M1 2023-2024: Modules sur un anneau commutatif

David Harari

Table des matières

1. Généralités

La notion de module est la généralisation naturelle de celle d'espace vectoriel. Elle est absolument fondamentale, par exemple en géométrie algébrique et en théorie des nombres. Dans toute la suite, A désigne un anneau commutatif, que l'on sera parfois amené à supposer *non nul*.

1.1. Premières notions

Définition 1.1 Un *A-module* $(M, +, .)$ est un ensemble équipé d'une loi interne $+$ et d'une loi externe $A \times M \to M$, $(\alpha, m) \mapsto \alpha.m$ (qu'on abrégera le plus souvent en αm) vérifiant :

— $(M, +)$ est un groupe abélien.

— On a en plus les quatre propriétés suivantes :

1. $\alpha(m + m') = \alpha m + \alpha m'$
2. $(\alpha + \beta)m = \alpha m + \beta m$
3. $(\alpha\beta)m = \alpha(\beta m)$
4. $1.m = m$

pour tous $\alpha, \beta \in A$ et tous $m, m' \in M$.

Remarque 1.2 Comme A est supposé commutatif, il n'y a pas lieu de distinguer entre modules à gauche et à droite (pour A non commutatif, le troisième axiome serait différent pour un module à droite).

Définition 1.3 Soit M un A-module. Un *sous-module* N de M est un sous-groupe de $(M, +)$ qui est en plus stable pour la multiplication externe par tout élément de A.

Autrement dit une partie N de M est un sous-module si et seulement s'il contient 0, et si pour tous x, y de N et tout α de A on a : $x + y \in N$ et $\alpha x \in N$.

Exemple 1.4 a) A est un A-module, l'opération externe étant la multiplication dans A.

b) Tout groupe abélien M peut être considéré comme un $\mathbf{Z}$-module pour la loi externe : $\alpha.m = \alpha m$.

c) Soient $n > 0$ et M un groupe abélien *de n-torsion*, c'est-à-dire tel que $nx = 0$ pour tout x de M. Alors M est un $\mathbf{Z}/n\mathbf{Z}$-module pour la loi $\bar{\alpha}.x = \alpha x$, où $\alpha \in \mathbf{Z}$ a pour classe $\bar{\alpha}$ dans $\mathbf{Z}/n\mathbf{Z}$.

d) Soit I une partie de A. Alors I est un sous A-module de A si et seulement si c'est un idéal de A.

e) Soit $(M_i)_{i \in I}$ une famille (finie ou non) de A-modules. Alors l'ensemble produit $\prod_{i \in I} M_i$ est un A-module pour les lois évidentes ; on l'appelle le *A-module produit* des M_i.

f) Soit S une partie d'un A-module M. Alors le *sous-module engendré* par S est l'ensemble des combinaisons linéaires $\sum_{s \in S} \alpha_s s$, où $(\alpha_s)_{s \in S}$ est une famille presque nulle d'éléments de A. C'est le plus petit sous-module de M qui contient S. Cette notion est surtout utile quand S est fini.

Définition 1.5 Un *homomorphisme* (ou morphisme) de A-modules est une application $f : M \to M'$ entre deux A-modules qui vérifie : $f(x+y) = f(x)+f(y)$ et $f(\alpha.x) = \alpha.f(x)$ pour tous x, y de M et tout α de A. On note $\ker f := f^{-1}(\{0\})$ le *noyau* de f et $\operatorname{Im} f := f(M)$ son image. Ce sont des sous-modules de M, M' respectivement.

Au lieu de morphisme de A-modules, on dit parfois application A-linéaire. On a bien sûr les notions d'isomorphisme et d'automorphisme de A-modules.

On a aussi le théorème de factorisation habituel (preuve immédiate) :

Proposition 1.6 *Soient M un A-module et N un sous-module de M. Alors le groupe quotient M/N, équipé de la loi externe $\alpha.\bar{m} = \overline{\alpha.m}$ est un A-module, appelé module quotient de M par N. Si $f : M \to M'$ est un morphisme de A-modules, il existe un unique morphisme $\tilde{f} : M/\ker f \to M'$ tel que $f = \tilde{f} \circ \pi$, où $\pi : M \to M/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injective d'image* $\operatorname{Im} f$.

Remarque 1.7 Si $f : M \to M'$ est un morphisme de A-modules et N est un sous-module de M inclus dans $\ker f$, alors f se factorise encore par un morphisme $M/N \to M'$ d'image $\operatorname{Im} f$ (on perd par contre l'injectivité qui est valable quand $N = \ker f$).

La définition suivante est analogue à celle qu'on a dans les espaces vectoriels :

Définition 1.8
- Soit $(M_i)_{i\in I}$ une famille de A-modules. La *somme directe* ("externe") des M_i est le sous module $\bigoplus_{i\in I} M_i$ du produit $\prod_{i\in I} M_i$ constitué des familles $(m_i)_{i\in I}$ presque nulles. Si I est fini, la somme directe coïncide avec le produit direct. Notons que chaque M_i se plonge dans $\bigoplus_{i\in I} M_i$ en envoyant m_i sur l'élement dont toutes les composantes sont nulles sauf celle en i qui vaut m_i. Du coup, on peut écrire tout élément de $\bigoplus_{i\in I} M_i$ de façon unique sous la forme $\sum_{I\in I} m_i$ avec $m_i \in M_i$ et la famille des m_i presque nulle.
- Soit $(M_i)_{i\in I}$ une famille de sous-modules du A-module M. Alors le sous-module *somme* $\sum_{i\in I} M_i$ est le module engendré par la réunion des M_i. Plus explicitement, c'est l'ensemble des sommes $\sum_{i\in I} m_i$, où $(m_i)_{i\in I}$ est une famille presque nulle avec $m_i \in M_i$ pour chaque $i \in I$. Si de plus la condition $\sum_{i\in I} m_i = 0$ implique $m_i = 0$ pour tout i, on dit que la somme des M_i est *directe*; dans ce cas $\sum_{i\in I} M_i$ est isomorphe à la somme directe externe $\bigoplus_{i\in I} M_i$, et on notera $\bigoplus_{i\in I} M_i$ pour $\sum_{i\in I} M_i$ ("somme directe interne").

On notera que deux sous-modules M_1, M_2 d'un A-module M sont en somme directe si et seulement si $M_1 \cap M_2 = \{0\}$, mais ceci ne se généralise pas à plus de deux sous-modules. D'autre part si $M = M_1 \oplus M_2$, alors M/M_1 est isomorphe à M_2 (via la projection sur M_2) mais contrairement au cas des espaces vectoriels, il n'y a pas de réciproque[1] (par exemple $\mathbf{Z}$ n'est pas isomorphe à la somme directe externe de $n\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z}$ puisque $\mathbf{Z}$ n'a pas d'élément non nul annulé par n).

Proposition 1.9 ("Propriété universelle de la somme directe") *Soit $f_i : M_i \to N$ une famille de morphismes de A-modules. Alors, il existe un unique morphisme f de $\bigoplus_{i\in I} M_i$ dans N qui induit le morphisme f_i sur chaque M_i (identifié à un sous-module de $\bigoplus_{i\in I} M_i$).*

Démonstration : De façon évidente, le morphisme $f := \bigoplus_{i\in I} f_i$ défini par $f(\sum_i m_i) = \sum_i f_i(m_i)$ est la seule solution.

□

Remarque 1.10 Le produit direct $\prod_i M_i$ vérifie quant à lui une propriété universelle "dans l'autre sens" : pour toute famille de morphismes $g_i : N \to M_i$, il existe un unique morphisme $N \to \prod_i M_i$ qui induit g_i en composant avec la projection sur M_i.

1.2. Intermède : déterminant d'une matrice à valeurs dans un anneau commutatif

On va avoir besoin d'étendre aux anneaux commutatifs quelconques les résultats classiques sur le déterminant des matrices à coefficient dans un corps. On commence par généraliser aux modules la notion de forme n-linéaire :

Définition 1.11 Soit A un anneau commutatif. Une *application n-linéaire* (bilnéaire si $n = 2$, trilinéaire si $n = 3$) sur un A-module M et à valeurs dans un A-module N est une application $f : M^n \to N$ qui vérifie, pour tout entier $j \in \{1, ..., n\}$ et tout $(x_1, ..., x_{j-1}, x_{j+1}, ..., x_n)$ de M^n que l'application

$$x \mapsto f(x_1, ..., , x_{j-1}, x, x_{j+1}, ..., x_n)$$

est A-linéaire de M dans N. Quand $N = A$, on parle de *forme n-linéaire*. Une forme n-linéaire f est dite *alternée* si $f(x_1, ..., x_n) = 0$ dès qu'il existe $i \neq j$ avec $x_i = x_j$.

1. Autrement dit : une suite exacte d'espaces vectoriels est toujours scindée, mais pas une suite exacte de A-modules.

On définit l'anneau $M_n(A)$ des matrices (n,n) à coefficients dans A de la façon habituelle. Le déterminant d'une matrice $M = (a_{ij})_{1\leq i,j\leq n} \in M_n(A)$ est alors défini par la formule usuelle :

$$\det M := \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i}.$$

Les propriétés usuelles du déterminant sont en général montrées quand A est un corps en utilisant les propriétés des espaces vectoriels, dont certaines ne sont plus valables dans le cadre général où nous sommes. Il est possible de développer les propriétés des formes n-linéaires alternées sur A^n et d'obtenir ainsi ces résultats. Nous allons ici utiliser une autre approche, consistant à se ramener au cas où A est un corps.

Theorème 1.12 *a) Si M et N sont deux matrices de $M_n(A)$, alors*

$$\det(MN) = \det M.\det N.$$

b) L'application qui associe à n vecteurs-colonne (resp. ligne) le déterminant de la matrice M formée avec ces vecteurs est une forme n-linéaire alternée sur A^n. En particulier, on ne change pas le déterminant d'une matrice $M \in M_n(A)$ en ajoutant à une colonne (resp. à une ligne) une combinaison linéaire des autres.

c) On peut calculer le déterminant d'une matrice quelconque M de $M_n(A)$ en développant par rapport à une ligne ou une colonne, avec la même formule que quand A est un corps.

d) Soit $M \in M_n(A)$ et $\widetilde{M}$ la matrice complémentaire de M (transposée de la matrice des cofacteurs de M), alors

$$M\widetilde{M} = \widetilde{M}M = (\det M)I_n.$$

Démonstration : Tous les énoncés se prouvent par la même technique : on observe d'abord que si A est un anneau intègre, on peut le voir comme sous-anneau de son corps des fractions K, et les formules découlent alors immédiatement du cas d'un corps. De plus, on voit immédiatement que si un de ces énoncés est vrai pour un anneau A, il est vrai aussi pour tout anneau quotient A/I (où I est un idéal de A). En particulier, on a le résultat pour tout anneau A qui est un quotient de l'anneau intègre $\mathbf{Z}[X_1,...,X_r]$ (où r est un entier), c'est à dire qui est de type fini en tant que $\mathbf{Z}$-algèbre.

Maintenant, il suffit de remarquer[2] que pour démontrer par exemple l'énoncé a), il suffit de remplacer A par le sous-anneau de A engendré par les coefficients de M et N (lequel est par définition une $\mathbf{Z}$-algèbre de type fini). De même pour b), c), et d) en remplaçant A par le sous-anneau de A engendré par les coefficients de M.

□

Noter qu'on peut aussi démontrer par ce procédé le théorème de Cayley-Hamilton sur un anneau commutatif A quelconque : pour toute matrice $M \in M_n(A)$ de polynôme caractéristique $\chi_M \in A[X]$, on a $\chi_M(M) = 0$.

1.3. Modules libres, modules de type fini

Définition 1.13 Un A-module M est dit *de type fini* s'il existe une partie finie S de M tel que M soit engendré par S. Il est dit *libre* s'il admet une base, i.e. une famille $(x_i)_{i\in I}$ telle que tout élément x de M s'écrive de manière unique $x = \sum_{i\in I} \alpha_i x_i$, avec $(\alpha_i)_{i\in I}$ famille presque nulle d'éléments de A.

Remarque 1.14 a) On verra que si M est libre et de type fini, alors il admet une base finie mais pour l'instant cela n'a rien d'évident !

b) Dire que $(x_i)_{i\in I}$ est une base équivaut au fait que la famille (x_i) soit à la fois génératrice et *libre*, ce dernier point signifiant que la condition $\sum_{i\in I} \alpha_i x_i = 0$ implique que la famille presque nulle (α_i) est nulle.

c) Un A-module M admet une base de cardinal n si et seulement s'il est isomorphe à A^n. Plus généralement il admet une base de cardinal I si et seulement s'il est isomorphe à $A^{(I)} = \bigoplus_I A$ (ensemble des familles $(\alpha_i)_{i\in I}$ presque nulles dans A^I).[3]

d) Un A-module M est de type fini si et seulement s'il s'écrit comme quotient de A^n pour un certain $n > 0$. On ne confondra pas cette notion avec celle de A-algèbre de type fini rencontrée dans le cours sur les anneaux (qui correspond à être un quotient de l'anneau de polynômes $A[X_1, ..., X_n]$). Quand une A-algèbre est de type fini en tant que A-module, on parle parfois de A-algèbre *finie*.

Exemple 1.15 a) $\mathbf{Z}/n\mathbf{Z}$ est un $\mathbf{Z}$-module de type fini (il est engendré par $\bar{1}$), mais il n'est pas libre car dans un $\mathbf{Z}$-module libre, la condition $\alpha x = 0$ implique $\alpha = 0$ ou $x = 0$ si $\alpha \in \mathbf{Z}$, $x \in M$ (on dit qu'un tel module est *sans*

2. On peut aussi simplement observer que A est isomorphe à un quotient d'un anneau de polynômes sur $\mathbf{Z}$ (en général à une infinité d'indéterminées).

3. Attention, si I est infini, il n'y a aucune raison que A^I soit libre. On peut par exemple montrer (difficile) que $\mathbf{Z}^{\mathbf{N}}$ n'est pas un $\mathbf{Z}$-module libre.

torsion. C'est plus généralement le cas dans tout module libre sur un anneau intègre).

b) Bien que le $\mathbf{Z}$-module $\mathbf{Q}$ soit sans torsion, il n'est pas libre car il est *divisible* : si $n > 0$, tout élément x de $\mathbf{Q}$ s'écrit ny avec $y \in \mathbf{Q}$, ce qui n'est pas possible dans un $\mathbf{Z}$-module libre (prendre un élément dont l'une des composantes sur la base est 1 et $n \geq 2$). On verra que sur un anneau *principal*, un module de type fini et sans torsion est libre.

c) De manière immédiate, un quotient d'un module de type fini est encore de type fini.

d) Si A est un anneau non noethérien, un idéal de A qui n'est pas engendré par un nombre fini d'éléments n'est pas de type fini comme A-module, bien que ce soit un sous-module de A (qui est engendré par 1). On verra que si A est noethérien, un sous-module d'un module de type fini sur A est encore de type fini.

e) Soient A un anneau et B une A-algèbre. Supposons que B soit un A-module de type fini. Alors tout B-module M de type fini est aussi un A-module de type fini. En effet, si $(m_1, ..., m_n)$ engendre le B-module M et $(b_1, ..., b_r)$ engendre le A-module B, on voit immédiatement que la famille $(b_i m_j)$ (pour $1 \leq i \leq r$ et $1 \leq j \leq n$) engendre le A-module M.

Ainsi, la situation est beaucoup moins bonne pour les modules que pour les espaces vectoriels. Il y a quand même un énoncé qui est vrai en toute généralité, c'est que les bases de M sont finies et de même cardinal si M est libre et de type fini. C'est l'objet du théorème suivant :

Theorème 1.16 *Soit A un anneau commutatif* **non nul**. *Supposons qu'il existe un morphisme surjectif de A-modules $f : A^r \to A^s$. Alors $r \geq s$. En particulier si f est un isomorphisme, alors $r = s$.*

Démonstration : Nous allons donner deux preuves. La première consiste à se ramener au résultat connu pour les espaces vectoriels, la seconde à effectuer un calcul matriciel utilisant les propriétés du déterminant.

Preuve 1 : Comme $A \neq \{0\}$, A possède au moins un idéal maximal I (ce résultat utilise le théorème de Zorn en général, mais il est immédiat si A est noethérien). Pour tout A-module M, on définit le sous A-module IM comme le module engendré par les im pour $i \in I$ et $m \in M$. Alors M/IM est un espace vectoriel sur le corps $K := A/I$ via $\bar{a}\bar{m} := \overline{am}$, $a \in A$, $m \in M$. On applique cela à $M = A^r$, $N = A^s$. Le morphisme surjectif de A-modules $f : M \to N$ induit un morphisme $\bar{f}$ de K-espaces vectoriels $M/IM \to N/IN$ défini par $\bar{f}(\bar{m}) = \overline{f(m)}$ et il est clair que $\bar{f}$ est encore surjectif.

L'application $M/IM \to K^r$ qui envoie la classe de $(a_1, ..., a_r)$ sur $(\bar{a}_1, ..., \bar{a}_r)$ est un morphisme de K-espaces vectoriels, qui est clairement surjectif et de noyau trivial, via le fait que tous les $\bar{a}_i$ sont nuls si et seulement si $(a_1, ..., a_r)$ est dans IM (vérification immédiate). Ainsi le K-espace vectoriel M/IM est isomorphe à K^r, et de même N/IM est isomorphe à K^s. On obtient finalement un morphisme surjectif de K-espaces vectoriels de K^r sur K^s, donc $r \geq s$ par la théorie de la dimension (théorème du rang). [4]

Preuve 2 : Soit $B \in M_{s,r}(A)$ la matrice de l'application A-linéaire $f : A^r \to A^s$. Comme f est surjectif, les éléments $\varepsilon_1, ..., \varepsilon_s$ de la base canonique de A^s ont chacun un antécédent par f, d'où des vecteurs colonnes $X_1, ..., X_s$ de A^r tels que $BX_i = \varepsilon_i$. La matrice C de $M_{r,s}(A)$ dont les vecteurs colonnes sont les X_i vérifie alors $BC = I_s$. Si on avait $s > r$, on pourrait considérer la matrice B_1 obtenue en ajoutant $s - r$ colonnes nulles à B, et la matrice C_1 obtenue en ajoutant $s - r$ lignes nulles à C, et on aurait encore $B_1C_1 = I_s$, avec B_1 et C_1 dans $M_s(A)$. Mais alors $\det B_1 \det C_1 = 1$ (qui est non nul car A n'est pas nul !), ce qui est impossible vu que d'après le théorème 1.12, une matrice qui a une ligne ou une colonne nulle a un déterminant nul.

□

Corollaire 1.17 *Soit M un module sur un anneau non nul A. Si M est de type fini et admet une base, alors cette base est finie. On dit dans ce cas que M est libre de type fini, et toutes les bases de M ont le même cardinal, qu'on appelle le rang de M.*

Démonstration : Soit r un entier. Notons d'abord que si M possède une base (finie ou non) de cardinal $> r$, alors il existe un sous-module N de M tel que M/N soit isomorphe à A^{r+1} car on obtient un morphisme surjectif de M sur A^{r+1} en choisissant $e_1, ..., e_{r+1}$ dans la base, puis en envoyant tout x de M sur ses composantes sur $e_1, ..., e_{r+1}$. Ceci dit, supposons que M soit engendré par une famille finie $(f_1, ..., f_r)$. Alors on a un morphisme surjectif de A-modules $u : A^r \to M$ défini par $u(a_1, ..., a_r) = \sum_{i=1}^r a_i f_i$. Si M possédait une base infinie (en particulier de cardinal $> r$), on aurait un quotient M/N tel que M/N soit isomorphe à A^{r+1}. En composant u avec la surjection canonique $M \to M/N$, on obtiendrait alors une application A-linéaire surjective de A^r dans A^{r+1}, ce qui contredit le théorème 1.16. Ainsi, si M admet une base,

4. Quand nous aurons vu la notion de produit tensoriel, nous pourrons reformuler cette démonstration : on tensorise M et N par le A-module $K = A/I$; or, cette opération préserve le caractère surjectif (mais pas injectif en général) des morphismes, et transforme A^r en K^r. Noter que si A n'est pas intègre, on ne peut pas faire la même chose en utilisant un corps de fractions.

cette base est finie. Le fait que les bases aient toutes le même cardinal résulte alors immédiatement du théorème 1.16.

□

1.4. Sous-modules sur un anneau noethérien

Bien que dans un module libre de type fini sur un anneau commutatif non nul A, toutes les bases aient même cardinal, on ne peut espérer avoir des résultats sur les sous-modules comparables à ceux dans les espaces vectoriels :

Exemple 1.18 On observe que $2\mathbf{Z}$ est un sous $\mathbf{Z}$-module strict de $\mathbf{Z}$, bien qu'ils aient tous deux pour rang 1 (le premier admet pour base $\{2\}$, le deuxième $\{1\}$). Ainsi $2\mathbf{Z}$ n'a pas de supplémentaire dans $\mathbf{Z}$, car un tel supplémentaire N serait alors isomorphe à $\mathbf{Z}/2\mathbf{Z}$, alors que $\mathbf{Z}$ n'a pas de sous-module isomorphe à $\mathbf{Z}/2\mathbf{Z}$ (il n'a pas d'élément non nul x tel que $2x = 0$). Par conséquent, la famille libre (2) ne peut pas être complétée en une base de $\mathbf{Z}$. D'autre part, si A n'est pas noethérien, le A-module A est libre de rang 1 mais a des sous-modules (=idéaux de A) qui ne sont pas de type fini.

Theorème 1.19 *Soient A un anneau noethérien et M un A-module de type fini. Alors tout sous-module de M est de type fini.*

Démonstration : Comme M est de type fini, on peut l'écrire comme un quotient A^r/M' avec M' sous-module de A^r ; un sous-module de A^r/M' est de la forme N'/M', avec N' sous-module de A^r contenant M'. Ainsi il suffit de prouver le résultat pour $M = A^r$ car un quotient d'un module de type fini est encore de type fini.

On montre cela par récurrence sur r. Pour $r = 1$, c'est la définition d'un anneau noethérien. Supposons le résultat vrai pour tout entier $< r$, et soit N un sous-module de A^r. Appelons M_1 le sous-module de A^r constitué des $(a, 0, 0, .., 0)$ avec $a \in A$, alors M_1 est isomorphe à A. D'après le cas $r = 1$, $N_1 := N \cap M_1$ est de type fini. D'autre part l'application linéaire $\pi : N \to A^r/M_1$ qui à x associe $\bar{x}$ a pour noyau N_1 ; le module A^r/M_1 est isomorphe à A^{r-1}, donc $\operatorname{Im}\pi$ est de type fini par hypothèse de récurrence. Soit $(\bar{x}_1, ..., \bar{x}_n)$ une famille finie engendrant $\operatorname{Im}\pi$ ($x_i \in N$) et $(y_1, ..., y_m)$ une famille finie engendrant N_1, alors $(x_1, ..., x_n, y_1, ..., y_m)$ engendre N.[5] En effet, si $x \in N$, on peut écrire $\bar{x} = \sum_{i=1}^{r} \alpha_i \bar{x}_i$ avec les α_i dans A, ce qui signifie que

$$x = \sum_{i=1}^{r} \alpha_i x_i + y,$$

5. Plus généralement si $0 \to M_1 \to M \to M_2 \to 0$ est une suite exacte de A-modules, il est clair que le fait que M_1 et M_2 soient de type fini implique que M est de type fini.

avec $y \in (N \cap M_1) = N_1$, puis

$$x = \sum_{i=1}^{r} \alpha_i x_i + \sum_{i=1}^{m} \beta_i y_i,$$

avec les β_i dans A.

□

Remarque 1.20 Noter qu'on peut avoir besoin de plus de générateurs pour un sous-module de M que pour N, prendre par exemple un idéal de A qui n'est pas principal. On verra que précisément, cette difficulté disparaît quand l'anneau A est principal.

Définition 1.21 Un module M sur un anneau commutatif A est dit *noethérien* si tout sous-module de M est de type fini.

De façon équivalente, M est un module noethérien ssi toute suite croissante de sous-modules de M est stationnaire, ou encore ssi toute famille non vide E de sous-modules possède un élément maximal dans E (preuve identique que pour les anneaux noethériens). Le théorème 1.19 dit qu'un module de type fini sur un anneau noethérien est un module noethérien (il peut arriver par contre que M soit noethérien sans que A le soit, prendre par exemple un anneau non noethérien et un idéal I tel que le quotient $M = A/I$ soit fini ; il est facile de fabriquer un tel exemple avec $A = \mathbf{Z}[(X_n)_{n\in\mathbf{N}^*}]$).

Theorème 1.22 *Soit A un anneau commutatif non nul. On suppose qu'il existe une application linéaire injective f de A^r ver A^s. Alors $r \leq s$.*

On utilise un lemme général :

Lemme 1.23 *Soit A un anneau commutatif. Soit M un module-noethérien. Soit P un A-module, on suppose qu'il existe une application A-linéaire injective $u : M \oplus P \to M$. Alors $P = 0$.*

Démonstration : En prenant les images de M et P par u, on obtient un sous-module $M_1 \oplus P_1$ de M, avec M_1 isomorphe à M et P_1 isomorphe à P. Par récurrence, on construit des suites (M_r) et (P_r) telles que $M_r \oplus \bigoplus_{i=1}^{r} P_i$ soit un sous-module de M, avec M_r isomorphe à M et chaque P_i isomorphe à P. Si $P \neq 0$, la suite des $\bigoplus_{i=1}^{r} P_i$ pour $r > 0$ est alors strictement croissante, contredisant le fait que M est un module noethérien.

On passe maintenant à la preuve du théorème 1.22. On commence par le cas où A est noethérien. Si $r > s$, posons $M = A^s$ et $P = A^{r-s}$, alors

comme $A \neq 0$ le module P est non nul avec $M \oplus P$ équipé d'un morphisme injectif vers M, ce qui contredit le lemme car le module M est noethérien via le théorème 1.19.

Passons au cas général. Soit B la matrice de f, dans les bases canoniques de A^r et A^s. Soit R la sous $\mathbf{Z}$-algèbre de A engendrée par les coefficients de B, elle est de type fini sur $\mathbf{Z}$ et c'est donc un anneau noethérien. D'après ce qui précède, l'application R-linéaire $R^r \to R^s$ induite par B ne peut pas être injective, et il existe donc un vecteur-colonne non nul X de R^r tel que $B.X = 0$, ce qui fournit un vecteur-colonne non-nul $X \in A^r$ tel que $B.X = 0$. Ainsi f ne peut pas être injective.

□

Corollaire 1.24 *Soit A un anneau non nul. Si M est un sous-module libre de A^s, alors son rang r est au plus s. Si un A-module P admet une famille génératrice comportant s éléments, alors toute famille comportant au moins $s+1$ éléments est liée*[6].

Démonstration : La première assertion vient du théorèeme 1.22 et de ce que M est isomorphe à A^r (on sait que M est de rang fini, sinon il contiendrait un sous-module isomorphe à A^{s+1}, qui ne peut pas être un sous-module de A^s), Pour la deuxième, on observe que P est isomorphe à un quotient A^s/N. Si $(\bar{e}_1, ..., \bar{e}_r)$ est une famille d'éléments de P (avec les e_i dans A^r) et $r \geq s+1$, alors la famille des e_i est liée dans A^r d'après ce qui précède, donc aussi celle des $\bar{e}_i$ en passant au quotient.

□

En particulier un idéal I d'un anneau A ne peut pas être un A-module libre s'il n'est pas engendré par un seul élément. On ne peut donc espérer un énoncé positif pour la liberté des sous-modules d'un module libre que pour les anneaux principaux ; on verra que c'est effectivement le cas.

Remarque 1.25 On peut montrer (en utilisant des calculs un peu fastidieux sur les déterminants ; voir exercice en TD...) que si B est une matrice de $M_r(A)$ et f est l'application A-linéaire $A^r \to A^r$ qu'elle induit, alors f est injective si et seulement si $\det B$ est non nul et non diviseur de zéro dans l'anneau A. On peut alors retrouver le théorème 1.22 : si on avait $r > s$, la matrice obtenue en rajoutant $r - s$ lignes nulles à la matrice de f représenterait encore une application linéaire injective (car elle représenterait le composé de f avec l'injection $A^s \to A^r$ définie par $x \mapsto (x, 0, 0, ...)$) et serait de déterminant nul.

6. De façon étonnante, il est difficile de démontrer ce résultat directement si l'anneau A n'est pas supposé intègre ; voir aussi la remarque 1.25 ci-dessous.

2. Produit tensoriel

2.1. Introduction

La notion de produit tensoriel est un peu difficile à appréhender au début, mais elle se révèle indispensable quand on veut traiter de sujet avancés en algèbre (notamment en théorie des nombres ou en géométrie algébrique). Nous nous contenterons dans ce cours d'une initiation, consistant en les propriétés de base et quelques exemples. Il nous a par contre semblé important de ne pas nous limiter au cas des espaces vectoriels sur un corps, qui est vraiment trop restrictif (d'autant que sur un corps on peut souvent utiliser le calcul matriciel, sans avoir vraiment besoin de la notion de produit tensoriel).

Avant de rentrer dans les détails, signalons dès à présent quelques exemples (vus précédemment dans ce cours, ou encore les années antérieures) où le produit tensoriel est sous-jacent :

- Complexifié d'un espace vectoriel réel.
- Quand A est un sous-anneau d'un anneau commutatif B, regarder une matrice à coefficients dans A comme étant aussi à coefficients dans B.
- Preuve 1 du théorème 1.16.

Dans toute cette section, A désigne un anneau commutatif.

2.2. Produit tensoriel de deux modules

Rappelons d'abord une définition déjà rencontrée quand $L = A$:

Définition 2.1 Soient M, N, et L des modules sur l'anneau commutatif A. Une application $f : M \times N \to L$ est dite *A-bilinéaire* (ou bilinéaire si A est sous-entendu) si pour tous $m \in M, n \in N$, les applications $f(m, .)$ et $f(., n)$ sont A-linéaires de N (resp. M) dans L.

Soient M et N deux A-modules. On cherche à construire un A-module H, équipé d'une application bilinéaire $\Phi : M \times N \to H$, vérifiant la *propriété universelle* suivante :

(P) Pour tout A-module L et toute application bilinéaire $f : M \times N \to L$, il existe un unique morphisme de A-modules $\tilde{f} : H \to L$ tel que $f = \tilde{f} \circ \Phi$.

Explicitement, étant donnés f et Φ, on veut qu'il y ait toujours une unique application A-linéaire $\tilde{f}$ qui fait commuter le diagramme :

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & L \\ {\scriptstyle \Phi}\downarrow & \nearrow_{\tilde{f}} & \\ H & & \end{array}$$

Theorème 2.2 *Un tel module H existe et est unique à isomorphisme près. On l'appelle le produit tensoriel des deux A-modules M et N, et on le note $M \otimes_A N$.*

Démonstration : Si H et H' vérifient tous deux (P) (avec des applications bilinéaires associées Φ et Φ'), alors on applique d'abord (P) à (H, Φ) en prenant pour f l'application bilinéaire Φ', d'où une application A-linéaire $\tilde{\Phi'} : H \to H'$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} M \times N & \xrightarrow{\Phi'} & H' \\ {\scriptstyle \Phi}\downarrow & \nearrow_{\tilde{\Phi'}} & \\ H & & \end{array}$$

On a ainsi une factorisation $\Phi' = \tilde{\Phi'} \circ \Phi$; on a de même par symétrie une application A-linéaire $\tilde{\Phi} : H' \to H$ telle que $\Phi = \tilde{\Phi} \circ \Phi'$ Ainsi

$$\tilde{\Phi} \circ \tilde{\Phi'} \circ \Phi = \tilde{\Phi} \circ \Phi' = \Phi,$$

ce qu'on peut récrire $\mathrm{Id}_H \circ \Phi = (\tilde{\Phi} \circ \tilde{\Phi'}) \circ \Phi$. L'unicité dans la propriété universelle (P) (appliquée au couple (H, Φ) avec l'application bilinéaire $f = \Phi$) donne alors $\tilde{\Phi} \circ \tilde{\Phi'} = \mathrm{Id}_H$ et de même $\tilde{\Phi'} \circ \tilde{\Phi} = \mathrm{Id}_{H'}$, d'où un isomorphisme entre H et H'.

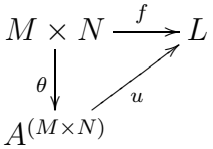
Montrons maintenant l'existence de (H, Φ) vérifiant (P). On considère le A-module $A^{(M \times N)}$ des familles presque nulles d'éléments de A indexées par $M \times N$, dont on note $(e_{x,y})_{(x,y) \in M \times N}$ la base canonique (toutes les composantes de $e_{x,y}$ sont nulles sauf celle sur (x, y) qui vaut 1). On note alors H le quotient de $A^{(M \times N)}$ par le sous-module R engendré par les éléments d'une des formes suivantes :

$$e_{x_1+x_2,y} - e_{x_1,y} - e_{x_2,y}; e_{x,y_1+y_2} - e_{x,y_1} - e_{x,y_2}; e_{ax,y} - a e_{x,y}; e_{x,ay} - a e_{x,y},$$

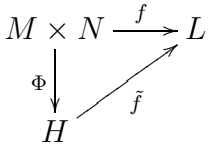
avec $x_1, x_2, x \in M$, $y_1, y_2, y \in N$ et $a \in A$.

Soit alors $\theta : M \times N \to A^{(M \times N)}$ l'application qui envoie (x, y) sur $e_{x,y}$. Elle n'est pas a priori bilinéaire, mais si on note $\Phi : M \times N \to H$ l'application induite par θ, qui envoie (x, y) sur l'image $\overline{e_{x,y}}$ de $e_{x,y}$ dans $H = A^{(M \times N)}/R$, alors Φ est bilinéaire par définition de R.

Si maintenant $f : M \times N \to L$ est une application bilinéaire, le morphisme u de A-modules $A^{(M \times N)} \to L$ qui envoie chaque $e_{x,y}$ sur $f(x, y)$ a un noyau qui contient R par bilinéarité de f, il induit donc un morphisme $\tilde{f} : H \to L$ par passage au quotient. Par définition de θ, on a un diagramme commutatif



d'où en passant au quotient un diagramme commutatif



Autrement dit on a $f = \tilde{f} \circ \Phi$, et il est immédiat que $\tilde{f}$ est le seul morphisme de A-modules de H dans L qui vérifie cette propriété. On a donc bien démontré la propriété universelle (P) pour le couple (H, Φ).

□

Remarque 2.3 a) Stricto sensu, on devrait utiliser la notation $(M \otimes_A N, \Phi)$ pour le produit tensoriel, mais en général l'application bilinéaire Φ est sous-entendue.

b) Quand M et N sont des groupes abéliens, on notera souvent $M \otimes N$ pour $M \otimes_{\mathbf{Z}} N$.

c) Pour $(x, y) \in M \times N$, on notera $x \otimes y$ l'image de (x, y) par Φ. Ainsi, tout élément de $M \otimes_A N$ s'écrit (de manière non unique en général) comme une somme finie $\sum_i x_i \otimes y_i$ avec $(x_i, y_i) \in M \times N$, comme il résulte de la construction explicite du produit tensoriel. De plus, l'application $(x, y) \mapsto x \otimes y$ est A-bilinéaire sur $M \times N$.

La propriété universelle s'écrit donc maintenant : pour toute application bilinéaire $f : M \times N \to L$, il existe une unique application linéaire $\tilde{f} : M \otimes N \to L$ telle que

$$f(x, y) = \tilde{f}(x \otimes y)$$

pour tous $x \in M$, $y \in N$.

d) Les éléments de $M \otimes_A N$ de la forme $x \otimes y$ avec $x \in M$ et $y \in N$ sont parfois appelés éléments *décomposables* de $M \otimes_A N$. On prendra garde au fait qu'ils engendrent le A-module $M \otimes_A N$, mais leur ensemble peut ne pas être un sous-module de $M \otimes_A N$. Néanmoins, la propriété universelle dit qu'on peut définir une application A-linéaire u sur $M \otimes_A N$ par une formule du genre $u(x \otimes y) = f(x, y)$, dès lors que f est une expression A-bilinéaire en (x, y).

Exemple 2.4 a) Si $N = Ae_1$ est libre de base (e_1) (et donc isomorphe à A), alors $u : m \mapsto e_1 \otimes m$ est un isomorphisme de M sur $N \otimes_A M$ (on a un énoncé analogue avec $M \otimes_A N$). Posons en effet $f(\lambda e_1, m) = \lambda m$ pour tous $\lambda \in A$,

$m \in M$, ce qui donne une application bilinéaire bien définie de $N \times M$ dans M (vu que (e_1) est une base de N). La propriété universelle donne alors une application linéaire $\tilde{f} : N \otimes_A M \to M$ qui fait commuter le diagramme

$$\begin{array}{ccc} N \times M & \xrightarrow{f} & M \\ {\scriptstyle \Phi}\downarrow & \nearrow_{\tilde{f}} & \\ N \otimes_A M & & \end{array}$$

Ainsi $\tilde{f}(e_1 \otimes m) = m$ pour tout $m \in M$, ce qui implique que $\tilde{f}$ est un inverse pour l'application linéaire u (en notant que tout élément de $N \otimes_A M$ est somme d'éléments de la forme $\lambda e_1 \otimes m$ avec $m \in M$ et $\lambda \in A$, donc par bilinéarité s'écrit $e_1 \otimes m$ avec $m \in M$).

b) Soient r, s deux entiers premiers entre eux. Alors $\mathbf{Z}/r\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/s\mathbf{Z} = 0$. En effet, il existe des entiers u, v tels que $ur+vs = 1$ (Bezout). Pour $x \in \mathbf{Z}/r\mathbf{Z}$ et $y \in \mathbf{Z}/s\mathbf{Z}$, on a alors :

$$x \otimes y = (ur + vs)(x \otimes y) = urx \otimes y + x \otimes vsy = 0 \otimes y + x \otimes 0 = 0.$$

c) Soit I un idéal de A. Soit M un A-module. Vérifions avec la propriété universelle que

$$M \otimes_A (A/I) \simeq M/IM.$$

On définit en effet $\Phi : M \times A/I \to M/IM$ par $\Phi(m, \bar{a}) = \overline{a.m}$ pour tout $m \in M$ et $a \in A$, où $\bar{a}$ est la classe de a dans A/I ; ceci a bien un sens car si on modifie a par un élément de I, on modifie $a.m$ par un élément de IM. Alors, si $f : M \times A/I \to L$ est bilinéaire, on a pour tous $m \in M$, $a \in A$:

$$f(m, \bar{a}) = f(m, a\bar{1}) = f(am, \bar{1}),$$

d'où un diagramme commutatif

$$\begin{array}{ccc} M \times A & \xrightarrow{f} & L \\ {\scriptstyle \Phi}\downarrow & \nearrow_{\tilde{f}} & \\ M/IM & & \end{array}$$

où $\tilde{f}$ est l'application A-linéaire $\bar{m} \mapsto f(m, \bar{1})$, qui est bien définie sur M/IM : en effet si on modifie m par un élément de la forme $i.x$ avec $i \in I$ et $x \in M$, on modifie $f(m, \bar{1})$ par

$$f(ix, \bar{1}) = f(x, i.\bar{1}) = f(x, \bar{i}) = 0.$$

De plus $\tilde{f}$ est clairement la seule application A-linéaire possédant cette propriété.

En particulier, si M est un groupe abélien et $n \in \mathbf{N}^*$, on a $M \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} = M/nM$ et si M est divisible (par exemple $M = \mathbf{Q}$), on a $M \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} = 0$.

Proposition 2.5 *a) (Commutativité) Si M et N sont des A-modules, alors*

$$M \otimes_A N \simeq N \otimes_A M.$$

b) (Associativité) Si M, N, P sont des A-modules, alors

$$P \otimes_A (M \otimes_A N) \simeq (P \otimes_A M) \otimes_A N.$$

c) (Distributivité) Si (M_i) est une famille de A-modules et N est un A-module, alors[7]

$$(\bigoplus_i M_i) \otimes_A N \simeq \bigoplus_i (M_i \otimes N).$$

Autrement dit, "le produit tensoriel commute avec les sommes directes".

Démonstration : Tout résulte de la propriété universelle (P). Montrons par exemple c), en vérifiant que $\bigoplus_i (M_i \otimes_A N)$ satisfait la propriété universelle de $(\bigoplus_i M_i) \otimes_A N$. On définit

$$\Phi : (\bigoplus_i M_i) \times N \to \bigoplus_i (M_i \otimes_A N)$$

en envoyant $(\sum_i m_i, n)$ sur $\sum_i (m_i \otimes n)$. Soit alors $f : (\bigoplus_i M_i) \times N \to L$ bilinéaire, elle induit pour chaque i une application bilinéaire $f_i : M_i \times N \to L$, qui se factorise (via la propriété universelle de $M_i \otimes_A N$) par une unique application linéaire $\tilde{f}_i : M_i \otimes_A N \to L$. Alors, via la propriété universelle de la somme directe (remarque 1.10) on a un unique morphisme $\tilde{f} : \bigoplus_i (M_i \otimes_A N) \to L$ vérifiant $f = \tilde{f} \circ \Phi$: il est défini par $\tilde{f} = \bigoplus \tilde{f}_i$.

Pour a), la propriété universelle permet de définir une application A-linéaire $M \otimes_A N \to N \otimes_A M$ qui envoie tout $x \otimes y$ (où $x \in M, y \in N$) sur $y \otimes x$, et sa réciproque qui envoie tout $y \otimes x$ sur $x \otimes y$. Pour b), on définit un isomorphisme $\tilde{f}$ de $P \otimes_A (M \otimes_A N)$ sur $(P \otimes_A M) \otimes_A N$ qui envoie $z \otimes (x \otimes y)$ sur $(z \otimes x) \otimes y$ pour tous $x \in M, y \in N, z \in P$: pour cela, on observe que si $z \in P$ est fixé, alors on a une application A-linéaire $f_z : M \otimes_A N \to (P \otimes_A M) \otimes_A N$ qui envoie $x \otimes y$ sur $(z \otimes x) \otimes y$, puis on observe que f_z dépend A-linéairement de z, ce qui donne une application bilinéaire $f : P \otimes_A (M \otimes_A N) \to (P \otimes_A M) \otimes_A N$ via $f(z, u) = f_z(u)$, puis on prend $\tilde{f}$ tel que $\tilde{f}(z \otimes u) = f(z, u)$ pour tous $z \in P$, $u \in (M \otimes_A N)$. L'isomorphisme réciproque de $\tilde{f}$ est construit exactement de la même manière.

□

7. Attention, cette propriété n'est pas vraie en général si on remplace la somme directe par le produit direct d'un nombre infini de modules ; en revanche, elle s'étend à ce que l'on appelle une *limite inductive* de A-modules, voir TD.

Corollaire 2.6 *Soit M un A-module libre de base $(e_i)_{i\in I}$. Alors tout élément de $M\otimes_A N$ s'écrit de manière unique $\sum_i e_i\otimes y_i$, où (y_i) est une famille presque nulle d'éléments de N. En particulier, si K est un corps et $(f_j)_{j\in J}$ est une base du K-ev N, alors $(e_i\otimes f_j)_{i\in I,j\in J}$ est une base du K-ev $M\otimes_K N$. Dans le cas où M et N sont de dimension finie sur K, on a donc :*

$$\dim(M\otimes_K N) = \dim M.\dim N.$$

Démonstration : On écrit $M = \bigoplus_i Ae_i$, d'où $M\otimes_A N = \bigoplus_i (Ae_i)\otimes_A N$ via la proposition 2.5, c). On utilise alors l'exemple 2.4, a), qui dit que tout élément de $(Ae_i)\otimes_A N$ s'écrit de manière unique $e_i\otimes y_i$ avec $y_i\in N$.

□

Remarque 2.7 L'associativité du produit tensoriel permet de définir sans ambiguîté le produit tensoriel $M_1\otimes_A\otimes_A ...\otimes_A M_n$ de n modules, pour lequel on dispose d'une propriété universelle analogue à (P) : on a une application n-linéaire

$$\Phi : M_1\times ...\times M_n\to M_1\otimes_A ...\otimes_A M_n;\quad (m_1,...,m_n)\mapsto m_1\otimes ...\otimes m_n$$

telle que pour toute application n-linéaire $f : M_1\times ...\times M_n\to L$, il existe une unique application linéaire $\tilde{f} : M_1\otimes_A\otimes_A ...\otimes_A M_n\to L$ qui fait commuter le diagramme

$$\begin{array}{ccc} M_1\times ...\times M_n & \xrightarrow{f} & L \\ \Phi\downarrow & \nearrow_{\tilde{f}} & \\ M_1\otimes_A ...\otimes_A M_n & & \end{array}$$

Autrement dit, on a

$$f(m_1,...,m_n) = \tilde{f}(m_1\otimes ...\otimes m_n).$$

pour tous $m_1,...,m_n$ dans M.

Définition 2.8 Soient $u : M\to M'$ et $v : N\to N'$ des morphismes de A-modules. Alors, par la propriété universelle (P) appliquée à l'application bilinéaire $(x,y)\mapsto u(x)\otimes v(y)$, il existe un unique morphisme de A-modules

$$u\otimes v : M\otimes_A N\to M'\otimes_A N'$$

tel que

$$(u\otimes v)(x\otimes y) = u(x)\otimes v(y)$$

pour tous $x\in M, y\in N$. On appelle $u\otimes v$ le *produit tensoriel* des morphismes u et v.

Remarque 2.9 Notons $L(M, M')$ le A-module des applications linéaires de M dans M'. Le procédé précédent définit une application linéaire canonique de $L(M, M') \otimes_A L(N, N')$ vers $L(M \otimes_A N, M' \otimes_A N')$ (d'où le choix de notation $u \otimes v$ pour noter l'image de $u \otimes v$ par cette application canonique). On prendra quand même garde que cette application est un isomorphisme si les A-modules M et N sont libres, mais pas en général (voir TD).

2.3. Produit tensoriel par une A-algèbre

Soit B une A-algèbre, associée à un morphisme d'anneaux $\varphi : A \to B$. Soit M un A-module. Noter qu'un B-module N est ipso facto aussi un A-module en posant $a.n = \varphi(a).n$ pour tous $a \in A$, $n \in N$. Le produit tensoriel permet en quelque sorte de faire l'opération inverse :

Définition 2.10 Soit B une A-algèbre. Soit M un A-module. On définit une structure de B-module sur $M \otimes_A B$ en posant, pour tout $b \in B$, $b.z := (\mathrm{Id}_M \otimes m_b)(z)$, où $m_b : B \to B$ est la multiplication par b. Autrement dit, on a

$$b.(m \otimes b') := m \otimes bb' \tag{1}$$

pour tous $m \in M$, $b, b' \in B$. On dit que le B-module $M \otimes_A B$ est obtenu à partir de M par *extension des scalaires* de A à B.

Noter qu'on vérifie immédiatement les axiomes de la structure de B-module via la formule (1) et le fait que tout élément de $M \otimes_A B$ est somme d'éléments de la forme $m \otimes b'$ avec $m \in M$ et $b' \in B$.

Définition 2.11 Le même procédé permet de définir une structure de B-module sur $M \otimes_A N$ pour tout A-module M et tout B-module N, en posant $b.(m \otimes n) := m \otimes (b.n)$ pour tous $m \in M, n \in N, b \in B$. La définition 2.10 correspond au cas $N = B$.

Exemple 2.12 a) Soient L un corps et K un sous-corps de L. Pour tout K-espace vectoriel M, on dispose du L-espace vectoriel $M \otimes_K L$. D'après le corollaire 2.6, sa dimension comme L-ev est celle de M comme K-ev car si (e_i) est une base du K-ev M, alors $(e_i \otimes 1)$ est une base du L-ev $M \otimes_K L$ puisque tout élément x de $M \otimes_K L$ admet une écriture unique

$$x = \sum_i e_i \otimes l_i = \sum_i l_i.(e_i \otimes 1),$$

avec les l_i dans L. On retrouve par exemple la notion de complexifié d'un $\mathbf{R}$-ev.

b) Plus généralement, le même raisonnement donne que si M est un A-module libre de rang r, alors $M \otimes_A B$ est un B-module libre de rang r, et si on suppose seulement que M est un A-module de type fini, on obtient encore que $M \otimes_A B$ est un B-module de type fini.

c) Soit M et N des A-modules libres de rang fini. Soient $(e_i)_{1\leq i\leq r}$ et $(f_j)_{1\leq j\leq s}$ des bases respectives de M et N. Soit $f : M \to N$ une application A-linéaire, de matrice Q dans ces bases. Alors l'application

$$f \otimes \mathrm{Id}_B : M \otimes_A B \to N \otimes_A B$$

est B-linéaire et sa matrice est Q (vue comme matrice à coefficients dans B) dans les bases $(e_i \otimes 1)_{1\leq i\leq r}$, $(f_j \otimes 1)_{1\leq j\leq s}$. On peut par exemple appliquer cela à une application A-linéaire $A^r \to A^s$, pour obtenir en tensorisant par B une application B-linéaire $B^r \to B^s$ dont la matrice reste la même. C'est ce procédé qu'on a utilisé dans la première preuve du théorème 1.16, en prenant $B = A/I$, où I est un idéal maximal de A.

d) Si M est un A-module et I un idéal de A, alors on a l'isomorphisme $M \otimes_A A/I \simeq M/IM$, où IM désigne le sous-module de M engendré par les im avec $i \in I$ et $m \in M$. La preuve est tout à fait analogue à celle du cas particulier $A = \mathbf{Z}$, $I = n\mathbf{Z}$ (exemple 2.4, c), en considérant l'application A-bilinéaire $\Phi : (m, \bar{a}) \mapsto \overline{am}$ de $M \times A/I$ dans M/IM qui induit un A-isomorphisme (ou encore un A/I-isomorphisme) $M \otimes_A A/I \simeq M/IM$, lequel envoie $m \otimes \bar{a}$ sur $\overline{am}$ pour tous $a \in A, m \in M$.

Proposition 2.13 *On a un isomorphisme de B-modules :*

$$(M \otimes_A B) \otimes_B N \simeq M \otimes_A N$$

Démonstration : On va vérifier que le B-module $M \otimes_A N$ vérifie la propriété universelle requise pour être isomorphe au produit tensoriel (sur l'anneau B) $(M \otimes_A B) \otimes_B N$. On commence par définir une application B-bilinéaire $\Phi : (M \otimes_A B) \times N \to M \otimes_A N$ qui vérifie

$$\Phi(m \otimes_A b, n) = m \otimes_A bn = b.(m \otimes_A n) \tag{2}$$

pour tous $m \in M, n \in N, b \in B$. Pour ce faire, on prend (pour chaque $n \in N$ fixé) pour $\Phi(., n)$ l'application A-linéaire $\mathrm{Id}_M \otimes_A (.n)$ de $M \otimes_A B$ vers $M \otimes_A N$. Par définition, l'application Φ est alors A-bilinéaire, et elle est en fait B-bilinéaire via la formule (2) et la définition de la structure de B-module sur $M \otimes_A B$.

Soit maintenant $f : (M \otimes_A B) \times N \to L$ une application B-bilinéaire. Par la propriété universelle du produit tensoriel $M \otimes_A N$, il existe une unique application A-linéaire $\tilde{f} : M \otimes_A N \to L$ telle que

$$\tilde{f}(m \otimes_A n) = f(m \otimes_A 1, n)$$

pour tous $m \in M, n \in N$. Comme f est B-bilinéaire, on a

$$f(m \otimes_A 1, bn) = b.f(m \otimes_A 1, n) = f(m \otimes_A b, n). \tag{3}$$

Ainsi

$$\tilde{f}(b.(m \otimes_A n)) = \tilde{f}(m \otimes_A bn) = f(m \otimes_A 1, bn) = b.f(m \otimes_A 1, n) = b.\tilde{f}(m \otimes_A n),$$

ce qui montre déjà que $\tilde{f}$ est B-linéaire. De plus $\tilde{f}$ fait commuter le diagramme

$$\begin{array}{ccc} (M \otimes_A B) \times N & \xrightarrow{f} & L \\ \Big\downarrow{\scriptstyle \Phi} & \nearrow_{\tilde{f}} & \\ M \otimes_A N & & \end{array}$$

car

$$\tilde{f}(\Phi(m \otimes_A b, n)) = \tilde{f}(m \otimes_A bn) = f(m \otimes_A 1, bn) = f(m \otimes_A b, n)$$

d'après (3). Il est en outre immédiat que c'est la seule qui a cette propriété. □

2.4. Produit tensoriel de deux A-algèbres

Quand B et C sont deux A-algèbres, alors on peut munir $B \otimes_A C$ d'une structure de A-algèbre en définissant un produit interne sur $B \otimes_A C$ vérifiant

$$(b \otimes c).(b' \otimes c') = (bb') \otimes (cc') \tag{4}$$

pour tous $b, b' \in B$ et $c, c' \in C$. Pour définir formellement ce produit, on considère l'application quadrilinéaire

$$g : B \times C \times B \times C \to B \otimes_A C$$

définie par $g(b, c, b', c') = (bb') \otimes (cc')$ pour tous $b, b' \in B$ et $c, c' \in C$. Par la propriété universelle de la remarque 2.7, elle se factorise par une application A-linéaire

$$\tilde{g} : B \otimes_A C \otimes_A B \otimes_A C \to B \otimes_A C,$$

ce qui permet de définir $z.z' = \tilde{g}(z \otimes z')$ pour tous $z, z' \in B \otimes_A C$. La formule (4) (jointe au fait que tout élément de $B \otimes_A C$ est somme d'éléments décomposables) implique alors immédiatement que ce produit est associatif, commutatif, distributif par rapport à l'addition, et compatible avec la structure de A-module de $B \otimes_A C$, autrement dit il fait de $B \otimes_A C$ une A-algèbre.

Définition 2.14 L'algèbre $B \otimes_A C$ est la A-algèbre *produit tensoriel des deux A-algèbres B et C*. Elle est équipée [8] de morphismes de A-algèbres $u_B : B \to B \otimes_A C$ et $u_C : C \to B \otimes_A C$ définis respectivement par $b \mapsto b \otimes 1$ et $c \mapsto 1 \otimes c$. Ainsi, $B \otimes_A C$ est également munie d'une structure de B-algèbre via u_B et de C-algèbre via u_C.

La A-algèbre $B \otimes_A C$ possède la propriété universelle suivante :

Proposition 2.15 *Pour toute A-algèbre D et toute paire de morphismes de A-algèbres $f_B : B \to D$ et $f_C : C \to D$, il existe un unique morphisme de A-algèbres $f : B \otimes_A C \to D$ tel que $f_B = f \circ u_B$ et $f_C = f \circ u_C$.*

Démonstration : On applique la propriété universelle de $B \otimes_A C$ à l'application A-bilinéaire $\varphi : B \times C \to D$ définie par

$$\varphi(b, c) = f_B(b) f_C(c); \quad b \in B, c \in C.$$

On obtient une application A-linéaire $f : B \otimes_A C \to D$ vérifiant

$$f(b \otimes c) = f_B(b) f_C(c) \tag{5}$$

pour tous $b \in B$, $c \in C$, d'où $f(b \otimes 1) = f_B(b)$ et $f(1 \otimes c) = f_C(c)$. Il résulte de (5) que f est de plus un morphisme d'anneaux, et il est immédiat que c'est le seul qui convient.

□

Exemple 2.16 a) Prenons $B = A[X_1, ..., X_r]$. On a alors un isomorphisme de C-algèbres :

$$f : B \otimes_A C \simeq C[X_1, ..., X_r],$$

qui envoie $P \otimes c$ sur cP pour tous $P \in B, c \in C$ En effet, la propriété universelle du produit tensoriel dit qu'on a une unique application A-linéaire f telle que $f(P \otimes c) = cP$ pour tous $P \in B, c \in C$; cette formule montre que c'est en fait un morphisme de C-algèbres. Par ailleurs on définit une application réciproque $g : C[X_1, ..., X_r] \to B \otimes_A C$ comme l'unique morphisme de C-algèbres qui envoie chaque X_i sur $X_i \otimes 1$, ce qui est licite via la propriété universelle des algèbres de polynômes.

b) On en déduit par exemple que

$$A[X_1, ..., X_r] \otimes_A A[Y_1, ..., Y_s] \simeq A[X_1, ..., X_r, Y_1, ..., Y_s].$$

8. Noter que ces morphismes n'ont pas d'analogue quand B et C sont juste des A-modules.

c) Plus généralement, si $F_1, ..., F_s$ sont des polynômes de $A[X_1, ..., X_r]$, on a un isomorphisme de C-algèbres

$$(A[X_1, ..., X_r]/(F_1, ..., F_s)) \otimes_A C \simeq (C[X_1, ..., X_r]/(F_1, ..., F_s)),$$

où on a encore noté $F_1, ..., F_s$ les images de $F_1, ..., F_s$ dans $C[X_1, ..., X_r]$ par le morphisme canonique $A[X_1, ...X_r] \to C[X_1, ...X_r]$ induit par la structure de A-algèbre de C. La preuve est similaire à a), la donnée d'un morphisme de C-algèbres sur $C[X_1, ..., X_r]/(F_1, ..., F_s)$ équivalant à celle d'un morphisme de C-algèbres sur $C[X_1, ..., X_r]$ s'annulant sur l'idéal $(F_1, ..., F_s)$.

d) Prenons $A = \mathbf{Z}$, $B = \mathbf{Z}[i\sqrt{5}]$ et $C = \mathbf{Z}/p\mathbf{Z}$ avec p premier. En écrivant $B \simeq \mathbf{Z}[X]/(X^2 + 5)$, on obtient

$$B \otimes_A C \simeq \mathbf{Z}/p\mathbf{Z}[X]/(X^2 + 5).$$

Si $p = 5$, cette dernière algèbre est isomorphe à $\mathbf{Z}/p\mathbf{Z}[\varepsilon]$. Si $p \neq 5$, elle est isomorphe à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ ou au corps de cardinal 25, suivant que -5 est ou pas un carré modulo p (voir le chapitre sur les corps).

2.5. Produit tensoriel et suites exactes

Une suite exacte de A-modules ne le reste pas forcément quand on la tensorise par un A-module.

Exemple 2.17 Considérons l'injection f de $\mathbf{Z}$ dans $\mathbf{Q}$ (vus comme des $\mathbf{Z}$-modules). L'application $\mathbf{Z}$-linéaire

$$\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \to \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z}$$

obtenue en tensorisant par l'identité de $\mathbf{Z}/n\mathbf{Z}$ dans lui-même donne (cf. exemple 2.4, c) l'application nulle $\mathbf{Z}/n\mathbf{Z} \to 0$, qui n'est pas injective.

On ne peut donc pas espérer conserver l'injectivité en tensorisant par n'importe quel A-module. On a cependant :

Theorème 2.18 *Soit*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$$

une suite exacte de A-modules. Soit M un A-module. Alors la suite

$$N' \otimes_A M \xrightarrow{f_M} N \otimes_A M \xrightarrow{g_M} N'' \otimes_A M \to 0$$

(obtenue en tensorisant les flèches f, g par le morphisme identité $M \to M$) reste exacte.

On traduit cette propriété en disant que le foncteur $\otimes_A M$ est *exact à droite.*

Démonstration : Comme $N'' \otimes_A M$ est engendré par les $x'' \otimes y$ avec $x'' \in N'', y \in M$, la surjectivité de g_M résulte immédiatement de celle de g et de la formule $g_M(x \otimes y) = g(x) \otimes y$ pour tous $x \in N, y \in M$. De même, le fait que $g \circ f = 0$ implique immédiatement que $g_M \circ f_M = 0$ vu que $g_M(f_M(x' \otimes y)) = g(f(x')) \otimes y$ pour tous $x' \in N', y \in M$. Ainsi, g_M se factorise par une application surjective

$$\tilde{g}_M : (N \otimes_A M)/f_M(N' \otimes_A M) \to N'' \otimes_A M$$

et il reste à montrer que $\tilde{g}_M$ est injective.

Pour tout $x'' \in N''$, notons $u(x'') \in N/f(N')$ son antécédent par l'isomorphisme $N/f(N') \to N''$ induit par g. Notons également $\bar{z}$ la classe dans $(N \otimes_A M)/f_M(N' \otimes_A M)$ d'un élément z de $N \otimes_A M$. On définit alors une application A-linéaire $\theta : N'' \otimes_A M \to (N \otimes_A M)/f_M(N' \otimes_A M)$ vérifiant

$$\theta(x'' \otimes y) = \overline{u(x'') \otimes y}$$

pour tous $x'' \in N'', y \in M$, ce qui est possible via la propriété universelle du produit tensoriel (noter que $u(x'') \otimes y$ est bien défini modulo $f_M(N' \otimes_A M)$ car $u(x'')$ est défini modulo $f(N')$). Si $x \in N$, on a $u(g(x)) = x$ dans $N/f(N')$ car x est un antécédent de $g(x)$ par g. Par construction, on a alors pour tous $x \in N, y \in M$:

$$(\theta \circ \tilde{g}_M)(\overline{x \otimes y}) = \theta(g(x) \otimes y) = \overline{u(g(x)) \otimes y} = \overline{x \otimes y},$$

ce qui montre que $\theta \circ \tilde{g}_M$ est l'identité de $(N \otimes_A M)/f_M(N' \otimes_A M)$. En particulier $\tilde{g}_M$ est bien injective.

□

Exemple 2.19 a) Si $f : A^r \to A^s$ est une application A-linéaire surjective, alors pour toute A-algèbre B, le B-morphisme $B^r \to B^s$ induit en tensorisant par B est surjectif. En prenant $B = A/I$, où I est un idéal maximal, on retrouve la première preuve du théorème 1.16.

Définition 2.20 On dit qu'un A-module M est *plat* si pour toute application linéaire injective $u : N' \to N$, l'application $N' \otimes_A M \to N \otimes_A M$ induite par u reste injective.

D'après le théorème 2.18, M est plat si et seulement si tensoriser par M transforme toute suite exacte courte en suite exacte courte (ce qu'on traduit par "le foncteur $\otimes_A M$ est exact").

Exemple 2.21 a) Tout module libre est plat. En effet, cela résulte du fait qu'un tel module est isomorphe à $\bigoplus_I A$ (pour un certain ensemble I), qui tensorisé avec un A-module N donne $\bigoplus_I N$. En particulier, si K est un corps, tout K-module (=K-espace vectoriel) est plat.

b) Si A est un anneau intègre, un A-module plat M est nécessairement *sans torsion*, i.e. la propriété $ax = 0$ avec $a \in A$ et $x \in M$ implique $a = 0$ ou $x = 0$. En effet, si $a \neq 0$, la multiplication par a est une application linéaire injective de A dans A, qui doit le rester après tensorisation par M, ce qui signifie que la multiplication par a est injective dans M.

c) Réciproquement, un A-module sans torsion est plat si A est un anneau principal (voir TD), mais pas en général. En fait, si A est un anneau noethérien, un A-module M de type fini est plat si et seulement s'il est *projectif* (cela signifie qu'il existe un A-module N tel que $M \oplus N$ soit libre).

Définition 2.22 Un homomorphisme $f : A \to B$ d'anneaux commutatifs est plat s'il fait de B un A-module plat.

Proposition 2.23 *a) Le composé de deux homomorphismes plats est plat.*

b) Si M est un A-module plat et B est une A-algèbre, alors $M \otimes_A B$ est un B-module plat.

Démonstration : a) Soient $A \to B$ et $B \to C$ des homomorphismes plats. Soit $N' \hookrightarrow N$ un morphisme injectif de A-modules. Alors $N' \otimes_A B \to N \otimes_A B$ est injectif (parce que B est plat sur A), d'où (comme C est plat sur B) l'injectivité de

$$(N' \otimes_A B) \otimes_B C = N' \otimes_A C \to (N \otimes_A B) \otimes_B C = N \otimes_A C$$

via la proposition 2.13. Ainsi, C est plat sur A.

b) Soit $N' \hookrightarrow N$ un morphisme injectif de B-modules. Alors l'application

$$N' \otimes_B (M \otimes_A B) \to N \otimes_B (M \otimes_A B)$$

s'identifie (via loc. cit. et la commutativité du produit tensoriel) à

$$N' \otimes_A M \to N \otimes_A M,$$

qui est bien injective par platitude du A-module M.

□

Définition 2.24 Un A-module M est *fidèlement plat* s'il est plat et si de plus la propriété $M \otimes_A N = 0$ (où N est un A-module) implique $N = 0$. Un homomorphisme d'anneaux $A \to B$ est fidèlement plat s'il fait de B un A-module fidèlement plat.

Par exemple, un A-module libre non nul est fidèlement plat. On peut montrer que si M est fidèlement plat, alors une suite de A-modules est exacte si et seulement s'il reste exacte après tensorisation par M. Par ailleurs, un homomorphisme d'anneaux $f : A \to B$ est fidèlement plat si et seulement s'il est plat et pour tout idéal premier $\wp$ de A, il existe un idéal premier I de B tel que $f^{-1}(I) = \wp$. Voir [4], chapitre 2, §4.

3. Modules sur un anneau principal

3.1. Les grands théorèmes

Dans tout ce paragraphe, A désigne un anneau principal. Le premier résultat raffine considérablement le théorème 1.19 dans ce cadre.

Theorème 3.1 *Soit A un anneau principal. Alors tout sous-module N de A^n est libre et de rang fini $m \leq n$.*

Remarque 3.2 Comme A est noethérien, on sait déjà que N est de type fini. Si on savait que N était libre, le fait que son rang soit au plus n résulte du corollaire 1.24, mais c'est bien la liberté de N qui est le point difficile, et qui ne marche pas dès que A n'est pas principal.

Démonstration : On procède par récurrence sur n. Pour $n = 1$, c'est la définition d'un anneau principal. Supposons donc le résultat vrai pour tous les entiers $< n$. Soit N un sous-module de A^n, posons $M_1 = Ae_2 \oplus ... \oplus Ae_n$, où $(e_1, ..., e_n)$ est la base canonique de A^n. Autrement dit, M_1 est le sous-module de A^n constitué des éléments de la forme $(0, ..., ...)$. Si $N \subset M_1$, c'est fini par hypothèse de récurrence car M_1 est isomorphe à A^{n-1}. On suppose donc désormais $N \not\subset M_1$. Par hypothèse de récurrence, $(N \cap M_1)$ possède une base $(f_2, ..., f_m)$ avec $m \leq n$. La difficulté est maintenant de trouver un élément de N pour compléter cette base en une base de N.

Posons $I = p(N)$ où $p : N \to A$ est la projection $A^n \to A$ sur la première coordonnée. Comme p est A-linéaire, on a que I est un idéal de A, et cet idéal n'est pas nul car N contient un élément qui n'est pas dans M_1. Comme A est principal, on peut écrire $I = (d)$ avec $d \neq 0$ dans A. Par définition de I, on a alors un élément $f_1 = de_1 + y_1$ dans N avec $y_1 \in M_1$. Notons que $f_1 \neq 0$, sinon d serait nul vu que $A^n = Ae_1 \oplus M_1$. Nous allons montrer que $(f_1, ..., f_m)$ est une base de N.

Montrons d'abord que $(f_1, ..., f_m)$ engendre N. Si $x \in N$, on a $x = be_1 + y$ avec $b \in A$ et $y \in M_1$. Mais alors $b \in I$ d'où $b = ad$ avec $a \in A$. Ceci donne

$x = af_1 + (y - ay_1)$, donc $(x - af_1)$ est dans $N \cap M_1$, ce qui permet de le décomposer sur la base $(f_2, ..., f_m)$ de $N \cap M_1$. Ainsi $x = af_1 + x'$ avec $x' \in Af_2 + ... + Af_m$, ce qui montre que $(f_1, ..., f_m)$ engendre N.

Montrons enfin que $(f_1, ..., f_m)$ est libre. Pour cela il suffit de montrer que (f_1) est libre et qu'on a $Af_1 \cap (N \cap M_1) = \{0\}$, car $(f_2, ..., f_m)$ est déjà libre par hypothèse. Le premier point est évident en décomposant f_1 (qui est non nul) sur la base canonique de A^n et en utilisant l'intégrité de A. D'autre part si λf_1 est dans M_1 avec $\lambda \in A$, alors $\lambda d e_1 + \lambda y_1 \in M_1$, d'où $(\lambda d)e_1 \in M_1$ mais par définition de M_1 et de la base canonique de A^n, ceci implique $\lambda d = 0$ donc $\lambda = 0$ par intégrité de A.

□

Pour aller plus loin dans la classification des modules sur un anneau principal, il faut connaître le résultat plus précis suivant. C'est sans doute le théorème le plus important de toute la théorie.

Theorème 3.3 ("Base adaptée") *Soient A un anneau principal, M un A-module libre de rang n et N un sous-module de M. Alors il existe une base $(e_1, ..., e_n)$ de M et des éléments $(d_1, ..., d_r)$ de A (avec $r \leq n$) tels que :*

1. *$(d_1e_1, ..., d_re_r)$ soit une base de N.*
2. *on ait les divisibilités : $d_1 \mid d_2 \mid ... \mid d_r$.*

En particulier les d_i sont non nuls, et on peut remplacer chaque d_i par n'importe quel élément de A qui lui est associé. Notons qu'on savait déjà que N était libre de rang $\leq n$ via le théorème 3.1.

La preuve du théorème de la base adaptée est longue et assez compliquée. On commence par un lemme qui initialise un raisonnement par récurrence sur n.

Lemme 3.4 *On suppose $N \neq \{0\}$. Alors il existe une application linéaire $f_1 : M \to A$ telle que*

1. *$f_1(N)$ soit maximal (pour l'inclusion) parmi les $f(N)$ avec $f : M \to A$ linéaire.*
2. *Si on pose $f_1(N) = (d_1)$ et qu'on choisit $u_1 \in N$ tel que $f_1(u_1) = d_1$, alors il existe $e_1 \in M$ tel que $u_1 = d_1e_1$ et $f_1(e_1) = 1$.*

Démonstration : Fixons une base $(\varepsilon_1, ..., \varepsilon_n)$ de M (qui n'a aucune raison d'être adaptée pour N). On dispose alors (pour $1 \leq i \leq n$) de la forme linéaire $\varepsilon_i^* : M \to A$ qui associe à tout $x \in M$ sa i-ième coordonnée dans cette base. Pour toute forme linéaire $f : M \to A$, $f(N)$ est un idéal de A. Le premier

point résulte alors de ce que A est principal, (donc noethérien), ce qui permet aussi d'écrire $f_1(N) = (d_1)$, avec d_1 non nul car N est non nul, donc l'une des formes linéaires ε_i^* a une restriction non nulle à N.

Soit alors $u_1 \in N$ tel que $f_1(u_1) = d_1$. L'ensemble de tous les $f(u_1)$ pour $f : M \to A$ forme linéaire est un idéal de l'anneau principal A, qui est donc engendré par un élément d. En particulier d divise d_1, mais comme il existe une forme linéaire f avec $f(u_1) = d$, on a $f(N) \supset (d) \supset (d_1) = f_1(N)$, donc par maximalité de $f_1(N)$ ceci implique $(d) = (d_1)$, et finalement d_1 divise $f(u_1)$ pour toute forme linéaire $f : M \to A$. Ceci s'applique en particulier aux formes linéaires ε_i^*, ce qui montre que toutes les coordonnées de u_1 dans la base $(\varepsilon_1, ..., \varepsilon_n)$ sont divisibles par d_1. On peut donc trouver $e_1 \in M$ tel que $u_1 = d_1 e_1$. Alors $f_1(e_1) = 1$ vu que $f_1(u_1) = d_1 \neq 0$ et A est intègre.

□

Remarque 3.5 Une difficulté est que pour l'instant, on sait juste que $f_1(N)$ est maximal parmi les $f(N)$, et pas que c'est un plus grand élément (ce sera prouvé dans le lemme 3.6 ci-dessous), ce qui a compliqué la preuve de l'existence de e_1. Noter aussi que l'ensemble des $f(x)$, pour f forme linéaire sur M et $x \in N$, n'est pas a priori un idéal de A, d'où la nécessité de procéder en deux temps en construisant d'abord u_1 puis en considérant les $f(u_1)$.

On a ensuite :

Lemme 3.6 *Avec les hypothèses et notations du lemme précédent, on a :*

1. $M = Ae_1 \oplus \ker f_1$ *et* $N = Au_1 \oplus (\ker f_1 \cap N)$.
2. *Pour toute forme linéaire* $f : M \to A$, *on a* $f(N) \subset d_1 A$.

Démonstration : 1. Comme $f_1(e_1) = 1$, $Ae_1 \cap \ker f_1 = \{0\}$ est clair. Tout x de M s'écrit $x = f_1(x)e_1 + (x - f_1(x)e_1)$ avec $(x - f_1(x)e_1) \in \ker f_1$ donc $M = Ae_1 \oplus \ker f_1$. De même tout x de N vérifie $f_1(x) = ad_1$ avec $a \in A$, d'où $x = au_1 + (x - au_1)$ avec $(x - au_1) \in (\ker f_1 \cap N)$ vu que $f_1(u_1) = d_1$. Enfin $Au_1 \cap \ker f_1 = \{0\}$ résulte de $f_1(u_1) = d_1 \neq 0$, et A intègre.

2. Soit $f : M \to A$ linéaire. Via 1., on définit $g : M \to A$ linéaire par : $g(x) = f(x)$ si $x \in \ker f_1$, et $g(e_1) = 1$. Alors comme $g(u_1) = d_1$, on a $g(N) \supset d_1 A$, donc $g(N) = d_1 A$ par maximalité de $f_1(N) = d_1 A$. En particulier la restriction de f à $(\ker f_1 \cap N)$ a son image incluse dans $d_1 A$, donc celle de f à N aussi puisque N est la somme de $(\ker f_1 \cap N)$ et de Au_1, tandis que $f(u_1) = d_1 f(e_1)$ est divisible par d_1.

□

Fin de la preuve du théorème de la base adaptée : Les cas $n = 0$ et $N = 0$ sont triviaux. Pour $n = 1$, on peut supposer $M = A$ et le résultat vient de la définition d'un anneau principal en prenant $e_1 = 1$ et d_1 un générateur de l'idéal $N \subset A$ (noter que (d_1) est bien alors une base de N par intégrité de A). Supposons le résultat vrai pour les entiers $< n$. On applique alors le lemme 3.6, et l'hypothèse de récurrence au A-module $\ker f_1$ (qui est libre par le théorème 3.1, puis de rang $n-1$ par le corollaire 1.17 et l'égalité $M = Ae_1 \oplus \ker f_1$, vu que le rang de Ae_1 est 1) et à son sous-module ($\ker f_1 \cap N$). On obtient une base $(e_2, ..., e_n)$ de $\ker f_1$, et des éléments $d_2, ..., d_r$ de A avec $r \leq n$ et $d_2 \mid ... \mid d_r$ tels que $M = Ae_1 \oplus ... \oplus Ae_n$ et $N = A(d_1e_1) \oplus ... \oplus A(d_re_r)$. Enfin d_1 divise d_2 en appliquant le lemme 3.6 à la forme linéaire "deuxième coordonnée" (dans la base $(e_1, ..., e_n)$) sur M.

□

Attention aux erreurs habituelles : le théorème de la base adaptée ne dit pas que N admet un supplémentaire, ni qu'on peut compléter une base de N en une base de M (prendre simplement $A = \mathbf{Z}$, $M = \mathbf{Z}$, $N = 2\mathbf{Z}$).

Theorème 3.7 *Soit M un module de type fini sur A principal. Alors il existe $d_1, ..., d_s$ dans A, non nuls et non inversibles, tels que M soit isomorphe à*

$$A^m \oplus \bigoplus_{i=1}^{s} (A/d_iA)$$

avec $m \in \mathbf{N}$ et $d_1 \mid d_2 \mid ... \mid d_s$.

Comme d'habitude, on convient que $A^0 = \{0\}$, et que si $s = 0$, la somme vide $\bigoplus_{i=1}^{s}(A/d_iA)$ est également nulle. Noter aussi que $M \otimes_A K$ est isomorphe à K^m, où $K := \operatorname{Frac} A$, i.e. m apparaît comme la dimension du K-ev $M \otimes_A K$.

Démonstration : Comme M est de type fini, il est engendré par n éléments, d'où une suite exacte de A-modules

$$0 \to N \to A^n \xrightarrow{p} M \to 0$$

(cela signifie simplement que M est isomorphe à un quotient de A^n).

On applique alors le théorème de la base adaptée au sous-module N du A-module libre A^n. On obtient

$$A^n = \bigoplus_{i=1}^{n} Aei$$

$$N = \bigoplus_{i=1}^{r} A(d_i e_i)$$

Soit alors z_i l'image de e_i dans M (par p). Alors $M = \bigoplus_{i=1}^{n} Az_i$: en effet d'une part les z_i engendrent M (par surjectivité de p), d'autre part si $\sum_{i=1}^{n} \lambda_i z_i = 0$ avec $\lambda_i \in A$, alors $\sum_{i=1}^{n} \lambda_i e_i \in N$ donc chaque λ_i est multiple de d_i pour $1 \leq i \leq r$ (resp. est nul pour $r < i \leq n$) puisque $(d_i e_i)_{1 \leq i \leq r}$ est une base de N ; ainsi chaque $\lambda_i e_i$ est dans N, i.e. $\lambda_i z_i = 0$. On obtient aussi que le noyau de la surjection $\lambda \mapsto \lambda z_i$ de A dans $A.z_i$ est $d_i A$ pour $1 \leq i \leq r$ et 0 pour $r < i \leq n$, ce qui montre que chaque $A.z_i$ est isomorphe à $(A/d_i A)$ pour $1 \leq i \leq r$ et à A pour $r < i \leq n$. On obtient finalement $M \simeq A^{n-r} \oplus \bigoplus_{i=1}^{r} (A/d_i A)$, mais pour d_i inversible on a $A/d_i A = 0$, donc on peut ne garder que les d_i non inversibles.

□

Définition 3.8 Soit M un module sur un anneau commutatif A. On rappelle que M est dit *sans torsion* si la condition $ax = 0$ (avec $a \in A$, $x \in M$) implique $a = 0$ ou $x = 0$. On dit que M est *de torsion* si pour tout x de M, il existe a non nul dans A tel que $ax = 0$.

Attention, "sans torsion" n'est pas en général le contraire de "de torsion". Par exemple $\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ n'est ni sans torsion, ni de torsion en tant que $\mathbf{Z}$-module. De manière évidente un module libre sur un anneau intègre est sans torsion. On peut maintenant démontrer une réciproque pour un anneau principal :

Corollaire 3.9 *Soit M un module de type fini sur A principal. Alors M est libre si et seulement s'il est sans torsion.*

Démonstration : Cela résulte immédiatement du théorème 3.7, car la condition que M est sans torsion implique que $s = 0$ (pour d non inversible, A/dA est non nul, et tout élément de A/dA est annulé par d).

□

Ce dernier corollaire est très spécifique aux anneaux principaux. Si A est intègre noethérien, tout idéal I de A est un A-module de type fini et sans torsion, mais d'après le corollaire 1.24, I n'est pas libre dès qu'il n'est pas principal. De plus, l'hypothèse de type fini est importante car par exemple $\mathbf{Q}$ est un $\mathbf{Z}$-module sans torsion et on a déjà vu qu'il n'était pas libre (exemple 1.15).

Remarque 3.10 Rappelons qu'un A-module (de type fini) M est dit projectif s'il est *facteur direct* d'un module libre, i.e. s'il existe un A-module N

tel que $M \oplus N$ soit libre. On a donc en particulier qu'un module projectif (de type fini) sur un anneau principal est toujours libre.[9] C'est également vrai pour tout anneau *local*, c'est-à-dire qui n'a qu'un idéal maximal, et pour $K[X_1, ...X_n]$ quand K est un corps (théorème de Quillen-Suslin, 1976, *quondam* conjecture de Serre).

3.2. Décomposition p-primaire

Pour finir la classification des modules de type fini sur un anneau principal A, on a besoin d'assertions d'unicité. De manière un peu surprenante, il n'est pas évident de prouver un tel résultat directement à partir du théorème 3.7 ; il est nettement plus commode d'introduire la notion de *composantes p-primaires*, qui est par ailleurs utile.

Définition 3.11 Soit p un irréductible de A. On dit qu'un A-module est *p-primaire* s'il est isomorphe à un module du type $\bigoplus_{i=1}^{s}(A/p^{v_i}A)$ avec $v_i \in \mathbf{N}^*$ pour tout $i \in [1, s]$.

En particulier un A-module p-primaire est de type fini et de torsion (avec les notations ci-dessus, tout élément x d'un A-module p-primaire est annulé par $p^{\max(v_i)}$).

Pour tout d non nul dans l'anneau principal A, on note comme d'habitude $v_p(d)$ la plus grande puissance de l'irréductible p qui divise d.

Proposition 3.12 *a) Soit $d = u\prod_{p\in S} p^{\alpha_p}$ une décomposition de d (où S est un ensemble fini d'irréductibles deux à deux non associés et $u \in A^*$). Alors*

$$A/dA \simeq \bigoplus_{p\in S}(A/p^{\alpha_p}A).$$

b) Soit M un A-module de type fini et de torsion. Alors

$$M = \bigoplus_{p\in S} M_p$$

où M_p est un module p-primaire et S un ensemble fini d'irréductibles deux à deux non associés. De plus, on a $M_p = M/p^kM$ pour k assez grand.

On dit que les M_p sont les *composantes p-primaires* de M.

9. L'hypothèse de finitude n'est pas indispensable, mais la preuve est nettement plus compliquée sans ; voir l'article de Kaplansky dans *Ann. Math.* **68** (1958).

Démonstration : a) C'est le classique lemme chinois quand $A = \mathbf{Z}$. En raisonnant par récurrence sur le cardinal de S, il suffit de démontrer que $A/(d_1d_2)A \simeq A/d_1A \times A/d_2A$ quand d_1, d_2 sont deux éléments de A premiers entre eux. Or l'application qui à $a \in A$ associe (a_1, a_2), où a_i est la classe de a dans A/d_iA pour $i = 1, 2$, a clairement pour noyau $(d_1d_2)A$ car d_1 et d_2 sont premiers entre eux. Elle est surjective via Bezout : soient en effet $b, c \in A$, il existe $\alpha, \beta \in A$ tels que $\alpha d_1 + \beta d_2 = 1$, alors $x := \beta b d_2 + \alpha c d_1$ a même classe que b dans A/d_1A et que c dans A/d_2A.

b) Le théorème 3.7 et le a) permettent de décomposer M sous la forme $M = \bigoplus_{p \in S} M_p$ avec M_p module p-primaire, puisque M est somme directe d'un nombre fini de modules de la forme A/dA. Soit maintenant p et q deux irréductibles distincts de S (non associés donc). Alors la multiplication par p est bijective dans A/q^mA pour tout $m \in \mathbf{N}$, car la classe de p est un inversible de l'anneau A/q^mA via une identité de Bezout pour q^m et p (qui sont premiers entre eux). Du coup, la multiplication par p est bijective dans M_q, ce qui montre que $M_q/p^kM_q = 0$ pour tout $k \in \mathbf{N}$. Ainsi, $M/p^kM = M_p/p^kM_p$, qui vaut aussi M_p dès que k est plus grand que tous les α_i, où on a écrit $M_p = \bigoplus_{i=1}^{s}(A/p^{\alpha_i}A)$.

□

On va en déduire le résultat d'unicité annoncé :

Theorème 3.13 *Soit M un module de type fini sur A principal. Écrivons*

$$M \simeq A^m \oplus \bigoplus_{i=1}^{s}(A/d_iA)$$

avec $d_1, ..., d_s$ non nuls et non inversibles tels que $d_1 \mid ... \mid d_s$. Alors m, s, et les d_i à association près ne dépendent que de M.

En d'autres termes si on a une autre décomposition

$$M \simeq A^{m'} \oplus \bigoplus_{i=1}^{s'}(A/d'_iA)$$

alors $m = m'$, $s = s'$, et d'_i est associé à d_i pour tout i.

Démonstration : Soit M_{tors} le *sous-module de torsion* de M, c'est-à-dire l'ensemble des x de M tels qu'il existe $a \neq 0$ dans A avec $ax = 0$. Alors $M_{\text{tors}} \simeq \bigoplus_{i=1}^{s}(A/d_iA)$ et $M/M_{\text{tors}} \simeq A^m$. Par invariance du rang d'un module libre de type fini, m ne dépend que de M et on se ramène à M de

torsion (on pouvait aussi noter que r est la dimension du K-espace vectoriel $M \otimes_A K$, où $K = \mathrm{Frac}\, A$).

Il suffit alors de montrer que pour tout irréductible p, la suite des $v_p(d_i)$ est bien déterminée. Comme un A-module de torsion M est la somme directe de ses composantes p-primaires $M_p = \bigoplus_{i=1}^{s}(A/p^{v_p(d_i)}A)$, qui sont caractérisées par $M_p = M/p^kM$ pour k assez grand, on est ramené au cas où M est p-primaire.

Supposons donc $M = \bigoplus_{i=1}^{s}(A/p^{\alpha_i}A)$, où (α_i) est une suite croissante d'entiers strictement positifs. Comme A est principal et p irréductible, A/pA est un corps et d'autre part pour tout $k \in \mathbf{N}$, le A-module de p-torsion $p^kM/p^{k+1}M$ est muni canoniquement d'une structure de A/pA-espace vectoriel (comme dans l'exemple 1.4, c). On remarque que si $M_i := (A/p^{\alpha_i}A)$, on a pour tout entier k : $p^kM_i/p^{k+1}M_i = 0$ si $k \geq \alpha_i$ (puisqu'alors $p^kM_i \subset p^{\alpha_i}M_i = 0$) ; mais si $k < \alpha_i$, alors $p^kA \supset p^{k+1}A \supset p^{\alpha_i}A$, d'où

$$p^kM_i/p^{k+1}M_i = (p^kA/p^{\alpha_i}A)/(p^{k+1}A/p^{\alpha_i}A) \simeq p^kA/p^{k+1}A.$$

Or A/p est isomorphe à $p^kA/p^{k+1}A$ via $\bar{a} \mapsto p^k\bar{a}$, donc finalement on obtient que $p^kM_i/p^{k+1}M_i \simeq A/pA$ si $k < \alpha_i$. En particulier pour tout $k \in \mathbf{N}$, le nombre de $\alpha_i > k$ n'est autre que la *dimension du A/pA-espace vectoriel* $p^kM/p^{k+1}M \simeq \bigoplus_{i=1}^{s} p^kM_i/p^{k+1}M_i$, soit $\sum_{\alpha_i > k} 1$. Ainsi ce nombre ne dépend que de M, et donc la suite finie croissante d'entiers (α_i) aussi.

□

Le cas $A = \mathbf{Z}$ des théorèmes 3.7 et 3.13 donne le classique théorème de structure des groupes abéliens de type fini :

Theorème 3.14 *Soit M un groupe abélien engendré par une partie finie. Alors M est isomorphe à $\mathbf{Z}^m \times \prod_{i=1}^{s} \mathbf{Z}/d_i\mathbf{Z}$, où $m \in \mathbf{N}$ et les d_i sont des entiers ≥ 2 vérifiant $d_1|d_2|...|d_s$. De plus cette décomposition est unique.*

Notons que dans ce cas, M est fini si et seulement si $m = 0$, et on obtient le p-Sylow M_p de M via la décomposition p-primaire.

Nous allons maintenant présenter deux autres applications de la théorie des modules sur les anneaux principaux.

3.3. Équivalence de matrices à coefficients dans un anneau principal

Soit A un anneau commutatif. On note $\mathrm{GL}_n(A)$ le groupe des inversibles de l'anneau (non commutatif si $n \geq 2$) $M_n(A)$. D'après l'identité de

la comatrice, il s'agit simplement des matrices de $M_n(A)$ dont le déterminant est inversible dans A, l'inverse d'une telle matrice M étant donné par $M^{-1} = (\det M)^{-1}.\widetilde{M}$ (réciproquement, s'il existe une matrice $N \in M_n(A)$ avec $MN = I_n$, alors $(\det M).(\det N) = 1$ donc $\det M$ est inversible).

Définition 3.15 Soient p et q deux entiers > 0. On dit que deux matrices B, C de $M_{p,q}(A)$ sont *équivalentes* s'il existe $U \in \mathrm{GL}_p(A)$ et $V \in \mathrm{GL}_q(A)$ telles que $C = UBV$. Il revient au même de dire qu'il existe des bases respectives $\mathcal{B}$, $\mathcal{B}'$ de A^q, A^p telles que si u désigne l'application linéaire représentée par B dans les bases canoniques de A^q, A^p, on ait : $\mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(u) = C$.

Quand A est un corps, on retrouve la définition classique (qu'on prendra garde de ne pas confondre avec la relation plus fine de similitude si $p = q$). Le théorème suivant décrit les classes d'équivalence pour la relation définie ci-dessus quand A est principal.

Theorème 3.16 *Soit A un anneau principal. Alors :*

1. *Toute matrice B de $M_{p,q}(A)$ est équivalente à une matrice-bloc de la forme*
$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$
où $D = \mathrm{Diag}(d_1, ..., d_r)$, $r \leq \min(p, q)$, et $d_1, ..., d_r$ sont des éléments non nuls de A vérifiant $d_1 \mid ... \mid d_r$.
2. *Deux matrices $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix}$ avec $D = \mathrm{Diag}(d_1, ..., d_r)$, $D' = \mathrm{Diag}(d'_1, ..., d'_{r'})$ de la forme ci-dessus sont équivalentes si et seulement si : $r = r'$ et pour tout i, d_i et d'_i sont associés. En d'autres termes, la suite $(d_1, ..., d_r)$ du 1. ne dépend (à association près) que de la classe d'équivalence de B.*

On dit que $d_1, ..., d_r$ sont les *facteurs invariants* de B, et on appelle parfois les quotients d_2/d_1,..., d_r/d_{r-1} ses *diviseurs élémentaires*. Notons que r n'est autre que le *rang* de B vue comme matrice de $M_{p,q}(K)$, où $K := \mathrm{Frac}\, A$.

Preuve de 1. Soit $u : A^q \to A^p$ l'application définie par B dans les bases canoniques. Il s'agit de trouver des base respectives $\mathcal{B}$, $\mathcal{B}'$ de A^q, A^p telles que la matrice de u dans ces bases ait la forme voulue. On applique le théorème de la base adaptée au sous-module $\mathrm{Im}\, u$ du module libre de type fini A^p. On obtient une base $(e_1, ..., e_p)$ de A^p et une suite $(d_1, ..., d_r)$ d'éléments de $A \setminus \{0\}$, avec $d_1 \mid ... \mid d_r$, telle que $(d_1 e_1, ...d_r e_r)$ soit une base de $\mathrm{Im}\, u$. On

choisit alors $\varepsilon_1, ..., \varepsilon_r$ dans A^q tels que $u(\varepsilon_i) = d_i e_i$ pour $i = 1, ..., r$. Alors $(u(\varepsilon_1), ..., u(\varepsilon_r))$ est libre, donc a fortiori $(\varepsilon_1, ..., \varepsilon_r)$ est libre. D'autre part on a

$$A^q = \ker u \oplus \bigoplus_{i=1}^{r} A\varepsilon_i$$

car $(u(\varepsilon_1), ..., u(\varepsilon_r))$ est libre (ce qui donne $\ker u \cap \bigoplus_{i=1}^{r} A\varepsilon_i = \{0\}$), et tout élément x de A^q vérifie : $u(x)$ est combinaison linéaire des $d_i e_i = u(\varepsilon_i)$, donc x s'écrit comme somme d'un élément de $\ker u$ et d'une combinaison linéaire des ε_i. On peut alors (grâce aux théorèmes 3.1 et 1.17) prendre une base $(\varepsilon_{r+1}, ..., \varepsilon_q)$ de $\ker u$, et on obtient une base $\mathcal{B} = (\varepsilon_1, ..., \varepsilon_q)$ de A^q. Il suffit alors de prendre $\mathcal{B}' = (e_1, ..., e_p)$ pour obtenir la forme voulue.

□

Remarque 3.17 Notons que si B est la matrice d'une injection u de A^q dans A^p, les d_i qui lui sont associés apparaissent comme ceux donnés par le théorème de la base adaptée pour le sous-module $\operatorname{Im} u \simeq A^q$ de A^p. Ceux qui sont non inversibles sont donc aussi ceux qui apparaissent dans la structure du A-module $A^p/\operatorname{Im} u$.

Preuve de 2. L'étape essentielle consiste à démontrer le lemme suivant :

Lemme 3.18 *Pour toute matrice B de $M_{p.q}(A)$ et tout entier s (inférieur ou égal à $\min(p, q)$, ou encore au rang r de B), on note $m_s(B)$ le pgcd des mineurs de taille s de B. Alors :*

a) Si B et C sont équivalentes, $m_s(B)$ et $m_s(C)$ sont associés.

b) Si $B = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ avec $D = \operatorname{Diag}(d_1, ..., d_r)$ et $d_1 \mid ... \mid d_r$, alors :

$$m_s(B) = d_1 ... d_s$$

pour tout $s \in \{1, ..., r\}$.

Démonstration : a) Il suffit de remarquer que si $U \in M_p(A)$, alors les lignes de UB sont combinaisons linéaires des lignes de B et si $V \in M_q(A)$, les colonnes de BV sont combinaisons linéaires des colonnes de B. On en déduit (avec le théorème 1.12, b) que tout mineur de taille s de UBV est combinaison linéaire à coefficient dans A de mineurs de taille s de B, ce qui implique que $m_s(B)$ divise $m_s(UBV)$. Par symétrie, $m_s(B)$ et $m_s(C)$ sont associés si B et C sont équivalentes.

b) Quand B a cette forme particulière, tout mineur m de taille s est somme de termes nuls et de produits $e_1 ... e_s$, où les e_i sont deux à deux

distincts dans l'ensemble $\{d_1, ..., d_r\}$. D'après la propriété de divisibilité des d_i, $e_1...e_s$ est divisible par $d_1...d_s$. Comme d'autre part le mineur principal d'ordre s de B est $d_1...d_s$, on obtient le résultat voulu.

□

Fin de la preuve du théorème 3.16, 2. : On a déjà $r = r'$ par invariance du rang de deux matrices équivalentes. D'après le lemme 3.18, a), on a $m_s(D) = m_s(D')$ (à association près), d'où avec le b) de ce même lemme :

$$d_1...d_s = d'_1...d'_s$$

pour tout s avec $1 \leq s \leq r$. Par récurrence sur s, on voit alors que $d_s = d'_s$ (à association près) pour tout s de $[1, r]$.

□

Remarque 3.19 Il est beaucoup plus difficile de déterminer les classes de *similitude* des matrices de $M_n(A)$. En fait on ne sait le faire que quand A est un corps, car comme on va maintenant le voir, ceci est lié à la classification des modules sur l'anneau $A[X]$, qui n'est pas principal si A n'est pas un corps.

3.4. Réduction des endomorphismes d'un K-espace vectoriel de dimension finie

Soient K un corps, E un K-espace vectoriel de dimension finie n, et u un endomorphisme de E. On cherche à trouver une base dans laquelle la matrice de u a une forme agréable, et plus précisément à déterminer les classes de similitude dans $M_n(K)$. C'est l'objet du théorème principal de cet alinéa. On commence par rappeler une notation :

Définition 3.20 Soit $P = X^d + \sum_{i=0}^{d-1} a_i X^i$ un polynôme unitaire à coefficients dans K. On note $C(P)$ la matrice

$$\begin{pmatrix} 0 & ... & ... & ... & -a_0 \\ 1 & 0 & ... & ... & -a_1 \\ 0 & 1 & 0 & ... & -a_2 \\ ... & ... & ... & ... & ... \\ 0 & ... & ... & 1 & -a_{d-1} \end{pmatrix}$$

qu'on appelle *matrice compagnon* associée à P.

Si u est l'endomorphisme associé à $C(P)$ dans une base $\mathcal{B}$ et x est le premier vecteur de cette base, alors $\mathcal{B} = (x, u(x), ..., u^{d-1}(x))$. En particulier un polynôme annulateur non nul de u est de degré au moins d, et comme $P(u) = 0$ (vu que $u^d(x) = -\sum_{k=0}^{d-1} a_k u^k(x)$, et de même en composant plusieurs fois avec u, ce qui montre que $P(u)$ s'annule sur la base $\mathcal{B}$), le polynôme minimal de $C(P)$ est P. D'après le théorème de Cayley-Hamilton, c'est aussi son polynôme caractéristique (on peut également le vérifier directement par un calcul du déterminant). Un tel endomorphisme u est dit *cyclique*.

Theorème 3.21 *1. Pour tout endomorphisme u d'un K-espace vectoriel de dimension finie E, il existe une base de E dans laquelle la matrice de u est diagonale par blocs, de la forme (dite "décomposition de Frobenius")*

$$\begin{pmatrix} C(P_1) & & & \\ & C(P_2) & & \\ ... & & & \\ & & & C(P_s) \end{pmatrix}$$

où les P_i sont des polynômes unitaires de $K[X]$ de degré au moins 1, vérifiant : $P_1 \mid P_2 \mid ... \mid P_s$.

2. Les P_i sont entièrement déterminés par u ; on les appelle les invariants de similitude de u (ou encore d'une matrice représentant u dans une base). Deux matrices de $M_n(K)$ sont semblables si et seulement si elles ont les mêmes invariants de similitude.

3. Soient $B \in M_n(K)$ et $C := XI_n - B$ la matrice caractéristique de B (c'est une matrice de rang n de $M_n(K[X])$). Alors la suite des facteurs invariants de C est $(1, ..., 1, P_1, ..., P_s)$, où $P_1, ..., P_s$ sont les invariants de similitude de B. En particulier ces invariants sont donnés par la formule :

$$P_1 ... P_h = m_{h+n-s}(C)$$

pour $h = 1, ..., s$, où $m_i(C)$ désigne le pgcd des mineurs d'ordre i de C dans $K[X]$. [10]

Notons que le polynôme minimal de u est P_s (attention, c'est le "plus grand" P_i, pas le plus petit !) et le polynôme caractéristique de u est $P_1 ... P_s$. On peut calculer les P_i successivement en commençant par P_s, avec les formules $P_s = m_n(C)/m_{n-1}(C)$, $P_{s-1} = m_{n-1}(C)/m_{n-2}(C)$ etc.

La preuve de ce théorème repose sur la théorie des modules sur l'anneau principal $A := K[X]$. Plus précisément on définit une structure de A-module

10. Attention au décalage d'indices, dû aux facteurs invariants inversibles de C.

M sur le K-espace vectoriel E via : $P.v := P(u)(v)$ pour $P \in K[X]$ et $v \in E$. Notons tout de suite que ce A-module est de torsion car si π est un polynôme annulateur non nul de u (par exemple son polynôme caractéristique), on a $\pi.v = 0$ pour tout v de M.

Preuve des points 1. et 2. du théorème 3.21 : Comme le A-module M est de torsion, il est isomorphe (d'après le théorème 3.7) à $\bigoplus_{i=1}^{s}(A/P_i.A)$, où les P_i sont des éléments de $A = K[X]$ non nuls et non inversibles, donc de degré au moins 1, qu'on peut choisir unitaires. Comme chaque $A/P_i.A$ est engendré par un élément (la classe de 1 modulo P_iA), cela signifie que $M = \bigoplus_{i=1}^{s} A.z_i$, où z_i est un vecteur de E dont l'annulateur dans A est l'idéal P_iA. Soit alors E_i le sous-module $A.z_i$ de M, alors E_i est en particulier un sous-espace vectoriel de E, et il est stable par u ; plus précisément c'est l'image de l'application K-linéaire $P \mapsto P.z_i = P(u)(z_i)$ de A dans M. Par définition, E_i est isomorphe à $A/P_i.A$, qui est un K-espace vectoriel de dimension $d_i := \deg P_i$ (une base est constituée des classes de $(1, X, ...X^{d_i-1})$, via la division euclidienne par P_i). Maintenant la famille $\mathcal{B}_i := (z_i, u(z_i), ...u^{d_i-1}(z_i))$, est une base du K-espace vectoriel E_i (elle est de cardinal d_i ; de plus elle est libre parce que l'annulateur de z_i est $P_i.A$). La matrice de la restriction de u à E_i dans $\mathcal{B}_i$ est $C(P_i)$ par définition de $C(P_i)$ et parce que $(P_i(u))(z_i) = 0$, Comme $E = \bigoplus_{i=1}^{s} E_i$ (comme A-module ou comme K-espace vectoriel), on en déduit le premier point en recollant les bases $\mathcal{B}_i$.

Si maintenant u a une matrice de la forme ci-dessus avec des polynômes $(Q_1, ..., Q_{s'})$ dans une autre base, alors le A-module M est la somme directe de sous-modules N_i, tel que chaque N_i corresponde à un endomorphisme $v = u_{|N_i}$ dont la matrice dans une certaine base $(y, u(y), ...u^{m-1}(y))$ est $C(Q_i)$, où $m = \deg Q_i$. Comme ci-dessus, le A-module N_i est isomorphe à $(A/Q_i.A)$ via l'application A-linéaire $w : P \mapsto P.y = P(u)(y)$ de A dans N_i, car le noyau de w est $Q_i.A$ via le fait que Q_i est le polynôme minimal de $C(Q_i)$, donc de v. Finalement le A-module M est isomorphe à $\bigoplus_i (A/Q_i.A)$. Le fait que les P_i soient entièrement déterminés par u vient alors du théorème d'unicité 3.13. D'où le deuxième point.

□

Pour démontrer le troisième point du théorème, fixons une base $(\varepsilon_1, ..., \varepsilon_n)$ du K-ev E, alors le A-module M est engendré par cette base puisque A contient toutes les constantes de K. Soit B la matrice de u dans la base $(\varepsilon_1, ..., \varepsilon_n)$. On note $(e_1, ..., e_n)$ la base canonique du A-module A^n, puis φ l'application A-linéaire surjective qui envoie chaque e_i sur ε_i. Soit ψ l'injection canonique de $\ker \varphi$ dans $K[X]^n$. D'après la remarque 3.17, le A-module $M \simeq (K[X]^n / \ker \varphi)$ est alors isomorphe à $\bigoplus_{i=1}^{s}(A/P_i.A)$, où la suite des facteurs

invariants de la matrice de ψ dans des bases de $\ker\varphi$ et $K[X]^n$ est de la forme $(1,...,1,P_1,...,P_s)$ avec $P_1 \mid ... \mid P_s$. On est donc ramené (via le lemme 3.18) pour conclure à trouver une base $(f_1,...,f_n)$ de $\ker\varphi$ telle que la matrice de ψ dans les bases $(f_1,...,f_n)$ et $(e_1,...,e_n)$ soit la matrice de déterminant non nul $C = XI_n - B$. Il suffit donc de démontrer le lemme suivant :

Lemme 3.22 *Posons* $B = (a_{ij})$ *et* $f_j = Xe_j - \sum_{i=1}^n a_{ij}e_i$ *pour* $j = 1,...,n$. *Alors* $(f_1,...,f_n)$ *est une base du* A*-module* $\ker\varphi$.

Démonstration : Déjà $f_j \in \ker\varphi$ vu que $\varphi(f_j) = X.\varepsilon_j - \sum_{i=1}^n a_{ij}\varepsilon_i = u(\varepsilon_j) - \sum_{i=1}^n a_{ij}\varepsilon_i = 0$ par définition de la matrice B.

Montrons que $(f_1,...,f_n)$ engendre le A-module $\ker\varphi$. Tout élément $\mathbf{Y}$ de $K[X]^n$ s'écrit $\mathbf{Y} = \sum_{j=1}^n \lambda_j e_j$ avec $\lambda_j \in K[X]$. On observe alors qu'on peut récrire $\mathbf{Y}$ sous la forme $\mathbf{Y} = \sum_{j=1}^n \mu_j f_j + \sum_{j=1}^n b_j e_j$ avec $\mu_j \in K[X]$ et b_j constante de K : en effet, par K-linéarité il suffit de le voir quand $\mathbf{Y} = X^k e_j$ avec $k \in \mathbf{N}$; or dans ce cas cela se déduit par récurrence sur k de l'égalité $f_j = Xe_j - \sum_{i=1}^n a_{ij}e_i$.

Si maintenant $\mathbf{Y}$ est de plus dans $\ker\varphi$, alors $\sum_{j=1}^n b_j e_j$ aussi, d'où l'égalité $\sum_{j=1}^n b_j\varepsilon_j = 0$ et finalement tous les b_j sont nuls parce que $(\varepsilon_1,...,\varepsilon_n)$ est une base du K-espace vectoriel E.

Montrons enfin que la famille $(f_1,...,f_n)$ est libre dans le A-module $\ker\varphi$. Si $\sum_{j=1}^n \lambda_j f_j = 0$ avec $\lambda_j \in A$, alors

$$\sum_{j=1}^n (\lambda_j X)e_j = \sum_{1\le i,j\le n} \lambda_j a_{ij} e_i = \sum_{j=1}^n (\sum_{i=1}^n a_{ji}\lambda_i)e_j$$

et comme $(e_1,...,e_n)$ est une base du A-module $K[X]^n$, on obtient pour tout $j = 1,...,n$: $X\lambda_j = \sum_{i=1}^n a_{ji}\lambda_i$, ce qui implique que tous les λ_j sont nuls, sinon on obtient une contradiction en prenant j tel que λ_j soit de degré maximal (disons d) parmi $\lambda_1,...,\lambda_n$, puisqu'alors $X\lambda_j$ est de degré $d+1$ et $\sum_{i=1}^n a_{ji}\lambda_i$ de degré au plus d.

□

Remarque 3.23 a) Dans le cas particulier où le polynôme caractéristique de u est scindé, on retrouve la réduction de Jordan comme la décomposition en composantes p-primaires de M, vu que les facteurs irréductibles de chaque P_i sont de la forme $(X-\lambda)$ avec $\lambda \in K$. En effet, la composante p-primaire associée à λ correspond à une matrice de la forme $\lambda I + N$ avec N nilpotente ; mais comme une matrice compagnon de la forme $C(X^k)$ n'est autre qu'une

matrice de Jordan [11], la réduction de Frobenius de N donne bien sa réduction de Jordan.

b) Le théorème 3.21 permet par exemple de voir immédiatement que si deux matrices de $M_n(K)$ sont semblables sur un surcorps de K, elles sont déjà semblables sur K, résultat qui n'est pas du tout évident (en particulier si K est fini). D'autres applications seront vues en TD.

Références

[1] R. Godement : Cours d'algèbre. Hermann, Paris, 1987.

[2] N. Jacobson : *Basic Algebra*. W. H. Freeman and Company, New York, 1985.

[3] Q. Liu : *Algebraic geometry and arithmetic curves*. Oxford Graduate Texts in Mathematics, **6**, Oxford Science Publications, Oxford University Press, Oxford, 2002.

[4] H. Matsumura : *Commutative Algebra*, Second edition, Mathematics Lecture Note Series **56**, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

11. A transposition près, mais il suffit d'écrire la base dans l'autre sens pour avoir la forme de Jordan classique.