THÉORIE DES NOMBRES
BESANÇON

Années 1994/95-1995/96

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

H. LOMBARDI

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 1997

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 homorphisme

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

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 économisera 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 : $\forall x \in M \quad x = \Sigma\, \alpha_i(x) g_i$.
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 : $\forall x \in M \quad x = \Sigma\, \beta_i(x) h_i$.
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) $\Rightarrow$ (c) : considérer les applications canoniques $M \to M \oplus N$ et $M \oplus N \to M$.

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

(b) $\Rightarrow$ (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.

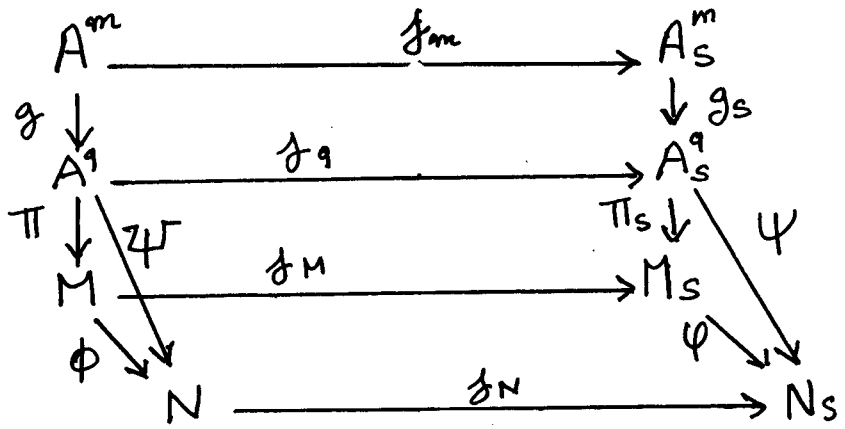
Fait 1.9 *Soit $f : M \to N$, $g : M \to N$ deux applications linéaires entre A-modules,* avec M de type fini. *Soit S un monoïde de A. Alors $f_S = g_S$ si et seulement si il existe $s \in S$ tel que $sf = sg$. En d'autres termes, l'application canonique $(\mathrm{Hom}_A(M,N))_S \to \mathrm{Hom}_{A_S}(M_S, N_S)$ 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 $x \in M$ $\varphi(x/1) = \phi(x)/ss'$.



□

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 $s_1, \ldots s_n \in A$ avec $s_1 A + \cdots + s_n A = A$, et soit $a \in A$. Alors on a les équivalences suivantes :*

Recollement concret des égalités :

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

Recollement concret des non diviseurs de zéro :
a est non diviseur de zéro dans A $\Leftrightarrow \forall i \in \{1,\ldots,n\}$ *a/1 est non diviseur de zéro dans* A_{s_i}

Recollement concret des inversibles :

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

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 :

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

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.