Constructions cachées en algèbre abstraite (2) le principe local-global

Henri Lombardi ([1]), Claude Quitté ([2])

24 Mai 2002

Résumé

Nous appliquons une forme constructive de principes local-global en algèbre commutative pour décrypter, cachées dans des théorèmes d'algèbre abstraite, des constructions de matrices inversibles dans des anneaux de polynomes. Ceci nous donne une nouvelle preuve constructive de la conjecture de Serre (théorème de Quillen-Suslin) et une preuve constructive du théorème de stabilité de Suslin.

Abstract

Wa apply a constructive form of local-global principles in commutative algebra in order to decipher some constructions of invertible polynomial matrices hidden in theorems of abstract algebra. This leads us to a new constructive proof of Serre's conjecture (Quillen-Suslin theorem). We get also a constructive proof of Suslin's stability theorem.

MSC 2000 : 13C10, 19A13, 14Q20, 03F65.

Mots clés : Théorème de Horrocks, Théorème de Quillen-Suslin, Théorème de stabilité de Suslin, Modules projectifs de type fini, Principes local-global, Mathématiques constructives.

Key words : Horrocks' theorem, Quillen-Suslin's theorem, Suslin's stability theorem, Finitely generated projective modules, Local-global principles, Constructive mathematics.

[1] Equipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE, email: lombardi@math.univ-fcomte.fr

[2] Laboratoire de Mathématiques, SP2MI, Boulevard 3, Teleport 2, BP 179, 86960 FUTUROSCOPE Cedex, FRANCE, email: quitte@mathlabo.univ-poitiers.fr

Table des matières

Introduction

Nous nous situons dans la philosophie développée dans les articles [4, 5, 17, 18, 19, 20, 21, 22, 23]. Il s'agit de débusquer un contenu constructif caché dans des preuves abstraites de théorèmes concrets.

La méthode générale consiste à remplacer certains objets abstraits idéaux qui n'existent qu'en vertu du principe du tiers exclu et de l'axiome du choix, par des spécifications incomplètes de ces mêmes objets.

Dans cet article nous nous attaquons à la méthode abstraite qui utilise des principes du type local-global. Un résultat est démontré vrai après localisation en n'importe quel idéal premier. On déduit ensuite qu'il est vrai globalement par un argument adéquat.

Notre but n'est en aucun cas de donner des algorithmes performants, mais de montrer qu'il n'y a pas de miracle en mathématiques : si une preuve abstraite donne un résultat concret, le calcul concret du résultat doit d'une manière ou d'une autre être caché dans la preuve abstraite (sauf à croire en la réalité de l'Univers Cantorien censé officiellement justifier la preuve abstraite).

Ou encore pour le dire autrement. Nos preuves explicites ont ceci de particulier qu'elles sont obtenues par un simple décryptage des arguments contenus dans une preuve abstraite. Par contre ces algorithmes sont a priori peu efficaces. Ils n'ont pas pour but de reposer la machine, mais de reposer le concepteur d'algorithmes. Et surtout d'annoncer une bonne nouvelle : les méthodes abstraites en algèbre sont, en fait, constructives.

Nous pensons engager ainsi un début de réalisation du programme de Hilbert pour ce qui concerne les méthodes de l'algèbre abstraite.

Dans son esprit, notre méthode est à rapprocher de celle de Kreisel lorsqu'il "déroule" (unwind) des preuves classiques pour en faire des preuves constructives "sans introduire de nouvelles idées" (cf. la description du programme de Kreisel par Feferman dans [7]). Mais nous utilisons des moyens purement algébriques, relativement élémentaires, tandis que Kreisel met en oeuvre une artillerie métamathématique assez impressionnante (cf. [6]).

Dans la section 1 nous expliquons la machinerie de relecture constructive grâce à laquelle nous remplaçons "la localisation en tous les idéaux premiers" par des localisations en des monoïdes convenables, décrits explicitement en termes finis à partir d'une lecture attentive de la preuve abstraite. En pratique les idéaux premiers "purement idéaux" qui interviennent dans la preuve abstraite sont remplacés par certaines spécifications incomplètes d'idéaux premiers, qui suffisent à faire fonctionner la preuve, et qui la font fonctionner de manière constructive. Notre procédé de relecture automatique transforme la preuve du théorème local en celle d'un théorème que nous appelons quasi-global.

Quant à la preuve que la version quasi-globale implique la version globale, elle est en général déjà dans la littérature classique, sous la forme d'un *lemme de propagation* (pas toujours énoncé sous forme d'un lemme séparé), qui est au coeur de la preuve du principe local-global concret abstrait correspondant. Nous préférons quant à nous énoncer le lemme de propagation sous forme d'un principe local-global concret, car cette terminologie nous paraît plus parlante.

Dans les sections 2 et 3 nous donnons deux exemples de théorèmes célèbres pour lesquels nous appliquons cette méthode. Le théorème de Quillen-Suslin (conjecture de Serre) et le théorème de stabilité de Suslin. Dans les deux cas nous nous limitons au cas des corps (il y a des versions plus générales que nous ne traitons pas ici).

Pour ces théorèmes (dans le cas des corps) d'autres preuves constructives basées sur des

idées différentes sont déjà connues.

Tous les anneaux considérés sont commutatifs unitaires. Soit $\mathbf{A}$ un tel anneau. Un vecteur $f = {}^{\mathrm{t}}(f_1, \ldots, f_n)$ de $\mathbf{A}^{n\times 1}$ est dit *unimodulaire* lorsque l'idéal $\mathcal{I}(f_1, \ldots, f_n)$ contient 1. On dit encore que les éléments $f_1, \ldots, f_n$ de $\mathbf{A}$ sont *comaximaux*. Nous notons $\mathrm{Rad}(\mathbf{A})$ le radical (de Jacobson) de $\mathbf{A}$, c.-à-d. l'ensemble des x tels que $1 + x\mathbf{A} \subset \mathbf{A}^\times$ (le groupe des unités de $\mathbf{A}$). Nous notons $\mathbf{M}_n(\mathbf{A})$ l'anneau des matrices carrées d'ordre n à coefficients dans $\mathbf{A}$, $\mathbb{SL}_n(\mathbf{A})$ le groupe des matrices de déterminant 1, $\mathbb{E}_n(\mathbf{A})$ le sous-groupe du précédent engendré par les matrices élémentaires.

La section 2 décrypte une preuve "à la Quillen" du théorème de Quillen-Suslin.

Rappelons le théorème suivant dû à Horrocks (cf. [10]).

Théorème de Horrocks local
Soit un entier $n \geq 3$, $\mathbf{A}$ un anneau local et $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ un vecteur unimodulaire dans $\mathbf{A}[X]^{n\times 1}$, avec f_1 unitaire, alors il existe une matrice $H(X) \in \mathbb{E}_n(\mathbf{A}[X])$ telle que $H(X)f(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

Ce théorème possède une preuve constructive lorsque l'anneau local vérifie explicitement l'axiome suivant :

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

(en mathématiques constructives, cet axiome signifie que l'anneau est local et que son corps résiduel est discret, cf. [24]).

Nous rappelons cette preuve dans la section 2.1 (nous l'avons extraite d'une preuve un peu moins explicite dans [14]). Nous nous intéressons ensuite à une version située à mi-chemin entre la version locale et la version globale.

Théorème de Horrocks quasi-global
Soit un entier $n \geq 3$, $\mathbf{A}$ un anneau et $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ un vecteur unimodulaire dans $\mathbf{A}[X]^{n\times 1}$, avec f_1 unitaire, alors il existe des éléments comaximaux $a_1, \ldots, a_\ell \in \mathbf{A}$ et pour chaque $i = 1, \ldots, \ell$ une matrice $H_i(X) \in \mathbb{E}_n(\mathbf{A}[1/a_i][X])$ telle que $H_i(X)f(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

Nous montrons dans la section 2.1 que la preuve constructive du théorème quasi-global est cachée dans la preuve (constructive) du théorème local. Nous appliquons pour ce faire la machinerie décrite à la section 1.

Dans la section 2.2, nous établissons un principe local-global concret qui est la version constructive d'un principe local-global abstrait de Quillen.

Dans la section 2.3, nous déduisons des résultats précédents la version globale du théorème de Horrocks puis la conjecture de Serre.

Théorème de Horrocks global
Soit un entier $n \geq 3$, $\mathbf{A}$ un anneau intègre et $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ un vecteur unimodulaire dans $\mathbf{A}[X]^{n\times 1}$, avec f_1 unitaire, alors il existe une matrice $H \in \mathbb{SL}_n(\mathbf{A}[X])$ telle que $H(X)f(X) = f(0)$.

La conjecture de Serre dont nous donnons ici une nouvelle preuve constructive, a été résolue indépendamment par D. Quillen et A. Suslin en 1976 [26, 27]. L'exposé classique de leurs travaux est le livre de Lam [13]. On peut également citer le livre de Kunz [12] et celui de Gupta et Murthy [9]. D'autres solutions constructives, parfois relativement efficaces, ont été proposées notamment dans [1, 2, 3, 8, 15, 16, 25]. Aucune cependant ne découle comme la nôtre du décryptage automatique d'une preuve abstraite.

Dans la section 3 nous examinons la preuve du théorème de stabilité de Suslin dans le cas des corps, telle qu'elle est donnée dans [9] en s'appuyant sur une méthode locale-globale. Pareillement, nous la décryptons en une preuve constructive selon la méthode exposée dans la section 1. Le seul véritable argument non constructif dans [9] est l'utilisation du lemme 3.6 page 46. Ce lemme est de nature locale mais il est ensuite utilisé dans un argument de type local-global. C'est le lemme suivant, dans lequel $\binom{f}{g}$ désigne le symbole de Mennicke.

Lemme 20 (local) *Soit* $\mathbf{A}$ *un anneau local et* $f, g \in \mathbf{A}[X]$ *avec* f *unitaire et* $af+bg=1$. *Alors, on a*

$$\binom{f}{g} = \binom{f(0)}{g(0)} = 1.$$

Autrement dit la matrice

$$\begin{bmatrix} f & g & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

est dans $\mathbb{E}_3(\mathbf{A}[X])$.

Notre machinerie de relecture automatique de la preuve locale donne le lemme quasi-global suivant :

Lemme 21 (quasi-global) *Soit* $\mathbf{A}$ *un anneau et* $f, g \in \mathbf{A}[X]$ *avec* f *unitaire et* $af+bg=1$. *Alors, il existe des éléments comaximaux* s_i *tels que dans chaque localisé* $\mathbf{A}[1/s_i]$ *on ait l'égalité des symboles de Mennicke suivante*

$$\binom{f}{g} = \binom{f(0)}{g(0)} = 1.$$

Et cette version quasi-globale permet de remplacer l'utilisation abstraite du lemme local par une construction explicite pour aboutir à la version constructive du théorème global suivant, qui est la clef du théorème de stabilité de Suslin.

Théorème 24 (version globale du lemme 20)
Soit $\mathbf{A}$ *un anneau et* $f, g \in \mathbf{A}[X]$ *avec* f *unitaire et* $af+bg=1$. *Alors on a l'égalité des symboles de Mennicke suivante*

$$\binom{f}{g} = \binom{f(0)}{g(0)}.$$

1 Le principe de la méthode

Nous donnons ici quelques explications sur le fonctionnement du décryptement constructif des preuves classiques utilisant un principe local-global en algèbre commutative.

1.1 Du local au quasi-global

L'argument de localisation classique fonctionne comme suit. Lorsque l'anneau est local une certaine propriété P est vérifiée en vertu d'une preuve 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.

Nous examinons avec un peu d'attention la première preuve. Nous voyons alors apparaître certains calculs qui sont faisables en vertu du principe suivant :

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

Principe qui est appliqué à des éléments x provenant de la preuve elle-même. Dans le cas d'un anneau non nécessairement local, nous répétons la même preuve, en remplaçant chaque disjonction "x est une unité ou x est dans le radical", par la considération des deux anneaux $\mathbf{B}_x$ et $\mathbf{B}_{1+x\mathbf{B}}$, où $\mathbf{B}$ est la localisation "courante" de l'anneau $\mathbf{A}$ de départ, à l'endroit de la preuve où 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. En outre les ouverts de Zariski $\mathbf{U}_{S_i}$ correspondants recouvrent $\mathrm{Spec}(\mathbf{A})$ et cela implique que la propriété P est vraie avec $\mathbf{A}$, cette fois-ci de manière entièrement explicite.

Notons que cette méthode consiste pour l'essentiel à mettre à plat les calculs qui sont impliqués par la mise en oeuvre de la méthode de l'évaluation dynamique donnée dans [17].

Dans la suite, lorsqu'on parle d'un monoïde dans un anneau, on entend toujours une partie contenant 1 et stable pour la multiplication. Un monoïde S d'un anneau $\mathbf{A}$ est dit *saturé* lorsqu'on a l'implication

$$\forall s, t \in \mathbf{A} \ \ (st \in S \ \Rightarrow \ s \in S).$$

On note $\mathbf{A}_S$ le localisé $S^{-1}\mathbf{A}$ de $\mathbf{A}$ en S. Si S est engendré par $s \in \mathbf{A}$, on note $\mathbf{A}_s$ ou $\mathbf{A}[1/s]$ le localisé, qui est isomorphe à $\mathbf{A}[T]/(sT-1)$. Si on sature un monoïde, on ne change pas la localisation. Deux monoïdes sont dits *équivalents* s'ils ont même saturé.

Définition 1

(1) *Des monoïdes $S_1, \ldots, S_n$ de l'anneau $\mathbf{A}$ sont dits* comaximaux *si un idéal de $\mathbf{A}$ qui coupe chacun des S_i contient toujours* 1*, autrement dit si on a :*

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

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

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

En algèbre classique (avec l'axiome de l'idéal premier) cela revient à dire dans le premier cas que les ouverts de Zariski $\mathbf{U}_{S_i}$ recouvrent $\mathrm{Spec}(\mathbf{A})$ et dans le deuxième cas que les ouverts de Zariski $\mathbf{U}_{S_i}$ recouvrent l'ouvert $\mathbf{U}_S$. Du point de vue constructif, $\mathrm{Spec}(\mathbf{A})$ est un espace topologique connu via ses ouverts $\mathbf{U}_S$ mais dont les points sont souvent difficilement accessibles.

Un recouvrement de recouvrements est un recouvrement (calculs immédiats) :

Lemme 2 (associativité et transitivité des recouvrements)

(1) *(associativité) Si les monoïdes $S_1, \ldots, S_n$ de l'anneau $\mathbf{A}$ recouvrent le monoïde S et si chaque S_ℓ est recouvert par des monoïdes $S_{\ell,1}, \ldots, S_{\ell,m_\ell}$, alors les $S_{\ell,j}$ recouvrent S.*

(2) *(transitivité) Soit S un monoïde de l'anneau $\mathbf{A}$ et $S_1, \ldots, S_n$ des monoïdes comaximaux de l'anneau $\mathbf{A}_S$. Pour $\ell = 1, \ldots, n$ soit V_ℓ le monoïde de $\mathbf{A}$ formé par les numérateurs des éléments de S_ℓ. Alors les monoïdes $V_1, \ldots, V_n$ recouvrent S*

Définition et notation 3 *Soient I et U deux parties de $\mathbf{A}$. Nous noterons $\mathcal{M}(U)$ le monoïde engendré par U, $\mathcal{I}_{\mathbf{A}}(I)$ ou $\mathcal{I}(I)$ l'idéal engendré par I et $\mathcal{S}(I;U)$ le monoïde $\mathcal{M}(U)+\mathcal{I}(I)$. Si $I=\{a_1,\ldots,a_k\}$ et $U=\{u_1,\ldots,u_\ell\}$, on note respectivement $\mathcal{M}(U)$, $\mathcal{I}(I)$ et $\mathcal{S}(I;U)$ par $\mathcal{M}(u_1,\ldots,u_\ell)$, $\mathcal{I}(a_1,\ldots,a_k)$ et $\mathcal{S}(a_1,\ldots,a_k;u_1,\ldots,u_\ell)$.*

Il est clair que si u est égal au produit $u_1\cdots u_\ell$, les monoïdes $\mathcal{S}(a_1,\ldots,a_k;u_1,\ldots,u_\ell)$ et $\mathcal{S}(a_1,\ldots,a_k;u)$ sont équivalents.

Notez que lorsqu'on localise en $S=\mathcal{S}(I;U)$, les éléments de U deviennent inversibles et ceux de I se retrouvent dans le radical de $\mathbf{A}_S$.

Notre sentiment est que la "bonne catégorie" serait celle dont les objets sont les couples $(\mathbf{A},I)$ où $\mathbf{A}$ est un anneau commutatif et I un idéal contenu dans le radical de $\mathbf{A}$, et les flèches de $(\mathbf{A},I)$ vers $(\mathbf{A}',I')$ sont les homomorphismes $f:\mathbf{A}\to\mathbf{A}'$ tels que $f(I)\subset I'$. On retrouve les anneaux usuels en prenant $I=0$ et les anneaux locaux (avec la notion de morphisme local) en prenant I égal à l'idéal maximal. Pour "localiser" un objet $(\mathbf{A},I)$ dans cette catégorie, on utilise un monoïde U et un idéal J de manière à former le nouvel objet $(\mathbf{A}_{\mathcal{S}(J_1;U)},J_1\mathbf{A}_{\mathcal{S}(J_1;U)})$, où $J_1=I+J$.

Le lemme fondamental suivant récupère la mise constructivement lorsqu'on relit avec un anneau arbitraire une preuve donnée dans le cas d'un anneau local.

Lemme 4 *Soit U et I des parties de l'anneau $\mathbf{A}$ et $a\in\mathbf{A}$, alors les monoïdes $\mathcal{S}(I;U,a)$ et $\mathcal{S}(I,a;U)$ recouvrent le monoïde $\mathcal{S}(I;U)$.*

Preuve Pour $x\in\mathcal{S}(I;U,a)$ et $y\in\mathcal{S}(I,a;U)$ on doit trouver une combinaison linéaire $x_1x+y_1y\in\mathcal{S}(I;U)$ ($x_1,y_1\in\mathbf{A}$). On écrit $x=u_1a^k+j_1$, $y=(u_2+j_2)-(az)$ avec $u_1,u_2\in\mathcal{M}(U)$, $j_1,j_2\in\mathcal{I}(I)$, $z\in\mathbf{A}$. L'identité classique $c^k-d^k=(c-d)\times\cdots$ donne un $y_2\in\mathbf{A}$ tel que $y_2y=(u_2+j_2)^k-(az)^k=(u_2^k+j_3)-(az)^k$ et on écrit $z^kx+u_1y_2y=u_1u_2^k+u_1j_3+j_1z^k=u_4+j_4$. □

On en déduit le principe général de décryptage suivant, qui *permet d'obtenir automatiquement une version quasi-globale d'un théorème à partir de sa version locale.*

Principe général 5 *Lorsqu'on relit une preuve explicite, donnée pour le cas où l'anneau $\mathbf{A}$ est local, 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)*

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

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.

On notera que si $b=a/(u+i)$ avec $u\in\mathcal{M}(U)$ et $i\in\mathcal{I}(I)$ et si la disjonction porte sur "$b\in\mathbf{A}^\times\ \vee\ b\in\mathrm{Rad}(\mathbf{A})$", alors il faut considérer les localisés $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$.

Les exemples suivants sont fréquents et résultent immédiatement des lemmes 2 et 4, sauf le premier qui se fait par un petit calcul simple.

Exemples 6 Soit $\mathbf{A}$ un anneau, U et I des parties de $\mathbf{A}$, $S=\mathcal{S}(I;U)$.

(1) Soient $s_1,\ldots,s_n\in\mathbf{A}$ des éléments comaximaux (c'est-à-dire tels que $\mathcal{I}(s_1,\ldots,s_n)=\mathbf{A}$). Alors les monoïdes $S_i=\mathcal{M}(s_i)$ sont comaximaux.
Plus généralement, si $t_1,\ldots,t_n\in\mathbf{A}$ sont des éléments comaximaux dans $\mathbf{A}_S$, les monoïdes $\mathcal{S}(I;U,t_i)$ recouvrent le monoïde S.

(2) Soient $s_1, \ldots, s_n \in \mathbf{A}$. Les monoïdes $S_1 = \mathcal{S}(0; s_1)$, $S_2 = \mathcal{S}(s_1; s_2)$, $S_3 = \mathcal{S}(s_1, s_2; s_3)$, ..., $S_n = \mathcal{S}(s_1, \ldots, s_{n-1}; s_n)$ et $S_{n+1} = \mathcal{S}(s_1, \ldots, s_n; 1)$ sont comaximaux.
Plus généralement, les monoïdes $V_1 = \mathcal{S}(I; U, s_1)$, $V_2 = \mathcal{S}(I, s_1; U, s_2)$, $V_3 = \mathcal{S}(I, s_1, s_2; U, s_3)$, ..., $V_n = \mathcal{S}(I, s_1, \ldots, s_{n-1}; U, s_n)$ et $V_{n+1} = \mathcal{S}(I, s_1, \ldots, s_n; U)$ recouvrent le monoïde S.

(3) Si $S, S_1, \ldots, S_n \subset \mathbf{A}$ sont des monoïdes comaximaux et si $b = a/(u+i) \in \mathbf{A}_S$ alors $\mathcal{S}(I; U, a), \mathcal{S}(I, a; U), S_1, \ldots, S_n \in \mathbf{A}$ sont comaximaux.

1.2 Du quasi-global au global

Différentes variantes du principe local-global abstrait en algèbre commutative ont leur contrepartie concrète dans laquelle la localisation en tout idéal premier est remplacée par la localisation en une famille finie de monoïdes comaximaux.

Autrement dit, dans ces versions "concrètes" on affirme que certaines propriétés passent du quasi-global au global.

Citons par exemple les résultats suivants, qui sont souvent utiles pour terminer notre travail de relecture constructive.

Principe local-global concret 7 *Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$ et soit $a, b \in \mathbf{A}$. Alors on a les équivalences suivantes :*

(1) *Recollement concret des égalités :*

$$a = b \quad \text{dans} \quad \mathbf{A} \qquad \Longleftrightarrow \qquad \forall i \in \{1, \ldots, n\} \;\; a/1 = b/1 \quad \text{dans} \quad \mathbf{A}_{S_i}$$

(2) *Recollement concret des non diviseurs de zéro :*

$$\begin{array}{c} a \text{ est non diviseur de zéro dans } \mathbf{A} \qquad \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \;\; a/1 \;\; \text{est non diviseur de zéro dans } \mathbf{A}_{S_i} \end{array}$$

(3) *Recollement concret des inversibles :*

$$\begin{array}{c} a \text{ est inversible dans } \mathbf{A} \quad \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \;\; a/1 \;\; \text{est inversible dans } \mathbf{A}_{S_i} \end{array}$$

(4) *Recollement concret des solutions de systèmes linéaires : soit B une matrice $\in \mathbf{A}^{m\times p}$ et C un vecteur colonne $\in \mathbf{A}^{m\times 1}$.*

$$\begin{array}{c} \text{Le système linéaire } BX = C \text{ admet une solution dans } \mathbf{A}^{p\times 1} \quad \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \text{ le système linéaire } BX = C \text{ admet une solution dans } \mathbf{A}_{S_i}^{p\times 1} \end{array}$$

(5) *Recollement concret de facteurs directs : soit M un sous module de type fini d'un module de présentation finie N.*

$$\begin{array}{c} M \text{ est facteur direct dans } N \quad \Longleftrightarrow \\ \forall i \in \{1, \ldots, n\} \; M_{S_i} \text{ est facteur direct dans } N_{S_i} \end{array}$$

Principe local-global concret 8 (recollement concret de propriétés de finitude pour les modules) *Soient $S_1, \ldots S_n$ des monoïdes comaximaux de $\mathbf{A}$ et soit 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.*

On trouve rarement ces principes énoncés sous cette forme dans la littérature classique usuelle. Citons cependant le petit livre d'algèbre commutative de Knight [11] : le lemme 3.2.3 signale que l'anneau produit $\prod_{i=1}^{k} \mathbf{A}[1/s_i]$ est une extension fidèlement plate de $\mathbf{A}$ lorsque les s_i sont comaximaux. Un certain nombre de propriétés des extensions fidèlement plates sont par ailleurs démontrées. Mis ensemble ces résultats couvrent à peu près les principes local-global concrets 7 et 8.

Dans le style de Quillen, on voit en général énoncé le principe correspondant sous la forme abstraite (on localise en tous les idéaux premiers). Mais la preuve fait souvent intervenir un lemme crucial qui a exactement la signification du principe local-global concret correspondant. Par exemple on pourrait énoncer le principe local-global concret 8 sous la forme suivante "à la Quillen".

Lemme 9 (lemme de propagation pour certaines propriétés de finitude pour les modules)
Soit M un $\mathbf{A}$-module. Les parties I_k suivantes de $\mathbf{A}$ sont des idéaux.

(1) $I_1 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module de type fini* $\}$.

(2) $I_2 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module de présentation finie* $\}$.

(3) $I_3 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module plat* $\}$.

(4) $I_4 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module projectif de type fini* $\}$.

(5) $I_5 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module projectif de rang* k $\}$.

(6) $I_6 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module cohérent* $\}$.

(7) $I_7 = \{\ s \in \mathbf{A}\ :\ M_s$ *est un* $\mathbf{A}_s$*-module noethérien* $\}$.

Remarque 10 De manière générale soit une propriété P qui reste vraie après localisation en un monoïde. Alors la version *principe local-global concret pour des éléments comaximaux* :

– pour tout anneau $\mathbf{A}$, si P est vraie après localisation en des éléments comaximaux de $\mathbf{A}$, alors elle est vraie dans $\mathbf{A}$,

et la version *lemme de propagation* :

– l'ensemble $I_P = \{\ s \in \mathbf{A}\ :\ P$ est vraie dans $\mathbf{A}_s\ \}$, est un idéal de $\mathbf{A}$,

sont équivalentes. D'une part la version lemme de propagation implique clairement la première. Dans l'autre sens, si $s, s' \in I_P$ et $t = s + s'$ alors $s/1$ et $s'/1$ sont des éléments comaximaux de $\mathbf{A}_t$ et P est vraie dans $(\mathbf{A}_t)_s \simeq (\mathbf{A}_s)_t \simeq \mathbf{A}_{st}$ et $(\mathbf{A}_t)_{s'} \simeq (\mathbf{A}_{s'})_t \simeq \mathbf{A}_{s't}$ donc par le principe local-global concret vraie dans $\mathbf{A}_t$.
Notons aussi qu'en général on a pour tout monoïde S l'implication suivante

– P vraie dans $\mathbf{A}_S \Rightarrow P$ vraie dans $\mathbf{A}_s$ pour un $s \in S$,

ce qui donne l'équivalence du *principe local-global concret pour les éléments comaximaux* et du *principe local-global concret pour les monoïdes comaximaux*. Ceci nous est en général indispensable car notre système de relecture (principe général 5) produit naturellement une version quasi-globale avec des monoïdes comaximaux plutôt qu'avec des éléments comaximaux.

2 Théorèmes de Horrocks, versions constructives

2.1 Preuves constructives du théorème local et du théorème quasi-global

Si $\mathbf{G}$ est un sous-groupe de $\mathbb{GL}_n(\mathbf{A})$ et $A, B \in \mathbf{A}^{n\times 1}$ nous noterons $A \overset{\mathbf{G}}{\simeq} B$ pour $\exists H \in \mathbf{G},\ HA = B$. Il est clair qu'il s'agit d'une relation d'équivalence.

Nous sommes intéressés par la possibilité de trouver dans la classe d'équivalence d'un vecteur défini sur $\mathbf{A}[X]$ un vecteur défini sur $\mathbf{A}$, en un sens convenable. La remarque banale suivante nous sera utile.

Remarque 11 Soit $f(X) \in \mathbf{A}[X]^{n\times 1}$. Alors on a :

$$f(X) \overset{\mathbb{SL}_n(\mathbf{A}[X])}{\simeq} f(0) \iff \exists g \in \mathbf{A}^{n\times 1}\ \ f(X) \overset{\mathbb{SL}_n(\mathbf{A}[X])}{\simeq} g.$$

En effet si $f(X) = H(X)g$ avec $H(X) \in \mathbb{SL}_n(\mathbf{A}[X])$, alors $f(0) = H(0)g$.

Nous utiliserons aussi le lemme suivant :

Lemme 12 *Soit* $\mathbf{A}$ *un anneau et* $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ *un vecteur unimodulaire dans* $\mathbf{A}[X]^{n\times 1}$*, avec* f_1 *unitaire de degré* d *et* $f_2, \ldots, f_n$ *de degrés* $< d$*. Notons* $f_{i,j}$ *le coefficient de* X^j *dans* f_i*. Alors l'idéal engendré par les* $f_{i,j}$ *pour* $i = 2, \ldots, n$ *contient* 1*.*

Preuve du lemme Soit I cet idéal. On a : $1 \equiv u_1 f_1$ modulo I. Soit m le degré de u_1 on a $u_{1,m} \equiv 0$ modulo I puisque f_1 est unitaire. De proche en proche, on montre en descendant que tous les coefficients $u_{1,j}$ de u_1 sont dans I. Supposons qu'on l'ait déjà montré pour $j+1, \ldots, m$. Exprimons le coefficient de degré $j+d$ dans $u_1 f_1$. On trouve $0 = u_{1,j} + u_{1,j+1} f_{1,d-1} + \cdots$ ce qui donne $0 \equiv u_{1,j}$ modulo I. Donc finalement $1 \equiv u_1 f_1 \equiv 0$ modulo I. □

Théorème de Horrocks local
Soit un entier $n \geq 3$*,* $\mathbf{A}$ *un anneau local et* $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ *un vecteur unimodulaire dans* $\mathbf{A}[X]^{n\times 1}$*, avec* f_1 *unitaire. Alors*

$$f(X) = \begin{bmatrix} f_1 \\ \vdots \\ \vdots \\ f_n \end{bmatrix} \overset{\mathbb{E}_n(\mathbf{A}[X])}{\simeq} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Preuve Soit d le degré de f_1. Par manipulations élémentaires de lignes, on ramène $f_2, \ldots, f_n$ à être de degrés $< d$. Notons $f_{i,j}$ le coefficient de X^j dans f_i. Le vecteur ${}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ reste unimodulaire. Si $d = 0$ c'est terminé. Sinon vu le lemme 12 et puisque l'anneau est local, l'un des $f_{i,j}$ pour $i = 2, \ldots, n$ est une unité. Supposons par exemple que $f_{2,k}$ est inversible. On va voir que l'on peut trouver deux polynomes v_1 et v_2 tels que le polynome $g_2 = v_1 f_1 + v_2 f_2$ soit unitaire de degré $d-1$. Si $k = d-1$ cela marche avec $v_1 = 0$ et v_2 constant. Si $k < d-1$ considérons la disjonction suivante

$$f_{2,d-1} \in \mathbf{A}^\times \ \vee\ f_{2,d-1} \in \mathrm{Rad}(\mathbf{A}).$$

Dans le premier cas, on est ramené à $k = d-1$. Dans le deuxième cas le polynome $q_2 = X f_2 - f_{2,d-1} f_1$ est de degré $\leq d-1$ et vérifie : $q_{2,k+1}$ est une unité. On a donc gagné un cran. Il suffit donc d'itérer le processus.

Nous avons donc maintenant $g_2 = v_1 f_1 + v_2 f_2$ de degré $d-1$ et unitaire. On peut donc diviser f_3 par g_2 et on obtient $g_3 = f_3 - g_2 q$ de degré $< d-1$ ($q \in \mathbf{A}$), donc le polynome

$$h_1 = g_2 + g_3 = f_3 + g_2(1-q) = f_3 + (1-q)v_1 f_1 + (1-q)v_2 f_2$$

est unitaire de degré $d-1$. Ainsi par une manipulation élémentaire de lignes on a pu remplacer ${}^{\mathrm{t}}(f_1, f_2, f_3)$ par ${}^{\mathrm{t}}(f_1, f_2, h_1)$ avec h_1 unitaire de degré $d-1$.
Nous pouvons donc par une suite de transformations élémentaires de lignes ramener ${}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ avec f_1 unitaire de degré d à ${}^{\mathrm{t}}(h_1(X), \ldots, h_n(X))$ avec h_1 unitaire de degré $d-1$. □

Le lemme suivant est immédiat.

Lemme 13 *Soit* $\mathbf{A}$ *un anneau,* S *un monoïde dans* $\mathbf{A}$*. Soit une matrice* $H(X) \in \mathbb{E}_n(\mathbf{A}_S[X])$*, alors il existe* $s \in S$ *tel que* $H(X) \in \mathbb{E}_n(\mathbf{A}[1/s][X])$*.*

Théorème de Horrocks quasi-global
Soit un entier $n \geq 3$*,* $\mathbf{A}$ *un anneau et* $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ *un vecteur unimodulaire dans* $\mathbf{A}[X]^{n\times 1}$*, avec* f_1 *unitaire. Alors il existe des éléments comaximaux* $a_1, \ldots, a_\ell$ *tels que*

$$f(X) = \begin{bmatrix} f_1 \\ \vdots \\ \vdots \\ f_n \end{bmatrix} \overset{\mathbb{E}_n(\mathbf{A}[1/a_i][X])}{\simeq} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Autrement dit pour chaque $i = 1, \ldots, \ell$ il existe une matrice $H_i(X) \in \mathbb{E}_n(\mathbf{A}[1/a_i][X])$ telle que $H_i(X) f(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

Preuve En relisant la preuve du théorème local comme on l'a indiqué dans la section 1.1, on voit que, pour faire descendre le degré de d à $d-1$ il faut, après avoir rendu les degrés de $f_2, \ldots, f_n$ strictement inférieurs à d par division euclidienne, rendre inversible l'un des $f_{i,j}$ pour $i = 2, \ldots, n$. Et on sait que les $f_{i,j}$ sont comaximaux d'après le lemme 12. Ensuite, on utilise plusieurs fois (au plus $d-1$ fois) une disjonction du type

$$f_{2,d-1} \in \mathbf{A}^\times \ \vee \ f_{2,d-1} \in \mathrm{Rad}(\mathbf{A}),$$

(dans le cas inversible le calcul se termine sans nouvelle disjonction). Notre relecture de la preuve, pour faire descendre le degré de d à $d-1$ crée donc des localisés $\mathbf{A}_{S_j}$ (avec les S_j comaximaux) dont le nombre est majoré par $d(n-1)(d-1)$.
La mise à plat complète de la preuve crée en définitive des localisés (avec des monoïdes comaximaux) dont le nombre est majoré par

$$d(d-1)(n-1) \times \cdots \times 6(n-1) \times 2(n-1) \times (n-1) \ \leq \ (d!)^2 \times (n-1)^d < (nd^2)^d.$$

Pour chacun des localisés $\mathbf{A}_i$ on a une matrice $H_i(X) \in \mathbb{E}_n(\mathbf{A}_i[X])$ telle que $H_i(X) f(X) = {}^{\mathrm{t}}(1, 0, \ldots, 0)$. On termine en appliquant le lemme 13. □

Remarque 14 Ce calcul peut être fait dans la situation générique où l'entier n ainsi que les degrés des f_i et les degrés des u_i sont fixés dans l'égalité polynomiale

$$u_1 f_1 + \cdots + u_n f_n = 1 \quad (*).$$

En outre on prend tous les coefficients comme des indéterminées, soumises aux seules relations données par l'égalité $(*)$.

2.2 Un principe local-global concret

Les calculs dans cette section n'ont rien de bien original, mais leur agencement et l'interprétation que nous leur donnons en termes de principe local-global concret nous semblent particulièrement éclairants.

Lemme 15 *Soit* $\mathbf{A}$ *un anneau intègre,* $b \in \mathbf{A}$ *et* $H(X) \in \mathbb{SL}_n(\mathbf{A}[1/b][X])$*. Alors pour un* $a \in \mathbf{A}$ *égal à une certaine puissance de* b *on a* $H(X+aY)H(X)^{-1} \in \mathbb{SL}_n(\mathbf{A}[X,Y])$*.*
De manière équivalente : si S *est un monoïde de* $\mathbf{A}$ *et* $H(X) \in \mathbb{SL}_n(\mathbf{A}_S[X])$*, alors pour un* $s \in S$ *on a* $H(X+sY)H(X)^{-1} \in \mathbb{SL}_n(\mathbf{A}[X,Y])$*.*

Preuve Soit $L(X) = s_1 H(X) \in \mathbf{M}_n(\mathbf{A}[X])$ avec $s_1 \in S$ et

$$s = s_1^n = \det(L(X)) = \det(L(X+Y)).$$

Soit $M(X)$ la matrice cotransposée de $L(X)$. On considère la matrice

$$B(X,Y) = H(X+Y)H(X)^{-1} = L(X+Y)L(X)^{-1} = s^{-1}L(X+Y)M(X) = s^{-1}B_1(X,Y).$$

On a $B_1(X,Y) \in \mathbf{A}[X,Y]$, $B_1(X,0) = s\mathrm{I}_n$ et donc $B_1(X,Y) = s\mathrm{I}_n + YC_1(X,Y))$ avec $C_1(X,Y) \in \mathbf{A}[X,Y]$. Donc $B_1(X,sY) = s(\mathrm{I}_n + YC_1(X,sY)$ et $H(X+sY)H(X)^{-1} = s^{-1}B_1(X,sY) = \mathrm{I}_n + YC_1(X,sY) \in \mathbf{A}[X,Y]$. □

Corollaire 16 *Soit* $\mathbf{A}$ *un anneau intègre,* S *un monoïde de* $\mathbf{A}$ *et* $f(X) \in \mathbf{A}[X]^{n\times 1}$*. Alors*

$$f(X) \overset{\mathbb{SL}_n(\mathbf{A}_S[X])}{\simeq} f(0) \implies \exists s \in S \;\; f(X+sY) \overset{\mathbb{SL}_n(\mathbf{A}[X,Y])}{\simeq} f(X)$$

Preuve Si $f(X) = H(X)f(0)$ avec $H(X) \in \mathbb{SL}_n(\mathbf{A}_S[X])$ alors $f(X+sY) = H(X+sY)f(0)$ et $H(X+sY)H(X)^{-1}f(X) = f(X+sY)$. Il suffit donc de prendre s comme dans le lemme 15. □

Lemme 17 *Soit* $f(X) \in \mathbf{A}[X]^{n\times 1}$*, soit*

$$I = \left\{ a \in \mathbf{A} \;:\; f(X+aY) \overset{\mathbb{SL}_n(\mathbf{A}[X,Y])}{\simeq} f(X) \right\}.$$

Alors I *est un idéal de* $\mathbf{A}$*.*

Preuve Si $f(X+aY) = P_a(X,Y)f(X)$ et $f(X+bY) = P_b(X,Y)f(X)$ alors,

$f(X+(a+b)Y) = f((X+aY)+bY) = P_b(X+aY,Y)f(X+aY) = P_b(X+aY,Y)P_a(X,Y)f(X)$

et $f(X+acY) = P_a(X,cY)f(X)$. □

Le corollaire 16 et le lemme 17 mis ensemble peuvent être énoncés sous forme d'un principe local-global concret :

Principe local-global concret 18 *Soient* $\mathbf{A}$ *un anneau intègre,* $S_1, \ldots, S_k$ *des monoïdes comaximaux et* $f(X) \in \mathbf{A}[X]^{n\times 1}$*. Alors*

$$f(X) \overset{\mathbb{SL}_n(\mathbf{A}[X])}{\simeq} f(0) \iff \bigwedge_{i=1}^{k} f(X) \overset{\mathbb{SL}_n(\mathbf{A}_{S_i}[X])}{\simeq} f(0).$$

Preuve En appliquant les résultats précédents on obtient

$$f(X+Y) \overset{\mathbb{SL}_n(\mathbf{A}[X,Y])}{\simeq} f(X)$$

c'est-à-dire $f(X+Y) = Q(X,Y)f(X)$ avec $Q(X,Y) \in \mathbb{SL}_n(\mathbf{A}[X,Y])$ et donc aussi, en faisant $X=0$, $f(Y) = Q(0,Y)f(0)$. □

2.3 Preuve du théorème global et de la conjecture de Serre

Le principe local-global concret 18 permet de transformer le théorème de Horrocks quasi-global en sa version globale, de manière constructive.

Théorème de Horrocks global
Soit un entier $n \geq 3$, $\mathbf{A}$ un anneau intègre et $f(X) = {}^{\mathrm{t}}(f_1(X), \ldots, f_n(X))$ un vecteur unimodulaire dans $\mathbf{A}[X]^{n\times 1}$, avec f_1 unitaire, alors il existe une matrice $H \in \mathbb{SL}_n(\mathbf{A}[X])$ telle que $H(X)f(X) = f(0)$.

Preuve Vue la remarque 11 on applique le théorème quasi-global puis le principe local-global concret 18. □

Remarque 19 Si l'anneau générique décrit dans la remarque 14 est intègre (ce qui semble probable), le calcul peut être fait une fois pour toutes (dans cet anneau) et se spécialise ensuite dans n'importe quel anneau, intègre ou non, ce qui permet d'enlever l'hypothèse d'intégrité dans le théorème global.

Théorème de Quillen-Suslin
Soit $\mathbf{K}$ un corps, $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_r]$ et dans $\mathbf{A}^{n\times 1}$ un vecteur unimodulaire

$$f = {}^{\mathrm{t}}(f_1(X_1, \ldots, X_r), \ldots, f_n(X_1, \ldots, X_r)),$$

alors il existe une matrice $H \in \mathbb{SL}_n(\mathbf{A})$ telle que $Hf = {}^{\mathrm{t}}(1, 0, \ldots, 0)$.

Preuve Si $n = 1$ ou 2, le résultat est immédiat. Si $n > 2$ et $r = 1$ le résultat provient du fait que $\mathbf{A}$ est un anneau principal. Il est donné explicitement par une réduction de Smith de la matrice colonne f. Pour $r \geq 2$ on raisonne par induction sur r. En appliquant le théorème de Horrocks global à l'anneau $\mathbf{B} = \mathbf{K}[X_1, \ldots, X_{r-1}]$ on a gagné si l'un des f_i est un polynome unitaire en X_r. Si le corps a suffisamment d'éléments, on obtient cela par un changement linéaire de variable. Sinon, on fait un changement de variable à la Nagata : $Y_r = X_r$, et pour $1 \leq j < r$, $Y_j = X_j + X_r^{d^j}$, avec un entier d suffisamment grand. □

Solution de la conjecture de Serre (Quillen-Suslin)
Soit $\mathbf{K}$ un corps, $\mathbf{A} = \mathbf{K}[X_1, \ldots, X_r]$ et M un $\mathbf{A}$-module projectif de type fini stablement libre, alors M est libre.

Preuve On a par hypothèse un isomorphisme

$$\varphi : \mathbf{A}^k \oplus M \longrightarrow \mathbf{A}^{\ell+k}$$

pour deux entiers k et ℓ. Si $k = 0$ il n'y a rien à faire. Supposons $k > 0$. Le vecteur $f = \varphi((e_{k,1}, 0_M))$ (où $e_{k,1}$ est le premier vecteur de la base canonique de $\mathbf{A}^k$) est unimodulaire : considérer la forme linéaire λ sur $\mathbf{A}^{\ell+k}$ qui à un vecteur y fait correspondre la première coordonnée de $\varphi^{-1}(y)$. On a $\lambda(y_1, \ldots, y_{k+\ell}) = u_1y_1 + \cdots + u_{k+\ell}y_{k+\ell}$ et $\lambda(f) = 1$.
Considérons f comme un vecteur colonne. En composant φ avec l'isomorphisme donné dans le théorème de Quillen-Suslin on obtient un isomorphisme ψ qui envoie $(e_{k,1}, 0_M)$ sur $e_{k+\ell,1}$. En passant au quotient par $\mathbf{A}(e_{k,1}, 0_M)$ et $\mathbf{A}e_{k+\ell,1}$ on obtient un isomorphisme

$$\theta : \mathbf{A}^{k-1} \oplus M \longrightarrow \mathbf{A}^{\ell+k-1}.$$

□

3 Une preuve constructive d'un théorème de stabilité de Suslin

Dans cette section, nous examinons la preuve du théorème de stabilité de Suslin dans le cas des corps, telle qu'elle est donnée dans [9] en s'appuyant sur une méthode locale-globale. Nous la décryptons en une preuve constructive selon la méthode exposée dans la section 1.

3.1 Un théorème local et sa version quasi-globale

Le seul véritable argument non constructif dans [9] est *l'utilisation* du lemme II 3.6 page 46. Ce lemme est de nature locale mais il est ensuite utilisé dans un argument de type local-global. C'est le lemme suivant, dans lequel $\binom{f}{g}$ désigne le symbole de Mennicke.

Lemme 20 *(local)*
Soit $\mathbf{A}$ *un anneau local et* $f, g \in \mathbf{A}[X]$ *avec* f *unitaire et* $af + bg = 1$. *Alors on a :*

$$\binom{f}{g} = \binom{f(0)}{g(0)} = 1.$$

Preuve (cf. [9])
Notons pour commencer qu'on peut diviser b par f et qu'on obtient alors une égalité $a_1 f + b_1 g = 1$ avec $\deg(b_1) < \deg(f)$ et donc, puisque f est unitaire, $\deg(a_1) < \deg(g)$. Nous supposerons donc sans perte de généralité que $\deg(b) < \deg(f)$ et $\deg(a) < \deg(g)$.
Rappelons que $\mathbb{E}_n(\mathbf{A})$ est un sous-groupe distingué de $\mathbb{SL}_n(\mathbf{A})$ si $n \geq 3$, et que le symbole de Mennicke $\binom{f}{g}$ représente la classe d'équivalence de la matrice

$$B = \begin{bmatrix} f & g & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

dans le groupe quotient $\mathbb{SL}_3/\mathbb{E}_3$ (la classe d'équivalence ne dépend pas du choix de a et b), et qu'on a les propriétés suivantes (cf. Proposition II 3.5 page 44 dans [9]) :

$$\binom{u}{a} = \binom{1}{0} = 1 \text{ pour } u \in \mathbf{A}^\times,\ \binom{aa'}{b} = \binom{a}{b}\binom{a'}{b},\ \binom{a}{b} = \binom{b}{a},\ \binom{a+bd}{b} = \binom{a}{b}.$$

Soit r le reste de la division euclidienne de g par f. Alors $\binom{f}{g} = \binom{f}{r}$. En particulier si $\deg(f) = 0$ on a terminé. Sinon on peut supposer $\deg(g) < \deg(f)$ et on raisonne par induction sur $\deg(f)$.
Puisque $\mathbf{A}$ est local, $g(0)$ est inversible ou dans le radical $\mathcal{M}$ de $\mathbf{A}$.
Supposons tout d'abord $g(0)$ inversible. Alors

$$\binom{f}{g} = \binom{f - g(0)^{-1} f(0) g}{g}$$

si bien que nous pouvons supposer $f(0) = 0$ et $f = X f_1$. Alors

$$\binom{X f_1}{g} = \binom{X}{g}\binom{f_1}{g} = \binom{X}{g(0)}\binom{f_1}{g} = \binom{f_1}{g}$$

et la preuve est terminée par induction puisque f_1 est unitaire.
Supposons maintenant que $g(0)$ est dans $\mathcal{M}$. On note que $a(0)f(0)+b(0)g(0)=1$, donc $a(0)f(0)\in 1+\mathcal{M}\subseteq \mathbf{A}^\times$ et donc $a(0)\in\mathbf{A}^\times$. Or

$$\begin{bmatrix} f & g & 0\\ -b & a & 0\\ 0 & 0 & 1\end{bmatrix} \equiv \begin{bmatrix} f-b & g+a & 0\\ -b & a & 0\\ 0 & 0 & 1\end{bmatrix} \mod \mathbb{E}_3(\mathbf{A}[X]),$$

donc

$$\begin{pmatrix} f\\ g\end{pmatrix} = \begin{pmatrix} f-b\\ g+a\end{pmatrix}$$

avec $f-b$ unitaire de même degré que f, $\deg(g+a)<\deg(f)$ et $(g+a)(0)\in\mathbf{A}^\times+\mathcal{M}=\mathbf{A}^\times$. On est donc ramené au cas précédent. La preuve est complète. □

Notre machinerie de relecture automatique de la preuve locale donne le lemme quasi-global suivant (qui ne se trouve pas dans [9]), par application directe du principe général 5 :

Lemme 21 *(quasi-global)*
Soit $\mathbf{A}$ *un anneau et* $f,g\in\mathbf{A}[X]$ *avec* f *unitaire et* $af+bg=1$. *Alors, il existe dans* $\mathbf{A}$ *des éléments comaximaux* s_i *tels que dans chaque localisé* $\mathbf{A}[1/s_i]$ *on ait l'égalité des symboles de Mennicke suivante*

$$\begin{pmatrix} f\\ g\end{pmatrix} = \begin{pmatrix} f(0)\\ g(0)\end{pmatrix} = 1.$$

3.2 Un principe local-global concret et la preuve constructive d'un théorème global

Maintenant nous rappelons le lemme I 5.9 page 26 dans [9].

Lemme 22 *Soit* $n\geq 3$ *et* $A\in\mathbb{SL}_n(\mathbf{A}[X])$ *avec* $A(0)=\mathrm{I}_n$. *Soit*

$$I=\{s\in\mathbf{A}\mid A\in\mathbb{E}_n(\mathbf{A}[1/s][X])\}.$$

Alors I *est un idéal de* $\mathbf{A}$.

La belle preuve constructive de ce beau lemme (dont seule la version abstraite est qualifiée de théorème) occupe les pages 22 à 26 de [9].

Ce lemme aurait pu être reformulé sous la forme du principe local-global concret suivant, qui est d'ailleurs à très peu près le lemme I 5.8 de [9] :

Principe local-global concret 23 *Soient* $n\geq 3$, $\mathbf{A}$ *un anneau,* $S_1,\ldots,S_k$ *des monoïdes comaximaux et* $A\in\mathbb{SL}_n(\mathbf{A}[X])$ *avec* $A(0)=\mathrm{I}_n$. *Alors*

$$A\in\mathbb{E}_n(\mathbf{A}[X]) \iff \bigwedge_{i=1}^{k} A\in\mathbb{E}_n(\mathbf{A}_{S_i}[X])$$

Le principe local-global concret 23 et le lemme 21 donnent alors le théorème global suivant (corollaire II 3.8 de [9]).

Théorème 24 *(version globale du lemme 20)*
Soient $n\geq 3$, $\mathbf{A}$ *un anneau et* $f,g\in\mathbf{A}[X]$ *avec* f *unitaire et* $af+bg=1$. *Alors on a l'égalité des symboles de Mennicke suivante*

$$\begin{pmatrix} f\\ g\end{pmatrix} = \begin{pmatrix} f(0)\\ g(0)\end{pmatrix}.$$

Preuve Soit B la matrice donnée au début de la preuve du lemme 20. L'égalité $\binom{f}{g} = \binom{f(0)}{g(0)}$ signifie : $A = BB(0)^{-1} \in \mathbb{E}_3(\mathbf{A}[X])$. On a évidemment $A(0) = \mathrm{I}_3$. Le principe local-global concret 23 nous dit qu'il suffit de vérifier l'assertion dans des anneaux localisés $\mathbf{A}_{s_i}$ pour une famille s_i d'éléments comaximaux. Et le lemme 21 nous construit cette famille. □

Enfin la preuve que ce corollaire implique le théorème de stabilité de Suslin est simple et constructive, telle que donnée dans [9].

Théorème de stabilité de Suslin (cas des corps)
Si $\mathbf{K}$ *est un corps et* $n \geq 3$, $\mathbb{SL}_n(\mathbf{K}[X_1, \ldots, X_k]) = \mathbb{E}_n(\mathbf{K}[X_1, \ldots, X_k])$.

Remarque 25 Du point de vue constructif, pour faire tourner les algorithmes correspondants au théorème précédent et au théorème de Quillen-Suslin, nous devons supposer que les opérations du corps et le test d'égalité sont explicites, c'est-à-dire dans le langage de l'algèbre constructive ([24]), que le corps est un corps discret. En fait le test d'égalité à 0 est nécessaire pour pouvoir faire les changements de variables en vue de rendre des polynômes unitaires. Enfin il reste un travail intéressant à faire pour rendre constructives des versions plus générales de ces théorèmes. Notamment les versions qui utilisent comme anneau de base, non plus un corps, mais un anneau noethérien de dimension de Krull fixée.

Une preuve de nature différente pour le dernier théorème, utilisant l'artillerie des bases de Gröbner et basée sur la connaissance des vrais idéaux maximaux de $\mathbf{K}[X_1, \ldots, X_n]$ a été donnée par Park et Woodburn dans [25].

Une preuve basée sur les mêmes idées que les nôtres, mais s'appliquant dans un cadre beaucoup plus général (anneaux noethériens de dimension de Krull majorée) nous a été signalée par I. Yengui (cf. [28]).

Références

[1] Almeida M., Blaum M., D'Alfonso L., Solernó P. *Computing bases of complete intersection rings in Noether position.* Journal of Pure and Applied Algebra **162** (2001) 127–170. 4

[2] Almeida M., D'Alfonso L., Solernó P. *On the degrees of bases of free modules over a polynomial ring.* Math. Zeitschrift **231** (1999), 679–706. 4

[3] Caniglia L., Cortinas G., Danón S., Heintz J., Krick T., Solernó P. *Algorithmic Aspects of Suslin's Proof of Serre's Conjecture.* Computational Complexity **3** (1993), 31–55. 4

[4] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* Preprint. 3

[5] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111** (2001), 203–256. 3

[6] Delzell C.N. *Kreisel's unwinding of Artin's proof*, 113–245 in Kreiseliana : About and Around Georg Kreisel, ed. P. Odifreddi, A K Peters, Wellesley, MA, 1996. 3

[7] Feferman S. *Kreisel's "unwinding" program*, 247–273 in Kreiseliana : About and Around Georg Kreisel, ed. P. Odifreddi, A K Peters, Wellesley, MA, 1996. 3

[8] Fitchas N., Galligo A. *Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel.* Math. Nachr. **149** (1990), 231–253. 4

[9] Gupta S., Murthy M. *Suslin's work on linear groups over polynomial rings and Serre conjecture*. ISI Lecture Notes n°8. The Macmillan Company of India Limited. 1980. 4, 5, 14, 15, 16

[10] Horrocks G. *Projective modules over an extension of a local ring*. Proc. Lond. Math. Soc. **14** (1964), 714–718. 4

[11] Knight J. *Commutative Algebra*. London Mathematical Society LNS n°5. Cambridge University Press, 1971. 9

[12] Kunz E. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 1991. 4

[13] Lam T. Y. *Serre's conjecture*. Lecture Notes in Mathematics, Vol. 635. Springer-Verlag, Berlin-New York, 1978. 4

[14] Lang S. *Algebra*. Addison-Wesley, troisième édition. 1993. 4

[15] Laubenbacher, R., Woodburn, C. *An algorithm for the Quillen-Suslin theorem for monoid rings. Algorithms for algebra (Eindhoven, 1996)*. J. Pure Appl. Algebra **117/118** (1997), 395–429. 4

[16] Logar A., Sturmfels B. *Algorithms for the Quillen-Suslin theorem*. J. Algebra **145** no. 1, (1992), 231–239. 4

[17] 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. 1997. 3, 6

[18] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier*. Annals of Pure and Applied Logic **91** (1998), 59–92. 3

[19] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique*. Math. Zeitschrift, **242** (2002), 23–46. 3

[20] Lombardi H. *Hidden constructions in abstract algebra (1) Integral dependance relations*. Journal of Pure and Applied Algebra **167** (2002), 259–267. 3

[21] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive*. Publications Mathématiques de Besançon. Théorie des nombres. 2002. 3

[22] Lombardi H. *Constructions cachées en algèbre abstraite (4) La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier*. Publications Mathématiques de Besançon. Théorie des nombres. 2002. 3

[23] Lombardi H. *Constructions cachées en algèbre abstraite (5) Principe local-global de Pfister et variantes*. Preprint 2002. 3

[24] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra*. Universitext. Springer-Verlag, 1988. 4, 16

[25] Park, H., Woodburn, C. *An algorithmic proof of Suslin's stability theorem for polynomial rings*. J. Algebra **178** no. 1 (1995), 277–298. 4, 16

[26] Quillen D. *Projective modules over polynomial rings*. Invent. Math. **36** (1976), 167–171. 4

[27] Suslin A. *Projective modules over polynomial rings are free. (en Russe)*. Dokl. Akad. Nauk SSSR **229** no. 5 (1976), 1063–1066. 4

[28] Yengui I. *An algorithmic proof of Suslin's stability theorem for Noetherian rings*. Preprint. 16