Module sur Anneau Principal

Rakdi Mohamed Anour

30 mai 2017

Table des matières

Introduction

Le terme module a été introduit en 1871 par Richard Dedekind pour désigner un sous- groupe du groupe additif d'un anneau.

Par la suite, cette notion a été largement généralisée puisque aujourd'hui on désigne par le mot module un ensemble vérifiant toutes les hypothèses qui définissent un espace vectoriel à l'exception d'une seule : les scalaires sont des éléments d'un anneau et pas forcément d'un corps.

Ainsi notre mémoire comporte trois chapitres :

Dans le premier chapitre on présente des notions fondamentales sur les anneaux et leurs propriétés comme la division et des notions sur les anneaux principaux .

Dans le deuxième chapitre on définit les modules et les sous-modules sur les anneaux, les morphismes de module, modules quotients, somme directe et produit direct, modules de type fini, modules libres en donnant un exemple de $\mathbb{Z}$-module libre sur l'anneau d'entiers d'un corps de nombres .

Dans le troisième chapitre on donne des propriétés sur les modules des anneaux principaux, la structure des modules sur un anneau principal, les facteurs invariants, on présente à la fin de ce chapitre une approche matricielle du théorème de base adapté avec une application directe.

Chapitre 1

Notions fondamentales

1.1 Notions sur les anneaux

Définition 1.1

Un anneau $(A, +, \cdot)$ est la donnée d'un ensemble non vide A muni de deux lois de composition internes, notées " $+$ " et " $\cdot$ " (appelées respectivement addition et multiplication), telles que :

1. $(A, +)$ est un groupe abélien (on notera 0 son élément neutre)
2. La loi " $\cdot$ " est associative i.e. $\forall x, y, z \in A,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
3. La loi " $\cdot$ " est distributive par rapport à la loi " $+$ "

$$\forall x, y, z \in A,\ x \cdot (y + z) = x \cdot y + x \cdot z \ \text{ et } \ (x + y) \cdot z = x \cdot z + y \cdot z$$

Remarques 1.1

1. Si la loi " $\cdot$ " est commutative i.e $\forall x, y \in A,\ x \cdot y = y \cdot x$, on dit que l'anneau A est commutatif.
2. Si la loi " $\cdot$ " posséde un élément neutre 1, on dit que A est un anneau unitaire et 1 s'appelle l'unite de A.

Exemples 1.1

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux commutatifs unitaires.

Définition 1.2

Un anneau commutatif A est dit intègre s'il est non nul, et si pour tous a,b de A, la condition $a \cdot b = 0$ implique $a = 0$ ou $b = 0$.

Exemple 1.2

Pour $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

1.2 Propriétés sur les anneaux

Définition 1.3

Soit A un ensemble non vide et soient " $+$ " et " $\cdot$ " deux lois internes sur A.

Le triplet $(A, +, \cdot)$ possède une structure de corps si :

1. $(A, +, .)$ a une structure d'anneau commutatif unitaire.
2. $(A \setminus \{0\}, \cdot)$ a une structure de groupe (abélien).

Exemple 1.3

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ des corps pour leur addition et multiplication respectives.

Définition 1.4

Soit $(A, +, \cdot)$ un anneau.

Un idéal (bilatère) de A est une partie non vide de A tel que :

1. $\forall x, y \in I$ on a $x - y \in I$
2. $\forall a \in A, \forall x \in I$ on a $x \cdot a \in I$ et $a \cdot x \in I$.

Exemples 1.4

1. $\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps.
2. Les ideaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Proposition 1.1

Soient A un anneau commutatif unitaire, et I un idéal de A.

a) $1 \in I \iff I = A$

b) *Soit* $x \in U(A)$

$$x \in I \iff I = A$$

Preuve.

a) L'implication ($\Leftarrow$) est evidente

($\Rightarrow$)

Supponsons que $1 \in I$. Comme $I \subset A$, il suffit de montrer que $A \subset I$.

Soit $x \in A$ et $1 \in I$ et comme I est un idéal de A alors $x \cdot 1 = 1 \cdot x = x \in I$

Donc $A \subset I$.

b) Soit $x \in U(A)$

L'implication ($\Leftarrow$) est evidente

($\Rightarrow$)

Si $x \in I$ avec $x \in U(A)$, alors $\exists y \in A$ tel que $x \cdot y = y \cdot x = 1$

Il resulte que $1 \in I$, donc $I = A$. ■

1.3 Division dans un anneau

Définition 1.5

Soient A un anneau commutatif unitaire intègre, a et b deux éléments de A. On dit que a divise b et on ecrit $a \mid b$ si il existe q de A tel que : $b = a \cdot q$.

Exemples 1.5

1) $A = \mathbb{Z}$, $3 \mid 9$ et $(-3) \mid 9$

2) $A = \mathbb{Z}/6\mathbb{Z}$, $\overline{5} \mid \overline{4}$ car $\overline{2} \cdot \overline{5} = \overline{10} = \overline{4}$

Théorème 1.1

On a l'équivalence suivante :

$$a \mid b \iff (b) \subset (a)$$

où $(a) = \{ax \mid x \in A\}$ *est l'idéal principal engendré par* a.

Preuve.

($\Rightarrow$)

Soit $x \in (b)$ alors $\exists k \in A$ tel que $x = b \cdot k$, et comme $a \mid b$ il existe $k' \in A$ tel que $b = a \cdot \ k'$ d'où $x = a \cdot (k' \cdot k)$.

On pose $z = k^{'} \cdot k$ et $z \in A$ alors $x = a \cdot z$ et $\quad z \in A$ d'ou $x \in (a)$

$(\Leftarrow)$

On a $b \in (b)$ alors $b \in (a)$ d'où $\exists k \in A$ tel que $b = a \cdot k$. Donc $a \mid b$. ■

Définition 1.6

Deux éléments a et b d'un anneau A sont dit associés et on ecrit :

$$a \sim b, \text{ ssi } a \mid b \text{ et } b \mid a.$$

Proposition 1.2

Soit A un anneau intègre.

a et b sont associés $\iff (a) = (b) \iff \exists q \in A^*$ *tel que* $a = q \cdot b$.

où A^* designe le groupe des unites de A

Preuve.

1) $a \sim b \iff (a) = (b)$

$a \sim b \iff a \mid b$ et $b \mid a$

$\iff (a) \subset (b)$ et $(b) \subset (a)$

$\iff (a) = (b)$

2) $(a) = (b) \iff \exists q \in A^*$ tel que $a = q \cdot b$

$(\Rightarrow)$

$(a) = (b) \iff a \mid b$ et $b \mid a$ alors il existe $q, u \in A$ tels que $a = q \cdot b$ et $b = u \cdot a$

d'ou $a = q \cdot u \cdot a$ c ést à dire $a \cdot (q \cdot u - 1) = 0$

Si $a = 0, b = a = 0$ et $a = b \cdot 1$

Si $a \neq 0$, comme A est intègre alors $q \cdot u = 1$ d'où q est inversible donc $q \in A^*$

$(\Leftarrow)$

S'il existe un élément inversible q de A tel que $a = q \cdot b$, alors $b \mid a$, donc $(a) \subset (b)$

. La relation $a = q \cdot b$ implique $b = q^{-1} \cdot a$, donc $a \mid b$et par suite $(b) \subset (a)$.

Finalement, on a bien $(a) = (b)$. ■

1.4 Anneaux principaux

Définition 1.7

Soit A un anneau et I un idéal de A. On dit que I est un idéal principal de A si $\exists\ a \in A$ tel que $I = (a) = \{a \cdot x \mid x \in A\}$

Définition 1.8

Un anneau est dit principal si il est intègre et si tout ses idéaux sont principaux.

Exemples 1.6

1) $\mathbb{Z}$ est un anneau principal .

2) Soit $\mathbb{k}$ un corps commitatif, l'anneau $\mathbb{k}[X]$ est principal.

Définition 1.9

Soit A un anneau. Un idéal I est dit premier, s'il est propre ($I \neq A$), et s'il vérifie :

$$\forall x, y \in A,\ x \cdot y \in I \Rightarrow x \in I \text{ ou } y \in I.$$

Exemple 1.7

pour $A = \mathbb{Z}$, soit $I = (5) = 5\mathbb{Z}$. I est idéal premier de $\mathbb{Z}$ car si $x, y \in \mathbb{Z}$, tels que $x \cdot y \in 5\mathbb{Z}$.

On a $5 \mid x \cdot y$, et comme 5 est premier, alors $5 \mid x$ ou $5 \mid y$ c ést à dire $x \in 5\mathbb{Z}$ ou $y \in 5\mathbb{Z}$.

Définition 1.10

Un idéal I est un idéal maximal dans A si :

a) $I \neq A$ et,

b) Si J est un idéal de A tel que : $I \subset J$ alors $J = I$ ou $J = A$

Exemple 1.8

$A = \mathbb{Z}$, $I = 3\mathbb{Z}$, I est idéal maximal car on a $3\mathbb{Z} \neq \mathbb{Z}$, et si $J = n\mathbb{Z}$ un idéal de $\mathbb{Z}$ vérifiant $3\mathbb{Z} \subset n\mathbb{Z}$, alors $n \mid 3$ d'ou $n = 1$ ou $n = 3$

Si $n = 1$ alors $J = \mathbb{Z} = A$.

Si $n = 3$ alors $J = 3\mathbb{Z} = I$.

Théorème 1.2 ***(Krull)***

Dans un anneau commutatif A, tout idéal $I \neq A$ est inclus dans un idéal maximal.

Preuve.

L'ensemble des idéaux de A contenant I et distincts de A est inductif car si $(I_\alpha)_{\alpha\in\Lambda}$ est une famille totalement ordonnée d'idéaux de A distincts de A, la réunion est encore un idéal

(parce que la famille est totalement ordonnée) distinct de A (parce qu'elle ne contient pas 1). On applique alors le lemme de Zorn. ■

Définition 1.11

L'anneau $(A,+,\cdot)$ est dit euclidien s'il est intègre et s'il est muni d'une application $\varphi : A\backslash\{0\} \to \mathbb{N}$ telle que, pour tout couple (a,b) d'éléments non nuls de A ,

- Si b divise a, $\varphi(b) \leq \varphi(a)$;

- Si b ne divise pas a, il existe q et r dans A vérifiant $a = b\cdot q + r$ et $\varphi(r) \leq \varphi(b)$.

On dit que φ un stathme euclidien de A.

On pose $\varphi(0_A) = -\infty$. Ainsi le second point reste correct si b divise a.

Exemple 1.9

L'application de $\mathbb{Z}$ dans $\mathbb{N}$ définie par : $\varphi(n) = |n|$, fait de $\mathbb{Z}$ un anneau euclidien.

Proposition 1.3

Si $(A,+,\cdot)$ est un anneau euclidien, alors A est principal.

Preuve.

Soit I un idéal de A.

Si $I = \{0\}$, alors $I = (0)$.

Supposons que $I \neq \{0\}$, soit $a \in I - \{0\}$ tel que $\varphi(a) = \min\{\varphi(x),\ x \in I - \{0\}\}$ $a \in I$ alors

$$(a) \subset I \ldots\ldots (1)$$

Soit $x \in I$, $\exists\ q, r \in A$ tels que $x = a\cdot q + r$ avec $r = 0$ ou $\varphi(r) \leq \varphi(a)$.

On a $r = x - a\cdot q \in I$ car I est idéal et on a $\varphi(r) \leq \varphi(a)$ est imposible par définition de a .

Donc $r = 0$ d'où $x = a \cdot q$ et donc $x \in (a)$ alors

$$I \subset (a) \ldots\ldots (2)$$

De (1) et (2) on a $I = (a)$, donc A est principal . ■

Chapitre 2

Module sur un anneau

Dans tout ce chapitre et le chapitre suivant, Le terme "A est un anneau" designe un anneau commutatif unitaire.

2.1 Module et sous-module

Définition 2.1

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

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longrightarrow & a \cdot m \end{array}$$

vérifiant les quatres propriétés suivantes :

$\forall a, b \in A$ et $\forall\ m_1, m_2 \in M$

1. $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$
2. $(a + b) \cdot m_1 = a \cdot m_1 + b \cdot m_1$
3. $a \cdot (b \cdot m_1) = (a \cdot b) \cdot m_1$
4. $1 \cdot m_1 = m_1$

Les éléments de M sont appelés les vecteures, et ceux de A sont les scalaies .

Exemples 2.1

- Si A est un corps , un A-module est un A-espace vectoriel .
- Soit A un anneau et soit I un idéal de A, on définit une loi externe :

$$\begin{array}{ccc} A \times I & \longrightarrow & I \\ (a, m) & \longrightarrow & a \cdot m \end{array}$$

donnée par la multiplication dans A. Les quatres axiomes de module 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.

- Si $(G, +)$ est un groupe commutatif d'element neutre 0, G est un $\mathbb{Z}$-module pour la loi externe

$$\begin{array}{ccc} \mathbb{Z} \times G & \longrightarrow & G \\ (n, g) & \longrightarrow & n \cdot g \end{array}$$

avec

$$n \cdot g = \begin{cases} \underbrace{g + \ldots + g}_{n \text{ fois}} & si \quad n > 0 \\ 0_G & si \quad n = 0 \\ \underbrace{(-g) + \ldots + (-g)}_{(-n) \text{ fois}} & si \quad n < 0 \end{cases}$$

- Soit A un anneau et soit s un ensemble non vide quelconque.

A^S est l'ensemble des application de s dans A.

Si $\begin{array}{rccc} f: & s & \longrightarrow & A \\ & i & \longrightarrow & f_i = f(i) \end{array}$ est un element de A^S, généralement f est noté $(f)_{i \in S}$.

C'est à dire $A^S = \{(f)_{i \in S} \mid f_i \in A\}$.

En particulier si $S = \{1, 2, \ldots, n\}$ alors A^S est noté A^n et on a

$A^S = A^n = \{(f_1, f_2, \ldots, f_n) \mid f_i \in A\}$.

$A^{(S)} = \{(f_i)_{i \in S} \mid f_i \in A,\ f_i = 0$ sauf pour un nombre fini de $i\}$

et on a $A^{(S)} \subset A^S$

A^S(respectivement $A^{(S)}$) est un A-module pour les lois :

$$(f_i)_{i \in S} + (g_i)_{i \in S} = (f_i + g_i)_{i \in S}$$

et

$$a \cdot ((f_i)_{i \in S}) = (a \cdot f_i)_{i \in S}$$

pour tous $(f_i)_{i \in S}$, $(g_i)_{i \in S} \in A^S$(respectivement $A^{(S)}$) et $a \in A$. un A-module .

Définition 2.2

Soit M un A-module et $N \subset M$. On dit que N est un sous-module de M si et seulement si,

1. N est un sous-groupe de M
2. Pour tout $a \in A$ et $m \in N$, on a $a \cdot m \in N$.

Ainsi, tout sous-module d'un A-module M est aussi un A-module.

Si $\Bbbk$ est un corps, la notion de sous-modules coincide avec celle de $\Bbbk$-espace vectoriel.

Exemples 2.2

- Si M est un A-module, Les parties $\{0\}$ et M sont des sous-modules de M appelés sous-modules triviaux.
- Les sous-modules d'un groupe G sont exactement les sous-groupes de G.
- 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

$$IM := \left\{ \sum_{i=1}^{n} a_i \cdot m_i \mid n \in \mathbb{N}^*,\ \forall i \in \{1....n\},\ a_i \in I \text{ et } m_i \in M \right\}$$

est un sous-module de M.

Proposition 2.1

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 $\lambda \in A$ et $(m, n) \in N^2$, on a $\lambda \cdot m + n \in N$.

Preuve.

Il est evident que si N est un sous-module de M alors il satisfait à la propriété ci-dessus.

Réciproquement, supposons que pour tout $\lambda \in A$ et $(m, n) \in N^2$, on a $\lambda \cdot m + n \in N$.

En prenant $n = m \in N$ et $\lambda = -1 \in A$, on trouve $0 = \lambda \cdot m + n \in N$

En prenant $n = 0$, on voit que l'axiome 2. de sous-modules est satisfait.

En prenant $\lambda = -1$,on voit que $n - m \in N$. Donc N est un sous-groupe de M.

Ceci permet de conclure que N est un sous-module de M. ■

2.2 Morphisme de modules

Définition 2.3

Soient M et N deux A-modules. Un morphisme de A-modules ou application linéaire est une application $f : M \longrightarrow N$ vérifiant :

1. f est un morphisme de groupes ,
2. pour tout $a \in A$ et $m \in M$, on a $f(a \cdot m) = a \cdot f(m)$.

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

Remarques 2.1

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

2) Remarquons que lorsque $\Bbbk$ est un corps, les morphismes de $\Bbbk$-modules sont exactement les morphismes de $\Bbbk$-espaces vectoriels.

3) 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.

Exemple 2.3

Soient $a \in A$ et $M = N = A$. L'application

$$\begin{array}{rccc} f_a : & A & \longrightarrow & A \\ & x & \longrightarrow & xa \end{array}$$

est une application A-linéaire (morphisme de A-modules)

Proposition 2.2

Soient M et N deux A-modules. On note $Hom_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N. Alors $Hom_A(M, N)$ a une structure de A-module pour les lois :

1)
$$\begin{array}{ccc} Hom_A(M,N) \times Hom_A(M,N) & \longrightarrow & Hom_A(M,N) \\ (f,g) & \longrightarrow & f+g \end{array}$$

2)
$$\begin{array}{ccc} A \times Hom_A(M,N) & \longrightarrow & Hom_A(M,N) \\ (a,f) & \longrightarrow & a \cdot f \end{array}$$

avec

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (af)(x) &= af(x)\end{aligned}$$

Preuve.

1) Supposons que pour tout $(m,m^{'}) \in M^2$et $(f,g) \in Hom_A(M,N)^2$,

on a :

$$\begin{aligned}(f+g\,)(m+\ m^{'}) &= f(m+\ m^{'})+g(m+\ m^{'})\\ &= f(m)+f(m^{'})+g(m)+g(m^{'}) \text{ car } f \text{ et } g \text{ sont des morphismes}\\ &= (f+g)(m)+(f+g)(m^{'})\end{aligned}$$

et pour $\lambda \in A$:

$$(f+g)(\lambda m) = f(\lambda m)+g(\lambda m) = \lambda f(m)+\lambda g(m) = \lambda(f+g)(m)$$

2) Supposons que pour tout $a \in A$ et $(m,m^{'}) \in M^2$et $f \in Hom_A(M,N)$,on a :

$$\begin{aligned}(af)(m+\ m^{'}) &= af(m+\ m^{'})\\ &= a(f(m)+f(m^{'})) \qquad \text{car } f \text{ est un morphisme}\\ &= af(m)+af(m^{'})\\ &= (af)(m)+(af)(m^{'})\end{aligned}$$

et pour $\lambda \in A$:

$$(af)(\lambda m) = af(\lambda m) = a(\lambda f(m)) = (a\lambda)f(m) = \lambda(af(m)) = \lambda(af)(m)$$

Ce qui achève la preuve. ■

Définition 2.4

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

$$\ker(f) = f^{-1}(\{0\}) = \{x \in M \mid f(x) = 0\}$$

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 2.3

Soient M et N deux A-modules et soit $f : M \longrightarrow N$ un morphisme de A-modules.

1. *Si $N^{'}$ est un sous-module de N alors l'image réciproque $f^{-1}(N^{'})$ est un sous-module de M.*

   En particulier $\ker(f)$ *est un sous-module de M. De plus, on a*

   $$\ker(f) = \{0\} \text{ si et seulement si } f \text{ est injective.}$$

2. *Si $M^{'}$ est un sous-module de M alors l'image directe $f(M^{'})$ est un sous-module de N.*

   En particulier, $\mathrm{Im}(f)$ *est un sous-module de N. De plus, on a*

   $$\mathrm{Im}(f) = N \text{ si et seulement si } f \text{ est surjective.}$$

Preuve.

1. Soit $N^{'}$ un sous-module de N. Pour $a \in A$ et $m, n \in f^{-1}(N^{'})$, on a

$f(a \cdot m + n) = a \cdot f(m) + f(n) \in N^{'}$ car $N^{'}$ est un sous-module de N donc $a \cdot m + n$ est un élément de $f^{-1}(N^{'})$. Il suit que $f^{-1}(N^{'})$ est un sous-module de M.

En particulier, pour $N^{'} = \{0\}$, on obtient que $\ker(f)$ est un sous-module de M.

supposons que $\ker(f) = \{0\}$ on a $\forall m, m' \in M$, $f(m) = f(m^{'})$ alors $f(m) - f(m^{'}) = 0$ d'où $f(m - m^{'}) = 0$. Donc $m - m^{'} \in \ker(f)$ et par suite alors $m = m^{'}$.

Réciproquement, on suppose que f est injective , si $m \in \ker f$, alors on a $f(m) = 0 = f(0)$, donc $m = 0$ ce qui assure que $\ker f = \{0\}$.

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 $f(a \cdot m_1 + n_1) = a \cdot m + n$ avec $a \cdot m_1 + n_1 \in M'$ 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. ■

Exemple 2.4

Soit A un anneau et soit $A[X]$ l'anneau des polyônmes, 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

$$f(P) = f(\sum_{i=0}^{n} a_i X^i\ ) = \sum_{i=0}^{n} f(a_i X^i\ ) = \sum_{i=0}^{n} a_i f(X)^i = \sum_{i=0}^{n} a_i x_0^i$$

est bien un morphisme de A-modules. Le morphisme f est appelé morphisme d'évaluation.

2.3 Module quotient

Rappel

Soient $M = (M, +)$ un groupe abélien et $N \subset M$ un sous-groupe. Considérons la relation $\mathcal{R}_N$ définie sur M par

$$x \mathcal{R}_N y \iff x - y \in N$$

La relation $\mathcal{R}_N$ est une relation d'équivalence, on note M/N l'ensemble des classes d'équivalences modulo $\mathcal{R}_N$ et $p : M \longrightarrow M/N$ la surjection canonique $x \hookrightarrow p(x) = \overline{x}$. Alors il existe une unique structure de groupe (abélien) sur M/N telle que la surjection canonique soit un morphisme de groupes (de telle sorte que $\overline{x + y} = \overline{x} + \overline{y}$, le neutre est $\overline{0} = p(0)$).

Définition 2.5

On considère un anneau A, un A-module M et un sous-A-module N de M.

Sur le groupe quotient M/N on met une structure de A-module : pour a dans A et m dans M on pose $a \cdot \overline{m} := \overline{a \cdot m}$ où $\overline{m}$ désigne la classe de m dans le quotient M/N

Proposition 2.4

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 $\forall a \in A, \forall x \in M$, $a \cdot (x + N) = a \cdot x + N$. De plus, cette structure est l'unique structure faisant de la projection

$$p : M \longrightarrow M/N$$

un morphisme de A-modules.

Preuve.

Il faut tout d'abord vérifier que la formule

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

a un sens, c'est a dire que si y est un élément de la classe $x + N$ alors $a \cdot y$ est dans la méme classe que $a \cdot x$. Mais ceci est clair car si $x - y \in N$ alors $a \cdot (x - y)$ $\in N$ 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 p est un morphisme de groupes et que si $a \in A$, $m \in M$, on a $\quad p(a \cdot m) = a \cdot m + N$ et $a \cdot p(m) = a \cdot (m + N)$ on obtient bien $p(a \cdot m) = a \cdot p(m)$ ce qui prouve que p est un morphisme de A-modules . ■

Exemples 2.5

- Un idéal I d'un anneau A est un sous-A module de A et le quotient A/I est aussi un A-module .
- Pronons $A = M = \mathbb{Z}$ et $N = n\mathbb{Z}$, alors le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module.

Théorème 2.1

Soient $f : M \longrightarrow L$ un morphisme de A-modules, N un sous-module de M et soit $p : M \longrightarrow M/N$ la projection canonique. Supposons que N soit contenu dans $\ker(f)$. *Alors f se factorise de maniére unique à travers M/N c'est a dire qu'il existe un unique morphisme de A-modules*

$$\overline{f} : \quad M/N \quad \longrightarrow \quad Im(f)$$

tel que $\quad \overline{f} \circ p = f$

En particulier, si $N = \ker(f)$ *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 $\overline{f} \circ p = f$, 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 $\overline{f} \circ p = f$, il faut vérifier que ceci est bien définie .

Supposons y dans la même classe que x modulo N c'est a 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 $\ker(f)$. 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

$$\overline{f} : \quad M/N \quad \longrightarrow \quad Im(f)$$

Montrons que c'est un morphisme de A-modules. Soit $(x_1, x_2) \in M^2$ et soit $a \in A$, on a :

$$\begin{aligned} \overline{f}(x_1 + x_2 + N) &= f(x_1) + f(x_2) = \overline{f}(x_1 + N) + \overline{f}(x_2 + N) \\ \text{et } \overline{f}(a \cdot (x_1 + N)) &= f(a \cdot x_1) = a \cdot f(x_1) = a \cdot \overline{f}(x_1 + N) \end{aligned}$$

d'où le résultat

Il est clair que l'image de $\overline{f}$ est $\mathrm{Im}(f)$. Supposons maintenant que $N = \ker(f)$ 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 $\overline{f}$ est injectif. On conclut que dans ce cas $\overline{f}$ est un isomorphisme. ■

2.4 Produit direct et somme direct

Définition 2.6

Soient I un ensemble non vide et $(M_i)_{i \in I}$ une famille de A-modules. Alors les lois suivantes :

$$(x_i) + (y_i) = (x_i + y_i) \ , \ a \cdot (x_i) = (a \cdot x_i) \quad \text{pour tout } i \in I$$

munissent $\prod_{i \in I} M_i = \{(x_i)_{i \in I} \ ; x_i \in M_i\}$ d'une structure de A-module ,

Le A-module obtenu, noté encore $\prod_{i \in I} M_i$, est appelé le A-module produit des $(M_i)_{i \in I}$.

Exemple 2.6

Si $M_i = M$ pour tout i, le A-module $\prod_{i \in I} M_i$ est l'ensemble des suites d'éléments

de M indexées par I. Il s'identifie au A-module M^Ides applications $I \longrightarrow M$

Définition 2.7

Soit $(M_i)_{i\in I}$ une famille de A-modules. On note

$$\bigoplus_{i\in I} M_i = \{(x_i) \in \prod_{i\in I} M_i \mid \exists J \subset I \text{ fini tel que } x_i = 0 \text{ pour } i \notin J\}$$

Alors $\bigoplus_{i\in I} M_i$ est un sous-module de $\prod_{i\in I} M_i$, appelé somme directe des $(M_i)_{i\in I}$.

Exemple 2.7

Si $M_i = M$ pour tout i, le A-module $\bigoplus_{i\in I} M_i$ est l'ensemble des suites d'éléments de M indexées par I et à support fini. Il s'identifie au A-module $M^{(I)}$ des applications à support fini $I \longrightarrow M$.

2.5 Modules libres, modules de type fini

Définition 2.8

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

1. 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 $\quad m = \sum_{i\in I} a_i m_i$
2. 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.
3. Une base si la famille est à la fois libre et génératrice.

Exemple 2.8

La famille $\{e_1 = (1, 0, \ldots, 0)\ , \ldots,\ e_n = (0, 0, \ldots, 1)\}$ est une base de $\mathbb{Z}^n$

Remarque 2.2

Une sous-famille d'une famille libre est nécessairement libre et une sur famille d'une famille génératrice est génératrice.

2.5.1 Modules de type fini

Définition 2.9

On dit que M est un A-module de type fini si M a une famille génératrice finie.

Remarque 2.3

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 génératrice finie : l'anneau des polynômes sur un corps $\mathbb{k}[X]$ par exemple en tant que $\mathbb{k}$-espace vectoriel.

Exemples 2.9

- 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 de type fini, une famille génératrice etant donnée par $\{1_A\}$.
- Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas de type fini.

Proposition 2.5

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 fnie.

Preuve.

Come M est de type fini, il exise $\mathcal{N}$=$\{n_i, i = 1, ..., k\}$ une famille génératrice finie de M.

Par hypothèse, pour tout $i \in \{\ 1, ..., k\}$, il existe des scalaires tous nuls sauf pour un nombre fini a_{i,m_i} où $m_i \in \mathcal{M}$ tel que

$$n_i = \sum_{i \in I} a_{i,m_i} \cdot m_i$$

Notons $\mathcal{M}_i \subset \mathcal{M}$ l'ensemble des m_i tel que $a_{i,m_i} \neq 0$. C'est un ensemble fini. Donc l'ensemble $\mathcal{P} = \mathcal{M}_1 \cup ....\cup \mathcal{M}_n \subset \mathcal{M}$ 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 $\mathcal{P}$. Ceci implique que $\mathcal{P}$ est une famille génératrice finie. ■

Proposition 2.6

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

Preuve.

Si $(m_i)_{i=1,....,n}$ est une famille génératrice finie de M alors $(m_i + N)_{i=1,....,n}$ est une famille génératrice finie de M/N. ■

2.5.2 Modules libres

Définition 2.10

Soit M un A-module. On dit que M est un A-module libre si M posséde une base.

Exemples 2.10

- Si $A = \Bbbk$ est un corps alors tout A-module est libre car tout A-module posséde une base.
- Le $\mathbb{Z}$-module $\mathbb{Z}$ est libre.
- Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas libre .
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a,b \in \mathbb{Z}\}$ est $\mathbb{Z}$-module libre .
- $A^{(I)}$ est A-module libre

Proposition 2.7

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-modules :

$$\begin{array}{rccc} \Psi : & A^{(I)} & \longrightarrow & M \\ & (a_i\ )_{i\in I} & \longrightarrow & \sum\limits_{i\in I} a_i \cdot m_i \end{array}$$

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

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

ce qu'il fallait montrer. ■

Proposition 2.8

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

$$\begin{array}{rccc} \Psi : & A^{(I)} & \longrightarrow & M \\ & (a_i)_{i\in I} & \longrightarrow & \sum\limits_{i\in I} a_i \cdot m_i \end{array}$$

celui-ci est surjectif par définition et injectif car M est libre donc c'est un isomorphisme ce qui permet de conclure. ■

Remarque 2.4

Si M est A-module libre de type fini alors il posséde une base finie $(e_{1,}.....,e_n)$ de n éléments pour un $n \in \mathbb{N}^*$.

On voit alors que M est isomorphe à A^n à travers l'isomorphisme

$$\begin{array}{rccc} \Phi : & A^n & \longrightarrow & M \\ & (a_1, ..., a_n) & \longrightarrow & \sum\limits_{i=1}^{n} a_i \cdot e_i \end{array}$$

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.

Proposition 2.9

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

Preuve.

Supposons maintenant que M admette deux bases B_1 et B_2 de cardinal respectifs n_1 et n_2. En utilisant la remarque 2.4, on voit que M est isomorphe

a la fois a A^{n_1} et à A^{n_2}, on a un isomorphisme φ_1 entre ces deux A-modules.

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

d'inverse

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

A ces deux morphismes s'associent naturellement deux matrices $P \in Mat_{n_2 \times\, n_1}(A)$ et $Q \in Mat_{n_1 \times\, n_2}(A)$ qui vérifient donc :

$$Q.P = Id_{n_1} \text{ et } P.Q = Id_{n_2}$$

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

$$\pi(Q).\pi(P) = Id_{n_1} \text{ et } \pi(P).\pi(Q) = Id_{n_2}$$

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

Ceci implique que $n_1 = n_2$ et conclut la démonstration. ■

Remarque 2.5

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

Définition 2.11

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.

Exemple 2.11

Soit A un anneau, Le A-module A^nest libre de type fini de rang n.

Proposition 2.10

Soit M et N deux A-modules de type fini de rang m et n respectivement alors $M \bigoplus N$ est libre de type fini et de rang $m + n$.

Preuve.

Soit $(e_1....,e_m)$ une base de M et soit $(f_1,....,f_n)$ 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 $M\bigoplus N$ ■

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

Définition 2.12

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

Exemple 2.12

$\mathbb{C}$ est une extension de $\mathbb{R}$, de degré fini $[\mathbb{C}:\mathbb{R}]=2$.

Définition 2.13

Un corps de nombres est une extension de degré fini de $\mathbb{Q}$.

Dans tout ce qui suit, on suppose que $\Bbbk$ est un corps de nombres.

Définition 2.14

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

Exemple 2.13

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 $X^{\,2}-2\in\mathbb{Z}[X]$.

Proposition 2.11

Soit $x\in\Bbbk$. Alors x est un entier algébrique si et seulement si il existe $M\subset\Bbbk$ un sous $\mathbb{Z}$-module de $\Bbbk$ 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 $\{1, x, ..., x^{n-1}\}$ et on a $x\mathbb{Z}[x] \subset \mathbb{Z}[x]$.

Réciproquement, on suppose qu'il existe $M \subset \Bbbk$ un sous $\mathbb{Z}$-module de $\Bbbk$ non nul et de type fini tel que $xM \subset M$. Soit $v_1, ..., v_n$ un système générateur de M.

Il existe des éléments $a_{i,j}$ de $\mathbb{Z}$ avec $1 \leq i, j \leq n$ tel que

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

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

$$f \quad \Bbbk^n \quad \longrightarrow \quad \Bbbk^n$$

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

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

Ainsi $(v_{1,}...., v_n)$ est un vecteur propre de valeur propre x pour f ce qui implique

$$\det(x \cdot Id_n - f) = 0$$

Posons alors $P(x) = \det(x \cdot Id_n - f)$.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. ■

Théorème 2.2

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

Preuve.

$\mathcal{O}_{\mathbb{k}} \neq \emptyset$; car $\mathbb{Z} \subset \mathcal{O}_{\mathbb{k}}$. Soit x et y deux entiers algébriques. Alors d'aprés la proposition 2.11, il existe deux sous $\mathbb{Z}$-modules M et N de type fini de $\mathbb{k}$ tel que $xM \subset M$ et $yN \subset N$. Supposons que M est engendré par $x_1, ..., x_n$ et N par $y_1, ..., y_m$ alors le $\mathbb{Z}$-module L engendré par les $x_i \cdot y_j$ pour $1 \leq i \leq n$ et $1 \leq j \leq m$ (c'est a dire, l'ensemble des combinaisons linéaires de ces éléments) est de type fini et non nul. De plus, il vérfie $(x - y)L \subset L$ et $xy \cdot L \subset L$. Ceci implique que $x - y$ et xy sont tout deux entiers algébriques donc $\mathcal{O}_{\mathbb{k}}$ est bien un sous-anneau de $\mathbb{k}$. ■

Chapitre 3

Module sur un anneau principal

3.1 Structure des modules sur un anneau principal

Théorème 3.1

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 $n = 1$, M est isomorphe à A et un sous-module non nul de A est un idéal de A non nul, il est donc principal engendré par $a \in A$ non nul.

Alors $\{a\}$ est une base de N si : $a \cdot \lambda = 0$ pour $\lambda \in A$ alors $\lambda = 0$ car A est intègre.

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

$$Ae_2 \oplus ... \oplus Ae_n$$

Si N est contenu dans M_1, on peut conclure par hypothése de récurrence. On suppose donc que N n'est pas contenu dans M_1. On considére le A-module $N \cap M_1$. C'est un sous-module de M_1.

Par hypothèse de récurrence, il est libre. Soit $(f_2, ..., f_m)$ une base de ce module avec $m \leq n$.

On considére maintenant l'ensemble suivant :

$$I = \{b \in A \mid \exists y \in M_1,\ b \cdot e_1 + y \in N\}$$

Un élément quelconque de N s'écrit $b \cdot e_1 + y$ 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 M_1.

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 $f_1 := d \cdot e_1 + y_1 \in N$.

Notons tout d'abord que cet élément est non nul car M_1 et $A \cdot e_1$ sont en somme directe.

On va montrer que $(f_1, ..., f_m)$ est une base de N. C'est une famille génératrice. En effet, si $x \in N$ on a $x = b \cdot e_1 + y$ avec $b \in A$ et $y \in M_1$. Mais on a $b \in I$ et donc b s'ecrit $a \cdot d$ avec $a \in A$.

On a donc $x = a \cdot f_1 - a \cdot y_1 + y$. Alors $- a \cdot y_1 + y$ est dans $N \cap M_1$ donc s'ecrit comme combinaison d'éléments de $(f_1, ..., f_m)$.

On montre maintenant que la famille est libre. Supposons $a_1 \cdot f_1 + a_2 \cdot f_2 + ... + a_m \cdot f_m = 0$ pour $(a_1, ..., a_m) \in A^m$ non tous nuls. On a $a_1 \neq 0$ car la famille $(f_2, ..., f_m)$ est libre.

On a donc $a_1 \cdot f_1$ dans M_1 et donc $a_1 \cdot d \cdot e_1 + a_1 y_1 \in M_1$ ce qui implique $a_1 \cdot d \cdot e_1 \in M_1$. Ceci implique $a_1 \cdot d = 0$ et donc $a_1 = 0$ car $d \neq 0$ et A est intégre. ■

Exemple 3.1

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

Remarque 3.1

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

Remarque 3.2

Si A est principal A est un A-module libre de type fini et de rang 1, les sous-modules (non nuls) 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.

Remarque 3.3

L'hypothése A principal est essentiel dans ce théorème. En effet, un sous-module d'un module libre n'est pas forcément libre.

On prend par exemple $A = M = \mathbb{Z}/4\mathbb{Z}$ et $N = 2\mathbb{Z}/4\mathbb{Z}$.

Lemme 3.1

Il existe un morphisme de A-modules

$$f : \quad M \quad \longrightarrow \quad A$$

vérifiant les propriétés suivantes :

1. *Pour tout morphisme $g : M \longrightarrow A$, 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 $g : M \longrightarrow A$, on a $g(y) \in (d)$.*
4. *Il existe $x \in M$ tel que $f(x) = 1$ et $y := d \cdot x \in N$.*
5. *On a $M = Ax \oplus \ker(f)$ et $N = A \cdot y \oplus (\ker(f) \cap N) \cdots\cdots (**)$.*

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'ideaux 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

hypothéses 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" $g_j : M \longrightarrow A$ 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 $f(y) = df(x) = d$ donc $f(x) = 1$.

Abordons le point 5, on a déjà $Ax \cap \ker(f) = \{0\}$car pour tout $a \in A$, $f(a.x) = a = 0$. Maintenant, si $z \in M$, on a $z = f(z).x + (z - f(z)x) \in Ax + \ker(f)$ d'où $M = Ax \oplus \ker(f)$.

Ensuite, si $a \in A$ est tel que $ay \in \ker(f) \cap N$ 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 $z = ay + (z - ay) \in A.y + (\ker(f) \cap N)$. ■

Théorème 3.2 *(théorème de la base adaptée)*

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 $(e_1, ..., e_n)$ de M, il existe des éléments $a_1, a_2, .., a_r$ de $A \backslash \{0\}$ tels que a_i divise a_{i+1} pour $i = 1, ..., r - 1$. et $(a_1 \cdot e_1, a_2 \cdot e_2, ..., a_r \cdot e_r)$ est une base de N. On dit que la base $(e_1, ..., e_n)$ de M est adaptée au sous-module N.

Preuve.

On raisonne par récurrence sur le rang n de M.

- Si $n = 1$, M est isomorphe a A. On peut donc supposer $M = A$. Les sous-modules de M sont des idéaux tel qu'il existe $d \in A$ tel que $M = (d)$.

Une base est $\{d\}$, cet ensemble etant 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 il existe un morphisme de A-modules

$$f : \quad M \quad \rightarrow \quad A$$

vérifiant les 5 points du lemme. Posons $M' := \ker(f)$. C'est un sous module de M et il est donc libre et de type fini d'apres le théorème 3.1 Le point 5 du lemme nous

dit que

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

Ax est libre de rang 1 car x est générateur et libre. Il en est de même pour Ay. 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 $(e_2, ..., e_n)$ une base quelconque de M'.

Si $M' \cap N \neq 0$ on peut appliquer l'hypothése de récurrence a M' et a son sous-module $M' \cap N$. Il existe une base $(e_2, ..., e_n)$ de M' et des éléments $a_2, \ldots, a_r$ de A tels que $r \leq n$, $a_2 \mid a_3 \ldots \mid a_r$ et

$$M' = Ae_2 \oplus \ldots \oplus Ae_n \qquad\qquad M' \cap N = Aa_2e_2 \oplus \ldots \oplus Aa_re_r$$

On a alors :

$$M = Ae_1 \oplus \ldots \oplus Ae_n \qquad\qquad N = Aa_1e_1 \oplus \ldots \oplus Aa_re_r$$

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

Proposition 3.1

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 $(e_1, ..., e_n)$ et $(e'_1, ..., e'_n)$ soient deux bases adaptés à N. Soit $a_1, ..., a_r$ et $a'_1, ..., a'_r$ les éléments non nuls de A tels que a_i divise a_{i+1} et a'_i divise a'_{i+1} pour $i = 1, ..., r-1$, et tel que $(a_1e_1, ..., a_re_r)$ et $(a'_1e'_1, ..., a'_re'_r)$ soient deux bases de N. Alors on a $(a_i) = (a'_i)$ pour tout $i = 1, ..., r$.

Preuve.

On considère le morphisme $g_1 : M \to A$ tel que $g_1(\sum_{1 \leq i \leq n} b_ie_i) = b_1$. On voit facilement que l'on a $g_1(N) = a_1A$ d'une part. D'autre part si $m \in N$ alors $m = \sum_{1 \leq i \leq r} a'_ie'_ik_i$ et $g_1(m) = \sum_{1 \leq i \leq r} k_ia'_ig_1(e_i)' \subset a'_1A$. 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 $k = 1, ..., i-1$. On va montrer que $(a_1 \cdots a_i) = (a'_1 \cdots a'_i)$ ce qui implique bien $(a_i) = (a'_i)$. On considère l'application multilinéaire alternée

$$\begin{array}{rccc} \mathcal{D}: & M^i & \to & A \\ & & & \left| \begin{array}{ccc} u_{1,1} & \cdots & u_{1,i} \\ . & & . \\ . & & . \\ . & \cdots & . \\ u_{i,1} & & u_{i,i} \end{array} \right| \\ & (u_1, ..., u_i) & \longrightarrow & \end{array}$$

où pour tout $j = 1, ..., i$, on a pose $u_j = u_{1,j}e_1 + ... + u_{n,j}e_n$. On a $\mathcal{D}(a_1e_1, ..., a_ie_i) = a_1...a_i$ d'une part. D'autre part, si on écrit pour tout $j = 1, ..., n$, $a_ie_j = \sum_{1 \leq k_j \leq n} \mu_{k_j,j} a'_{k_j} e'_{k_j}$ on obtient :

$$\mathcal{D}(a_1e_1, ..., a_ie_i) = \sum_{1 \leq k_1, ..., k_i \leq n} \mu_{k_1,1} ... \mu_{ki,i} a'_{k_i} ... \mathcal{D}(e'_{k_1}, ..., e'_{k_i})$$

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

Remarque 3.4

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

Exemple 3.2

Soit $A = \mathbb{Z}$ et soit $M = \mathbb{Z}^2$. On considére 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 sur la base adaptée n'est pas unique.Par exemple $(e_1 + e_2, e_1 + 2e_2)$ est

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

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

3.2 Facteurs invariants

Lemme 3.2

Soit $M_1, ..., M_n$ des A-modules et pour tout $i \in \{1, ..., n\}$, 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 :

$$\begin{array}{ccc} \oplus_{1\leq i\leq n} M_i & \longrightarrow & \oplus_{1\leq i\leq n} M_i/N_i \\ (m)_{i=1,...,n} & \longrightarrow & (m_i + N_i)_{i=1,...,n} \end{array}$$

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

Théorème 3.3 *(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

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

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

Preuve.

Existence : Comme M est de type fini, d'aprés la proposition 2.7, on a un isomorphisme

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

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 $A \backslash \{0\}$ 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 N. On a donc

$$A^n = Ae_1 \oplus \ldots \oplus Ae_n \quad et\ N\ = Aa_1e_1 \oplus \ldots \oplus Aa_re_r$$

On obtient en utilisant le lemme précédent :

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

c'est ce qu'il fallait montrer. ■

3.3 Approche matricielle

Nous allons maintenant donner une version matricielle equivalente au théorème 3.3. Nous illustrons ce nouveau résultat par quelques exemples. Tout d'abord, on a la définition suivante :

Définition 3.1

Soit $X \in Mat_{n\times m}(A)$.

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

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 $J_3(X) = 3\mathbb{Z}$.

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

Théorème 3.4

Soit A un anneau principal et soit $X \in Mat_{n\times m}(A)$ non nulle. Alors il existe $r \geq 1$, des matrices inversibles $P \in GL_n(A)$ et $Q \in GL_m(A)$ 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 $X \in Mat_{n\times m}(A)$ non nulle. Cette matrice représente un morphisme $f : A^m \longrightarrow A^n$. 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 $A\backslash\{0\}$ 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

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

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' él éments de* A *et si* $x \in \ker(f)$

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

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

ce qui montre que

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

On a bien montré la décomposition annoncée. Notons qu'on peut en déduire qu'une base de $\ker(f)$ *a nécessairement* $m - r$ *éléments.*

Choisissons donc une base $(u_{r+1}, \ldots, u_m)$ *de* $\ker(f)$*. On a alors une base de* A^m *:*

$$(u_1, \ldots, u_m)$$

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

Remarque 3.5

Si f est un morphisme entre deux A-modules libres, on dira que les facteurs invariants de f sont ceux de la matrice de f dans des bases arbitraires.

Proposition 3.2

En gardant les notations du théorème 3.4, on a

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

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 3.4 sont précisement donnés par ceux de l'énoncé. Soit $Q \in GL_m(A)$ 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 $P \in GL_n(A)$ et supposons que $Y = PX$ alors $Y^t = X^t P^t$ et comme ci-dessus on montre que $J_i(X) = J_i(Y)$.

Finalement dans le cadre général où il existe $P \in GL_n(A)$ et $Q \in GL_m(A)$ tel que $Y = PXQ$, on obtient :

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

pour tout $i = 1, \ldots, r$. ■

Exemple 3.4

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* 12. *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.*

3.4 Une application

Une application directe du théorème se trouve en théorie des groupes dans le probléme de classification de groupes abéliens de type fini on peut utiliser le théorème de la base adaptée.

Théorème 3.5

Soit G *un groupe abélien de type fini. Alors il existe un entier* s *et des entiers naturels* $a_1, ..., a_r$ *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.

Exemple 3.5

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 :

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

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

Conclusion

Nous avons présenté dans ce travail la notion de module sur anneau principal et les principaux résultats comme le théorème de la base adaptée, la différence et la relation entre les modules et les espaces vectoriels, aussi une approche matricielle avec une application directe.

Bibliographie

[1] **Arnault.F and all**, *Mathématiques L3 Algèbre*, Cours complet avec 400 tests et exercices corrigés, Pearson Education France, 2009

[2] **Bichion.J,** *Algèbre Approfondie,* Département de Mathématiques Université Blaise Pascal, 2013-2014.

[3] **Harari.D**, *Cours d'algèbre* 1, fait à l'E.N.S. (première année du M.M.F.A.I.) en 2003-2004 et 2004-2005.

[4] **Jacon.N,** *Cours de theorie des modules,* Université de Franche Comt, 27 novembre 2012

[5] **Qurré.J**, *Cours D'algébre*, Université Bretagne Occidentale, 1976.

[6] **Ladjlat.L**, *Cours Master1, Algèbre Arithmétique*, Université M.Boudiaf de Msila. Année univ 2014-2015.

[7] **Lissy.P,** *Anneaux Principaux. Applications,* Université Paris Dauphine, 6 May 2010.

[8] **Mado.J.C**, *Cours d'Algèbre,* 2002-2003.

[9] **Vieillard-Baron.E. and all**, *Anneau et corps,* Janvier 2001.