Master Mathématiques Appliquées et Ingénierie de l'Enseignement

Mohamed Aqalmoun

Algèbra de base et applications

Module *M*

Cahier-Cours

ENS-MEKNÈS

Avant-propos

Ce cahier-cours (version $\frac{1}{2}$-cours) est destiné aux étudiants de première année du master mathématiques appliquées et ingénierie de l'enseignement de l'école normale supérieure de Meknès. Il propose un cours non complet (sans démonstrations) de l'algèbre de base.

Table des matières

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 $\prod_{i\in} A_i$ des deux lois :

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

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 $A_1,\ldots,A_m$ sont des anneaux commutatifs unitaires alors $\prod_{i=1}^{m} A_i = A_1 \times \ldots \times A_m$ 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 $x, y \in A$, $xy = 0 \Longrightarrow x = 0$ 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 $\mathbb{R}$.
$\mathbb{Z}[X] := \{\sum_{k=0}^{n} a_k X^k \ / \ n \in \mathbb{N}, a_k \in \mathbb{Z}\}$ est un sous anneau de $\mathbb{R}[X]$.

Définition 1.5.

Soit A, B deux anneaux et $f : A \to B$ 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 $f : A \to B$ 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 $f : A \to B$ 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 $I + J := \{x + y \ / \ (x, y) \in I \times J\}$ 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

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

Proposition 2.3.

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

— $(S) = \{\sum_{i=1}^{m} a_i s_i \ / \ m \geq 1,\ a_i \in A, s_i \in S\}$

— $(\emptyset) = \{0\}$.

Proof : .....

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

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 saut peut être un nombre fini d'entre eux.
On définit d'une manière analogue le produit d'un nombre fini d'idéaux $I_1, \ldots, I_m$, 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 principal[1] *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 ($\overline{x}\ \overline{y} = \overline{xy}$). De plus l'application $\pi : A \to A/I$ définie par $\pi(x) = \overline{x}$ est un morphisme d'anneaux (surjectif).

Proposition 2.7.

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

Proof : .....

Proposition 2.8.

Soit $f : A \to B$ 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. $\mathrm{Im} f$ *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 $f : A \to B$ un morphisme d'anneaux. L'application

$$\overline{f} : A/\ker f \to \mathrm{Im} f, \quad \overline{f}(\overline{x}) = f(x)$$

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

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 $f : A \to B$ 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 a dire $A \neq 0$, alors $\mathrm{Max}(A) \neq \emptyset$. 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

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

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. *$. : A \times M \to M, (a,m) \mapsto a.m$ 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 $\mathbb{Z} \times G \to G$, $(n, g) \mapsto ng$.
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 $f : M \to N$ 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 $s : A \to A/I$, $x \mapsto s(x) = \overline{x}$ 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 Nest 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 $\mathrm{Hom}_A(M, N)$ ou simplement $\mathrm{Hom}(M, N)$ 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,*

2. $(B,+,.)$ *est un* A*-module,*
3. $a(xy) = (ax)y = x(ay)$, $\forall a \in A, x, y \in B$.

Exemples : Soit A un anneau.

1. A est naturellement une $\mathbb{Z}$-algèbre.
2. $A[X]$ est une A-algèbre.
3. Soit $f : A \to B$ un morphisme d'anneaux. Alors B est un A-module ($a.b := f(a)b$), plus précisément c'est une A-algèbre.

Définition 4.4.

Soit M un A-module et N une partie de M. On dit que N est un sous module de M si ;

1. *N est un sous groupe de M,*
2. *$\forall a \in A, \forall n \in N, an \in N$.*

Remarque : Si N est un sous module de M, alors N lui même est un A-module.

Exemples :

1. Si I est un idéal de A, alors I est un sous module de A.
2. Soit $f : M \to N$ un morphisme de A-modules. Alors $\ker f$ est un sous module de M et $\mathrm{Im} f$ est un sous module de N.
3. Si $x \in M$, alors $\{ax \,/\, a \in A\}$ est un sous module de M et il se note Ax.

Proposition 4.5.

Soit M un A-module.

1. *Si $(N_i)_{i\in I}$ est une famille de sous modules de M, alors $\cap_{i\in I} N_i$ est un sous module de M.*
2. *Si N et N' sont des sous modules de M, alors $N+N'$ est un sous module de M, où $N+N' = \{x+y \,/\, x \in N, y \in N'\}$.*

Proof : .....

Soit M un A-module et N un sous module de M. Alors M/N est un groupe abélien où l'addition est définie par;

$$\overline{x}+\overline{y}=\overline{x+y}\ ,\ x,y\in M$$

C'est aussi un A-module muni de la multiplication externe suivante;

$$a\overline{x}=\overline{ax}\ ,\ a\in A, x\in M.$$

de plus l'application $s: M\to M/N$ définie par $s(x)=\overline{x}$ est un morphisme de A-modules surjectif.

Théorème 4.6. (Théorème d'isomorphisme)

Soit $f: M\to M'$ un morphisme de A-modules. Alors f induit un isomorphisme $\overline{f}: M/N\to \mathrm{Im}f$ où $\overline{f}(\overline{x})=f(x)$.

Proof : .....

Sous module engendré par une famille :

Définition 4.7.

Soit M un A-module et $(x_i)_{i\in I}$ une famille d'éléments de M. Le sous module engendré par la famille $(x_i)_{i\in I}$ est l'intersection de tous les sous modules de M contenant les éléments de la famille $(x_i)_{i\in I}$, il se note $(x_i, i\in I)$. C'est le plus petit (au sens de l'inclusion) sous module de M contenant les éléments de la famille $(x_i)_{i\in I}$.

Proposition 4.8.

Soit M un A-module et $(x_i)_{i\in I}$ une famille d'éléments de M. Alors

$$(x_i, i\in I)=\{\sum_{j\in J} a_j x_j\ \ /\ J \text{ partie finie de } I, a_j\in A\}$$

Proof : .....On pose $N'=\{\sum_{j\in J} a_j x_j\ \ /\ J$ partie finie de $I, a_j\in A\}$. Il suffit de démontrer que N' est le plus petit (au sens de l'inclusion) sous module de M contenant les x_i, $i\in I$. Il clear que $0\in N'$. Soient $x,y\in N'$ et $a\in A$. Par définition $x=\sum_{j\in J} a_j x_j$ et $y=\sum_{j\in J'} b_j x_j$ où $a_j, b_j\in A\in$, J et J' sont des parties finies de I.

On a $x+ay=\sum_{j\in J}a_jx_j+\sum_{j\in J}aa_jx_j=\sum_{j\in J\cup J'}a'_jx_j$ où

$$a'_j=\begin{cases}a_j & \text{si} \quad j\in J-J'\\ a_j+ba'_j & \text{si} \quad j\in J\cap J'\\ aa'_j & \text{si} \quad j\in J'-J\end{cases}$$

Ainsi $x+ay\in N'$. Il est clair que N' contient les x_i ; en effet $x_i=\sum_{j\in\{i\}}1.x_j\in N'$.

Soit maintenant N un sous module de M contenant les x_i. Si $x\in N'$, alors $x=\sum_{j\in J}a_jx_j$ où J est une partie finie de I, puisque x est une combinaison d'éléments de N, c'est bien que $x\in N$. Ainsi $N'\subseteq N$. On en déduit que $(x_i;i\in I)=N'$.

Exemples : Soit M un A-module.

1. Soit $x\in M$. Le sous module engendré par x est le sous module Ax.
2. Si $x_1,\dots,x_n\in M$, alors $(x_1,\dots,x_n)=\{a_1x_1+\dots+a_nx_n\ /\ a_i\in A,\ \text{pour } 1\leq i\leq n\}$.
3. Soit I un idéal de A et N un sous module de M. Si on note IN le sous module de M engendré par tous les éléments de la forme ax où $a\in I$ et $x\in N$, alors
$$IN=\left\{\sum_{i=1}^{n}a_ix_i\ /\ n\in\mathbb{N}^*,a_i\in I,x_i\in N\right\}$$

Remarque : Notons que si $(N_i)_{i\in I}$ est une famille de sous modules d'un A-module M, alors $\cup_{i\in I}N_i$ n'est pas (en général) un sous module de M.

Définition 4.9.

Soit M un A-module et $(N_i)_{i\in I}$ une famille de sous modules de M. La somme des sous modules N_i, $i\in I$ est le sous module engendré par tous les éléments de $\cup_{i\in I}N_i$, il se note $\sum_{i\in I}N_i$. Ainsi

$$\sum_{i\in I}N_i=(\cup_{i\in I}N_i)$$

Proposition 4.10.

Soit M un A-module et $(N_i)_{i\in I}$ une famille de sous modules de M. Alors

$$\sum_{i\in I} N_i = \left\{ \sum_{j\in J} x_j \ / \ J \text{ partie finie de } I, x_j \in N_j \right\}$$

Proof : ..... On posons $N' = \{\sum_{j\in J} x_j \ / \ J \text{ partie finie de } I, x_j \in N_j\}$, puis par un raisonnement analogue à celui de la démonstration de la proposition 1.4, on montre que N' est le plus petit sous module de M contenant $\cup_{i\in I} N_i$.

Remarques : Soit M un A-module.

1. Si $N_1, \ldots, N_n$ sont des sous modules de M, alors
$$\sum_{i=1}^{n} N_i = \{\sum_{i=1}^{n} x_i \ / \text{ pour } 1 \leq i \leq n, x_i \in N_i\}$$
2. Si $(x_i)_{i\in I}$ est une famille d'éléments de M, alors $\sum_{i\in I} Ax_i$ est le sous module engendré par la famille $(x_i)_{i\in I}$, autrement dit
$$\sum_{i\in I} Ax_i = (x_i, i \in I)$$

Définition 4.11.

Soit M un A-module. On dit que M est de type fini s'il existe $m_1, \ldots, m_r \in M$ tels que $M = (m_1, \ldots, m_r)$, autrement dit M est engendré par un nombre fini d'éléments.

Exemples :

1. Le $\mathbb{Z}$-module $\mathbb{Z}^2$ est de type fini.
2. Le A-module A^n est de type fini.

Définition 4.12.

Soit M un A-module et $(m_1, \ldots, m_r)$ une famille d'éléments de M. On dit que $(m_1, \ldots, m_r)$ est libre si pour tout $(\alpha_1, \ldots, a_r) \in A^r$, $\sum_{k=1}^{r} \alpha_k m_k =$

$0 \Longrightarrow \alpha_1 = \ldots = \alpha_r = 0$.
Une base de M est une famille qui est à la fois libre et génératrice M.
Un module M est dit libre s'il admet une base.
Le rang d'un module libre est le nombre d'éléments d'une base.

Exemple : Si A est un anneau, le A-module A^n est libre.

Théorème 4.13.

Soit A un anneau et M un A-module libre de rang r. Alors M est isomorphe à A^r.