VI. COMPLÉMENTS SUR LES MODULES, THÉORÈME CHINOIS, FACTEURS INVARIANTS

SÉANCES DU 15, 16 ET 22 OCTOBRE

12. Compléments sur les modules

12.1. Théorème de Zorn et conséquences. — Soient A un anneau commutatif et M un A-module.

Définition 12.1. — Un sous-module **propre** de M est un sous-module $N \neq M$. De même, un **idéal propre** de A est un idéal $\neq A$.

Définition 12.2. — Soit N un sous-module de M. On dit que N est un sous-module **maximal** s'il n'existe pas de sous-module propre N' contenant N strictement, c.-à-d., si N est un élément maximal (pour la relation d'inclusion) de l'ensemble des sous-modules propres.

Lemme 12.3. — *Soit* M *un* A*-module* **de type fini** *et soit* $(M_i)_{i\in I}$ *une famille filtrante de sous-modules* **propres** *de* M. *Alors* $\bigcup_{i\in I} M_i$ *est un sous-module* **propre** *de* M.

Démonstration. — Posons $U := \bigcup_{i\in I} M_i$; on a déjà vu que c'est un sous-module de M (Lemme 8.3). Montrons que c'est un sous-module propre. Supposons au contraire que $U = M$ et soient $x_1, \dots, x_r$ des générateurs de M.

Alors, il existe des indices $i_1, \dots, i_r \in I$ tels que $x_1 \in M_{i_1}$, …, $x_r \in M_{i_r}$. Comme la famille $(M_i)_{i\in I}$ est filtante, il existe ℓ tel que M_ℓ contienne $x_1, \dots, x_r$, et comme ces derniers engendrent M, ceci entraîne $M_\ell = M$, en contradiction avec l'hypothèse que chaque M_i, $i \in I$, est un sous-module propre. Cette contradiction montre que $U \neq M$. Le lemme est démontré. □

Définition 12.4. — Rappelons qu'un **ensemble ordonné** est un ensemble E muni d'une relation $x \leqslant y$ qui soit une relation *d'ordre partiel*, c.-à-d., qui est

1) réflexive : $\forall\, x \in E, \quad x \leqslant x$;
2) antisymétrique : $\forall\, x, y \in E, \quad x \leqslant y$ et $y \leqslant x \Rightarrow x = y$;
3) transitive : $\forall\, x, y, z \in E, \quad x \leqslant y$ et $y \leqslant z \Rightarrow x \leqslant z$.

Exemple 12.5. — Soit M un A-module de type fini. L'ensemble des sous-modules *propres* de M est ordonné par inclusion et, si $(M_i)_{i\in I}$ est une famille filtrante de sous-modules propres, alors $U = \bigcup_{i\in I} M_i$ est un sous-module *propre* (d'après le lemme 12.3), qui est un **majorant** de chacun des M_i, c.-à-d., tel que $M_i \subseteq U$ pour tout $i \in I$.

On peut maintenant énoncer la définition et le théorème suivants.

Définition 12.6. — Soit $(E, \leqslant)$ un ensemble ordonné.

1) On dit qu'un sous-ensemble F de E est **filtrant** s'il vérifie la propriété suivante : pour tout $f, f' \in F$, il existe $f'' \in F$ tel que $f \leqslant f''$ et $f' \leqslant f''$.

2) On dit qu'un élément $x \in E$ est un élément **maximal** s'il n'existe pas d'élément $y \in E$ tel que $y > x$.

3) Soit S un sous-ensemble de E et soit $x \in E$. On dit que x est un **majorant** de S si l'on a $s \leqslant x$ pour tout $s \in S$ (on ne demande pas que x appartienne à S).

***Théorème 12.7* (Zorn)**. — *Soit* E *un ensemble ordonné non-vide vérifiant la propriété suivante :*

$(*)$ *Tout sous-ensemble filtrant de* E *admet un majorant dans* E.

Alors E *possède au moins un élément maximal.*

Démonstration. — Nous ne démontrerons pas ce théorème, qui appartient au domaine de la théorie des ensembles, et l'on renvoie le lecteur intéressé à [**Dou**, Chap.1] ou [**La**, Appendix 2].

Dans ces références, il est montré comment le théorème de Zorn se déduit de l'axiome du choix. Il est aussi montré que le théorème de Zorn entraîne le théorème de Zermelo, qui lui-même entraîne l'axiome du choix. Donc, en fait, l'axiome du choix et les théorèmes de Zorn et de Zermelo sont équivalents. □

Théorème 12.8. — *Soit* M *un* A*-module non nul de type fini et soit* N *un sous-module propre. Alors* M *possède au moins un sous-module maximal contenant* N.

Démonstration. — L'ensemble E des sous-modules propres de M contenant N est non-vide (il contient N) et vérifie la propriété $(*)$, d'après le lemme 12.3. Il possède donc un élément maximal M′, et M′ est un sous-module maximal de M contenant N. □

Remarque 12.9. — L'hypothèse que M soit de type fini est nécessaire, comme le montre l'exercice suivant.

Exercice 12.10. — Soit A le sous-anneau du corps $\mathbb{C}(X)$ formé des fractions rationnelles définies en 0, c.-à-d.,

$$A = \left\{ \frac{P}{Q} \;\middle|\; P, Q \in \mathbb{C}[X],\ Q(0) \neq 0 \right\}.$$

Soit N un sous-A-module de $\mathbb{C}(X)$. Montrez que N est engendré par X^n, pour un certain $n \in \mathbb{Z}$. En déduire que le A-module $\mathbb{C}(X)$ ne possède pas de sous-module maximal.

Corollaire 12.11 **(Théorème de Krull)**. — *Soient* A *un anneau commutatif non nul et* I *un idéal propre de* A. *Alors* I *est contenu dans un idéal maximal* $\mathfrak{m}$.

Démonstration. — Ceci résulte du théorème 12.8, puisque $A = A \cdot 1$ est un A-module de type fini. □

12.2. Rang d'un module libre de type fini. — Soit A un anneau commutatif $\neq (0)$.

Lemme 12.12. — *Si* M *est un* A*-module libre de type fini, toute base de* M *est formée d'un nombre fini d'éléments.*

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

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

Théorème 12.13 **(Rang d'un module libre de type fini)**. — *Soit* A *un anneau commutatif* $\neq (0)$. *Si l'on a un isomorphisme de* A*-modules* $A^m \xrightarrow{\sim} A^n$, *alors* $m = n$.

Par conséquent, tout A*-module* M $\neq (0)$ *libre de type fini est de la forme* A^n, *pour un entier* $n \geqslant 1$ *uniquement déterminé, appelé le* **rang** *de* M *et noté* $\operatorname{rang} M$.

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

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

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

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

et l'on a

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

Comme A est un anneau commutatif $\neq (0)$, il possède (d'après le Théorème de Krull 12.11) un idéal maximal $\mathfrak{m}$, et le quotient $\mathrm{A}/\mathfrak{m}$ est un corps k. Soit π la projection $\mathrm{A} \to k$. Pour toute matrice $\mathrm{C} = (c_{i,j}) \in \mathrm{M}_{r,s}(\mathrm{A})$, notons $\pi(\mathrm{C})$ la matrice dont les coefficients sont les $\pi(c_{i,j})$; on dit que $\pi(\mathrm{C})$ 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 $\mathrm{C}' \in \mathrm{M}_{s,t}(\mathrm{A})$ on a l'égalité suivante dans $\mathrm{M}_{r,t}(k)$:

$$\pi(\mathrm{CC}') = \pi(\mathrm{C})\pi(\mathrm{C}').$$

Par conséquent, $(*)$ entraîne $\pi(\mathrm{P})\pi(\mathrm{Q}) = \mathrm{I}_n$ et $\pi(\mathrm{Q})\pi(\mathrm{P}) = \mathrm{I}_m$; donc $\pi(\mathrm{P})$ induit un isomorphisme

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

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

Remarque 12.14. — 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 $\mathrm{V} = k[\mathrm{X}]$) et soit R l'anneau des endomorphismes de V. On voit facilement que $\mathrm{V} \cong \mathrm{V} \oplus \mathrm{V}$, et l'on peut en déduire que $\mathrm{R} \cong \mathrm{R}^2$ 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.

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

Définition 12.15 **(Annulateurs)**. — Soit $m \in \mathrm{M}$. On pose :

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

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

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

Définition 12.16. — M est un A-module **de torsion** si $\mathrm{Ann}(m) \neq (0)$, pour tout $m \in \mathrm{M}$.

Lemme 12.17. — *Supposons* A **intègre** *et soit* M *un* A*-module* **de torsion** *et* **de type fini**. *Alors* $\mathrm{Ann}(\mathrm{M}) \neq (0)$.

Démonstration. — Soit $x_1, \ldots, x_n$ un système fini de générateurs de M. Comme M est de torsion, $\mathrm{I}_k := \mathrm{Ann}(x_k)$ est non nul, pour tout k. Alors $\mathrm{Ann}(\mathrm{M}) = \mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n$ est non nul, car il contient $\mathrm{I}_1 \cdots \mathrm{I}_n$, qui est $\neq (0)$ puisque A est intègre. □

Exercice 12.18. — 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 12.19. — Soit M un A-module. On note

$$\mathrm{M}_{\mathrm{tors}} = \{m \in \mathrm{M} \mid \mathrm{Ann}(m) \neq (0)\}$$

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

Définition et proposition 12.20 **(Sous-module de torsion)**. — *Si* A *est* **intègre**, *alors :*

1) $\mathrm{M}_{\mathrm{tors}}$ *est un sous-module de* M, *appelé le* **sous-module de torsion**.

2) *Le module quotient* $\mathrm{M}/\mathrm{M}_{\mathrm{tors}}$ *est sans torsion.*

Démonstration. — Soient $m, m' \in \mathrm{M}_{\mathrm{tors}}$ et $b \in \mathrm{A}\setminus\{0\}$. Par hypothèse, il existe $a, a' \in \mathrm{A}\setminus\{0\}$ 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 $\mathrm{M}_{\mathrm{tors}}$. Ceci prouve 1).

Prouvons 2). Soient $m \in \mathrm{M}$ et $b \in \mathrm{A} \setminus \{0\}$ tels que $b\pi(m) = 0$, où π désigne la projection $\mathrm{M} \to \mathrm{M}/\mathrm{M}_{\mathrm{tors}}$. Alors $bm \in \mathrm{M}_{\mathrm{tors}}$, donc il existe $a \in \mathrm{A} \setminus \{0\}$ tel que $abm = 0$. Comme $ab \neq 0$ (puisque A est intègre), ceci implique $m \in \mathrm{M}_{\mathrm{tors}}$, d'où $\pi(m) = 0$. La proposition est démontrée. □

12.4. Modules d'homomorphismes et module dual. — [(3)]

Définition 12.21. — 1) Soient M, N deux A-modules, $\phi, \phi' \in \mathrm{Hom}_{\mathrm{A}}(\mathrm{M}, \mathrm{N})$ et $a \in \mathrm{A}$. On note

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

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

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

Proposition 12.22. — *Soient* $\mathrm{M}, \mathrm{M}', \mathrm{N}$ *des* A*-modules. On a un isomorphisme de* A*-modules :*

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

où $\phi|_{\mathrm{M}}$ *et* $\phi|_{\mathrm{M}'}$ *désignent les restrictions de* ϕ *à* M *et* M'. *En particulier, pour* $\mathrm{N} = \mathrm{A}$, *on obtient*

$$(\mathrm{M} \oplus \mathrm{M}')^* \cong \mathrm{M}^* \oplus \mathrm{M}'^*.$$

(3) Ce paragraphe n'a pas été traité en cours

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

Remarque 12.23. — Supposons A intègre. Si M est un A-module de torsion, alors $\mathrm{M}^* = (0)$. En effet, soit $\phi \in \mathrm{M}^*$. Pour tout $m \in \mathrm{M}$, $\phi(m) \in \mathrm{A}$ est un élément de torsion, donc nul puisque A est supposé intègre. Donc $\phi = 0$, ce qui montre que $\mathrm{M}^* = (0)$.

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

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

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

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

12.5. Suites exactes. — [4]

Définition 12.25. — 1) On dit qu'un diagramme

$$\mathrm{N} \xrightarrow{f} \mathrm{M} \xrightarrow{g} \mathrm{P}$$

de morphismes de A-modules est **exact en** M si $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

2) On dit qu'une suite de morphismes de A-modules

$$\cdots \xrightarrow{f_{n-1}} \mathrm{M}_{n-1} \xrightarrow{f_n} \mathrm{M}_n \xrightarrow{f_{n+1}} \mathrm{M}_{n+1} \xrightarrow{f_{n+2}} \cdots$$

est un **complexe** si pour tout n on a

$$f_{n+1} \circ f_n = 0, \quad \text{c.-à-d.,} \quad \mathrm{Im}(f_n) \subseteq \mathrm{Ker}(f_{n+1}).$$

On dit que ce complexe est une **suite exacte** si le diagramme ci-dessus est exact en chaque M_n, c.-à-d., si pour tout n on a $\mathrm{Im}(f_n) = \mathrm{Ker}(f_{n+1})$.

[4] Ce paragraphe n'a pas été traité en cours

3) On appelle **suite exacte courte** une suite exacte de la forme suivante :

$$(*) \qquad 0 \longrightarrow \mathrm{N} \xrightarrow{f} \mathrm{M} \xrightarrow{g} \mathrm{P} \longrightarrow 0.$$

Donc, dire qu'un diagramme $(*)$ est une suite exacte courte équivaut à dire que : f est injectif et g induit un isomorphisme $\mathrm{M}/f(\mathrm{N}) \cong \mathrm{P}$.

Donc, se donner une suite exacte courte $(*)$ équivaut à se donner : un sous-module N' de M, et deux isomorphismes $f : \mathrm{N} \xrightarrow{\sim} \mathrm{N}'$ et $g : \mathrm{M}/\mathrm{N}' \xrightarrow{\sim} \mathrm{P}$. Ceci est plus souple que d'exiger que N soit égal à N', comme le montrent les deux exemples suivants.

Exemple 12.26. — On a une suite exacte de $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

où le morphisme $\xrightarrow{2}$ est la multiplication par 2, et π est la projection canonique.

Exemple 12.27. — Soit $\lambda \in \mathbb{C}$ et soit $\phi_\lambda : \mathbb{C}[\mathrm{X}] \to \mathbb{C}$ le morphisme de $\mathbb{C}$-algèbres défini par $\phi_\lambda(\mathrm{X}) = \lambda$. Alors on a une suite exacte de $\mathbb{C}[\mathrm{X}]$-modules

$$0 \longrightarrow \mathbb{C}[\mathrm{X}] \xrightarrow{\mathrm{X}-\lambda} \mathbb{C}[\mathrm{X}] \xrightarrow{\phi_\lambda} \mathbb{C} \longrightarrow 0,$$

où la seconde flèche désigne la multiplication par $\mathrm{X} - \lambda$.

Remarque 12.28. — Soit

$$\cdots \xrightarrow{f_{n-1}} \mathrm{M}_{n-1} \xrightarrow{f_n} \mathrm{M}_n \xrightarrow{f_{n+1}} \mathrm{M}_{n+1} \xrightarrow{f_{n+2}} \cdots$$

un complexe de A-modules. Pour tout n, posons $\mathrm{K}_n = \mathrm{Ker}(f_n)$ et $\mathrm{I}_n = \mathrm{Im}(f_n)$. Alors, on a des suites exactes

$$0 \longrightarrow \mathrm{K}_n \longrightarrow \mathrm{M}_n \longrightarrow \mathrm{I}_n \longrightarrow 0$$

et des complexes

$$(*_n) \qquad 0 \longrightarrow \mathrm{I}_{n-1} \longrightarrow \mathrm{M}_n \longrightarrow \mathrm{I}_n \longrightarrow 0,$$

et le complexe est exact si, et seulement si, chaque $(*_n)$ est une suite exacte courte.

12.6. Anneaux d'endomorphismes. — [5]

Définition 12.29. — Soit M un groupe abélien, c.-à-d., un $\mathbb{Z}$-module. L'ensemble des **$\mathbb{Z}$-endomorphismes** de M, c.-à-d., des morphismes de groupe abélien $f : \mathrm{M} \to \mathrm{M}$, est noté $\mathrm{End}_{\mathbb{Z}}(\mathrm{M})$, ou simplement $\mathrm{End}(\mathrm{M})$.

[5] Ce paragraphe n'a pas été traité en cours

Proposition 12.30. — *Pour* $f, g \in \mathrm{End(M)}$*, on définit* $f+g$ *par*

$$(f+g)(m) = f(m) + g(m).$$

Ceci munit End(M) *d'une structure de groupe abélien. De plus,* End(M) *est un anneau non commutatif, la multiplication étant la composition des endomorphismes.*

Démonstration. — Il faut d'abord vérifier que $f+g$ est bien un élément de End(M). Mais ceci est clair, car pour $m, n \in \mathrm{M}$, on a

$$\begin{aligned}(f+g)(m+n) = f(m+n) + g(m+n) &= f(m) + f(n) + g(m) + g(n) \\ &= (f+g)(m) + (f+g)(n).\end{aligned}$$

Ensuite, on voit facilement que l'addition des endomorphismes est associative, commutative, et admet pour 0 le morphisme nul, et que tout endomorphisme f admet pour opposé le morphisme $-f : m \mapsto -f(m)$.

De plus, la composition des endomorphismes est associative, et admet pour élément neutre l'application identique $\mathrm{id_M} \in \mathrm{End(M)}$. Il reste à vérifier la distributivité. Soient $f, g, h \in \mathrm{End(M)}$. L'égalité $(g+h) \circ f = g \circ f + h \circ f$ résulte de la définition de l'addition. D'autre part, pour tout $m \in \mathrm{M}$, on a

$$(f \circ (g+h))(m) = f(g(m) + h(m)) \overset{*}{=} f(g(m)) + f(h(m)),$$

où dans l'égalité $(*)$ on a utilisé le fait que f est un morphisme de groupes abéliens. Ceci prouve que $f \circ (g+h) = f \circ g + f \circ h$. La proposition est démontrée. □

Proposition 12.31. — *Soient* A *un anneau commutatif et* M *un groupe abélien. Se donner une structure de* A*-module*

$$\mu : \mathrm{A} \times \mathrm{M} \longrightarrow \mathrm{M}$$

équivaut à se donner un morphisme d'anneaux $\phi : \mathrm{A} \to \mathrm{End(M)}$*.*

Démonstration. — Supposons donné μ et définissons $\phi : \mathrm{A} \to \mathrm{End(M)}$ par

$$\phi(a)(m) = \mu(a, m), \qquad \forall\, a \in \mathrm{A},\ m \in \mathrm{M}.$$

L'axiome de bi-additivité assure que ϕ est bien à valeurs dans End(M), et est un morphisme de groupes abéliens. Les deux autres axiomes (associativité et unité) assurent que ϕ est un morphisme d'anneaux.

Réciproquement, supposons donné un morphisme d'anneaux $\phi : \mathrm{A} \to \mathrm{End(M)}$, et posons $\mu(a, m) = \phi(a)(m)$, pour tout $a \in \mathrm{A}$, $m \in \mathrm{M}$. On vérifie facilement que ceci fait de M un A-module. □

Soient A un anneau commutatif et I un idéal de A. Notons π la projection $A \to A/I$. Tout A/I-module N est, par « restriction des scalaires » via π, un A-module, c.-à-d., pour l'action

$$a \cdot n = \pi(a)n \qquad \forall\, a \in A,\, n \in N.$$

Alors, pour tout $x \in I$ on a $xN = 0$ et donc, comme A-module, N est annulé par I.

Maintenant, soit M un A-module.

Définition 12.32. — On note IM le sous-module de M engendré par les éléments xm, pour $x \in I$ et $m \in M$. C.-à-d., IM est l'ensemble des sommes finies $x_1m_1 + \cdots + x_nm_n$, où $n \in \mathbb{N}^*$, $x_i \in I$, $m_i \in M$.

On peut donc former le A-module quotient M/IM. Il est annulé par I puisque $Im \subseteq IM$ pour tout $m \in M$.

Théorème 12.33. — *L'action de* A *sur* M/IM *se factorise en une action de* A/I *sur* M*, telle que*

$$(*) \qquad (a + I)(m + IM) = am + IM, \qquad \forall\, a \in A, m \in M.$$

Démonstration. — D'après la proposition 12.31, la structure de A-module sur M/IM équivaut à la donnée du morphisme d'anneaux

$$\phi : A \longrightarrow \mathrm{End}(M)$$

défini par $\phi(a)(m) = am$. Par hypothèse, ce morphisme est nul sur I. Donc d'après la propriété universelle de A/I, appliquée à l'anneau non-commutatif $B = \mathrm{End}(M)$, cf. point 2) du théorème 4.10, ϕ se factorise en un morphisme d'anneaux

$$\overline{\phi} : A/I \longrightarrow \mathrm{End}(M),$$

et l'action $\overline{\mu} : (A/I) \times (M/IM)$ associée vérifie $(*)$. □

Corollaire 12.34. — *Un* A*-module annulé par* I *est la même chose qu'un* A/I*-module.*

Démonstration. — On a déjà vu qu'un A/I-module peut être vu comme un A-module annulé par I. Réciproquement, si M est un A-module annulé par I, alors $IM = (0)$ et donc $M = M/IM$ est un A/I-module. □

13. Théorème chinois et applications

13.1. Idéaux étrangers. — Soient A un anneau commutatif et $I_1, \ldots, I_m$ des idéaux de A, non nécessairement distincts. Commençons par rappeler les définitions suivantes, déjà vues dans le § 5.3.

***Définition 13.1* (Sommes et produits d'idéaux).** — 1) On note $\mathrm{I}_1 + \cdots + \mathrm{I}_m$ l'idéal formé des sommes $x_1 + \cdots + x_m$, où $x_j \in \mathrm{I}_j$ pour $j = 1, \ldots, m$.

2) On note $\mathrm{I}_1 \cdots \mathrm{I}_m$ l'idéal engendré par les produits $x_1 \cdots x_m$, où $x_j \in \mathrm{I}_j$ pour $j = 1, \ldots, m$. C'est l'ensemble des sommes finies de tels produits.

3) On observe que si chaque I_j est principal, c.-à-d., $\mathrm{I}_j = (a_j)$, alors $\mathrm{I}_1 \cdots \mathrm{I}_m$ est l'idéal engendré par $a_1 \cdots a_m$.

4) Si $\mathrm{I}_1, \ldots, \mathrm{I}_m$ sont tous égaux à I, on obtient l'idéal I^m, formé des sommes finies arbitraires de produits de m éléments de I :

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

Remarque 13.2. — 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 $\mathrm{A} = \mathbb{R}[\mathrm{X}, \mathrm{Y}]$ et si I est l'idéal engendré par X et Y, alors I^2 est engendré par $\mathrm{X}^2, \mathrm{XY}$ et Y^2, et XY n'est pas un carré.

2) On a toujours $\mathrm{I}_1 \cdots \mathrm{I}_m \subseteq \mathrm{I}_1 \cap \cdots \cap \mathrm{I}_m$, et l'inclusion est en général stricte (prendre, par exemple, $\mathrm{I}_j = (a)$, pour tout j).

***Définition 13.3* (Idéaux étrangers).** — Soient $\mathrm{I}_1, \ldots, \mathrm{I}_n$ des idéaux de A.

1) On dit que $\mathrm{I}_1, \ldots, \mathrm{I}_n$ sont **étrangers** (ou *« premiers entre eux »*) si l'on a $\mathrm{I}_1 + \cdots + \mathrm{I}_n = \mathrm{A}$.

2) On dit que $\mathrm{I}_1, \ldots, \mathrm{I}_n$ sont **étrangers deux à deux** si I_r et I_s sont étrangers, pour tout $r \neq s$.

Remarque 13.4. — On prendra garde à ne pas confondre ces deux notions. Si $n \geqslant 3$, la deuxième condition est beaucoup plus forte que la première ! Pour éviter les confusions, on dira parfois dans le premier cas que $\mathrm{I}_1, \ldots, \mathrm{I}_n$ sont étrangers *« dans leur ensemble »* .

Lemme 13.5. — *Soient* I *et* J_1, *...,* J_m *des idéaux de* A *(les* J_i *n'étant pas nécessairement distincts). On suppose que* I *est étranger à chaque* J_i. *Alors* I *est étranger au produit* $\mathrm{J}_1 \cdots \mathrm{J}_m$.

Démonstration. — Par hypothèse, il existe, pour $i = 1, \ldots, m$, des éléments $x_i \in \mathrm{I}$ et $y_i \in \mathrm{J}_i$ 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 $\mathrm{J}_1 \cdots \mathrm{J}_m$, et une somme de termes qui contiennent au moins un x_i donc appartiennent à I. Ceci prouve le lemme. □

Corollaire 13.6. — *Supposons* $\mathrm{I}_1, \ldots, \mathrm{I}_n$ *étrangers deux à deux, et soient* m_1, $\ldots, m_n$ *des entiers* $\geqslant 1$.

1) *On a* $\mathrm{I}_1 \cdots \mathrm{I}_n = \mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n$.

2) $\mathrm{I}_1^{m_1}, \ldots, \mathrm{I}_n^{m_n}$ *sont étrangers deux à deux.*

3) *Posons, pour* $k = 1, \ldots, n$,

$$\mathrm{J}_k = \prod_{j \neq k} \mathrm{I}_j^{m_j}; \qquad \textit{alors} \qquad \mathrm{J}_1 + \cdots + \mathrm{J}_n = \mathrm{A},$$

c.-à-d., $\mathrm{J}_1, \ldots, \mathrm{J}_n$ *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 $x_1 \in \mathrm{I}_1$ et $x_2 \in \mathrm{I}_2$ tels que $x_1 + x_2 = 1$. Alors, pour tout $a \in \mathrm{I}_1 \cap \mathrm{I}_2$, l'on a :

$$a = a \cdot 1 = ax_1 + ax_2 \in \mathrm{I}_1\mathrm{I}_2,$$

d'où $\mathrm{I}_1\mathrm{I}_2 = \mathrm{I}_1 \cap \mathrm{I}_2$. D'autre part, d'après le lemme précédent, I_1 est étranger à $\mathrm{I}_2^{m_2}$, puis $\mathrm{I}_2^{m_2}$ est étranger à $\mathrm{I}_1^{m_1}$, ce qui prouve 2) dans le cas $n = 2$.

Supposons $n \geqslant 3$ et les deux assertions établies pour $n-1$. Par hypothèse de récurrence, $\mathrm{I}_2 \cap \cdots \cap \mathrm{I}_n = \mathrm{I}_2 \cdots \mathrm{I}_n$, et, d'après le lemme, cet idéal est étranger à I_1. On a donc

$$\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n = \mathrm{I}_1 \cap (\mathrm{I}_2 \cdots \mathrm{I}_n) = \mathrm{I}_1 \cdot \mathrm{I}_2 \cdots \mathrm{I}_n,$$

ce qui prouve 1). D'autre part, par hypothèse de récurrence, $\mathrm{I}_2^{m_2}, \ldots, \mathrm{I}_n^{m_n}$ sont étrangers deux à deux. De plus, d'après le cas $n = 2$, chaque $\mathrm{I}_k^{m_k}$ est étranger avec $\mathrm{I}_1^{m_1}$. L'assertion 2) est démontrée.

Démontrons l'assertion 3). D'abord, $\mathrm{I}_1^{m_1}, \ldots, \mathrm{I}_r^{m_r}$ 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 13.5, donc il existe $x_k \in \mathrm{I}_k$ et $y_k \in \mathrm{J}_k$ 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 $\mathrm{J}_1 + \cdots + \mathrm{J}_r$; le seul autre terme est $x_1 \cdots x_r$, qui appartient à J_k pour tout k. Ceci montre que $1 \in \mathrm{J}_1 + \cdots + \mathrm{J}_r$, ce qui termine la preuve du corollaire. □

Remarque 13.7. — a) On voit facilement que si un idéal premier P contient un produit d'idéaux $\mathrm{J}_1 \cdots \mathrm{J}_r$, alors il contient l'un des J_k.

b) En utilisant a) et le corollaire 12.11 (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 $\mathrm{I}_r^{m_r}$ et $\mathrm{I}_s^{m_s}$ ne soient pas étrangers. Alors $\mathrm{I}_r^{m_r} + \mathrm{I}_s^{m_s}$ est un idéal propre, donc est contenu dans un idéal maximal $\mathfrak{m}$. Comme $\mathfrak{m}$ est premier et contient $\mathrm{I}_r^{m_r}$ et $\mathrm{I}_s^{m_s}$, il contient I_r et I_s, ce qui contredit l'hypothèse $\mathrm{I}_r + \mathrm{I}_s = \mathrm{A}$.

13.2. Théorème chinois des restes. —

***Définition 13.8* (Produits d'anneaux)**. — Soit $(\mathrm{A}_i)_{i\in\mathrm{I}}$ une famille d'anneaux. Le groupe abélien $\prod_{i\in\mathrm{I}} \mathrm{A}_i$ est muni d'une structure d'anneau, où la multiplication est définie coordonnée par coordonnée :

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

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

$$\mathrm{A}_1 \times \cdots \times \mathrm{A}_n \quad \text{ou} \quad \mathrm{A}_1 \oplus \cdots \oplus \mathrm{A}_n.$$

***Théorème 13.9* (Théorème chinois des restes)**. — *On suppose* $\mathrm{I}_1, \ldots, \mathrm{I}_n$ *étrangers deux à deux. Alors le morphisme naturel* $\psi : \mathrm{A} \to \mathrm{A}/\mathrm{I}_1 \oplus \cdots \oplus \mathrm{A}/\mathrm{I}_n$ *induit un isomorphisme*

$$\mathrm{A}/(\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n) \xrightarrow{\sim} \bigoplus_{r=1}^{n} \mathrm{A}/\mathrm{I}_r.$$

Démonstration. — Il est clair que $\operatorname{Ker}\psi = \bigcap_{r=1}^{n} \mathrm{I}_r$. On va établir l'isomorphisme annoncé par récurrence sur n. Commençons par remarquer que, pour démontrer la surjectivité de ψ, il suffit de trouver $\varepsilon_1, \cdots, \varepsilon_n \in \mathrm{A}$ 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 $x_1 \in \mathrm{I}_1$ et $x_2 \in \mathrm{I}_2$ tels que $x_1 + x_2 = 1$. Alors $1 - x_1 = x_2$ appartient à $1 + \mathrm{I}_1$ 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 $n \geqslant 3$ et le théorème établi pour $n - 1$. D'après le lemme 13.5 et le corollaire 13.6, $\mathrm{I}_2 \cap \cdots \cap \mathrm{I}_n$ égale $\mathrm{I}_2 \cdots \mathrm{I}_n$ et est étranger à I_1. Donc, d'après le cas $n = 2$, la projection

$$\mathrm{A} \longrightarrow \mathrm{A}/\mathrm{I}_1 \bigoplus \mathrm{A}/(\mathrm{I}_2 \cap \cdots \cap \mathrm{I}_n)$$

induit un isomorphisme

$$\mathrm{A}/(\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n) \xrightarrow{\sim} \mathrm{A}/\mathrm{I}_1 \bigoplus \mathrm{A}/(\mathrm{I}_2 \cap \cdots \cap \mathrm{I}_n). \tag{1}$$

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

$$\mathrm{A}/(\mathrm{I}_2 \cap \cdots \cap \mathrm{I}_n) \xrightarrow{\sim} \bigoplus_{r=2}^{n} \mathrm{A}/\mathrm{I}_r. \tag{2}$$

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

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

Définition 13.10. — Pour tout $\lambda \in \Lambda$, on pose

$$\mathrm{M}_\lambda := \{m \in \mathrm{M} \mid \exists\, n \geqslant 1 \text{ tel que } \mathrm{I}_\lambda^n\, m = 0\};$$

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

Lemme 13.11. — *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 $x_k \in \mathrm{M}_{\lambda_k}$ pour tout k. Alors, il existe des entiers $n_1, \ldots, n_r \geqslant 1$ tels que

$$\mathrm{I}_{\lambda_k}^{n_k}\, x_k = 0, \qquad \text{pour } \ k = 1, \ldots, r.$$

Alors $x_1 = x_2 + \cdots + x_r$ est annulé par $\mathrm{I}_{\lambda_1}^{n_1}$ et par $\mathrm{I}_{\lambda_2}^{n_2} \cdots \mathrm{I}_{\lambda_r}^{n_r}$. Or, ces deux idéaux sont étrangers, d'après le corollaire 13.6. Ceci entraîne $x_1 = 0$, et le lemme en découle. □

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

Définition 13.12. — On dira que M est un A-module **de $\mathscr{I}$-torsion** si tout $m \in \mathrm{M}$ est annulé par un produit fini

$$\mathrm{I}_{\lambda_1}^{n_1} \cdots \mathrm{I}_{\lambda_r}^{n_r}. \tag{$*$}$$

Théorème 13.13 **(Décomposition des modules de $\mathscr{I}$-torsion)**
Soit $\mathscr{I} = (\mathrm{I}_\lambda)_{\lambda\in\Lambda}$ *une famille d'idéaux de* A*,* **deux à deux étrangers***, et soit* M *un* A*-module* **de $\mathscr{I}$-torsion***. Alors :*

$$\mathrm{M} = \bigoplus_{\lambda\in\Lambda} \mathrm{M}_\lambda. \tag{1}$$

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*

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

et $\mathrm{M}_\lambda = (0)$ *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* $\mathrm{I}_{\lambda_i}^{n_i}$ *de* I_{λ_i}.

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

$$\mathrm{J}_k = \prod_{j \neq k} \mathrm{I}_{\lambda_j}^{n_j}.$$

D'après le corollaire 13.6, $\mathrm{J}_1, \dots, \mathrm{J}_r$ sont étrangers, donc on peut écrire

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

où $y_k \in \mathrm{J}_k$. Chaque $y_k m$ est annulé par $\mathrm{I}_k^{n_k}$, 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 $x_1, \dots, x_n$. Chaque x_i a des composantes $x_{i,\lambda}$ non nulles seulement pour λ dans un ensemble fini d'indices Λ_i. Alors $\Lambda_1 \cup \cdots \cup \Lambda_n$ est un ensemble fini $\{\lambda_1, \dots, \lambda_r\}$, et l'on a

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

En comparant avec 1), on obtient $\mathrm{M}_\lambda = (0)$ 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 $\mathrm{I}_{\lambda_i}^{n_i}$ de I_{λ_i}. Le théorème est démontré. □

Exemples 13.14. — 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 $m_i \geqslant 1$ tels que

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

Donc, A est un A-module de $\mathscr{I}$-torsion, où

$$\mathscr{I} = \{\mathfrak{m}_1^{m_1}, \dots, \mathfrak{m}_r^{m_r}\}.$$

Il résulte donc du théorème précédent que

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

D'autre part, on peut aussi montrer que chaque A_i est isomorphe à l'anneau *localisé* $\mathrm{A}_{\mathfrak{m}_i}$ (voir un chapitre ultérieur sur la localisation) et l'on obtient un isomorphisme d'anneaux

$$\mathrm{A} \cong \mathrm{A}_{\mathfrak{m}_1} \times \cdots \times \mathrm{A}_{\mathfrak{m}_r}.$$

(Le slogan à retenir est : une k-algèbre de dimension finie est le produit de ses localisés en ses idéaux maximaux.)

13.4. Décomposition primaire des modules de torsion sur un anneau principal. —

Soit A un anneau principal.

***Définition 13.15* (Idéaux maximaux de A).** — Notons $\mathscr{P}$ l'ensemble des idéaux (p), où p est irréductible ; ce sont les idéaux maximaux de A (Th. 9.26). En particulier, les éléments de $\mathscr{P}$ sont deux à deux étrangers.

***Remarque 13.16*.** — $\mathscr{P}$ 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 13.17*.** — *Tout idéal propre* $\mathrm{I} \neq (0)$ *s'écrit de façon unique comme un produit* $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ *d'éléments de* $\mathscr{P}$.

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

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

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

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

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 $i = 1, \ldots, n$. Ceci prouve l'unicité. □

***Définition 13.18* (Composantes primaires).** — 1) Soient M un A-module et $p \in \mathrm{A}$ un élément irréductible. On pose

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

C'est un sous-module de $\mathrm{M}_{\mathrm{tors}}$, appelé la **composante p-primaire**.

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

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

Lemme 13.19. — *Soit* M *un* A*-module p-primaire.*

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

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

Démonstration. — Posons $\mathrm{Ann}(x) = (a)$; c'est un idéal propre, puisque $x \neq 0$. D'autre part, par hypothèse, il existe $t \geqslant 1$ 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 $1 \leqslant n \leqslant t$. Ceci prouve la première 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

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

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

Lemme 13.20. — *Soit* M *un* A*-module. La somme des sous-modules* $\mathrm{M}_{\mathfrak{p}}$*, pour* $\mathfrak{p} \in \mathscr{P}$*, est une somme directe.*

Démonstration. — C'est une conséquence du lemme 13.11. Répétons la démonstration, pour la commodité du lecteur.

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

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

où $x_k \in \mathrm{M}_{\mathfrak{p}_k}$ pour tout k. Il existe des entiers $n_1, \ldots, n_r \geqslant 1$ tels que

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

Alors $x_1 = x_2 + \cdots + x_r$ est annulé par $\mathfrak{p}_1^{n_1}$ et par $\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$. Or, ces deux idéaux sont étrangers, d'après le corollaire 13.6. Ceci entraîne $x_1 = 0$, et le lemme en découle. □

Théorème 13.21 **(Décomposition primaire des modules de torsion sur un anneau principal)**

Soient A *un anneau principal et* M *un* A*-module* **de torsion**. *Alors*

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

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

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

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

Démonstration. — Ceci découle du théorème 13.13, combiné avec le lemme 13.19. Pour la commodité du lecteur, répétons la démonstration, sans faire référence au théorème 13.13.

1) On a déjà vu que la somme des $\mathrm{M}(\mathfrak{p})$ est directe. Montrons qu'elle vaut M. Soit $m \in \mathrm{M}$, non nul. Comme M est de torsion, $\mathrm{Ann}(m)$ est non nul donc, d'après le lemme 13.17, on a

$$\mathrm{Ann}(m) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$$

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

$$\mathrm{J}_k = \prod_{j \neq k} \mathfrak{p}_j^{n_j}.$$

D'après le corollaire 13.6, les idéaux $\mathrm{J}_1, \ldots, \mathrm{J}_r$ sont étrangers dans leur ensemble, donc on peut écrire

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

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

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

Ceci prouve 1).

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

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

De plus, chaque $\mathrm{M}(\mathfrak{p}_i)$, étant un quotient de M, est de type fini, donc $\mathrm{Ann}\ \mathrm{M}(p_i) = \mathfrak{p}_i^{n_i}$, pour un certain $n_i \geqslant 1$, d'après le lemme 13.19.

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

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

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

Corollaire 13.22 **(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 :*

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

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

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

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

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

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

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

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

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

L'assertion 1) en découle.

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

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

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

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

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

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

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

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

avec $a_0, b_0, \ldots, a_n, b_n \in \mathrm{A}$ et $\rho(p) > \rho(a_i), \rho(b_i)$ 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 $n \geqslant 1$ et l'assertion établie pour $n-1$. Il résulte de (3) que $a_0 - b_0 = p\alpha$, avec $\alpha \in \mathrm{A}$. Si on avait $\alpha \neq 0$, on aurait

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

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

Corollaire 13.24 **(Décomposition des fractions rationnelles en éléments simples)**
Soient k un corps et $k(\mathrm{X})$ le corps des fractions rationnelles sur k. Notons $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires de $k[\mathrm{X}]$.

1) *Tout élément $\mathrm{F} \in k(\mathrm{X})$ s'écrit de façon unique comme une somme finie*

$$\mathrm{F} = \mathrm{E} + \sum_{\mathrm{P} \in \mathscr{P}} \sum_{j \geqslant 1} \frac{a_{\mathrm{P},j}}{\mathrm{P}^j},$$

avec E et les $a_{\mathrm{P},j}$ dans $k[\mathrm{X}]$, nuls sauf pour un nombre fini d'indices, et $\deg(a_{\mathrm{P},j}) < \deg \mathrm{P}$ pour tout P et j.

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

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

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

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

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

où $\mathrm{E} \in \mathbb{R}[\mathrm{X}]$ 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 $\deg : k[\mathrm{X}] \setminus \{0\} \to \mathbb{N}$ vérifie l'hypothèse $(**)$.

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

Remarque 13.25. — 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 $\mathbb{Z} \to \mathbb{N}$ 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 $0 \leqslant r < n$.

14. Modules de type fini sur un anneau principal

14.1. 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.

Théorème 14.1 **(Structure des modules de type fini sur un anneau principal)**
Soit A *un anneau principal.*

1) *Soient* $n \geqslant 1$ *et* N *un sous-module non nul du* A*-module libre* A^n*. Alors,* N *est libre de rang* $r \leqslant n$ *et il existe :*

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

et les idéaux $(a_r) \subseteq \cdots \subseteq (a_1)$ *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*

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

2) *Soit* M *un* A*-module de type fini. Il existe* $r, s \geqslant 0$ *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*

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

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

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

En particulier :

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

De plus, les idéaux $(a_r) \subseteq \cdots \subseteq (a_1)$ *sont uniquement déterminés. On les appelle les* **idéaux (ou facteurs) invariants** *de* M.

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

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

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

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

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

Définition 14.2 **(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 14.3 **(Réduction des matrices sur un anneau principal)**

Soit A *un anneau principal et soit* $\mathrm{F} \in \mathrm{M}_{n,m}(\mathrm{A})$ *non nulle. Alors, il existe* $r \geqslant 1$*, des matrices inversibles* $\mathrm{P} \in \mathrm{GL}_n(\mathrm{A})$, $\mathrm{Q} \in \mathrm{GL}_m(\mathrm{A})$*, et des éléments* $a_1, \ldots, a_r$ *de* A*, vérifiant* $a_i \mid a_{i+1}$ *pour* $i < r$*, tels que*

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

De plus, r *et les idéaux* $(a_1), \ldots, (a_r)$ *sont entièrement déterminés par* F.

Démonstration de l'équivalence. — La matrice F définit un morphisme de A-modules $\phi : \mathrm{A}^m \to \mathrm{A}^n$, 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 $\mathscr{B} = (e_1, \ldots e_m)$ de A^m et $\mathscr{C} = (f_1, \ldots, f_n)$ 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 $x_1, \ldots, x_m$ et est donc l'image d'un morphisme de A-modules

$$\phi : \mathrm{A}^m \longrightarrow \mathrm{A}^n.$$

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

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

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 $(f'_1, \ldots, f'_n)$ est une base de A^n et si $a'_1, \ldots, a'_s$ sont des éléments de A tels que $a'_i \mid a'_{i+1}$ pour $i < s$, et que $(a'_1 f'_1, \ldots, a'_s f'_s)$ soit une base de $\mathrm{N} = \mathrm{Im}(\phi)$, alors l'unicité énoncée dans le théorème de réduction entraîne que $s = r$ et $(a'_i) = (a_i)$ pour $i = 1, \ldots, r$. Ceci montre que le théorème de réduction 14.3 entraîne le point 1) du théorème de structure 14.1.

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

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

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

$$\mathrm{A}^m = \mathrm{A}e_1 + \cdots + \mathrm{A}e_r + \mathrm{Ker}\,\phi,$$

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

$$\mathrm{A}^m = \mathrm{A}e_1 \oplus \cdots \oplus \mathrm{A}e_r \oplus \mathrm{Ker}\,\phi.$$

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

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

Alors, la matrice de ϕ dans les bases $\mathscr{B}$ et $\mathscr{C}$ est de la forme voulue. De plus, les idéaux (a_i) sont uniquement déterminés par $\mathrm{N} = \mathrm{Im}(\phi)$, donc par ϕ. Ceci prouve que le point 1) du théorème de structure 14.1 entraîne le théorème de réduction 14.3. □

Pour démontrer les deux théorèmes précédents, il y a donc deux approches. On peut démontrer d'abord le théorème de réduction 14.3, d'où le point 1) du théorème de structure 14.1. On montre ensuite les points 1′)–3).

Ou bien, on peut démontrer d'abord le théorème de structure 14.1, 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).

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

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

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

$$\begin{pmatrix} 14 & 21 & 30 & 35 \\ 21 & 14 & 12 & 42 \\ 30 & 20 & 28 & 15 \end{pmatrix} \xrightarrow{\mathrm{L}_1 \to \mathrm{L}_1 - \mathrm{L}_3} \begin{pmatrix} -16 & 1 & 2 & 20 \\ 21 & 14 & 12 & 42 \\ 30 & 20 & 28 & 15 \end{pmatrix},$$

puis $\mathrm{C}_3 \to -\mathrm{C}_3 + 2\mathrm{C}_2$ et $\mathrm{C}_4 \to -\mathrm{C}_4 - \mathrm{C}_1 + 4\mathrm{C}_2$ donnent

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

Alors, $\mathrm{C}_1 \to \mathrm{C}_1 + 3\mathrm{C}_4$ et $\mathrm{C}_2 \to \mathrm{C}_2 + 2\mathrm{C}_4$ 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 :

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

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 $\mathrm{L}_3 + a\mathrm{L}_2$ on se ramène à $a = 0$.

Remplaçons, de plus, C_1 par $\mathrm{C}_1 + 16\mathrm{C}_2$. Comme

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

alors, posant

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

on obtient la matrice

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

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

Enfin, comme $90 \equiv -1$ mod. 7, on obtient que $\mathrm{Im}(\mathrm{F})$ 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

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

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

Définition 14.4. — Pour tout $s \geqslant 1$, on note $\mathrm{GL}_s(\mathrm{A})$ le groupe des matrices $\mathrm{P} \in \mathrm{M}_s(\mathrm{A})$ qui sont **inversibles**, c.-à-d., telles qu'il existe $\mathrm{Q} \in \mathrm{M}_s(\mathrm{A})$ vérifiant

$$\mathrm{PQ} = \mathrm{I}_s = \mathrm{QP}.$$

Dans ce cas, $\mathrm{dét}(\mathrm{P})\,\mathrm{dét}(\mathrm{Q}) = 1$, donc $\mathrm{dét}(\mathrm{P})$ est un élément inversible de A. Réciproquement, cette condition est suffisante, car si $\widetilde{\mathrm{A}}$ 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

$${}^t\widetilde{\mathrm{A}}\mathrm{A} = \mathrm{dét}(\mathrm{A})\mathrm{I}_s = \mathrm{A}\,{}^t\widetilde{\mathrm{A}}.$$

Définition 14.5 **(Matrices équivalentes)**. — Soient $m, n \geqslant 1$. On dit que deux matrices $\mathrm{F}, \mathrm{F}' \in \mathrm{M}_{n,m}(\mathrm{A})$ sont **équivalentes** s'il existe $\mathrm{P} \in \mathrm{GL}_n(\mathrm{A})$ et $\mathrm{Q} \in \mathrm{GL}_m(\mathrm{A})$ telles que $\mathrm{F}' = \mathrm{PFQ}$.

Remarque 14.6. — Soit u le morphisme de A-modules $\mathrm{A}^m \to \mathrm{A}^n$ défini par F. Comme multiplier F à droite (resp. à gauche) par une matrice inversible $\mathrm{Q} \in \mathrm{GL}_m(\mathrm{A})$ (resp. $\mathrm{P} \in \mathrm{GL}_n(\mathrm{A})$) 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 $\mathscr{B}$ de A^m et $\mathscr{C}$ de A^n telles que F' soit la matrice de u dans ces bases.

Définition 14.7 **(Idéaux de Fitting)**. — Soit $\mathrm{F} \in \mathrm{M}_{n,m}(\mathrm{A})$.

1) Pour tout $i \leqslant \min(m,n)$, on note $\mathrm{J}_i(\mathrm{F})$ l'idéal de A engendré par les mineurs $i \times i$ de F. On convient que $\mathrm{J}_0(\mathrm{F}) = \mathrm{A}$.

2) Le **rang** de F est le plus grand entier $r \geqslant 0$ tel que $\mathrm{J}_r(\mathrm{F}) \neq 0$, c.-à-d., le plus grand entier r tel qu'il existe un mineur $r \times r$ de F qui soit nul.

Les idéaux $\mathrm{J}_i(\mathrm{F})$ ne dépendent que de la classe d'équivalence de F, d'après la proposition suivante.

Proposition 14.8. — 1) *Soient* $\mathrm{F} \in \mathrm{M}_{n,m}(\mathrm{A})$, $\mathrm{P} \in \mathrm{M}_n(\mathrm{A})$ *et* $\mathrm{Q} \in \mathrm{M}_m(\mathrm{A})$. *Pour tout* i, *on a* $\mathrm{J}_i(\mathrm{PF}) \subseteq \mathrm{J}_i(\mathrm{F})$ *et* $\mathrm{J}_i(\mathrm{FQ}) \subseteq \mathrm{J}_i(\mathrm{F})$.

2) *Si* F *et* F' *sont équivalentes, on a* $\mathrm{J}_i(\mathrm{F}) = \mathrm{J}_i(\mathrm{F}')$ *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 $\mathrm{J}_i(\mathrm{PF}) \subseteq \mathrm{J}_i(\mathrm{F})$. On obtient de même que $\mathrm{J}_i(\mathrm{FQ}) \subseteq \mathrm{J}_i(\mathrm{F})$.

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

$$\mathrm{J}_i(\mathrm{F}') \subseteq \mathrm{J}_i(\mathrm{F}) \subseteq \mathrm{J}_i(\mathrm{F}'),$$

d'où $\mathrm{J}_i(\mathrm{F}) = \mathrm{J}_i(\mathrm{F}')$ pour tout i. La proposition est démontrée. □

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

Théorème 14.9 **(Réduction des matrices sur un anneau principal)**

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

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

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

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

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 $m, n \geqslant 3$) ; 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 $\sigma \in \mathrm{S}_n$. Effectuer sur les lignes de F la permutation σ équivaut à multiplier F à gauche par la matrice de permutation $\mathrm{M}(\sigma) \in \mathrm{GL}_n(\mathrm{A})$ définie par :

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

où $(f_1, \dots, f_n)$ est la base canonique de A^n. En d'autres termes, $\mathrm{M}(\sigma)$ 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 $\mathrm{M}(\sigma)$ est inversible, d'inverse $\mathrm{M}(\sigma^{-1})$.

De même, on voit que multiplier F à droite par une matrice de permutation $\mathrm{M}'(\tau)$ (où $\tau \in \mathrm{S}_m$), 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 $\mathrm{T}_{ij}(\alpha)$ **et** $\mathrm{T}'_{k\ell}(\beta)$**.** 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

$$\mathrm{T}_{i,j}(\alpha) = \mathrm{I}_n + \alpha \mathrm{E}_{i,j},$$

qui est clairement inversible, d'inverse $\mathrm{T}_{i,j}(-\alpha)$. (On rappelle que I_n désigne la matrice identité et que $\mathrm{E}_{i,j}$ 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

$$\mathrm{T}'_{k\ell}(\beta) = \mathrm{I}_m + \beta \mathrm{E}_{k\ell}.$$

III) Les matrices de Bézout $\mathrm{B}_i(a,b)$ et $\mathrm{B}'_j(a,b)$. Soient $a, b \in \mathrm{A} \setminus \{0\}$ et soit d un pgcd de a et b. D'après le théorème de Bézout, il existe $x, y \in \mathrm{A}$ tels que $ax + by = d$. On note $\mathrm{B}_2(a,b)$ la matrice suivante de $\mathrm{GL}_n(\mathrm{A})$:

$$\mathrm{B}_2(a,b) = \left(\begin{array}{cc|c} x & y & \\ -b/d & a/d & 0 \\ \hline 0 & & \mathrm{I}_{n-2} \end{array}\right).$$

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

Alors, la matrice $\mathrm{B}_2(a,b)\mathrm{F}$ 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. $\mathrm{B}_2(a,b)\mathrm{F}$), on a pour tout j :

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

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 $\mathrm{B}_2(a,b)\mathrm{F}$ 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 de la matrice $\mathrm{B}_2(a,b)$.

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

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

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

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

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 $\mathrm{B}_i(a,b)\mathrm{F}$ est identique à celle de F, sauf qu'on a remplacé a par $d = \mathrm{pgcd}(a,b)$ et b par 0.

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

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

et $b'_{kj} = 0$ dans les autres cas. Comme précédemment, $\mathrm{B}'_j(a,b)$ 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 $\mathrm{FB}'_j(a,b)$ est identique à celle de F, sauf qu'on a remplacé a par $d = \mathrm{pgcd}(a,b)$ et b par 0.

Remarque 14.10. — Les matrices $\mathrm{T}_{1i}(\alpha)$ et $\mathrm{T}'_{1\ell}(\beta)$ 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 $\geqslant 0$ 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 14.11. — Soit $a \in \mathrm{A} \setminus \{0\}$. 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 $s \geqslant 1$.

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

$$\mathrm{F}_1 = \begin{pmatrix} d_1 & 0 \\ 0 & \mathrm{B} \end{pmatrix}$$

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

i) Annulation des coefficients f_{1j}, pour $j \geqslant 2$. Si f_{11} divise tous les f_{1j}, pour $j \geqslant 2$, on remplace chaque colonne C_j, pour $j \geqslant 2$, par la colonne $\mathrm{C}_j - f_{1j}/f_{11}\mathrm{C}_1$.

Sinon, s'il existe $k \geqslant 2$ tel que f_{11} ne divise pas f_{1k}, on multiplie F à droite par la matrice de Bézout $\mathrm{B}'_{1k}(f_{11}, f_{1k})$. 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 répète le processus. On arrive ainsi, en au plus $m-1$ opérations, à une matrice équivalente

$$\mathrm{F}' = \mathrm{FQ},$$

dont la 1ère ligne est $(f'_{11}, 0, \ldots, 0)$, 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 $i \geqslant 2$. Si f'_{11} divise tous les f'_{i1}, pour $i \geqslant 2$, on remplace chaque ligne L_i, pour $i \geqslant 2$, par la ligne $\mathrm{L}_i - f'_{i1}/f'_{11}\mathrm{L}_1$. 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 $i \geqslant 2$ 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

$$\mathrm{F}'' = \mathrm{PF}' = \mathrm{PFQ},$$

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 :

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

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

$$(\mathrm{I}_n + \mathrm{E}_{1i})\mathrm{F}_1 = \begin{pmatrix} d_1 & c_{i2} & \cdots & c_{im} \\ 0 & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix},$$

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

$$\mathrm{F}'_1 = \begin{pmatrix} d'_1 & 0 & \cdots & 0 \\ 0 & c'_{22} & \cdots & c'_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c'_{n2} & \cdots & c'_{nm} \end{pmatrix},$$

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 ($\leqslant \ell(d_1)$) d'aller-retour entre les étapes **1)** et **2)**, une matrice équivalente F_2 de la forme

$$\mathrm{F}_2 = \begin{pmatrix} a_1 & 0 \\ 0 & \mathrm{B} \end{pmatrix},$$

où a_1 divise chaque coefficient de $\mathrm{B} \in \mathrm{M}_{n-1,m-1}(\mathrm{A})$. On observe alors que a_1 est un générateur de l'idéal $\mathrm{J}_1(\mathrm{F}_2)$, qui égale $\mathrm{J}_1(\mathrm{F})$ d'après la proposition 14.8. 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

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

où $a_i \mid a_{i+1}$ pour $i = 2, \ldots, r-1$. D'une part, a_2 est un générateur de $\mathrm{J}_1(\mathrm{PBQ}) = \mathrm{J}_1(\mathrm{B})$, lequel est contenu dans $\mathrm{J}_1(\mathrm{F}_2) = (a_1)$. Par conséquent, a_1 divise a_2. D'autre part, F_2, et donc F, est semblable à la matrice

$$\mathrm{F}_3 = \begin{pmatrix} a_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & a_r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}.$$

Ceci achève la démonstration de l'existence dans le théorème 14.9.

De plus, d'après la proposition 14.8, on a :

$$\forall\, s \leqslant \min(m,n), \qquad \mathrm{J}_s(\mathrm{F}) = \mathrm{J}_s(\mathrm{F}_3).$$

Or les idéaux $\mathrm{J}_s(\mathrm{F}_3)$ se calculent facilement : F_3 est de rang r, et pour $s \leqslant r$ 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

$$\mathrm{J}_s(\mathrm{F}) = (a_1 \cdots a_s), \qquad \forall\, s = 1, \ldots, r.$$

Enfin, comme A est intègre, on voit que

$$(a_i) = \{x \in \mathrm{A} \mid x\mathrm{J}_{i-1}(\mathrm{F}) \subseteq \mathrm{J}_i(\mathrm{F})\}.$$

Ceci montre que les idéaux (a_i) sont déterminés par les $\mathrm{J}_s(\mathrm{F})$, et donc ne dépendent que de la classe d'équivalence de F. Ceci termine la démonstration du théorème 14.9. □

On obtient donc le point 1) du théorème de structure 14.1, d'après l'équivalence établie après le théorème 14.3. Montrons le point 1′).

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

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

D'une part, comme $a_i e_i \in \mathrm{N}$ pour $i = 1, \ldots, r$, on a $\mathrm{M}_1 \subseteq \mathrm{N}'$. D'autre part, comme $\mathrm{M} = \mathrm{M}_1 \oplus \mathrm{M}_2$, alors M/M_1 est isomorphe à M_2 et donc libre. Ceci entraîne l'inclusion $\mathrm{N}' \subseteq \mathrm{M}_1$. En effet, soit $x \in \mathrm{N}'$. Il existe $a \in \mathrm{A} \setminus \{0\}$ tel que $ax \in \mathrm{N} \subseteq \mathrm{M}_1$, donc l'image de x dans M/M_1 est un élement de torsion. Comme ce module est libre, donc sans torsion, ceci entraîne $x \in \mathrm{M}_1$. Ceci prouve l'égalité $\mathrm{M}_1 = \mathrm{N}'$, et 1′) est démontré. □

14.4. 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 14.1. Commençons par le lemme ci-dessous.

Lemme 14.12. — *Soient* B *un anneau et* $\mathrm{M}_1, \ldots, \mathrm{M}_n$ *des* B*-modules. Pour* $i = 1, \ldots, n$*, soit* N_i *un sous-module de* M_i *et soit* $\pi_i : \mathrm{M}_i \to \mathrm{M}_i/\mathrm{N}_i$*. Alors, le noyau du morphisme*

$$\bigoplus_{i=1}^{n} \mathrm{M}_i \longrightarrow \bigoplus_{i=1}^{n} (\mathrm{M}_i/\mathrm{N}_i), \quad (x_1, \ldots, x_n) \mapsto (\pi_1(x_1), \ldots, \pi_n(x_n))$$

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

$$(\bigoplus_{i=1}^{n} \mathrm{M}_i)/(\bigoplus_{i=1}^{n} \mathrm{N}_i) \cong (\mathrm{M}_1/\mathrm{N}_1) \bigoplus \cdots \bigoplus (\mathrm{M}_n/\mathrm{N}_n).$$

Démonstration. — La première assertion est claire, et la seconde en découle, d'après le théorème 4.10. □

Revenons au théorème 14.1 et montrons le **point 2).** Soit M un A-module de type fini. Soit $\{x_1, \ldots, x_n\}$ un système de générateurs de M et soit $\phi : \mathrm{A}^n \to \mathrm{M}$ le morphisme de A-modules envoyant tout $(b_1, \ldots, b_n)$ sur $b_1 x_1 + \cdots + b_n x_n$. Alors, ϕ induit un isomorphisme

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

D'après le point 1) du théorème, il existe une base $(e_1, \dots, e_n)$ de A^n, un entier $r \leqslant n$, 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

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

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

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

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

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

Remarque 14.13. — 1) On a choisi un système de générateurs $x_1, \dots, x_n$ de M, donnant lieu au morphisme surjectif $\phi : \mathrm{A}^n \to \mathrm{M}$. Ce choix étant fait, il est clair que $(a_1), \dots, (a_r)$ sont les idéaux invariants du sous-module $\operatorname{Ker}(\phi) \subseteq \mathrm{A}^n$.

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 14.9.

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 :

$$\mathrm{A}/\mathrm{I}_1 \oplus \cdots \oplus \mathrm{A}/\mathrm{I}_r$$

où $\mathrm{I}_1 \subseteq \cdots \subseteq \mathrm{I}_r \neq \mathrm{A}$. Attention, ici on suppose la suite $(\mathrm{I}_k)_{k=1,\dots,r}$ croissante ! (Donc, dans la situation du théorème 14.1, on aurait $(a_k) = \mathrm{I}_{r+1-k}$ 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

$$\bigwedge^k(\mathrm{M}),$$

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 $\mathrm{M} = \mathrm{M}_{\mathrm{tors}}$ et soit $(a) = (p_1)^{m_1} \cdots (p_n)^{m_n}$ son annulateur. D'après le théorème 13.21, on a

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

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

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

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

Or, d'après le lemme 13.19, l'annulateur de tout élément non nul de $\mathrm{M}(p_i)$ est une puissance de (p_i). Par conséquent, il existe une suite

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

telle que

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

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

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

Lemme 14.14. — *Soient* A *un anneau intègre et* $p \in \mathrm{A} \setminus \{0\}$. *Pour tout* $i \geqslant 0$, *l'application*

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

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

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

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

Il est clairement surjectif. De plus, comme A est intègre, p^{i+1} divise ap^i ssi p divise a. Par conséquent, $\operatorname{Ker} \phi = (p)$ et ϕ induit un isomorphisme de A-modules $\mathrm{A}/(p) \cong (p^i)/(p^{i+1})$. C'est aussi un isomorphisme de $\mathrm{A}/(p)$-modules, d'après le corollaire 12.34. □

Théorème 14.15 **(Unicité des facteurs invariants)**. — *Soit* A *un anneau principal et soit* M *un* A*-module de torsion de type fini. Soient* $a_1, \ldots, a_r$ *des éléments*

non nuls et non inversibles de A *vérifiant* $a_i \mid a_{i+1}$ *pour tout* i*, et tels que*

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

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 $\mathrm{M} = \mathrm{M}(p)$. Dans ce cas, il existe des entiers $n_1 \leqslant \cdots \leqslant n_r$ 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 $\mathrm{A}/(p^{n_i})$ pour lesquels $n_i < k$. D'autre part, $\mathrm{K} = \mathrm{A}/(p)$ est un corps, puisque (p) est un idéal maximal. Donc, d'après le lemme précédent, on obtient que

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

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

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

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

Démontrons maintenant le théorème dans le cas général. Supposons que

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

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

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

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

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

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

$$(*) \qquad 0 \leqslant v_j(1) \leqslant \cdots \leqslant v_j(r).$$

Alors, d'après le théorème chinois,

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

et donc

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

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

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

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. □

Remarque 14.16. — On verra plus bas (14.5) 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 14.1.

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

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

sont les facteurs invariants de M/N, donc sont entièrement 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 14.1 n'utilisant pas le théorème de réduction des matrices.

Remarque 14.17. — 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].

14.5. Autre démonstration. — [(6)] 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 14.18* (Matrices échelonnées).** — Soit $\mathrm{P} \in \mathrm{M}_{nr}(\mathrm{A})$ une matrice à n lignes et r colonnes. Notons p_{ij} les coefficients de P et $\mathrm{P}_1, \ldots, \mathrm{P}_r$ ses colonnes. On suppose que chaque colonne P_j est non nulle. On définit la *longeur* $\ell(\mathrm{P}_j)$ de la colonne P_j comme étant le plus grand $i \in \{1, \ldots, n\}$ tel que $p_{ij} \neq 0$. On dit alors que P est une matrice **échelonnée** si l'on a $\ell(\mathrm{P}_1) < \cdots < \ell(\mathrm{P}_r)$.

Par exemple, la matrice suivante, dans $\mathrm{M}_{6,3}(\mathbb{Z})$, 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 14.19. — *Soient* A *principal et* M *un* A*-module libre de rang* n*. Tout sous-module de* M *est libre de rang* $r \leqslant n$*.* (*On convient que le module* (0) *est libre de rang* 0)*.*

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

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

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

Supposons donc $\mathrm{J}_i = (a) \neq 0$. Alors il existe

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

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

$$\mathrm{N}_i = \mathrm{N}_{i-1} \oplus \mathrm{A}v_{s+1},$$

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

[(6)] Ce paragraphe n'a pas été traité en cours

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 $a \in \mathrm{A}$. De plus, $\mathrm{N}' = \mathrm{A}$ dans ce cas.

Supposons $n \geqslant 2$ et le théorème démontré pour $n-1$. Notons $(\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $\mathrm{M} := \mathrm{A}^n$ et $(\varepsilon_1^*, \ldots, \varepsilon_n^*)$ la base duale de M^* (cf. 12.24). Comme N est supposé non nul, il existe un indice i tel que $\varepsilon_i^*(\mathrm{N}) \neq 0$.

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

Lemme 14.20. — *Pour tout $g \in \mathrm{M}^*$, a divise $g(x)$.*

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

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

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

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

$$(*) \qquad \mathrm{M} = \mathrm{A}e_1 \oplus \operatorname{Ker} f_0 \quad \text{et} \quad \mathrm{N} = \mathrm{A}x \oplus (\mathrm{N} \cap \operatorname{Ker} f_0).$$

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

$$\mathrm{M} = \operatorname{Ker} f_0 \oplus \mathrm{A}e_1.$$

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

Lemme 14.21. — *On a $f(\mathrm{N}) \subseteq (a)$, pour tout $f \in \mathrm{M}^*$.*

Démonstration. — Posons $\mathrm{K} = \operatorname{Ker} f_0$; on a $\mathrm{M} = \mathrm{K} \oplus \mathrm{A}e_1$. Alors K^* s'identifie au sous-module

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

de M^*, et l'on a $\mathrm{M}^* = \mathrm{K}^* \oplus \mathrm{A}f_0$ (car $f_0(e_1) = 1$). Comme $\mathrm{N} = (\mathrm{N} \cap \mathrm{K}) \oplus \mathrm{A}ae_1$, pour prouver le lemme il suffit donc de montrer que $g(\mathrm{N} \cap \mathrm{K}) \subseteq (a)$ pour tout $g \in \mathrm{K}^*$.

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

D'après la proposition 14.19, le sous-module $\mathrm{Ker}\, f_0$ est libre, disons de rang s. Comme $\mathrm{M} \cong \mathrm{Ker}\, f_0 \oplus \mathrm{A}e_1$, alors $n = s+1$ (car une base de M est obtenue en adjoignant e_1 à une base de $\mathrm{Ker}\, f_0$). Donc $s = n-1$. Par hypothèse de récurrence, appliquée au sous-module $\mathrm{N} \cap \mathrm{Ker}\, f_0$ de $\mathrm{Ker}\, f_0$, on obtient qu'il existe une base $(e_2, \ldots, e_n)$ de $\mathrm{Ker}\, f_0$ et $a_2, \ldots, a_n \in \mathrm{A} \setminus \{0\}$, tels que $(a_2 e_2, \ldots, a_n e_n)$ soit une base de $\mathrm{N} \cap \mathrm{Ker}\, f_0$ et $a_i \mid a_{i+1}$ pour $i = 2, \ldots, r-1$.

Alors, d'après $(*)$, $(e_1, \ldots, e_n)$ est une base de M et $(ae_1, a_2 e_2, \ldots, a_n e_n)$ une base de N. Soit $(e_1^*, \ldots, e_n^*)$ la base duale de M^*. Alors a_2 appartient à $e_2^*(\mathrm{N})$ donc est divisible par a, d'après le lemme 14.21. Ceci achève la démonstration de l'existence d'une base adaptée. □

TABLE DES MATIÈRES

I. Les anneaux de la géométrie algébrique ou de la théorie des nombres 1
1. Courbes algébriques et fonctions polynomiales 1
1.1. Courbes algébriques 1
1.2. Fonctions polynomiales 2
1.3. Espaces tangents 4
1.4. Sous-variétés algébriques de $\mathbb{C}^n$ 4
1.5. Morphismes 6
1.6. Fonctions rationnelles 7
1.7. Sujet du cours 8
2. Anneaux de nombres 8
2.1. Notations et définitions 8
2.2. Division euclidienne et conséquences 9
2.3. Solutions entières de $x^2 + y^2 = z^2$ 13
2.4. Somme de deux carrés et entiers de Gauss 14
2.5. Les anneaux de nombres $\mathbb{Z}[\sqrt{n}\,]$ 18
2.6. Les anneaux $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ 20
2.7. Entiers algébriques 21

II. Anneaux et modules 25
3. Anneaux et modules 25
3.0. Complément d'introduction 25
3.1. Anneaux 25
3.2. Morphismes 27
3.3. A-modules 28
4. Modules et anneaux quotients, théorèmes de Noether 31
4.1. Définition des modules quotients 31
4.2. Noyaux et théorèmes de Noether 34

5. Construction de modules ou d'idéaux 37
5.1. Sous-module ou idéal engendré 37
5.2. Sommes de sous-modules et sommes directes 38
5.3. Sommes et produits d'idéaux 39
5.4. Racine d'un idéal, et idéaux premiers 40
6. Modules libres 42
6.1. Définitions et exemples 42
6.2. Les modules libres $A^{(I)}$ 44

III. Anneaux de polynômes, conditions de finitude 47
7. Anneaux de polynômes 47
7.1. Polynômes en une variable 47
7.2. Polynômes à n variables 49
8. Conditions de finitude 51
8.1. Union filtrante de sous-modules 51
8.2. Modules de type fini 52
8.3. Anneaux et modules noethériens 55
8.4. Le théorème de transfert de Hilbert 57

IV. Anneaux factoriels, principaux, euclidiens

Semaine du 1er octobre 61
9. Anneaux factoriels 61
9.1. Une motivation 61
9.2. Anneaux intègres 61
9.3. Divisibilité, éléments irréductibles 62
9.4. Anneaux factoriels, lemmes d'Euclide et Gauss 65
9.5. Anneaux principaux et anneaux euclidiens 67
9.6. PPCM et PGCD dans un anneau factoriel 69
9.7. Corps des fractions d'un anneau intègre 71
9.8. Corps des fractions d'un anneau factoriel 73
9.9. Le théorème de transfert de Gauss 73
9.10. Sous-variétés algébriques fermées de $\mathbb{C}^2$ 77
9.11. Exemples d'anneaux noethériens non factoriels 80

V. Extensions algébriques, théorème des zéros

Semaine du 8 octobre 83
10. Extensions de corps 83
10.1. Généralités sur les extensions de corps 83
10.2. L'alternative algébrique/transcendant 85
10.4. Extensions algébriques et degré 86
10.5. Corps algébriquement clos 89
10.6. $\mathbb{C}$ est algébriquement clos 89

11. Le théorème des zéros de Hilbert 91
11.1. Idéaux maximaux de $\mathbb{C}[X_1, \ldots, X_n]$ 91
11.2. Sous-variétés algébriques de $\mathbb{C}^n$ 92
11.3. Composantes irréductibles 95
11.4. Topologie de Zariski 97

VI. Compléments sur les modules, théorème chinois, facteurs invariants

Séances du 15, 16 et 22 octobre 99
12. Compléments sur les modules 99
12.1. Théorème de Zorn et conséquences 99
12.2. Rang d'un module libre de type fini 101
12.3. Annulateurs et modules de torsion 102
12.4. Modules d'homomorphismes et module dual 103
12.5. Suites exactes 104
12.6. Anneaux d'endomorphismes 105
13. Théorème chinois et applications 107
13.1. Idéaux étrangers 107
13.2. Théorème chinois des restes 110
13.3. Modules se décomposant en composantes primaires 111
13.4. Décomposition primaire des modules de torsion sur un anneau principal 113
14. Modules de type fini sur un anneau principal 118
14.1. Structure des modules de type fini sur un anneau principal 118
14.2. Un exemple 121
14.3. Réduction des matrices 122
14.4. Décomposition en somme de modules monogènes 129
14.5. Autre démonstration 134
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.

[Ca] J.-C. Carrega, Théorie des corps – La règle et le compas, Hermann, 1981, 2ème édition 1989.

[ChL] A. Chambert-Loir, Algèbre corporelle, Éditions de l'École Polytechnique, 2005.

[Co] H. S. M. Coxeter, Introduction to Geometry, 2nd edition, Wiley, 1969.

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

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

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

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

[Fu] W. Fulton, Algebraic Curves, Benjamin, 1969.

[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/~nekovar/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.

[Re] M. Reid, Undergraduate commutative algebra, Cambridge Univ. Press, 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.

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