Master Mathématiques 1ère année

COURS DE THEORIE DES MODULES

Nicolas JACON

Université de Franche Comté

Table des matières

Chapitre 1

Modules sur un anneau

La notion de module généralise naturellement la notion d'espace vectoriel déjà vu les années précédentes. Au lieu de se placer sur un corps comme pour ces derniers objets, on se place sur un anneau. Nous verrons que, si certaines notions passent facilement d'un objet à l'autre, d'autres posent problèmes. Ce chapitre aura une structure "classique". Nous définirons tout d'abord la structure essentielle de ce cours : la structure de modules, en toute généralité. Ensuite, nous nous intéresserons à la notion de morphismes de modules, de sous-modules, de modules quotients etc. Plusieurs exemples seront également explicités.

1.1 Premières définitions

Dans toute la suite, on suppose que A, muni des applications $+$ et $.$ est un anneau unitaire et commutatif c'est à dire que A est un ensemble muni de deux applications internes $+$ l'addition, et $.$ la multiplication, vérifiant :

- A muni de l'addition $+$ est un groupe commutatif (d'élément neutre 0).
- la multiplication $.$ est associative, distributive par rapport à l'addition, et elle possède un élément neutre que l'on note 1.
- la loi de multiplication est commutative.

Voici la définition de l'objet principal d'étude de ce cours :

Définition 1.1.1 Un *A-module* (à gauche) M est un groupe abélien $(M, +)$ muni d'une loi externe :

$$\begin{array}{ccc} A \times M & \to & M \\ (a, m) & \mapsto & a.m \end{array}$$

vérifiant les trois propriétés suivantes :

1. la bi-additivité, $a.(m_1 + m_2) = am_1 + am_2$, $(a + b).m_1 = a.m_1 + b.m_1$,
2. l'associativité, $a.(b.m_1) = (ab).m_1$.
3. l'action triviale de l'unité, $1.m = m$

où $(a, b) \in A^2$ et $(m_1, m_2) \in M^2$.

On prendra bien soin de ne pas confondre les lois d'addition dans M et dans A, et de même pour la loi de multiplication dans A avec la loi externe de M. On omettra la plus part du temps la terminologie "à gauche", tous nos modules

étant considérés comme des modules à gauche. On adapte facilement la définition ci-dessus pour définir les modules à droite (en faisant agir A par la droite).

Remarque 1.1.2 On dit que la loi externe fournit une action de A sur l'ensemble M (même si A pour la multiplication n'est pas un groupe).

{ex0chap1}

Remarque 1.1.3 Remarquons que si M est un A-module, la bi-additivité implique que pour tout $m \in M$, on a $(0+0).m = 0.m + 0.m$ et donc $0.m = 0$.

{inverse}

Remarque 1.1.4 Une autre remarque importante : comme A est un anneau unitaire , on dispose de l'unité 1 et de l'inverse de cet élément (pour la loi d'addition) qui est noté -1. On a alors $(1+(-1)).m = 0$ pour tout $m \in M$, ceci implique $(-1).m = -m$ l'inverse de m pour la loi d'addition.

Exemple 1.1.5 Soit A un anneau commutatif et soit I un idéal de A, c'est à dire un sous-groupe de A pour la loi d'addition qui vérifie la propriété suivante :

$$\forall a \in A, \forall i \in I,\ ai \in I$$

Ainsi on a une loi :

$$\begin{array}{ccc} A \times I & \to & I \\ (a,m) & \mapsto & am \end{array}$$

donnée par la multiplication dans A. Les trois axiomes de modules sont vérifiés et on en conclut donc que I est un A-module. Donc tout idéal d'un anneau est aussi un module sur celui-ci. En particulier A est un A-module. Attention, la réciproque est **fausse** : tout A-module n'est pas forcément un idéal de A, un A-module n'étant pas nécessairement contenu dans A, comme nous le voyons dans l'exemple suivant !

{chap1exn}

Exemple 1.1.6 Soit $n \in \mathbb{N}$, alors le groupe commutatif $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module. La loi externe est donnée par

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ (a, m+n\mathbb{Z}) & \mapsto & am+n\mathbb{Z} \end{array}$$

qui, comme on peut facilement vérifier, satisfait aux trois axiomes ci-dessus.

{chap1exn2}

Exemple 1.1.7 Si A est un anneau commutatif alors l'anneau des polynômes $A[X]$ est un A-module pour la loi

$$\begin{array}{ccc} A \times A[X] & \to & A[X] \\ (a,P) & \mapsto & a.P \end{array}$$

"." désignant la multiplications dans $A[X]$.

Soit $\mathbb{K}$ un corps. Alors, il est clair que les $\mathbb{K}$-modules sont exactement les $\mathbb{K}$-espaces vectoriels. Ainsi, on peut penser un A-module comme une généralisation d'espace vectoriel ... sur un anneau. Attention, cependant, beaucoup de résultats valables sur les espaces vectoriels ne seront pas vrai dans ce nouveau cadre.

Concernant la structure de module, il est souvent aisé de se servir de la caractérisation suivante :

{chap1stru}

Proposition 1.1.8 *Supposons que M soit un groupe commutatif. Alors, se donner une structure de A-module sur M revient exactement à se donner un morphisme d'anneaux*

$$f : A \to \mathrm{End}(M).$$

où $\mathrm{End}(M)$ *désigne l'ensemble des endomorphismes du groupe M. La loi externe et f sont reliés de la façon suivante :*

$$\forall a \in A, \forall m \in M,\ f(a)(m) = a.m$$

Preuve. Supposons tout d'abord que M soit un A-module et considérons l'application

$$f : A \to \mathrm{End}(M).$$

telle que

$$\forall a \in A, \forall m \in M,\ f(a)(m) = a.m$$

f est bien défini. En effet, supposons que $a \in A$, alors $f(a)$ est un morphisme de groupes. La bi-additivité implique que pour tout $(m_1, m_2) \in M^2$, on a

$$\begin{aligned} f(a)(m_1 + m_2) &= a(m_1 + m_2) \\ &= am_1 + am_2 \\ &= f(a)(m_1) + f(a)(m_2) \end{aligned}$$

et le résultat suit. Maintenant f est un morphisme d'anneaux. En effet :

- on a $f(1) = \mathrm{Id}_M$ en utilisant l'action triviale de l'unité,
- pour tout $(a, b) \in A^2$, on a $f(a + b) = f(a) + f(b)$ car la bi-additivité implique pour tout $m \in M$, on a $f(a + b)(m) = (f(a) + f(b))(m)$
- pour tout $(a, b) \in A^2$, on a $f(ab) = f(a) \circ f(b)$ car pour tout $m \in M$, on a $f(ab)(m) = (ab).m$ d'une part et $f(a) \circ f(b)(m) = a.(bm)$ d'autre part. L'associativité permet alors de conclure.

Si on suppose maintenant que

$$f : A \to \mathrm{End}(M).$$

est un morphisme d'anneaux, on veut montrer que la loi externe

$$\begin{array}{ccc} A \times M & \to & M \\ (a, m) & \mapsto & f(a)(m) \end{array}$$

muni M d'une structure de A-modules. On vérifie alors que

1. la bi-additivité provient du fait que f est à valeurs dans $\mathrm{End}(M)$ et que f est un morphisme de groupes,
2. l'associativité provient du fait que f est un morphisme d'anneaux.
3. l'action triviale de l'unité provient du fait que le morphisme est unitaire (et envoie donc 1 sur l'identité).

□

Avant de détailler quelques exemples, signalons comment on peut facilement construire de nouvelles structures de modules à partir de morphismes d'anneau.

Proposition 1.1.9 *Soit A et B deux anneaux commutatifs et soit $\Phi : A \to B$ un morphisme d'anneaux. Supposons que M soit un B-module. Alors M est aussi un A-module pour la loi externe :*

$$\begin{array}{ccc} A \times M & \to & M \\ (a, m) & \mapsto & \Phi(a).m \end{array}$$

On dit que la structure de A-module est obtenu à partir d'une restriction des scalaires.

Preuve. On pourrait vérifier les axiomes de modules mais il est plus rapide de se servir de la proposition 1.1.8. M est un groupe commutatif et on sait que l'on a un morphisme d'anneaux :

$$f : B \to \mathrm{End}(M).$$

En composant avec Φ, on obtient donc un morphisme d'anneaux :

$$f \circ \Phi : A \to \mathrm{End}(M)$$

Ceci prouve bien que M est un A-module et, pour éviter les confusions, si on note $*$ la loi externe, on voit qu'elle est donnée par :

$$\forall a \in A, \forall m \in M, a * m := f(\Phi(a))(m) = \Phi(a).m$$

□

Exemple 1.1.10 Supposons que $A \subset B$ soient deux anneaux. On a alors une injection canonique $i : A \to B$ qui est un morphisme d'anneaux. Si M est un B-module, c'est donc un A-module par restriction des scalaires. L'action de A sur M est trivialement donnée par l'action de B. On peut ainsi voir l'example 1.1.7 comme une restriction des scalaires.

Remarque 1.1.11 Si A et B sont deux anneaux et si $f : A \to B$ est un morphisme d'anneaux, B a une structure de A-module par restriction des scalaires. En fait, B est un exemple d'algèbre associative unitaire.

Exemple 1.1.12 Si E est un $\mathbb{C}$-espace vectoriel alors, c'est aussi un $\mathbb{R}$-espace vectoriel par restriction des scalaires. Nous avons déjà rencontré cette situation dans les cours d'algèbres linéaires des années précédentes.

1.2 Quelques exemples

{kdex}

Prenons tout d'abord $A = \mathbb{Z}$. On cherche à étudier la notion de $\mathbb{Z}$-modules .

{ssgpe}

Proposition 1.2.1 *L'ensemble des $\mathbb{Z}$-modules correspond à l'ensemble des groupes abéliens. Plus précisement, si M est un $\mathbb{Z}$-module, l'action de $\mathbb{Z}$ est donnée par*

$$\forall n \in \mathbb{Z},\ \forall x \in M,\ n.x = \begin{cases} \underbrace{x + x + \ldots + x}_{n\ fois} & si\ n > 0 \\ 0 & si\ n = 0 \\ \underbrace{(-x) + (-x) + \ldots + (-x)}_{-n\ fois} & si\ n < 0 \end{cases}$$

Preuve. Si M est un $\mathbb{Z}$-module, alors c'est un groupe abélien et il résulte des axiomes que

$$n.x = (\underbrace{1+1+\ldots+1}_{n \text{ fois}}).x = \underbrace{x+x+\ldots+x}_{n \text{ fois}}$$

pour tout $n > 0$. De même, on a $0.x = 0$ par la remarque 1.1.3 et

$$n.x = (\underbrace{-1-1-\ldots-1}_{-n \text{ fois}}).x = \underbrace{-x+(-x)+\ldots+(-x)}_{-n \text{ fois}}$$

si $n < 0$. Maintenant, si M a une structure de groupe abélien. On vérifie facilement que la loi externe comme ci-dessus vérifie aux axiomes de modules.

□

Il résulte de cette proposition que les $\mathbb{Z}/n\mathbb{Z}$ sont bien des $\mathbb{Z}$-modules comme on l'a vu dans l'exemple 1.1.6.

Donnons nous maintenant $\mathbb{K}$ un corps et considérons l'anneau des polynômes $\mathbb{K}[X]$. On va chercher à déterminer exactement l'ensemble des $\mathbb{K}[X]$-modules. Soit donc M un $\mathbb{K}[X]$-module avec loi externe

$$\begin{array}{ccc} \mathbb{K}[X] \times M & \to & M \\ (P, m) & \mapsto & P.m \end{array}$$

- Comme $\mathbb{K} \subset \mathbb{K}[X]$, le $\mathbb{K}[X]$-module M est aussi un $\mathbb{K}$ espace vectoriel par restriction des scalaires.
- Considérons l'application :

  $$\begin{array}{rccc} u: & M & \to & M \\ & m & \mapsto & X.m \end{array}$$

  Celle-ci est bien définie car pour tout $m \in M$, comme M est un $\mathbb{K}[X]$-module, on a $X.m \in M$. En fait, on obtient un endomorphisme du $\mathbb{K}$-espace vectoriel de M car si $\lambda \in \mathbb{K}$

  $$u(\lambda.m) = X.(\lambda.m) = (\lambda.X).m = \lambda.(X.m) = \lambda u(m)$$

  par définition et par associativité de la loi de $\mathbb{K}[X]$-module. Si $(m_1, m_2) \in M^2$, on a

  $$u(m_1 + m_2) = X.(m_1 + m_2) = u(m_1) + u(m_2)$$

- La structure de $\mathbb{K}[X]$-module est maintenant entièrement déterminée par la donnée de u. En effet, si $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{K}[X]$ et $m \in M$, on a

  $$\begin{array}{rcl} P.m & = & a_0 1.m + a_1 Xm + \ldots + a_n X^n m \\ & = & a_0 u^0(m) + a_1 u^1(m) + \ldots + a_n u^n(m) \\ & = & P(u)(m) \end{array}$$

Réciproquement, si on se donne un $\mathbb{K}$-espace vectoriel M et un endomorphisme u de M alors on a une loi :

$$\begin{array}{ccc} \mathbb{K}[X] \times M & \to & M \end{array}$$

tel que pour $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{K}[X]$ et $m \in M$, on a

$$\begin{array}{rcl} P.m & = & a_0 u^0(m) + a_1 u^1(m) + \ldots + a_n u^n(m) \\ & = & P(u)(m) \end{array}$$

On vérifie que les axiomes de modules sont bien vérifiés :

- Si $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{K}[X]$ et $Q = b_0 + b_1X + \ldots + b_nX^n \in \mathbb{K}[X]$ et si $(m_1, m_2) \in M^2$, on vérifie que

$$(P+Q).m = P.m + Q.m \qquad \text{et} \qquad P.(m_1 + m_2) = P.m_1 + P.m_2$$

ce qui est clair.
- Si $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{K}[X]$ et $m \in M$, on a pour $j \in \mathbb{N}$:

$$(X^j.P).m = a_0u^j(m) + a_1u^{j+1}(m) + \ldots + a_nu^{j+n}(m)$$

d'une part et

$$X^j.(P.m) = a_0X^j.m + a_1X^j.u(m) + \ldots + a_nX^j.u^n(m)$$

d'où :

$$(X^j.P).m = X^j.(P.m)$$

Notons également que si $\lambda \in \mathbb{K}$, on a

$$(\lambda.P).m = \lambda.(P.m) \quad (\star)$$

Maintenant, si $Q = b_0 + b_1X + \ldots + b_nX^n \in \mathbb{K}[X]$, on obtient :

$$(Q.P).m = (b_0P + b_1XP + \ldots + b_nX^nP).m$$

par la biadditivité, on obtient :

$$(Q.P).m = (b_0P).m + (b_1XP).m + \ldots + (b_nX^nP).m$$

soit encore par $(\star)$:

$$(Q.P).m = b_0(P.m) + b_1(XP).m + \ldots + b_n(X^nP).m$$

en utilisant le résultat précédent, il suit :

$$(Q.P).m = b_0(P.m) + b_1X(P.m) + \ldots + b_nX^n(P.m)$$

ce qui permet de conclure :

$$(QP).X = Q.(P.X)$$

- Pour tout $m \in M$, on a

$$1.m = m$$

On vient de montrer :

{modpoly}

Proposition 1.2.2 *Un $\mathbb{K}[X]$-module M est exactement la donnée d'un $\mathbb{K}$-espace vectoriel M et d'un endomorphisme $\mathbb{K}$-linéaire de M.*

Cette proposition permet de faire un lien entre la théorie des $\mathbb{K}[X]$-modules et celles de $\mathbb{K}$-espace vectoriel. Ceci sera fondamental pour la suite ...

Exemple 1.2.3 Soit $\mathbb{K}$ un corps et I un idéal de $\mathbb{K}[X]$. C'est donc un $\mathbb{K}[X]$-module. C'est aussi un $\mathbb{K}$-espace vectoriel et l'endomorphisme qui lui est associé est l'endomorphisme de multiplication par X d'après la discussion ci-dessus.

Exemple 1.2.4 On considère un $\mathbb{K}$-espace vectoriel E et l'endomorphisme u identité de E . On doit pouvoir associer à ces données un $\mathbb{K}[X]$-module d'après la discussion ci-dessus. C'est l'ensemble E et X agit sur E de la façon :

$$\forall m \in E, X.m = u(m)$$

dans ce cas, on a $u(m) = m$ et l'action d'un polynôme $a_0 + a_1.X + \ldots + a_k X^k$ de $\mathbb{K}[X]$ est donc donné par :

$$(a_0 + a_1.X + \ldots + a_k X^k).m = (a_0 + a_1 + \ldots a_k).m$$

1.3 Sous-modules et Morphismes

Comme dans le cas des groupes, anneaux ou espaces vectoriels, un sous-module est une partie non vide d'un module, stable pour les lois de modules :

Définition 1.3.1 Soit M un A-module et $N \subset M$. Alors, on dit que N est un *sous-module* de M si et seulement si

1. N est un sous-groupe de M (N est donc non vide),
2. Pour tout $a \in A$ et $m \in N$, on a $a.m \in N$.

Ainsi, tout sous-module d'un A-module M est aussi un A-module. Si $\mathbb{K}$ est un corps, la notion de sous-modules coïncide avec celle de $\mathbb{K}$-espace vectoriel.

Exemple 1.3.2 Les exemples suivants sont classiques.

- Si M est un A-module, $\{0\}$ et M sont des sous-modules de M appelés sous-modules triviaux.
- Les sous-modules d'un $\mathbb{Z}$-modules M sont exactement les sous-groupes de M.
- Les sous-modules du A-module A sont exactement les idéaux de A.
- Soit M un A-module et I un idéal de A. Alors l'ensemble

$$IM := \left\{ x = \sum_{i=1}^{n} a_i m_i \mid \forall i \in \{1, \ldots, n\},\ a_i \in I,\ m_i \in M \right\}$$

  est un sous-module de M

Il est souvent aisé d'utiliser le critère suivant :

{criteresousmod}

Proposition 1.3.3 *Soit M un A-module et $N \subset M$. Alors, N est un sous-module de M si et seulement si N est non vide et pour tout $a \in A$ et $(m, n) \in N$, on a $a.m + n \in N$.*

Preuve. Il est évident que si N est un sous-module de M alors il satisfait à la propriété ci-dessus. Réciproquement, supposons que pour tout $a \in A$ et $(m, n) \in N$, on a $a.m + n \in N$. En prenant $n = 0$, on voit que l'axiome 2. de sous-modules est satisfait. En prenant $a = -1$ et en utilisant la remarque 1.1.4, on voit que $n - m \in N$. Donc N est un sous-groupe de M. Ceci permet de conclure

□

De même, un morphisme de A-module est une application entre deux modules préservant les lois de ces modules :

Définition 1.3.4 Soit M et N deux A-modules. Un *morphisme* de A-module

$$f : M \to N$$

est une application vérifiant
- f est un morphisme de groupes,
- pour tout $a \in A$ et $m \in M$, on a $f(am) = af(m)$.

Un morphisme bijectif est appelé un *isomorphisme*. Un morphisme de M dans M est appelé un *endomorphisme* et un endomorphisme bijectif un *automorphisme*.

Exemple 1.3.5 Si f est un morphisme de A-modules, c'est un morphisme de groupes, donc on a $f(0_M) = 0_N$.

Remarquons que lorsque $\mathbb{K}$ est un corps, les morphismes de $\mathbb{K}$-modules sont exactement les morphismes de $\mathbb{K}$-espaces vectoriels. Avec ces définitions viennent naturellement des généralisations naturelles d'objects déjà connus dans le cadre des espaces vectoriels.

Remarque 1.3.6 On vérifie facilement que si M, N et L sont trois A-modules et si $f : M \to N$ et $g : N \to L$ sont des morphismes de A-modules alors $g \circ f$ est aussi un morphisme de A-modules.

Proposition 1.3.7 *Soit M et N deux A-modules. On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N. Alors, $\mathrm{Hom}_A(M, N)$ a une structure de A-module pour*
- *l'addition de fonctions, si $(f, g) \in \mathrm{Hom}_A(M, N)^2$ alors $f + g$ est le morphisme*
$$\begin{array}{ccc} M & \to & N \\ m & \mapsto & f(m) + g(m) \end{array}$$
- *la loi externe, si $a \in A$ et $f \in \mathrm{Hom}_A(M, N)$, alors $a.f$ est le morphisme*
$$\begin{array}{ccc} M & \to & N \\ m & \mapsto & a.f(m) \end{array}$$

Preuve. On vérifie facilement que les lois ci-dessus satisfont aux axiomes de A-modules.

□

La proposition suivante est classique lorsqu'on considère la structure de groupe ou d'espace vectoriel :

Proposition 1.3.8 *Soient M et N deux A-modules et $f : M \to N$ un morphisme de A-modules. Alors f est un isomorphisme si et seulement si il existe un morphisme $g : N \to M$ de A-modules tels que $f \circ g = \mathrm{Id}_N$ et $g \circ f = \mathrm{Id}_M$. On note $f^{-1} := g$ l'application réciproque de f.*

Preuve. Si un tel morphisme g existe alors c'est l'application réciproque de f (au sens ensembliste) donc f est bien bijective. Réciproquement, supposons que f soit bijective, alors on dispose de son application réciproque $g : N \to M$ et on sait que cette application est un morphisme de groupes (voir le cours de

Théorie de groupes de L3). Il faut montrer que pour tout $m \in M$ et $a \in A$, on a $g(a.m) = a.g(m)$. Soit donc $m \in M$ et $a \in A$, on a d'une part

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

par définition et d'autre part $f(a.g(m)) = a.(f(g(m))$ car f est un morphisme de A-modules. On voir alors que $f(g(a.m)) = f(a.g(m))$ ce qui implique que $g(a.m) = a.g(m)$ car f est injective. C'est ce qu'il fallait montrer.

□

Définition 1.3.9 Soit M et N deux A-modules et soit $f : M \to N$ un morphisme de A-modules. Le sous ensemble

$$\mathrm{Ker}(f) = \{x \in M \mid f(x) = 0\}$$

est appelé le *noyau* de f et le sous ensemble

$$\mathrm{Im}(f) = \{f(x) \in N \mid x \in M\}$$

est appelé l'*image* de f.

Proposition 1.3.10 *Soit M et N deux A-modules et soit $f : M \to N$ un morphisme de A-modules.*

1. *Si N' est un sous-module de N alors $f^{-1}(N')$ est un sous-module de M. En particulier* $\mathrm{Ker}(f)$ *est un sous-module de M. De plus, on a* $\mathrm{Ker}(f) = \{0\}$ *si et seulement si f est injective.*
2. *Si M' est un sous-module de M alors $f(M')$ est un sous-module de N. En particulier,* $\mathrm{Im}(f)$ *est un sous-module de N. De plus, on a* $\mathrm{Im}(f) = N$ *si et seulement si f est surjective.*

Preuve.

1. Soit N' un sous-module de N. Soit $a \in A$ et soit $(m, n) \in f^{-1}(N')^2$, on a $f(a.m + n) = a.f(m) + f(n) \in N'$ car N' est un sous-module de N donc $a.m + n \in f^{-1}(N')$. Il suit que $f^{-1}(N')$ est un sous-module de M. En particulier, pour $N' = \{0\}$, on obtient que $\mathrm{Ker}(f)$ est un sous-module de M. Le fait que $\mathrm{Ker}(f) = \{0\}$ si et seulement si f est injective est classique (voir le cours de L3 de théorie des groupes par exemple).
2. Soit M' un sous-module de M. Soit $a \in A$ et soit $(m, n) \in f(M')$ alors il existe $(m_1, n_1) \in M'$ tel que $f(m_1) = m$ et $f(n_1) = n$. On a alors $f(a.m_1 + n_1) = a.m + n$ avec $a.m_1 + n_1 \in M'$ car M' est un sous-module de M. Il suit que $f(M')$ est un sous-module de N. En particulier, pour $M' = M$, on a $f(M) = \mathrm{Im}(f)$ qui est donc un sous-module de N et il est evident que $\mathrm{Im}(f) = N$ si et seulement si f est surjective.

□

Attention, nous n'avons pas de notion de dimension dans le cadre des modules, c'est d'ailleurs une des principales différence avec la théorie des espaces vectoriels. Les raisonnements du type " Si E et F sont deux espaces vectoriels de même dimension et $f : E \to F$ est tel que $\mathrm{Ker}(f) = \{0\}$ alors f est un isomorphisme" ne sont donc pas possible ici !

Exemple 1.3.11 Soit A un anneau et soit $A[X]$ l'anneau des polynômes, alors pour tout $x_0 \in A$, il existe un morphisme de A-modules $f : A[X] \to A$ tel que $f(X) = x_0$. En effet, si $P = \sum_{i=0}^{n} a_i X^i$ alors f défini par $f(P) = \sum_{i=0}^{n} a_i x_0^i$ est bien un morphisme de A-modules. Le morphisme f est appelé *morphisme d'évaluation.*

1.4 Quotients

Comme dans le cas des groupes et des idéaux, on a une notion de modules quotients. Rappelons qu'un module est un groupe commutatif. Ainsi, on peut donc utiliser la notion de groupe quotient : si M un A-module et N un sous-module de M, on peut définir le groupe quotient M/N, rappelons que :

- ces éléments sont les classes d'équivalence dans M pour la relation suivante :
$$x \equiv y \iff x - y \in N$$
La classe d'un élément $x \in M$ est désignée par $x + N$.
- l'addition est donnée par
$$(x + N) + (y + N) = (x + y) + N$$
pour $x \in M$ et $y \in M$

On sait que ceci définit bien une structure de groupe. il faut maintenant voir si ce groupe a une structure de A-module.

Proposition 1.4.1 *Soit A un anneau, M un A-module et N un sous-module de M. Alors le sous-groupe M/N a une structure de A-module pour la loi*

$$\forall a \in A,\ \forall x \in M,\ a.(x + N) = a.x + N$$

De plus, cette structure est l'unique structure faisant de la projection de

$$\pi : M \to M/N$$

un morphisme de A-modules.

Preuve. Il faut tout d'abord vérifier que la formule

$$\forall a \in A,\ \forall x \in M,\ a.(x + N) = ax + N$$

a un sens, c'est à dire que si y est un élément de la classe $x+N$ alors $a.y$ est dans la même classe que $a.x$. Mais ceci est clair car si $x - y \in N$ alors $a(x - y) \in N$ car N est un sous-module de M. On vérifie ensuite facilement les axiomes de A-modules pour cette nouvelle structure, ceci découle du fait que M est un A-module.

Pour cette structure, notons que π est un morphisme de groupes et que si $a \in A$, $m \in M$, on a

$$\pi(a.m) = am + N$$

d'une part

$$a.\pi(m) = a(m + N)$$

on obtient bien $\pi(a.m) = a.\pi(m)$ ce qui prouve que π est un morphisme et il est clair, par les formules ci-dessus que si on impose que π soit un morphisme, la structure de A-module sur M/N est uniquement définie.

□

Remarque 1.4.2 Prenons $M = A$, si I est un idéal de A alors c'est aussi un A-module. On a donc une structure de A-module sur le quotient A/I. En fait, comme on sait que A/I est un anneau, on a une structure de A/I-module sur A/I. Par restriction des scalaires, on considérant la projection $A \to A/I$, on obtient une structure de A-module. Celle-ci correspond en fait à la structure ci-dessus.

Attention, sous les hypothèses ci-dessus, M/N n'est PAS un sous-module de M, étant donnée que ce n'est même pas un sous-groupe de M !

Exemple 1.4.3 Prenons $A = M = \mathbb{Z}$ et $N = n\mathbb{Z}$ alors M/N est le groupe quotient $\mathbb{Z}/n\mathbb{Z}$. C'est donc un $\mathbb{Z}$-module ce qui est en adéquation avec la proposition 1.2.1 car c'est un groupe abélien.

{expoly}

Exemple 1.4.4 Soit $\mathbb{K}$ un corps et soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré n. $\mathbb{K}[X]$ est un $\mathbb{K}$-module (c'est même un $\mathbb{K}$ espace vectoriel). Considérons l'idéal (P) engendré par P. C'est un sous-module de $\mathbb{K}[X]$ et on peut alors former le module quotient $\mathbb{K}[X]/(P)$. C'est un $\mathbb{K}$-module donc un $\mathbb{K}$-espace vectoriel. Fixons un $\lambda \in \mathbb{K}$, alors $\mathbb{K}[X]/(P)$ admet une base formée des éléments que l'on note

$$\overline{1}, \overline{X-\lambda}, \ldots, \overline{(X-\lambda)}^{n-1}$$

et qui sont les classes des polynômes associées modulo (P). En effet, ceci fournit bien une famille libre de $\mathbb{K}[X]/(P)$: une combinaison linéaire de ces éléments ne peut appartenir à (P) sauf si elle est nul car P est de degré n.

De plus, si Q est un polynôme de $\mathbb{K}[X]$, la division euclidienne de Q par P implique l'existence d'un polynôme de degré plus petit que n tel que :

$$Q = P.S + R$$

où $S \in \mathbb{K}[X]$. On a donc

$$Q \equiv R(\mathrm{mod}(P))$$

Comme R s'écrit comme combinaison linéaire de $\overline{1}, \overline{X-\lambda}, \ldots, \overline{(X-\lambda)}^{n-1}$, on peut conclure (on peut voir ceci en faisant un changement de variable $Y = X - \lambda$).

{exjordan}

Exemple 1.4.5 Prenons cette fois $\mathbb{K} = \mathbb{C}$, $\lambda \in \mathbb{C}$ et considérons le $\mathbb{C}[X]$-module $\mathbb{C}[X]/(X-\lambda)^n$. On a vu que l'on peut associer naturellement à ce module un endomorphisme u de $\mathbb{C}$-espace vectoriel $\mathbb{C}[X]/(X-\lambda)^n$. La structure de module est même équivalente à la donnée de la structure d'espace vectoriel et de cet endomorphisme, qui est donné par multiplication par X. Prenons notre base $\overline{1}, \overline{X-\lambda}, \ldots, \overline{(X-\lambda)}^{n-1}$ de $\mathbb{C}[X]/(X-\lambda)^n$ obtenu dans l'exemple 1.4.4. On essaie maintenant d'écrire la matrice de u dans cette base (au départ et à

l'arrivée). On a

$$\begin{array}{lcl} u(\overline{1}) & = & \overline{X} \\ & = & \overline{(X-\lambda)} + \lambda\overline{1} \\ u(\overline{X-\lambda}) & = & X(\overline{X-\lambda}) \\ & = & (\overline{X-\lambda})^2 + \lambda(\overline{X-\lambda}) \\ \dots & \dots & \dots \\ & \dots & \dots \\ u(\overline{X-\lambda})^{n-1} & = & X(\overline{X-\lambda})^{n-1} \\ & = & (\overline{X-\lambda})^n + \lambda(\overline{X-\lambda})^{n-1} \\ & = & \lambda(\overline{X-\lambda})^{n-1} \end{array}$$

La matrice obtenue est la suivante :

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 1 & \lambda & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & \lambda & 0 \\ 0 & \dots & 0 & 1 & \lambda \end{pmatrix}$$

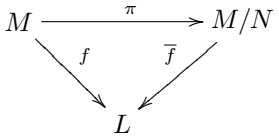
qui n'est autre que la matrice appelée "bloc de Jordan".

Nous allons maintenant passer à des résultats très utiles pour construire des morphisimes de modules.

Théorème 1.4.6 *Soit $f : M \to L$ un morphisme de A-module, N un sous-module de M et soit $\pi : M \to M/N$ la projection canonique. Supposons que N soit contenu dans* $\mathrm{Ker}(f)$*. Alors f se factorise de manière unique à travers M/N c'est à dire qu'il existe un unique morphisme de A-modules*

$$\overline{f} : M/N \to \mathrm{Im}(f)$$

tel que $\overline{f} \circ \pi = f$.



En particulier, si $N = \mathrm{Ker}(f)$ et $L = \mathrm{Im}(f)$, $\overline{f}$ est un isomorphisme.

Preuve. Commençons par définir l'application $\overline{f}$. Soit $x \in M$, comme on veut avoir $\overline{f} \circ \pi = f$, il est naturel de définir

$$\overline{f}(x + N) = f(x)$$

on voit que c'est la seule définition possible pour $\overline{f}$ afin que $\overline{f} \circ \pi = f$. il faut vérifier que ceci est bien définie. Supposons y dans la même classe que x modulo N c'est à dire $x - y \in N$, alors, comme f est un morphisme, on a $f(x) - f(y) \in f(N)$. Or, N est contenu dans $\mathrm{Ker}(f)$. Ceci implique que $f(N) = \{0_L\}$ et donc que $f(x) = f(y)$ ce qu'il fallait montrer. Notons de plus

que l'image de $\overline{f}$ est contenu dans l'image de f. On a donc bien construit une application

$$\overline{f} : M/N \to \mathrm{Im}(f)$$

Montrons que c'est un morphisme de A-modules. Soit $(x_1, x_2) \in M$ et soit $a \in A$, on a :

$$\overline{f}(x_1 + x_2 + N) = f(x_1) + f(x_2) = \overline{f}(x_1 + N) + \overline{f}(x_2 + N)$$

et

$$\overline{f}(a.(x_1 + N)) = f(a.x_1) = a.f(x_1) = a.\overline{f}(x_1 + N)$$

d'où le résultat.

Il est clair que l'image de $\overline{f}$ est $\mathrm{Im}(f)$. Supposons maintenant que $N = \mathrm{Ker}(f)$ et calculons le noyau de $\overline{f}$. Supposons que $x \in M$ est tel que $\overline{f}(x+N) = 0_L$ alors $f(x) = 0_L$ donc $x \in N$. D'où le résultat. On conclut que dans ce cas $\overline{f}$ est un isomorphisme.

□

Si M et N sont deux sous-modules d'un A-module E alors l'ensemble

$$M + N := \{x + y \mid x \in M, y \in N\}$$

est un sous-module de E appelé somme des sous-modules M et N. De même l'intersection $M \cap N$ est un sous-module de M.

Voici un exemple d'application du théorème ci-dessus :

Corollaire 1.4.7 *Soit M et N deux sous-modules d'un A-module alors on a un isomorphisme de A-modules*

$$M/N \cap M \simeq (M + N)/N$$

Preuve. On dispose de deux morphismes naturels de A-modules :

$$M \to M + N \text{ et } M + N \to (M + N)/N$$

Si on les compose, on obtient un morphisme de A-modules.

$$\varphi : M \to (M + N)/N$$

qui est surjectif car si $x \in M$, $y \in N$ alors $\varphi(x) = x + N = x + y + N$. De plus, si $x \in N$ alors $\varphi(x + N) = 0_{(M+N)/N}$. Le noyau de φ est donc N. On peut appliquer le théorème de passage au quotient qui nous donne l'existence d'un isomorphisme

$$M/N \cap M \simeq (M + N)/N$$

□

Le résultat ci-dessus est connu comme le "premier théorème d'isomorphisme". Voici le second :

Corollaire 1.4.8 *Soit M un A-module, N un sous-module de M et P un sous-module de N alors P est un sous-module de M et on a un isomorphisme de A-modules*

$$(M/P)/(N/P) \simeq M/N$$

Preuve. Notons tout d'abord que N/P est bien un sous-ensemble de M/P et que ces deux ensembles ont ue structure de A-modules. Le quotient $(M/P)/(N/P)$ a donc bien un sens.

On a un morphisme naturel $M \to M/N$. Celui-ci passe au quotient M/P car P est contenu dans son noyau (qui est N). On dispose donc d'un morphisme de A-modules

$$\varphi : M/P \to M/N$$

. Celui-ci est surjectif car si $x \in M$ alors $\varphi(x+P) = x+N$. Calculons son noyau. Supposons que $x \in M$ est tel que $\varphi(x+P) = 0_{M/N}$ alors $x \in N$ et on a donc $x+P \in N/P$. Il suit $\mathrm{Ker}(\varphi) = N/P$. On a donc bien un isomorphisme

$$(M/P)/(N/P) \simeq M/N$$

□

1.5 Produit direct et somme direct

Proposition 1.5.1 *Soit A un anneau et soit $(M_i)_{i\in I}$ une famille de A-modules. Alors le produit cartésien*

$$\prod_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i\}$$

peut être muni d'une structure de A-module en posant, pour tout $a \in A$, $(m_i)_{i\in I} \in (M_i)_{i\in I}$ et $(m'_i)_{i\in I} \in (M_i)_{i\in I}$:

- $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$
- $a.(m_i)_{i\in I} = (a.m_i)_{i\in I}$

Cette structure est l'unique structure possible faisant des projections

$$\begin{array}{rccc} p_j : & \prod_{i\in I} M_i & \to & M_j \\ & (m_i)_{i\in I} & \mapsto & m_j \end{array}$$

des morphismes de A-modules (pour tout $j \in I$). .

Preuve. Commençons par l'unicité : si on impose que les p_j soient des morphismes, ceci implique que pout tout $j \in I$, $a \in A$ et $m_j \in M_j$, on a

$$p_j(a.((m_i)_{i\in I})) = a.p_j(((m_i)_{i\in I}))$$

soit encore

$$p_j(a.((m_i)_{i\in I})) = a.m_j$$

Ceci impose donc que

$$a.(m_i)_{i\in I} = (a.m_i)_{i\in I}$$

D'où l'unicité. Le fait que l'on obtient une structure de A-module avec ces lois est facilement vérifié.

□

Définition 1.5.2 Soit A un anneau et soit $(M_i)_{i\in I}$ une famille de A-modules. La somme directe (externe) des modules M_i ($i \in I$) est le sous-module de $\prod_{i\in I} M_i$ défini comme

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \mid \forall i \in I, m_i \in M_i, \text{ tous nuls sauf pour un nbre fini}\}$$

Il est clair que $\bigoplus_{i\in I} M_i$ a bien une structure de sous-module de $\prod_{i\in I} M_i$! notons que si I est fini, les deux modules coïncident. Attention ici ! étant donnée la définition ci-dessus, on pourra TOUJOURS écrire la somme directe de deux sous-modules. Par exemple, si M est un A-module, on peut tout à fait considérer le module $M \oplus M$ qui n'est autre que le produit direct $M \times M$. Par contre, il ne faut pas le confondre avec $M + M$ qui est simplement le module M ! on peut alors se demander quand la somme directe telle que définie ci-dessus est la même chose que la somme classique. C'est ce que l'on voit dans le théorème suivant.

Théorème 1.5.3 *Soit A un anneau et $M_1, \ldots, M_n$ une famille finie de sous-modules vérifiant la propriété suivante.*

$$(\star) \qquad \forall i \in \{1, \ldots, n\},\ M_i \cap (M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_n) = 0$$

Alors on a un isomorphisme de A-modules

$$M_1 + \ldots + M_n \simeq \bigoplus_{1\leq i\leq n} M_i$$

Preuve. On doit donc construire un isomorphisme entre $M_1 + \ldots + M_n$ et $\prod_{1\leq i\leq n} M_i$. On considère le morphisme de A-modules

$$\begin{array}{rccc} f: & \prod_{1\leq i\leq n} M_i & \to & M_1 + \ldots + M_n \\ & (m_1, \ldots, m_n) & \mapsto & m_1 + \ldots + m_n \end{array}$$

Il est clair que f est surjectif. Supposons que $(m_1, \ldots, m_n) \in \mathrm{Ker}(f)$ alors

$$m_1 + \ldots + m_n = 0$$

alors pour tout $i = 1, \ldots, n$, on a $m_i = -(m_1 + \ldots + m_{i-1} + m_{i+1} + m_n) \in M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_n$. Les m_i sont donc nuls donc $(m_1, \ldots, m_n) = 0_{\prod_{i\in I} M_i}$ donc f est injective donc un isomorphisme.

□

Grâce au théorème précedent on voit que lorsque l'hypothèse $(\star)$ est vérifiée alors $M_1 + \ldots + M_n$ peut être identifié à $\bigoplus_{i\in I} M_i$. Dans ce cas, on fera systématiquement cette identification. On dira en particulier que $M_1, \ldots, M_n$ sont des sous-modules en *somme directe* si ils satisfont à la propriété $(\star)$. Si M ne peut jamais s'écrire comme somme directe de sous-modules non triviales alors on dira que M est *indécomposable*. Sinon, M est dit *décomposable*. Il y a donc une petite subtilité à comprendre :

- On peut toujours faire la somme directe (externe) de deux A-modules,
- mais deux sous-modules d'un même module ne sont pas nécessairement en somme directe. Ils le sont en fait précisement quand la somme coïncident avec la somme directe (externe). On peut alors parler de *somme directe interne*

Revenons maintenant au cas général où I est éventuellement infini. Si tous les M_i sont égaux au même module M, on note $M^{(I)}$ la somme directe $\bigoplus_{i\in I} M_i$. C'est donc l'ensemble des familles d'éléments indexés par I, ces éléments étant nuls, sauf pour un nombre fini. C'est un sous-module du A-module $M^I = \prod_{i\in I} M$. On se servira en particulier des notations A^I et $A^{(I)}$ dans la suite, les deux A-modules étant distincts, sauf dans le où I est fini.

Remarque 1.5.4 Attention, il peut en résulter un léger conflit de notation : si I est un idéal, la notation I^n peut aussi bien désigner le A-module $I \oplus I \oplus \ldots \oplus I$ que le produit $I.I. \ldots .I$. Cependant, le contexte donnera à quel objet on se réfère, notons en effet que les deux objets n'ont pas la même structure, $I.I. \ldots .I$ est un idéal de A ce qui n'est pas le cas de $I \oplus I \oplus \ldots \oplus I$, sous-module de A^n.

Exemple 1.5.5 Considérons le $\mathbb{R}$-module (= $\mathbb{R}$-espace vectoriel) $\mathbb{C}$ alors on a $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$ (somme directe interne !).

Exemple 1.5.6 Si on se donne un anneau A alors $A \times A$ est un A-module et les A sous-modules $A \times \{e\}$ et $\{e\} \times A$ satisfont à la propriété ($\star$). on a donc $A \times A = A \times \{e\} \oplus \{e\} \times A \simeq A \oplus A$

Exemple 1.5.7 Considérons le $\mathbb{Z}$-module $\mathbb{Z}$. Les sous-modules sont les idéaux de $\mathbb{Z}$ et comme $\mathbb{Z}$ est principal, ils sont de la forme $a\mathbb{Z}$ où $a \in \mathbb{Z}$. Notons d'ailleurs que ces $\mathbb{Z}$-modules sont isomorphes à $\mathbb{Z}$. deux sous-modules de $\mathbb{Z}$, $a\mathbb{Z}$ et $b\mathbb{Z}$ avec $(a, b) \in \mathbb{Z}^2$ non nuls ne peuvent être en somme directe car ab appartient nécessairement aux deux modules. Le $\mathbb{Z}$-module $\mathbb{Z}$ est donc indécomposable.

La notion d' "indécomposabilité" est importante. En effet, si un module se décompose en somme directe, il suffit de connaître ses composantes pour connaître le module lui-même. Un problème naturel en algèbre consiste donc à trouver tous les modules indécomposables (à isomorphisme près) pour un certain anneau A.

Afin de déterminer si un A-module est "décomposable" et afin de trouver sa décomposition, la notion de "suite exacte" est très utile.

Définition 1.5.8 Soit M, N et P trois A-modules et soit $\phi : M \to N$ et $\psi : N \to P$ deux morphismes. Alors on dit que que l'on a une *suite exacte* :

$$0 \to M \underset{\phi}{\longrightarrow} N \underset{\psi}{\longrightarrow} P \to 0$$

si les trois propriétés suivantes sont vérifiés :

1. ϕ est injective,
2. ψ est surjective,
3. $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$.

Si de plus, il existe un morphisme $\chi : P \to N$ tel que $\psi \circ \chi = \mathrm{Id}_P$ alors on dit que cette suite exacte est *scindée*.

Remarque 1.5.9 Attention ce n'est pas parce qu'une suite est scindée que le second morphisme ψ est un isomorphisme ! par exemple $\psi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ tel que $\psi(a, b) = a$ pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ est un morphisme de $\mathbb{Z}$-modules. Alors $\chi : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ tel que $\chi(a) = (a, 0)$ est un morphisme de $\mathbb{Z}$-modules tel que $\psi \circ \chi = \mathrm{Id}_{\mathbb{Z}}$ pourtant il est clair que ψ n'est pas injective.

Pour construire une suite exacte, on peut se servir du quotient de modules : c'est un exemple classique, il suffit de prendre M un A-module, N un sous-module de M alors si $i : N \to M$ est l'injection canonique et $p : M \to M/N$ la projection, on voit facilement que la suite

$$0 \to N \underset{\phi}{\longrightarrow} M \underset{\psi}{\longrightarrow} M/N \to 0$$

est exacte.

Par contre, une suite exacte quelconque n'est pas scindée en général : prenons $M = \mathbb{Z}$, $N = 2\mathbb{Z}$. La suite suivante est donc exacte :

$$0 \to 2\mathbb{Z} \underset{\phi}{\longrightarrow} \mathbb{Z} \underset{\psi}{\longrightarrow} \mathbb{Z}/2\mathbb{Z} \to 0$$

Il n'existe pas de morphisme de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}$ autre que le morphisme nul. Ceci implique qu'un morphisme $\chi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ tel que $\psi \circ \chi = \mathrm{Id}_{\mathbb{Z}/2\mathbb{Z}}$ ne peut exister.

Comment construire une suite scindée ? ceci se fait grâce à la somme directe. il suffit de prendre M un A-module, N un autre A-module. On considère $\phi : M \to M \oplus P$ l'injection canonqiue et $\psi : M \oplus P \to P$ la projection, alors la suite

$$0 \to M \underset{\phi}{\longrightarrow} M \oplus P \underset{\psi}{\longrightarrow} P \to 0$$

est exacte et scindée grâce à $\chi : P \to M \oplus P$ tel que $\chi(m) = (0, m)$ pour $m \in P$.

En fait, ces deux propriétés admettent des "réciproques" :

Proposition 1.5.10 *Soit M, N et P trois A-module. On suppose que l'on a une suite exacte*

$$0 \to M \underset{\phi}{\longrightarrow} N \underset{\psi}{\longrightarrow} P \to 0$$

Alors on a

$$N/\phi(M) \simeq P$$

avec $\phi(M) \simeq M$. Si de plus la suite est scindée on a :

$$N \simeq M \oplus P.$$

Preuve. La première partie de la preuve est évidente par passage au quotient et parce que ϕ est injective. Pour la seconde partie, on considère le morphisme de A-modules :

$$\begin{array}{rccc} f : & M \oplus P & \to & N \\ & (m, p) & \mapsto & \phi(m) + \chi(p) \end{array}$$

celui-ci est surjectif. En effet, si $n \in N$, prenons $p = \psi(n)$ et remarquons que $n - \chi(\psi(n)) \in \mathrm{Ker}(\psi) = \phi(M)$. Il existe donc $m \in M$ tel que $\phi(m) = n - \chi(\psi(n))$. On a donc

$$\phi(m) + \chi(p) = n$$

ce qui prouve la surjectivité. Prouvons l'injectivité en calculant le noyau de f. Suppons que $(m, p) \in M \oplus P$ vérifie :

$$\phi(m) + \chi(p) = 0$$

en composant par ψ, on obtient $p = 0$ car $\psi \circ \phi = 0$. Alors $\phi(m) = 0$ donc $m = 0$ car ϕ est injective. Ceci prouve l'injectivité. Donc f est bien un isomorphisme. □

Une suite exacte est donc liée à la structure de quotient, une suite exacte scindée à celle de somme directe.

Exemple 1.5.11 Soit p un nombre premier. Considérons le morphisme de $\mathbb{Z}$-modules

$$\begin{array}{rccc} f: & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p^2\mathbb{Z} \\ & x+p\mathbb{Z} & \mapsto & px+p\mathbb{Z} \end{array}$$

son noyau est triviale donc f est injective et son image est $p\mathbb{Z}/p^2\mathbb{Z}$. Maintenant, le morphisme

$$\begin{array}{rccc} g: & \mathbb{Z}/p^2\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & x+p^2\mathbb{Z} & \mapsto & x+p\mathbb{Z} \end{array}$$

est surjective et a un noyau égale à $p\mathbb{Z}/p^2\mathbb{Z}$. Ceci implique que la suite suivante de $\mathbb{Z}$-modules est exacte :

$$0 \to \mathbb{Z}/p\mathbb{Z} \underset{f}{\longrightarrow} \mathbb{Z}/p^2\mathbb{Z} \underset{g}{\longrightarrow} \mathbb{Z}/p\mathbb{Z} \to 0$$

Mais cette suite ne peut être scindée. En effet, si elle l'était, on aurait un isomorphisme

$$\mathbb{Z}/p^2\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$

de $\mathbb{Z}$-modules donc de groupes. Ceci est absurde car on a au moins un élément d'ordre p^2 dans $\mathbb{Z}/p^2\mathbb{Z}$ et aucun dans $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Chapitre 2

Modules libres, modules de type fini

Dans ce chapitre, on s'intéresse aux classifications de modules. Nous donnons la définition d'un module irréductible (l'équivalent d'un groupe simple pour les modules) puis nous nous intéressons aux généralisations possibles de certaines propriétés des espaces vectoriels. En particulier, le concept de "base" nous amenera à introduire les définitions de modules libres et modules de type fini.

2.1 Problématique

On désire ici trouver des équivalents aux théorèmes fondametaux d'algèbre linéaire, déjà connus pour les espaces vectoriels, à savoir l'existence de base, l'existence d'une théorie de la dimension pour les modules. Pour celà nous, avons besoin de la définition de familles libres, génératrices, de bases etc ... celles-ci sont assez naturelles dans le cadre de ce cours.

Définition 2.1.1 Soit M un A-module et soit $\mathcal{M} := (m_i)_{i\in I}$ une famille d'éléments de A. On dit que la famille $\mathcal{M}$ est

- une *famille génératrice* si pour tout $m \in M$, il existe une collection d'éléments $(a_i)_{i\in I} \in A^{(I)}$ tels que
$$m = \sum_{i\in I} a_i m_i$$
- une *famille libre* si l'égalité
$$0 = \sum_{i\in I} a_i m_i$$
pour une collection d'éléments $(a_i)_{i\in I} \in A^{(I)}$ implique que tous les a_i sont nuls.
- une *base* si la famille est à la fois libre et génératrice.

Remarque 2.1.2 Notons que tout module admet une partie génératrice : il suffit de prendre tous ses éléments.

La notion de base est d'une importance considérable dans le cas des espaces vectoriels. Avoir une base pour un espace vectoriel c'est avoir un ensemble d'éléments qui contrôlent entièrement et de façon minimale l'espace. C'est grâce à cette notion que l'on peut :

- développer une théorie de la dimension,
- définir de façon simple et complète un morphisme en envoyant les éléments d'une base vers une combinaison linéaire d'éléments d'une base d'arrivée et ainsi ...
- ... développer le concept de matrice et toutes les notions qui lui sont rattachées (déterminant, inversibilité, matrices semblables etc.)

Or, dans le cadre général que l'on adopte dans ce cours, des problèmes apparaissent déjà sur les exemples les plus classiques de A-modules :

- Si A n'est pas un anneau intègre, on a alors des diviseurs de zéros. Si on prend un idéal engendré par un diviseur de zéro $a \in A$, il ne peut avoir de base. En effet, il existe $b \in A$ tel que $a.b = 0$. Mais alors pour tout élément x dans l'idéal on aura $b.x = 0$, sans que b soit nul ! par exemple, dans l'anneau $\mathbb{Z}/4\mathbb{Z}$, l'ensemble $\{2 + 4\mathbb{Z}, 0 + 4\mathbb{Z}\}$ est un idéal et on a $(2 + 4\mathbb{Z}).(2 + 4\mathbb{Z}) = 0 + 4\mathbb{Z}$. Cet idéal ne peut dons pas être un $\mathbb{Z}/4\mathbb{Z}$-module libre.
- Même dans le cas non intègre, prenons $A = \mathbb{Z}$ et $M = \mathbb{Z}/4\mathbb{Z}$ alors on voit que pour tout élément x de M, on a $4.x = 0$ donc aucune famille de M ne peut être libre !

Remarque 2.1.3 Une sous-famille d'une famille libre est nécessairement libre et une surfamille d'une famille génératice est génératrice.

La remarque ci-dessus motive les définitions suivantes :

Définition 2.1.4 Soit M un A-module. On dit que M est un A-module *libre* si M possède une base. On dit que M est un A-module *de type fini.* si M a une famille génératrice finie.

Il est clair que tout module n'est pas nécessairement de type fini, ceci est déjà le cas pour les espaces vectoriels : il existe des espaces vectoriels sans partie génératices finie : l'anneau des polynômes sur un corps $\mathbb{K}[X]$ par exemple en tant que $\mathbb{K}$-espace vectoriel.

Exemple 2.1.5 Si $A = \mathbb{K}$ est un corps alors tout A-module est libre car tout A-module possède une base.

{exideal}

Exemple 2.1.6 Un idéal de A est aussi un A-module et il est clair qu'il est de type fini en tant que A-module si et seulement si il est de type fini en tant qu'idéal. En particulier, A est toujours un A-module libre de type fini, une base étant donné par $\{1_A\}$. Supposons maintenant que I soit un idéal, libre comme A-module. Alors on a une famille libre $\mathcal{F}$ de I. Supposons que cette famille contienne strictement plus d'un élément : disons a et b. Ces éléments sont non nuls, mais on a alors :

$$a.b - b.a = 0$$

ce qui contredit le fait que $\mathcal{F}$ soit libre. Donc si I est libre, I a une famille libre et génératrice d'un seul élément. Ceci implique que I est principal engendré par un élément non diviseur de zéro.

Exemple 2.1.7 $A^{(I)}$ est toujours un A-module libre, une base étant donnée par la famille $\{n_j \mid j \in I\}$ où pour tout $j \in I$, on a $n_j = (n_j^i)_{i\in I}$ avec $n_j^i = 1$ si $i = j$ et 0 sinon. Si I est infini, ce module n'est pas de type fini. Si I est fini, c'est un module libre de type fini.

Exemple 2.1.8 Par contre, $\mathbb{Z}^{\mathbb{N}}$ n'est pas un $\mathbb{Z}$-module libre, c'est d'ailleurs assez difficile à montrer.

{mat}

Remarque 2.1.9 Prenons $I = \{1, \ldots, n\}$ alors A^n est libre de type fini et possède une base "canonique" : $\{e_j \mid j = 1, \ldots, n\}$ où pour tout $j = 1, \ldots, n$, on a $e_j = (x_j^i)_{i=1,\ldots,n}$ avec $x_j^i = 1$ si $i = j$ et 0 sinon. Un morphisme f de A^n dans A^m est uniquement et entièrement défini par la donnée des $f(e_j)$ avec $j = 1, \ldots, n$, que l'on peut exprimer dans la base canonique de A^m. Ces informations peuvent être stockées dans une matrice, exactement comme pour les espaces vectoriels, où on dispose les coefficients des éléments de la base canonique de A^m apparaissant dans les $f(e_j)$ avec $j = 1, \ldots, n$ en colonnes. On obtient une matrice à m lignes et n colonnes. On voit facilement que la matrice d'une composition de morphismes est la multiplication des matrices associées (dans les bases appropriées). Il est aussi clair que si $n = m$, la matrice identité représente le morphisme identité.

Un module n'est pas nécessairement libre comme on vient de le voir. Par contre, on a le résultat suivant :

{modquo}

Proposition 2.1.10 *Tout module M est (isomorphe au) quotient d'un module libre.*

Preuve. On prend une partie génératrice $(m_i)_{i\in I}$ de M et on considère le morphisme de A-module :

$$\begin{array}{rccc} \Psi : & A^{(I)} & \to & M \\ & (a_i)_{i\in I} & \mapsto & \sum_{i\in I} a_i m_i \end{array}$$

celui-ci est surjectif par définition. Par passage au quotient, on obtient

$$M \simeq A^{(I)}/\mathrm{Ker}(\Psi)$$

ce qu'il fallait montrer.

□

Dans la preuve de la proposition précédente, on retiendra le rôle joué par l'application surjective $\Psi : A^{(I)} \to M$. Nous allons maintenant étudier plus en profondeur la structure des modules de type fini puis des modules libres.

2.2 Modules de type fini

Dans cette partie, nous essayons de déterminer des propriétés fondamentales des modules de type fini. En adaptant la preuve de la proposition 2.1.10 : on voit que tout module de type fini est isomorphe à un quotient de A^n où $n \in \mathbb{N}$. On a déjà vu qu'un A-module arbitraire n'est pas nécessairement de type fini. Pour ceci, il suffit de prendre un idéal qui ne soit pas de type fini dans un anneau. Voici un exemple d'un tel anneau.

Exemple 2.2.1 Soit A l'anneau des entiers algébriques sur $\mathbb{Z}$ c'est à dire l'ensemble des racines des polynômes unitaires à coefficients dans $\mathbb{Z}$ [1]. Soit $a \in A$ un élément non inversible de A, par exemple, $a = 2$ (on montre facilement que les rationnels non entiers ne sont pas des entiers algébriques). Pour tout $n \in \mathbb{N}$, il existe a_n une racine 2^nième de a tel que l'on a une suite d'idéaux emboîtés :

$$(a_0) \subset (a_1) \subset .... \subset (a_n).$$

En effet, on a $a_n^{2^n} = a$ donc il suffit de choisir $a_{n-1} = a_n^2$, ensuite $a_{n-2} = a_{n-1}^2$ etc. De plus, une racine 2^nième de a est bien dans A car racine de $X^{2^n} - a ? in \mathbb{Z}[X]$. La suite d'idéaux est strictement croissante car si $(a_k) = (a_{k+1})$ alors il existe $\gamma \in A$ tel que $a_{k+1} = \gamma a_k$. Par hypothèse, on a

$$a_k^{2^k} = a.$$

On obtient donc $a_{k+1}^{2^{k+1}} = \gamma^{2^{k+1}} a_k^{2^{k+1}}$. Il suit ainsi $a = \gamma^{2^{k+1}} a^2$ d'où $\gamma^{2^{k+1}} a = 1$ car A est intègre. Ceci est absurde car a est non inversible.

Ceci implique que l'idéal

$$I = \bigcup_{n \in \mathbb{N}} (a_n)$$

n'est pas de type fini. En effet, si il était engendré par un nombre fini d'éléments de I, ces éléments se trouveraient dans un certain idéal (a_p) et la suite serait stationnaire à partir de (a_p).

Mais cet exemple nous dit plus : un sous-module d'un A-module de type fini n'est pas nécessairement de type fini ! en effet l'anneau A ci-dessus est un A-module de type fini et l'idéal, un sous-module de cet anneau qui ne l'est pas. Un anneau pour lequel tout idéal est de type fini est appelé un anneau *noethérien* (un exemple est un anneau principal). Pour ces anneaux, la situation est beaucoup plus agréable :

{noeth}

Théorème 2.2.2 *Soit A un anneau noethérien alors tout sous-module d'un A-module de type fini est de type fini.*

Preuve. Soit A un anneau noetherien, M un A-module de type fini engendré par des éléments m_1,...,m_r et soit N un sous-module de M. On considère l'application

$$\begin{array}{rccc} \phi : & A^r & \to & M \\ & (a_1, ..., a_r) & \mapsto & \sum_{i=1}^r a_i m_i \end{array}$$

On montre que les sous-modules de A^r sont de types finis. Soit N' un sous-module de A^r. On a des morphismes surjectifs de A-modules

$$\begin{array}{rccc} \pi_i : & A^r & \to & A \\ & (a_1, ..., a_r) & \mapsto & a_i \end{array}$$

et il est clair que $N' = \bigoplus_{1 \leq i \leq r} \pi_i(N')$. Comme les $\pi(N')$ sont des sous modules du A-modules A donc des idéaux, ils sont de types finis. Ainsi N' est aussi de type fini. Il suit en particulier que $N' := \Phi^{-1}(N)$ est de type fini donc engendré

1. on démontrera ou redémontrera plus loin que cet ensemble est bien un sous-anneau de $\mathbb{C}$.

par des éléments f_1, ..., f_k de A^r. Alors N est engendré par $\phi(f_1)$, ..., $\phi(f_k)$. En effet, si $n \in N$, comme Φ est surjective (car M est de type fini), il existe $f \in A^r$ et des éléments b_1,....,b_s de A tels que tel que $f = \sum_{i=1}^{s} b_i f_i$ et $n = \phi(f)$. On a alors

$$n = \sum_{i=1}^{s} b_i \phi(f_i)$$

d'où le résultat.

□

{typefini}

Proposition 2.2.3 *Soit M un A-module de type fini et soit $\mathcal{M}$ une famille génératrice de M alors il existe une sous famille de $\mathcal{M}$ qui est génératrice et finie.*

Preuve. Come M est de type fini, il exise $\mathcal{N} = \{n_i, \quad i = 1, \ldots, k\}$ une famille génératrice finie de M. Par hypothèse, pour tout $i \in \{1, \ldots, k\}$, il existe des scalaires tous nuls sauf pour un nombre fini $a_{i,m}$ où $m \in \mathcal{M}$ tel que

$$n_i = \sum_{m \in \mathcal{M}} a_{i,m}.m$$

Notons $\mathcal{M}_i \subset \mathcal{M}$ l'ensemble des m tel que $a_{i,m} \neq 0$. C'est un ensemble fini. Donc l'ensemble $\mathcal{N} = \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_n$ est aussi finie. Tout éléments de M s'écrit comme une combinaison des n_i et tout n_i s'écrit comme combinaison d'éléments de $\mathcal{N}$. Ceci implique que $\mathcal{N}$ est une famille génératrice.

□

Ainsi, si M est un A-module libre, M admet une base qui est a priori infini. Pourtant si on suppose M de type fini, la proposition ci-dessus nous assure l'existence d'une sous-famille finie de notre base qui est encore g{enératrice. En tant que sous-famille d'une famille libre, elle le reste également. On a donc alors une base fini. Bref, un A-module libre de type fini admet une base avec un nombre fini d'éléments.

On va maintenant analyser le comportement de cette propriété pour les structures évoqués ans le chapitre précédent.

Proposition 2.2.4 *Soit M un A-module de type fini et N un sous-module de M alors M/N est de type fini.*

Preuve. Si $(m_i)_{i=1,\ldots,n}$ est une famille génératrice de M alors $(m_i + N)_{i=1,\ldots,n}$ est une famille génératrice de M/N et le résultat suit.

□

Proposition 2.2.5 *Soient A et B deux anneaux, $f : A \to B$ un morphisme d'anneaux. Soit M un B-module. Alors, par restriction des scalaires, M est aussi un A-module. Si celui-ci est de type fini alors M est de type fini en tant que B-module.*

Preuve. Si $(m_i)_{i=1,\ldots,n}$ est une famille génératrice de M en tant que B-module. Montrons que cette famillle reste génératrice pour M en tant que A-module. Soit

$m \in M$ alors il existe une famille $(a_i)_{i=1,\dots,n}$ d'éléments de A telle que

$$m = \sum_{i=1}^{n} a_i.m_i$$

alors par définition de l'action de A on a

$$m = \sum_{i=1}^{n} f(a_i).m_i$$

d'où le résultat.

□

Remarque 2.2.6 Attention, la réciproque du résultat ci-dessus est fausse : si on prend $B = \mathbb{K}[X]$ et $A = \mathbb{K}$ alors $M = B = \mathbb{K}[X]$ est un A-module de type fini mais par restriction des scalaires (via l'injection canonique), on obtient une structure de $\mathbb{K}$-module qui n'est pas de type fini !

{fini}

Exemple 2.2.7 Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et soit u un endomorphisme de E. Alors on peut associer à cette donnée une structure de $\mathbb{K}[X]$ module sur E comme nous l'avons vu dans la section 1.2. Toute famille génératrice de E comme $\mathbb{K}$-module est bien sûr génératrice comme $\mathbb{K}[X]$-module car $\mathbb{K} \subset \mathbb{K}[X]$. Il suit que E est un $\mathbb{K}[X]$-module de type fini.

2.3 Torsion d'un module

Le premier obstacle quand à la liberté d'un module se trouve dans l'eventuelle "torsion" de celui-ci.

{torsion}

Définition 2.3.1 Soit M un A-module, soit $m \in M$ et soit S un sous-ensemble de M.

- On dit que $m \in M$ est un *élément de torsion* si il existe $\lambda \in A$ non nul et non diviseur de zéro tel que $\lambda.m = 0$. L'ensemble des éléments de torsion est noté $T_A(M)$.
- On dit que M est *de torsion* si $T_A(M) = M$ et sans torsion si $T_A(M) = \{0\}$.
- On note $\mathrm{Ann}_A(S)$ l'ensemble des éléments λ de A tels que pour tout $s \in S$, on a $\lambda.s = 0$.

Exemple 2.3.2 Si $A = \mathbb{Z}$ et si $M = \mathbb{Z}^n$ alors M est sans torsion.

Exemple 2.3.3 Si $A = \mathbb{Z}$ et si $M = \mathbb{Z}/n\mathbb{Z}$ alors on voit que $T_A(M) = \mathbb{Z}/n\mathbb{Z}$ car pour tout $x \in \mathbb{Z}$, on a $n.(x + n\mathbb{Z}) = 0_{\mathbb{Z}/n\mathbb{Z}}$.

Exemple 2.3.4 $\mathbb{Q}$ est un $\mathbb{Z}$-module dont $\mathbb{Z}$ est un sous-module. On peut considérer le module quotient $\mathbb{Q}/\mathbb{Z}$. Si $p/q \in \mathbb{Q}$ avec $(p, q) \in (\mathbb{Z}^*)^2$ alors $q.(p/q) \in \mathbb{Z}$. Donc $p/q + \mathbb{Z} \in T_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z})$. Il suit que $T_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

Exemple 2.3.5 $\mathbb{R}$ est un $\mathbb{Z}$-module dont $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-modules. On peut considérer le module quotient $\mathbb{R}/\mathbb{Z}$. Si $x \in \mathbb{R}$ alors $x + \mathbb{Z}$ est de torsion si et seulement si il existe $n \in \mathbb{Z}$ tel que $nx \in \mathbb{Z}$. Ceci implique que $x \in \mathbb{Q}$. Réciproquement, si $x = p/q \in \mathbb{Q}$ avec $(p, q) \in (\mathbb{Z}^*)^2$ alors $q.(x + \mathbb{Z}) = 0_{\mathbb{R}/\mathbb{Z}}$. Il suit que $T_{\mathbb{Z}}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

Proposition 2.3.6 *Soit M un A-module alors $T_A(M)$ est un sous-module de M appelé le sous-module de torsion de M. Pour toute partie $S \subset M$, l'ensemble $\mathrm{Ann}_A(S)$ est un idéal de A appelé l'annulateur de S dans A.*

Preuve. $T_A(M)$ est un sous-module de M. En effet, $T_A(M) \neq \emptyset$ car $0 \in T_A(M)$. De plus, si $a \in A$ et $(m_1, m_2) \in T_A(M)^2$. Il existe des éléments λ_1 et λ_2 de A non nul et non diviseurs de zéro tels que

$$\lambda_1 m_1 = 0 \text{ et } \lambda_2 m_2 = 0$$

Il suit alors (par commutativité de A).

$$\lambda_1 \lambda_2 (m_1 - m_2) = 0$$

et comme $\lambda_1\lambda_2$ est non nul et n'est pas un diviseur de zéro, on peut conclure que $m_1 - m_2 \in T_A(M)$. Si $a \in A$ et $m \in T_A(M)$, il existe $\lambda \in A$ non diviseur de zéro tel que $\lambda.m = 0$ alors $\lambda.a.m = a.(\lambda.m) = 0$ donc $a.m \in T_A(M)$. Tout ceci prouve que $T_A(M)$ est un sous-module de M.

Soit maintenant $S \subset M$ alors $\mathrm{Ann}_A(S)$ est un sous-groupe de A. En effet, $\mathrm{Ann}_A(S)$ est non vide car $0 \in \mathrm{Ann}_A(S)$. Si a_1 et a_2 sont dans $\mathrm{Ann}_A(S)$, alors pour tout $s \in S$, on a $(a_1 - a_2).s = 0$ donc $a_1 - a_2 \in \mathrm{Ann}_A(S)$. Soit $a \in A$ et $a_1 \in \mathrm{Ann}_A(S)$ alors pour tout $s \in S$, on a $a.a_1.s = 0$. Donc on a $a.a_1 \in \mathrm{Ann}_A(S)$. Ceci implique que $\mathrm{Ann}_A(S)$ est un idéal de A.

□

Remarque 2.3.7 La preuve ci-dessus nous montre que l'hypothèse "$\lambda \in A$ non nul et non diviseur de zéro" dans la définition 2.3.1 est essentiel afin d'obtenir une structure de module sur $T_A(M)$.

On voit facilement que si un module est de torsion, il ne peut être libre car trouver une famille libre dans ce module s'avère impossible. Mieux (ou pire !) : si M n'est pas sans torsion, il existe un élément non nul $m \in M$ de torsion. Soit alors $\lambda \in A$ non nul et non diviseur de 0 tel que $\lambda.m = 0$. Supposons alors M libre de base $\{m_i \mid i \in I\}$ alors il existe $(a_i)_{i\in I}$ une famille d'éléments de A tous nuls sauf pour un nombre fini (et non tous nuls) tel que

$$m = \sum_{i\in I} a_i m_i$$

On a alors

$$\lambda.m = \sum_{i\in I} \lambda.a_i m_i = 0$$

Or au moins un des a_i est non nul et on a $\lambda.a_i = 0$ car $\{m_i \mid i \in I\}$ forme une base. Ceci contredit le fait que λ est non diviseur de 0. On vient de montrer :

Proposition 2.3.8 *Soit M un A-module libre. Alors M est sans torsion.*

On peut alors toujours “fabriquer” un module sans torsion à partir d'un module arbitraire.

Proposition 2.3.9 *Soit M un A-module alors le A-module $M/T_A(M)$ est sans torsion.*

Preuve. Soit $m \in M$, supposons que $m + T_A(M)$ soit un élément de torsion. Alors il existe un élément $a \in A$ non nul et non diviseur de zéro tel que $a.m + T_A(M) = 0_{M/T_A(M)}$ il suit donc $a.m \in T_A(M)$. Mais alors, il existe $b \in A$ non nul et non diviseur de zéro tel que $b.a.m = 0$. Comme b et a sont non diviseur de zéro, l'élément $b.a$ est non nul et non diviseur de zéro. Il suit $m \in T_A(M)$. On conclut donc $m + T_A(M) = 0_{M/T_A(M)}$ et donc $M/T_A(M)$ est sans torsion. □

On vient de dire qu'un module libre est toujours sans torsion, mais la réciproque est-elle vrai ? la réponse est NON en général. Pour trouver un contre-exemple, l'example 2.1.6 nous indique qu'il suffit de trouver un anneau intègre et non principal : on disposera alors d'un idéal non principal dont tous les éléments sont non diviseurs de zéro. D'après cet exemple, cet idéal ne pourra comporter de base. On prendra donc par exemple $\mathbb{K}[X, Y]$ pour X et Y deux indéterminées et l'idéal (X, Y) ne peut être libre.

Dans le prochain chapitre, nous étudierons précisement cette question dans le cas où A est principal.

2.4 Modules libres

Commençons par un analogue à la proposition 2.1.10

Proposition 2.4.1 *Si M est un A-module libre de base $\mathcal{M} = \{m_i \mid i \in I\}$ alors M est isomorphe à $A^{(I)}$.*

Preuve. On a un morphisme

$$\begin{array}{rccc} \Psi : & A^{(I)} & \to & M \\ & (a_i)_{i\in I} & \mapsto & \sum_{i\in I} a_i m_i \end{array}$$

celui-ci est surjectif par définition et injectif car $\mathcal{M}$ est libre donc c'est un isomorphisme ce qui permet de conclure. □

{libriso}

Remarque 2.4.2 Si M est A-module libre de type fini alors il possède une base fini $(e_1, \ldots, e_n)$ de n éléments pour un $n \in \mathbb{N}$. On voit alors que M est isomorphe à A^n à travers l'isomorphisme

$$\begin{array}{rccc} \phi : & A^n & \to & M \\ & (a_1, ..., a_n) & \mapsto & \sum_{i=1}^{n} a_i e_i \end{array}$$

On se demande maintenant si, comme dans le cas des espaces vectoriels, le nombre d'éléments dans une base est un invariant des modules libres. La réponse est oui.

{com}

Proposition 2.4.3 *Soit M un module libre de type fini. Alors toutes les bases de M sont finies et ont même cardinal.*

Preuve. On se donne une base de M. D'après la proposition 2.2.3, on peut extraire une famille génératrice finie $\mathcal{B}$ de cette base. Comme c'est une sous-famille d'une famille libre, c'est aussi une famille libre et donc une base. Il est alors claire que la base de départ est égal à $\mathcal{B}$ sinon celle-ci ne serait pas une famille libre. On voit donc déjà que toutes les bases de M ont un cardinal fini.

Supposons maintenant que M admette deux bases $\mathcal{B}_1$ et $\mathcal{B}_2$ de cardinal respectifs n_1 et n_2. En utilisant la remarque 2.4.2, on voit que M est isomorphe à la fois à A^{n_1} et à A^{n_2}. Bref, on a un isomorphisme φ_1 entre ces deux A-modules.

$$\varphi_1 : A^{n_1} \to A^{n_2}$$

d'inverse

$$\varphi_2 : A^{n_2} \to A^{n_1}$$

A ces deux morphismes s'associent naturellement deux matrices $P \in \mathrm{Mat}_{n_2 \times n_1}(A)$ et $Q \in \mathrm{Mat}_{n_1 \times n_2}(A)$ qui vérifient donc (voir la remarque 2.1.9) :

$$Q.P = \mathrm{Id}_{n_1} \text{ et } P.Q = \mathrm{Id}_{n_2}$$

Or A est un anneau commutatif. D'après le théorème de Krull, A possède un idéal maximal $\mathfrak{m}$. Pour toute matrice C, nous notons $\pi(C)$ la matrice dont tous les coefficients sont réduits modulo $\mathfrak{m}$. On voit que les égalités ci-dessus entraîne :

$$\pi(Q).\pi(P) = \mathrm{Id}_{n_1} \text{ et } \pi(P).\pi(Q) = \mathrm{Id}_{n_2}$$

mais ces matrices sont à coefficients dans un corps $\mathbb{K} := A/\mathfrak{m}$ car $\mathfrak{m}$ est maximal. On sait qu'alors on a un isomorphisme de $\mathbb{K}$-espace vectoriel entre $\mathbb{K}^{n_1}$ et $\mathbb{K}^{n_2}$. Ceci implique que $n_1 = n_2$ et conclut la démonstration.

□

Remarque 2.4.4 Ainsi si M est libre avec une base infini, toutes ses bases ont un cardinal infini.

Définition 2.4.5 Si M est un module libre de type fini. On appelle *rang* du module M le cardinal commun des bases de M.

Cette notion de rang généralise donc la notion de dimension pour les espaces vectoriels.

{oplus}

Proposition 2.4.6 *Soit M et N deux A-modules de type fini de rang m et n alors $M \oplus N$ est libre de type fini et de rang $m + n$.*

Preuve. Soit $(e_1, \ldots, e_m)$ une base de M et soit $(f_1, \ldots, f_n)$ une base de N. Alors on vérifie facilement que $((e_i, 0), (0, f_j), 1 \leq i \leq m,\ 1 \leq j \leq n)$ est une base $M \oplus N$.

□

{exlibre}

Exemple 2.4.7 On pose

$$L := \left\{ r \in \mathbb{Q}^{+,*} \mid r = p/q,\ p \text{ et } q \text{ uniquement divisible par les nbres premiers } 2, 3, 5, 7 \right\}$$

L est un groupe abélien pour la loi de multiplication. Par la proposition 1.2.1, on peut mettre ensuite une structure de $\mathbb{Z}$-modules. Attention, comme la loi est ici multiplicative, la structure est donnée comme suit :

$$r.(p/q) = (p/q)^r$$

L est alors libre sur $\mathbb{Z}$ et de rang 4 avec pour base $\{2, 3, 5, 7\}$. En effet, cette famille est libre, si $(a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$, on a

$$2^{a_1}3^{a_2}5^{a_3}7^{a_4} = 1$$

si et seulement si $a_1 = a_2 = a_3 = a_4 = 0$ car 2, 3, 5 et 7 sont tous premiers. La famille est maintenant génératrice : tout élément de L s'écrit :

$$2^{a_1}3^{a_2}5^{a_3}7^{a_4}$$

pour $(a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$.

{det}

Exemple 2.4.8 Nous terminons cette section par un exemple de module libre de rang fini qui nous servira dans la partie suivante. Soit M un A-module libre de type fini et de rang n avec base $(e_1, \ldots, e_n)$.

Une *forme n-linéaire* est une application $f : M^n \to A$ telle que, pour tout $m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n \in M$, l'application

$$\left\{ \begin{array}{ccc} M & \longrightarrow & A \\ x & \longmapsto & f(m_1, \ldots, m_{i-1}, x, m_{i+1}, \ldots, m_n) \end{array} \right.$$

est un morphisme de A-module. En d'autres termes, f est n-linéaire si et seulement si elle est linéaire par rapport à chacune de ses variables.

Soit $f : M^n \to A$ une forme n-linéaire. On dit :

- f est *antisymétrique* lorsque, pour toute permutation $\sigma \in \mathfrak{S}_n$ et pour tous vecteurs $m_1, \ldots, m_n \in M$, on a $f(m_{\sigma(1)}, \ldots, m_{\sigma(n)}) = \varepsilon(\sigma) f(m_1, \ldots, m_n)$.
- f est *alternée* lorsque, pour toute famille $(m_1, \ldots, m_n)$ de vecteurs de M dont deux d'entre eux sont égaux, alors $f(m_1, \ldots, m_n) = 0$.

Notons qu'une forme n linéaire alternée est nécessairement antisymétrique. On vérifie que l'espace des formes linéaires alternées $\mathcal{F}_M^n(A)$ a naturellement une structure de A-module pour les opérations naturelles. Ensuite, on montre qu'étant donnée $a \in A$, il existe une unique forme n-linéaire alternée $f : M^n \to A$ telle que $f(e_1, \ldots, e_n) = a$.

- on montre d'abord l'unicité. Si f est une telle forme, on montre que ceci implique que, étant donnée :

  $$x_j = \sum_{1 \leq i \leq n} a_{i,j} e_i$$

  avec $j = 1, \ldots, n$, une collection d'éléments de M, on a

  $$f(x_1, \ldots, x_n) = a. \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \leq i \leq n} a_{i,\sigma(i)}$$

- on montre que la formule ci-dessus définit bien une forme n-linéaire alternée $f : M^n \to A$ telle que $f(e_1, \ldots, e_n) = a$.

Si on note $\mathcal{B} = (e_1, \ldots, e_n)$, on définit $\det_{\mathcal{B}}$ l'unique forme n linéaire alternée $f : M^n \to A$ telle que $f(e_1, \ldots, e_n) = 1$. Alors, soit $g \in \mathcal{F}_M^n(A)$, on a d'après la discussion ci-dessus $g = g(e_1, \ldots, e_n).f$ ce qui implique que $\mathcal{F}_M^n(A)$ est un A-module libre de rang 1. Une base est donnée par l'application déterminant.

2.5 Théorie matricielle

Dans cette section, nous donnons, assez brièvement, des généralisations de propriétés matricielles déjà connues sur les corps.

Soit M un A-module libre de type fini et de rang n et soit P un A-module arbitraire. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de M.

- Si on se donne un morphisme de A-modules de M dans P alors f est entièrement déterminée par l'image des éléments e_i car la famille de ces éléments est génératrice de M.
- Si on se donne n éléments $p_1, \ldots, p_n$ de P, il existe un morphisme de A-modules envoyant les e_j sur les p_j. Celui-ci est (bien) défini par

$$f(\sum_{1\leq j\leq n} a_j e_j) = \sum_{1\leq j\leq n} a_j p_j$$

les $(a_j)_{1\leq j\leq n}$ étant des éléments de A, car la famille des e_i est libre.

On a donc un unique morphisme qui envoie les e_i sur des éléments p_i donnés dans P. Ceci signifie que l'on a une application bijective :

$$\begin{array}{rccc} \Psi : & \mathrm{Hom}_A(M,P) & \to & P^n \\ & f & \mapsto & (f(e_1), \ldots, f(e_n)) \end{array}$$

On voit facilement que Ψ a une structure de morphisme de A-modules, ce qui montre la proposition suivante :

Proposition 2.5.1 *Soit M un A-module libre de type fini et de rang n et soit P un A-module arbitraire alors on a un isomorphisme*

$$\mathrm{Hom}_A(M,P) \simeq P^n$$

Gardons les hypothèses ci-dessus et ajoutons le fait que P est un A-module libre de rang fini r de base $(e'_1, \ldots, e'_r)$. Considérons l'ensemble des matrices $\mathcal{M}_{r\times n}(A)$ à r lignes et n colonnes et à coefficients dans A. Cet ensemble a une structure de A-modules pour les lois suivantes :

- Soit $(a_{i,j})_{1\leq i\leq r, 1\leq j\leq n} \in \mathcal{M}_{r\times n}(A)$ et $(b_{i,j})_{1\leq i\leq r, 1\leq j\leq n} \in \mathcal{M}_{r\times n}(A)$ alors :

$$(a_{i,j})_{1\leq i\leq r, 1\leq j\leq n} + (b_{i,j})_{1\leq i\leq r, 1\leq j\leq n} = (a_{i,j} + b_{i,j})_{1\leq i\leq r, 1\leq j\leq n}$$

- Soit $(a_{i,j})_{1\leq i\leq r, 1\leq j\leq n} \in \mathcal{M}_{r\times n}(A)$ et $a \in A$ alors :

$$a.(a_{i,j})_{1\leq i\leq r, 1\leq j\leq n} = (a.a_{i,j})_{1\leq i\leq r, 1\leq j\leq n}$$

Il est aussi facile de voir que $\mathcal{M}_{r\times n}(A)$ est un A-module libre de rang rn car une base est donnée par les matrices dont les coefficients sont tous nuls sauf pour un de ceux-ci. Notons $\mathcal{B}_1 = (e_1, \ldots, e_n)$ base de M et $\mathcal{B}_2 = (e'_1, \ldots, e'_r)$, base de P. On vérifie alors qu'on a un isomorphisme :

$$\begin{array}{rccc} \Phi : & \mathrm{Hom}_A(M,P) & \to & \mathcal{M}_{r\times n}(A) \\ & f & \mapsto & \mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f) \end{array}$$

où $\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f) = (a_{i,j})_{1\leq i\leq r, 1\leq j\leq n}$ est défini par :

$$\forall j \in \{1, \ldots, n\},\ f(e_j) = \sum_{1\leq i\leq r} a_{i,j} e'_i$$

et étant donnée des choix de bases, on peut donc identifier un morphisme de A-modules avec la matrice associée. Il suit donc (ce que l'on pouvait aussi déduire de la proposition précédente) :

Proposition 2.5.2 *Soit M un A-module libre de type fini et de rang n et soit P un A-module libre de type fini de rang r alors $\mathrm{Hom}_A(M,P)$ est un A-module libre de rang $r.n$.*

Il est maintenant aisé de généraliser toute la théorie des matrices sur un corps à celle sur un anneau. Tout se passe exactement de la même façon dans ce cadre plus général :

- Si M, N et P sont trois A-modules libres de rang fini respectifs m, n et p et avec bases $\mathcal{B}_1$, $\mathcal{B}_2$ et $\mathcal{B}_3$, et si on a deux morphismes $f : M \to N$ et $g : N \to P$, on a
$$\mathrm{Mat}_{\mathcal{B}_3,\mathcal{B}_1}(g \circ f) = \mathrm{Mat}_{\mathcal{B}_3,\mathcal{B}_2}(g)\,\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f)$$
- Si $f : M \to N$ est un isomorphisme et si M et N sont libres de rang fini, ils ont même rang n. Alors si $\mathcal{B}_1$ et $\mathcal{B}_2$ sont deux bases de M et N alors on a :
$$\mathrm{Mat}_{\mathcal{B}_1,\mathcal{B}_2}(f^{-1})\,\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f) = \mathrm{Id}_n$$
et
$$\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f)\,\mathrm{Mat}_{\mathcal{B}_1,\mathcal{B}_2}(f^{-1}) = \mathrm{Id}_n$$
et $\mathrm{Mat}_{\mathcal{B}_1,\mathcal{B}_2}(f^{-1})$ est appelée matrice inverse de $\mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(f)$.
- si M possède deux bases $\mathcal{B}_1$ et $\mathcal{B}_2$, la matrice de passage de $\mathcal{B}_2$ à $\mathcal{B}_1$ est la matrice de l'identité lorsque la base de départ est $\mathcal{B}_1$ et la base d'arrivée est $\mathcal{B}_2$.
$$P_{\mathcal{B}_2 \to \mathcal{B}_1} = \mathrm{Mat}_{\mathcal{B}_2,\mathcal{B}_1}(\mathrm{Id})$$
- On dit que deux matrices X et Y dans $\mathcal{M}_{r\times n}(A)$ sont équivalentes si elles représentent la même application dans des bases (pour le départ et pour l'arrivée) distinctes. Ceci signifie qu'il existe des matrices $P \in \mathcal{M}_{r\times r}(A)$ et $Q \in \mathcal{M}_{n\times n}(A)$ inversibles tel que
$$X = P.Y.Q$$
P et Q sont alors vu comme des matrices de passages. Si on impose que le morphisme est un endomorphisme et que les bases de départ et d'arrivée soient les mêmes, on dit alors que X et Y sont semblables, ceci signifie que $r = n$ et que P et Q sont inverses l'une de l'autre.

Nous allons maintenant nous concentrer sur le cas $M = N$. Soit f un morphisme de M dans M, module libre de rang fini avec base $\mathcal{B}$. On considère la matrice $U := \mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f) = (u_{i,j})_{1\le i,j\le n}$ dans cette base. On définit le déterminant de U comme suit :
$$\det(U) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{1\le i\le n} u_{i,\sigma(i)}$$
on voit que cet élément n'est rien d'autre que le déterminant de l'exemple 2.4.8 appliqué au vecteurs de composantes $(u_{i,j})_{1\le i\le n}$ pour $1 \le j \le n$. Deux propriétés essentielles de ce déterminant sont :

- Si V est une autre matrice de taille $n \times n$, on a

$$\det(UV) = \det(U).\det(V)$$

ceci se montre en utilisant la caractérisation du déterminant faisant intervenir l'unicité. Les vecteurs colonnes de U, de V et de UV sont les coordonnées des vecteurs $u(e_1), \ldots, u(e_n)$, des vecteurs $v(e_1), \ldots, v(e_n)$ et des vecteurs $uv(e_1), \ldots, uv(e_n)$ dans la base $\mathcal{B}$. Par conséquent, nous avons :

$$\det_{\mathcal{B}}(u(e_1), \ldots, u(e_n)) = \det(U), \qquad \det_{\mathcal{B}}(v(e_1), \ldots, v(e_n)) = \det(V)$$
$$\text{et} \quad \det_{\mathcal{B}}(uv(e_1), \ldots, uv(e_n)) = \det(UV).$$

Or l'application $f : \left\{ \begin{array}{ccc} M^n & \longrightarrow & A \\ (x_1, \ldots, x_n) & \longmapsto & \det_{\mathcal{B}}(u(x_1), \ldots, u(x_n)) \end{array} \right.$ est n-linéaire alternée. D'après le théorème fondamental sur le déterminant, elle vaut donc $f(e_1, \ldots, e_n) \det_{\mathcal{B}}$.
Or $f(e_1, \ldots, e_n) = \det_{\mathcal{B}}(u(e_1), \ldots, u(e_n)) = \det(U)$. Par conséquent, nous trouvons, pour tous vecteurs $x_1, \ldots, x_n$ de M :

$$\det_{\mathcal{B}}(u(x_1), \ldots, u(x_n)) = \det(U)\ \det_{\mathcal{B}}(x_1, \ldots, x_n).$$

En appliquant cette formule avec les vecteurs $x_1 = v(e_1)$, ..., $x_n = v(e_n)$, on trouve :

$$\det_{\mathcal{B}}(uv(e_1), \ldots, uv(e_n)) = \det(U)\ \det_{\mathcal{B}}(v(e_1), \ldots, v(e_n))$$

Ainsi

$$\det(UV) = \det(U) \det(V).$$

- Si deux colonnes sont égales, le déterminant est nul (car il est alternée) et ainsi si une combinaison linéaire (avec coefficients dans A) des colonnes est nul alors le déterminant est nul.

Comme le déterminant de l'identité est 1, on voit que si U est inversible, on a alors

$$1 = \det(U).\det(U^{-1})$$

et donc $\det(U) \in A^\times$. Ceci admet une réciproque : si U est non inversible, on peut voir que ceci implique que les colonnes de U sont dépendantes et que $\det(U) \notin A^\times$. On trouve :

Théorème 2.5.3 *$U := \mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f) = (u_{i,j})_{1 \leq i,j \leq n}$ est inversible dans $\mathrm{Mat}_{n \times n}(A)$ si et seulement son déterminant est inversible dans A.*

Notons enfin que les formules indiquent que deux matrices semblables ont même déterminant. On dit que le déterminant est un invariant de similitude et ceci permet de définir le déterminant d'un endomorphisme comme le déterminant de sa matrice dans une base arbitraire (la même au départ et à l'arrivée). En particulier, le déterminant d'un endomorphisme de A-module libre est bien défini et ne dépen pas du choix d'une base. Enfin, notons que deux matrices équivalentes ont le même déterminant à un inversible près.

Exemple 2.5.4 On retrouve les résultats bien connus sur les espaces vectoriels.

2.6 Un exemple de $\mathbb{Z}$-module libre : l'anneau d'entiers d'un corps de nombre

Rappelons que l'on dit que le corps $\mathbb{K}$ est une extension de k si et seulement si $k \subset \mathbb{K}$. Dans ce cas $\mathbb{K}$ est un k-espace vectoriel. Si $\mathbb{K}$ est de dimension fini sur k, on dit que l'extension est de degré fini et son degré est noté $[\mathbb{K} : k]$.

Définition 2.6.1 Un *corps de nombres* est par définition une extension de degré fini de $\mathbb{Q}$.

Dans tout ce qui suit, on suppose que $\mathbb{K}$ est un corps de nombres.

Définition 2.6.2 On dit qu'un élément $x \in \mathbb{K}$ est un *entier algébrique* si et seulement si il existe un polynôme de $\mathbb{Z}[X]$ unitaire P tel que $P(x) = 0$.

Exemple 2.6.3 Les éléments a de $\mathbb{Z}$ sont des entiers algébriques car racines de $X - a \in \mathbb{Z}[X]$. Le nombre $\sqrt{2}$ est aussi un entier algébrique car racine de $X^2 - 2 \in \mathbb{Z}[X]$.

Voici un lien avec la théorie des modules :

{lementier}

Proposition 2.6.4 *Soit $x \in \mathbb{K}$. Alors x est un entier algébrique si et seulement si il existe $M \subset \mathbb{K}$ un sous $\mathbb{Z}$-module de $\mathbb{K}$ non nul et de type fini tel que $xM \subset M$.*

Preuve. Supposons que x est un entier algébrique. Alors le $\mathbb{Z}$-module $\mathbb{Z}[x]$ est un $\mathbb{Z}$-module de type fini. En effet, il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$ avec P de degré n. L'élément x^n est donc une $\mathbb{Z}$-combinaison linéaire des x^j avec $1 \leq j \leq n-1$. Donc $\mathbb{Z}[x]$ est engendré par $\{1, x, \ldots, x^{n-1}\}$ et on a $x\mathbb{Z}[x] \subset \mathbb{Z}[x]$.

Réciproquement, on suppose qu'il existe $M \subset \mathbb{K}$ un sous $\mathbb{Z}$-module de $\mathbb{K}$ non nul et de type fini tel que $xM \subset M$. Soit $v_1, \ldots, v_n$ un système générateur de M. Il existe des éléments $a_{i,j}$ de $\mathbb{Z}$ avec $1 \leq i, j \leq n$ tel que

$$x.v_j = a_{1,j}v_1 + a_{2,j}v_2 + \ldots + a_{n,j}v_n$$

pour tout $1 \leq j \leq n$. On définit un endomorphisme

$$f : \mathbb{K}^n \to \mathbb{K}^n$$

tel que la matrice de f dans les bases canoniques est la matrice $A = (a_{i,j})_{1 \leq i,j \leq n}$. Alors on a

$$\begin{array}{rcl} f(v_1, \ldots, v_n) & = & v_1 f(e_1) + \ldots + v_n f(e_n) \\ & = & v_1 \sum_{1 \leq j \leq n} a_{1,j} e_j + \ldots + v_n \sum_{1 \leq j \leq n} a_{n,j} e_j \\ & = & \sum_{1 \leq i \leq n} a_{i,1} v_i e_1 + \ldots + \sum_{1 \leq i \leq n} a_{i,n} v_i e_n \\ & = & x.(v_1.e_1 + \ldots + v_n e_n) \end{array}$$

Ainsi $(v_1, \ldots, v_n)$ est un vecteur propre de valeur propre x pour f ce qui implique

$$\det(x\mathrm{Id}_n - f) = 0$$

Posons alors $P(X) = \det(X\mathrm{Id}_n - f)$. Comme x est une valeur propre de f, on a bien $P(x) = 0$ avec P unitaire, à coefficient dans $\mathbb{Z}$ et non nul. Ainsi x est un entier algébrique.

□

On dispose donc d'une traduction de "entier algébrique" en terme de modules. Ceci nous aide pour la démonstration de la preuve suivante :

Théorème 2.6.5 *L'ensemble des éléments de $\mathbb{K}$ qui sont des entiers algébriques est un sous-anneau de $\mathbb{K}$ appelé la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{K}$ ou l'anneau des entiers de $\mathbb{K}$. On le note $\mathcal{O}_{\mathbb{K}}$.*

Preuve. $\mathcal{O}_{\mathbb{K}} \neq \emptyset$ car $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}}$. Soit x et y deux entiers algébriques. Alors d'après la proposition 2.6.4, il existe deux sous $\mathbb{Z}$-modules de type fini de $\mathbb{K}$ tel que $xM \subset M$ et $xN \subset N$. Supposons que M est engendré par $x_1, \ldots, x_n$ et N par $y_1, \ldots, y_m$ alors le $\mathbb{Z}$-module engendré par les $x_i y_j$ pour $1 \leq i \leq n$ et $1 \leq j \leq m$ (c'est à dire, l'ensemble des combinaisons linéaires de ces éléments, ceci est bien un $\mathbb{Z}$-module) est de type fini et non nul De plus, il vérifie $(x-y)L \subset L$ et $xyL \subset L$. Ceci implique que $x-y$ et xy sont tout deux entiers algébriques donc $\mathcal{O}_{\mathbb{K}}$ est bien un sous-anneau de K.

Remarque 2.6.6 L'anneau $\mathcal{O}_{\mathbb{K}}$ est en fait un $\mathbb{Z}$-module libre de type fini. ceci se prouve en utlisant la fonction trace $\mathbb{K} \to \mathbb{Q}$.

Si nous cherchons à aller plus loin dans la généralisation des propriétés déjà connues pour les espaces vectoriels. Un problème naturel serait d'essayer de généraliser le théorème de la base incomplète. C'est le but du prochain chapitre ...

Chapitre 3

Modules de type fini sur un anneaux principal

Le but de ce chapitre est de continuer nos tentatives de généralisations de théorèmes "bien connus" sur les espaces vectoriels aux modules sur un anneau. Pour ceci, il semble nécessaire de se restreindre aux modules libres afin d'avoir une notion de base. On s'intéresse ici particulièrement au théorème de la base incomplète : nous allons voir qu'un analogue (faible) à ce théorème fondamental est disponible dans le cas A principal (et pour les modules libres de type fini).

3.1 Le théorème de la base adaptée

Le but de cette partie est d'étudier la notion de base dans le cadre des anneaux principaux. On sait déjà que dans ceux-ci, tout sous-module d'un module de type fini l'est également (grâce au théorème 2.2.2, un anneau principal étant toujours noethérien). Que se passe t-il pour la notion de liberté d'un module ?

{princ}

Théorème 3.1.1 *Soit A un anneau principal alors tout sous-module N d'un module libre de type fini M de rang n est libre de type fini et de rang $m \leq n$.*

Preuve. On va procéder par récurrence sur n. Pour $n = 1$, N est isomorphe à A et un sous-module de A est un idéal de A, il est donc principal engendré par $a \in A$ non nul. Alors $\{a\}$ est une base de N : si $\lambda.a = 0$ pour $\lambda \in A$ alors $\lambda = 0$ car A est intègre.

Supposons donc $n > 1$ et $N \neq 0$. Soit $(e_1, \ldots, e_n)$ une base de M. On note M_1 le A-module libre de rang $n-1$:

$$Ae_2 \oplus \ldots \oplus Ae_n$$

Si N est contenu dans M_1, on peut conclure par hypothèse de récurrence. On suppose donc que N n'est pas contenu dans M_1. On considère le A-module $N \cap M_1$. C'est un sous-module de M_1. Par hypothèse de récurrence, il est libre. Soit $(f_2, \ldots, f_m)$ une base de ce module avec $m \leq n$.

On considère maintenant l'ensemble suivant :

$$I = \{b \in A \mid \exists y \in M_1,\ be_1 + y \in N\}$$

Un élément quelconque de N s'écrit be_1+y avec $y \in M_1$ donc I est non vide et il est même non nul car il existe un élément de N qui n'est pas dans $M1$. On voit facilement que c'est un idéal de A. Il est donc principal engendré par un élément $d \neq 0$ de A. Il existe alors un élément y_1 de M_1 tel que $f_1 := de_1 + y_1 \in N$. Notons tout d'abord que cet élément est non nul car M_1 et Ae_1 sont en somme directe.

On va montrer que $(f_1, \ldots, f_m)$ est une base de N. C'est une famille génératrice. En effet, si $x \in N$ on a $x = be_1 + y$ avec $b \in A$ et $y \in M_1$. Mais on a $b \in I$ et donc b s'écrit ad avec $a \in A$. On a donc $x = af_1 - ay_1 + y$. Alors $-ay_1 + y$ est dans $N \cap M_1$ donc s'écrit comme combinaison d'éléments de $(f_2, \ldots, f_m)$. On peut alors conclure.

On montre maintenant que la famille est libre. Supposons $a_1f_1+a_2f_2+\ldots+a_mf_m = 0$ pour $(a_1, \ldots, a_m) \in A^m$ non tous nuls. On a $a_1 \neq 0$ car la famille $(f_2, \ldots, f_m)$ est libre. On a donc a_1f_1 dans M_1 et donc $a_1de_1 + a_1y \in M_1$ ce qui implique $a_1de_1 \in M_1$. Ceci implique $a_1d = 0$ et donc $a_1 = 0$ car $d \neq 0$ et A est intègre.

□

Exemple 3.1.2 Les sous-modules de $\mathbb{Z}^n$ sont donc des modules libres de type fini et de rang $r \leq n$.

Remarque 3.1.3 Attention, contrairement aux espaces vectoriels, si N est un sous-module libre du module libre N et que les deux modules ont même rang, ceci n'implique pas qu'ils sont égaux. Prendre par exemple, le sous-module $2\mathbb{Z}$ de $\mathbb{Z}$.

Remarque 3.1.4 Si A est principal A est un A-module libre de type fini et de rang 1, les sous-modules sont des idéaux qui sont donc libres de type fini et de rang 1. En effet, ce sont des idéaux principaux engendrés par des éléments non diviseurs de zéro (voir l'exemple 2.1.6).

Remarque 3.1.5 L'hypothèse A principal est essentiel dans ce théorème. En effet, on a déjà vu qu'un sous-module d'un module libre n'est pas forcément libre. On prend par exemple $A = M = \mathbb{Z}/4\mathbb{Z}$ et $N = 2\mathbb{Z}/4\mathbb{Z}$.

Le théorème suivant peut être considérer comme le résultat le plus important de ce cours.

{thmada1}

Théorème 3.1.6 *Soit A un anneau principal. Soit M un module libre de rang fini $n \in \mathbb{N}$. Soit $N \neq 0$ un sous-module de M. Alors N est un module libre de rang $r \leq n$. De plus,*

- *il existe une base $(e_1, \ldots, e_n)$ de M*
- *il existe des éléments $a_1, a_2, \ldots, a_r$ de $A \setminus \{0\}$ tels que a_i divise a_{i+1} pour $i = 1, \ldots, r-1$.*

tels que $(a_1e_1, \ldots, a_re_r)$ est une base de M. De plus la suite des idéaux $(a_r) \subset (a_{r-1}) \subset \ldots \subset (a_1)$ est unique et ne dépend que de M. On dit que la base $(e_1, \ldots, e_n)$ de M est adaptée au sous-module N.

La démonstration de ce théorème est relativement longue. Avant de rentrer dans le vif du sujet, nous avons besoin d'un lemme.

{adalem1}

Lemme 3.1.7 *Sous les hypothèse du théorème 3.1.6, il existe un morphisme de A-modules*

$$f : M \to A$$

vérifiant les propriétés suivantes :

1. *Pour tout morphisme $g : M \to A$, on a $g(N) \subset f(N)$.*
2. *Il existe $d \in A$ non nul tel que $f(N) = (d)$ et il existe $y \in N$ tel que $f(y) = d$.*
3. *Pour tout $g : M \to A$, on a $g(y) \in (d)$.*
4. *Il existe $x \in M$ tel que $f(x) = 1$ et $y := d.x \in N$.*
5. *On a $M = Ax \oplus \mathrm{Ker}(f)$ et $N = A.y \oplus (\mathrm{Ker}(f) \cap N)$.*

Preuve. Pour le point 1., on considère l'ensemble des morphismes de M dans A et l'ensemble $\mathcal{X}$ des images de N selon ces morphismes. C'est un ensemble d'idéaux de A. Cet ensemble est inductif pour l'inclusion. En effet, donnons nous une chaîne $\mathcal{C}$ d'idéaux de $\mathcal{X}$, c'est à dire un ensemble d'idéaux emboités. La réunion de tout ces idéaux est encore un idéal et comme A est principal, il est engendré par un élément $a \in A$. Il existe donc un idéal I de $\mathcal{C}$ tel que $a \in I$. Alors $\mathcal{C}$ admet un majorant I dans $\mathcal{X}$. Comme $\mathcal{X}$ est non vide (car $(0) \in \mathcal{X}$), on peut appliquer le Lemme de Zorn pour conclure que $\mathcal{X}$ admet un plus grand élément qui satisfait donc aux hypothèses de 1.

Le point 2 est facile : comme A est principal, il existe $d \in A$ tel que l'idéal $f(N)$ est égal à (d) et donc $y \in N$ tel que $f(y) = d$. Prenons une base $(e_1, \ldots, e_n)$ de M et considérons les applications "coordonnées" $g_j : M \to A$ tel que

$$g_j(\sum_{1 \leq i \leq n} a_i e_i) = a_j$$

pour tout $j = 1, \ldots, n$. On a $N \neq 0$ donc au moins un $g_j(N)$ est non nul et donc, comme $g_j(N) \subset (d)$ pour tout $j = 1, \ldots, n$, on a $d \neq 0$.

Passons au point 3. Comme $y \in N$ et $g(N) \subset f(N) = (d)$, on a bien $g(y) \in (d)$.

Considérons maintenant le point 4. En appliquant le point 3 aux morphismes g_j ci-dessus, il suit que si $y = \sum_{1 \leq i \leq n} a_i e_i$ alors tous les a_i sont divisibles par d. Ceci implique par exemple que d est non nul car N est non nul. Donc il existe $x \in M$ tel que $y = dx$. On a bien $f(y) = d.f(x) = d$ donc $f(x) = 1$.

Abordons le point 5, on a déjà $Ax \cap \mathrm{Ker}(f) = \{0\}$ car pour tout $a \in A$, $f(a.x) = a = 0$. Maintenant, si $z \in M$, on a $z = f(z).x + (z - f(z)x) \in Ax + \mathrm{Ker}(f)$ d'où $M = Ax \oplus \mathrm{Ker}(f)$. Ensuite, si $a \in A$ est tel que $ay \in \mathrm{Ker}(f) \cap N$ alors $f(ay) = a.d = 0$ et donc $a = 0$ car $d \neq 0$. De plus, si $z \in N$ alors $f(z) = a.d$ pour $a \in A$ et on a $z = ay + (z - ay) \in A.y + (\mathrm{Ker}(f) \cap N)$.

□

Nous montrons maintenant la première partie du théorème 3.1.6.

{propada}

Proposition 3.1.8 *Soit A un anneau principal. Soit M un A-module libre de rang fini $n \in \mathbb{N}$. Soit $N \neq 0$ un sous-module de M. Alors N est un module libre de rang $r \leq n$. De plus,*

- *il existe une base* $(e_1, \ldots, e_n)$ *de* M
- *il existe des éléments* $a_1, a_2, \ldots, a_r$ *de* $A \setminus \{0\}$ *tels que* a_i *divise* a_{i+1} *pour* $i = 1, \ldots, r-1$.

tels que $(a_1 e_1, \ldots, a_r e_r)$ *est une base de* N.

Preuve. On raisonne par récurrence sur le rang n de M.

- Si $n = 1$, M est isomorphe à A. On peut donc supposer $M = A$. Les sous-modules de M sont des idéaux tels qu'il existe $d \in A$ tel que $M = (d)$. Une base est $\{d\}$, cet ensemble étant libre par intégrité de A. Le résultat suit en posant $n = r = 1$,$e_1 = 1$ et $a_1 = d$.
- Si $n > 1$. Supposons le résultat vrai pour les modules libres de type fini et de rang strictement plus petit que n. On applique alors le lemme 3.1.7. il existe un morphisme de A-modules

$$f : M \to A$$

vérifiant les 5 points du lemme. Posons $M' := \mathrm{Ker}(f)$. C'est un sous-module de M et il est donc libre et de type fini d'après le théorème 3.1.1. Le point 5 du lemme nous dit que

$$M = Ax \oplus M' \qquad N = Ay \oplus (M' \cap N)$$

Ax est libre de rang 1 car x est générateur et libre (car c'est une combinaison linéaire d'élément de la base de M et que A est intègre). Il en est de même pour Ay. La propositon 2.4.6 implique que M' est de rang $n-1$. Si $M' \cap N = 0$ alors on a

$$M = Ax \oplus M' \qquad N = Adx$$

et le résultat est vérifié, en prenant $e_1 = x$ et pour $(e_2, \ldots, e_n)$ une base quelconque de M'.
Si $M' \cap N \neq 0$ on peut appliquer l'hypothèse de récurrence à M' et à son sous-module $M' \cap N$. Il existe une base $(e_2, \ldots, e_n)$ de M' et des éléments $a_2, \ldots, a_r$ de A tel que $r \leq n$, $a_2 | a_3 \ldots | a_r$ et

$$M' = Ae_2 \oplus \ldots \oplus Ae_n \qquad M' \cap N = Aa_2 e_2 \oplus \ldots \oplus Aa_r e_r$$

On a alors :

$$M = Ae_1 \oplus \ldots \oplus Ae_n \qquad N = Aa_1 e_1 \oplus \ldots \oplus Aa_r e_r$$

où $a_1 := d$ et $e_1 = x$. Enfin on a que a_1 divise a_2 en appliquant le point 3 au morphisme $g_2 : M \to A$. On a $g_2(\sum_{1 \leq i \leq n} a_i e_i) = a_2 \in (a_1)$ donc a_1 divise a_2.

□

La proposition suivante correspond à l'unicité du théorème et donc permet de compléter la preuve de celui-ci. Notons que dire que $a \in A$ divise $b \in A$ signifie que l'idéal (b) est contenu dans (a). Dire que a est unique à inversible près signifie que l'idéal (a) est unique.

{propada}

Proposition 3.1.9 *Soit* A *un anneau principal. Soit* M *un module libre de rang fini* $n \in \mathbb{N}$. *Soit* $N \neq 0$ *un sous-module de* M. *Supposons que* $(e_1, \ldots, e_n)$

et $(e'_1, \dots, e'_n)$ soient deux bases adaptés à N. Soit $a_1, \dots, a_r$ et $a'_1 \dots, a'_r$ les éléments non nuls de A tels que a_i divise a_{i+1} et a'_i divise a'_{i+1} pour $i = 1, \dots, r-1$, et tel que $(a_1 e_1, \dots, a_r e_r)$ et $(a'_1 e'_1, \dots, a'_r e'_r)$ soient deux bases de N. Alors on a $(a_i) = (a'_i)$ pour tout $i = 1, \dots, r$.

Preuve On considère le morphisme $g_1 : M \to A$ tel que $g_1(\sum_{1 \leq i \leq n} b_i e_i) = b_1$. On voit facilement que l'on a $g_1(N) = a_1 A$ d'une part. D'autre part si $m \in N$ alors $m = \sum_{1 \leq i \leq r} a'_i e'_i k_i$ et $g_1(m) = \sum_{1 \leq i \leq r} k_i a'_i g_1(e_i)' \subset a'_1 A$. On a donc $(a_1) \subset (a'_1)$. Et par analogie $(a'_1) \subset (a'_1)$ donc $(a'_1) = (a'_1)$.

Supposons maintenant que l'on ait montré que $(a_k) = (a'_k)$ pour tout $k = 1, \dots, i-1$. On va montrer que $(a_1 \dots a_i) = (a'_1 \dots a'_i)$ ce qui implique bien $(a_i) = (a'_i)$. On considère l'application multilinéaire alternée

$$\begin{array}{rccc} \mathcal{D} : & M^i & \to & A \\ & (u_1, \dots, u_i) & \mapsto & \begin{vmatrix} u_{1,1} & \dots & u_{1,i} \\ \vdots & \dots & \vdots \\ u_{i,1} & \dots & u_{i,i} \end{vmatrix} \end{array}$$

où pour tout $j = 1, \dots, i$, on a posé $u_j = u_{1,j} e_1 + \dots + u_{n,j} e_n$. On a

$$\mathcal{D}(a_1 e_1, \dots, a_i e_i) = a_1 \dots a_i$$

d'une part. D'autre part, si on écrit pour tout $j = 1, \dots, n$,

$$a_j e_j = \sum_{1 \leq k_j \leq n} \mu_{k_j, j} a'_{k_j} e'_{k_j}$$

on obtient :

$$\mathcal{D}(a_1 e_1, \dots, a_i e_i) = \sum_{1 \leq k_1, \dots, k_i \leq n} \mu_{k_1, 1} \dots \mu_{k_i, i} a'_{k_1} \dots a'_{k_i} \mathcal{D}(e'_{k_1}, \dots, e'_{k_i})$$

comme l'application est alternée, il faut retenir dans cette somme seulement les termes avec les e'_{k_j} distincts. Les facteurs $a'_{k_1} \dots a'_{k_i}$ sont alors des multiples de $a'_1 \dots a'_i$ car a'_{i+1} est un multiple de a'_i. On obtient donc $a_1 \dots a_i$ multiple de $a'_1 \dots a'_i$. Les a_j et a'_j jouant un rôle symétrique, on peut conclure

$$a_1 \dots a_i A = a'_1 \dots a'_i A$$

c'est ce qu'il fallait montrer.

Exemple 3.1.10 Que signifie ce théorème dans le cadre des espaces vectoriels ? dans ce cadre, c'est exactement le théorème de la base incomplète. En effet, les a_i sont définis à inversible près, l'unicité ne signifie rien dans ce contexte car tout élément non nul est inversible.

Exemple 3.1.11 Soit $A = \mathbb{Z}$ et soit $M = \mathbb{Z}^2$. On considère le sous-module

$$N = \mathbb{Z}(0, 2) \oplus \mathbb{Z}(1, 1)$$

Alors la base $(e_1 + e_2, e_2)$ est une base de M adaptée à N, on a en effet

$$N = 1\mathbb{Z}(e_1 + e_2) \oplus 2\mathbb{Z} e_2$$

Les idéaux associés sont $(2) \subset (1) = A$. N est de rang 2. On a $a_1 = 1$ et $a_2 = 2$. Bien sûr la base adaptée n'est pas unique. Par exemple $(e_1 + e_2, e_1 + 2e_2)$ est aussi une base adapté car on a

$$N = 1\mathbb{Z}(e_1 + e_2) \oplus 2\mathbb{Z}e_1$$

Par contre, les idéaux $(1) = A$ et (2) sont, eux, uniques.

Nous verrons plus loin des exemples de calculs explicites nous montrant comment calculer une base adaptée. Avant nous allons donner une conséquence remarquable sur la classification des modules sur un anneau principal.

3.2 Facteurs invariants

Dans cette section, Nous donnons deux théorèmes de structure qui découlent du théorème de la base adaptée. Le premier de ces théorèmes est d'une importance considérable. Il permet de classifier entièrement les modules de type fini sur un anneau principal. Nous avons tout d'abord besoin d'un petit résultat concernant la somme directe.

Lemme 3.2.1 *Soit $M_1, \ldots, M_n$ des A-modules et pour tout $i \in \{1, \ldots, n\}$, soit N_i, un sous-module de M_i alors on a*

$$\bigoplus_{1\leq i\leq n} M_i / \bigoplus_{1\leq i\leq n} N_i \simeq \bigoplus_{1\leq i\leq n} M_i/N_i$$

Preuve. On considère le morphisme surjectif :

$$\begin{array}{ccc} \bigoplus_{1\leq i\leq n} M_i & \to & \bigoplus_{1\leq i\leq n} M_i/N_i \\ (m_i)_{i=1,\ldots,n} & \mapsto & (m_i + N_i)_{i=1,\ldots,n} \end{array}$$

on voit que son noyau est exactement $\bigoplus_{1\leq i\leq n} N_i$ ce qui permet de conclure grâce au théorème de factorisation.

□

{thmada}

Théorème 3.2.2 (dit des facteurs invariants) *Soit A un anneau principal et M un module de type fini. Alors il existe un unique couple (r, s) d'entiers et une unique suite $(a_r) \subset (a_{r-1}) \subset \ldots \subset (a_1)$ d'idéaux de A non nuls et distincts de A tels que*

$$M \simeq A^s \oplus \bigoplus_{1\leq i\leq r} A/(a_i)$$

Les a_i sont déterminés à inversibles près et sont appelés les facteurs invariants du modules.

Preuve.
Existence : Comme M est de type fini, d'après la proposition 2.1.10, on a un isomorphisme

$$M \simeq A^n/N$$

pour un entier $n \in \mathbb{N}$ et un sous-module N de A^n. N est donc un sous-module d'un A-module libre de type fini de rang n. On peut appliquer le théorème de la base adaptée : N est un module libre de rang $r \leq n$. De plus,

- il existe une base $(e_1, \ldots, e_n)$ de A^n
- il existe des éléments $a_1, a_2, \ldots, a_r$ de $A \setminus \{0\}$ tels que a_i divise a_{i+1} pour $i = 1, \ldots, r-1$.

tels que $(a_1 e_1, \ldots, a_r e_r)$ est une base de N. On a donc

$$A^n = Ae_1 \oplus \ldots \oplus Ae_n \qquad \text{et} \qquad N = Aa_1 e_1 \oplus \ldots \oplus Aa_r e_r$$

On obtient en utilisant le lemme précédent :

$$M \simeq A^{n-r} \oplus A/(a_1) \oplus \cdots \oplus A/(a_r)$$

c'est ce qu'il fallait montrer. Notons que pour être tout à fait en adéquation avec l'énoncé du théorème, il faut aussi supprimer les a_i inversibles : dans ce cas $A/(a_r) = 0$ car $(a_r) = A$.

Unicité : ceci découle de l'exercice ci-après.

□

Exercice 3.2.3 Soit A un anneau principal et soit M un A-module. On suppose que M s'écrit

$$M = A/d_1A \times A/d_2A \times ... \times A/d_sA,$$

où $d_1, ..., d_s$ sont des éléments de A tels que d_i divise d_{i+1} pour $i = 1, ..., s-1$.

1. Que peut-on dire du facteur A/d_iA si d_i est inversible ? dans la suite, on supposera que les d_i sont tous non inversibles.
2. Soit π un élément irréductible de A qui divise d_1.
   (a) Pourquoi l'anneau $k = A/\pi A$ est-il un corps ?
   (b) Posons $d_1 = \pi b_1$. Montrer que le noyau dans A/d_1A de la multiplication par π est b_1A/d_1A.
   (c) Justifier rapidement que b_1A/d_1A est un k-espace vectoriel.
   (d) Donner un isomorphisme
   $$\phi : A/\pi A \to b_1A/d_1A$$
   (e) Déterminer le noyau dans A/d_1A de la multiplication par π si π ne divise pas d_1.
   (f) On suppose ici que π ne divise pas d_1. Soit M_π le noyau dans M de la multiplication par π. Quelle est sa dimension comme espace vectoriel sur k ?
3. On suppose qu'il existe une autre décomposition de M :
   $$M = A/d'_1A \times A/d'_2A \times ... \times A/d'_rA,$$
   où $d'_1, ..., d'_r$ sont des éléments non inversibles de A tels que d_i divise d_{i+1} pour $i = 1, ..., r-1$.
   (a) S'inspirer de 2) pour montrer que $\dim_k M_\pi \leq r$ où π est toujours un élément irréductible de A.
   (b) Montrer que $r = s$.

(c) Soit $i \in \{1, ..., s\}$ et soit e le plus grand entier tel que π^e divise d_i. Soit e' le plus grand entier tel que $\pi^{e'}$ divise d'_i. On suppose $e' > e$ et on pose $N = \pi^e M$. En étudiant la dimension sur k de N_π, trouver une contradiction. En déduire $d_i A = d'_i A$.

(d) Conclure

{facannu}

Remarque 3.2.4 Le théorème ci-dessous permet de décomposer n'importe quel module sur un anneau principal sous la forme d'un module de torsion en somme directe avec un module sans torsion. En effet, si

$$M \simeq A^s \oplus \bigoplus_{1 \leq i \leq r} A/(a_i)$$

où les a_i sont non inversibles, on a :

$$T(M) = \bigoplus_{1 \leq i \leq r} A/(a_i)$$

et le A-module A^s est bien sûr libre et de type fini. On voit de plus que l'idéal annulateur de $T(M)$ est (a_r).

Pour le théorème suivant, on note $\mathcal{P}$ l'ensemble des éléments irréductibles de A. On dit qu'un élément p de A est irréductible s'il vérifie :

- p n'est pas inversible dans A.
- La condition $p = ab$ avec a et b dans A implique que a ou b soit inversible.

Dans un anneau principal donc factoriel, les idéaux engendré par les nombres irréductibles sont exactement les idéaux premiers (donc maximaux).

{thmadaj}

Théorème 3.2.5 (dit de Jordan) *Soit A un anneau principal et M un module de type fini. Alors il existe un unique entier r et pour tout nombre premier $p \in \mathcal{P}$, un unique $j_p \in \mathbb{N}$ et une unique famille décroissante d'entiers non nuls*

$$n_{p,1} \geq n_{p,2} \geq \ldots \geq n_{p,j_p}$$

tel que :

$$M \simeq A^r \oplus \bigoplus_{p \in \mathcal{P}} \bigoplus_{1 \leq j \leq j_p} A/(p^{n_{p,j}})$$

(avec un nombre fini dans la somme.) Les nombres premiers p tels que $n_{p,1} \neq 0$ sont appelés diviseurs élémentaires.

Preuve. Ceci résulte du lemme chinois d_1 et d_2 sont deux éléments de A premiers entre eux alors

$$A/(d_1 d_2) \simeq A/(d_1) \oplus A/(d_2)$$

Dans le théorème des facteurs invariants, on considère l'idéal (a_r). Comme A est factoriel car principal, celui-ci se décompose sous la forme :

$$(a_r) = (p_1)^{m_1} \ldots (p_n)^{m_n}$$

où les p_i sont des éléments irréductibles. On fait de même pour tous les (a_i) et Il suffit alors de décomposer grâce au lemme chinois. Le fait que

$$n_{p,1} \geq n_{p,2} \geq \ldots \geq n_{p,j_p}$$

provient du fait que a_i divise a_{i+1} pour tout $i = 1, \ldots, r-1$. On peut alors conclure. L'unicité découle de l'unicité de la décomposition en éléments irréductibles (A étant factoriel car principal) et de celle énoncée dans le théorème.

□

Remarque 3.2.6 Il faut vraiment voir ce théorème comme une reformulation du théorème des facteurs invariants. Il est d'ailleurs aisé de passer d'un formulation à une autre

- on passe des facteurs invariants à Jordan en décomposant en produits de facteurs premiers puis en utilisant le lemme Chinois. Par exemple, considérons le $\mathbb{Z}$-module

  $$M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}$$

  On a $12 = 2^2 \times 3$ et $60 = 5 \times 2^2 \times 3$.

  $$M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$

  qui est la décomposition de Jordan.
- on passe de Jordan aux facteurs invariants en regroupant grâce au lemme Chinois les $n_{p,i}$ pour tout $p \in \mathcal{P}$. Par exemple, considérons :

  $$M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5^2\mathbb{Z}$$

  il faut regrouper 2^3, 5 et 3 puis 2^2 et 5, on obtient :

  $$M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/600\mathbb{Z}$$

3.3 Approche matricielle

Nous allons maintenant donner une version matricielle équivalente au théorème 3.2.2. Nous illustrons ce nouveau résultat par quelques exemples. Tout d'abord, on a la définition suivante :

Définition 3.3.1 Soit $X \in \mathrm{Mat}_{n\times m}(A)$.

1. Pour tout $i \in \min(m, n)$, on note $J_i(X)$ l'idéal de A engendré par les mineurs de taille $i \times i$. Par convention, on note $J_0(X) = A$.
2. Le rang de X est le plus grand entier $r \geq 0$ tel que $J_i(X) \neq 0$

Les idéaux $J_i(X)$ sont appelés *idéaux de Fitting.*

Exemple 3.3.2 Prenons $A = \mathbb{Z}$ et la matrice

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

On a $J_1(X) = A$, $J_2(X) = A$ et $J_3(X) = (3)$!

Dans un anneau principal, $J_i(X)$ est engendré par le plus grand commun diviseur des mineurs de taille i.

{matrice}

Théorème 3.3.3 *Soit A un anneau principal et soit $X \in \mathrm{Mat}_{n\times m}(A)$ non nulle. Alors il existe $r \geq 1$, des matrices inversibles $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_m(A)$ et des éléments $a_1, \ldots, a_r$ de A non nuls tels que a_i divise a_{i+1} pour tout $i = 1, \ldots, r-1$ vérifiant :*

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

De plus, les idéaux (a_i) sont uniquement déterminés par X. La famille des a_i est appelée la famille des facteurs invariants de X.

Preuve Soit $X \in \mathrm{Mat}_{n\times m}(A)$ non nulle. Cette matrice représente un morphisme $f : A^m \to A^n$. On applique le théorème de la base adaptée au A-module libre A^n et à son sous-module $\mathrm{Im}(f)$.

- il existe une base $(e_1, \ldots, e_n)$ de A^n
- il existe des éléments $a_1, a_2, \ldots, a_r$ de $A \setminus \{0\}$ tels que a_i divise a_{i+1} pour $i = 1, \ldots, r-1$.

tels que $(a_1e_1, \ldots, a_re_r)$ est une base de $\mathrm{Im}(f)$ qui est donc libre de type fini. Il existe des éléments $u_1, \ldots, u_r$ de A^m tel que pour tout $i = 1, \ldots, r$, on a :

$$f(u_i) = a_ie_i$$

Montrons que

$$A^m = (\bigoplus_{1\leq i\leq r} Au_i) \oplus \mathrm{Ker}(f)$$

On voit tout d'abord que la somme des Au_i $(1 \leq i \leq r)$ est directe car la famille $(a_1e_1, \ldots, a_re_r)$ est libre. Si $x = \sum_{1\leq i\leq r} b_iu_i$ avec $(b_i)_{1\leq i\leq r}$ une famille d'éléments de A et si $x \in \mathrm{Ker}(f)$ alors on a

$$f(x) = \sum_{1\leq i\leq r} b_ia_ie_i = 0$$

ce qui implique que $b_ia_i = 0$ pour tout $i = 1, \ldots, r$ et donc $b_i = 0$ pour tout $i = 1, \ldots, r$ car l'anneau A est intègre et les a_i $(1 \leq i \leq r)$ non nuls. Enfin, si $x \in A^m$ alors il existe $(b_i)_{1\leq i\leq r}$ une famille d'éléments de A tel que

$$f(x) = \sum_{1\leq i\leq r} b_ia_ie_i \in \mathrm{Im}(f)$$

On remarque alors que

$$x - \sum_{1\leq i\leq r} b_iu_i \in \mathrm{Ker}(f)$$

ce qui montre que

$$x \in (\bigoplus_{1\leq i\leq r} Au_i) \oplus \mathrm{Ker}(f)$$

On a bien montré la décomposition annoncée. Notons qu'on peut en déduire qu'une base de $\mathrm{Ker}(f)$ a nécessairement $m-r$ éléments. Choisissons donc une base $(u_{r+1},\dots,u_m)$ de $\mathrm{Ker}(f)$. On a alors une base de A^m :

$$(u_1,\dots,u_m)$$

La matrice de f dans les bases $(u_1,\dots,u_m)$ et $(e_1,\dots,e_n)$ a alors la forme voulue et celle-ci est équivalente à A. L'unicité découlera de la proposition suivante

□

Remarque 3.3.4 Si f est un morphisme entre deux A-modules libres, on dira dans ce cours que les facteurs invariants de f sont ceux de la matrice de f dans des bases arbitraires (ce qui est bien défini).

{fitting}

Proposition 3.3.5 *En gardant les notations du théorème 3.3.3, on a*

$$J_i(X) = \begin{cases} (a_1 \dots a_i) & \text{si } i = 1,\dots r \\ 0 & \text{sinon} \end{cases}$$

Preuve. Il s'agit de montrer que si X et Y sont équivalentes alors

$$J_i(X) = J_i(Y)$$

pour tout $1 \leq i \leq \min(m,n)$. On pourra alors conclure via le théorème précédent car les idéaux de Fitting de la matrice remarquable du théorème 3.3.3 sont précisement donnés par ceux de l'énoncé. Soit $Q \in \mathrm{GL}_m(A)$ et supposons que $Y = XQ$. Ceci implique que les colonnes de Y sont des combinaisons linéaires de colonnes de X. Comme le déterminant est multilinéaire, on en déduit que les mineurs de taille i de Y sont des combinaisons linéaires des mineurs de taille i de X. On en déduit que $J_i(Y) \subset J_i(X)$. Comme on a aussi $X = YQ^{-1}$, on en déduit que $J_i(X) = J_i(Y)$ dans ce cas.

Maintenant supposons qu'il existe $P \in \mathrm{GL}_n(A)$ et supposons que $Y = PX$ alors $Y^t = X^tP^t$ et comme ci-dessus on montre que $J_i(X) = J_i(Y)$.

Finalement dans le cadre général où il existe $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_m(A)$ tel que $Y = PXQ$, on obtient :

$$J_i(Y) = J_i(XQ) = J_i(X)$$

pour tout $i = 1,\dots,r$.

□

Ceci montre effectivement que les idéaux (a_i) sont uniquement déterminés par X.

Exemple 3.3.6 On obtient ainsi une première méthode pour déterminer les facteurs invariants d'une matrice. Prenons ici $A = \mathbb{Z}$ et la matrice :

$$X = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 0 \\ 0 & 6 & 4 \end{pmatrix}$$

On a $J_1(X) = (1)$, $J_2(X) = (2)$, $J_3(X) = (12)$. Les facteurs invariants sont 1, 2 et 6. Si on prend maintenant :

$$Y = \begin{pmatrix} 7 & 0 & 6 \\ 2 & 2 & 2 \\ 6 & 0 & 6 \end{pmatrix}$$

on trouve les mêmes facteurs invariants et donc X et Y sont équivalentes.

{imp}

Remarque 3.3.7 La preuve ci-dessus montre que le théorème de la base adaptée implique le résultat ci-dessus sur l'équivalence de matrices. On peut en fait montrer une réciproque : si M est un module libre et N un sous-module de celui-ci, d'après le théorème 3.1.1, N est libre de rang $\leq n$. On prend alors une base $\mathcal{B} = (b_1, \ldots, b_n)$ (de cardinal n) de M. On se donne aussi un système générateur de N (par exemple une base) $(v_1 \ldots, v_s)$ que l'on suppose de cardinal $s \leq n$. On considère le morphisme

$$f : M \to M$$

qui envoie chaque b_i sur v_i pour $i = 1, \ldots, s$ et 0 pour $i = s+1, \ldots, n$. L'image de f est N. On considère la matrice $\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f)$. On utilise alors le théorème 3.3.3, il existe deux bases $\mathcal{E} = (e_1, \ldots, e_n)$ et $\mathcal{E}'$ de M tel que

$$\mathrm{Mat}_{\mathcal{E},\mathcal{E}'}(f) = \begin{pmatrix} a_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & a_r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

où les éléments $a_1, \ldots, a_r$ de A sont non nuls et tels que a_i divise a_{i+1} pour tout $i = 1, \ldots, r-1$. Il existe donc une base $\mathcal{E} = (e_1, \ldots, e_n)$ de M tel que $(a_1 e_1, \ldots, a_r e_r)$ est une base de N : en effet par définition c'est un ensemble générateur (car l'image de f est N) et c'est évidement une famille libre. Ceci nous assure l'existence de base adaptée.

On a ainsi une justification de l'appellation "facteurs invariants" pour les matrices. Concrètement, ceci nous donne un (début) de méthode pour calculer une base adaptée.

- On suppose que N est engendré par un certain nombre de vecteurs v_1, $\ldots$, v_s que l'on écrit sous forme de combinaison linéaire d'une base $\mathcal{B}$ du module libre M de rang n. On peut supposer $s \leq n$.
- On écrit la matrice $\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f)$: c'est la matrice dont chaque colonne est donnée par un v_j exprimé sur la base $\mathcal{B}$ et les $n - s$ dernières colonnes sont nuls.
- Il existe deux bases $\mathcal{E} = (e_1, \ldots, e_n)$ et $\mathcal{E}'$ de M et N tels que

  $$P_{\mathcal{E}\to\mathcal{B}} \,\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f) P_{\mathcal{B}\to\mathcal{E}'} = \mathrm{Mat}_{\mathcal{E},\mathcal{E}'}(f)$$

  a la forme voulue ci-dessus.
- La matrice $P_{\mathcal{E}\to\mathcal{B}}$ est celle qui nous intéresse, si on l'inverse, on obtient $P_{\mathcal{B}\to\mathcal{E}}$ qui exprime $\mathcal{E}$ dans la base $\mathcal{B}$.

{lien}

Remarque 3.3.8 Soit $f : M \to M$ un endomorphisme de A-module libre de type fini. Soient $(a_1, \ldots, a_r)$ les facteurs invariants de f. Il existe deux bases $\mathcal{E}'$ et $\mathcal{E}$ de M dans lequel la matrice $\mathrm{Mat}_{\mathcal{E},\mathcal{E}'}(f)$ a la forme diagonale avec les facteurs invariants sur celle-ci. Soit $\mathcal{E} = (e_1, \ldots, e_n)$ alors

$$\mathrm{Im}(f) = Aa_1 e_1 \oplus \ldots \oplus Aa_r e_r$$

On a alors

$$A^n/\mathrm{Im}(f) \simeq A^{n-r} \oplus A/(a_1) \oplus \ldots \oplus A/(a_r)$$

donc les facteurs invariants (non inversibles) de f sont les facteurs invariants du A-module $A^n/\mathrm{Im}(f)$

Remarque 3.3.9 Soit E un $\mathbb{K}$ espace vectoriel de dimension finie. Alors, les facteurs invariants étant définis à inversibles près et étant non nuls, ils peuvent être considérés comme tous égaux à 1. Le seul invariant est alors ici le nombre r de tels facteurs. Ce nombre correspond au rang de le matrice et on retrouve le fait que deux matrices sont équivalentes si et seulement si elles ont mêmes rang lorsque l'anneau de base est un corps. Dans ce cas, on a

$$J_1(X) = \ldots = J_r(X) = 1,\ J_{r+1}(X) = \ldots = J_n(X) = 0$$

3.4 Algorithme

{algo}

Dans cette partie, on donne un algorithme explicite pour calculer les facteurs invariants d'une matrice dans le cas où A est un anneau euclidien. A est donc intègre et on dispose donc d'une application

$$\varphi : A \setminus \{0\} \to \mathbb{N}$$

telle que pour tout $a \in A$ et $b \in A \setminus \{0\}$, il existe q et r dans A tel que

$$a = bq + r, \quad \text{et } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

et pour tout a et b dans $A \setminus \{0\}$ non nuls on a

$$\varphi(b) \leq \varphi(ab)$$

On sait alors que A est un enneau principal.

Nous commençons par quelques considérations élémentaires sur le calcul matriciel. Soit $X = (u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m} \in \mathrm{Mat}_{n \times m}(A)$. On numérote

$$L_1, \ldots, L_n \in A^m$$

les vecteurs lignes de X et

$$C_1, \ldots, C_m \in A^n$$

les vecteurs colonnes de X. On décrit une liste *d'opérations élémentaires* sur ces vecteurs lignes (respectivement colonnes) de X. Il s'agit de modifications que l'on peut apporter à ces vecteurs sans changer la classe d'équivalence de X. En un sens que l'on ne précisera pas dans ce cours, lorsque l'anneau A est euclidien, ce sont les seules opérations avec cette propriété. Effectuer une opération sur les lignes de X revient à multiplier à gauche X par une certaine *matrice élémentaire*. Effectuer une opération sur les colonnes de X revient à multiplier à droite X par une autre matrice élémentaire.

Définition 3.4.1 Soit $t \in \{m, n\}$.

1. Soit $\lambda \in A$ et $k \in \{1, \ldots, t\}$, $l \in \{1, \ldots t\}$ tels que $l \neq k$. On note $E^t_{k,l}(\lambda) = (e_{i,j})_{1 \leq i,k \leq t} \in \mathrm{GL}_t(A)$ la matrice dont les coefficients sont

$$e_{i,j} = \begin{cases} 1 \text{ si } i = j \\ \lambda \text{ si } i = k \text{ et } j = l \\ 0 \text{ sinon} \end{cases}$$

2. Soit k, $l \in \{1, \ldots, t\}$ tels que $l \neq k$. On note $S_{k,l} = (s_{i,j})_{1 \leq i,j \leq t} \in \mathrm{GL}_t(A)$ la matrice dont les coefficients sont

$$s_{i,j} = \begin{cases} 1 \text{ si } i = j,\ i \neq k \text{ et } i \neq l \\ 0 \text{ si } i = j = k \text{ ou } i = j = l \\ 1 \text{ si } \{i, j\} = \{k, l\} \\ 0 \text{ sinon} \end{cases}$$

Les matrices ci-dessus s'appellent des matrices élémentaires. Examinons l'effet sur les lignes (respectivement les colonnes) de la multiplication par ces matrices :

Proposition 3.4.2

$$E^n_{k,l}(\lambda) \begin{bmatrix} L_1 \\ \vdots \\ L_k \\ \vdots \\ L_l \\ \vdots \\ L_n \end{bmatrix} = \begin{bmatrix} L_1 \\ \vdots \\ L_k + \lambda L_l \\ \vdots \\ L_l \\ \vdots \\ L_n \end{bmatrix}$$

$$[C_1, \ldots, C_k, \ldots, C_l, \ldots C_m] E^m_{k,l}(\lambda) = [C_1, \ldots, C_k, \ldots, C_l + \lambda C_k, \ldots, C_m].$$

$$S^n_{k,l} \begin{bmatrix} L_1 \\ \vdots \\ L_k \\ \vdots \\ L_l \\ \vdots \\ L_n \end{bmatrix} = \begin{bmatrix} L_1 \\ \vdots \\ L_l \\ \vdots \\ L_k \\ \vdots \\ L_n \end{bmatrix}.$$

$$[C_1, \ldots, C_k, \ldots, C_l, \ldots, C_m] S^m_{k,l} = [C_1, \ldots, C_l, \ldots, C_k, \ldots, C_m]$$

Lorsqu'on multiplie une matrice M à gauche par la matrice $E^n_{k,l}(\lambda)$ on laisse toutes les lignes de de M inchangées sauf la k-ième ligne qui est remplacée par $L_k + \lambda L_l$. Lorsqu'on multiplie à droite une matrice M par la matrice $E^m_{k,l}(\lambda)$ on laisse toute les colonnes de M inchangées sauf la l ième qui est remplacée par $C_l + \lambda C_k$. Multiplier une matrice M à gauche par la matrice $S^n_{k,l}$ échange les k ième et l ième lignes de M. Multiplier à droite une matrice M par la matrice $S^m_{k,l}$ échange les k ième et l ième lignes de M. Ces opérations (dites opérations élémentaires sur les lignes et colonnes de M) ne changent donc pas la classe d'équivalence de M.

Passons maintenant à l'algorithme. Soit $X = (u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m} \in \mathrm{Mat}_{n \times m}(A)$. On garde la même notation pour la matrice modifiée à chaque étape. On note C_j sa j ème colonne et L_i sa $i$ème ligne.

1. Si $X = 0$ alors l'algorithme est terminé. Sinon, soit (i_0, j_0) tel que $\varphi(u_{i_0,j_0}) = \inf\{\varphi(u_{i,j}) \mid u_{i,j} \neq 0\}$. Permuter les colonnes C_1 et C_{j_0} puis les lignes L_1 et L_{i_0}. On obtient ainsi u_{i_0,j_0} sur la première ligne et première colonne.

2. On fait des opérations sur les lignes et colonnes afin d'annuler le terme $u_{i,1}$. Pour ceci, on fait la division euclidienne de $u_{i,1}$ par $u_{1,1}$:

$$u_{i,1} = u_{1,1}q + r, \quad \text{et } r = 0 \text{ ou } \varphi(r) < \varphi(u_{1,1})$$

on soustrait q fois L_1 à L_i. Si notre reste est le plus petit des éléments de la matrice, on échange les lignes 1 et i, sinon, on continue. Ceci se termine bien grâce à la définition de la divison euclidienne.

3. On fait de même pour les colonnes.

4. A ce stade, la première colonne et la première ligne sont nuls sauf pour le terme $u_{1,1}$. Si tous les termes de la matrice sont divisibles par $u_{1,1}$. On continue pour la matrice extraite

$$X_2 = (u_{i,j})_{2\leq i\leq n, 2\leq j\leq m} \in \mathrm{Mat}_{(n-1)\times(m-1)}(A).$$

Sinon, il existe i_1 et j_1 tels que $u_{1,1}$ ne divise pas u_{i_1,j_1}, on ajoute la colonne C_{j_1} à la colonne C_1 et on retourne en 2.

On vérifie que cet algorithme se termine car $\varphi(u_{1,1})$ diminue.

Exemple 3.4.3 On considère la matrice à coefficients dans $\mathbb{Z}$

$$X = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 2 & 0 & 0 \\ 0 & 6 & 6 & 0 \\ 3 & 2 & 1 & 1 \end{pmatrix}$$

1. La phase 1 est triviale et notre matrice ne bouge pas.

2. Ensuite, selon les phases 2 et 3, on retranche 2 fois la première ligne à la seconde, 3 fois la première à la 4ème, puis la première colonne à la troisième et à la quatrième. On obtient :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -2 & -2 \\ 0 & 6 & 6 & 0 \\ 0 & 2 & -2 & -2 \end{pmatrix}$$

et en recommençant, on obtient

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

Les facteurs invariants sont donc 1, 2 et 6.

L'algorithme permet en fait de calculer explicitement la matrice $P_{\mathcal{E}\to\mathcal{B}}$ de la remarque 3.3.7 : c'est celle qui enregistre les opérations sur les lignes de la matrice. Il est donc utile de garder en mémoire ces opérations. L'algorithme permet donc théoriquement de calculer explictement une base adaptée. Nous illustrons cette remarque par l'exemple suivant :

Exemple 3.4.4 On se donne le sous-module N de $\mathbb{Z}^4$ engendré par $(1,2,0,0)$, $(0,2,8,0)$, $(1,2,8,0)$ et on désire trouve une base de $\mathbb{Z}^4$ adaptée à N. On écrit la matrice comme dans la remarque 3.3.7.

$$X = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

La stratégie consiste à faire le moins d'opérations possibles sur les lignes afin que la matrice à inverser soit le plus simple possible. On note x, y, z, t les lignes de la matrices. X est équivalente à

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et les lignes restent x, y, z, t. L_2 devient $L_2 - 2L_1$. On obtient :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et les lignes sont x, $y - 2x$, z, t. Ensuite L_3 devient $C_2 - C_3$ et on obtient

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et les lignes sont x, $y - 2x$, z, t. La matrice à inverser pour obtenir la base adaptée est :

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

son inverse est

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

une base adaptée est donnée par $(1,2,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ et $(0,0,0,1)$. On vérifie que $(1,2,0,0)$, $(0,2,0,0)$, $(0,0,8,0)$ est bien une base de N. Les éléments 2 et 8 sont les facteurs invraiants de $\mathbb{Z}^4/N$ et on a donc :

$$\mathbb{Z}^2/N \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$

3.5 Une application

Une application directe du théorème se trouve en théorie des groupes dans le problème de classification de groupes abéliens de type fini. Rappelons qu'un tel groupe est par définition un groupe abélien engendré par un nombre fini de générateurs. Comme un groupe abélien est exactement un $\mathbb{Z}$-module et comme les générateurs en tant que $\mathbb{Z}$-modules sont exactement les générateurs en tant que groupes abéliens, on peut utiliser le théorème 3.1.9 comme $\mathbb{Z}$ est principal :

Théorème 3.5.1 *Soit G un groupe abélien de type fini. Alors il existe un entier s et des entiers naturels $a_1, \ldots, a_r$ tel que a_i divise a_{i+1} pour tout $i = 1, \ldots, r-1$ tels que*

$$G \simeq \mathbb{Z}^s \oplus \bigoplus_{1 \leq i \leq r} \mathbb{Z}/a_i\mathbb{Z}$$

De plus, les a_i et s sont uniquement déterminés par G.

Remarque 3.5.2 Si maintenant, on veut obtenir une classification des groupes abéliens finis, on voit qu'il faut supposer $s = 0$ dans le théorème ci-dessus.

Remarque 3.5.3 Le théorème 3.2.5 de Jordan donne une autre version de la classification grâce au diviseur élémentaires, on passe de l'un à l'autre par le théorème Chinois.

Exemple 3.5.4 Peut-on donner la liste de tous les groupes abéliens d'ordre 108 ? on a $108 = 3^3 \times 2^2$. Les groupes abéliens d'ordres 27 sont

$$\mathbb{Z}/27\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

les groupes abéliens d'ordre 4 sont

$$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

On obtient la liste des groupes abéliens d'ordre 108 :

$$\mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

$$\mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Chapitre 4

Applications des théorèmes de structures

Le but de ce chapitre est d'appliquer toute la théorie exposée dans les chapitres précédents à la théorie des espaces vectoriels. Cependant, nous n'allons pas simplement affirmer qu'un $\mathbb{K}$-espace vectoriel est un $\mathbb{K}$-module et que tous les théorèmes énoncés s'appliquent au $\mathbb{K}$-espace vectoriel (la plupart de ceux-ci était de toute façon déjà connue avant ce cours). Nous allons utiliser ici la structure de $\mathbb{K}[X]$-module afin d'en tirer des information sur les $\mathbb{K}$ espaces vectoriels. Le point de départ essentiel est ici la proposition 1.2.2 qui nous dit que la donnée d'un $\mathbb{K}[X]$-module est exactement la donnée d'un $\mathbb{K}$ espace vectoriel et d'un endomorphisme de celui-ci.

4.1 Invariants de similitudes

Soit $\mathbb{K}$ un corps. Donnons nous E un $\mathbb{K}$-espace vectoriel de dimension finie et u une application linéaire de E dans E. Par la proposition 1.2.2, on a vu qu'on peut alors définir une structure de $\mathbb{K}[X]$-module sur E. Pour prendre en compte cette structure (et la donnée de u), nous notons ce $\mathbb{K}[X]$-module E_u (qui est donc le $\mathbb{K}$-espace vectoriel E muni de sa structure de $\mathbb{K}[X]$-module). Pour tout $P \in \mathbb{K}[X]$ et $x \in E$, on a :

$$P.x := P(u)(x)$$

Le premier résultat suivant est une application du théorème 3.2.2 des facteurs invariants.

{simi}

Théorème 4.1.1 *Soit E un $\mathbb{K}$ espace vectoriel de dimension finie et u un endomorphisme de E. Il existe une unique famille de polynômes unitaires non constant P_i avec $i = 1, ..., r$ tels que*

$$P_i \text{ divise } P_{i+1} \text{ pour tout } i = 1, ..., r-1$$

et tels que

$$E_u \simeq \bigoplus_{i=1}^{r} \mathbb{K}[X]/(P_i).$$

Preuve. On sait que $\mathbb{K}[X]$ est un anneau principal et par l'exemple 2.2.7, on sait que E_u est un $\mathbb{K}[X]$-module de type fini. On peut donc appliquer le théorème 3.2.2 des facteurs invariants , il existe une unique suite d'idéaux non nuls et distincts de $\mathbb{K}[X]$

$$(P_r) \subset \ldots \subset (P_1)$$

où pour $1 \leq i \leq r$ les P_i sont dans $\mathbb{K}[X]$ et il existe un entier s tel que

$$E_u \simeq \mathbb{K}[X]^s \oplus \bigoplus_{1 \leq i \leq r} \mathbb{K}[X]/(P_i)$$

On a donc que P_i divise P_{i+1} pour tout $i = 1, ..., r-1$ et on peut choisir ces polynômes unitaires car ils sont définis à inversibles près (et donc à un élément de $\mathbb{K}$ près). Ils sont non inversibles donc non constants et non nuls. Il reste donc à montrer que $s = 0$. L'isomorphisme ci-dessus est un isomorphisme de $\mathbb{K}[X]$-module. Il a ainsi une structure de morphisme de $\mathbb{K}$-espace vectoriel. Comme il est bijectif, c'est un isomorphisme de $\mathbb{K}$ espace vectoriel. Or la dimension de E est fini, comme la dimension de $\mathbb{K}[X]$ est infini, on conclut que $s = 0$ ce qui achève la démonstration.

Définition 4.1.2 Les polynômes $P_1, \ldots, P_r$ du théorème ci-dessus sont appelés les *invariants de similitude* de u.

Remarque 4.1.3 Affinons la propriété de dimension utilisée dans la preuve ci-dessus. Notons que la dimension d'un $\mathbb{K}$-espace vectoriel du type $\mathbb{K}[X]/(P)$ avec $P \in \mathbb{K}[X]$ est de $\deg(P)$ (avec la remarque 1.4.4). L'isomorphisme du théorème indique donc que

$$\dim(E) = \deg(P_1) + \ldots + \deg(P_r)$$

Ainsi le nombre d'invariants de similitudes est toujours inférieur à la dimension de E.

Le terme "invariant de similitudes" va se justifier grâce aux deux résultats suivants.

Proposition 4.1.4 *Soit u et v deux endomorphismes d'un $\mathbb{K}$-espace vectoriel E. Alors on a*

$$E_u \simeq E_v \iff u \text{ et } v \text{ sont semblables}$$

(l'isomorphisme est un isomorphisme de $\mathbb{K}[X]$-module)

Preuve. On suppose u et v semblables alors il existe un endomorphisme inversible ϕ de E tel que

$$v \circ \phi = \phi \circ u$$

On considère le morphisme naturel

$$\Phi : E_u \to E_v$$

tel que $\Phi(x) = \phi(x)$ pour tout $x \in E_u$ (on change de notation simplement pour mettre en valeur le fait que les structures changent). C'est bien un morphisme de $\mathbb{K}[X]$-modules. En effet, si P est un polynôme, on a

$$\Phi(P.x) = \Phi(P(u)(x)) = \phi(P(u)(x)).$$

La propriété $v \circ \phi = \phi \circ u$ implique alors que

$$\Phi(P.x) = P(v)(\phi(x)) = P.\phi(x) = P.\Phi(x)$$

Il est clair que ce morphisme est bijectif. On a donc un isomorphisme $\mathbb{K}[X]$-modules entre E_u et E_v.

Réciproquement, si E_u et E_v sont isomorphes, on a un morphisme bijectif de $\mathbb{K}[X]$-modules

$$\Phi : E_u \to E_v$$

qui définit un morphisme d'espace vectoriel $\Phi : E \to E$ bijectif tel que $\phi(x) = \Phi(x)$. Pour tout $x \in E$, le fait que Φ soit un morphisme implique que pour tout $x \in E$, on a $X.\Phi(x) = \Phi(X.x)$ ce qui se traduit par $u(\phi(x)) = \phi(v(x))$. On a donc $u \circ \phi = \phi \circ v$.

□

Par unicité des invariants de similitude, on obtient le théorème suivant qui donne un critère pratique pour déterminer si deux endomorphismes sont semblables.

{similitude}

Théorème 4.1.5 *Deux endomorphismes d'un $\mathbb{K}$-espace vectoriel de dimension finie E sont semblables si et seulement si ils ont les mêmes invariants de similitudes.*

Si M est une matrice représentant l'endomorphisme u de E. Les invariants de similtudes de M sont par définition ceux de u. Bien sûr, deux matrices sont alors semblables si et seulement si elles ont les mêmes invariants de similitudes.

Le principal problème est donc maintenant de calculer explicitement ces invariants de similitudes. C'est le but du chapitre suivant.

4.2 Méthodes de calculs

Dans cette section, nous donnons une manière simple de calculer les invariants de similitudes d'un endomorphisme d'un $\mathbb{K}$-espace vectoriel E.

{le1}

Lemme 4.2.1 *Soit E un $\mathbb{K}$ espace vectoriel de dimension n et u un endomorphisme de E. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. Soit*

$$\mathcal{A} = \mathrm{Mat}_{\mathcal{B},\mathcal{B}}(u) = (a_{i,j})_{1 \leq i,j \leq n}$$

la matrice de u dans la base $\mathcal{B}$ (au départ et à l'arrivée). Soit $\mathfrak{B} = (\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique du $\mathbb{K}[X]$-module libre $\mathbb{K}[X]^n$. On définit $\Psi \in \mathrm{End}_{\mathbb{K}[X]}(\mathbb{K}[X]^n)$ par

$$\forall j \in \{1, \ldots, n\},\ \Psi(\varepsilon_j) = X\varepsilon_j - \sum_{1 \leq i \leq n} a_{i,j}\varepsilon_i$$

Alors :

- $\det(\Psi) = \det(X\,Id - \mathcal{A})$ *est le polynôme caractéristique de u.*
- *La dimension du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]^n / \mathrm{Im}(\Psi)$ est de n*

Preuve. La matrice de Ψ dans la base $\mathfrak{B}$ de $\mathbb{K}[X]^n$ n'est autre que $X\mathrm{Id} - \mathcal{A}$ donc la première partie du lemme suit. Le $\mathbb{K}[X]$-module $\mathbb{K}[X]^n / \mathrm{Im}(\Psi)$ est de type fini donc d'après le théorème des facteurs invariants, comme il existe des

polynômes P_i pour $i = 1, \ldots, r$ tel que P_i divise P_{i+1} pour tout $i = 1, ..., r-1$ tels que

$$\mathbb{K}[X]^n / \operatorname{Im}(\Psi) \simeq \mathbb{K}[X]^s \oplus \bigoplus_{1 \leq i \leq r} \mathbb{K}[X]/(P_i)$$

avec $s \in \mathbb{N}$.D'après la remarque 3.3.8, quitte à supposer que certains de ces polynômes sont égaux à 1 (ce qui peut arriver lorsque l'on regarde les facteurs invariants d'une matrice), les polynomes P_i sont les facteurs invariants d'une matrice de Ψ. Or, Le déterminant de Ψ engendre $J_n(X\mathrm{Id} - A)$.

On voit tout d'abord que, ce déterminant étant non nul, on a nécessairement $r = n$. $J_n(X\mathrm{Id} - A)$ est alors engendré par le produit des P_i (qui sont donc tous non nuls). Ainsi, à multiplication par un élément de $\mathbb{K}$ près, le polynôme caractéristique est égale au produit des P_i. Ce produit est donc de degré n. Or, on a

$$\dim_{\mathbb{K}}(\bigoplus_{1 \leq i \leq r} \mathbb{K}[X]/(P_i)) = \sum_{1 \leq i \leq n} \deg(P_i) = n$$

d'où le résultat.

□

{reimp}

Remarque 4.2.2 Dans la preuve, nous avons montré que le polynôme caractéristique de u est le produit des facteurs invariants de $\mathbb{K}[X]^n / \operatorname{Im}(\Psi)$

{equival}

Proposition 4.2.3 *Sous les hypothèses du lemme 4.2.1, on a :*

$$E_u \simeq \mathbb{K}[X]^n / \operatorname{Im}(\Psi)$$

Preuve On définit le morphisme surjectif de $\mathbb{K}[X]$-modules

$$\varphi : \mathbb{K}[X]^n \to E_u$$

tel que pour tout $1 \leq j \leq n$, on a $\varphi(\varepsilon_j) = e_j$. Montrons que $\operatorname{Im}(\Psi) \subset \operatorname{Ker}(\varphi)$. Soit donc $1 \leq j \leq n$, on a :

$$\begin{array}{rcl} \varphi(\Psi(\varepsilon_j)) & = & \varphi(X.\varepsilon_j - \sum_{1 \leq i \leq n} a_{i,j}\varepsilon_j) \\ & = & X.\varphi(\varepsilon_j) - \sum_{1 \leq i \leq n} a_{i,j}\varphi(\varepsilon_j) \\ & = & X.e_j - \sum_{1 \leq i \leq n} a_{i,j}e_j \\ & = & u(e_j) - \sum_{1 \leq i \leq n} a_{i,j}e_j \\ & = & 0 \end{array}$$

par définition de l'action de $\mathbb{K}[X]$. On peut donc factoriser le morphisme φ en un morphisme surjectif

$$\widetilde{\varphi} : \mathbb{K}[X]^n / \operatorname{Im}(\Psi) \to E_u$$

c'est un morphisme $\mathbb{K}[X]$-modules donc aussi un morphisme de $\mathbb{K}$-espaces vectoriels. Or, on a d'une part

$$\dim(E) = n$$

et d'autre part la dimension de $\mathbb{K}[X]^n / \operatorname{Im}(\Psi)$ est aussi n d'après le lemme 4.2.1. Le morphisme de $\mathbb{K}$-espaces vectoriels est donc bijectif. $\widetilde{\varphi}$ est donc un morphisme bijectif de $\mathbb{K}[X]$-module. Ceci conclut la démonstration.

□

De cette proposition, nous pouvons en tirer une méthode de calcul pratique pour les invariants de similitudes d'un morphisme :

- les invariants de similitudes de u sont les facteurs invariants de E_u,
- on sait que $E_u \simeq \mathbb{K}[X]^n / \operatorname{Im}(\Psi)$
- on sait que les facteurs invariants de $\mathbb{K}[X]^n / \operatorname{Im}(\Psi)$ sont ceux d'une matrice de Ψ (en enlevant les polynômes constants).

Ainsi, on obtient le théorème suivant :

Théorème 4.2.4 *Soit u un endomorphisme de E de matrice U alors les invariants de similitudes de u sont les facteurs invariants non inversibles de la matrice $U - XId$ de $\mathcal{M}_n(\mathbb{K}[X])$.*

{exinv}

Exemple 4.2.5 On considère la matrice suivante à coefficients dans $\mathbb{C}$

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

et on va chercher ces invariants de similitudes, on doit donc chercher les facteurs invariants de la matrice suivante à coefficients dans $\mathbb{C}[X]$.

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

On applique l'algorithme décrit dans la section 3.4 afin de trouver les facteurs invariants. Cette matrice est équivalente à

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

puis à

$$\begin{pmatrix} 1 & 2-X & 1 \\ 0 & (2-X)(X-3) & X-2 \\ 0 & X-2 & 2-X \end{pmatrix}$$

puis à

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & (2-X)(X-3) & X-2 \\ 0 & X-2 & 2-X \end{pmatrix}$$

qui est équivalente à

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)(4-X) \end{pmatrix}$$

ce qui nous donne les invariants de similtudes de A : $(X-2)$ et $(X-2)(X-4)$. Pour vérifier si une matrice quelconque est semblable à celle-ci, il suffit donc de montrer que ces invariants de siiltudes sont les mêmes. Pour calculer ces invariants, on aurait aussi pu se servir des idéaux de Fitting et de la proposition 3.3.5

Maintenant nous allons interpréter certains polynômes faisant partis des invariants de similtiudes d'un endomorphisme.

Proposition 4.2.6 *Soit $P_1, \ldots, P_r$ les invariants de similitudes d'un endomorphisme u de E. Alors P_r est le polynôme minimal de u et le produit $P_1.P_2.\ldots.P_r$, le polynôme caractéristique.*

Preuve. Le fait que le produit des invariants de similitudes est le polynôme caractéristique est une combinaison de la remarque 4.2.2 avec la proposition 4.2.3. Ensuite, on a $E_u \simeq \mathbb{K}[X]^n/\operatorname{Im}(\Psi)$. De plus, on a d'une part

$$\operatorname{Ann}_{\mathbb{K}[X]}(\mathbb{K}[X]/\operatorname{Im}(\Psi)) = (P_r)$$

d'après la remarque 3.2.4. D'autre part, on a $P \in \operatorname{Ann}_{\mathbb{K}[X]}(E_u)$ si et seulement si pour tout $x \in E$, on a $P.x = 0$ soit encore $P(u)(x) = 0$. $\operatorname{Ann}_{\mathbb{K}[X]}(E_u)$ est donc l'ensemble des polynômes annulateurs de$u$. On sait que cet idéal est engendré par le polynôme minimal de u d'où le résultat.

□

Remarque 4.2.7 Notons que le théorème de Cayley-Hamilton (le polynôme caractéristique est annulateur) est un corollaire immédiat de la proposition précédente !

Exemple 4.2.8 Le polynôme minimal de la matrice A de l'exemple 4.2.5 est donc $(X-2)(X-4)$ et le polynôme caractéristique est $(X-2)^2(X-4)$ ce que l'on vérifie facilement.

Nous passons maintenant à deux méthodes remarquables de réduction d'une matrice. On cherche dans les deux cas des matrices simples se trouvant dans la classe de similtude d'une matrice donnée.

4.3 Réduction de Frobenius

Donnons nous $P = a_0 + a_1X + ... + a_nX^n$ un polynôme dans $\mathbb{K}[X]$ et considérons le $\mathbb{K}[X]$-module $\mathbb{K}[X]/(P)$. C'est aussi un $\mathbb{K}$ espace vectoriel. On va considérer l'application

$$u_P : \mathbb{K}[X]/(P) \to \mathbb{K}[X]/(P)$$

de multiplication par X. Il est facile de voir qu'il est bien défini et que c'est un morphisme d'espace vectoriel.

Prenons la base $(\pi(1), ..., \pi(X^{n-1}))$ de $\mathbb{K}[X]/(P)$ (π étant la surjection canonique de $\mathbb{K}[X]$ dans $\mathbb{K}[X]/(P)$). Si on écrit la matrice de u_P dans cette base, on obtient la matrice

$$C_P = \begin{pmatrix} 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & \cdots & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Celle-ci est appelée la **matrice compagnon de** P. Si maintenant, on considère le $\mathbb{K}$ espace vectoriel $\bigoplus_{i=1}^{s} \mathbb{K}[X]/(P_i)$, on montre de même que le morphisme

de multiplication par X est représenté dans une base appropriée (obtenue en réunissant les bases données ci-dessus) par la matrice suivante.

$$C = \begin{pmatrix} C_{P_1} & 0 & ... & 0 \\ 0 & C_{P_2} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & C_{P_s} \end{pmatrix}$$

Notons $\mathcal{B}$ la base de $\bigoplus_{i=1}^{s} \mathbb{K}[X]/(P_i)$ dans laquelle cette matrice est écrite

Si u a comme invariants de similitudes $P_1, \ldots, P_s$ alors E_u est isomorphe à $\bigoplus_{i=1}^{s} \mathbb{K}[X]/(P_i)$ comme $\mathbb{K}[X]$-module via un morphisme

$$\Psi : E_u \to \bigoplus_{i=1}^{s} \mathbb{K}[X]/(P_i)$$

On a alors

$$\Psi(u(x)) = \Psi(X.x) = X.\Psi(x) = u_P(\Psi(x))$$

On voit alors que u et u_P sont semblables en tant que morphisme de $\mathbb{K}$ espace vectoriel. Plus précisement, la matrice de u dans la base $\Psi^{-1}(\mathcal{B})$ du $\mathbb{K}$ espace vectoriel E est C. On vient de montrer :

Théorème 4.3.1 *Soit u un endomorphisme dont les invariants de similitudes sont P_1, ..., P_s alors il existe une base de E dans laquelle, la matrice de u est la matrice par blocs :*

$$C = \begin{pmatrix} C_{P_1} & 0 & ... & 0 \\ 0 & C_{P_2} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & C_{P_s} \end{pmatrix}$$

une telle matrice est dite **réduite de Frobenius**.

De plus, il n'est pas difficile de montrer que si on impose les conditions usuelles "P_i divise P_{i+1} pour tout $i = 1, ..., s-1$", on a l'unicité de cette décomposition.

Exemple 4.3.2 Ainsi une matrice 3×3 dont les invariants de similitudes sont $P_1 = (X-2)$ et $P_2 = (X-2)(X-4) = X^2 - 6X + 8$ est semblable à une matrice par blocs donnés par les matrices compagnons C_{P_1} et C_{P_2} c'est à dire à

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -8 \\ 0 & 1 & 6 \end{pmatrix}$$

On peut d'ailleurs facilement vérifier que les invariants de similitude de cette matrice sont bien P_1 et P_2.

Une autre possibilité de réduction est donnée dans la section suivante.

4.4 Réduction de Jordan

La réduction de Frobenius correspond essentiellement en une application du théorème 3.2.5 des facteurs invariants au $\mathbb{K}[X]$-module E_u. Celui-ci est équivalent au théorème précédent par le lemme chinois and la mesure où on suppose que $\mathbb{K}$ est algébriquement clos ce que l'on fait dans cette section.

Si u a comme invariants de similitudes $P_1, \ldots, P_s$ alors E_u est isomorphe à $\bigoplus_{i=1}^{s} \mathbb{K}[X]/(P_i)$, les éléments irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1, i.e. les $(X-\lambda)$ où $\lambda \in \mathbb{K}$. En décomposant grâce au lemme chinois, on voit qu'il existe une famille $(\lambda_1, \ldots, \lambda_l)$ d'éléments de $\mathbb{K}$ deux à deux distincts et pour tout $i = 1, \ldots, l$, un entier j_i et une famille d'entiers

$$n_{i,1}, \ldots, n_{i,j_i} > 0$$

tel que

$$E_u \simeq \bigoplus_{1 \leq i \leq l} \bigoplus_{1 \leq j \leq j_i} \mathbb{K}[X]/(X-\lambda_i)^{n_{i,j}}$$

En appliquant le même raisonnement que dans la section précédente, on voit que u est semblable à u_P le morphisme de multiplication par X dans le $\mathbb{K}[X]$-module

$$\bigoplus_{1 \leq i \leq l} \bigoplus_{1 \leq j \leq j_i} \mathbb{K}[X]/(X-\lambda_i)^{n_{i,j}}$$

Or, en appliquant l'exemple 1.4.5, on voit que dans une base appropriée, ce morphisme se représente par la matrice suivante (en adoptant la même démarche que dans la section précédente) :

$$\begin{pmatrix} J_{\lambda_1,n_{1,1}} & 0 & \ldots & 0 \\ 0 & J_{\lambda_1,n_{1,2}} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & J_{\lambda_l,n_{l,j_l}} \end{pmatrix}$$

où on note :

$$J_{\lambda,n} := \begin{pmatrix} \lambda & 0 & 0 & \ldots & 0 \\ 1 & \lambda & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & \lambda & 0 \\ 0 & \ldots & 0 & 1 & \lambda \end{pmatrix} \in \mathcal{M}_{n,n}(\mathbb{K})$$

On vient de montrer :

Théorème 4.4.1 *Soit u un endomorphisme dont les invariants de similitudes sont P_1, ..., P_s alors il existe une base de E dans laquelle, la matrice de u est la matrice par blocs :*

$$\begin{pmatrix} J_{\lambda_1,n_{1,1}} & 0 & \ldots & 0 \\ 0 & J_{\lambda_1,n_{1,2}} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & J_{\lambda_l,n_{l,j_l}} \end{pmatrix}$$

une telle matrice est dite réduite de Jordan. Les λ_i et les entiers $n_{i,j}$ sont entièrement déterminés par la décomposition des P_i en facteurs irréductibles.

Remarque 4.4.2 Comme P_1 est le polynôme minimal, on voit que les λ ci-dessus sont les valeurs propres de u

Remarque 4.4.3 La donnée de la réduite de Jordan permet le calcul aisé des dimension des sous-espaces propres de u. En effet, on voit que pour tout $i = 1, \ldots, l$, on a

$$\mathrm{Ker}(u - \lambda_i \mathrm{id}) = j_i$$

car chaque bloc $J_{\lambda,n}$ est telle que $\dim(\mathrm{Ker}(J_{\lambda,n} - \lambda \mathrm{id})) = 1$.

Remarque 4.4.4 Le théorème ci-dessus est en fait valable si $\mathbb{K}$ n'est pas algébriquement clos mais il faut supposer que le polynôme caractéristique est scindée. Ceci implique que les invariants de similitudes le sont et on peut donc développer la démonstration comme ci-dessus.

Exemple 4.4.5 Pour trouver la réduite de Jordan d'une matrice 3×3 dont les invariants de similitudes sont $P_1 = (X - 2)$ et $P_2 = (X - 2)(X - 4)$, il faut utiliser le Lemme Chinois :

$$\mathbb{K}[X]/P_1 \oplus \mathbb{K}[X]/P_2 \simeq \mathbb{K}[X]/(X - 2) \oplus \mathbb{K}[X]/(X - 2) \oplus \mathbb{K}[X]/(X - 4)$$

et la réduite de Jordan associé est :

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

Ceci est logique : le polynôme minimal est ici scindée à racine simple. L'endomorphisme associée et donc diagonalisable, c'est à dire semblable à une matrice diagonale. Dans ce cas, chaque bloc de Jordan est de taille 1×1 et donc la réduite de Jordan est diagonale.

Exemple 4.4.6 Pour trouver la réduite de Jordan d'une matrice 4×4 dont le seul invariant de similitude est $P_1 = (X - 2)^2(X - 4)^2$, il faut utiliser le Lemme Chinois :

$$\mathbb{K}[X]/P_1 \simeq \mathbb{K}[X]/(X - 2)^2 \oplus \mathbb{K}[X]/(X - 4)^2$$

et la réduite de Jordan associée est :

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

Chapitre 5

Introduction à la théorie des réseaux

Dans ce chapitre, on s'intéresse aux conséquence des théorèmes de structures sur la théorie des réseaux. Comme nous allons le voir, un réseau est un cas particulier de $\mathbb{Z}$-module libre. Nous allons étudier la structure de ces nouveaux objets et nous verrons cerrtaines applications en arithmétique notamment.

5.1 Sous groupes discrets

On rappelle que $\mathbb{R}^n$ muni du produit scalaire usuel est un espace euclidien :

$$\langle (x_1, x_2, \cdots, x_n), (y_1, y_2, \cdots, y_n) \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n = \sum_{i=1}^{n} x_iy_i,$$

On note $||\ .\ ||$ la norme associée. La boule fermé de centre $a \in \mathbb{R}^n$ et de rayon R sera noté $B(a, R)$.

Définition 5.1.1 On appelle réseau de $\mathbb{R}^n$ un $\mathbb{Z}$-module libre de rang n engendré par une $\mathbb{Z}$-base de $\mathbb{R}^n$.

Un réseau est un cas particulier de sous groupe discret de $\mathbb{R}^n$ (ie un sous-groupe de $\mathbb{R}^n$ dont ces sous ensembles sont ouverts). On peut assez facilement montrer que dans $\mathbb{R}$; les sous groupes discret sont soit denses soit discret ! Soit $(\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $\mathbb{R}^n$. Un réseau est engendré par une base $(e_1, \ldots, e_n)$ de $\mathbb{R}^n$. On sait qu'il existe une matrice inversible M envoyant $(\varepsilon_1, \ldots, \varepsilon_n)$ sur $(e_1, \ldots, e_n)$. Le réseau est alors égal à $M.\mathbb{Z}^n$ où :

$$M\mathbb{Z}^n := \{Mx \mid x \in \mathbb{Z}^n\}$$

Lemme 5.1.2 *Soit M et N deux matrices de $GL_n(\mathbb{R})$. Supposons que $G = M\mathbb{Z}^n = N\mathbb{Z}^n$ soit un réseau de $\mathbb{R}^n$ alors $N^{-1}M \in GL_n(\mathbb{Z})$ et ainsi $det(M) = \pm det(N)$. L'élément $|det(M)|$ est un invariant pour G appelé le déterminant de G.*

Preuve. On a $N^{-1}M\mathbb{Z}^n = \mathbb{Z}^n$ et donc NM^{-1} est à coefficients dans $\mathbb{Z}$. On a alors $\det(N)^{-1}\det(M) \in \mathbb{Z}$ ce qui implique bien le résultat.

□

Définition 5.1.3 Soit $G = \oplus_{1\leq i\leq n}\mathbb{Z}e_i$ un reseau de $\mathbb{R}^n$ où $(e_1, \ldots, e_n)$ est une base de $\mathbb{R}^n$. On appelle parallélotope fondamental de G le convexe suivant :

$$\mathcal{P}(e_1, \ldots, e_n) = \{x \in \mathbb{R}^n \mid x = \sum_{1\leq i\leq n} \lambda_i e_i,\ 0 \leq \lambda_i < 1\}$$

Nous allons chercher un invariant des parallélotopes fondamentaux :

Proposition 5.1.4 *Un parallélotope fondamental d'un réseau G est mesurable au sens de Lebesgue et on a $\mu(\mathcal{P}) = det(G)$. Cet invariant que l'on note μ_G s'appelle le covolume ou la mesure de la maille du réseau G.*

Preuve Si on prend la base canonique $(\varepsilon_1, \ldots, \varepsilon_n)$ de $\mathbb{R}^n$, on obtient un parallélotope $\mathcal{P}_0$ qui est un pavage de $\mathbb{R}^n$, il est donc mesurable. Ensuite si $(e_1, \ldots, e_n)$ est une base quelconque, il existe une matrice M tel que $M(\varepsilon_1, \ldots, \varepsilon_n) = (e_1, \ldots, e_n)$. Donc $\mathcal{P}$ est l'image réciproque d'un ensemble mesurable par une application continue. Cet ensemble est donc mesurable comme image réciproque d'un mesurable par une application continue. Ensuite par changement de variable :

$$\mu(\mathcal{P}) = \int_{\mathcal{P}} d\mu = \int_{M(\mathcal{P}_0)} d\mu = |\det(M)| \int_{\mathcal{P}_0} d\mu = |\det(M)|.$$

□

{quo}

Proposition 5.1.5 *Si $H \subset G$ est un réseau de $\mathbb{R}^n$ contenu dans le réseau G, on a :*

$$\mu_H = \mu_G \times (G : H)$$

Preuve. H est un sous-module du $\mathbb{Z}$-module G. Il existe une base $(e_1, \ldots, e_n)$ de G adapté à H c'est à dire des éléments a_1, a_2, …, a_n de $\mathbb{Z}$ tel que a_i divise a_{i+1} pour tout $i = 1, \ldots, n-1$ et tel que

$$G = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \ldots \oplus \mathbb{Z}e_n$$

$$H = \mathbb{Z}a_1e_1 \oplus \mathbb{Z}a_2e_2 \oplus \ldots \oplus a_n\mathbb{Z}e_n$$

On a $G = M\mathbb{Z}^n$ où M est la matrice de changement de base de la base canonique de $\mathbb{R}^n$ à $(e_1, \ldots, e_n)$. On a alors $H = MA\mathbb{Z}^n$ où A est la matrice de changement de base de $(e_1, \ldots, e_n)$ à $(a_1e_1, \ldots a_ne_n)$. On a alors

$$\begin{array}{rcl} \det(H) & = & \det(MA) \\ & = & a_1 \ldots a_n \det(G) \end{array}$$

ce qu'il fallait montrer.

□

5.2 Le théorème de Minkowski et applications

Lemme 5.2.1 *Soit G un réseau de $\mathbb{R}^n$ et soit $\mathcal{M}$ un sous-ensemble mesurable de $\mathbb{R}^n$ tel que $\mu(\mathcal{M}) > \mu_G$ alors il existe $(x, y) \in \mathcal{M}^2$ avec $x \neq y$ et $x - y \in G$.*

Preuve. Soit $\mathcal{P}$ un parallèlotope fondamental pour G On voit que l'on a une partition :

$$\mathbb{R}^n = \sqcup_{g\in G}(\mathcal{P} + g).$$

D'où une partition :

$$\mathcal{M} = \sqcup_{g\in G}(\mathcal{P} + g) \cap \mathcal{M}.$$

On obtient :

$$\mu(\mathcal{M}) = \sum_{g\in G} \mu((\mathcal{P} + g) \cap \mathcal{M}) = \sum_{g\in G} \mu(\mathcal{P} \cap (\mathcal{M} - g))$$

Supposons maintenant que les $\mathcal{P}\cap(\mathcal{M}-g)$ soient disjoints alors le dernier terme est plus petit que $\mu(\mathcal{P})$ ce qui est exclus. Donc il existe $(g, g') \in G^2$ tel que $g \neq g'$ et $\mathcal{P}\cap(\mathcal{M}-g)\cap(\mathcal{M}-g') \neq \emptyset$. Ainsi, il existe $(x, y) \in \mathcal{M}^2$ avec $x-g = y-g'$. On conclut que $x-y = g-g' \in G\backslash\{0\}$ puisque $g \neq g'$ sont deux éléments distincts de G. □

Théorème 5.2.2 (Minkowski) *Soit G un réseau de $\mathbb{R}^n$ et soit $S \subset \mathbb{R}^n$ un ensemble mesurable vérifiant les trois propriétés suivantes :*

1. *S est symétrique par rapport à 0,*
2. *S est convexe.*
3. *$\mu(S) > 2^n\mu_G$ ou $\mu(S) \geq 2^n\mu_G$ avec S compact.*

Alors $S \cap G$ contient un élément non nul.

Preuve. On suppose tout d'abord que $\mu(S) > 2^n\mu_G$. On applique le lemme précédent à $(1/2)S$ sachant que $\mu((1/2)S) = \mu(S)/2^n$. On trouve l'existence de x et y distincts dans $(1/2)S$ tels que $x-y \in G$. Or, on a $x-y = (1/2)(2x-2y) \in S$ puisque S est symétrique et convexe d'où le résultat dans le cas $\mu(S) > 2^n\mu_G$.

Si $\mu(S) \geq 2^n\mu_G$ et S compact, on applique le premier cas à $(1 + 1/n)S$ et on obtient une suite décroissante de compacts non vide :

$$K_n = ((1 + 1/n)S) \cap G$$

L'intersection est donc non vide et un élément dans l'intersection est dans $S\cap G$ par compacité.

□

Passons maintenant à un exemple d'application intéressante en arithmétique. On dit qu'un entier n est somme de deux carrés si il existe a et b dans $\mathbb{N}$ tel que $n = a^2 + b^2$. Voici un premier résultat concernant les entiers somme de deux carrés relativement facile :

Proposition 5.2.3 *Un nombre entier positif congrue à 3 modulo 4 ne peut être somme de deux carrés.*

Preuve. On considère l'équation $a^2+b^2 = n$ que l'on réduit modulo 4. Un carré est congru à 0 ou 1 modulo 4 donc cette équation ne peut avoir de solution.

□

Théorème 5.2.4 *Si p est un nombre premier congru à 1 ou 2 modulo 4 alors p est somme de deux carrés.*

Preuve. Si p est premier congru à 2 modulo 4 alors p est égal à 2, il est alors égal à $1^2 + 1^2$. Supposons maintenant $p \equiv 1[4]$. On sait que le groupe $\mathbb{F}_p^\times$ est cyclique d'ordre divisible par 4. Il existe donc un élément u d'ordre 4 qui vérifie donc $u^2 = -1$. Considérons l'ensemble $R = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv ub[p]\}$. C'est un réseau avec $\mathbb{Z}$-base $(u, 1)$ et $(p, 0)$. Notons que l'on a une application surjective $\mathbb{Z}^2 \to \mathbb{F}_p$ envoyant (a, b) sur la classe de $a - ub$ dont le noyau est R. L'indice de R dans le réseau $\mathbb{Z}^2$ est donc p. Donc par la proposition 5.1.5, le déterminant de $\mathbb{Z}^2$ étant égal à 1, on conclut que le covolume de R est p.

On utilise le théorème de Minkowski pour S, un disque de rayon $r \in \mathbb{R}^+$. On sait alors que si $\mu(S) > 2^2 p$ alors $R \cap S$ contient un élément non nul. On a $\mu(S) = \pi r^2$. On choisit donc r tel que $(4p/\pi) < r^2 < 2p$. On obtient un élément (a, b) dans l'intersection. On a alors $0 < a^2 + b^2 < 2p$ d'une part et $a^2 + b^2 \equiv 0[p]$ d'autre part. Ceci implique $a^2 + b^2 = p$.

□