Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini

H. Lombardi

6 Janvier 97

Laboratoire de Mathématiques de Besançon
URA CNRS 741
UFR des Sciences et Techniques
Université de Franche-Comté
email : lombardi@math.univ-fcomte.fr

Résumé

Nous étudions la structure d'une matrice projecteur F sur un anneau commutatif. Nous explicitons le système fondamental d'idempotents orthogonaux, caché dans cette matrice, pour chacun desquels la matrice a un rang bien défini. De même nous trouvons un nombre fini d'éléments de l'anneau qui l'engendrent en tant qu'idéal et qui permettent d'expliciter le module projectif image de F comme localement libre. Nos preuves sont basées sur le principe local-global abstrait. Nous donnons deux méthodes pour récupérer une preuve constructive des résultats obtenus. La plus intéressante est une interprétation constructive du principe local-global abstrait le plus élémentaire. Il nous semble qu'il s'agit là d'un pas non négligeable dans la mise en place du "programme de Hilbert" pour l'algèbre abstraite, i.e. la traduction *automatique* des preuves d'algèbre abstraite en preuves constructives.

Classification AMS : 03F65, 13C10, 13B10

Mots clés : Mathématiques constructives, Programme de Hilbert, Évaluation dynamique, Modules projectifs de type fini, Matrices de projection, Idéaux de Fitting, Principes local-globals.

Table des matières

Introduction

Dans cet article, tous les anneaux considérés sont commutatifs.
Notre but est de comprendre en termes concrets les théorèmes suivants.

Théorème 1 (caractérisation locale des modules projectifs de type fini) *Un module M sur un anneau A est projectif de type fini si et seulement si il est* localement libre *au sens suivant : il existe $s_1, \ldots, s_m$ dans A tels que,*
• $s_1A + \cdots + s_mA = A$, *et*
• *les M_{s_i} obtenus à partir de M en étendant les scalaires aux A_{s_i} (A_s désigne le localisé où on autorise le dénominateur s) sont libres.*

Théorème 2 (décomposition d'un module projectif de type fini en somme directe de modules de rang constant) *Si M est un module projectif de type fini sur un anneau A engendré par n éléments, il existe un système fondamental d'idempotents orthogonaux $r_0, r_1, \ldots, r_n$ tel que chaque localisé M_{r_k} soit un module projectif de rang k sur A_{r_k}. En outre A est naturellement isomorphe à $A_{r_0} \times A_{r_1} \times \cdots \times A_{r_n}$ et M à $M_{r_0} \times M_{r_1} \times \cdots \times M_{r_n}$.*

La partie la plus mystérieuse du théorème 1 est que la condition est nécessaire. En pratique, le module M peut être vu comme l'image dans A^n d'une *matrice de projection* F (i.e., $F^2 = F$) à coefficients dans A. On veut récupérer les s_k à partir des coefficients $f_{i,j}$ de F. De même dans le théorème 2 on veut récupérer les r_k à partir des coefficients $f_{i,j}$ de F. Ceci est réalisé dans les théorèmes 3 et 4.

L'idée générale pour obtenir ces résultats est la suivante. On remarque pour commencer que si A est intègre, le module est de rang k avec $0 \leq k \leq n$ et le polynome[1] caractéristique de F est alors $(X-1)^k X^{n-k}$. Son coefficient de degré $n-k$ est égal à $(-1)^k$ et c'est la somme des mineurs diagonaux d'ordre k. Ce sont ces mineurs qu'il faut prendre comme s_i pour obtenir les localisés libres dans le théorème 1. Enfin, si on ne suppose pas A intègre, et notamment dans le cas générique, les rangs possibles se mélangent de manière bien contrôlée grâce à un système fondamental d'idempotents orthogonaux qui se lisent sur le polynome caractéristique de F.

En fait on est particulièrement intéressé par le cas générique : $A = \mathbf{B}_n = \mathbb{Z}[(f_{i,j})_{1\leq i,j\leq n}]/\mathcal{J}_n$, où $\mathcal{J}_n$ est l'idéal défini par les n^2 relations obtenues en écrivant $F^2 = F$.

Le principe local-global abstrait en algèbre commutative est un principe informel selon lequel certaines propriétés concernant les modules sur les anneaux commutatifs sont vraies si et seulemment si elles sont vraies après localisation en n'importe quel idéal premier. Dans nos preuves, le seul ingrédient non constructif est un principe local-global abstrait de recollement des égalités. La preuve de ce principe utilise des outils hautement non constructifs (dont le recours à la considération de tous les idéaux premiers de A). Dans la section 3, nous expliquons comment interpréter de manière constructive ce principe local-global. En gros, le cadre de l'évalutation dynamique permet de traiter les idéaux premiers de l'anneau comme des objets idéaux présents seulement à l'état latent et parfaitement inoffensifs. Ceci nous permet d'interpréter l'utilisation du principe abstrait de recollement des égalités comme une machinerie purement calculatoire à l'intérieur des évalutations dynamiques. En définitive, nous récupérons une preuve constructive complète des théorèmes concrets que ce principe permet de démontrer.

[1] Depuis 1990, les accents circonflexes ne sont jamais obligatoires sur le "o", n'en déplaise à Messieurs Larousse et Robert.

Il nous semble qu'il s'agit là d'un pas non négligeable dans la mise en place du "programme de Hilbert" pour l'algèbre abstraite, i.e. la traduction automatique des preuves d'algèbre abstraite en preuves constructives[2]. Notre espoir est notamment d'obtenir une relecture constructive automatique du chapitre IV de [7] concernant la méthode générale de passage du local au global.

Les références générales pour ce travail sont les suivantes. Dans [11] on trouve une approche constructive des bases de l'algèbre. Les théorèmes cités ci-dessus, pour lesquels nous demandons une explicitation précise, ainsi que ceux cités dans la section suivante (Rappels) sont dans les traités classiques d'algèbre commutative (cf. par exemple [6], [1], [7], [12].) Plus précisément on peut trouver le théorème 1 comme (partie du) théorème 1 dans [1] chap. II §5, ou comme (partie du) théorème 3.3.7 de [6], on peut trouver le théorème 2 comme exercice 3 dans [1] chap. II §5.

Nous n'avons pas trouvé dans la littérature concernant la structure des modules projectifs de type fini des théorèmes aussi explicites que les théorèmes 4, 5 et 6, que nous donnons à la section 2. Il nous semble également que pour certains autres résultats de nature concrète contenus dans cet article, il n'existait pas pour le moment de preuve entièrement constructive. Nous l'avons alors signalé dans le cours de l'article.

L'article est organisé comme suit. Dans la section 1, nous faisons quelques rappels d'algèbre commutative, dans le but notamment de mettre en valeur le caractère constructif de nombreux théorèmes de base et de présenter quelques aspects du principe local-global.

Dans la section 2, nous donnons une explicitation précise des théorèmes 1 et 2. Nous faisons appel dans la preuve à un principe local-global abstrait élémentaire mais non constructif. Nous terminons en remarquant que dans le cas générique, toute la preuve peut être rendue constructive, moyennnant un gros travail sur les idéaux des anneaux de polynomes à coefficients entiers. Ceci assure la validité constructive de tous les théorèmes de la section 2, dans tous les cas (pas seulement le cas générique).

Dans la section 3, nous donnons une interprétation constructive du principe local-global abstrait de recollement des égalités. Ceci permet de rendre constructives les preuves de la section 2 selon l'esprit du programme de Hilbert : donner une garantie automatique de la validité constructive des résultats concrets obtenus par des méthodes abstraites.

Dans la section 4, nous apportons quelques compléments sur le thème du programme de Hilbert.

Dans l'article en préparation [10], nous donnons un traitement entièrement élémentaire, sans recours aux principes local-globals abstraits ni à leur version dynamique et constructive, des résultats que nous démontrons ici. Dans un autre article en préparation ([9]), nous essayons de tenir la promesse d'une relecture constructive automatique des principes local-globals abstraits dont nous avons connaissance.

Remerciements : Nous remercions Fred Richman pour sa lecture attentive et ses suggestions.

1 Rappels

Nous donnons ici quelques rappels concernant les modules projectifs de type fini et la localisation, de manière à faciliter la lecture de la suite au lecteur ou à la lectrice non averti(e), et à

[2] Du moins lorsque le résultat est de nature concrète

faciliter la discussion, dans la section 3, au sujet du caractère constructif des résultats obtenus précédemment. Le lecteur ou la lectrice[3] qui connaît bien ces sujets mais qui est intéressé(e) par la critique constructive des preuves classiques pourra donc également jeter un coup d'oeil sur cette section.

1.1 Modules de présentation finie

Un module *de présentation finie* est un A-module donné par un nombre fini de générateurs et de relations. De manière équivalente, c'est un module M isomorphe au conoyau d'un homomorphisme

$$g : A^m \to A^q$$

La matrice G de g a pour colonnes les relations entre les générateurs $a_1, \ldots, a_q$ (les images de la base canonique de A^q par g). Une telle matrice s'appelle une *matrice de présentation du module* M. On ne change pas la structure de M lorsqu'on fait subir à G une des transformations suivantes :
— ajout d'une colonne nulle, (ceci ne change pas le module des relations entre des générateurs fixés)
— suppression d'une colonne nulle, sauf à aboutir à une matrice vide,
— remplacement de G, de type $q \times m$, par G' de type $(q+1) \times (m+1)$ obtenue à partir de G en rajoutant une ligne nulle en dessous puis une colonne à droite avec 1 en position $(q+1, m+1)$, (ceci revient à rajouter un vecteur parmi les générateurs, en indiquant sa dépendance par rapport aux générateurs précédents) :

$$G \;\mapsto\; G' \;=\; \begin{pmatrix} G & C \\ 0_{1,m} & 1 \end{pmatrix}$$

— opération inverse de la précédente, sauf à aboutir à une matrice vide,
— ajout à une colonne d'une combinaison linéaire des autres colonnes, (ceci ne change pas le module des relations entre des générateurs fixés)
— ajout à une ligne d'une combinaison linéaire des autres lignes, (ceci revient à changer le système générateur en remplaçant par exemple le générateur a_q par un élément de la forme $a_q - \Sigma_{i=1,\ldots,q-1}\ \lambda_i a_i$ sans changer les autres générateurs)
— permutation de colonnes ou de lignes,
— multiplication d'une colonne ou d'une ligne par un élément inversible (facultatif).

On voit aisément que si G et H sont deux matrices de présentation d'un même module M, on peut passer de l'une à l'autre au moyen des transformations décrites ci-dessus. Un peu mieux : on voit que pour tout système générateur fini de M, on peut construire à partir de G, en utilisant ces transformations, une matrice de présentation de M correspondant au nouveau système générateur. Notez aussi qu'un changement de base de A^q ou A^m correspond à la multiplication de G (à gauche ou à droite) par une matrice inversible, et peut être réalisé par les opérations décrites précédemment.

Un module libre de rang k est présenté par une matrice colonne formée de k zéros.

Il existe un cas facile où une matrice présente un module libre. Rappelons que deux matrices de même type $q \times m$ sont dites *équivalentes* lorsqu'on passe de la première à la seconde en multipliant la première, à droite et à gauche, par deux matrices inversibles.

[3] Désormais, la personne humaine qui intervient au cours de cet article subira la règle inexorable de l'alternance des sexes. Espérons que les lecteurs n'en seront pas plus affectés que les lectrices. En tout cas, cela nous éconmisera bien des "ou" et bien des "(e)".

Lemme de la liberté *Soit M un module de présentation finie, (isomorphe au) conoyau d'une matrice G de type $q \times m$ (i.e. le module est donné par q générateurs soumis à m relations). Si la matrice G contient un mineur d'ordre k inversible et si tous les mineurs d'ordre $(k+1)$ sont nuls, alors elle est équivalente à la matrice canonique*

$$\mathrm{I}_{k,q,m} \;=\; \begin{pmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & 0_{q-k,m-k} \end{pmatrix}$$

Alors, le module M est libre de rang $q-k$. En fait, dans ce cas, l'image, le noyau et le conoyau de G sont libres, respectivement de rangs k, $m-k$ et $q-k$. En outre l'image et le noyau possèdent des supplémentaires libres.

Preuve En permutant éventuellement les lignes et les colonnes on ramène le mineur inversible en haut à gauche. Puis en multipliant à droite (ou à gauche) par une matrice inversible on se ramène à la forme

$$G_1 \;=\; \begin{pmatrix} \mathrm{I}_k & A \\ B & C \end{pmatrix}$$

puis par des manipulations élémentaires de lignes et de colonnes, on obtient

$$G_2 \;=\; \begin{pmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_3 \end{pmatrix}$$

et G_3 est nulle parce que tous les mineurs d'ordre $(k+1)$ de G_2 sont nuls. □

1.2 Modules projectifs de type fini

Ils sont caractérisés de la manière suivante.

Proposition et définition 1.1 (modules projectifs de type fini) *Les propriétés suivantes pour un A-module M sont équivalentes.*
a) M est isomorphe à un facteur direct dans un A-module A^n, i.e. il existe un entier n, un A-module N et un isomorphisme $M \oplus N \to A^n$.
b) Il existe un entier n, des générateurs $(g_i)_{i=1,\dots,n}$ de M et des formes linéaires $(\alpha_i)_{i=1,\dots,n}$ sur M telles que : $\quad \forall x \in M \qquad x = \Sigma\, \alpha_i(x) g_i$.
b') M est de type fini et pour tout système fini de générateurs $(h_i)_{i=1,\dots,m}$ de M il existe des formes linéaires $(\beta_i)_{i=1,\dots,m}$ sur M telles que : $\quad \forall x \in M \qquad x = \Sigma\, \beta_i(x) h_i$.
c) Il existe un entier n et deux applications linéaires $\varphi : M \to A^n$ et $\psi : A^n \to M$ telles que $\psi \circ \varphi = \mathrm{Id}_M$. On a alors $A^n = \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\psi)$ et $M \simeq \mathrm{Im}(\varphi)$.
c') M est de type fini et pour toute application linéaire surjective $\psi : A^m \to M$ il existe une application linéaire $\varphi : M \to A^m$ telle que $\psi \circ \varphi = \mathrm{Id}_M$. On a alors $A^m = \mathrm{Im}(\varphi) \oplus \mathrm{Ker}(\psi)$ et $M \simeq \mathrm{Im}(\varphi)$.

Lorsque ces conditions sont réalisées on dit que le module M est projectif de type fini.

Preuve Le (b) (resp (b')) n'est qu'une reformulation de (c) (resp. (c')).

(a) ⇒ (c) : considérer les applications canoniques $M \to M \oplus N$ et $M \oplus N \to M$.

(c) ⇒ (a) : considérer $\theta = \varphi \circ \psi$. On a $\theta^2 = \theta$. Cela fournit la projection de A^n sur M parallèlement à N.

(b) ⇒ (b') : en exprimant les g_i comme combinaisons linéaires des h_j on obtient les β_j à partir des α_i. □

Une matrice de projection est une matrice carrée F vérifiant $F^2 = F$. En pratique, conformément au (a) ci-dessus, nous considèrerons un module projectif de type fini comme (copie par isomorphisme de l') image d'une matrice de projection F.

Lorsqu'on voit un module projectif de type fini selon la définition (c), la matrice de projection est celle de l'application linéaire $\varphi \circ \psi$. De même, si on utilise la définition (b) la matrice de projection est celle ayant pour entrées les $\alpha_j(g_i)$ en position (i, j).

Si A est un anneau intègre, on obtient par passage au corps des fractions un espace vectoriel de dimension finie k. On en déduit que le polynome caractéristique de la matrice F est égal à $(X-1)^k X^{n-k}$ (nous considérons le polynome caractéristique comme polynome unitaire : $\det(X\mathrm{I}_n - F)$). Ceci caractérise en termes purement calculatoires la dimension k : le premier monome non nul du polynome caractéristique (en partant des bas degrés) est égal à $(-1)^k X^{n-k}$. En outre tous les mineurs d'ordre $k+1$ de F sont nuls.

Ceci conduit à la proposition suivante.

Proposition 1.2 *Soit k un entier naturel et M un module projectif de type fini sur un anneau A non trivial. Alors les conditions suivantes sont équivalentes :*
a) Pour tout idéal premier $\mathcal{P}$ de A, le module $M/\mathcal{P}M$ sur l'anneau intègre $A/\mathcal{P}$ est de rang k (i.e. tout système de $k+1$ éléments est linéairement dépendant et il existe un système de k éléments linéairement indépendant).
a') Pour tout idéal premier $\mathcal{P}$ de A, l'espace vectoriel obtenu à partir de M en étendant les scalaires au corps des fractions de $A/\mathcal{P}$ est de dimension k.
b) Le polynome caractéristique d'une matrice de projection F de type $n \times n$ ayant pour image (un module isomorphe à) M est égal, à des nilpotents près, au polynome $(X-1)^k X^{n-k}$.
b') Même chose que (b), mais pour toute matrice F.
c) Le polynome caractéristique d'une matrice de projection F de type $n \times n$ ayant pour image (un module isomorphe à) M est égal, à des nilpotents près, au polynome $(X-1)^k X^{n-k}$, et tous les mineurs d'ordre $k+1$ de F sont nilpotents.
c') Même chose que (c), mais pour toute matrice F.

Preuve D'un point de vue classique, la preuve est immédiate ; il suffit de se rappeler que l'intersection des idéaux premiers est le nilradical de A, i.e. l'ensemble des nilpotents.
Notez que d'un point de vue constructif, la condition (a) est a priori trop faible (par manque d'idéaux premiers), et les conditions (b) et (c) ne sont pas clairement équivalentes.
Une preuve constructive de l'équivalence de (b) et (b') est une conséquence le lemme qui suit. □

Lemme 1.3 *Soient F_1 de type $m \times m$ et F_2 de type $n \times n$ deux matrices de projection avec des images isomorphes. Alors on a*

$$X^n \det(X\mathrm{I}_m - F_1) = X^m \det(X\mathrm{I}_n - F_2)$$

Preuve On écrit $A^m \simeq M \oplus N_1$ et $A^n \simeq M \oplus N_2$ de sorte que $A^{n+m} \simeq M \oplus N_2 \oplus M \oplus N_1$ on considère l'endomorphisme f de A^{n+m} qui est égal à l'identité sur une composante M et à 0 sur les trois autres composantes. Selon la manière dont on regroupe les termes de la somme directe on trouve pour f une ou l'autre des matrices

$$\begin{pmatrix} F_1 & 0_{m,n} \\ 0_{n,m} & 0_n \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 0_m & 0_{m,n} \\ 0_{n,m} & F_2 \end{pmatrix}$$

qui ont pour polynomes caractéristiques les deux membres de l'égalité à démontrer. □

Ceci justifie constructivement la définition suivante :

Définition 1 *Un module M projectif de type fini sur un anneau A non trivial est dit* de rang constant égal à k *lorsque la condition (b') de la proposition 1.2 est réalisée : le polynome caractéristique d'une matrice de projection F de type $n \times n$ ayant pour image (un module isomorphe à) M est égal, à des nilpotents près, au polynome $(X-1)^k X^{n-k}$.*

En fait, nous verrons plus loin des caractérisations plus agréables des modules projectifs de rang constant. Notamment, on peut "supprimer les nilpotents" dans les conditions (b)–(c').

Remarque 1.4 Avec une preuve tout à fait analogue à celle du lemme 1.3, on peut démontrer que le déterminant (et donc aussi le polynome caractéristique) d'un endomorphisme d'un module projectif de type fini est bien défini[4]. On peut alors lire la condition (b) comme signifiant que le polynome caractéristique de l'endomorphisme Id_M est égal, à des nilpotents près, à $(X-1)^k$.

Convention 2 *Lorsque l'anneau A est trivial (réduit à $\{0\}$) tous les A-modules sont triviaux. Néanmoins, conformément à la définition ci-dessus, il est logique de considérer que le module trivial est projectif de type fini de rang constant égal à k, pour n'importe quelle valeur de l'entier $k \geq 0$. Cette convention permet une formulation plus uniforme des théorèmes et des preuves.*

Définition 3 *Un* anneau local *est un anneau où est vérifié l'axiome suivant :*

$$\forall x \in A \qquad x \text{ ou } 1-x \text{ est inversible}$$

Notez que selon cette définition l'anneau trivial est local. Dans un anneau local, les éléments "non inversibles" (ceux pour lesquels l'hypothèse d'inversibilité implique $1=0$ dans l'anneau A) forment un idéal. Le quotient de l'anneau par cet idéal est un corps, appelé corps résiduel de l'anneau A (nous admettons l'anneau trivial comme corps).

Définition 4 *Un ensemble A muni d'une relation d'égalité est appelé* discret *lorsque l'axiome suivant est vérifié*

$$\forall x, y \in A \qquad x = y \text{ ou } \neg(x = y)$$

Commentaire 1.5 Classiquement, tous les ensembles sont discrets, car le "ou" présent dans la définition est compris de manière "abstraite". Constructivement, le "ou" présent dans la définition est compris selon la signification du langage usuel : une des deux alternatives au moins doit avoir lieu de manière certaine. Il s'agit donc d'un "ou" de nature algorithmique. Un ensemble est discret si on a un test pour l'égalité de deux éléments arbitraires de cet ensemble. Constructivement l'ensemble des nombres réels n'est pas discret (plus précisément : le supposer discret impliquerait un principe d'omniscience qui n'est pas accepté constructivement, même si on ne peut prouver qu'un tel principe est absurde).
Le corps résiduel d'un anneau local est discret si et seulement si il y a un test d'inversibilité pour les éléments de A. On dit dans ce cas que le groupe des unités $A^\times$ est une *partie détachable* de A.

[4] Bien que la preuve du lemme 1.3 soit convaincante, il peut sembler un peu choquant que le déterminant d'un endomorphisme puisse être bien défini lorsque le rang du module lui-même n'est pas bien défini. Intuitivement, cela se passe comme suit : lorsqu'on décompose le module selon ses composantes équidimensionelles, chaque composante de l'endomorphisme a clairement un déterminant, et les déterminants en chaque dimension sont mis ensemble (via les idempotents correspondant aux composantes) pour former un déterminant global.

Rappelons que deux matrices carrées $m \times m$ sont dites *semblables* lorsqu'elles représentent le même endomorphisme de A^m sur deux bases distinctes (ou non).

Nous donnons maintenant trois preuves différentes pour un lemme fondamental, que nous appelons lemme de la liberté locale.

Lemme de la liberté locale *Soit A un anneau local. Tout module projectif de type fini sur A est libre. De manière équivalente : toute matrice de projection F de type $n \times n$ est semblable à une* matrice de projection standard*, c.-à-d. de la forme :*

$$\mathrm{I}_{k,n,n} = \begin{pmatrix} \mathrm{I}_k & 0_{k,n-n} \\ 0_{n-k,k} & 0_{n-k} \end{pmatrix}$$

Première preuve *(preuve classique usuelle)* Cette preuve suppose que le corps résiduel est discret. A fortiori, on sait si l'anneau est trivial ou non. Si l'anneau est trivial, c'est clair. Si l'anneau est non trivial et si le corps résiduel est discret cela va aussi, en suivant la preuve classique usuelle. Notons $\varphi : A^n \to A^n$ la projection de matrice F. On passe au corps résiduel, la matrice F est alors la matrice de la projection sur le sous espace $\mathrm{Im}(\varphi)$ parallèlement au sous espace $\mathrm{Im}(\mathrm{Id} - \varphi)$. On considère alors un mineur résiduellement non nul d'ordre maximum k dans F, et de même un mineur résiduellement non nul d'ordre maximum $n-k$ dans $\mathrm{I}_n - F$. En mettant cote à cote les k colonnes de F et les $n-k$ colonnes de $\mathrm{I}_n - F$ correspondant à ces mineurs, on obtient une matrice Q qui est résiduellement inversible, donc inversible (car son déterminant est inversible). La matrice $G = QFQ^{-1}$ représente l'application linéaire φ sur une nouvelle base dont les k premiers vecteurs sont dans $\mathrm{Im}(\varphi)$ et les $n-k$ derniers sont dans $\mathrm{Im}(\mathrm{Id} - \varphi)$. Puisque $\varphi^2 = \varphi$ ceci implique que G est la matrice de projection standard sur le sous espace des k premiers vecteurs de base parallèlement au sous espace des $n-k$ derniers. □

Deuxième preuve *(preuve par la platitude)* Cette preuve suppose aussi que le corps résiduel est discret. C'est une preuve un peu plus "calculatoire", qui sera plus facile à utiliser dans la section 4. Nous l'avons extraite de la preuve classique qui démontre d'abord qu'un module projectif est plat, puis qu'un module plat de présentation finie sur un anneau local est libre.
Tout d'abord, nous établissons le lemme suivant :

Lemme 1.6 (Lemme de la présentation locale) *Soit A un anneau local dont le corps résiduel est discret. Une matrice G de type $q \times m$ à coefficients dans A est équivalente (sur A) à une matrice :*

$$\begin{pmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G' \end{pmatrix}$$

où G' a tous ses coefficients dans l'idéal maximal de A.
Tout module de présentation finie sur A peut être présenté par une matrice G' de ce type.

Preuve du lemme On recopie, mutatis mutandis, la preuve du lemme de la liberté. Notez que les matrices de passage P et Q se calculent explicitement à partir de G une fois qu'on a repéré un mineur d'ordre k inversible, tous les mineurs d'ordre $k+1$ étant non inversibles. □

En appliquant le lemme précédent, on obtient un entier k, des matrices P, Q, P_1, Q_1 inversibles et H résiduellement nulle, avec

$$PFQ \;=\; \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & H \end{pmatrix}, \quad QQ_1 = \mathrm{I}_n\,, \quad PP_1 = \mathrm{I}_n$$

On a

$$(PFQ)(Q_1P_1)(PFQ) = (PF^2Q) = (PFQ)$$

ce qui se réécrit, avec (Q_1P_1) décomposée en blocs :

$$\begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & H \end{pmatrix} \begin{pmatrix} B & C \\ D & E \end{pmatrix} \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & H \end{pmatrix} = \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & H \end{pmatrix}$$

c.-à-d., tous calculs faits

$$\begin{pmatrix} B & CH \\ HD & HEH \end{pmatrix} = \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & H \end{pmatrix}$$

Ainsi $B = \mathrm{I}_k$ et $HEH = H$, donc $(\mathrm{I}_{n-k} - HE)H = 0_{n-k}$. Mais HE a ses coefficeints dans l'idéal maximal, donc $\det(\mathrm{I}_{n-k} - HE) = 1 + j$ avec j dans l'idéal maximal est inversible. Donc $(\mathrm{I}_{n-k} - HE)$ est inversible, et $H = 0_{n-k}$. Ceci implique que l'image de F est un module libre de rang k puisque

$$F \;=\; P_1 \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & 0_{n-k} \end{pmatrix} Q_1$$

En fait, on a même

$$PFP^{-1} = PFP_1 = PFQQ_1P_1 = \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & 0_{n-k} \end{pmatrix} \begin{pmatrix} \mathrm{I}_k & C \\ D & E \end{pmatrix} = \begin{pmatrix} \mathrm{I}_k & C \\ 0_{n-k,k} & 0_{n-k} \end{pmatrix}$$

et donc en posant

$$R := \begin{pmatrix} \mathrm{I}_k & C \\ 0_{n-k,k} & I_{n-k} \end{pmatrix}$$

on obtient

$$R^{-1} = \begin{pmatrix} \mathrm{I}_k & -C \\ 0_{n-k,k} & I_{n-k} \end{pmatrix} \quad \text{et} \quad (RP)F(RP)^{-1} = \begin{pmatrix} \mathrm{I}_k & 0_{k,n-k} \\ 0_{n-k,k} & 0_{n-k} \end{pmatrix}$$

□

Troisième preuve *(preuve par Azuyama)* Cette preuve ne suppose pas le corps résiduel discret. Elle est la traduction matricielle de la preuve du théorème d'Azuyama III.6.2 dans [11], pour le cas qui nous occupe ici. Nous allons diagonaliser la matrice F. La preuve fonctionne avec un anneau local non nécessairement commutatif.
Appelons f_1 le vecteur colonne $f_{1..n,1}$ de la matrice F, et $e_1, \ldots, e_n$ la base canonique de A^n.
– Premier cas, $f_{1,1}$ est inversible. Alors $f_1, e_2, \ldots, e_n$ est une base de A^n. Par rapport à cette base φ a une matrice :

$$G := \begin{pmatrix} 1 & li \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

En écrivant $G^2 = G$ on obient $F_1^2 = F_1$ et $F_1 li = 0$. On a alors :

$$LGL^{-1} := \begin{pmatrix} 1 & li \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{pmatrix} \begin{pmatrix} 1 & li \\ 0_{n-1,1} & F_1 \end{pmatrix} \begin{pmatrix} 1 & -li \\ 0_{n-1,1} & \mathrm{I}_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

– Deuxième cas, $1 - f_{1,1}$ est inversible. Alors $e_1 - f_1, e_2, \ldots, e_n$ est une base de A^n. Par rapport à cette base, $\mathrm{Id}_n - \varphi$ a une matrice :

$$G := \begin{pmatrix} 1 & li \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

avec $G^2 = G$. Avec le même calcul que dans le cas précédent, $\mathrm{I}_n - F$ est donc semblable à une matrice :

$$\begin{pmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & F_1 \end{pmatrix}$$

avec $F_1^2 = F_1$, ce qui signifie que F est semblable à une matrice :

$$\begin{pmatrix} 0 & 0_{1,n-1} \\ 0_{n-1,1} & H_1 \end{pmatrix}$$

avec $H_1^2 = H_1$.
On termine la preuve par induction sur n. □

Commentaire 1.7 Du point de vue classique, tous les ensembles sont discrets, et l'hypothèse correspondante est superflue dans les deux premières preuves. Nous avons signalé les trois preuves parce que le lemme de la liberté locale est un lemme crucial dans la suite, et que les différentes preuves conduisent à différentes méthodes, plus ou moins compliquées, permettant de rendre constructifs les théorèmes que nous avons en vue.

1.3 Localisation

Nous supposons la lectrice familière du processus de localisation en une partie multiplicative S de A, ainsi qu'avec les notations A_S, M_S (pour le localisé du A-module M), et A_s, M_s lorsque S est engendré par l'élément s de A. Nous voulons cependant garder la possibilité de localiser en un monoïde (multiplicatif) pouvant contenir 0. Le résultat est alors l'anneau trivial (et le module trivial).

Des résultats essentiels sont les suivants :

Fait 1.8 *Si M est un sous module de N, on a l'identification canonique de M_S avec un sous module de N_S et de $(N/M)_S$ avec N_S/M_S.*
Si $f : M \to N$ est une application A-linéaire, $\mathrm{Im}(f_S)$ *s'identifie canoniquement à* $(\mathrm{Im}(f))_S$, $\mathrm{Ker}(f_S)$ *s'identifie canoniquement à* $(\mathrm{Ker}(f))_S$ *et* $\mathrm{Coker}(f_S)$ *s'identifie canoniquement à* $(\mathrm{Coker}(f))_S$.
Si

$$M \xrightarrow{f} N \xrightarrow{g} P$$

est une suite exacte de A-modules et $S \subset A$ un monoïde, alors

$$M_S \xrightarrow{f_S} N_S \xrightarrow{g_S} P_S$$

est une suite exacte de A_S-modules.

Fait 1.9 *Soit $f : M \to N$, $g : M \to N$ deux applications linéaires entre A-modules,* avec M de type fini. *Soit S un monoïde de A. Alors $f_S = g_S$ si et seulement si il existe $s \in S$ tel que $sf = sg$. En d'autres termes, l'application canonique* $(\mathrm{Hom}_A(M,N))_S \to \mathrm{Hom}_{A_S}(M_S, N_S)$ *est injective.*

Fait 1.10 *Soit M et N deux A-modules, S un monoïde de A et $\varphi : M_S \to N_S$ une application A_S-linéaire.* Supposons que M est de présentation finie.

Alors il existe une application A-linéaire $\phi : M \to N$ et $s \in S$ tels que

$$\forall x \in M \quad \varphi(\frac{x}{1}) = \frac{\phi(x)}{s}$$

En d'autres termes, l'application canonique $(\mathrm{Hom}_A(M,N))_S \to \mathrm{Hom}_{A_S}(M_S, N_S)$ *est bijective.*

Preuve (Cf. [12] exercice 9 p. 50 ou [7] chap. IV proposition 1.10) Supposons que M est le conoyau de l'application linéaire $g : A^m \to A^q$ avec une matrice $G = (g_{i,j})$ par rapport aux bases canoniques, alors d'après le fait 1.8 M_S est le conoyau de l'application linéaire $g_S : A_S^m \to A_S^q$ avec la matrice $G_S = (g_{i,j}/1)$ par rapport aux bases canoniques. On note $j_m : A^m \to A_S^m$, $j_q : A^q \to A_S^q$, $j_M : M \to M_S$, $j_N : N \to N_S$, $\pi : A^q \to M$, $\pi_S : A_S^q \to M_S$ les applications canoniques. Soit $\psi := \varphi \circ \pi_S$, de sorte que $\psi \circ g_S = 0$. Donc $\psi \circ g_S \circ j_m = 0 = \psi \circ j_q \circ g$. Il existe un dénominateur commun $s \in S$ pour les images par ψ des vecteurs de la base canonique, donc il existe une application linéaire $\Psi : A^q \to N$ avec $(s\psi) \circ j_q = j_N \circ \Psi$. D'où $j_N \circ \Psi \circ g = s(j_m \circ g_S \circ \psi) = 0$. D'après le fait 1.9 appliqué à $\Psi \circ g$, l'égalité $j_N \circ (\Psi \circ g) = 0$ dans N_S implique qu'il existe $s' \in S$ tel que $s'(\Psi \circ g) = 0$. Donc $s'\Psi$ se factorise sous forme $\phi \circ \pi$. On obtient alors $(ss'\varphi) \circ j_M \circ \pi = ss'(\varphi \circ \pi_S \circ j_q) = ss'\psi \circ j_q = s' j_N \circ \Psi = j_N \circ \phi \circ \pi$, et puisque π est surjective $ss'\varphi \circ j_M = j_N \circ \phi$. C.-à-d., pour tout $x \in M$ $\varphi(x/1) = \phi(x)/ss'$.

⋮
⋮
⋮
⋮
⋮
dessin
⋮
⋮
⋮
⋮

□

Un cas particulier est le suivant.

Fait 1.11 *Soit M un A-module de présentation finie, S un monoïde de A et $\varphi : M_S \to A_S$ une forme A_S-linéaire.*
Alors il existe une forme A-linéaire $\phi : M \to A$ et $s \in S$ tels que

$$\forall x \in M \quad \varphi(\frac{x}{1}) = \frac{\phi(x)}{s}$$

Fait 1.12 *Si $S \subset S'$ sont deux monoïdes de A et M un A-module on a des identifications canoniques $(A_S)_{S'} \simeq A_{S'}$ et $(M_S)_{S'} \simeq M_{S'}$.*

1.4 Système fondamental d'idempotents orthogonaux

Dans la suite nous serons amenés à considérer l'anneau localisé A_r où r est un idempotent, ainsi que le localisé M_r pour un A-module M. Il est bon de remarquer que A_r s'identifie canoniquement à l'idéal rA muni de la structure d'anneau où r est l'élément neutre de la multiplication. L'application canonique de A vers A_r identifié à rA est donnée par $x \mapsto rx$. Quant à M_r, il s'identifie naturellement à rM (avec l'application canonique $M \to rM,\ x \mapsto rx$).

Si M est image d'une application linéaire $f : A^n \to A^n$ de matrice F, le module M_r s'identifie aussi naturellement à l'image de l'application linéaire $f_r : A_r^n \to A_r^n$ ayant pour matrice la matrice rF (lorsqu'on identifie A_r avec rA). Ceci résulte du fait 1.8 modulo les identifications canoniques.

Rappelons que dans un anneau A un *système fondamental d'idempotents orthogonaux* (sfio) est une liste d'éléments de A, $(r_1, \ldots, r_n)$, qui vérifie

$$r_i r_j = 0 \ \text{ si } \ i \neq j, \quad \text{et} \quad \Sigma\, r_i = 1$$

(nous ne réclamons pas qu'ils soient tous non nuls). Ceci implique que $r_i = r_i^2$ pour chaque i.

On obtient alors :

Fait 1.13 *Si $(r_1, \ldots, r_n)$ est un sfio d'un anneau A, et si M est un A-module, on a :*

$$A \simeq A_{r_1} \times \cdots \times A_{r_n}$$
$$M = r_1 M \oplus \cdots \oplus r_n M \simeq M_{r_1} \times \cdots \times M_{r_n}$$

1.5 Le principe local-global

Un outil essentiel en algèbre classique est la localisation en (le complémentaire d') un idéal premier. Cet outil est a priori difficile à utiliser constructivement parce qu'on ne sait pas fabriquer les idéaux premiers qui interviennent dans les preuves classiques, et dont l'existence repose sur l'axiome du choix. Cependant, on peut remarquer que ces idéaux premiers sont en général utilisés à l'intérieur de preuves par l'absurde, et ceci donne une explication du fait que le recours à ces objets "idéaux" pourra être contourné et même interprété constructivement dans la section 3.

Le principe local-global abstrait en algèbre commutative est un principe informel selon lequel certaines propriétés concernant les modules sur les anneaux commutatifs sont vraies si et seulemment si elles sont vraies après localisation en n'importe quel idéal premier.

Nous étudions maintenant quelques cas élémentaires où le principe local-global s'applique.

Nous commençons à chaque fois par des versions concrètes en apparence plus faibles, mais qui s'avèreront bien utiles, au moins d'un point de vue constructif. Pour ces versions concrètes, la localisation n'est pas réclamée "en n'importe quel idéal premier" mais en un nombre fini d'éléments de A qui engendrent A en tant qu'idéal. En langage savant, dans un principe local-global concret on recouvre le spectre de l'anneau par un nombre fini d'ouverts, tandis que dans un principe local-global abstrait on voit le spectre comme l'ensemble de ses points.

Nous disons qu'un élément a de A est *non diviseur de zéro* si la suite

$$0 \longrightarrow A \xrightarrow{a.} A$$

est exacte. Autrement dit, on a :

$$\forall b \in A \quad (ba = 0 \ \Rightarrow \ b = 0)$$

C'est seulement pour l'anneau trival que 0 est non diviseur de zéro.

Principe local-global concret 1 *Supposons que $s_1, \dots s_n \in A$ avec $s_1A + \cdots + s_nA = A$, et soit $a \in A$. Alors on a les équivalences suivantes :*

Recollement concret des égalités :

$$a = 0 \ \Leftrightarrow \ \forall i \in \{1, \dots, n\} \ \ a/1 = 0 \quad \textit{dans} \quad A_{s_i}$$

Recollement concret des non diviseurs de zéro :

a est non diviseur de zéro dans A $\Leftrightarrow$ $\forall i \in \{1, \dots, n\}$ $a/1$ est non diviseur de zéro dans A_{s_i}

Recollement concret des inversibles :

$$\textit{a est inversible dans A} \ \Leftrightarrow \ \forall i \in \{1, \dots, n\} \ \ a/1 \ \ \textit{est inversible dans } A_{s_i}$$

Preuve Les conditions sont nécessaires en raison du fait 1.8. Une vérification directe est d'ailleurs immédiate.
Pour prouver que les conditions sont suffisantes, nous traitons sans perte de généralité le cas avec $n = 2$ et $s_1 = s, \ s_2 = t, \ s + t = 1$.

Supposons d'abord que $a/1 = 0$ dans A_s et dans A_t. Pour un entier $h \leq 0$ convenable on a donc $s^h a = 0 = t^h a$ dans A. Or $1 = (s+t)^{2h} = us^h + vt^h$ pour u et v convenables dans A. Donc $a = 1a = us^h a + vt^h a = u \times 0 + v \times 0 = 0$ dans A.

Supposons maintenant que $a/1$ soit non diviseur de zéro dans A_s et dans A_t. Soit $b \in A$ avec $ab = 0$ dans A donc aussi $ab/1 = 0$ dans A_s et dans A_t. On a donc $b/1 = 0$ dans A_s et dans A_t, donc aussi dans A.

Supposons enfin que $a/1$ soit inversible dans A_s et dans A_t. Soient donc $b, c \in A$ et un entier $k \geq 0$ avec $ab/s^k = 1$ dans A_s et $ac/t^k = 1$ dans A_t, i.e., pour un entier $p \geq 0$, $abs^p = s^{p+k}$ et $act^p = t^{p+k}$ dans A. Posons $h = p + k$ et comme ci-dessus déterminons u et v dans A tels que $us^h + vt^h = 1$ dans A. Alors $a \times (ubs^p + vct^p) = us^h + vt^h = 1$ dans A. □

Notation 5 On note $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de A.
Pour $\mathcal{P} \in \mathrm{Spec}(A)$ et $S = A \setminus \mathcal{P}$ on note $A_{\mathcal{P}}$ pour A_S (l'ambiguité entre les deux notations contradictoires $A_{\mathcal{P}}$ et A_S est levée en pratique par le contexte).
Si x est un élément d'un A-module M, nous notons

$$\mathrm{Ann}(x) := \{a \in A \ ; \ ax = 0\}$$

l'idéal annulateur de x.

La relation étroite qui existe entre les localisés locaux d'un anneau A et ses idéaux premiers est précisée dans le fait suivant.

Fait 1.14 *Un monoïde S d'un anneeau A est dit* saturé *lorsqu'on a l'implication*

$$\forall s, t \in A \ \ (st \in S \ \Rightarrow \ s \in S)$$

Pour qu'un monoïde multiplicatif saturé S fasse de A_S un anneau local non trivial, il faut et suffit que $S = A \setminus \mathcal{P}$ où $\mathcal{P}$ est un idéal premier.
Par ailleurs, tout homomorhisme $A \to B$ de A vers un anneau local B se factorise de manière unique par $A_{\mathcal{P}}$ où $\mathcal{P}$ est l'image réciproque de l'idéal maximal de B.

La version abstraite puissante du principe local-global concret précédent est la suivante.

Principe local-global abstrait 1 *Soit $a \in A$. Alors on a les équivalences suivantes :*
Recollement abstrait des égalités :

$$a = 0 \;\Leftrightarrow\; \forall \mathcal{P} \in \mathrm{Spec}(A)\;\; a/1 = 0 \quad \textit{dans} \quad A_{\mathcal{P}}$$

Recollement abstrait des non diviseurs de zéro :

a est non diviseur de zéro dans A $\Leftrightarrow$ $\forall \mathcal{P} \in \mathrm{Spec}(A)$ $a/1$ est non diviseur de zéro dans $A_{\mathcal{P}}$

Recollement abstrait des inversibles :

a est inversible dans A $\Leftrightarrow$ $\forall \mathcal{P} \in \mathrm{Spec}(A)$ $a/1$ est inversible dans $A_{\mathcal{P}}$

Preuve *(non constructive)* Les conditions sont nécessaires en raison du fait 1.8. Une vérification directe est d'ailleurs immédiate.
Pour les réciproques, nous supposons sans perte de généralité que l'anneau A est non trivial.
Première preuve
Supposons d'abord $a \neq 0$ dans A, soit $\mathrm{Ann}(a)$ l'idéal annulateur de a, qui est un idéal strict, soit $\mathcal{P}$ un idéal premier contenant $\mathrm{Ann}(a)$ et soit $S = A \setminus \mathcal{P}$. L'ensemble $S \cap \mathrm{Ann}(a)$ est vide, donc $a/1 \neq 0$ dans A_S.
On en déduit la deuxième réciproque comme dans le cas analogue du principe local-global concret 1.
Supposons enfin a non inversible dans A. Soit $\mathcal{P}$ un idéal premier contenant aA et soit $S = A \setminus \mathcal{P}$. Alors $a/1$ est non inversible dans A_S.
Deuxième preuve (pour les cas $a = 0$ et a inversible)
Pour chaque idéal premier $\mathcal{P}$ on peut trouver $s \notin \mathcal{P}$ tel que $a/1$ est nul (resp. inversible) dans A_s. Les ouverts correspondants $U_s = \{\mathcal{P} \in \mathrm{Spec}(A);\; s \notin \mathcal{P}\}$ recouvrent $\mathrm{Spec}(A)$, donc les s correspondants engendrent A comme idéal, donc un nombre fini d'entre eux, $s_1, \ldots, s_m$ engendrent A comme idéal. On peut donc faire appel au principe local-global concret correspondant. □

Commentaire 1.15 La deuxième preuve montre bien le lien entre le principe local-global abstrait et le principe local-global concret. Cependant, il ne semble pas qu'elle puisse jamais être rendue constructive. La première preuve n'est pas non plus "en général" constructive, mais il existe des cas où elle l'est. Il suffit pour cela que les conditions suivantes soient vérifiées :
Dans le cas du recollement des égalités
— l'anneau A est discret
— pour tout $a \neq 0$ dans A on sait construire un idéal premier $\mathcal{P}$ de A contenant $\mathrm{Ann}(a)$.
Dans le cas du recollement des inversibles
— l'ensemble des $a \in A$ inversibles est une partie détachable de A.
— pour tout $a \in A$ non inversible, on sait construire un idéal premier $\mathcal{P}$ de A contenant aA.
C'est par exemple le cas lorsque A est une algèbre de présentation finie sur $\mathbb{Z}$ ou sur un corps "pleinement factoriel" (voir [11]).

En pratique, on peut comprendre le principe local-global abstrait 1 sous la forme intuitive suivante : pour démontrer un théorème d'algèbre commutative dont la signification est qu'un certain élément d'un anneau commutatif A est nul, non diviseur de zéro, ou inversible, il suffit de traiter le cas où l'anneau est local. C'est un principe du même genre que le principe de Lefschetz : pour démontrer un théorème d'algèbre commutative dont la signification est qu'une certaine identité algébrique a lieu, il suffit de traiter le cas où l'anneau est le corps des complexes (ou n'importe quel sous anneau qui nous arrange, d'ailleurs).

Un résultat local-global concret, qui donne la moitié la plus facile du théorème 1, est le suivant.

Principe local-global concret 2 (recollement concret de modules de type fini, de présentation finie ou projectifs de type fini) *Supposons que $s_1, \dots s_n \in A$ avec $s_1A + \cdots + s_nA = A$, et soit M un A-module. Alors on a les équivalences suivantes :*
• *M est de type fini si et seulement si chacun des M_{s_i} est un A_{s_i}-module de type fini.*
• *M est de présentation finie si et seulement si chacun des M_{s_i} est un A_{s_i}-module de présentation finie.*
• *M est projectif de type fini si et seulement si chacun des M_{s_i} est un A_{s_i}-module projectif de type fini.*

Preuve Les conditions sont clairement nécessaires. Pour prouver qu'elles sont suffisantes, nous traitons sans perte de généralité le cas avec $n = 2$ et $s_1 = s,\ s_2 = t,\ s + t = 1$.

Tout d'abord supposons que M_s est un A_s-module de type fini et M_t est un A_t-module de type fini. Montrons que M est de type fini. Soit $g_1, \dots, g_q$ des éléments de M qui engendrent M_s et M_t. Soit $x \in M$ arbitraire. On a pour un certain exposant m et certains éléments $a_1, \dots, a_q$ de A :

$$s^m x = a_1 g_1 + \cdots + a_q g_q \quad \text{dans} \quad M_s$$

donc pour un certain exposant p :

$$s^{m+p} x = s^p a_1 g_1 + \cdots + s^p a_q g_q \quad \text{dans} \quad M$$

On écrit une égalité du même style avec t, et on les combine selon la procédure $us^h + vt^h = 1$ comme dans les preuves précécentes.

Supposons maintenant que M_s est un A_s-module de présentation finie et M_t est un A_t-module de présentation finie. Montrons que M est de de présentation finie.
Soit $g_1, \dots, g_q$ un système générateur de M.
Soit $(a_{i,1}, \dots, a_{i,q}) \in A_s^q$ des relations entre les $g_i/1 \in M_s$ (i.e., $\Sigma_j\ a_{i,j} g_j = 0$ dans M_s) pour $i = 1, \dots, k_1$, qui engendrent le A_s-module (contenu dans A_s^q) des relations entre les $g_j/1$. On peut supposer sans perte de généralité que chaque $a_{i,j}$ est en fait un élément $a'_{i,j}/1$ avec $a'_{i,j} \in A$. Il existe alors un exposant n convenable tel que les vecteurs $s^n(a'_{i,1}, \dots, a'_{i,q}) = (a''_{i,1}, \dots, a''_{i,q}) \in A^q$ soient des A-relations entre les $g_j \in M$.
Considérons de la même manière un système générateur de relations $(b_{i,1}, \dots, b_{i,q}) \in A_t^q$ (où $i = 1, \dots, k_2$) entre les $g_i/1 \in M_t$, avec $b_{i,j} = b'_{i,j}/1$ où $a'_{i,j} \in A$, puis $t^m(b'_{i,1}, \dots, b'_{i,q}) = (b''_{i,1}, \dots, b''_{i,q}) \in A^q$ qui sont des A-relations entre les $g_j \in M$.
Montrons que les deux systèmes de relations ainsi construits entre les g_j engendrent toutes les relations. Soit en effet une relation arbitraire $(c_1, \dots, c_q)$ entre les g_j. Considérons là comme une relation entre les $g_j/1 \in M_s$ et écrivons là en conséquence comme combinaison A_s-linéaire des vecteurs $(a''_{i,1}, \dots, a''_{i,q}) \in A_s^q$. Après multiplication par une puissance convenable s^h de s on obtient une égalité dans A^q :

$$s^h(c_1, \dots, c_q) = e_1(a''_{1,1}, \dots, a''_{1,q}) + \cdots + e_q(a''_{k_1,1}, \dots, a''_{k_1,q})$$

On fait de même avec t et il reste à combiner les deux résultats selon la procédure $us^h + vt^h = 1$ comme dans les preuves précécentes.

Supposons enfin que M_s est un A_s-module projectif de type fini et M_t est un A_t-module projectif de type fini. Montrons que M est projectif de type fini. Puisque M_s est projectif de type fini, il existe des formes A_s-linéaires $\alpha_1, \dots, \alpha_q$ sur M_s telles que

$$\forall x \in M_s \quad x = \alpha_1(x) g_1 + \cdots + \alpha_q(x) g_q \quad \text{dans} \quad M_s$$

D'après le fait 1.11, puisque M est de présentation finie, il existe un exposant m et des formes A-linéaires $\alpha'_1, \ldots, \alpha'_q$ sur M telles que

$$\forall x \in M \quad s^m \alpha_1(x) = \alpha'_1(x), \ldots, s^m \alpha_q(x) = \alpha'_q(x) \quad \text{dans} \quad M_s$$

et donc

$$\forall x \in M \quad s^m x = \alpha'_1(x) g_1 + \cdots + \alpha'_q(x) g_q \quad \text{dans} \quad M_s$$

donc, comme M est de type fini (voir le fait 1.9) il existe un exposant p tel que

$$\forall x \in M \quad s^{m+p} x = s^p \alpha'_1(x) g_1 + \cdots + s^p \alpha'_q(x) g_q$$

On écrit une égalité du même style avec t, et on les combine selon la procédure $us^h + vt^h = 1$ comme dans les preuves précécentes. □

Remarque 1.16 Les preuves sont toujours "les mêmes". Il existe un traitement un peu plus abstrait, s'appuyant sur la notion de module fidèlement plat qui permet de voir pourquoi. Voir par exemple [6] proposition 2.3.5 et lemme 3.2.3. L'exposé dans [6] du principe de recollement concret des modules projectifs de type fini manque de peu une preuve entièrement constructive. Dans [7] ce principe est l'objet de la règle 1.14 du chapitre IV, mais là aussi la preuve n'est pas constructive.

La principe local-global concret 2 de recollement des modules projectifs admet la version abstraite suivante. Nous n'utiliserons pas ce résultat.

Principe local-global abstrait 2 (recollement abstrait de modules projectifs) *Soit M un A-module. Supposons que M soit de présentation finie ou que M soit de type fini et A intègre, alors M est projectif de type fini si et seulement si les localisés $M_{\mathcal{P}}$, pour tous les $\mathcal{P} \in \mathrm{Spec}(A)$ sont libres.*

Preuve (cf. [12] chap. 2, théorème 14 p.43 et exercice 10 p.51, [6] théorème 3.3.7).
Nous donnons une preuve pour le cas d'un module de présentation finie, distincte de celles citées ci-dessus. Cette preuve fonctionne comme la deuxième preuve du principe local-global abstrait 1.
Il faut montrer que la condition est suffisante. Dire qu'une matrice G présente un module libre de rang k revient à dire qu'on peut passer de G à une matrice nulle de type $k \times 1$ par une suite finie de transformations élémentaires décrites à la section 1.1.
Soit maintenant $\mathcal{P}$ un idéal premier. Si ce que nous venons d'expliquer fonctionne pour le $A_{\mathcal{P}}$-module $M_{\mathcal{P}}$ et un certain entier k, cela fonctionne aussi pour le A_s-module M_s pour un $s \in A \setminus \mathcal{P}$ convenable, ceci en vertu du nombre fini d'égalités dans $A_{\mathcal{P}}$ mises en jeu lors de ces transformations élémentaires.
Il reste à recouvrir $\mathrm{Spec}(A)$ par un nombre fini d'ouverts U_{s_i} et à faire appel au principe local-global concret de recollement des modules projectifs de type fini. □

Les deux principes qui suivent (concret et abstrait) ne seront pas utilisés dans la suite de l'article. Les preuves sont analogues à celles des principes 1. Le principe concret peut par exemple être trouvé dans le livre de Knight [6].

Principe local-global concret 3 (recollement concret des suites exactes)
Supposons que $s_1, \dots s_n \in A$ *avec* $s_1A + \cdots + s_nA = A$, *et soit* $f : M \to N$ *et* $g : N \to P$ *des applications A-linéaires entre A-modules. Alors la suite*

$$M \xrightarrow{f} N \xrightarrow{g} P$$

est exacte si et seulement si les suites

$$M_{s_i} \xrightarrow{f_{s_i}} N_{s_i} \xrightarrow{g_{s_i}} P_{s_i}$$

sont exactes pour $i \in \{1, \dots, n\}$.

Principe local-global abstrait 3 (recollement abstrait des suites exactes)
Soit $f : M \to N$ *et* $g : N \to P$ *des applications A-linéaires entre A-modules. Alors la suite*

$$M \xrightarrow{f} N \xrightarrow{g} P$$

est exacte si et seulement si les suites

$$M_{\mathcal{P}} \xrightarrow{f_{\mathcal{P}}} N_{\mathcal{P}} \xrightarrow{g_{\mathcal{P}}} P_{\mathcal{P}}$$

sont exactes pour tous les $\mathcal{P} \in \mathrm{Spec}(A)$.

2 Matrices de projection

2.1 Cas d'un anneau local

Proposition 2.1 (cas d'un anneau local) *Soit A un anneau local,* $F \in \mathrm{Mat}_n(A)$ *avec* $F^2 = F$ *et M le module projectif de type fini image de F dans* A^n. *Il existe un entier k* $(0 \leq k \leq n)$ *tel que* $\det(\mathrm{I}_n + XF) = (1 + X)^k$. *En outre tous les mineurs d'ordre* $k + 1$ *de F sont nuls.*

Preuve Il s'agit d'une conséquence immédiate du lemme de la liberté locale : toute matrice de projection sur un anneau local est semblable à une matrice de projection standard $\mathrm{I}_{k,n,n}$. L'entier k est uniquement déterminé si l'anneau est non trivial. □

Notez que la preuve précédente est entièrement constructive lorsqu'elle est basée sur la troisième preuve du lemme de la liberté locale. Les deux autres preuves réclameraient que l'anneau local ait un corps résiduel discret.

2.2 Cas général

Théorème 3 (matrices de projection : idempotents et localisations libres) *Soit A un anneau,* $F \in \mathrm{Mat}_n(A)$ *avec* $F^2 = F$ *et M le module projectif de type fini image de F dans* A^n. *Posons* $\mathrm{R}_F(1 + X) := \det(\mathrm{I}_n + XF)$, $\mathrm{R}_F(X) =: r_0 + r_1X + \cdots + r_nX^n$. *Alors le système* $(r_0, r_1, \dots, r_n)$ *est un système fondamental d'idempotents orthogonaux.*
En outre, les mineurs d'ordre $(k + 1)$ *de la matrice* r_kF *sont tous nuls. Et si s est un mineur diagonal d'ordre k de* r_kF, *alors le module* M_s *est libre de rang k sur l'anneau* A_s.

Remarque 2.2 On notera que la dernière affirmation du théorème reste vraie si $s = 0$ en raison de la convention 2. De même, avec cette convention la proposition 2.1 reste vraie dans le cas d'un anneau trivial si on ne demande pas l'unicité de k.

Remarque 2.3 La définition des r_i attachés à la matrice F peut être relue comme suit en utilisant le polynome caractéristique sous sa forme usuelle :

$$\det(X\mathrm{I}_n - F) =: r_0X^n + r_1X^{n-1}(X-1) + \cdots + r_iX^{n-i}(X-1)^i + \cdots + r_n(X-1)^n$$

(les $X^{n-i}(X-1)^i$ forment une base du module des polynomes de degré $\leq n$, triangulaire par rapport à la base usuelle)

Preuve du théorème : On a trivialement $\mathrm{R}_F(1) = 1$, i.e. $\Sigma_i r_i = 1$. On utilise le principe local-global abstrait de recollement des égalités pour montrer que $r_ir_j = 0$ pour $i \neq j$. En effet cette égalité est vraie dans le cas des anneaux locaux d'après la proposition 2.1 puisque tous les r_i sont égaux à 0, sauf un égal à 1.
La même astuce fonctionne pour démontrer que les mineurs d'ordre $k+1$ de r_kF sont nuls. Soit en effet t un mineur d'ordre $k+1$ de F, on doit montrer que $tr_k = 0$ dans A. Si A est local, ou bien $r_k = 0$ (si le rang est $h \neq k$), ou bien $r_k = 1$ et $t = 0$ (si le rang est k). Voyons enfin la dernière affirmation. Nous notons F_s la matrice F vue dans A_s. Il est clair que le mineur diagonal s est inversible dans A_s et on vient de voir que tous les mineurs d'ordre $k+1$ de $r_kF \simeq F_{r_k}$ sont nuls, donc a fortiori tous les mineurs d'ordre $k+1$ de F_s sont nuls. On peut donc appliquer le lemme de la liberté (page 6) et déduire que le A_s-module M_s image de la matrice F_s est libre. □

Théorème 4 (forme explicite des théorèmes 1 et 2)
Sous les mêmes hypothèses et avec les mêmes notations qu'au théorème 3, pour chaque $k = 0, \ldots, n$, la matrice r_kF, vue comme matrice à coefficients dans A_{r_k} (identifié à r_kA) a pour image un module projectif de rang k sur l'anneau A_{r_k} (ceci prouve le théorème 2).
Si les $t_{k,i}$ sont les mineurs diagonaux d'ordre k de F, et si on pose $s_{k,i} = r_kt_{k,i}$, la somme (pour k fixé) des $s_{k,i}$ est égale à r_k, et chaque module $M_{s_{k,i}}$ est libre de rang k. Donc la famille de tous les $s_{k,i}$ a pour somme 1 et convient pour le théorème 1. En particulier, pour tout module projectif de type fini à n générateurs, 2^n éléments s_i suffisent pour le théorème 1.

Preuve : Conséquence immédiate du théorème 3. □

Commentaire 2.4 Le théorème précédent donne une version complètement explicite des théorèmes 1 et 2. Nous sommes ici dans une situation typique que se proposait de "résoudre" le programme de Hilbert. Un énoncé explicite concret a été démontré par des méthodes abstraites a priori peu fiables. Nous donnons dans la suite deux moyens de récupérer une preuve entièrement fiable de l'énoncé concret. L'argument parfois cité que tout théorème d'arihmétique prouvé dans ZFC peut également être prouvé sans recours à l'axiome du choix offre au moins trois inconvénients. Le premier (mineur) est qu'une analyse assez poussée doit être menée pour se convaincre qu'un théorème comme le théorème 2 a, en fait, la signification d'un théorème d'arithmétique. Le deuxième (nettement plus sérieux) est que le recours à l'axiome du choix n'est pas le seul ingrédient non constructif dans la preuve qui a été fournie. Le troisième (redoutable) est que rien ne garantit que ZFC soit une théorie cohérente.

Un autre corollaire du théorème 3 est le suivant :

Théorème 5 (polynome caractéristique des matrices de projection de rang constant)
Soit $F \in \mathrm{Mat}_n(A)$ avec $F^2 = F$ et M le module projectif de type fini image de F dans A^n. Alors le module M est de rang k si et seulement si le polynome caractéristique de F est égal à $(X-1)^kX^{n-k}$. Dans ce cas tous les mineurs d'ordre $k+1$ de F sont nuls.

Preuve : La condition est clairement suffisante. Montrons qu'elle est nécessaire. Nous supposons donc que le polynome caractéristique de F est égal, à des nilpotents près, au polynome $(X-1)^k X^{n-k}$. En appliquant le théorème 2, cela implique que pour $h \neq k$ l'idempotent r_h est nilpotent, donc nul. En ce qui concerne les mineurs d'ordre $k+1$ de F, on peut alors appliquer le théorème 3. □

Commentaire 2.5 Notez que dans la mesure où le théorème peut être prouvé constructivement, ceci nous donne une version constructivement satisfaisante de la proposition 1.2 (on ne considère pas le (a), et dans les autres conditions équivalentes, on peut évacuer les nilpotents). Nous verrons encore un peu mieux à la section 3.4.

Un dernier corollaire immédiat dans le même style est le suivant. (cf. théorème 2 dans [1] chap. II §5).

Théorème 6 (caractérisation locale des modules projectifs de rang constant)
Un A-module M engendré par n éléments est projectif de rang constant k si et seulement si il existe un entier $m \leq \binom{n}{k}$ et des éléments $s_1, \ldots, s_m$ de A tels que, d'une part $s_1A + \cdots + s_mA = A$, et d'autre part les modules M_{s_i} soient libres de rang k.

Nous terminons cette section par une proposition facile.

Proposition 2.6 (quand le localisé en un élément de A est de rang constant)
Soit F une matrice de projection ayant pour image un module M, et $r_0, \ldots, r_n$ le sfio défini au théorème 3.
Soit s un élément de A. Pour que le localisé M_s soit projectif de rang h il faut et suffit que $r_h/1 = 1$ dans A_s, c.-à-d. que $r_h s^m = s^m$ dans A pour un certain exposant m. Si s est un idempotent, cela signifie que r_h divise s.
Enfin si $s_0, \ldots, s_n$ est un sfio tel que chaque M_{s_h} soit de rang h, alors $r_h = s_h$ pour $h = 0, \ldots, n$.

2.3 Cas générique

Qu'est-ce que nous appelons le cas générique, concernant un module projectif à n générateurs ? On considère l'anneau $A = \mathbf{B}_n = \mathbb{Z}[(f_{i,j})_{1\leq i,j\leq n}]/\mathcal{J}_n$, où $\mathcal{J}_n$ est l'idéal défini par les n^2 relations obtenues en écrivant $F^2 = F$. Dans cet anneau $\mathbf{B}_n$, nous avons la matrice $F = (f_{i,j})$ dont l'image dans $\mathbf{B}_n^n$ est ce qui mérite d'être appelé *le module projectif générique à n générateurs*.

Reprenons les notations du théorème 3 dans ce cas particulier. Dire que $r_h r_k = 0$ dans $\mathbf{B}_n$ (pour $0 \leq h \neq k \leq n$) signifie que, dans $\mathbb{Z}[\mathbf{f}] = \mathbb{Z}[(f_{i,j})_{1\leq i,j\leq n}]$

$$r_h(\mathbf{f}) r_k(\mathbf{f}) \in \mathcal{J}_n \qquad (*)$$

Cela implique une identité algébrique qui permet d'exprimer cette appartenance. Cette identité algébrique est naturellement valable dans tous les anneaux commutatifs. Il est donc clair que si l'appartenance $(*)$ est vérifiée dans le cas générique, elle implique $r_h r_k = 0$ pour n'importe quelle matrice de projection pour n'importe quel anneau commutatif.

La même chose vaut pour les égalités $r_h s = 0$ lorsque s est un mineur d'ordre $h+1$.

En résumé : si le théorème 3 est vérifié dans le cas générique, il est vérifié dans tous les cas.

Le seul ingrédient non constructif dans la preuve du théorème 3 était l'appel au principe local-global abstrait 1. Dans le commentaire après ce théorème, nous avons indiqué que le

théorème admettait une preuve constructive pour certains anneaux, en particulier pour les anneaux $\mathbb{Z}[x_1,\ldots,x_n]/\mathcal{I}$ lorsque $\mathcal{I}$ est donné comme un idéal de type fini.

Ainsi la preuve classique est constructive dans le cas générique modulo un gros travail sur les idéaux des anneaux $\mathbb{Z}[x_1,\ldots,x_n]$. Donc les théorèmes 1, 2, 3, 4, 5 et 6 sont constructivement prouvés.

Dans la section suivante, nous expliquons comment il est possible de suivre de beaucoup plus près la preuve classique. Autrement dit encore, l'appartenance $(*)$ peut être construite sans appel à la (belle) théorie constructive de la noetherianité et des décompositions primaires pour l'anneau $\mathbb{Z}[x_1,\ldots,x_n]$.

3 Le contenu constructif du principe local-global

Notre but ici est donc de faire une relecture constructive de la preuve du théorème 3 dans le cas général (et non plus le cas générique) "sans autres ingrédients algorithmiques que ceux contenus dans la preuve classique". Cette affirmation quelque peu brutale ne doit pas être prise comme une boutade ni comme une provocation. Nous prétendons réellement débusquer un contenu algorithmique précis dans les *preuves* qui utilisent le principe local-global abstrait 1, même quand les idéaux premiers ne peuvent absolument pas être explicités en tant que tels.

3.1 L'idée générale

Soit A un anneau commutatif et a un élément de A qui est le résultat d'un certain calcul fait sous certaines hypothèses. Le principe local-global abstrait le plus élémentaire nous dit que a est nul dans A si et seulement si $a/1$ est nul dans tous les $A_{\mathcal{P}}$ (pour $\mathcal{P}\in \mathrm{Spec}(A)$).

Supposons que nous ayions une preuve que $a/1$ est nul dans tous les $A_{\mathcal{P}}$. Comme toute preuve, elle est de nature finie. En particulier, l'*axiome des anneaux locaux*

$$\forall s,t\in A \qquad (\ s+t=1\ \Rightarrow\ s\ \text{ ou }\ t\ \text{ est inversible})$$

n'est utilisé qu'un nombre fini de fois dans la preuve (cela est en relation étroite avec le théorème qui affirme que $\mathrm{Spec}(A)$ est quasicompact).

Au bout du compte la preuve aura produit des éléments $s_1,\ldots,s_m$ de A qui vérifient $s_1A+\cdots+s_mA=A$ et pour lesquels $a/1$ est nul dans chaque A_{s_i}.

A condition d'être capable de suivre la preuve de façon suffisamment précise, on pourra donc conclure que $a=0$ dans A en utilisant cette fois-ci le principe local-global *concret* 1.

A vrai dire, cette idée générale semble si simple et si naturelle qu'il est étonnant qu'elle n'ait pas encore été exploitée systématiquement. En fait, lorsqu'on essaie de mener ce travail en détail, on voit apparaître un obstacle, c'est que la plupart des preuves usuelles, même très simples, sont néanmoins un peu trop compliquées pour pouvoir être traitées directement selon l'idée générale précédente. Par exemple, la preuve classique usuelle du lemme de la liberté locale utilise de manière cruciale le fait que le corps résiduel est discret (cf. la première preuve page 9), ce qui est un cas particulier d'usage du tiers exclu en logique classique.

Il s'avère cependant que l'usage du tiers exclu n'est pas un obstacle bien grave : l'usage de la logique classique est inoffensif lorsqu'il s'agit de prouver des faits suffisamment concrets ! (cf. [2] théorème 1.1).

3.2 Structures algébriques dynamiques

Pour mettre en oeuvre notre idée générale, nous aurons besoin de la notion de *structure algébrique dynamique* (cf. [8] et [2]).

L'idée qui gouverne la définition d'une structure algébrique dynamique est la suivante : il s'agit d'une structure algébrique incomplètement spécifiée, dans laquelle on calcule selon des règles de nature algébrique simple, celles qui définissent axiomatiquement une structure algébrique ordinaire. Le fait que la structure est incomplètement spécifiée introduit une arborescence dans les calculs.

Par exemple si on dit : voici un corps engendré par 2 éléments a et b qui vérifient $a^2+b^2+1 = 0$, les calculs qui s'ensuivent peuvent faire apparaître dans les différentes branches n'importe quelle situation correspondant à cette "présentation". Dans un premier embranchement a sera nul et dans un autre, a sera inversible, puisque tout élément dans un corps est nul ou inversible. D'autres embranchements peuvent apparaître si à un moment donné du calcul, on se pose par exemple la question de savoir si 5 est nul ou inversible.

Autre exemple, qui nous concerne directement ici. Si on dit : voici un anneau A complètement spécifié en tant qu'anneau, mais appliquons lui les règles de calcul valables dans les anneaux locaux, les calculs vont faire apparaitre des embranchements chaque fois qu'on a besoin d'utiliser l'axiome des anneaux locaux. On est alors en train de calculer ce qui se passe dans les différents localisés $A_{\mathcal{P}}$ de A. Différents cas peuvent se produire : ils sont pris en compte dans les différentes branches du calcul. Si la preuve aboutit, un nombre fini de feuilles seulement apparaitront dans l'arbre du calcul. Cela veut dire qu'on n'a pas eu besoin de construire vraiment des localisés $A_{\mathcal{P}}$, mais seulement des localisés A_s (qui en général ne sont pas des anneaux locaux). En langage savant : on a recouvert le spectre de A par un nombre fini d'ouverts $U_s = \{\mathcal{P} \in \mathrm{Spec}(A);\ s \notin \mathcal{P}\}$. La différence entre le point de vue classique et le point de vue constructif est alors seulement que le mathématicien classique "admet" que les idéaux $\mathcal{P}$ existent en vertu (d'une version faible) de l'axiome du choix, tandis que la mathématicienne constructive (qui ne croit qu'à ce qu'elle voit) veut bien "faire comme si" ils existaient, puisque la seule chose importante dans ce spectre, ce ne sont pas ses points, mais ses recouvrements ouverts finis.

Tout ceci semble avoir quelque rapport avec les tableaux sémantiques en logique. Des rapports étroits existent également avec la théorie des topos cohérents (cf. [2]) et avec la théorie des esquisses (cf. [4] et [5]). Notre première inspiration a été fournie par l'évaluation dynamique de la cloture algébrique d'un corps "à la D5" (cf. [3]) qui réalisait le fait remarquable suivant : *calculer de manière sûre dans la cloture algébrique d'un corps arbitraire alors même que cette cloture algébrique ne peut pas être construite (pour un corps général).*

3.3 Anneau versus anneau local (dynamiques)

La structure d'anneau (commutatif) est la structure algébrique usuelle d'anneau commutatif, basée sur $(1, 0, +, -, \times)$. Nous considérons une structure d'anneau comme une structure "où on calcule" et pour laquelle on utilise le seul prédicat "$x = 0$" à l'exclusion de tous autres prédicats plus compliqués. L'égalité $t = t'$ est elle-même considérée simplement comme une autre écriture pour $t - t' = 0$.

Se donner une *présentation d'anneau*, c'est donner un ensemble G de "générateurs" et un ensemble $R_{=0}$ de "relations" qui sont toutes de la forme $t = 0$ avec t un élément de $\mathbb{Z}[G]$. Dans la suite pour simplifier, nous considérons $R_{=0}$ simplement comme une partie de $\mathbb{Z}[G]$.

La plupart des axiomes d'anneau commutatifs sont absorbés par les calculs dans $\mathbb{Z}[G]$ et il nous reste alors les axiomes suivants, qui sont les règles que nous pourrons appliquer dans nos calculs.

$$\begin{array}{rll} & \vdash\ 0=0 & A(1)\\ (x=0,\ y=0) & \vdash\ x+y=0 & A(2)\\ x=0 & \vdash\ xy=0 & A(3)\end{array}$$

Le but est de calculer, pour la présentation $(G; R_{=0})$, tous les termes $t \in \mathbb{Z}[G]$ pour lesquels $t = 0$ peut être prouvé. Ce type de calcul ne comporte aucun embranchement, ce qui fait que nous sommes dans un cadre "non dynamique", même si on peut penser la structure comme une structure dynamique. En fait, la différence, lorsqu'on pense la structure comme dynamique, c'est qu'on ne prouve que des égalités $t = 0$, et rien d'autre. On ne peut pas prouver, par exemple $1 \neq 0$, parce que le prédicat $x \neq 0$ n'a pas été introduit, et on n'a pas dit selon quelles règles on le manipulerait.

Un anneau dynamique n'est rien d'autre qu'une présentation $(G; R_{=0})$ (où $R_{=0}$) est une partie de $\mathbb{Z}[G]$) à partir de laquelle on fait les calculs conformément aux 3 axiomes $A(1, 2, 3)$ des anneaux. Du point de vue des égalités $t = 0$, il n'y a aucune différence avec la structure d'anneau usuelle (non dynamique), comme le dit la proposition triviale suivante.

Proposition 3.1 *Soit $(G; R_{=0})$ un anneau dynamique, et $t \in \mathbb{Z}[G]$. Alors $t = 0$ est prouvable si et seulement si t est dans l'idéal $\mathcal{I}_{=0}$ de $\mathbb{Z}[G]$ engendré par $R_{=0}$.*

Le fait que, lorsque la présentation est finie, il existe une méthode algorithmique pour tester la prouvabilité des faits n'a rien d'évident.

Cependant, en l'absence de toute théorie constructive des bases de Gröbner, ou bien encore dans le cas d'une présentation non finie, la tâche de déterminer les faits prouvables peut être grandement facilitée par l'usage d'un analogue du principe local-global abstrait, que nous pouvons formuler constructivement dans le cadre des structures dynamiques.

Tout d'abord nous devons introduire la notion d'anneau local dynamique. Un *anneau local dynamique* est simplement un anneau dynamique où on a le droit d'appliquer une nouvelle règle de calcul, donnée par l'axiome des anneaux locaux :

$$(x+y=1)\ \vdash\ (\exists u\ ux=1)\ \vee\ (\exists v\ vy=1) \qquad AL$$

Comment cet axiome doit-il être appliqué ? Chaque fois qu'on a prouvé, dans une branche du calcul, une égalité $t+t' = 1$, on a la possibilité d'ouvrir deux sous branches, dans la première un nouveau paramètre u est introduit (i.e. un paramètre qui ne figure ni dans G ni parmi les paramètres précédemment introduits dans la branche) ainsi qu'une nouvelle relation $ut = 1$, dans la seconde branche on introduit un nouveau paramètre v et la nouvelle relation $vt' = 1$. Si P est l'ensemble des paramètres introduits au dessus d'un certain point de notre calcul arborescent, les termes qui peuvent être considérés à cet endroit sont les éléments de $\mathbb{Z}[G \cup P]$.

Un tel calcul arborescent, arrêté au bout d'un temps fini, s'appelle une *évaluation dynamique* de l'anneau local (dynamique) $(G; R_{=0})$. A chaque feuille du calcul ont été prouvées des égalités $t = 0$ avec $t \in \mathbb{Z}[G \cup P]$.

Quand un fait $t = 0$, avec $t \in \mathbb{Z}[G]$, est-il déclaré prouvé pour un anneau local dynamique ? C'est *lorsqu'il est prouvé à toutes les feuilles d'une évaluation dynamique de l'anneau local.*

Le principe local-global abstrait admet maintenant une *interprétation* constructive : c'est l'objet de la proposition (facile mais non triviale) suivante.

Principe local-global dynamique 1 (recollement dynamique des égalités, première version)
Pour prouver un fait $t = 0$ dans un anneau, vous pouvez aussi bien faire comme si l'anneau était local.
De manière plus formelle : Soit $(G; R_{=0})$ un anneau dynamique, et $t \in \mathbb{Z}[G]$. Si le fait $t = 0$ est prouvé dans l'anneau local dynamique $(G; R_{=0})$ alors il est également prouvable dans l'anneau dynamique $(G; R_{=0})$: ajouter l'axiome des anneaux locaux ne permet pas de prouver plus de faits.
Ou si l'on préfère : l'évaluation dynamique d'un anneau comme anneau local dynamique est une procédure légitime pour prouver les faits $t = 0$.

Remarque 3.2 L'énoncé précédent doit être compris de manière constructive : nous vous donnons une procédure uniforme qui transforme toute preuve dynamique d'un fait $t = 0$ dans un anneau local dynamique de présentation $(G; R_{=0})$ en une preuve dynamique du même fait $t = 0$ dans l'anneau dynamique ayant la même présentation $(G; R_{=0})$.

Preuve Il suffit de montrer que l'utilisation une fois de l'axiome des anneaux locaux ne permet pas de prouver de nouveaux faits.

Soit $\mathcal{I}_{=0}$ l'idéal de $\mathbb{Z}[G]$ engendré par $R_{=0}$ et $s, t, p \in \mathbb{Z}[G]$. Supposons que $s + t - 1 \in \mathcal{I}_{=0}$. Supposons également sans perte de généralité que s et t ne sont pas nuls dans $\mathbb{Z}[G]$. Appliquons l'axiome des anneaux locaux avec $s + t = 1$, et supposons qu'ensuite, nous sachions prouver $p = 0$ dans chacune des deux branches créées.

Dans la première branche on a introduit le paramètre u avec la relation $us - 1 = 0$, donc si on prouve $p = 0$ c'est qu'on a une égalité dans $\mathbb{Z}[G][u]$:

$$p = i_0(u) + (us - 1)r_0(u)$$

avec $i_0 = i_{0,0} + i_{0,1}u + \cdots + i_{0,n}u^n \in \mathcal{I}_{=0}[u]$ et $r_0(u) \in \mathbb{Z}[G][u]$. Nous utilisons le symbole $=$ pour désigner une égalité dans $\mathbb{Z}[G]$, c.-à-d. une identité algébrique, en vue de distinguer cette égalité du prédicat $= 0$ dans la structure algébrique dynamique. En mutlipliant par s^n et en réduisant dans $i_0(u)$ les $u^k s^k$ modulo $us - 1$, on obtient une nouvelle égalité :

$$s^n p = i_1 + (us - 1)r_1(u)$$

avec $i_1 \in \mathcal{I}_{=0}$ et $r_1(u) \in \mathbb{Z}[G][u]$. Mais comme la variable u ne figure que dans le dernier terme, on a $r_1 = 0$, et donc

$$s^n p = i_1 \qquad (1)$$

(ceci est couramment appelé le *truc de Rabinovitch*).

De la même manière, dans la seconde branche, on obtient une égalité

$$t^m p = i_2 \qquad (2)$$

avec $i_2 \in \mathcal{I}_{=0}$.

Il reste à recoller ces deux égalités selon la procédure qui a été constamment utilisée dans les preuves "local-global concrètes". Précisément, on considère l'égalité $s + t = 1 + i_3$ dans $\mathbb{Z}[G]$ avec $i_3 \in \mathcal{I}_{=0}$. Cela donne, en élevant à la puissance $m + n$,

$$as^n + bt^m = 1 + i_4 \qquad (3)$$

dans $\mathbb{Z}[G]$ avec $i_4 \in \mathcal{I}_{=0}$. En combinant (1), (2) et (3) on obtient $p \in \mathcal{I}_{=0}$. □

3.4 Relectures constructives d'énoncés et de preuves

Muni de cette interprétation constructive du principe local-global abstrait 1, pouvons-nous maintenant directement traiter la preuve du théorème 3 ?

Une inspection détaillée de cette preuve nous montre que ce que nous avons à faire se résume en deux grandes étapes :
— fournir une preuve du lemme de la liberté locale (page 9) sous forme d'une preuve par évaluation dynamique ; la troisième preuve que nous avons indiquée, la preuve par Azuyama, est justement de ce type.
— dans la preuve du théorème 3 utiliser le principe local-global dynamique 1 en lieu et place du principe local-global abstrait 1.

Ainsi nous avons gagné notre pari : nous obtenons une preuve entièrement constructive du théorème 3, et par exemple, dans le cas générique, cette preuve construit les identités algébriques recherchées. En outre cette preuve est une traduction "mot à mot" de la preuve classique. Nous avons seulement à remplacer le recollement abstrait des égalités par le recollement dynamique des égalités. Notez aussi que, du point de vue classique, ces deux théorèmes de recollement sont équivalents.

Nous traiterons la question : "comment faire avec une preuve moins élémentaire (que celle par Azuyama) du lemme de la liberté locale ?" dans la section 4.

Signalons aussi le fait remarquable suivant (qui court-circuite notre constructivisation de la preuve classique) :
la réalisation dynamique de la preuve du lemme de la liberté locale dans la théorie des anneaux locaux fournit, pour un module projectif de type fini M sur un anneau arbitraire (lorsqu'il est évalué dynamiquement comme un anneau local), la construction d'un nombre fini d'éléments s_i qui engendrent A comme idéal et tels que les M_{s_i} sont libres.

En effet, cette preuve dynamique fournit un arbre aux feuilles duquel "M est libre (après avoir rendu inversibles suffisamment d'éléments de A)" et dont chaque embranchement est obtenu en rendant inversible un des deux éléments s, t pour lesquels on a prouvé $s+t=1$. Une inspection détaillée de la preuve par Azumaya nous montre d'ailleurs que l'arbre d'évaluation dynamique a exactement 2^n feuilles lorsque la matrice de projection F est de type $n\times n$. On peut donc se poser la question de savoir si la borne 2^n, obtenue par deux voies assez différentes, est la borne la plus naturelle[5] (bien que peut-être pas optimale) pour l'explicitation du théorème 1.

Ce n'est pas seulement le principe local-global abstrait 1 qui admet une interprétation constructive.

Chaque fois qu'on a un théorème local-global d'algèbre commutative, c.-à-d. un énoncé du genre "telle propriété est vraie pour l'anneau A et le A-module M si et seulement si elle est vraie en tous les localisés $A_{\mathcal{P}}$ et $M_{\mathcal{P}}$", on lui donnera alors l'interprétation constructive suivante "telle propriété est vraie pour l'anneau A et le A-module M si et seulement si elle est vraie lorsqu'on se place dans un cadre dynamique et qu'on rajoute les axiomes des anneaux locaux".

Dire qu'une propriété est vraie dans un cadre dynamique signifie qu'on peut construire une évaluation dynamique de la situation telle qu'à chaque feuille de l'arbre la propriété soit démontrée vraie.

[5] Il est difficile de qualifier cette question de mathématique, à cause du mot "naturel" qui, ici, semble résister à tout interprétation en termes de foncteurs. Mais parfois les questions "non mathématiques" sont importantes en mathématiques.

Du point de vue classique, les deux théorèmes (le théorème classique et son interprétation dynamique et constructive) sont en général équivalents (cela dépend cependant de la propriété en cause). Du point de vue constructif, seul le deuxième énoncé fait sens. L'important, mais c'est là une thèse qui reste à vérifier en pratique, c'est que la preuve classique de l'énoncé classique se réécrit "automatiquement" comme preuve constructive de l'énoncé dynamique.

Nous donnons deux exemples de tels énoncés.

Concernant les modules projectifs de type fini, on a le théorème dynamique suivant qui est la version dynamique et constructive du principe local-global abstrait de recollement des modules projectifs.

Théorème 7 *Soit M un A-module de présentation finie. Les propriétés suivantes sont équivalentes :*

- *Le module M est projectif de type fini.*
- *Lorsqu'on évalue dynamiquement A comme anneau local, le module M est projectif de type fini.*
- *Lorsqu'on évalue dynamiquement A comme anneau local, le module M est libre.*

Concernant les modules projectifs de rang constant, on a le théorème dynamique suivant, qui constitue notre version constructive la plus élaborée de la proposition 1.2.

Théorème 8 *Soit M un A-module de présentation finie et k un entier naturel. Les propriétés suivantes sont équivalentes :*

- *Le module M est projectif de type fini et lorsqu'on évalue dynamiquement A comme corps, l'espace vectoriel M est de dimension k.*
- *Lorsqu'on évalue dynamiquement A comme anneau local, le module M est libre de rang k.*
- *Le module M est projectif de type fini et si F est une matrice de projection $n\times n$ ayant pour image un module isomorphe à M, le polynome caractéristique de F est égal à $X^{n-k}(X-1)^k$, à des nilpotents près.*
- *Le module M est projectif de type fini et si F est une matrice de projection $n\times n$ ayant pour image un module isomorphe à M, le polynome caractéristique de F est égal à $X^{n-k}(X-1)^k$ et tous les mineurs d'ordre $k+1$ de F sont nuls.*

4 Compléments sur l'interprétation constructive du principe local-global

Nous reprenons dans cette section la question de la relecture constructive de la preuve du théorème 3. Comme nous l'avons déjà signalé, une inspection détaillée de cette preuve nous montre que ce que nous avons à faire se résume en deux grandes étapes :
— fournir une preuve du lemme de la liberté locale sous forme d'une preuve par évaluation dynamique.
— dans la preuve du théorème 3 utiliser le principe local-global dynamique 1 en lieu et place du principe local-global abstrait 1.

La troisième preuve du lemme de la liberté locale remplit la première condition. Cependant, si on considère la première ou la deuxième preuve du lemme de la liberté locale, on constate qu'elle n'est pas directement une preuve par évaluation dynamique dans la théorie des anneaux

locaux (telle que nous l'avons définie à la section 3.3). Il s'agit néanmoins dans les deux cas d'une preuve *élémentaire*, i.e. qui peut être développée en tant que preuve formelle à l'intérieur de la théorie du premier ordre des anneaux locaux.

Le théorème 1.1 de [2], qui est un théorème de logique (une variante du *théorème d'élimination des coupures*), nous permet de transformer toute preuve d'un fait $t = 0$ dans la théorie formelle du premier ordre des anneaux locaux en une preuve par simple évaluation dynamique. Ainsi, nous avons mis à jour un contenu algorithmique caché pour la preuve classique abstraite que nous avons donnée du théorème 3, même si nous prenons la première ou la deuxième preuve du lemme de la liberté locale (qui ne sont pas entièrement constructives).

Pour ne pas faire appel à ce théorème de logique, nous donnons dans la section 4.1, le moyen de récupérer directement la preuve lemme de la liberté locale comme preuve par évaluation dynamique lorsque nous utilisons la deuxième preuve. Pour cela il nous faut introduire en tant que tels les prédicats d'inversibilité et de non inversibilité qui figurent explicitement dans les deux premières preuves du lemme de la liberté locale.

4.1 Anneau avec idéal et préinversibles : définition des structures

Notre premier travail consiste ici à décrire un anneau muni d'un monoïde et d'un idéal, comme première approche d'un anneau local avec ses inversibles et son idéal maximal.

La structure d'anneau (commutatif) avec idéal et préinversibles est la structure d'anneau commutatif, basée sur $(1, 0, +, -, \times)$, où on rajoute deux prédicats : $\mathrm{Unit}(x)$ pour dire "x est préinversible" (i.e. x est inversible modulo l'idéal), et $\mathrm{Rnul}(x)$ pour dire "x est dans l'idéal (c.-à-d. résiduellement nul)". Nous avons déjà les trois axiomes $A(1)$, $A(2)$, $A(3)$ et nous rajoutons le système d'axiomes suivant.

$$
\begin{array}{rcll}
x = 0 & \vdash & \mathrm{Rnul}(x) & AI(1)\\
(\mathrm{Rnul}(x),\ \mathrm{Rnul}(y)) & \vdash & \mathrm{Rnul}(x+y) & AI(2)\\
\mathrm{Rnul}(x) & \vdash & \mathrm{Rnul}(xy) & AI(3)\\
\mathrm{Rnul}(x^2) & \vdash & \mathrm{Rnul}(x) & AI(4)\\
 & \vdash & \mathrm{Unit}(1) & AU(1)\\
(\mathrm{Unit}(x),\ \mathrm{Rnul}(y)) & \vdash & \mathrm{Unit}(x+y) & AU(2)\\
(\mathrm{Unit}(x),\ \mathrm{Unit}(y)) & \vdash & \mathrm{Unit}(xy) & AU(3)\\
\mathrm{Unit}(xy) & \vdash & \mathrm{Unit}(x) & AU(4)\\
(\mathrm{Unit}(x),\ xy = 0) & \vdash & y = 0 & AU(5)\\
(\mathrm{Unit}(x),\ \mathrm{Rnul}(xy) & \vdash & \mathrm{Rnul}(y) & AU(6)
\end{array}
$$

Nous considérons une structure d'anneau avec idéal et préinversibles comme une structure dynamique, une structure "où on calcule" et pour laquelle on n'utilise que les trois prédicats "$x = 0$", $\mathrm{Rnul}(x)$ et $\mathrm{Unit}(x)$ *à l'exclusion de tous autres prédicats plus compliqués*. Rappelons que l'égalité $t = t'$ est elle-même considérée simplement comme une autre écriture pour $t-t' = 0$.

Se donner une *présentation d'anneau avec idéal et préinversibles*, c'est donner un ensemble G de "générateurs" et un ensemble R de "relations" qui sont toutes de la forme $t = 0$ ou de la forme $\mathrm{Unit}(t)$ ou de la forme $\mathrm{Rnul}(t)$ avec t un élément de $\mathbb{Z}[G]$. Le but du calcul est de construire des termes t' tels que $t' = 0$ ou tels que $\mathrm{Rnul}(t')$ ou tels que $\mathrm{Unit}(t')$. Pour simplifier, nous considèrerons que la présentation est donnée par G et par trois parties de $\mathbb{Z}[G]$, $R_{=0}$, R_{Unit} et R_{Rnul}, qui correspondent aux trois types de relations données dans la présentation.

Notez que les trois faits suivants sont équivalents : $1 = 0$, $\mathrm{Rnul}(1)$ et $\mathrm{Unit}(0)$. Dans ce cas, pour tout terme t les faits $t = 0$, $\mathrm{Unit}(t)$ et $\mathrm{Rnul}(t)$ sont prouvables.

Récapitluons : nous définissons la structure d'*anneau avec idéal et préinversibles*, comme une structure basée sur $(1, 0, +, -, \times, \mathrm{Rnul}, \mathrm{Unit})$, et soumise aux axiomes $A(1), \ldots, A(3)$, $AI(1), \ldots, AI(4)$, $AU(1), \ldots, AU(6)$. Un anneau dynamique avec idéal et préinversibles est donné par une présentation $(G; R_{=0}, R_{\mathrm{Rnul}}, R_{\mathrm{Unit}})$ où $R_{=0}$, R_{Rnul} et R_{Unit} sont trois parties de $\mathbb{Z}[G]$.

Le lecteur pourra protester et dire que nous n'avons pas mis exactement les axiomes correspondant à la structure. Nous demandons en effet que l'idéal soit radical, et par ailleurs nous ne donnons aucun axiome pour garantir que les préinversibles peuvent être inversés modulo l'idéal. Disons que ce n'était pas là notre but. Nous décrivons en fait une bonne structure intermédiaire pour arriver à la structure d'anneau local avec son idéal maximal et ses inversibles.

En fait notre structure "pauvre" est intéressante parce qu'elle contient suffisamment d'axiomes sans toutefois comporter aucun axiome avec $\exists$ ni aucun axiome avec $\vee$. Cela permet de démontrer facilement quels sont les faits prouvables pour une structure dynamique donnée.

Nous introduisons maintenant la structure dynamique d'*anneau local avec idéal maximal et inversibles*. C'est la structure d'anneau avec idéal et préinversibles qu'on évalue dynamiquement en considérant les trois axiomes supplémentaires suivants :

$$\begin{array}{rcll} \mathrm{Unit}(x) & \vdash & \exists u\ ux = 1 & ALMI(1) \\ & \vdash & (\mathrm{Unit}(x) \vee \mathrm{Rnul}(x)) & ALMI(2) \\ x + y = 1 & \vdash & (\mathrm{Unit}(x) \vee \mathrm{Unit}(y)) & ALMI(3) \end{array}$$

Remarque 4.1 En fait le dernier axiome résulte facilement des précédents : si on a $\mathrm{Rnul}(x)$, puisque on a $\mathrm{Unit}(1)$ on en déduit $\mathrm{Unit}(1 - x)$.

La lectrice n'aura pas de mal à se convaincre que les axiomes de la structure d'anneau local avec idéal maximal et inversibles sont exactement ceux qui caractérisent les anneaux locaux à corps résiduel discret avec des prédicats spécifiant les éléments de l'idéal maximal et les inversibles.

En fait, on aurait pu, de manière plus naturelle, introduire la structure d'anneau local avec idéal maximal et inversibles en donnant seulement cinq axiomes qui traduisent la définition des éléments inversibles, des éléments non inversibles et l'axiome des anneaux locaux. Sans introduire les axiomes AI ni les axiomes AU on aurait simplement pris les trois axiomes $ALMI$ ci-dessus et les deux suivants :

$$\begin{array}{rcll} xy = 1 & \vdash & \mathrm{Unit}(x) & ALMI(1bis) \\ (\mathrm{Unit}(x), \mathrm{Rnul}(x)) & \vdash & 1 = 0 & ALMI(2bis) \end{array}$$

4.2 Faits prouvables et interprétation du principe local-global abstrait

Proposition 4.2 *Soit $(G; R_{=0}, R_{\mathrm{Rnul}}, R_{\mathrm{Unit}})$ un anneau avec idéal et préinversibles, dynamique, et $t \in \mathbb{Z}[G]$. Soit $\mathcal{I}_{=0}$ l'idéal de $\mathbb{Z}[G]$ engendré par $R_{=0}$, $\mathcal{I}_{\mathrm{Rnul}}$ l'idéal de $\mathbb{Z}[G]$ engendré par R_{Rnul} et $\mathcal{M}_{\mathrm{Unit}}$ le monoïde multiplicatif de $\mathbb{Z}[G]$ engendré par R_{Unit}.*
Alors :

– *$t = 0$ est prouvable si et seulement si on a dans $\mathbb{Z}[G]$ une égalité du type*

$$(u + j)t + i = 0$$

avec $u \in \mathcal{M}_{\mathrm{Unit}}$, $j \in \mathcal{I}_{\mathrm{Rnul}}$, et $i \in \mathcal{I}_{=0}$.

– Rnul(t) *est prouvable si et seulement si on a dans* $\mathbb{Z}[G]$ *une égalité du type*

$$ut^n + j + i = 0$$

avec $n \in \mathbb{N}$, $u \in \mathcal{M}_{\text{Unit}}$, $j \in \mathcal{I}_{\text{Rnul}}$ *et* $i \in \mathcal{I}_{=0}$.

– Unit(t) *est prouvable si et seulement si on a dans* $\mathbb{Z}[G]$ *une égalité du type*

$$u + j + at + i = 0$$

avec $u \in \mathcal{M}_{\text{Unit}}$, $j \in \mathcal{I}_{\text{Rnul}}$, $a \in \mathbb{Z}[G]$ *et* $i \in \mathcal{I}_{=0}$.

Un corollaire immédiat est le suivant (dans la lignée du théorème 1.1 de [2] : on peut toujours rajouter des nouveaux prédicats à condition de les soumettre à des axiomes "logiques" raisonnables).

Corollaire 4.3 *Si un anneau dynamique* $(G; R_{=0})$ *est vu comme un anneau avec idéal et préinversibles dynamique* $(G; R_{=0}, \emptyset, \emptyset)$, *les faits prouvables* $t = 0$ *sont les mêmes pour les deux structures dynamiques.*

Un autre corollaire remarquable et immédiat est le suivant.

Corollaire 4.4 *Dans un anneau dynamique avec idéal et préinversibles :*
a) un fait Unit(t) *est prouvable si et seulement si la relation* Rnul(t) *(rajoutée dans la présentation) rend prouvable* $1 = 0$,
b) un fait Rnul(t) *est prouvable si et seulement si la relation* Unit(t) *(rajoutée dans la présentation) rend prouvable* $1 = 0$.

Preuve de la proposition On voit facilement que les conditions sont suffisantes.
Pour voir qu'elles sont nécessaires, il suffit de vérifier que les éléments de $R_{=0}$, R_{Rnul} et R_{Unit} sont "conformes" et que chaque axiome produit des éléments "conformes" à partir d'éléments "conformes". La plupart des calculs ne présentent aucune difficulté. Nous traitons les cas des axiomes $AI(2)$, $AU(2)$, $AU(6)$.
Cas de l'axiome $AI(2)$. On suppose que l'on a deux faits prouvables "conformes" Rnul(t_1) et Rnul(t_2), c.-à-d. qu'on a deux égalités dans $\mathbb{Z}[G]$

$$\begin{aligned} u_1 t_1^m + j_1 + i_1 &= 0 \\ u_2 t_2^n + j_2 + i_2 &= 0 \end{aligned}$$

(avec les mêmes conventions que dans l'énoncé pour u, j et i), on en déduit

$$\begin{aligned} u_1 u_2 (t_1 + t_2)^{m+n} \;=\; u_1 u_2 (a t_1^m + b t_2^n) \;=\; (u_2 a)(u_1 t_1^m) + (u_1 b)(u_2 t_2^n) \;= \\ u_2 a(-j_1 - i_1) + u_1 b(-j_2 - i_2) \;=\; -j_3 - i_3 \end{aligned}$$

Et le fait prouvable Rnul($t_1 + t_2$) est donc bien "conforme".
Cas de l'axiome $AU(2)$. On suppose qu'on a deux faits prouvables "conformes" Rnul(t_1) et Unit(t_2), c.-à-d. deux égalités dans $\mathbb{Z}[G]$

$$\begin{aligned} u_1 t_1^m + j_1 + i_1 &= 0 \\ u_2 + j_2 + a_2 t_2 + i_2 &= 0 \end{aligned}$$

d'où

$$u_1u_2 + a_2u_1(t_1 + t_2) + j_3 + i_3 \;=\; a_2u_1t_1$$

on élève à la puissance m, dans chaque membre on regroupe judicieusement les termes, on obtient

$$u_4 + a_4(t_1 + t_2) + j_4 + i_4 \;=\; a_5u_1t_1^m \;=\; -\,a_5(j_1 + i_1);\; =\; j_5 + i_5$$

Et le fait prouvable $\mathrm{Unit}(t_1 + t_2)$ est donc bien "conforme".

Cas de l'axiome $AU(6)$. On suppose qu'on a deux faits prouvables "conformes" $\mathrm{Unit}(t_1)$ et $\mathrm{Rnul}(t_1t_2)$, c.-à-d. deux égalités dans $\mathbb{Z}[G]$

$$\begin{aligned} u_1 + j_1 + a_1t_1 + i_1 &= 0 \\ u_2(t_1t_2)^m + j_2 + i_2 &= 0 \end{aligned}$$

Dans la première égalité, on fait passer a_1t_1 dans le second membre, on élève à la puissance m et on regroupe judiceusement les termes, on obtient

$$u_3 + j_3 + i_3 \;=\; a_3t_1^m$$

puis on multiplie par $u_2t_2^m$, cela donne

$$u_4t_2^m + j_4 + i_4 \;=\; a_3u_2(t_1t_2)^m \;=\; j_5 + i_5$$

Et le fait prouvable $\mathrm{Rnul}(t_2)$ est donc bien "conforme".

□

Proposition 4.5 *Soit* $A = (G; R_{=0}, R_{\mathrm{Rnul}}, R_{\mathrm{Unit}})$ *un anneau avec idéal et préinversibles dynamique et* $t \in \mathbb{Z}[G]$.
Si on l'évalue dynamiquement comme anneau local avec idéal maximal et inversibles, tout fait prouvé (du type $t = 0$ *ou* $\mathrm{Rnul}(t)$ *ou* $\mathrm{Unit}(t)$*) peut également être prouvé sans recours aux trois axiomes supplémentaires* $ALMI(1, 2, 3)$.

Preuve Vues[6] la remarque 4.1 et le corollaire 4.4, il suffit de montrer que l'utilisation une fois de l'axiome $ALMI(1)$ ou de l'axiome $ALMI(2)$ ne change pas les faitrs prouvés de la forme $p = 0$. Pour $ALMI(1)$ c'est l'usuel truc de Rabinovitch.
Voyons $ALMI(2)$. On considère un terme t et on ouvre deux branches, l'une avec $\mathrm{Unit}(t)$ et l'autre avec $\mathrm{Rnul}(t)$. On part de deux égalités dans $\mathbb{Z}[G]$ qui correspondent à la prouvabilité de $p = 0$ respectivement dans chacune des deux branches :

$$\begin{aligned} (u_1t^m + j_1)p + i_1 \;&=\; 0 \qquad (1) \\ (u_2 + j_2 - ta_2)p + i_2 \;&=\; 0 \qquad (2) \end{aligned}$$

avec $u_h \in \mathcal{M}_{\mathrm{Unit}}$, $j_h \in \mathcal{I}_{\mathrm{Rnul}}$, $a_h \in \mathbb{Z}[G]$ et $i_h \in \mathcal{I}_{=0}$.
On se base sur l'identité $(u - s)\times$(quelque chose) $=$ $(u^m - s^m)$ avec $u := u_2 + j_2$ et $s := ta_2$. En multipliant (2) par "quelque chose", on obtient

$$(u_3 + j_3 - t^ma_3)p + i_3 \;=\; 0 \qquad (3)$$

On multiplie (1) par a_3, on obtient :

$$(a_3u_1t^m + j_4)p + i_4 \;=\; 0 \qquad (4)$$

[6] Accord de genre avec le plus proche cité.

On multiplie (3) par u_1, on obtient :

$$(u_5 + j_5 - a_3u_1t^m)p + i_5 \;=\; 0 \qquad (5)$$

Enfin on additionne (4) et (5), on obtient :

$$(u_5 + j_6)p + i_6 \;=\; 0$$

ce qui est l'égalité cherchée. □

Nous voici en état de prouver constructivement une nouvelle forme concrète, un peu plus sophistiquée que le principe local-global dynamique 1, du principe local-global abstrait 1. Cette fois-ci, les inversibles sont pris en compte.

Principe local-global dynamique 2 *Soit $A = (G; R_{=0}, \emptyset, \emptyset)$ un anneau avec idéal et préinversibles dynamique (avec R_{Rnul} et R_{Unit} vides) et $t \in \mathbb{Z}[G]$. Alors on a :*

— (recollement dynamique des égalités, deuxième version)
Pour prouver un fait $t = 0$ dans un anneau, vous pouvez aussi bien faire comme si l'anneau était local, en utilisant les prédicats d'inversibilité et non inversibilité.
De manière plus formelle : un fait du type $t = 0$ est prouvable dans la structure d'anneau local dynamique avec idéal maximal et inversibles si et seulement si il est prouvable dans A comme anneau dynamique.

— (recollement dynamique des inversibles) *Un fait du type* Unit(t) *est prouvable dans la structure d'anneau local dynamique avec idéal maximal et inversibles si et seulement si t est inversible dans A comme anneau dynamique, i.e., s'il existe un $u \in \mathbb{Z}[G]$ avec $tu = 1$ prouvable.*
De manière moins formelle : Pour prouver un fait "t est inversible" dans un anneau, vous pouvez aussi bien faire comme si l'anneau était local, en utilisant les prédicats d'inversibilité et non inversibilité.

— (une caractérisation dynamique des nilpotents)
Un fait du type Rnul(t) *est prouvable dans la structure d'anneau local dynamique avec idéal maximal et inversibles si et seulement si t est nilpotent dans A comme anneau dynamique, i.e., s'il existe un entier naturel m avec $t^m = 0$ prouvable.*

Preuve Cela résulte de la proposition 4.5 et de la caractérisation donnée dans la proposition 4.2. □

Remarque 4.6 Comme conséquence du recollement dynamique des égalités dans le théorème précédent, si $(G; R_{=0})$ est un anneau local dynamique, tout fait prouvé en le considérant comme un anneau local avec idéal maximal et inversibles peut être prouvé dans la structure d'anneau local (on peut toujours rajouter des nouveaux prédicats à condition de les soumettre à des axiomes "logiques" raisonnables).

4.3 Récapitulons

On récapitule sur la relecture constructive dynamique de la preuve du théorème 3. Un aspect un peu déroutant est que, une fois qu'on dispose des prédicats d'inversibilité et non inversibilité pour un anneau local, c.-à-d. en fait des prédicats d'égalité à zéro et de non égalité à zéro dans le corps résiduel, la théorie de la dimension des espaces vectoriels sur les corps, vue comme théorie

du rang des matrices, et nécessaire pour la *première preuve* du lemme de la liberté locale[7], n'est pas si simple à formuler et à prouver dynamiquement sans recours aux prédicats de dépendance linéaire et d'indépendance linéaire. Il nous faut introduire des disjonctions de conjonctions : un mineur d'ordre k non nul et tous les mineurs d'ordre $k+1$ nuls... Cela demande donc un travail qui est faisable, mais qu'on ne prendra pas la peine de faire ici.
Par contre, toujours pour le lemme de la liberté locale, la *deuxième preuve* que nous avons donnée se lit très aisément comme une preuve par évaluation dynamique pour la structure anneau local avec inversibles et idéal maximal. Ceci, joint à la preuve du principe local-global dynamique 2 fournit une preuve constructive du théorème 3, et par exemple construit les identités algébriques recherchées dans le cas générique.

Références

[1] Bourbaki. *Algèbre Commutative.* Hermann, 1961. 4, 20

[2] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze* preprint 1996. 21, 22, 27, 29

[3] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields* Proceedings Eurocal'85. Lecture Notes in Computer Science 204, p. 289-290 (1985). (Springer) 22

[4] Duval D., Reynaud J.-C. *Sketches and Computation (Part I) Basic Definitions and Static Evaluation.* Mathematical Structures in Computer Science 4 (1994) 185–238. 22

[5] Duval D., Reynaud J.-C. *Sketches and Computation (Part II) Dynamic Evaluation and Applications.* Mathematical Structures in Computer Science 4 (1994) 239–271. 22

[6] Knight J. *Commutative Algebra.* London Mathematical Society LNS n°5. Cambridge University Press, 1971. 4, 17

[7] Kunz E. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, 1991. 4, 12, 17

[8] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier* 1994, à paraitre dans le Journal of Pure and Applied Logic, special issue on Logic Colloquium'94. 22

[9] Lombardi H.. *Interprétation constructive de principes local-globals abstraits en algèbre commutative.* en préparation. 4

[10] Lombardi H., Quitte C.. *Théorie constructive élémentaire des modules projectifs de type fini.* en préparation. 4

[11] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, 1988. 4, 10, 15

[12] Northcott D. *Finite free resolutions.* Cambridge tracts in mathematics n°71. Cambridge University Press, 1976. 4, 12, 17

[7] Nous pensons par exemple à la partie soulignée de la phrase suivante : On considère alors un mineur résiduellement non nul d'ordre maximum k dans F, et de même un mineur résiduellement non nul d'ordre maximum $n-k$ dans $\mathrm{I}_n - F$.