MAT 541: Modules et matrices

Chapitre 1: Modules

1.1. Définitions et exemples

On commence par un rappel de la notion d'un anneau.

1.1.1. Définition. Un anneau est un ensemble non vide A muni d'une addition

$$+ : A \times A \to A : (a, b) \mapsto a + b$$

et d'une multiplication

$$\bullet : A \times A \to A : (a, b) \mapsto ab$$

satisfaisant aux axiomes suivants:

(1) Il existe un zéro, noté 0_A, tel que $(A, +, 0_A)$ est un groupe abélien.

(2) $(ab)c = a(bc)$ pour tous $a, b, c \in A$.

(3) il existe un *identité*, noté 1_A, tel que $1_A a = a$, pour tout $a \in A$.

(4) $a(b + c) = ab + ac$ et $(a + b)c = ac + bc$, pour tous $a, b, c \in A$.

En outre, A est dit *commutatif* si $ab = ba$, pour tous $a, b \in A$; et *trivial* si $A = \{0_A\}$.

Remarque. (1) $A = \{0_A\}$ si, et seulement si, $1_A = 0_A$.

(2) On note $A^* = \{a \in A \mid a \neq 0_A\}$.

Exemple. (1) L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif pour l'addition et la multiplication usuelles.

(2) L'ensemble $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ des entiers de Gauss est un anneau commutatif pour l'addition et la multiplication usuelles.

(3) Si A est un anneau commutatif, alors l'ensemble $A[x]$ des polynômes sur A est un anneau commutatif pour les opérations usuelles.

(4) Si A est un anneau alors, pour tout $n \geq 1$, l'ensemble $M_n(A)$ des matrices carrées sur A est un anneau. Remarquons que si A est non trivial et $n > 1$, alors $M_n(A)$ est non commutatif même si A est commutatif.

1.1.2. Définition. Soit A un anneau non trivial.

(1) On dit que $a \in A^*$ est *inversible* s'il existe $b \in A$ tel que $ab = ba = 1_A$. Dans ce cas, b est appelé *inverse* de a et noté a^{-1}.

(2) On dit que A est un *corps-gauche* si tout $a \in A^*$ est inversible.

(3) On dit que A est un *corps* si A est un corps-gauche commutatif.

Exemple. (1) Dans l'anneau commutatif $\mathbb{Z}$, les éléments inversibles sont 1 et -1.

(2) Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ des nombres rationnels, des nombres réels et des nombres complexes, respectivement, sont des corps pour l'addition et la multiplication usuelles.

(3) L'ensemble des quaternions

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

est un corps-gauche dont l'addition est usuelle et la multiplication est définie par $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ et $ki = -ik = j$.

(4) Soit $K[x]$ l'anneau des polynômes sur un corps K. Si $f(x) \in K[x]$, alors $f(x)$ est inversible si et seulement si $f = a$ avec $a \in K^*$.

1.1.3. Définition. Soit A un anneau. Une partie B de A s'appelle *sous-anneau* si les conditions suivantes sont vérifiées:

(1) $1_A \in B$.

(2) $a - b \in B$, pour tous $a, b \in B$.

(3) $ab \in B$, pour tous $a, b \in B$.

Remarque. Un sous-anneau de A lui-même est un anneau pour les opérations induites de celles de A ayant le même identité que A.

Exemple. (1) Un anneau A est un sous-anneau de A.

(2) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, et $\mathbb{C}$ est un sous-anneau de $\mathbb{H}$.

(3) L'ensemble $\mathbb{N}$ des entiers non négatifs n'est pas un sous-anneau de $\mathbb{Z}$.

Dès maintenant, on se fixe A un anneau.

1.1.4. Définition. Soit A un anneau. Un groupe abélien additif $(M, +, 0_M)$ s'appelle *A-module à gauche*, noté ${}_AM$, s'il est muni d'une multiplication à gauche

$$\bullet : A \times M \to M : (a, u) \mapsto au$$

satisfaisant aux axiomes suivants:

(1) $1_A u = u$, pour tout $u \in M$.

(2) $(ab)u = a(bu)$, pour tous $a, b \in A$ et $u \in M$.

(3) $a(u + v) = au + av$, pour tous $a \in A$ et $u, v \in M$.

(4) $(a + b)u = au + bu$, pour touts $a, b \in A$ et $u \in M$.

En outre, on dit que M est *nul* si $M = \{0_M\}$.

Remarque. (1) Si D est un corps-gauche, alors un D-module à gauche s'appelle un *D-espace vectoriel à gauche*.

(2) Si K est un corps, alors un K-module à gauche est simplement un K-espace vectoriel.

Exemple. (1) Tout groupe abélien M est un $\mathbb{Z}$-module à gauche si, pour tous $n \in \mathbb{Z}$ et $u \in M$, on définit

$$nu = \begin{cases} \overbrace{u + \cdots + u}^{n \text{ fois}}, & \text{si } n > 0, \\ 0, & \text{si } n = 0, \\ \overbrace{(-u) + \cdots + (-u)}^{|n| \text{ fois}}, & \text{si } n < 0. \end{cases}$$

(2) Si B est un sous-anneau de A, alors A est un B-module à gauche pour la multiplication à gauche

$$B \times A \to A : (b, a) \mapsto ba.$$

En particulier, A est un A-module à gauche pour la multiplication à gauche, appelé le A-module à gauche *régulier* et noté ${}_AA$.

(3) Considérons l'anneau $M_n(A)$ avec $n > 0$. On voit aisément que

$$A^{(n)} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in A \right\}$$

est un $M_n(A)$-module à gauche pour les opérations matricielles. En particulier, $\mathbb{R}^{(2)}$ est un $M_2(\mathbb{R})$-module à gauche.

(4) Pour tout entier $n > 0$, $A^n = \{(a_1, \cdots, a_n) \mid a_i \in A\}$ est un A-module à gauche si l'on définit $(a_1, \cdots, a_n) + (b, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n)$ et $a(a_1, \cdots, a_n) = (aa_1, \cdots, aa_n)$.

Soit E un espace vectoriel sur un corps K dont f est un endomorphisme (c'est-à-dire, une application K-linéaire $f : E \to E$). Si $p(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, alors $p(f) = a_0\mathbb{1}_E + a_1f + \cdots + a_nf^n$ est aussi un endomorphisme de ${}_KE$. On voit aisément que si $p(x), q(x) \in K[x]$, alors

$$(p + q)(f) = p(f) + q(f),\ p(f)q(f) = (pq)(f).$$

1.1.5. Proposition. Soit E un espace vectoriel sur un corps K. Si f est un endomorphisme de ${}_KE$, alors E devient un $K[x]$-module à gauche pour la multiplication suivante:

$$p(x) \cdot v = p(f)(v),$$

pour tous $p(x) \in K[x]$ et $v \in E$. En outre, toute structure de $K[x]$-module à gauche sur $(E, +, 0_E)$ est de cette forme.

Démonstration. D'abord, $(E, +, 0_E)$ est un groupe abélien. Soient $u, v \in E$ et $p, q \in K[x]$. Premièrement. on a $1 \cdot u = (1 \cdot \mathbb{1})(u) = \mathbb{1}(u) = u$. Ensuite,

$$(pq) \cdot u = (pq)(f)(u) = (p(f)q(f))(u) = p(f)(q(f)(u)) = p(x) \cdot (q(x) \cdot u).$$

En outre, comme $p(f)$ est K-linéaire, on a $p \cdot (u + v) = p(f)(u + v) = p(f)(u) + p(f)(v) = p \cdot u + p \cdot v$. Enfin, d'après la définition de la somme des K-endomrophismes de E, on a $(p + q) \cdot u = (p + q)(f)(u) = (p(f) + q(f))(u) = p(f)(u) + q(f)(v) = p \cdot u + q \cdot v$.

Enfin, supposons maintenant que E est un $K[x]$-module à gauche. Alors E est un K-espace vectoriel si l'on définit $a \cdot u = au$ pour tous $a \in K$ et $u \in E$. De plus, l'application $f : E \to E : u \mapsto xu$ est un K-endomorphisme de E. On voit aisément que $p(f)(u) = p(x)u$, pour tous $p(x) \in K[x]$ et $u \in E$. Ceci achève la démonstreation.

Remarque. Pour tout $u \in E$ et $\alpha \in K$, on a $x \cdot u = f(u)$ et $\alpha \cdot u = \alpha u$.

Exemple. Considérons le $\mathbb{R}[x]$-module $\mathbb{R}^{(2)}$ défini par l'endomorphisme de l'espace vectoriel réel $\mathbb{R}^{(2)}$ suivant:

$$f : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On voit que

$$(2 - x + x^2) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}^2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 8 \\ 8 \end{pmatrix}.$$

Par symétrie, on définit un A-module à droite.

1.1.6. Définition. Soit A un anneau. Un groupe abélien additif $(M, +, 0_M)$ s'appelle *A-module à droite*, noté M_A, s'il est muni d'une multiplication à droite

$$\bullet : M \times A \to M : (u, a) \mapsto ua$$

satisfaisant aux axiomes suivants:

(1) $u1_A = u$, pour tout $u \in M$.

(2) $u(ab) = (ua)b$, pour tous $a, b \in A$ et $u \in M$.

(3) $(u + v)a = ua + va$, pour tous $a \in A$ et $u, v \in M$.

(4) $u(a + b) = ua + ub$, pour touts $a, b \in A$ et $u \in M$.

Exemple. (1) Si B est un sous-anneau de A, alors A est un B-module à droite pour la multiplication à droite

$$A \times B \to A : (a, b) \mapsto ab.$$

En particulier, A est un A-module à droite pour la multiplication à droite, appelé le A-module à droite *régulier* et noté A_A.

(2) Pour tout entier $n > 0$, on voit que $A^n = \{(a_1, \cdots, a_n) \mid a_i \in A\}$ est un $M_n(A)$-module à droite pour les opérations matricielles. Remarquons que $A^n = \{(a_1, \cdots, a_n) \mid a_i \in A\}$ est aussi un A-module à droite pour les opérations suivantes:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n),\ (a_1, \cdots, a_n)a = (a_1a, \cdots, a_na).$$

Remarque. Soit A un anneau commutatif. Si M est un A-module à gauche, alors M est aussi un A-module à droite si, pour tous $a \in A$ et $x \in M$, on définit $x \cdot a = ax$. De même, un A-module à droite est un A-module à gauche d'une façon naturelle. Ainsi, dans ce cas, on ne distingue pas un A-module à gauche et un A-module à droite.

1.1.7. Proposition. Soit M un A-module à gauche.

(1) Pour tous $a \in A$ et $u \in M$, on a $au = 0_M$ lorsque $a = 0_A$ ou $u = 0_M$.

(2) Si $au = 0_M$ avec a inversible, alors $u = 0_M$.

(3) Pour tous $a \in A$ et $u \in M$, on a $a(-u) = -(au) = (-a)u$.

(4) Pour tous $a \in A$ et $u_1, \cdots, u_n \in M$, on a $a(u_1 + \cdots + u_n) = au_1 + \cdots + au_n$.

(5) Pour tous $a_1, \cdots, a_n \in A$ et $u \in M$, on a $(a_1 + \cdots + a_n)u = a_1u + \cdots + a_nu$.

(6) Pour tous $a \in A$, $u \in M$ et $n \in \mathbb{Z}$, on a $a(nu) = n(au) = (na)u$.

Remarque. L'équalité $au = 0_M$ n'entraîne pas $a = 0_A$ ou $u = 0_M$. Par exemple, prenons $A = M_2(\mathbb{R})$ et $M = \mathbb{R}^{(2)}$, on a

$$\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

1.2. Sous-modules et modules quotients

Partout dans cette section, on se fixe M un A-module à gauche.

1.2.1. Définition. Une partie non vide N de M s'appelle *sous-module* de M si

(1) $u + v \in N$ pour tous $v, v \in N$, et

(2) $au \in N$ pour tous $a \in A$ et $u \in N$.

Remarque. (1) Si N est un sous-module de M, alors $0_M \in N$. En outre, N lui-même est un A-module à gauche avec $0_N = 0_M$.

(2) On peut définir la notion d'un sous-module d'un A-module à droite d'une façon symétrique.

Exemple. (1) M et $\{0_M\}$ sont toujours des sous-modules de M.

(2) Une partie I de A est un sous-module du A-module à gauche régulier ${}_AA$ si et seulement si I est un idéal à gauche de l'anneau A.

(3) Considérons le $M_2(\mathbb{Z})$-module à gauche $\mathbb{Z}^{(2)}$. On voit aisément que

$$N = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}^{(2)} \mid a, b \text{ paires} \right\}$$

est un sous-module de $\mathbb{Z}^{(2)}$.

(4) Soit $A = M_2(K)$, où K est un corps. Alors

$$N = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in K \right\}$$

est un sous-module du A-module à gauche régulier ${}_AA$.

Soit E un espace vectoriel sur un corps K dont f est un endomorphisme. Un sous-espace F de E est dit *f-invariant* if $f(F) \subseteq F$.

1.2.2. Proposition. Soient E un espace vectoriel sur un corps K dont f est un endomorphisme. Alors une partie non vide F de E est un sous-module du $K[x]$-module ${}_{K[x]}E$ défini par f si et seulement si F est un sous-espace de ${}_KE$ qui est f-invariant.

Démonstration. Supposons que F est un sous-module de ${}_{K[x]}E$. Pour tous $\alpha, \beta \in K$, $u, v \in F$, on a $(\alpha u + \beta v) = (\alpha \mathbb{1})(u) + (\beta \mathbb{1})(v) = \alpha \cdot u + \beta \cdot v \in F$, et $f(u) = x \cdot u \in F$. Ainsi F est un sous-espace de ${}_KE$, qui est f-invariant. Réciproquement, supposons que F est un sous-espace de ${}_KE$ qui est f-invariant. Alors F est fermé pour l'addition. Pour tout $u \in F$, on a $f(u) \in F$, $f^2(u) = f(f(u)) \in F$, et ainsi $f^i(u) \in F$, pour tout $i \geq 0$. Si $p(x) = \sum_{i=0}^{n} a_i x^i$ et $u \in F$, alors $p(x) \cdot u = \sum_{i=0}^{n} a_i f^i(u) \in F$. Ceci montre que F est un sous-module de ${}_{K[x]}E$. La preuve s'achève.

Exemple. Considérons le $\mathbb{R}[x]$-module $\mathbb{R}^{(3)}$ défini par l'application $\mathbb{R}$-linéaire suivante:

$$f : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)} : \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 \\ 3 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

On voit que

$$N = \left\{ \begin{pmatrix} a \\ b \\ 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

est un sous-espace vectoriel de ${}_{\mathbb{R}}\mathbb{R}^{(3)}$ qui est f-invariant. Ainsi F est un sous-module de ${}_{\mathbb{R}[x]}\mathbb{R}^{(3)}$.

1.2.3. Lemme. Une partie non vide N de M est un sous-module si et seulement si pour tous $u, v \in N$ et $a, b \in A$, on a $au + bv \in N$.

Démonstration. Soit N un sous-module de M. Si $a, b \in A$ et $u, v \in M$, alors $au, av \in N$. Ainsi $au + bv \in N$. Réciproquement, supposons que $au + bv \in N$, pour tous $u, v \in N$ et $a, b \in A$. En particulier, $au = au + 0_A 0_M \in N$ et $u + v = 1_A \cdot u + 1_A \cdot v \in N$. D'où N est un sous-module de M. Ceci achève la démonstration.

On va étudier des opérations sur les sous-modules d'un A-module.

1.2.4. Proposition. Si $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille non vide de sous-modules de M, alors $\cap_{\lambda\in\Lambda} M_\lambda$ est également un sous-module de M.

Démonstration. Posons $N = \cap_{\lambda\in\Lambda} M_\lambda$. Comme $0_M \in M_\lambda$, pour tout $\lambda \in \Lambda$, on a $0_M \in N$. Soient $a, b \in A$ et $u, v \in N$. Pour tout $\lambda \in \Lambda$, on a $u, v \in M_\lambda$ et donc $au + bv \in M_\lambda$. Ainsi $au + bv \in N$. Par conséquent, N est un sous-module de M. Ceci achève la démonstration.

Exemple. Considéons le A-module à gauche régulier ${}_A A$ où $A = M_3(\mathbb{Z})$. On voit que

$$N_1 = \left\{ \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 0 \end{pmatrix} \mid a_{ij} \in \mathbb{Z} \right\}, \text{ et } N_2 = \left\{ \begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix} \mid a_{ij} \in \mathbb{Z} \right\}$$

sont deux sous-modules ${}_A A$ tels que

$$N_1 \cap N_2 = \left\{ \begin{pmatrix} 0 & a & 0 \\ 0 & b & 0 \\ 0 & c & 0 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}.$$

Remarque. L'union de sous-modules n'est pas nécessairement un sous-module. Par exemple, supposons que A est un anneau non nul. Considérons le A-module à gauche $A^2 = \{(a,b) \mid a,b \in A\}$. Alors $N = \{(a,0) \mid a \in A\}$ et $L = \{(0,b) \mid b \in A\}$ sont deux sous-modules de A^2 tels que $N \cup L = \{(a,b) \in A^2 \mid a = 0 \text{ ou } b = 0\}$, qui n'est pas un sous-module de A^2.

1.2.5. Proposition. Si $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille non vide de sous-modules de M, alors *la somme*

$$\sum\nolimits_{\lambda\in\Lambda} M_\lambda = \{u \in M \mid u = u_1 + \cdots + u_n,\ n \geq 1,\ u_i \in M_{\lambda_i},\ \lambda_1, \ldots, \lambda_n \in \Lambda\}$$

est le plus petit sous-module de M contenant $\cup_{\lambda\in\Lambda} M_\lambda$.

Démonstration. Posons $N = \sum_{\lambda\in\Lambda} M_\lambda$. Par définition, $M_\lambda \subseteq N$, pour tout $\lambda \in \Lambda$. Ainsi $\cup_{\lambda\in\Lambda} M_\lambda \subseteq N$. Si $u, v \in N$, alors $u = u_1 + \cdots + u_n$ avec $u_i \in M_{\lambda_i}$ et $\lambda_i \in \Lambda$, et $v = v_1 + \cdots + v_m$ avec $v_j \in M_{\mu_j}, \mu_j \in \Lambda$. Pour tous $a, b \in A$, on a

$$au + bv = au_1 + \cdots + au_n + bv_1 + \cdots + bv_m,$$

où $au_i \in M_{\lambda_i}$ et $bv_j \in M_{\mu_j}$. Donc $au + bv \in N$. Ansi N est un sous-module de M. Supposons que L est un sous-module de M contenant $\cup_{\lambda\in\Lambda} M_\lambda$. Si $u \in N$, alors $u = u_1 + \cdots + u_n$ avec $u_i \in M_{\lambda_i}$ et $\lambda_i \in \Lambda$. Comme $M_{\lambda_i} \subseteq L$, pour tout $1 \leq i \leq n$, on a $u \in L$. Donc N est le plus petit sous-module de M contenant $\cup_{\lambda\in\Lambda} M_\lambda$. Ceci achève la démontrsation.

Remarque. Si $\{M_1, \ldots, M_n\}$ est une famille finie de sous-modules de M, alors

$$\sum\nolimits_{i=1}^{n} M_i = \{u \in M \mid u = u_1 + \cdots + u_n,\ u_i \in M_i,\ i = 1, \cdots, n\}.$$

Exemple. (1) Soit $A = M_2(\mathbb{Z})$ et considérons le A-module à gauche régulier ${}_AA$. Alors

$$M_1 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \text{ et } M_2 = \left\{ \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \mid c, d \in \mathbb{Z} \right\}$$

sont deux sous-modules de ${}_AA$ tels que ${}_AA = M_1 + M_2$.

(2) Considérons le $\mathbb{Z}$-module $\mathbb{Z}[x]$ des polynômes sur $\mathbb{Z}$. Pour tout $n \geq 0$, on voit que $P_n = \{ax^n \mid a \in \mathbb{Z}\}$ est un sous-module de $\mathbb{Z}[x]$. Il est évident que $\sum_{n=0}^{\infty} P_n = \mathbb{Z}[x]$.

Soit N un sous-module de M. En particulier, N est un sous-groupe du groupe abélien $(M, +, 0_M)$. Rappelons que deux éléments $u, v \in M$ sont dits *congruents modulo* N, noté

$u \equiv v \,(\mathrm{mod} N)$, si $u - v \in N$. Il s'agit d'une relation d'équivalence dans M. Pour tout $u \in M$, la classe d'équivalence de u est $\bar{u} = u + N = \{u + v \mid v \in N\}$, et l'ensemble des classes d'équivalence de M modulo N est

$$M/N = \{\bar{u} \mid u \in M\}.$$

1.2.6. Théorème. Si N un sous-module de M, alors $M/N = \{\bar{u} \mid u \in M\}$ est un A-module à gauche, appelé le *module quotient* de M par N, lorsqu'on définit, pour $\bar{u}, \bar{v} \in M/N$ et $a \in A$, que

$$\bar{u} + \bar{v} = \overline{u + v}, \quad a\bar{u} = \overline{au}.$$

Démonstration. Comme N est sous-groupe de $(M, +, 0_M)$, on sait que $(M/N, +, \bar{0}_M)$ est un groupe abélien. Soient $\bar{u}$ et $\bar{v} \in M/N$ et $a \in A$. Par définition, on a $a\bar{u} = \overline{au}$ et $a\bar{v} = \overline{av}$. Si $u + N = v + N$, alors $u - v \in N$. Comme N est un sous-module, $au - av = a(u - v) \in N$. D'où $\overline{au} = \overline{av}$. Ceci montre que la multiplication scalaire à gauche est correctement définie, qui satisfait évidemment aux axiomes énoncés dans la définition 1.1.1. La preuve s'achève.

Remarque. Pour tout $u \in M$, on a $\bar{u} = \bar{0}$ si et seulement si $u \in N$. Par conséquent, $M/N = \{\bar{0}_M\}$ si et seulement si $N = M$.

Exemple. (1) Soit $n > 1$ un entier. Alors $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ est un sous-module de $\mathbb{Z}$ tel que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. Pour tout $\bar{a} \in \mathbb{Z}_n$, on voit que $\bar{a} = \bar{0}$ si et seulement si $a \in n\mathbb{Z}$ si et seulement si n divise a.

(2) Soit K un corps avec $\lambda \in K$. On voit que $N = \{(x - \lambda)f(x) \mid f(x) \in K[x]\}$ est un sous-module du $K[x]$-module régulier $K[x]$ tel que $K[x]/N = \{\bar{\mu} \mid \mu \in K\}$. Pour tout $\bar{\mu} \in K[x]/N$, on a $x \cdot \bar{\mu} = \overline{\lambda\mu}$.

1.2.7. Théorème. Soit E un espace vectoriel de dimension finite sur un corps K. Si F est un sous-espace vectoriel de E, alors

$$\dim_K(E/F) = \dim_K(E) - \dim_K(F).$$

Démonstration. Comme E est de K-dimension finie, F l'est aussi. Prenons une base $\{u_1, \ldots, u_r\}$ de F, qui se prolonge dans une base $\{u_1, \ldots, u_r, u_{r+1}, \ldots, u_n\}$ de E. Soit $\bar{u} =$

$u + F \in E/F$ avec $u \in E$. On a $u = \alpha_1 u_1 + \cdots + \alpha_r u_r + \alpha_{r+1} u_{r+1} + \cdots + \alpha_n u_n$ avec $\alpha_i \in K$. Alors $\bar{u} = \overline{\alpha_{r+1} u_{r+1} + \cdots + \alpha_n u_n} = \alpha_{r+1}\bar{u}_{r+1} + \cdots + \alpha_n \bar{u}_n$. Donc E/F est engendré par $\bar{u}_{r+1}, \ldots, \bar{u}_n$. En outre, supposons que $\beta_{r+1}\bar{u}_{r+1} + \cdots + \beta_n \bar{u}_n = \bar{0}$ avec $\beta_j \in K$, c'est-à-dire, $\beta_{r+1} u_{r+1} + \cdots + \beta_n u_n \in F$. Ainsi $\beta_{r+1} u_{r+1} + \cdots + \alpha_n u_n = \beta_1 u_1 + \cdots + \beta_r u_r$. Ceci nous donne $(-\beta_1)u_1 + \cdots + (-\beta_r)u_r + \beta_{r+1} u_{r+1} + \cdots + \beta_n u_n = 0_E$. Par conséquent, $-\beta_1 = \cdots = -\beta_r = \beta_{r+1} = \cdots = \beta_n = 0$. Ceci implique que $\{\bar{u}_{r+1}, \cdots, \bar{u}_n\}$ est une base de E/F. Donc $\dim_K(E/F) = n - r = \dim_K(E) - \dim_K(F)$. Ceci achève la démonstration.

Exemple. Considérons le sous-espace vectoriel $F = \{(0, a, 0, b) \mid a, b \in \mathbb{R}\}$ du $\mathbb{R}$-espace vectoriel $\mathbb{R}^4$. On voit que $\mathbb{R}^4/F$ est de dimension deux ayant pour base $\{\bar{e}_2, \bar{e}_4\}$.

1.3. Bases

Partout dans cette section, on se fixe M un A-module à gauche.

1.3.1. Définition. Soit X un sous-ensemble de M. Alors l'intersection des sous-modules de M contenant X est le plus petit sous-module de M contenant X, qui s'appelle le sous-module de M *engendré* par X et est noté $< X >$.

Remarque. (1) Si X est un sous-module de M, alors $X =< X >$.

(2) Si $M =< X >$, on dit alors que X est un *ensemble de générateurs* de M.

Si $X = \emptyset$, alors il est évident que $< X >= \{0_M\}$. On va étudier $< X >$ lorsque X est non vide.

1.3.2. Définition. Soit $u_1, \ldots, u_n \in M$. On dit que $u \in M$ est une *combinaison linéaire* de $u_1, \ldots, u_n$ si $u = a_1 u_1 + \cdots + a_n u_n$, où $a_1, \cdots, a_n \in A$.

Remarque. (1) Tout $u \in M$ est une combinaison linéaire de lui-même, car $u = 1_A \cdot u$.

(2) 0_M est combinaison linéaire de n'importe quels n éléments $u_1, \cdots, u_n \in M$.

Exemple. (1) Considérons le $\mathbb{Z}$-module régulier ${}_{\mathbb{Z}}\mathbb{Z}$. Si $m, n \in \mathbb{Z}$, alors 1 est une combinaison linéaire de m, n si et seulement si m et n sont co-premiers.

(2) Soient

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{R}^{(2)}.$$

Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}^{(2)}$, e_1 n'est pas une combinaison linéaire de e_2. Mais dans le $M_2(\mathbb{R})$-module à gauche $\mathbb{R}^{(2)}$, e_1 est une combinaison linéaire de e_2. En effet,

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

Le résultat suivant se découle du lemme 1.2.3 par récurrence.

1.3.3. Proposition. Un sous-ensemble N de M est un sous-module si et seulement si N est fermé pour les combinaisons linéaires d'éléments de N (c'est-à-dire, si $u_1, \ldots, u_n \in N$, alors $a_1u_1 + \cdots + a_nu_n \in N$, pour tous $a_1, \ldots, a_n \in A$).

1.3.4. Lemme. Si X est un sous-ensemble non vide de M, alors $< X >$ se compose des combinaisons linéaires d'éléments de X.

Démonstration. Posons $L = \{a_1u_1 + \cdots + a_nu_n \mid n \geq 1, u_1, \ldots, u_n \in X, a_1, \ldots, a_n \in A\}$. Pour tout $u \in L$, on a $u = a_1u_1 + \cdots + a_nu_n$, où $u_1, \ldots, u_n \in X, a_1, \ldots, a_n \in A$. Comme $u_1, \ldots, u_n \in < X >$, d'après la proposition 1.3.3, $u \in < X >$. Ceci implique $L \subseteq < X >$. D'autre part, on a $X \subseteq L$ par définition. En particulier, L est non vide. Si $u, v \in L$, alors $u = \sum_{i=1}^{n} a_iu_i$ et $v = \sum_{j=1}^{m} b_jv_j$, où $a_i, b_j \in A$ et $u_i, v_j \in X$. Pour tous $a, b \in A$, on a $au + bv = \sum_{i=1}^{n}(aa_i)u_i + \sum_{j=1}^{m}(bb_j)v_j \in L$. Donc L est un sous-module de M contenant X. Par conséquent, $< X > \subseteq L$. Ceci achève la démonstration.

Remarque. (1) Pour tout $u \in M$, on a $< u >= \{au \mid a \in A\}$ et on écrit donc $< u >= Au$.

(2) Si X est une partie non-vide de M, alors $< X >= \sum_{u \in X} Au$.

Exemple. Le $\mathbb{Z}$-module $\mathbb{Z}[x]$ est engendré par $1, x, x^2, \cdots, x^n, \cdots$.

1.3.5. Définition. On dit que M est dit *cyclique* si $M =< u >$ pour un certain élément $u \in M$, de *type fini* si $M =< X >$ pour une certaine famille finie X de M, et de *type infini* si M n'est pas de type fini.

Remarque. Soit K un corps. Un K-espace vectoriel est de type fini si et seulement si, il est dimension finie.

Exemple. (1) Considérons le A-module à gauche régulier ${}_AA$. Pour tout $a \in A$, on a $a = a1_A$. Ainsi A est cyclique engendré par 1_A.

(2) Pour tout $n \geq 1$, le A-module à gauche $A^n = \{(a_1, \cdots, a_n) \mid a_i \in A, i = 1, \cdots, n\}$ est de type fini engendré par $e_1, \ldots, e_n$.

(3) Soit A un anneau commutatif non trivial. Si $n > 1$, alors A^n n'est pas cyclique. En effet, supposons au contraire que A^n est cyclique engendré par un certain élément $u = (a_1, \cdots, a_n)$. Pour tout $1 \leq i \leq n$, il existe $b_i \in A$ tel que $e_i = b_i u$. Ceci nous donne $b_i a_i = 1_A$ et $b_i a_j = 0_A$ lorsque $i \neq j$. En particulier, $b_1 a_1 = 1$ et $b_2 a_1 = 0_A$. Alors $b_2 = b_2(b_1 a_1) = b_1(b_2 a_1) = 0$. D'où $1_A = b_2 a_2 = 0_A a_2 = 0_A$. Ainsi $A = 0$, une contradiction.

(4) Le $\mathbb{Z}$-module $\mathbb{Z}[x]$ est de type infini. En effet, soit $X = \{p_1, \ldots, p_n\}$ une famille finie d'éléments de $\mathbb{Z}[x]$. Posons d le plus grand degré de $p_1, \ldots, p_n$. Alors

$$< X > \subseteq \mathbb{Z}_d[x] = \{a_0 + a_1 x + \cdots + a_d x^d \mid a_i \in \mathbb{Z}, i = 1, \ldots, d\} \neq \mathbb{Z}[x].$$

Ainsi $\mathbb{Z}[x]$ n'est pas de type fini.

1.3.6. Définition. Soit A un anneau non trivial. Une famille $X = \{u_\lambda \mid \lambda \in \Lambda\}$ d'éléments de M est dite *liée* s'il existe des indices distincts $\lambda_1, \ldots, \lambda_n \in \Lambda$ avec $n \geq 1$ et des scalaires non tous nuls $a_1, \cdots, a_n \in A$, tels que $a_1 u_{\lambda_1} + \cdots + a_n u_{\lambda_n} = 0_M$; et *libre* sinon (c'est-à-dire, toute égalité possible $a_1 u_{\lambda_1} + \cdots + a_n u_{\lambda_n} = 0_M$, $a_1, \cdots, a_n \in A$, $\lambda_1, \cdots, \lambda_n \in \Lambda$, entraîne que $a_1 = \cdots = a_n = 0_A$).

Remarque. (1) Par definition, la famille vide est libre.

(2) Si X est une famille libre de M, alors toute sous-famille de X est également libre.

Exemple. (1) Considérons le $\mathbb{Z}$-module $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ avec $n > 0$. La famille $\{\bar{1}\}$ est liée. En effet, $n \cdot \bar{1} = \bar{n} = \bar{0}$.

(2) Considérons le $\mathbb{Z}_n$-module $\mathbb{Z}_n$ avec $n > 0$. La famille $\{\bar{1}\}$ est libre. En effet, si $\bar{n} \neq \bar{0}$, alors $\bar{n} \cdot \bar{1} = \bar{n} \neq \bar{0}$.

(3) Considérons le A-module à gauche $A^n = \{(a_1, \cdots, a_n) \mid a_i \in A\}$. La famille $\mathcal{E} = \{e_1, e_2, \cdots, e_n\}$ est libre. En effet, si $a_1, a_2, \cdots, a_n \in A$ sont tels que

$$a_1e_1 + a_2e_2 + \cdots + a_ne_n = 0_{A^n},$$

alors $(a_1, a_2, \cdots, a_n) = (0, 0, \cdots, 0)$, c'est-à-dire, $a_1 = a_2 = \cdots = a_n = 0$.

(4) Considérons le $\mathbb{Z}$-module $\mathbb{Z}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \geq 0, a_i \in \mathbb{Z}\}$ des polynômes sur $\mathbb{Z}$. On voit aisément que la famille $\{x^i \mid i = 0, 1, 2, \cdots\}$ est libre.

(5) Soient

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{R}^{(2)}.$$

Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}^{(2)}$, $\{e_1, e_2\}$ est libre. Mais dans le $M_2(\mathbb{R})$-module à gauche $\mathbb{R}^{(2)}$, la famille $\{e_1, e_2\}$ est liée. En effet,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0.$$

1.3.7. Définition. Un sous-ensemble X de M s'appelle une *base* de M si X est libre et $M =< X >$.

Exemple. (1) Si $M = \{0_M\}$, alors la famille vide $\emptyset$ est une base de M.

(2) Pour tout $n \geq 1$, le A-module à gauche A^n admet une base $\mathcal{E} = \{e_1, e_2, \ldots, e_n\}$.

(3) Pour tout $n > 1$, le $\mathbb{Z}$-module $\mathbb{Z}_n$ n'a aucune base. Soit X une partie de $\mathbb{Z}_n$. Si $X = \emptyset$, alors $< X >= \{\bar{0}\} \neq \mathbb{Z}_n$. Supposons que X est non vide. Prenons $\bar{a} \in X$. Alors $n\bar{a} = \overline{na} = \bar{0}$ avec $n \neq 0$. Ainsi $\{\bar{a}\}$ n'est pas libre. Par conséquent, X n'est pas libre. Donc X n'est pas une base du $\mathbb{Z}$-module $\mathbb{Z}_n$. Mais en tant que $\mathbb{Z}_n$-module, $\mathbb{Z}_n$ a pour base $\{\bar{1}\}$.

(4) Soit A un anneau commutatif non trivial. Le A-module $A[x]$ a pour base $\{x^i \mid i = 0, 1, \ldots, \}$.

1.3.8. Définition. Soit E un ensemble non vide. Une relation $\leq$ dans E s'appelle un *ordre* si les conditions suivantes sont vérifiées pour tous $a, b, c \in E$:

(1) $a \leq a$.

(2) Si $a \leq b$ et $b \leq a$, alors $a = b$.

(3) Si $a \leq b$ et $b \leq c$, alors $a \leq c$.

Dans ce cas, on dit que E est ordonné par $\leq$, ou bien, que $(E, \leq)$ est un ensemble ordonné.

Exemple. (1) L'ensemble $\mathbb{R}$ est ordonné par l'ordre usuel.

(2) L'ensemble $\mathbb{C}$ n'est pas ordonné par un ordre évident.

1.3.9. Définition. $(E, \leq)$ un ensemble ordonné et F un sous-ensemble non vide de E.

(1) F est dit une *chaîne* si pour tous $a, b \in F$, on a $a \leq b$ ou $b \leq a$.

(2) F est dit *borné supérieurement* s'il existe $b \in E$ tel que $a \leq b$, pour tout $a \in F$.

(3) Un élément $a \in E$ est dit *maximal* si toute relation $a \leq b$ entraîne que $a = b$.

Exemple. (1) $\mathbb{Z}$ est une chaîne de $\mathbb{R}$ qui n'est pas bornée supérieurement.

(2) $\mathbb{R}$ n'a aucun élément maximal.

On accepte l'énoncé suivant comme un axiome.

1.3.10. Lemme de Zorn. Soit $(E, \leq)$ un ensemble ordonné non vide. Si toute chaîne dans E est bornée supérieurement, alors E admet un élément maximal.

1.3.11. Théorème. Soit M un espace vectoriel sur un corps-gauche D. Si X est une famille libre d'éléments de M, alors X est contenue dans une base de M.

Démonstration. Soit Σ l'ensemble des familles libres d'éléments de M contenant X. Alors Σ est non vide et ordonné par l'inclusion $\subseteq$. Soit $\mathcal{C} = \{X_\lambda \mid \lambda \in \Lambda\}$ une chaîne dans Σ. Posons $Y = \cup_{\lambda \in \Lambda} X_\lambda$. Alors $X \subseteq Y$. Soient $u_1, \ldots, u_n \in Y$. Il existe $\lambda_1, \ldots, \lambda_n \in \Lambda$ tels que $u_i \in X_{\lambda_i}$, $i = 1, \ldots, n$. Par l'hypothèse, $X_{\lambda_i} \subseteq X_{\lambda_j}$ ou $X_{\lambda_j} \subseteq X_{\lambda_i}$, pour tous $1 \leq i, j \leq n$. Ainsi il existe s avec $1 \leq s \leq n$ tel que $X_{\lambda_i} \subseteq X_{\lambda_s}$, pour tout $1 \leq i \leq n$. Par conséquent, $u_1, \ldots, u_n \in X_{\lambda_s}$. Comme X_{λ_s} est libre, on a $\{u_1, \cdots, u_n\}$ est libre. Ceci montre que Y est libre. Donc $Y \in \Sigma$ tel que $X_\lambda \subseteq Y$, pour tout $\lambda \in \Lambda$. C'est-à-dire, $\mathcal{C}$ est bornée supérieurement. D'après le lemme de Zorn, Σ admet un élément maximal, noté X_0. Supposons que X_0 n'est pas une base de M. Alors $M \neq < X_0 >$. Donc il existe $u_0 \in M$ tel que $u_0 \notin < X_0 >$. En particulier, $0_M \neq u_0 \notin X_0$. Donc $X_0 \subset X_0 \cup \{u_0\}$. D'après la maximalité de X_0, la famille $X_0 \cup \{u_0\}$ est liée. Ainsi il existe $v_1, \ldots, v_t \in X_0 \cup \{u_0\}$ distincts,

et $c_1, \ldots, c_t \in D$ non tous nuls, tels que $c_1v_1 + \cdots + c_{t-1}v_{t-1} + c_tv_t = 0_M$. Si $v_i \neq u_0$ pour tout $1 \leq i \leq t$, alors $v_1, \ldots, v_t \in X_0$. Donc X_0 est liée, une contradiction. Donc on peut supposer que $v_t = u_0$ et $v_1, \ldots, v_{t-1} \in X_0$. Si $c_t = 0$, alors $c_1, \ldots, c_{t-1}$ sont non tous nuls tels que $c_1u_1 + \cdots + c_{t-1}u_{t-1} = 0$. D'où, X_0 est liée, une contradiction. Donc $c_t \neq 0$. Comme D est un corps-gauche, c_t est inversible. Ainsi $u_0 = -c_t^{-1}(c_1u_1 + \cdots + c_{t-1}u_{t-1}) \in < X_0 >$, une contradiction. Ceci montre que X_0 est une base de M. La preuve s'achève.

1.3.12. Théorème. Si D est un corps-gauche, alors tout D-espace vectoriel à gauche (ou à droite) admet une base.

Démonstration. La famille vide $\emptyset$ est libre. D'après le théorème 1.3.11, $\emptyset$ se prolonge dans une base X de M. La preuve s'achève.

1.4. Annulateurs

1.4.1. Lemme. Soit M un A-module à gauche.

(1) Pour tout $u \in M$, $\mathrm{ann}(u) = \{a \in A \mid au = 0_M\}$ est un idéal à gauche de A, appelé l'*annulateur* de u dans A.

(2) $\mathrm{ann}(M) = \{a \in A \mid au = 0_M, \text{ pour tout } u \in M\}$ est un idéal bilatère de A, appelé l'*annulateur* de M.

Démonstration. (1) Soit $u \in M$. Comme $0_Au = 0_M$, on a $0_A \in \mathrm{ann}(u)$. Si $a, b \in \mathrm{ann}(u)$ et $r, s \in A$, on a $(ra + sb)u = r(au) + s(bu) = 0_M$. Ainsi $\mathrm{ann}(u)$ est un idéal de A.

(2) Comme $\mathrm{ann}(M) = \cap_{u \in M}\mathrm{ann}(u)$, on voit que $\mathrm{ann}(M)$ est un idéal à gauche. En outre, soient $a \in \mathrm{ann}(M)$ et $b \in A$. Pour tout $u \in M$, on a $(ab)u = a(bu) = 0_M$. D'où $\mathrm{ann}(M)$ est un idéal bilatère de A. Ceci achève la démonstration.

Exemple. (1) Considérons le $\mathbb{Z}$-module $\mathbb{Z}_n$ avec $n > 1$. Pour tout $\bar{a} \in \mathbb{Z}_n$, on a $\mathrm{ann}(\bar{a}) = n_1\mathbb{Z}$, où $n_1 = \frac{n}{\mathrm{pgcd}(n,a)}$. En effet, posons $d = \mathrm{pgcd}(n, a)$. Alors $n = dn_1$ et $a = da_1$ avec n_1, a_1 co-premiers. Pour tout $b \in \mathbb{Z}$, on voit que $b \in \mathrm{ann}(\bar{a})$ si et seulement si $b\bar{a} = \overline{ba} = \bar{0}$ si et seulement si $n \mid ab$ si et seulement si $n_1 \mid a_1b$ si et seulement si $n_1 \mid b$. D'où, $\mathrm{ann}(\bar{a}) = n_1\mathbb{Z}$. En conséquence, $\mathrm{ann}(\mathbb{Z}_n) = \mathrm{ann}(\bar{1}) = n\mathbb{Z}$.

(2) Soit E un espace vectoriel sur un corps K dont f est un endomorphisme. Si $m(x)$ est le polynôme minimal de f, alors l'annulateur du $K[x]$-module E défini par f est l'idéal engendré par $m(x)$.

1.4.2. Définition. Un A-module à gauche M est dit *fidèle* si $\mathrm{ann}(M) = \{0_A\}$.

Exemple. (1) Le A-module à gauche régulier ${}_AA$ est fidèle.

(2) Si D est un corps-gauche, alors tout D-espace vectoriel non nul est fidèle.

(3) Pour tout $n \geq 1$, le $\mathbb{Z}$-module $\mathbb{Z}_n$ n'est pas fidèle.

On rappelle que A est *intègre* si A est commutatif non trivial et vérifie la propriété que $ab = 0_A$ entraîne que $a = 0_A$ ou $b = 0_A$.

1.4.2. Définition. Soient A un anneau intègre et M un A-module.

(1) Un élément $u \in M$ est dit *de torsion* si $\mathrm{ann}(u) \neq 0$ (c'est-à-dire, $au = 0_M$, pour un certain élément non nul $a \in A$).

(2) M est *de torsion* si tous ses éléments sont de torsion.

(3) M est dit *sans torsion* si aucun de ses éléments non nuls n'est de torsion.

Remarque. (1) Comme $1_A \neq 0_A$, on voit que 0_M est de torsion. En outre, M est sans torsion si et seulement si 0_M est le seul élément de torsion.

(2) Si M est un $\mathbb{Z}$-module, alors $u \in M$ est de torsion si et seulement si u est d'ordre fini.

Exemple. (1) Pour tout $n > 1$, le $\mathbb{Z}$-module $\mathbb{Z}_n$ est de torsion.

(2) Si A est un anneau intègre, alors le A-module régulier ${}_AA$ est sans torsion.

1.4.3. Lemme. Soient A un anneau intègre et M un A-module.

(1) L'ensemble $\mathcal{T}(M)$ des éléments de torsion de M est le plus grand sous-module de torsion de M.

(2) $M/\mathcal{T}(M)$ est sans torsion.

Démonstration. D'abord, $0_M \in \mathcal{T}(M)$. Soient $u, v \in \mathcal{T}(M)$ et $r, s \in A$. Il existe $a, b \in A$ non nuls tels que $au = 0_M$ et $bv = 0_M$. Comme A est intègre, $ab \neq 0_A$ et $(ab)(ru + sv) = (br)(au) + (as)(bv) = 0_M$. Ainsi $ru + sv \in \mathcal{T}(M)$. Ceci montre que $\mathcal{T}(M)$

est un sous-module de M. Soit L un sous-module de torsion de M. Si $u \in L$, alors u est de torsion, et donc $u \in \mathcal{T}(M)$. D'où, $L \subseteq \mathcal{T}(M)$. Enfin, on considère le module quotient $M/\mathcal{T}(M)$. Si $\bar{u} = u + \mathcal{T}(M)$ est de torsion, alors il existe $a \in A$ non nul tel que $a\bar{u} = \overline{au} = \bar{0}$, c'est-à dire, $au \in \mathcal{T}(M)$. Ainsi il existe $b \in A$ non nul tel que $b(au) = 0_M$. D'où $(ab)u = 0_M$. Comme A est intègre, on a $ab \neq 0_A$. Donc $u \in \mathcal{T}(M)$. Cela veut dire que $\bar{u} = \bar{0}$. Ceci achève la preuve.

Remarque. (1) M est de torsion si et seulement si $\mathcal{T}(M) = M$.
(2) M est sans torsion si et seulement si $\mathcal{T}(M) = 0$.

Exemple. Considérons le $\mathbb{Z}$-module $\mathbb{Z}_n \times \mathbb{Z} = \{(\bar{a}, b) \mid a, b \in \mathbb{Z}\}$, où $n \geq 1$. Alors $\mathcal{T}(\mathbb{Z}_n \times \mathbb{Z}) = \{(\bar{a}, 0) \mid a \in \mathbb{Z}\}$.

1.5. Exercices

1. Soit A un anneau. Montrer que A est trivial si et seulement si tout A-module à gauche est nul.

2. Soit M un espace vectoriel à gauche sur un corps-gauche D. Si $au = 0_M$ avec $a \in D$ et $u \in M$, montrer que $a = 0_D$ ou $u = 0_M$.

3. Trouver les éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

4. Considérer le $M_n(K)$-module à gauche $K^{(n)}$, où K est un corps. Si $u, v \in K^{(n)}$ avec u non nul, montrer qu'il existe $P \in M_n(K)$ telle que $v = Pu$. *Indication*: Si u se réduit à v par des opération élémentaires sur les lignes, alors $v = Pu$ avec P une matrice inversible sur K.

5. Considérer le $\mathbb{R}[x]$-module $\mathbb{R}^{(3)}$ défini par l'application $\mathbb{R}$-linéaire suivante:

$$f : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)} : \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

(1) Pour tout $u \in \mathbb{R}^{(3)}$, calculer $(3 - 2x^2 + 4x^3 - 5x^{10}) \cdot u$.

(2) Pour tout $p(x) \in \mathbb{R}[x]$, vérifier qu'il existe un polynôme $r(x)$ de degré au plus deux tel que $p(x) \cdot u = r(x) \cdot u$, pour tout $u \in \mathbb{R}^{(3)}$.

(3) Déterminer, avec justification, lequel des ensembles suivants est un sous-module du $\mathbb{R}[x]$-module $\mathbb{R}^{(3)}$.

$$N = \left\{ \begin{pmatrix} a \\ b \\ 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}, \; L = \left\{ \begin{pmatrix} 0 \\ a \\ b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

6. Considérer l'anneau $M_n(K)$ où K est un corps. Pour $\Sigma \subseteq \{1, 2, \cdots, n\}$, soit $I(\Sigma)$ l'ensembles des matrices $P \in M_n(K)$ dont la j-ième colonne est nulle pour tout $j \in \Sigma$. Si $I \subseteq A$, montrer que I est un idéal à gauche de $M_n(K)$ si et seulement si $I = I(\Sigma)$ pour un certain $\Sigma \subseteq \{1, 2, \cdots, n\}$.

7. Soit E un espace vectoriel sur un corps K dont f est un endomorphisme. Si F est un sous-espace vectoriel de E de dimension un, montrer que F est un sous-module du $K[x]$-module E défini par f si et seulement si F est un sous-espace de E engendré par un vecteur propre de f.

8. Considérer l'endomorphisme de l'espace vectoriel réel $\mathbb{R}^{(2)}$ suivant:

$$f : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Trouver tous les sous-modules du $\mathbb{R}[x]$-module $\mathbb{R}^{(2)}$ défini par f. *Indication*: Utiliser le numéro 5.

9. Soient M un module à gauche sur un anneau A et $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non vide de sous-modules de M telle que $M_\lambda \subseteq M_\mu$ ou $M_\mu \subseteq M_\lambda$ pour tous $\lambda, \mu \in \Lambda$. Montrer que $\cup_{\lambda \in \Lambda} M_\lambda$ est un sous-module de M.

10. Soient A un anneau et I un idéal bilatère de A. Si M est un A-module à gauche, montrer que M est un A/I-module à gauche de sorte que $\bar{a} \cdot u = au$, pour tous $\bar{a} \in A/I$ et $u \in M$ si, et seulement si, $IM = 0$ (c'est-à-dire, $au = 0_M$ pour tous $a \in I$ et $u \in M$).

11. Considérer le $\mathbb{Z}$-module $M = M_2(\mathbb{Z})$ et

$$N = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b \in \mathbb{Z}, c \in 2\mathbb{Z}, d \in 3\mathbb{Z} \right\}.$$

(1) Vérifier que N est un sous-module de M.

(2) Donner les éléments deux à deux distincts du module quotient M/N.

12. Soient $M_3(\mathbb{R})$ l'espace vectoriel réel des matrices carrées réelles d'ordre 3 et F le sous-espace vectoriel de $M_3(\mathbb{R})$ des matrices symétriques. Donner une base de l'espace quotient de $M_3(\mathbb{R})$ modulo F.

13. Soient M un A-module à gauche et N un sous-module de M.

(1) Si $M =< X >$, montrer que $M/N =< \overline{X} >$, où $\overline{X} = \{\bar{u} = u + N \mid u \in X\}$.

(2) Si M est de type fini, montrer que M/N est de type fini.

(3) Si M est cyclique, montrer que M/N est cyclique.

14. Considerer les sous-modules $L = \{(0, a, b) \mid a, b \in \mathbb{Z}\}$ et $M =< (0, 1, 1), (1, 1, 0) >$ du $\mathbb{Z}$-module $\mathbb{Z}^3$. Vérifier que $\mathbb{Z}^3 = L + M$ et calculer $L \cap M$.

15. Considérer le $\mathbb{Z}$-module régulier $\mathbb{Z}$. Si a, b sont deux entiers positifs, montrer que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, où d est le plus grand commun diviseur, et m est le plus petit commun multiple, de a et b.

16. Considérer le $\mathbb{Z}$-module $\mathbb{Q}$. Pour tous $\alpha, \beta \in \mathbb{Q}$, déterminer la famille $\{\alpha, \beta\}$ est liée ou libre.

17. Soit K un corps. Montrer, pour tout $n > 1$, que le $M_n(K)$-module à gauche $K^{(n)}$ n'a aucune base. *Indication*: vérifier, pour tout $u \in K^{(n)}$, qu'il existe $P \in M_n(K)$ non nulle telle que $Pu = 0$.

18. Soit K un corps. Si $p(x) \in K[x]$ est de degré $n\,(\geq 1)$, montrer que la dimension du K-espace vectoriel $K[x]/<p(x)>$ est n.

19. Montrer, pour tout $n \geq 1$, que le $M_n(A)$-module à gauche $A^{(n)}$ est cyclique et fidèle.

20. Soient K un corps et E un K-espace vectoriel de dimension finie positive dont f est un endomorphisme. Si f est nilpotent, montrer que le $K[x]$-module E défini par f est cyclique si et seulement si $\mathrm{Im}(f)$ est de co-dimension un, où la *co-dimension* d'un sous-espace F de E est $\dim(E) - \dim(F)$.

    Indication: Vérifier que le $K[x]$-module E est engendré par u si et seulement si $\bar{u} = u + \mathrm{Im}(f)$ forme une base du K-espace vectoriel $E/\mathrm{Im}(f)$.

21. Soient K un corps et E un K-espace vectoriel de dimension finie positive. Soient f un endomorphisme de E et F un sous-espace f-invariant de E.

    (1) Montrer que $\bar{f} : E/F \to E/F : \bar{u} \mapsto \overline{f(u)}$ est un endomorphisme du K-espace vectoriel E/F.

    (2) Montrer qu'il existe une base de E dans laquelle la matrice de f est une matrice partagée de la forme suivante:

$$\begin{pmatrix} B & C \\ 0 & D \end{pmatrix},$$

    où B est une matrice carrée et D est la matrice de $\bar{f}$ dans une base de E/F. *Indication*: Si $\{u_1, \ldots, u_r\}$ est une base de F et $\{\bar{v}_1, \ldots, \bar{v}_s\}$ est une base de E/F, vérifier que $\{u_1, \ldots, u_r, v_1, \ldots, v_s\}$ est une base de E dans laquelle la matrice de f est de la forme désirée.

22. Soit E un espace vectoriel complexe de dimension finie positive. Si f est un endomorphisme de E, montrer qu'il existe une base de E dans laquelle la matrice de f est triangulaire supérieure.

    Indication: Procéder par récurrence sur la dimension de E, en remarquant que f a toujours une valeur propre et utilisant la partie (2) du numéro 21.

23. Soient E un espace vectoriel sur un corps K et f un K-endomorphisme de E. Si E est de dimension finie, montrer que le $K[x]$-module E défini par f est de torsion. *Indication*: Utiliser le théorème de Hamilton-Cayley.

24. Soit A un anneau non trivial. Si I est un idéal bilatère de A, montrer que $\mathrm{ann}(A/I) = I$.

Chapitre 2: Applications linéaires et suites exactes

Partout dans ce chapitre, on se fixe A un anneau. Notre but sera d'étudier les applications entre les A-modules qui sont compatibles avec la structure de A-modules.

2.1. Applications linéaires

Partout dans cette section, on se fixe M et N des A-modules à gauche.

2.1.1. Définition. Une application $f : M \to N$ est dite A-*linéaire* si

(1) $f(u+v) = f(u) + f(v)$, pour tous $u, v \in M$, et

(2) $f(au) = af(u)$, pour tous $a \in A$ et $u \in M$.

Remarque. (1) Si $f : M \to N$ est A-linéaire, alors $f(0_M) = 0_N$, $f(-u) = -f(u)$, et $f(u-v) = f(u) - f(v)$, pour tous $u, v \in M$. Plus généralement, $f(nu) = nf(u)$, pour tous $n \in \mathbb{Z}$ et $u \in M$.

(2) Si $A = \mathbb{Z}$, alors une application $f : M \to N$ est $\mathbb{Z}$-linéaire si et seulement si $f(u+v) = f(u) + f(v)$, pour tous $u, v \in M$.

Exemple. (1) L'application nulle $0 : M \to N : x \mapsto 0_N$ est toujours A-linéaire.

(2) Si N est un sous-module de M, alors l'inclusion $j_{_N} : N \to M : u \mapsto u$ ainsi que la projection canonical $p_{_M} : M \to M/N : u \mapsto u+N$ est A-lináire. En particulier, l'application identité $\mathbb{1}_M : M \to M : u \mapsto u$ est A-linéaire.

2.1.2. Lemme. Soit $f : M \to N$ une application. Les conditions suivantes sont équivalentes:

(1) f est A-linéaire.

(2) Pour tous $a, b \in A$ et $u, v \in M$, on a $f(au + bv) = af(u) + bf(v)$.

(3) Pour tous $a_1, \ldots, a_n \in A$ et $u_1, \ldots, u_n \in M$ avec $n \geq 1$, on a

$$f(a_1u_1 + \cdots + a_nu_n) = a_1f(u_1) + \cdots + a_nf(u_n).$$

Démonstration. Si f est A-linéaire alors, pour tous $a, b \in A$ et $u, v \in M$, on a $f(au + bv) = f(au) + f(bv) = af(u) + bf(v)$. Si f satisfait à (2) alors, pour tous $u, v \in M$,

on a $f(u+v) = f(1_A u + 1_A v) = 1_A f(u) + 1_A f(v) = f(u) + f(v)$ et $f(au) = f(au + 0_A u) = af(u) + 0_A f(u) = af(u)$, pour tout $a \in A$. Ceci montre l'équivalence de (1) et (2). Il est évident que (3) implique (2). Enfin, si f satisfait à (2), alors l'énoncé (3) est valide pour $n = 1, 2$. Par récurrence, on montre que (3) est valide pour tout $n \geq 1$. Ceci achève la démonstration.

2.1.3. Proposition. Soient E, F deux espaces vectoriels sur un corps K, vus comme deux $K[x]$-modules définis par un K-endomorphisme f de E et par un K-endomorphisme g de F respectivement. Alors une application $h : E \to F$ est $K[x]$-linéaire si et seulement si h est K-linéaire et $hf = gh$.

Démonstration. Supposons que h est $K[x]$-linéaire. Pour tous $\alpha \in K$ et $u \in E$, on a $h(\alpha u) = h(\alpha \cdot u) = \alpha \cdot h(u) = \alpha h(u)$. Ainsi h est K-linéaire. De plus, pour tout $u \in E$, on a $(hf)(u) = h(f(u)) = h(x \cdot u) = x \cdot h(u) = g(h(u))$, D'où $hf = gh$. Supposons réciproquement que h est K-lináire et $hf = gh$. Soit $u \in E$. D'abord, comme h est K-linéaire, $h(\alpha \cdot u) = h(\alpha u) = \alpha g(u) = \alpha \cdot h(u)$. Ensuite, $h(x \cdot u) = h(f(u)) = (hf)(u) = (gh)(u) = g(h(u)) = x \cdot h(u)$, et $h(x^2 \cdot u) = h(x \cdot (x \cdot u)) = x \cdot (h(x \cdot u)) = x \cdot (x \cdot g(u)) = x^2 \cdot h(u)$. En général, on a $h(x^i \cdot u) = x^i \cdot h(u)$, pour tout $i \geq 0$. Ainsi $h((\alpha x^i) \cdot u) = (\alpha x^i) h(u)$, pour tous $\alpha \in K$ et $i \geq 0$. Or si $p = \sum_{i=0}^{n} \alpha_i x^i \in K[x]$, on a $h(p \cdot u) = h(\sum_{i=0}^{i} (\alpha_i x^i) \cdot u)) = \sum_{i=0}^{n} h((\alpha_i x^i) \cdot u) = \sum_{i=0}^{n} (\alpha_i x^i) \cdot h(u) = (\sum_{i=0}^{n} \alpha_i x^i) \cdot h(u) = p \cdot h(u)$. Ceci montre que h est $K[x]$-linéaire. La preuve de la proposition s'achève.

Exemple. Considérons le $\mathbb{R}[x]$-module $\mathbb{R}^{(2)}$ défini par l'application $\mathbb{R}$-linéaire suivante:

$$f : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Alors

$$g : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

est $\mathbb{R}$-linéaire telle que $fg = gf$. Ainsi g est $\mathbb{R}[x]$-linéaire.

Soient M, N des A-modules à gauche. L'ensemble des applications A-linéaires de M dans N est noté $\mathrm{Hom}_A(M, N)$. Pour $f, g \in \mathrm{Hom}_A(M, N)$, on définit la *somme* de f et g par

$$f + g : M \to N : u \mapsto f(u) + g(v),$$

qui est évidemment A-linéaire. Si A est commutatif, on définit le *produit* de $f \in \mathrm{Hom}_A(M,N)$ et $a \in A$ par

$$af : M \to N : u \mapsto au,$$

ce qui est aussi A-linéaire. Ceci nous donne le résultat facile suivant.

2.1.4. Proposition. Si M, N sont des A-modules à gauche, alors $\mathrm{Hom}_A(M,N)$ est un groupe abélien pour l'addition définie ci-dessus. En outre, si A est commutatif, alors $\mathrm{Hom}_A(M,N)$ est un A-module.

2.1.5. Lemme. Si $f : M \to N$ et $g : N \to L$ sont des applications A-linéaires de A-modules à gauche, alors $gf : M \to L$ est également A-linéaire.

Démonstration. Supposons que f, g sont A-linéaires. Pour tous $a, b \in A$ et $u, v \in M$, on a $(gf)(au+bv) = g(f(au+bv)) = g(af(u)+bf(v)) = ag(f(u)) + bg(f(v)) = a(gf)(u) + b(gf)(v)$. Ainsi gf est A-linéaire. Ceci achève la démonstration.

Soit M un A-module à gauche. Une application A-linéaire $f : M \to M$ s'appelle un *endomorphisme* de M. L'ensemble des endomorphismes du A-module M est noté $\mathrm{End}_A(M)$. Il suit du lemme 2.1.5 que si $f, g \in \mathrm{End}_A(M)$, alors $fg \in \mathrm{End}_A(M)$. Ceci nous conduit au résultat suivant.

2.1.6. Proposition. Si M est un A-module à gauche, alors $\mathrm{End}_A(M)$ est un anneau.

Démonstration. D'après la proposition 2.1.4, il suffit de vérifier la distributivité. Soient $f, g, h \in \mathrm{End}_A(M)$. Pour tout $u \in M$, on a

$$((f+g)h)(u) = (f+g)(h(u)) = f(h(u)) + g(h(u)) = (fh)(u) + (gh)(u) = (fh+gh)(u)$$

et

$$(h(f+g))(u) = h((f+g)(u)) = h(f(u)) + g(u)) = (hf)(u) + (hg)(u) = (hf+hg)(u).$$

D'où $(f+g)h = fh + gh$ et $h(f+g) = hf + hg$. Ceci achève la démonstration.

2.1.7. Lemme. Soit $f : M \to N$ une application A-linéaire.

(1) $\mathrm{Im}(f) = \{v \in N \mid v = f(u), \text{ pour un certain } u \in M\}$ est un sous-module de N.

(2) $\mathrm{Ker}(f) = \{u \in M \mid f(u) = 0_N\}$ est sous-module de M, appelé le *noyau* de f.

(3) f est injective si et seulement si $\mathrm{Ker}(f) = \{0_M\}$.

Démonstration. (1) Si $v_1, v_2 \in \mathrm{Im}(f)$, alors $v_i = f(u_i)$ avec $u_i \in M$, $i = 1, 2$. Pour tous $a_1, a_2 \in A$, on a $a_1v_1 + a_2v_2 = a_1f(u_1) + a_2f(u_2) = f(a_1u_1 + a_2u_2) \in \mathrm{Im}(f)$. Ainsi $\mathrm{Im}(f)$ est un sous-module de N.

(2) Si $u_1, u_2 \in \mathrm{Ker}(f)$ et $a_1, a_2 \in A$, alors $f(a_1u_1 + a_2u_2) = a_1f(u_1) + a_2f(u_2) = 0_N$, c'est-à-dire, $a_1u_1 + a_2u_2 \in \mathrm{Ker}(f)$. Donc $\mathrm{Ker}(f)$ est un sous-module de M.

(3) Supposons que f est injective. Si $u \in \mathrm{Ker}(f)$, alors $f(u) = 0_N = f(0_M)$. Donc $u = 0_M$ par l'injectivité. Cela signifie que $\mathrm{Ker}(f) = \{0_M\}$. Supposons réciproquement que $\mathrm{Ker}(f) = \{0_M\}$. Si $u, v \in M$ sont tels que $f(u) = f(v)$, alors $f(u - v) = f(u) - f(v) = 0_N$, c'est-à-dire, $u - v \in \mathrm{Ker}(f)$, et donc $u - v = 0_M$. Par conséquent, f est injective. Ceci achève la démonstration.

Exemple. (1) Soit N un sous-module de M. Considérons l'inclusion $j_{_N} : N \to M$ et la projective canonique $p_{_M} : M \to M/N$. On voit aisément que $\mathrm{Ker}(j_{_N}) = \{0_M\}$ et $\mathrm{Ker}(p_{_M}) = N$. Ainsi $j_{_N}$ est injective, mais p_N est injective si et seulement si $N = \{0_M\}$.

(2) Considérons le $\mathbb{R}[x]$-module $\mathbb{R}^{(2)}$ définie par l'application $\mathbb{R}$-linéaire

$$f : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On a vu que l'application

$$g : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

est $\mathbb{R}[x]$-linéaire. Or

$$\mathrm{Ker}(g) = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^{(2)} \mid \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a \\ -a \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

En particulier, g n'est pas injective.

2.1.8. Définition. Soit $f : M \to N$ une application linéaire de A-modules à gauche. On appelle $N/\mathrm{Im}f$ le *co-noyau* de f, noté $\mathrm{coker}f$.

Remarque. On voit aisément qu'une application A-linéaire f est surjective si et seulement si $\mathrm{coker} f = 0$.

Exemple. (1) Si N est un sous-module d'un A-module M, alors M/N est le co-noyau de l'inclusion $j : N \to M$.

(2) Considérons le $\mathbb{R}[x]$-module $\mathbb{R}^{(2)}$ via l'application $\mathbb{R}$-linéaire

$$f : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On a vu que l'application

$$g : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

est $\mathbb{R}[x]$-linéaire avec

$$\mathrm{Im} g = \left\{ \begin{pmatrix} c \\ c \end{pmatrix} \mid c \in \mathbb{R} \right\}.$$

Donc

$$\mathrm{coker} g = \left\{ \overline{\begin{pmatrix} a \\ 0 \end{pmatrix}} \mid a \in \mathbb{R} \right\},$$

qui est un $\mathbb{R}[x]$-module tel que

$$x \cdot \overline{\begin{pmatrix} a \\ 0 \end{pmatrix}} = \overline{\begin{pmatrix} -a \\ 0 \end{pmatrix}}.$$

2.1.9. Définition. Soient M, N des A-modules à gauche.

(1) Une application A-linéaire $f : M \to N$ s'appelle un *isomorphisme* si elle est bijective.

(2) Un isomorphisme $f : M \to M$ s'appelle un *automorphisme* de M.

(3) On dit que M, N sont *isomorphes*, noté $M \cong N$, s'il existe un certain isomorphisme $f : M \to N$.

Exemple. (1) $\mathbb{1}_M : M \to M$ est un automorphisme de M.

(2) Si N est un sous-module de M, alors la projection canonique $p_N : M \to M/N$ est un isomorphisme si et seulement si $N = \{0_M\}$.

(3) Considérons les A-modules à gauche A^n et

$$A^{(n)} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_1, \ldots, a_n \in A \right\}.$$

On voit aisément que

$$f : A^n \to A^{(n)} : (a_1, \ldots, a_n) \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

est un isomorphisme.

(4) Considérons les $\mathbb{Z}$-modules $\mathbb{Z}$ et $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$. L'application

$$j : \mathbb{Z} \to n\mathbb{Z} : a \mapsto na$$

est un isomorphisme.

2.1.10. Proposition. Soit $f : M \to N$ une application A-linéaire de A-modules à gauche.

(1) Si f est un isomorphisme, alors $f^{-1} : N \to M$ est A-linéaire, et donc un isomorphisme.

(2) f est un isomorphisme si et seulement s'il existe une application A-linéaire $g : N \to M$ telle que $gf = \mathbb{1}_M$ et $fg = \mathbb{1}_N$.

Démonstration. (1) Supposons que f est bijective. Alors $f^{-1} : N \to M$ est une application telle que $f^{-1}f = \mathbb{1}_M$ et $ff^{-1} = \mathbb{1}_N$. Soient $x, y \in N$ et $a, b \in A$. Alors $f(af^{-1}(x) + bf^{-1}(y)) = af(f^{-1}(x)) + bf(f^{-1}(y)) = a(ff^{-1})(x) + (ff^{-1})(y) = ax + by$. Donc $af^{-1}(x) + bf^{-1}(y) = f^{-1}(ax + by)$. Ceci montre que f^{-1} est A-linéaire.

(2) La nécessité suit directement de l'énoncé (1). Supposons qu'il existe une application A-linéaire $g : N \to M$ telle que $gf = \mathbb{1}_M$ et $fg = \mathbb{1}_N$. Si $x, y \in M$ sont tels que $f(x) = f(y)$, alors $g((f(x)) = g(f(y))$, c'est-à-dire, $(fg)(x) = (fg)(y)$, D'où, $x = y$. Ainsi f est injective. En outre, si $y \in N$, alors $x = g(y) \in M$ est tel que $f(x) = (fg)(y) = y$. Donc f est surjective. Ceci achève la démonstration.

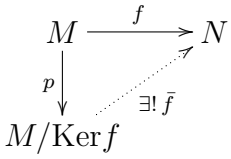
2.1.11. Corollaire. La relation d'isomorphisme $\cong$ est une relation d'équivalence sur les A-modules à gauche.

Démonstration. Soient M, N, L des A-modules á gauche. Comme $\mathbb{1}_M : M \to M$ est un isomorphisme, on a $M \cong M$. Si $M \cong N$, alors $N \cong M$ d'après la proposition 2.1.9(1). Enfin, si $f : M \to N$ et $g : N \to L$ sont des isomorphismes alors $gf : M \to L$ est évidemment bijective et A-linéaire d'après le lemme 2.1.5. Ceci montre que si $M \cong N$ et $N \to L$, alors $M \cong L$. La preuve s'achève.

2.2. Les théorèmes d'isomorphisme

Partout dans cette section, on se fixe M, N des A-modules à gauche.

2.2.1. Théorème. Soit $f : M \to N$ une application A-linéaire. Il existe une unique application A-linéaire injective $\bar{f} : M/\mathrm{Ker}f \to N$ telle que la diagramme



soit commutative (c'est-à-dire, $f = \bar{f} \circ p$), où p est la projection canonique.

Démonstration. Pour tout $\bar{u} \in M/\mathrm{Ker}f$, on définit $\bar{f}(\bar{u}) = f(u)$. Ceci est correctement définie. En effet, si $\bar{u} = \bar{v}$, alors $u - v \in \mathrm{Ker}f$. Ainsi $f(u) - f(v) = f(u - v) = 0_N$, c'est-à-dire, $f(u) = f(v)$. Pour tous $a, b \in A$ et $\bar{u}, \bar{v} \in M/\mathrm{Ker}f$, on a

$$\bar{f}(a\bar{u} + b\bar{v}) = \bar{f}(\overline{au + bv}) = f(au + bv) = af(u) + bf(v) = a\bar{f}(\bar{u}) + b\bar{f}(\bar{v}).$$

Cela veut dire que $\bar{f}$ est A-linéaire. Si $\bar{u} \in M/\mathrm{Ker}f$ est tel que $\bar{f}(\bar{u}) = 0$, alors $f(u) = 0$. Donc $u \in \mathrm{Ker}f$, et ainsi $\bar{u} = \bar{0}$. Par conséquent, $\bar{f}$ est injective. Enfin, pour tout $u \in M$, on a $(\bar{f}p)(u) = \bar{f}(p(u)) = \bar{f}(\bar{u}) = f(u)$. Donc $\bar{f}p = f$. Ceci achève la démonstration.

2.2.2. Corollaire. Soit $f : M \to N$ une application A-linéaire.

(1) $M/\mathrm{Ker}f \cong \mathrm{Im}f$.

(2) Si f est surjective, alors $N \cong M/\mathrm{Ker}f$.

Démonstration. (1) Définissons $\tilde{f} : M/\mathrm{Ker}f \to \mathrm{Im}f : \bar{u} \mapsto \bar{f}(\bar{u})$. Alors $\tilde{f}$ est une application A-linéaire injective. Pour tout $v \in \mathrm{Im}f$, on a $v = f(u)$ pour un certain $u \in M$. Donc $\tilde{f}(\bar{u}) = \bar{f}(\bar{u}) = f(u) = v$. Ainsi $\tilde{f}$ est bijective, et donc un isomorphisme.

(2) Si f est surjective, alors $N = \mathrm{Im}f \cong M/\mathrm{Ker}f$. Ceci achève la démonstration.

Exemple. (1) Considérons le $\mathbb{R}[x]$-module $\mathbb{R}^{(2)}$ via l'application $\mathbb{R}$-linéaire

$$f : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On a vu que l'application

$$g : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

est $\mathbb{R}[x]$-linéaire avec

$$\mathrm{Ker}(g) = \left\{ \begin{pmatrix} a \\ -a \end{pmatrix} \mid a \in \mathbb{R} \right\} = \mathbb{R}[x]u, \text{ où } u = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Or

$$\mathrm{Im}g = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} c \\ c \end{pmatrix} \mid c \in \mathbb{R} \right\} = \mathbb{R}[x]v, \text{ où } v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

D'après le corollaire 2.2.2(1), on a $\mathbb{R}^{(2)}/\mathbb{R}[x]u \cong \mathbb{R}[x]v$.

(2) Soit K un corps. Considérons les $M_2(K)$-modules à gauche $M_{2\times 3}(K)$ et $M_2(K)$. On voit aisément que l'application

$$f : M_{2\times 3}(K) \to M_2(K) : \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

est $M_2(K)$-linéaire surjective. En outre le noyau de f est

$$N = \left\{ \begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & a_{23} \end{pmatrix} \mid a_{ij} \in K \right\}.$$

D'après le corollaire 2.2.2(2), on a

$$M_{2\times 3}(K)/N = \left\{ \overline{\begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \end{pmatrix}} \mid a_{ij} \in K \right\} \cong M_2(K).$$

2.2.3. Corollaire. Un A-module à gauche M est cyclique si et seulement si $M \cong A/I$, où I est un idéal à gauche de A.

Démonstration. Supposons qu'il existe un isomorphisme $f : M \to A/I$, où I est un idéal à gauche de A. Comme f est surjective, il existe $u \in M$ tel que $f(u) = \bar{1}$. Pour tout $v \in M$, posons $f(v) = \bar{a}$ avec $a \in A$. Or $f(au) = af(u) = a\bar{1} = \bar{a}$. Comme f est injective, on a $v = au$. Donc $M = Au$, c'est-à-dire, M est cyclique. Réciproquement supposons que $M = Au$ avec $u \in M$. Alors $g : A \to M : a \mapsto au$ est une application A-linéaire surjective. Ainsi $I = \mathrm{Ker}f = \{a \in A \mid au = 0\}$ est un sous-module de ${}_AA$, c'est-à-dire, un idéal à gauche de A. D'après le corollaire 2.2.2(2), on a $M \cong A/I$. Ceci achève la démonstration.

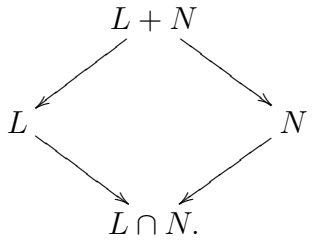
2.2.4. Théorème. Soit M un A-module à gauche. Si L, N sont des sous-modules de M, alors $(L + N)/N \cong L/(L \cap N)$.

Démonstration. Soient L, N des sous-modules de M. Alors N est sous-module de $L + N$. Considérons le module quotient $(L + N)/N$. On voit aisément que l'application

$$f : L \to (L + N)/N : u \mapsto u + N$$

est A-linéaire. Pour tout $w + N \in (L + N)/N$ avec $w \in L + N$, on a $w = u + v$ avec $u \in L$ et $v \in N$. Ainsi $w - u = v \in N$, et donc $w + N = u + N = f(u)$. Ceci montre que f est surjective. Pour tout $u \in L$, on a $u \in \mathrm{Ker}f$ si et seulement si $f(u) = 0 + N$ si et seulement si $u + N = 0 + N$ si et seulement si $u \in N$ si et seulement si $u \in L \cap N$. Donc $\mathrm{Ker}f = L \cap N$. D'aprés le corollaire 2.2.2(2), on a $(L + N)/N \cong L/\mathrm{Ker}f = L/(L \cap N)$. Ceci achève la démonstration.

Remarque. Considérons le parallélogramme suivant:



Le théorème 2.2.4 s'exprime par la *Loi de parallélogramme*: deux côtés opposés du parallélogramme sont isomorphes.

Soit $f : X \to Y$ une application quelconque. Si X' est un sous-ensemble de X, alors $f(X') = \{f(x) \mid x \in X'\}$ s'appelle l'*image* de X' par f. Si Y' est un sous-ensemble de Y, alors $f^{-1}(Y') = \{x \in X \mid f(x) \in Y'\}$ s'appelle le *pré-image* de Y' par f.

2.2.5. Lemme. Soit $f : M \to N$ une application A-linéaire.

(1) Si Q est un sous-module de N alors $f^{-1}(Q)$ est un sous-module de M contenant $\mathrm{Ker}f$.

(2) Si L est un sous-module de M, alors $f(L)$ est un sous-module de N contenu dans $\mathrm{Im}(f)$ et $f^{-1}(f(L)) = L + \mathrm{Ker}(f)$.

Démonstration. (1) Soit Q un sous-module de N. Si $u \in \mathrm{Ker}f$, alors $f(u) = 0_N \in Q$. D'où, $u \in f^{-1}(Q)$. Ainsi $\mathrm{Ker}f \subseteq f^{-1}(Q)$. En particulier, $f^{-1}(Q) \neq \emptyset$. Pour tous $a, b \in A$ et $u, v \in f^{-1}(Q)$, on a $f(u), f(v) \in Q$, et donc, $f(au + bv) = af(u) + bf(v) \in Q$. Cela veut dire que $au + bv \in f^{-1}(Q)$. Ainsi $f^{-1}(Q)$ est un sous-module de M.

(2) Par définition, $\emptyset \neq f(L) \subseteq \mathrm{Im}f$. Pour tous $a, b \in A$ et $u, v \in f(L)$, on a $u = f(u')$ et $v = f(v')$ avec $u', v' \in L$. Or $au + bv = af(u') + bf(v') = f(au' + bv') \in f(L)$, puisque $au' + bv' \in L$. Donc $f(L)$ est un sous-module de N. En outre, $L \subseteq f^{-1}(f(L))$ par définition, et $\mathrm{Ker}(f) \subseteq f^{-1}(f(L))$ par (1). Par conséquent, $L + \mathrm{Ker}f \subseteq f^{-1}(f(L))$. Si $u \in f^{-1}(f(L))$, alors $f(u) \in f(L)$, c'est-à-dire, il existe $v \in L$ tel que $f(u) = f(v)$. Ainsi $w = u - v \in \mathrm{Ker}(f)$. Donc $u = v + w \in L + \mathrm{Ker}(f)$. Ainsi $f^{-1}(f(L)) = L + \mathrm{Ker}(f)$. Ceci achève la démonstration.

Exemple. Considérons la projection canonique $p : \mathbb{Z} \to \mathbb{Z}_{12}$. Comme $\mathrm{Ker}p = 12\mathbb{Z}$, on a $p^{-1}(p(4\mathbb{Z})) = 4\mathbb{Z} + 12\mathbb{Z} = 4\mathbb{Z}$, mais $p^{-1}(p(5\mathbb{Z})) = 5\mathbb{Z} + 12\mathbb{Z} = \mathbb{Z}$.

2.2.6. Théorème. Soit $f : M \to N$ une application A-linéaire surjective. Soient $\mathcal{S}$ l'ensemble des sous-modules de M contenant $\mathrm{Ker}f$ et Σ l'ensemble des sous-modules de N.

(1) L'application $F : \mathcal{S} \to \Sigma : L \mapsto f(L)$ est une bijection qui préserve l'inclusion.

(2) Si Q est un sous-module de N, alors $M/f^{-1}(Q) \cong N/Q$.

Démonstration. (1) On prétend que F a pour inverse $G : \Sigma \to \mathcal{S} : Q \mapsto f^{-1}(Q)$. En effet, pour tout $Q \in \Sigma$, on a $f^{-1}(Q) \in \mathcal{S}$ tel que $f(f^{-1}(Q)) \subseteq Q$. Si $v \in Q$, alors $v = f(u)$ pour un ceratin $u \in E$. Or $u \in f^{-1}(Q)$, et donc $v = f(u) \in f(f^{-1}(Q))$. Ceci nous donne $Q = f(f^{-1}(Q))$. D'autre part, pour tout $L \in \mathcal{S}$, on a $f^{-1}(f(L)) = L + \mathrm{Ker}f = L$. Ceci montre l'énoncé. En outre, si $L_1 \subseteq L_2$, alors $f(L_1) \subseteq f(L_2)$. Réciproquement, si $f(L_1) \subseteq f(L_2)$, alors $L_1 = f^{-1}(f(L_1)) \subseteq f^{-1}(f(L_2)) = L_2$. Donc F préserve l'inclusion.

(2) Soit Q un sous-module de N. Considérant la projection canonique $p : N \to N/Q$, on voit que $pf : M \to N/Q$ est A-linéaire et surjective. Pour tout $u \in M$, on a $(pf)(u) = p(f(u)) = f(u) + Q = 0 + Q$ si et seulement si $f(u) \in Q$ si et seulement si $u \in f^{-1}(Q)$. Donc $\mathrm{Ker}(pf) = f^{-1}(Q)$. D'après le corollaire 2.2.2(2), $N/Q \cong M/f^{-1}(Q)$. Ceci achève la démonstration.

Remarque. Si $f : M \to N$ est un isomorphisme, alors tout sous-module de M contient $\mathrm{Ker}(f)$. Par conséquent, les sous-modules de M sont en bijection avec ceux de N.

2.2.7. Corollaire. Soit N un sous-module de M.

(1) L'application $L \mapsto L/N$ est une bijection entre l'ensemble des sous-modules de M contenant N et l'ensemble des sous-modules de M/N.

(2) Si L est un sous-module de M contenant N, alors $(M/N)/(L/N) \cong M/L$.

Démonstration. La projective canonique $p : M \to M/N$ est surjective avec $\mathrm{Ker}p = N$. Si L est un sous-module de M contenant N, alors $p(L) = \{u + N \mid u \in L\} = L/N$, et $p^{-1}(L/N) = p^{-1}(p(L)) = L + \mathrm{Ker}p = L + N = L$. Donc le corollaire est une conséquence immédiate du théorème 2.2.6. Ceci achève la démonstration.

Exemple. Considérons le $\mathbb{Z}$-module $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \cdots, \bar{11}\}$. Pour trouver ses sous-modules, il suffit de trouver les sous-modules de $\mathbb{Z}$ contenant $12\mathbb{Z}$. Soit N un tel sous-module de $\mathbb{Z}$. Alors $N = n\mathbb{Z}$ avec $n > 0$. Or $12\mathbb{Z} \subseteq n\mathbb{Z}$ si et seulement si $n|12$ si et seulement si $n = 1, 2, 3, 4, 6, 12$. Par conséquent, les sous-modules de $\mathbb{Z}_{12}$ sont $M_n = n\mathbb{Z}/12\mathbb{Z}$ avec $n = 1, 2, 3, 4, 6, 12$. Or $M_1 = \mathbb{Z}_{12}$, $M_{12} = \{\bar{0}\}$, $M_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$, $M_3 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $M_4 = \{\bar{0}, \bar{4}, \bar{8}\}$, et $M_6 = \{\bar{0}, \bar{6}\}$. En outre, $\mathbb{Z}_{12}/M_n = (\mathbb{Z}/12\mathbb{Z})/(n\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$, pour tout $n = 1, 2, 3, 4, 6, 12$.

2.3. Modules simples

On se fixe M un A-module à gauche. On sait que $\{0_M\}$ et M sont des sous-modules de M.

2.3.1. Définition. On dit que M est *simple* si M a exactement deux sous-modules distincts $\{0_M\}$ et M.

Remarque. Si $M \cong N$, alors les sous-modules de M sont en bijection avec ceux de N. En particulier, M est simple si et seulement si N l'est.

Exemple. Soit D un corps-gauche. Un D-module à gauche M est simple si et seulement si M est de dimension un. En particulier, ${}_DD$ est simple.

2.3.2. Définition. Un sous-module N de M est dit *maximal* si $N \neq M$ et il n'y a aucun sous-module L de M tel que $N \subset L \subset M$.

Remarque. (1) Un module M est simple si et seulement si $\{0_M\}$ est un sous module maximal.

(2) Un sous-module maximal de ${}_AA$ est un idéal à gauche maximal de A.

2.3.3. Lemme. Soit M un A-module à gauche non nul.

(1) Un sous-module N de M est maximal si et seulement si M/N est simple.

(2) Si M est cyclique, alors M admet au moins un sous-module maximal.

Démonstration. (1) Soit N un sous-module de M. Si N n'est pas maximal, alors soit $N = M$ soit il existe un sous-module L de M tel que $N \subset L \subset M$. Donc soit M/N est nul soit M/N admet un sous-module propre L/N. D'où M/N n'est pas simple. Supposons maintenant que N est maximal. Alors M/N est non nul. Si L' est un sous-module non nul de M/N, alors $L' = L/N$ avec L un sous-module de M avec $N \subset L$. Comme N est maximal, on a $L = M$ et donc $L' = M/N$. Ceci implique que M/N est simple.

(2) Supposons que $M = Au$ avec $u \in M$. Soit Σ l'ensemble des sous-modules L de M avec $u \notin L$, qui est ordonné par l'inclusion. Comme M est non nul, on voit que $\{0_M\}$ appartient à Σ. Si $\{L_\lambda \mid \lambda \in \Lambda\}$ est une chaîne de Σ, on voit que $L = \cup_{\lambda\in\Lambda} L_\lambda$ appartient à Σ. D'après le lemme de Zorn, Σ admet un membre maximal L_0. Comme $u \notin L_0$, on a $L_0 \neq M$. En outre si N est un sous-module de M tel que $L_0 \subset N$. Par la maximalité, on a N n'appartient pas à Σ, c'est-à-dire, $u \in N$, et donc $M \subseteq N$. D'où $M = N$. Cela veut dire que L_0 est un sous-module maximal de M. Ceci achève la démonstration.

2.3.4. Corollaire. Si A est un anneau non trivial, alors A admet au moins un module à gauche simple.

Démonstration. Étant non nul et cyclique ${}_AA$, d'après le lemme 2.3.3(2), a un sous module maximal I_0. D'après le lemme 2.3.3(1), A/I_0 est simple. Ceci achève la démonstration.

2.3.5. Proposition. Soit S un A-module à gauche non nul. Les conditions suivantes sont équivalentes.

(1) S est simple.

(2) Pour tout élément non nul u de S, on a $S = Au$.

(3) Il existe un idéal à gauche maximal I de A tel que $S \cong A/I$.

Démonstration. Supposons que (1) est valide. Si u est un élément non nul u de S, alors Au est un sous-module non nul de S. Comme S est simple, on a $S = Au$. D'où (2) est valide. Supposons réciproquement que (2) est valide. Si L est un sous-module non nul de S, alors L contient un élément non nul u. Or $S = Au \subseteq L$. D'où $L = S$. Ceci montre l'équivalence de (1) et (2).

Enfin, il suit du lemme 2.3.3(1) que (3) implique (1). Supposons que S est simple. Alors $S = Au$ avec u un élément non nul de S. Or

$$f : A \to S : a \mapsto au$$

est une application A-linéaire surjective. Ainsi $S = A/I$, où $I = \mathrm{Ker}(f)$. Comme A/I est simple, d'après le lemme 2.3.3(1), I est un idéal à gauche maximal de A. Ceci montre l'équivalence de (1) et (3). La preuve s'achève.

Exemple. Soit K un corps. Pour tout entier $n \geq 1$, le $M_n(K)$-module à gauche $K^{(n)}$ est simple. En effet, soit

$$u = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

un élément non nul de $K^{(n)}$, disons $a_r \neq 0$ avec $1 \leq r \leq n$. Pour tous $1 \leq i, j \leq n$, posons $E_{ij} \in M_n(K)$ dont le (i,j)-terme est 1_D et les autres sont tous nuls. Alors $e_r = (a_r^{-1}E_{rr})u$, et donc $e_i = E_{ir}e_r$, $i = 1, \ldots, n$. Par conséquent, $K^{(n)} = M_n(K) \cdot u$.

Rappelons qu'un anneau principal est un anneau intègre dont tous les idéaux sont engendrés par un seul élément.

2.3.6. Corollaire. Si A est un anneau principal, alors un A-module S est simple si et seulement si $S \cong A/<p>$, où p est un élément irréductible de A.

Démonstration. Si I est un idéal de A, alors $I =< a >$. Or I est maximal si et seulement si a est irrédutible. Maintenant le résulat se découle immédiatement de la proposition 2.3.5. La preuve s'achève.

Exemple. Les $\mathbb{Z}$-modules simples sont $\mathbb{Z}/p\mathbb{Z}$ avec p premier qui sont deux à deux non isomorphes.

2.3.7. Proposition. Soit S un A-modules à gauche non nul. Les conditions suivantes sont équivalentes:

(1) S est simple.

(2) Toute application A-linéaire $f : S \to M$ est nulle ou injective.

(3) Toute application A-linéaire $g : M \to S$ est nulle ou surjective.

Démonstration. Supposons que S est simple. Soit $f : S \to M$ une application A-linéaire. Si $\mathrm{Ker}f = 0$, alors f est injective. Sinon, $\mathrm{Ker}f = S$. Donc $f(u) = 0_M$ pour tout $u \in S$. C'est-à-dire, f est nulle.

Supposons que (2) est valide. Soit $g : M \to S$ une application A-linéaire. Considérons la projection canonique $p : S \to S/\mathrm{Im}(g)$. Si p est nulle, alors $S/\mathrm{Im}(g) = 0$. D'où $S = \mathrm{Im}(g)$. C'est-à-dire, g est surjective. Sinon, p est injective par (2). D'où $\mathrm{Im}(g) = \mathrm{Ker}(p) = 0$. C'est-à-dire, g est nulle.

Supposons que (3) est valide. Soit L un sous-module de S. Considérons l'inclusion $j : L \to S$. Si j est nulle, alors $L = 0$. Sinon j est surjective par (3). D'où $S = \mathrm{Im}(j) = L$. Donc S est simple. Ceci achève la démonstration.

2.3.8. Lemme de Shur. Si S est un A-module à gauche simple, alors $\mathrm{End}_A(S)$ est un corps-gauche.

Démonstration. Si $f : S \to S$ est une application A-linéaire non nul alors, d'après la proposition 2.3.6, f est bijective et donc un automorphisme de S. Par conséquent, $\mathrm{End}_A(S)$ est un anneau dont tous les éléments non nuls sont inversibles. C'est-à-dire, $\mathrm{End}_A(S)$ est un corps-gauche. La preuve s'achève.

Exemple. Soit $A = M_n(K)$ avec K un corps et $n \geq 1$ un entier. Alors

$$\mathrm{End}_A(K^{(n)}) = \{\lambda \mathbb{1} \mid \lambda \in K\},$$

ce qui est un corps.

Démonstration. Soit $f : K^{(n)} \to K^{(n)}$ une application A-linéaire. Pour tous $\lambda \in K$ et $u \in K^{(n)}$, on a $f(\lambda u) = f((\lambda I_n)u) = (\lambda I_n)f(u) = \lambda f(u)$. Ainsi f est K-linéaire. Donc f est de la forme $f : K^{(n)} \to K^{(n)} : u \mapsto Pu$, où $P = (p_{ij})_{n\times n} \in M_n(K)$. Soit $Q \in M_n(K)$. Pour tout $u \in K^{(n)}$, on a $(PQ)u = f(Qu) = Qf(u) = (QP)u$. D'où $PQ = QP$ pour toute $Q \in M_n(K)$. On se fixe i, j avec $1 \leq i, j \leq n$ et $i \neq j$. Alors $PE_{ji} = E_{ji}P$. Remarquons que la j-ième ligne de $E_{ji}P$ est la i-ième ligne de P, c'est-à-dire, $(p_{i1}, \ldots, p_{in})$. Et la j-ième ligne de PE_{ji} est $(0, \ldots, 0, p_{jj}, 0, \ldots, 0)$, où p_{jj} se trouve dans la i-ième composante. Ainsi $p_{ij} = 0$ et $p_{ii} = p_{jj}$. Cela veut dire que $P = p_{11}I_n$. Par conséquent, $f = p_{11}\mathbb{1}$.

2.4. Produit et co-produit

À partir du A-module à gauche régulier ${}_AA$, on a vu que le produit cartésien

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A, i = 1, \ldots, n\}$$

est un A-module à gauche. On va généraliser cette construction pour une famille arbitraire (finie ou infinie) de A-modules à gauche. Étant donnée une famille non vide $\{M_\lambda \mid \lambda \in \Lambda\}$ de A-modules à gauche. Si une application

$$u : \Lambda \to \cup_{\lambda\in\Lambda} M_\lambda : \lambda \mapsto u(\lambda)$$

est telle que $u(\lambda) \in M_\lambda$ pour tout $\lambda \in \Lambda$, alors on écrit $u = (u_\lambda)_{\lambda\in\Lambda}$, où $u_\lambda = u(\lambda)$. Évidemment, $(u_\lambda)_{\lambda\in\Lambda} = (v_\lambda)_{\lambda\in\Lambda}$ si et seulement si $u_\lambda = v_\lambda$, pour tout $\lambda \in \Lambda$.

2.4.1. Proposition. Si $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille non vide de A-modules à gauche, alors

$$\prod\nolimits_{\lambda\in\Lambda} M_\lambda = \{(u_\lambda)_{\lambda\in\Lambda} \mid u_\lambda \in M_\lambda, \text{ pour tout } \lambda \in \Lambda\}$$

est un A-module à gauche, appelé le *produit* de la famille $\{M_\lambda \mid \lambda \in \Lambda\}$.

Démonstration. Pour tous $u = (u_\lambda)_{\lambda\in\Lambda},\ v = (v_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda$ et $a \in A$, on définit

$$au = (au_\lambda)_{\lambda\in\Lambda},\ u + v = (u_\lambda + v_\lambda)_{\lambda\in\Lambda}.$$

Il est évident que $(0_{M_\lambda})_{\lambda\in\Lambda}$ est le zéro pour l'addition et tout élément $(u_\lambda)_{\lambda\in\Lambda}$ a pour opposé $(-u_\lambda)_{\lambda\in\Lambda}$. On peut vérifier que les autres axiomes d'un A-module à gauche sont valides. Ceci achève la démonstration.

Remarque. (1) Si $\Lambda = \{1, 2, \ldots, n\}$, alors

$$\prod_{i=1}^{n} M_i = \{(a_1, \ldots, a_n) \mid a_i \in M_i, i = 1, \ldots, n\}.$$

(2) Si $M_\lambda = M$, pour tout $\lambda \in \Lambda$, on note alors $\prod_{\lambda\in\Lambda} M_\lambda = M^\Lambda$.

Exemple. Si $\mathbb{N} = \{1, 2, \cdots, n, \cdots,\}$, alors

$$A^{\mathbb{N}} = \{(a_1, a_2, \cdots, a_n, \cdots,) \mid a_i \in A, i = 1, 2, \cdots\}.$$

2.4.2. Définition. Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non vide de A-modules à gauche. Pour tout $\mu \in \Lambda$, l'application

$$p_\mu : \prod\nolimits_{\lambda\in\Lambda} M_\lambda \to M_\mu : (u_\lambda)_{\lambda\in\Lambda} \mapsto u_\mu$$

est A-linéaire et appelée la *projection* de $\prod_{\lambda\in\Lambda} M_\lambda$ sur M_μ.

Exemple. Si $\Lambda = \{1, 2, \cdots, n\}$, il existe n projections

$$p_j : \prod\nolimits_{i=1}^{n} M_i \to M_j : (a_1, \cdots, a_n) \mapsto a_j;\ \ j = 1, 2, \ldots, n.$$

Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non vide de A-modules à gauche. Un élément

$$u = (u_\lambda)_{\lambda\in\Lambda} \in \prod\nolimits_{\lambda\in\Lambda} M_\lambda$$

est dit *à support fini* si $\{\lambda \in \Lambda \mid u_\lambda \neq 0_{M_\lambda}\}$ est fini. C'est le cas si et seulement s'il existe un sous-ensemble fini Λ_1 de Λ tel que $u_\lambda = 0_{M_\lambda}$ pour tout $\lambda \in \Lambda\backslash\Lambda_1$.

2.4.3. Proposition. Si $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille non vide de A-modules à gauche, alors

$$\amalg_{\lambda\in\Lambda} M_\lambda = \Big\{ u \in \prod\nolimits_{\lambda\in\Lambda} M_\lambda \ \mid \ u \text{ est à support fini} \Big\}$$

est un sous-module de $\prod_{\lambda\in\Lambda} M_\lambda$, appelé le *co-produit* de la famille $\{M_\lambda \mid \lambda \in \Lambda\}$.

Démonstration. D'abord, $(0_{M_\lambda})_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$. Soient $u = (u_\lambda)_{\lambda\in\Lambda},\ v = (v_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$. Par définition, $\Lambda_1 = \{\lambda \in \Lambda \mid u_\lambda \neq 0_{M_\lambda}\}$ et $\Lambda_2 = \{\lambda \in \Lambda \mid v_\lambda \neq 0_{M_\lambda}\}$ sont tous finis. Donc $\Lambda_0 = \Lambda_1 \cup \Lambda_2$ est fini tel que $u_\lambda = v_\lambda = 0_{M_\lambda}$, pour tout $\lambda \in \Lambda\backslash\Lambda_0$. Ainsi $au_\lambda + b\lambda = 0_{M_\lambda}$, pour tout $\lambda \in \Lambda\backslash\Lambda_0$. Par conséquent, $au + bv = (au_\lambda + bv_\lambda)_{\lambda\in\Lambda}$ est à support fini. Donc $\amalg_{\lambda\in\Lambda} M_\lambda$ est un sous-module de $\prod_{\lambda\in\Lambda} M_\lambda$. Ceci achève la démonstration.

Remarque. (1) Si Λ est fini, alors $\amalg_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$. Par exemple, $A^n = \amalg_{i=1}^n A_i$, où $A_i = {}_AA$.

(2) Si $M_\lambda = M$ pour tout $\lambda \in \Lambda$, on note alors $M^{(\Lambda)} = \amalg_{\lambda\in\Lambda} M_\lambda$.

2.4.4. Définition. Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non vide de A-modules à gauche. Pour tout $\mu \in \Lambda$, l'application

$$q_\mu : M_\mu \to \amalg_{\lambda\in\Lambda} M_\lambda : u_\mu \mapsto (u_\lambda)_{\lambda\in\Lambda},\ \text{où } u_\lambda = 0_{M_\lambda},\ \text{pour tout } \lambda \neq \mu$$

est A-linéaire et appelée l'*injection* de M_μ dans $\amalg_{\lambda\in\Lambda} M_\lambda$.

Exemple. Si $\Lambda = \{1, 2, \cdots, n\}$, alors il existe n injections

$$q_j : M_j \to \prod\nolimits_{i=1}^n M_i \to M_i : a_j \mapsto (0_{M_1}, \cdots, 0_{M_{j-1}}, a_j, 0_{M_{j+1}}, \cdots, 0_{M_n}).$$

Soit $M = M_1 \prod M_2 = \{(u_1, u_2) \mid u_i \in M_i, i = 1, 2\}$, où M_1, M_2 des A-modules à gauche. Soient $p_i : M \to M_i$ les projections et $q_i : M_i \to M$ les injections, $i = 1, 2$. On vérifie aisément que $q_1p_1 + q_2p_2 = \mathbb{1}_M$, et pour tous $1 \leq i, j \leq 2$,

$$p_iq_j = \begin{cases} \mathbb{1}_{M_i}, & \text{si} \quad i = j; \\ 0, & \text{si} \quad i \neq j. \end{cases}$$

2.4.5. Théorème. Soient $M, M_1, \ldots, M_n$ des A-modules à gauche. Alors $M \cong \prod_{i=1}^n M_i$ si et seulement s'il existe des applications A-linéaires $f_i : M \to M_i$ et $g_i : M_i \to M$,

$i = 1, \cdots, n$, tels que $\sum_{i=1}^{n} g_i f_i = \mathbb{1}_M$, et pour tous $1 \leq i, j \leq n$,

$$f_i g_j = \begin{cases} \mathbb{1}_{M_i}, & \text{si} \quad i = j; \\ 0, & \text{si} \quad i \neq j. \end{cases}$$

Démonstration. Posons $L = \prod_{i=1}^{n} M_i$. Considérons les projections $p_i : L \to M_i$ et les injections $q_i : M_i \to L$, $i = 1, \ldots, n$. On voit facilement que $\sum_{i=1}^{n} q_i p_i = \mathbb{1}_L$, et pour tous $1 \leq i, j \leq n$, on a $p_i q_i = \mathbb{1}_{M_i}$ et $p_i q_j = 0$ lorsque $i \neq j$. Supposons qu'il existe un isomorphisme $f : M \to L$. Posons $f_i = p_i f$ et $g_i = f^{-1} q_i$, $i = 1, \cdots, n$. Alors $\sum_{i=1}^{n} g_i f_i = \sum_{i=1}^{n} f^{-1} q_i p_i f = f^{-1}(\sum_{i=1}^{n} q_i p_i) f = f^{-1} f = \mathbb{1}_M$, $f_i g_i = p_i f f^{-1} q_i = p_i q_i = \mathbb{1}_{M_i}$, et $f_i g_j = p_i f f^{-1} q_j = p_i q_j = 0$, pour $1 \leq i, j \leq n$ avec $i \neq j$.

Maintenant on montrera la suffisance. En effet, il est evident que l'application

$$f : L \to M : (u_1, \ldots, u_n) \mapsto \sum\nolimits_{i=1}^{n} g_i(u_i)$$

est A-linéaire. Pour tout $u \in M$, on a $v = (f_1(u), \ldots, f_n(u)) \in L$ tel que

$$f(v) = \sum_{i=1}^{n} g_i(f_i(u)) = \sum_{i=1}^{n} (g_i f_i)(u) = \mathbb{1}_M(u) = u.$$

D'où, f est surjective. Si $u = (u_1, \ldots, u_n) \in \mathrm{Ker} f$, alors $\sum_{i=1}^{n} g_i(u_i) = 0_M$. Pour tout $1 \leq j \leq n$, on a $0_{M_j} = f_j(0_M) = \sum_{i=1}^{n} (f_j g_i)(u_i) = f_j g_j(u_j) = \mathbb{1}_{M_j}(u_j) = u_j$. D'où, f est injective, et donc un isomorphisme. Ceci achève la démonstration.

2.5. Sommes directs

Partout dans cette section, on se fixe M un A-module à gauche.

2.5.1. Définition. Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non vide de sous-modules de M. Si $(u_\lambda)_{\lambda \in \Lambda} \in \amalg_{\lambda \in \Lambda} M_\lambda$, alors $\Lambda_0 = \{\lambda \in \Lambda \mid u_\lambda \neq 0_M\}$ est fini. On définit $\sum_{\lambda \in \Lambda} u_\lambda \in \sum_{\lambda \in \Lambda} M_\lambda$ par

$$\sum\nolimits_{\lambda \in \Lambda} u_\lambda = \begin{cases} 0_M, & \text{si } \Lambda_0 = \emptyset, \\ \sum_{\lambda \in \Lambda_0} u_\lambda, & \text{si } \Lambda_0 \neq \emptyset. \end{cases}$$

Remarque. (1) Si $\Lambda_1 \subseteq \Lambda$ tel que $u_\lambda = 0_M$ pour tout $\lambda \in \Lambda \backslash \Lambda_1$, alors

$$\sum\nolimits_{\lambda \in \Lambda} u_\lambda = \sum\nolimits_{\lambda \in \Lambda_1} u_\lambda.$$

(2) Si $\Lambda = \Lambda_1 \cup \Lambda_2$ et $\Lambda_1 \cap \Lambda_2 = \emptyset$, alors $\sum_{\lambda\in\Lambda} u_\lambda = \sum_{\lambda\in\Lambda_1} u_\lambda + \sum_{\lambda\in\Lambda_2} u_\lambda$.

(3) Si $f : M \to N$ est A-linéaire, alors $f(\sum_{\lambda\in\Lambda} u_\lambda) = \sum_{\lambda\in\Lambda} f(u_\lambda)$.

2.5.2. Lemme. Si $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille non vide de sous-modules de M, alors l'application

$$\rho : \amalg_{\lambda\in\Lambda} M_\lambda \to \sum\nolimits_{\lambda\in\Lambda} M_\lambda : (u_\lambda)_{\lambda\in\Lambda} \mapsto \sum\nolimits_{\lambda\in\Lambda} u_\lambda$$

est A-linéaire et surjective.

Démonstration. Si $v \in \sum_{\lambda\in\Lambda} M_\lambda$, alors v s'écrit $v = \sum_{i=1}^{n} u_{\lambda_i}$, où $\lambda_1, \ldots, \lambda_n \in \Lambda$ et $u_{\lambda_i} \in M_{\lambda_i}$. Posons $u_\lambda = 0_M$, pour tout $\lambda \in \Lambda\backslash\{\lambda_1, \cdots, \lambda_n\}$. Alors $u = (u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$ tel que $v = \rho(u)$. Ainsi ρ est surjective.

Il reste à montrer que ρ est A-linéaire. Si $u = (u_\lambda)_{\lambda\in\Lambda}, v = (v_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$ et $a, b \in A$, alors $au + bv = (au_\lambda + bv_\lambda)_\lambda$. On veut montrer que $\rho(au + bv) = a\rho(u) + b\rho(v)$. C'est-à-dire,

$$(*) \qquad \sum\nolimits_{\lambda\in\Lambda} (au_\lambda + bv_\lambda) = a\left(\sum\nolimits_{\lambda\in\Lambda} u_\lambda\right) + b\left(\sum\nolimits_{\lambda\in\Lambda} v_\lambda\right).$$

Pour ce faire, posons $\Lambda_1 = \{\lambda \in \Lambda \mid u_\lambda \neq 0_M\}$, $\Lambda_2 = \{\lambda \in \Lambda \mid v_\lambda \neq 0_M\}$, et $\Lambda_0 = \Lambda_1 \cup \Lambda_2$. Alors Λ_0 est fini tel que pour tout $\lambda \in \Lambda\backslash\Lambda_0$, on a $u_\lambda = v_\lambda = au_\lambda + bv_\lambda = 0_M$. Si $\Lambda_0 = \emptyset$, alors $\Lambda_1 = \Lambda_2 = \emptyset$. Par définition, $\sum_{\lambda\in\Lambda} u_\lambda = 0_M$, $\sum_{\lambda\in\Lambda} v_\lambda = 0_M$, et $\sum_{\lambda\in\Lambda}(au_\lambda + bv_\lambda) = 0_M$. D'où l'éaglité $(*)$. Sinon, on a

$$\begin{aligned} a\left(\sum_{\lambda\in\Lambda} u_\lambda\right) + b\left(\sum_{\lambda\in\Lambda} v_\lambda\right) &= a\left(\sum_{\lambda\in\Lambda_0} u_\lambda\right) + b\left(\sum_{\lambda\in\Lambda_0} v_\lambda\right) \\ &= \sum_{\lambda\in\Lambda_0}(au_\lambda + bv_\lambda) \\ &= \sum_{\lambda\in\Lambda}(au_\lambda + bv_\lambda). \end{aligned}$$

D'où l'égalité $(*)$. Ceci achève la démonstration.

2.5.3. Définition. Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non-vide de sous-modules de M. Si l'application

$$\rho : \amalg_{\lambda\in\Lambda} M_\lambda \to \sum\nolimits_{\lambda\in\Lambda} M_\lambda : (u_\lambda)_{\lambda\in\Lambda} \mapsto \sum\nolimits_{\lambda\in\Lambda} u_\lambda$$

est un isomorphisme, on dit alors que $\sum_{\lambda\in\Lambda} M_\lambda$ est une *somme directe*. Dans ce cas, la somme est notée $\oplus_{\lambda\in\Lambda} M_\lambda$.

Exemple. Soit K un corps. Considérons le K-espace vectoriel $K[x]$. On voit aisément que $V_n = \{ax^n \mid a \in K\}$, $n = 0, 1, 2, \ldots$, sont des sous-espaces vectoriels de $K[x]$ tels que

$K[x] = \sum_{n=0}^{\infty} V_n$. En outre, l'application

$$\rho : \amalg_{n=0}^{\infty} V_n \to \sum_{n=0}^{\infty} V_n : (a_0, a_1 x, \cdots, a_n x^n, \cdots,) \mapsto \sum_{n=0}^{\infty} a_n x^n$$

est injective, et donc un isomorphisme. Ceci implique que $K[x] = \oplus_{n=0}^{\infty} V_n$.

Remarque. Si $\Lambda = \{1\}$, alors la somme $\sum_{\lambda\in\Lambda} M_\lambda = M_1$ est évidemment directe.

2.5.4. Théorème. Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille de sous-modules de M avec Λ ayant au moins deux indices. Les conditions suivantes sont équivalentes:

(1) $\sum_{\lambda\in\Lambda} M_\lambda = \oplus_{\lambda\in\Lambda} M_\lambda$.

(2) Tout $u \in \sum_{\lambda\in\Lambda} M_\lambda$ s'écrit uniquement $u = \sum_{\lambda\in\Lambda} u_\lambda$, où $(u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$.

(3) Toute égalité $\sum_{\lambda\in\Lambda} u_\lambda = 0_M$, $(u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$, entraîne $u_\lambda = 0_M$ pour tout $\lambda \in \Lambda$.

(4) $M_\lambda \cap \left(\sum_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu\right) = \{0_M\}$, pour tout $\lambda \in \Lambda$.

Démonstration. Supposons que ρ est un isomorphisme. Soit $u \in \sum_{\lambda\in\Lambda} M_\lambda$. Par définition, il existe un unique $(u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$ tel que $u = \rho((u_\lambda)_{\lambda\in\Lambda}) = \sum_{\lambda\in\Lambda} u_\lambda$. Ceci montre que (1) implique (2).

Supposons que (2) est valide. Soit $\sum_{\lambda\in\Lambda} u_\lambda = 0_M$, où $(u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$. Mais $0_M = \sum_{\lambda\in\Lambda} 0_M$. D'après l'unicité, $(u_\lambda)_{\lambda\in\Lambda} = (0_M)_{\lambda\in\Lambda}$, c'est-à-dire, $u_\lambda = 0_M$, pour tout $\lambda \in \Lambda$. Ainsi (3) est valide.

Supposons que (3) est valide. On se fixe un $\lambda \in \Lambda$. Étant un sous-module de M, $M_\lambda \cap \sum_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu$ contient 0_M. Soit $u_\lambda \in M_\lambda \cap \sum_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu$. Alors il existe $(v_\mu)_{\mu\in\Lambda\setminus\{\lambda\}} \in \amalg_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu$ tel que $u_\lambda = \sum_{\mu\in\Lambda\setminus\{\lambda\}} v_\mu$. Posant $v_\lambda = -u_\lambda$, on a $(v_\mu)_{\mu\in\Lambda} \in \amalg_{\mu\in\Lambda} M_\mu$ tel que $\sum_{\mu\in\Lambda} v_\mu = 0_M$. Ainsi $v_\mu = 0_M$, pour tout $\mu \in \Lambda$. En particulier, $u_\lambda = -v_\lambda = 0_M$. D'où, $M_\lambda \cap \sum_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu = \{0_M\}$. Ceci montre que (4) est valide.

Supposons que (4) est valide. Si $(u_\lambda)_{\lambda\in\Lambda} \in \mathrm{Ker}\rho$, alors $\sum_{\lambda\in\Lambda} u_\lambda = 0_M$. On se fixe un élément quelconque λ de Λ. Alors $-u_\lambda = \sum_{\mu\in\Lambda\setminus\{\lambda\}} u_\mu \in M_\lambda \cap \sum_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu$, et ce dernier contient seulement 0_M. Ainsi $-u_\lambda = 0_M$. Donc $u_\lambda = 0_M$, pour tout $\lambda \in \Lambda$. Ceci montre que $\mathrm{Ker}\rho = \{0_M\}$. Donc ρ est injective. Par conséquent, (1) est valide. Ceci achève la démonstration.

Remarque. Si M_1, M_2 sont des sous-modules de M, alors $M_1 + M_2 = M_1 \oplus M_2$ si et seulement si $M_1 \cap M_2 = \{0_M\}$.

2.5.5. Proposition. Si $\mathcal{B} = \{u_\lambda \mid \lambda \in \Lambda\}$ est un sous-ensemble non vide de M, alors $\mathcal{B}$ est une base de M si et seulement si tout $u \in M$ s'écrit d'une façon unique $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Dans ce cas, $M = \oplus_{\lambda\in\Lambda} Au_\lambda$.

Démonstration. D'abord, supposons que tout $u \in M$ s'écrit d'une façon unique $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. En particulier, $M =< \mathcal{B} >$. Étant donné un sous-ensemble fini $\{u_{\lambda_1}, \ldots, u_{\lambda_n}\}$ de Λ. Supposons que $a_1u_{\lambda_1} + \cdots + a_nu_{\lambda_n} = 0_M$ avec $a_1, \ldots, a_n \in A$. Pour tout $\lambda \in \Lambda$, posons $a_\lambda = a_i$ si $\lambda = \lambda_i$ pour un certain $1 \leq i \leq n$; et $a_\lambda = 0_\lambda$ sinon. Alors $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\lambda)}$ est tel que $0_M = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$. Mais $0_M = \sum_{\lambda\in\Lambda} 0_A u_\lambda$. D'après l'unicité, on a $(a_\lambda)_{\lambda\in\Lambda} = (0_A)_{\lambda\in\Lambda}$, c'est-à-dire, $a_\lambda = 0_A$, pour tout $\lambda \in \Lambda$. En particulier, $a_i = 0_A$ pour tout $1 \leq i \leq n$. Ceci montre que $\mathcal{B}$ est libre, et donc une base de M.

Supposons réciproquement que $\mathcal{B}$ est une base de M. Soit $u \in M$. Alors il existe $\lambda_1, \ldots, \lambda_n \in \Lambda$ et $a_1, \ldots, a_n \in A$ tels que $u = a_1u_{\lambda_1} + \cdots + a_nu_{\lambda_n}$. Pour tout $\lambda \in \Lambda$, on pose $a_\lambda = a_i$ si $\lambda = \lambda_i$ avec $1 \leq i \leq n$ et $a_\lambda = 0_A$ sinon. Alors $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\lambda)}$ est tel que $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$. Supposons maintenant que $u = \sum_{\lambda\in\Lambda} b_\lambda u_\lambda$ avec $(b_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Comme $(a_\lambda)_{\lambda\in\Lambda}, (b_\lambda)_{\lambda\in\Lambda} \in A^{(\lambda)}$, il existe un sous-ensemble fini Λ_1 de Λ tel que $a_\lambda = b_\lambda = 0_A$ pour tout $\lambda \in \Lambda\backslash\Lambda_1$. En outre, $\sum_{\lambda\in\Lambda_1} (a_\lambda - b_\lambda)u_\lambda = 0_M$. Comme $\{u_\lambda \mid \lambda \in \Lambda_1\}$ est une famille finie libre, on a $a_\lambda - b_\lambda = 0_A$, c'est-à-dire, $a_\lambda = b_\lambda$, pour tout $\lambda \in \Lambda_1$. Ainsi $(a_\lambda)_{\lambda\in\Lambda} = (b_\lambda)_{\lambda\in\Lambda}$. Ceci montre l'unicité. Enfin, on a vu que $M = \sum_{\lambda\in\Lambda} Au_\lambda$. Soit $(v_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} Au_\lambda$ tel que $\sum_{\lambda\in\Lambda} v_\lambda = 0_M$. Posons $v_\lambda = a_\lambda u_\lambda$ avec $a_\lambda \in A$. Il existe un sous-ensemble fini Λ_0 de Λ tel que $v_\lambda = 0_M$, pour tout $\lambda \in \Lambda\backslash\Lambda_0$. Alors $0_M = \sum_{\lambda\in\Lambda_0} a_\lambda u_\lambda$. Comme $\{u_\lambda \mid \lambda \in \Lambda_0\}$ est finie et libre, on a $a_\lambda = 0_A$ et donc $v_\lambda = a_\lambda u_\lambda = 0_M$, pour tout $\lambda \in \Lambda_0$. D'après le théorème 2.5.4, la somme $\sum_{\lambda\in\Lambda} Au_\lambda$ est directe. Ceci achève la démonstration.

2.5.6. Proposition. Si $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille non vide de A-modules à gauche, alors $\amalg_{\lambda\in\Lambda} M_\lambda = \oplus_{\lambda\in\Lambda} q_\lambda(M_\lambda)$, où q_λ est l'injection de M_λ dans le co-produit.

Démonstration. Posons $M = \amalg_{\lambda\in\Lambda} M_\lambda$. Comme $q_\lambda : M_\lambda \to M$ est A-linéaire, $q_\lambda(M_\lambda)$ est un sous-module de M. Ainsi $\sum_{\lambda\in\Lambda} q_\lambda(M_\lambda) \subseteq M$. D'autre part, si $u = (u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$, alors $\Lambda_0 = \{\lambda \in \Lambda \mid u_\lambda \neq 0_{M_\lambda}\}$ est fini. Remarquons que $u = \sum_{\lambda\in\Lambda_0} q_\lambda(u_\lambda) \in \sum_{\lambda\in\Lambda} q_\lambda(M_\lambda)$. C'est-à-dire, $M \subseteq \sum_{\lambda\in\Lambda} q_\lambda(M_\lambda)$. D'où, $M = \sum_{\lambda\in\Lambda} q_\lambda(M_\lambda)$.

Enfin, on se fixe $\lambda_0 \in \Lambda$. On voit aisément que $N = \{(u_\lambda)_{\lambda\in\Lambda} \in M \mid u_{\lambda_0} = 0_{M_{\lambda_0}}\}$ est un

sous-module de M. Comme $q_\mu(M_\mu) \subseteq N$ pour tout $\mu \neq \lambda_0$, on a $\sum_{\mu\in\Lambda\setminus\{\lambda_0\}} q_\mu(M_\mu) \subseteq N$. Soit $u = (u_\lambda)_{\lambda\in\Lambda} \in q_{\lambda_0}(M_{\lambda_0}) \cap \sum_{\mu\in\Lambda\setminus\{\lambda_0\}} q_\mu(M_\mu)$. Comme $u \in q_{\lambda_0}(M_{\lambda_0})$, on a $u_\lambda = 0_{M_\lambda}$ pour tout $\lambda \neq \lambda_0$. Comme $u \in N$, on a $u_{\lambda_0} = 0_{M_{\lambda_0}}$. D'où $u = 0_M$. D'après le théorème 2.5.4(4), $M = \oplus_{\lambda\in\Lambda} q_\lambda(M_\lambda)$. Ceci achève la démonstration.

Remarque. Comme q_λ est injective, on voit que $M_\lambda \cong q_\lambda(M_\lambda)$ pour tout $\lambda \in \Lambda$.

Exemple. Considérons un co-produit $M \amalg M$ avec deux injections $q_1, q_2 : M \to M \amalg M$. On a $q_1(M) = (M, 0_M) \cong M$ et $q_2(M) = (0_M, M) \cong M$ tels que $M \amalg M = (M, 0_M) \oplus (0_M, M)$.

2.5.7. Proposition. Soit $M = \oplus_{\lambda\in\Lambda} M_\lambda$, où $\{M_\lambda \mid \lambda \in \Lambda\}$ est une famille de sous-modules de M. Si $N = \sum_{\lambda\in\Lambda} N_\lambda$ avec N_λ un sous-module de M_λ, alors $N = \oplus_{\lambda\in\Lambda} N_\lambda$ et $M/N \cong \amalg_{\lambda\in\Lambda} M_\lambda/N_\lambda$.

Démonstration. D'abord, pour tout $\lambda \in \Lambda$, on a

$$N_\lambda \cap \sum\nolimits_{\mu\in\Lambda\setminus\{\lambda\}} N_\mu \subseteq M_\lambda \cap \sum\nolimits_{\mu\in\Lambda\setminus\{\lambda\}} M_\mu = \{0_M\}.$$

Ainsi $N = \oplus_{\lambda\in\Lambda} N_\lambda$. Or tout $u \in M$ s'exprime d'une façon unique $u = \sum_{\lambda\in\Lambda} u_\lambda$ avec $(u_\lambda)_{\lambda\in\Lambda} \in \amalg_{\lambda\in\Lambda} M_\lambda$. Définissions

$$f : M \to \amalg_{\lambda\in\Lambda} M_\lambda/N_\lambda : \sum\nolimits_{\lambda\in\Lambda} u_\lambda \mapsto (u_\lambda + N_\lambda)_{\lambda\in\Lambda},$$

qui est clairement A-linéaire et surjective. Pour tout $u = \sum_{\lambda\in\Lambda} u_\lambda \in M$, on a $u \in \mathrm{Ker} f$ si et seulement si $u_\lambda + N_\lambda = 0_M + N_\lambda$, pour tout $\lambda \in \Lambda$ si et seulement si $u_\lambda \in N_\lambda$, pour tout $\lambda \in \Lambda$, si et seulement si $u \in N$. Ainsi $\mathrm{Ker} f = N$. D'après le corollaire 2.2.2(2), on a $\amalg_{\lambda\in\Lambda} M_\lambda/N_\lambda \cong M/\mathrm{Ker} f = M/N$. Ceci achève la démonstration.

2.5.8. Définition. Un sous-module N de M s'appelle *facteur direct* s'il existe un sous-module L tel que $M = N \oplus L$.

Remarque. Si $M = N \oplus L$, alors $L \cong M/N$ et $N \cong M/L$.

Exemple. (1) $\{0_M\}$ et M sont des facteurs directs de M puisque $M = M \oplus \{0_M\}$.

(2) Le $\mathbb{Z}$-module $2\mathbb{Z}$ n'est pas un facteur direct de $\mathbb{Z}$. En effet, si $n \in \mathbb{Z}$ est tel que $\mathbb{Z} = 2\mathbb{Z} \oplus n\mathbb{Z}$, alors $n \neq 0$. Ainsi $0 \neq 2n \in 2\mathbb{Z} \cap n\mathbb{Z}$, une contradiction.

2.5.9. Proposition. Soit D un corps-gauche. Si M est un D-espace vectoriel à gauche, alors tout sous-espace vectoriel N de M est un facteur direct de M.

Démonstration. Prenons une base $\mathcal{B} = \{u_\lambda \mid \lambda \in \Lambda\}$ de N. D'après le théorème 1.3.10, $\mathcal{B}$ est contenue dans une base $\mathcal{C} = \{u_\lambda \mid \lambda \in \Sigma\}$ de M, où $\Lambda \subseteq \Sigma$. Posons $\Lambda' = \Sigma \backslash \Lambda$, $\mathcal{B}' = \{u_\lambda \mid \lambda \in \Lambda'\}$, et $L =< \mathcal{B}' >$. Alors $M =< \mathcal{B} \cup \mathcal{B}' >=< \mathcal{B} > + < \mathcal{B}' >= N + L$. Si $u + v = 0_M$, où $u \in N$ et $v \in L$, alors $u = a_1 u_{\lambda_1} + \cdots + a_r u_{\lambda_r}$, où $a_i \in D$ et les λ_i sont des indices distincts de Λ, et $v = b_1 u_{\mu_1} + \cdots + b_s u_{\mu_s}$, où $b_j \in D$ et les μ_j sont des indices distincts de Λ'. Ceci donne $a_1 u_{\lambda_1} + \cdots + a_r u_{\lambda_r} + b_1 u_{\mu_1} + \cdots + b_s u_{\mu_s} = 0_M$, où les indices λ_i, μ_j sont deux à deux distincts. Comme $\mathcal{C}$ est libre, on a $a_i = b_j = 0_D$, pour tous $1 \leq i \leq r$ et $1 \leq j \leq s$. Par conséquent, $u = 0_M$ et $v = 0_M$. D'où $M = N \oplus L$. Ceci achève la démonstration.

2.5.10. Définition. Soit M un A-module non nul. On dit que M est *indécomposable* si $\{0_M\}$ et M sont les seuls facteurs directs de M, c'est-à-dire, toute égalité $M = N \oplus L$ entraîne que $N = 0$ ou $L = 0$; et *décomposable* sinon.

Remarque. Si $M \cong N$, alors M est indécomposable si et seulement si N l'est.

Exemple. (1) Tout module simple est indécomposable.

(2) Un espace vectoriel sur un corps est indécomposable si et seulement s'il est de dimension un.

(3) Le $\mathbb{Z}$-module $\mathbb{Z}$ est indécomposable. En effet, si $\mathbb{Z} = N \oplus L$, alors $N = p\mathbb{Z}$ et $L = q\mathbb{Z}$. Comme $pq \in N \cap L$, on a $pq = 0$. Donc $p = 0$ ou $q = 0$. C'est-à-dire, $N = 0$ ou $L = 0$.

2.5.11. Lemme. Si M est non nul, alors M est indécomposable si et seulement si tout isomorphisme $M \cong N \amalg L$ entraîne que $N = 0$ ou $L = 0$.

Démonstration. Supposons que M est indécomposable. Si $M \cong N \amalg L$, alors $N \amalg L$ est indécomposable. Comme $N \amalg N = (N, 0_L) \oplus (0_N, L)$, on a $(N, 0_L) = \{(0_N, 0_L)\}$ ou $(0_N, L) = \{(0_N, 0_L)\}$. D'où $N = \{0_N\}$ ou $L = \{0_L\}$. Réciproquement, si M est décomposable, alors $M = N \oplus L$ avec N, L des sous-modules de M. Or $M \cong N \amalg L$ avec N, L tous non nuls. Ceci achève la démonstration.

Un élément e d'un anneau est dit *idempotent* si $e^2 = e$. Par exemple, 0_A et 1_A sont tous idempotents.

2.5.12. Théroème. Si M est un A-module à gauche non nul, alors M est indécomposable si et seulement si l'anneau $\mathrm{End}_A(M)$ n'a que deux idempotents $\mathbf{0}$ et $\mathbb{1}_M$.

Démonstration. Supposons que $f \in \mathrm{End}_A(M)$ est un idempotent avec $f \neq 0$ et $f \neq \mathbb{1}$. Alors $f(M)$ et $(\mathbb{1} - f)(M)$ sont deux sous-modules non nuls de M. Pour tout $u \in M$, on a $u = f(u) + (u - f(u) = f(u) + (\mathbb{1} - f)(u)$. D'où $M = f(M) + (\mathbb{1} - f)(M)$. Si $u \in f(M) \cap (\mathbb{1} - f)(M)$, alors $u = f(u) = (\mathbb{1} - f)(w)$ avec $v, w \in M$. Or

$$u = f^2(u) = f((\mathbb{1} - f)(u)) = (f(\mathbb{1} - f))(u) = \mathbf{0}(u) = 0_M.$$

Ainsi $M = f(M) \oplus (\mathbb{1} - f)(M)$. C'est-à-dire, M est décomposable.

Supposons que $M = L \oplus N$ avec L, N deux sous-modules non nuls de M. Comme tout $u \in M$ s'écrit uniquement $u = v + w$ avec $v \in L$ et $w \in N$. On a une application

$$f : M \to M : v + w \mapsto v,$$

ce qui est évidemment A-linéaire. Par hypothèse, il existe des éléments non nuls $v_0 \in L$ et $w_0 \in N$. Par définition, $f(v_0) = f(v_0 + 0_M) = v_0$ et $f(w_0) = f(0_M + w_0) = 0_M$. D'où $f \neq \mathbf{0}$ et $f \neq \mathbb{1}$. Pour tout $u = v + w \in M$ avec $v \in L$ et $w \in N$, on a $f^2(u) = f(v) = f(v + 0_M) = v = f(u)$. D'où $f^2 = f$. Ceci achève la démonstration.

2.6. Modules libres

Partout dans cette section, on se fixe A un anneau non trivial.

2.6.1. Définition. Un A-module à gauche L est dit *libre* s'il admet une base.

Remarque. Soit $f : L \to L'$ un isomorphisme de A-modules à gauche. Si L est libre, alors L' l'est aussi. En effet, si $\mathcal{B}$ est une base de L, alors $f(\mathcal{B})$ est une base de L'.

Exemple. (1) Le A-module nul est libre.

(2) Si A est un corps-gauche, alors tout A-module à gauche est libre.

(3) Pour tout $n > 0$, $A^n = \{(a_1, \ldots, a_n) \mid a_i \in A\}$ est libre. En particulier, ${}_AA$ est libre.

(4) Pour tout entier $n > 0$, le $\mathbb{Z}$-module $\mathbb{Z}_n$ n'est pas libre. Par contre, $\mathbb{Z}_n$ est libre en tant que $\mathbb{Z}_n$-module.

2.6.2. Lemme. Soit L un A-module à gauche non nul. Si $\mathcal{B} = \{u_\lambda \mid \lambda \in \Lambda\}$ est une famille d'éléments de L, alors $\mathcal{B}$ est une base de L si et seulement si tout $u \in L$ s'écrit uniquement $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$.

Démonstration. Supposons que $\mathcal{B}$ est une base de L. Si $u \in L$, alors $u = a_1u_{\lambda_1} + \cdots + a_nu_{\lambda_n}$, où $a_1, \cdots, a_n \in A$ et $\lambda_1, \cdots, \lambda_n \in \Lambda$ sont distincts. Pour tout $\lambda \in \Lambda$, posons $a_\lambda = a_i$ si $\lambda \in \{\lambda_1, \cdots, \lambda_n\}$ et $a_\lambda = 0_A$ sinon. Alors $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$ tel que $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$. Soit $u = \sum_{\lambda\in\Lambda} b_\lambda u_\lambda$ avec $(b_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Alors il existe un sous-ensemble finie Λ_0 de Λ tel que $a_\lambda = b_\lambda = 0_A$, pour tout $\lambda \in \Lambda\backslash\Lambda_0$. Comme $u = \sum_{\lambda\in\Lambda_0} a_\lambda u_\lambda = \sum_{\lambda\in\Lambda_0} b_\lambda u_\lambda$, on a $\sum_{\lambda\in\Lambda_0} (a_\lambda - b_\lambda)u_\lambda = 0_L$. Comme $\{u_\lambda \mid \lambda \in \Lambda_0\}$ est libre, on a $a_\lambda - b_\lambda = 0_A$, c'est-à-dire, $a_\lambda = b_\lambda$, pour tout $\lambda \in \Lambda_0$. Ainsi $(a_\lambda)_{\lambda\in\Lambda} = (b_\lambda)_{\lambda\in\Lambda}$.

Supposons réciproquement que la condition énoncée dans le lemme est vérifiée. Pour tout $u \in L$, il existe $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$ tel que $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$. Or $\Lambda_0 = \{\lambda \in \Lambda \mid u_\lambda \neq 0_A\}$ est fini tel que $u = \sum_{\lambda\in\Lambda_0} a_\lambda u_\lambda$. D'où, $L =< \mathcal{B} >$. Supposons que $a_1u_{\lambda_1} + \cdots + a_nu_{\lambda_n} = 0_L$, où $a_1, \cdots, a_n \in A$ et $\lambda_1, \cdots, \lambda_n \in \Lambda$ sont distincts. Pour tout $\lambda \in \Lambda$, posons $a_\lambda = a_i$ si $\lambda \in \{\lambda_1, \cdots, \lambda_n\}$ et $a_\lambda = 0_A$ sinon. Alors $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$ tel que $0_L = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$. Mais $(0_A)_{\lambda\in\Lambda}$ est aussi tel que $0_L = \sum_{\lambda\in\Lambda} 0_A u_\lambda$. D'après l'unicité, $(a_\lambda)_{\lambda\in\Lambda} = (0_A)_{\lambda\in\Lambda}$. En particulier, $a_i = a_{\lambda_i} = 0_A$, $i = 1, \ldots, n$. Ceci montre que $\mathcal{B}$ est libre, et donc une base de L. La preuve s'achève.

2.6.3. Proposition. Soit L un A-module à gauche libre non nul dont $\mathcal{B}$ est une base. Si M est un A-module à gauche et $\varphi : \mathcal{B} \to M$ est une application, alors il existe une unique application A-linéaire $f : L \to M$ telle que $f(u) = \varphi(u)$, pour tout $u \in \mathcal{B}$.

Démonstration. Posons $\mathcal{B} = \{u_\lambda \mid \lambda \in \Lambda\}$. Supposons que M est un A-module à gauche et $\varphi : \mathcal{B} \to M$ est une application. Notons $v_\lambda = \varphi(u_\lambda) \in M$, pour $\lambda \in \Lambda$. D'après le lemme 2.6.2, tout $u \in E$ s'écrit $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda \in L$ pour un unique $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Comme $(a_\lambda v_\lambda)_{\lambda\in\Lambda}$ est à support fini, on peut définir $f(u) = \sum_{\lambda\in\Lambda} a_\lambda v_\lambda \in M$. Si $a, b \in A$, et $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$ et $v = \sum_{\lambda\in\Lambda} b_\lambda u_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda}, (b_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$, alors $au+bv = \sum_{\lambda\in\Lambda}(aa_\lambda+bb_\lambda)u_\lambda$

avec $(aa_\lambda + bb_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Ainsi

$$f(au+bv) = \sum\nolimits_{\lambda\in\Lambda}(aa_\lambda + bb_\lambda)v_\lambda = a\sum\nolimits_{\lambda\in\Lambda}a_\lambda v_\lambda + b\sum\nolimits_{\lambda\in\Lambda}b_\lambda v_\lambda = af(u) + bf(v).$$

Ceci montre que f est A-linéaire. D'après la définition, $f(u_\lambda) = f(1\cdot u_\lambda) = 1\cdot v_\lambda = \varphi(u_\lambda)$, pour tout $\lambda \in \Lambda$. En outre, supposons que $g : L \to M$ est A-linéaire telle que $f(u_\lambda) = v_\lambda$, pour tout $\lambda \in \Lambda$. Si $u = \sum_{\lambda\in\Lambda} a_\lambda u_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$, alors $g(u_\lambda) = \sum_{\lambda\in\Lambda} g(a_\lambda u_\lambda) = \sum_{\lambda\in\Lambda} a_\lambda v_\lambda = f(u)$. D'où, $g = f$. Ceci achève la démonstration.

Remarque. Soit L un A-module libre de base $\mathcal{B}$. Si $f : L \to L$ est A-linéaire telle que $f(u) = u$ pour tout $u \in \mathcal{B}$, alors $f = \mathbb{1}_L$. En effet, considérons l'inclusions $j : \mathcal{B} \to L$. Alors $f, \mathbb{1}_L : L \to L$ sont toutes A-linéaires telles que $f(u) = j(u) = \mathbb{1}_L(u)$, pour tout $u \in \mathcal{B}$. D'après l'unicité, on a $f = \mathbb{1}_L$.

Par convention, on note A^0 le A-module nul.

2.6.4. Proposition. Soit L un A-module à gauche. Les conditions suivantes sont équivalentes:

(1) L est libre de type fini.

(2) $L \cong A^n$ pour un certain $n \geq 0$.

(3) L admet une base finie.

Démonstration. Si $L = 0$, alors toute les conditions sont vérifiées. Supposons maintenant que $L =< v_1, \ldots, v_m >$ est non nul et admet une base $\mathcal{B}$. Comme chacun des v_i est une combinaison linéaire d'un nombre fini d'éléments de $\mathcal{B}$, il existe $u_1, \ldots, u_n \in \mathcal{B}$, deux à deux distincts, tels que $v_i = a_{i1}u_1 + \cdots + a_{in}u_n$, $a_{ij} \in A$, c'est-à-dire, $v_i \in < u_1, \ldots, u_n >$, $i = 1, \ldots, m$. Ainsi $L =< v_1, \ldots, v_m > \subseteq < u_1, \ldots, u_n > \subseteq < \mathcal{B} >= L$. D'où $L =< u_1, \ldots, u_n >$. Comme $\mathcal{B}$ est libre, on a $\mathcal{B} = \{u_1, \ldots, u_n\}$. Soient $\{e_1, \ldots, e_n\}$ la base canonique de A^n. D'après la proposition 2.6.2, il existe des applications A-linéaires $f : A^n \to L$ et $g : L \to A^n$ telles que $f(e_i) = u_i$ et $g(u_i) = e_i$, $i = 1, \ldots, n$. Or $gf : A^n \to A^n$ est A-linéaire telle que $(fg)(e_i) = e_i$, $i = 1, \ldots, n$. Ainsi $fg = \mathbb{1}_{A^{(n)}}$. De même, $gf = \mathbb{1}_L$. C'est-à-dire, $L \cong A^n$. Ceci montre que (1) implique (2). En outre, on voit aisément que (2) implique (3), et (3) implique (1). La preuve s'achève.

Remarque. Un isomorphisme $A^m \cong A^n$ avec $m, n > 0$ néntraîne pas $m = n$.

2.6.5. Proposition. Si M est un A-module à gauche, alors M est de type fini si et seulement s'il existe une application A-linéaire surjective $g : A^n \to M$, pour un certain $n > 0$.

Démonstration. D'abord, supposons que $M =< u_1, \cdots, u_n >$. Considérons le A-module libre A^n dont $\{e_1, \cdots, e_n\}$ est la base canonique. D'après le théorème 2.6.3, il existe une application A-linéaire $f : A^n \to M$ telle que $f(e_i) = u_i$, $i = 1, \cdots, n$. Pour tout $v \in M$, on a $v = a_1u_1 + \cdots + a_nu_n$, où $a_1, \cdots, a_n \in A$. Or $u = a_1e_1 + \cdots + a_ne_n \in A^n$ est tel que $f(u) = v$. D'où f est surjective.

Réciproquement supposons qu'il existe une application A-linéaire surjective $g : A^n \to M$. Comme g est surjective, $M =< g(e_1), \ldots, g(e_n) >$. Ceci achève la démonstration.

Soit A un anneau commutatif. Une matrice $P \in M_n(A)$ est dite *inversible* s'il existe $Q \in M_n(A)$ telle que $PQ = QP = I_n$, la matrice-identité d'ordre n sur A. Par exemple, considérons les matrices sur $\mathbb{Z}$ suivantes:

$$\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Alors la première matrice est inversible, mais la deuxième ne l'est pas.

2.6.7. Proposition. Soit A un anneau commutatif. Soit L un A-module libre ayant pour base $\{u_1, \ldots, u_n\}$. Si $(v_1, \ldots, v_n) = (u_1, \ldots, u_n)P$ avec P une matrice inversible d'ordre n sur A, alors $\{v_1, \ldots, v_n\}$ est une base de L.

Démonstration. Comme $(u_1, \ldots, u_n) = (v_1, \ldots, v_n)P^{-1}$, chaque u_i est une combinaison linéaire de $v_1, \cdots, v_n$. Ainsi $L =< u_1, \ldots, u_n > \subseteq < v_1, \ldots, v_n > \subseteq L$. Par conséquent, $L =< v_1, \ldots, v_n >$. En outre, supposons que $a_1, \ldots, a_n \in A$ sont tels que

$$0_L = a_1v_1 + \cdots + a_nv_n = (v_1, \ldots, v_n) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (u_1, \ldots, u_n)P \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Comme $\{u_1, \ldots, u_n\}$ est libre, on a

$$P \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0_A \\ \vdots \\ 0_A \end{pmatrix}.$$

Comme P est inversible, on a

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0_A \\ \vdots \\ 0_A \end{pmatrix},$$

c'est-à-dire, $a_i = 0_A$, $i = 1, \ldots, n$. Donc $\{v_1, \ldots, v_n\}$ est libre et ainsi une base de L. Ceci achève la démonstration.

On rappelle que toutes les bases d'un espace vectoriel de dimension finie ont le même nombre de vecteurs. Cette propriété n'est pas valide pour les modules libres sur un anneau général. Mais c'est le cas si l'anneau est intègre.

2.6.8. Lemme. Soit A un anneau intègre. Si L est un A-module libre ayant une base de n éléments, alors toute famille de m éléments de L est liée lorsque $m > n$.

Démonstration. Supposons que $\{u_1, \ldots, u_n\}$ est une base de L et $\{v_1, \ldots, v_m\} \subseteq L$ avec $m > n$. Il suffit de montrer que $\{v_1, \ldots, v_n, v_{n+1}\}$ est liée. C'est évident si un des v_i est nul. Considérons maintenant le cas où $v_i \neq 0_L$, $i = 1, \ldots, n, n+1$. Si $n = 1$, alors $v_1 = a_1 u_1$ et $v_2 = a_2 u_1$, où $a_1, a_2 \in A$. Comme $v_i \neq 0_L$, on a $a_i \neq 0_A$, $i = 1, 2$. Or $a_2 v_1 - a_1 v_2 = (a_2 a_1)u_1 - (a_1 a_2)u_1 = 0_L$, puisque A est commutatif. D'où, $\{v_1, v_2\}$ est liée. Supposons que $n > 1$ et l'énoncé est vrai pour les modules libres ayant une base de $n-1$ éléments. Posons $M =< u_1, \ldots, u_{n-1} >$, qui a pour base $\{u_1, \ldots, u_{n-1}\}$. Si $\{v_1, \ldots, v_{n+1}\} \subseteq M$, alors $\{v_1, \ldots, v_{n+1}\}$ est liée par l'hypothèse de récurrence. Sinon, on peut supposer que $v_{n+1} \notin M$. Comme $\{u_1, \ldots, u_n\}$ est une base de L, on a $L = Au_1 \oplus Au_2 \oplus \cdots \oplus Au_n = M \oplus Au_n$. Ainsi $L/M \cong Au_n \cong_A A$. Comme A est intègre, ${}_AA$ est sans torsion, et donc L/M est sans torsion. En particulier, $v_{n+1} + M$ n'est pas de torsion. En outre, L/M admet une base d'un seul élément. Comme l'énoncé est valide pour $n = 1$, $\{v_i + M, v_{n+1} + M\}$ est liée, pour $i = 1, \ldots, n$. Ainsi il existe $a_i, b_i \in A$, non tous nuls, tels que $a_i(v_i + M) + b_i(v_{n+1} + M) = 0 + M$, c'est-à-dire, $a_i v_i + b_i v_{n+1} \in M$, $i = 1, \ldots, n$. Supposons qu'il existe un certain $1 \leq i \leq n$ tel que

$a_i = 0_A$, alors $b_i \neq 0_A$ est tel que $b_i(v_{n+1} + M) = 0 + M$. Cela veut dire que $v_{n+1} + M$ est de torsion, une contradiction. Donc $a_i \neq 0_A$, pour $i = 1, \ldots, n$.

Comme M a une base de $n-1$ éléments, d'après l'hypothèse de récurrence, il existe $c_1, \ldots, c_n \in A$, non tous nuls, tels que $\sum_{i=1}^{n} c_i(a_i v_i + b_i v_{n+1}) = 0_L$, c'est-à-dire,

$$(c_1 a_1)v_1 + \cdots + (c_n a_n)v_n + (\sum\nolimits_{i=1}^{n} c_i b_i)v_{n+1} = 0_L.$$

Comme A est intègre, $c_1 a_1, \ldots, c_n a_n$ ne sont pas tous nuls. Ainsi $\{v_1, \ldots, v_n, v_{n+1}\}$ est liée. Ceci achève la démonstration.

2.6.9. Théorème. Soit A un anneau intègre. Si L est un A-module libre de type fini, alors les bases de L ont le même nombre d'éléments, et ce nombre commun s'appelle le *rang* de L.

Démonstration. Supposons que L est libre de type fini. Si L est nul, alors la famille vide est la seule base de L. Supposons que L est non nul. D'après la proposition 2.6.4, L admet une base finie $\{u_1, \ldots, u_n\}$. Si $\mathcal{B}$ est une base quelconque de L. D'après le lemme 2.6.7, $|\mathcal{B}| \leq n$. De même, si $\mathcal{B} = \{v_1, \ldots, v_m\}$ avec $m \leq n$, alors $n \leq m$. D'où, $m = n$. Ceci achève la démonstration.

Remarque. (1) Si A est un corps et E est un A-espace vectoriel de dimension finie, alors le rang de E est la dimension de E.

(2) Un A-module libre L est de rang 0 si et seulement si $L = 0$.

(3) Soit V un espace vectoriel de dimension infinie sur un corps K. Considérant l'anneau $A = \mathrm{End}_K(V)$, on a ${}_AA \cong {}_AA \amalg {}_AA$.

2.6.10. Lemme. Soit A un anneau intègere. Si $n \geq 0$, alors un A-module libre L est de rang n si et seulement si $L \cong A^n$.

Démonstration. Le résultat est évident si $n = 0$. Supposons que $n > 0$. Alors A^n admet une base canonique $\{e_1, \ldots, e_n\}$. Si $f : A^n \to L$ est un isomorphisme, alors $\{f(e_1), \ldots, f(e_n)\}$ est une base de L. Ainsi L est de rang n. Réciproquement, si L admet une base $\{u_1, \ldots, u_n\}$, alors

$$f : A^n \to L : (a_1, \ldots, a_n) \mapsto a_1 u_1 + \cdots + a_n u_n$$

est un isomorphisme. Ceci achève la démonstration.

En général, un sous-module d'un module libre n'est pas nécessairement libre. Par exemple, soit $A = M_n(K)$ avec $n > 1$ et K un corps. On sait que ${}_AA$ est libre et

$$I = \left\{ \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \mid a_1, \cdots, a_n \in K \right\}$$

est un sous-module de A. En tant que A-modules, on a $I \cong K^{(n)}$ et on sait que $K^{(n)}$ n'est pas libre. En cas où A est principal (c'est-à-dire, A est intègre et tout idéa de A est engendré par un seul élément), on montrera qu'un sous-module d'un A-module libre est libre.

2.6.11. Théorème. Soit A un anneau principal. Si L est un A-module libre de rang n, alors tout sous-module de L est libre de rang plus petit ou égal à n.

Démonstration. Soit N un sous-module de L. Si $N = 0$, alors N est libre de rang zéro. Supposons maintenant que $N \neq 0$. Soit $\{u_1, \ldots, u_n\}$ une base de L. Si $n = 1$, il existe un isomorphisme $f : A \to L$. Alors $I = f^{-1}(N)$ est sous-module de A tel que $N \cong I$. Comme A est principal, $I = Aa$. Or $a \neq 0_A$ car $N \neq 0$. Comme A est intègre, $\{a\}$ est libre et donc une base de I. Par conséquent, N est libre de rang un. Supposons que $n > 1$ et le résultat est valide pour tout A-module libre de rang $n-1$. Remarquons que $M =< u_1, \ldots, u_{n-1} >$ est libre de rang $n-1$ et Au_n est libre de rang un tel que $L = M \oplus Au_n$. Remarquons que $N/(N \cap M) \cong (N+M)/M$, un sous-module de L/M. Étant isomorphe à Au_n, le module L/M est libre de rang un. Ainsi $N/(N \cap M)$ est libre de rang au plus un. Si $N/(N \cap M)$ est nul, alors $N \subseteq M$. Par hypothèse de récurrence, N est libre de rang au plus $n-1$. Sinon, $N/(N \cap M)$ admet une base $\{v_0 + (N \cap M)\}$ avec $v_0 \in N$. Si $N \cap M = 0$, alors $\{v_0\}$ est une base de N. Sinon, comme M est libre de rang $n-1$, d'après l'hypothèse de récurrence, $N \cap M$ admet une base $v_1, \ldots, v_m$ avec $m \leq n-1$. Il reste à montrer que $\{v_0, v_1, \ldots, v_m\}$ est une base de N. Pour tout $u \in N$, on a $u + (N \cap M) = a_0(v_0 + (N \cap M))$ avec $a_0 \in A$, c'est-à-dire, $u - a_0 v_0 \in N \cap M$. Ainsi $u - a_0 v_0 = a_1 v_1 + \cdots + a_m v_m$, $a_i \in A, i = 1, \ldots, m$, et donc $N =< v_0, v_1, \ldots, v_m >$. En outre, si $b_0 v_0 + b_1 v_1 + \cdots + b_m v_m = 0_L$, $b_0, b_1, \ldots, b_m \in A$, alors $b_0 v_0 = -(b_1 v_1 + \cdots + b_m v_m) \in N \cap M$. D'où $b_0(v_0 + (N \cap M)) = 0 + (N \cap M)$. Donc $b_0 = 0_A$. Ceci nous donne $b_1 v_1 + \cdots + b_m v_m = 0_L$. Par conséquent, $b_1 = \cdots = b_m = 0_A$.

Donc $\{v_0, v_1, \ldots, v_m\}$ est libre et donc une base de N. Cela veut dire que N est de rang $m+1 \leq n$. Ceci achève la démonstration.

Remarque. Rappelons que si E est un espace vectoriel de n sur un corps, alors un sous-espace F de E est de dimension n si et seulement si $F = E$. C'est pas le cas pour les modules libres de type fini sur un anneau principal. Par exemple, $\mathbb{Z}$ est un $\mathbb{Z}$-module libre de rang un, et $2\mathbb{Z}$ est un sous-module libre de $\mathbb{Z}$ de rang un, mais $2\mathbb{Z} \neq \mathbb{Z}$.

2.7. Suites exactes

Considérons une suite $M \xrightarrow{f} N \xrightarrow{g} L$ de deux applications A-linéaires de A-modules à gauche. On voit aisément que $gf = 0$ si et seulement si, $\mathrm{Im}f \subseteq \mathrm{Ker}g$. Si $\mathrm{Im}f = \mathrm{Ker}g$, on dit alors que la suite est *exacte.* Plus généralement, on a la notion suivante.

2.7.1. Définition. Soit $n > 1$ un entier. Une suite de n applications A-linéaires

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} M_{n-1} \xrightarrow{f_n} M_n$$

de A-modules à gauche est dite *exacte* si $\mathrm{Ker}f_{i+1} = \mathrm{Im}f_i$ pour tout $1 \leq i < n$. Dans ce cas, $f_{i+1}f_i = 0$, $i = 1, \ldots, n-1$.

Exemple. (1) Considérons l'application $\mathbb{Z}$-linéaire $f : \mathbb{Z} \to \mathbb{Z} : a \mapsto 3a$ et la projection canonique $p : \mathbb{Z} \to \mathbb{Z}_3 : a \mapsto \bar{a}$. La suite $\mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{p} \mathbb{Z}_3$ est exacte.

(2) Considérons l'application $\mathbb{Z}$-linéaire $g : \mathbb{Z}_4 \to \mathbb{Z}_4 : \bar{a} \mapsto \overline{2a}$. La suite suivante est exacte:

$$\mathbb{Z}_4 \xrightarrow{g} \mathbb{Z}_4 \xrightarrow{g} \mathbb{Z}_4 \xrightarrow{g} \cdots \xrightarrow{g} \mathbb{Z}_4 \xrightarrow{g} \mathbb{Z}_4.$$

En effet, $\mathrm{Im}g = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \{\bar{0}, \bar{2}\}$, et $\mathrm{Ker}g = \{\bar{0}, \bar{2}\}$.

2.7.2. Lemme. Soit $f : M \to N$ une application A-linéaire de A-modules à gauche.

(1) f est injective si et seulement si la suite $0 \to M \xrightarrow{f} N$ est exacte.

(2) f est surjective si et seulement si la suite $M \xrightarrow{f} N \to 0$ est exacte.

(3) f est un isomorphisme si et seulement si la suite $0 \to M \xrightarrow{f} N \to 0$ est exacte.

(4) La suite $0 \to \mathrm{Ker}f \xrightarrow{j} M \xrightarrow{f} N \xrightarrow{p} \mathrm{Coker}f \to 0$ est exacte, où j est l'inclusion et p est la projection canonique.

Démonstration. (1) D'abord, $\mathrm{Im}(\mathbf{0}) = \{0_M\}$. Donc $0 \to M \xrightarrow{f} N$ est exacte si et seulement si $\mathrm{Ker}f = \{0_M\}$ si et seulement si f est injective.

(2) On a $\mathrm{Ker}0 = N$. Ainsi $M \xrightarrow{f} N \to 0$ est exacte si et seulement si $\mathrm{Im}f = N$ si et seulement si f est surjective.

(3) La suite $0 \to M \xrightarrow{f} N \to 0$ est exacte si et seulement si les suites $0 \to M \xrightarrow{f} N$ et $M \xrightarrow{f} N \to 0$ sont toutes exactes si et seulement si f est injective et surjective si et seulement si f est un isomorphisme.

(4) Comme j est injective et p est surjective, la suite exacte en $\mathrm{Ker}f$ et en $\mathrm{Coker}f$. Comme $\mathrm{Im}j = \mathrm{Ker}f$ et $\mathrm{Ker}p = \mathrm{Im}f$, la suite est exacte en M et en N. Ceci achève la démonstration.

2.7.3. Définition. Une suite exacte $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ d'applications A-linéaires de A-modules à gauche s'appelle une *suite exacte courte*.

Exemple. (1) Si $g : M \to N$ est surjective, alors $0 \to \mathrm{Ker}g \xrightarrow{j} M \xrightarrow{g} N \to 0$ est une suite exacte courte, où j est inclusion.

(2) Si $f : L \to M$ est injective, alors $0 \to L \xrightarrow{f} M \xrightarrow{p} \mathrm{Coker}f \to 0$ est une suite exacte courte, où p est la projection canonique.

(3) Si L est un sous-module de M, alors $0 \to L \xrightarrow{j} M \xrightarrow{p} M/L \to 0$ est une suite exacte courte, où j est l'inclusion et p est la projection canonique.

2.7.4. Proposition. Soit $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ une suite d'applications A-linéaires de A-modules à gauche. Soient $j : \mathrm{Ker}g \to M$ l'inclusion et $p : M \to \mathrm{Coker}f$ la projection canonique. Les conditions suivantes sont équivalentes:

(1) La suite $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est exacte courte.

(2) f est injective et il existe un isomorphisme $\bar{g} : \mathrm{coker}f \to N$ telle que $g = \bar{g}p$.

(3) g est surjective et il existe un isomorphisme $\tilde{f} : L \to \mathrm{Ker}g$ telle que $f = j\tilde{f}$.

Démonstration. Supposons que (1) est valide. En particulier, f est injective. Ainsi $\tilde{f} : L \to \mathrm{Im}f : u \mapsto f(u)$ est un isomorphisme tel que $f = j\tilde{f}$. Comme $\mathrm{Im}f = \mathrm{Ker}g$, (2) est valide.

En outre, g est surjective. D'après le théorème 2.2.1, il existe un isomorphisme $\bar{g}$: $M/\mathrm{Ker}g \to N$ tel que $g = \bar{g}p$. Comme $\mathrm{Ker}g = \mathrm{Im}f$, on a $M/\mathrm{Ker}g = M/\mathrm{Im}f = \mathrm{Coker}f$. Donc (3) est valide.

Supposons maintenant que (2) est valide. Alors la suite $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est exacte en N. Comme $\tilde{f}$ et j sont toutes injectives, f l'est aussi. Donc la suite est exacte en L. En outre, pour tout $u \in L$, on a $f(u) = (j\tilde{f})(u) = j(\tilde{f}(u)) = \tilde{f}(u) \in \mathrm{Ker}g$. Ainsi $\mathrm{Im}f \subseteq \mathrm{Ker}g$. Réciproquement si $v \in \mathrm{Ker}g$, comme $\tilde{f}$ est surjective, il existe $u \in L$ tel que $v = \tilde{f}(u) = j(\tilde{f}(u)) = f(u) \in \mathrm{Im}f$. Donc $\mathrm{Im}f = \mathrm{Ker}g$, et ainsi la suite est exacte en M. C'est-à-dire, (1) est valide.

Supposons maintenant que (3) est valide. Alors la suite $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est exacte en L. Comme $\bar{g}$ et p sont toutes surjectives, g l'est aussi. Ainsi la suite est exacte en N. Pour tout $u \in L$, on a $(gf)(u) = \bar{g}(p(f(u))) = \bar{g}(f(u) + \mathrm{Im}f) = \bar{g}(0 + \mathrm{Im}f) = 0_N$. Donc $\mathrm{Im}f \subseteq \mathrm{Ker}g$. Réciproquement, si $v \in \mathrm{Ker}g$, alors $0_N = g(v) = \bar{g}(p(v)) = \bar{g}(v + \mathrm{Im}f)$. Comme $\bar{g}$ est injective, on a $v + \mathrm{Im}f = 0 + \mathrm{Im}f$. C'est-à-dire, $v \in \mathrm{Im}f$. Cela veut dire que $\mathrm{Ker}g = \mathrm{Im}f$. Ainsi la suite est exacte en M, et donc (1) est valide. La preuve s'achève.

Soient M_1, M_2 deux A-modules à gauche. On a alors une suite exacte courte

$$0 \longrightarrow M_1 \xrightarrow{q_1} M_1 \amalg M_2 \xrightarrow{p_2} M_2 \longrightarrow 0,$$

où q_1 est l'injection et p_2 est la projection. Remarquons que $M_1 \amalg M_2 = (M_1, 0) \oplus (0, M_2)$ avec $(M_1, 0) = \mathrm{Im}q_1 = \mathrm{Ker}p_2$.

2.7.5. Définition. Une suite exacte courte $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ d'applications A-linéaires de A-modules à gauche est dite *scindée* si $\mathrm{Im}(f)$, ou bien $\mathrm{Ker}(g)$, est un facteur direct de M.

Exemple. Si D est un corps-gauche, alors toute suite exacte courte

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

d'applications D-linéaires de D-espaces vectoriels à gauche est scindée. En effet, $\mathrm{Im}f$ est un sous-espace vectoriel de M. Comme D est un corps-gauche, $\mathrm{Im}f$ est un facteur direct de M.

2.7.6. Proposition. Soit $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ une suite exacte courte d'applications A-linéaires de A-modules à gauche. Si la suite est scindée, alors $M \cong L \amalg N$.

Démonstration. Comme la suite est exacte, on a $L \cong \mathrm{Im}f$ et $N \cong M/\mathrm{Im}f$. Supposons maintenant que $M = \mathrm{Im}f \oplus M'$ avec M' un sous-module de M. Alors $M' \cong M/\mathrm{Im}f \cong N$. Ainsi $M = \mathrm{Im}f \oplus M' \cong \mathrm{Im}f \amalg M' \cong L \amalg N$. Ceci achève la démonstration.

Exemple. Considérons $0 \longrightarrow \mathbb{Z}_2 \xrightarrow{f} \mathbb{Z}_4 \xrightarrow{g} \mathbb{Z}_2 \longrightarrow 0$, où f, g sont définies par $f(\bar{n}) = 2\tilde{n}$ et $g(\tilde{n}) = \bar{n}$, pour tout $n \in \mathbb{Z}$. Il s'agit d'une suite exacte courte, mais non-scindée. En effet, supposons que la suite est scindée, alors $\mathbb{Z}_4 \cong \mathbb{Z}_2 \amalg \mathbb{Z}_2$. Soit $h : \mathbb{Z}_4 \to \mathbb{Z}_2 \amalg \mathbb{Z}_2$ un tel isomorphisme. Alors $h(\tilde{1}) = (\bar{m}, \bar{n})$ avec $m, n \in \mathbb{Z}$. Or $h(\tilde{2}) = 2(\bar{m}, \bar{n}) = (2\bar{m}, 2\bar{n}) = (\bar{0}, \bar{0})$. D'où, h n'est pas injective, une contradiction.

2.7.7. Théorème. Soit une suite exacte courte d'applications A-linéaires de A-modules à gauche:

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0\,.$$

Les conditions suivantes sont équivalentes:

(1) La suite est scindée.

(2) Il existe une application A-linéaire $g' : N \to M$ telle que $gg' = \mathbb{1}_N$.

(3) Il existe une application A-linéaire $f' : M \to L$ telle que $f'f = \mathbb{1}_L$.

Démonstration. Supposons que (1) est valide. Alors il existe un sous-module M' de M tel que $M = \mathrm{Im}f + M' = \mathrm{Ker}g + M'$ et $\mathrm{Ker}g \cap M' = 0$. Pour tout $u \in N$, on prétend qu'il existe un unique $u' \in M'$ tel que $g(u') = u$. En effet, comme g est surjective, il existe $w \in M$ tel que $g(w) = u$. Comme $M = \mathrm{Ker}g + M'$, on a $w = w_0 + u'$ avec $w_0 \in \mathrm{Ker}g$ et $u' \in M'$. Or $u = g(w) = g(w_0) + g(u') = g(u')$. Si $u'' \in M'$ tel que $g(u'') = u$, alors $g(u' - u'') = 0_N$. D'où $u' - u'' \in M' \cap \mathrm{Ker}g = \{0_M\}$, et donc $u' = u''$. Ceci montre que l'application $g' : N \to M : u \mapsto u'$ est bien définie, où $u' \in g^-(u) \cap M'$. Si $u, v \in N$ et $a, b \in A$, alors $u = g(u')$ et $v = g(v')$ avec $u', v' \in M'$. Or $au' + bv' \in M'$ tel que $g(au' + bv') = au + bv$. Donc $g'(au + bv) = au' + bv' = ag'(u) + bg'(v)$. Ainsi g' est A-linéaire. Or pour tout $u \in N$, on a $u = g(u') = g(g'(u)) = (gg')(u)$. Donc $gg' = \mathbb{1}_N$, c'est-à-dire, (2) est valide. En outre, pour tout $y \in M$, il existe un unique $y_0 \in \mathrm{Im}f$ et un unique $y_1 \in M'$ tels que $y = y_0 + y_1$. Comme f est injective, il existe un unique $y' \in L$ tel que $f(y') = y_0$.

Ceci nous donne une application bien définie: $f' : M \to L : y \mapsto y'$, où y' est unique tel que $y - f(y') \in M'$. Soient $y, z \in M$ et $a, b \in A$. Posons $y' = f'(y)$ et $f'(z) = z'$. Alors $y - f(y'), z - f(z') \in M'$. Comme $(ay + bz) - f(ay' + bz') = a(y - f(y')) + b(z - f(z')) \in M'$, on a $f'(ay + bz) = ay' + bz' = af'(y) + bf'(z)$. Ceci montre que f' est A-linéaire. Pour tout $y' \in L$, posons $y = f(y') \in M$. Comme $y - f(y') = 0_M \in M'$, on a $f'(y) = y'$. D'où $(f'f)(y') = f'(y) = y'$. C'est-à-dire, $f'f = \mathbb{1}_L$. Ceci montre que (3) est valide.

Supposons maintenant qu'il existe une application A-linéaire $g' : N \to M$ telle que $gg' = \mathbb{1}_N$. On montrera $M = \mathrm{Im}f \oplus \mathrm{Im}g'$. En effet, pour tout $v \in M$, on a

$$g(v) = (gg')(g(v)) = g((g'(g(v))),$$

c'est-à-dire, $g(v - g'(g(v))) = 0_M$. D'où $v' = v - g'(g(v)) \in \mathrm{Ker}g = \mathrm{Im}f$. Ainsi $v = v' + g'(g(v)) \in \mathrm{Im}f + \mathrm{Im}g'$. Par conséquent, $M = \mathrm{Im}f + \mathrm{Im}g'$. En outre, si $v \in \mathrm{Im}f \cap \mathrm{Im}g' = \mathrm{Ker}g \cap \mathrm{Im}g'$, alors $g(v) = 0_N$ et $v = g'(u)$ avec $u \in N$. Donc $u = (gg')(u) = g(g'(u)) = g(v) = 0_N$. Par conséquent, $v = g'(u) = 0_M$. Donc $\mathrm{Im}f \cap \mathrm{Im}g' = \{0_M\}$. D'où (1) est valide.

Supposons enfin qu'il existe une application A-linéaire $f' : M \to L$ telle que $f'f = \mathbb{1}_L$. On montrera que $M = \mathrm{Ker}(g) \oplus \mathrm{Ker}(f')$. Pour tout $v \in M$, on a $f'(v) = (f'f)(f'(v))) = f'(f(f'(v)))$, c'est-à-dire, $f'(v - f(f'(w))) = 0_L$. D'où $v' = v - f(f'(v)) \in \mathrm{Ker}f'$, et donc $v = f(f'(v)) + v' \in \mathrm{Im}f + \mathrm{Ker}f' = \mathrm{Ker}g + \mathrm{Ker}f'$. Par conséquent, $M = \mathrm{Ker}g + \mathrm{Ker}f'$. Si $v \in \mathrm{Ker}g \cap \mathrm{Ker}f' = \mathrm{Im}f \cap \mathrm{Ker}f'$, alors $f'(v) = 0_L$ et $v = f(w)$ avec $w \in L$. Or $w = f'(f(w)) = f'(v) = 0_L$, et ainsi $v = f(w) = 0_M$. Donc $\mathrm{Ker}g \cap \mathrm{Ker}f' = 0$. D'où $M = \mathrm{Ker}g \oplus \mathrm{Ker}f'$. Ceci montre que (1) est valide. La preuve s'achève.

2.7.8. Proposition. Soit $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} L \longrightarrow 0$ une suite exacte courte d'applications linéaires de A-modules à gauche. Si L est libre, alors la suite est scindée.

Démonstration. Supposons que L admet une base $\mathcal{B} = \{u_\lambda \mid \lambda \in \Lambda\}$. Pour tout $\lambda \in \Lambda$, comme g est surjective, $u_\lambda = g(v_\lambda)$ avec $v_\lambda \in N$. Considérons l'application $\varphi : \mathcal{B} \to N : u_\lambda \mapsto v_\lambda$. D'après la proposition 2.6.2, il existe une application A-linéaire $g' : L \to N$ telle que $g'(u_\lambda) = v_\lambda$. Or $gg' : L \to L$ est A-linéaire telle que $(gg')(u_\lambda) = g(g'(u_\lambda)) = g(v_\lambda) = u_\lambda$, pour tout $\lambda \in \Lambda$. Ainsi $gg' = \mathbb{1}_L$, et donc la suite est scindée. Ceci achève la démonstration.

2.8. Exercices

1. Considérer l'application $f : \mathbb{Z}^3 \to \mathbb{Z}^3 : (a, b, c) \mapsto (a-b+2c, 5b+c, 3a+b+2c)$. Montrer que f est $\mathbb{Z}$-linéaire, et calculer son noyau et son image.

2. Considérer les $\mathbb{R}[x]$-modules $\mathbb{R}^{(3)}$ et $\mathbb{R}^{(2)}$ définis respectivement par les applications $\mathbb{R}$-linéaires $f : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)} : u \mapsto Pu$ et $g : \mathbb{R}^{(2)} \to \mathbb{R}^{(2)} : v \mapsto Qv$, où

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

   Trouver les applications $\mathbb{R}[x]$-linéaires $h : \mathbb{R}^{(3)} \to \mathbb{R}^{(2)}$.

3. Considérer les modules ${}_{\mathbb{Z}}\mathbb{Q}$ et ${}_{\mathbb{Q}}\mathbb{Q}$.
   (1) Montrer qu'une application $f : \mathbb{Q} \to \mathbb{Q}$ est $\mathbb{Q}$-linéaire si et seulement si f est $\mathbb{Z}$-linéaire.
   (2) Montrer que $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ en tant qu'anneaux. *Indication*: Considérer l'application $\phi : \mathrm{End}_{\mathbb{Z}}(\mathbb{Q}) \to \mathbb{Q} : f \mapsto f(1)$.

4. Si n est un entier positif, montrer que $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n) \cong \mathbb{Z}_n$ en tant qu'anneaux. *Indication*: Considérer l'application $\phi : \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_n) \to \mathbb{Z}_n : f \mapsto f(\bar{1})$.

5. Si M et N sont des A-modules à gauche isomorphes, montrer que $\mathrm{End}_A(M) \cong \mathrm{End}_A(N)$ en tant qu'anneaux. *Indication*: Si $\varphi : M \to N$ est un isomorphisme A-linéaire, considérer l'application $\psi : \mathrm{End}_A(M) \to \mathrm{End}_A(N) : f \mapsto \varphi f \varphi^{-1}$.

6. Soit A un anneau intègre. Soit $f : M \to N$ une application A-linéaires de A-modules.
   (1) Montrer que $f(\mathcal{T}(M)) \subseteq \mathcal{T}(N)$.
   (2) Si M est de torsion, montrer que $\mathrm{Im}f \subseteq \mathcal{T}(N)$.
   (3) Si N est sans torsion, montrer que $\mathcal{T}(M) \subseteq \mathrm{Ker}f$.
   (4) Si M est de torsion et N est sans torsion, montrer que $f = 0$.

7. Soit $f : M \to N$ une application A-linéaire de A-modules à gauche.
   (1) Si f est injective, montrer que $\mathrm{ann}(N) \subseteq \mathrm{ann}(M)$.
   (2) Si f est surjective, montrer que $\mathrm{ann}(M) \subseteq \mathrm{ann}(N)$.

(3) Si f est un isomorphisme, montrer que $\mathrm{ann}(M) = \mathrm{ann}(N)$.

8. Soient I, J deux idéaux bilatères d'un anneau A. Si $A/I \cong A/J$ en tant que A-modules à gauche, montrer que $I = J$. *Indication*: Utiliser la partie (3) du numéro 5 et le dernier numéro des Exercices 1.5.

9. Soit K un corps. Si $p(x), q(x)$ sont deux polynômes distincts irréductibles et normalisés (c'est-à-dire, le coefficient directeur est 1) sur K, montrer que toute application $K[x]$-linéaire $f : K[x]/<p(x)> \to K[x]/<q(x)>$ est nulle. *Indication*: Utiliser le numéro précédant.

10. Trouver les sous-modules du $\mathbb{R}[x]$-module $\mathbb{R}[x]/<x^3 - 3x - 2>$.

11. Soit M un module à gauche sur un anneau A. Soient N, N', L, L' des sous-modules de M tels que $N \subseteq L$ et $N' \subseteq L'$. Montrer que

$$\frac{(L \cap L') + N}{(L \cap N') + N} \cong \frac{L \cap L'}{(N \cap L') + (L \cap N')} \cong \frac{(L \cap L') + N'}{(N \cap L') + N'}.$$

Indication: Construire une application linéaire $L \cap L' \to ((L \cap L') + N) \,/\, ((L \cap N') + N)$.

12. Soit E un espace vectoriel sur un corps K, vu comme un $K[x]$-module défini par le K-endomorphisme $\mu \mathbb{1}_E$ avec $\mu \in K$. Si ${}_K E$ est de dimension un, montrer que ${}_{K[x]}E \cong K[x]/<x - \mu>$.

13. Soient A un anneau intègre et a un élément non nul de A. Montrer les énoncés suivants.

(1) Le A-module régulier ${}_A A$ admet une suite décroissante de sous-modules:

$$A \supseteq Aa \supseteq Aa^2 \supseteq \cdots \supseteq Aa^{n-1} \supseteq Aa^n \supseteq \cdots .$$

(2) Pour tout entier $n \geq 1$, on a $Aa^{n-1}/Aa^n \cong A/Aa$.

14. Soient M un A-module à gauche et N un sous-module de M.

(1) Si L est un sous-module de M contenant N, alors L est un sous-module maximal de M si et seulement si L/N est un sous-module maximal de M/N.

(2) Si M/N est non nul et cyclique, alors N est contenu dans un sous-module maximal de M.

15. Pour tout $\lambda \in \mathbb{C}$, poser $S_\lambda = \mathbb{C}[x]/<x-\lambda>$.

    (1) Montrer qu'un $\mathbb{C}[x]$-module S est simple si et seulement si $S \cong S_\lambda$ pour un certain $\lambda \in \mathbb{C}$.

    (2) Montrer, pour tous $\lambda, \mu \in \mathbb{C}$, que $S_\lambda \cong S_\mu$ si, et seulement si, $\lambda = \mu$. *Indication*: Utiliser le numéro 7.

16. Si S est un $\mathbb{Z}$-module simple, montrer que $\mathrm{End}_{\mathbb{Z}}(S)$ est un corps.

17. Soit K un corps. Considérer le $K[x]$-module simple $S = K[x]/<p(x)>$, où $p(x)$ est un polynôme irréductible de $K[x]$. Vérifier que $\mathrm{End}_{K[x]}(S) \cong K[x]/<p(x)>$ en tant qu'anneaux. *Indication*: Considérer l'application suivante:

$$\varphi : \mathrm{End}_{K[x]}(S) \to K[x]/<p(x)> : f \mapsto f(\bar{1}).$$

18. Si p est un entier positif, montrer que l'application

$$f : \mathbb{Z} \to \prod_{n=1}^{\infty} \mathbb{Z}_{p^n} : a \mapsto (a + p\,\mathbb{Z}, a + p^2\mathbb{Z}, \cdots, a + p^n\mathbb{Z}, \cdots)$$

    est $\mathbb{Z}$-linéaire, injective, et non surjective. *Indication*: Pour la dernière partie, considérer l'élément $(a_1 + p\,\mathbb{Z}, a_2 + p^2\mathbb{Z}, \cdots, a_n + p^n\mathbb{Z}, \cdots,)$, où $a_n = p^{n-1}$.

19. Soit $\{M_\lambda \mid \lambda \in \Lambda\}$ une famille non vide de A-modules à gauche. Montrer que $\amalg_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$ si et seulement si l'ensemble $\{\lambda \in \Lambda \mid M_\lambda \neq 0\}$ est fini.

20. Soient A un anneau intègre et M un A-module. Si $M_1, \cdots, M_n$ sont des sous-modules de M tels que $M = M_1 \oplus \cdots \oplus M_n$, montrer que $\mathcal{T}(M) = \mathcal{T}(M_1) \oplus \cdots \oplus \mathcal{T}(M_n)$ et

$$\frac{M}{\mathcal{T}(T)} \cong \frac{M_1}{\mathcal{T}(M_1)} \amalg \cdots \amalg \frac{M_n}{\mathcal{T}(M_n)}.$$

21. Soit E un espace vectoriel sur un corps K de base $\mathcal{B} = \{u_\lambda \mid \lambda \in \Lambda\}$. Si $\mu \in K$, montrer que le $K[x]$-module E défini par l'endomoprhisme $\mu\mathbb{1}_E$ est isomorphe à $S^{(\Lambda)}$, où $S = K[x]/<x-\mu>$.

22. Soit I un idéal à gauche de A. Montrer que I est un facteur direct ${}_AA$ si et seulement si $I = Ae$ avec e un idempotent.

23. Montrer que le $\mathbb{Z}$-module $\mathbb{Q}$ est indécomposable. *Indication*: Utiliser la partie (2) du numéro 3 et le théorème 2.5.12.

24. Soit A un anneau non nul. Soient L, M deux A-modules à gauche libres de bases $\mathcal{U}$ et $\mathcal{V}$ respectivement. S'il existe une bijection $\phi : \mathcal{U} \to \mathcal{V}$, montrer que $L \cong M$.

25. Montrer que tout sous-module du $\mathbb{Z}$-module $\mathbb{Z}$ est libre.

26. Soit A un anneau fini et I un idéal à gauche de A. Montrer que I, en tant que sous-module du A-module ${}_AA$, est libre si et seulement si $I = 0$ ou $I = A$. *Indication*: Utiliser la proposition 2.6.4.

27. Montrer que le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas libre. *Indication*: tout couple de deux nombres rationnels est lié sur $\mathbb{Z}$.

28. Soit A un anneau non trivial. Si I est un idéal bilatère de A, montrer que A/I est libre en tant que A-module à gauche si et seulement si $I = 0$ ou $I = A$. *Indication*: A/I est annulé par I.

29. Soit E un $K[x]$-module avec K un corps. Si ${}_KE$ est de dimension finie, montrer que ${}_{K[x]}E$ n'est pas libre.

30. Soient $a, b > 1$ des entiers co-premiers. Montrer que le $\mathbb{Z}$-module $\mathbb{Z}$ est engendré par a et b, mais que l'ensemble $\{a, b\}$ ne contient pas de base de $\mathbb{Z}$. Ainsi, contrairement à ce qui se passe pour les espaces vectoriels, un ensemble générateur d'un module libre de type fini ne contient pas nécessairement de base.

31. Soit A un anneau commutatif non trivial.
    (1) Montrer qu'un idéal I de A est principal (c'est-à-dire, engendré par un seul élément) lorsque I est libre en tant que A-module.
    (2) Si tout sous-module du A-module régulier ${}_AA$ est libre, montrer que A est un anneau principal. *Attention*: Il faut montrer que A est intègre.

32. Soit $n = ab$ avec a, b des nombres positifs. Montrer que l'on a une suite exacte courte a'applications $\mathbb{Z}$-linéaires de $\mathbb{Z}$-modules comme suit:

$$0 \longrightarrow a\mathbb{Z}_n \xrightarrow{j} \mathbb{Z}_n \xrightarrow{g} b\mathbb{Z}_n \longrightarrow 0,$$

où j est l'inclusion et g est la multiplication par b.

33. Soit K un corps. Si l'on a une suite exacte courte de K-espaces vectoriels de dimension finie

$$0 \longrightarrow F \xrightarrow{f} E \xrightarrow{g} G \longrightarrow 0,$$

montrer que $\dim(E) = \dim(F) + \dim(G)$.

34. Soient A un anneau principal et M un A-module. Si M est de type fini, montrer qu'il existe une suite exacte courte

$$0 \to L_1 \xrightarrow{f} L_0 \xrightarrow{g} M \to 0$$

d'applications linéaires de A-modules avec L_0, L_1 libres de type fini.

35. Soit $L \xrightarrow{f} M \xrightarrow{g} N$ une suite d'applications A-linéaires de A-modules à gauche. Montrer que la suite $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N$ est exacte si et seulement si $gf = 0$, et pour toute application A-linéaire $h : P \to M$ telle que $gh = 0$, il existe une unique application A-linéaire $h' : P \to L$ telle que $h = fh'$.

36. Soit $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ une suite exacte courte d'applications A-linéaires de A-modules à gauche. Montrer que la suite est scindée si, et seulement si, il existes des applications A-linéaires $f' : M \to L$ et $g' : N \to M$ telles que $ff' + g'g = \mathbb{1}_M$.

37. Soit un diagramme commutatif à lignes exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \longrightarrow & 0 \end{array}$$

d'applications A-linéaires de A-modules à gauche. Montrer que

$$0 \longrightarrow M \amalg L' \xrightarrow{\phi} M \amalg M' \xrightarrow{\psi} N' \longrightarrow 0$$

est une suite exacte courte, où $\phi(u, u') = (u, \beta(u) + f'(u'))$ et $\psi(v, v') = \gamma(g(v)) - g'(v')$.

38. Soient I, J des idéaux à gauche d'un anneau A. Si $A = I + J$, montrer que

$$I \amalg J \cong A \amalg (I \cap J).$$

Indication: Construire une suite exacte courte $0 \to I \cap J \to I \amalg J \to A \to 0$.

39. Soient M un module à gauche sur un anneau A et N un sous-module de M. Si $M/N \cong {}_AA$, montrer que $M = N \oplus Au$ pour un certain $u \in M$.

Chapitre 3: Modules de type fini sur un anneau euclidien

Partout dans ce chapitre, on se fixe A un anneau euclidien. C'est-à-dire, A est un anneau intègre muni d'une valuation $\varphi : A^* \to \mathbb{N}$, où $A^* = A\backslash\{0_A\}$, vérifiant les conditions suivantes:

(1) Pour tous $a, b \in A^*$, on a $\varphi(a) \leq \varphi(ab)$.

(2) Si $a \in A$ et $b \in A^*$, alors $a = qb + r$, où $r, q \in A$ tels que $r = 0_A$ ou $\varphi(r) < \varphi(b)$.

On voit que $\varphi(1_A) \leq \varphi(a)$ pour tout $a \in A^*$. Remarquons que $a \in A^*$ est inversible si et seulement si $\varphi(a) = \varphi(1_A)$. Dans ce cas, on dit que a est une *unité*. Soient $a, b \in A$. On dit que a *divise* b, noté $a \mid b$, si $b = aq$ avec $q \in A$, ou bien $(b) \subseteq (a)$. Pour tout $a \in A$, on a $a \mid 0_A$, et de l'autre côté, $0_A \mid a$ si et seulement si $a = 0_A$. En outre, on dit que a, b sont *associés*, noté $a \sim b$, si l'un divise l'autre, c'est-à-dire, $a = bc$ avec c un unité.

Les exemples classiques d'anneaux euclidiens sont $\mathbb{Z}$ et $K[x]$ avec K un corps.

3.1. Modules cycliques

Rappelons que A est toujours principal. En particulier, pour tous $a_1, \cdots, a_n \in A$, on a $(a_1) + \cdots + (a_n) = (d)$ et $(a_1) \cap \cdots \cap (a_n) = (m)$, où $d, m \in A$. Dans ce cas, on dit que d est *le plus grand commun diviseur* et m *le plus petit commun multiple* de $a_1, \ldots, a_n$. Remarquons, pour tout $a \in A$, que le plus grand commun diviseur de $0_A, a$ est a, et le plus petit commun multiple de $0_A, a$ est 0_A.

Comme A est principal, un A-module M est cyclique si et seulement si $M \cong A/(a)$, où $a \in A$. Dans ce cas, $M = 0$ si et seulement si a est inversible.

3.1.1. Proposition. Si $d = bc$ avec $b, c \in A$ co-premiers, alors

$$A/(d) \cong A/(b) \amalg A/(c).$$

Démonstration. Pour tout $y \in A$, on écrit $\bar{y} = y + (b) \in A/(b)$, $\tilde{y} = y + (d) \in A/(d)$ et $\hat{y} = y + (c) \in A/(c)$. Considérons la suite exacte courte

$$0 \longrightarrow A/(b) \xrightarrow{f} A/(d) \xrightarrow{g} A/(c) \longrightarrow 0,$$

où f, g sont définies par $f(\bar{a}) = \widetilde{ac}$ et $g(\tilde{a}) = \hat{a}$, pour tout $a \in A$. Comme b, c sont co-premiers, il existe $u, v \in A$ tels que $1_A = bu + cv$. Or $g' : A/(c) \to A/(d) : \hat{a} \mapsto \widetilde{bua}$ est bien définie et A-linéaire. Pour tout $a \in A$, on a $a = (bu)a + c(va)$. Donc $\hat{a} = \widehat{bua}$. Ceci nous donne $(gg')(\hat{a}) = g(\widetilde{bua}) = \widehat{bua} = \hat{a}$, c'est-à-dire, $gg' = \mathbb{1}$. D'après le théorème 2.7.8, la suite est scindée. D'après la proposition 2.7.7, $A/(d) \cong A/(b) \amalg A/(c)$. Ceci achève la démonstration.

3.1.2. Corollaire. Si $d \sim p_1^{n_1} \cdots p_r^{n_r}$, où les $p_i \in A$ sont premiers deux à deux non associés et les n_i sont des entiers positifs, alors

$$A/(d) \cong A/(p_1^{n_1}) \amalg \cdots \amalg A/(p_r^{n_r}).$$

Démonstration. Par l'hypothèse, $d = up_1^{n_1} \cdots p_r^{n_r}$ avec u une unité. Alors $(d) = (p_1^{n_1} \cdots p_r^{n_r})$. On procède par recurrence sur r. Si $r = 1$, il n'y a rien à prouver. Supposons que $r > 1$ et le résultat est valide pour $r - 1$. Remarquons que $p_1^{n_1} \cdots p_{r-1}^{n_{r-1}}$ et $p_r^{n_r}$ sont co-premiers. D'après la proposition 3.1.1, on a

$$A/(p_1^{n_1} \cdots p_r^{n_r}) \cong A/(p_1^{n_1} \cdots p_{r-1}^{n_{r-1}}) \amalg A/(p_r^{n_r}) \cong A/(p_1^{n_1}) \amalg \cdots \amalg A/(p_{r-1}^{n_{r-1}}) \amalg A/(p_r^{n_r}),$$

où le dernier isomorphisme suit de l'hypothèse de récurrence. Ceci achève la démonstration.

Exemple. $\mathbb{Z}_{180} \cong \mathbb{Z}_4 \amalg \mathbb{Z}_9 \amalg \mathbb{Z}_5$.

3.1.3. Théorème. Si $d \in A$ est non inversible, alors $A/(d)$ est indécomposable si et seulement si $d = 0$ ou $d \sim p^n$ avec $p \in A$ premier et n un entier positif.

Démonstration. Supposons que $A/(d)$ est indécomposable avec d non nul. Comme $A/(d) \neq 0$, on a d n'est pas une unité. D'où $d \sim p_1^{n_1} \cdots p_r^{n_r}$, où les p_i sont des éléments premiers deux à deux non associés de A et les n_i sont des entiers positifs. Ainsi $A/(d) = A/(p_1^{n_1} \cdots p_r^{n_r})$. D'après le corollaire 3.1.2, $r = 1$. Ceci montre la nécessité.

Pour la suffisance, on suppose premièrement que $d = 0$. Alors $A/(d) \cong A$. Si N, L sont des sous-modules non nuls de A, alors $N = (b)$ et $L = (c)$ avec b, c tous non nuls. Comme $0 \neq bc \in N \cap L$, la somme $N + L$ n'est pas directe. En particulier, $A \neq N \oplus L$. Ainsi A est indécomposable.

Supposons maintenant que $d \sim p^n$, où p est un élément premier et $n > 0$. Alors $(d) = (p^n)$. Si N un sous-module non nul de $A/(p^n)$, alors $N = L/(p^n)$, où L est un sous-module de A avec $(p^n) \subset L$. Comme A est principal, $L = (a)$ avec $a \in A$ tel que $a \mid p^n$ et $p^n \not| a$. Comme p est premier, on a $a = p^m$ avec $0 \leq m \leq n-1$. Ainsi $a \mid p^{n-1}$, d'où $(p^{n-1}) \subseteq L$, et donc $(p^{n-1})/(p^n) \subseteq N$. Si N_1 et N_2 sont deux sous-modules non nuls de $A/(p^n)$, alors $(p^{n-1})/(p^n) \subseteq N_1 \cap N_2$, et donc la somme $N_1 + N_2$ ne peut être directe. En particulier, $A/(d) \neq N_1 \oplus N_2$. Ceci montre que $A/(d)$ est indécomposable. La preuve s'achève.

Exemple. (1) Le $\mathbb{Z}$-module $\mathbb{Z}_{64}$ est indécomposable mais $\mathbb{Z}_{100}$ est décomposable.

(2) Le $\mathbb{R}[x]$-module $\mathbb{R}[x]/<(x^2+x+1)^2>$ est indécomposable.

(3) Le $\mathbb{C}[x]$-module $\mathbb{C}[x]/<(x^2+x+1)^2>$ est décomposable.

3.2. Forme normale de Smith

Si m, n sont des entiers positifs, on désigne par $M_{m\times n}(A)$ l'ensemble des matrices de type $m \times n$ sur A. Soit $J = (a_{ij})_{m\times n} \in M_{m\times n}(A)$. On appelle les a_{ii} avec $1 \leq i \leq \min\{m, n\}$ les *termes diagonaux* de J. En outre, on dit que J est *associé* à $J' = (b_{ij})_{m\times n}$, noté $J \sim J'$, si $a_{ij} \sim b_{ij}$, pour tous i, j avec $1 \leq i \leq m; 1 \leq j \leq n$. Le but de cette section est de réduire une matrice sur A à une matrice normale de Smith telle que définie ci-dessous.

3.2.1. Définition. Une matrice $D = (d_{ij})_{m\times n}$ sur A s'appelle une *matrice de Smith* si les conditions suivantes sont vérifiées:

(1) $d_{ij} = 0_A$ lorsque $i \neq j$.

(2) $(d_{11}) \supseteq (d_{22}) \supseteq \cdots \supseteq (d_{ss})$, où $s = \min\{m, n\}$.

Remarque. Si $d_{ii} = 0_A$, alors $d_{jj} = 0_A$ pour tout $i \leq j \leq \min\{m, n\}$.

Exemple. (1) Une matrice nulle ainsi qu'une matrice identité est une matrice de Smith.

(2) Considérons les matrices sur $\mathbb{Z}$ suivantes:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}.$$

La première matrice est une matrice de Smith, mais la deuxième ne l'est pas.

Soit $J \in M_{m\times n}(A)$. On se fixe i avec $1 \leq i \leq \min\{m,n\}$. Un *mineur d'ordre* i de J est le déterminant d'une sous-matrice carrée d'ordre i de J. Désignons par $\Delta_i(J)$ le plus grand commun diviseur des mineurs d'ordre i de J.

Exemple. Considérons la matrice sur $\mathbb{Z}$ suivante:

$$J = \begin{pmatrix} 3 & 6 & 0 \\ 6 & 0 & 3 \\ 0 & 3 & 2 \end{pmatrix}.$$

On trouve que $\Delta_1(J) = 1$, $\Delta_2(J) = 3$ et $\Delta_3(J) = 99$.

3.2.2. Lemme. Si $J \in M_{m\times n}(A)$, alors $\Delta_{r-1}(J) \mid \Delta_r(J)$ pour tout r avec $1 < r \leq \min\{m,n\}$.

Démonstration. Si $M = (a_{ij})_{r\times r}$ est une sous-matrice de J, alors

$$\det(M) = \sum\nolimits_{j=1}^{n} (-1)^{1+j} a_{1j}\, m_{1j}(M),$$

où $m_{1j}(M)$ est le $(1,j)$-mineur de M. Remarquons que chacun des $m_{1j}(M)$ est un mineur d'ordre $r-1$ de J. D'où, $\Delta_{r-1}(J) \mid \det(M)$. Par conséquent, $\Delta_{r-1}(J) \mid \Delta_r(J)$. Ceci achève la démonstration.

Remarque. Si $\Delta_i(J) = 0_A$, alors $\Delta_j(J) = 0_A$ pour tout j avec $i \leq j \leq \min\{m,n\}$.

3.2.3. Lemme. Si $D = (d_{ij})_{m\times n}$ est une matrice de Smith sur A, alors $\Delta_i(D) = d_{11}\cdots d_{ii}$, pour tout $1 \leq i \leq \min\{m,n\}$.

Démonstration. On se fixe $1 \leq r \leq \min\{m,n\}$. Alors $\det(d_{ij})_{r\times r} = d_{11}\cdots d_{rr}$. Soit

$$M = \begin{pmatrix} d_{i_1,j_1} & d_{i_1,j_2} & \cdots & d_{i_1,j_r} \\ d_{i_2,j_1} & d_{i_2,j_2} & \cdots & d_{i_2,j_r} \\ \vdots & \vdots & \ddots & \vdots \\ d_{i_r,j_1} & d_{i_r,j_2} & \cdots & d_{i_r,j_r} \end{pmatrix}$$

une sous-matrice de A, où $i_1 < \cdots < i_r$ et $j_1 < \cdots < j_r$. Si M contient une ligne nulle ou une colonne nulle, alors $\det(M) = 0$, ceci est divisible par $d_{11}\cdots d_{rr}$. Supposons maintenant

que M ne contient aucune ligne nulle ni colonne nulle. Alors d_{i_1,i_1} se trouve dans la première ligne de M. Ainsi $i_1 = j_t$ pour un certain $1 \leq t \leq r$. En particulier, $j_1 \leq j_t = i_1$. De même, comme d_{j_1,j_1} se trouve dans la première colonne de M, on a $j_1 = i_{t'}$ avec $1 \leq t' \leq r$, et donc $i_1 \leq i_{t'} = j_1$. Par conséquent, $i_1 = j_1$. De la même façon, on voit que $i_s = j_s$, pour $s = 1, \ldots, r$. D'où, $\det(M) = d_{i_1\, i_1} \cdots d_{i_r i_r}$, ceci est divisible par $d_{11} \cdots d_{rr}$. Par conséquent, $\Delta_r(D) = d_{11} \cdots d_{rr}$. La preuve s'achève.

Deux matrices $J, J' \in M_{m\times n}(A)$ sont dites *équivalentes* si $J' = PJQ$ avec P, Q des matrices inversibles sur A. Le résultat suivant est fondamental dans notre étude.

3.2.4. Lemme. Si $J, J' \in M_{m\times n}(A)$ sont équivalentes, alors $\Delta_i(J) \sim \Delta_i(J')$, pour tout $1 \leq i \leq \min\{m, n\}$. En particulier, $\det(J) \sim \det(J')$ lorsque $m = n$.

Démonstration. Considérons premièrement le cas où $J' = PJ$ avec $P = (p_{ij})_{m\times m}$ inversible. On se fixe un r avec $1 \leq r \leq \min\{m, n\}$. Partageons

$$J = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix},\ J' = \begin{pmatrix} L'_1 \\ \vdots \\ L'_n \end{pmatrix}$$

en lignes. Pour tout $1 \leq i \leq m$, on a $L'_i = (p_{i1} \cdots p_{in})J = \sum_{j=1}^{n} p_{ij} L_j,\ i = 1, \ldots, m$. On en déduit que si

$$M = \begin{pmatrix} b_{i_1,j_1} & b_{i_1,j_2} & \cdots & b_{i_1,j_r} \\ b_{i_2,j_1} & b_{i_2,j_2} & \cdots & ba_{i_2,j_r} \\ \vdots & \vdots & \ddots & \vdots \\ b_{i_r,j_1} & b_{i_r,j_2} & \cdots & b_{i_r,j_r} \end{pmatrix}$$

est une sous-matrice carrée de J', alors chacune des lignes de M est une combinaison linéaires des lignes de la sous-matrice

$$\begin{pmatrix} a_{1,j_1} & a_{1,j_2} & \cdots & a_{1,j_r} \\ a_{2,j_1} & a_{2,j_2} & \cdots & a_{2,j_r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,j_1} & a_{m,j_2} & \cdots & a_{m,j_r} \end{pmatrix}$$

de A. Comme la fonction

$$\det : M_r(A) \to A : J \mapsto \det(J)$$

est multi-linéaire par rapport aux lignes, on voit que $\det(M)$ est une combinaison linéaire de mineurs d'ordre r de J. Ainsi $\Delta_r(J) \mid \det(M)$. Par conséquent, $\Delta_r(J) \mid \Delta_r(J')$. De même, comme $J = P^{-1}J'$, on a $\Delta_r(J') \mid \Delta_r(J)$. D'où $\Delta_r(J) \sim \Delta_r(J')$. Par symétrie, on peut établir le résultat lorsque $J' = JQ$ avec Q inversible. Enfin, si $J' = PJQ$ avec P, Q inversible, alors $\Delta_r(J') \sim \Delta_r(PJ) \sim \Delta_r(J)$. Ceci achève la démonstration.

3.2.5. Définition. Les opérations suivantes s'appellent *opérations élémentaires* sur les lignes (respectivement, les colonnes) d'une matrice sur A:

Type 1: Échanger deux lignes (respectivement, deux colonnes).

Type 2: Additionner à une ligne (respectivement, une colonne) un multiple d'une autre ligne (respectivement, une autre colonne).

Type 3: Multiplier une ligne (respectivement, une colonne) par une unité de A.

En outre, on dit qu'une matrice J *se réduit à* une matrice J' si cette dernière est obtenue à partir de la première par une suite finie d'opérations élémentaires sur les lignes ou sur les colonnes.

Remarque. Les opérations élémentaires sont toutes inversibles.

Pour tout entier $n \geq 1$, on désigne par I_n la matrice identité d'ordre n sur A.

3.2.6. Définition. Une matrice obtenue à partir de I_n par une seule opération élémentaire T sur les lignes ou sur les colonnes s'appelle une *matrice élémentaire* associée à T.

3.2.7. Proposition. Si J est une matrice sur A, alors effectuer une opération élémentaire T sur les lignes (respectivement, les colonnes) de J est équivalent à multiplier J à gauche (respectivement, à droite) par la matrice élémentaire associée à T.

3.2.8. Corollaire. (1) Les matrices élémentaires sont inversibles.

(2) Si J se réduit à J', alors J et J' sont équivalentes.

Démonstration. Soient P la matrice élémentaire obtenue à partir de I_n par une opération élémentaire T, et Q celle-ci obtenue à partir de I_n par T^{-1}. On ne considère que le cas où T est éffectué sur les lignes. Comme P se réduit à I_n par T^{-1}, on a $QP = I_n$.

En outre, comme Q se réduit à I_n par T, on a $QP = I_n$. Ceci prouve la partie (1). Maintenant la partie (2) se découle par récurrence de la partie (1) et la proposition 3.2.6. La preuve s'achève.

Le résultat facile suivant est pratique dans la normalisation de matrices.

3.2.9. Lemme. Si $a, b \in A$, alors la matrice

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

se réduit à la matrice

$$\begin{pmatrix} d & 0 \\ 0 & m \end{pmatrix},$$

où d est le plus grand commun diviseur et m le plus petit commun multiple de a, b.

Démonstration. Soient $a, b \in A^*$ dont d est le plus grand commun diviseur et m le plus petit commun multiple. Alors il existe $u, v \in A$ tels que $au + bv = d$. Posant $a = a_1 d$ et $b = b_1 d$, on a $m = ab_1 = a_1 b$. Or, par les opérations $L_2 + uL_1$ et $C_1 + vC_2$, la matrice

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

se réduit à la matrice

$$J = \begin{pmatrix} a & 0 \\ d & b \end{pmatrix}.$$

Et cette dernière, par les opérations $L_1 - a_1 L_2$ et $C_2 - b_1 C_1$, se réduit à la matrice

$$J_1 = \begin{pmatrix} 0 & -m \\ d & 0 \end{pmatrix}.$$

Il est evident que J_1 se réduit à la matrice désirée. Ceci achève la démonstration.

Exemple. La matrice sur $\mathbb{Z}$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{pmatrix}$$

se réduit à la matrice de Smith suivante:

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

3.2.10. Lemme. Toute matrice sur A de type $m \times n$ se réduit à une matrice $(b_{ij})_{m\times n}$ telle que $b_{11} \mid b_{ij}$, pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$.

Démonstration. Soit $J = (a_{ij})_{m\times n}$ non nulle. Rappelons que A est muni d'une valuation $\varphi : A^* \to \mathbb{N}$. Posons $\varphi(J) = \min\{\varphi(a_{ij}) \mid a_{ij} \neq 0, 1 \leq i \leq m, 1 \leq j \leq n\}$, sur lequel on procède par récurrence. Échangeant des lignes et des colonnes si nécessaire, on peut supposer que $\varphi(J) = \varphi(a_{11})$. Si $\varphi(J) = \varphi(1_A)$, alors a_{11} est une unité. Ainsi le résultat est valide.

Supposons que $\varphi(J) > \varphi(1_A)$. Si la première ligne de J contient un terme, disons a_{1j_0}, qui n'est pas un multiple de a_{11}. Alors $a_{1j_0} = a_{11}q + s$, où $s \in A^*$ avec $\varphi(s) < \varphi(a_{11})$. En effectuant l'opération $C_{j_0} - qC_1$, on obtient une matrice J_1 avec $\varphi(J_1) < \varphi(J)$. Par l'hypothèse de récurrence, J_1, et ainsi que J, se réduit à une matrice désirée. De même, le résultat est valide si la première colonne de J contient un terme qui n'est pas un multiple de a_{11}. On considère maintenant le cas où $a_{11} \mid a_{i1}$ et $a_{11} \mid a_{1j}$ pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$. Dans ce cas, J se réduit à une matrice de la forme suivante:

$$J_2 = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & \cdots & b_{mn} \end{pmatrix}.$$

Supposons que $a_{11} \not| b_{i_0j_0}$ pour certains $2 \leq i_0 \leq m$ et $2 \leq j_0 \leq n$. Alors J_2 se réduit à la matrice

$$J_3 = \begin{pmatrix} a_{11} & b_{i_02} & \cdots & b_{i_0j_0} & \cdots & b_{i_0n} \\ 0 & b_{22} & \cdots & b_{2j_0} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & & \\ 0 & b_{m2} & \cdots & b_{mj_0} & \cdots & b_{mn} \end{pmatrix}.$$

Comme on a vu précédemment, J_3 se réduit à une matrice J_4 avec $\varphi(J_4) < \varphi(a_{11}) = \varphi(J)$. Par l'hypothèse de récurrence, J_4 ainsi que J se réduit à une matrice désirée. Ceci achève la démonstration.

3.2.11. Théorème. Toute matrice J sur A se réduit à une matrice de Smith, appelée une *forme normale de Smith* de J.

Démonstration. On procède par récurrence sur la taille de J. Posons $J = (a_{ij})_{m\times n}$. D'après le lemme 3.2.10, on peut supposer que $a_{11} \mid a_{ij}$, pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$. Posons $a_{ij} = a_{11}a'_{ij}$ avec $a'_{ij} \in A$, pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$. En effectuant premièrement les opérations $L_i - a'_{i1}L_1$, $i = 2, \ldots, m$ et ensuite les opérations $C_j - a'_{1j}C_1$, $j = 2, \ldots, n$, on obtient une matrice de la forme

$$J_2 = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & \cdots & b_{mn} \end{pmatrix},$$

où les b_{ij} sont des combinaison linéaires des a_{pq} avec $1 \leq p \leq m$ et $1 \leq q \leq n$. Ainsi $a_{11} \mid b_{ij}$, pour tous $2 \leq i \leq m$ et $2 \leq j \leq n$. Par conséquent, $a_{11} \mid \Delta_1(J_3)$, où $J_3 = (b_{ij})_{2\leq i\leq m;2\leq j\leq n}$. Par l'hypothèse de récurrence, la matrice J_3 se réduit à une matrice de Smith $J_4 = (d_{ij})_{2\leq i\leq m;2\leq j\leq n}$. D'après le corollaire 3.2.8(2) et les lemmes 3.2.3 et 3.2.4, on a $\Delta_1(J_3) = \Delta_1(J_4) = d_{22}$. D'où $a_{11} \mid d_{22}$. Donc

$$J_5 = \begin{pmatrix} a_{11} & 0 \\ 0 & J_4 \end{pmatrix}$$

est une matrice de Smith. Remarquons J se réduit à J_5. La preuve s'achève.

Exemple.

$$\begin{pmatrix} 3 & 6 & 0 \\ 6 & 0 & 3 \\ 0 & 3 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 3 & 6 & 0 \\ 3 & 0 & 3 \\ -2 & 3 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 9 & 2 \\ 3 & 0 & 3 \\ -2 & 3 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 9 & 2 \\ 0 & -27 & -3 \\ 0 & 21 & 6 \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -27 & -3 \\ 0 & 21 & 6 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 27 & 3 \\ 0 & 21 & 6 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 27 \\ 0 & 6 & 21 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 33 \end{pmatrix}.$$

Soient $a, b \in A$ avec $b \neq 0_A$. Si $a = bc$ avec $c \in A$, alors c est unique car A est intègre. Par l'abus de notation, on note $c = \dfrac{a}{b}$.

3.2.12. Théorème. Soient $J \in M_{m\times n}(A)$ dont $D = (d_{ij})_{m\times n}$ est une forme normale de Smith.

(1) $d_{11} \sim \Delta_1(J)$.

(2) Pour tout $1 < i \leq \min\{m, n\}$, on a $d_{ii} = 0$ si $\Delta_i(J) = 0_A$; et sinon, $d_{ii} \sim \frac{\Delta_i(J)}{\Delta_{i-1}(J)}$.

(3) D est unique à associé près.

Démonstration. On se fixe $1 \leq i \leq \min\{m, n\}$. D'après les lemmes 3.2.2 et 3.2.10, on a $d_{11} \cdots d_{ii} = \Delta_i(D) \sim \Delta_i(J)$. Supposons que $d_{ii} \neq 0_A$. Alors $d_{11}, \ldots, d_{i-1,i-1}$ sont tous non nuls. Donc $d_{11} \cdots d_{ii} \neq 0_A$. D'où, $\Delta_i(J) \neq 0_A$. En outre, $\Delta_i(J) \sim \Delta_{i-1}(J)d_{ii}$. Par conséquent, $d_{ii} \sim \frac{\Delta_i(J)}{\Delta_{i-1}(J)}$. D'après les parties (1) et (2), D est uniquement déterminée, à associée près, par les $\Delta_i(J)$ avec $1 \leq i \leq \min\{m, n\}$. Ceci achève la démonstration.

Exemple. Considérons la matrice sur $\mathbb{Z}$ suivante:

$$J = \begin{pmatrix} 2 & 0 & 3 & 0 \\ 1 & 5 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

D'abord, comme 1 est un mineur d'ordre un et un mineur d'ordre 2, on a $\Delta_1(J) = \Delta_2(J) = 1$. Enfin, comme 13 est le seul mineur non nul de J, on a $\Delta_3(J) = 13$. D'où, la forme normale de Smith de J est comme suit:

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 13 & 0 \end{pmatrix}.$$

3.2.13. Corollaire. Soient $J, J' \in M_{m\times n}(A)$. Les conditions suivantes sont équivalentes:

(1) J et J' sont équivalentes.

(2) $\Delta_i(J) \sim \Delta_i(J')$, pour tout $1 \leq i \leq \min\{m, n\}$.

(3) J se réduit à J'.

Démonstration. D'après le lemme 3.2.4, (1) implique (2). Et d'après le corollaire 3.2.8(2), (4) implique (1). Il suffit de montrer que (2) implique (3). Soient $D = (d_{ij})_{m\times n}$

une forme normale de Smith de J et $D' = (d'_{ij})_{m\times n}$ une forme normale de Smith de J'. Si $\Delta_i(J) \sim \Delta_i(J')$, pour tout $1 \leq i \leq \min\{m, n\}$, alors $d_{ii} \sim d'_{ii}$, pour tout $1 \leq i \leq \min\{m, n\}$. Ainsi D se réduit à D', et donc J se réduit à J'. Ceci achève la démonstration.

3.3. Modules de type fini

Le but de cette section est d'étudier les modules de type fini sur A.

3.3.1. Lemme. Soit L un A-module libre de rang m. Si N est un sous-module non nul de L, alors il existe une base $\{u_1, \ldots, u_m\}$ de L, et des éléments $d_1, \ldots, d_n$ de A avec $1 \leq n \leq m$ et $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_n)$ tels que $\{d_1u_1, \ldots, d_nu_n\}$ est une base de N.

Démonstration. D'après le théorème 2.6.10, N est libre de rang $n \leq m$. Prenons une base $\{v_1, \ldots, v_m\}$ de L et une base $\{w_1, \ldots, w_n\}$ de N. Alors $w_j = \sum_{i=1}^{m} a_{ij}v_i$, $j = 1, \ldots, n$. Posant $J = (a_{ij})_{m\times n}$, on a $(w_1, \ldots, w_n) = (v_1, \ldots, v_m)J$. D'après le théorème 3.2.11 et le corollaire 3.2.8(2), il existe une matrice inversible P d'ordre m et une matrice inversible Q d'ordre n telles que $P^{-1}JQ = D = (d_{ij})_{m\times n}$, une matrice de Smith. Posons $d_i = d_{ii}, i = 1, \ldots, n$. Alors $d_1 \mid d_2 \mid \cdots \mid d_m$. Posons $(u_1, \ldots, u_m) = (v_1, \ldots, v_m)P$ et $(w'_1, \ldots, w'_n) = (w_1, \ldots, w_n)Q$. Comme P et Q sont inversibles, $\{u_1, \ldots, u_m\}$ est une base de L et $(w'_1, \ldots, w'_n)$ est une base de N. En outre,

$$(w'_1, \ldots, w'_n) = (w_1, \ldots, w_n)Q = (v_1, \ldots, v_m)JQ = (u_1, \ldots, u_m)P^{-1}JQ = (u_1, \ldots, u_m)D.$$

D'où, $w'_j = u_jd_j$, $j = 1, \ldots, n$. Ceci achève la démonstration.

3.3.2. Théorème. Si M est un A-module de type fini, alors il existe $d_1, \ldots, d_m \in A$ avec $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_m)$ tels que

$$M \cong A/(d_1) \amalg A/(d_2) \amalg \cdots \amalg A/(d_m).$$

Démonstration. D'après la proposition 2.6.5, il existe une application surjective $g : L \to M$, où L est libre de type fini. Supposons que L est de rang m et $\mathrm{Ker}g$ est de rang n. D'après le lemme 3.3.1, il existe une base $\{u_n, \ldots, u_m\}$ de L et $d_1, \ldots, d_n \in A$ avec $d_{i-1} \mid d_i$, $i = 2, \ldots, n$, tels que $\{d_1u_n, \ldots, d_nu_n\}$ est une base de $\mathrm{Ker}g$. Posons $d_i = 0_A$, pour tout

$n < i \leq m$. Alors $d_{i-1} \mid d_i$, $i = 2, \ldots, m$, et $\mathrm{Ker}g =< d_1u_1, \ldots, d_nu_n, \ldots, d_mu_m >$. Or l'application $f : A^m \to L : (a_1, \ldots, a_m) \mapsto a_1u_1 + \cdots + a_mu_m$ est un isomorphisme. Posons $N = \{(a_1d_1, \cdots, a_md_m) \mid a_i \in A\} = (d_1) \amalg (d_2) \amalg \cdots \amalg (d_m)$. Il est évident que $f(N) \subseteq \mathrm{Ker}g$. Réciproquement si $(b_1, \ldots, b_m) \in f^{-1}(\mathrm{Ker}g)$, c'est-à-dire, $f(b_1, \ldots, b_n) \in \mathrm{Ker}g$, alors $b_1u_1 + \cdots + b_mu_m = a_1d_1u_1 + \cdots + a_md_mu_m$, où $a_1, \ldots, a_m \in A$. Comme $\{u_1, \ldots, u_m\}$ est libre, $b_i = a_id_i$, $i = 1, \ldots, m$. Cela veut dire que $f^{-1}(\mathrm{Ker}g) = N$. En appliquant le théorème 2.2.6(2), on voit que

$$M \cong L/\mathrm{Ker}g \cong A^m/N \cong A/(d_1) \amalg A/(d_2) \amalg \cdots \amalg A/(d_m),$$

où le dernier isomorphisme suit de la proposition 2.5.7. Ceci achève la démonstration.

Le résultat suivant est une conséquence du théorème 3.3.2 et le corollaire 3.1.2.

3.2.3. Théorème. Si M est un A-module de type fini, alors

$$M \cong A/(p_1^{n_1}) \amalg \cdots \amalg A/(p_r^{n_r}) \amalg A^s,$$

où $r \geq 0$, $s \geq 0$, et $p_1, \ldots, p_r$ sont des éléments premiers de A.

3.3.4. Théorème. Soit M un A-module de type fini. Si M est non nul, alors M est indécomposable si et seulement si $M \cong A$ ou $M \cong A/(p^n)$ avec p un élément premier de A et $n > 0$.

Démonstration. La nécessité sui du théorème 3.3.3, et la suffisance suit de la proposition 3.1.3. La preuve s'achève.

Appliquant les théorèmes 3.3.3 et 3.3.4, on a le résultat suivant.

3.3.5. Corollaire. Soit M un A-module de type fini. Si M est non nul, alors $M = M_1 \oplus \cdots M_r$, où $M_1, \ldots, M_r$ sont des A-modules indécomposables.

3.3.6. Proposition. Un A-module de type fini est libre si et seulement s'il est sans torsion.

Démonstration. Comme A est intègre, tout A-module libre est sans torsion. Soit $d \in A$. Si d est une unité, alors $A/(d) = 0$. Sinon, $A/(d)$ est sans torsion si et seulement

si $d = 0_A$. Soit M un A-module sans torsion de type fini. Si $M = 0$, alors M est libre. Supposons que $M \neq 0$. D'après le théorème 3.3.2, il existe $d_1, \ldots, d_n \in A$ tels que $M \cong A/(d_1) \amalg A/(d_2) \amalg \cdots \amalg A/(d_m)$. Comme $M \neq 0$, on peut supposer qu'aucun des d_i n'est une unité. Comme

$$\mathcal{T}(M) \cong \mathcal{T}(A/(d_1) \amalg A/(d_2) \amalg \cdots \amalg A/(d_m)) \cong \mathcal{T}(A/(d_1)) \amalg \mathcal{T}(A/(d_2)) \amalg \cdots \amalg \mathcal{T}(A/(d_m)),$$

on a $\mathcal{T}(A/(d_i)) = 0$, et donc $d_i = 0, i = 1, \ldots, m$. Par conséquent, M est libre. Ceci achève la démonstration.

3.3.7. Proposition. Si M est un A-module de type fini, alors $M = \mathcal{T}(M) \oplus L$, où L est un A-module libre de type fini.

Démonstration. On a une suite exacte courte

$$0 \longrightarrow \mathcal{T}(M) \xrightarrow{j} M \xrightarrow{p} M/\mathcal{T}(M) \longrightarrow 0\,,$$

où j est l'inclusion et p est la projection canonique. Étant sans torsion de type fini, $M/\mathcal{T}(M)$ est libre d'après la proposition 3.3.6. Ainsi la suite est scindée. Donc il existe un sous-module L de M tel que $M = \mathrm{Im}j \oplus L = \mathcal{T}(M) \oplus L$. Comme $L \cong M/\mathcal{T}(M)$, on voit que L est libre de type fini. Ceci achève la démonstration.

3.4 Exercices

1. Montrer qu'un anneau euclidien est principal.

2. Soit A un anneau euclidien de valuation $\varphi : A^* \to \mathbb{N}$. Si $a \in A^*$, montrer que a est inversible si et seulement si $\varphi(a) = \varphi(1_A)$.

3. Soient $n = ab$ avec a, b des entiers positifs. Montrer que $\mathbb{Z}_n \cong \mathbb{Z}_a \amalg \mathbb{Z}_b$ si et seulement si a, b sont co-premiers. *Indication*: Pour la nécessité, remarquer $n = dm$, où d est le plus grand commun diviseur de a, b; et m, le plus petit commun multiple.

4. Dans chacun des cas suivants, factoriser le module en co-produit de modules indécomposables.

(1) Le $\mathbb{Z}$-module $\mathbb{Z}_{3600}$.

(2) Le $\mathbb{Q}[x]$-module $\mathbb{Q}[x]/<x^3 - x^2 - x + 1>$.

(3) Le $\mathbb{C}[x]$-module $\mathbb{C}[x]/<x^4 + 2x^2 + 1>$.

5. Déterminer si le $\mathbb{Z}$-module $\mathbb{Z}_n$ est décomposable ou indécomposable, où

(1) $n = 841$; (2) $n = 175$.

6. Déterminer avec justification si le $\mathbb{Q}[x]$-module $\mathbb{Q}[x]/ < f(x) >$ est décomposable ou indécomposable, où

(1) $f(x) = x^3 - 6x^2 + 12x - 8$; (2) $f(x) = x^4 - 2x^2 + 1$.

7. Soient A un anneau principal et p un élément premier de A. Pour tout entier $n > 0$, trouver les sous-modules ainsi que les modules quotients de $A/(p^n)$.

8. Considérer la matrice sur $\mathbb{Z}$ suivante:

$$J = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 10 & 0 \end{pmatrix}.$$

(1) Réduire J à une matrice de Smith.

(2) Calculer, d'après la définition, $\Delta_i(J)$ pour $i = 1, 2, 3, 4$.

9. Réduire la matrice suivante sur $\mathbb{Z}$ à sa forme normale de Smith, en donnant à chaque fois les matrices élémnetaires associées.

$$\begin{pmatrix} 0 & 6 & -9 & 3 \\ 12 & 24 & 9 & 9 \\ 30 & 42 & 45 & 27 \\ 66 & 78 & 81 & 63 \end{pmatrix}.$$

10. Réduire la matrice suivante sur $\mathbb{Q}[x]$ à sa forme normale de Smith:

$$\begin{pmatrix} 1-x & x^2 & x \\ x & -x & x \\ 1+x^2 & x^2 & -x^2 \end{pmatrix}.$$

11. Soit K un corps. Considérer la matrice sur $K[x]$ suivante:

$$J = \begin{pmatrix} f_1(x) & a_1 & 0 & \cdots & 0 & 0 \\ 0 & f_2(x) & a_2 & \cdots & 0 & 0 \\ 0 & 0 & f_3(x) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & f_{n-1}(x) & a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & f_n(x) \end{pmatrix},$$

où $a_1, \cdots, a_{n-1} \in K$ sont tous non nuls. Calculer $\Delta_i(J)$, $i = 1, \cdots, n$, et en déduire la forme normale de Smith de J.

12. Soit J une matrice carrée d'ordre n sur un anneau euclidien A. Montrer que les énoncés suivants sont équivalents:
    (1) J est inversible.
    (2) $\det(J)$ est inversible.
    (3) J se réduit à I_n.
    (4) J se décompose en produit de matrices élémentaires.

13. Soit A un anneau euclidien, et soit $J \in M_{m\times n}(A)$ dont D est une forme canonique de Smith de J.
    (1) Si $m \geq n$, montrer que les termes diagonaux de D sont tous associés à 1_A si, et seulement si, il existe $J' \in M_{n\times m}(A)$ telle que $J'J = I_n$.
    (2) Si $m \leq n$, montrer que les termes diagonaux de D sont tous associés à 1_A si, et seulement si, il existe $J' \in M_{n\times m}(A)$ telle que $JJ' = I_m$.

14. Factoriser le $\mathbb{R}[x]$-module $\mathbb{R}[x]/<x^3 - 1>$ en produit de deux $\mathbb{R}[x]$-modules cycliques non nuls.

15. Déterminer si le $\mathbb{Z}$-module $\mathbb{Q}$ est de type fini ou infini.

16. Soient A un anneau euclidien et M un A-module non nul de torsion. Montrer que M est cyclique si et seulement s'il existe des éléments premiers $p_1, \cdots, p_r \in A$ deux à deux non associés et des entiers positifs $n_1, \cdots, n_r$ tels que

$$M \cong A/(p_1^{n_1}) \amalg \cdots \amalg A/(p_r^{n_r}).$$

Chapitre 4: Forme canonique de Jordan

Partout dans ce chapitre, on se fixe K un corps algébriquement clos. C'est-à-dire, tout polynôme non nul sur K se décompose comme produit de facteurs de degré un. Soit $K[\lambda]$ l'anneau des polynômes en indéterminée λ à coefficients dans K. Rappelons que $K[\lambda]$ est un anneau euclidien dont les éléments premiers sont les polynômes de degré un.

Dès maintenant, on se fixe E un K-espace vectoriel non nul de dimension fini et $f : E \to E$ une application K-linéaire. Soit $\mathcal{U} = \{u_1, \ldots, u_n\}$ une K-base de E. Alors la matrice de f dans la base $\mathcal{B}$, notée $[f]_{\mathcal{U}}$, est une matrice carrée d'ordre n sur K telle que

$$(f(u_1), \cdots, f(u_n)) = (u_1, \cdots, u_n)[f]_{\mathcal{U}}.$$

Rappelons que le *polynôme charactéristique* de f est le polynôme de degré n suivant:

$$\chi_f(\lambda) = \det([f]_{\mathcal{U}} - \lambda I_n).$$

Exemple. Considérons l'espace complexe $\mathbb{C}^3$ et la transformation linéaire $\mathbb{C}$-linéaire

$$f : \mathbb{C}^3 \to \mathbb{C}^3 : (x, y, z) \mapsto (3x - y, 2y - z, z - x).$$

Alors la matrice de f dans la base canonique est

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

Donc

$$\chi_f(\lambda) = \begin{vmatrix} 3-\lambda & -1 & 0 \\ 0 & 2-\lambda & -1 \\ -1 & 0 & 1-\lambda \end{vmatrix} = 5 + 6\lambda - 11\lambda^2 - \lambda^3.$$

Il est connu que les matrices de f dans deux bases distinctes sont semblables. Notre but est de trouver une base de E dans laquelle la matrice de f est la plus simple possible.

On dit que $p(\lambda) \in K[\lambda]$ est un *annulateur* de f si $p(f) = \mathbf{0}$. Le résultat suivant est classique en algèbre linéaire.

4.1. Théorème de Hamilton-Cayley. Si $f : E \to E$ est une transformation K-linéaire, alors $\chi_f(\lambda)$ est un annulateur de f.

À partir de maintenant, on considère E comme un $K[\lambda]$-module défini par f, qui est évidemment de type fini. En outre, pour tout $u \in E$, on a $\chi_f(\lambda) \cdot u = \chi_f(f)(u) = \mathbf{0}(u) = 0_E$. Ainsi E est un $K[\lambda]$-module de torsion.

4.2. Lemme. Soient $a \in K$ et $n > 0$ un entier. Le K-espace vectoriel $K[\lambda]/((\lambda - a)^n)$ a pour base $\{\, \bar{1},\ \overline{\lambda - a},\ \ldots,\ \overline{(\lambda - a)^{n-1}} \,\}$.

Démonstration. Comme $(\lambda - a)^n$ est de degré n, on voit que $K[\lambda]/((\lambda - a)^n)$ est de K-dimension n. On prétend que $\{\, \bar{1},\ \overline{\lambda - a},\ \ldots,\ \overline{(\lambda - a)^{n-1}} \,\}$ est libre. Si ce n'est pas vrai, alors il existe $a_0, a_, \ldots, a_{n-1} \in K$, non tous nuls, tels que

$$a_0\bar{1} + a_1\overline{(\lambda - a)} + \cdots + a_{n-1}\overline{(\lambda - a)^{n-1}} = \bar{0}.$$

Alors $(\lambda - a)^n$ divise $p(\lambda) = a_0 + a_1(\lambda - a)\cdots + a_{n-1}(\lambda - a)^{n-1}$, ceci est impossible puisque $a_0 + a_1(\lambda - a)\cdots + a_{n-1}(\lambda - a)^{n-1}$ est non nul de degré au plus $n - 1$. Ainsi $\{\bar{1}, \overline{\lambda - a}, \ldots, \overline{(\lambda - a)^{n-1}}\}$ est libre, et donc une K-base de $K[\lambda]/((\lambda - a)^n)$. La preuve s'achève.

Pour tout $a \in K$, on appelle la matrice carrée

$$J_n(a) = \begin{pmatrix} a & 0 & \cdots & 0 & 0 \\ 1 & a & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a & 0 \\ 0 & 0 & \cdots & 1 & a \end{pmatrix}_{n \times n}$$

un *bloc de Jordan* de valeur propre a d'ordre n. Remarquons qu'une matrice carrée d'ordre 1 est un bloc de Jordan.

4.3. Proposition. Le $K[\lambda]$-module E défini par f est indécomposable si et seulement si $E \cong K[\lambda]/((\lambda - a)^n)$, où $a \in K$ et $n > 0$. Dans ce cas, E admet une K-base $\mathcal{U}$ telle que $[f]_{\mathcal{U}} = J_n(a)$.

Démonstration. La suffisance suit immédiate du théorème 3.2.9. Supposons maintenant que E est indécomposable. D'après le théorème 3.2.9, soit $E \cong K[\lambda]$ soit $E \cong K[\lambda]/(p(\lambda)^n)$ avec $p(\lambda)$ irréductible et $n > 0$. Comme ${}_{K[\lambda]}E$ est de torsion, le premier cas ne se produit pas. Ainsi $E \cong K[\lambda]/(p(\lambda)^n)$ avec $p(\lambda)$ irréductible et $n > 0$. Comme K est algébriquement clos, on peut supposer que $p(\lambda) = \lambda - a$ avec $a \in K$. Ceci nous donne la nécessité. Soit maintenant $\varphi : K[\lambda]/((\lambda - a)^n) \to E$ un isomorphisme de $K[\lambda]$-modules. Posons $u_i = \varphi(\overline{(\lambda - a)^i}),\ i = 0, 1, \ldots, n$. Alors $u_n = 0_E$ et $\mathcal{U} = \{u_0, u_1, \ldots, u_{n-1}\}$ est une K-base de E. Or

$$f(u_i) = x \cdot u_i = x \cdot \varphi(\overline{(x-a)^i}) = \varphi(x\overline{(x-a)^i}) = \varphi(\overline{(x-a)^{i+1} + a(x-a)^i}) = au_i + u_{i+1},$$

pour $i = 0, 1, \cdots, n-1$. En particulier, $f(u_{n-1}) = au_{n-1} + u_n = au_{n-1}$. D'où, $[f]_{\mathcal{U}} = J_n(a)$. La preuve s'achève.

Si F est un sous-module du $K[\lambda]$-module E, alors F est un sous-espace de ${}_KE$ tel que $f(F) \subseteq F$. Ainsi

$$f|_F : F \to F : u \mapsto f(u)$$

est une transformation linéaire de F. Si $\mathcal{V}$ est une base de F, par abus de notation, on note $[f|_F]_{\mathcal{V}} = [f]_{\mathcal{V}}$. Par exemple, considérons le $\mathbb{C}$-endomorphisme de l'espace complexe $\mathbb{C}^3$ suivant:

$$f : \mathbb{C}^3 \to \mathbb{C}^3 : (x, y, z) \mapsto (x + y - z, y - z, z).$$

On voit que $F = \{(x, y, 0) \mid x, y \in \mathbb{C}\}$ est un sous-espace de $\mathbb{C}^3$ de base $\{e_1, e_2\}$ qui est f-invariant. Or

$$[f]_{\{e_1,e_2\}} = [f|_F]_{\{e_1,e_2\}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

4.4. Lemme. Supposons que $E = E_1 \oplus E_2$, où E_1 et E_2 sont des sous-modules non nuls du $K[\lambda]$-module E. Si $\mathcal{U} = \{u_1, \ldots, u_r\}$ est une K-base de E_1 et $\mathcal{V} = \{v_1, \ldots, v_s\}$ est une

K-base de E_2, alors $\mathcal{W} = \mathcal{U} \cup \mathcal{V}$ est une K-base de E telle que

$$[f]_{\mathcal{W}} = \begin{pmatrix} [f]_{\mathcal{U}} & 0 \\ 0 & [f]_{\mathcal{V}} \end{pmatrix}.$$

Démonstration. Comme E_1 et E_2 sont des sous-espaces vectoriels de ${}_KE$ tels que $E = E_1 \oplus E_2$, on voit que $\mathcal{W}$ est une K-base de E. Posons $[f]_{\mathcal{U}} = (a_{ij})_{r\times r}$ et $[f]_{\mathcal{V}} = (b_{ij})_{s\times s}$. Alors

$$\begin{array}{rcccccccccccc}
f(u_1) &=& a_{11}u_1 &+& \cdots &+& a_{r1}u_r &+& 0v_1 &+& \cdots &+& 0v_s \\
&& \vdots & & & & & & & & & & \\
f(u_r) &=& a_{1r}u_1 &+& \cdots &+& a_{rr}u_r &+& 0v_1 &+& \cdots &+& 0v_s \\
f(v_1) &=& 0u_1 &+& \cdots &+& 0u_r &+& b_{11}v_1 &+& \cdots &+& b_{s1}v_s \\
&& \vdots & & & & & & & & & & \\
f(v_s) &=& 0u_1 &+& \cdots &+& 0u_r &+& b_{1s}v_1 &+& \cdots &+& b_{ss}v_s.
\end{array}$$

D'où le résultat. Ceci achève la démonstration.

Une *matrice de Jordan* sur K est une matrice carrée partagée de la forme

$$\begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{n_2}(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{n_r}(\lambda_r) \end{pmatrix},$$

où $\lambda_1, \lambda_2, \ldots, \lambda_r \in K$. Remarquons qu'une matrice diagonale est une matrice de Jordan dont chaque bloc de Jordan est d'ordre un. Par exemple,

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

est une matrice de Jordan.

4.5. Théorème. Soit E un K-espace vectoriel non nul de dimension finie. Si f est un K-endomorphisme de E, alors E admet une K-base $\mathcal{B}$ telle que $[f]_{\mathcal{B}}$ est une matrice de Jordan.

Démonstration. D'après le corollaire 3.2.10, le $K[\lambda]$-module E défini par f se décompose comme $E = E_1 \oplus E_2 \oplus \cdots \oplus E_r$, où $E_1, \ldots, E_r$ sont des sous-modules indécomposables de E. D'après la proposition 4.3, il existe une base $\mathcal{B}_i$ de E_i telle que $[f]_{\mathcal{B}_i} = J_{n_i}(\lambda_i)$ avec $\lambda_i \in K$, $i = 1, 2, \ldots, r$. D'après le lemme 4.4, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_r$ est une base de E et

$$[f]_{\mathcal{B}} = \begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{n_2}(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{n_r}(\lambda_r) \end{pmatrix}.$$

Ceci achève la démonstration.

4.6. Théorème. Toute matrice carrée M sur K est semblable à une matrice de Jordan, appelé une *forme canonique de Jordan* de M.

Démonstration. Si M est d'ordre n, on considère la transformation K-linéaire

$$f : K^n \to K^n : (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n)M^T.$$

Alors $[f]_{\{e_1,\ldots,e_n\}} = M$, où $\{e_1, \ldots, e_n\}$ est la base canonique de K^n. D'après le théorème 4.5, K^n admet une K-base $\mathcal{B}$ telle que $[f]_{\mathcal{B}}$ est une matrice de Jordan. Or le résultat suit du fait que M est semblable à $[f]_{\mathcal{B}}$. La preuve s'achève.

Le reste de ce chapitre sera consacré au calcul de la forme canonique de Jordan d'une matrice carrée. Un polynôme $p(\lambda)$ sur K est dit *normalisé* si le coefficient du terme de degré le plus haut est 1. Évidemment, tout polynôme non nul est associé à un unique polynôme normalisé. Plus généralement, une matrice sur $K[\lambda]$ est dite *normalisée* si chacun de ses terms est soit nul soit un polynôme normalisé. On voit aisément que toute matrice sur $K[\lambda]$ est associée à une unique matrice normalisée. Si $p(\lambda) \in K[\lambda]$ est normalisé non constant, comme K algébriquement clos, alors $p(\lambda)$ se factorise comme

$$p(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_r)^{n_r},$$

où les $\lambda_i \in K$ sont deux à deux distincts et $n_i > 0$. Dans ce cas, $(\lambda - \lambda_1)^{n_1}, \cdots, (\lambda - \lambda_r)^{n_r}$ s'appellent les *facteurs primaires* de $p(\lambda)$.

Exemple. Si $p(\lambda) = (\lambda-3)^3(\lambda-5)^2(\lambda-7)$, alors les facteurs primaires de $p(\lambda)$ sont $(\lambda-3)^3, (\lambda-5)^2, (\lambda-7)$.

4.7. Définition. Soit $M \in M_n(K)$. Considérons $M - \lambda I_n \in M_n(K[\lambda])$. Comme $\Delta_n(M-\lambda I_n) = \chi_M(\lambda)$ est non nul, $M - \lambda I_n$ se réduit à une unique matrice de Smith normalisée

$$\begin{pmatrix} d_1(\lambda) & 0 & \cdots & 0 \\ 0 & d_2(\lambda) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n(\lambda) \end{pmatrix}.$$

On appellent $d_1(\lambda), d_2(\lambda), \cdots, d_n(\lambda)$ les *facteurs invariants* de M. En outre, les facteurs primaires de $d_i(\lambda)$, $i = 1, \ldots, n$, s'appellent les *facteurs élémentaires* de M.

Remarque. (1) Un facteur invariant non constant est un produit de certains facteurs élémentaires.

(2) $(-1)^n\chi_M(\lambda)$ est égal au produit des facteurs invariants de M.

(3) $(-1)^n\chi_M(\lambda)$ est égal au produit des facteurs élémentaires de M.

Exemple. (1) Soit

$$J = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Considérons

$$J - \lambda I = \begin{pmatrix} 1-\lambda & 1 & 1 \\ 0 & 2-\lambda & 0 \\ 0 & 0 & 1-\lambda \end{pmatrix}.$$

On voit que $\Delta_1(J-\lambda I) = \Delta_2(J-\lambda I) = 1$, et $\Delta_3(J-\lambda I) = (\lambda-2)(\lambda-1)^2$. D'où $d_1(J-\lambda I) = d_2(J-\lambda I) = 1$ et $d_3(J-\lambda I) = (\lambda-2)(\lambda-1)^2$. Ainsi la forme canonique de Smith de $J - \lambda I$ est la matrice suivante:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (\lambda-2)(\lambda-1)^2 \end{pmatrix}.$$

Par conséquent, les facteurs invariants de J sont $\{1, 1, (\lambda-2)(\lambda-1)^2\}$ et les facteurs élémentaires de J sont $\lambda-2$ et $(\lambda-1)^2$.

(2) Soit M une matrice carrée complexe. Si les facteurs élémentaires de M sont $\lambda-1, \lambda-1, \lambda-3, (\lambda-1)^2, (\lambda-2)^2, (\lambda-2)^3$, alors M est d'ordre 9 dont les facteurs invariants sont

$$d_9 = (\lambda-3)(\lambda-1)^2(\lambda-2)^3,\ d_8 = (\lambda-1)(\lambda-2)^2, d_7 = d_6 = \lambda-1, d_5 = d_4 = d_3 = d_2 = d_1 = 1.$$

(3) Considérons un bloc de Jordan $J_n(\lambda_0)$ avec $\lambda_0 \in K$. Comme

$$\begin{vmatrix} 1 & \lambda_0-\lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda_0-\lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \lambda_0-\lambda \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{vmatrix}_{(n-1)\times(n-1)}$$

est un mineur d'ordre $n-1$ de $J_n(\lambda_0)-\lambda I_n$, on a $\Delta_{n-1}(J_n(\lambda_0)-\lambda I_n) = 1$, et par conséquent, $\Delta_i(J_n(\lambda_0) - \lambda I_n) = 1,\ i = 1, 2, \ldots, n-1$. En outre, $\Delta_n(J_n(\lambda_0)) = (\lambda-\lambda_0)^n$. D'après le théorème 3.1.11(2), les facteurs invariants de $J_n(\lambda_0)$ sont $\{1, \ldots, 1, (\lambda-\lambda_0)^n\}$. D'où, $(\lambda-\lambda_0)^n$ est le seul facteur élémentaire de $J_n(\lambda_0)$.

Plus généralement, on a le résultat suivant.

4.8. Lemme. Si

$$J = \begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{n_2}(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{n_r}(\lambda_r) \end{pmatrix},$$

alors les facteurs élémentaires de J sont $(\lambda-\lambda_1)^{n_1}, (\lambda-\lambda_2)^{n_2}, \cdots, (\lambda-\lambda_r)^{n_r}$.

Démonstration. On a vu que le résultat est vrai pour $r = 1$. Supposons que $r > 1$ et le résultat est vrai pour $r-1$. Échangeant des blocs diagonaux si nécesseaire, on peut supposer que $n_1 \leq n_i$ pour tout $1 < i \leq r$. Posons $J' = \text{diag}\{J_{n_2}(\lambda_2), \ldots, J_{n_r}(\lambda_r)\}$. Par l'hypothèse de récurrences, les facteurs élémentaires de J' sont $(\lambda-\lambda_2)^{n_2}, \cdots, (\lambda-\lambda_r)^{n_r}$. Soient

$d_1(\lambda), \cdots, d_s(\lambda)$ les facteurs invariants normalisés de J'. Alors $(\lambda-\lambda_2)^{n_2}, \cdots, (\lambda-\lambda_r)^{n_r}$ sont les facteurs primaires de $d_i(\lambda)$, $i = 1, \cdots, s$, et $J' - \lambda I$ se réduit à $\mathrm{diag}\{d_1(\lambda), \cdots, d_s(\lambda)\}$. En outre, comme les facteurs invariants de $J_{n_1}(\lambda_1)$ sont $1, \cdots, 1, (\lambda - \lambda_1)^{n_1}$, la matrice $J_{n_1}(\lambda_1) - \lambda I_{n_1}$ se réduit à la matrice $\mathrm{diag}\{1, \cdots, 1, (\lambda - \lambda_1)^{n_1}\}$. Par conséquent, $J - \lambda I = \mathrm{diag}\{J_{n_1}(\lambda_1) - \lambda I_{n_1}, J' - \lambda I\}$ se réduit à $D = \mathrm{diag}\{1, \cdots, 1, (\lambda - \lambda_1)^{n_1}, d_1(\lambda), \cdots, d_s(\lambda)\}$.

Supposons que $(\lambda - \lambda_1) \mid d_1(\lambda)$. Alors $d_1(\lambda) = (\lambda - \lambda_i)^{n_i} p(\lambda)$, où $2 \leq i \leq r$ avec $\lambda_i = \lambda_1$ et $p(\lambda) \in K[\lambda]$. Comme $n_1 \leq n_i$ par l'hypothèse, on a $(\lambda - \lambda_1)^{n_1} \mid d_1(\lambda)$. Ainsi D est une matrice de Smith sur $K[\lambda]$. Par conséquent, les facteur élémentaires de J sont $(\lambda-\lambda_1)^{n_1}$ plus les facteurs primaires de $d_i(\lambda)$, $i = 1, \ldots, s$, c'est-à-dire, $(\lambda-\lambda_1)^{n_1}, (\lambda-\lambda_2)^{n_2}, \ldots, (\lambda-\lambda_r)^{n_r}$.

Supposons maintenant que $(\lambda - \lambda_1) \nmid d_1(\lambda)$. Soit j avec $1 \leq j \leq s$ l'indice maximal tel que $\lambda - \lambda_1 \nmid d_j(\lambda)$. Alors $(\lambda - \lambda_1)^{n_1}$ et $d_j(\lambda)$ sont co-premiers. D'après le lemme 3.1.9, D se réduit à $D_1 = \mathrm{diag}\{1, \cdots, 1, 1, d_1(\lambda), \cdots, d_{j-1}(\lambda), d_j(\lambda)(\lambda - \lambda_1)^{n_1}, d_{j+1}(\lambda), \ldots, d_s(\lambda)\}$. Si $j = s$, alors D_1 est évidemment une matrice de Smith sur $K[\lambda]$. Sinon, $(\lambda - \lambda_1) \mid d_{j+1}(\lambda)$, d'après la maximalité de j. Ainsi $d_{j+1}(\lambda) = q(\lambda)(\lambda - \lambda_i)^{n_i}$, où $2 \leq i \leq r$ tel que $\lambda_i = \lambda_1$. Comme $d_j(\lambda)$ divise $d_{j+1}(\lambda)$ et co-premier à $\lambda - \lambda_1$, on a $d_j(\lambda) \mid q(\lambda)$. En outre, $n_1 \leq n_i$ par l'hypothèse. D'où, $d_j(\lambda)(\lambda - \lambda_1)^{n_1} \mid d_{j+1}(\lambda)$. Ainsi D_1 est une matrice de Smith. Par conséquent, les facteurs élémentaires de J sont $(\lambda-\lambda_1)^{n_1}$ plus les facteurs primaires de $d_i(\lambda)$, $i = 1, \cdots, s$, c'est-à-dire, $(\lambda-\lambda_1)^{n_1}, (\lambda-\lambda_2)^{n_2}, \ldots, (\lambda-\lambda_r)^{n_r}$. Ceci achève la démonstration.

4.9. Lemme. Si M, N deux matrices carrées sembalables sur K, alors M, N ont les mêmes facteurs invariants ainsi que les mêmes facteurs élémentaires.

Démonstration. Par hypothèse, $N = P^{-1}MP$ avec P une matrice inversible sur K. Ainsi $N - \lambda I_n = P^{-1}(M - \lambda I_n)P$. D'après le corollaire 3.1.12, $N - \lambda I_n$ sont $M - \lambda I_n$ équivalentes, et donc elles ont la même forme canonique de Smith. C'est-à-dire, M, N ont les mêmes facteurs invariants, et donc ont les mêmes facteurs élémentaires. Ceci achève la démonstration.

4.10. Théorème. Si $M \in M_n(K)$, alors

$$\begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{n_2}(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{n_r}(\lambda_r) \end{pmatrix}$$

est une forme canonique de Jordan de M si et seulement si $(\lambda-\lambda_1)^{n_1}, (\lambda-\lambda_2)^{n_2}, \ldots, (\lambda-\lambda_r)^{n_r}$ sont les facteurs élémentaires de M. Par conséquent, la forme canonique de Jordan de M est unique à permutation de blocs diagonaux près.

Démonstration. La necessité se découle des lemmes 4.8 et 4.9. Supposons maintenant que $(\lambda - \lambda_1)^{n_1}, (\lambda - \lambda_2)^{n_2}, \ldots, (\lambda - \lambda_r)^{n_r}$ sont les facteurs élémentaires de M. D'après le corollaire 4.6, M est semblable à une matrice de Jordan comme suit:

$$J = \begin{pmatrix} J_{m_1}(\mu_1) & 0 & \cdots & 0 \\ 0 & J_{m_2}(\mu_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{m_s}(\mu_s) \end{pmatrix}.$$

D'après les lemmes 4.8 et 4.9, $(\lambda - \mu_1)^{m_1}, (\lambda - \mu_2)^{m_2}, \ldots, (\lambda - \mu_s)^{m_s}$ sont les facteurs élémentaires de M. Par conséquent, $s = r$, et on peut réarrange les indices de sorte que $\mu_i = \lambda_i$ et $n_i = m_i$, $i = 1, 2, \ldots, r$. Ceci achève la démonstration.

Exemple. (1) Soit

$$M = \begin{pmatrix} 1 & 1 & 1 \\ -2 & -2 & -2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Comme

$$\begin{pmatrix} 1-\lambda & 1 & 1 \\ -2 & -2-\lambda & -2 \\ 1 & 1 & 1-\lambda \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 1 & 1-\lambda \\ 0 & -\lambda & -2\lambda \\ 0 & \lambda & \lambda(\lambda-2) \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\lambda & -2\lambda \\ 0 & 0 & \lambda^2 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2 \end{pmatrix},$$

les facteurs élémentaires de M sont λ, λ^2. D'où, la forme canonique de Jordan de M est

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

(2) Soit

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On voit que les facteurs élémentaires de M sont $\lambda - 2$ et $(\lambda - 1)^2$. Ainsi la forme canonique de Jordan de M est

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Le résultat suivant est une conséquence immédiate du théorème 4.9.

4.11. Corollaire. Une matrice carrée sur K est diagonalisable si et seulement si ses facteurs élémentaires sont tous de degré un.

Le résultat suit du théorème 4.9 et le lemme 4.10.

4.12. Corollaire. Soient M, N deux matrices carrées de même ordre sur K. Les conditions sont équivalentes:

(1) M, N sont semblables.

(2) M, N ont les mêmes facteurs invariants.

(3) M, N ont les mêmes facteurs élémentaires.

Soit $M \in M_n(K)$. Rappelons que le polynôme minimal de M est l'annulateur normalisé de M dont le degré est le plus petit parmi les degrés des annulateurs de M. Il est bien connu que le polynôme minimal de M divise tous les annulateurs de M et que deux matrices semblables ont le même polynôme minimal.

4.13. Théorème. Le polynôme minimal de $M \in M_n(K)$ coïncide avec le plus grand facteur invariant de M.

Démonstration. Soit $m(\lambda)$ le polynôme minimal de M. Supposons que $d_1(\lambda), \ldots, d_n(\lambda)$ sont les facteurs invariants de M. On décompose

$$d_n(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_r)^{n_r},$$

où les λ_i sont les éléments deux à deux distincts de K et $n_i > 0$. D'après la définition, pour tout $1 \leq i \leq r$, il existe des entiers $n_{i1}, \cdots, n_{i,s_i}$ avec $0 < n_{i1} \leq \cdots \leq n_{i,s_i} = n_i$ tels que les facteurs élémentaires de M sont

$$\{(\lambda - \lambda_i)^{n_{ij}} \mid j = 1, \cdots, s_i; i = 1, \cdots, r\}.$$

D'après le théorème 4.10, M est semblable à la matrice de Jordan suivante:

$$J = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & J_r \end{pmatrix},$$

où $J_i = \operatorname{diag}\{J_{n_{i1}}(\lambda_i), \cdots, J_{n_{i,s_i}}(\lambda_i)\}$, $i = 1, \cdots, r$. Comme $J_{n_{ij}}(\lambda_i) - \lambda_i I_{n_{ij}}$ est nipotente d'indice n_{ij}, pour $j = 1, \ldots, s_i$, la matrice $J_i - \lambda_i I$ est nilpotente d'indice n_i. Mais $J_j - \lambda_i I$ est inversible lorsque $j \neq i$. D'où, $(J - \lambda_i I)^{n_i - 1} = \operatorname{diag}\{M_{i1}, \cdots, M_{ir}\}$, où $M_{ii} \neq 0$ et les M_{ij} avec $j \neq i$ sont tous inversibles, et $(J - \lambda_i I)^{n_i} = \operatorname{diag}\{N_{i1}, \cdots, N_{ir}\}$, où $N_{ii} = 0$ et les N_{ij} avec $j \neq i$ sont tous inversibles, Donc

$$(J - \lambda_1 I)^{n_1} \cdots (J - \lambda_r I)^{n_r} = \begin{pmatrix} N_{11}N_{21}\cdots N_{r1} & 0 & \cdots & 0 \\ 0 & N_{12}N_{22}\cdots N_{r2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & N_{1r}N_{2r}\cdots N_{rr} \end{pmatrix} = 0.$$

Ceci implique $d_n(J) = 0$. Ainsi le polynôme minimal de J est un facteur de $d_n(\lambda)$. En outre,

$(J-\lambda_1 I)^{n_1-1}(J-\lambda_2 I)^{n_2} \cdots (J-\lambda_r I)^{n_r} =$

$$\begin{pmatrix} M_{11}N_{21}\cdots N_{r1} & 0 & \cdots & 0 \\ 0 & M_{12}N_{22}\cdots N_{r2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & M_{1r}N_{2r}\cdots N_{rr} \end{pmatrix}$$

est non nul, puisque $M_{11}N_{21}\cdots N_{r1} \neq 0$. Ceci implique $(\lambda-\lambda_1)^{n_1-1}(\lambda-\lambda_2)^{n_2}\cdots(\lambda-\lambda_r)^{n_r}$ n'annule pas J. De même, on voit que $\dfrac{d_n(\lambda)}{\lambda-\lambda_i}$ ne l'annule pas non plus, pour $i=2,\ldots,r$. Ceci montre que $d_n(\lambda)$ est le polynôme minimal de J. La preuve s'achève.

Exemple. Soit

$$J = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On a vu que les facteurs invariants de J sont $\{1, 1, (\lambda-2)(\lambda-1)^2\}$. Ainsi le polynôme minimal de J est $(\lambda-2)(\lambda-1)^2$.

Le résultat suivant est utile dans la calcul pratique.

4.14. Lemme. Si

$$M = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

avec B et C sont des matrice carrées sur K, alors les facteurs élémentaires de M sont les facteurs élémentaires de B plus ceux-ci de C.

Démonstration. Soient $(\lambda-\lambda_1)^{n_1},\cdots,(\lambda-\lambda_r)^{n_r}$ les facteurs élémentaires de B, et $(\lambda-\mu_1)^{m_1},\cdots,(\lambda-\mu_s)^{m_s}$ ceux de C. D'après le théorème 4.10, B, C sont semblables respectivement à des matrices de Jordan suivantes:

$$J_1 = \begin{pmatrix} J_{n_1}(\lambda_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & J_{n_r}(\lambda_r) \end{pmatrix}, \quad J_2 = \begin{pmatrix} J_{m_1}(\mu_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & J_{m_s}(\mu_s) \end{pmatrix}.$$

Remarquons que M est semblable à la matrice de Jordan suivante:

$$J = \begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix}.$$

D'après le lemme 4.9 et le théorème 4.10, on voit que les facteurs élémentaires de M sont $(\lambda-\lambda_1)^{n_1},\cdots,(\lambda-\lambda_r)^{n_r}$, $(\lambda-\mu_1)^{m_1},\cdots,(\lambda-\mu_s)^{m_s}$. Ceci achève la démonstration.

Exemple. Trouver la forme canonique de Jordan de la matrice suivante:

$$M=\begin{pmatrix}1&1&1&0&0&0\\0&2&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&1&1\\0&0&0&-2&-2&-2\\0&0&0&1&1&1\end{pmatrix}.$$

Démonstration. Considérons les matrices suivantes:

$$B=\begin{pmatrix}1&1&1\\0&2&0\\0&0&1\end{pmatrix},\ C=\begin{pmatrix}1&1&1\\-2&-2&-2\\1&1&1\end{pmatrix}.$$

On a vu que les facteurs élémentaires de B sont $\lambda-2$ et $(\lambda-1)^2$, et ceux-ci de C sont λ,λ^2. Ainsi les facteurs élémentaires de M sont $\lambda-2,(\lambda-1)^2,\lambda,\lambda^2$. Par conséquent, la forme canonique de Jordan de M est

$$\begin{pmatrix}0&0&0&0&0&0\\0&2&0&0&0&0\\0&0&1&0&0&0\\0&0&1&1&0&0\\0&0&0&0&0&0\\0&0&0&0&1&0\end{pmatrix}.$$

4.15. Exercices

1. Soit E un espace vectoriel sur un corps K de dimension $n>1$. Si f est un K-endomorphisme de E, montrer que f est nilpotent d'indice n (c'est-à-dire, $f^n=0$ mais $f^{n-1}\neq 0$) si et seulement si E admet une K-base dans laquelle la matrice de f est

$J_n(0)$. *Indication*: Pour la nécessité, vérifier que si $v \in E$ est tel que $f^{n-1}(v) \neq 0_E$, alors $\{v, f(v), \cdots, f^{n-1}(v)\}$ est une K-base de E.

2. Soit f l'endomorphisme de l'espace réel $\mathbb{R}^3$ défini par

$$f(x, y, z) = (3x + 5y - 2z, -2x - 3y + z, -x - y).$$

Vérifier que f est nilpotent d'indice 3 et trouver une base de $\mathbb{R}^3$ dans laquelle la matrice de f est $J_3(0)$.

3. Trouver les facteurs élémentaires de chacune de matrices complexes suivantes.

$$(1) \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 1 & 1 \end{pmatrix}; \qquad (2) \quad \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

4. Soient K un corps algébriquement clos et $M \in M_n(K)$. Montrer les énoncés suivants.
   (1) Le polynôme caractéristique de M est associé au produit des facteurs élémentaires de M. Par conséquent, la racine d'un facteur élémentaire est une valeur propre.
   (2) M est nilpotente si et seulement si M est semblable à une matrice de Jordan suivante:

$$\begin{pmatrix} J_{n_1}(0) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & J_{n_r}(0) \end{pmatrix}.$$

5. Soit P une matrice complexe carrée d'ordre n. Montrer que le plus petit facteur invariant de P est non constant si et seulement si $P = aI_n$, où $a \in \mathbb{C}$ et I_n est la matrice identité d'ordre n.

6. Soit $M \in M_6(\mathbb{C})$ dont le polynôme minimal est $(\lambda - 2)^2(\lambda - 3)(\lambda - 4)$. Donner toutes les possibiltés de la forme canonique de Jordan de M.

7. Montrer que les matrices complexes suivantes sont semblables.

$$M = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

8. Donner, à l'aide du numéro 6(1), toutes les possibiltés de facteurs élémentaires des matrices complexes ayant les polynômes caractéristiques suivants:

   (1) $(1-\lambda)^3(2-\lambda)^2$; (2) $(-3-\lambda)^4(1-\lambda)^2$.

9. Soient K un corps algébriquement clos et $M \in M_n(K)$. Montrer les énoncés suivants:

   (1) M est diagonalisable sur K si et seulement si le polynôme minimal de M n'a aucune racine multiple. *Rappel*: $a \in K$ est racine multiple de $p(\lambda)$ si $(\lambda - a)^2 \mid p(\lambda)$.

   (2) M est semblable à un bloc de Jordan si et seulement si M est indécomposable, c'est-à-dire, M n'est semblable à aucune matrice de la forme

$$\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix},$$

   où B, C sont des matrices carrées.

10. Calculer le polynôme minimal de M et en déduire qu'elle est diagonalisable, où

$$M = \begin{pmatrix} 2 & 1 & 1 & -1 \\ 1 & 2 & 1 & -1 \\ 1 & 1 & 2 & -1 \\ -1 & -1 & -1 & 2 \end{pmatrix}.$$

11. Trouver la forme canonique de Jordan de la matrice suivante.

$$\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}.$$

12. Montrer que les matrices suivantes sont semblables.

$$\begin{pmatrix} 2 & -1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

13. Discuter, selon les valeurs de a, b, la forme canonique de Jordan de la matrice suivante:

$$\begin{pmatrix} -1 & a & b \\ 0 & 3 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$