5 Rang d'un module libre, modules de type fini sur un anneau principal

Version du 16 novembre 2005

20 A-modules libres de type fini, invariance du rang

20.1 Rang d'un module libre de type fini

Soient A un anneau commutatif et M un A-module de type fini.

Lemme 20.1.1 *Si M est un A-module libre, alors toute base de M est formée d'un nombre fini d'éléments.*

Démonstration. Soient $x_1, \ldots, x_r$ des générateurs, et supposons que $(b_i)_{i\in I}$ soit une base de M. Chaque x_s s'écrit comme une combinaison linéaire finie des b_i, et donc il existe un sous-ensemble fini J de I tel que $x_1, \ldots, x_r$ soient combinaisons linéaires des b_j, pour $j \in J$.

Ceci entraîne que $I = J$ est fini. En effet, s'il existait $i \in I \setminus J$, alors b_i serait combinaison linéaire des x_s et donc des b_j, pour $j \in J$, contredisant l'indépendance linéaire de $\{b_i\} \cup \{b_j \mid j \in J\}$. Ceci prouve le lemme. □

Définition 20.1.2 *On dit que M est un A-module libre* **de rang** *n s'il est libre et admet une base formée de n éléments, c.-à-d., si $M \cong A^n$.*

Théorème 20.1.3 (Rang d'un module libre de type fini) *Soit $M \neq 0$ un A-module libre de type fini. Il existe un* **unique** *entier $n \geq 1$ tel que $M \cong A^n$. En d'autres termes, si M admet une base formée de n éléments, alors* **toute** *base de M a n éléments. Par conséquent, le rang de M est bien défini ; on le note* $\operatorname{rg} M$.

Si A est intègre, alors $\operatorname{rg} M$ *égale la dimension du K-espace vectoriel $S^{-1}M$, où $S = A \setminus \{0\}$ et $K = S^{-1}A$ est le corps des fractions de A.*

Démonstration. Démontrons d'abord le résultat dans le cas particulier où A est intègre, qui est plus simple et est suffisant pour l'application au cas où A est principal.

Supposons que $(e_1, \dots, e_n)$ soit une base de M comme A-module. Comme M est libre, donc sans torsion, le morphisme naturel $M \to S^{-1}M$ est injectif, et l'on peut identifier M à un sous-A-module du K-espace vectoriel $S^{-1}M$. Alors on voit facilement que $(e_1, \dots, e_n)$ est une base de $S^{-1}M$ comme K-espace vectoriel. Donc $n = \dim_K S^{-1}M$, ce qui montre que n est uniquement déterminé.

Dans le cas général, l'idée est exactement la même, mais il faut remplacer le corps des fractions par un quotient $A/\mathfrak{m}$, où $\mathfrak{m}$ est un idéal maximal de A. Un tel idéal existe, d'après le corollaire 11.2.8, et dans ce cas l'anneau quotient $k := A/\mathfrak{m}$ est un corps.

Pour démontrer le théorème, on aura besoin du lemme suivant.

Lemme 20.1.4 *Soient I un idéal de A et $\pi : A \to A/I$. Le noyau du morphisme*

$$\phi : A^n \to (A/I)^n, \qquad (a_1, \dots, a_n) \mapsto (\pi(a_1), \dots, \pi(a_n))$$

est le sous-module $IA^n = \{(x_1, \dots, x_n) \mid x_i \in I \text{ pour } i = 1, \dots, n\}$. Par conséquent, ϕ induit un isomorphisme

$$A^n/IA^n \xrightarrow{\sim} (A/I)^n.$$

Démonstration. On voit facilement que IA^n est comme indiqué, et c'est le noyau de ϕ. Comme ϕ est surjectif, le lemme découle du théorème fondamental d'isomorphisme (9.2.5). □

On peut maintenant démontrer le théorème dans le cas général. Supposons $M \cong A^n$. Alors, d'après le théorème 9.6.4, $M/\mathfrak{m}M$ est isomorphe comme $A/\mathfrak{m}$-module, c.-à-d., comme k-espace vectoriel, à $A^n/\mathfrak{m}A^n$. Or, d'après le lemme précédent, ce dernier est un k-espace vectoriel de dimension n. Donc $n = \dim_k M/\mathfrak{m}M$, et ceci montre que n est uniquement déterminé. Le théorème est démontré. □

Remarque 20.1.5 On peut aussi démontrer le théorème précédent en étudiant l'algèbre extérieure d'un A-module libre. Voir par exemple [BM, §IV.2].

Remarque 20.1.6 Le théorème n'est pas vrai pour les anneaux non commutatifs. En effet, soient k un corps, V un k-espace vectoriel de dimension dénombrable (par exemple $V = k[X]$) et soit R l'anneau des endomorphismes de V. On voit facilement que $V \cong V \oplus V$, et l'on peut en déduire que $R \cong R^2$ comme R-module à gauche.

Pour un anneau non-commutatif, il existe aussi des idéaux bilatères maximaux, mais l'anneau quotient n'est pas un corps en général ; c'est ici qu'intervient la différence avec le cas commutatif traité dans le théorème.

20.2 Modules d'homomorphismes et module dual

Définition 20.2.1 *1) Soient M, N deux A-modules, $\phi, \phi' \in \mathrm{Hom}_A(M, N)$ et $a \in A$. On note $\phi + \phi'$, resp. $a\phi$, l'application $M \to N$ qui à tout $m \in M$ associe $\phi(m)+\phi'(m)$, resp. $a\phi(m)$. Alors $\phi+\phi'$ et $a\phi$ sont des A-morphismes ; on obtient ainsi une structure de A-module sur $\mathrm{Hom}_A(M, N)$.*

2) Dans le cas particulier où $N = A$, on pose $M^* = \mathrm{Hom}_A(M, A)$; on l'appelle le module **dual** *de M.*

Proposition 20.2.2 *Soient M, M', N des A-modules. L'application $\phi \mapsto (\phi|_M, \phi|_{M'})$ est un isomorphisme de A-modules*

$$\mathrm{Hom}_A(M \oplus M', N) \xrightarrow{\sim} \mathrm{Hom}_A(M, N) \oplus \mathrm{Hom}_A(M', N).$$

En particulier, pour $N = A$, on obtient $(M \oplus M')^* \cong M^* \oplus M'^*$.

Démonstration. On voit facilement que $\phi \mapsto (\phi|_M, \phi|_{M'})$ est un morphisme de A-modules ; il en est de même de l'application qui à un couple de morphismes $\psi : M \to N$ et $\psi' : M' \to N$ associe le morphisme $\psi + \psi' : M \oplus M' \to N$ défini par $(\psi+\psi')(m+m') = \psi(m)+\psi(m')$. Il est clair que ces deux applications sont des bijections réciproques. Ceci prouve la proposition. □

Remarque 20.2.3 Supposons A intègre. Si M est un A-module de torsion, alors $M^* = (0)$. En effet, soit $\phi \in M^*$. Pour tout $m \in M$, $\phi(m) \in A$ est un élément de torsion, donc nul puisque A est supposé intègre. Donc $\phi = 0$, ce qui montre que $M^* = (0)$.

Par exemple, pour tout $n > 1$, le dual du $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ est nul. Ceci montre qu'en général on perd de l'information en passant de M à M^*. Toutefois, pour les modules libres on a le résultat suivant.

Proposition 20.2.4 (Dual d'un module libre de rang fini) *Soit M un A-module libre de rang n, et soit $(e_1, \dots, e_n)$ une base de M. Pour tout i, notons e_i^* l'élément de M^* défini par $e_i^*(a_1e_1 + \cdots + a_ne_n) = a_i$.*

Alors $(e_1^*, \dots, e_n^*)$ est une base de M^*, appelée la **base duale***. De plus, le morphisme canonique $M \to M^{**}$ est un isomorphisme.*

Démonstration. D'une part, $e_1^*, \dots, e_n^*$ sont linéairement indépendants, car si $f = a_1e_1^* + \cdots + a_ne_n^* = 0$, alors $0 = f(e_i) = a_i$ pour tout i. De même, $e_1^*, \dots, e_n^*$ engendrent M^* car $f = f(e_1)e_1^* + \cdots + f(e_n)e_n^*$, pour tout $f \in M^*$. Il en résulte que $(e_1^*, \dots, e_n^*)$ est une base de M^*.

Notons $(e_1^{**}, \dots, e_n^{**})$ sa base duale dans M^{**}. Alors le morphisme naturel $M \to M^{**}$ envoie chaque e_i sur e_i^{**}, donc est un isomorphisme. □

21 Modules de type fini sur un anneau principal

Dans cette section et la suivante, A est un anneau principal. Dans ce cas, on a une compréhension complète des A-modules de type fini grâce à un théorème fondamental de structure.

21.1 Matrices échelonnées

Soient $r, n \in \mathbb{N}^*$ et soit $P \in M_{nr}(A)$ une matrice à n lignes et r colonnes. Notons p_{ij} les coefficients de P et $P_1, \dots, P_r$ ses colonnes. On suppose que chaque colonne P_j est non nulle.

Définition 21.1.1 *On définit la* longueur $\ell(P_j)$ *de la colonne P_j comme étant le plus grand $i \in \{1, \dots, n\}$ tel que $p_{ij} \neq 0$. On dit alors que P est une matrice* **échelonnée** *si l'on a $\ell(P_1) < \cdots < \ell(P_r)$.*

Par exemple, la matrice suivante, dans $M_{6,3}(\mathbb{Z})$, est échelonnée :

$$\begin{pmatrix} 1 & 0 & 3 \\ 2 & 3 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 4 \end{pmatrix}$$

21.2 Les résultats fondamentaux

Proposition 21.2.1 *Soient A principal et M un A-module libre de rang n. Tout sous-module de M est libre de rang $r \leq n$. (On convient que le module (0) est libre de rang 0).*

Plus précisément, soit $(e_1, \ldots, e_n)$ une base de M et soit N un sous-module non nul de M. Il existe une base $(v_1, \ldots, v_r)$ de N telle que la matrice exprimant les v_j en fonction des e_i soit échelonnée.

Démonstration. Pour $i = 1, \ldots, n$, soit M_i le sous-module de M engendré par $e_1, \ldots, e_i$ et soit $N_i := N \cap M_i$. On va montrer l'assertion pour N_i, par récurrence sur i. Si $i = 0$, il n'y a rien à montrer. Supposons $i \geq 1$ et l'assertion établie pour $i - 1$.

Soit $\pi_i : M_i \to A$ la i-ème projection et soit $J_i = \pi_i(N_i)$; c'est un idéal de A. Si $J_i = 0$, alors N_i égale N_{i-1}, qui admet une base $(v_1, \ldots, v_s)$, où $s \leq i - 1$, qui s'exprime de façon échelonnée en fonction de $e_1, \ldots, e_{i-1}$.

Supposons donc $J_i = (a) \neq 0$. Alors il existe

$$x = a_1 e_1 + \cdots + a_{i-1} e_{i-1} + a e_i \in N \cap M_i,$$

tel que $\pi_i(x) = a$. Comme A est intègre, $Ax \cap M_{i-1} = (0)$, puisque la i-ème coordonnée de bx est non nulle si $b \neq 0$. On a donc $Ax \cap N_{i-1} = (0)$. D'autre part, on a $N_i = N_{i-1} + Ax$. En effet, soit $y \in N_i$. Alors $\pi_i(y) = a\alpha$, avec $\alpha \in A$, et donc $y - \alpha x \in N_{i-1}$. Par conséquent, posant $v_{s+1} = x$ on a

$$N_i = N_{i-1} \oplus A v_{s+1},$$

et $(v_1, \ldots, v_{s+1})$ est une base de N_i vérifiant les propriétés voulues. □

Théorème 21.2.2 (Théorème fondamental de structure pour les modules de type fini sur un anneau principal)

Soit A un anneau principal.

1) *Soient $n \geq 1$ et N un sous-module non nul du A-module libre A^n. Alors, il existe une base $(e_1, \ldots, e_n)$ de A^n, un entier $r \in \{1, \ldots, n\}$, et des éléments non nuls $a_1, \ldots, a_r$ de A vérifiant $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r - 1$, tels que*

$$(a_1 e_1, \ldots, a_r e_r)$$

soit une base de N. En particulier, r est le rang de N. De plus, les idéaux $(a_r) \subseteq \cdots \subseteq (a_1)$ sont uniquement déterminés par le sous-module N. Enfin, le sous-module de A^n engendré par $e_1, \ldots, e_r$ ne dépend que de N, et égale

$$N' = \{x \in A^n \mid \exists a \in A \setminus \{0\} \text{ tel que } ax \in N\}.$$

2) *Soit M un A-module de type fini. Il existe $s \geq 0$ et des éléments non nuls $a_1, \ldots, a_r$ de A vérifiant $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r-1$, tels que*

$$M_{tors} = A/(a_1) \oplus A/(a_2) \oplus \cdots \oplus A/(a_r); \tag{1}$$

$$\mathrm{Ann}(M_{tors}) = (a_r); \tag{2}$$

$$M \cong A^s \oplus M_{tors}, \qquad et \qquad A^s \cong M/M_{tors}. \tag{3}$$

En particulier, M **est libre ssi** *M* **est sans torsion**. *De plus, les idéaux $(a_r) \subseteq \cdots \subseteq (a_1)$ sont uniquement déterminés. On les appelle les* **idéaux (ou facteurs) invariants** *de M.*

3) *Pour M un A-module de torsion de type fini, la décomposition* (1) *ci-dessus se raffine comme suit. Soit $\mathrm{Ann}(M) = (p_1)^{m_1} \cdots (p_n)^{m_n}$ la décomposition de $\mathrm{Ann}(M)$ en produits d'idéaux maximaux. Alors, on a la décomposition primaire*

$$M = \bigoplus_{i=1}^{n} M(p_i). \tag{4}$$

et, d'après le point 2)*, chaque $M(p_i)$ se décompose en un somme directe*

$$M(p_i) = \bigoplus_{s=1}^{t_i} A/(p_i)^{n_s(p_i)}, \tag{5}$$

où la suite $1 \leq n_1(p_i) \leq \cdots \leq n_{t_i}(p_i)$ est uniquement déterminée. En particulier, $n_{t_i}(p_i) = m_i$ et $\mathrm{Ann}\, M(p_i) = (p_i^{m_i})$.

La démonstration du théorème se fera en trois étapes. On va montrer d'abord l'existence dans les points 1), 2) et 3). On établira ensuite l'unicité des $n_s(p_i)$ dans le point 3) et des idéaux (a_i) dans le point 2), et l'on en déduira l'unicité des (a_i) dans le point 1).

Définition 21.2.3 *On dira que la base de M donnée dans le point 1) est* **adaptée** *au sous-module N.*

21.3 Existence d'une base adaptée

On va démontrer l'existence d'une base adaptée par récurrence sur n. Si $n = 1$ alors N est un idéal de A, donc est librement engendré par un élément $a \in A$. De plus, $N' = A$ dans ce cas.

Supposons $n \geq 2$ et le théorème démontré pour $n-1$. Notons $(\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $M := A^n$ et $(\varepsilon_1^*, \ldots, \varepsilon_n^*)$ la base duale de M^*. Comme N est supposé non nul, il existe un indice i tel que $\varepsilon_i^*(N) \neq 0$.

Pour tout $f \in M^*$, $f(N)$ est un idéal de A. Comme A est noethérien, l'ensemble de ces idéaux $f(N)$, pour f variant dans M^*, admet un élément maximal $f_0(N) = (a)$, et $a \neq 0$ puisque $\varepsilon_i(N) \neq 0$. Soit $x = (x_1, \ldots, x_n) \in N$ tel que $f_0(x) = a$. Montrons d'abord le lemme suivant.

Lemme 21.3.1 *Pour tout $g \in M^*$, a divise $g(x)$.*

Démonstration. Soit d le PGCD de a et $g(x)$. D'après le théorème de Bezout, il existe $u, v \in A$ tels que $d = ua + vg(x)$. Posons $f = uf_0 + vg$. Alors $d = f(x)$ appartient à $f(N)$, d'où

$$f_0(N) = (a) \subseteq (d) \subseteq f(N).$$

D'après le choix de f_0, les deux extrêmes sont égaux, d'où $(d) = (a)$. Donc a est associé à d et divise $g(x)$. Ceci prouve le lemme. □

En particulier, a divise chaque $x_i = \varepsilon_i(x)$, donc on peut écrire $x = ae_1$ pour un certain $e_1 \in M$, et l'on a $f_0(e_1) = 1$. Par conséquent, on a :

$$(*) \qquad M = Ae_1 \oplus \operatorname{Ker} f_0 \quad \text{et} \quad N = Ax \oplus (N \cap \operatorname{Ker} f_0).$$

En effet, comme $f_0(e_1) = 1$, il est clair que $Ae_1 \cap \operatorname{Ker} f_0 = (0)$, et a fortiori $\operatorname{Ker} f_0 \cap Ax = (0)$. Soit $m \in M$ arbitraire. Alors $m - f_0(m)e_1 \in \operatorname{Ker} f_0$ et il en résulte que

$$M = \operatorname{Ker} f_0 \oplus Ae_1.$$

Si $n \in N$, il existe $b \in A$ tel que $f_0(n) = ba$, et alors $n - bx \in \operatorname{Ker} f_0 \cap N$. Ceci montre que $N = Ax \oplus (N \cap \operatorname{Ker} f_0)$.

Lemme 21.3.2 *On a $f(N) \subseteq (a)$, pour tout $f \in M^*$.*

Démonstration. Posons $K = \operatorname{Ker} f_0$; on a $M = K \oplus Ae_1$. Alors K^* s'identifie au sous-module

$$e_1^{\perp} = \{g \in M^* \mid g(e_1) = 0\}$$

de M^*, et l'on a $M^* = K^* \oplus Af_0$ (car $f_0(e_1) = 1$). Comme $N = (N \cap K) \oplus Aae_1$, pour prouver le lemme il suffit donc de montrer que $g(N \cap K) \subseteq (a)$ pour tout $g \in K^*$.

Soit $n \in N \cap K$ et soit d le PGCD de a et $g(n)$. Par Bezout, il existe $u, v \in A$ tels que $ua + vg(n) = d$. Alors, posant $f = vg + uf_0$, on a $d = f(n+x) \in f(N)$. D'après le choix de f_0, ceci entraîne, comme précédemment, que a est associé à d donc divise $g(n)$. Ceci prouve le lemme. □

D'après la proposition 21.2.1, le sous-module $\mathrm{Ker}\, f_0$ est libre, disons de rang s. Comme $M \cong \mathrm{Ker}\, f_0 \oplus Ae_1$, alors $n = s + 1$ (car une base de M est obtenue en adjoignant e_1 à une base de $\mathrm{Ker}\, f_0$). Donc $s = n - 1$. Par hypothèse de récurrence, appliquée au sous-module $N \cap \mathrm{Ker}\, f_0$ de $\mathrm{Ker}\, f_0$, on obtient qu'il existe une base $(e_2, \ldots, e_n)$ de $\mathrm{Ker}\, f_0$ et $a_2, \ldots, a_n \in A \setminus \{0\}$, tels que $(a_2e_2, \ldots, a_ne_n)$ soit une base de $N \cap \mathrm{Ker}\, f_0$ et $a_i \mid a_{i+1}$ pour $i = 2, \ldots, r-1$.

Alors, d'après $(*)$, $(e_1, \ldots, e_n)$ est une base de M et $(ae_1, a_2e_2, \ldots, a_ne_n)$ une base de N. Soit $(e_1^*, \ldots, e_n^*)$ la base duale de M^*. Alors a_2 appartient à $e_2^*(N)$ donc est divisible par a, d'après le lemme 21.3.2. Ceci achève la démonstration de l'existence d'une base adaptée.

Maintenant, notons M_1 (resp. M_2) le sous-module de M engendré par $e_1, \ldots, e_r$ (resp., par $e_{r+1}, \ldots, e_n$). On a introduit dans le point 1) du théorème fondamental le sous-module

$$N' = \{x \in A^n \mid \exists a \in A \setminus \{0\} \text{ tel que } ax \in N\}.$$

D'une part, comme $a_ie_i \in N$ pour $i = 1, \ldots, r$, on a $M_1 \subseteq N'$. D'autre part, comme $M = M_1 \oplus M_2$, alors M/M_1 est isomorphe à M_2 et donc libre. Ceci entraîne l'inclusion $N' \subseteq M_1$. En effet, soit $x \in N'$. Il existe $a \in A \setminus \{0\}$ tel que $ax \in N \subseteq M_1$, donc l'image de x dans M/M_1 est un élement de torsion. Comme ce module est libre, donc sans torsion, ceci entraîne $x \in M_1$. Ceci prouve l'égalité $M_1 = N'$. On a ainsi démontré le point 1) du théorème, à l'exception de l'unicité des idéaux $(a_1) \supseteq \cdots \supseteq (a_r)$.

21.4 Décomposition des modules de type fini

Lemme 21.4.1 *Soient B un anneau et $M_1, \ldots, M_n$ des B-modules. Pour $i = 1, \ldots, n$, soit N_i un sous-module de M_i et soit $\pi_i : M_i \to M_i/N_i$. Alors, le noyau du morphisme*

$$\oplus_{i=1}^n M_i \to \oplus_{i=1}^n (M_i/N_i), \quad (x_1, \ldots, x_n) \mapsto (\pi_1(x_1), \ldots, \pi_n(x_n))$$

est le sous-module $\oplus_{i=1}^n N_i$. Par conséquent, on a un isomorphisme :

$$(M_1 \oplus \cdots \oplus M_n)/(N_1 \oplus \cdots \oplus N_n) \cong (M_1/N_1) \oplus \cdots \oplus (M_n/N_n).$$

Démonstration. La première assertion est claire, et la seconde en découle, d'après le Théorème fondamental d'isomorphisme 9.2.5. □

On va maintenant démontrer l'existence des décompositions annoncées dans les points 2) et 3) du théorème fondamental.

Point 2) Soit M un A-module de type fini. Soit $\{x_1, \ldots, x_n\}$ un système de générateurs de M et soit $\phi : A^n \to M$ le morphisme de A-modules envoyant tout $(b_1, \ldots, b_n)$ sur $b_1x_1 + \cdots + b_nx_n$. Alors, ϕ induit un isomorphisme

$$A^n / \operatorname{Ker} \phi \xrightarrow{\sim} M.$$

D'après le point 1) du théorème, il existe une base $(e_1, \ldots, e_n)$ de A^n, un entier $r \leq n$, et des éléments non nuls $a_1, \ldots, a_r$ de A, vérifiant $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r-1$, tels que

$$(a_1e_1, a_2e_2, \ldots, a_re_r)$$

soit une base de $\operatorname{Ker} \phi$. Alors, d'après le lemme précédent, l'on a

$$(*) \qquad M \cong A^n / \ker \phi \cong A/(a_1) \oplus \cdots \oplus A/(a_r) \oplus A^s,$$

où $s = n - r$. Identifions M au terme de droite via ces isomorphismes, et notons alors M' le sous-module $A/(a_1) \oplus \cdots \oplus A/(a_r)$. Il est clair que $M' \subseteq M_{\text{tors}}$. De plus, comme $M/M' \cong A^s$ est sans torsion, on en déduit que $M' = M_{\text{tors}}$ (car sinon tout $m \in M_{\text{tors}}$ tel que $m \notin M'$ serait un élément de torsion non nul dans M/M'). Enfin, il est clair d'après $(*)$ que $\operatorname{Ann} M = (a_r)$. Ceci prouve le point 2), à l'exception de l'unicité des idéaux

$$(a_1) \supseteq \cdots \supseteq (a_r).$$

Point 3) Supposons de plus $M = M_{\text{tors}}$ et soit $(a) = (p_1)^{m_1} \cdots (p_n)^{m_n}$ son annulateur. D'après le théorème 19.2.7, on a

$$M = \bigoplus_{i=1}^{n} M(p_i),$$

et chaque $M(p_i)$ est un A-module de type fini, vérifiant $\operatorname{Ann} M(p_i) = (p_i^{m_i})$.

Fixons un indice i. Comme $M(p_i)$ est de type fini et de torsion, on peut, d'après le point 2), le décomposer en somme directe

$$M(p_i) = \bigoplus_{s=1}^{t_i} A/(a_s), \quad \text{avec } a_s \mid a_{s+1} \text{ pour } s < t_i.$$

Or, d'après le lemme 19.2.5, l'annulateur de tout élément non nul de $M(p_i)$ est une puissance de (p_i). Par conséquent, il existe une suite

$$n_1(p_i) \leq \cdots \leq n_{t_i}(p_i),$$

telle que

$$M(p_i) = \bigoplus_{s=1}^{t_i} A/(p_i)^{n_s(p_i)}.$$

De plus, on a $n_{t_i}(p_i) = m_i$, car sinon l'annulateur de $M(p_i)$ serait contenu dans $(p_i)^{m_i-1}$. Ceci prouve l'existence dans le point 3). □

21.5 Unicité des facteurs invariants

Lemme 21.5.1 *Soient A un anneau intègre et $p \in A \setminus \{0\}$. Pour tout $i \geq 0$, l'application*

$$A \longrightarrow Ap^i/Ap^{i+1}, \quad a \mapsto ap^i + Ap^{i+1}$$

induit un isomorphisme $A/(p) \cong (p^i)/(p^{i+1})$ de $A/(p)$-modules.

Démonstration. Soient $i \geq 0$ et ϕ le morphisme de A-modules $A \to (p^i)/(p^{i+1})$ défini par

$$\phi(a) = ap^i + Ap^{i+1}, \quad \forall a \in A.$$

Il est clairement surjectif. De plus, comme A est intègre, p^{i+1} divise ap^i ssi p divise a. Par conséquent, $\operatorname{Ker}\phi = (p)$ et ϕ induit un isomorphisme de A-modules $A/(p) \cong (p^i)/(p^{i+1})$. C'est aussi un isomorphisme de $A/(p)$-modules, d'après le corollaire 9.6.5. □

Théorème 21.5.2 (Unicité des facteurs invariants) *Soit A un anneau principal et soit M un A-module de torsion de type fini. Soient $a_1, \ldots, a_r$ des éléments non nuls et non inversibles de A vérifiant $a_i \mid a_{i+1}$ pour tout i, et tels que*

$$M \cong \bigoplus_{i=1}^{r} A/(a_i).$$

Les idéaux $(a_1), \ldots, (a_r)$ sont déterminés de façon unique par M ; on les appelle les **idéaux (ou facteurs) invariants** *de M.*

Démonstration. La démonstration se fait en deux étapes. Démontrons d'abord le théorème dans le cas p-primaire, c.-à-d., dans le cas où $M = M(p)$. Dans ce cas, il existe des entiers $n_1 \leq \cdots \leq n_r$ tels que $a_i = p^{n_i}$ pour tout i. Il faut montrer que les n_i sont déterminés par le module M. Pour commencer, observons que $n_r = k$, où (p^k) est l'annulateur de M. De plus, p^{k-1} annule tous les termes $A/(p^{n_i})$ pour lesquels $n_i < k$. D'autre part, $K = A/(p)$ est un

corps, puisque (p) est un idéal maximal. Donc, d'après le lemme précédent, on obtient que

$$p^{k-1}M = \bigoplus_{\substack{i \\ n_i=k}} p^{k-1}A/p^kA,$$

est un espace vectoriel sur K de dimension $\#\{i \mid n_i = k\}$. On obtient de même, pour tout $\ell \leq k$, que

$$\dim_K \left(p^{\ell-1}M/p^\ell M\right) = \#\{i \mid n_i = \ell\}.$$

Ceci montre que la suite (n_i) est uniquement déterminée par le module M. Ceci prouve le théorème dans le cas primaire.

Démontrons maintenant le théorème dans le cas général. Supposons que

$$M \cong \bigoplus_{i=1}^{r} A/(a_i),$$

avec $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r-1$. D'abord, l'idéal (a_r) égale $\operatorname{Ann} M$ donc est déterminé par M. Écrivons

$$a_r = p_1^{v_1(r)} \cdots p_n^{v_n(r)},$$

où les p_j sont des éléments irréductibles deux à deux non associés. Alors, la décomposition en composantes primaires de M est

$$M = \bigoplus_{j=1}^{n} M(p_j).$$

D'autre part, comme chaque a_i divise a_{i+1}, on peut écrire, pour tout $i \leq r$,

$$a_i = p_1^{v_1(i)} \cdots p_n^{v_n(i)}, \tag{1}$$

et l'on a pour tout $j = 1, \ldots, n$:

$$0 \leq v_j(1) \leq \cdots \leq v_j(r). \tag{$*$}$$

Alors, d'après le théorème chinois,

$$A/(a_i) \cong \bigoplus_{j=1}^{n} A/(p_j^{v_j(i)}),$$

et donc

$$M \cong \bigoplus_{j=1}^{n} \bigoplus_{i=1}^{r} A/(p_j^{v_j(i)}). \tag{2}$$

En prenant les composantes primaires dans (2), on obtient, pour tout $j = 1, \ldots, n$:

$$M(p_j) \cong \bigoplus_{i=1}^{r} A/(p_j^{v_j(i)}). \tag{$**$}$$

Or, tenant compte des inégalités $(*)$, on a vu que la décomposition $(**)$ est unique. Par conséquent, les entiers $v_j(i)$ sont entièrement déterminés par M. De plus, en raison de $(*)$, ils déterminent les (a_i) par la formule (1). Ceci achève la démonstration de l'unicité des facteurs invariants. □

On peut maintenant démontrer l'unicité dans le point 1). Soit N un sous-module non nul de $M = A^n$. On a vu qu'il existe une base $(e_1, \ldots, e_n)$ de M, et $a_1, \ldots, a_r \in A \setminus \{0\}$ tels que $(a_1e_1, \ldots, a_re_r)$ soit une base de N, et a_i divise a_{i+1} pour $i = 1, \ldots, r-1$. Il résulte de ce qui précède que les idéaux

$$(a_1) \supseteq \cdots \supseteq (a_r)$$

sont les facteurs invariants de M/N, donc sont entièrement par le sous-module N. Ceci termine la démonstration du théorème fondamental. □

Remarque 21.5.3 1) En fait, pour un anneau commutatif A quelconque, on peut montrer que si un A-module M est isomorphe à une somme directe

$$A/I_1 \oplus \cdots \oplus A/I_r$$

où les I_k sont des idéaux propres de A tels que $I_1 \supseteq \cdots \supseteq I_r$, alors les I_k sont uniquement déterminés par le module M. Voir [BAlg], Chap.VII, §4, Proposition 2.

2) On peut aussi montrer que la suite croissante

$$I_1 \cdots I_r \subseteq I_1 \cdots I_{r-1} \subseteq \cdots \subseteq I_1 I_2 \subseteq I_1$$

est la suite des **idéaux de Fitting** du module M, voir [BM, Chap.V, §§ 1–3], et le théorème 22.2.3 plus loin. De plus, si $I_\ell = (a_\ell)$ pour $\ell = 1, \ldots, r$ et si A est intègre, alors la donnée des idéaux

$$(a_1), (a_1a_2), \ldots, (a_1 \cdots a_r)$$

permet de retrouver les idéaux (a_ℓ), puisque pour tout $a, b \in A \setminus \{0\}$, on a :

$$\{x \in A \mid ax \in (ab)\} = (b).$$

Remarque 21.5.4 Pour l'application du théorème fondamental à l'étude des endomorphismes d'un espace vectoriel de dimension finie, on renvoie à l'excellente exposition donnée dans [BM, Chap.5, §5].

22 Autre approche : réduction des matrices sur un anneau principal

22.1 Une conséquence de l'existence de bases adaptées

Soient $n \geq 1$ et N un sous-module non nul de A^n. D'après la proposition 21.2.1, N est libre de rang $r \leq n$. Soit $(x_1, \ldots, x_r)$ une base arbitraire de N. On peut exprimer les x_j dans la base canonique $(\varepsilon_1, \ldots, \varepsilon_n)$ de A^n sous la forme d'une matrice à r colonnes et n lignes $F \in M_{n,r}(A)$.

Pour tout $s \geq 1$, notons $\mathrm{GL}_s(A)$ le groupe des matrices $s \times s$ inversibles, à coefficients dans A. Alors, effectuer un changement de base dans $N \cong A^r$ (resp. dans A^n), revient à multiplier la matrice précédente F à droite (resp. à gauche) par une matrice inversible $Q \in \mathrm{GL}_r(A)$ (resp. $P \in \mathrm{GL}_n(A)$).

L'existence d'une base de A^n adaptée à N est donc équivalente à l'existence de matrices inversibles $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_r(A)$ telles que

$$PFQ = \begin{pmatrix} a_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & a_r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix},$$

avec $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r-1$.

On peut démontrer ceci par une approche matricielle directe, pour tout $m, n \in \mathbb{N}^*$ et tout $F \in M_{n,m}(A)$, et ceci fournit une autre démonstration, algorithmique, de l'existence d'une base adaptée.

22.2 Réduction des matrices

Définition 22.2.1 *1) On dit que $F, F' \in M_{n,m}(A)$ sont* **équivalentes** *s'il existe $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_m(A)$ telles que $F' = PFQ$.*

2) Pour tout $i \leq \min(m, n)$, on note $\mathbf{J_i(F)}$ l'idéal de A engendré par les mineurs $i \times i$ de F. On convient que $J_0(F) = A$.

3) Le **rang** *de F est le plus grand entier $r \geq 0$ tel que $J_r(F) \neq 0$, c.-à-d., le plus grand entier r tel qu'il existe un mineur $r \times r$ de F qui soit nul.*

Lemme 22.2.2 1) *Soient $F \in M_{n,m}(A)$, $P \in M_n(A)$ et $Q \in M_m(A)$. Pour tout i, on a $J_i(PF) \subseteq J_i(F)$ et $J_i(FQ) \subseteq J_i(F)$.*

2) *Si F et F' sont équivalentes, on a $J_i(F) = J_i(F')$ pour tout i.*

Démonstration. 1) Toute ligne de PF est combinaison linéaire de lignes de F. D'après les propriétés de multilinéarité des déterminants, on en déduit que tout i-mineur de PF est combinaison linéaire de i-mineurs de F. Ceci montre que $J_i(PF) \subseteq J_i(F)$. On obtient de même que $J_i(FQ) \subseteq J_i(F)$.

2) Supposons $F' = PFQ$, avec P et Q inversibles. Alors, on a aussi $F = P^{-1}F'Q^{-1}$. D'après le point 1), on obtient les inclusions $J_i(F') \subseteq J_i(F) \subseteq J_i(F')$, d'où $J_i(F) = J_i(F')$ pour tout i. Le lemme est démontré. □

Théorème 22.2.3 (Réduction des matrices sur A principal)
Soient $m, n \geq 1$ et soit $F \in M_{n,m}(A)$ non nulle. Il existe $a_1, \ldots, a_r \in A$, avec $r \geq 1$, vérifiant $a_i \mid a_{i+1}$ pour $i < r$, et $P \in \mathrm{GL}_n(A)$, $Q \in \mathrm{GL}_m(A)$ tels que

$$PFQ = \begin{pmatrix} a_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & a_r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}.$$

De plus, les idéaux $(a_1), \ldots, (a_r)$ sont entièrement déterminés par les égalités :

$$J_i(F) = \begin{cases} (a_1 \cdots a_i), & \text{pour } i = 1, \ldots, r; \\ 0, & \text{pour } i > r. \end{cases}$$

Ils ne dépendent que de la classe d'équivalence de F, et r est le rang de F.

Démonstration. On va montrer qu'on peut construire de telles matrices P et Q comme produits de matrices très simples, de l'un des trois types décrits ci-dessous. Ceci fournit de plus un procédé algorithmique de réduction de la matrice F à une matrice diagonale de la forme ci-dessus.

Type I : les matrices de permutations Soit $\sigma \in S_n$, le groupe des permutations de $\{1, \ldots, n\}$. On lui associe la matrice $M(\sigma)$, définie par

$$M(\sigma)(f_j) = f_{\sigma(j)}, \tag{1}$$

où $(f_1, \ldots, f_n)$ est la base canonique de A^n. En d'autres termes, $M(\sigma)$ est la matrice dont tous les coefficients a_{ij} sont nuls sauf les coefficients $a_{\sigma(j),j}$ qui valent 1. En utilisant (1), on voit que $M(\sigma)$ est inversible, d'inverse $M(\sigma^{-1})$.

Multiplier $F \in M_{n,m}(A)$ à gauche par une matrice de permtutation $M(\sigma)$ revient à effectuer sur les lignes de F la permutation σ. De même, on voit que multiplier F à droite par une matrice de permutation $M'(\tau)$ (où $\tau \in S_m$), revient à effectuer sur les colonnes la permutation τ^{-1}, c.-à-d., mettre la colonne $\tau(j)$ à la place j.

Type II : les matrices $T_{ij}(\alpha)$ et $T'_{k\ell}(\beta)$ Pour $\alpha, \beta \in A$ et $i \neq j$ dans $\{1, \ldots, n\}$, resp. $k \neq \ell$ dans $\{1, \ldots, m\}$, on pose

$$T_{ij}(\alpha) = I_n + \alpha E_{ij}, \quad \text{resp.} \quad T'_{k\ell}(\beta) = I_m + \beta E_{k\ell},$$

où I désigne la matrice identité, et E_{ij} désigne la matrice élémentaire dont le seul coefficient non nul est celui d'indices (i, j), qui vaut 1.

On voit que multiplier F à gauche par $T_{ij}(\alpha)$ revient à ajouter α fois la ligne j à la ligne i. De même, multiplier F à droite par $T'_{k\ell}(\beta)$ revient à ajouter β fois la colonne k à la colonne ℓ.

On est ainsi équipé pour faire des opérations élémentaires sur la matrice F. On aura besoin d'un 3ème type de matrices.

Type III : les matrices de Bezout $B_i(a, b)$ et $B'_j(a, b)$

Soit $i \in \{2, \ldots, n\}$ et soient $a, b \in A \setminus \{0\}$. Soit d un pgcd de a et b. Comme A est principal, d est un générateur de l'idéal $(a) + (b)$ et donc (Théorème de Bezout), il existe $x, y \in A$ tels que $ax + by = d$. On note $B_i(a, b)$ la matrice (b_{kj}) telle que

$$b_{11} = x, \quad b_{1i} = y, \quad b_{i1} = -\frac{b}{d}, \quad b_{ii} = \frac{a}{d},$$

$b_{kk} = 1$ pour $k \neq 1, i$, et $b_{kj} = 0$ dans les autres cas. C.-à-d., $B_i(a, b)$ est de la forme :

$$\begin{pmatrix} x & 0 & y & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{b}{d} & 0 & \frac{a}{d} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

C'est une matrice inversible, car son déterminant vaut $(ax + by)/d = 1$. De plus, elle vérifie la propriété suivante : si a (resp. b) est le coefficient f_{11} (resp. f_{i1}) de la 1ère colonne de F, alors la 1ère colonne de $B_i(a, b)F$ est identique à celle de F, sauf qu'on a remplacé a par $d = \text{pgcd}(a, b)$ et b par 0. (Ceci explique l'introduction des matrices $B_i(a, b)$).

De même, pour $j \in \{2, \ldots, m\}$, on définit $B'_j(a, b) \in \text{GL}_m(A)$ par

$$b'_{11} = x, \quad b'_{j1} = y, \quad b'_{1j} = -\frac{b}{d}, \quad b'_{jj} = \frac{a}{d},$$

$b'_{kk} = 1$ pour $k \neq 1, j$, et $b'_{kj} = 0$ dans les autres cas. C.-à-d., $B'_j(a,b)$ est de la forme :

$$\begin{pmatrix} x & 0 & -\frac{b}{d} & 0 \\ 0 & 1 & 0 & 0 \\ y & 0 & \frac{a}{d} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Comme précédemment, $B'_j(a,b)$ est de déterminant 1, et vérifie la propriété suivante. Si a (resp. b) est le coefficient f_{11} (resp. f_{1j}) de la 1ère ligne de F, alors la 1ère ligne de $FB'_j(a,b)$ est identique à celle de F, sauf qu'on a remplacé a par $d = \mathrm{pgcd}(a,b)$ et b par 0.

Remarque 22.2.4 Les matrices $T_{1i}(\alpha)$ et $T'_{1\ell}(\beta)$ sont des cas particuliers de matrices de type III. Toutefois, il est commode de les considérer séparément, *cf.* ci-dessous.

Maintenant, on va montrer qu'on peut multiplier F à droite ou à gauche par des matrices de l'un des trois types précédents, afin d'arriver de proche en proche à une matrice D de la forme voulue. Il faut encore introduire une notion de "longueur" de la matrice F : un entier ≥ 0 qui va décroître strictement au cours de la procédure, ce qui assurera que l'algorithme se termine en un nombre fini d'étapes et permet bien d'atteindre une matrice diagonale de la forme voulue.

Définition 22.2.5 *1) Soit $a \in A \setminus \{0\}$. On définit sa* **longueur** *$\ell(a)$ comme le nombre d'éléments irréductibles apparaissant dans sa décomposition en facteurs irréductibles. Ceci est bien défini, puisque A est principal donc factoriel. En particulier, $\ell(a) = 0 \Leftrightarrow a$ est inversible ; et si p est irréductible, $\ell(p^s) = s$ pour tout $s \geq 1$.*

2) Soit $F \in M_{n,m}(A)$, non nulle. On définit $\ell(A)$ comme la plus petite longueur de ses coefficients non nuls.

Fin de la preuve du théorème de réduction des matrices 22.2.3. Soit $F = (f_{ij}) \in M_{n,m}(A)$, non nulle. Soit f_{ij} un coefficient non nul de longueur minimale. Quitte à permuter des lignes et des colonnes, on peut supposer $(i,j) = (1,1)$. On effectue alors l'algorithme suivant.

Étape 1) i) Si f_{11} divise tous les coefficients f_{1k} et f_{k1}, pour $k \geq 2$, on va à l'étape 2) ci-dessous.

ii) S'il existe $k \geq 2$ tel que f_{11} ne divise pas f_{1k}, on multiplie F à droite par $B'_{1k}(f_{11}, f_{1k})$. On annule ainsi le coefficient $(1,k)$, tandis que f_{11} est remplacé par $d = \mathrm{pgcd}(f_{11}, f_{1k})$, qui est de longueur $< \ell(f_{11})$. S'il existe

$k' \neq k$ tel que d ne divise pas $f_{1k'}$, on repète le processus. On arrive ainsi, en au plus $m-1$ opérations, à un matrice équivalente

$$F' = FB',$$

dont la 1ère ligne est $(f'_{11}, 0, \ldots, 0)$, avec $\ell(f'_{11}) < \ell(f_{11})$.

iii) Si f'_{11} divise tous les coefficients de la 1ère colonne de F', on va à l'étape 2) ci-dessous. Sinon, en multipliant F' à gauche par une suite de matrices de Bezout, on obtient une matrice équivalente

$$F'' = BF' = BFB',$$

dont la 1ère colonne est ${}^t(f''_{11}, 0, \ldots, 0)$, avec $\ell(f''_{11}) < \ell(f'_{11})$. En faisant cela, on peut obtenir, à nouveau, des termes non nuls sur la 1ère ligne de F''. Mais ce n'est pas gênant, car la longueur du coefficient d'indice $(1,1)$ décroît strictement à chaque opération. Donc, après un nombre fini ($\leq \ell(F)$) d'opérations de multiplications à droite ou à gauche par des matrices de Bezout, on obtient une matrice équivalente

$$F_1 = B_r \cdots B_1 BFB' B'_1 \cdots B'_s,$$

dont le coefficient d'indice $(1,1)$, appelons-le d_1, divise tous les coefficients de la 1ère ligne et de la 1ère colonne. On peut alors passer à l'étape 2).

Étape 2) Sous les hypothèses précédentes, on peut soustraire à chaque colonne un multiple de la 1ère, pour obtenir une matrice dont la 1ère ligne est $(d_1, 0, \ldots, 0)$. On peut ensuite soustraire à chaque ligne un multiple de la 1ère, de façon à obtenir une matrice de la forme suivante :

$$F'_1 = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix}.$$

Si d_1 divise tous les c_{ij}, on va à l'étape 3). Sinon, si d_1 ne divise pas un certain c_{ij}, on forme la matrice équivalente

$$(I_n + E_{1i})F'_1 = \begin{pmatrix} d_1 & c_{i2} & \cdots & c_{im} \\ 0 & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix},$$

à laquelle on applique l'étape 1). On obtient ainsi une matrice équivalente

$$F_1'' = \begin{pmatrix} d_1' & 0 & \cdots & 0 \\ 0 & c_{22}' & \cdots & c_{2m}' \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2}' & \cdots & c_{nm}' \end{pmatrix},$$

où $\ell(d_1') < \ell(d_1)$ et où d_1' divise tous les coefficients de la ligne i. Si d_1' ne divise pas tous les coefficients d'une autre ligne, on recommence le processus. On obtient ainsi, après un nombre fini ($\leq \min(\ell(d_1), n-1)$) d'aller-retour entre les étapes 1) et 2), une matrice équivalente F_2 de la forme

$$F_2 = \begin{pmatrix} a_1 & 0 \\ 0 & B \end{pmatrix},$$

où a_1 divise chaque coefficient de $B \in M_{n-1,m-1}(A)$. On observe alors que a_1 est un générateur de l'idéal $J_1(F_2)$, qui égale $J_1(F)$ d'après le lemme 22.2.2. On passe alors à l'étape 3)

Étape 3) Par hypothèse de récurrence (ou d'après l'algorithme appliqué à B), il existe P, Q inversibles telles que

$$PBQ = \begin{pmatrix} a_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & a_r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix},$$

où $a_i \mid a_{i+1}$ pour $i = 2, \ldots, r-1$. D'une part, a_2 est un générateur de $J_1(PBQ) = J_1(B)$, lequel est contenu dans $J_1(F_2) = (a_1)$. Par conséquent, a_1 divise a_2. D'autre part, F_2, et donc F, est semblable à la matrice

$$F_3 = \begin{pmatrix} a_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & a_r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}.$$

Ceci achève la démonstration de l'existence dans le théorème 22.2.3. De plus, d'après le lemme 22.2.2, on a pour tout $s \leq \min(m, n)$, $J_s(F) = J_s(F_3)$. Or

ces derniers idéaux se calculent facilement : F_3 est de rang r, et pour $s \leq r$ les seuls mineurs $s \times s$ non nuls sont les produits

$$a_{i_1} \cdots a_{i_s}, \qquad \text{avec } i_1 < \cdots < i_s.$$

Comme $a_i \mid a_{i+1}$, pour $i < r$, chacun de ces produits est multiple de $a_1 \cdots a_s$. Ceci prouve que

$$J_s(F) = (a_1 \cdots a_s), \quad \forall s = 1, \ldots, r.$$

Enfin, comme A est intègre, on voit que $(a_i) = \{x \in A \mid xJ_{i-1}(F) \subseteq J_i(F)\}$. Ceci montre que les idéaux (a_i) sont déterminés par les $J_s(F)$, et donc ne dépendent que de la classe d'équivalence de F. Ceci termine la démonstration du théorème 22.2.3. □

Remarque 22.2.6 Lorsque (A, v) est euclidien, on n'a besoin que des matrices de type I ou II et l'algorithme se simplifie considérablement, *cf.* [Ja1], §3.7, pp. 177-178.

Références citées dans ce chapitre

[BAlg], [BM], [Ja1]

Table des matières

Bibliographie

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1979, et 2ème édition, Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.