

Chapitre 1

Modules sur anneau principal

1.1 Anneaux et morphismes

Définition 1.1.

Un anneau est un triplet $(A, +, \times)$ vérifiant :

- $(A, +)$ est un groupe abélien (de neutre 0).
- La multiplication \times est associative c'est à dire pour tous $a, b, c \in A$, $a(bc) = (ab)c$.
- La multiplication \times est distributive par rapport à l'addition $+$ c'est à dire; pour tous $a, b, c \in A$, $(a + b) \times c = a \times c + b \times c$ et $a \times (b + c) = a \times b + a \times c$.

L'anneau A est dit unitaire si \times admet un élément neutre appelé unité et se note 1_A ou 1.

L'anneau A est dit commutatif si la multiplication \times est commutative.

Notation : Si $a, b \in A$, l'élément $a \times b$ sera noter ab .

Dans ce qui suit on ne considère que les anneaux commutatifs unitaires, ainsi par anneau on désigne un anneau commutatif unitaire.

Soit $(A_i)_{i \in I}$ une famille d'anneaux. On muni le produit cartésien $\prod_{i \in I} A_i$ des deux lois :

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}, \quad (x_i)_{i \in I} (y_i)_{i \in I} = (x_i y_i)_{i \in I}$$

Alors $(\prod_{i \in I} A_i, +, \times)$ est un anneau (commutatif unitaire) dit anneau produit direct des anneaux A_i , $i \in I$.

Un anneau trivial est un anneau réduit à un singleton, dans ce cas $1 = 0$.

Un cas particulier : Si A_1, \dots, A_m sont des anneaux commutatifs unitaires alors $\prod_{i=1}^m A_i = A_1 \times \dots \times A_m$ est un anneau commutatif.

Soit A un anneau et $a \in A$. On dit que a est inversible s'il existe $b \in B$ tel que $ab = 1$. Si c'est le cas l'élément b est unique et se note a^{-1} . L'ensemble des éléments inversibles de A se note A^\times ou $U(A)$ appelé groupe des unités. On vérifie facilement que A^\times est un groupe (muni de la multiplication).

Définition 1.2.

Un anneau A est dit intègre si

1. *A non trivial ($1 \neq 0$),*
2. *Pour tous $x, y \in A$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$.*

Exemples :

1. \mathbb{Z}
2. $\mathbb{R}[X]$

Définition 1.3.

Un corps est un anneau A tel que

1. *A non trivial ($1 \neq 0$),*
2. *$A^\times = A \setminus \{0\}$.*

Remarque : Un corps est un anneau non trivial dans lequel tout élément non nul est inversible.

Si A est un corps alors il est intègre.

Exemples :

1. \mathbb{R}, \mathbb{Q} et \mathbb{C} sont des corps.
2. $\mathbb{R}(X)$ est un corps.

Définition 1.4.

Soit A un anneau et B une partie de A . On dit que B est un sous anneau de A si $(B, +)$ est un sous groupe de $(A, +)$, B stable par la multiplication et $1 \in B$.

Exemple : \mathbb{Z} est un sous anneau de \mathbb{R} .

$\mathbb{Z}[X] := \{\sum_{k=0}^n a_k X^k \mid n \in \mathbb{N}, a_k \in \mathbb{Z}\}$ est un sous anneau de $\mathbb{R}[X]$.

Définition 1.5.

Soit A, B deux anneaux et $f : A \rightarrow B$ une application. On dit que f est un morphisme d'anneaux si : pour tout $x, y \in A$, $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1) = 1$.

Si $f : A \rightarrow B$ est un morphisme d'anneaux alors $f(0) = 0$, $f(x-y) = f(x) - f(y)$ et si de plus x est un élément inversible de A alors $f(x)$ est aussi inversible dans B . Un morphisme d'anneaux $f : A \rightarrow B$ est un isomorphisme si de plus il est bijectif. Deux anneaux sont isomorphes, lorsqu'il existe un isomorphisme entre eux.

1.2 Idéaux

Définition 2.1.

Soit A un anneau et I une partie de A . On dit que I est un idéal de A si ;

1. I est un sous groupe de $(A, +)$,
2. $\forall a \in A, \forall x \in I, ax \in I$.

Remarque :

1. $\{0\}$ et A sont des idéaux de A .
2. Si I est un idéal de A contenant un élément inversible alors $I = A$.
3. Un anneau A (non trivial) est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A .

Proposition 2.2.

Soit A un anneau.

- Si I et J sont des idéaux de A alors $I+J := \{x+y \mid (x, y) \in I \times J\}$ est un idéal de A appelé la somme de I et J .
- Si $(I_\alpha)_{\alpha \in \Gamma}$ est une famille d'idéaux de A alors $\cap_{\alpha \in \Gamma} I_\alpha$ est un idéal de A , autrement dit une intersection quelconque d'idéaux de A .

est un idéal de A .

Proof :

Soit S une partie de A . L'intersection de tous les idéaux de A contenant S est appelé l'idéal engendré par S et se note (S) . Ainsi

$$(S) = \bigcap_{I \text{ idéal de } A} I$$

Proposition 2.3.

Mq

Soit A un anneau et S une partie non vide de A .

- $(S) = \{ \sum_{i=1}^m a_i s_i \mid m \geq 1, a_i \in A, s_i \in S \}$
- $(\emptyset) = \{0\}$.

Proof :

Remarque: Si $S = \{s_1, \dots, s_n\}$, alors $(S) = \{ \sum_{i=1}^n a_i s_i \mid a_i \in A \}$ il se note aussi (s_1, \dots, s_n) .

Définition 2.4.

Soit A un anneau.

1. Soit I, J deux idéaux de A . Le produit de I et J noté IJ est l'idéal engendré par les éléments de la forme ab où $a \in I$ et $b \in J$.
2. Soit $(I_\alpha)_{\alpha \in \Gamma}$ une famille d'idéaux. La somme des idéaux I_α , $\alpha \in \Gamma$, est l'idéal engendré par $\bigcup_{\alpha \in \Gamma} I_\alpha$ on le note $\sum_{\alpha \in \Gamma} I_\alpha$

Les éléments de IJ sont de la forme $\sum_{k=1}^m a_k b_k$ où les $a_k \in I$ et les $b_k \in J$.

Les éléments de $\sum_{\alpha \in \Gamma} I_\alpha$ sont de la forme $\sum_{\alpha \in \Gamma} a_\alpha$ où $a_\alpha \in I_\alpha$ sont tous nuls sauf peut être un nombre fini d'entre eux.

On définit d'une manière analogue le produit d'un nombre fini d'idéaux I_1, \dots, I_m , comme étant l'idéal engendré par les éléments de la forme $a_1 \cdots a_m$ où $a_k \in I_k$.

Définition 2.5.

Soit A un anneau et I un idéal de A .

1. On dit que I est un idéal principal s'il est engendré par un élément, c'est à dire $I = (a)$, où $a \in A$.
2. On dit que I est un idéal de type fini s'il est engendré par un ensemble fini c'est à dire $I = (a_1, \dots, a_n)$ où $a_1, \dots, a_n \in A$.

Exemples :

1. Dans l'anneau $\mathbb{Z}[X]$, l'idéal $I = \{P \in \mathbb{Z}[X] / P(0) = 0\}$ est principal. En effet $I = (X)$.
2. Si I et J sont des idéaux de type fini alors IJ et $I + J$ sont de type fini.

Définition 2.6.

Un anneau est dit principal¹ s'il est intègre et tous ses idéaux sont principaux.

Soit I un idéal de A . Le groupe quotient A/I hérite d'une multiplication définie de manière unique de A qui en fait un anneau commutatif unitaire ($\bar{x} \bar{y} = \bar{xy}$). De plus l'application $\pi : A \rightarrow A/I$ définie par $\pi(x) = \bar{x}$ est un morphisme d'anneaux (surjectif).

Proposition 2.7.

Soit A un anneau et I un idéal de A . Le morphisme $\pi : A \rightarrow A/I$ induit une bijection entre les idéaux de A/I et les idéaux de A contenant I .

Proof :

Proposition 2.8.

Soit $f : A \rightarrow B$ un morphisme d'anneaux.

1. Si J est un idéal de B alors $f^{-1}(J)$ est un idéal de A . En particulier $\ker f$ est un idéal de A .
2. $\text{Im } f$ est un sous anneau de B .

1. Il est dit quasi-principal si tous ses idéaux sont principaux (sans condition intègre).

Proof :

Théorème 2.9. (théorème d'isomorphisme)

Soit $f : A \rightarrow B$ un morphisme d'anneaux. L'application

$$\bar{f} : A/\ker f \rightarrow \text{Im } f, \quad \bar{f}(\bar{x}) = f(x)$$

est (bien définie et c'est) un isomorphisme

Proof :

1.3 Idéaux premiers et idéaux maximaux

Définition 3.1.

Soit A un anneau.

1. Un idéal P de A est dit premier si $P \neq A$ et $\forall x, y \in A, xy \in P \Rightarrow x \in P$ ou $y \in P$.
2. Un idéal M de A est dit maximal s'il n'existe pas d'idéal I de A tel que $M \subset I \subset A$ (inclusions strictes).

L'ensemble des idéaux premiers de A s'appelle le spectre premier de A et se note $\text{Spec}(A)$ et celui des idéaux maximaux de A s'appelle le spectre maximal de A et se note $\text{MaxSpec}(A)$ ou $\text{Max}(A)$.

Définition 3.2.

Soit A un anneau.

1. Un idéal P est premier si et seulement si A/P est intègre.
2. Un idéal M est maximal si et seulement si A/M est un corps.

Proof :

Proposition 3.3.

1. Tout idéal maximal est premier.
2. Soit $f : A \rightarrow B$ un morphisme d'anneaux. Si P est un idéal pre-

mier de B alors $f^{-1}(P)$ est un idéal premier de A .

Proof :

Théorème 3.4. (de Krull)

Soit A un anneau non trivial c'est à dire $A \neq 0$, alors $\text{Max}(A) \neq \emptyset$. Autrement dit A contient au moins un idéal maximal.

Proof :

Corollaire 3.5.

Soit A un anneau.

1. Tout idéal propre (i.e $\neq A$) de A est contenu dans un idéal maximal.
2. Si $a \in A$ est non inversible alors a appartient à un idéal maximal.

Proof :

Remarque : Une conséquence immédiate du Corollaire précédent est que

$$A^\times = A \setminus \left(\bigcup_{M \in \text{Max}(A)} M \right)$$

1.4 Modules

Définition 4.1.

Soit A un anneau commutatif. Un A -module ou module sur A est un triplet $(M, +, .)$ tel que;

1. $(M, +)$ est un groupe abélien.
2. $\therefore A \times M \rightarrow M, (a, m) \mapsto a.m$ est une loi externe sur M de base A vérifiant les propriétés suivantes; pour tous $a, b \in A, m, m' \in M$,
 - $a.(m + m') = a.m + a.m'$
 - $(a + b).m = a.m + b.m$

- $(ab).m = a.(b.m)$
- $1.m = m$

Remarque : Les modules peuvent être vus comme une généralisation des espaces vectoriels. En effet un \mathbb{K} -module sur un corps commutatif \mathbb{K} est tout simplement un \mathbb{K} -espace vectoriel.

Exemples :

1. Soit G un groupe abélien. Alors G est naturellement un \mathbb{Z} -module où la multiplication externe “.” est définie par $\mathbb{Z} \times G \rightarrow G$, $(n, g) \mapsto ng$.
2. Si I est un idéal de A alors I est naturellement un A -module.
3. Si I est un idéal de A alors A/I est un A -module.

Définition 4.2.

Soient M et N deux A -modules et $f : M \rightarrow N$ une application. On dit que f est un morphisme de A -modules si, pour tous $a \in A$, $m, m' \in M$;

1. $f(m + m') = f(m) + f(m')$.
2. $f(am) = af(m)$.

Exemples :

1. Soit I un idéal de A . L'application $s : A \rightarrow A/I$, $x \mapsto s(x) = \bar{x}$ est un morphisme de A -modules.
2. Un morphismes de groupes abéliens est un morphisme de \mathbb{Z} -modules.

Le composé de deux morphismes de A -modules est un morphisme de A -modules. L'ensemble de tous les morphismes de A -modules de M dans N est un A -module, où pour f, g deux morphismes de A -modules et $a \in A$, $(f + g)(x) = f(x) + g(x)$ et $(af)(x) = af(x)$. On note $\text{Hom}_A(M, N)$ ou simplement $\text{Hom}(M, N)$ le A -module des morphismes de A -modules de M dans N .

Définition 4.3. (A -algèbre)

Soit A un anneau. Une A -algèbre est un quadruplet $(B, +, \times, .)$ tels que;

1. $(B, +, \times)$ est un anneau,