الجمهورية الجزائرية الديموقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. ***/12***

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Fondamentales**

Thème

Modules sur un Anneau (Définitions et Propriétés)

Présenté par :
1- Djelama Soumia
-
2- Bouhali Manal

Dirigé par :
Mr.Bouguebina Mounir

Année universitaire 2011-2012

Modules sur un Anneau (Définitions et Propriétés)

Djelama Soumia et Bouhali Manal

Remerciements

Nous tenons à remercier dieu le tout puissant de nous avoir donné la foi et le courage.

Nous remercions nos parents,pour tous les sacrifices qu'ils ont consentis pour nous permettre de suivre nos ètudes dans les meilleures conditions et de nous avoir encouragé tout au long de ces annèes.

Nous remercions infiniment notre encadreur Mr Bouguebina Mounir qui nous encouragé en nous faisant part d'observations constructives et pour ses prèscieux conseils.

Nous remercions toutes les personnes de l'institut de sciences et de la technologie qui nous ont enseigné durant toutes ces années d'etude.

Enfin nous remercions toutes les personnes qui ont aidé de près ou de loin à réaliser ce modeste travail.

Introduction

Les modules sur un anneau sont les analogues des espaces vectoriels sur un corps. Ce sont des groupes abéliens muni d'une opération externe des éléments de l'anneau qui a des propriétés similaires à celle qu'on trouve en algèbre linéaire. Les modules sont trés utiles dans bon nombre de branches mathématiques et notamment en Algèbre Homologique, Toplogie Algébrique et Géométrie Algébrique. Le but de ce mémoire est de présenter les définitions et les principales propriétés des modules en mettant un accent particulier sur une construction trés importante qui est le produit tensoriel de modules. Cette notion permet par exemple de comprendre l'idée de l'extension des scalaires d'un sous-anneau vers un anneau plus grand.

Ce mémoire est constitué de trois chapitres et est organisé de la manière suivante : Dans le premier chapitre, on rappelle les notions connues de groupe et d'anneaux dont nous aurons besoin par la suite. Le deuxième chapitre est le coeur de ce travail. On y donne les principales définitions et propriétés des modules sur un anneau en mentionnant rapidement les sommes directes et les suites exactes de modules et les liens entre elles. Une classe importante de modules est formée par les modules projectifs et libres qui sont étudiés à la fin de ce chapitre. Dans le troisième chapitre, aprés avoir défini le produit tensoriel de deux modules sur un anneau, on en montre l'existence et l'unicité à isomorphisme prés à travers une construction algébrique qu'on illustre par plusieurs exemples. Enfin on explique l'idée de l'extension des scalaires et on montre comment le produit tensoriel permet d'en donner une formulation algébrique.

Table des matières

Chapitre 1

Groupes et Anneaux

Dans ce chapitre on rappelle les différentes notions dans on aura besoin par la suite, en rappelant notamment les définitions et principales propriétés des groupes et des anneaux. Un soin particulier est donné aux idéaux dans un anneau à la fin du chapitre.

1.1 Groupes

Soit G un ensemble non vide et $*$ une loi de composition interne.

Définition 1 *On dit que $(G, *)$ un groupe s'il vérifie les trois propriétés suivantes :*

1. *La loi $*$ est associative : $x * (y * z) = (x * y) * z$ pour tous $x, y \in G$.*
2. *$(G, *)$ possède un élément neutre $e \in G$: $x * e = e * x = x$ pour tout $x \in G$.*
3. *Tout élément $x \in G$ admet un symétrique $x^{'} \in G$ pour $*$: $x * x^{'} = x^{'} * x = e$*

Si la loi $*$ est commutative $(x * y = y * x, \forall x, y \in G)$, le groupe G est dit commutatif ou encore abélien. On vérifie facilement que dans un groupe l'élément neutre et le symétrique sont uniques.

Exemple

1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sont des groupes abélien. L'élément neutre est $e = 0$ et le symétrique de x est $x^{'} = -x$.

2) $(\mathbb{Z}, \times)$ n'est pas un groupe. La multiplication est associative dans $\mathbb{Z}$

d'élément neutre 1, mais si $x \neq 1$, alors x n'a pas de symétrique.
3) $(\mathbb{Q}, .)$ n'est pas un groupe car 0 n'a pas d'inverse mais $(\mathbb{Q}^*, .)$ est un groupe abélien.

Définition 2 *Soit $(G, *)$ un groupe et soit H une partie non vide de G. On dit que H est un sous-groupe de G si :*

- *H est stable pour la loi $* : x, y \in H \Rightarrow x * y \in H$.*
- *$(H, *)$ est un groupe*

En pratique pour montre que H est un sous-groupe de G, il suffit de vérifier que $x, y \in H \Rightarrow x * y^{'} \in H$. Remarquer aussi que G et H ont même élément neutre : $e_G = e_H$.

Exemple

1) Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. En effet $n\mathbb{Z}$ est clairement un sous-groupe de $\mathbb{Z}$. Inversement soit H un sous-groupe de $\mathbb{Z}$. Soit n le plus petit élément positif non nul de H. Si $x \in H$, la division euclidienne de x par n donne $x = kn + r$ avec $k \in \mathbb{Z}$ et $0 \leq r < n$. Comme H est un sous-groupe, on doit avoir $x - kn = r \in H$. Par définition de n, on doit avoir $r = 0$ et $x = kn$. Donc $H = n\mathbb{Z}$
2) Soit G un groupe. Alors $H = \{e_G\}$ est un sous-groupe de G appelé le sous-groupe trivial.

Définition 3 *: Soient $(G, *)$ et $(H, \perp)$ deux groupes. Une application $f : G \longrightarrow H$ est un morphisme de groupes si :*

$$f(x * y) = f(x) \perp f(y)$$

$\forall x, y \in G$.

Autrement dit f préserve les structures de groupes de G et H. Si f est bijective, on dit que c'est un isomorphisme. Si $G = H$ et $* = \perp$, on parle d'endomorphisme et d'automorphisme. Noter que $f(e_G) = e_H$. Le noyau du morphisme f est :

$$Kerf = \{x \in G : f(x) = e_H\} = f^{-1}(e_H).$$

C'est un sous-groupe de G. Le noyau est utile pour detecter si f est injective ou non. En effet on a : f injective $\Leftrightarrow Kerf = \{e_G\}$. Par exemple le morphisme $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ donné par $f(x) = 3x$ est injectif puisque $Kerf = \{0\}$ (la loi de groupe est l'addition).

Soit $(G, *)$ un groupe abélien et soit H un sous-groupe de G. On définit une relation sur G par :

$$x \Re y \Leftrightarrow x * y^{'} \in H.$$

On vérifie facilement que $\Re$ est une relation d'équivalence. On a donc l'ensemble quotient, ensemble des classes d'équivalence :

$$\frac{G}{\Re} = \frac{G}{H} = \{\overline{x}, x \in G\}.$$

Définissons $\overline{*}$ par $\overline{x} \ \overline{*} \ \overline{y} = \overline{x * y}$. On a donc une loi $\overline{*}$ sur $\frac{G}{H}$ qui devient ainsi un groupe abélien appelé le groupe quotient de G par H. En effet :

- l'associativité de $\overline{*}$ découle de celle de $*$ par définition.
- l'élément neutre de $\overline{*}$ est $\overline{e}$ avec e l'élément neutre de $*$.
- le symétrique de $\overline{x}$ est $\overline{x^{'}}$ avec $x^{'}$ le symétrique de x.

On a automatiquement un morphisme surjectif canonique de groupes :

$$\phi : G \longrightarrow \frac{G}{H}$$

qui à x associe $\overline{x}$, de noyau $Ker\phi = H$.
Exemple : On prend $(G, *) = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. On a $x \Re y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow x \equiv y \ mod(n)$ et :

$$\frac{G}{H} = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Convention : Dans la suite un groupe $(G, *)$ sera noté multiplicativement : $* = .$ et $e_G = 1$. Le symétrique $x^{'}$ de x sera noté x^{-1}. Si la loi est commutative, on le notera additivement : $* = +$, $e_G = 0$ et le symétrique $x^{'}$ de x sera noté $-x$.

1.2 Anneaux

Soit A un ensemble muni de deux lois de composition interne $+$ et $.$.

Définition 4 *: On dit que le triplet $(A, +, .)$ est un anneau si :*

- *$(A, +)$ est un groupe abélien d'élément neutre 0_A.*
- *La loi $.$ est associative et admet un élément neutre $1_A \neq 0_A$.*

– *La loi . est distributive à gauche et à droite par rapport à la loi + : $\forall x, y, z \in A$, on a :*

$$x.(y+z) = x.y + x.z$$

$$(x+y).z = x.z + y.z$$

Si la loi . est commutative, l'anneau est dit commutatif.

On a appelé ici anneau ce que d'autres appelent anneau unitaire : autrement dit dans la définition d'un anneau, la loi . n'est pas obligée d'avoir un élément neutre 1_A. Comme les anneaux que nous allons rencontrer sont tous unitaires, cela ne pose pas vraiment de problème. De plus dans un anneau, on a $0_A.x = 0_A$, $\forall x \in A$. En effet : $0_A.x = (x-x).x = x.x - x.x = 0_A$.

Exemple

1) $(\mathbb{Z}, +, .), (\mathbb{Q}, +, .)$ et $(\mathbb{R}, +, .)$ sont des exemples bien connus d'anneaux commutatifs.

2) Soit $A = P(E)$ l'ensemble des parties d'un ensemble E. On prend $+ = \cup$ et $. = \cap$. $(A, +, .)$ est alors un anneau commutatif avec $0_A = \emptyset$ et $1_A = E$.

Définition 5 *: Soit $(A, +, .)$ un anneau soit B une partie de A contenant 1_A et stable pour les lois + et .. On dit que B est un sous-anneau de A si muni de ces deux lois B est lui-même un anneau.*

Remarquer que la condition $1_A \in B$ est necessaire. Par exemple $2\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car il ne contient pas 1. Par contre $B = \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Q}, +, .)$. Dans la pratique pour montrer que B est un sous-anneau de A, il suffit de vérifier que $1_A \in B$ et que $\forall x, y \in B$, on a $x - y$ et $x.y \in B$.

Définition 6 *: Une partie I d'un anneau A est appelé idéal à gauche (respectivement à droite) si :*

– *I est un sous-groupe de $(A, +)$.*

– *$\forall a \in A, \forall x \in I : a.x \in I$ (respectivement $x.a \in I$.*

Si I est un idéal à gauche et à droite à la fois de A, on dit que c'est un idéal bilatère de A.

Remarque

1) Si A est commutatif, les idéaux à gauche et à droite coincident.

2) $\{0_A\}$ et A sont des idéaux de A. Ils sont appelés idéaux triviaux. Les autre idéaux de A sont dits propres.

3) Un idéal de A n'est pas forcément un sous-anneau de A, car il ne contient pas en général 1_A. Plus précisément on a :

$$1_A \in I \Leftrightarrow I = A.$$

4) Dans la suite, on va considérer uniquement des anneaux commutatifs. On dira donc anneau pour anneau commutatif.

Exemple

1) Soit A un anneau et soit $a \in A$. Alors l'ensemble $I = aA = \{a.x, x \in A\}$ est un idéal de A. On l'appelle l'idéal principal engendré par$a$. L'anneau A sera dit principal si tous ses idéaux sont principaux.

2) $(\mathbb{Z}, +, .)$ est un anneau principal. En effet, on a vu que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$ et ce sont donc les seuls idéaux de $\mathbb{Z}$.

3) L'intersection d'un nombre quelconque idéaux est un idéal. Plus généralement l'intersection de tous les idéaux contenant une partie G de A est un idéal. On l'appelle l'idéal engendré par la partie G. Ses éléments sont les sommes finies $\sum_{k=1}^{n} a_k x_k$ avec $a_k \in A$ et $x_k \in G$.

4) la somme de deux idéaux I_1 et I_2 est l'ideal $I_1 + I_2 = \{x+y, x \in I_1, y \in I_2\}$. On peut aussi le définir comme étant l'idéal engendré par$I_1 \cup I_2$. En particulier il contient I_1 et I_2 De manière plus générale la somme $\sum_\lambda I_\lambda$ d'une famille d'idéaux I_λ est le plus petit idéal de A contenat chacun des I_{lambda}.

5) Le produit de deux idéaux I et J est l'idéal IJ engendré par les produits $x.y$ avec $x \in I$ et $y \in J$. Concrètement ses éléments sont les sommes finies $\sum x_i.y_i$ avec $x_i \in I$ et $y_i \in J$.

Soient $a, b \in A$. On dit que a divise b ou que b est un multiple de a s'il existe $c \in A$ avec $b = ac$. L'idéal $I = aA$ est donc l'ensemble des multiples de a. Remarquer que a divise b si et seulement si $bA \subset aA$. Un élément a est une unité s'il a un inverse a^{-1} pour la multiplication. a est dit premier ou irréductible si $a = bc$ implique que b ou c est une unité. $a \neq 0$ est un diviseur de 0 s'il existe $b \neq 0$ tel que $a.b = 0$. Les anneaux qui n'ont pas de diviseurs de zéro sont appelés des anneaux intègres. Par exemple dans $\mathbb{Z}$, les éléments premiers sont (au signe prés) les nombres premiers p. L'equation $a.b = 0$ n'a pas de solution non nulle dans $\mathbb{Z}$ qui est donc un anneau intègre.

Définition 7 *: Un idéal propre I d'un anneau A est dit premier si $ab \in I$ implique $a \in I$ ou $b \in I$. I est dit maximal s'il n'est contenu dans aucun autre idéal propre de A.*

Proposition 1 *: Un idéal maximal est premier. Les idéaux premiers de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier et ils sont tous maximaux.*

Preuve : Soit I un idéal maximal. Soient $a, b \in A$ avec $ab \in I$. Supposons que $a \notin I$. Alors l'idéal $I + aA$ est égal à A, car I est maximal. Il existe alors $d \in I$ et $x \in A$ avec $d + a.x = 1$ et donc $d.b + a.b.x = b \in I$ (rappelons que A est commutatif). Ceci montre que I est premier. Tout idéal propre de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \neq 0 \in \mathbb{N}$. Supposons que $n\mathbb{Z}$ premier. $ab \in n\mathbb{Z}$ implique $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$ s'écrit n divise ab implique n divise a ou n divise b, ce qui par le lemme de gauss veut dire que $n = p$ un nombre premier. Enfin $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si m divise n. Ceci montre que tout idéal premier de $\mathbb{Z}$ est maximal.

Une application $f : A \longrightarrow B$ entre deux anneaux est un morphisme si :

$$f(x + y) = f(x) + f(y)$$

$$f(x.y) = f(x).f(y)$$

$$f(1_A) = 1_B$$

pour tous $x, y \in A$. Autrement dit f préserve les opérations d'anneau. Si f est de plus bijective, on dit que c'est un isomorphisme entre A et B. Si $A = B$, on parle d'endomorphisme et d'automorphismes, respectivement. Le noyau d'un morphisme f est :

$$Kerf = \{x \in A : f(x) = 0_B\} = f^{-1}(0_B).$$

C'est un idéal de A. L'image de f est :

$$Imf = \{f(x), x \in A\} = f(A).$$

C'est un sous-anneau de B.

Soit A un anneau et soit I un idéal de A. On définit une relation $\Re$ sur A par :

$$x\Re y \Leftrightarrow x - y \in I.$$

On verifie facilement que $\Re$ est une relation d'equivalence sur A. Sur l'ensemble quotient

$$\frac{A}{\Re} = \frac{A}{I} = \{\overline{x}, x \in A\},$$

on définit deux opérations $\overline{+}$ et $\overline{\cdot}$ en posant : $\overline{x} \ \overline{+} \ \overline{y} = \overline{x + y}$ et $\overline{x} \ \overline{\cdot} \ \overline{y} = \overline{x.y}$. Ces deux opérations sont bien définies et font de $\frac{A}{I}$ un anneau. C'est

l'anneau quotient de A par I. Remarquer que $\overline{x} = x + I$. En particulier $\overline{0} = I$ est l'élément neutre de $\overline{+}$.

On a un morphisme canonique surjectif d'anneaux :

$$\phi : A \longrightarrow \frac{A}{I}$$

qui à x associe sa classe modulo I, $\overline{x} = x + I$ et de noyau $Ker\phi = I$. De plus il y a une correspondance bijective entre les idéaux J de A qui contiennent I et les idéaux $\overline{J}$ de $\frac{A}{I}$ donnée par $J = \phi^{-1}(\overline{J})$.
Exemple : On prend $A = \mathbb{Z}$ et $I = n\mathbb{Z}$. On a alors $x - y \in n\mathbb{Z} \Longleftrightarrow x \equiv y \ mod(n)$. L'ensemble quotient est donc l'ensemble des classes de congruence modulo n :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et les opérations d'anneau sont celles bien connues de l'addition et de la multiplication des congruences.

Proposition 2 *: L'idéal I est premier si et seulement si l'anneau quotient $\frac{A}{I}$ est intègre.*

Preuve : Un anneau est intègre s'il n'a pas de diviseurs de 0. Supposons I premier et soient $\overline{a}$ et $\overline{b}$ tels que $\overline{a}.\overline{b} = \overline{0}$. donc $a.b \in I$. Comme I est premier, cela veut dire que $a \in I$ ou $b \in I$, c'est à dire que $\overline{a} = \overline{0}$ ou que $\overline{b} = \overline{0}$ et donc que l'anneau quotient est intègre. Inversement supposons l'anneau quotient intègre et soient $a, b \in A$ avec $a.b \in I$. Donc $\overline{a}.\overline{b} = \overline{0}$ et donc $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, c'est à dire que $a \in I$ ou $b \in I$. Ceci montre que I est premier.

Chapitre 2

Modules sur un Anneau

On commence, dans ce chapitre, l'étude proprement dite des modules sur un anneau. Dans la première section, on donne la définition d'un R-module pour R un anneau et quelques exemples. On travaillera toujours avec un anneau commutatif et on ne fera donc pas de distinction entre modules à gauche et modules à droite. On parle aussi dans cette section de sous-modules, de modules quotients et de morphismes de modules. Dans la seconde section, on présente une construction importante en théorie des modules : la somme directe et on fait le lien entre cette notion et une autre non moins importante : les suites exactes de modules. On verra que toute somme directe fait partie d'une suite exacte assez particulière. Dans la troisième section, on définit les modules libres et les modules projectifs et on montre en particulier que tout module projectif fait partie d'une somme directe qui est un module libre. Enfin on donnera une caractérisation des modules projectifs eu utilisant le foncteur $Hom(M, .)$ da la catégorie des R-modules vers celle des groupes abéliens et les suites exactes courtes.

2.1 Modules et morphismes de modules

Soit R un anneau (unitaire).

Définition 8 *Soit M un groupe abélien. On dit que M est un module à gauche sur R si on a une application (une opération à gauche de R sur M)*

$$\begin{array}{rcl} R \times M & \longrightarrow & M \\ (r, m) & \longmapsto & r.m \end{array}$$

telle que :

- *r.(m+n)=r.m+r.n*
- *(r+s).m=r.m+s.m*
- *(rs).m=r.(s.m)*
- *1.m=m*

$\forall r, s \in R$ *et* $\forall m, n \in M$.

On dit que M est un module à droite sur R si on a une opération à droite de R sur M :

$$\begin{array}{rcl} M \times R & \longrightarrow & M \\ (m, r) & \longmapsto & m.r \end{array}$$

telle que

- *(m+n).r=m.r+n.r*
- *m.(r+s)=m.r+m.s*
- *m.(rs)=(m.r).s*
- *m.1=m*

$\forall r, s \in R$ *et* $\forall m, n \in M$.

Si R est un anneau commutatif, tout module M à gauche sur R est aussi un module à droite sur R en posant

$$m.r = r.m$$

Dans la suite de ce mémoire on travaillera uniquement avec des anneaux commutatifs. On ne fera donc pas de distinction entre modules à gauche et modules à droite. On parlera tout simplement de modules sur un anneau.

Exemple

1) Tout groupe abélien G est un $\mathbb{Z}$-module avec $\mathbb{Z}$ l'anneau des entiers en posant :

$$n.g = \underbrace{g + \ldots + g}_{n}$$

pour $n \in \mathbb{Z}$ et $g \in G$.

2)Tout idéal I d'un anneau R est un R-module. En effet comme I est un idéal de R, on a

$$r.a \in I$$

$\forall r \in R$ et $\forall a \in I$ (la multiplication est celle de l'anneau R). Ceci définit une opération de R sur I qui a les propriétés requises.

3) Soit S un sous-anneau de l'anneau R. Si M est un R-module alors M est

aussi un S-module. L'opération de S sur M est la restriction de l'opération de R sur M.
4) Soit $\phi : R \to S$ un morphisme d'anneaux. Soit M un S-module. Alors M devient aussi un R-module en posant :

$$r.m = \phi(r).m$$

5) Soit $M = R[X]$ l'anneau des polynômes à une variable à coefficients dans l'anneau R. Alors M est un R-module. Si $F(X) = a_0 + a_1X + \ldots + a_nX^n \in R[X]$ avec $a_0, \ldots, a_n \in R$, on pose

$$r.F(X) = ra_0 + ra_1X + \ldots + ra_nX^n$$

6) Si $R = K$ est un corps alors un K-module est tout simplement un K-espace vectoriel.
Ce dernier exemple explique pourquoi on parle d'algèbre linéaire sur un anneau quand on parle de modules sur un anneau.

Définition 9 *Soit R un anneau et soit M un R-module. Une partie $N \subseteq M$ est appelé un sous-module de M si N est un sous-groupe de M et si*

$$n \in N \Rightarrow r.n \in N$$

Autrement dit N est un sous-groupe de M et N est stable sous l'action de R.

Rappelons que dans le cas abélien tout sous-groupe N de M est distingué et on peut donc former le groupe quotient $\frac{M}{N}$. Il se trouve que ce groupe quotient est aussi un R-module.

Proposition 3 *Soit M un R-module et soit N un sous-module de M. Alors le groupe quotient $\frac{M}{N}$ est aussi un R-module.*

Preuve : Soit $\overline{m} = m+N$ la classe de m modulo N. On définit une opération de R sur $\frac{M}{N}$ en posant :

$$r.(m + N) = r.m + N$$

ou encore

$$r.\overline{m} = \overline{r.m}$$

Cette opération est bien définie. En effet supposons que $\overline{m} = \overline{m'}$ i.e $m - m' \in N$. Alors on a $r.m - r.m' = r.(m - m') \in N$ et donc $\overline{r.m} = \overline{r.m'}$. Il reste à montrer que cette opération vérifie bien les propriétés définissant un module :

- $r.(\overline{m}) = \overline{r.(m+n)} = r.\overline{m} + r.\overline{n}$.
- $(r+s).\overline{m} = \overline{(r+s).m} = \overline{r.m + s.m} = r.\overline{m} + s.\overline{m}$.
- $(rs).\overline{m} = \overline{(rs).m} = \overline{r.(s.m)} = r.(s.\overline{m})$.
- $1.\overline{m} = \overline{1.m} = \overline{m}$.

Définition 10 *Soient M et N deux R-modules. Un morphisme de modules est une application :*

$$\phi : M \longrightarrow N$$

qui vérifie :

- $\phi(m + m') = \phi(m) + \phi(m')$.
- $\phi(r.m) = r.\phi(m)$.

$\forall m, m' \in M$ *et* $\forall r \in R$.

Le noyau de ϕ est :

$$Ker(\phi) = \{m \in M / \phi(m) = 0_N\}$$

C'est un sous-module de M. L'image de ϕ est :

$$Im(\phi) = \{n \in N / \exists m \in M / n = \phi(m)\}$$

C'est aussi un sous-module de N. L'application est injective si et seulement si :

$$Ker(\phi) = \{o_M\}$$

Remarquer que $\{0_M\}$ est un sous-module de M (appelé le sous-module trivial). De même le morphisme ϕ est surjectif si et seulement si :

$$Im(\phi) = N$$

Un morphisme bijectif est appelé un isomorphisme. En fait un morphisme induit toujours un isomorphisme comme l'indique la :

Proposition 4 *Soit $\phi : M \to N$ un morphisme de modules. Alors on a un isomorphisme canonique :*

$$\begin{array}{rcl} \frac{M}{Ker(\phi)} & \longrightarrow & Im(\phi) \\ \overline{m} & \longmapsto & \phi(m) \end{array}$$

Preuve : Appelons cette application $\tilde{\phi}$. Donc $\tilde{\phi}(\overline{m}) = \phi(m)$. $\tilde{\phi}$ est bien définie. En effet si $\overline{m} = \overline{m'}$ alors $m - m' \in Ker(\phi)$ et donc $\phi(m - m') = \phi(m) - \phi(m') = 0$ i.e $\phi(m) = \phi(m')$. Si $\tilde{\phi}(\overline{m}) = 0$ alors $\phi(m) = 0$ et donc $m \in Ker(\phi)$. Ceci montre que $\overline{m} = 0$ et que $\tilde{\phi}$ est injective. Il reste à montrer que $\tilde{\phi}$ est surjective. Soit $n \in Im(\phi)$. $\exists m \in M$ avec $\phi(m) = n$. Donc $\tilde{\phi}(\overline{m}) = \phi(m) = n$ et donc $\tilde{\phi}$ est surjective.

2.2 Sommes directes et suites exactes

Définition 11 *Soient M et N deux R-modules. Leur somme directe est le module :*

$$M \oplus N = \{(m, n), m \in M, n \in N\}$$

avec l'opération de R :

$$r.(m, n) = (r.m, r.n)$$

La proposition suivante caractérise la somme directe par une propriété universelle :

Proposition 5 *Soient L,M,N des R-modules. Alors $L \cong M \oplus N$ si et seulement si il existe des morphismes de R-modules $\pi_1 : L \to M$,$\pi_2 : L \to N$ et $i_1 : M \to L$, $i_2 : N \to L$ tels que :*

- $\pi_1 \circ i_1 = Id_M$ *et* $\pi_2 \circ i_2 = Id_N$.
- $\pi_k \circ i_l = 0$ *si* $k \neq l$.
- $i_1 \circ \pi_1 + i_2 \circ \pi_2 = Id_L$.

Preuve : Pour tous R-modules M,N, on a des morphismes injectifs (des inclusions) $i_1 : M \to M \oplus N$ et $i_2 : N \to M \oplus N$ données par $i_1(m) = (m, 0)$ et $i_2(n) = (0, n)$ et des projections $\pi_2 : M \oplus N \to M$ et $\pi_2 : M \oplus N \to N$ données par $\pi_1(m, n) = m$ et $\pi_2(m, n) = n$ et qui vérifient les propriétés de la proposition. Donc si $\phi : L \cong M \oplus N$ est un isomorphisme, alors les $\pi_k \circ \phi$ et les $\phi^{-1} \circ i_k$ fournissent ces applications sur L. Inversement etant donnés les π_k et les i_k, on définit $\phi : L \to M \oplus N$ par $\phi(x) = (\pi_1(x), \pi_2(x))$ et $\psi : M \oplus N \to L$ par $\psi(m, n) = i_1(m) + i_2(n)$. On vérifie facilement que ce sont des morphismes. De plus on a $\phi \circ \psi(m, n) = (m, n)$ et $\psi \circ \phi(x) = x$, ce qui montre que ϕ et ψ sont inverses l'une de l'autre.

La propriété universelle dégagée par cette proposition est la suivante : Etant donnés deux R-modules M_1 et M_2 et un R-module N avec des morphismes $f_i : M_i \to N$, alors il existe un unique morphisme $f : M_1 \oplus M_2 \to N$

tel que $f_i = f \circ i_i$. L'application f est donnée par $f(m_1, m_2) = f_1(m_1) + f_2(m_2)$.

Une autre caractérisation des sommes directes utilise la notion de suite exacte.

Définition 12 *Soit $M_i, i \in \mathbb{Z}$ des R-modules. Soit*

$$\ldots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots$$

une suite de morphismes de modules. Cette suite est dite exacte en M_i si :

$$Ker(f_i) = Im(f_{i-1})$$

La suite est dite exacte si elle est exacte en M_i pour tout i.

Une suite exacte pour laquelle $M_i = 0$ pour $\mid i \mid > 1$ est dite suite exacte courte. Une telle suite s'écrit :

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

l'exactitude veut dire que f est injective, que g est surjective et que $Ker(g) = Im(f)$. Par exemple toute somme directe $M_1 \oplus M_2$ de deux R-modules fait partie d'une suite exacte courte :

$$0 \longrightarrow M_1 \xrightarrow{i_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$$

avec $i_1(m_1) = (m_1, 0)$ et $\pi_2(m_1, m_2) = m_2$.

Définition 13 *Une suite exacte courte de R-modules :*

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

est scindée s'il existe un morphisme $s : N \longrightarrow M$ tel que $g \circ s = Id_M$. Le morphisme s est appelé le scindage de la suite exacte.

La proposition suivante montre le lien entre suites exactes courtes scindées et sommes directes :

Proposition 6 *Soit $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ une suite exacte courte scindée. Alors on a un isomorphisme*

$$M \cong M_1 \oplus M_2$$

Preuve : Soit $s : M_2 \longrightarrow M$ un scindage de la suite exacte courte. On définit des applications $\pi_1 : M \longrightarrow M_1$, $\pi_2 : M \longrightarrow M_2$, $i_1 : M_1 \longrightarrow M$ et $i_2 : M_2 \longrightarrow M$ en posant $\pi_1(m) = f^{-1}(m - s \circ g(m))$, $\pi_2(m) = g(m)$, $i_1(m_1) = f(m_1)$ et $i_2(m_2) = s(m_2)$. On a $g(m - s \circ g(m)) = g(m) - g \circ s \circ g(m) = g(m) - g(m) = 0$, donc $m - s \circ g(m) \in Ker(g) = Im(f)$, ce qui montre que π_1 est bien définie. Ces applications vérifient les propriétés caractérisant une somme directe, ce qui finit de démontrer la proposition.

2.3 Modules libres et modules projectifs

Soit M un R-module et soit $X \subset M$ une partie de M. On dit que X engendre M si :

$$m = \sum_{i=1}^{k} r_i.x_i$$

pour tout $m \in M$, avec $r_i \in R$ et $x_i \in X$. Autrement dit tout élément de M s'écrit (de manière unique) comme combinaison linéaire (sur R) d'éléments de X. On dit que M est un module de type fini s'il est engendré par une partie X finie.

Exemple

1) le $\mathbb{Z}$-module $\mathbb{Z}$ est de type fini engendré par $X = \{1\}$.

2) Le $\mathbb{Z}$-module $\mathbb{Z}^n$ est de type fini engendré par $X = \{e_1, \ldots, e_n\}$ avec $e_i = (0, \ldots, 1, \ldots, 0)$ le vecteur dont toutes les entrées sont nulles sauf celle de rang i qui vaut 1.

3) Le $\mathbb{Z}$-module $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est de type fini engendré par $X = \{\overline{1}\}$ mais aussi par $X = \{\overline{m}\}$ avec $pgcd(m, n) = 1$.

4) Si $R = K$ est un corps et $M = V$ un K-espace vectoriel, une partie génératrice de V est une partie qui engendre V au sens de l'algèbre linéaire.

Si M est un R-module de type fini, on a une application

$$\phi : R^n \longrightarrow M$$

donnée par :

$$\phi(r_1, \ldots, r_n) = \sum_{i=1}^{n} r_i.x_i$$

ϕ est un morphisme surjectif de modules (R^n est un R-module engendré par $X = \{e_1, \ldots, e_n\}$).

Une base d'un R-module M est une partie génératrice X de M telle que tout élément de M s'écrive de manière unique comme combinaison linéaire d'éléments de X ou, autrement dit, si :

$$\sum_{i=1}^{n} r_i.x_i = 0 \Longrightarrow r_i = 0, \forall i$$

pour toute partie finie $\{x_1, \ldots, x_n\}$ de X. Cette définition généralise la notion de base d'un espace vectoriel en algèbre linéaire.

Définition 14 ***(Somme directe infinie)*** *Soit I un ensemble d'indices et soit $(M_i)_{i\in I}$ une famille de R-modules indexée par I. On définit le module somme directe des M_i par :*

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} / m_i \in M_i\}$$

avec la condition que les m_i sont tous nuls sauf un nombre fini.

L'addition sur cette somme directe infinie est donnée par :

$$(m_i)_{i\in I} + (m_i^{'})_{i\in I} = (m_i + m_i^{'})_{i\in I}$$

et l'opération de R par :

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

Exemple
Si $I = \mathbb{N}$ et $M_i = R, \forall i \in \mathbb{N}$, on obtient un module somme directe :

$$R^{\infty} = \bigoplus_{n\in\mathbb{N}} R$$

R^{∞} a une base formée des vecteurs $e_i = (\ldots, 0, 1, 0, \ldots)$.

Proposition 7 *Soit M un R-module et soit $X \subset M$ une base de M. Alors on a un isomorphisme :*

$$M \cong \bigoplus_{x\in X} R.$$

Preuve : On définit une application

$$\phi : \bigoplus_{x \in X} R \longrightarrow M$$

par

$$\phi((r_x)_{x \in X}) = \sum_{x \in X} r_x.x$$

L'application ϕ est bien définie car $r_x = 0$ pour presque tout x et donc la somme à droite est une somme finie. Comme X engendre M, ϕ est surjective et c'est clairement un morphisme. Il reste à montrer qu'elle est injective. Supposons $\phi((r_x)) = 0$ Donc $\sum r_x.x = 0$. Comme X est une base, on doit avoir $r_x = 0, \forall x$ et donc $(r_x)_{x \in X} = 0$.

Définition 15 *Un R-module M est dit libre s'il a une base $X \subset M$.*

Par exemple le R-module $R^n = R \times \ldots \times R$ est libre engendré par $X = \{e_1, \ldots, e_n\}$.

Proposition 8 *Soit M un R-module. Alors il existe un R-module libre F et un morphisme surjectif $f : F \longrightarrow M$.*

Preuve : Soit X une partie génératrice de M (on peut toujours prendre $X = M$). L'application :

$$f : F = \bigoplus_{x \in X} R \longrightarrow M$$

qui à $(r_x)_{x \in X}$ associe $\sum_{x \in X} r_x.x$ est bien un morphisme surjectif et F est libre.

Une classe importante de R-modules est constituée par les modules projectifs.

Définition 16 *Un R-module P est dit projectif si pour tout R-module M, tout morphisme $g : M \longrightarrow P$ a un scindage $s : P \longrightarrow M$.*

L'interêt des modules projectif est clarifié par la proposition suivante. Elle montre que tout module projectif est un morceau d'un module libre. En particulier tout module libre est projectif.

Proposition 9 *Soit P un R-module. Alors P est projectif si et seulement si il existe un R-module Q tel que :*

$$P \oplus Q = \bigoplus_{x \in X} R$$

pour un certain ensemble X. Si P est de type fini alors X peut-être choisi fini.

Preuve : Soit X une partie génératrice de P. On a un morphisme surjectif $g : \bigoplus_{x \in X} R \longrightarrow P$. Comme P est projectif il y a un scindage $s : P \longrightarrow \bigoplus_{x \in X} R$ de g. Comme $Ker(g) \subset \bigoplus_{x \in X} R$, on obtient une suite exacte scindée :

$$0 \longrightarrow Ker(g) \longrightarrow \bigoplus_{x \in X} R \xrightarrow{g} P \longrightarrow 0$$

et donc :

$$Ker(g) \oplus P \cong \bigoplus_{x \in X} R$$

Inversement soit $g : M \longrightarrow P$ un morphisme surjectif de R-modules. Alors $g \oplus Id_Q : M \oplus Q \longrightarrow P \oplus Q$ est aussi un morphisme surjectif. Comme $P \oplus Q \cong \bigoplus_{x \in X} R$, on peut choisir des éléments $x_i \in (g \oplus Id_Q)^{-1}(e_i)$ et définir $t : P \oplus Q \longrightarrow M \oplus Q$ par $t(\sum r_i e_i) = \sum r_i x_i$. On a alors $g \oplus Id_Q \circ t = Id_{P \oplus Q}$. Posons alors $s(p) = t(p, 0)$ pour $p \in P$. Ceci définit $s : P \longrightarrow M$. En effet on a dans tous les cas $s(p) = (m, q) \in M \oplus Q$ et il faut montrer que $q = 0$. Or on a

$$(p, 0) = g \oplus Id_Q \circ t(p, 0) = g \oplus Id_Q(m, q) = (g(m), q)$$

. De plus on a

$$g \oplus Id_Q(s(p), 0) = g \oplus Id_Q \circ t(p, 0) = (p, 0)$$

et donc $g(s(p)) = p$, ce qui montre que s est un scindage de g.

Une autre définition souvent utilisée d'un module projectif est la suivante : P est un module projectif si pour tous morphismes $f : P \longrightarrow N$ et $g : P \longrightarrow M$ avec g surjectif, il existe un morphisme $h : P \longrightarrow M$ tel que $g \circ h = f$. Nous laissons au lecteur le soin de vérifier que cette définition est équivalente à la précédente.

Si M et N sont des R-modules, l'ensemble $Hom_R(M, N)$ des morphismes entre M et N est un groupe abélien pour l'addition des applications :

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

Si M est fixé alors l'application

$$Hom_R(M,.) : N \longmapsto Hom_R(M,N)$$

associe à un R-module N un groupe abélien. Si $N \longrightarrow L$ est un morphisme, on obtient une application

$$\phi_* : Hom_R(M,N) \longrightarrow Hom_R(M,L)$$

donnée par $\phi_*(f) = f \circ \phi$ et qui est un morphisme de groupes abéliens.

En utilisant ces Hom, on peut donner une autre caractérisation des modules projectifs et faisant intervenir les suites exactes courtes.

Théorème 1 *Le R-module P est projectif si et seulement si pour toute suite exacte courte de R-modules :*

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

la suite :

$$0 \longrightarrow Hom_R(P,M) \xrightarrow{\phi_*} Hom_R(P,N) \xrightarrow{\psi_*} Hom_R(P,L) \longrightarrow 0$$

est une suite exacte de groupes abéliens.

Preuve : Il faut montrer que ϕ_* est injective, ψ_* surjective et $Ker(\psi_*) = Im(\phi_*)$. Supposons que $\phi_*(f) = 0$ i.e $\phi \circ f(p) = 0$ pour tout $p \in P$. Comme ϕ est injective, on a $f(p) = 0$ pour tout $p \in P$ et donc $f = 0$. D'autre part soit $\psi_*(g) = 0$ et donc $\psi \circ g(p) = 0$ pour tout $p \in P$. Ainsi $g(p) \in Ker(\psi) = Im(\phi)$ et $g(p) = \phi(m_p)$ pour un certain $m_p \in M$. L'application $\phi^{-1} \circ g : p \mapsto m_p$ est un morphisme bien défini puisque ϕ est injective. Donc $g(p) = \phi(\phi^{-1} \circ g) = \phi_*(\phi^{-1} \circ g)$ et $Ker(\psi_*) \subset Im(\phi_*)$. Inversement si $g = \phi_*(f)$ alors $g(p) = \phi \circ f(p)$, ce qui veut dire que $g(p) \in Im(\phi) = Ker(\psi)$ et $\psi_*\psi(p) = \psi \circ \phi \circ f(p)$. ceci montre que $Im(\phi_*) \subset Ker(\psi_*)$. Il reste à montrer que ψ_* est surjective. Soit $h \in Hom(P,L)$. Comme ψ est surjective, on applique la seconde définition d'un module projectif aux morphismes ψ et h. Il existe donc un morphisme $k : P \longrightarrow M$ tel que $\psi \circ k = h$ i.e $\psi_*(k) = h$.

Chapitre 3

Produit Tensoriel de Modules

Le produit tensoriel de modules est une construction mathématique qui permet de ramener l'étude d'opérations bilinéaires ou multilinéaires à celles d'opérations linéaires sur les modules (les applications bilinéaires sont ramenés aux applications linéaires ou plus exactement ici aux morphismes de modules). Le produit tensoriel est trés utile dans beaucoup de branches mathématiques telles que l'Algèbre Homologique, la Topologie Algébrique ou encore la Géométrie Algébrique. Le produit tensoriel vérifie une propriété universelle qui le caractérise à isomorphisme prés.

Le plan de ce chapitre est le suivant : dans la première section, on présentera brièvement les définitions des applications bilinéaires (et multilinéaires) entre modules. Dans la deuxième section, on donnera la définition du produit tensoriel de modules ainsi que sa construction. Des exemples de produit tensoriel seront donnés dans la troisième section. Enfin dans la dernière section on étudiera rapidement l'opération importante d'extensions de la base qui est un mécanisme qui transforme un R-module en un S-module pour S une extension de R.

3.1 Applications bilinéaires

Soit R un anneau (toujours commutatif) et soient M, N, P des R-modules.

Définition 17 *Une application $B : M \times N \longrightarrow P$ est dite bilinéaire si :*
- $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$.
- $B(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$.
- $B(r.m, n) = B(m, r.n) = rB(m, n)$.

$\forall m, m_1, m_2 \in M,\ \forall n, n_1, n_2 \in N$ *et* $\forall r \in R$

Autrement dit $B(m, .)$ est un morphisme (application linéaire) $N \longrightarrow P$ et $B(., n)$ est un morphisme $M \longrightarrow P$ pour tout $m \in M$ et tout $n \in N$. L'ensemble des applications bilinéaires $M \times N \longrightarrow P$ sera noté $Bil(M, N; P)$. Il a une structure naturelle de R-module.

Exemple

1) On prend $M = N = P = R$. Alors la multiplication d'anneau $R \times R \longrightarrow R$ est une application bilináire.

2) Soit M un R-module. Alors la multiplication par les scalaires $R \times M \longrightarrow M$ est bilinéaire.

3) Soit $Hom_R(M, N)$ l'ensemble des morphismes de N vers P. Il a une structure naturelle de R-module. Soit $f : M \longrightarrow Hom_R(N, P)$ un morphisme de R-modules. Alors l'application :

$$\begin{array}{rcl} M \times N & \longrightarrow & P \\ (m, n) & \longmapsto & f(m)(n) \end{array}$$

est bilinéaire.

Il existe bien sûr des fonctions de deux variables sur les modules qui ne sont pas bilinéaires. Par exemple si M est un R-module, alors l'addition :

$$\begin{array}{rcl} M \times M & \longrightarrow & M \\ (m_1, m_2) & \longmapsto & m_1 + m_2 \end{array}$$

n'est pas bilinéaire puisqu'en général :

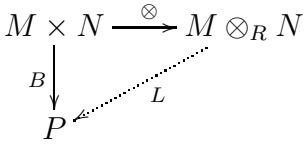
$$(m_1 + m_2) + m \neq (m_1 + m) + (m_2 + m).$$

Les applications multilinéaires généralisent les applications bilinéaires. Une application $f : M_1 \times \ldots \times M_k \longrightarrow P$ est multilinéaire si elle est linéaire en chaque variable, les autres étant considérées comme des constantes. Contrairement aux morphismes de modules, les applications bilinéaire (et multilinéaires) n'ont pas de noyau (car $M \times N$ n'est pas un module en général) et leurs images ne forment pas de sous-modules (de P).

3.2 Définition et construction du produit tensoriel

Définition 18 *Soient M et N deux R-modules. On appelle produit tensoriel de M et N (sur R), un R-module noté $M \otimes_R N$ muni d'une application*

bilinéaire $\otimes : M \times N \longrightarrow M \otimes_R N$ *telle que pour toute application bilinéaire* $B : M \times N \longrightarrow P$, *il existe un morphisme unique* $L : M \otimes_R N \longrightarrow P$ *qui rend le diagramme suivant commutatif*



i.e $B = L \circ \otimes$.

Nous allons montrer que le produit tensoriel existe toujours et est unique (à isomorphisme prés).

Si X est un ensemble, le groupe abélien libre sur X est le groupe :

$$F(X) = \bigoplus_{x \in X} \mathbb{Z}$$

C'est l'ensemble des sommes finies $\sum_{i=1}^{k} n_i x_i$ avec $x_i \in X$ et $n_i \in \mathbb{Z}$. Si $Y \subset X$, le sous-groupe de $F(X)$ engendré par Y est l'ensemble des sommes finies $\sum_{i=1}^{k} n_i y_i$ avec $y_i \in Y$ et $n_i \in \mathbb{Z}$. Pour M et N deux R-modules, on applique cette définition à $X = M \times N$ pour obtenir le groupe abélien libre $F(M \times N)$. Ses éléments sont les sommes finies $\sum_{i=1}^{k} a_i(m_i, n_i)$ avec $a_i \in \mathbb{Z}, m_i \in M$ et $n_i \in N$. Soit $G \subset F(M \times N)$ le sous-groupe engendré par les éléments de la forme :

- $(m + m^{'}, n) - (m, n) - (m^{'}, n)$.
- $(m, n + n^{'}) - (m, n) - (m, n^{'})$.
- $(r.m, n) - (m, r.n)$.

avec $m, m^{'} \in M, n, n^{'} \in N$ et $r \in R$. Posons :

$$M \otimes_R N = \frac{F(M \times N)}{G}$$

La classe d'équivalence de (m, n) modulo G sera notée $m \otimes n$:

$$m \otimes n = \overline{(m, n)} = (m, n) \mod G$$

L'application quotient :

$$F(M \times N) \longrightarrow M \otimes_R N$$

sera notée π. On a $\pi(m, n) = m \otimes n$ et bien sûr $\pi(G) = 0$.

Proposition 10 *Le groupe abélien $M \otimes_R N$ est engendré par les éléments de la forme $M \otimes n$ avec $m \in M$ et $n \in N$. Ces éléments satisfont aux relations :*

- $(m + m^{'}) \otimes n = m \otimes n + m^{'} \otimes n$.
- $m \otimes (n + n^{'}) = m \otimes n + m \otimes n^{'}$.
- $r.m \otimes n = m \otimes r.n$.

De plus $M \otimes_R N$ est un R-module.

Preuve : Les éléments $m \otimes n$ engendrent $M \otimes_R N$ car les éléments (m, n) engendrent $F(M \times N)$ et parce que l'application $F(M \times N) \longrightarrow M \otimes_R N$ est surjective. Les relations découlent de la définition de G. Par exemple

$$(m + m^{'}) \otimes n - m \otimes n - m^{'} \otimes n$$

$$= \pi((m + m^{'}, n) - (m, n) - (m^{'}, n)) = 0$$

car $(m + m^{'}) \otimes n - m \otimes n - m^{'} \otimes n \in G$, etc. D'autre part pour $r \in R$, on pose :

$$r(m \otimes n) = (r.m) \otimes n = m \otimes (r.n)$$

Ceci définit une opération de R sur $M \otimes_R N$ qui fait de celui-ci un R-module.

On peut maintenant énoncer le :

Théorème 2 *Le produit tensoriel de M et N (sur R) existe.*

Preuve : On pose :

$$M \otimes_R N = \frac{F(M \times N)}{G}$$

On a vu que c'est un R-module et on a une application bilinéaire :

$$\otimes : M \times N \longrightarrow M \otimes_R N$$

donnée par $\otimes(m, n) = m \otimes n$. Il reste à montrer que pour toute application bilinéaire $B : M \times N \longrightarrow P$, il existe un unique morphisme $L : M \otimes_R N \longrightarrow P$ tel que $B = L \circ \otimes$. Définissons L par $L(m \otimes n) = B(m, n)$. L est bien définie car B étant bilinéaire, elle s'annule sur $G \subset F(M \times N)$ et on a bien :

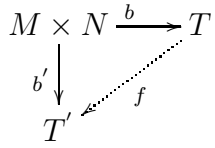
$$B(m, n) = L \circ \otimes(m, n) = L(m \otimes n))$$

Si $L^{'}$ est un autre morphisme tel que $B = L^{'} \circ \otimes$, on doit avoir $L(m \otimes n) = L^{'}(m \otimes n)$ et donc $L = L^{'}$. Ceci prouve l'unicité de L.

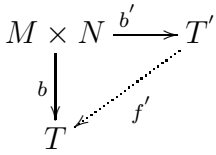
L'unicité du produit tensoriel est assuré par le :

Théorème 3 *Soient T et $T^{'}$ deux produits tensoriels de M et N (sur R). Alors T et $T^{'}$ sont isomorphes.*

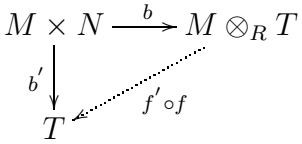
Preuve : Par hypothèse on a des applications bilinéaires $b : M \times N \longrightarrow T$ et $b^{'} : M \times N \longrightarrow T^{'}$ qui vérifient la propriété universelle du produit tensoriel et on a des diagrammes commutatifs :



et



avec T produit tensoriel dans le premier et $T^{'}$ produit tensoriel dans le second. Remarquer l'existence des applications $f : T \longrightarrow T^{'}$ et $f^{'} : T^{'} \longrightarrow T$. En combinant ces deux diagrammes, on en obtient un nouveau :



Comme f et $f^{'}$ sont uniques, on doit avoir $f^{'} \circ f = Id_T$. De même $f \circ f^{'} = Id_{T'}$ et donc f nous fournit un isomorphisme $T \cong T^{'}$.

En combinant ces deux théorèmes on obtient :

Théorème 4 *Le produit tensoriel $M \otimes_R N$ de deux R-modules M et N existe toujours et est unique à isomorphisme prés.*

Les éléments de $M \otimes_R N$ sont appelés des tenseurs et sont combinaisons linéaires des $m \otimes n$ qu'on appelle des tenseurs élémentaires. Tout élément $x \in M \otimes_R N$ s'écrit donc :

$$x = \sum_{i=1}^{k} a_i m_i \otimes n_i$$

avec $a_i \in \mathbb{Z}, m_i \in M$ et $n_i \in N$.
Exemple
1) Dans $M \otimes_R N$, on a $m \otimes 0 = 0$ et $0 \otimes n = 0$. En effet :

$$m \otimes 0 = m \otimes (0 + 0) = m \otimes 0 + m \otimes 0$$

et donc $m \otimes 0 = 0$. On montre de même que $0 \otimes n = 0$.
2) Soit A un groupe abélien dont tout élément est d'ordre fini. Regardons A comme un $\mathbb{Z}$-module. Alors on a :

$$\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$$

En effet soit $a \in A$ et soit $n \in \mathbb{N}$ tel que $na = 0$. Alors on a dans $\mathbb{Q} \otimes_{\mathbb{Z}} A$:

$$r \otimes a = n(\frac{r}{n}) \otimes a = \frac{r}{n} \otimes na = \frac{r}{n} \otimes 0 = 0$$

3) $m \otimes n = 0$ si et seulement si toute application bilinéaire sur $M \times N$ s'annule en (m, n).
4) $M \otimes_R N = 0$ si et seulement si toute application bilinéaire sur $M \times N$ est nulle.

Pour finir cette section remarquons que le produit tensoriel se généralise à un nombre quelconque de modules. Si $M_1, \ldots, M_k$ sont des R-modules, leur produit tensoriel $M_1 \otimes_R \ldots \otimes_R M_k$ est un R-module qui vérifie une propriété universelle concernant les applications multilinéaires : Pour toute application multilinéaire $B : M_1 \times \ldots \times M_k \longrightarrow P$ vers un R-module P, il existe un unique morphisme $L : M_1 \otimes_R \ldots \otimes_R M_k \longrightarrow P$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} M_1 \times \ldots \times M_k & \xrightarrow{\otimes} & M_1 \otimes_R \ldots \otimes_R M_k \\ {\scriptstyle B}\downarrow & \swarrow_{L} & \\ P & & \end{array}$$

L'image de $(m_1, \ldots, m_k)$ par $\otimes$ est notée $m_1 \otimes \ldots \otimes m_k$. La construction de $M_1 \otimes_R \ldots \otimes_R M_k$ se fait de la même manière que dans le cas de deux modules. Nous laissons les détails au lecteur.

3.3 Exemples de produit tensoriel

Pour illustrer la théorie générale, on présente ici quelques exemples de produit tensoriel.

Exemple 1
Soient a et b deux entiers positifs et soit $d = pgcd(a, b)$. Les groupes abéliens $\frac{\mathbb{Z}}{a\mathbb{Z}}$ et $\frac{\mathbb{Z}}{b\mathbb{Z}}$ peuvent-être vus comme des $\mathbb{Z}$-modules. On a alors un isomorphisme de groupes abéliens :

$$\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}} \cong \frac{\mathbb{Z}}{d\mathbb{Z}}$$

En particulier

$$\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}} = 0 \Longleftrightarrow pgcd(a, b) = 1$$

Preuve : $\frac{\mathbb{Z}}{a\mathbb{Z}}$ et $\frac{\mathbb{Z}}{b\mathbb{Z}}$ sont tous deux engendrés par 1. Donc $1 \otimes 1$ engendre $\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}}$. On a :

$$a(1 \otimes 1) = a \otimes 1 = 0 \otimes 1 = 0$$

$$b(1 \otimes 1) = 1 \otimes b = 1 \otimes 0 = 0$$

Donc l'ordre de $1 \otimes 1$ divise a et b et donc aussi $d = pgcd(a, b)$. Ainsi :

$$\#(\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}}) \leq d.$$

Soit l'application bilinéaire :

$$B : \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{d\mathbb{Z}}$$

définie par $B(x \mod a, y \mod b) = xy \mod d$. Par la propriété universelle du produit tensoriel, il existe un unique morphisme :

$$f : \frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{d\mathbb{Z}}$$

tel que $f(x \otimes y) = xy$. En particulier $f(x \otimes 1) = x$ et donc f est surjective. Le produit tensoriel a ainsi au moins d éléments.
Par exemple :

$$\frac{\mathbb{Z}}{3\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{5\mathbb{Z}} = 0.$$

Exemple 2
Soit R un anneau (commutatif) et soient I et J deux idéaux de R. Les anneaux quotients $\frac{R}{I}$ et $\frac{R}{J}$ sont des R-modules de manière naturelle et on a :

$$\frac{R}{I} \otimes_R \frac{R}{J} \cong \frac{R}{I + J}$$

Preuve : Soit l'application bilinéaire :

$$B : \frac{R}{I} \times \frac{R}{J} \longrightarrow \frac{R}{I+J}$$

définie par $B(x \mod I, y \mod J) = xy \mod I+J$. Par la propriété universelle du produit tensoriel, il existe un unique morphisme

$$f : \frac{R}{I} \otimes_R \frac{R}{J} \longrightarrow \frac{R}{I+J}$$

tel que $f(x \otimes y) = xy$. Nous allons montrer que f est l'isomorphisme recherché. Pour cela considérons l'application :

$$g : R \longrightarrow \frac{R}{I} \otimes_R \frac{R}{J}$$

donnée par $g(r) = r.(\overline{1} \otimes \overline{1})$. g est linéaire. De plus on a :

$$r \in I \Longrightarrow g(r) = r.(\overline{1} \otimes \overline{1}) = \overline{r} \otimes \overline{1} = \overline{0} \otimes \overline{1} = 0$$

$$r \in J \Longrightarrow g(r) = r.(\overline{1} \otimes \overline{1}) = \overline{1} \otimes \overline{r} = \overline{1} \otimes \overline{0} = 0$$

donc $I + J \in Ker(g)$ et g passe au quotient :

$$g : \frac{R}{I+J} \longrightarrow \frac{R}{I} \otimes_R \frac{R}{J}$$

avec $g(r \mod I+J) = r.(\overline{1} \otimes \overline{1}) = \overline{r} \otimes \overline{1} = \overline{1} \otimes \overline{r}$. Montrons que g est l'inverse de f. On a

$$f(g(r \mod I+J)) = f(\overline{r} \otimes \overline{1}) = r \mod I+J$$

et donc $f \circ g = Id_{\frac{R}{I+J}}$ Pour calculer $g \circ f$, remarquons que tout tenseur élémentaire $\overline{x} \otimes \overline{y}$ s'écrit :

$$\overline{x} \otimes \overline{y} = x.\overline{1} \otimes y.\overline{1} = xy.(\overline{1} \otimes \overline{1}) = r.(\overline{1} \otimes \overline{1})$$

et donc

$$g(f(r.(\overline{1} \otimes \overline{1})) = r.g(1 \mod I+J) = r.(\overline{1} \otimes \overline{1})$$

Ainsi $g \circ f = Id_{\frac{R}{I} \otimes_R \frac{R}{J}}$.
En prenant $I = J = 0$, on obtient un isomorphisme :

$$R \otimes_R R \cong R$$

Remarquer aussi que si on prend $R = \mathbb{Z}, I = a\mathbb{Z}$ et $J = b\mathbb{Z}$, on retrouve l'exemple précédent.

Exemple 3

Soient R un anneau et I un idéal de R. $\frac{R}{I}$ est un R-module. Si M est un R-module, alors on a un isomorphisme :

$$\frac{R}{I} \otimes_R M \cong \frac{M}{IM}$$

Preuve : Soit l'application bilinéaire :

$$B : \frac{R}{I} \times M \longrightarrow \frac{M}{IM}$$

définie par $B(\overline{r}, m) = \overline{r.m}$. Par la propriété universelle du produit tensoriel, il existe un unique morphisme :

$$f : \frac{R}{I} \otimes_R M \longrightarrow \frac{M}{IM}$$

tel que $f(\overline{r} \otimes m) = \overline{r.m}$. Montrons que f est un isomorphisme. Soit l'application :

$$g : M \longrightarrow \frac{R}{I} \otimes_R M$$

donnée par $g(m) = \overline{1} \otimes m$. g est linéaire en m et IM est engendré par les $r.m$ pour $r \in I$ et $m \in M$ et on a :

$$g(r.m) = \overline{1} \otimes r.m = \overline{r} \otimes m = \overline{0} \otimes m = 0$$

Donc g annule IM et passe au quotient :

$$g : \frac{M}{IM} \longrightarrow \frac{R}{I} \otimes_R M$$

avec $g(\overline{m}) = \overline{1} \otimes m$. On a :

$$f(g(\overline{m})) = f(\overline{1} \otimes m) = \overline{1.m} = \overline{m}$$

et donc $f \circ g = Id_{\frac{M}{IM}}$. Pour calculer $g \circ f$, remarquons que tout tenseur de $\frac{R}{I} \otimes_R M$ est de la forme $\overline{1} \otimes m$. En effet un tenseur élémentaire est de la forme $\overline{r} \otimes m = \overline{1} \otimes r.m$ et tout tenseur est somme de tenseurs élémentaires $\sum_i \overline{1} \otimes m_i = \overline{1} \otimes \sum_i m_i$. On a alors

$$g(f(\overline{1} \otimes m)) = g(\overline{m}) = \overline{1} \otimes m$$

et donc $g \circ f = Id_{\frac{R}{I} \otimes_R M}$.
En particulier si $I = (0)$, on obtient un isomorphisme :

$$R \otimes_R M \cong M$$

et si $R = M$, on retrouve l'isomorphisme de l'exemple précédent :

$$R \otimes_R R \cong R.$$

Exemple 4
Soient M, N et P des R-modules. Alors on a des isomorphimes :

$$M \otimes_R N \cong N \otimes_R M$$

et

$$(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$$

Preuve : On procède de la même manière que dans les exemples précédents en utilisant toujours la propriété universelle du produit tensoriel. Disons simplement que les deux isomorphismes sont donnés respectivement par :

$$m \otimes n \longmapsto n \otimes m$$

et

$$(m \otimes n) \otimes p \longmapsto m \otimes (n \otimes p)$$

3.4 Extension de la base

Soit $f : R \longrightarrow S$ un morphisme d'anneaux commutatifs. Soit N un S-module. On peut utiliser f pour regarder N comme un R-module en posant :

$$r.n = f(r).n$$

pour $r \in R$ et $n \in N$. En particulier S lui-même est un R-module en posant :

$$r.s = f(r)s$$

pour $s \in S$. Cette opération du passage d'un S-module à un R-module est souvent appelée la restriction des scalaires et tire son nom du cas particulier où f est une inclusion (R est un sous-anneau de S) : $R \subset S$. Par exemple, en utilisant l'inclusion $\mathbb{R} \subset \mathbb{C}$ tout module (espace vectiel) sur $\mathbb{C}$ est aussi un module (espace vectoriel) sur $\mathbb{R}$.

Le processus inverse i.e le passage d'un R-module à un S-module est appelé l'extension des scalaires ou l'extension de la base. Soit M un R-module. Si $f : R \longrightarrow S$ est un morphisme d'anneaux, S devient un R-module via $f : r.s = f(r)s$. On peut donc parler du produit tensoriel $S \otimes_R M$ qui est un R-module.

Proposition 11 *Le groupe additif $S \otimes_R M$ a une unique structure de S-module en posant :*

$$s^{'}.(s \otimes m) = s^{'}s \otimes m$$

$\forall s, s^{'} \in S$ et $\forall m \in M$. Cette structure de S-module est compatible avec la structure de R-module dans le sens que :

$$r.t = f(r).t$$

pour tout $r \in R$ et tout $t \in S \otimes_R M$

Preuve : On va se contenter d'exhiber l'opération $S \times S \otimes_R M \longrightarrow S \otimes_R M$. Pour tout $s^{'} \in S$, on considère l'application bilinéaire $S \times M \longrightarrow S \otimes_R M$ donnée par $(s, m) \longmapsto (s^{'}s) \otimes m$. Par la propriété universelle du produit tensoriel, il existe un unique morphisme $g_{s'} : S \otimes_R M \longrightarrow S \otimes_R M$ tel que $g_{s'}(s \otimes m) = (s^{'}s) \otimes m$. On définit alors une opération de S sur $S \otimes_R M$ par $s^{'}.t = g_{s'}(t)$.

Définition 19 *$S \otimes_R M$ (en tant que S-module) est appelé l'extension des scalaires (de R à S) de M.*

Remarquons que de la même manière $M \otimes_R S$ est aussi un S-module et on a un isomorphisme :

$$S \otimes_R M \xrightarrow{\cong} M \otimes_R S$$

qui envoie $s \otimes m$ vers $m \otimes s$.

Exemple

En utilisant l'inclusion $\mathbb{R} \subset \mathbb{C}$, tout module (espace vectoriel) V sur $\mathbb{R}$ devient un module (espace vectoriel) $V \otimes_{\mathbb{R}} \mathbb{C}$ sur $\mathbb{C}$. Si $V = \mathbb{R}^n$, alors on a :

$$\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}^n.$$

Si $M_n(\mathbb{R})$ est l'espace vectoriel réel des matrices d'ordre n sur $\mathbb{R}$, alors on a aussi un isomorphisme :

$$M_n(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} \cong M_n(\mathbb{C}).$$

Bibliographie

[1] S.Lang, Algebra, third edition, Springer, 2002.

[2] M.F.Atiyah, L.G.Macdonald, Introduction to commutative algebra, Addison-Wesley, 1969.

[3] N.Bourbaki, Eléments de Mathématiques, Algèbre, Hermann, Paris, 1965.

[4] B.L.Van Der Waerden, Modern algebra, Volume I, II, Frederick Ungar publishing Co, New York, 2008.