Chapitre 6

Modules sur les anneaux principaux

Version du 1er novembre 2004

6.1 Idéaux étrangers et théorème chinois

Soit A un anneau commutatif.

Définition 6.1.1 (Produits d'idéaux de A) *Soient I, J deux idéaux de A. On rappelle que IJ désigne l'idéal engendré par les produits xy, où $x \in I$ et $y \in J$; on vérifie que c'est l'ensemble des sommes finies $\sum_i x_i y_i$, où $x_i \in I$, $y_i \in J$.*

Pour une famille quelconque d'idéaux $I_1, \ldots, I_m$, on définit de même le produit $I_1 \cdots I_m$. En particulier, si $I_1, \ldots, I_m$ sont tous égaux à I, on obtient l'idéal I^m, formé des sommes finies arbitraires de produits de m éléments de I :

$$I^m := \left\{ \sum x_1 \cdots x_m \mid x_i \in I \right\}.$$

Remarque 6.1.1 1) On prendra garde que, en général, I^m n'est pas l'idéal engendré par les puissances m-ièmes d'éléments de I. Par exemple, si $A = k[X, Y]$ (anneau des polynômes en deux variables) et si I est l'idéal engendré par X et Y, alors I^2 est engendré par X^2, XY et Y^2, et XY n'est pas un carré.

2) On a toujours $IJ \subseteq I \cap J$, et l'inclusion est en général stricte (prendre, par exemple, $I = J$).

Soient I, J deux idéaux propres de A. On note $I + J$ l'ensemble des sommes $x + y$, où $x \in I$ et $y \in J$; on voit facilement que c'est un idéal de A, pas nécessairement propre. Par exemple, dans $\mathbb{Z}$, $(2) + (3) = \mathbb{Z}$.

Définition 6.1.2 *Soient $I_1, \ldots, I_n$ des idéaux de A.*

1) On dit que $I_1, \ldots, I_n$ sont étrangers (on dit aussi "premiers entre eux") si l'on a $I_1 + \cdots + I_n = A$.

2) On dit que $I_1, \ldots, I_n$ sont étrangers deux à deux si I_r et I_s sont étrangers, pour tout $r \neq s$.

Remarque 6.1.2 On prendra garde à ne pas confondre ces deux notions. Si $n \geq 3$, la 2ème condition est beaucoup plus forte que la 1ère ! Pour éviter les confusions, on dira parfois dans le 1er cas que $I_1, \ldots, I_n$ sont étrangers "dans leur ensemble"

Lemme 6.1.1 *On suppose que I est étranger à $J_1, \ldots, J_m$ (on ne suppose pas les J_i nécessairement distincts). Alors I est étranger à $J_1 \cdots J_m$.*

Démonstration. Par hypothèse, il existe, pour $i = 1, \ldots, m$, des éléments $x_i \in I$ et $y_i \in J_i$ tels que $x_i + y_i = 1$. Alors

$$1 = \prod_{i=1}^{m} (x_i + y_i),$$

et en développant ce produit on obtient le terme $y_1 \cdots y_m$ qui appartient à $J_1 \cdots J_m$, et une somme de termes qui contiennent au moins un x_i donc appartiennent à I. Ceci prouve le lemme. □

Corollaire 6.1.2 *Supposons $I_1, \ldots, I_n$ étrangers deux à deux, et soient m_1, $\ldots, m_n$ des entiers ≥ 1.*

1) On a $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

2) $I_1^{m_1}, \ldots, I_n^{m_n}$ sont étrangers deux à deux.

3) Posons $J_k = \prod_{j \neq k} I_j^{m_j}$, pour $k = 1, \ldots, n$. Alors, $J_1, \ldots, J_n$ sont étrangers "dans leur ensemble", c.-à-d., on a $J_1 + \cdots + J_n = A$.

Démonstration. Dans 1), il suffit de montrer l'inclusions $\supseteq$, puisque l'autre est évidente. On va prouver les assertions 1) et 2) par récurrence sur n. Supposons d'abord $n = 2$.

Par hypothèse, il existe $x_1 \in I_1$ et $x_2 \in I_2$ tels que $x_1 + x_2 = 1$. Alors, pour tout $a \in I_1 \cap I_2$, l'on a :

$$a = a \cdot 1 = ax_1 + ax_2 \in I_1 I_2,$$

d'où $I_1 I_2 = I_1 \cap I_2$. D'autre part, d'après le lemme précédent, I_1 est étranger à $I_2^{m_2}$, puis $I_2^{m_2}$ est étranger à $I_1^{m_1}$, ce qui prouve 2) dans le cas $n = 2$.

Supposons $n \geq 3$ et les deux assertions établies pour $n-1$. Par hypothèse de récurrence, $I_2 \cap \cdots \cap I_n = I_2 \cdots I_n$, et, d'après le lemme, cet idéal est étranger à I_1. On a donc

$$I_1 \cap \cdots \cap I_n = I_1 \cap (I_2 \cdots I_n) = I_1 \cdot I_2 \cdots I_n,$$

ce qui prouve 1). D'autre part, par hypothèse de récurrence, $I_2^{m_2}, \ldots, I_n^{m_n}$ sont étrangers deux à deux. De plus, d'après le cas $n = 2$, chaque $I_k^{m_k}$ est étranger avec $I_1^{m_1}$. L'assertion 2) est démontrée.

Démontrons l'assertion 3). D'abord, $I_1^{m_1}$,..., $I_r^{m_r}$ sont étrangers deux à deux, d'après l'assertion 2). Donc, sans perte de généralité, on peut se limiter au cas où $m_k = 1$ pour tout k.

Pour chaque k, I_k et J_k sont étrangers, d'après le lemme 6.1.1, donc il existe $x_k \in I_k$ et $y_k \in J_k$ tels que $1 = x_k + y_k$. On obtient donc

$$1 = \prod_{k=1}^{n} (x_k + y_k).$$

Développons le produit : les termes qui contiennent un y_k appartiennent à J_k et donc à $J_1 + \cdots + J_r$; le seul autre terme est $x_1 \cdots x_r$, qui appartient à J_k pour tout k. Ceci montre que $1 \in J_1 + \cdots + J_r$, ce qui termine la preuve du corollaire. □

Remarque 6.1.3 a) On voit facilement que si un idéal premier P contient un produit d'idéaux $J_1 \cdots J_r$, alors il contient l'un des J_k.

b) En utilisant a) et le corollaire 2.9.4 (existence d'idéaux maximaux), on peut démontrer le point 2) du corollaire de façon plus conceptuelle. Supposons en effet qu'il existe $r \neq s$ tels que $I_r^{m_r}$ et $I_s^{m_s}$ ne soient pas étrangers. Alors $I_r^{m_r} + I_s^{m_s}$ est un idéal propre, donc est contenu dans un idéal maximal $\mathfrak{m}$. Comme $\mathfrak{m}$ est premier et contient $I_r^{m_r}$ et $I_s^{m_s}$, il contient I_r et I_s, ce qui contredit l'hypothèse $I_r + I_s = A$.

Définition 6.1.3 (Produits d'anneaux) *Soit $(A_i)_{i \in I}$ une famille d'anneaux. Le groupe abélien $\prod_{i \in I} A_i$ est muni d'une structure d'anneau, où la multiplication est définie coordonnée par coordonnée :*

$$\left(\prod_{i \in I} a_i \right) \left(\prod_{i \in I} b_i \right) = \prod_{i \in I} a_i b_i.$$

L'élément neutre, noté 1, *est la famille* $\underline{1}$ *telle que* $a_i = 1$ *pour toput* $i \in I$. *Si* I *est fini, disons* $I = \{1, \ldots, n\}$, *cet anneau se note*

$$A_1 \times \cdots \times A_n \quad ou \quad A_1 \oplus \cdots \oplus A_n.$$

Théorème 6.1.3 (Théorème chinois des restes)

On suppose $I_1, \ldots, I_n$ *étrangers deux à deux. Alors le morphisme naturel* $\psi : A \to A/I_1 \oplus \cdots \oplus A/I_n$ *induit un isomorphisme*

$$A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} \bigoplus_{r=1}^{n} A/I_r.$$

Démonstration. Il est clair que $\ker \psi = \bigcap_{r=1}^{n} I_r$. On va établir l'isomorphisme annoncé par récurrence sur n. Commençons par remarquer que, pour démontrer la surjectivité de ψ, il suffit de trouver $\varepsilon_1, \cdots, \varepsilon_n \in A$ tels que $\psi(\varepsilon_r) = (0, \ldots, 0, 1, 0, \ldots, 0)$ (où 1 est à la r-ième place), car alors un élément arbitraire

$$(\overline{a_1}, \ldots, \overline{a_n})$$

sera l'image de $a_1\varepsilon_1 + \cdots + a_n\varepsilon_n$.

Supposons $n = 2$. Par hypothèse, il existe $x_1 \in I_1$ et $x_2 \in I_2$ tels que $x_1 + x_2 = 1$. Alors $1 - x_1 = x_2$ appartient à $1 + I_1$ et à I_2 et donc on peut prendre $\varepsilon_1 = 1 - x_1$, et de même $\varepsilon_2 = 1 - x_2$. Ceci prouve le théorème dans le cas $n = 2$.

Supposons $n \geq 3$ et le théorème établi pour $n - 1$. D'une part, d'après le corollaire précédent, $I_2 \cap \cdots \cap I_n$ égale $I_2 \cdots I_n$ et donc est étranger à I_1. Donc, d'après le cas $n = 2$, la projection

$$A \longrightarrow A/I_1 \bigoplus A/(I_2 \cap \cdots \cap I_n)$$

induit un isomorphisme

$$A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} A/I_1 \bigoplus A/(I_2 \cap \cdots \cap I_n). \tag{1}$$

De plus, par hypothèse de récurrence, la projection $A \to \bigoplus_{r=2}^{n} A/I_r$ induit un isomorphisme

$$A/(I_2 \cap \cdots \cap I_n) \xrightarrow{\sim} \bigoplus_{r=2}^{n} A/I_r. \tag{2}$$

En composant les isomorphismes (1) et (2), on obtient l'isomorphisme annoncé. Ceci prouve le théorème. □

6.2 Annulateurs et décomposition de modules

6.2.1 Annulateurs et modules de torsion

Définition 6.2.1 *Soient M un A-module et $m \in M$. On pose*

$$\mathrm{Ann}(m) = \{a \in A \mid am = 0\}, \text{ et } \mathrm{Ann}(M) = \{a \in A \mid \forall x \in M,\, ax = 0\}.$$

Ce sont des idéaux de A. De plus, si $(x_i)_{i\in I}$ est un système de générateurs de M (fini ou infini), on voit facilement que

$$\mathrm{Ann}(M) = \bigcap_{x\in M} \mathrm{Ann}(x) = \bigcap_{i\in I} \mathrm{Ann}(x_i).$$

Définition 6.2.2 *M est un A-module monogène (ou cyclique) s'il peut être engendré par un seul générateur x. Ceci équivaut à dire que $M \cong A/I$, où $I = \mathrm{Ann}(x)$.*

Lemme 6.2.1 *Soient A intègre et M un A-module de torsion de type fini. Alors $\mathrm{Ann}(M) \neq (0)$.*

Démonstration. Soit $x_1, \ldots, x_n$ un système fini de générateurs de M. Comme M est de torsion, $I_k := \mathrm{Ann}(x_k)$ est non nul, pour tout k. Alors $\mathrm{Ann}(M) = I_1 \cap \cdots \cap I_n$ est non nul, car il est contient $I_1 \cdots I_n$, qui est $\neq (0)$ puisque A est intègre. □

Exercice 6.2.1 Le $\mathbb{Z}$-module quotient $\mathbb{Q}/\mathbb{Z}$ est de torsion mais pas de type fini, et l'on a $\mathrm{Ann}(\mathbb{Q}/\mathbb{Z}) = 0$.

Définition 6.2.3 *Soit M un A-module. On note*

$$M_{\mathrm{tors}} = \{m \in M \mid \exists a \in A \setminus \{0\} \text{ tel que } am = 0\}$$

l'ensemble des éléments de torsion de M.

Lemme 6.2.2 *Pour A intègre, M_{tors} est un sous-module de M, appelé le sous-module de torsion, et le module quotient M/M_{tors} est sans torsion.*

Démonstration. Soient $m, m' \in M_{\mathrm{tors}}$ et $b \in A \setminus \{0\}$. Par hypothèse, il existe $a, a' \in A \setminus \{0\}$ tels que $am = 0 = a'm'$. Comme A est intègre, $aa' \neq 0$ et $ba \neq 0$ et donc les égalités

$$0 = (aa')(m - m'), \quad \text{et} \quad (ba)m = 0$$

montrent que $m - m'$ et bm appartiennent à M_{tors}. Ceci prouve la 1ère assertion.

Prouvons la seconde. Soient $m \in M$ et $b \in A \setminus \{0\}$ tels que $b\pi(m) = 0$, où π désigne la projection $M \to M/M_{\text{tors}}$. Alors $bm \in M_{\text{tors}}$, donc il existe $a \in A \setminus \{0\}$ tel que $abm = 0$. Comme $ab \neq 0$ (puisque A est intègre), ceci implique $m \in M_{\text{tors}}$, d'où $\pi(m) = 0$. Le lemme est démontré. □

6.2.2 Décomposition des modules de $\mathcal{I}$-torsion

Soit $\mathcal{I} = (I_\lambda)_{\lambda \in \Lambda}$ une famille d'idéaux de A, deux à deux étrangers. Soit M un A-module.

Définition 6.2.4 *Pour tout $\lambda \in \Lambda$, on pose*

$$M_\lambda := \{m \in M \mid \exists n \geq 1 \text{ tel que } I^n m = 0\};$$

c'est un sous-module de M, qu'on appelle composante λ-primaire de M.

Lemme 6.2.3 *La somme des sous-modules M_λ, pour $\lambda \in \Lambda$, est une somme directe.*

Démonstration. Soient $\lambda_1, \ldots, \lambda_r \in \Lambda$, deux à deux distincts. Supposons qu'on ait une égalité

$$x_1 = x_2 + \cdots + x_r,$$

où $x_k \in M_{\lambda_k}$ pour tout k. Alors, il existe des entiers $n_1, \ldots, n_r \geq 1$ tels que

$$I_k^{n_k} x_k = 0, \qquad \forall k = 1, \ldots, r.$$

Alors $x_1 = x_2 + \cdots + x_r$ est annulé par $I_1^{n_1}$ et par $I_2^{n_2} \cdots I_r^{n_r}$. Or, ces deux idéaux sont étrangers, d'après le corollaire 6.1.2. Ceci entraîne $m_1 = 0$, et le lemme en découle. □

Pour un A-module arbitraire, il peut fort bien arriver que $M_\lambda = (0)$ pour tout $\lambda \in \Lambda$. C'est le cas, par exemple, si A est intègre et M sans torsion !

Définition 6.2.5 *On dira que M est (un A-module) de $\mathcal{I}$-torsion si tout $m \in M$ est annulé par un produit fini*

$$(*) \qquad I_{\lambda_1}^{n_1} \cdots I_{\lambda_r}^{n_r}.$$

Proposition 6.2.4 (Décomposition des modules de $\mathcal{I}$-torsion)
Soit M un A-module de $\mathcal{I}$-torsion. Alors :

1) $$M = \bigoplus\nolimits_{\lambda\in\Lambda} M_\lambda.$$

2) *Si de plus M est de type fini, la somme ci-dessus est une somme finie, c.-à-d., il existe $\lambda_1, \ldots, \lambda_r \in \Lambda$ tels que*

$$M = \bigoplus_{i=1}^{r} M_{\lambda_i},$$

et $M_\lambda = (0)$ si $\lambda \notin \{\lambda_1, \ldots, \lambda_r\}$. De plus, chaque M_{λ_i} est de type fini et est annulé par une certaine puissance $I_{\lambda_i}^{n_i}$ de I_{λ_i}.

Démonstration. 1) On a déjà vu que la somme est directe. Montrons qu'elle vaut M. Soit $m \in M$. Il est annulé par un certain produit fini $(*)$. Pour $k = 1, \ldots, r$, posons

$$J_k = \prod_{j\neq k} I_{\lambda_j}^{n_j}.$$

D'après le corollaire 6.1.2, $J_1, \ldots, J_r$ sont étrangers, donc on peut écrire

$$1 = y_1 + \cdots + y_r,$$

où $y_k \in J_k$. Chaque $y_k m$ est annulé par $I_k^{n_k}$, donc appartient à M_{λ_k}. De plus, on a

$$m = 1 \cdot m = y_1 m + \cdots + y_r m.$$

Ceci prouve la première assertion.

Supposons de plus que M soit engendré par un nombre fini d'éléments $x_1, \ldots, x_n$. Chaque x_i a des composantes $x_{i,\lambda}$ non nulles seulement pour λ dans un ensemble fini d'indices Λ_i. Alors $\Lambda_1 \cup \cdots \cup \Lambda_n$ est un ensemble fini $\{\lambda_1, \ldots, \lambda_r\}$, et l'on a

$$M = \bigoplus_{i=1}^{r} M_{\lambda_i}.$$

En comparant avec 1), on obtient $M_\lambda = (0)$ si λ n'est pas l'un des λ_i. Enfin, chaque M_{λ_i}, étant un quotient de M, est de type fini et est donc annulé par une certaine puissance $I_{\lambda_i}^{n_i}$ de I_{λ_i}. La proposition est démontrée. □

6.2.3 Décomposition primaire des modules de torsion sur un anneau principal

Soit A un anneau principal. On note $\mathcal{P}$ l'ensemble des idéaux (p), où p est irréductible ; ce sont les idéaux maximaux de A. En particulier, les éléments de $\mathcal{P}$ sont deux à deux étrangers. De plus, d'après les résultats du Chapitre 5, A est factoriel et donc tout idéal propre $(a) \neq (0)$ s'écrit de façon unique comme un produit d'éléments de $\mathcal{P}$.

Définition 6.2.6 *1) Soient M un A-module, $\mathfrak{p} \in \mathcal{P}$ et p un générateur de $\mathfrak{p}$. On pose*

$$M(\mathfrak{p}) := \{m \in M \mid \exists n \geq 1 \text{ tel que } \mathfrak{p}^n m = 0\}.$$

C'est un sous-module de M, appelé la composante $\mathfrak{p}$-primaire. On le désignera aussi par $M(p)$, qu'on appellera la composante p-primaire de M.

2) On dit que M est p-primaire s'il est égal à sa composante $\mathfrak{p}$-primaire $M(\mathfrak{p})$.

Lemme 6.2.5 *Soit M un A-module p-primaire. Pour tout $x \in M \setminus \{0\}$, on a $\mathrm{Ann}(x) = (p^n)$, pour un certain $n \geq 1$. De plus, si M est de type fini, on a aussi $\mathrm{Ann}(x) = (p^n)$, pour un certain $n \geq 1$.*

Démonstration. Posons $\mathrm{Ann}(x) = (a)$; c'est un idéal propre, puisque $x \neq 0$. D'autre part, par hypothèse, il existe $t \geq 1$ tel que $p^t x = 0$. Donc $p^t \in (a)$ et donc a divise p^t. Comme p est irréductible, on obtient que a est associé à un certain p^n, avec $n \leq t$. Ceci prouve la 1ère assertion.

Supposons de plus que M soit engendré par des éléments $x_1, \ldots, x_r$. Posons $\mathrm{Ann}(x_i) = (p^{n_i})$, pour tout i. Alors

$$\mathrm{Ann}(M) = \bigcap_{i=1}^{r} \mathrm{Ann}(x_i) = (p^n),$$

où $n = \max(n_1, \ldots, n_r)$. Ceci prouve le lemme. □

Théorème 6.2.6 (Décomposition primaire des modules de torsion sur un anneau principal)

Soit A principal et soit M un A-module de torsion. Alors

1) $$M = \bigoplus_{\mathfrak{p} \in \mathcal{P}} M(\mathfrak{p}).$$

2) *Supposons de plus M de type fini et soit* $\mathrm{Ann}(M) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ *la décomposition de son annulateur en produits d'idéaux maximaux. Alors,*

$$M = \bigoplus_{i=1}^{r} M(\mathfrak{p}_i),$$

et l'on a $\mathrm{Ann}\, M(\mathfrak{p}_i) = \mathfrak{p}_i^{n_i}$*, pour* $i = 1, \ldots, r$.

Démonstration. Puisque tout idéal non nul de A est un produit fini $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, les hypothèses de la proposition 6.2.4 sont satisfaites. On obtient donc le point 1). De plus, si M est de type fini, c'est une somme directe finie

$$M = \bigoplus_{i=1}^{r} M(\mathfrak{p}_i),$$

où chaque $M(\mathfrak{p}_i)$ est de type fini. D'après le lemme précédent, il existe $n_1, \ldots, n_r$ tels que $\mathrm{Ann}\, M(\mathfrak{p}_i) = \mathfrak{p}_i^{n_i}$ pour tout i. Alors, en utilisant le corollaire 6.1.2, on obtient

$$\mathrm{Ann}(M) = \bigcap_{i=1}^{r} \mathfrak{p}_i^{n_i} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}.$$

Ceci prouve la 2ème assertion. Le théorème est démontré. □

Corollaire 6.2.7 (Décomposition des fractions sur un anneau principal ou euclidien)

Soit A principal et K son corps des fractions.

1) *Le A-module K/A est de torsion et se décompose*

$$K/A = \bigoplus_{(p)\in\mathcal{P}} A[\tfrac{1}{p}]/A,$$

où $A[\frac{1}{p}] = \{\frac{a}{p^n} \mid n \geq 1, a \in A\} = \bigcup_{n\geq 0} \frac{1}{p^n} A$.

2) *Si (A, v) est euclidien, tout $x \in A[\frac{1}{p}]$ s'écrit comme une somme finie*

$$(*) \qquad x = a + \sum_{i=1}^{r} \frac{a_i}{p^i},$$

où $a, a_i \in A$ et $v(a_i) < v(p)$ si $a_i \neq 0$. De plus, cette écriture est unique si v vérifie, pour tout $a, b \in A \setminus \{0\}$,

$$(**) \qquad v(a-b) \leq \max\{v(a), v(b)\} \leq v(ab).$$

(Si $a = b$, on convient que $v(a-a) = v(0) = -\infty$).

Démonstration. D'abord, $K/A = \bigoplus_{(p)\in\mathcal{P}}(K/A)(p)$, d'après le théorème précédent. Notons π la projection $K \to K/A$. Pour tout $t \in K$, on a

$$\pi(t) \in (K/A)(p) \Leftrightarrow \exists n \geq 1 \text{ tel que } p^n t = a \in A.$$

L'assertion 1) en découle.

2) On convient que $v(0) = -\infty$. Montrons par récurrence sur n que tout $x \in \frac{1}{p^n}A$ s'écrit

$$x = \sum_{i=0}^{n-1} \frac{a_i}{p^{n-i}} + a_n,$$

où $a_0, \ldots, a_n \in A$ et $v(a_i) < v(p)$ pour $i = 0, \ldots, n-1$. C'est clair si $n = 0$. Supposons $n \geq 1$ et le résultat établi pour $n-1$. Soit $x = a/p^n$, où $a \in A$. Comme (A, v) est euclidien, il existe $a', a_0 \in A$ tels que $a = pa' + a_0$ et $v(a_0) < v(p)$. Alors, d'une part,

$$\frac{a}{p^n} = \frac{a_0}{p^n} + \frac{a'}{p^{n-1}}. \tag{1}$$

D'autre part, par hypothèse de récurrence, il existe $a_1, \ldots, a_n \in A$ tels que $v(a_i) < v(p)$ pour $i = 1, \ldots, n-1$ et

$$\frac{a'}{p^{n-1}} = \sum_{i=1}^{n-1} \frac{a_i}{p^{n-i}} + a_n. \tag{2}$$

En combinant (1) et (2), on obtient le résultat au cran n. Ceci prouve l'existence.

Supposons maintenant que v vérifie la condition $(**)$. Pour montrer l'unicité annoncée, il suffit de montrer que si l'on a une égalité

$$a_0 + a_1 p + \cdots + a_n p^n = b_0 + b_1 p + \cdots + b_n p^n, \tag{3}$$

avec $a_0, b_0, \ldots, a_n, b_n \in A$ et $v(p) > v(a_i), v(b_i)$ pour $i = 0, \ldots, n-1$, alors $a_i = b_i$ pour tout i. Procédons par récurrence sur n. C'est clair si $n = 0$. Supposons $n \geq 1$ et l'assertion établie pour $n-1$. Il résulte de (3) que $a_0 - b_0 = p\alpha$, avec $\alpha \in A$. Si on avait $\alpha \neq 0$, on aurait

$$v(p) \leq v(p\alpha) = v(a_0 - b_0) \leq \max\{v(a_0), v(b_0)\} < v(p),$$

une contradiction. Donc $a_0 = b_0$, et (3) entraîne

$$a_1 + \cdots + a_n p^{n-1} = b_1 + \cdots + b_n p^{n-1}.$$

Par hypothèse de récurrence, on conclut que $b_i = a_i$ pour tout i. Le corollaire est démontré. □

Remarque 6.2.1 L'hypothèse $(**)$ sur v entraîne l'unicité du couple $(q, r) =$ (quotient, reste) dans la division euclidienne, *cf.* la démonstration ci-dessus, et celle de la proposition 5.2.2.

Corollaire 6.2.8 (Décomposition des fractions rationnelles en éléments simples)

Soient k un corps et $k(X)$ le corps des fractions rationnelles (c.-à-d., le corps des fractions de $k[X]$). Notons $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires de $k[X]$. Alors, tout élément $F \in k(X)$ s'écrit de façon unique comme une somme finie

$$F = E + \sum_{P \in \mathcal{P}} \sum_{j \geq 1} \frac{a_{P,j}}{P^j},$$

avec E et les $a_{P,j}$ dans $k[X]$, nuls sauf un nombre fini d'entre eux, et $\deg(a_{P,j}) < \deg P$ pour tout P et j. En particulier, si k est algébriquement clos,

$$F = E + \sum_{\lambda \in k} \sum_{j \geq 1} \frac{a_{\lambda,j}}{(X - \lambda)^j},$$

où $E \in k[X]$ et $a_{\lambda,j} \in k$.

Démonstration. Ceci résulte du corollaire précédent, puisque l'application $\deg : k[X] \setminus \{0\} \to \mathbb{N}$ vérifie l'hypothèse $(**)$. □

Remarque 6.2.2 Dans $\mathbb{Q}$, et a fortiori dans $\mathbb{Q}/\mathbb{Z}$, on a l'égalité

$$\frac{1}{2} - \frac{1}{3} = \frac{2}{3} - \frac{1}{2}.$$

Ceci s'explique par le fait que dans $\mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$ et $\mathbb{Z}[\frac{1}{3}]/\mathbb{Z}$ on a les égalités

$$\frac{1}{2} \equiv -\frac{1}{2} \quad \text{et} \quad -\frac{1}{3} \equiv \frac{2}{3}.$$

La valeur absolue $v : \mathbb{Z} \to \mathbb{N}$ ne vérifie pas la condition $(**)$. En fait, pour la division par un entier $n > 0$, la condition $|r| < n$ ne suffit pas à déterminer uniquement le reste ; on a unicité seulement si l'on impose à r de vérifier $0 \leq r < n$.

6.3 Modules de type fini sur un anneau principal

Dans toute cette section, 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.

6.3.1 Les résultats fondamentaux

Proposition 6.3.1 *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).*

Démonstration. Soit $(e_1, \ldots, e_n)$ une base de M. Pour $i = 1, \ldots, n$, soit M_i le sous-module de M engendré par $e_1, \ldots, e_i$; il est libre de rang i. On va montrer par récurrence sur i que $N_i := N \cap M_i$ est libre de rang $r_i \leq i$. La proposition en résultera, puisque $N = N_n$.

Pour $i = 1$, on a $M_1 = Ae_1 \cong A$. Par conséquent, N_1 est isomorphe à un idéal de A, donc est nul ou bien libre de rang 1. Supposons $i \geq 2$ et l'assertion établie au cran $i - 1$. Soit $\pi_i : M_i \to A$ la i-ème coordonnée, 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} donc est libre de rang $\leq i - 1$. Supposons $J_i = (a) \neq 0$. 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, on a

$$N_i = N_{i-1} \oplus Ax.$$

Il en résulte que N_i est libre, de rang $1 + r_{i-1} \leq i$. Ceci prouve la proposition. □

Théorème 6.3.2 (Théorème fondamental de structure pour les modules de type fini sur un anneau principal)

Soient 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*

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

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

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

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 $\text{Ann}(M) = (p_1)^{m_1} \cdots (p_n)^{m_n}$ la décomposition de $\text{Ann}(M)$ 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 $\text{Ann}\, M(p_i) = (p_i^{m_i})$.

La démonstration du théorème se fera en trois étapes. On va montrer d'abord le point 1), puis l'existence dans les points 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). Ceci fournira une autre démonstration de l'unicité des (a_i) dans le point 1).

Définition 6.3.1 *On dira que la base de M donnée dans le point 1) est adaptée au sous-module N.*

Notation Pour tout $s \geq 1$, on note $\text{GL}_s(A)$ le groupe des matrices $s \times s$ inversibles, à coefficients dans A.

D'après la proposition 6.3.1, N est un sous-module libre de rang $r \leq n$. Soit $(x_1, \ldots, x_r)$ une base de N. On peut exprimer les x_j dans la base canonique $(f_1, \ldots, f_n)$ de A^n sous la forme d'une matrice à r colonnes et n lignes $F \in M_{n,r}(A)$. Effectuer un changement de base dans $N \cong A^r$ (resp.

dans A^n), revient à multiplier F à droite (resp. à gauche) par une matrice inversible $Q \in \mathrm{GL}_r(A)$ (resp. $P \in \mathrm{GL}_n(A)$). L'assertion à démontrer est donc **l'existence** de matrices inversibles P, Q telles que

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

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

On va voir, plus généralement, que ceci est vrai quelques soient $m, n \geq 1$ et $F \in M_{n,m}(A)$.

6.3.2 Réduction des matrices sur un anneau principal

Définition 6.3.2 *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 6.3.3 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 6.3.4 (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 $i \in \{2,\dots,n\}$ 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 $d=\mathrm{pgcd}(a,b)$ et b par 0. (Ceci explique l'introduction des matrices $B_i(a,b)$).

De même, pour $j \in \{2,\dots,m\}$, on définit $B'_j(a,b) \in \mathrm{GL}_m(A)$ 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 6.3.1 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 6.3.3 *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 6.3.4. 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

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

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 6.3.3. 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 6.3.4. De plus, d'après le lemme 6.3.3, 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 6.3.4. □

Remarque 6.3.2 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.

6.3.3 Démonstration du point 1) du théorème fondamental

Comme indiqué précédemment, le théorème 6.3.4 assure l'existence d'une base adaptée. Si $(e'_1, \ldots, e'_n)$ est une autre base de A^n telle que $(a'_1 e_1, \ldots, a'_s e_s)$ soit une base de N, où a'_i divise a'_{i+1}, alors s égale r, le rang de N, et les matrices $n \times r$ dont les coefficients diagonaux sont $a_1, \ldots, a_r$, resp. $a'_1, \ldots, a'_r$ sont équivalentes. Il résulte alors du théorème 6.3.4 que $(a'_i) = (a_i)$ pour tout i. Ceci achève la preuve du point 1), sauf en ce qui concerne le sous-module engendré par $e_1, \ldots, e_r$.

Notons N_1 ce module et N_2 le sous-module engendré par $e_{r+1}, \ldots, e_n$. On a introduit

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

D'une part, comme $a_i e_i \in N$ pour $i = 1, \ldots, r$, on a $N_1 \subseteq N'$. D'autre part, comme $A^n = N_1 \oplus N_2$, alors N/N_1 est isomorphe à N_2 et donc libre. Ceci entraîne l'inclusion $N' \subseteq N_1$. En effet, soit $x \in N'$. Il existe $a \in A \setminus \{0\}$ tel que $ax \in N \subseteq N_1$, donc l'image de x dans N/N_1 est un élement de torsion. Comme ce module est libre, donc sans torsion, ceci entraîne $x \in N_1$. Ceci prouve l'égalité $N_1 = N'$ et achève la démonstration du point 1). □

Exercice 6.3.1 Montrer que le théorème de réduction 6.3.4 se déduit du point 1) du théorème fondamental 6.3.2 (en utilisant le lemme 6.3.3 pour ce qui concerne les idéaux $J_i(F)$).

Remarque 6.3.3 Pour une autre démonstration de l'existence d'une base adaptée, voir [Sa, §1.5] ou [BAlg], Chap. VII, §3, N$^{\text{os}}$ 3 et 4.

6.3.4 Décomposition en somme de modules monogènes

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 défini par $\phi(f_i) = x_i$, où $(f_1, \ldots, f_n)$ désigne la base canonique de A^n. Alors, ϕ induit un isomorphisme

$$(*) \qquad \psi : A^n / \ker \phi \xrightarrow{\sim} M.$$

Identifions M à $A^n / \ker \phi$ via cet isomorphisme. D'après l'assertion 1), 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

$$(a_1 e_1, a_2 e_2, \ldots, a_r e_r)$$

soit une base de $\ker \phi$. Alors, d'après le corollaire 2.6.4, l'on a

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

où $s = n - r$. Notons 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'). La première partie du point 2) en découle. □

Pour démontrer l'unicité des idéaux $(a_1), \ldots, (a_r)$, on va d'abord établir l'existence dans le point 3), et ensuite démontrer l'unicité dans 3) puis 2).

Remarque 6.3.4 Une autre méthode pour démontrer l'unicité est la suivante. On a choisi ci-dessus un système de générateurs $x_1, \ldots, x_n$ de M, donnant lieu à un morphisme surjectif $\psi : A^n \to M$. Ce choix étant fait, il est clair que $(a_1), \ldots, (a_r)$ sont les idéaux invariants du sous-module $\ker \psi \subset A^n$. On peut en fait montrer que ces idéaux ne dépendent que de M, et pas des générateurs choisis. Plus précisément, on peut montrer que les idéaux $(a_1 \ldots a_i)$, pour $i = 1, \ldots, r$ sont les idéaux de Fitting (distincts de A) de M, qui sont définis pour tout module de type fini sur un anneau noethérien, [BM], Chap. V, §§1–3.

Point 3) Soit M un A-module de torsion de type fini et soit $(a) = (p_1)^{m_1} \cdots (p_n)^{m_n}$ son annulateur. D'après le théorème 6.2.6, 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 6.2.1, 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). □

6.3.5 Unicité des facteurs invariants

Lemme 6.3.5 *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, $\ker \phi = (p)$ 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 lemme 2.4.1. □

Théorème 6.3.6 (Unicité des facteurs invariants)
Soient A un anneau principal et 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.

Pour démontrer le théorème dans le cas général, il suffit de démontrer que l'application qui à une décomposition

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

associe la décomposition raffinée

$$M \cong \bigoplus_{i=1}^{n} \bigoplus_{s=1}^{t_i} A/(p_i^s) \tag{2}$$

est injective, c.-à-d., que la décomposition (1) peut-être retrouvée à partir de la décomposition (2). Comme on a vu l'unicité de la seconde, ceci entraînera l'unicité de la première.

Écrivons

$$(a_r) = \prod_{\mathfrak{p}\in\mathcal{P}_0} \mathfrak{p}^{v_\mathfrak{p}(a_r)},$$

où $\mathcal{P}_0$ désigne l'ensemble des idéaux maximaux $\mathfrak{p}$ tels que $v_\mathfrak{p}(a_r) \geq 1$. Comme $(a_r) = \mathrm{Ann}(M)$, cet ensemble est entièrement déterminé, ainsi que les $v_\mathfrak{p}(a_r)$, par M.

Comme $a_i \mid a_{i+1}$, pour tout $i < r$, on a

$$v_\mathfrak{p}(a_1) \leq \cdots \leq v_\mathfrak{p}(a_r), \qquad \forall \mathfrak{p} \in \mathcal{P} \tag{$*$}$$

Par conséquent, pour $i = 1, \ldots, r$, on a :

$$(a_i) = \prod_{\mathfrak{p}\in\mathcal{P}_0} \mathfrak{p}^{v_\mathfrak{p}(a_i)},$$

et donc, d'après le théorème chinois,

$$A/(a_i) \cong \bigoplus_{\mathfrak{p}\in\mathcal{P}_0} A/\mathfrak{p}^{v_\mathfrak{p}(a_i)}.$$

On en déduit que $M = \bigoplus_{\mathfrak{p}\in\mathcal{P}_0} M(\mathfrak{p})$. De plus, tenant compte des inégalités $(*)$, on obtient que chaque $M(\mathfrak{p})$, pour $\mathfrak{p} \in \mathcal{P}_0$, se décompose, comme dans l'assertion 3) du théorème fondamental 6.3.2, de la façon suivante :

$$(**) \qquad M(\mathfrak{p}) = A/\mathfrak{p}^{n_1(\mathfrak{p})} \oplus \cdots \oplus A/\mathfrak{p}^{n_r(\mathfrak{p})},$$

où $n_1(\mathfrak{p}) = v_\mathfrak{p}(a_1) \leq \cdots \leq n_r(\mathfrak{p}) = v_\mathfrak{p}(a_r)$.

Réciproquement, on a vu que la décomposition $(**)$ est unique, et de plus la donnée des $n_i(\mathfrak{p})$, pour $\mathfrak{p} \in \mathcal{P}_0$ et $i = 1, \ldots, r$, détermine les idéaux (a_i) puisque

$$(a_i) = \prod_{\mathfrak{p}\in\mathcal{P}_0} \mathfrak{p}^{n_i(\mathfrak{p})}.$$

Ceci achève la preuve du théorème d'unicité. □

Remarque 6.3.5 D'après le théorème précédent les idéaux (a_i) associés au sous-module $N \subset A^n$ sont les idéaux invariants du quotient A^n/N. Ceci fournit une autre démonstration de l'unicité dans le point 1) du théorème fondamental.

Remarque 6.3.6 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 $I_1 \subseteq \cdots \subseteq I_r$, 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

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

est la suite des idéaux de Fitting du module M, voir [BM], Chap.V, §§ 1–3. De plus, si $I_k = (a_k)$ pour tout k et si A est intègre, la donnée des idéaux

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

permet de retrouver les idéaux (a_k), puisque $\{x \in A \mid ax \in (ab)\} = (b)$ pour tout $a, b \in A \setminus \{0\}$.

Table des matières

1 Anneaux, idéaux, localisation **1**

1.1 Anneaux et corps 1
1.2 Idéaux, idéaux premiers et maximaux 3
1.3 Anneaux quotients 5
1.3.1 Anneaux non-commutatifs et idéaux bilatères 8
1.4 Anneaux de fractions, localisation 9
1.4.1 Le cas intègre 9
1.4.2 Le cas général 12

2 Modules et produit tensoriel **15**

2.1 Modules : définitions 15
2.2 Modules quotients 18
2.3 Modules de type fini 19
2.4 Modules quotients associés à un idéal bilatère 21
2.5 Groupes ou modules d'homomorphismes 23
2.5.1 Applications à valeurs dans un A-module 24
2.5.2 Morphismes de A-modules 24
2.6 Produits et sommes directes 25
2.7 A-modules libres et A-modules sans torsion 30
2.8 A-modules libres de type fini, invariance du rang 34
2.9 Lemme de Zorn et existence de sous-modules maximaux . . . 36
2.9.1 Le lemme de Zorn 36
2.9.2 Sous-modules maximaux des modules de type fini . . . 37
2.10 Produit tensoriel 38
2.10.0 Remarque préliminaire 39
2.10.1 Applications bilinéaires 39
2.10.2 Définition du produit tensoriel 41
2.10.3 Propriétés du produit tensoriel 43

3 Algèbres, polynômes, algèbres de type fini **49**
3.1 Algèbres et extension des scalaires 49
3.1.1 Algèbres 49
3.1.2 Extension et restriction des scalaires 49
3.1.3 Localisation de modules 51
3.1.4 Produit tensoriel de A-algèbres 52
3.2 Algèbres de polynômes et algèbres de type fini 53
3.2.1 Monoïdes et algèbres associées 53
3.2.2 Algèbres de polynômes 55
3.2.3 Algèbres de type fini 56

4 Anneaux et modules noethériens **57**
4.1 Modules noethériens 57
4.2 Anneaux noethériens 59
4.3 Le théorème de transfert de Hilbert 60
4.4 Un résultat d'Artin et Tate 61
4.5 Divisibilité, éléments irréductibles 62

5 Anneaux euclidiens, principaux, factoriels **65**
5.1 Anneaux principaux et anneaux euclidiens 65
5.2 Propriétés de l'anneau $A[X]$ 66
5.3 Anneaux factoriels 67
5.3.1 Anneaux factoriels, lemmes d'Euclide et Gauss 67
5.3.2 Les anneaux principaux sont factoriels 70
5.4 Valuations, PGCD et PPCM 71
5.4.1 Valuations 71
5.4.2 PPCM et PGCD 73
5.4.3 Le théorème de Bezout 74
5.5 Le théorème de transfert de Gauss 75
5.5.1 Énoncé du théorème 75
5.5.2 Contenu d'un polynôme 76
5.5.3 Preuve du théorème de transfert de Gauss 78

6 Modules sur les anneaux principaux **79**
6.1 Idéaux étrangers et théorème chinois 79
6.2 Annulateurs et décomposition de modules 83
6.2.1 Annulateurs et modules de torsion 83
6.2.2 Décomposition des modules de $\mathcal{I}$-torsion 84
6.2.3 Décomposition primaire des modules de torsion sur un anneau principal 86

6.3 Modules de type fini sur un anneau principal 89
6.3.1 Les résultats fondamentaux 90
6.3.2 Réduction des matrices sur un anneau principal 92
6.3.3 Démonstration du point 1) du théorème fondamental . 98
6.3.4 Décomposition en somme de modules monogènes . . . 98
6.3.5 Unicité des facteurs invariants 100

Bibliographie

[] Voici une bibliographie provisoire (elle aussi en évolution au fil du texte).

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[Bla] A. Blanchard, Les corps non commutatifs, P.U.F., 1972.

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

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

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

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, tome 1/Algèbre, Cedic Fernand Nathan, 1977.

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

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

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[Kri] J.-L. Krivine, Théorie des ensembles, Cassini, 1998.

[Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.

[La] S. Lang, Algebra, Addison-Wesley, 1965.

[Laf] J.-P. Lafon, Les formalismes fondamentaux de l'algèbre commutative, Hermann, 1974.

[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.

[SD] H.P.F. Swinnerton-Dyer, A brief guide to algebraic number theory, C.U.P., 2001.