MODULES DE TYPE FINI SUR UN ANNEAU PRINCIPAL

JEAN-MARC COUVEIGNES

RÉSUMÉ. On expose la théorie classique des modules de type fini sur un anneau principal.

TABLE DES MATIÈRES

Soit A un anneau principal (donc intègre donc commutatif). Il est possible de classifier les modules de type fini sur A. On commence par étudier les sous-modules d'un module libre de type fini.

1. SOUS-MODULES D'UN MODULE LIBRE DE TYPE FINI

On montre d'abord que les sous-modules d'un module libre de type fini sont libres.

Théorème 1. *Soit A un anneau principal. Soit r un entier positif et M un A-module libre de rang r. Soit N un sous-module de M. Alors N est un A-module libre de rang $\leqslant r$.*

La démonstration se fait par récurrence sur le rang r de M. Si $r = 1$ soit b une base de M. L'application linéaire $\varphi : x \mapsto x.b$ est une bijection de A sur M. L'image inverse de N par φ est un idéal de A. Soit a un générateur de cet idéal. On vérifie que $N = Aa.b$ ce qui prouve le théorème dans ce cas.

Supposons que $r > 1$. Soit $\hat{M} = \mathrm{Hom}(M, A)$ le dual de M. Soit $(b_1, \ldots, b_r)$ une base de M. Pour tout i tel que $1 \leqslant i \leqslant r$ on définit une forme linéaire $\varphi_i : M \to A$ par

$$\varphi_i\Big(\sum_{1 \leqslant j \leqslant r} a_j.b_j\Big) = a_i.$$

Date: 2 octobre 2018.

Les $(\varphi_i)_{1\leqslant i\leqslant r}$ forment une base de $\hat{M}$. Ce sont les formes coordonnées associées à la base $(b_i)_{1\leqslant i\leqslant r}$. Le noyau de φ_r est $K = Ab_1 \oplus \cdots \oplus Ab_{r-1}$. L'image de N par φ_r est un idéal de A. Soit $a \in A$ un générateur de cet idéal. Si $a = 0$ alors $N \subset K$ et l'hypothèse de récurrence permet de conclure car le rang de K est $r-1$. Supposons donc que $a \neq 0$. Soit $n \in N$ tel que $\varphi_r(n) = a$.

On vérifie que

$$N = (K \cap N) \oplus An.$$

D'une part, si $x \in N$ alors $\varphi_r(x) = ac$ avec $c \in A$. On pose $y = x - cn$ et on vérifie que $x = y + cn$ et $y \in K \cap N$ et $cn \in An$. D'autre part si x appartient à l'intersection $An \cap (K \cap N)$ alors $x = cn$ pour un $c \in A$ et $\varphi_r(x) = 0 = c\varphi_r(n) = ca$. Comme $a \neq 0$ on en déduit que $c = 0$ donc $x = 0$.

On peut appliquer l'hypothèse de récurrence à $K \cap N$ qui est un sous-module du module K, libre de rang $r-1$. Ainsi $K \cap N$ est libre de rang $\leqslant r-1$. Donc la somme directe $N = (K \cap N) \oplus An$ est libre elle aussi et de rang $\leqslant r$. □

On peut maintenant énoncer un résultat plus précis.

Théorème 2 (Théorème de la base adaptée)**.** *Soit A un anneau principal. Soit r un entier positif et M un A-module libre de rang r. Soit N un sous-module de M. Il existe une base $(b_1, \ldots, b_r)$ de M et des éléments $a_1, \ldots, a_r$ de A tels que $a_1A \supset a_2A \supset \cdots \supset a_rA$ et*

$$N = Aa_1.b_1 \oplus \cdots \oplus Aa_r.b_r.$$

Notons que les derniers a_i peuvent être nuls.

La demonstration se fait par récurrence sur le rang r de M. Si $r = 1$ soit b_1 une base de M. L'application linéaire $\varphi : x \mapsto x.b_1$ est une bijection de A sur M. L'image inverse de N pas φ est un idéal de A. Soit a_1 un générateur de cet idéal. On vérifie que $N = Aa_1.b_1$ ce qui prouve le théorème dans ce cas.

Supposons que $r > 1$. Soit $\hat{M}$ le dual de M. À tout couple (φ, n) dans $(\hat{M}, N)$ on associe l'idéal $\varphi(n)A$.

L'ensemble $\mathcal{V}$ des idéaux ainsi obtenus, ordonné par l'inclusion, satisfait les hypothèses du lemme de Zorn. En effet, soit $(\varphi_i, n_i)_{i\in I}$ dans $(\hat{M}, N)^I$ tel que la famille d'idéaux $\mathcal{I} = (\varphi_i(n_i)A)_{i\in I}$ soit totalement ordonnée pour l'inclusion. Appelons U l'union de ces idéaux. C'est un idéal de A.

En effet, si x et y sont dans U il existe i et j dans I tels que $x \in \varphi_i(n_i)A$ et $y \in \varphi_j(n_j)A$. Comme la famille $\mathcal{I}$ est totalement ordonnée, l'un des deux idéaux $\varphi_i(n_i)A$ et $\varphi_j(n_j)A$ contient l'autre. Il contient donc x et y et donc aussi leurs combinaisons linéaires.

L'idéal U est principal. Soit a un générateur de U. Il existe un o dans I tel que $a \in \varphi_o(n_o)A$. Comme $\varphi_o(n_o)$ est un multiple de a et a est un multiple de $\varphi_o(n_o)$ il existe une unité u telle que $a = u\varphi_o(n_o)$. L'idéal $aA = (u\varphi_o)(n_o)A$ appartient à $\mathcal{V}$ et il contient tous les $\varphi_i(n_i)A$. Donc les $(\varphi_i(n_i)A)_{i\in I}$ ont un majorant dans $\mathcal{V}$.

Donc toute chaîne de $\mathcal{V}$ est majorée dans $\mathcal{V}$.

L'application du lemme de Zorn nous donne un idéal maximal $\varphi_1(n_1)A$ parmi les $\varphi(n)A$. On pose

$$a_1 = \varphi_1(n_1).$$

Si a_1 est nul alors N est nul et le résultat est trivial. On suppose donc que a_1 est non-nul.

On montre que l'image de N par φ_1 est l'idéal a_1A. Sinon il existe un $n \in N$ tel que $\varphi_1(n)$ n'est pas dans a_1A. Soit c un générateur de $\varphi_1(n)A + a_1A$. Soient $\lambda, \mu \in A$ tels que $\lambda\varphi_1(n) + \mu a_1 = c$. On vérifie que $c = \varphi_1(\lambda n + \mu n_1)$ engendre un idéal strictement plus grand que a_1A. Contradiction.

On verifie de même que pour tout forme linéaire $\psi \in \hat{M}$, la valeur $\psi(n_1)$ de ψ en n_1 est dans a_1A. Sinon il existe un $\psi \in \hat{M}$ tel que $\psi(n_1)$ n'est pas dans a_1A. Soit c un générateur de $\psi(n_1)A + a_1A$. Soient $\lambda, \mu \in A$ tels que $\lambda\psi(n_1) + \mu a_1 = c$. On vérifie que $c = (\lambda\psi + \mu\varphi_1)(n_1)$ engendre un idéal strictement plus grand que a_1A. Contradiction.

En particulier, toutes les formes coordonnées associées à une base de M prennent en n_1 des valeurs divisibles par a_1. On peut donc écrire

$$n_1 = a_1.b_1$$

avec $b_1 \in M$.

On vérifie que $a_1(\varphi_1(b_1) - 1) = 0$. Donc

$$\varphi_1(b_1) = 1$$

puisque a_1 est non-nul et A intègre.

On montre alors que

$$M = \mathrm{Ker}(\varphi_1) \oplus Ab_1.$$

En effet, tout x de M s'écrit $x = (x - \varphi_1(x)b_1) + \varphi_1(x)b_1$. Et si x appartient à l'intersection $Ab_1 \cap \mathrm{Ker}(\varphi_1)$ alors $x = a.b_1$ pour un $a \in A$ et $\varphi_1(x) = 0 = a\varphi_1(b_1) = a$. Donc $x = 0$.

On montre de même que

$$N = (N \cap \mathrm{Ker}(\varphi_1)) \oplus Aa_1.b_1.$$

En effet, tout x de N s'écrit $x = (x - \varphi_1(x)b_1) + \varphi_1(x)b_1$. Et $\varphi_1(x)$ est un multiple de a_1. On pose alors $\varphi_1(x) = a_1c$ avec c dans A. Donc $x = (x - cn_1) + cn_1$ avec $n_1 = a_1.b_1$. Et si x appartient à l'intersection $An_1 \cap (N \cap \mathrm{Ker}(\varphi_1))$ on a déjà montré qu'il est nul.

Le sous-module $K = \mathrm{Ker}(\varphi_1)$ est libre d'après le théorème 1. Comme $M = K \oplus Ab_1$ et $b_1 \neq 0$, le rang de K est $r - 1$. Le module $L = N \cap K$ est un sous-module de K. D'après l'hypothèse de récurrence il existe une base $b_2, \ldots, b_r$ de K et des scalaires $a_2, \ldots, a_r$ tels que $a_2A \supset a_3A \supset \cdots \supset a_rA$ et $L = Aa_2.b_2 \oplus \cdots \oplus Aa_r.b_r$.

Donc $b_1, \ldots, b_r$ est une base de M et $N = Aa_1.b_1 \oplus Aa_2.b_2 \oplus \cdots \oplus Aa_r.b_r$.

Il reste à montrer que $a_1A \supset a_2A$. Dans le cas contraire, soit c un générateur de l'idéal engendré par a_1 et a_2. Il existe λ et μ tels que $\lambda a_1 + \mu a_2 = c$. Soient $\beta_1, \ldots, \beta_r$ les formes coordonnées de M associées à la base $b_1, \ldots, b_r$. On vérifie que $(\lambda\beta_1 + \mu\beta_2)(a_1b_1 + a_2b_2) = c$. Donc l'idéal engendré par $(\lambda\beta_1 + \mu\beta_2)(a_1b_1 + a_2b_2)$ est strictement plus grand que l'idéal engendré par $\varphi_1(n_1)A$. Contradiction. □

2. Modules de type fini sur un anneau principal

Soit A un anneau principal. Le théorème suivant décrit les A-modules de type fini.

Théorème 3. *Soit A un anneau principal et M un A-module de type fini. Il existe un entier $r \geqslant 0$ et un entier $m \geqslant 0$ et des scalaires $a_1, \ldots, a_m$ dans A non-nuls et non-inversibles tels que $a_1|a_2|\ldots|a_m$ et $M \simeq A^r \times A/a_1A \times \cdots \times A/a_mA$.*

On choisit des générateurs $x_1, \ldots, x_n$ de M. Soit $f : A^n \to M$ l'application linéaire définie par $f((a_i)_{1\leqslant i\leqslant n}) = \sum_{1\leqslant i\leqslant n} a_i x_i$. Le noyau K de f est le module des relations entre les x_i. Le quotient A^n/K est isomorphe à M. On applique le théorème 2 à $K \subset A^n$. On obtient une base $b_1, \ldots, b_n$ de A^n et des scalaires $\alpha_1, \ldots, \alpha_n$ tels que $\alpha_1 A \supset \alpha_2 A \supset \cdots \supset \alpha_n A$ et $K = \oplus_{1\leqslant i\leqslant n} \alpha_i . b_i$. Soit s le plus grand des entiers i tels que α_i soit une unité. Si aucun des α_i n'est une unité on pose $s = 0$. Soit t le plus grand des entiers i tels que α_i soit non-nul. On pose $m = t - s$ et $r = n - t$ et $a_1 = \alpha_{s+1}, \ldots, a_m = \alpha_t$. On a bien $M \simeq A^r \times A/a_1 A \times \cdots \times A/a_m A$. □

On obtient donc une décomposition de M comme produit d'un sous-module libre et d'un sous module de torsion. Le sous-module de torsion est bien défini. C'est l'ensemble M_{tors} des $x \in M$ tels que $\mathrm{Ann}(x) \neq \{0\}$.

En revanche, le facteur libre A^r n'est pas unique. Le sous-module de torsion peut avoir plusieurs supplémentaires dans M.

La première application du théorème 3 est la classification des groupes commutatifs de type fini. En effet, un groupe commutatif n'est autre qu'un $\mathbf{Z}$-module et il est de type fini comme groupe si et seulement s'il est de type fini comme $\mathbf{Z}$-module. Comme l'anneau $\mathbf{Z}$ est principal on en déduit le théorème suivant.

Théorème 4. *Tout groupe commutatif G de type fini s'écrit*

$$\mathbf{Z}^r \times (\mathbf{Z}/a_1\mathbf{Z}) \times (\mathbf{Z}/a_2\mathbf{Z}) \times \cdots \times (\mathbf{Z}/a_m\mathbf{Z})$$

avec $a_1 | a_2 | \ldots | a_m$.

La classe d'isomorphismes de G est caractérisée par $(r, a_1, \ldots, a_m)$.

Exercice 1 : Décrivez (à isomorphisme près) tous les groupes finis commutatifs de cardinal 16.

Exercice 2 : Décrivez (à isomorphisme près) tous les groupes finis commutatifs de cardinal 36.

Exercice 3 : Soit A un anneau principal et M un A-module libre de type fini. Soit N un sous-module de M. Montrer que N admet un supplémentaire dans M si et seulement si le quotient M/N est sans-torsion.

Notons d'abord que M est libre sur un anneau intègre, donc sans-torsion. On note r le rang de M. Notons aussi que si $a \in A$, le quotient A/aA est sans-torsion si et seulement si $a = 0$ ou a est une unité.

Supposons que N admet un supplémentaire P dans M. Donc $M = N \oplus P$. Le module quotient M/N est isomorphe à P, qui est sans torsion car il est contenu dans M.

Supposons maintenant que M/N est sans-torsion. Soit $(b_1, \ldots, b_r)$ une base adaptée à $N \subset M$. On a $N = \oplus_{1\leqslant i\leqslant r} A a_i . b_i$ et $a_1 A \supset a_2 A \supset \cdots \supset a_r A$. Donc $M/N \simeq \oplus_{1\leqslant i\leqslant r} A/a_i A$. Puisque M/N est sans torsion, tous les a_i sont soit nuls soit inversibles. On suppose que les s premiers a_i sont inversibles. Donc les $r - s$ derniers a_i sont nuls et $N \simeq A^s$ est libre.

Exercice 4 : Soit $A = \mathbf{Z}$ et $M = (\mathbf{Z}/3\mathbf{Z}) \oplus \mathbf{Z}$.

1. Calculer M_{tors}.

Soit $m = (x \bmod 3, y)$ dans M. Si y est non-nul alors $n.m$ est non-nul pour tout n non-nul dans $\mathbf{Z}$. Si y est nul alors $3.m = 0$. Donc la torsion de M est $(\mathbf{Z}/3\mathbf{Z}) \oplus \{0\} \subset (\mathbf{Z}/3\mathbf{Z}) \oplus \mathbf{Z}$.

2. Soit S un supplémentaire de M_{tors} dans M. Montrer que la restriction à S de la projection sur le second facteur $\pi_2 : M = (\mathbf{Z}/3\mathbf{Z}) \oplus \mathbf{Z} \to \mathbf{Z}$ est une bijection.

Si $s \in S$ et $\pi_2(s) = 0$ alors $s \in S \cap M_{\text{tors}} = \{0\}$ donc π_2 est injective.
Soit $n \in \mathbf{Z}$ et soit $m = (0 \bmod 3, n) \in M = (\mathbf{Z}/3\mathbf{Z}) \oplus \mathbf{Z}$. On écrit $m = (0 \bmod 3, n) = t + s$ avec $t \in M_{\text{tors}}$ et $s \in S$. Et t s'écrit $(u \bmod 3, 0) \in M$. Donc $s = m - t = (-u \bmod 3, n)$ est envoyé sur n par π_2. Donc π_2 est surjective.

3. Donner tous les supplémentaires de M_{tors} dans M.

Soit S un tel supplémentaire. On vient de montrer que S est un module libre de rang 1. Un générateur de S est par exemple l'unique élément de S qui est envoyé sur 1 par π_2. Il s'écrit $(u \bmod 3, 1)$ avec $u \in \mathbf{Z}/3\mathbf{Z}$. Il y a donc trois supplémentaires.

Exercice 5 : Soit A un anneau principal, $r \geqslant 0$ un entier, $m \geqslant 0$ un entier et $a_1, \ldots, a_m$ des scalaires non-nuls et non-inversibles dans A tels que $a_1 A \supset a_2 A \supset \cdots \supset a_m A$. Soit M le A-module $A^r \times A/a_1 A \times \cdots \times A/a_m A$.

1. Montrer que si $r \geqslant 1$ alors l'annulateur $\mathrm{Ann}(M)$ de M est l'idéal nul de A.

2. On suppose que $r = 0$ et $m \geqslant 1$. Montrer que $\mathrm{Ann}(M) = a_m A$.

Exercice 6 : Soit A un anneau principal et p un élément irréductible de A. Soit $m \geqslant 0$ un entier. Soient $a_1, \ldots, a_m$ des scalaires dans A, tous non-nuls et non-inversibles. Soit M le module $A/a_1 A \times \cdots \times A/a_m A$. Soit $k \geqslant 0$ un entier. On rappelle que $p^k M$ est l'image de la multiplication par p^k

$$[p^k] : \qquad M \longrightarrow M$$

$$m \longmapsto p^k.m.$$

On note $p^k M(p)$ la p-torsion de $p^k M$. On a vu que c'est un espace vectoriel sur $K = A/pA$.

Montrer que la dimension de cet espace vectoriel est égale au nombre de a_i qui sont divisibles par p^{k+1}.

Tout d'abord $p^k M = p^k(A/a_1 A) \times p^k(A/a_2 A) \times \cdots \times p^k(A/a_m A)$.
Ensuite $p^k M(p) = p^k(A/a_1 A)(p) \times p^k(A/a_2 A)(p) \times \cdots \times p^k(A/a_m A)(p)$.

Pour tout scalaire $a \in A$ non-nul et non-inversible $p^k(A/aA) \simeq A/bA$ avec $b = a/\mathrm{pgcd}(a, p^k)$. Et $(A/bA)[p]$ est isomorphe à A/pA si p divise b et il est nul sinon. Donc $p^k(A/aA)[p]$ est isomorphe à A/pA si p^{k+1} divise b et il est nul sinon.

Donc $p^k M(p)$ est isomorphe à $\prod_{\substack{1 \leqslant i \leqslant r \\ p^{k+1} | a_i}} A/pA$.

Exercice 7 : Soit A un anneau principal et M un A-module de type fini. On a vu que la décomposition donnée par le théorème 3 n'est pas unique. On va montrer cependant que certaines quantités qui apparaissent dans cette décomposition sont caractéristiques de M.

Soient donc un entier $r \geqslant 0$ et un entier $m \geqslant 0$ et des scalaires $a_1, \ldots, a_m$ dans A non-nuls et non-inversibles tels que $a_1 | a_2 | \ldots | a_m$. On pose

$$M = A^r \times A/a_1A \times \cdots \times A/a_mA.$$

Soient $s \geqslant 0$ et $n \geqslant 0$ des entiers et soient $b_1, \ldots, b_n$ dans A des scalaires non-nuls et non-inversibles tels que $b_1 | b_2 | \ldots | b_m$. On pose

$$N = A^s \times A/b_1A \times \cdots \times A/b_nA.$$

On suppose que M et N sont isomorphes.

1. Montrer que $M/M_{\text{tors}} \simeq A^r$ et $N/N_{\text{tors}} \simeq A^s$.

2. En déduire que $r = s$.

On a supposé l'existence d'un isomorphisme de A-modules $f : M \to N$. Soit $g : N \to M$ l'application linéaire réciproque. On vérifie que $f(M_{\text{tors}}) \subset N_{\text{tors}}$ et $g(N_{\text{tors}}) \subset M_{\text{tors}}$. Donc l'application f passe au quotient et définit une application linéaire $F : M/M_{\text{tors}} \to N/N_{\text{tors}}$. De même l'application g passe au quotient et définit une application linéaire $G : N/N_{\text{tors}} \to M/M_{\text{tors}}$. On sait que $f \circ g$ est l'application identité de N. Donc $F \circ G$ est l'application identité de N/N_{tors}. Donc les quotients M/M_{tors} et N/N_{tors} sont isomorphes. Comme ce sont deux modules libres de rangs r et s respectivement on en déduit que $r = s$.

3. Montrer que $\mathrm{Ann}(M_{\text{tors}}) = A$ si $m = 0$ et $\mathrm{Ann}(M_{\text{tors}}) = a_mA$ sinon. Montrer que $\mathrm{Ann}(N_{\text{tors}}) = A$ si $n = 0$ et $\mathrm{Ann}(N_{\text{tors}}) = b_nA$ sinon. En déduire que $m > 0$ si et seulement si $n > 0$ et que dans ce cas il existe une unité u dans A telle que $a_m = ub_n$.

4. Soit p un irréductible de A. Soit $k \geqslant 1$ un entier. En utilisant l'exercice précédent montrer qu'il existe autant de a_i que de b_j qui soient divisibles par p^k :

$$\#\{i \in [1, m] \mid p^k | a_i\} = \#\{j \in [1, n] \mid p^k | b_j\}.$$

On remarque que $f(p^{k-1}M) \subset p^{k-1}N$ et $g(p^{k-1}N) \subset p^{k-1}M$. On note f_k la restriction de f à $p^{k-1}M$ et g_k la restriction de g à $p^{k-1}N$. Ce sont deux isomorphismes reciproques l'un de l'autre. On note φ_k la restriction de f à $p^{k-1}M(p)$ et γ_k la restriction de g à $p^{k-1}N(p)$. On vérifie que $\varphi_k(p^{k-1}M(p)) \subset p^{k-1}N(p)$ et $\gamma_k(p^{k-1}N(p)) \subset p^{k-1}M(p)$. Donc $p^{k-1}M(p)$ et $p^{k-1}N(p)$ sont deux A-modules isomorphes. Les applications φ_k et γ_k sont des isomorphismes de A-modules.

Comme $p^{k-1}M(p)$ et $p^{k-1}N(p)$ sont annulés par p on peut les voir comme de A/pA-espaces vectoriels. Les applications φ_k et γ_k sont des isomorphismes d'espaces vectoriels.

On note $\delta(p,k)$ la dimension du A/pA-espace vectoriel $p^{k-1}M(p)$. C'est aussi la dimension du A/pA-espace vectoriel $p^{k-1}N(p)$.

D'après l'exercice 6 la dimension de $p^{k-1}M(p)$ est le nombre de a_i qui sont divisibles par p^k. Et la dimension de $p^{k-1}N(p)$ est le nombre de b_j qui sont divisibles par p^k. Donc

$$\delta(p,k) = \#\{i \in [1,m] \mid p^k | a_i\} = \#\{j \in [1,n] \mid p^k | b_j\}.$$

5. En déduire que $m = n$ et que pour tout i il existe un unité u_i telle que $a_i = u_i b_i$. Les a_i sont donc définis à association près. On les appelle les **facteurs invariants** de M. Deux A-modules de type fini M et N sont isomorphes si et seulement si

— Les modules libres M/M_{tors} et N/N_{tors} ont le même rang,

— et les facteurs invariants de M et de N sont les mêmes.

Pour tout p et tout k on a $\delta(p,k) \leqslant m$ par définition. Si p divise a_1 alors $\delta(p,1) = m$. Donc m est le maximum des $\delta(p,1)$ quand p parcours l'ensemble des irréductibles de A.

De même, pour tout p et tout k on a $\delta(p,k) \leqslant n$ par définition. Si p divise b_1 alors $\delta(p,1) = n$. Donc n est le maximum des $\delta(p,1)$ quand p parcours l'ensemble des irréductibles de A.

On a donc montré que $m = n$.

On note $v_p : A \setminus \{0\} \to \mathbf{N}$ la valuation associée à p. On veut montrer que pour tout $1 \leqslant i \leqslant m$ les scalaires a_i et b_i sont associés. Il suffit de montrer que pour tout p irréductible et pour tout $1 \leqslant i \leqslant m$ les valuations $v_p(a_i)$ et $v_p(b_i)$ sont égales.

On observe d'abord que les applications $i \mapsto v_p(a_i)$ et $i \mapsto v_p(b_i)$ sont croissantes.

Supposons qu'il existe un i tel que $v_p(a_i) > v_p(b_i)$. On pose $\alpha = v_p(a_i)$.

On sait que p^α divise a_j pour tout $j \geqslant i$. Donc $\delta(p,\alpha) \geqslant m - i + 1$.

Mais p^α ne divise pas b_i. Donc le nombre de b_j divisibles par p^α est au plus $m - i$. Donc $\delta(p,\alpha) \leqslant m - i$. Contradiction.

Donc $v_p(a_i) \leqslant v_p(b_i)$ pour tout p et pour tout i.

On montre inégalité opposée de la même manière.

6. On suppose que $A = \mathbf{Z}$. Soit M un A-module de torsion de type fini. On suppose que l'annulateur de M est $2^5 3^3 \mathbf{Z}$.

On donne dans le tableau ci-dessous les dimensions des espaces vectoriels $p^k M(p)$ pour $p = 2$ et $p = 3$.

k	0	1	2	3	4	5
$\dim_{\mathbf{Z}/2\mathbf{Z}}(2^k M(2))$	3	2	2	2	1	0
$\dim_{\mathbf{Z}/3\mathbf{Z}}(3^k M(3))$	4	3	1	0	0	0

Donnez les facteurs invariants de M.

3. Diviseurs élémentaires

Soit A un anneau principal.

On rappelle que le sous-module de torsion M_{tors} d'un A-module M est l'ensemble des $x \in M$ tels que $\mathrm{Ann}(x) \neq \{0\}$.

On déduit du théorème 3 que si M est de type fini alors M_{tors} est de type fini lui aussi.

Si M_{tors} est nul on dit que M est sans torsion. On déduit du théorème 3 que tout A-module de type fini sans torsion est libre.

Si M est un A-module et $a \in A$ un scalaire on note $M(a) \subset M$ le sous-module formé des éléments de M annulés par a :

$$M(a) = \{m \in M \mid a.m = 0\}.$$

Si a est b sont deux scalaires non-nuls premiers entre eux alors $aA + bA = A$ et

$$M(ab) = M(a) \oplus M(b).$$

Si λ et μ sont deux scalaires tels que $\lambda a + \mu b = 1$, la décomposition d'un élément m de $M(ab)$ est donnée par

$$m = \lambda a.m + \mu b.m.$$

Plus généralement on montre le théorème suivant.

Théorème 5 (Lemme des noyaux)**.** *Soit A un anneau principal et M un A-module. Soient a_1, a_2, …, $a_I \in A$ des scalaires non-nuls et non inversibles. On suppose que les $(a_i)_{1 \leqslant i \leqslant I}$ sont premiers entre eux deux à deux. On pose $a = \prod_{1 \leqslant i \leqslant I} a_i$. Alors*

$$M(a) = \oplus_{1 \leqslant i \leqslant I} M(a_i).$$

On pose $b_i = \prod_{j \neq i} a_j$. Les $(b_i)_{1 \leqslant i \leqslant I}$ sont premiers entre eux dans leur ensemble : ils n'ont pas de diviseur commun. Donc l'idéal qu'ils engendrent est A. Il existe donc des $(\lambda_i)_{1 \leqslant i \leqslant I}$ tels que $\sum_{1 \leqslant i \leqslant I} \lambda_i b_i = 1$. Si $m \in M(a)$ alors

$$m = \sum_{1 \leqslant i \leqslant I} \lambda_i b_i.m \tag{1}$$

et $\lambda_i b_i.m$ est dans $M(a_i)$. Donc $M(a) = \sum_{1 \leqslant i \leqslant I} M(a_i)$.

Soit $\pi_i : M(a) \to M(a)$ l'application linéaire qui envoie m sur $\lambda_i b_i.m$. On vérifie que

(1) $\pi_1 + \cdots + \pi_I = \mathrm{Id}$,

(2) si $i \neq j$ alors $\pi_i \circ \pi_j = 0$,

(3) $\pi_i^2 = \pi_i$.

La première identité résulte de l'équation (1).

On montre la seconde en vérifiant que $\pi_i \circ \pi_j$ n'est autre que la multiplication par $\lambda_i \lambda_j b_i b_j$. Or a divise $b_i b_j$ si $i \neq j$.

La troisième identité est obtenue en multipliant la première par π_i.

On déduit de ces trois identités que $M(a)$ est la somme directe des $\mathrm{Im}(\pi_i)$. On pose $E_i = \mathrm{Im}(\pi_i)$. On vérifique que π est la projection sur E_i parallèlement à $\oplus_{j \neq i} E_j$.

Il est évident que $E_i \subset M(a_i)$. Réciproquement, si $m \in M(a_i)$ alors $m \in M(a)$ donc $m = \sum_{1\leqslant j\leqslant I} \pi_j(m) = \pi_i(m)$ donc $m \in E_i$. Donc

$$E_i = \mathrm{Im}(\pi_i) = M(a_i) \text{ et } M(a) = \oplus_{1\leqslant i\leqslant I} M(a_i).$$

□

Definition 1. *Soit A un anneau principal et soit p un élément irréductible de A. Soit M un A-module. On appelle* **composante** *p-primaire et on note M_p le sous-module de M formé de tous les éléments de m annulés par une puissance de p :*

$$M_p = \cup_{n\geqslant 0} M(p^n).$$

Théorème 6. *Soit A un anneau principal et M un A-module de type fini et de torsion. Alors M est somme directe de tous les M_p*

$$M = \oplus_{p\in P} M_p$$

où P est l'ensemble des éléments irréductibles de A à association près.

On peut supposer que M est non-nul. Soient $(g_j)_{1\leqslant j\leqslant J}$ des générateurs de M. Comme M est de torsion il existe un a_j non-nul dans A tel que $a_j.g_j = 0$. Le produit des a_j n'est pas nul car A est intègre. Donc l'annulateur de M n'est pas l'idéal nul. C'est un idéal principal. Soit a un générateur de $\mathrm{Ann}(M)$. On écrit la factorisation de a en produit d'irréductibles

$$a = \prod_{1\leqslant i\leqslant I} p_i^{e_i}$$

où les p_i sont des éléments irréductibles deux-à-deux non-associés.

Par définition $M(p_i^{e_i}) \subset M_{p_i}$. Réciproquement si $m \in M_{p_i}$ il est annulé par une puissance p_i^k de p_i. Mais il est aussi annulé par a. Donc il est annulé par $\mathrm{pgcd}(p_i^k, a)$ et ce scalaire divise $p_i^{e_i}$. Donc $M(p_i^{e_i}) = M_{p_i}$.

Comme $M = M(a)$ le lemme des noyaux permet de conclure.

□

Exercice 8 : Soit A un anneau principal et $a \in A$ non-nul et non-inversible. Soit $a = \prod_{1\leqslant i\leqslant I} p_i^{e_i}$ la décomposition de a en produit d'irréductibles. Montrer que A/aA est isomorphe à $\prod_{1\leqslant i\leqslant I} A/p_i^{e_i}A$.

On montre d'abord que l'on peut définir une application linéaire $f : A/aA \to \prod_{1\leqslant i\leqslant I} A/p_i^{e_i}A$ en posant $f(x+aA) = (x+p_1^{e_1}A, x+p_2^{e_2}A, \ldots, x+p_I^{e_I}A)$. On montre facilement que f est injective. Soit $b_i = \prod_{j\neq i} p_j^{e_j}$. Les $(b_i)_{1\leqslant i\leqslant I}$ sont premiers entre eux dans leur ensemble. Il existe des $(\lambda_i)_{1\leqslant i\leqslant I}$ tels que $\sum_{1\leqslant i\leqslant I} \lambda_i b_i = 1$. On vérifie que $\lambda_i b_i$ est congru à 1 modulo $p_i^{e_i}$ et à 0 modulo $p_j^{e_j}$ pour $j \neq i$. Soit $x = (x_i + p_i^{e_i}A)_{1\leqslant i\leqslant I}$ dans $\prod_{1\leqslant i\leqslant I} A/p_i^{e_i}A$. Alors $f(\sum_{1\leqslant i\leqslant I} x_i\lambda_i b_i) = x$. Donc f est surjective.

Exercice 9 : Soit $A = \mathbf{Z}$ et $M = (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/20\mathbf{Z}) \times (\mathbf{Z}/120\mathbf{Z})$. Calculez les composantes p-primaires de M.

Comme $20 = 2^2.5$ et $120 = 2^3.3.5$ on a des isomorphisme $(\mathbf{Z}/20\mathbf{Z}) \simeq (\mathbf{Z}/2^2\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$ et $(\mathbf{Z}/120\mathbf{Z}) \simeq (\mathbf{Z}/2^3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$. Donc M est isomorphe à $N = (\mathbf{Z}/2^2\mathbf{Z}) \times (\mathbf{Z}/2^3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$. Les composantes primaires de M et N sont isomorphes. Il est clair que $N_2 \simeq (\mathbf{Z}/2^2\mathbf{Z}) \times (\mathbf{Z}/2^3\mathbf{Z})$ et $N_3 \simeq (\mathbf{Z}/3\mathbf{Z})$ et $N_5 \simeq (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$.

Exercice 10 : Soit A un anneau principal. Montrer que si $f : M \to N$ est une application linéaire entre deux A-modules de type fini et de torsion, alors pour tout $p \in A$ irréductible on a $f(M_p) \subset N_p$.

Exercice 11 :

Soit A un anneau principal. Soient M et N deux modules de type fini et de torsion.

Montrer que la composante p-primaire de $M \times N$ est $M_p \times N_p$.

Definition 2 (Diviseurs élémentaires)**.** *Si M est un module de torsion de type fini sur un anneau principal et si $a_1|a_2|\dots|a_m$ sont ses facteurs invariants alors les facteurs invariants de sa composante p-primaire sont les $p^{v_p(a_i)}$ qui ne sont pas égaux à 1. En réunissant les facteurs invariants de toutes les composantes p-primaires on obtient un collection d'idéaux $p^{v_p(a_i)}A$ (certains peuvent apparaître plusieurs fois) appelés* **diviseurs élémentaires** *du module M.*

Exercice 12 : Soit $A = \mathbf{Z}$ et $M = (\mathbf{Z}/15\mathbf{Z}) \times (\mathbf{Z}/60\mathbf{Z}) \times (\mathbf{Z}/120\mathbf{Z})$. Calculez les composantes p-primaires et les diviseurs élémentaires de M.

Comme $15 = 3.5$ et $60 = 2^2.3.5$ et $120 = 2^3.3.5$ on a un isomorphisme de $\mathbf{Z}$-modules entre M et $N = (\mathbf{Z}/2^2\mathbf{Z}) \times (\mathbf{Z}/2^3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$. Les composantes p-primaires de M et N sont isomorphes et $N_2 \simeq (\mathbf{Z}/2^2\mathbf{Z}) \times (\mathbf{Z}/2^3\mathbf{Z})$ et $N_3 = (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})$ et $N_5 = (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$.

Les diviseurs élémentaires de M sont 2^2, 2^3, 3, 3, 3, 5, 5, 5.

Exercice 13 : Soit $A = \mathbf{Z}$ et soit M un module de torsion et de type fini de diviseurs élémentaires 2, 2^4, 2^4, 3, 3, 3^3, 3^5, 5^2, 5^6, 7. Quels sont les facteurs invariants de M ?

Parmi les diviseurs élémentaires de M on a trois puissances de 2, quatre puissances de 3, deux puissances 5, une puissance de 7. On pose $m = 4$, $a_4 = 2^4.3^5.5^6.7$, $a_3 = 2^4.3^3.5^2$, $a_2 = 2.3$, $a_1 = 3$. On vérifie que $a_1|a_2|a_3|a_4$ et que $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2^4\mathbf{Z}) \times (\mathbf{Z}/2^4\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3^3\mathbf{Z}) \times (\mathbf{Z}/3^5\mathbf{Z}) \times (\mathbf{Z}/5^2\mathbf{Z}) \times (\mathbf{Z}/5^6\mathbf{Z}) \times (\mathbf{Z}/7\mathbf{Z})$ est isomorphe à $(\mathbf{Z}/a_1\mathbf{Z}) \times (\mathbf{Z}/a_2\mathbf{Z}) \times (\mathbf{Z}/a_3\mathbf{Z}) \times (\mathbf{Z}/a_4\mathbf{Z})$. Donc les facteurs invariants de M sont a_1, a_2, a_3, a_4.

Exercice 14 : Soit $A = \mathbf{Z}$ et soit $M = (\mathbf{Z}/150\mathbf{Z}) \times (\mathbf{Z}/160\mathbf{Z}) \times (\mathbf{Z}/120\mathbf{Z})$.
1. Quels sont les diviseurs élémentaires de M ?
2. Quels sont les facteurs invariants de M ?

4. Endomorphismes d'un espace vectoriel de dimension finie

La classification des endomorphismes d'un espace vectoriel de dimension finie est une application importante des théorèmes 3, 6 et 5.

Definition 3 (Endomorphismes conjugués)**.** *Soit K un corps commutatif. Soient E et F deux K-espaces vectoriels non-nuls de dimension finie. Soient $f : E \to E$ et $g : F \to F$ deux applications linéaires. On dit que u et v sont* **conjuguées** *ou* **similaires** *s'il existe un isomorphisme d'espaces vectoriels $u : E \to F$ tel que $g = u \circ f \circ u^{(-1)}$.*

Pour K un corps commutatif et E un K-espace vectoriel non-nul, on souhaite classifier les endomorphismes de E à conjugaison près.

On dit qu'un scalaire $\lambda \in K$ est une **valeur propre** de l'endomorphisme $f : E \to E$ s'il existe un vecteur non-nul $v \in E$ tel que $f(v) = \lambda.v$. Dans ce cas, on dit que v est un **vecteur propre** associé à λ. On appele **espace propre** associé à λ l'ensemble des vecteurs propres associés à λ. C'est le noyau de $f - \lambda \mathrm{Id}_E$.

Une première remarque évidente : les valeurs propres de deux endomorphismes conjugués sont les mêmes. Et les espaces propres se correspondent par la conjugaison.

4.1. Équivalence entre endomorphismes d'espaces vectoriels et $K[x]$-modules.

On note $K[x]$ l'anneau des polynômes en une indéterminée et à coefficients dans K. On peut associer à tout endomorphisme $f : E \to E$ de E, une structure de $K[x]$-module sur E en posant, pour $P(x) = \sum_{0 \leqslant i \leqslant \deg(P)} p_i x^i \in K[x]$ et $v \in E$

$$P(x).v = \sum_{0 \leqslant i \leqslant \deg(P)} p_i f^{\circ i}(v).$$

On note $P(f)$ l'application linéaire $\sum_{0 \leqslant i \leqslant \deg(P)} p_i f^{\circ i}$. L'application $\varphi : P(x) \mapsto P(f)$ est un morphisme d'anneau de $(K[x], +, \times)$ vers $(\mathrm{End}_K(E), +, \circ)$. Attention, le premier anneau est commutatif et le second ne l'est pas en général.

On note que $\mathrm{End}_K(E)$ et $K[x]$ sont aussi des K-espaces vectoriels et que φ est une application K-linéaire. Comme $\mathrm{End}_K(E)$ est de dimension finie et $K[x]$ de dimension infinie, le noyau $\mathrm{Ker}(\varphi)$ de φ n'est pas nul. Or $\mathrm{Ker}(\varphi)$ est un idéal de $K[x]$ car φ est un morphisme d'anneaux. Comme $K[x]$ est euclidien, il est principal. Donc $\mathrm{Ker}(\varphi)$ est un idéal principal. On note $P_f(x)$ l'unique polynôme unitaire qui engendre $\mathrm{Ker}(\varphi)$. On l'appelle le **polynôme minimal** de f. Si E est non-nul alors le degré de P_f est au mois égal à 1. L'idéal $P_f(x)K[x]$ est par définition l'annulateur du $K[x]$-module E. Le $K[x]$-module E est annulé par $P_f(x)$ qui n'est pas nul. C'est donc un module de torsion. Comme E est un K-espace vectoriel de dimension finie, il est *a fortiori* un $K[x]$-module de type fini.

Tout K-espace vectoriel de dimension finie muni d'un endomorphisme $f : E \to E$ hérite donc d'une structure de $K[x]$-module de torsion et de type fini.

Réciproquement, considérons un $K[x]$-module M de torsion et de type fini. Comme K est inclus dans $K[x]$ on peut regarder M comme un K-espace vectoriel. Soient g_1, g_2, …, g_m des éléments de M qui l'engendrent comme $K[x]$-module. Comme M est de torsion il existe des polynômes non-nuls $a_1(x)$, …, $a_m(x)$ dans $K[x]$ tels que $a_i(x).g_i = 0 \in M$. Tout élément m de M s'écrit $m = \sum_{1 \leqslant i \leqslant m} u_i(x).g_i$ avec $\deg(u_i) < \deg(a_i)$. Donc le K-espace vectoriel M est engendré par les $x^j.g_i$ avec $1 \leqslant i \leqslant m$ et $0 \leqslant j < \deg(a_i)$. C'est donc un espace vectoriel de dimension finie. L'application $f : m \mapsto x.m$ est K-linéaire. C'est un endomorphisme du K-espace vectoriel M.

On a ainsi deux constructions réciproques l'une de l'autre qui associent à tout K-espace vectoriel de dimension finie muni d'un endomorphisme un $K[x]$-module de torsion et de type fini.

Soit maintenant deux K-espaces vectoriels E et F de dimension finie et soient $f : E \to E$ et $g : F \to F$ deux applications K-linéaires. On se demande sous quelle condition les deux $K[x]$-modules associés sont isomorphes. Supposons donc qu'il existe un isomorphisme de $K[x]$-modules $u : E \to F$. C'est a fortiori un isomorphisme de K-espaces vectoriels car K est inclus dans $K[x]$. De plus pour tout m dans E on a $u(x.m) = x.u(m)$. Donc $u(f(m)) = g(u(m))$. Autrement dit les applications linéaires f et g sont conjuguées par u. Réciproquement, il est clair que si f et g sont conjuguées par u alors u est une bijection $K[x]$-linéaire.

Classifier les applications K-linéaires entre K-espaces vectoriels de dimension finie à conjugaison près est donc équivalent à classifier les $K[x]$-modules de torsion et de dimension finie à isomorphisme près. Or le théorème 3 donne une telle classification.

4.2. **Quelques exemples.** On étudie des $K[x]$-modules particuliers appelés cycliques car ils sont engendrés par un unique vecteur. Soit

$$Q(x) = q_0 + q_1 x + \cdots + q_{d-1}x^{d-1} + x^d$$

un polynôme unitaire de degré $d \geqslant 1$. On pose

$$M = K[x]/Q(x)K[x].$$

C'est un $K[x]$-module engendré par $1+Q(x)K[x]$. On note $f : M \to M$ l'application K-linéaire définie par $f(m) = x.m$. On décrit sa matrice dans la base

$$B = (1 + Q(x)K[x], x + Q(x)K[x], x^2 + Q(x)K[x], \ldots, x^{d-1} + Q(x)K[x]).$$

Comme $f(x^i) = x^{i+1}$ pour $0 \leqslant i \leqslant d-2$ et $f(x^{d-1}) = -q_0 - q_1 x - \cdots - q_{d-1}x^{d-1}$ la matrice de f dans la base B est

$$\mathcal{C}(Q) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -q_0 \\ 1 & 0 & 0 & \ldots & 0 & -q_1 \\ 0 & 1 & 0 & \ldots & 0 & -q_2 \\ 0 & 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \ldots & 0 & 1 & -q_{d-1} \end{pmatrix}.$$

On appelle $\mathcal{C}(Q)$ la **matrice compagnon** du polynôme $Q(x)$.

Dans le cas particulier où $Q(x) = (x-\lambda)^d$ avec $\lambda \in K$ on peut considérer la base

$$C = ((x-\lambda)^{d-1} + Q(x)K[x], (x-\lambda)^{d-2} + Q(x)K[x], \dots, (x-\lambda) + Q(x)K[x], 1 + Q(x)K[x]).$$

La matrice de f dans la base C est

$$\mathcal{J}(d,\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \ddots & \vdots & \vdots \\ 0 & 0 & \lambda & \ddots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

Les matrices $\mathcal{J}(d,\lambda)$ sont appelées **matrices de Jordan**.

4.3. **Formes canoniques.** L'application des théorèmes 3 et 6 dans le contexte des endomorphismes d'un K-espace vectoriel de dimension finie donne les deux théorèmes suivants.

Théorème 7 (Forme canonique rationnelle)**.** *Soit K un corps commutatif et soit E un K-espace vectoriel non-nul de dimention finie. Soit $f : E \to E$ un endomorphisme de E. Il existe un entier $m \geqslant 1$, des polynômes $Q_1(x)$, …, $Q_m(x)$ dans $K[x]$ et une base B de E tels que $Q_1(x)|Q_2(x)|\dots|Q_m(x)$ et $\sum_{1\leqslant i\leqslant m} \deg(Q_i) = \dim(E)$ et la matrice de f dans la base B soit la matrice diagonale par blocs $\mathrm{Diag}(\mathcal{C}(Q_1), \mathcal{C}(Q_2), \dots, \mathcal{C}(Q_m))$. Les $(Q_i(x))_{1\leqslant i\leqslant m}$ sont uniques et caractérisent la classe de conjugaison de f. On les appelle les* **facteurs invariants** *de f.*

L'application linéaire f munit E d'une structure de $K[x]$-module. Le théorème 3 fournit un isomorphisme u de $K[x]$-modules entre E et $\oplus_{1\leqslant i\leqslant m} K[x]/Q_i(x)K[x]$. Dans chacun de ces m facteurs la section 4.2 fournit une base telle que la multiplication par x ait pour matrice la matrice compagnon de $Q_i(x)$. On transporte la réunion de ces m bases par l'isomorphisme u et l'on obtient la base B annoncée par le théorème. □

Théorème 8 (Forme canonique de Jordan)**.** *Soit K un corps commutatif et soit E un K-espace vectoriel non-nul de dimention finie. Soit $f : E \to E$ un endomorphisme de E. On suppose que le polynôme minimal de f est scindé. Il existe alors une base C de E et une collection $(d_i, \lambda_i)_{1\leqslant i\leqslant n}$ de couples formés d'un entier positif et d'un scalaire de K tels que la matrice de f dans la base C soit la matrice diagonale par blocs $\mathrm{Diag}(\mathcal{J}(d_1,\lambda_1), \mathcal{J}(d_2,\lambda_2), \dots, \mathcal{J}(d_n,\lambda_n))$. Les $(\mathcal{J}(d_i,\lambda_i))_{1\leqslant i\leqslant n}$ sont uniques et caractérisent la classe de conjugaison de f. On les appelle les* **blocs de Jordan** *de f.*

L'application linéaire f munit E d'une structure de $K[x]$-module. L'annulateur de ce $K[x]$-module est $P_f(x) = \prod_{1\leqslant i\leqslant \ell}(x-\lambda_i)^{d_i}$. D'après le lemme des noyaux E se décompose en somme directe de ses ℓ composantes $(x-\lambda_i)$-primaires E_i pour $1 \leqslant i \leqslant \ell$. Chacune de ces composantes admet une décomposition de la forme

$$E_i \simeq \oplus_{1\leqslant j\leqslant m_j} K[x]/(x-\lambda_i)^{d_{i,j}} K[x].$$

La collection des $(\lambda_i, d_{i,j})$ pour $1 \leqslant i \leqslant \ell$ et $1 \leqslant j \leqslant m_j$ définit les diviseurs principaux $(x-\lambda_i)^{d_{i,j}}$ de E. Et E est isomorphe à

$$\oplus_{1\leqslant i\leqslant \ell} \oplus_{1\leqslant j\leqslant m_j} K[x]/(x-\lambda_i)^{d_{i,j}}K[x].$$

La section 4.2 fournit pour chaque couple (i,j) une base telle que la multiplication par x dans $K[x]/(x-\lambda_i)^{d_{i,j}}K[x]$ ait pour matrice la matrice de Jordan $\mathcal{J}(d_{i,j},\lambda_i)$. On transporte dans E la réunion de toutes ces bases et l'on obtient la base C annoncée par le théorème. □

4.4. **Théorème de Cayley-Hamilton.** On rappelle que le **polynôme caractéristique** d'une matrice carrée M d'ordre d est le déterminant de $x\mathrm{I}_d - M$ où I_d est la matrice identité. On note χ_M ce polynôme. Si E est un espace vectoriel non-nul de dimension finie, le polynôme caractéristique d'un endomorphisme $f : E \to E$ est le polynôme caractéristique de la matrice de f dans n'importe quelle base de E. On le note χ_f. Ses racines sont les valeurs propres de f.

Théorème 9 (Théorème de Cayley-Hamilton)**.** *Soit K un corps commutatif et E un K-espace vectoriel non-nul de dimension d finie et $f : E \to E$ une application linéaire. Soit $\chi_f(x) \in K[x]$ le polynôme caractéristique de f. Alors $\chi_f(f) = 0$.*

On va montrer ce théorème de deux manières différentes.

4.4.1. *Preuve par la forme canonique de Jordan.* On observe que le polynôme caractéristique d'une matrice de Jordan $\mathcal{J}(d,\lambda)$ est $(x-\lambda)^d$. De plus $\mathcal{J}(d,\lambda) - \lambda$ est une matrice **nilpotente** d'**indice** d. Autrement dit, sa puissance d est nulle mais sa puissance $d-1$ ne l'est pas. Donc

$$(\mathcal{J}(d,\lambda) - \lambda)^d = 0.$$

Une matrice de Jordan annule donc son polynôme caractéristique.

Soit maintenant $M = \mathrm{Diag}(\mathcal{J}(d_1,\lambda_1), \mathcal{J}(d_2,\lambda_2), \ldots, \mathcal{J}(d_n,\lambda_n))$ une matrice diagonale par blocs telle que chaque bloc soit une matrice de Jordan. Le polynôme caractéristique $\chi_M(x)$ de M est

$$\chi_M(x) = \prod_{1\leqslant i\leqslant n} (x-\lambda_i)^{d_i}.$$

Comme $(x-\lambda_i)^{d_i}$ annule le bloc $\mathcal{J}(d_i,\lambda_i)$, le produit des $(x-\lambda_i)^{d_i}$ annule tous les blocs de M. Donc

$$\chi_M(M) = 0.$$

On déduit de cette observation et du théorème 8 que si $f : E \to E$ est un endomorphisme d'un espace vectoriel non-nul de dimension finie dont le polynôme minimal $P_f(x) \in K[x]$ est scindé alors $\chi_f(f) = 0$. Il existe en effet une base B de E où la matrice M de f est diagonale par blocs de Jordan. Donc $\chi_M(M) = 0$. Mais $\chi_M = \chi_f$. Donc $\chi_f(M) = 0$. Mais $\chi_f(M)$ est la matrice dans la base B de $\chi_f(f)$. Donc $\chi_f(f) = 0$.

En toute généralité, soit K un corps commutatif et E un K-espace vectoriel non-nul de dimension d finie et $f : E \to E$ une application linéaire. Soit B une base de E. Soit M la matrice de f dans B. Soit χ_f le polynôme caractéristique de f et de M. Soit P_f le polynôme minimal de f. Il existe un corps L qui contient K et tel que P_f soit scindé dans $L[x]$. Soit $F : L^d \to L^d$ l'application linéaire qui envoie la colonne $c \in L^d$ sur $M.c$. La matrice de F dans

la base canonique de L^d est $M \in \mathcal{M}_{d\times d}(K) \subset \mathcal{M}_{d\times d}(L)$. Donc son polynôme caractéristique est $\chi_F = \chi_M = \chi_f \in K[x] \subset L[x]$. Comme le polynôme minimal de F est P_f, il est scindé dans $L[x]$. On a donc $\chi_F(F) = 0$. Donc $\chi_M(M) = 0$. Donc $\chi_f(M) = 0$ donc $\chi_f(f) = 0$.

4.4.2. *Preuve par la forme canonique rationnelle.* Si $Q(x) \in K[x]$ est un polynôme unitaire de degré $\geqslant 1$ on observe que le polynôme caractéristique de la matrice compagnon $\mathcal{C}(Q)$ de $Q(x)$ est $Q(x)$. Le calcul est facile en développant le déterminant le long de la dernière colonne ou bien le long de la première ligne.

Comme $\mathcal{C}(Q)$ est la matrice de la multiplication par x dans $K[x]/Q(x)$ il est évident que $Q(\mathcal{C}(Q))$ est la matrice nulle. Une matrice compagnon annule donc son polynôme caractéristique.

Soit maintenant $M = \mathrm{Diag}(\mathcal{C}(Q_1), \mathcal{C}(Q_2), \ldots, \mathcal{C}(Q_m))$ une matrice diagonale par blocs telle que chaque bloc soit une matrice compagnon. Le polynôme caractéristique $\chi_M(x)$ de M est

$$\chi_M(x) = \prod_{1\leqslant i\leqslant m} Q_i.$$

Comme $Q_i(x)$ annule le bloc $\mathcal{C}(Q_i)$, le produit des Q_i annule tous les blocs de M. Donc

$$\chi_M(M) = 0.$$

On déduit de cette observation et du théorème 8 que si $f : E \to E$ est un endomorphisme d'un espace vectoriel non-nul de dimension finie alors $\chi_f(f) = 0$. Il existe en effet une base B de E où la matrice M de f est diagonale par blocs avec des blocs qui sont matrices compagnons de polynômes Q_1, Q_2, …, Q_m tels que $Q_1|Q_2|\ldots|Q_m$. Donc $\chi_M(M) = 0$. Mais $\chi_M = \chi_f$. Donc $\chi_f(M) = 0$. Mais $\chi_f(M)$ est la matrice dans la base B de $\chi_f(f)$. Donc $\chi_f(f) = 0$.

Exercice 15 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Soit f un endomorphisme de E. Soit χ_f son polynôme caractéristique et P_f son polynôme minimal. Soient $(Q_i(x))_{1\leqslant i\leqslant m}$ les polynômes (facteurs invariants) donnés par le théorème 7.

1. Montrer que

$$P_f(x) = Q_m(x) \text{ et } \chi_f = \prod_{1\leqslant i\leqslant m} Q_i(x).$$

2. En déduire que les facteurs irréductibles de P_f et χ_f sont les mêmes.

3. Montrer que P_f est scindé si et seulement si χ_f est scindé.

4. Donnez une démonstration courte du théorème de Cayley-Hamilton.

4.5. **Décomposition de Dunford.** Soit K un corps commutatif et E un K-espace vectoriel non-nul de dimension d finie et $f : E \to E$ une application linéaire.

On dit que f est **nilpotente** d'indice n si $f^{\circ n} = 0$ et $f^{\circ(n-1)} \neq 0$. Cela revient à dire que la matrice de f dans n'importe quelle base de E est nilpotente.

On dit que f est **diagonalisable** s'il existe une base de E telle que la matrice de f dans cette base soit diagonale. Cela revient à demander qu'il existe une décomposition de E en somme directe $E = \oplus_{1\leqslant i\leqslant I} E_i$ telle que la restriction de f à chaque E_i soit la multiplication par un scalaire λ_i. Cela revient encore à demander que E soit somme directe des espaces propres de f.

Exercice 16 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Montrer qu'un endomorphisme de E nilpotent et diagonalisable est nul.

Exercice 17 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Soit f un endomorphisme de E. Soit P_f le polynôme minimal de f. Montrer que f est diagonalisable si et seulement si P_f est scindé et sans facteur carré (toutes les racines de P_f sont simples).

Supposons que f est diagonalisable. Soient $(\lambda_i)_{1\leqslant i\leqslant I}$ les valeurs propres de f. L'espace E est somme directe des espaces propres associés aux λ_i. Donc le polynôme minimal de f est $\prod_{1\leqslant i\leqslant I}(x-\lambda_i)$. C'est un polynôme scindé et sans facteur carré.

Supposons maintenant que P_f est scindé et sans facteurs carrés. Écrivons $P_f(x)=\prod_{1\leqslant i\leqslant I}(x-\lambda_i)$. D'après le lemme des noyaux (théorème 5) l'espace E est somme des $E_i=\mathrm{Ker}(f-\lambda_i)$. Et la restriction de f à E_i est un scalaire. Donc f est diagonalisable.

Exercice 18 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Soit f un endomorphisme de E. Soit $F\subset E$ un sous-espace stable par f. Montrer que si f est diagonalisable alors sa restriction à F est diagonalisable elle aussi.

D'après l'exercice précédent, le polynôme minimal P_f de f est scindé et sans facteur carré. Or le polynôme minimal de la restriction de f à F est un diviseur de P_f. Il est donc lui aussi scindé et sans facteur carré. Donc cette restriction est diagonalisable elle aussi.

Exercice 19 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Soient f et g deux endomorphismes diagonalisables de E qui commutent. Montrer qu'il existe une décomposition de E en somme directe $E=\oplus_{1\leqslant i\leqslant I}E_i$ telle que les restrictions de f et de g à chaque E_i soient des scalaires. En déduire qu'il existe une base de E dans laquelle les matrices de f et de g sont diagonales toutes les deux. On dit que f et g sont **codiagonalisables**.

Soient $(\lambda_i)_{1\leqslant i\leqslant I}$ les valeurs propres de f. Et soient $E_i=\mathrm{Ker}(f-\lambda_i\mathrm{Id})$ les espaces propres correspondants. On sait que $E=\oplus_{1\leqslant i\leqslant I}E_i$ car f est diagonalisable. Si $v\in E_i$ alors $f(g(v))=g(f(v))=g(\lambda_i v)=\lambda_i g(v)$. Donc les espaces propres de f sont stabilisés par g. La restriction de g à E_i est diagonalisable. Il existe donc des sous-espaces $(F_{i,j})_{1\leqslant j\leqslant J_i}$ tels que $E_i=\oplus_{1\leqslant j\leqslant J_i}F_{i,j}$ et la restriction de g (et de f) à chaque $E_{i,j}$ soit un scalaire. En fin de compte $E=\oplus_{1\leqslant i\leqslant I}\oplus_{1\leqslant j\leqslant J_i}F_{i,j}$ et la restriction de f et de g à chaque $E_{i,j}$ est un scalaire. En rassemblant des bases de chacun de ces $E_{i,j}$ on obtient une base de E qui diagonalise f et g.

Exercice 20 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Soient f et g deux endomorphismes diagonalisables de E qui commutent. Montrer que toute combinaison linéaire $af + bg$ avec a et b dans K est un endomorphisme diagonalisable.

D'après l'exercice précédent f et g sont codiagonalisables. Il existe une base B de E dans laquelle les matrices M_f de f et M_g de g sont diagonales. La matrice $aM_f + bM_g$ est diagonale elle aussi. Et c'est la matrice dans B de $af + bg$.

Exercice 21 : Soit K un corps commutatif et E un espace vectoriel non-nul de dimension d finie. Soient f et g deux endomorphismes nilpotents de E qui commutent. Montrer que toute combinaison linéaire $af + bg$ avec a et b dans K est un endomorphisme nilpotent.

Puisque f et g sont nilpotentes il existe un entier u tel que $f^{\circ u} = g^{\circ u} = 0$. Comme f et g commutent, pour tout entier $k \geqslant 1$ on a $(af + bg)^{\circ k} = \sum_{1 \leqslant i \leqslant k} \binom{k}{i} a^i b^{k-i} f^{\circ i} g^{\circ (k-i)}$. Si $k \geqslant 2u - 1$ on vérifie que tous les termes dans la somme précédente sont nuls.

Soit maintenant $f : E \to E$ un endomorphisme dont le polynôme minimal P_f est scindé. On rappelle que la donnée de f munit E d'une structure de $K[x]$-module et que le produit d'un polynôme $a(x) = \sum_{1 \leqslant i \leqslant \deg(a)} a_i x^i \in K[x]$ par un vecteur $v \in E$ est défini par

$$a(x).v = a(f)(v) = \sum_{1 \leqslant i \leqslant \deg(a)} a_i f^{\circ i}(v).$$

On écrit

$$P_f(x) = \prod_{1 \leqslant i \leqslant I} (x - \lambda_i)^{e_i}$$

et pour tout $1 \leqslant i \leqslant I$ on note $a_i(x) = (x - \lambda_i)^{e_i}$ et $b_i(x) = \prod_{j \neq i} a_i(x)$. Les a_i sont premiers entre eux deux à deux. Les b_i sont premiers entre eux dans leur ensemble. Il engendrent donc $K[x]$. Il existe donc des $c_i(x)$ tels que

$$\sum_{1 \leqslant i \leqslant I} c_i b_i = 1. \tag{2}$$

On note $h_i(x) = c_i(x) b_i(x)$ et $\pi_i = h_i(f)$. Les π_i sont des endomorphismes de E qui vérifient

(1) $\pi_1 + \cdots + \pi_I = \mathrm{Id}$,

(2) si $i \neq j$ alors $\pi_i \circ \pi_j = 0$,

(3) $\pi_i^2 = \pi_i$.

La première identité résulte de l'équation (2).

On montre la seconde en vérifiant que $\pi_i \circ \pi_j$ n'est autre que la multiplication par $c_i c_j b_i b_j$ dans le $K[x]$-module E associé à f. Or P_f divise $b_i b_j$ si $i \neq j$. Donc $b_i(f) \circ b_j(f)$ est nul dans ce cas.

La troisième identité est obtenue en multipliant la première par π_i.

On déduit de ces trois identités que E est la somme directe des $\mathrm{Im}(\pi_i)$. On pose $E_i = \mathrm{Im}(\pi_i)$. On vérifique que π est la projection sur E_i parallèlement à $\oplus_{j \neq i} E_j$.

Il est évident que $E_i \subset \mathrm{Ker}(a_i(f))$. Réciproquement, si $v \in \mathrm{Ker}(a_i(f))$ alors $v = \sum_{1\leqslant j\leqslant I} \pi_j(v) = \pi_i(v)$ donc $v \in E_i$. Donc

$$E_i = \mathrm{Ker}(a_i(f)) = \mathrm{Im}(\pi_i) \text{ et } E = \oplus_{1\leqslant i\leqslant I} E_i.$$

On vérifie que $E_i = \mathrm{Ker}(a_i(f))$ est la composante $(x-\lambda_i)$-primaire $E_{x-\lambda_i}$ du $K[x]$-module E. Par définition $\mathrm{Ker}(a_i(f)) \subset E_{x-\lambda_i}$. Réciproquement si $v \in E_{x-\lambda_i}$ il est annulé par une puissance $(x-\lambda_i)^k$ de $x-\lambda_i$. Mais il est aussi annulé par P_f. Donc il est annulé par $\mathrm{pgcd}((x-\lambda_i)^k, P_f)$ et ce polynôme divise $(x-\lambda_i)^{e_i}$. Donc $E_{x-\lambda_i} \subset \mathrm{Ker}(a_i(f))$.

Les

$$E_i = E_{x-\lambda_i} = \mathrm{Ker}\left((f-\lambda_i)^{e_i}\right)$$

sont appelés **sous-espaces caractéristiques** de f.

On note

$$\delta = \sum_{1\leqslant i\leqslant I} \lambda_i \pi_i = \sum_{1\leqslant i\leqslant I} \lambda_i h_i(f).$$

C'est un endomorphisme diagonalisable. Et c'est un polynôme en f. Donc $\delta \circ f = f \circ \delta$.

On pose

$$\nu = f - \delta = \sum_{1\leqslant i\leqslant I} (f-\lambda_i) \circ \pi_i.$$

C'est encore un polynôme en f. On vérifie que pour tout entier $k \geqslant 1$

$$\nu^{\circ k} = \sum_{1\leqslant i\leqslant I} (f-\lambda_i)^{\circ k} \circ \pi_i.$$

Si $k \geqslant e_i$ alors $(x-\lambda_i)^k h_i(x)$ est divisible par $P_f(x)$ donc $(f-\lambda_i)^{\circ k} \circ \pi_i = 0$. Donc ν est nilpotent. Comme ν et δ sont des polynômes en f ils commutent entre eux et avec f.

On a donc décomposé f comme somme d'un endomorphisme diagonalisable δ et d'un endomorphisme nilpotent ν qui commutent entre eux.

Supposons maintenant qu'il existe un endomorphisme diagonalisable δ_1 et un endomorphisme nilpotent ν_1 qui commutent entre eux et tels que $f = \delta_1 + \nu_1$. Comme ν_1 commute avec δ_1 et avec lui-même, il commute avec f. On peut en dire autant de δ_1.

Puisque ν_1 commute avec f, il commute avec tous les polynômes en f, et en particulier avec δ et ν. On peut en dire autant de δ_1.

On a $\delta - \delta_1 = \nu_1 - \nu$.

Or le membre de droite est la différence de deux endomorphismes nilpotents qui commutent. C'est donc un endomorphisme nilpotent.

Et le membre de gauche est la différence de deux endomorphismes diagonalisables qui commutent. C'est donc un endomorphisme diagonalisable.

Donc $\delta - \delta_1 = \nu_1 - \nu = 0$.

On a montré le théorème suivant.

Théorème 10 (Décomposition de Dunford)**.** *Soit K un corps commutatif et E un espace vectoriel non-nul et de dimension finie. Soit $f : E \to E$ une application linéaire. On suppose que le polynôme minimal de f est scindé. Il existe un unique couple (δ, ν) d'endomorphismes de E tels que*

- *δ est diagonalisable,*

- ν *est nilpotent,*
- $\delta \circ \nu = \nu \circ \delta$,
- $f = \delta + \nu$.

Exercice 22 : *Soit* $\mathbf{Q}$ *le corps des rationnels. Soit* $E = \mathbf{Q}^2$. *Soit* $f : E \to E$ *l'application linéaire dont la matrice dans la base canonique de* E *est*

$$M = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}.$$

Calculez la décomposition de Dunford de f.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, BORDEAUX INP, INRIA, CNRS, UMR 5251, F-33400 TALENCE, FRANCE.

E-mail address: Jean-Marc.Couveignes@u-bordeaux.fr