الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :...............

Centre Universitaire
Abd elhafid boussouf Mila

Institut des sciences et de la technologie
Département de Mathématiques et Informatique

Mémoire préparé En vue de l'obtention du diplôme de Licence

En: Filière mathématiques

Les modules sur les anneaux principaux

Préparé par: ***Amimour Amel***
Bend jeddou Hemza
Bensghir Nadjet

Encadrer par: ***Halim Yacine***
Grade: ***M.A.A***

Année universitaire :2014/2015

كلمة شكر

لا بد لنا ونحن نخطوا خطواتنا الأخيرة في الحياة الجامعية من وقفة نعود الى أعوام قضيناها في رحاب الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في بناء جيل الغد لتبعث الأمة من جديد وقبل أن نمضي نقدم أسمى آيات الشكر و الإمتنان و التقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة إلى الذين مهدوا لنا طريق العلم والمعرفة

إلى جميع أساتذتنا الأفاضل "كن عالما...فإن لم تستطع فكن متعلما, فإن لم تستطع فأحب العلماء فإن لم تستطع فلا تبغضهم"

وأخص بالتقدير والشكر

الأستـــــاذ "حـــــــــــــــــليم ياســــــــــين"

الذي نقول له بشراك قول رســـــول الله صـــلى الله عليه وسلم "إن الحوت في البحر, والطير في السـماء, ليصـلون على معـلم النــاس"

كما أنني أتوجه له بخالص الشكر وأقول له شكـــرا يامن علمتني التفاؤل والمضي إلى الأمام

وكذلك نشكر كل من ساعد على إتمام هذه المذكرة وقدم لنا العون ومد لنا يد المساعدة وزودنا بالمعلومات اللازمة لإتمام هذه المذكرة ونخص بالذكر

الأستـــــاذ "كعــــــــواش إسماعيـــل"

TABLE DES MATIÈRES

INTRODUCTION

En mathématiques, et plus précisément en algèbre générale, au sein des structures algébriques, « un module est à un anneau ce qu'un espace vectoriel est à un corps », pour un espace vectoriel, l'ensemble des scalaires forme un corps tandis que pour un module, cet ensemble est seulement muni d'une structure d'anneau (unitaire, mais non nécessairement commutatif). Une partie des travaux en théorie des modules consiste à retrouver les résultats spectaculaires de la théorie des espaces vectoriels, quitte pour cela à travailler avec des anneaux plus maniables, comme les anneaux principaux.

Ce mémoire est réparti sur l'introduction générale et trois chapitres.

Dans le premier chapitre, nous avons donnés des définitions et résultats généraux sur les groupes et les Anneaux.

Dans le deuxième chapitre, On s'intéressera aux modules, qui sont légèrement plus généraux que les espaces vectoriels, avec comme objectif leétude des espaces vectoriels.

Dans le dernier chapitre, on s'est intéressé au A-modules dans le cas au A est un anneau principale.

CHAPITRE 1

GROUPES ET ANNEAUX

1.1 Groupes

1.1.1 Structure de groupe

Définition 1.1.1 *Un groupe commutatif (additif) est un ensemble G muni d'une loi de composition interne + vérifiant les xiomes :*

1. *(Existence d'un neutre additif) il existe $0_G \in G$ tel que pour tout $g \in G$ on ait :*

$$0_G + g = g + 0_G = g.$$

2. *(Existence d'un symétrique additif) pour tout $g \in G$ il existe$(-g) \in G$ tel que :*

$$g + (-g) = (-g) + g = 0_G.$$

3. *(Associativité additive) pour tout $a, b, c \in G$ on a*

$$(a+b)+c = a+(b+c)\,.$$

4. *(Commutativité additive) pour tout $a, b, \in G$ on a*

$$a+b = b+a.$$

1.1.2 Morphisme des groupes

Définition 1.1.2 *Soit A et B deux groupes (additives). On appelle morphisme des groupes de A dans B une application $f : A \rightarrow B$ compatible avec les structures des groupes c'est-à-dire pour tout $x, y \in A$ on ait :*

$$f(x+y) = f(x) + f(y)\,.$$

Définition 1.1.3 *Soit $f : A \rightarrow B$ un morphisme des groupes (additifs) :*

1. *On appelle **image** de f et on note $\mathrm{Im}\, f$ le sous-groupe :*

$$Imf = \Big\{b \in B; \exists\, a \in A, tel\ que\ b = f(a)\Big\}.$$

2. *On appelle **noyau** de f et on note $\mathrm{Ker}\, f$ le sous groupe :*

$$Kerf = \Big\{a \in A; tel\ que\ f(a) = 0_B\Big\}.$$

1.1.3 Sous-groupe

Définition 1.1.4 *Soit G un groupe(additif). On appelle **sous-groupe** de G tout sous-ensemble H de G vérifiant les axiomes*

1. *$H \neq \phi$.*
2. *Pour tout $a, b \in H$, on a $a + (-b) \in H$.*

Proposition 1.1.1 *Soit $f : A \to B$ un morphisme des groupes (additifs)*

1. *L'ensemble $\{b \in B; \exists\, a \in A.$ tel que $b = f(a)\}$ est un sous-groupe de B.*
2. *L'ensemble $\{a \in A; f(a) = 0_B\}$ est un sous-groupe de A.*

1.2 Anneaux

1.2.1 Structure d'anneaux

Définition 1.2.1 *Un anneau A est un groupe additif muni d'une seconde loi de composition interne(multiplication) $\times$ vérifiant les axiomes*

1. *(Existence d'un neutre multiplicatif). Il existe $1_A \in A$ tel que pour tout $a \in A$;on ait*

$$1_A \times a = a \times 1_A = a.$$

2. *(Associativité multiplicative), pour tout $a, b, c \in A$, on a*

$$a \times (b \times c) = (a \times b) \times c.$$

3. *(Distributivité), pour tout $a, b, c \in A$, on a :*

$$(a + b) \times c = (a \times c) + (b \times c)\,,$$

$$a \times (b + c) = (a \times b) + (a \times c)\,.$$

1.2.2 Anneaux commutatifs

Définition 1.2.2 *Lorsque A est un anneau et que la multiplication est commutative, on dit que A est un anneau commutatif.*

Remarque 1.2.1 *Si A est anneau, l'ensemble A muni de la multiplication n'est pas un group* *puisqu'on ne suppose pas l'existence d'un inverse multiplicatif (une telle structure est parfois appelée monoïde).*

1.2.3 corps

Définition 1.2.3 *Lorsque tous les éléments non nuls de A sont inversible on dit que A est un corps.*

Exemple 1.2.1

1. *Les corps des nombres rationnels réels ou complexes(notés respectivement $\mathbb{Q}$ et $\mathbb{C}$).*
2. *L'anneau des entiers rationnels noté $\mathbb{Z}$.*
3. *Lorsque A est un anneau commutatif, l'anneau des polynomes à une indéterminée à coefficients dans A, noté $A[X]$ est un anneau.*
4. *Lorsque $(A_s)_{s\in S}$ est une famille d'anneaux le produit cartésien $\prod A_s$ muni des loi de composition internes composantes par composantes précisées ci-dessous est un anneau*

$$(a_s)_{s\in S} + (b_s)_{s\in S} = (a_s + b_s)_{s\in S},$$

$$(a_s)_{s\in S} \times (B_s)_{s\in S} = (a_s \times b_s)_{s\in S}.$$

1.2.4 Morphisme des anneaux

Définition 1.2.4 *Soient A et B deux anneaux. On appelle morphisme d'anneaux une application $f : A \to B$ qui vérifie les axiomes suivants*

1. *f est un morphisme de groupe : pour tout $x, y \in A$; $f(x+y) = f(x) + f(y)$.*
2. *f est compatible avec la multiplication : pour tout $x, y \in A$; $f(x \times y) = f(x) \times f(y)$.*
3. *f est un morphisme unitaire : $f(1_A) = 1_{B.}$*

Remarque 1.2.2 *Soit de la définition de groupe que $f(0_A) = f(0_A)$. Mais cela utilise l'existence des inverses additifs et le point 3 n'est pas rendant. Soit A un anneau commutatif unitaire muni de l'addition et la multiplication composant l'anneau produit $A \times A$ est bien un anneau. Le morphisme des groupes additif $a \to (a, 0)$ de A dans $A \times A$ vérifie les deux premières propriétés mais pas la dernière.*

La structure d'anneaux est le cadre naturel pour généraliser les questions de divisibilité (autrement dit d'arithmétique) que chacun a rencontré dans $\mathbb{Z}$. Au contraire dans un corps tous les éléments (non nuls) sont inversibles et se divisent les uns les autre : il n'ya plus de question d'ordre arithméque. L'algèbre linéaire que vous connaissez suppose que les coefficients appartiennent à un corps (en pratique les auteurs supposent même très souvent le corps des coefficients égal à $\mathbb{R}$ ou $\mathbb{C}$: une partie en généralité regrettable). L'algèbre lineaire classique s'applique a de nombreux domaines des mathématique, notamment la géométrie ou la théorie des des groupes à travers leurs représentations(linéaire). Mais pour la raison évoquée plus haut cette algèbre linéaire ne suffit pas aux applications par un anneau on obtient une structure de module.

1.2.5 Sous-anneaux

Définition 1.2.5 *Soit A un anneau et B un sous-groupe(additif) de A. On dit que B est un sous-anneau de A lorsqu'il satisfait en autre aux axiomes*

1. $1_A \in B$.
2. *Pour tout $x, y \in B$, on a $x \times y \in B$.*

1.3 Idéaux

Définition 1.3.1 *Soit A un anneau et I un sous-groupe additif de A. On dit que I est idéal bilatère de A lorsque I est multiplicativement absorbant à gauche et à droite c'est-à-dire lorsque :*

1. *Pour tout $a \in A$ et tout $i \in I$, on a $a \times i \in I$.*
2. *Pour tout $a \in A$ et tout $i \in I$, on a $i \times a \in I$.*

Remarque 1.3.1

1. *Lorsque seul le point* 1 *est vérifié, on dit que I est un idéal à gauche.*
2. *Lorsque seul le point* 2 *est vérifié,on dit que I est un idéal à droite.*
3. *Lorsque A est commutatif les trois notions sont équivalentes(et on parle d'idéal sans préciser bilatére).*

Exemple 1.3.1 *Soit A un anneau commutatif et $a \in A$. L'ensemble $I = \{x \times a; x \in A\}$ est un idéal (forcèment bilatére) de A. On dit que I est l'idéal principal engendré par a. (En fait I est le plus petit idéal contenant a c'est donc bien l'idéal ayant pour partie génératrice le singleton $\{a\}$).*

Définition 1.3.2 *Soit A un anneau commutatif et $I \in A$ un idéal de A :*

1. *On dit que I est principal lorsqu'il existe $a \in A$ tel que*

   $I = \{x \times a; x \in A\}$.
2. *On dit que A est principal lorsque tous les idéaux de A sont principaux.*

1.3.1 Opération sur les idéaux

Proposition 1.3.1 *Soient A un anneau et I et J deux idéaux(à gauche si A n'est pas commutatif) de A :*

1. *$I \cap J$ est un idéaux(à gauche) de A.*
2. *L'ensemble noté IJ formé des sommes finies de produit ij ou $i \in I, j \in J$ est un idéal(à gauche) de A. On l'appelle l'idéal produit de I par J.*

CHAPITRE 2

MODULES

Le but de ce chapitre est de défnir leobjet de base de lealgèbre linéaire. On s'intéressera aux modules, qui sont légèrement plus généraux que les espaces vectoriels, avec comme objectif leétude des espaces vectoriels, du Z-module associé à un groupe abélien et du $k[X]$-module associé à un endomorphisme d'un espace vectoriel.

2.1 Structure de A-module

Définition 2.1.1 *Un A-module* $(M, +, .)$ *est un groupe abélien* $(M, +)$ *muni d'une loi externe* $(a, m) \in A \times M \to a.m \in M$ *qui vérifie*

1. $(ab).m = a.(b.m)$,
2. $(a + b).m = a.m + b.m$,
3. $1.m = m$,
4. $a.(m + n) = a.m + a.n$,

pour tout $(a, b) \in A^2$ *et tout* $(m, n) \in M^2$.

2.2 Morphisme de A-modules

Définition 2.2.1 *Soient M et N deux A-modules. On appelle application A-linéaire ou morphisme de A-modules un morphisme de groupes* $f : M \to N$ *compatible avec l'opération de A, autrement dit tel que, pour tout* $m \in M$ *et tout* $a \in A$, *on ait* $f(am) = af(m)$. *On note* $Hom_A(M, N)$ *l'ensemble des applications A-linéaires de M dans N.*

2.3 Sous-modules

Définition 2.3.1 *Soit M un A-module,* $N \subset M$ *est un sous-module de M si et seulement si c'est un sous-groupe de M stable par la loi externe. N est alors un A-module pour les lois induites.*

Proposition 2.3.1

1. $0_A m = 0_M$.
2. $(-1_A).m = -m$.
3. $a.0_M = 0_M$.
4. *N est un sous-module de M si et seulement si* $N \neq \phi$ *et pour tout* $x, y \in N$ *et tout* $\alpha, \beta \in A$ *alors* $\alpha x + \beta y \in N$.
5. *Une application* $f : M \to P$ *est A-linéaire si et seulement si pour tout* $\alpha, \beta \in A$ *et tout* $x, y \in M$ *on a*
$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y).$$

Preuve.

1. On a $0_A m + m = (0_A + 1_A)m = (1_A)m = m$. Et comme dans le groupe additif M on peut simplifier par m, on obtient $0_A m = 0_M$.

2. Il s'agit de montrer l'égalité $(-1_A)m + m = 0_M$. Cela suit du 1., car

$$(-1_A)m + m = (-1_A)m + (1_A)m = (-1_A + 1_A)m = 0_A m = 0_M.$$

3. On a $am = a(0_M + m) = a0_M + am$. Pour conclure on simplifie par am dans le groupe additif M.

4. On suppose que N est un sous-module de M. Alors N est un sous-groupe donc non vide. Soient donc $\alpha, \beta \in A$ et $x, y \in N$. Puisque N est un sous-module $\alpha x \in N$ et $\beta y \in N$. Puisque N est un sous-groupe $\alpha x + \beta y \in N$. Cela montre le sens direct de l'équivalence. Réciproquement on suppose N non vide et contenant $\alpha x + \beta y$ pour tout $\alpha, \beta \in A$ et tout $x, y \in N$. En particulier pour $\beta = 0$, on voit que N contient αx pour tout $\alpha \in A$ et tout $x \in N$. Il suffit de montrer que N est un sous-groupe de M. Mais N est supposé non vide, et pour tout $x, y \in N$ on a $x - y = 1_A x + (-1_A)y \in N$: cela montre que N est un sous-module de M.

5. Soient $x, y \in M$ et soit $\alpha, \beta \in A$. Si f est A-linéaire c'est un morphisme de groupes. Donc $f(\alpha x + \beta y) = f(\alpha x) + f(\beta y)$. Puis comme f est A-linéaire on a $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$. Cela donne le sens direct de l'équivalence annoncée.

   Réciproquement on suppose que pour tout $\alpha, \beta \in A$ et tout $x, y \in M$ on ait $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$. Alors si on prend $\alpha = \beta = 1_A$ dans la formule qui précède on montre que f est un morphisme de groupes. Si on prend $\beta = 0_A$ on montre que f vérifie la seconde propriété des morphismes de A-modules.

■

2.4 Sommes de sous-modules

Définition 2.4.1 *Soit $(N_i)_{i\in I}$ une famille de sous-modules de M. On note $\sum_{i\in I} N_i$ le sous-module de M engendré par l'ensemble $\bigcup_{i\in I} N_i$. On l'appelle la somme des sous-modules (N_i) et on a*

$$\sum_{i\in I} N_i = \left\{ \sum_{i\in I} m, (m_i) \in \prod_{i\in I} N_i, presque\ nulle \right\}.$$

Définition 2.4.2 *Soit $(N_i)_{i\in I}$ une fammille de sous-modules de M. On dit que la somme $\sum_{i\in I} N_i$ est directe si et seulement si tout élément $m \in \sum_{i\in I} N_i$ admet une unique décompotion $m = \sum_{i\in I} m_i$ avec $(m_i) \in \prod N_i$ presque nulle. On note alors $\sum_{i\in I} N_i = \oplus_{i\in I} N_i$.*

Proposition 2.4.1 *:Soit M un A-module,sont $(N_s)_{s\in S}$ une famille quelconque de sous-modules de M et P_1 et P_2 deux sous-module de M.*

1. *L'intersection $N = \bigcap_{s\in S} N_s$ est un sous-module de M.*
2. *On note $\sum_{s\in S} N_s$ l'ensemble des sommes finies d'éléments de N_s. C'est un sous-modules de M. En particulier lorsque $S = \{1, 2\}$ l'ensemble $N_1 + N_2$ des sommes d'éléments de N_1 et de N_2 est un sous-module de M.*
3. *Si $P_1 \cup P_2$ est un sous-module de M alors $P_1 \subset P_2$ et $P_2 \subset P_1$.*

Exemple 2.4.1

1. *Si A est un corps, la structure de A-module est identique à celle de A-espace vectoriel.*
2. *A est un A-module : la multiplication interne lieu d'opération externe.*
3. *Les sous A-module de A sont les idéaux de A.*
4. *Si M est un A-module il contient les sous modules triviaux$\{0_M\}$ et M. On dit que M est simple s'il n'en contient pas d'autre (et si $M \neq \{0_M\}$) .*

2.5 Applications linéaires

Définition 2.5.1 *Soient M et N deux A-modules. Une application $f : M \to N$ est dite linéaire si et seulement si c'est un morphisme pour les lois internes et externes(ie : $f(a.m) = af(m)$ et $f(m + m') = f(m) + f(m')$). On dit alors que f est un morphisme de A-modules. Dans le cas $M = N$, on parle d'endomorphisme.*

Définition 2.5.2 *Soient M et N deux A-modules.*

1. *On appelle endomorphisme de M une application A-linéaire de M dans M. On note donc $End_A(M) = Hom_A(M, N)$ l'ensemble des endomorphismes de M.*
2. *On appelle isomorphisme de M dans N un morphisme linéaire bijectif.*
3. *On appelle automorphisme de M un isomorphisme de M dans M. On note $Aut_A(M)$ l'ensemble des automorphismes de M.*

   La terminologie ≪ isomorphisme ≫ pour morphisme bijectif est justifiée car la bijection réciproque d'un morphisme linéaire.

Proposition 2.5.1 *Soient M et N deux A-modules et soit $f : M \to N$ un isomorphisme. Alors la bijectoin réciproque de f est A-linéaire.*

Exemple 2.5.1
1. *Un groupe additif M est canoniquement un $\mathbb{Z}$-module.*
2. *Se donne une structure de A-module sur un groupe additif M équivaut à se donner un morphisme d'anneau $A \to End_{\mathbb{Z}}(A)$.*
3. *Soit $\Bbbk$ un corps(commutatif), V un $\Bbbk$-espace vectoriel. Se donner une structure de $\Bbbk[X]$-module sur V qui étante la structure de $\Bbbk$-espace vectoriel de V équivaut à se donner un morphisme.*
4. *$\Bbbk$-algèbre $\varphi : \Bbbk[X] \to End_{\Bbbk}(V)$. Pour toute $\Bbbk$-algèbre Bet tout $b \in B$,ilexiste un unique morphisme de $\Bbbk$-algèbre $\varphi : \Bbbk[X] \to B$ tel que $\varphi(X) = b$. En résumé les structures de $\Bbbk[X]$-modules sur V compatibles avec la structure de $\Bbbk$-espace vectoriel initiale sont en bijection avec $End_{\Bbbk}(V)$.*

2.6 Noyaux, images

Proposition 2.6.1 *Soit $f : M \to N$ un morphisme de A-modules(en particulier un morphisme de groupes additifs).*

1. *Le noyau de f, $Ker\ f = \{m \in M. f(m) = 0\}$ est un sous-module de M.*
2. *L'image de f, $Im\ f = \{n \in N; \exists m \in M$ tel que $n = f(m)\}$ est un sous-module de N.*

2.7 Produits directs

Définition 2.7.1 *On appelle module produit des $(M_s)_{s\in S}$ et on note $\prod_{s\in S} M_s$ le A-modules de cette proposition.*

Proposition 2.7.1 *Soit S un ensemble et $(M_s)_{s\in S}$ une famille de A-modules indexée par S. L'ensemble des $(m_s)_{s\in S} \in \prod_{s\in S} M_s$ tel que $m_s = 0$ pour tout $s \in S$ sauf un nombre fini, est un sous module de $\prod_{s\in S} M_s$.*

2.8 Sommes directs

Définition 2.8.1 *On appelle somme direct des $(M_s)_{s\in S}$ et on note $\oplus_{s\in S} M_s$ le sous-module de $\prod_{s\in S} M_s$ de cette proposition.*

Proposition 2.8.1 *Pour tout $t \in S$, on définit des applications $i_t : M_t \to \oplus_{s\in S} M_s$ et $p_t : \prod_{s\in S} M_s \to M_t$ comme suit.*

pour $m \in M_t$ on pose $i(m) = (i_s(m)) = \begin{Bmatrix} 0 \text{ si } s \neq t \\ m \text{ si } s = t \end{Bmatrix}$

pour $(m_s)_{s\in S} \in \prod_{s\in S} M_s$ on pose $p_t((m_s)_{s\in S}) = m_t$.

On a :

1. *Les applications p_t et i_t sont A-linéaires.*
2. *Soit $\iota : \oplus_{s\in S} M_s \to \prod_{s\in S} M_s$ l'injection canonique. Alors le morphisme composé $p_t \circ \iota \circ i_t$ est égal à l'indentité de M_t.*

Remarque 2.8.1

1. *Lorsque les modules M_s sont tous égaux à M l'application $f \to (f(s))_{s\in S}$ est un isomorphisme de M_s sur $\prod_{s\in S} M$. L'usage est d'identifier ces deux modules. Par cette identification la somme directe $\oplus_{s\in S} M$ s'indentifie au sous-module $M^{(S)}$ formé des application $f : S \to M$ à support fini (c'est-à-dire telle que $f(s) = 0_M$ pour tout s sauf éventuellement pour un nombre fini de s).*
2. *Prenons $S = N$. Le module $A^{(N)}$ est naturellement isomorphe(en tant que module) au module $A[X]$ des polynômes à une indéterminée et à coefficients dans A. Le module $A^{\mathbb{N}}$ est naturellement isomorphe (en tant que module) au module $A[[X]]$ des séries formelles à une indéterminée à coefficients dans A. Pour $A = F_2$ le corps à deux éléments le module $F_2^{(\mathbb{N})}$ est dénombrable tandis que $F_2^{\mathbb{N}}$ est en bijection avec l'ensemble des parties de $\mathbb{N}$,c'est-à-dire en bijection avec $\mathbb{R}$. Il n'existe donc aucune bijection entre $F_2^{(\mathbb{N})}$ et $F_2^{\mathbb{N}}$.*

Définition 2.8.2 *Soient M un A-module, M_1 et M_2 des sous-modules de M.*

1. *On dit que M est somme directe de M_1 et M_2 lorsque $M = M_1 + M_2$ et $M_1 \cap M_2 = \{0\}$.*
2. *Lorsque M est somme directe interne de M_1 et M_2 on dit que M_1 est facteur direct de M,et que M_2 est un supplémentaire à M_1 dans M.*

Définition 2.8.3 *Soient M un A-module et $(M_i)_{i\in I}$ une famille de sous-modules de M. On dite que M est somme directe interne des M_i lorsque $M = \sum_{i\in I} M_i$ et que pour tout $j \in I$ l'intersection $M_j \cap \sum_{j\neq i} M_i$ est réduite à $\{0\}$.*

Proposition 2.8.2 *Soient M un A-module et $(M_i)_{i\in I}$ une famille de sous-modules de M. Soient $f_i : M_i \to M$ les injections canoniques. Les assertions suivantes sont équivalentes :*

1. *Pour tout $m \in M$ il existe une unique famille finie de $m_i \in M_i$ telle que $m = \sum_i m_i$*
2. *f est un isomorphisme.*

2.9 Factorisation des morphismes de modules

Théorème 2.9.1 *Soit $f : M \to N$ un morphisme de A-modules, et soit P un sous-module de M. L'existence d'un morphisme $f^- : M/P \to N$ tel que $f = f^- \circ \pi_p$ est équivalente à l'inclusion $P \subset Ker\ f$.*

1. *Lorsque f^- existe :*
2. *f^- est unique.*
3. *f^- est surjectif si et seulement si f l'est.*
4. *f^- est injectif si et seulement si l'inclusion $H \subset Ker\ f$ est une égalité.*

2.10 Premier théorème d'isomorpie de Noether

Corollaire 2.10.1 *Soient M et N deux sous-modules d'un même A-module. On a un isomorphisme naturel $\frac{M}{M\cap N} \cong \frac{M+N}{N}$.*

2.11 Second théoreme d'isomorphie

Corollaire 2.11.1 *Soient $P \subset N$ deux sous-modules d'un même A-module M. On a un isomorphisme naturel* $\frac{M}{N} \cong \frac{M/P}{N/P}$.

CHAPITRE 3

MODULES SUR LES ANNEAUX PRINCIPAUX

Dans ce chapitre on s'intéressera aux A-modules dans le cas ou A est un anneau praincipale, et on donne les définition des modules libres, générateurs et les bases, et la fin on donne la structure des modules de type fini sur un anneau principal.

3.1 Modules libres, générateurs, bases, rangs

3.1.1 Modules libres

Définition 3.1.1 *Dorénavant on suppose en autre que l'anneau unitaire A est commutatif. La notation de rang d'un module libre sur un anneau commutatif unitaire est analogue à la dimension des espaces vectoriels. Elle nécessite cependant (au moins) une étape supplémentaire pour être définie, et ne subsiste par en toute généralité. On définit ici le rang d'un module libre* *sur un anneau commutatif unitaire. Signalons qu'il est possible de définir le rang d'un module quelconque sur un anneau intègre et une famille de P-rangs (a priori distincts) d'un module quelconque indexée par les les idéaux premiers P de l'anneau A.*

3.1.2 Modules générateurs

Définition 3.1.2 *Soit M un A-module, soit S un ensemble, $T \subset M$ un sous-ensemble de M et $\mathcal{F} = (m_s)_{s\in S}$ une famille d'élément de M.*

1. *On dite que T est un **système générateurs** de M (ou que T engendre M) lorsque pour tout x dans M il existe une famille $(\lambda_t)_{t\in T}$ d'élément de A tous nuls sauf un nombre fini et tels que $x = \sum_{t\in T} \lambda_t t$.*
2. *On dite que $\mathcal{F}$ est une **famille générateurs** lorsgue le sous-ensemble $\cup_{s\in S} \{m_s\} \subset M$ est un système générateur, c'est-à-dire lorsque pour tout x dans M il existe une famille $(\lambda_{s\in T})$ d'éléments de A tous nuls sauf un nombre fini et tels que $x = \sum_{s\in S} \lambda_s m_s$.*
3. *On dite que $\mathcal{F}$ est une **famille libre** lorsque la seule famille $(\lambda_s)_{s\in S}$ d'éléments de A tous nuls sauf éventuellement un nombre fini et vérifiant $0 = \sum_{s\in S} \lambda_s m_s$ est la famille nulle.*
4. *On dite que $\mathcal{F}$ est une **base** de M lorsque pour tout x dans famille $(\lambda_s)_{s\in S}$ d'élément de A tous nuls sauf un nombre fini et tels que $x = \sum_{s\in S} \lambda_s m_s$.*

3.1.3 Bases

Définition 3.1.3 *On dite que M est un A module libre (de base B) lorsqu'il existe une famille B d'éléments de M qui soit une base de M.*

On rencontre ici la première vraie différence entre la théorie des modules sus un anneau et celle des espaces vectoriels sur un corps : ces derniers sont tous libres. Par exemple 2 et 3 engendrent $\mathbb{Z}$ mais sont liés par $2 \times 3 = 3 \times 2$, et ni $\{2\}$ ni $\{3\}$ ne sont des systèmes générateurs de $\mathbb{Z}$. Le problème à ce que l'on ne peut pas plus diviser les relations de dépend ance linéaire $\lambda_1 x_1 = \sum_{i\neq 1} \lambda_i x_i$ par λ_1 méme si λ_1 est non nul. De sorte qu'une telle relation linéaire n'implique pas forcément que x_1 appartient au sous-module engendré par les autres x_i.

Proposition 3.1.1 *Soit S un ensemble et soit $\mathcal{F} = (m_s)_{s\in S}$ une famille d'éléments d'un A-module M.*

1. *La famille $\mathcal{F}$ est une A-base de M si et seulement si $\mathcal{F}$ est à la fois libre et génératrice.*
2. *On suppose que $\mathcal{F}$ est une A-base de M. Soit $f : A^{(S)} \to M$ l'application définie par la formule $f((a_s)_{s\in S}) = \sum a_s m_s$. Alors f est un isomorphisme de A-modules.*
3. *Soit N le plus petit sous-module de M contenant $\mathcal{F}$. Alors $\mathcal{F}$ est une famille génératrice de N.*

3.1.4 Rang

Définition 3.1.4 *Soit M un module libre. On appelle rang de M le cardinal d'une base de M.*

Bien entendu si S est un ensemble alors $A^{(S)}$ est un module libre avec sa base canonique. Le rang de $A^{(S)}$ est donc le cardinal de S. Dans le cas particulier où $S = \{1, ...s\}$ est l'ensemble fini de cardinal s on retrouve la notation standard $A^s = A^S = A^{(S)}$.

3.2 Suite exactes, torsion

Définition 3.2.1 *Soit $(f_n : M_n \longrightarrow M_{n+1})_{n\in N}$ une famille de morphisme de A-modules.*

1. *On dit que la suite*

$$\cdots \to M_{n-1} \xrightarrow{f_{n-1}} M \xrightarrow{f_n} M_{n+1} \to \cdots$$

est exacte en M_n lorsque $Im\,(f_{n-1}) = Ker\,(f_n)$.

2. *On dit que la suite*

$$\cdots \to M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \to \cdots$$

est exacte lorsqu'elle est exacte en M_n pour tout n.

3. *Dire que* $M \underset{\rightarrow}{\alpha} N \underset{\rightarrow}{} 0$ *est une suite exacte de module revient à dire que* α *est un morphisme de modules surjectif.*

4. *Dire que* $0 \underset{\rightarrow}{} M \underset{\rightarrow}{\beta} N$ *est une suite exacte de module revient à dire que* β *est un morphisme de module injectif.*

5. *Si un module M apparaît dans une suite exacte* $0 \longrightarrow M \longrightarrow 0$ *alors le module M est nul.*

6. *Dire que* $0 \underset{\rightarrow}{} M \underset{\rightarrow}{\gamma} N \underset{\rightarrow}{} 0$ *est une suite exacte revient à dire que* γ *est un isomorphisme.*

Lemme 3.2.1 *Soit* $0 \underset{\rightarrow}{} A \underset{\rightarrow}{\alpha} B \underset{\rightarrow}{\beta} C \underset{\rightarrow}{} 0$ *une suite exacte de A-modules.*

Les assertions suivantes sont équivalentes :

1. *Le sous-module* $\alpha(A)$ *est facteur direct de B.*

2. *Il existe un sous-module* $F \subset B$ *tel que la restriction de* β *à F soit un isomorphisme* $F \cong C$.

3. *Il existe un morphisme* $a : B \longrightarrow A$ *tel que* $a \circ \alpha = Id_A$.

4. *Il existe un morphisme* $b : C \longrightarrow B$ *tel que* $\beta \circ b = Id_C$.

   Lorsque ces conditions sont vérifiées,le morphisme $b \longrightarrow (\alpha(b), \beta(b))$ *est un isomorphisme* $B \cong A \oplus C$.

Exemple 3.2.1 *Soit* $N \subset M$ *des A-modules. On note* $\iota : N \longrightarrow M$ *et* $\pi : M \longrightarrow M/N$ *les morphismes canoniques. Alors la composée* $\pi \circ \iota$ *est nulle et on a méme l'égalité* $Im(\iota) = Ker(\pi)$ *. Cette situation se trés souvent et il commonde de parler dans ce ces de suites exactes de A-modules :*

$$0 \underset{\rightarrow}{} N \underset{\rightarrow}{\iota} M \underset{\rightarrow}{\pi} M/N \underset{\rightarrow}{} 0.$$

Dans cette suite de morphismes les applications$\{0\} \longrightarrow N$ *et* $M/N \longrightarrow \{0\}$ *sont les seules.*

Possibles et on note 0 *le module réduit à* $\{0\}$ *par abus. Plus généralement on peut parler de suite exacte de longueur quelconque.*

Remarque 3.2.1 *Lorsque A est un corps tous les sous-espaces vectoriels sont facteurs directs et toutes les suites courtes sont scindées. Il est alors préférable d'utiliser la notion de somme* *directe plus facile à manier et il serait ridicule de parler de suites exactes d'espaces vectoriels. Bien entendu pour les modules il existe des suites qui ne sont pas scindées.*

1. *Soit* $....\underset{\rightarrow}{}M \underset{\rightarrow}{f} N$ *une suite exacte ne terminant pas par* 0. *Alors la suite* $....\underset{\rightarrow}{}M \underset{\rightarrow}{f} N \underset{\longrightarrow}{\pi f(M)} N/f(M) \underset{\rightarrow}{} 0$ *est une suite exacte terminant par* 0.
2. *Soit* $N \underset{\rightarrow}{g} M \underset{\rightarrow}{}...$ *une suite exacte qui commence par* 0. *Alors la suite* $0 \underset{\rightarrow}{} Ker\ g \underset{\rightarrow}{} N \underset{\rightarrow}{g} M \underset{\rightarrow}{}...$ *est une suite exacte qui commence par* 0.
3. *Soit* $...\underset{\rightarrow}{}A\underset{\rightarrow}{}B \underset{\rightarrow}{f} C\underset{\rightarrow}{}...$ *une suite exacte avec plus de trois modules non nuls. Alors on peut la* $\ll$ *couper* $\gg$ *pour obtenir une suite exacte à trois termes non nuls(dite suite exacte courte) et les deux suites moins longues qui suinent :*.... $\longrightarrow A \longrightarrow Ker\ f \longrightarrow 0$

$$0 \underset{\rightarrow}{} Kerf \underset{\rightarrow}{} B \underset{\rightarrow}{f} Imf \underset{\rightarrow}{} 0$$

$$0 \longrightarrow Imf \longrightarrow C \longrightarrow ...$$

4. *On peut conclure des remarques* $2, 3$ *et* 4 *ci-dessus que l'étude des suites exactes se ramène à celle des suites exactes courtes c'est-à-dire aux modules quotients. Cependant il est plus commode et élégant lorsque c'est possible de ne considérer qu'une seule suite longue plutôt que de multiplier les suites courtes.*

3.3 Anneaux principaux

Définition 3.3.1 *Un A est dit principal s'il est intègre et si tous ses idéaux sont principaux.*

Exemple 3.3.1

1. *Tout corps est un anneau principal.*
2. *Les anneaux* $\mathbb{Z}$ *et* $\mathbb{Z}_{(p)} = \{a/b \in Q, p\ b\}$ *sont principaux.*
3. *Si k est un corps, l'anneau des polynômes en une variable* $k[X]$ *et l'anneau des séries formelles en une variable* $k[X]$ *sont principaux.*

4. *L'anneau $\mathbb{Z}[X]$ n'est pas principal, car l'idéal $(2;X)$ n'est pas principal.*

5. *L'anneau $\mathbb{Z}[X,Y]$ n'est pas principal, car l'idéal $(X;Y)$ n'est pas principal.*

6. *Si $n > 2$ est un entier composé, l'anneau $Z = nZ$ n'est pas intègre donc n'est pas principal, alors que tous ses idéaux sont principaux.*

3.4 Matrices à coéfficients dans un anneau principal

Pour tout anneau commutatif A, nous notons $M_{n,p}(A)$ le $A-$module des matrices de taille (n,p), qui s'identifie au $A-$module des morphismes de A^P dans A^n. C'est un $A-$module libre de rang np, dont la base cononique est formée des matrices $E_{i,j}$ avec $1 \leq j \leq n$ et $1 \leq j \leq p$, dont le seul coéfficient non nul est celui placé en position (i,j) qui vaut 1 :

$E_{i,j} = i \rightarrow \binom{j}{1}$

Si $E_{i,j} \in M_{n,p}(A)$ et $E_{k,l} \in M_{p,p}(A)$, on a :

$E_{i,j}\,E_{k,l} = \delta_{j,k}E_{i,l}$

où $\delta_{j,k}$ désigne le symbole de kronecker.

Le $A-$module $M_n(A) = M_{n,n}(A)$ des matrices carrées, qui s'identifie à $End(A^n)$, est muni d'une structure d'anneau et même de $A-$algèbre. Le groupe de ses élèments inversibles. Nous noterons aussi $SL_n(A)$ définies pour $i \neq j$ et $a \in A$ par :

$$E_{i,j}(a) = Id + aE_{i,j} = i \rightarrow \begin{pmatrix} 1 & & \\ & \ddots & \\ & a & 1 \end{pmatrix}$$

On a clairement $E_{i,j}(a) \in SL_n(A)$ le sous-groupe de $SL_n(A)$ engendré par les $E_{i,j}(a)$; ce groupe a une importance algorithmique dans les calculs que nous ferons ci-dessous.

Lemme 3.4.1 *Soient $M \in M_{i,j}(A)$, L_i sa $i-$ième ligne et C_j sa $j-$ième colonne.*

1. *Miltiplier M à droite par une matrice élèmentaire $E_{i,j}(a) \in M_p(A)$ a pour seul effet de remplacer la $j-$ième colonne C_j par $C_j + aC_i$. En abrégé : $C_j \longrightarrow C_j + aC_i$.*
2. *Miltiplier M à gauche par une matrice élèmentaire $E_{i,j}(a) \in M_n(A)$ a pour seul effet de remplacer la $i-$ième ligne L_i par $L_i + aL_j$.En abrégé : $L_i \longrightarrow L_i + aL_j$.*

Définition 3.4.1 *On dit que deux motrices M, M' de $M_{n,p}(A)$ sont :*

1. *Equivalentes s'il existe $P \in GL_n(A)$ et $Q \in GL_p(A)$ telles que $M' = PMQ$; on note $M \sim M'$.*
2. *$S-$équivalentes s'il existe P et Q peuvent être choisies dans SL_n et SL_p; on note $M \sim M'$.*
3. *$E-$équivalentes s'il existe P et Q peuvent être choisies dans E_n et E_p; on note $M \sim M'$.*

Définition 3.4.2 *Soit $(G, .)$ un groupe, X un ensemble non vide.*

On dit que "G agit à droite sur l'ensemble X" ou que "X est un G ensemble droite" si et seulement si il existe une application noté :$X \times G \longrightarrow X$ tel que :

1. *$x.(g.g') = (x.g).g', \forall x \in X, \forall g.g' \in G$ (associativité mixte).*
2. *$x.1_G = x, \forall x \in X, 1_G$ est le neutre de G (la neutralité).*

   De même pour l'action à gauche.

Définition 3.4.3 *Soit A une matrice carrée de taille n à coéfficients dans un anneau commutatif R. Fixons un couple (i, j) d'entiers entre 1 et n, et notons $M_{i,j}$ la matrice obtenue à partir de A en effaçant la $i-$ième ligne et la $j-$ième colonne.*

1. *le mineur d'indice (i, j) de A est le déterminant $u_{i,j} = \det\left(M_{i,j}\right)$.*

Notation 3.4.1 *Soient A un anneau, $M \in M_{n,p}(A)$ et $r \geq 0$. On note $I_r(M)$ l'ideal de A engendré par les mineurs de taille r de M.*

Proposition 3.4.1 *Les idéaux $I_r(M)$ vérifient les propriétés :*

1. *$I_r({}^tM) = I_r(M)$,*
2. *$I_{r+1}(M) \subset I_r(M)$,*
3. *$I_{r+1}(MN) \subset I_r(M) \cap I_r(N)$ pour $M \in M_{n,p}(A)$ et $M_{p,q}(A)$,*
4. *$I_r(PMQ) = I_r(M)$*
5. *pour $p \in GL_n(A)$ et $Q \in GL_p(A)$,*
6. *Soit $D = diag(d_1, ..., d_n)$ avec $d_1 \backslash ... \backslash d_n$. Alors $I_r(D) = (d_1 ... d_r)$ si $0 \leq r \leq n$, et $I_r(M) = (0)$ si $r > n$.*

Corollaire 3.4.1 *Soient M, N des $A-$modules libres de type fini de rangs respectifs p et n. Soit $\rightarrow N$ un morphisme. Alors il existe des bases B et C pour M et N tels que $Mat_{B,C}(u)$ soit une matrice diagonale de smith $diag(d_1, ..., d_r)$ ne dépendent que de u.De plus :*

1. *u est injectif si et seulement si $r = p$,*
2. *u est surjectif si et seulement si $r = n$ et $d_i \in A^*$ pour tout i.*

3.5 Structure des modules de type fini sur un anneau principal

Lemme 3.5.1 *Soient A un anneau commutatif noetherien et $n \geq 1$ un entier. Alors tout sous-module de A^n est de type fini. Si A est principal, tout sous-module de A^n est engendré par ou plus de n élèments.*

Preuve. On fait une récurrence sur n. Si $n = 1$, un sous-module de A n'est rien d'autre que idéal.

En général, soit M un sous-module de A^n avec $n \geq 2$. Notrons A^{n-1} le sous-module libre de rang $n-1$ engendrépar les $n-1$ premiers vecteurs de la base cononique de A^n.

Par l'hpothèse de récurrence, le module $N = M \cap A^{n-1}$ est de type fini. De plus, l'inclusion $M \subset A^n$ induit une application A-linéaire injective $M/N \longrightarrow A^n/A^{n-1} \simeq A$

ce qui montre, encore par hypothèse de récurrence, que M/N est de type fini. Soient $x_1, ..., x_r$ des générateurs de N et $x_{r+1}, ..., x_s$ des éléments de M dont les images dont M/N sont des générateurs. Alors $x_1, ..., x_s$ sont des générateurs de M. Dans le cas où A est principal, d'après l'hypothèse de récurrence on a $r \leq n-1$ et de plus M/N est engendré par un seul élément x_{r+1}. Donc $x_1, ..., x_{r+1}$ sont des générateurs de M en nombre $r+1 \leq n$.
■

3.5.1 Théorème de structure des modules

Soit A un anneau principal et M un A-module de type fni. Alors il existe un entier $n \geq 0$ et des éléments $d_1, ..., d_r$ de A non inventuellement nuls, tels que $d_1 \mid ... \mid d_r$ et :

$$M \simeq A/(d_1) \oplus ... \oplus A/(d_n)$$

L'entier n et la suite d'idéaux (d_i) ne dépendent que de M; ces derniers sont appelés les facteurs invariants de M.

En notant q le nombre de d_i qui sont nuls (ce sont les derniers de la liste) et $r = n-q$, on obtient une variante intéréssante de cet énoncé : il existe des entiers $q, r \geq 0$ et des éléments $d_1, ..., d_r$ de A, non nuls et non inversibles, tels que $d_1 \mid ... \mid d_r$ et :

$$M \simeq A^q \oplus A/(d_1) \oplus ... \oplus A/(d_r)$$

Les entiers q, r et la suite d'idéaux (d_i) ne dépendent que de M. L'entier q est le rang de M, défini comme nombre d'élément d'une partie libre maximale de M.

BIBLIOGRAPHIE

[1] E. Aubry, *Algèbre linéaire et bilinéaire*, France, 2012.

[2] A. Ducros, *Modules de type fini sur un anneau pricipal*, Université de Remes, 2001.

[3] D. Guin, *Algèbre Tome 2, Anneaux, modules et algèbre multilinéaire*, Eco sciences, France, 2013.

[4] A. Tchoudjem, *Math IV algèbre Formes (bi) linéaire*, Université Claude Bernard LYON 1, 2011.

RESUMÉ

Le présent travail est un scène a présenté la structure des modules, cette notion qui retrouve partout en algèbre moderne, Généralise le notions de l'espace vectoriel sur un corps à une ensemble quelconque.

Mots clés: Modules, Anneaux principaux, corps, espace vectoriel.

ملخص

نقوم في هذا العمل بتقديم البنية الجبرية للمقاييس، هذا المفهوم الذي له أهمية كبيرة في الجبر المعاصر، والذي هو عبارة عن تعميم لبنية الفضاء الشعاعي على حقل الى مجموعة كيفية.

الكلمات الأساسية: المقاييس، الحلقات الأساسية، الحقول، فضاء شعاعي.

Abstract

in this work we show the structure of the modules, this concept found in modern Algébra generalised the concept of vector space.

Key Words: Modules, principal anneaux, corps, vector spaces.