

IV. THÉORÈME CHINOIS ET APPLICATIONS, MODULES SUR LES ANNEAUX PRINCIPAUX

Séances des 30, 31 octobre et 6 novembre

12. Théorème chinois et applications

12.1. Idéaux étrangers. — Soient A un anneau commutatif et I_1, \dots, I_m des idéaux de A , non nécessairement distincts. Commençons par rappeler les définitions suivantes, déjà vues dans le §3.3.

Définition 12.1 (Sommes et produits d'idéaux). — 1) On note $I_1 + \dots + I_m$ l'idéal formé des sommes $x_1 + \dots + x_m$, où $x_j \in I_j$ pour $j = 1, \dots, m$.

2) On note $I_1 \cdots I_m$ l'idéal engendré par les produits $x_1 \cdots x_m$, où $x_j \in I_j$ pour $j = 1, \dots, m$. C'est l'ensemble des sommes finies de tels produits.

3) On observe que si chaque I_j est principal, c.-à-d., $I_j = (a_j)$, alors $I_1 \cdots I_m$ est l'idéal engendré par $a_1 \cdots a_m$.

4) Si I_1, \dots, 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 12.2. — 1) On prendra garde que, en général, I^m est strictement plus grand que l'idéal engendré par les puissances m -ièmes d'éléments de I . Par exemple, si $A = \mathbb{R}[X, Y]$ 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 $I_1 \cdots I_m \subseteq I_1 \cap \dots \cap I_m$, et l'inclusion est en général stricte (prendre, par exemple, $I_j = (a)$, pour tout j).

⁽⁰⁾Version du 2/11/06

Définition 12.3 (Idéaux étrangers). — Soient I_1, \dots, I_n des idéaux de A .

1) On dit que I_1, \dots, I_n sont **étrangers** (ou « premiers entre eux ») si l'on a $I_1 + \dots + I_n = A$.

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

Remarque 12.4. — On prendra garde à ne pas confondre ces deux notions. Si $n \geq 3$, la deuxième condition est beaucoup plus forte que la première! Pour éviter les confusions, on dira parfois dans le premier cas que I_1, \dots, I_n sont étrangers « dans leur ensemble ».

Lemme 12.5. — On suppose que I est étranger à J_1, \dots, 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 $i = 1, \dots, m$, 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. \square

Corollaire 12.6. — Supposons I_1, \dots, I_n étrangers deux à deux, et soient m_1, \dots, m_n des entiers ≥ 1 .

- 1) On a $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.
- 2) $I_1^{m_1}, \dots, I_n^{m_n}$ sont étrangers deux à deux.
- 3) Posons, pour $k = 1, \dots, n$,

$$J_k = \prod_{j \neq k} I_j^{m_j}; \quad \text{alors} \quad J_1 + \cdots + J_n = A,$$

c.-à-d., J_1, \dots, J_n sont étrangers « dans leur ensemble ».

Démonstration. — Dans 1), il suffit de montrer l'inclusion \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, $I_2^{m_2}, \dots, I_n^{m_n}$ 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, $I_1^{m_1}, \dots, I_r^{m_r}$ 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 12.5, 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. \square

Remarque 12.7. — 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 5.18 (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 $I_r + I_s = A$.

12.2. Théorème chinois des restes. —

Définition 12.8 (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 :

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i b_i)_{i \in I}$$

L'élément neutre, noté 1, est la famille $(a_i)_{i \in I}$ telle que $a_i = 1$ pour tout $i \in I$. Si I est fini, disons $I = \{1, \dots, n\}$, cet anneau se note

$$A_1 \times \cdots \times A_n \quad \text{ou} \quad A_1 \oplus \cdots \oplus A_n.$$

Théorème 12.9 (Théorème chinois des restes). — On suppose I_1, \dots, I_n étrangers deux à deux. Alors le morphisme naturel $\psi : A \rightarrow A/I_1 \oplus \dots \oplus A/I_n$ induit un isomorphisme

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

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

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

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

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'après le lemme 12.5 et le corollaire 12.6, $I_2 \cap \dots \cap I_n$ égale $I_2 \cdots I_n$ et est étranger à I_1 . Donc, d'après le cas $n = 2$, la projection

$$A \longrightarrow A/I_1 \oplus A/(I_2 \cap \dots \cap I_n)$$

induit un isomorphisme

$$(1) \quad A/(I_1 \cap \dots \cap I_n) \xrightarrow{\sim} A/I_1 \oplus A/(I_2 \cap \dots \cap I_n).$$

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

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

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

12.3. Annulateurs et modules de torsion. — Soit M un A -module.

Définition 12.10 (Annulateurs). — Soit $m \in M$. On pose :

$$\begin{aligned} \text{Ann}(m) &= \{a \in A \mid am = 0\}, \\ \text{Ann}(M) &= \{a \in A \mid \forall x \in M, ax = 0\}. \end{aligned}$$

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

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

Définition 12.11. — M est un A -module **de torsion** si $\text{Ann}(m) \neq (0)$, pour tout $m \in M$.

Lemme 12.12. — *Supposons A intègre et soit M un A -module de torsion et de type fini. Alors $\text{Ann}(M) \neq (0)$.*

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

Exercice 12.13. — Le \mathbb{Z} -module quotient \mathbb{Q}/\mathbb{Z} est de torsion mais pas de type fini, et l'on a $\text{Ann}(\mathbb{Q}/\mathbb{Z}) = 0$.

Définition 12.14. — Soit M un A -module. On note

$$M_{\text{tors}} = \{m \in M \mid \text{Ann}(m) \neq (0)\}$$

l'ensemble des éléments de torsion de M . On dit que M est **sans torsion** si $M_{\text{tors}} = (0)$.

Définition et proposition 12.15 (Sous-module de torsion). — *Si A est intègre, alors :*

- 1) M_{tors} est un sous-module de M , appelé le **sous-module de torsion**.
- 2) Le module quotient M/M_{tors} est sans torsion.

Démonstration. — Soient $m, m' \in M_{\text{tors}}$ 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 $0 = (aa')(m - m')$ et $(ba)m = 0$ montrent que $m - m'$ et bm appartiennent à M_{tors} . Ceci prouve 1).

Prouvons 2). Soient $m \in M$ et $b \in A \setminus \{0\}$ tels que $b\pi(m) = 0$, où π désigne la projection $M \rightarrow M/M_{\text{tors}}$. 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 $\pi(m) = 0$. La proposition est démontrée. \square

12.4. Modules se décomposant en composantes primaires. — Soit $\mathcal{I} = (I_\lambda)_{\lambda \in \Lambda}$ une famille d'idéaux de A , **deux à deux étrangers**. Soit M un A -module.

Définition 12.16. — Pour tout $\lambda \in \Lambda$, on pose

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

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

Lemme 12.17. — *La somme des sous-modules M_λ , pour $\lambda \in \Lambda$, est une somme directe.*

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

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

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

$$I_{\lambda_k}^{n_k} x_k = 0, \quad \text{pour } k = 1, \dots, r.$$

Alors $x_1 = x_2 + \dots + x_r$ est annulé par $I_{\lambda_1}^{n_1}$ et par $I_{\lambda_2}^{n_2} \dots I_{\lambda_r}^{n_r}$. Or, ces deux idéaux sont étrangers, d'après le corollaire 12.6. Ceci entraîne $m_1 = 0$, et le lemme en découle. \square

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 12.18. — On dira que M est un A-module **de \mathcal{I} -torsion** si tout $m \in M$ est annulé par un produit fini

$$(*) \quad I_{\lambda_1}^{n_1} \dots I_{\lambda_r}^{n_r}.$$

Théorème 12.19 (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, et soit M un A-module **de \mathcal{I} -torsion**. Alors :

$$1) \quad M = \bigoplus_{\lambda \in \Lambda} M_\lambda.$$

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

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

et $M_\lambda = (0)$ si $\lambda \notin \{\lambda_1, \dots, \lambda_r\}$. 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 $k = 1, \dots, r$, posons

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

D'après le corollaire 12.6, J_1, \dots, J_r sont étrangers, donc on peut écrire

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

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

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

Ceci prouve la première assertion.

Supposons de plus que M soit engendré par un nombre fini d'éléments x_1, \dots, 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 $\Lambda_1 \cup \dots \cup \Lambda_n$ est un ensemble fini $\{\lambda_1, \dots, \lambda_r\}$, 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 annihilé par une certaine puissance $I_{\lambda_i}^{m_i}$ de I_{λ_i} . Le théorème est démontré. \square

Exemples 12.20. — 1) Dans le paragraphe suivant on déduira du théorème précédent un théorème de structure pour les modules de torsion sur un anneau principal.

2) Voici un autre exemple important. Soit k un corps et soit A une k -algèbre **de dimension finie**. Alors, on peut montrer que A n'a qu'un nombre fini d'idéaux premiers, tous maximaux : $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ et qu'il existe des entiers $m_i \geq 1$ tels que

$$(0) = \mathfrak{m}_1^{m_1} \dots \mathfrak{m}_r^{m_r} = \mathfrak{m}_1^{m_1} \cap \dots \cap \mathfrak{m}_r^{m_r}.$$

Donc, A est un A -module de \mathcal{S} -torsion, où

$$\mathcal{S} = \{\mathfrak{m}_1^{m_1}, \dots, \mathfrak{m}_r^{m_r}\}.$$

Il résulte donc du théorème précédent que

$$A = \bigoplus_{i=1}^r A_i, \quad \text{où } A_i = \{a \in A \mid a \mathfrak{m}_i^{m_i} = 0\}.$$

D'autre part, on peut aussi montrer (cf. Problème 2) que chaque A_i est isomorphe au localisé $A_{\mathfrak{m}_i}$ et l'on obtient un isomorphisme d'anneaux

$$A \cong A_{\mathfrak{m}_1} \times \dots \times A_{\mathfrak{m}_r}.$$

(Une k -algèbre de dimension finie est le produit de ses localisés en ses idéaux maximaux.)

12.5. Décomposition primaire des modules de torsion sur un anneau principal. — Soit A un anneau principal.

Définition 12.21 (Idéaux maximaux de A). — Notons \mathcal{P} l'ensemble des idéaux (p) , où p est irréductible; ce sont les idéaux maximaux de A (Th. 11.32). En particulier, les éléments de \mathcal{P} sont deux à deux étrangers.

Remarque 12.22. — \mathcal{P} est en bijection avec l'ensemble des classes d'équivalence d'éléments irréductibles de A , pour la relation $p \sim p'$ si p et p' sont associés.

Lemme 12.23. — *Tout idéal propre $I \neq (0)$ s'écrit de façon unique comme un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ d'éléments de \mathcal{P} .*

Démonstration. — Soit a un générateur de I et $a = p_1 \cdots p_n$ sa décomposition en facteurs irréductibles. Posant $\mathfrak{p}_i = (p_i)$, on obtient

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n = (p_1) \cdots (p_n) = (a).$$

Ceci prouve l'existence. D'autre part, supposons

$$(*) \quad (a) = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

avec $\mathfrak{q}_i \in \mathcal{P}$. Alors $\mathfrak{q}_i = (q_i)$, avec q_i irréductible, et $(*)$ entraîne :

$$a = u q_1 \cdots q_s, \quad \text{avec } u \text{ inversible.}$$

L'unicité de la décomposition en facteurs irréductibles entraîne que $s = n$ et que, quitte à renuméroter, q_i et p_i sont associés, c.-à-d., $(q_i) = (p_i)$, pour $i = 1, \dots, n$. Ceci prouve l'unicité. \square

Définition 12.24 (Composantes primaires). — 1) Soient M un A -module et $p \in A$ un élément irréductible. On pose

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

C'est un sous-module de M_{tors} , appelé la **composante p -primaire**.

2) On dit que M est **p -primaire** s'il est égal à $M(p)$.

3) Soit $\mathfrak{p} = (p)$. On désignera aussi $M(p)$ par $M(\mathfrak{p})$ et l'on dira que c'est la composante **\mathfrak{p} -primaire** de M .

Lemme 12.25. — *Soit M un A -module p -primaire.*

1) *Pour tout $x \in M \setminus \{0\}$, on a $\text{Ann}(x) = (p^n)$, pour un certain $n \geq 1$.*

2) *Si M est de type fini, alors $\text{Ann}(M) = (p^n)$, pour un certain $n \geq 1$.*

Démonstration. — Posons $\text{Ann}(x) = (a)$; 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 $1 \leq n \leq t$. Ceci prouve la première assertion.

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

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

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

Lemme 12.26. — *Soit M un A -module. La somme des sous-modules $M_{\mathfrak{p}}$, pour $\mathfrak{p} \in \mathcal{P}$, est une somme directe.*

Démonstration. — C'est une conséquence du lemme 12.17. Répétons la démonstration, pour la commodité du lecteur.

Soient $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P}$, deux à deux distincts. Supposons qu'on ait une égalité

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

où $x_k \in M_{\mathfrak{p}_k}$ pour tout k . Il existe des entiers $n_1, \dots, n_r \geq 1$ tels que

$$\mathfrak{p}_k^{n_k} x_k = 0, \quad \text{pour } k = 1, \dots, r.$$

Alors $x_1 = x_2 + \dots + x_r$ est annulé par $\mathfrak{p}_1^{n_1}$ et par $\mathfrak{p}_2^{n_2} \dots \mathfrak{p}_r^{n_r}$. Or, ces deux idéaux sont étrangers, d'après le corollaire 12.6. Ceci entraîne $x_1 = 0$, et le lemme en découle. \square

Théorème 12.27 (Décomposition primaire des modules de torsion sur un anneau principal)

Soient A un anneau principal et 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 $\text{Ann}(M) = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$ la décomposition de son annulateur en produits d'idéaux maximaux. Alors,

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

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

Démonstration. — Ceci découle du théorème 12.19, combiné avec le lemme 12.25. Pour la commodité du lecteur, répétons la démonstration, sans faire référence au théorème 12.19.

1) On a déjà vu que la somme des $M(\mathfrak{p})$ est directe. Montrons qu'elle vaut M . Soit $m \in M$, non nul. Comme M est de torsion, $\text{Ann}(m)$ est non nul donc, d'après le lemme 12.23, on a

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$$

où $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P}$ sont deux à deux distincts. Pour $k = 1, \dots, r$, posons

$$J_k = \prod_{j \neq k} \mathfrak{p}_j^{n_j}.$$

D'après le corollaire 12.6, les idéaux J_1, \dots, J_r sont étrangers dans leur ensemble, donc on peut écrire

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

avec $y_k \in J_k$. Chaque $y_k m$ est annulé par $\mathfrak{p}_k^{n_k}$, donc appartient à $M(\mathfrak{p}_k)$. De plus, on a

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

Ceci prouve 1).

2) Supposons de plus que M soit engendré par un nombre fini d'éléments x_1, \dots, x_n . Chaque x_i a des composantes $x_{i,\mathfrak{p}}$ non nulles seulement pour \mathfrak{p} dans un sous-ensemble fini \mathcal{P}_i de \mathcal{P} . La réunion de ces sous-ensembles est un sous-ensemble fini $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ de \mathcal{P} , et l'on a

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

De plus, chaque $M(\mathfrak{p}_i)$, étant un quotient de M , est de type fini, donc $\text{Ann } M(\mathfrak{p}_i) = \mathfrak{p}_i^{n_i}$, pour un certain $n_i \geq 1$, d'après le lemme 12.25.

Par conséquent, $\text{Ann}(M) = \bigcap_{i=1}^r \mathfrak{p}_i^{n_i}$, et comme les \mathfrak{p}_i sont deux à deux étrangers, on obtient

$$\text{Ann}(M) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}.$$

Ceci achève la preuve du point 2). Le théorème est démontré. \square

Corollaire 12.28 (Décomposition des fractions sur un anneau principal ou euclidien)

Soient A un anneau principal et K son corps des fractions.

1) *Le A -module K/A est de torsion et sa décomposition primaire est la suivante :*

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

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 est euclidien, relativement à $\rho : A \setminus \{0\} \rightarrow \mathbb{N}$, alors tout $x \in A[\frac{1}{p}]$ s'écrit comme une somme finie*

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

où $a, a_i \in A$ et $\rho(a_i) < \rho(p)$ si $a_i \neq 0$. De plus, cette écriture est **unique** si ρ vérifie la condition ci-dessous :

$$(**) \quad \rho(a - b) \leq \max\{\rho(a), \rho(b)\} \leq \rho(ab), \quad \forall a, b \in A \setminus \{0\}.$$

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

Démonstration. — D'abord, $K/A = \bigoplus_{(p) \in \mathcal{P}} (K/A)(p)$, d'après le théorème précédent. Notons π la projection $K \rightarrow K/A$. 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 $\rho(0) = -\infty$. 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 $a_0, \dots, a_n \in A$ et $\rho(a_i) < \rho(p)$ pour $i = 0, \dots, n-1$. 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, ρ) est euclidien, il existe $a', a_0 \in A$ tels que $a = pa' + a_0$ et $\rho(a_0) < \rho(p)$. Alors, d'une part,

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

D'autre part, par hypothèse de récurrence, il existe $a_1, \dots, a_n \in A$ vérifiant $\rho(a_i) < \rho(p)$ et

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

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

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

$$(3) \quad a_0 + a_1p + \dots + a_np^n = b_0 + b_1p + \dots + b_np^n,$$

avec $a_0, b_0, \dots, a_n, b_n \in A$ et $\rho(p) > \rho(a_i), \rho(b_i)$ pour $i = 0, \dots, n-1$, 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

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

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

$$a_1 + \dots + a_np^{n-1} = b_1 + \dots + b_np^{n-1}.$$

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

Remarque 12.29. — L'hypothèse (**) sur ρ entraîne l'unicité du quotient et du reste dans la division euclidienne, cf. la démonstration ci-dessus.

Corollaire 12.30 (Décomposition des fractions rationnelles en éléments simples)

Soient k un corps et $k(X)$ le corps des fractions rationnelles sur k . Notons \mathcal{P} l'ensemble des polynômes irréductibles unitaires de $k[X]$.

1) 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 pour un nombre fini d'indices, et $\deg(a_{P,j}) < \deg P$ pour tout P et j .

2) En particulier, si k est algébriquement clos, disons si $k = \mathbb{C}$, alors

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

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

3) Si $k = \mathbb{R}$, tout $F \in \mathbb{R}(X)$ se décompose en :

$$F = E + \sum_{\lambda \in \mathbb{R}} \sum_{j \geq 1} \frac{a_{\lambda,j}}{(X - \lambda)^j} + \sum_{\substack{b,c \in \mathbb{R} \\ b^2 < 4c}} \sum_{j \geq 1} \frac{\alpha_{(b,c),j} X + \beta_{(b,c),j}}{(X^2 - bX + c)^j}$$

où $E \in \mathbb{R}[X]$ et $a_{\lambda,j}, \alpha_{(b,c),j}, \beta_{(b,c),j} \in \mathbb{R}$.

Démonstration. — Le point 1) résulte du corollaire précédent, puisque l'application $\deg : k[X] \setminus \{0\} \rightarrow \mathbb{N}$ vérifie l'hypothèse (**).

Alors, les points 2) et 3) découlent de la description des polynômes irréductibles unitaires sur \mathbb{C} , resp. sur \mathbb{R} . \square

Remarque 12.31. — 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 $\mathbb{Z} \rightarrow \mathbb{N}$ ne vérifie pas la condition (**) car, par exemple $|-1 - 1| = 2 > \max\{|-1|, |1|\}$. De même, dans la division euclidienne 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 $0 \leq r < n$.

13. Modules de type fini sur un anneau principal

13.1. Rang d'un module libre de type fini. — Dans ce paragraphe, A est un anneau commutatif $\neq (0)$ arbitraire. Soit M un A -module de type fini. Commençons par l'observation suivante.

Lemme 13.1. — Si M est un A -module libre, alors toute base de M est formée d'un nombre fini d'éléments.

Démonstration. — Soient x_1, \dots, 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, \dots, 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. \square

Donc, tout A -module libre de type fini est de la forme A^n , pour un certain $n \geq 1$. L'entier n est entièrement déterminé, d'après la proposition suivante.

Proposition 13.2. — Soit A un anneau commutatif $\neq 0$. Si l'on a un isomorphisme de A -modules $A^m \xrightarrow{\sim} A^n$, alors $m = n$.

Démonstration. — Supposons qu'il existe des isomorphismes réciproques :

$$A^m \xrightarrow{\phi} A^n \xrightarrow{\psi} A^m.$$

Soient (e_1, \dots, e_m) et (f_1, \dots, f_n) les bases standard de A^m et A^n . Alors ϕ et ψ sont représentés par des matrices

$$P \in M_{n,m}(A), \quad Q \in M_{m,n}(A)$$

et l'on a

$$(*) \quad QP = I_m \quad \text{et} \quad PQ = I_n.$$

Comme A est un anneau commutatif $\neq 0$, il possède un idéal maximal \mathfrak{m} et le quotient A/\mathfrak{m} est un corps k . Soit π la projection $A \rightarrow k$. Pour toute matrice $C \in M_{r,s}(A)$, notons $\pi(C)$ la matrice dont les coefficients sont les $\pi(c_{i,j})$; on dit que $\pi(C)$ est obtenue (à partir de C) par **réduction modulo \mathfrak{m}** . On voit facilement que la réduction commute au produit des matrices, c.-à-d., pour tout $C' \in M_{s,t}(A)$ on a l'égalité suivante dans $M_{s,t}(k)$:

$$\pi(CC') = \pi(C)\pi(C').$$

Par conséquent, $(*)$ entraîne $\pi(P)\pi(Q) = I_n$ et $\pi(Q)\pi(P) = I_m$; donc $\pi(P)$ induit un isomorphisme

$$k^m \xrightarrow{\sim} k^n,$$

donc ces deux k -espaces vectoriels ont même dimension, d'où $m = n$. \square

Définition 13.3. — Soit $M \neq (0)$ un A -module libre de type fini. L'unique entier n tel que $M \cong A^n$ s'appelle le **rang** de M et se note $\text{rang } M$.

Alors, toute base de M est formée de n éléments. On a, de plus, la caractérisation suivante du rang.

Théorème 13.4 (Rang d'un module libre de type fini). — Soit $M \neq (0)$ un A -module libre de type fini.

1) Soient \mathfrak{m} un idéal maximal de A et $k = A/\mathfrak{m}$. Alors,

$$\text{rg } M = \dim_k M \otimes_A k = \dim_k M/\mathfrak{m}M.$$

2) Si A est intègre, soit K son corps des fractions. Alors

$$\text{rg } M = \dim_K M \otimes_A K.$$

Démonstration. — Posons $n = \text{rg } M$. Alors, $M \cong A^n$. Soit B une A -algèbre arbitraire. Comme le produit tensoriel commute aux sommes directes (7.36), et comme $A \otimes_A B = B$ (8.6), on obtient que

$$M \otimes_A B \cong B^n$$

et ceci est un isomorphisme de B -modules. Appliquant ceci lorsque B est un corps A/\mathfrak{m} , ou le corps des fractions de A si A est intègre, on obtient le théorème. \square

Remarque 13.5. — On peut aussi démontrer le théorème précédent en utilisant l'algèbre extérieure $\bigwedge_A(M)$. En effet, d'après la proposition 9.13, si $n = \text{rang } M$ l'on a :

$$\bigwedge_A^n(M) \cong A \quad \text{et} \quad \bigwedge_A^i(M) = 0 \quad \text{si } i > n.$$

Ceci montre que n est uniquement déterminé par M . Pour plus de détails sur l'algèbre extérieure, le lecteur pourra consulter aussi [BM, § IV.2].

Remarque 13.6. — 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.

13.2. Modules d'homomorphismes et module dual. —

Définition 13.7. — 1) Soient M, N deux A -modules, $\phi, \phi' \in \text{Hom}_A(M, N)$ et $a \in A$. On note

$$\phi + \phi', \quad \text{resp.} \quad a\phi,$$

l'application $M \rightarrow N$ qui à tout $m \in M$ associe $\phi(m) + \phi'(m)$, resp. $a\phi(m)$. Alors $\phi + \phi'$ et $a\phi$ sont des A -morphisms ; on obtient ainsi une **structure de A -module** sur $\text{Hom}_A(M, N)$.

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

Proposition 13.8. — Soient M, M', N des A -modules. On a un isomorphisme de A -modules :

$$\begin{array}{ccc} \text{Hom}_A(M \oplus M', N) & \xrightarrow{\sim} & \text{Hom}_A(M, N) \oplus \text{Hom}_A(M', N), \\ \phi & \mapsto & (\phi|_M, \phi|_{M'}), \end{array}$$

où $\phi|_M$ et $\phi|_{M'}$ désignent les restrictions de ϕ à M et M' . 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 $\psi : M \rightarrow N$ et $\psi' : M' \rightarrow N$ associe le morphisme $\psi + \psi' : M \oplus M' \rightarrow N$ 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. \square

Remarque 13.9. — 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 13.10 (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 $e_i^*(a_1 e_1 + \dots + a_n e_n) = a_i$.

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

Démonstration. — D'une part, e_1^*, \dots, e_n^* sont linéairement indépendants, car si $f = a_1 e_1^* + \dots + a_n e_n^* = 0$, alors $0 = f(e_i) = a_i$ pour tout i . De même, e_1^*, \dots, e_n^* engendrent M^* car $f = f(e_1)e_1^* + \dots + f(e_n)e_n^*$, 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 $M \rightarrow M^{**}$ envoie chaque e_i sur e_i^{**} , donc est un isomorphisme. \square

13.3. Structure des modules de type fini sur un anneau principal. — Désormais, on suppose A **principal**. On a le théorème fondamental suivant, dont la démonstration occupera le reste de la section 13.

Théorème 13.11 (Structure des 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, N est libre de rang $r \leq n$ et il existe :

$$\left\{ \begin{array}{l} \text{une base } (e_1, \dots, e_n) \text{ de } A^n; \\ a_1, \dots, a_r \in A \setminus \{0\} \text{ vérifiant } a_i \mid a_{i+1} \text{ pour } i = 1, \dots, r-1; \\ \text{tels que } (a_1 e_1, \dots, a_r e_r) \text{ soit une base de } N, \end{array} \right.$$

et les idéaux $(a_r) \subseteq \dots \subseteq (a_1)$ sont uniquement déterminés par N .

1') De plus, le sous-module de A^n engendré par e_1, \dots, 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 $r, s \geq 0$ et des éléments non nuls a_1, \dots, a_r de A vérifiant $a_i \mid a_{i+1}$ pour $i = 1, \dots, r-1$, tels que

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

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

$$(3) \quad M \cong A^s \oplus M_{\text{tors}}, \quad \text{et} \quad A^s \cong M/M_{\text{tors}}.$$

En particulier :

M est libre $\Leftrightarrow M$ est sans torsion.

De plus, les idéaux $(a_r) \subseteq \dots \subseteq (a_1)$ 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 $\text{Ann}(M) = (p_1)^{m_1} \dots (p_n)^{m_n}$ la décomposition de $\text{Ann}(M)$ en produits d'idéaux maximaux. Alors, on a la décomposition primaire

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

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

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

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

Définition 13.12 (Base adaptée). — On dira que la base de M donnée dans le point 1) est **adaptée** au sous-module N .

Le point 1) du théorème précédent est équivalent au théorème suivant.

Théorème 13.13 (Réduction des matrices sur un anneau principal)

Soit A un anneau principal et soit $F \in M_{n,m}(A)$ non nulle. Alors, il existe $r \geq 1$, des matrices inversibles $P \in GL_n(A)$, $Q \in GL_m(A)$, et des éléments a_1, \dots, a_r de A , vérifiant $a_i \mid a_{i+1}$ pour $i < r$, 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, r et les idéaux $(a_1), \dots, (a_r)$ sont entièrement déterminés par F .

Démonstration de l'équivalence. — La matrice F définit un morphisme de A -modules $\phi : A^m \rightarrow A^n$, et multiplier F à gauche (resp. à droite) par une matrice inversible équivaut à faire un changement de base dans le module d'arrivée A^n (resp. le module de départ A^m). Donc, le théorème de réduction signifie qu'il existe des bases $\mathcal{B} = (e_1, \dots, e_m)$ de A^m et $\mathcal{C} = (f_1, \dots, f_n)$ de A^n telles que la matrice de F dans ces bases soit de la forme indiquée.

Supposons maintenant que N soit un sous-module de A^n . Comme A est principal, donc noethérien, N est engendré par un nombre fini d'éléments x_1, \dots, x_m et est donc l'image d'un morphisme de A -modules

$$\phi : A^m \longrightarrow A^n.$$

Alors, le théorème de réduction entraîne qu'il existe une base (f_1, \dots, f_n) de A^n et des éléments a_1, \dots, a_r de A , vérifiant $a_i \mid a_{i+1}$ pour $i < r$, tels que $N = \text{Im}(\phi)$ soit engendré par les éléments

$$a_1 f_1, \dots, a_r f_r.$$

Or, ces éléments sont linéairement indépendants sur A , puisque les f_i le sont et que A est intègre. Donc ces éléments forment une base de N .

De plus, si (f'_1, \dots, f'_n) est une base de A^n et si a'_1, \dots, a'_s sont des éléments de A tels que $a'_i \mid a'_{i+1}$ pour $i < s$, et que $(a'_1 f'_1, \dots, a'_s f'_s)$ soit une base de $N = \text{Im}(\phi)$, alors l'unicité énoncée dans le théorème de réduction entraîne que $s = r$ et $(a'_i) = (a_i)$ pour $i = 1, \dots, r$. Ceci montre que le théorème de réduction 13.13 entraîne le point 1) du théorème de structure 13.11.

Réciproquement, supposons ce point vérifié et soit $\phi : A^m \rightarrow A^n$ un morphisme de A -modules. Alors, il existe une base $\mathcal{C} = (f_1, \dots, f_n)$ de A^n et des éléments a_1, \dots, a_r de A , vérifiant $a_i \mid a_{i+1}$ pour $i < r$, tels que

$$(a_1 f_1, \dots, a_r f_r)$$

soit une base de $N = \text{Im}(\phi)$. Pour $i = 1, \dots, r$ soit e_i un élément de A^m tel que $\phi(e_i) = a_i f_i$. Alors, on obtient que

$$A^m = Ae_1 + \dots + Ae_r + \text{Ker } \phi,$$

et comme les f_i sont linéairement indépendants et que A est intègre, on obtient que la somme ci-dessus est directe :

$$A^m = Ae_1 \oplus \dots \oplus Ae_r \oplus \text{Ker } \phi.$$

Enfin, d'après l'hypothèse 1), à nouveau, $\text{Ker } \phi$ est un A -module libre, donc (e_1, \dots, e_r) se complète en une base

$$\mathcal{B} = (e_1, \dots, e_n) \text{ de } A^n, \text{ où } (e_{r+1}, \dots, e_n) \text{ est une base de } \text{Ker } \phi.$$

Alors, la matrice de ϕ dans les bases \mathcal{B} et \mathcal{C} est de la forme voulue. De plus, les idéaux (a_i) sont uniquement déterminés par $N = \text{Im}(\phi)$, donc par ϕ . Ceci prouve que le point 1) du théorème de structure 13.11 entraîne le théorème de réduction 13.13. \square

Pour démontrer les deux théorèmes précédents, il y a donc deux approches. On peut démontrer d'abord le théorème de réduction 13.13, d'où le point 1) du théorème de structure 13.11. On montre ensuite les points 1')–3).

Ou bien, on peut démontrer d'abord le théorème de structure 13.11, en trois étapes. Dans cette approche, on montre d'abord l'existence dans les points 1), 2) et 3). On établit ensuite l'unicité des $n_s(p_i)$ dans le point 3) et des idéaux (a_i) dans le point 2), puis l'on en déduit l'unicité des (a_i) dans le point 1).

Avant de passer aux démonstrations, traitons un exemple (qui montre qu'il est bon de combiner les deux approches, c.-à-d., d'utiliser à la fois les opérations matricielles et la notion de base adaptée).

13.4. Un exemple. — Considérons la matrice suivante, à coefficients dans \mathbb{Z} .

$$F = \begin{pmatrix} 14 & 21 & 30 & 35 \\ 21 & 14 & 12 & 42 \\ 30 & 20 & 28 & 15 \end{pmatrix}.$$

Elle définit un morphisme de \mathbb{Z} -modules $\mathbb{Z}^4 \rightarrow \mathbb{Z}^3$. On va la réduire à sa forme diagonale, en commençant par les opérations suivantes, sur les lignes ou les colonnes.

$$\begin{pmatrix} 14 & 21 & 30 & 35 \\ 21 & 14 & 12 & 42 \\ 30 & 20 & 28 & 15 \end{pmatrix} \xrightarrow{L_1 \rightarrow L_1 - L_3} \begin{pmatrix} -16 & 1 & 2 & 20 \\ 21 & 14 & 12 & 42 \\ 30 & 20 & 28 & 15 \end{pmatrix},$$

puis $C_3 \rightarrow -C_3 + 2C_2$ et $C_4 \rightarrow -C_4 - C_1 + 4C_2$ donnent

$$\begin{pmatrix} -16 & 1 & 0 & 0 \\ 21 & 14 & 16 & -7 \\ 30 & 20 & 12 & 35 \end{pmatrix}.$$

Alors, $C_1 \rightarrow C_1 + 3C_4$ et $C_2 \rightarrow C_2 + 2C_4$ donnent

$$\begin{pmatrix} -16 & 1 & 0 & 0 \\ 0 & 0 & 16 & -7 \\ 135 & 90 & 12 & 35 \end{pmatrix}.$$

Comme $3 \cdot 16 - 7 \cdot 7 = -1$, on va multiplier à droite par la matrice de Bézout :

$$\left(\begin{array}{cc|cc} 1 & 0 & & \\ 0 & 1 & & 0 \\ \hline & & 3 & 7 \\ 0 & & 7 & 16 \end{array} \right),$$

et comme

$$12 \times 7 + 35 \times 16 = 4 \times 7 \times (3 + 5 \times 4) = 4 \times 7 \times 23,$$

on obtient la matrice

$$\begin{pmatrix} -16 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 135 & 90 & a & 4 \cdot 7 \cdot 23 \end{pmatrix}.$$

Il n'est pas nécessaire de calculer a , car en remplaçant L_3 par $L_3 + aL_2$ on se ramène à $a = 0$.

Remplaçons, de plus, C_1 par $C_1 + 16C_2$. Comme

$$135 + 16 \cdot 90 = 45 \times (3 + 16 \cdot 2) = 3^2 \cdot 5 \times 5 \cdot 7,$$

alors, posant

$$m = 3^2 \cdot 5^2 \cdot 7, \quad n = 2^2 \cdot 7 \cdot 23,$$

on obtient la matrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ m & 90 & 0 & n \end{pmatrix}.$$

Donc $\text{Im}(F)$ contient me_3 et ne_3 , et comme $\text{PGCD}(m, n) = 7$ alors $\text{Im}(F)$ contient $7e_3$.

Enfin, comme $90 \equiv -1 \pmod{7}$, on obtient que $\text{Im}(F)$ est engendré par

$$e_1 - e_3, \quad e_2, \quad 7e_3.$$

Bien sûr, $(e_1 - e_3, e_2, e_3)$ est une base de \mathbb{Z}^3 , et il en résulte que la matrice de départ est équivalente à la matrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & 0 \end{pmatrix}.$$

13.5. Réduction des matrices. — On va démontrer d'abord le théorème de réduction.

Définition 13.14. — Pour tout $s \geq 1$, on note $GL_s(A)$ le groupe des matrices $P \in M_s(A)$ qui sont **inversibles**, c.-à-d., telles qu'il existe $Q \in M_s(A)$ vérifiant

$$PQ = I_s = QP.$$

Dans ce cas, $\det(P)\det(Q) = 1$, donc $\det(P)$ est un élément inversible de A . Réciproquement, cette condition est suffisante, car si \tilde{A} est la matrice des cofacteurs de A , c.-à-d., la matrice dont le coefficient d'indice (i, j) est le déterminant de la matrice carrée de taille $s - 1$ obtenue en barrant la i -ème ligne et la j -ème colonne, alors on sait que

$${}^t\tilde{A}A = \det(A)I_s = A {}^t\tilde{A}.$$

Définition 13.15 (Matrices équivalentes). — Soient $m, n \geq 1$. On dit que deux matrices $F, F' \in M_{n,m}(A)$ sont **équivalentes** s'il existe $P \in GL_n(A)$ et $Q \in GL_m(A)$ telles que $F' = PFQ$.

Remarque 13.16. — Soit u le morphisme de A -modules $A^m \rightarrow A^n$ défini par F . Comme multiplier F à droite (resp. à gauche) par une matrice inversible $Q \in GL_m(A)$ (resp. $P \in GL_n(A)$) revient à effectuer un changement de base dans A^m (resp. A^n), on voit que F' est équivalente à F si et seulement si il existe des bases \mathcal{B} de A^m et \mathcal{C} de A^n telles que F' soit la matrice de u dans ces bases.

Définition 13.17 (Idéaux de Fitting). — Soit $F \in M_{n,m}(A)$.

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

2) 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.

Les idéaux $J_i(F)$ ne dépendent que de la classe d'équivalence de F , d'après la proposition suivante.

Proposition 13.18. — 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 $J_i(\text{PF}) \subseteq J_i(\text{F})$. On obtient de même que $J_i(\text{FQ}) \subseteq J_i(\text{F})$.

2) Supposons $\text{F}' = \text{PFQ}$, avec P et Q inversibles. Alors, on a aussi $\text{F} = \text{P}^{-1}\text{F}'\text{Q}^{-1}$. D'après le point 1), on obtient les inclusions

$$J_i(\text{F}') \subseteq J_i(\text{F}) \subseteq J_i(\text{F}'),$$

d'où $J_i(\text{F}) = J_i(\text{F}')$ pour tout i . La proposition est démontrée. \square

On peut maintenant énoncer le théorème de réduction sous la forme plus précise ci-dessous.

Théorème 13.19 (Réduction des matrices sur un anneau principal)

Soit A un anneau principal et soit $\text{F} \in \text{M}_{n,m}(\text{A})$ non nulle. Il existe $a_1, \dots, a_r \in \text{A}$, avec $r \geq 1$, vérifiant $a_i \mid a_{i+1}$ pour $i < r$, et $\text{P} \in \text{GL}_n(\text{A})$, $\text{Q} \in \text{GL}_m(\text{A})$ tels que

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

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

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

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.

En fait, on ne s'intéresse pas aux matrices P et Q elles-mêmes, et dans la pratique on ne **multiplie pas** des matrices (peu commode si $m, n \geq 3$); on se contente de faire des opérations simples sur les matrices qui sont des **opérations permises**, c.-à-d., qui correspondent à multiplier par une matrice **inversible**. Ces opérations permises simples sont de l'un des trois types suivants.

I) Permutations de lignes ou de colonnes. On peut, bien sûr, permuter les lignes (ou bien les colonnes) de la matrice F.

Soit S_n le groupe des permutations de $\{1, \dots, n\}$ et soit $\sigma \in S_n$. Effectuer sur les lignes de F la permutation σ équivaut à multiplier F à gauche par la matrice de permutation $M(\sigma) \in GL_n(A)$ définie par :

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

où (f_1, \dots, 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 $M(\sigma^{-1})$.

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 .

II) Les transvections $T_{ij}(\alpha)$ et $T'_{k\ell}(\beta)$. Sont également permises les opérations suivantes :

ajouter à une ligne (ou une colonne) **un multiple** d'une **autre** ligne (ou colonne).

En effet, ajouter α fois la ligne j à la ligne $i \neq j$ revient à multiplier F à gauche par la matrice

$$T_{i,j}(\alpha) = I_n + \alpha E_{i,j},$$

qui est clairement inversible, d'inverse $T_{i,j}(-\alpha)$. (On rappelle que I_n désigne la matrice identité et que $E_{i,j}$ est la matrice élémentaire dont le seul coefficient non nul est celui d'indice (i, j) , qui vaut 1.)

De même, ajouter β fois la colonne k à la colonne ℓ revient à multiplier F à droite par la matrice inversible

$$T'_{k\ell}(\beta) = I_m + \beta E_{k\ell}.$$

III) Les matrices de Bézout $B_i(a, b)$ et $B'_j(a, b)$. Soient $a, b \in A \setminus \{0\}$ et soit d un pgcd de a et b . D'après le théorème de Bézout, il existe $x, y \in A$ tels que $ax + by = d$. On note $B_2(a, b)$ la matrice suivante de $GL_n(A)$:

$$B_2(a, b) = \left(\begin{array}{cc|c} x & y & 0 \\ -b/d & a/d & \\ \hline 0 & & I_{n-2} \end{array} \right).$$

(Elle est inversible, car son déterminant est $(ax + by)/d = 1$.)

Alors, la matrice $B_2(a, b)F$ ne diffère de F que sur les deux 1ères lignes. En effet, notant $f_{i,j}$ (resp. $f'_{i,j}$) les coefficients de F (resp. $B_2(a, b)F$), on a pour tout j :

$$\begin{aligned} f'_{1,j} &= x f_{1,j} + y f_{2,j}; \\ f'_{2,j} &= (-b f_{1,j} + a f_{2,j})/d; \\ f'_{i,j} &= f_{i,j} \quad \text{si } i \notin \{1, 2\}. \end{aligned}$$

Par conséquent, si a (resp. b) est le coefficient f_{11} (resp. f_{21}) de la 1ère colonne de F , alors la 1ère colonne de $B_2(a, b)F$ 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 de la matrice $B_2(a, b)$.

De façon analogue, pour tout $i \geq 2$, on note $B_i(a, b)$ la matrice (b_{kj}) telle que

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

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

$$\begin{pmatrix} x & 0_{i-2} & y & 0_{n-i} \\ 0_{i-2} & I_{i-2} & 0_{i-2} & 0 \\ -\frac{b}{d} & 0_{i-2} & \frac{a}{d} & 0_{n-i} \\ 0_{n-i} & 0 & 0_{n-i} & I_{n-i} \end{pmatrix},$$

où les 0_s désignent des lignes ou colonnes de zéros (et les 0 sans indices désignent des matrices rectangulaires formées de zéros). C'est une matrice inversible, puisque son déterminant est $(ax + by)/d = 1$. 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.

De même, pour $j \in \{2, \dots, m\}$, on définit $B'_j(a, b) \in GL_m(A)$ par

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

et $b'_{kj} = 0$ dans les autres cas. 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 $d = \text{pgcd}(a, b)$ et b par 0.

Remarque 13.20. — Les matrices $T_{1i}(\alpha)$ et $T'_{1\ell}(\beta)$ sont des cas particuliers, plus simples, de matrices de Bézout. Toutefois, il est commode de les considérer séparément.

Maintenant, on va montrer qu'on peut effectuer des « opérations élémentaires permises » 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 13.21. — 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 $s \geq 1$.

Algorithme de réduction. Soit $F = (f_{ij}) \in M_{n,m}(A)$, non nulle. Soit f_{1j} 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) On va remplacer F , en plusieurs sous-étapes, par une matrice équivalente F_1 de la forme

$$F_1 = \begin{pmatrix} d_1 & 0 \\ 0 & B \end{pmatrix}$$

avec $d_1 \in A \setminus \{0\}$ et $B \in M_{n-1, m-1}(A)$. Ceci se fait comme suit.

i) Annulation des coefficients f_{1j} , pour $j \geq 2$. Si f_{11} divise tous les f_{1j} , pour $j \geq 2$, on remplace chaque colonne C_j , pour $j \geq 2$, par la colonne $C_j - f_{1j}/f_{11}C_1$.

Sinon, s'il existe $k \geq 2$ tel que f_{11} ne divise pas f_{1k} , on multiplie F à droite par la matrice de Bézout $B'_{1k}(f_{11}, f_{1k})$. On annule ainsi le coefficient $(1, k)$, tandis que f_{11} est remplacé par $d = \text{pgcd}(f_{11}, f_{1k})$, qui est de longueur $< \ell(f_{11})$. S'il existe $k' \neq k$ tel que d ne divise pas $f_{1k'}$, on répète le processus. On arrive ainsi, en au plus $m - 1$ opérations, à une matrice équivalente

$$F' = FQ,$$

dont la 1ère ligne est $(f'_{11}, 0, \dots, 0)$, avec $f'_{11} = f_{11}$ si l'on n'a pas effectué d'opérations de Bézout, et $\ell(f'_{11}) < \ell(f_{11})$ sinon.

ii) Annulation des coefficients f'_{i1} , pour $i \geq 2$. Si f'_{11} divise tous les f'_{i1} , pour $i \geq 2$, on remplace chaque ligne L_i , pour $i \geq 2$, par la ligne $L_i - f'_{i1}/f'_{11}L_1$. Ce faisant, on ne modifie pas la 1ère ligne de F' , et l'on obtient donc une matrice F_1 comme voulue, c.-à-d., on peut passer à l'étape 2).

Sinon, s'il existe $i \geq 2$ tel que f'_{11} ne divise pas f'_{i1} alors, en multipliant F' à gauche par une suite de matrices de Bézout, on obtient une matrice équivalente

$$F'' = PF' = PFQ,$$

dont la 1ère colonne est nulle, sauf le 1er coefficient f''_{11} , qui vérifie $\ell(f''_{11}) < \ell(f'_{11})$.

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 $\ell(f''_{11}) < \ell(f_{11})$ et on répète alors la sous-étape i). Comme la longueur du coefficient d'indice $(1, 1)$ décroît

strictement à chaque opération de Bézout, on obtient, après un nombre fini de sous-étapes i) et ii), une matrice équivalente F_1 de la forme voulue :

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

Étape 2) 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

$$(\mathbf{I}_n + \mathbf{E}_{1i})F_1 = \begin{pmatrix} d_1 & c_{i2} & \cdots & c_{im} \\ 0 & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix},$$

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 $\ell(d'_1) < \ell(d_1)$. Si d'_1 ne divise pas tous les coefficients, on recommence le processus. On obtient ainsi, après un nombre fini ($\leq \ell(d_1)$) 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 la proposition 13.18. 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 $i = 2, \dots, r-1$. 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 13.19.

De plus, d'après la proposition 13.18, on a :

$$\forall s \leq \min(m, n), \quad J_s(F) = J_s(F_3).$$

Or les idéaux $J_s(F_3)$ 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

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

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

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

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 13.19. \square

On obtient donc le point 1) du théorème de structure 13.11, d'après l'équivalence établie après le théorème 13.13. Montrons le point 1').

Notons M_1 (resp. M_2) le sous-module de M engendré par e_1, \dots, e_r (resp., par e_{r+1}, \dots, e_n). On a introduit dans le point 1') 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 $a_i e_i \in N$ pour $i = 1, \dots, r$, 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 élément de torsion. Comme ce module est libre, donc sans torsion, ceci entraîne $x \in M_1$. Ceci prouve l'égalité $M_1 = N'$, et 1') est démontré. \square

13.6. Décomposition en somme de modules monogènes. — On va maintenant démontrer l'existence des décompositions annoncées dans les points 2) et 3) du théorème de structure 13.11. Commençons par le lemme ci-dessous.

Lemme 13.22. — *Soient B un anneau et M_1, \dots, M_n des B -modules. Pour $i = 1, \dots, n$, soit N_i un sous-module de M_i et soit $\pi_i : M_i \rightarrow M_i/N_i$. Alors, le noyau du morphisme*

$$\bigoplus_{i=1}^n M_i \longrightarrow \bigoplus_{i=1}^n (M_i/N_i), \quad (x_1, \dots, x_n) \mapsto (\pi_1(x_1), \dots, \pi_n(x_n))$$

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

$$\left(\bigoplus_{i=1}^n M_i\right) / \left(\bigoplus_{i=1}^n N_i\right) \cong (M_1/N_1) \oplus \cdots \oplus (M_n/N_n).$$

Démonstration. — La première assertion est claire, et la seconde en découle, d'après le théorème 2.16. \square

Revenons au théorème 13.11 et montrons le **point 2)**. Soit M un A -module de type fini. Soit $\{x_1, \dots, x_n\}$ un système de générateurs de M et soit $\phi : A^n \rightarrow M$ le morphisme de A -modules envoyant tout (b_1, \dots, b_n) sur $b_1x_1 + \cdots + b_nx_n$. Alors, ϕ induit un isomorphisme

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

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

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

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

$$(*) \quad M \cong A^n / \text{ker } \phi \cong A/(a_1) \oplus \cdots \oplus A/(a_r) \oplus A^s,$$

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 $\text{Ann}(M) = (a_r)$. Ceci prouve le point 2), à l'exception de l'unicité des idéaux

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

Remarque 13.23. — 1) On a choisi un système de générateurs x_1, \dots, x_n de M , donnant lieu au morphisme surjectif $\phi : A^n \rightarrow M$. Ce choix étant fait, il est clair que $(a_1), \dots, (a_r)$ sont les idéaux invariants du sous-module $\text{Ker}(\phi) \subseteq A^n$.

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 $(a_1 \cdots a_i)$, pour $i = 1, \dots, r$, sont les idéaux de Fitting (distincts de A) de M ; voir [BM, Ch. 5, § 1–3]. Comme A est intègre, ceci permet de retrouver les idéaux (a_i) , comme à la fin de la démonstration du théorème 13.19.

2) L'unicité des idéaux (a_i) peut aussi se déduire du résultat suivant. Soient A un anneau commutatif et M un A -module. On suppose M isomorphe à une somme directe de modules monogènes :

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

où $I_1 \subseteq \cdots \subseteq I_r \neq A$. Attention, ici on suppose la suite $(I_k)_{k=1, \dots, r}$ croissante ! (Donc, dans la situation du théorème 13.11, on aurait $(a_k) = I_{r+1-k}$ pour $k = 1, \dots, r$.) Alors on peut montrer que les I_k sont uniquement déterminés par le module M : plus précisément, I_k est l'annulateur du module

$$\bigwedge^k(M),$$

voir [BAlg], Chap. VII, § 4, Proposition 2.

3) On choisit ici l'approche plus élémentaire suivante : on va montrer l'existence et l'unicité de la décomposition dans le point 3), puis en déduire l'unicité des (a_i) dans le point 2).

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 12.27, on a

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

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

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 12.25, 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). \square

Pour démontrer l'unicité des facteurs invariants, commençons par le lemme suivant.

Lemme 13.24. — 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 $A \rightarrow (p^i)/(p^{i+1})$ 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, $\text{Ker } \phi = (p)$ 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 4.23. \square

Théorème 13.25 (Unicité des facteurs invariants). — Soit A un anneau principal et soit M un A -module de torsion de type fini. Soient a_1, \dots, 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 $(a_1), \dots, (a_r)$ 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 $n_1 \leq \dots \leq n_r$ 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

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

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 $i = 1, \dots, r-1$. D'abord, l'idéal (a_r) égale $\text{Ann}(M)$ 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 $i \leq r$,

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

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

$$(*) \quad 0 \leq v_j(1) \leq \cdots \leq v_j(r).$$

Alors, d'après le théorème chinois,

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

et donc

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

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

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

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. \square

Remarque 13.26. — On verra plus bas (13.7) une démonstration de l'existence d'une base adaptée n'utilisant pas la réduction des matrices. Pour compléter cette démonstration alternative d'existence, on peut aussi déduire de ce qui précède l'unicité dans le point 1) du théorème de structure 13.11.

En effet, soit N un sous-module non nul de $M = A^n$ et supposons donnés une base (e_1, \dots, e_n) de M et $a_1, \dots, a_r \in A \setminus \{0\}$ tels que $(a_1 e_1, \dots, a_r e_r)$ soit une base de N , et a_i divise a_{i+1} pour $i = 1, \dots, r-1$. Alors, il résulte de ce qui précède que les idéaux

$$(a_1) \supseteq \dots \supseteq (a_r)$$

sont les facteurs invariants de M/N , donc sont entièrement déterminés par le sous-module N . Modulo la démonstration alternative de l'existence d'une base adaptée donnée plus bas, ceci fournit une démonstration du théorème de structure 13.11 n'utilisant pas le théorème de réduction des matrices.

Remarque 13.27. — 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].

13.7. Autre démonstration. — Dans ce dernier paragraphe, on va donner une autre démonstration de l'existence d'une base adaptée, n'utilisant pas la réduction des matrices.

Définition 13.28 (Matrices échelonnées). — 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. 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 $\ell(P_1) < \dots < \ell(P_r)$.

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

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

Proposition 13.29. — 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, \dots, e_n) une base de M et soit N un sous-module non nul de M . Il existe une base (v_1, \dots, v_r) de N telle que la matrice exprimant les v_j en fonction des e_i soit échelonnée.

Démonstration. — Pour $i = 1, \dots, n$, soit M_i le sous-module de M engendré par e_1, \dots, 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 $\pi_i : M_i \rightarrow A$ 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, \dots, v_s) , où $s \leq i - 1$, qui s'exprime de façon échelonnée en fonction de e_1, \dots, e_{i-1} .

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

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

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

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

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

On va maintenant 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 $(\varepsilon_1, \dots, \varepsilon_n)$ la base canonique de $M := A^n$ et $(\varepsilon_1^*, \dots, \varepsilon_n^*)$ la base duale de M^* (cf. 13.10). 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 $x = (x_1, \dots, x_n) \in N$ tel que $f_0(x) = a$. Montrons d'abord le lemme suivant.

Lemme 13.30. — Pour tout $g \in M^*$, a divise $g(x)$.

Démonstration. — Soit d le PGCD de a et $g(x)$. D'après le théorème de Bézout, 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. \square

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 :

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

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

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

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

Lemme 13.31. — *On a $f(N) \subseteq (a)$, pour tout $f \in M^*$.*

Démonstration. — Posons $K = \text{Ker } f_0$; 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. \square

D'après la proposition 13.29, le sous-module $\text{Ker } f_0$ est libre, disons de rang s . Comme $M \cong \text{Ker } f_0 \oplus Ae_1$, alors $n = s + 1$ (car une base de M est obtenue en adjoignant e_1 à une base de $\text{Ker } f_0$). Donc $s = n - 1$. Par hypothèse de récurrence, appliquée au sous-module $N \cap \text{Ker } f_0$ de $\text{Ker } f_0$, on obtient qu'il existe une base (e_2, \dots, e_n) de $\text{Ker } f_0$ et $a_2, \dots, a_n \in A \setminus \{0\}$, tels que $(a_2e_2, \dots, a_n e_n)$ soit une base de $N \cap \text{Ker } f_0$ et $a_i \mid a_{i+1}$ pour $i = 2, \dots, n - 1$.

Alors, d'après (*), (e_1, \dots, e_n) est une base de M et $(ae_1, a_2e_2, \dots, a_n e_n)$ une base de N . Soit (e_1^*, \dots, e_n^*) la base duale de M^* . Alors a_2 appartient à $e_2^*(N)$ donc est divisible par a , d'après le lemme 13.31. Ceci achève la démonstration de l'existence d'une base adaptée. \square

TABLE DES MATIÈRES

I. Anneaux et modules, localisation	1
Introduction	1
1. Anneaux et modules	1
1.1. Anneaux	1
1.2. A-modules	4
2. Modules et anneaux quotients, théorèmes de Noether	7
2.1. Définition des modules quotients	7
2.2. A-modules simples et idéaux maximaux	10
2.3. Noyaux et théorèmes de Noether	12
3. Construction de modules ou d'idéaux	14
3.1. Sous-module ou idéal engendré	14
3.2. Sommes de sous-modules et sommes directes	15
3.3. Sommes et produits d'idéaux	16
4. Idéaux premiers et localisation	17
4.1. Idéaux premiers	17
4.2. Anneaux et modules de fractions	19
I. Anneaux et modules, localisation (suite)	23
4. Idéaux premiers et localisation (suite)	23
4.3. Anneaux d'endomorphismes	27
4.4. La localisation est un foncteur additif exact	29
4.5. Idéaux premiers de $S^{-1}A$, anneaux locaux	34
5. Modules de type fini, lemme de Zorn, existence d'idéaux maximaux	36
5.1. Modules de type fini	36
5.2. Union filtrante de sous-modules	38
5.3. Théorème de Zorn et conséquences	40
5.4. Un exemple d'application	41

6. Modules libres	41
6.1. Définitions et exemples	41
6.2. Les modules libres $A^{(I)}$	43
II. Produit tensoriel et applications	45
7. Produit tensoriel	45
7.1. Deux motivations	45
7.2. Applications bilinéaires	47
7.3. Produit tensoriel : définition et propriété universelle	49
7.4. Premières propriétés du produit tensoriel	51
7.5. Applications multilinéaires et produits tensoriels itérés	53
7.6. Produits tensoriels d'algèbres et produits de variétés	55
7.7. Produits et sommes directes	59
8. Extension des scalaires et changement de base	63
8.1. Extension et restriction des scalaires	63
8.2. Produit tensoriel par $S^{-1}A$	66
8.3. Produit tensoriel par A/I	67
9. Algèbres tensorielles, symétriques, et extérieures	67
9.1. A -algèbres non-commutatives	68
9.2. Algèbre tensorielle d'un A -module	68
9.3. Modules et algèbres gradués	69
9.4. Algèbre symétrique d'un A -module	71
9.5. Algèbre extérieure et applications multilinéaires alternées	73
III. Anneaux noethériens, factoriels, principaux	79
10. Modules et anneaux noethériens	79
10.1. Anneaux et modules noethériens	79
10.2. Anneaux de polynômes	81
10.3. Le théorème de transfert de Hilbert	85
11. Anneaux factoriels, principaux, euclidiens	87
11.1. Divisibilité, éléments irréductibles	87
11.2. Anneaux factoriels, lemmes d'Euclide et Gauss	90
11.3. PPCM et PGCD dans un anneau factoriel	93
11.4. Le théorème de transfert de Gauss	95
11.5. Anneaux principaux et anneaux euclidiens	98
11.6. Exemples d'anneaux noethériens non factoriels	99
IV. Théorème chinois et applications, modules sur les anneaux principaux	103
12. Théorème chinois et applications	103
12.1. Idéaux étrangers	103
12.2. Théorème chinois des restes	105
12.3. Annulateurs et modules de torsion	106

12.4. Modules se décomposant en composantes primaires	107
12.5. Décomposition primaire des modules de torsion sur un anneau principal	109
13. Modules de type fini sur un anneau principal	114
13.1. Rang d'un module libre de type fini	114
13.2. Modules d'homomorphismes et module dual	116
13.3. Structure des modules de type fini sur un anneau principal ...	117
13.4. Un exemple	120
13.5. Réduction des matrices	122
13.6. Décomposition en somme de modules monogènes	129
13.7. Autre démonstration	133
Bibliographie	iv

Bibliographie

- [Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.
- [AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.
- [BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.
- [BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.
- [ChL] A. Chambert-Loir, Algèbre corporelle, Presses de l'École polytechnique, 2005.
- [Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.
- [Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedric Fernand Nathan, 1977, 2ème éd., 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.
- [Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.
- [La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.
- [Ne04] J. Nekovář, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekoavar/co/ln
- [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.
- [Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.
- [Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.