_1(X)^p$ et l'on applique l'hypothèse de récurrence avec le polynôme h_1 ;
- ou bien g est séparable (par exemple, s'il est de degré 1) ;
- ou bien le polynôme $h = \operatorname{pgcd}(g, g')$ est un diviseur strict, de degré $\geqslant 1$, de g ; on écrit $g = hq$, et l'on applique l'hypothèse de récurrence[6] à h et q.

2. L'algorithme fonctionne à l'identique si l'on traite une famille de polynômes de degrés inférieurs à la caractéristique du corps, à ceci près que l'on ne tombe jamais sur le cas d'un polynôme de dérivée nulle. □

2. Algèbres finies sur un corps discret

Le système D5 calcule dans des algèbres « triangulaires » du type

$$\mathbf{K}[X_1, \ldots, X_n]/\langle f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)\rangle$$

où chaque f_k est unitaire en la variable X_k. Ce sont des $\mathbf{K}$-espaces vectoriels qui possèdent des bases finies explicites.

Nous appelons ***algèbre strictement finie sur un corps discret*** $\mathbf{K}$ une $\mathbf{K}$-algèbre $\mathbf{A}$ dont on connait une base finie comme $\mathbf{K}$-espace vectoriel.

Une ***algèbre finie*** correspond à une notion plus lâche : on ne demande pas une $\mathbf{K}$-base finie de $\mathbf{A}$, on demande seulement que $\mathbf{A}$ soit un $\mathbf{K}$-espace vectoriel de type fini. Par exemple si $\mathbf{A}$ est strictement finie et si on ne connait pas de base du nilradical $\mathfrak{N} = \sqrt[\mathbf{A}]{0}$, alors l'algèbre réduite $\mathbf{A}/\mathfrak{N}$ est finie, mais pas nécessairement strictement finie.

Une algèbre finie sur un corps discret est un cas particulier d'***anneau zéro-dimensionnel***, c'est-à-dire un anneau qui vérifie l'axiome suivant :

$$\forall x \in \mathbf{A}\ \exists y \in \mathbf{A}\ \exists k \in \mathbb{N} \qquad x^k = yx^{k+1}. \tag{2.1}$$

2.1. Fait. *Dans un tel cas l'élément $e = (yx)^k$ est idempotent, $ex^k = x^k$, et $\langle e\rangle = \langle x^k\rangle$. Ainsi :*

- $\mathbf{A} \simeq \mathbf{A}/\langle 1-e\rangle \times \mathbf{A}/\langle e\rangle$;
- *dans $\mathbf{A}/\langle 1-e\rangle$, x est inversible ;*
- *dans $\mathbf{A}/\langle e\rangle$, x est nilpotent.*

Plus généralement on a le résultat suivant.

2.2. Fait. *Soient $(x_1, \ldots, x_n)$ une famille d'éléments dans un anneau zéro-dimensionnel $\mathbf{A}$.*

1. *Il existe un système fondamental d'idempotents orthogonaux $(e_1, \ldots, e_r)$ tel que dans chaque composante $\mathbf{A}/\langle 1-e_i\rangle$, chacun des x_j est nilpotent ou inversible.*
2. *Lorsque l'anneau est réduit, dans chaque composante chacun des x_j est nul ou inversible :*
   - *le morphisme naturel $\mathbf{A} \to \prod_{i=1}^r \mathbf{A}/\langle 1-e_i\rangle$ est un isomorphisme ;*
   - *un anneau zéro-dimensionnel réduit se comporte dans les calculs comme un produit fini de corps discrets.*

3. Clôture algébrique à la D5

On explique dans cette section comment le système D5 fonctionne.

Le calcul mis en place est un calcul arborescent, qui se développe au fur et à mesure que l'on désire utiliser des zéros de polynômes unitaires apparaissant dans les démonstrations que l'on met en œuvre.

À chaque feuille de l'arbre, le calcul se développe dans une $\mathbf{K}$-algèbre triangulaire comme si elle était un corps discret. Lorsque l'axiome CDI doit être appliqué, la réponse est le plus souvent sans ambigüité, mais il peut arriver que la branche soit réorganisée depuis un noeud en amont

6. On peut aussi calculer une base de factorisation partielle $(g_1, \ldots, g_k)$ pour (h, q) et appliquer l'hypothèse de récurrence à chacun des g_i.

de la feuille. La branche se transforme alors en un arbre aux feuilles duquel sont des $\mathbf{K}$-algèbres représentant le même système triangulaire, mais de manière plus précise : certains polynômes unitaires définissant l'algèbre on été décomposés en produit de polynômes deux à deux étrangers, en outre des nilpotents ont pu être tués (réduits à 0).

Au départ, on a un corps discret $\mathbf{K}$, pour lequel : on connaît 0, 1 et -1, on dispose des opérations $+$ et $\times$ de façon explicite, et l'axiome CDI est réalisé par un algorithme.

Rajouter un zéro d'un polynôme unitaire et calculer dans l'extension obtenue. On rajoute lorsque cela est nécessaire un zéro x_p d'un polynôme unitaire $p \in \mathbf{K}[X]$. Le calcul qui s'ensuit se passe désormais dans l'algèbre $\mathbf{K}[x_p] = \mathbf{K}[X]/\langle p\rangle$, du moins tant qu'il ne s'agit pas de mettre en œuvre l'axiome CDI. À un certain moment du calcul, il peut se produire que l'on ait besoin d'expliciter l'axiome CDI pour un élément $a = q(x_p)$ de $\mathbf{K}[x_p]$. On peut supposer que $\deg(q) < \deg(p)$.

Cas où p est séparable. On calcule $r = \operatorname{pgcd}(p, q)) = up + vq$ dans $\mathbf{K}[X]$ de sorte que $p = p_1p_2$, avec $p_1 = p/r$ et $p_2 = r$ qui sont des polynômes séparables étrangers. On a $q = q_1r$ avec q_1 et p_1 étrangers, et $up_1 + vq_1 = 1$

Trois cas peuvent se présenter.

1. $r = 1$, on a alors $av(x_p) = 1$ dans $\mathbf{K}[x_p]$, on a la réponse (a inversible), et l'on ne change rien à $\mathbf{K}[x_p]$;
2. $r = p$, donc $q = 0$, et $a = 0$ dans $\mathbf{K}[x_p]$, on a la réponse, et l'on ne change rien à $\mathbf{K}[x_p]$;
3. $0 < deg(r) < \deg(p)$. On a une relation de Bezout $sp_1 + tp_2 = 1$ dans $\mathbf{K}[X]$. En posant $e_1 = (sp_1)(x_p)$ et $e_2 = (tp_2)(x_p)$, on voit que e_1 et e_2 sont deux idempotents complémentaires, qui cassent l'algèbre $\mathbf{K}[x_p]$ en deux. Dans la branche où $e_1 = 0$, $\mathbf{K}[x_p]/\langle e_1(x_p)\rangle \simeq \mathbf{K}[X]/\langle p_1\rangle$, on a $p_1 = 0$, r et q_1 inversibles, donc a inversible, et dans l'autre, la branche $\mathbf{K}[x_p]/\langle e_2(x_p)\rangle \simeq \mathbf{K}[X]/\langle r\rangle$, on a $r = 0$ d'où $a = 0$.
   En conséquence, on ouvre deux branches de calcul pour l'avenir :
   – dans la première branche, a est inversible (son inverse est obtenu au moyen du calcul de $\operatorname{pgcd}(p_1, q) = 1$) et p est remplacé par p_1 ($\mathbf{K}[x_p]$ est remplacée par $\mathbf{K}[X]/\langle p_1\rangle$) ;
   – dans la seconde branche, a est nul et p est remplacée par p_2.

La réponse de l'algorithme dans le dernier cas est donc la suivante :

– Il y a deux possibilités (deux paquets de zéros bien identifés), et selon le zéro de p envisagé, l'élément a peut être soit nul, soit inversible. Voici les polynômes p_2 et p_1 qui remplaceront p dans chacune des deux éventualités. À moins que vous ne me demandiez de choisir l'une de ces deux options, auquel cas j'obéirai, je poursuivrai désormais deux calculs en parallèle, correspondant aux deux possibilités que j'ai mentionnées. Naturellement vous avez le droit de me poser des questions indépendantes les unes des autres dans chaque branche. Soyez rassurés en tout cas : aucune erreur ne peut se produire dans mes calculs.

Si l'on souhaite la réponse à plusieurs questions correspondant à des éléments $a_1 = q_1(x_p)$, …, $a_\ell = q_\ell(x_p)$ après l'introduction d'un seul zéro, on peut envisager les choses de manière dynamique, comme on va bientôt l'expliquer, mais il est parfois préférable de traiter le problème en un seul bloc en calculant une base de factorisation partielle $(g_1, \ldots, g_t)$ pour $(p, q_1, \ldots, q_\ell)$ et d'ouvrir les branches dans chacune desquelles l'un des g_i, parmi ceux qui divisent p (leur produit est égal à p car p est séparable), annule x_p. Dans chacune de ces branches, chacun des a_j est nul ou inversible. Les g_i sont deux à deux étrangers, et $p = \prod_{i:g_i|p} g_i$. Précisément, le morphisme naturel $\mathbf{K}[X]/\langle p\rangle \to \prod_{i:g_i|p} \mathbf{K}[X]/\langle g_i\rangle$ est un isomorphisme. On retrouve ici, formulé de manière légèrement différente, le fait 2.2.

Cas où p n'est pas séparable. En caractérisique nulle, ce cas est artificiel, car on peut remplacer p par le quotient séparable $h = p/\operatorname{pgcd}(p, p')$ puisque p divise une puissance de h. Mais en caractéristique positive, ce cas peut s'avérer inévitable[7].

7. Cependant, si le corps $\mathbf{K}$ est parfait, on a l'algorithme de factorisation séparable 1.2 qui décompose n'importe quel polynôme en un produit de puissances de polynômes séparables deux à deux étrangers, ce qui nous ramène au cas où p est séparable.

On commence par calculer $r = \operatorname{pgcd}(p, q)$. Si $r = 1$ ou $r = p$, on conclut comme dans le cas où p est séparable. Sinon, on calcule une base de factorisation partielle $(g_1, \ldots, g_s)$ pour (p, q). On obtient ainsi une partition de $[\![1..s]\!]$ en trois ensembles I, J, K :

- les g_i pour $i \in I$ divisent p et q,
- ceux pour $i \in J$ divisent p mais pas q,
- les autres, pour $i \in K$ divisent q mais pas p.

Notons que I ne peut être vide (dans ce cas $\operatorname{pgcd}(p, q) = 1$). Une inspection détaillée de l'algorithme de factorisation partielle pour (p, q) montre que J et K ont chacun au plus un élément. Plusieurs éventualités pour la suite selon que J est vide ou pas.

1. $J = \emptyset$, donc a est nilpotent dans $\mathbf{K}[x_p]$, on a la réponse $a = 0$, voici ce que l'on fait pour $\mathbf{K}[x_p]$:
   - si I est le singleton $\{i\}$, alors p est une puissance de g_i, si l'exposant est > 1, p est remplacé par g_i, sinon p ne change pas ;
   - si I contient plusieurs éléments, on a deux possibilités,
     - ou bien l'on remplace p par p_1, où $p_1 = \prod_{i \in I} g_i$;
     - ou bien, si cela semble préférable, on ouvre plusieurs branches, dans chacune d'entre elles p est remplacée par l'un des g_i pour $i \in I$.
2. I et $J \neq \emptyset$. On écrit $p_1 = \prod_{i \in I} g_i$ et $p_2 = g_j$ où $J = \{j\}$. Comme $p_1 p_2$ divise p et p divise une puissance de $p_1 p_2$, on peut déjà remplacer p par $p_1 p_2$. Mais la réponse à la question relative à l'élément a est différente selon que $p_1 = 0$ ou $p_2 = 0$. En conséquence, on ouvre deux branches de calcul pour l'avenir.
   - Dans la première branche, a est nul et p est remplacé par p_1 ; en outre si I contient plusieurs éléments, on a parfois intérêt à ouvrir des branches de calcul séparées, pour chaque facteur de g_i de p_1.
   - Dans la seconde branche, a est inversible et p est remplacé par p_2.

Remarque. On voit que dans cet algorithme, du fait que p n'est pas nécessairement séparable, il arrive que l'on tue un élément nilpotent. Si par exemple on a détecté que $p = p_1^2 p_2^3$, on ouvre deux branches l'une où $p_1 = 0$, l'autre où $p_2 = 0$, et dans les deux cas on a tué le nilpotent $\overline{p_1 p_2}$ de $\mathbf{K}[x_p]$. Ainsi on obtient que le morphisme naturel surjectif

$$\mathbf{K}[X]/\langle p\rangle \to \mathbf{K}[X]/\langle p_1\rangle \times \mathbf{K}[X]/\langle p_2\rangle$$

n'est pas un isomorphisme : on obtient un isomorphisme en passant aux algèbres réduites associées. ∎

Exemple. Voici un exemple « trop simple », mais instructif, car il montre que l'algorithme apporte bien la réponse à laquelle on s'attend, et ceci de manière complètement automatique. Cet exemple est celui où l'on réalise l'axiome CDI pour un élément $x_p - a$ lorsque $p(a) = 0$. L'algorithme de factorisation partielle produit une base de factorisation partielle $(h, X - a)$ pour $(p, X - a)$ avec $p = (X - a)^k h(X)$ et $h(a) \neq 0$. Ainsi on ouvre deux branches, l'une où $x_p = a$ (l'élément $x_p - a$ est nilpotent dans cette branche et il a été réduit à 0), l'autre où $h(x_p) = 0$ et $x_p - a$ inversible. ∎

Si l'on souhaite la réponse à plusieurs questions correspondant à des éléments $a_1 = q_1(x_p)$, …, $a_\ell = q_\ell(x_p)$ après l'introduction d'un seul zéro, on peut calculer une base de factorisation partielle $(g_1, \ldots, g_t)$ pour $(p, q_1, \ldots, q_\ell)$ et ouvrir les branches dans chacune desquelles l'un des g_i, parmi ceux qui divisent p, annule x_p. Dans chacune de ces branches, chacun des a_j est nul ou inversible. Les g_i sont deux à deux étrangers, et leur produit a « les mêmes zéros » que p. Précisément, le morphisme naturel $\mathbf{K}[X]/\langle p\rangle \to \prod_{i : g_i | p} \mathbf{K}[X]/\langle g_i\rangle$ est surjectif et son noyau est formé d'éléments nilpotents.

Introduction d'un deuxième zéro, en cascade. Examinons maintenant ce qui se passe lorsque l'on veut introduire, après un zéro x_1 de $p_1 \in \mathbf{K}[X_1]$, un zéro d'un polynôme unitaire $p_2(X_2) \in \mathbf{K}_1[X_2]$, où $\mathbf{K}_1 = \mathbf{K}[x_1]$. Avec un léger abus, notons encore $p_2 \in \mathbf{K}[X_1, X_2]$ le polynôme en question.

Si l'on est en caractéristique nulle, on désire remplacer p_2 par sa partie sans carré : $p_2 / \operatorname{pgcd}_{X_2}(p_2, p_2')$. On voit en particulier que l'on doit réaliser l'axiome CDI avec le discriminant $\operatorname{disc}_{X_2}(p_2) \in \mathbf{K}_1$, ce qui va peut-être nous amener à scinder $\mathbf{K}_1$, c'est-à-dire à ouvrir des branches avant même d'introduire le zéro x_2.

Dans la situation générale, où l'on ne simplifie pas d'entrée de jeu le polynôme p_2, le même problème va se poser dès que l'on cherche à réaliser l'axiome CDI pour un élément

$$q(x_1, x_2) \in \mathbf{K}[x_1, x_2] = \mathbf{K}[X_1, X_2]/\langle p_1(X_1), p_2(X_1, X_2)\rangle\,.$$

On veut en effet calculer une base de factorisation partielle $(g_1, \ldots, g_t)$ pour (p_2, q_2) dans $\mathbf{K}_1[X_2]$. Mais $\mathbf{K}_1$ n'est peut-être par un corps, or l'algorithme de factorisation partielle nécessite l'axiome CDI. Ainsi en exécutant cet algorithme, on va peut-être devoir scinder $\mathbf{K}_1$ en morceaux clairement distincts.

Ceci présente certes une complication dans les calculs, mais cela ne pourra pas en définitive produire un arbre avec énormément de branches. Car p_1 ne pourra pas se décomposer en beaucoup de facteurs[8]. Même chose pour p_2 qui, dans chacune des branches ouvertes pour p_1, ne pourra pas donner beaucoup de facteurs distincts.

Tant que l'on n'introduit pas un troisième zéro, le calcul reste donc circonsrit à un arbre qui ne peut pas trop grandir. Aux feuilles de cet arbre qui décrit « différentes possibiliés pour l'algèbre de départ $\mathbf{L} = \mathbf{K}[x_1, x_2]$ lorsqu'on la voit comme un corps discret », on trouvera des algèbres $\mathbf{L}_j$ quotients de $\mathbf{L}$, de la forme

$$\mathbf{L}_j = \mathbf{K}[X_1, X_2]/\langle f_{j1}(X_1), f_{j2}(X_1, X_2)\rangle\,,$$

avec $f_{j1}|p_1$ dans $\mathbf{K}[X_1]$ et $f_{j2}|p_2$ dans $\mathbf{K}[X_1]/\langle f_{j1}\rangle\,[X_2]$.

La chose importante à noter est que les faits essentiels suivants sont assurés :

– tout calcul qui a eu lieu dans $\mathbf{L}$ reste valable dans chacun des quotients $\mathbf{L}_j$, en particulier les éléments qui ont été déclarés nuls, ou inversibles, dans $\mathbf{L}$ le restent dans chaque $\mathbf{L}_j$: on ne se trompe jamais dans les calculs et l'on n'a jamais besoin de renier une réponse donnée précédemment ;

– les algèbres $\mathbf{L}_j$ sont incompatibles deux à deux : deux $\mathbf{L}_j$ distinctes divergent concernant la réponse à au moins une question correspondant à une instance de l'axiome CDI ;

– aucune information ne peut être perdue lorsque l'on remplace $\mathbf{L}$ par les algèbres $\mathbf{L}_j$, examinées chacunes séparément.

En termes plus abstraits.

3.1. Théorème. *Dans la situation précédente :*

1. *l'algèbre* $\mathbf{L}$ *et les algèbres* $\mathbf{L}_j$ *sont toutes strictement finies sur* $\mathbf{K}$*, et chaque* $\mathbf{L}_j$ *est un quotient de* $\mathbf{L}$ *;*
2. *le morphisme* $\mathbf{L} \to \prod_j \mathbf{L}_j$ *est surjectif et donne un isomorphisme lorsque l'on passe aux algèbres réduites associées.*

Remarque. Ainsi, la méthode D5 est pour l'essentiel une variation sur le thème décrit dans le fait 2.2. Mais alors que le fait 2.2 est établi pour une liste fixée d'éléments dans anneau zéro-dimensionnel fixé, on traite ici les résultats de façon dynamique en faisant croître la $\mathbf{K}$-algèbre strictement finie au fur et à mesure que les besoins du calcul le réclament. ∎

Introduction de plusieurs zéros en cascade. Ce paragraphe est laissé au lecteur, qui pourra formuler les théorèmes généraux correspondants et expliquer en détail la variante en caractéristique nulle si l'on exige pour chaque nouveau zéro un polynôme séparable.

Remarque. Pourquoi l'***évaluation dynamique***, marque de fabrique de D5, n'est-elle rien d'autre qu'un cas particulier d'***évaluation paresseuse*** ? C'est qu'elle répond à l'adage suivant : rien ne sert de se fatiguer à connaître toute la vérité[9] si l'on peut se contenter d'une partie de la vérité pour répondre au problème qui nous est posé. L'important n'est pas d'être omniscient, mais de profiter intelligemment de notre peu de science[10]. ∎

8. Au maximum $\deg(p_1)$, et dans le cas extrême, tous les zéros sont dans $\mathbf{K}$ et la situation est même bien plus simple.

9. Lorsque « toute » la vérité est inaccessible, c'est clair, mais c'est valable même dans le cas contraire, car il est souvent sage de remettre au lendemain ce qu'il n'est pas indispensable de faire le jour même.

10. Nous avons tous seulement quelques lacunes dans notre ignorance.

4. Systèmes polynomiaux à la D5

Nous montrons dans cette section que la philosophie D5 permet non seulement d'analyser les extensions finies d'un corps discret, mais qu'elle permet plus généralement d'analyser l'ensemble des solutions d'un système polynomial sur un corps discret.

Il n'y a ici aucune préoccupation d'efficacité dans les calculs. C'est bien plutôt la simplicité conceptuelle des démonstrations qui est visée.

Introduction. Le théorème de Chevalley concerne les ensembles constructibles.

Si $\mathbf{K} \subseteq \mathbf{L}$, où $\mathbf{K}$ est un corps discret et $\mathbf{L}$ un corps discret algébriquement clos, une ***partie constructible de*** $\mathbf{L}^n$ ***définie sur*** $\mathbf{K}$ est une combinaison booléenne arbitraire de fermés et d'ouverts de base définis sur $\mathbf{K}$. Le fermé (de Zariski) de base F_f défini sur $\mathbf{K}$ est l'hypersurface ensemble des zéros dans $\mathbf{L}^n$ du polynôme non nul $f \in \mathbf{K}[X_1, \ldots, X_n]$, et son complémentaire est un ***ouvert de base*** (de Zariski) U_f.

Un fermé de Zariski arbitraire (on dit souvent ***ensemble algébrique***, ou ***variété algébrique***, mais certains auteurs réservent ce dernier terme aux variétés irréductibles) est une intersection finie d'hypersurfaces, c'est l'ensemble des zéros d'un système polynomial.

Quand on considère plusieurs hypersurfaces dans $\mathbf{L}^n$, leurs combinaisons booléennes minimales sont obtenues en attribuant le «signe» $= 0$ ou $\neq 0$ à chacun des polynômes qui définissent ces hypersurfaces. Tout ensemble constructible est réunion finie de telles briques constructibles élémentaires. Chacune de ces briques est l'intersection d'un ensemble algébrique et d'un ouvert de base : c'est un ensemble *localement fermé* de Zariski.

Mais certaines de ces 2^r «combinasons de signes» sont impossibles (on suppose qu'il y a r polynômes donnés), et *cela est certifié par une identité algébrique que l'on appelle un* ***certificat algébrique****, ou encore un Nullstellensatz.*

Le ***théorème de Chevalley*** affirme quant à lui que *si V est une partie constructible de $\mathbf{L}^n$ définie sur $\mathbf{K}$, la projection de V sur un sous-espace de coordonnées $\mathbf{L}^r$ est également une partie constructible définie sur $\mathbf{K}$.*

Par exemple la projection d'une hyperbole sur un axe de coordonnée est ou bien l'axe tout entier, ou bien l'axe privé d'un point.

Une chose remarquable, aussi bien pour le théorème de Chevalley que pour le Nullstellensatz, est que tous ces objets restent «définis sur $\mathbf{K}$», en fait sur le corps des coefficients des polynômes de départ. Le corps algébriquement clos $\mathbf{L}$ est utile pour qu'il y ait assez points dans l'espace, mais presque pas pour les calculs qui concrétisent les théorèmes. Quand un constructible est non vide il possède toujours un point dont les coordonnées sont algébriques sur $\mathbf{K}$, c'est là qu'intervient $\mathbf{L}$, mais si l'on ne dispose pas d'un corps algébriquement clos $\mathbf{L}$ contenant $\mathbf{K}$, on doit pouvoir quand même trouver des «bonnes formulations» pour le théorème de Chevalley et le Nullstellensatz.

Partition constructible de la droite (associée à une famille finie de polynômes en une variable). On suppose en un premier temps disposer d'un corps algébriquement clos $\mathbf{L}$ contenant $\mathbf{K}$.

Le problème est le suivant. On donne une famille finie $(f_1, \ldots, f_r)$ dans $\mathbf{K}[X]$. On désire décrire de manière simple la partition en constructibles de $\mathbf{L}$ qui lui est associée, et en particulier connaître ses systèmes de conditions de signes qui sont impossibles.

S'il y a des polynômes identiquement nuls dans la liste, on sait que pour eux la seule condition de signe possible est $= 0$. Les autres polynômes peuvent être supposés unitaires (il suffit de les multiplier par des constantes non nulles). On est ainsi ramené au cas d'une famille de polynômes unitaires. Ce que nous supposons désormais.

On utilise alors l'algorithme de factorisation partielle qui nous fournit une base de factorisation partielle $(g_1, \ldots, g_s)$ formée de polynômes unitaires deux à deux étrangers. Notons g le produit des g_i.

La droite $\mathbf{L}$ est ainsi décomposée en une partition de constructibles non vides :

1. l'ouvert $\{\, x \mid g(x) \neq 0 \,\}$, sur lequel tous les f_j sont partout $\neq 0$;
2. les fermés $\{\, x \mid g_i(x) = 0 \,\}$: sur chacun de ces fermés, chacun des f_j est
   - ou bien partout $= 0$, (s'il est divisible par g_i) ;
   - ou bien partout $\neq 0$ (sinon, car il est alors étranger à g_i).

Pour terminer, si, pour des indices i distincts, les tableaux de signes pour les f_j sont les mêmes, on pourra remplacer ces g_i par leur produit.

Bref, tous les éléments de notre partition de $\mathbf{L}$ sont ouverts ou fermés. L'important à remarquer et que tout le calcul se passe dans le corps des coefficients des f_i et qu'il est complètement justifié par les axiomes des corps discrets (c'est-à-dire les axiomes des anneaux commutatifs et CDI).

Question subsidiaire 1

Que se passe-t-il lorsque l'on ne dispose pas d'un corps algébriquement clos $\mathbf{L}$? On voudrait bien une extension finie de $\mathbf{K}$ pour laquelle la partition décrite précédemment est bien une partition en ensembles non vides.

Tout d'abord, on a besoin d'avoir suffisamment d'éléments pour être certain que l'ouvert $g \neq 0$ soit non vide. Pour se débarrasser du problème on pourrait supposer que $\mathbf{K}$ est infini. Une autre manière plus élégante est de suivre Euclide et de construire un polynôme étranger aux g_i, par exemple le polynôme $g_{s+1} := 1 - g$, puis d'introduire formellement au moins un zéro de g_{s+1}.

Ensuite, pour chaque i, il faut introduire formellement au moins un zéro de g_i.

Tout ceci ne nous donne pas a priori un surcorps de $\mathbf{K}$, mais bien plutôt une $\mathbf{K}$-algèbre $\mathbf{A}$ strictement finie non nulle. On peut construire une telle algèbre $\mathbf{A}$, à la D5, sous la forme

$$\mathbf{A} = \mathbf{K}[z_1, \ldots, z_{s+1}] = \mathbf{K}[Z_1, \ldots, Z_{s+1}]/\big\langle (g_i(Z_i))_{i\in[\![1..s+1]\!]}\big\rangle.$$

On introduit la notation $a \# 0$ pour « a est inversible » dans les algèbres que l'on considère. La « droite » $\mathbf{A}$ contient alors les parties « constructibles » non vides et disjointes suivantes[11] :

1. l'ouvert $U_g = \{\, x \mid g(x) \# 0 \,\}$, sur lequel tous les f_j sont partout inversibles ; cet ouvert contient notamment le fermé $\{\, x \mid g_{s+1}(x) = 0 \,\}$, qui contient le point z_{s+1} ;
2. les fermés $F_{g_i} = \{\, x \mid g_i(x) = 0 \,\}$, pour $i \in [\![1..s]\!]$ (le fermé F_{g_i} contient le point z_i) : sur chacun de ces fermés, chacun des f_j est
   - ou bien partout $= 0$, (s'il est divisible par g_i) ;
   - ou bien partout inversible, (sinon, car il est alors étranger à g_i).

Question subsidiaire 2

Et le théorème de Chevalley ? Ici, il n'y a pas de sous-espace de coordonnées ...

Sauf si l'on considère le singleton $\mathbf{L}^0$ comme l'espace de coordonnées « sans variable ». La projection $\mathbf{L} \to \mathbf{L}^0$ est bien définie : c'est la fonction constante. La projection du constructible est vide si le constructible est vide, et égale au singleton dans le cas contraire. Dans la mesure où l'on veut un théorème de Chevalley explicite, il faut savoir calculer cette projection, c'est-à-dire décider si le constructible est vide. C'est ce que l'on a fait, et l'on comprend que le théorème de Chevalley sous forme explicite n'est rien d'autre qu'une procédure de décision d'existence améliorée.

Question subsidiaire 3

Et le Nullstellensatz ?

On voudrait montrer ici que tout système de conditions de signe impossible à réaliser (dans $\mathbf{L}$, ou à défaut dans n'importe quelle $\mathbf{K}$-algèbre strictement finie non nulle) est certifié par une identité algébrique.

Supposons par exemple que l'on a un système impossible

$$f_1(x) = f_2(x) = 0,\ f_3(x) \text{ et } f_4(x) \# 0.$$

On le remplace par : $f_1(x) = f_2(x) = 0$, $q(x) \# 0$, où $q = f_3 f_4$.

Le pgcd h de f_1 et f_2 s'écrit sous la forme $\prod_{i\in I} g_i^{m_i}$ pour une partie $I \subseteq [\![1..s]\!]$ et des $m_i > 0$. Chacun des g_i pour $i \in I$ divise q, donc h divise une puissance de q, ce qui donne une égalité $ch = q^N$, puis enfin une égalité $af_1 + bf_2 = q^N$. C'est le certificat algébrique cherché.

Le logiciel D5 peut également analyser la situation et fournir un certtificat algébrique, comme suit. On introduit un zéro formel x_1 de f_1. On soumet l'axiome CDI pour $f_2(x_1)$.
Si la réponse est que $f_2(x_1) \# 0$, c'est que $\operatorname{pgcd}(f_1, f_2) = 1$ avec une égalité $uf_1 + vf_2 = 1$ dans $\mathbf{K}[X]$. Le système $f_1 = f_2 = 0$ est impossible à lui tout seul, et l'on a un certificat algébrique.
Si la réponse est que $f_2(x_1) = 0$, c'est que f_1 divise une puissance de f_2 et la condition $f_2(x_1) = 0$ peut être omise. Le système $f_1 = 0$, $q \# 0$ est impossible à lui tout seul.

11. On a mis « constructibles » entre guillemets parce qu'avec un anneau qui n'est pas un corps discret, la définition change légèrement, en remplaçant « $\neq 0$ » par « $\# 0$ ». En conséquence on a en général seulement une réunion disjointe et non une partition de la droite $\mathbf{A}$. Mais il arrive aussi que $\mathbf{A}$ soit un corps discret.

Si la réponse est que les deux cas peuvent se présenter, alors D5 remplace la branche pour le système $f_1(x) = f_2(x) = 0$ par la condition unique $h(x) = 0$, où $h = \text{pgcd}(f_1, f_2)$, ou un diviseur ayant les mêmes zéros.
Dans les deux derniers cas, on soumet l'axiome CDI pour $q(x_1)$. D5 répond que $q(x_1) = 0$ et donne une puissance de q multiple de h (ou de f_1 dans le cas où l'on a directement $f_2(x_1) = 0$).
Ainsi, avec l'évaluation dynamique (de la situation proposée) par le système D5, on obtient explicitement dans toutes les situations un certificat algébrique du type

$$q^N = af_1 + bf_2 \text{ dans } \mathbf{K}[X],\ N \in \mathbb{N}.$$

Partition constructible du plan (associée à une famille finie de polynômes en deux variables). On suppose maintenant donnée une famille finie $(f_1, \ldots, f_r)$ dans $\mathbf{K}[X, Y]$. On désire décrire de manière simple la partition en constructibles de $\mathbf{L}^2$ qui lui est associée. En particulier on veut connaître les systèmes de conditions de signes qui sont impossibles. Et l'on veut démontrer le théorème de Chevalley, selon lequel la projection d'un constructible de $\mathbf{L}^2$ sur l'axe des x est un constructible de $\mathbf{L}$.

Il nous suffira d'ailleurs de savoir analyser complètement un constructible élémentaire

$$f_1 = \cdots = f_t = 0,\ f_r \# 0, \text{ où } t = r - 1$$

On suppose sans perte de généralité qu'aucun f_i n'est identiquement nul. On note $\mathbf{k} = \mathbf{K}[X]$ et $\mathbf{k}[Y] = \mathbf{K}[X, Y]$. On est «presque» ramené à la situation précédente, où il n'y avait qu'une variable, à ceci près que $\mathbf{k}$ n'est pas un corps discret.

La situation précédente était analysée grâce à l'algorithme de factorisation partielle, qui fonctionne sur un corps discret, c'est-à-dire sur un anneau vérifiant l'axiome CDI.

Qu'à cela ne tienne, exécutons l'algorithme de factorisation partielle avec $\mathbf{k}$ à la place de $\mathbf{K}$, et, comme dans la méthode D5, examinons la situation en détail chaque fois que l'axiome CDI est invoqué.
On obtient comme avec D5 un arbre de calcul. Supposons que nous soyons à une feuille où l'on a fait les hypothèses

$$a_1(x), \ldots, a_k(x) = 0 \text{ et } u_1(x), \ldots, u_\ell(x) \# 0$$

Ceci correspond à un constructible sur l'axe des x qui peut être analysé selon la méthode univariée. En particulier, on peut supposer que ce constructible n'est pas vide, car sinon, on aurait déclaré que la branche était morte[12].
Maintenant, supposons que l'algorithme de factorisation partielle (sur $\mathbf{k}[Y]$) invoque l'axiome CDI pour un $b \in \mathbf{k}$. Pas de souci ! nous savons analyser la situation «en x» selon la méthode univariée.
Ou bien un seul des deux cas $b = 0$, $b \# 0$ est possible : alors, on n'ouvre pas de branches et l'on poursuit le calcul selon l'indication qui nous a été fournie (lorsque $b \# 0$ on dispose de l'inverse de b sous forme explicite).
Ou bien les deux cas sont possibles, on ouvre deux branches, dans chacune desquelles le constructible précédent en x a été scindé en deux constructibles non vides.
Au bout d'un certain temps (certainement bien long, mais passons), l'algorithme de factorisation partielle pour $\mathbf{k}[Y]$ a été exécuté avec succès dans chaque branche, et donne des résultats divers et variés, selon le constructible en x qui a été construit.
Notons que l'on est parti du constructible ouvert $\mathbf{L}$ (tout entier) et que l'on a toujours scindé en deux des constructibles en x précédemment construits. Nous avons donc construit une partition constructible de l'axe des x. Et tout constructible élémentaire de $\mathbf{L}^2$ associé à la famille $(f_1, \ldots, f_r)$, ou bien est reconnu comme vide, ou bien se projette en x selon une réunion finie explicite d'éléments de la partition construite.
C'est exactement le théorème de Chevalley, sous une forme explicite[13]. Ainsi, vive les pgcd, vive l'algorithme de factorisation partielle ! Sous des dehors innocents, ils nous donnent accès à un grand théorème[14].

12. Ceci ne se produit jamais avec D5 car on travaille avec des algèbres strictement finies non nulles par construction, qui ne sont scindées en deux que dans le cas où l'idempotent correspondant est $\neq 0, 1$.

13. En pratique, naturellement, sur machine, si l'on ne veut pas un `out of memory`, il faudra inventer des méthodes plus rapides que celle indiquée ici.

14. Théorème dont la preuve est le plus souvent omise dans les traités usuels, qui ne veulent généralement pas s'abaisser à des considérations aussi terre à terre que D5 : le raisonnement cas par cas dans un corps discret ! Il y a cependant des exposés très clairs dans les livres d'algèbre qui incluent un peu de logique formelle dans leur cours,

Avec un peu de recul, on voit qu'il y a une situation, dite générique, qui correspond à la branche où l'on a choisi l'alternative $b \# 0$ chaque fois que la question est posée pour un élément b non nul de $\mathbf{k}$. On obtient ici la base de factorisation partielle générique au dessus de l'ouvert générique[15] en x.
Dans toutes les autres branches, la situation en x relève directement de la méthode D5 car on est dans un quotient d'une algèbre strictement finie $\mathbf{K}[X]/\langle b\rangle$ pour un $b(X) \neq 0$.

On obtient ainsi une ***décomposition cylindrique***[16] de $\mathbf{L}^2$.
Au dessus de chaque constructible C en x de la partition de $\mathbf{L}$ obtenue, la base de factorisation partielle de $(f_1(x,Y),\dots,f_1(x,Y))$ est donnée par des polynômes en Y dont les coefficients sont des polynômes[17] en x qui ne dépendent pas du point $x \in C$.

Question subsidiaire 1

Que se passe-t-il lorsque l'on ne dispose pas d'un corps algébriquement clos $\mathbf{L}$?
Nous laissons à la lectrice le soin de montrer que, comme dans le cas univarié, on peut construire une $\mathbf{K}$-algèbre strictement finie non nulle qui contient au moins un point dans chaque constructible qui a été identifié comme « possible » dans la description de la décomposition cylindrique.

Question subsidiaire 2

Et le Nullstellensatz ?

Considérons une situation impossible « $f_1 = \cdots = f_r = 0,\ h \# 0$ ».
Soit $\mathbf{B} = \mathbf{K}[X,Y]/\langle f_1,\dots,f_r\rangle\,[1/h]$ la $\mathbf{K}$-algèbre correspondante. Le Nullstellensatz affirme que cette algèbre est réduite à $\{0\}$. Un certificat algébrique n'est rien d'autre qu'une égalité dans $\mathbf{K}[X,Y]$ qui signifie $1 = 0$ dans $\mathbf{B}$.

Lorsque l'on évalue la situation « $f_1 = \cdots = f_r = 0,\ h \# 0$ » à la D5 (selon la méthode précédente avec $h = f_{r+1}$), on obtient une démonstration purement calculatoire du fait que la situation est impossible.

Que se passe-t-il lorsque, dans le cours de l'évaluation dynamique, on déclare qu'une branche est morte ? C'est que l'on a obtenu un certificat algébrique de nullité pour une algèbre $(\mathbf{B}/\mathfrak{a})[1/\ell]$, où $\mathfrak{a}$ est l'idéal engendré par les polynômes a apparaissant dans les hypothèses $a(x,y) = 0$ introduites aux noeuds de la branche, et ℓ est le produit des polynômes b apparaissant dans les hypothèses $b(x,y) \# 0$ introduites aux noeuds de la branche.

Or, lorsque l'on ouvre deux branches sous un nœud, dans la première branche on a rjouté une hypothèse $a = 0$ et dans l'autre l'hypothèse $a \# 0$.

On voit donc que le Nullstellensatz résulte de deux ingrédients suivants :
- la possibilité d'utiliser l'évaluation dynamique pour certifier les systèmes impossibles ;
- le lemme de Krull, énoncé sous la forme constructive suivante.

4.1. Lemme. (Lemme de Krull, forme constructive élémentaire) *Soit un élément b dans un anneau $\mathbf{B}$. Si les deux anneaux $\mathbf{B}/\langle b\rangle$ et $\mathbf{B}[1/b]$ sont triviaux, il en est de même de $\mathbf{B}$.*

Démonstration. D'une part on a $1 \in \langle b\rangle$, d'autre part $0 \in b^{\mathbb{N}}$ pour un $n \in \mathbb{N}$. Si $1 = xb$, cela donne $1 = (xb)^n = x^n b^n = 0$. □

Cas général, théorème de Chevalley et Nullstellensatz. Ce paragraphe est laissé au lecteur, du moins s'il en a le courage et s'il est sceptique. Il pourra écrire une démonstration en bonne et due forme par récurrence sur le nombre de variables.

---

avec le théorème d'élimination des quantificateurs dans la théorie des corps algébriquement clos pour une caractéristique fixée. Nous ne faisons ici que restituer sous forme très naïve et élémentaire l'esprit de ces démonstrations plus savantes et très éclairantes.

15. Calcul en la seule variable Y sur le corps $\mathbf{K}(X)$.

16. On dit aussi *décomposition algébrique cylindrique*, avec l'acronyme anglais CAD. La CAD la plus populaire se trouve en géométrie algébrique réelle.

17. Si l'on veut des polynômes unitaires pour la base de factorisation partielle, on devra parfois utiliser des fractions rationnelles en x dont les dénominateurs sont certifiés $\# 0$ dans la branche où l'on se trouve, du moins dans le cas générique.

Nullstellensatz et position de Noether via les résultants. Nous signalons maintenant une autre manière d'aboutir au Nullstellensatz «sans corps algébriquement clos ni décomposition des polynômes en facteurs irréductibles», un peu plus sophistiquée que la méthode dynamique, mais plus traditionnelle. Nous reprenons ici la formulation [ACMC, théorèmes VII-1.1 et 1.5], donnée sans référence à un corps algébriquement clos qui contiendrait le corps discret de départ.

Lorsque l'on n'a pas d'algorithme de factorisation complète des polynômes de $\mathbf{K}[X]$, on ne sait pas nécessairement construire des extensions algébriques de $\mathbf{K}$ dans lesquelles trouver les coordonnées des zéros des systèmes polynomiaux. En mathématiques constructives, on contourne la difficulté en énonçant que le système polynomial, s'il n'est pas certifié incompatible par une identité algébrique, admet au moins un zéro dans une $\mathbf{K}$-algèbre strictement finie non nulle[18].

Le théorème est démontré dans [ACMC] en utilisant une généralisation du polynôme résultant. Pour un anneau $\mathbf{k}$ et une famille $(f, g_1, \ldots, g_r)$ de polynômes de $\mathbf{k}[X]$ avec f unitaire, on construit un système générateur fini d'un ***idéal résultant*** $\mathfrak{b} \subseteq \mathbf{k}$ qui, à nilradical près, est égal à l'***idéal d'élimination*** $\mathfrak{a} = \langle f, g_1, \ldots, g_r\rangle \cap \mathbf{k}$. Cet outil, combiné avec des changements de variables rendant certains polynômes unitaires, conduit à la ***mise en position de Noether***, un théorème très important dont une conséquence est le Nullstellensatz faible. On passe ensuite facilement au Nullstellensatz sous sa forme générale.

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

- (Nullstellensatz faible)
  - *Ou bien* $\mathbf{A} = \{0\}$*, c'est-à-dire* $1 \in \langle f_1, \ldots, f_s\rangle$.
  - *Ou bien il existe un quotient non nul de* $\mathbf{A}$ *qui est une* $\mathbf{K}$*-algèbre strictement finie.*
- (Position de Noether) *Plus précisément, on a un entier* $r \in [\![-1..n]\!]$ *bien défini avec les propriétés suivantes.*

1. *Ou bien* $r = -1$ *et* $\mathbf{A} = \{0\}$*. Dans ce cas, le système* $(f_1, \ldots, f_s)$ *n'admet de zéro dans aucune* $\mathbf{K}$*-algèbre non triviale.*
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* $Y_1, \ldots, Y_n$*) qui satisfait les propriétés suivantes.*
   - *On a* $\mathfrak{f} \cap \mathbf{K}[Y_1, \ldots, Y_r] = 0$*. Autrement dit, l'anneau* $\mathbf{K}[Y_1, \ldots, Y_r]$ *s'identifie à un sous-anneau de l'algèbre quotient* $\mathbf{A}$*.*
   - *Chaque* Y_j *pour* $j \in [\![r+1..n]\!]$ *est entier sur* $\mathbf{K}[Y_1, \ldots, Y_r]$ *modulo* $\mathfrak{f}$ *et l'anneau* $\mathbf{A}$ *est un* $\mathbf{K}[Y_1, \ldots, Y_r]$*-module de présentation finie.*
   - *Il existe un entier* N *tel que pour chaque* $(\alpha_1, \ldots, \alpha_r) \in \mathbf{K}^r$*, l'algèbre quotient* $\mathbf{A}/\langle Y_1 - \alpha_1, \ldots, Y_r - \alpha_r\rangle$ *est un* $\mathbf{K}$*-espace vectoriel non nul de dimension finie* $\leqslant N$*.*
   - *On a des idéaux de type fini* $\mathfrak{f}_j \subseteq \mathbf{K}[Y_1, \ldots, Y_j]$ $(j \in [\![r..n]\!])$ *avec les inclusions et égalités suivantes.*

$$\begin{aligned}
&\langle 0\rangle = \mathfrak{f}_r \subseteq \mathfrak{f}_{r+1} \subseteq \ldots \subseteq \mathfrak{f}_{n-1} \subseteq \mathfrak{f}_n = \mathfrak{f}\\
&\mathfrak{f}_j \subseteq \mathfrak{f}_\ell \cap \mathbf{K}[Y_1, \ldots, Y_j] && (j < \ell,\ j, \ell \in [\![r..n]\!])\\
&\mathrm{D}(\mathfrak{f}_j) = \mathrm{D}\left(\mathfrak{f}_\ell \cap \mathbf{K}[Y_1, \ldots, Y_j]\right) && (j < \ell,\ j, \ell \in [\![r..n]\!])
\end{aligned}$$

Voici maintenant le Nullstellensatz classique ([ACMC, théorème VII-1.8]). Il se déduit du Nullstellensatz faible par l'astuce de Rabinovitch.

4.3. Théorème. (Nullstellensatz classique, version constructive générale)
Soit $\mathbf{K}$ *un corps discret et* f_1*, …,* f_s*,* g *dans* $\mathbf{K}[X_1, \ldots, X_n]$*. Considérons l'algèbre quotient* $\mathbf{A} = \mathbf{K}[\underline{X}]/\langle f_1, \ldots, f_s\rangle$.

18. En mathématiques classiques une telle algèbre possède un idéal maximal de type fini en vertu du tiers exclu, ce qui donne une solution du système polynomial dans une extension finie de $\mathbf{K}$. Le lemme de Zorn intervient donc uniquement lorsque l'on veut plonger cette extension finie dans un corps algébriquement clos.

1. *Ou bien il existe un quotient non nul* $\mathbf{B}$ *de* $\mathbf{A}$ *qui est une* $\mathbf{K}$*-algèbre strictement finie avec* $g \#_{\mathbf{B}} 0$[19].
2. *Ou bien* g *est nilpotent dans* $\mathbf{A}$*, autrement dit, il existe un entier* N *tel que* $g^N \in \langle f_1, \ldots, f_s\rangle_{\mathbf{K}[\underline{X}]}$*. A fortiori,* g *s'annule en tout zéro du système polynomial* $(f_1, \ldots, f_s)$ *dans n'importe* $\mathbf{K}$*-algèbre réduite.*

Signalons enfin le théorème [ACMC, VII-1.7]. Le point *2* de ce théorème exprime en termes explicites une première forme de caténarité et d'équidimensionalité de l'anneau $\mathbf{K}[X_1, \ldots, X_n]$ pour un corps discret $\mathbf{K}$.

4.4. Théorème. (Mise en position de Noether simultanée)
Soient $\mathfrak{f}_1, \ldots, \mathfrak{f}_k$ *des idéaux de type fini de* $\mathbf{K}[\underline{X}] = \mathbf{K}[X_1, \ldots, X_n]$.

1. *Il existe des entiers* $r_1, \ldots, r_k \in [\![-1..n]\!]$ *et un changement de variables tels que, en appelant* $Y_1, \ldots, Y_n$ *les nouvelles variables, on ait pour chaque* $j \in [\![1..k]\!]$ *la situation suivante.*
   Si $r_j = -1$*, alors* $\mathfrak{f}_j = \langle 1\rangle$*, sinon*
   a. $\mathbf{K}[Y_1, \ldots, Y_{r_j}] \cap \mathfrak{f}_j = \{0\}$,
   b. *pour* $\ell > r_j$*,* Y_ℓ *est entier modulo* $\mathfrak{f}_j$ *sur* $\mathbf{K}[Y_1, \ldots, Y_{r_j}]$.
   Lorsque $\mathbf{K}$ *est infini, on peut prendre un changement linéaire de variables.*
2. *Si* $\langle 1\rangle \neq \mathrm{D}(\mathfrak{f}_1) \supset \mathrm{D}(\mathfrak{f}_2) \supset \cdots \supset \mathrm{D}(\mathfrak{f}_k)$ *avec les dimensions* r_j *strictement croissantes, on peut intercaler des radicaux d'idéaux de type fini de sorte que la suite des dimensions obtenue soit* $0, 1, \ldots, n$.

19. A fortiori $g \# 0$ dans tout quotient de $\mathbf{B}$.

CHAPITRE 3

Dimension de Krull

Sommaire

Introduction

Des références pour cette section sont les chapitres XI, XII et XIV de [ACMC], ou encore l'article [7].

Les sources originales constructives sont notamment chez Stone, Joyal et Español [32, 19, 20, 11, 12, 13].

La forme plus manipulable exposée ici provient de [23, 5, 8].

La dernière section est pour l'essentiel due à Thierry Coquand [3, 6].

1. Le spectre de Zariski

Dans cette section, nous décrivons l'approche de la dimension de Krull en mathématiques classiques.

Pour nous il s'agit avant tout d'une heuristique. En effet, l'aspect constructif des espaces spectraux est entièrement concentré dans les treillis distributifs obtenus « par dualité ». En particulier, l'aspect constructif de la dimension de Krull est entièrement concentré dans la dimension de Krull des treillis distributifs et elle peut être définie de manière complètement indépendante des espaces spectraux.

Néanmoins l'heuristique donnée par les espaces spectraux est essentielle à la compréhension du petit miracle qui va advenir avec l'introduction des notions constructives duales. Petit miracle dont on ne prendra pleinement conscience que dans les sections suivantes, quand on verra de beaux théorèmes abstraits se transformer en algorithmes.

Treillis et spectre de Zariski. Nous notons $\mathrm{D}_{\mathbf{A}}(\mathfrak{a}) = \sqrt[\mathbf{A}]{\mathfrak{a}}$ le nilradical de l'idéal $\mathfrak{a}$ dans l'anneau $\mathbf{A}$ et $\mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ pour $\mathrm{D}_{\mathbf{A}}\big(\langle x_1, \ldots, x_n\rangle\big)$. Le ***treillis de Zariski*** de l'anneau $\mathbf{A}$, noté $\mathsf{Zar}\,\mathbf{A}$, est basé sur l'ensemble des $\mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ (pour $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in \mathbf{A}$). Cet ensemble, ordonné par la relation d'inclusion, est un treillis distributif avec

$$\mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1) \vee \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_2) = \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1 + \mathfrak{a}_2) \;\text{ et }\; \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1) \wedge \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_2) = \mathrm{D}_{\mathbf{A}}(\mathfrak{a}_1\,\mathfrak{a}_2).$$

NB. La structure de treillis est définie en disant que toute partie finie admet une borne supérieure et une borne inférieure ; en particulier le treillis doit comporter un élément minimum, noté généralement 0 et un élément maximum, noté généralement 1. La structure de treillis et celle de treillis distributif sont des structures algébriques purement équationnelles.

1.1. Définition. On appelle ***spectre de Zariski*** de l'anneau $\mathbf{A}$ et l'on note $\mathsf{Spec}\,\mathbf{A}$ l'ensemble des idéaux premiers premiers de $\mathbf{A}$. On le munit de la topologie possédant pour base d'ouverts les

$$\mathfrak{D}_{\mathbf{A}}(a) = \{\, \mathfrak{p} \in \mathsf{Spec}\,\mathbf{A} \mid a \notin \mathfrak{p} \,\}.$$

On note $\mathfrak{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ pour $\mathfrak{D}_{\mathbf{A}}(x_1) \cup \cdots \cup \mathfrak{D}_{\mathbf{A}}(x_n)$.
Pour $\mathfrak{p} \in \mathsf{Spec}\,\mathbf{A}$ et $S = \mathbf{A} \setminus \mathfrak{p}$ on note $\mathbf{A}_{\mathfrak{p}}$ pour $\mathbf{A}_S$ (l'ambigüité entre les deux notations contradictoires $\mathbf{A}_{\mathfrak{p}}$ et $\mathbf{A}_S$ est levée en pratique par le contexte).

En mathématiques classiques, on obtient alors le résultat suivant.

1.2. Théorème*.

1. *Les ouverts quasi-compacts de* $\mathsf{Spec}\,\mathbf{A}$ *sont les ouverts* $\mathfrak{D}_{\mathbf{A}}(x_1, \ldots, x_n)$.
2. *L'application* $\mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_n) \mapsto \mathfrak{D}_{\mathbf{A}}(x_1, \ldots, x_n)$ *est bien définie, c'est un isomorphisme de treillis distributifs.*

Spectre d'un treillis distributif. Le spectre de Zariski est l'exemple paradigmatique d'un ***espace spectral***. Les espaces spectraux ont été introduits par Stone [32] en 1937. Son but était d'interpréter la logique formelle intuitionniste en termes topologiques.

Les espaces spectraux ont envahi l'algèbre abstraite, mais presque tout le monde a oublié que les espaces spectraux s'interprètent en termes de treillis distributifs, comme le démontra Stone dans l'article où il introduisit ces espaces.

Ils peuvent être caractérisés comme les espaces topologiques vérifiant les propriétés suivantes :
- l'espace est quasi compact,
- tout ouvert est réunion d'ouverts quasi-compacts,
- l'intersection de deux ouverts quasi-compacts est un ouvert quasi-compact,
- pour deux points distincts, il y a un ouvert contenant l'un mais pas l'autre,
- tout fermé irréductible est l'adhérence d'un point.

Les ouverts quasi-compacts forment alors un treillis distributif, le sup et le inf étant la réunion et l'intersection. Une application continue entre espaces spectraux est dite ***spectrale*** si l'image réciproque de tout ouvert quasi-compact est un ouvert quasi-compact. Le résultat fondamental de Stone peut être énoncé comme suit.

En mathématiques classiques la catégorie des espaces spectraux et applications spectrales est antiéquivalente à la catégorie des treillis distributifs.

Voici comment cela fonctionne. Un ***idéal*** d'un treillis distributif est une partie initiale (i.e. si $x \in \mathfrak{a}$ alors $\downarrow x \subseteq \mathfrak{a}$), stable par $\vee$ et contenant 0. Un ***idéal premier*** est un idéal $\mathfrak{p}$ qui vérifie

$$x \wedge y \in \mathfrak{p} \;\Rightarrow\; (x \in \mathfrak{p} \text{ ou } y \in \mathfrak{p}), \qquad 1_{\mathbf{T}} \notin \mathfrak{p}$$

Le ***spectre*** de $\mathbf{T}$, noté $\mathsf{Spec}\,\mathbf{T}$ est alors défini comme l'espace dont les points sont les idéaux premiers de $\mathbf{T}$ et dont une base d'ouverts est donnée par les parties $\mathfrak{D}_{\mathbf{T}}(a) := \{\, \mathfrak{p} \in \mathsf{Spec}\,\mathbf{T} \mid a \notin \mathfrak{p} \,\}$ pour $a \in \mathbf{T}$.
Si $\varphi : \mathbf{T} \to \mathbf{V}$ est un morphisme de treillis distributifs, on définit l'application

$$\mathsf{Spec}\,\varphi : \mathsf{Spec}\,\mathbf{V} \to \mathsf{Spec}\,\mathbf{T}, \quad \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

C'est une application spectrale. Tout ceci définit Spec comme foncteur contravariant.
On montre que les $\mathfrak{D}_{\mathbf{T}}(a)$ sont les ouverts quasi-compacts de $\mathsf{Spec}\,\mathbf{T}$. En fait le théorème* 1.2 s'applique à tout treillis distributif $\mathbf{T}$:

1. *Les ouverts quasi-compacts de* $\mathsf{Spec}\,\mathbf{T}$ *sont exactement les* $\mathfrak{D}_{\mathbf{T}}(u)$.
2. *L'application* $u \mapsto \mathfrak{D}_{\mathbf{T}}(u)$ *est bien définie et c'est un isomorphisme de treillis distributifs.*

Dans l'autre sens, si X est un espace spectral on note $\mathsf{Qqc}(X)$ le treillis distributif formé par ses ouverts quasi-compacts. Si $\xi : X \to Y$ est une application spectrale, l'application

$$\mathsf{Qqc}(\xi) : \mathsf{Qqc}(Y) \to \mathsf{Qqc}(X), \quad U \mapsto \xi^{-1}(U)$$

est un homomorphisme de treillis distributifs. Ceci définit Qqc comme foncteur contravariant.

L'antiéquivalence de catégories qui était annoncée est définie par les foncteurs Spec et Oqc. Elle généralise une antiéquivalence classique entre ensembles ordonnés finis[20] et treillis distributifs finis.

Notez que l'espace spectral vide correspond au treillis **1**, et qu'un espace spectral réduit à un point correspond au treillis **2**.

Note de terminologie. La dénomination «espace spectral» est due à Hochster, qui a démontré que tout espace spectral était homéomorphe au spectre de Zariski d'un anneau convenable [18]. Auparavant, on parlait plutôt d'***espace cohérent***, en relation avec les faisceaux algébriques cohérents de Serre, faisceaux dont la base est un espace spectral, construit comme recollement d'un nombre fini de spectres affines (spectres de Zariski d'anneaux commutatifs) le long d'ouverts quasi-compacts. Cela a donné les schémas cohérents de Grothendieck, pain quotidien des géomètres contemporains. Pour des considérations historiques plus développées voir [Johnstone, page 78].

Sous-espaces spectraux. Par définition, un sous-ensemble Y d'un espace spectral X est un ***sous-espace spectral*** si la topologie induite fait de Y un espace spectral et si l'injection canonique $Y \to X$ est spectrale.

Cette notion est en fait exactement la notion duale de la notion de treillis distributif quotient (par une relation d'équivalence compatible).

Les sous-espaces fermés de X sont spectraux et correspondent aux quotients par les idéaux (quotient par la relation d'équivalence obtenue en forçant $\mathfrak{a} = 0$). Plus précisément un idéal $\mathfrak{a}$ de $\mathsf{Oqc}(X) = \mathbf{T}$ définit le fermé $\mathfrak{V}_{\mathbf{T}}(\mathfrak{a}) = \{\, \mathfrak{p} \in X \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$ (en identifiant les points de X avec les idéaux premiers de $\mathsf{Oqc}(X)$), et l'on a alors un isomorphisme canonique

$$\mathsf{Oqc}\big(\mathfrak{V}_{\mathbf{T}}(\mathfrak{a})\big) \simeq \mathsf{Oqc}(X)/(\mathfrak{a} = 0)\ .$$

Les fermés irréductibles correspondent aux idéaux premiers de $\mathsf{Oqc}(X)$.

Enfin les ouverts quasi-compacts correspondent aux quotients par des filtres principaux[21] :

$$\mathsf{Oqc}\big(\mathfrak{D}_{\mathbf{T}}(u)\big) \simeq \mathsf{Oqc}(X)/(\uparrow u = 1)\ .$$

Une approche heuristique pour la dimension de Krull. Nous remarquons que le spectre de Zariski d'un anneau commutatif s'identifie de façon naturelle avec le spectre de son treillis de Zariski.

En mathématiques classiques, la notion de dimension de Krull peut être définie, pour un espace spectral arbitraire X, comme la longueur maximale des chaînes strictement croissantes de fermés irréductibles.

Une manière plus intuitive d'appréhender cette notion de dimension, en ne mentionnant pas les fermés irréductibles, est la suivante. La dimension peut être caractérisée par récurrence en disant que d'une part, la dimension -1 correspond à l'espace vide, et d'autre part, pour $k \geqslant 0$, un espace X est de dimension $\leqslant k$ si, et seulement si, pour tout ouvert quasi-compact Y, le bord de Y dans X est de dimension $\leqslant k-1$ (ce bord est fermé donc c'est un sous-espace spectral de X).

Voyons par exemple, pour un anneau commutatif $\mathbf{A}$, comment on peut définir le bord de l'ouvert $\mathfrak{D}_{\mathbf{A}}(a)$ dans $\mathsf{Spec}\,\mathbf{A}$. Le bord est l'intersection de l'adhérence de $\mathfrak{D}_{\mathbf{A}}(a)$ et du fermé complémentaire de $\mathfrak{D}_{\mathbf{A}}(a)$, noté $\mathfrak{V}_{\mathbf{A}}(a)$. L'adhérence de $\mathfrak{D}(a)$ c'est l'intersection de tous les $\mathfrak{V}(x)$ qui contiennent $\mathfrak{D}(a)$, c'est-à-dire tels que $\mathfrak{D}(x) \cap \mathfrak{D}(a) = \emptyset$.
Comme $\mathfrak{D}(x) \cap \mathfrak{D}(a) = \mathfrak{D}(xa)$, et comme on a $\mathfrak{D}(y) = \emptyset$ si, et seulement si, y est nilpotent, on obtient une approche heuristique de l'idéal «bord de Krull de a», qui est l'idéal engendré par a d'une part (ce qui correspond à $\mathfrak{V}(a)$), et par tous les x tels que xa est nilpotent d'autre part (ce qui correspond à l'adhérence de $\mathfrak{D}(a)$) :

$$\langle x \rangle + \big(\mathrm{D}_{\mathbf{A}}(0) : x\big).$$

Ceci sera une clé pour une définition constructive acceptable de la dimension de Krull.

2. Lemme de Krull et généralisations

20. Un ensemble ordonné fini peut être vu comme un espace spectral dont les fermés sont les parties initiales. Les fermés irréductibles sont ceux de la forme $\downarrow x$.

21. En renversant la relation d'ordre d'un treillis distributif, on obtient le ***treillis opposé***. La notion opposée de celle d'idéal est la notion de ***filtre***. Le quotient par un filtre $\mathfrak{f}$ est obtenu en forçant $\mathfrak{f} = 1$.

2.1. Lemme*. (Lemme de Krull, en mathématiques classiques)
Soit dans un anneau $\mathbf{A}$ *un idéal* $\mathfrak{a}$ *et un monoïde* S*. Si* $\mathfrak{a} \cap S = \emptyset$*, il existe un idéal premier* $\mathfrak{p}$ *tel que* $\mathfrak{a} \subseteq \mathfrak{p}$ *et* $\mathfrak{p} \cap S = \emptyset$*.*

Lemme de Krull usuel. À défaut d'avoir un énoncé constructif, ce lemme a un contenu constructif que nous allons examiner.

Le couple $(\mathfrak{a}, S)$ doit être vu comme une approximation de l'idéal premier $\mathfrak{p}$. Il est dit ***compatible*** si $\mathfrak{a} \cap S = \emptyset$. Cette notion a un caractère plutôt négatif : si $\mathfrak{a}$ et S sont infinis, on n'est pas sorti de l'auberge ! Les mathématiques constructives sont mal à l'aise avec la négation. C'est la notion contraire qui est intéressante : $\boxed{0 \in \mathfrak{a} + S}$. Dans ce cas on dit que le couple $(\mathfrak{a}, S)$ ***collapse***, ou ***s'effondre***. Le projet de construire un idéal premier s'effondre !

Avec l'idée d'approximation en tête, nous appellerons ***premier idéal***[22] tout couple (I, U) formé de deux parties de $\mathbf{A}$. Le premier idéal (I, U) est une approximation de tout idéal premier $\mathfrak{p}$ qui contient I et ne contient aucun élément de U. Si I et U sont finiment énumérés, on parlera d'***approximation finie***.

On dit que ***le premier idéal*** (I, U) ***collapse***, si, en notant S le monoïde engendré par U, on a $0 \in \langle I \rangle + S$.

Un défi de l'algèbre constructive est de ramener tout discours sur les idéaux premiers à un discours sur leurs approximations finies.

Sur un anneau arbitraire, un idéal premier est un peu comme un nombre réel en analyse, lequel n'est connu en général que par ses approximations rationnelles finies.

On dit que le premier idéal (J, V) ***raffine*** le premier idéal (I, U), ce que l'on note $(I, U) \preccurlyeq (J, V)$ lorsque $I \subseteq J$ et $U \subseteq V$ (c'est comme l'inclusion entre deux intervalles rationnels représentant des approximations finies d'un même nombre réel). Ainsi un premier idéal correspond à un idéal premier si, et seulement si, il ne peut pas être raffiné sans collapser.

Rappelons qu'un monoïde S est appelé un ***filtre*** si $st \in S \Rightarrow s \in S$. Le filtre engendré par un monoïde S est obtenu en rajoutant tous les éléments qui divisent un élément de S. On obtient ainsi le ***saturé*** de S, noté S^{sat}. Enfin, un filtre S est dit ***premier*** lorsqu'il vérifie

$$x + y \in S \Rightarrow x \in S \text{ ou } y \in S.$$

En mathématiques classiques les filtres premiers sont exactement les complémentaires des idéaux premiers.

Le contenu constructif dans la démonstration usuelle du lemme de Krull est le lemme suivant.

2.2. Lemme. (Lemme de Krull : version constructive)
Soit (I, U) *un premier idéal et* x *un élément de* $\mathbf{A}$*. Si* $(I, x; U)$ *et* $(I; x, U)$ *collapsent, alors* (I, U) *collapse.*

Démonstration. On note $\mathfrak{a}$ (resp. S) l'idéal (resp. le monoïde) engendré par I (resp. par U). Il suffit alors d'appliquer le lemme 4.1 avec l'anneau $S^{-1}(\mathbf{A}/\mathfrak{a})$. On obtiendra à peu près le calcul suivant.
Les éléments de $\mathfrak{a}$ sont notés a avec un indice, ceux de S, s avec un indice. Par hypothèse, on a $a_1 + bx = s_1$ et $a_2 = x^n s_2$. On élimine x :

$$(bx)^n s_2 = b^n a_2 = a_3 \quad \text{et} \quad (bx)^n = (s_1 - a_1)^n = s_1^n + a_4$$

d'où $a_3 = s_2(s_1^n + a_4) = s_3 + a_5$ et enfin $0 = s_3 + a_5 - a_3 = s_3 + a_6$. □

À partir de ce lemme, on montre facilement les trois résultats suivants. *On suppose que* (I, U) *est un premier idéal compatible.*

1. *Si* (J, V) *est un premier idéal maximal parmi les premiers idéaux compatibles qui raffinent* (I, U)*,* J *est un idéal premier et* V *est son complémentaire.*
2. *Si* J *est un idéal maximal parmi les idéaux compatibles avec* U*,* J *est un idéal premier.*
3. *Si* V *est un filtre maximal parmi les filtres compatibles avec* I*,* V *est un filtre premier.*

Enfin, en mathématiques classiques, on en déduit le lemme 2.1 (et des variantes un peu plus sophistiquées, vu les trois résultats ci-dessus) en utilisant le principe du tiers exclu et le lemme de Zorn.

22. On pourrait aussi utiliser la terminologie « idéal premier potentiel », ou encore « idéal premier approché. »

Voici une version constructive sophistiquée.

2.3. Proposition et définition.
(Lemme de Krull avec précisions en mathématiques constructives)
Soit dans un anneau $\mathbf{A}$ *un premier idéal* $\mathfrak{P} = (I;U)$. *Soit* $\mathfrak{a}$ *l'idéal engendré par* I, S *le monoïde engendré par* U *et* $\mathbf{B} = (S^{-1}\mathbf{A})_{\mathrm{red}}$. *Soit enfin* $\lambda : \mathbf{A} \to \mathbf{B}$ *le morphisme canonique.*
On définit

$$\mathrm{idsat}_U(I) = \{\, x \in \mathbf{A} \mid (I; x, U) \text{ collapse} \,\}$$

et

$$\mathrm{monsat}_I(U) = \{\, x \in \mathbf{A} \mid (I, x; U) \text{ collapse} \,\}.$$

On note $\mathrm{sat}(\mathfrak{P}) = (\mathrm{idsat}_U(I), \mathrm{monsat}_I(U))$, *on l'appelle le* ***premier idéal saturé de*** $\mathfrak{P}$. *On a les résultats suivants :*

- $\mathrm{idsat}_U(I)$ *est l'idéal radical* $\lambda^{-1}(0_{\mathbf{B}})$;
- $\mathrm{monsat}_I(U)$ *est le filtre* $\lambda^{-1}(\mathbf{B}^\times) = (\mathfrak{a} + S)^{\mathrm{sat}}$;
- $\mathrm{sat}(\mathrm{sat}(\mathfrak{P})) = \mathrm{sat}(\mathfrak{P})$;
- $\mathfrak{P}$ *collapse si, et seulement si,* $\mathrm{sat}(\mathfrak{P}) = (\mathbf{A}, \mathbf{A})$;
- $\mathfrak{P}$ *est saturé (i.e.* $\mathfrak{P} = \mathrm{sat}(\mathfrak{P})$*) si, et seulement si, on a :*
  - I *est un idéal radical ;*
  - U *est un filtre ;*
  - $I + U = U$ *(si* $s + x \in U$ *et* $x \in I$, *alors* $s \in U$*) ;*
  - *si* $sx \in I$ *et* $s \in U$, *alors* $x \in I$.

Notons que pour un monoïde S on a $S^{\mathrm{sat}} = \mathrm{monsat}_{\{0\}}(S)$, et pour un idéal $\mathfrak{a}$ on a $\sqrt{\mathfrak{a}} = \mathrm{idsat}_{\{1\}}(\mathfrak{a})$

Commentaire. Le lemme 2.1 n'est pas constructif. Par hypthèse l'anneau $S^{-1}\mathbf{A}/\mathfrak{a}$ est non trivial, et l'on demande un idéal premier dans cet anneau, mais le «contre exemple» après le théorème 4.3, peut être modifé pour nous donner un quotient non nul de $\mathbb{Z}/15\mathbb{Z}$ dans lequel on ne sait pas construire d'idéal premier : on part de $\mathbb{Z}/15\mathbb{Z}$ au lieu de $\mathbb{Z}$. Une conjecture du type de celle de Riemann donne une fonction calculable $f : \mathbb{N} \to \{0, 1\}$ partout nulle, tant que la conjecture est vérifiée, jusqu'au moment où elle est infirmée (si elle l'est un jour). Si cette éventualité se produit la première fois pour $f(n)$ avec n pair, on met 3 dans l'idéal $\mathfrak{a}$, si c'est avec n impair, on met 5 dans l'idéal. Fournir un idéal premier dans l'anneau quotient revient à prédire si la conjecture sera infirmée pour n pair ou impair (si elle est infirmée). ∎

Lemme de Krull pour une chaine de longueur 1. Étant donnés deux premiers idéaux $\mathfrak{P}_0 = (I_0, U_0)$ et $\mathfrak{P}_1 = (I_1, U_1)$, à quelle condition peut-on les considérer comme des approximations d'idéaux premiers $\mathfrak{p}_0$ et $\mathfrak{p}_1$ vérifiant $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$?

C'est à cette question que répond la version généralisée suivante du lemme de Krull.

2.4. Lemme*. (Lemme de Krull pour une chaine de longueur 1)
Soient $\mathfrak{a}_i$ *deux idéaux et* S_i *deux monoïdes (*$i = 0, 1$*). Pour qu'il existe deux idéaux premiers* $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$ *vérifiant* $\mathfrak{a}_i \subseteq \mathfrak{p}_i$, $S_i \subseteq \mathbf{A} \setminus \mathfrak{p}_i$, *il faut et suffit que*

$$0 \notin \mathfrak{a}_0 + S_0(\mathfrak{a}_1 + S_1).$$

NB : l'inclusion $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$ est certainement stricte lorsque l'on a un $x \in \mathfrak{a}_1 \cap S_0$.

Un étape élémentaire de la «construction» de $\mathfrak{p}_0$ et $\mathfrak{p}_1$ en mathématiques classiques est gérée par un calcul qui représente le contenu constructif du lemme. C'est la première partie de la proposition 2.6.

2.5. Définition.
Si $\mathfrak{P}_0 = (I_0, U_0)$ et $\mathfrak{P}_1 = (I_1, U_1)$ sont deux premiers idéaux de $\mathbf{A}$, nous disons que $(\mathfrak{P}_0, \mathfrak{P}_1)$ une ***chaîne idéale de longueur*** 1 dans $\mathbf{A}$.
Nous disons qu'une telle chaîne idéale ***collapse*** lorsque

$$0 \in \mathfrak{a}_0 + S_0(\mathfrak{a}_1 + S_1), \text{ où } \mathfrak{a}_i = \langle I_i \rangle \text{ et } S_i = \mathcal{M}(U_i).$$

Nous disons que $\mathfrak{P}_1$ ***contient*** $\mathfrak{P}_0$, ce que l'on note $\mathfrak{P}_0 \leqslant \mathfrak{P}_1$, lorsque $I_0 \subseteq I_1$ et $U_1 \subseteq U_0$.
Nous disons que la chaîne idéale $\mathfrak{C}' = \big((J_0, V_0), (J_1, V_1)\big)$ ***raffine*** la chaîne idéale $\mathfrak{C} = \big((I_0, U_0), (I_1, U_1)\big)$, ce que l'on note $\mathfrak{C} \preccurlyeq \mathfrak{C}'$, si $J_i \supseteq I_i$ et $V_i \supseteq U_i$ pour chaque i.

2.6. Proposition et définition. (Lemme de Krull pour une chaine de longueur 1, version constructive) *Soient $\mathfrak{P}_i = (I_i, U_i)$ deux premiers idéaux ($i = 0, 1$) et $x \in \mathbf{A}$. Considérons la chaîne idéale $\mathfrak{C} = (\mathfrak{P}_0, \mathfrak{P}_1)$.*
(Lemme de Krull)

1. *Si les chaînes idéales $\big((I_0, x; U_0), \mathfrak{P}_1\big)$ et $\big((I_0; x, U_0), \mathfrak{P}_1\big)$ collapsent, alors $\mathfrak{C}$ collapse.*
2. *Si les chaînes idéales $\big(\mathfrak{P}_0, (I_1, x; U_1)\big)$ et $\big(\mathfrak{P}_0, (I_1; x, U_1)\big)$ collapsent, alors $\mathfrak{C}$ collapse.*

(Compléments) *Notons*
- $J_0 = \big\{\, x \mid \big((I_0; x, U_0), \mathfrak{P}_1\big)$ *collapse* $\big\}$;
- $V_0 = \big\{\, x \mid \big((I_0, x; U_0), \mathfrak{P}_1\big)$ *collapse* $\big\}$;
- $J_1 = \big\{\, x \mid \big(\mathfrak{P}_0, (I_1; x, U_1)\big)$ *collapse* $\big\}$;
- $V_1 = \big\{\, x \mid \big(\mathfrak{P}_0, (I_1, x; U_1)\big)$ *collapse* $\big\}$;
- $\mathrm{sat}(\mathfrak{C}) = \big((J_0, V_0), (J_1, V_1)\big)$.

La chaîne idéale $\mathrm{sat}(\mathfrak{C})$ *est appelée la* ***chaîne idéale saturée de*** $\mathfrak{C}$. *On a les résultats suivants :*
- $\mathrm{sat}(\mathrm{sat}(\mathfrak{C})) = \mathrm{sat}(\mathfrak{C})$;
- $\mathfrak{C}$ *collapse si, et seulement si,* $\mathrm{sat}(\mathfrak{C}) = \big((\mathbf{A}, \mathbf{A}), (\mathbf{A}, \mathbf{A})\big)$;
- $\mathfrak{C}$ *est* ***saturée*** *(i.e. $\mathfrak{C} = \mathrm{sat}(\mathfrak{C})$) si, et seulement si, on a :*
  - *chaque $\mathfrak{P}_i$ est un premier idéal saturé ;*
  - $\mathfrak{P}_0 \leqslant \mathfrak{P}_1$.

Nous notons $\mathsf{Kdim}\,\mathbf{A}$ la dimension de Krull de l'anneau $\mathbf{A}$. On s'intéresse à la question suivante en mathématiques classiques : $\mathsf{Kdim}\,\mathbf{A} \geqslant 1$? Autrement dit, existe-t-il une chaine d'idéaux premiers longueur 1, avec inclusion stricte ? Il faut pour cela avoir un élément x qui appartient au grand idéal premier et qui n'appartient pas au petit.
Cela revient à dire que la chaîne idéale $\mathfrak{C}\big((0; x), (x; 1)\big)$ peut être raffinée en une chaine d'idéaux premiers, i.e. qu'elle ne collapse pas. Cela donne :

$$\exists x \in \mathbf{A},\ 0 \notin x^{\mathbb{N}}(1 + \langle x \rangle)$$

On pourra donc prendre en mathématiques constructives la définition élémentaire suivante, dans laquelle on évite la négation ainsi que toute allusion aux idéaux premiers

$$\mathsf{Kdim}\,\mathbf{A} \leqslant 0 \overset{\text{def}}{\iff} \forall x \in \mathbf{A},\ \exists y \in \mathbf{A},\ n \in \mathbb{N},\ x^n(1 + yx) = 0.$$

Et l'on retrouve la définition que nous avons déjà donnée (sans justification) pour les anneaux zéro-dimensionnels.

Voyons ensuite quelle est la chaîne idéale saturée de $\mathfrak{C}$. C'est une chaîne idéale $\big((J_0, V_0), (J_1, V_1)\big)$ dans laquelle

$$V_0 = \big(x^{\mathbb{N}}(1 + \langle x \rangle)\big)^{\mathrm{sat}} \quad \text{et} \quad J_1 = \sqrt{\langle x \rangle + (\mathrm{D}_{\mathbf{A}}(0) : x)}.$$

Et ce n'est pas une coïncidence si nous voyons que l'idéal J_1 est à radical près l'idéal bord de Krull que nous avons introduit de manière heuristique à a fin de la section 1. Quant au monoïde $x^{\mathbb{N}}(1 + \langle x \rangle)$, il jouera un rôle « dual » de celui joué par l'idéal bord.

Lemme de Krull pour une chaine de longueur r. Nous donnons seulement ici la généralisation du lemme* 2.4.

2.7. Lemme*. (Lemme de Krull pour une chaine de longueur r)
Soient $r+1$ idéaux $\mathfrak{a}_i$ et $r+1$ monoïdes S_i ($i = 0, \ldots, r+1$). Pour qu'il existe $r+1$ idéaux premiers $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_{r+1}$ vérifiant $\mathfrak{a}_i \subseteq \mathfrak{p}_i$, $S_i \subseteq \mathbf{A} \setminus \mathfrak{p}_i$, il faut et suffit que

$$0 \notin \mathfrak{a}_0 + S_0(\mathfrak{a}_1 + S_1(\cdots S_r(\mathfrak{a}_{r+1} + S_{r+1}))).$$

Nous laissons à la lectrice le soin d'imaginer et de formuler précisément la version constructive de ce lemme, en analogie avec 2.6.

Ceci termine les deux premières sections dont le but essentiel était de motiver la définition constructive de la dimension de Krull.

3. Définition constructive de la dimension de Krull

3.1. Définition. Soient $\mathbf{A}$ un anneau commutatif, $x \in \mathbf{A}$ et $\mathfrak{a}$ un idéal de type fini.

(1) Le ***bord supérieur de Krull*** de $\mathfrak{a}$ dans $\mathbf{A}$ est l'anneau quotient

$$\mathbf{A}_{\mathrm{K}}^{\mathfrak{a}} := \mathbf{A}/\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(\mathfrak{a}) \quad \text{où} \quad \mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(\mathfrak{a}) := \mathfrak{a} + (\sqrt{0} : \mathfrak{a}). \tag{3.1}$$

On note $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x)$ pour $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(x\mathbf{A})$ et $\mathbf{A}_{\mathrm{K}}^{x}$ pour $\mathbf{A}_{\mathrm{K}}^{x\mathbf{A}}$. Cet anneau est appelé le *bord supérieur de x dans $\mathbf{A}$*.
On dira que $\mathcal{J}_{\mathbf{A}}^{\mathrm{K}}(\mathfrak{a})$ est ***l'idéal bord de Krull de $\mathfrak{a}$ dans $\mathbf{A}$.***

(2) Le ***bord inférieur de Krull*** de x dans $\mathbf{A}$ est l'anneau localisé

$$\mathbf{A}_{x}^{\mathrm{K}} := \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)^{-1}\mathbf{A} \quad \text{où} \quad \mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x) = x^{\mathbb{N}}(1 + x\mathbf{A}). \tag{3.2}$$

On dira que $\mathcal{S}_{\mathbf{A}}^{\mathrm{K}}(x)$ est le ***monoïde bord de Krull de*** x dans $\mathbf{A}$.

Rappelons qu'en mathématiques classiques la dimension de Krull d'un anneau est -1 si, et seulement si, l'anneau n'admet pas d'idéal premier, ce qui signifie qu'il est trivial.

Le théorème suivant donne alors en mathématiques classiques une caractérisation inductive élémentaire de la dimension de Krull d'un anneau commutatif.

3.2. Théorème*. *Pour un anneau commutatif $\mathbf{A}$ et un entier $k \geqslant 0$ les propriétés suivantes sont équivalentes.*

1. *La dimension de Krull de $\mathbf{A}$ est $\leqslant k$.*
2. *Pour tout $x \in \mathbf{A}$ la dimension de Krull de $\mathbf{A}_{\mathrm{K}}^{x}$ est $\leqslant k-1$.*
3. *Pour tout $x \in \mathbf{A}$ la dimension de Krull de $\mathbf{A}_{x}^{\mathrm{K}}$ est $\leqslant k-1$.*

En mathématiques constructives on remplace la définition usuellement donnée en mathématiques classiques par la définition plus élémentaire suivante.

3.3. Définition. La ***dimension de Krull*** (notée Kdim) d'un anneau commutatif $\mathbf{A}$ est définie par récurrence comme suit :

1. $\mathsf{Kdim}\,\mathbf{A} = -1$ si, et seulement si, $\mathbf{A}$ est trivial.
2. Pour $k \geqslant 0$, $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ signifie : $\forall x \in \mathbf{A}$, $\mathsf{Kdim}(\mathbf{A}_{x}^{\mathrm{K}}) \leqslant k-1$.

Exemples.
1) Si x est nilpotent ou inversible dans $\mathbf{A}$, l'idéal et le monoïde bords de x dans $\mathbf{A}$ sont tous deux égaux à $\mathbf{A}$. Les deux anneaux bords sont triviaux.

2) Pour $x \neq 0, 1, -1$ dans $\mathbb{Z}$, les anneaux bords $\mathbb{Z}_{\mathrm{K}}^{x} = \mathbb{Z}/x\mathbb{Z}$ et $\mathbb{Z}_{x}^{\mathrm{K}} = \mathbb{Q}$ sont zéro-dimensionnels. On retrouve donc que $\mathsf{Kdim}\,\mathbb{Z} \leqslant 1$.

3) Soit $\mathbf{K}$ un corps contenu dans un corps algébriquement clos discret $\mathbf{L}$. Soient $\mathfrak{a}$ un idéal de type fini de $\mathbf{K}[X_1, \ldots, X_n]$ et $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_n]/\mathfrak{a}$. Soient V la variété affine correspondant à $\mathfrak{a}$ dans $\mathbf{L}^n$, W la sous-variété de V définie par f. Alors le « bord de W dans V », défini comme l'intersection de W avec la clôture de Zariski de son complémentaire dans V, est la variété affine correspondant à l'anneau $\mathbf{A}_{\mathrm{K}}^{f}$. De manière abrégée :

$$\mathrm{bord}_V\, \mathcal{Z}(f) = \mathcal{Z}_V(\text{idéal bord de } f).$$

4) Soit $\mathbf{A}$ intègre et $k \geqslant 0$: $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ équivaut à $\mathsf{Kdim}(\mathbf{A}/a\mathbf{A}) \leqslant k-1$ pour tout a régulier.

5) Soit $\mathbf{A}$ local résiduellement discret et $k \geqslant 0$: $\mathsf{Kdim}\,\mathbf{A} \leqslant k$ équivaut à $\mathsf{Kdim}\,\mathbf{A}[1/a] \leqslant k-1$ pour tout $a \in \mathrm{Rad}\,\mathbf{A}$. ∎

3.4. Définition. Une suite $(x_0, \ldots, x_k)$ dans $\mathbf{A}$ est dite ***singulière*** s'il existe $a_0, \ldots, a_k \in \mathbf{A}$ et $m_0, \ldots, m_k \in \mathbb{N}$ tels que

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_k^{m_k}(1 + a_k x_k) + \cdots) + a_1 x_1) + a_0 x_0) = 0 \tag{3.3}$$

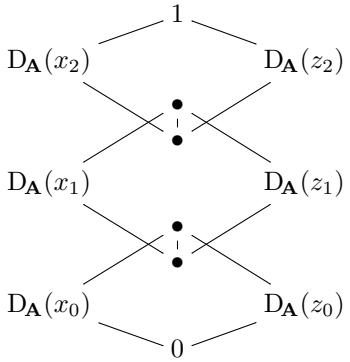
3.5. Proposition. *Pour un anneau commutatif $\mathbf{A}$ et un entier $k \geqslant 0$, les propriétés suivantes sont équivalentes.*

1. *Pour tout $x \in \mathbf{A}$ la dimension de Krull de $\mathbf{A}_{x}^{\mathrm{K}}$ est $\leqslant k-1$.*
2. *Pour tout $x \in \mathbf{A}$ la dimension de Krull de $\mathbf{A}_{\mathrm{K}}^{x}$ est $\leqslant k-1$.*
3. *Toute suite $(x_0, \ldots, x_k)$ dans $\mathbf{A}$ est singulière.*

4. Pour tous $x_0, \ldots, x_k \in \mathbf{A}$ *il existe* $z_0, \ldots, z_k \in \mathbf{A}$ *tels que*

$$\left.\begin{array}{rcl} \mathrm{D}_{\mathbf{A}}(z_0x_0) & = & \mathrm{D}_{\mathbf{A}}(0) \\ \mathrm{D}_{\mathbf{A}}(z_1x_1) & \leqslant & \mathrm{D}_{\mathbf{A}}(z_0, x_0) \\ \vdots & \vdots & \vdots \\ \mathrm{D}_{\mathbf{A}}(z_kx_k) & \leqslant & \mathrm{D}_{\mathbf{A}}(z_{k-1}, x_{k-1}) \\ \mathrm{D}_{\mathbf{A}}(1) & = & \mathrm{D}_{\mathbf{A}}(z_k, x_k) \end{array}\right\} \tag{3.4}$$

Par exemple pour $k = 2$ le point *4* correspond au dessin suivant dans $\mathsf{Zar}\,\mathbf{A}$.



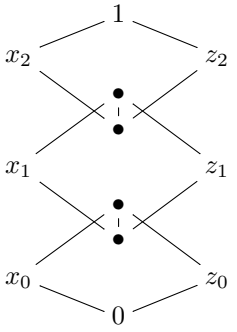
$$\mathrm{D}_{\mathbf{A}}(1) = \mathrm{D}_{\mathbf{A}}(z_2) \vee \mathrm{D}_{\mathbf{A}}(x_2).$$

$$\mathrm{D}_{\mathbf{A}}(z_2) \wedge \mathrm{D}_{\mathbf{A}}(x_2) \leqslant \mathrm{D}_{\mathbf{A}}(z_1) \vee \mathrm{D}_{\mathbf{A}}(x_1)$$

$$\mathrm{D}_{\mathbf{A}}(z_1) \wedge \mathrm{D}_{\mathbf{A}}(x_1) \leqslant \mathrm{D}_{\mathbf{A}}(z_0) \vee \mathrm{D}_{\mathbf{A}}(x_0)$$

$$\mathrm{D}_{\mathbf{A}}(z_0) \wedge \mathrm{D}_{\mathbf{A}}(x_0) = \mathrm{D}_{\mathbf{A}}(0)$$

Remarque. On définit de manière analogue la ***dimension de Krull d'un treillis distributif***. On peut la voir comme une définition élémentaire de la dimension de Krull d'un espace spectral en mathématiques classiques. Par exemple un treillis distributif est de dimension de Krull $\leqslant 2$ si, et seulement si, pour tous x_0, x_1, x_2, il existe z_0, z_1, z_2 réalisant le dessin suivant :



$$z_2 \vee x_2 = 1.$$

$$z_2 \wedge x_2 \leqslant z_1 \vee x_1$$

$$z_1 \wedge x_1 \leqslant z_0 \vee x_0$$

$$z_0 \wedge x_0 = 0$$

et l'on obtient que pour un anneau $\mathbf{A}$ on a $\mathsf{Kdim}(\mathbf{A}) = \mathsf{Kdim}(\mathsf{Zar}\,\mathbf{A})$ ∎

4. Théorèmes classiques sous forme constructive

La définition constructive de la dimension de Krull est un heureux événement pour les deux raisons suivantes.

– En pratique, on arrive à démontrer que la dimension de Krull de la plupart des anneaux qui interviennent dans la littérature satisfait la définition constructive au moyen d'une démonstration constructive.

– Les théorèmes des mathématiques classiques dans lesquels la dimension de Krull intervient de manière décisive, quand ils aboutissent à une conclusion de nature concrète, sont transformés en des théorèmes de mathématiques constructives[23], ce qui révèle un contenu concret satisfaisant pour le théorème abstrait de départ.

Un progrès décisif dans la compréhension des théorèmes dont nous allons rendre compte a été accompli par Heitmann [15] qui a montré comment se débarrasser des hypothèses noethériennes pour les théorèmes avec la dimension de Krull.

Un autre progrès décisif a été accompli par T. Coquand qui a montré comment obtenir tous les résultats classiques, parfois sous une forme améliorée du point de vue des mathématiques classiques, au moyen de démonstrations à la fois constructives et élémentaires.

23. Il s'agit d'un fait d'expérience et non d'un métathéorème.

Un théorème de Kronecker. Le lemme suivant, bien que terriblement anodin, est une clef essentielle.

4.1. Lemme. *Pour $u, v \in \mathbf{A}$ on a*

$$\mathrm{D}_{\mathbf{A}}(u,v) = \mathrm{D}_{\mathbf{A}}(u+v, uv) = \mathrm{D}_{\mathbf{A}}(u+v) \vee \mathrm{D}_{\mathbf{A}}(uv)\ .$$

En particulier, si $uv \in \mathrm{D}_{\mathbf{A}}(0)$, alors $\mathrm{D}_{\mathbf{A}}(u,v) = \mathrm{D}_{\mathbf{A}}(u+v)$.

Démonstration. On a l'inclusion évidente $\langle u+v, uv\rangle \subseteq \langle u, v\rangle$, ce qui donne $\mathrm{D}_{\mathbf{A}}(u+v, uv) \subseteq \mathrm{D}_{\mathbf{A}}(u,v)$. Par ailleurs, $u^2 = (u+v)u - uv \in \langle u+v, uv\rangle$, ce qui donne $u \in \mathrm{D}_{\mathbf{A}}(u+v, uv)$. □

Nous disons que deux suites qui vérifient les inégalités (3.4) dans la proposition 3.5 sont ***complémentaires***.

4.2. Lemme. *Soit $\ell \geqslant 1$. Si $(x_1, \ldots, x_\ell)$ et $(z_1 \ldots, z_\ell)$ sont deux suites complémentaires dans $\mathbf{A}$ alors pour tout $a \in \mathbf{A}$ on a :*

$$\mathrm{D}_{\mathbf{A}}(a, x_1, \ldots, x_\ell) = \mathrm{D}_{\mathbf{A}}(x_1 + az_1, \ldots, x_\ell + az_\ell),$$

c'est-à-dire encore : $a \in \mathrm{D}_{\mathbf{A}}(x_1 + az_1, \ldots, x_\ell + az_\ell)$.

Démonstration. On a les inégalités

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(x_1z_1) &= \mathrm{D}_{\mathbf{A}}(0)\\
\mathrm{D}_{\mathbf{A}}(x_2z_2) &\leqslant \mathrm{D}_{\mathbf{A}}(x_1, z_1)\\
&\vdots\ \vdots\ \vdots\\
\mathrm{D}_{\mathbf{A}}(x_\ell z_\ell) &\leqslant \mathrm{D}_{\mathbf{A}}(x_{\ell-1}, z_{\ell-1})\\
\mathrm{D}_{\mathbf{A}}(1) &= \mathrm{D}_{\mathbf{A}}(x_\ell, z_\ell).
\end{aligned}$$

On en déduit celles-ci

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(az_1x_1) &= \mathrm{D}_{\mathbf{A}}(0)\\
\mathrm{D}_{\mathbf{A}}(az_2x_2) &\leqslant \mathrm{D}_{\mathbf{A}}(az_1, x_1)\\
&\vdots\ \vdots\ \vdots\\
\mathrm{D}_{\mathbf{A}}(az_\ell x_\ell) &\leqslant \mathrm{D}_{\mathbf{A}}(az_{\ell-1}, x_{\ell-1})\\
\mathrm{D}_{\mathbf{A}}(a) &\leqslant \mathrm{D}_{\mathbf{A}}(az_\ell, x_\ell).
\end{aligned}$$

On a donc d'après le lemme 4.1

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(a) &\leqslant \mathrm{D}_{\mathbf{A}}(az_\ell + x_\ell) \vee \mathrm{D}_{\mathbf{A}}(az_\ell x_\ell)\\
\mathrm{D}_{\mathbf{A}}(az_\ell x_\ell) &\leqslant \mathrm{D}_{\mathbf{A}}(az_{\ell-1} + x_{\ell-1}) \vee \mathrm{D}_{\mathbf{A}}(az_{\ell-1}x_{\ell-1})\\
&\vdots\ \vdots\ \vdots\\
\mathrm{D}_{\mathbf{A}}(az_3x_3) &\leqslant \mathrm{D}_{\mathbf{A}}(az_2 + x_2) \vee \mathrm{D}_{\mathbf{A}}(az_2x_2)\\
\mathrm{D}_{\mathbf{A}}(az_2x_2) &\leqslant \mathrm{D}_{\mathbf{A}}(az_1 + x_1) \vee \mathrm{D}_{\mathbf{A}}(az_1x_1) = \mathrm{D}_{\mathbf{A}}(az_1 + x_1).
\end{aligned}$$

Donc finalement

$$\begin{aligned}
\mathrm{D}_{\mathbf{A}}(a) &\leqslant \mathrm{D}_{\mathbf{A}}(az_1 + x_1) \vee \mathrm{D}_{\mathbf{A}}(az_2 + x_2) \vee \cdots \vee \mathrm{D}_{\mathbf{A}}(az_\ell + x_\ell)\\
&= \mathrm{D}_{\mathbf{A}}(az_1 + x_1, az_2 + x_2, \ldots, az_\ell + x_\ell).
\end{aligned}$$

□

4.3. Théorème. (Théorème de Kronecker-Heitmann, avec la dimension de Krull, sans noethérianité)

1. *Soit $n \geqslant 0$. Si $\mathsf{Kdim}\,\mathbf{A} < n$ et x_1, …, $x_n \in \mathbf{A}$, il existe z_1, …, z_n tels que pour tout $a \in \mathbf{A}$, $\mathrm{D}_{\mathbf{A}}(a, x_1, \ldots, x_n) = \mathrm{D}_{\mathbf{A}}(x_1 + az_1, \ldots, x_n + az_n)$.*
2. *En conséquence, dans un anneau de dimension de Krull $\leqslant n$, tout idéal de type fini a même nilradical qu'un idéal engendré par au plus $n+1$ éléments.*

Démonstration. 1. Clair d'après le lemme 4.2 et la proposition 3.5 (si $n = 0$, l'anneau est trivial et $\mathrm{D}_{\mathbf{A}}(a) = \mathrm{D}_{\mathbf{A}}(\emptyset)$).
2. Découle de *1* car il suffit d'itérer le processus. En fait, si $\mathsf{Kdim}\,\mathbf{A} \leqslant n$ et $\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(x_1, \ldots, x_{n+r})$ ($r \geqslant 2$), on obtient en fin de compte

$$\mathfrak{a} = \mathrm{D}_{\mathbf{A}}(x_1 + y_1, \ldots, x_{n+1} + y_{n+1})$$

avec les $y_i \in \langle x_{n+2}, \ldots, x_{n+r}\rangle$. □

La signification géométrique du théorème énoncé par Kronecker pour l'anneau $\mathbf{K}[X_1, \ldots, X_n]$ est que toute variété algébrique (en n variables) peut être définie par seulement $n+1$ équations.

Une autre conséquence immédiate du lemme 4.2 est un théorème de Bass.

4.4. Théorème. (Théorème de Bass, avec la dimension de Krull, sans noethérianité) *Si* $\mathsf{Kdim}\,\mathbf{A} < n$, *pour tous* x_1, …, $x_n \in \mathbf{A}$, *il existe des* z_i *tels que l'implication suivante soit satisfaite :*

$$\forall a \in \mathbf{A} \quad (1 \in \langle a, x_1, \ldots, x_n\rangle \Rightarrow 1 \in \langle x_1 + az_1, \ldots, x_n + az_n\rangle).$$

Par suite, tout $\mathbf{A}$*-module stablement libre de rang* $\geqslant n$ *est libre.*

Théorèmes de Serre et de Forster. La démonstration des énoncés 4.6 et 4.7 est nettement plus sophistiquée que celle du théorème de Kronecker. Malgré leurs énoncés assez abstraits, ces résultats sont réalisés concrètement par des manipulations élémentaires de matrices. En fait le théorème crucial est le suivant. D'où l'on déduit les théorèmes de Serre et de Forster. En outre, il se démontre constructivement aussi avec la dimension de Heitmann.

4.5. Théorème. (Coquand) *On suppose* $\mathsf{Kdim}\,\mathbf{A} < n$. *Soit une matrice*

$$F = [\,C_0 \,|\, C_1 \,|\, \ldots \,|\, C_p\,], \quad \textit{(les } C_i \textit{ sont les colonnes).}$$

Notons $G = [\,C_1 \,|\, \ldots \,|\, C_p\,]$ *et supposons que* $1 \in \mathcal{D}_1(C_0) + \mathcal{D}_n(G)$.
Un algorithme donne une combinaison linéaire $C_0 + \sum_{i\in[\![1..p]\!]} a_i C_i$, *qui est unimodulaire.*

Nous disons qu'une matrice A est ***de rang*** $\geqslant k$ si l'idéal déterminantiel d'ordre k, $\mathcal{D}_k(A)$, est égal à $\mathbf{A}$.

Un module de présentation finie est dit ***localement engendré par*** r ***éléments***, si $\mathcal{F}_r(M) = \mathbf{A}$. Autrement dit, si $M \simeq \operatorname{Coker} A$, avec $A \in \mathbb{M}_{q,p}(\mathbf{A})$, alors A est de rang $\geqslant q - r$.

4.6. Théorème. (Splitting off de Serre pour la Kdim, sans noethérianité) *Soit* $k \geqslant 0$ *et* $r \geqslant 1$. *Supposons que* $\mathsf{Kdim}\,\mathbf{A} \leqslant k$.
Soit M *un* $\mathbf{A}$*-module projectif de rang* $k+r$. *Alors* $M \simeq N \oplus \mathbf{A}^r$ *pour un certain module* N *projectif de rang* k.
Plus généralement supposons que M *est isomorphe à l'image d'une matrice de rang* $\geqslant k+r$. *Alors* $M \simeq N \oplus \mathbf{A}^r$ *pour un certain module* N *isomorphe à l'image d'une matrice de rang* $\geqslant k$.

Le théorème suivant a été démontré en mathématiques classiques par Forster [14] en supposant l'anneau noethérien. Le version sans hypothèse noethérienne est due à Heitmann [15].

4.7. Théorème. (Théorème de Forster-Heitmann pour la Kdim, sans noethérianité) *Soit* $k \geqslant 0$ *et* $r \geqslant 1$. *Supposons que* $\mathsf{Kdim}\,\mathbf{A} \leqslant k$. *Soit* M *un* $\mathbf{A}$*-module de type fini localement engendré par* r *éléments. Alors* M *est engendré par* $k + r$ *éléments. Plus précisément, si* $M = \langle x_1, \ldots, x_{k+r+s}\rangle$, *on peut calculer*

$$z_1, \ldots, z_{k+r} \in \langle x_{k+r+1}, \ldots, x_{k+r+s}\rangle$$

tels que M *soit engendré par* $(x_1 + z_1, \ldots, x_{k+r} + z_{k+r})$.

Et le spectre maximal ? En mathématiques classiques, des versions des théorèmes précédents, dues pour l'essentiel à Richard Swan, sont obtenues dans le cadre des anneaux noethériens avec une dimension qui est parfois strictement inférieure à la dimension de Krull : la dimension du spectre maximal $\mathsf{Max}\,\mathbf{A}$. C'est aussi la dimension du « j-spectrum », qui est le sous-espace de $\mathsf{Spec}\,\mathbf{A}$ formé par les idéaux premiers qui sont intersections d'idéaux maximaux. Dans le cas noethérien, le j-spectrum est un espace spectral, mais pas dans le cas général.

Dans l'article [15], Heitmann introduit la dimension notée Jdim pour un anneau non nécessairement noethérien, en tant que bon substitut à la dimension du spectre maximal. C'est la dimension de $\mathsf{Jspec}\,\mathbf{A}$, le plus petit sous-espace spectral de $\mathsf{Spec}\,\mathbf{A}$ contenant $\mathsf{Max}\,\mathbf{A}$. Il établit le théorème « stable range » de Bass pour cette dimension. Par contre pour les théorèmes de Serre et de Forster-Swan, il doit utiliser une dimension ad hoc, la borne supérieure des $\mathsf{Jdim}(\mathbf{A}[1/x])$ pour les $x \in \mathbf{A}$. Comme cette dimension ad hoc est de toute manière majorée par la dimension de Krull, il obtient en particulier une version non noethérienne des grands théorèmes cités avec la dimension de Krull.

Une notion voisine, la dimension de Heitmann, notée Hdim, a été introduite dans [6] (voir aussi [7]). C'est elle au fond qui fait fonctionner les démonstrations dans l'article de Heitmann [15]. Le fait qu'elle soit a priori inférieure à la Jdim n'est pas le point essentiel. C'est bien plutôt le fait que

les théorèmes de Serre et de Forster-Swan passent pour la Hdim, et donc a fortiori pour la Jdim, ce qui donne la version non noethérienne complète de ces théorèmes, laquelle avait été conjecturée par Heitmann.
Dans le cas d'un anneau noethérien, la Hdim, la Jdim de Heitmann ainsi que la dimension du spectre maximal $\mathsf{Max}\,\mathbf{A}$ qui intervient dans les théorèmes de Serre et de Swan [30, 33] sont les mêmes (cf. [7, 15]).

Nous donnons maintenant les définitions du J-spectrum de Heitmann, puis celle de la dimension de Heitmann.

Le ***radical de Jacobson*** d'un anneau $\mathbf{A}$ est défini par

$$\mathrm{Rad}(\mathbf{A}) = \big\{\, x \in \mathbf{A} \mid 1 + x\mathbf{A} \subseteq \mathbf{A}^\times \,\big\}.$$

On démontre en mathématiques classiques que c'est l'intersection des idéaux maximaux, (au moyen d'une démonstration non constructive).

4.8. Définition et notation.

- Si $\mathfrak{a}$ est un idéal de $\mathbf{A}$ on note $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ son ***radical de Jacobson***, c'est-à-dire l'image réciproque de $\mathrm{Rad}(\mathbf{A}/\mathfrak{a})$ par la projection canonique $\mathbf{A} \to \mathbf{A}/\mathfrak{a}$.
- Si $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$ on notera $\mathrm{J}_{\mathbf{A}}(x_1, \ldots, x_n)$ pour $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$. En particulier, $\mathrm{J}_{\mathbf{A}}(0) = \mathrm{Rad}\,\mathbf{A}$.
- On note $\mathsf{Heit}\,\mathbf{A}$ l'ensemble des idéaux $\mathrm{J}_{\mathbf{A}}(x_1, \ldots, x_n)$. On l'appelle le ***treillis de Heitmann*** de l'anneau $\mathbf{A}$.
- On définit $\mathsf{Jdim}\,\mathbf{A}$ comme égale à $\mathsf{Kdim}(\mathsf{Heit}\,\mathbf{A})$.

On a donc $x \in \mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ si, et seulement si, pour tout $y \in \mathbf{A}$, $1 + xy$ est inversible modulo $\mathfrak{a}$. Autrement dit encore

$$x \in \mathrm{J}_{\mathbf{A}}(\mathfrak{a}) \iff 1 + x\mathbf{A} \subseteq (1 + \mathfrak{a})^{\mathrm{sat}},$$

et $\mathrm{J}_{\mathbf{A}}(\mathfrak{a})$ est le plus grand idéal $\mathfrak{b}$ tel que $1 + \mathfrak{b} \subseteq (1 + \mathfrak{a})^{\mathrm{sat}}$.
On a donc $\big(1 + \mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big)^{\mathrm{sat}} = (1 + \mathfrak{a})^{\mathrm{sat}}$ et $\mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big) = \mathrm{J}_{\mathbf{A}}(\mathfrak{a})$.
En particulier $\mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(0)\big) = \mathrm{J}_{\mathbf{A}}(0)$ et l'anneau $\mathbf{A}/\mathrm{Rad}\,\mathbf{A}$ a son radical de Jacobson réduit à 0.

Le lemme suivant montre une analogie certaine avec le lemme 4.1, et donne une idée de la raison pour laquelle on arrive à remplacer la Kdim par la Jdim dans les théorèmes de Serre et de Forster.

4.9. Lemme.

1. *Pour un idéal arbitraire* $\mathfrak{a}$ *on a* $\mathrm{J}_{\mathbf{A}}(\mathfrak{a}) = \mathrm{J}_{\mathbf{A}}\big(\mathrm{D}_{\mathbf{A}}(\mathfrak{a})\big) = \mathrm{J}_{\mathbf{A}}\big(\mathrm{J}_{\mathbf{A}}(\mathfrak{a})\big)$.
   En conséquence, $\mathsf{Heit}\,\mathbf{A}$ *est un treillis distributif quotient de* $\mathsf{Zar}\,\mathbf{A}$.
2. *Pour* $u, v \in \mathbf{A}$ *on a*
   $$\mathrm{J}_{\mathbf{A}}(u, v) \;=\; \mathrm{J}_{\mathbf{A}}(u + v, uv) \;=\; \mathrm{J}_{\mathbf{A}}(u + v) \vee \mathrm{J}_{\mathbf{A}}(uv).$$
   En particulier, si $uv \in \mathrm{J}_{\mathbf{A}}(0)$, *alors* $\mathrm{J}_{\mathbf{A}}(u, v) = \mathrm{J}_{\mathbf{A}}(u + v)$.

La définition de la dimension de Heitmann qui est donnée ci-après est assez naturelle, dans la mesure où elle mime la définition constructive de la dimension de Krull en remplaçant $\mathrm{D}_{\mathbf{A}}$ par $\mathrm{J}_{\mathbf{A}}$.

4.10. Définition. Soit $\mathbf{A}$ un anneau commutatif, $x \in \mathbf{A}$ et $\mathfrak{a}$ un idéal de type fini. Le *bord de Heitmann de* $\mathfrak{a}$ *dans* $\mathbf{A}$ est l'anneau quotient

$$\mathbf{A}_{\mathrm{H}}^{\mathfrak{a}} := \mathbf{A}\big/\mathcal{J}_{\mathbf{A}}^{\mathrm{H}}(\mathfrak{a})\,, \quad \text{où} \quad \mathcal{J}_{\mathbf{A}}^{\mathrm{H}}(\mathfrak{a}) := \mathfrak{a} + (\mathrm{J}_{\mathbf{A}}(0) : \mathfrak{a}).$$

Cet idéal est appelé *l'idéal bord de Heitmann de* $\mathfrak{a}$ *dans* $\mathbf{A}$.
On notera aussi $\mathcal{J}_{\mathbf{A}}^{\mathrm{H}}(x) := \mathcal{J}_{\mathbf{A}}^{\mathrm{H}}(x\mathbf{A})$ et $\mathbf{A}_{\mathrm{H}}^{x} := \mathbf{A}\big/\mathcal{J}_{\mathbf{A}}^{\mathrm{H}}(x)$.

4.11. Définition. La ***dimension de Heitmann*** de $\mathbf{A}$ est définie par récurrence comme suit :

- $\mathsf{Hdim}\,\mathbf{A} = -1$ si, et seulement si, $1_{\mathbf{A}} = 0_{\mathbf{A}}$.
- Soit $\ell \geqslant 0$, on définit :
  $$\mathsf{Hdim}\,\mathbf{A} \leqslant \ell \iff \text{pour tout } x \in \mathbf{A},\ \mathsf{Hdim}(\mathbf{A}_{\mathrm{H}}^{x}) \leqslant \ell - 1.$$

Cette dimension est inférieure ou égale à la Jdim définie par Heitmann dans [15], c'est-à-dire la dimension de Krull du treillis distributif $\mathsf{Heit}(\mathbf{A})$.

CHAPITRE 4

Idéaux premiers, minimaux, maximaux

Sommaire

Introduction

Ce chapitre est basé sur [ACMC, chapitre XV].

1. Idéaux premiers

Les idéaux premiers sont omniprésents en algèbre commutative moderne. On a déjà vu comme interpréter leur utilisation dans la dimension de Krull.

Il s'agissait pourtant seulement d'un exemple. Les idéaux premiers sont présents et semblent essentiels dans tout ce que l'on appelle le ***principe local-global*** en mathématiques classiques. Ce principe informel dit que les bonnes propriétés des anneaux ou des modules sont celles qui obéissent à la règle suivante :

• Forme usuelle d'un principe local-global abstrait. *La propriété est satisfaite si, et seulement si, elle est satisfaite après localisation en n'importe quel idéal premier*[24].

Il y a cependant des propriétés qui mériteraient d'être qualifiées de bonnes, comme le fait pour un module d'être de type fini ou cohérent, et qui n'obéissent pas à la règle ci-dessus, mais seulement à la règle suivante :

• Forme variante d'un principe local-global abstrait. *La propriété est satisfaite si, et seulement si, elle est satisfaite après localisation au voisinage de n'importe quel idéal premier.*

Dans la règle en question, « après localisation au voisinage de l'idéal premier $\mathfrak{P}$ » signifie qu'il existe un $s \notin \mathfrak{P}$ tel que la propriété est satisfaite pour le changement d'anneau de base $\mathbf{A} \to \mathbf{A}[1/s]$.

Dans la forme variante, la vérification de la propriété locale est plus délicate, car l'anneau $\mathbf{A}[1/s]$ n'est pas local, mais l'implication du local au global est plus facile à établir, et plus souvent satisfaite. Naturellement le lecteur aura noté que si une propriété stable par localisation est satisfaite après localisation au voisinage de tout idéal premier, elle est également satisfaite après localisation en tout idéal premier.

En fait cette deuxième forme de principe local-global est « la meilleure », car c'est elle qui permet de déclarer légitime le passage des « bonnes » propriétés des schémas affines aux schémas de Grothendieck. Par exemple la propriété pour un module d'être de présentation finie et cohérent

24. On voit souvent la variante : *après localisation en n'importe quel idéal maximal*, mais ce n'est pas une variante significative, la démonstration ne faisant jamais intervenir l'hypotèse « idéal maximal ».

vérifie la deuxième forme du principe local-global et c'est ce qui légitime la définition des « faisceaux de modules[25] cohérents ».

En mathématiques constructives, on a mis au point une contrepartie (une interprétation algorithmique) du principe local-global des mathématiques classiques sous forme de *théorèmes* appelés ***principes local-globals concrets*** d'une part, et d'une *méthode de décryptage* des démonstrations classiques, appelée ***machinerie locale-globale constructive de base***, ou encore ***machinerie locale-globale à idéaux premiers*** d'autre part. Nous allons expliquer ceci en détail, mais il est important de souligner ici qu'en mathématiques constructives, les démonstrations ne sont pas extérieures aux mathématiques mais font partie intégrante des mathématiques. C'est ce que l'on a déjà souligné avec le principe algorithmique « affirmer c'est prouver », principe qui conduit à renoncer à l'usage du tiers exclu.

1.1. Définition.

1. Des éléments $s_1, \ldots, s_n$ sont dits ***comaximaux*** si $\langle 1\rangle = \langle s_1, \ldots, s_n\rangle$. Deux éléments comaximaux sont aussi appelés ***étrangers***.
2. Des monoïdes $S_1, \ldots, S_n$ sont dits ***comaximaux*** si chaque fois que $s_1 \in S_1, \ldots, s_n \in S_n$, les s_i sont comaximaux.

Si $s_1, \ldots, s_n$ sont comaximaux, les monoïdes qu'ils engendrent sont comaximaux.

1.2. Définition. 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 $\{1\}$.

1.3. Définition et notation. 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 ***premier idéal***, et l'on note $\mathbf{A}_{\mathfrak{q}}$ 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* et le couple

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

est appelé un ***premier idéal fini***.

Le fait important à souligner est que, vues dans l'anneau $\mathbf{A}_{\mathfrak{q}}$, la partie U est contenue dans les unités et la partie I est contenue dans le radical de Jacobson.

C'est ce qui va permettre à notre décryptage constructif de fonctionner, car une fois que l'on aura forcé un élément à être dans le radical de Jacobson, il n'en sortira plus jamais.

Les exemples donnés dans le lemme suivant sont fréquents.

1.4. Lemme. *Soit $\mathbf{A}$ un anneau, U et I des parties de $\mathbf{A}$, et $S = \mathcal{S}(I,U)$.*

1. (Lemme de Krull constructif, variante)
   Pour tout $a \in \mathbf{A}$ les monoïdes $\mathcal{S}(I;U,a)$ et $\mathcal{S}(I,a;U)$ recouvrent le monoïde $\mathcal{S}(I,U)$. En particulier, les monoïdes $\mathcal{M}(a) = \mathcal{S}(0;a)$ et $\mathcal{S}(a;1) = 1 + a\mathbf{A}$ sont comaximaux.
   De même, si S, $S_1, \ldots, S_n \subseteq \mathbf{A}$ sont des monoïdes comaximaux et si $a \in \mathbf{A}$, alors les monoïdes $\mathcal{S}(I;U,a)$, $\mathcal{S}(I,a;U)$, $S_1, \ldots, S_n$ sont comaximaux.
2. *Si $s_1, \ldots, s_n \in \mathbf{A}$ sont des éléments comaximaux, les monoïdes $\mathcal{M}(s_i)$ sont comaximaux. Plus généralement, si $s_1, \ldots, s_n \in \mathbf{A}$ sont des éléments comaximaux dans $\mathbf{A}_S$, les monoïdes $\mathcal{S}(I;U,s_i)$ recouvrent le monoïde $S = \mathcal{S}(I,U)$.*
3. *Soient $s_1, \ldots, s_n \in \mathbf{A}$. Les monoïdes :*

$$S_1 = \mathcal{S}(0;s_1),\ S_2 = \mathcal{S}(s_1;s_2),\ S_3 = \mathcal{S}(s_1,s_2;s_3),\ \ldots,$$
$$S_n = \mathcal{S}(s_1,\ldots,s_{n-1};s_n) \text{ et } S_{n+1} = \mathcal{S}(s_1,\ldots,s_n;1)$$

25. Les faisceaux algébriques cohérents de Serre, à l'origine de l'histoire, sont localement « cohérents » au sens de Serre et Bourbaki, c'est-à-dire de présentation finie et cohérents dans la terminologie actuelle.

sont comaximaux.
Plus généralement, les monoïdes :

$$V_1 = \mathcal{S}(I; U, s_1),\ V_2 = \mathcal{S}(I, s_1; U, s_2),\ V_3 = \mathcal{S}(I, s_1, s_2; U, s_3),\ \ldots,$$
$$V_n = \mathcal{S}(I, s_1, \ldots, s_{n-1}; U, s_n) \text{ et } V_{n+1} = \mathcal{S}(I, s_1, \ldots, s_n; U)$$

recouvrent le monoïde $S = \mathcal{S}(I, U)$.

Principes local-globals concrets. Bien qu'intéressés par les principes local-globals concrets plutôt que par les principes local-globals abstraits, nous commençons par un paragraphe qui explique, en mathématiques classiques, les rapports étroits qui les relient.

Propriétés stables par localisation arbitraires. Le fait suivant est à peu près immédiat en mathématiques classiques.

1.5. Fait*. *Soit* P *une propriété stable par localisation (i.e. propriété qui reste vraie lorsque l'on fait un changement d'anneau de base* $\mathbf{A} \to \mathbf{A}_S$ *pour un monoïde* S*). Alors, en mathématiques classiques les propriétés suivantes sont équivalentes.*

1. *Il existe des éléments comaximaux tels que la propriété* P *soit vraie après localisation en chacun des éléments.*
2. *La propriété* P *est vraie après localisation au voisinage de tout idéal premier.*

1.6. Définition. Une propriété P concernant les anneaux commutatifs et les modules est dite ***de caractère fini*** si elle est conservée par localisation (par passage de $\mathbf{A}$ à $S^{-1}\mathbf{A}$) et si, lorsqu'elle est vérifiée avec $S^{-1}\mathbf{A}$, alors elle est vérifiée avec $\mathbf{A}[1/s]$ pour un certain $s \in S$.

1.7. Fait*. *Soit* P *une propriété de caractère fini. Alors, en mathématiques classiques les propriétés suivantes sont équivalentes.*

1. *Il existe des monoïdes comaximaux tels que la propriété* P *soit vraie après localisation en chacun des monoïdes.*
2. *La propriété* P *est vraie après localisation en tout idéal premier.*

Il s'ensuit que pour les propriétés qui sont de caractère fini, ou qui sont des conjonctions de propriétés de caractère fini, il revient au même en mathématiques classiques d'établir le principe local-global concret ou le principe local-global abstrait correspondant.

Mais comme nous voulons des démonstrations constructives nous ne démontrerons (et ne pourrons démontrer) que la version concrète. L'important pour nous est que le principe concret permet d'aboutir aux mêmes conclusions que celles obtenues avec le principe abstrait lorsque celles-ci ont a priori un contenu concret.

Pour les propriétés qui ne sont pas de caractère fini ni conjonctions de propriétés de caractère fini, il faut a priori faire appel en mathématiques classiques à la localisation au voisinage de tout idéal premier, et en mathématiques constructives, parfois, se restreindre à la localisation en des éléments comaximaux plutôt qu'en des monoïdes comaximaux.

1.8. Principe local-global concret. (Suites exactes, systèmes linéaires)
Soient $S_1, \ldots, S_n$ *des monoïdes comaximaux de* $\mathbf{A}$, M, N, P *des* $\mathbf{A}$*-modules,* φ, ψ *des applications linéaires de* M *dans* N, $\theta : N \to P$ *une application linéaire, et* x, y *des éléments de* N. *On note* $\mathbf{A}_i$ *pour* $\mathbf{A}_{S_i}$, M_i *pour* M_{S_i} *etc. Alors on a les équivalences suivantes.*

1. *Recollement concret des égalités :*
$$x = y \quad \text{dans} \quad N \quad \Longleftrightarrow \quad \forall i \in [\![1..n]\!]\ x/1 = y/1 \quad \text{dans} \quad N_i.$$
2. *Recollement concret des égalités d'applications linéaires :*
$$\varphi = \psi \quad \text{dans} \quad \mathscr{L}_{\mathbf{A}}(M, N) \quad \Longleftrightarrow$$
$$\forall i \in [\![1..n]\!]\ \varphi/1 = \psi/1 \quad \text{dans} \quad \mathscr{L}_{\mathbf{A}_i}(M_i, N_i).$$

3. *Recollement concret des éléments réguliers :*
$$x \text{ est régulier dans } N \iff \forall i \in [\![1..n]\!]\ x/1 \text{ est régulier dans } N_i.$$
4. *Recollement concret des solutions de systèmes linéaires :*
$$x \in \operatorname{Im}\varphi \iff \forall i \in [\![1..n]\!]\ x/1 \in \operatorname{Im}\varphi_i$$
5. *Recollement concret des suites exactes. La suite*
$$M \xrightarrow{\varphi} N \xrightarrow{\theta} P$$
est exacte si, et seulement si, les suites
$$M_i \xrightarrow{\varphi_i} N_i \xrightarrow{\theta_i} P_i$$
sont exactes pour $i \in [\![1..n]\!]$.
6. *Recollement concret de facteurs directs dans les modules de présentation finie. Ici M est un sous-module de type fini d'un module de présentation finie N.*
$$M \text{ est facteur direct dans } N \iff \forall i \in [\![1..n]\!],\ M_i \text{ est facteur direct dans } N_i.$$

Notez que la propriété *5* n'est pas de caractère fini mais qu'elle est une conjonction de propriétés du type *1* et *4* qui sont de caractère fini, ce qui explique qu'elle obéit au principe local-global abstrait correspondant.

1.9. Principe local-global concret. (Recollement concret de propriétés de finitude pour les modules) *Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$ et M un $\mathbf{A}$-module. Alors on a les équivalences suivantes.*

1. *M est de type fini si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module de type fini.*
2. *M est de présentation finie si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module de présentation finie.*
3. *M est plat si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module plat.*
4. *M est projectif de type fini si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module projectif de type fini.*
5. *M est projectif de rang k si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module projectif de rang k.*
6. *M est cohérent si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module cohérent.*
7. *M est noethérien si, et seulement si, chacun des M_{S_i} est un $\mathbf{A}_{S_i}$-module noethérien.*

1.10. Principe local-global concret. (Recollement concret de propriétés des anneaux commutatifs) *Soient $S_1, \ldots, S_n$ des monoïdes comaximaux et $\mathfrak{a}$ un idéal de $\mathbf{A}$. Alors on a les équivalences suivantes.*

1. *L'anneau $\mathbf{A}$ est cohérent si, et seulement si, chaque $\mathbf{A}_{S_i}$ est cohérent.*
2. *L'anneau $\mathbf{A}$ est localement sans diviseur de zéro si, et seulement si, chaque $\mathbf{A}_{S_i}$ est localement sans diviseur de zéro.*
3. *$\mathbf{A}$ est quasi intègre si, et seulement si, chaque $\mathbf{A}_{S_i}$ est quasi intègre.*
4. *L'anneau $\mathbf{A}$ est réduit si, et seulement si, chaque $\mathbf{A}_{S_i}$ est réduit.*
5. *L'idéal $\mathfrak{a}$ est localement principal si, et seulement si, chaque $\mathfrak{a}_{S_i}$ est localement principal.*
6. *L'anneau $\mathbf{A}$ est arithmétique si, et seulement si, chaque $\mathbf{A}_{S_i}$ est arithmétique.*
7. *L'anneau $\mathbf{A}$ est de Prüfer si, et seulement si, chaque $\mathbf{A}_{S_i}$ est de Prüfer.*
8. *L'idéal $\mathfrak{a}$ est intégralement clos si, et seulement si, chaque $\mathfrak{a}_{S_i}$ est intégralement clos.*
9. *L'anneau $\mathbf{A}$ est normal si, et seulement si, chaque $\mathbf{A}_{S_i}$ est normal.*
10. *Une suite finie dans $\mathbf{A}$ est singulière si, et seulement si, elle est singulière dans chaque $\mathbf{A}_{S_i}$.*

11. *L'anneau* $\mathbf{A}$ *est de dimension de Krull* $\leqslant k$ *si, et seulement si, chaque anneau* $\mathbf{A}_{S_i}$ *est de dimension de Krull* $\leqslant k$.
12. *L'anneau* $\mathbf{A}$ *est noethérien si, et seulement si, chaque anneau* $\mathbf{A}_{S_i}$ *est noethérien.*

1.11. Principe local-global concret.
Soient $S_1, \ldots, S_n$ *des monoïdes comaximaux d'un anneau* $\mathbf{k}$ *et* $\mathbf{A}$ *une* $\mathbf{k}$*-algèbre. Les propriétés suivantes sont équivalentes.*

1. $\mathbf{A}$ *est de type fini (resp. plate, fidèlement plate, de présentation finie, finie, entière, strictement finie, séparable) sur* $\mathbf{k}$.
2. *Chacune des algèbres* $\mathbf{A}_{S_i}$ *est de type fini (resp. plate, fidèlement plate, de présentation finie, finie, entière, strictement finie, séparable) sur* $\mathbf{k}_{S_i}$.

Algèbres, localisation en haut. Il y a aussi des principes local-globals pour une $\mathbf{k}$-algèbre $\mathbf{A}$ qui correspondent à des propriétés dites « locales dans $\mathbf{A}$ ». Ici nous avons besoin de localisations en des éléments comaximaux (les monoïdes comaximaux ne suffisent pas).

1.12. Principe local-global concret.
Soit $\mathbf{A}$ *une* $\mathbf{k}$*-algèbre et* $s_1, \ldots, s_m$ *des éléments comaximaux de* $\mathbf{A}$. *Alors les propriétés suivantes sont équivalentes.*

1. $\mathbf{A}$ *est de type fini (resp. de présentation finie, plate) sur* $\mathbf{k}$.
2. *Chacune des algèbres* $\mathbf{A}_{s_i}$ *est de type fini (resp. de présentation finie, plate) sur* $\mathbf{k}$.

Machinerie locale-globale à idéaux premiers. Nous commençons par préciser les versions constructives pertinentes de quelques notions classiques.

Un ***anneau local*** est un anneau $\mathbf{A}$ où est vérifié l'axiome suivant :

$$\forall x, y \in \mathbf{A} \qquad x + y \in \mathbf{A}^\times \implies (x \in \mathbf{A}^\times \text{ ou } y \in \mathbf{A}^\times)\,. \tag{1.1}$$

Il revient au même de demander :

$$\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^\times \text{ ou } 1 - x \in \mathbf{A}^\times\,.$$

Un élément x d'un anneau $\mathbf{A}$ est dit ***noninversible*** (en un seul mot) s'il vérifie l'implication suivante

$$x \in \mathbf{A}^\times \;\Rightarrow\; 1 =_{\mathbf{A}} 0.$$

Dans l'anneau trivial l'élément 0 est à la fois inversible et noninversible.

Rappelons que pour un anneau commutatif arbitraire, on appelle ***radical de Jacobson*** de $\mathbf{A}$, noté $\mathrm{Rad}(\mathbf{A})$, l'ensemble suivant :

$$\mathrm{Rad}(\mathbf{A}) := \big\{\, a \in \mathbf{A} \mid 1 + a\mathbf{A} \subseteq \mathbf{A}^\times \,\big\}. \tag{1.2}$$

C'est un idéal parce que si $a, b \in \mathrm{Rad}\,\mathbf{A}$, on peut écrire, pour $x \in \mathbf{A}$:

$$1 + (a+b)x = (1+ax)(1 + (1+ax)^{-1}bx),$$

qui est produit de deux éléments inversibles.

En mathématiques classiques, le radical de Jacobson est l'intersection des idéaux maximaux.

Dans un anneau local le radical de Jacobson est égal à l'ensemble des éléments noninversibles.

Un ***corps de Heyting***, ou simplement un corps, est par définition un anneau local dans lequel tout élément noninversible est nul, autrement dit un anneau local dont le radical de Jacobson est réduit à 0.

Le quotient d'un anneau local par son radical de Jacobson est un corps, appelé ***corps résiduel de l'anneau local***.

Par définition un ***anneau local résiduellement discret*** est un anneau local dont le corps résiduel est un corps discret. Un tel anneau $\mathbf{A}$ peut être caractérisé par l'axiome suivant

$$\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^\times \text{ ou } x \in \mathrm{Rad}(\mathbf{A}) \tag{1.3}$$

Un argument de type local-global 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 apparaître certains calculs qui sont faisables en vertu de l'axiome 1.3, axiome qui est appliqué à des éléments x provenant de la preuve elle-même. Autrement dit, la preuve classique donnée dans le cas local nous fournit une démonstration constructive sous l'hypothèse d'un anneau local résiduellement discret.

Voici maintenant notre décryptage dynamique constructif. Dans le cas d'un anneau arbitraire, nous répétons la même démonstration, en remplaçant chaque disjonction «$x \in \mathbf{A}^\times$ ou $x \in \mathrm{Rad}(\mathbf{A})$», par la considération des deux anneaux

$$\mathbf{A}_{\mathcal{S}(I;x,U)} \text{ et } \mathbf{A}_{\mathcal{S}(I,x;U)},$$

où $\mathbf{A}_{\mathcal{S}(I,U)}$ est la localisation «courante» de l'anneau $\mathbf{A}$ de départ, à l'endroit de la preuve où l'on se trouve. Lorsque la preuve initiale est ainsi déployée, on a construit à la fin un certain nombre, fini parce que la preuve est finie, de localisés $\mathbf{A}_{S_i}$, pour lesquels la propriété est vraie. D'un point de vue constructif, nous obtenons au moins le résultat «quasi global», c'est-à-dire après localisation en des monoïdes comaximaux, en vertu du point *1* du lemme 1.4. On fait alors appel à un principe local-global concret pour conclure.

La première partie de notre décryptage de la preuve classique est rendu possible par le simple fait que la propriété P étudiée est stable par localisation.

Le décryptage complet contient donc deux ingrédients essentiels.

– Le premier est le décryptage constructif de la preuve donnée dans le cas d'un anneau local résiduellement discret. Cela n'est généralement pas un grand travail, car il faut bien que les mathématiques classiques fassent elles-mêmes quelques calculs. Ce décryptage fonctionne parce que la propriété est stable par localisation et il permet d'obtenir un résultat quasi global : la propriété est satisfaite après localisation en des monoïdes comaximaux, et même en des éléments comaximaux si 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. Là aussi, nous pouvons en général trouver les calculs nécessaires en examinant la démonstration du principe local-global abstrait en mathématiques classiques. Ici peut intervenir le fait que la propriété est de caractère fini, si c'est le cas.

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.

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

La méthode indiquée ci-dessus donne donc, comme corollaire du lemme 1.4, le principe général de décryptage suivant, qui *permet d'obtenir automatiquement une version constructive 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. Dans chacun de ces anneaux, le calcul a été poursuivi avec succès et a donné le résultat souhaité.

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

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

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 $\mathbf{A}_{\mathcal{S}(I,a;U)}$.

Dans la suite nous parlerons de la machinerie locale-globale à idéaux premiers comme de la «machinerie locale-globale de base».

Cette méthode, qui est une extension raisonnée de l'évaluation dynamique à la D5, est annoncée et analysée dans [22] et [24].

Dans l'ouvrage [ACMC], on a rarement besoin d'utiliser cette machinerie car les principes local-globals concrets suffisent souvent à résoudre directement les problèmes. Néanmoins, cette machinerie devient indispensable dans le chapitre XVI pour décrypter des démonstrations sophistiquées : la démonstration par Quillen du théorème de Quillen-Suslin, la généralisation du résultat aux anneaux principaux, puis la généralisation non noethérienne aux domaines de Bezout de dimension 1 (due à Brewer&Costa), et enfin, nettement plus fort encore, la généralisation aux anneaux de Bezout arbitraires et aux anneaux arithmétiques due à Lequain&Simis.

Nous nous contenterons ici d'un exemple assez simple, mais significatif.

Un exemple. On veut démontrer le résultat suivant.

1.13. Lemme. *Soit $f \in \mathbf{A}[X]$ un polynôme primitif et $r \in \mathbf{A}$ un élément régulier avec $\mathsf{Kdim}\,\mathbf{A} \leqslant 1$. Alors l'idéal $\langle f, r\rangle$ contient un polynôme unitaire.*

Démonstration. On commence par montrer le lemme dans le cas où $\mathbf{A}$ est un anneau local résiduellement discret. On peut écrire $f = f_1 + f_2$ avec $f_1 \in (\operatorname{Rad}\mathbf{A})[X]$ et f_2 pseudo unitaire. Par ailleurs, pour tout $e \in \operatorname{Rad}\mathbf{A}$ on a une égalité $r^m(e^m(1+ye)+zr) = 0$, donc r divise e^m. Par suite r divise une puissance de f_1, disons d'exposant N. On a ${f_2}^N = (f-f_1)^N \in \langle f, f_1^N\rangle \subseteq \langle f, r\rangle$. Alors, f_2^N fournit le polynôme unitaire cherché.

Pour un anneau arbitraire on reprend la preuve précédente de manière dynamique. Par exemple si $f = aX^2 + bX + c$, on explicite le raisonnement précédent sous la forme suivante.

Ou bien a est inversible, ou bien il est dans le radical. Si a est inversible, alors on prend $f_2 = f$, $f_1 = 0$.

Sinon, ou bien b est inversible, ou bien il est dans le radical. Si b est inversible, alors on prend $f_2 = bX + c$, $f_1 = aX^2$.

Sinon, ou bien c est inversible, ou bien il est dans le radical. Si c est inversible, alors on prend $f_2 = c$, $f_1 = aX^2 + bX$.

Sinon $\langle 1\rangle = \langle a, b, c\rangle \in \operatorname{Rad}\mathbf{A}$ donc l'anneau est trivial.

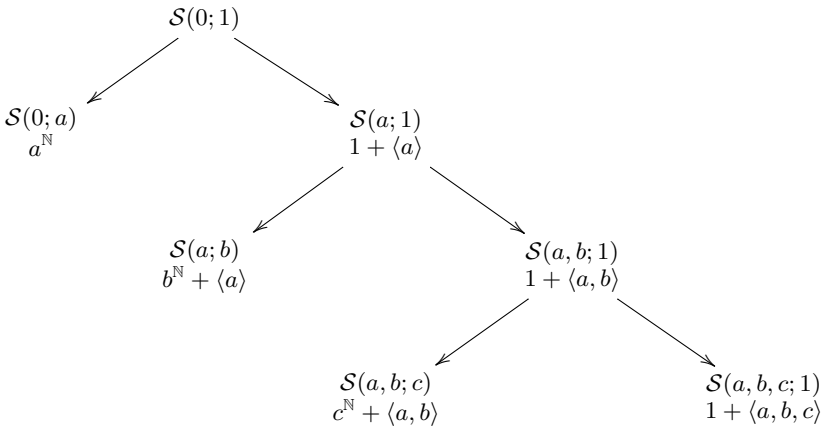
Voir plus loin le dessin de l'arbre des localisations successives. Les monoïdes comaximaux se trouvent aux feuilles de l'arbre, le dernier contient 0 et n'intervient pas dans le calcul.

Terminons en indiquant comment on construit un polynôme unitaire dans l'idéal $\langle f, r\rangle$ de $\mathbf{A}_{\mathcal{S}(I,U)}[X]$ à partir de deux polynômes unitaires g et h dans les idéaux $\langle f, r\rangle$ de $\mathbf{A}_{\mathcal{S}(I,y;U)}[X]$ et $\mathbf{A}_{\mathcal{S}(I;y,U)}[X]$. On a d'une part

$$sg = sX^m + g_1 \text{ avec } \deg g_1 < m,\ s \in \mathcal{S}(I, y; U) \text{ et } sg \in \langle f, r\rangle_{\mathbf{A}[X]},$$

et d'autre part

$$th = tX^n + h_1 \text{ avec } \deg h_1 < n,\ t \in \mathcal{S}(I; y, U) \text{ et } th \in \langle f, r\rangle_{\mathbf{A}[X]}.$$



Les polynômes $sX^n g$ et $tX^m h$ de degré formel $n+m$ ont pour coefficients formellement dominants s et t. En prenant $us+vt \in \mathcal{S}(I,U)$, le travail est terminé avec $usX^n g + vtX^m h$. □

2. Idéaux premiers maximaux

Un anneau qui n'a pas d'idéaux maximaux est réduit à 0.
Une mathématicienne classique

On trouve dans la littérature un certain nombre de preuves dans lesquelles l'auteur démontre un résultat en considérant «le passage au quotient par un idéal maximal arbitraire». L'analyse de ces preuves 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, 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 donné en exergue : un anneau qui n'a pas d'idéaux maximaux est réduit à 0.

Le fait de présenter le raisonnement comme une preuve 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 preuve 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 le à $\mathfrak{a}$. 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 coté 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 preuve 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 apparaît, 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.

Machinerie locale-globale à idéaux maximaux. L'argument de passage au quotient par tous les idéaux maximaux de $\mathbf{A}/\mathfrak{a}$ (supposé par l'absurde non réduit à 0), qui semblait un peu magique, est ainsi remplacé par un calcul bien concret, donné en filigrane par la preuve classique. Résumons la discussion précédente.

Machinerie locale-globale à idéaux maximaux.
Objectif. *Décrypter une preuve 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 preuve fournit 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 preuve 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 preuve proposée pour le cas inversible (qui*

est maintenant certifié). Si la preuve 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.

Un exemple. Le lemme crucial suivant était le seul ingrédient vraiment non constructif dans la solution par Suslin du problème de Serre. Ici, nous donnons la démonstration du lemme crucial en mathématiques classiques, puis son décryptage constructif.

2.1. Lemme. *Soit* $\mathbf{A}$ *un anneau, n un entier* $\geqslant 2$ *et* $U = {}^{t}[\,v_1\ \cdots\ v_n\,]$ *un vecteur unimodulaire dans* $\mathbf{A}[X]^{n\times 1}$ *avec* v_1 *unitaire.*
Notons $V = {}^{t}[\,v_2\ \cdots\ v_n\,]$. *Il existe des matrices* $E_1, \ldots, E_\ell \in \mathbb{E}_{n-1}(\mathbf{A}[X])$, *telles que, en notant* w_i *la première coordonnée du vecteur* E_iV, *l'idéal* $\mathfrak{a}$ *ci-après contient 1 :*

$$\mathfrak{a} = \langle \mathrm{Res}_X(v_1, w_1), \mathrm{Res}_X(v_1, w_2), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle_{\mathbf{A}}\,.$$

Démonstration. Si $n = 2$, on a $u_1v_1 + u_2v_2 = 1$ et puisque v_1 est unitaire, $\mathrm{Res}(v_1, v_2) \in \mathbf{A}^\times$:

$$\mathrm{Res}(v_1, v_2)\mathrm{Res}(v_1, u_2) = \mathrm{Res}(v_1, u_2v_2) = \mathrm{Res}(v_1, u_2v_2 + u_1v_1) = \mathrm{Res}(v_1, 1) = 1.$$

Si $n \geqslant 3$, soit $d_1 = \deg v_1$. On suppose sans perte de généralité que les v_i sont des polynômes formels de degrés $d_i < d_1$ ($i \geqslant 2$). On a au départ des polynômes u_i tels que $u_1v_1 + \cdots + u_nv_n = 1$.

Démonstration classique de Suslin. On montre que pour tout idéal maximal $\mathfrak{m}$, on peut trouver une matrice $E_\mathfrak{m} \in \mathbb{E}_{n-1}(\mathbf{A}[X])$ telle que, en notant $w_\mathfrak{m}$ la première coordonnée de $E_\mathfrak{m}V$ on ait $1 \in \langle \mathrm{Res}_X(v_1, w_\mathfrak{m})\rangle$ modulo $\mathfrak{m}$. Pour cela on se place sur le corps $\mathbf{k} = \mathbf{A}/\mathfrak{m}$. En utilisant l'algorithme d'Euclide, le pgcd $w_\mathfrak{m}$ des v_i ($i \geqslant 2$) est la première coordonnée d'un vecteur obtenu par manipulations élémentaires sur V. On relève la matrice élémentaire qui a été calculée dans $\mathbb{E}_{n-1}(\mathbf{k}[X])$ en une matrice $E_\mathfrak{m} \in \mathbb{E}_{n-1}(\mathbf{A}[X])$. Alors, puisque v_1 et $w_\mathfrak{m}$ sont premiers entre eux, le résultant $\mathrm{Res}_X(v_1, w_\mathfrak{m})$ est non nul dans le corps $\mathbf{A}/\mathfrak{m}$.

Démonstration constructive (par décryptage).
Nous faisons une preuve par récurrence sur le plus petit des degrés formels d_i, que nous notons m (rappelons que $i \geqslant 2$). Supposons pour fixer les idées que ce soit d_2.
Initialisation : si $m = -1$, $v_2 = 0$ et par une transformation élémentaire on met $u_3v_3 + \cdots + u_nv_n$ en position 2, ce qui nous ramène au cas $n = 2$.
Récurrence : de $m-1$ à m. Soit a le coefficient de v_2 de degré m et $\mathbf{B}$ l'anneau $\mathbf{A}/\langle a\rangle$. Dans cet anneau l'hypothèse de récurrence est vérifiée. Ainsi, on a des matrices $E_1, \ldots, E_\ell \in \mathbb{E}_{n-1}(\mathbf{B}[X])$, telles que, en notant $\widetilde{w_i}$ la première coordonnée de E_iV, on a l'égalité

$$\langle \mathrm{Res}_X(v_1, \widetilde{w_1}), \mathrm{Res}_X(v_1, \widetilde{w_2}), \ldots, \mathrm{Res}_X(v_1, \widetilde{w_\ell})\rangle_{\mathbf{B}} = \langle 1\rangle\,.$$

Ceci signifie, en relevant les matrices dans $\mathbb{E}_{n-1}(\mathbf{A}[X])$ sans les changer de nom, et en notant w_i la première coordonnée de E_iV que l'on a :

$$\langle a, \mathrm{Res}_X(v_1, w_1), \mathrm{Res}_X(v_1, w_2), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle_{\mathbf{A}} = \langle 1\rangle\,.$$

Considérons alors $\mathfrak{b} = \langle \mathrm{Res}_X(v_1, w_1), \mathrm{Res}_X(v_1, w_2), \ldots, \mathrm{Res}_X(v_1, w_\ell)\rangle_{\mathbf{A}}$, et $\mathbf{C} = \mathbf{A}/\mathfrak{b}$. Puisque a est inversible dans $\mathbf{C}$, on peut par une manipulation élémentaire remplacer v_3 par un polynôme $v_3' = v_3 - qv_2$ avec $\deg v_3' \leqslant m-1$. On applique l'hypothèse de récurrence avec l'anneau $\mathbf{C}$, on a des matrices élémentaires $E_1', \ldots, E_q' \in \mathbb{E}_{n-1}(\mathbf{C}[X])$ que l'on relève dans $\mathbb{E}_{n-1}(\mathbf{A}[X])$ sans les changer de noms. Si $w_1', \ldots, w_q'$ sont les polynômes correspondants (pour chaque j, w_j' est la première coordonnée de $E_j'V$), on obtient

$$1 \in \big\langle \mathrm{Res}_X(v_1, w_1), \ldots, \mathrm{Res}_X(v_1, w_\ell), \mathrm{Res}_X(v_1, w_1'), \ldots, \mathrm{Res}_X(v_1, w_q')\big\rangle_{\mathbf{A}}\,.$$

□

Nous laissons au lecteur le soin de vérifier que ce décryptage correspond bien à la machinerie locale-globale à idéaux maximaux décrite précédemment.

3. Idéaux premiers minimaux

Un anneau qui n'a pas d'idéaux premiers minimaux est réduit à 0.
Un mathématicien classique

Rappelons qu'un idéal premier minimal est un idéal premier $\mathfrak{p}$ tel que le localisé $\mathbf{A}_\mathfrak{p}$ est un anneau local zéro-dimensionnel, et qu'un tel anneau est caractérisé par la propriété suivante.

Tout élément est inversible ou nilpotent.

Ainsi un anneau local zéro-dimensionnel réduit est un corps discret.

La lectrice est maintenant mise à contribution pour se convaincre de la justesse de la méthode de déryptage donnée ci-dessous, en échangeant dans la section précédente addition et multiplication, et en remplaçant le passage au quotient par la localisation.

Machinerie locale-globale à idéaux premiers minimaux. Objectif. *Décrypter une preuve classique qui démontre par l'absurde qu'un anneau* **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) et en trouvant la contradiction* $1 = 0$.
Procéder comme suit. *Premièrement s'assurer que la preuve fournit une démonstration constructive de l'égalité* $1 = 0$ *sous l'hypothèse supplémentaire que* **A** *est local et zéro-dimensionnel. Deuxièmement, supprimer l'hypothèse supplémentaire et suivre pas à pas la preuve 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 preuve proposée pour le cas nilpotent (qui est maintenant certifié). Si la preuve 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.*

Exemples. Un exemple assez spectaculaire est donné avec le décryptage constructif d'une preuve abstraite du théorème de Traverso concernant les anneaux seminormaux.

On renvoie pour cela à [Seminormal, Coquand] et à [ACMC, section XVI-2].

En fait, en essayant d'obtenir à partir de cette démonstration constructive un algorithme plus concret, on tombe sur un algorithme où l'on se débarrasse des appels récursifs implicites dans la démonstration au profit de calculs de polynômes sous-résultants (ou de modules sous-résultants) qui raccourcissent les calculs dynamiques de pgcds (ou d'idéaux résultants). Voir à ce sujet l'article [2].

D'autres exemples dans la littérature classique ont été décryptés selon la machinerie locale-globale à idéaux premiers minimaux. Par exemple la preuve du *Main Theorem de Zariski* par Peskine, décryptée dans [1], ou encore les principaux résultats du livre *Finite Free Resolutions* de Northcott, décryptés dans [9].

Là aussi une analyse détaillée de la démonstration constructive a permis ensuite de donner des arguments plus directs.

Conclusion

L'algèbre constructive n'est qu'une petite partie des mathématiques constructives. Celles-ci ont l'ambition de réécrire en termes algorithmiques *toutes* les mathématiques contemporaines.

Les mathématiques constructives modernes, minimalistes, ont été introduites par Errett Bishop dans [Bishop] et développées dans [Bishop & Bridges], [Bridges & Richman] et [MRR].

Ces ouvrages devraient faire partie de la culture mathématique de base.

La polémique sur la nature et l'usage de l'infini en mathématiques a été très vive au début du 20^{e} siècle : voir par exemple Hilbert [17, 1926], Poincaré [27, 1909], H. Weyl [35, 1918], [Brouwer, 1951] et [Infini, 1987]). Le débat a semblé en un premier temps se terminer à l'avantage du point de vue représenté par la logique classique.

En fait, depuis les années 60 et la parution du livre de Bishop, les deux points de vue sont nettement moins opposés qu'il ne pouvait paraître. Voir à ce sujet [26, Per Martin-Löf].

La logique constructive s'appelle souvent « logique intuitionniste ». Elle a été mise au point en tant que système formel par A. Heyting.

Concernant la discussion sur les rapports entre effectivité et récursivité voir [31, Skolem], [16, Heyting] et [4, Coquand].

La mise au point et la comparaison de systèmes formels pouvant servir de cadre aux mathématiques constructives pratiquées dans [Bishop] ou [MRR] est depuis longtemps un sujet très actif de recherche. On notera l'influence prépondérante de la théorie constructive des types **CTT** de Per Martin-Löf [25, 1973].

Voir aussi les développements récents dans [HoTT, 2014] et la page web de Thierry Coquand : `http://www.cse.chalmers.se/~coquand/`.

Références

[Bishop] Bishop E. *Foundations of Constructive Analysis.* McGraw Hill, (1967). Réédition : Ishi Press. New York and Tokio, (2012).

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

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

[Brouwer] Brouwer L. *Brouwer's Cambridge Lectures on Intuitionism, 1951* (Van Dalen ed.) Cambridge University Press, (1981).

[HoTT] *Homotopy Type Theory and the Univalent Foundation.* (2014). `http://homotopytypetheory.org/`

[Infini] Toraldo di Francia G. (ed.), *L'infinito nella scienza*, Istituto della Enciclopedia Italiana, Rome, (1987).

[Johnstone] Johnstone P. *Stone spaces,* Cambridges studies in advanced mathematics n° 3. Cambridge University Press, (1982).

[MRR] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988).

[ACMC] Lombardi H., Quitté C. *Algèbre Commutative, Méthodes Constructives.* Calvage & Mounet, (2011).

[Modules] Díaz-Toca G.-M., Lombardi H., Quitté C. *Modules sur les anneaux commutatifs.* Calvage & Mounet, (2014).

[Dynamic] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic, **111**, (2001), 203–256.
`http://hlombardi.free.fr/publis/NullstellensatzDynamic.pdf`

[Logic] Coquand T., Lombardi H. *A logical approach to abstract algebra.* (survey) Math. Struct. in Comput. Science **16** (2006), 885–900.
`http://hlombardi.free.fr/publis/AlgebraLogicCoqLom.pdf`

[Seminormal] Coquand T. *On seminormality.* Journal of Algebra, **305** (1), (2006), 585–602. `http://www.cse.chalmers.se/~coquand/min.pdf`

[Plaidoyer] Coquand T., Lombardi H. *Plaidoyer pour l'algèbre constructive.* Rapport technique. (2012) Paru en Espagnol dans *La Gaceta.*
`http://hlombardi.free.fr/publis/Plaidoyer.pdf`

[1] Alonso M., Coquand T., Lombardi H. *Revisiting Zariski Main Theorem from a constructive point of view.* Journal of Algebra. **406**, (2014) 46–68. `http://hlombardi.free.fr/publis/ZMT.pdf`

[2] Barhoumi S., Lombardi H. *An Algorithm for the Traverso-Swan theorem on seminormal rings.* Journal of Algebra **320** (2008), 1531–1542. `http://hlombardi.free.fr/publis/SemiNor.pdf`

[3] Coquand T. *Sur un théorème de Kronecker concernant les variétés algébriques.* C. R. Acad. Sci. Paris, Ser. I **338** (2004), 291–294.

[4] Coquand T. *Recursive functions and constructive mathematics.* À paraître dans : Bourdeau M., Dubucs J. (Eds.), Calculability and Constructivity. Historical and Philosophical Aspects. Logic, Epistemology and the Unity of Science. Dordrecht, Heidelberg, London, New Yort : Springer.

[5] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*, p. 477–499 dans : Commutative ring theory and applications, eds. Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker, (2002).
`http://hlombardi.free.fr/publis/Krull2.pdf`

[6] Coquand T., Lombardi H., Quitté C. *Generating non-Noetherian modules constructively.* Manuscripta mathematica, **115** (2004), 513–520. `http://hlombardi.free.fr/publis/forster.pdf`

[7] Coquand T., Lombardi H., Quitté C. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs.* Publications Mathématiques de Besançon. Théorie des nombres (2006). 51 pages. Version corrigée `http://hlombardi.free.fr/publis/Heitmann.pdf`

[8] Coquand T., Lombardi H., Roy M.-F. *An elementary characterisation of Krull dimension*, dans : From Sets and Types to Analysis and Topology : Towards Practicable Foundations for Constructive Mathematics ; Crosilla L., Schuster P., eds. Oxford University Press, (2005), 239–244. http://hlombardi.free.fr/publis/lebord.pdf

[9] Coquand T., Quitté C. *Constructive finite free resolutions.* Manuscripta Math., **137**, (2012), 331–345.

[10] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer (1985).

[11] Español L. *Dimensión en álgebra constructiva.* Thèse doctorale. Université de Zaragoza, Zaragoza, (1978).

[12] Español L. *Constructive Krull dimension of lattices.* Rev. Acad. Cienc. Zaragoza (2) **37** (1982), 5–9.

[13] Español L. *Le spectre d'un anneau dans l'algèbre constructive et applications à la dimension.* Cahiers de topologie et géométrie différentielle catégorique. **24** n° 2 (1983), 133–144.

[14] Forster O. *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring.* Math. Z. **84** (1964), 80–87.

[15] Heitmann R. *Generating non-Noetherian modules efficiently.* Michigan Math. **31** 2 (1984), 167–180.

[16] Heyting A. *After thirty years.* In : 1962 Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.) pp. 194–197 Stanford Univ. Press, Stanford, Calif.

[17] Hilbert D. *Über das Unendliche.* Math. Annalen **95** (1926), 161–190. (Sur l'infini) traduction anglaise dans [34] 367–392.

[18] Hochster M. *Prime ideal structure in commutative rings.* Trans. Amer. Math. Soc. **142** (1969), 43–60.

[19] Joyal A. *Spectral spaces and distibutive lattices.* Notices AMS **18** (1971), 393.

[20] Joyal A. *Les théorèmes de Chevalley-Tarski et remarques sur l'algèbre constructive.* Cahiers de topologie et géometrie différentielle catégorique, 1975.

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

[22] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini.* Publications Mathématiques de Besançon. Théorie des nombres. Fascicule (1997), 94–95 & 95–96.
http://hlombardi.free.fr/publis/protifiBesac.pdf

[23] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242**, (2002), 23–46.
http://hlombardi.free.fr/publis/Krull1.pdf

[24] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global*, p. 461–476 dans : Commutative ring theory and applications, eds. Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker, (2002). http://hlombardi.free.fr/publis/LocalGlobal2.pdf

[25] Per Martin-Löf *An intuitionistic theory of types : Predicative part.* In H. E. Rose and J. C. Shepherdson, editors, Logic Colloquium '73, pages 73–118. North Holland, (1975).

[26] Per Martin-Löf *The Hilbert-Brouwer controversy resolved ?* dans : One hundred years of intuitionism (1907-2007), (Cerisy), (Mark Van Atten & al., editors) Publications des Archives Henri Poincaré, Birkhäuser Basel, (2008), pp. 243–256.

[27] Poincaré H. *La logique de l'infini*, Revue de Métaphysique et de Morale **17**, 461–482, (1909) réédité dans *Dernières pensées*, Flammarion (1913).

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

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

[30] Serre J.-P. *Modules projectifs et espaces fibrés à fibre vectorielle.* Séminaire P. Dubreil, Année 1957/1958.

[31] Skolem T. *A critical remark on foundational research.* Norske Vid. Selsk. Forh., Trondheim **28** (1955), 100–105.

[32] Stone M. H. *Topological representations of distributive lattices and Brouwerian logics.* Cas. Mat. Fys. **67**, (1937), 1–25.

[33] Swan R. *The Number of Generators of a Module.* Math. Z. **102** (1967), 318–322.

[34] Van Heijenoort J. *From Frege to Gˆdel : A Source Book in Mathematical Logic, 1879-1931* Harvard University Press (1967).

[35] Weyl H. *Das Kontinuum, Kritische Untersuchungen über die Grundlagen der Analysis.* Veit, Leipzig (1918). Traduction italienne *Il Continuo. Indagine critiche sui fondamenti dell' Analisi.* par A. B. Veit Riccioli, Bibliopolis, Naples (1977). Traduction anglaise *The Continuum. A critical examination of the foundations of Analysis.* par S. Polard et T. Bole. Thomas Jefferson Press, University Press of America (1987). En français : *Le continu et autres écrits.* Traduits et commentés par Jean Largeault. Librairie Vrin (1994).

Département de mathématiques, Université de Franche-Comté, 25030 Besançon Cedex • henri.lombardi@univ-fcomte.fr

Index des termes