Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

A. Ducros

Modules de type fini sur un anneau principal

Antoine Ducros

Préparation à l'agrégation de l'Université de Rennes 1
Année 2000-2001

Le but de ce texte est de donner une démonstration du théorème de structure concernant les modules de type fini sur un anneau principal. La preuve présentée ici est théorique ; il en existe d'autres plus algorithmiques (parfois limitées aux anneaux euclidiens, cas qui englobe tout de même l'essentiel pour votre programme, à savoir $\mathbb{Z}$ et $k[t]$), utilisant les opérations élémentaires sur les lignes et les colonnes d'une matrice, et qui sont tout aussi recevables par un jury d'oral. A vous donc de choisir selon vos goûts. Par ailleurs la proposition 1 et les lemmes 1, 2 et 3 ont leur intérêt propre et peuvent être lus indépendamment du reste.

1 Modules libres de rang fini

Dans toute la suite on désigne par A un anneau commutatif, unitaire et principal, c'est-à-dire intègre et dont tout idéal est de la forme (d) avec d appartenant à A. L'idéal étant donné l'élément d est déterminé *à un inversible près*. Le quotient $A/(d)$ sera (abusivement) noté A/d. Notons que si d est nul A/d est isomorphe à A, et que si d est inversible A/d est nul. On va tout d'abord montrer un résultat fondamental sur les A-modules libres (rappelons que le module nul est libre de rang 0) :

Proposition 1. *Soit m un entier, soit M un A-module libre de rang m et soit N un sous-A-module de M. Alors N est libre de rang inférieur ou égal à m.*

Démonstration. On raisonne par récurrence sur m. Si $m = 0$ alors $M = \{0\}$ et le résultat est trivial. Supposons le vrai au rang m et soit M un A-module libre de rang $m+1$. Soit N un sous-module de M. Soit $e_1, e_2, \ldots, e_{m+1}$ une base de M. Notons M' le sous-module de M engendré par $e_2, \ldots, e_{m+1}$. Il est libre de rang m. L'intersection $N \cap M'$ est un sous-module de M', et donc d'après l'hypothèse de récurrence $N \cap M'$ est libre de rang inférieur ou égal à m. Soit I l'ensemble des coordonnées sur e_1 des éléments de N. Il est visiblement stable par addition et par multiplication par un élément de A, c'est donc un idéal de A et il est de la forme (d) avec d dans A.

Si $d = 0$ alors N est inclus dans M' et donc $N = N \cap M'$; on a vu que de dernier est libre de rang inférieur ou égal à m, donc *a fortiori* à $m + 1$.

Supposons d non nul. Soit f_1 un élément de N de la forme $de_1 + y$, où y est dans M' (il en existe un par la définition même de d). Soit $f_2, \dots f_n$ une base de $N \cap M'$. Il en existe une puisque $N \cap M'$ est libre ; l'entier n est inférieur ou égal à $m + 1$. On va montrer que N est libre de base $f_1, f_2, \dots, f_n$ ce qui achèvera la démonstration.

Montrons d'abord que $(f_1, f_2, \dots, f_n)$ engendre N. Si x appartient à N, sa première coordonnée est dans I donc est égale à ad pour un certain élément a de A. L'élément $x - af_1$ a pour première coordonnée $ad - ad$ soit 0. Il appartient donc à M', et également à N puisque x et f_1 sont dans N. C'est donc un élément de $N \cap M'$ et il est par conséquent de la forme $\sum_{i \geq 2} a_i f_i$. On peut donc écrire $x = af_1 + \sum_{i \geq 2} a_i f_i$ et la famille des f_i engendre bien N. Montrons maintenant qu'elle est libre. Si $\sum_{i \geq 1} a_i f_i = 0$ alors en considérant la première coordonnée on trouve $da_1 = 0$ et donc $d = 0$ puisque a_1 est non nul (et A intègre). Dès lors $\sum_{i \geq 2} a_i f_i = 0$ et comme les f_i pour $i \geq 2$ forment par hypothèse une famille libre les a_i sont tous nuls pour $i \geq 2$. Finalement tous les a_i sont nuls ; la famille des f_i est libre, et c'est donc bien une base de N. □

Autre preuve de la proposition 1, proposée par Pierre Bernard, agrégatif en 2000-2001. Elle est plus élégante mais vous paraîtra peut-être plus délicate. On raisonne là encore par récurrence sur le rang m de M, le résultat étant trivial pour $m = 0$ et vrai pour $m = 1$ par la définition même d'un anneau principal. Supposons-le montré en rang inférieur ou égal à m (pour un certain $m \geq 1$) et soit M un A-module libre de rang $m + 1$. Ecrivons M comme une somme directe $M' \oplus M''$ où M' et M'' sont tous deux libres de rangs respectifs m' et m'' avec $m' < m + 1$ et $m'' < m + 1$ (il suffit de choisir une base de M et de l'écrire comme réunion disjointe de deux de ses sous-ensembles stricts). On dispose ainsi d'une suite exacte

$$0 \to M' \to M \to M'' \to 0$$

Soit N un sous-module de M. Son image N'' par la flèche de M dans M'' est un sous-module N'' de M''. Comme M'' est libre de rang m'' avec $m'' < m + 1$ l'hypothèse de récurrence montre que N'' est libre et que son rang n'' est inférieur ou égal à m''. De même le noyau N' de la flèche de N dans N'' est un sous-module de M'. De l'hypothèse de récurrence on déduit que N' est libre de rang n' inférieur ou égal à m'. On dispose d'une suite exacte

$$0 \to N' \to N \to N'' \to 0$$

Comme N'' est libre elle est scindée et N s'identifie donc à la somme directe de N' et N'' ; il est donc libre de rang $n' + n''$ et l'on a $n' + n'' \leq m' + m'' = m$ ce qui achève la démonstration. □

On va avoir besoin dans la suite du lemme suivant, qui est intéressant en soi. On appellera *forme linéaire* sur M toute application A-linéaire de M dans A.

Lemme 1. *Soit M un A-module sans torsion et x un élément non nul de M. Les propriétés suivantes sont équivalentes :*

(i) Le module Ax admet un supplémentaire dans M.

(ii) Il existe une forme linéaire ϕ sur M telle que $\phi(x) = 1$.

Démonstration. Supposons (i). On écrit $M = Ax \oplus N$ pour un certain N. L'application de M dans A qui à $ax + y$ (avec a dans A et y dans N) associe a est bien définie, car $ax = a'x \Rightarrow a = a'$ puisque x est non nul et M sans torsion. Elle est A-linéaire et vaut 1 sur x, ce qui montre (ii).

Supposons (ii). Soit N le noyau de ϕ et soit z appartenant à M. Alors $\phi(z - \phi(z)x) = \phi(z) - \phi(z)\phi(x) = \phi(z) - \phi(z) = 0$ donc si on pose $y = z - \phi(z)x$ alors y appartient à N et donc z s'écrit $\phi(z)x + y$ ce qui montre que $M = Ax + N$. D'autre part si z appartient à $Ax \cap N$ alors z s'écrit az pour un certain a dans A et donc $\phi(z) = a\phi(x) = a$. D'autre part comme z appartient à N on a $\phi(z) = 0$; en conséquence $a = 0$ et z est nul, ce qui montre que $M = Ax \oplus N$. □

Le lecteur attentif aura remarqué que dans le lemme ci-dessus le fait que A soit principal n'intervient absolument pas ; il est valable sur un anneau commutatif unitaire quelconque. La principalité est par contre essentielle pour établir l'équivalence suivante :

Lemme 2. *Soit m un entier strictement positif et M un A-module libre de base $e_1, \ldots, e_m$. Soit x un élément de M. Les propositions suivantes sont équivalentes :*

(i) Il existe une forme linéaire ϕ sur M telle que $\phi(x) = 1$.

(ii) le PGCD des coordonnées de x dans la base e_i est égal à 1.

Démonstration. Commençons par remarquer que pour tout i l'application e_i^* qui à $\sum a_j e_j$ associe a_i est une forme linéaire sur M. On démontre exactement comme dans le cas des espaces vectoriels que les e_i^* forment une base du A-module des formes linéaires de M dans A. Posons $x_i = e_i^*(x)$. On a donc $x = \sum x_i e_i$.

Supposons (i). On peut écrire ϕ sous la forme $\sum a_i e_i^*$. On a donc $\sum a_i e_i^*(x) = \sum a_i x_i = 1$ et les x_i sont bien premiers entre eux.

Supposons (ii). Comme les x_i sont premiers entre eux il existe d'après Bezout des scalaires a_i tels que $\sum a_i x_i = 1$. Si on pose $\phi = \sum a_i e_i^*$ alors $\phi(x) = \sum a_i x_i = 1$. □

Nous allons maintenant montrer le théorème dit *de la base adaptée*.

Théorème. *Soit m un entier positif et M un A-module libre de rang m. Soit N un sous-module de M. Il existe un entier r inférieur ou égal à m et une famille $d_1, \ldots, d_r$ d'éléments non nuls de A vérifiant $d_1|d_2|\ldots|d_r$, et une base $f_1, \ldots, f_m$ de M tels que $(d_1 f_1, \ldots, d_r f_r)$ soit une base de N.*

Remarque. Une telle base $f_1, \ldots, f_m$ est dite *adaptée* à N. L'entier r défini ci-dessus est le rang de N. Il est nul si et seulement si $N = \{0\}$, auquel cas la famille des d_i est vide.

Démonstration du théorème. On procède par récurrence sur m, le cas $m = 0$ étant trivial. Supposons le théorème établi pour un certain entier m et montrons qu'il est vrai pour $m+1$. Soit M un module libre de rang $m+1$ et N un sous-module de M. Donnons-nous une base $e_1, \ldots, e_{m+1}$ de M. L'idée est la suivante : s'il existe effectivement une famille $d_1, \ldots, d_r$ et une base adaptée à N alors toute forme linéaire ϕ sur M prend sur N des valeurs multiples de d_1 ; c'est en se fondant sur cette remarque qu'on va définir l'entier d_1.

Considérons l'ensemble E des éléments de A de la forme $\phi(y)$ où ϕ est une forme linéaire sur M et y un élément de N. Si N est nul le théorème est démontré. Sinon E est non nul : en effet il existe alors un y non nul dans N. L'une de ses coordonnées de y dans la base $(e_1, \ldots, e_{m+1})$ est non nulle et si c'est la i-ième alors $e_i^*(y)$ est non nul. Considérons un élément d_1 non nul de E *minimal pour la divisibilité*. Il en existe un : en effet soit a un élément non nul de E. On peut l'écrire $\epsilon \prod p_i^{\alpha_i}$ où ϵ est inversible et où les p_i sont des premiers deux à deux distincts. Si a est minimal pour la divisibilité le problème est réglé. Sinon il existe b non nul dans E divisant strictement a et qui s'écrit donc $\epsilon' \prod p_i^{\beta_i}$ où pour tout i on a $\beta_i \leq \alpha_i$, l'une au moins de ces inégalités étant stricte. Le processus s'arrête donc nécessairement à un moment.

Il existe donc une forme linéaire ϕ sur M et un élément y de N tel que $\phi(y) = d_1$. Faisons deux remarques :

- Si ψ est une forme linéaire sur M alors d_1 divise $\psi(y)$. En effet soit d le PGCD de d_1 et de $\psi(y)$. Par Bezout il existe a et b dans A tels que $a\phi(y) + b\psi(y) = ad_1 + b\psi(y) = d$. L'élément $a\phi(y) + b\psi(y) = (a\phi + b\psi)(y)$ appartient à E et vaut d donc divise d_1. Par minimalité de d_1 il est égal à d_1 à un inversible près.

- Si x est un élément de N alors d_1 divise $\phi(x)$. En effet soit d le PGCD de d_1 et de $\phi(x)$. Par Bezout il existe a et b dans A tels que $a\phi(y) + b\phi(x) = ad_1 + b\phi(x) = d$. L'élément $a\phi(y) + b\phi(x) = \phi(ay + bx)$ appartient à E et vaut d donc divise d_1. Par minimalité de d_1 il est égal à d_1 à un inversible près.

En particulier $e_i^*(y)$ est un multiple de d_1 pour tout i. Ceci montre que y s'écrit $d_1 f_1$ pour un certain f_1 dans M. Comme $\phi(y) = d_1$ on a $\phi(f_1) = 1$ et

donc d'après le lemme 1, et plus précisément la partie $(ii) \Rightarrow (i)$, on peut écrire $M = Af_1 \oplus \text{Ker } \phi$. Le module Ker ϕ est libre d'après la proposition montrée plus haut puisque c'est un sous-module de M. Son rang est nécessairement m puisque Af_1 est libre de rang 1.

Si x est un élément de N il s'écrit $af_1 + z$ avec z dans Ker ϕ. On a alors $\phi(x) = a$ et d'autre part d'après la remarque ci-dessus $\phi(x)$ est multiple de d_1. On peut donc écrire $a = d_1 a'$ et $x = a' d_1 f_1 + z$. Or $d_1 f_1 = y \in N$ donc z appartient aussi à N et donc à $N \cap \text{Ker } \phi$. On a donc $N = Ad_1 f_1 \oplus N \cap \text{Ker } \phi$.

Or $N \cap \text{Ker } \phi$ est un sous-module de Ker ϕ qui est un module libre de rang m. D'après l'hypothèse de récurrence il existe donc un entier r, une base $f_2, \ldots, f_{m+1}$ de Ker ϕ et une famille $d_2, \ldots d_r$ d'éléments de A tels que $d_2 | d_3 | \ldots | d_r$ de sorte que $d_2 f_2, \ldots, d_r f_r$ soit une base de $N \cap \text{Ker } \phi$. La famille $f_1, \ldots, f_{m+1}$ est alors une base de M, et $d_1 f_1, \ldots, d_r f_r$ est une base de N. Il n'y a plus qu'à vérifier que d_1 divise d_2. Soit d le PGCD de d_1 et d_2. Il existe a et b dans A tels que $ad_1 + bd_2 = d$. La forme linéaire $af_1^* + bf_2^*$ prend donc la valeur d sur l'élément $d_1 f_1 + d_2 f_2$ de N. On en déduit que d, qui divise d_1, appartient à E. La minimalité de d_1 implique que d est égal à d_1 à un inversible près, et donc d_1 divise d_2 ce qui achève la démonstration. □

2 A-modules de type fini

On va maintenant énoncer, et démontrer, le théorème de structure.

Théorème de structure des A-modules de type fini. *Soit V un A-module de type fini. Il existe un entier n et une famille $d_1, d_2, \ldots, d_n$ d'éléments* non inversibles *de A tels que :*

- $d_1 | d_2 | \ldots | d_n$
- $V \simeq A/d_1 \oplus A/d_2 \oplus \ldots \oplus A/d_n$

De plus les d_i sont uniquement déterminés à un inversible près.

Remarque. Si d est inversible alors $A/d = \{0\}$; c'est pour cette raison qu'on exclut que les d_i soient inversibles : ceci rajouterait artificiellement des termes nuls dans la somme directe et il n'y aurait plus d'espoir d'avoir unicité. Par contre l'un des d_i peut très bien être égal à 0, dans ce cas tous les suivants le sont aussi par la relation de divisibilité. Si $d_i = 0$ alors $A/d_i = A$.

Démonstration du théorème de structure. Montrons tout d'abord l'existence. Comme V est de type fini il possède une famille génératrice finie $e_1, \ldots, e_m$. L'application de A^m dans V qui envoie (a_i) sur $\sum a_i e_i$ est linéaire surjective. Si N désigne son noyau on a $V \simeq A^m/N$. D'autre part le théorème de la base adaptée affirme l'existence d'une base $f_1, f_2, \ldots, f_m$ de A^m et d'une famille $d_1 | d_2 | \ldots | d_r$

de scalaires tels que $d_1 f_1, \ldots, d_r f_r$ soit une base de N. On en déduit que V est isomorphe à

$$\left(\bigoplus_{1 \leq i \leq r} A/d_i \right) \oplus A^{m-r}$$

On a donc le résultat voulu en ne gardant que les d_i non inversibles (et en les renumérotant pour commencer par d_1), et en remarquant que A^{m-r} est la somme directe de $m-r$ termes que l'on peut écrire $A/0$.

Le module V est donc isomorphe à $A/d_1 \oplus A/d_2 \oplus \ldots \oplus A/d_n$. On va montrer que la liste des d_i peut être déduite des propriétés intrinsèques du A-module V, ce qui établira l'unicité de la décomposition.

Soit r le nombre de d_i nuls ; on peut écrire $V \simeq \left(\bigoplus_{i \leq n-r} A/d_i \right) \oplus A^r$. Le sous-module V_{tors} de V formé des éléments de torsion (c'est-à-dire annulés par un élément non nul de A) s'identifie à $\bigoplus_{i \leq n-r} A/d_i$, et donc V/V_{tors} est isomorphe à A^r, donc libre de rang r. *Le nombre de d_i nuls est donc le rang du A-module libre V/V_{tors}.*

Le sous-module V_{tors} de V est donc isomorphe à

$$\bigoplus_{i \leq n-r} A/d_i$$

Comme $d_1 | \ldots | d_{n-r}$, il suffit, pour déterminer complètement la liste des d_i, de connaître pour tout élément premier p de A et tout entier α le nombre s de d_i multiples de p^α (les d_i en question sont alors exactement les s derniers). On va pour cela établir un lemme intermédiaire :

Lemme 3. *Soit p un élément premier de A, soient α et β deux entiers et d un élément premier à p. Alors le module $p^\alpha(A/p^\beta d)$ (image de la multiplication par p^α de $A/p^\beta d$ dans lui-même) est isomorphe à A/d si $\beta \leq \alpha$ et à $A/p^{\beta-\alpha}d$ sinon. Le module $(A/p^\beta d)/p(A/p^\beta d)$ est isomorphe à A/p si β est strictement positif et est nul sinon.*

Démonstration. Par le lemme chinois $A/p^\beta d$ est isomorphe à $A/p^\beta \oplus A/d$. Comme p^α est premier à d il est inversible dans A/d donc $p^\alpha(A/d) = A/d$. Quant à $p^\alpha(A/p^\beta)$ c'est l'image du morphisme composé $A \stackrel{a \mapsto p^\alpha a}{\longrightarrow} A \to A/p^\beta$. Le noyau de ce morphisme est l'ensemble des éléments a de A tels que $p^\alpha a$ soit multiple de p^β. C'est donc A tout entier si $\alpha \geq \beta$ et c'est l'idéal $(p^{\beta-\alpha})$ sinon. On a donc $p^\alpha(A/p^\beta) = \{0\}$ si $\alpha \geq \beta$ et $p^\alpha(A/p^\beta) \simeq A/p^{\beta-\alpha}$ sinon. En réutilisant le lemme chinois on achève la démonstration de la première partie du lemme.

Pour la seconde on considère le morphisme composé

$$A \to A/p^\beta d \to (A/p^\beta d)/p(A/p^\beta d)$$

qui est surjectif, chacune des deux flèches du diagramme l'étant. Son noyau est l'ensembles des a dont l'image dans $A/p^\beta d$ est multiple de p, c'est-à-dire l'ensemble des a tels qu'il existe u et v dans A vérifiant $a = pu + p^\beta dv$. C'est donc l'idéal $(p^\beta d, p)$ qui est égal, A étant principal, à (PGCD$(p^\beta d, p)$) et donc à A tout entier si β est nul, et à (p) sinon. On en déduit donc que $(A/p^\beta d)/p(A/p^\beta d)$ est nul si $\beta = 0$ et isomorphe à A/p sinon. Le lemme est démontré. □

Suite de la démonstration du théorème de structure. Soit p un élément premier de A et soit α un entier supérieur ou égal à 1. Soit i compris entre 1 et $n-r$, écrivons $d_i = p^\beta d$ où d est premier à p. D'après ce qui précède le A/p-espace vectoriel (il s'agit *a priori* d'un A-module, mais qui est annulé par p et est donc un A/p-espace vectoriel) $p^{\alpha-1}(A/d_i)/p^\alpha(A/d_i) = p^{\alpha-1}(A/d_i)/p(p^{\alpha-1}(A/d_i))$ est nul si $\beta \leq \alpha - 1$ et de rang 1 dans le cas contraire, c'est-à-dire dans le cas où p^α divise d_i. On en déduit que *le nombre de d_i (pour i compris entre 1 et $n-r$) multiples de p^α est égal à la dimension du A/p-espace vectoriel $p^{\alpha-1}V_{tors}/p^\alpha V_{tors}$.*

Récapitulons : soit V un A-module isomorphe à $A/d_1 \oplus A/d_2 \oplus \ldots \oplus A/d_n$ avec les d_i non inversibles et $d_1|d_2|\ldots|d_n$. Alors le nombre de d_i nuls est égal au rang du A-module libre V/V_{tors}. Pour tout p premier et tout entier $\alpha \geq 1$ le nombre de d_i non nuls et multiples de p^α est égal à la dimension du A/p-espace vectoriel $p^{\alpha-1}V_{tors}/p^\alpha V_{tors}$.

La démonstration du théorème est terminée. □

Remarque. On peut déduire de ce qui précède l'unicité des d_i (à inversible près) dans le théorème de la base adaptée : il suffit en effet de considérer le quotient M/N et de lui appliquer l'assertion du théorème de structure relative à l'unicité.

3 Interprétation matricielle

Rappelons que deux matrices B et C appartenant à $M_{m,n}(A)$ sont dites *équivalentes* s'il existe deux matrices P et Q qui sont respectivement inversibles dans $M_m(A)$ et $M_n(A)$ et telles que $B = P^{-1}AQ$. Comme dans le cas des espaces vectoriels, cette relation a une interprétation en termes d'applications linéaires : deux matrices sont équivalentes si et seulement si elles représentent la même application linéaire dans des bases différentes : P et Q sont alors les matrices respectives de changement de base de changement de base à l'arrivée et au départ.

Le théorème de la base adaptée peut être reformulé ainsi :

Théorème. *Soient n et m deux entiers strictement positif et B une matrice $m \times n$ à coefficients dans A. Alors B est équivalente à une matrice $D = (d_{ij})$ telle que :*

- *$d_{i,j}$=0 dès que $i \neq j$*

- $d_{1,1}|d_{2,2}|\ldots|d_{s,s}$ *où* $s = \min(n,m)$

De plus les $d_{i,i}$ *sont uniquement déterminés à un inversible près.*

Démonstration. La matrice B peut être vue comme la matrice d'une application A-linéaire ϕ de A^n dans A^m. Notons N son image. D'après le théorème de la base adaptée il existe une base $(f_1, f_2, \ldots, f_m)$ de A^m et des scalaires $d_1|d_2|\ldots|d_r$ non nuls tels que $d_1 f_1, \ldots, d_r f_r$ forme une base de N. Pour tout i compris entre 1 et r choisissons un antécédent l_i de $d_i f_i$ par ϕ. Les l_i forment une famille libre, puisque les $d_i f_i$ le sont. Montrons que $A^n = Al_1 \oplus Al_2 \oplus \ldots \oplus Al_r \oplus \mathrm{Ker}\ \phi$. Si x appartient à A^n son image appartient à N donc s'écrit $\sum a_i d_i f_i = \sum a_i \phi(l_i)$. En conséquence $x - \sum a_i l_i$ appartient à Ker ϕ et donc $A^n = Al_1 \oplus Al_2 \oplus \ldots \oplus Al_r + \mathrm{Ker}\ \phi$. D'autre part si x s'écrit $\sum a_i l_i$ et appartient à Ker ϕ on a $\sum a_i d_i f_i = 0$ et donc $a_i = 0$ pour tout i puisque la famille des $d_i f_i$ est libre, et en conséquence $x = 0$. On a donc bien $A^n = Al_1 \oplus Al_2 \oplus \ldots \oplus Al_r \oplus \mathrm{Ker}\ \phi$. Comme Ker ϕ est un sous-module de A^n il est libre d'après la proposition démontrée plus haut. Son rang est nécessairement $n - r$. Soit $l_{r+1}, \ldots, l_n$ une base de Ker ϕ. Alors $l_1, \ldots, l_n$ forme une base de A^n. La matrice de ϕ dans les bases $(l_1, \ldots, l_n)$ (au départ) et $(f_1, \ldots, f_m)$ (à l'arrivée) a tous ses coefficients nuls à l'exception de ses r premiers coefficients diagonaux qui sont précisément les d_i. La première partie du théorème est démontrée. On établit l'unicité en remarquant que si B est semblable à une matrice D du type évoqué dans l'énoncé du théorème alors $A^n/\phi(A^m)$ est isomorphe à $\bigoplus A/d_{i,i}$; c'est donc le résultat d'unicité dans le théorème de structure qui permet de conclure. □

On va donner à présent une caractérisation matricielle des $d_{i,i}$ du théorème ci-dessus. Rappelons que si on note $(b_{i,j})$ le terme général de la matrice B, on appelle *sous-matrice carrée de taille* k de B toute matrice de la forme $(b_{i,j})_{(i,j)\in I\times J}$ où I (resp. J) est un sous-ensemble de cardinal k de $\{1, \ldots, m\}$ (resp. de $\{1, \ldots, n\}$). On appelle *mineur d'ordre* k de B tout déterminant d'une sous-matrice carrée de taille k de B.

Proposition. *On reprend les notations du théorème ci-dessus. Soit* k *un entier inférieur ou égal à* n *et à* m. *Alors le produit* $d_{1,1}d_{2,2}\ldots d_{k,k}$ *des* k *premiers coefficients diagonaux de* B *est égal au PGCD des mineurs d'ordre* k *de* B.

Démonstration. Si $B = D$ c'est immédiat. Pour toute matrice C on note $\Delta_k(C)$ le PGCD des mineurs d'ordre k de C. Il suffit donc de montrer que Δ_k est invariant par équivalence. Par symétrie il suffit de montrer que si C et C' sont équivalentes alors $\Delta_k(C)|\Delta_k(C')$. Plus précisément il suffit de le montrer pour C' de la forme CQ avec Q carrée inversible. En effet dans ce cas ce sera vrai également pour toute matrice de la forme PC avec P inversible (et donc finalement pour PCQ) ; on le voit en utilisant le fait que Δ_k est invariant par

la transposition, laquelle transforme mutliplication à gauche en multiplication à droite.

Soit donc C une matrice de taille $m \times n$ à coefficients dans A et Q une matrice inversible de taille n. Pour tout entier i inférieur ou égal à n la i-ième colonne de CQ est combinaison A-linéaire des colonnes de C (les coefficients étant ceux de la i-ième colonne de Q). Le caractère multilinéaire alterné du déterminant par rapport aux colonnes montre alors que tout mineur d'ordre k de CQ est combinaison de mineurs d'ordre k de C, et donc est multiple de $\Delta_k(C)$. On en déduit que $\Delta_k(C)$ divise $\Delta_k(CQ)$, ce qu'il fallait démontrer. □

Terminons par une remarque concernant les endomorphismes d'espaces vectoriels en dimension finie. Soit donc k un corps et E un k-ev de base $(e_1, e_2, \ldots, e_n)$. Soit u un endomorphisme de E. Il induit une structure de $k[t]$-module sur E donnée par $Px = P(u)(x)$. L'application ϕ de $k[t]^n$ dans E qui envoie (P_i) sur $\sum_i P_i e_i$ est $k[t]$-linéaire et surjective. Notons $f_1, f_2, \ldots, f_n$ la base canonique du $k[t]$-module $k[t]^n$ (on a alors $\phi(f_j) = e_j$ pour tout j) et N le noyau de ϕ. Pour j fixé on a $u(e_j) = \sum a_{i,j} e_i$ où $(a_{i,j})$ est la matrice de u dans la base $(e_1, e_2, \ldots, e_n)$. On a donc $\sum_{i \neq j} a_{i,j} e_i + a_{j,j} e_j - u(e_j) = 0$ soit encore

$$\sum_{i \neq j} a_{i,j} e_i + (a_{j,j} - t) e_j = 0$$

On en déduit donc que pour tout entier j l'élément $\sum_{i \neq j} a_{i,j} f_i + (a_{j,j} - t) f_j$ est dans N.

Proposition 2. *La famille des* $\sum_{i \neq j} a_{i,j} f_i + (a_{j,j} - t) f_j$ *pour* j *variant de* 1 *à* n *forme une base du* $k[t]$*-module* N.

Démonstration. Pour tout j notons ω_j l'élément $\sum_{i \neq j} a_{i,j} f_i + (a_{j,j} - t) f_j$. On a

$$(*) \quad t f_j = \sum_i a_{i,j} f_i - \omega_j$$

pour tout j. On en déduit que tout élément $\sum_j P_j(t) f_j$ de $k[t]^n$ peut être mis sous la forme $\sum_j Q_j(t) \omega_j + \sum_j b_j f_j$ où les b_j sont des *scalaires*. Les ω_j étant dans N l'image par ϕ d'un tel élément est égale à $\sum_j b_j e_j$. Elle est donc nulle, les e_j formant une base de E, si et seulement si tous les b_j sont nuls. On en déduit que N est engendré par les ω_j.

Supposons maintenant que l'on ait $\sum_j Q_j(t) \omega_j = 0$. Alors de $(*)$ on déduit l'égalité

$$\sum_j Q_j(t) t f_j = \sum_{i,j} Q_j(t) a_{i,j} f_i$$

ce qui implique, les f_j formant une base de $k[t]^n$, que l'on a

$$Q_j(t)t = \sum_i a_{j,i} Q_i(t)$$

pour tout j. Si les Q_j sont non tous nuls alors en en considérant un de degré maximal on aboutit à une contradiction. La famille des ω_j est donc libre, et forme finalement une base de N. □

Références

Il y a bien entendu de très nombreuses références sur la question. La première démonstration de la proposition 1 est directement copiée sur celle du théorème 3.7 de Jacobson (Basic Algebra 1), celle de la proposition 2 provient elle aussi de Basic Algebra 1 (*cf.* le lemme suivant le théorème 3.13).

La preuve du théorème de la base adaptée est tirée de Bourbaki, Algèbre, Chapitre VII. Signalons d'une manière générale que ce chapitre de Bourbaki est (comme beaucoup d'autres) remarquablement écrit. Les démonstrations que l'on y trouve sont concises et élégantes, mais demandent une très bonne maîtrise de certains concepts abstraits ; ne vous y noyez pas si vou s n'aimez pas trop ce genre de choses. Dans le cas contraire vous pourrez par exemple savourer la preuve de l'unicité de la décomposition qui se fait en quelques lignes, et dans un cadre plus général que celui des anneaux principaux, à l'aide des puissances extérieures...

Vous trouverez par ailleurs dans le Goblot (§ 2.2) une preuve algorithmique du théorème de la base adaptée, qui est établi matriciellement ; un paragraphe spécial est consacré aux anneaux euclidiens pour lesquels le procédé est nettement plus simple.