Université Cadi Ayyad
Faculté Polydisciplinaire de Safi

Chapitre II : Les Modules

Algèbre commutative et Applications

SMA S6

Par :
Karmouni Mohammed

Année Universitaire : 2019-2020

Table des matières

Modules

Soit A un anneau unitaire.

Définition 0.1. *un A-module à gauche est un ensemble non vide muni*

1. *d'une loi de composition interne notée, en général, additivement et telle que $(M,+)$ est un groupe abélien ;*
2. *d'une loi de composition externe à opérateurs dans l'anneau A :*

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

vérifiant les conditions suivantes :

i) $\forall x \in M, \forall (a,b) \in A \times A,\ (a+b)x = ax + bx.$

ii) $\forall x \in M, \forall (a,b) \in A \times A,\ a.(bx) = (ab).x,$ *noté abx.*

iii) $\forall a \in A, \forall (x,y) \in M, \times M\ \ a(x+y) = ax + ay.$

iv) $\forall x \in M,\ 1_A x = x.$

On définit de même la notion de module à droite.

Définition 0.2. *un A-module à droite est un ensemble non vide muni*

1. *d'une loi de composition interne notée, en général, additivement et telle que $(M,+)$ est un groupe abélien ;*
2. *d'une loi de composition externe à opérateurs dans l'anneau A :*

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

vérifiant les conditions suivantes :

i) $\forall x \in M, \forall (a,b) \in A \times A,\ x.(a+b) = xa + xb.$

ii) $\forall x \in M, \forall (a,b) \in A \times A,\ (xb).a = x(ba),$ *noté xba.*

iii) $\forall a \in A, \forall (x,y) \in M, \times M\ \ (x+y)a = xa + ya.$

iv) $\forall x \in M,\ x1_A = x.$

Définition 0.3. *A et B étant deux anneaux unitaires, on dira que M est un $A-B$-bimodule, si M est à la fois un A-module à gauche et un B-module à droite vérifiant la condition :*

$$\forall x \in M, \forall (a,b) \in A \times B,\ (ax)b = a(xb),\ \text{noté } axb.$$

Lemme 0.4. *Si A est commutatif, alors A-module à droite est aussi un A-module à gauche, et réciproquement. Dans ce cas, on dit seulement que M est un A-module.*

Démonstration. Supposons que M est un A-module à droite, muni de la loi externe

$$\begin{array}{ccc} M \times A & \longrightarrow & M \\ (x,a) & \longrightarrow & x.a = ax. \end{array}$$

Montrons que ceci définit une structure de A-module à gauche sur M. On a $i), iii) et iv)$ sont évidents. Soient $a, b \in A$ et $x \in M$: $a.(bx) = a.(xb) = (xb).a = x(ba) = x(ab) = (ab)x$. La réciproque se démontre de façon analogue. □

Exemple 0.5. *1. Tout anneau unitaire A est un A-module à gauche et à droite ($a.x = ax$ et $x.a = xa$).*

2. Si $A := k$ est un corps, la structure de A-module est exactement celle de A-espace vectoriel. Les propriétés élémentaires des espaces vectoriels s'étendent aux A-modules ($0.x = 0$, $(-a)x = -ax$, ...).

3. Si $A = \mathbb{Z}$ et $(M, +)$ est un groupe abélien, M est muni d'une structure de $\mathbb{Z}$-module à travers la loi externe :

$$\begin{array}{ccc} \mathbb{Z} \times M & \longrightarrow & M \\ (n,x) & \longrightarrow & nx = \underbrace{x + ... + x}_{n fois}. \end{array}$$

Ainsi, il n'y a aucune différence entre la structure de $\mathbb{Z}$-module et celle du groupe abélien, par suite tout anneau unitaire A est un $\mathbb{Z}$-module à gauche, tout A-module à gauche est un $\mathbb{Z}$-module à gauche.

4. Si I est un idéal de A, alors I est un A-module à travers la loi externe :

$$\begin{array}{ccc} A \times I & \longrightarrow & I \\ (a,x) & \longmapsto & ax. \end{array}$$

5. Soient B un anneau et A un sous-anneau de B. L'anneau B est de manière naturelle un A-module à travers la loi externe :

$$\begin{array}{ccc} A \times B & \longrightarrow & B \\ (a,b) & \longrightarrow & ab. \end{array}$$

6. Soient K un corps et E un K-e.v. Soit $A = End(E)$. A est un anneau non commutatif si $dimE > 1$. E est un A-module à gauche via :

$$\begin{array}{ccc} A \times E & \longrightarrow & E \\ (\phi,v) & \longmapsto & \phi(v). \end{array}$$

$\boxed{0.1}$ Sous-Module

Définition 0.6. *Soit M un A-module à gauche. une partie non vide N de M est un sous-module (plus précisément, un sous-A-module) de M, si*

1. N est un sous groupe de $(M, +)$;

2. Pour tout $x \in N$ et tout $a \in A$, $ax \in N$.

Exemple 0.7. *1. (0) et M sont des sous-modules de M.*

2. Les sous-modules du A-module à gauche A (resp. à droite) sont les idéaux à gauche (resp. à droite) de l'anneau A.

Proposition 0.8. – *Soit* $(N_i)_{i\in I}$ *une famille non vide de sous-modules d'un* A*-module* M *; alors,* $\bigcap_{i\in I} N_i$ *est un sous-module de* M*.*
– $\bigcup_{i\in I} N_i$ *n'est pas, en général, un sous-module de* M*. Si la famille* $(N_i)_{i\in I}$ *est totalement ordonnée par l'inclusion, alors* $\bigcup_{i\in I} N_i$ *est un sous-module de* M*.*

Démonstration. - On a $(N_i,+)$ est un groupe pour tout $i \in I$ donc $0 \in N_i$ pour tout $i \in I$, ainsi $0 \in \bigcap_{i\in I} N_i$. Donc $\bigcap_{i\in I} N_i \neq \emptyset$.
Soient $x, y \in \bigcap_{i\in I} N_i \Longrightarrow x \in N_i$ pour tout $i \in I$. Donc $x - y \in N_i$ pour tout $i \in I \Longrightarrow x - y \in \bigcap_{i\in I} N_i$.
Soient $a \in A$ et $x \in \bigcap_{i\in I} N_i \Longrightarrow a \in A$ et $x \in N_i$ pour tout $i \in I \Longrightarrow ax \in N_i$ pour tout $i \in I$. Donc $ax \in \bigcap_{i\in I} N_i$. D'où, $\bigcap_{i\in I} N_i$ est un sous-module de A.

- Si la famille $(N_i)_{i\in I}$ est totalement ordonnée par l'inclusion, alors $\bigcup_{i\in I} N_i \neq \emptyset$.
Soient $x, y \in \bigcup_{i\in I} N_i$ donc il existe $j, k \in I$ tel que $x \in N_i$ et $y \in N_k$. Or $(N_i)_{i\in I}$ est totalement ordonnée par l'inclusion ce qui donne que $N_i \subset N_k$ ou $N_k \subset N_i$.
Si $N_i \subset N_k$ alors $x, y \in N_k \Longrightarrow x - y \in N_k \Longrightarrow x - y \in \bigcup_{i\in I} N_i$.
Si $N_k \subset N_i$ alors $x, y \in N_i \Longrightarrow x - y \in N_i \Longrightarrow x - y \in \bigcup_{i\in I} N_i$.
Donc $\bigcup_{i\in I} N_i$ est un sous-groupe de M.
Soient $a \in A$, $x \in \bigcup_{i\in I} N_i$, alors $a \in A$ et $x \in N_{i_0}$ avec $i_0 \in I \Longrightarrow ax \in N_{i_0} \Longrightarrow ax \in \bigcup_{i\in I} N_i$.

□

Définition 0.9. *Soit* S *un sous-ensemble non vide d'un* A*-module* M*. L'intersection de tous les sous-modules contenant* S *est appelé le sous-module engendré par* S*, souvent noté* (S) *ou* $< S >$*.*
Si M *est un* A*-module à gauche (resp. à droite), on notera* ${}_A(S)$ *(resp.* $(S)_A$*).*

Proposition 0.10.

$$ {}_A(S) = \{ \sum_{1\leqslant i\leqslant n} a_i x_i, n \in \mathbb{N}^*; \quad \forall i \in \{1, ..., n\} \quad a_i \in A, \quad x_i \in S\} $$

Démonstration. Notons par $N(S) = \{ \sum_{1\leqslant i\leqslant n} a_i x_i, n \in \mathbb{N}^*; \quad \forall i \in \{1, ..., n\} \quad a_i \in A, \quad x_i \in S\}$.
$N(S)$ est un sous-ensemble de M. $N(S) \neq \emptyset$ car $0_M \in N(S)$.
Soient $x, y \in N(S)$, alors $x = \sum_{1\leqslant i\leqslant n} a_i x_i$ et $y = \sum_{1\leqslant i\leqslant n} a'_i y_i$.
$x + y = \sum_{1\leqslant i\leqslant n} a_i x_i + \sum_{1\leqslant i\leqslant n} a'_i y_i \in N(S)$, donc c'est un sous-groupe de $(M, +)$.
Soit $a \in A$ et $x \in N(S)$, on a $ax = a \sum_{1\leqslant i\leqslant n} a_i x_i = \sum_{1\leqslant i\leqslant n} a a_i x_i \in N(S)$, donc $N(S)$ est un sous-module de M, donc il contient S, ainsi ${}_A(S) \subseteq N(S)$.
Soit $x \in N(S)$, alors $x = \sum_{1\leqslant i\leqslant n} a_i x_i$ avec $a_i \in A$ et $x_i \in S \subseteq N \Longrightarrow x \in N$ pour tout idéal $N \supset S \Longrightarrow x \in_A (S)$. D'où, $N(S) \subseteq_A (S)$. □

Définition 0.11. *Soit M un A-module à gauche et $x_1, x_2, ..., x_n$ sont des éléments de M ($n \in \mathbb{N}^*$), on appelle combinaison linéaire sur A des x_i ($1 \leqslant i \leqslant n$), tout élément $x \in M$ de la forme $x = \sum_{1 \leqslant i \leqslant n} a_i x_i$ avec $a_i \in A$, $i = 1, ..., n$.*

Remarque 0.12. *${}_A(S)$ est l'ensemble des combinaisons linéaires sur A de toutes les parties finies(non-vides) de S.*

Définition 0.13. *Une partie non vide S d'un A-module à gauche M est une partie génératrice de M, si ${}_A(S) = M$. On dit aussi, dans ce cas, que S engendre le A-module M ou que S est un ensemble de générateurs de M.*

Définition 0.14. *Soit M un A-module à gauche.*

1. *On dit que M est de type fini, s'il possède une partie génératrice finie. Dans ce cas, si $S = \{x_1, x_2, ..., x_n\}$ engendre M, alors*
$$x \in M \Longleftrightarrow x = \sum_{1 \leqslant i \leqslant n} a_i x_i, a_i \in A \text{ pour tout } i = 1, ..., n.$$
2. *M est dit monogène, s'il est engendré par un seul élément x ; alors $M = Ax = \{ax; a \in A\}$.*

0.1.1 Somme de sous-modules

Soit $(N_i)_{1 \leqslant i \leqslant n}$, $n \in \mathbb{N}$, une famille finie de sous-modules d'un A-module M. On pose
$$\sum_{1 \leqslant i \leqslant n} N_i = \{ \sum_{1 \leqslant i \leqslant n} x_i, \quad x_i \in N_i, 1 \leqslant i \leqslant n\}.$$
$\sum_{1 \leqslant i \leqslant n} N_i$ est un sous-module de M et appelé somme de sous-modules N_i, $1 \leqslant i \leqslant n$.

Proposition 0.15. *Soit $(N_i)_{1 \leqslant i \leqslant n}$ une famille de sous-modules d'un A-module M. $\sum_{1 \leqslant i \leqslant n} N_i$ est le sous-module de M engendré par $\bigcup_{1 \leqslant i \leqslant n} N_i$.*

Démonstration. Pour $n = 2$ $(N_1 \cup N_2) \supseteq N_1 + N_2 = \{n_1 + n_2, n_1 \in N_1, n_2 \in N_2\}$. On a $(N_1 \cup N_2) = \{ \sum_{1 \leqslant i \leqslant n} a_i x_i, \quad x_i \in N_1 \cup N_2, \quad a_i \in A \quad 1 \leqslant i \leqslant n\}$.
Soit $z \in (N_1 \cup N_2)$, alors $z = \sum_{1 \leqslant i \leqslant n_1} a_i x_i + \sum_{1 \leqslant k \leqslant n_2} b_k x_k$, $a_i, b_k \in A$, $x_i, \in N_1$ $1 \leqslant i \leqslant n_1$ et $x_k \in N_2$ $1 \leqslant k \leqslant n_2$. On a donc $\sum_{1 \leqslant i \leqslant n_1} a_i x_i \in N_1$ et $\sum_{1 \leqslant k \leqslant n_2} b_k x_k \in N_2 \Longrightarrow z \in N_1 + N_2$, d'où $(N_1 \cup N_2) \subseteq N_1 + N_2$.
Pour $n > 2$, on démontre la propriété par réccurence. □

Soit $(N_i)_{i \in I}$ une famille non vide de sous-modules d'un A-module M. On note
$$\sum_{i \in I} N_i = \{ \sum_{1 \leqslant j \leqslant m} x_{\lambda_j}, \quad m \in \mathbb{N}^*, \lambda_i \in I, \quad x_{\lambda_j} \in N_{\lambda_j}, 1 \leqslant j \leqslant m\}.$$
Nous avons : $\sum_{i \in I} N_i$ est un sous-module de M, appelé somme des sous-modules N_i, $i \in I$ et c'est le sous-module de M engendré par $\bigcup_{i \in I} N_i$.

Remarque 0.16.
1. *Pour tout $j \in I$, N_j est un sous-module de $\sum_{i \in I} N_i$.*

2. *L'expression des éléments de* $\sum_{i\in I} N_i$*, montre que si l'ensemble* I *est de cardinal infini, alors* $x \in \sum_{i\in I} N_i \Longleftrightarrow$ *il existe une partie finie* $\{\lambda_1, \lambda_2, ..., \lambda_m\}$ *de* I *telle que* $x \in \sum_{1\leqslant j\leqslant m} N_j$*. On pourra écrire :* $x = \sum_{i\in I} x_i$*, où pour tout* $i \in I$*,* $x_i \in N_i$*, les* x_i *étant "presque tous nuls" (c'est à dire nuls sauf un nombre fini d'entre eux), car tout* $x \in \sum_{i\in I} N_i$ *est une somme finie d'éléments de* $\bigcup_{i\in I} N_i$*.*

0.1.2 Somme directe de sous-modules

Définition 0.17. *Soit* $(N_i)_{i\in I}$ *une famille non vide de sous-modules d'un* A*-module* M*. On dit que la somme* $\sum_{i\in I} N_i$ *est une somme (interne) directe si tout* $x \in \sum_{i\in I} N_i$ *s'écrit de façon unique :* $x = \sum_{i\in I} x_{i_j}$ *; où* $m \in \mathbb{N}^*$*,* $i_j \in I$*,* $x_{i_j} \in N_{i_j}$ $1 \leqslant j \leqslant m$*. Dans ce cas, la somme est noté* $\bigoplus_{i\in I} N_i$*.*

Proposition 0.18. *Soit* $(N_i)_{i\in I}$ *une famille non vide de sous-modules d'un* A*-module* M*. Les conditions suivantes sont équivalentes :*

1. *La somme des sous-modules* N_i*, pour* $i \in I$*, est directe ;*
2. $(\sum_{i\in I} x_i = 0$ *dans* $\sum_{i\in I} N_i \Longrightarrow)$ $x_i = 0$*, pour tout* $i \in I$ *;*
3. $\forall j \in I$*,* $N_j \bigcap (\sum_{i\in I\setminus \{j\}} N_i) = \{0\}$*.*

Démonstration. 1) $\Longrightarrow$ 2). si la somme est directe, alors 0 s'écrit de façon unique, $0 = \sum_{i\in I} x_i$, d'où $x_i = 0$ pour tout $i \in I$.
2) $\Longrightarrow$ 3). Soit $x \in N_j \bigcap (\sum_{i\in I\setminus \{j\}} N_i$, si $x \neq 0$ alors $x = x_j = \sum_{1\leqslant j\leqslant m} x_{i_j}$, $\lambda_j \in I \setminus \{j\}$, donc $x_j - \sum_{1\leqslant j\leqslant m} x_{i_j} = 0$, d'après 2) on a $x = x_j = 0$.
3) $\Longrightarrow$ 1). Supposons que $x \in \sum_{i\in I} N_i$ tel que $x = \sum_{1\leqslant i\leqslant m} x_i = \sum_{1\leqslant i\leqslant m} y_i$ où les x_i et y_i sont presque tous nuls dans N_i. S'il existe $j \in I$ tel que $x_j \neq y_j$ alors $x_j - y_j = \sum_{i\in I\setminus\{j\}}(y_i - x_i)$. D'après 3) on a $x_j - y_j = 0$, contradiction. On en conclut que $x_i = y_i$ pour tout $i \in I$. □

Définition 0.19. *Soit* M *un* A*-module à gauche.*

1. *Deux sous-modules* N_1 *et* N_2 *de* M *sont dits supplémentaires dans* M*, si* $M = N_1 \oplus N_2$*.*
2. *Un sous-module* N *de* M *est dit facteur direct dans* M*, s'il existe un sous-module* N' *de* M *tel que* $M = N \oplus N'$*.*

Remarque 0.20.

1. $M = N_1 \oplus N_2 \Longleftrightarrow M = N_1 \oplus N_2$ *et* $N_1 \cap N_2 = \{0\}$*.*
2. *Un sous-module* N' *d'un* A*-module* M *n'est pas, en général, un facteur dans* M*. On sait cependant que dans un* $\mathbb{K}$*.e-v tout s.e.v a un supplémentaire, donc facteur direct.*
3. *Un* A*-module est dit semi-simple si tous sous-modules soient facteurs directs.*

0.1.3 Morphismes de A-modules

Définition 0.21. *Soient* M *et* N *deux* A*-modules. On appelle un morphisme de* A*-modules (homomorphisme ou application* A*-linéaire) de* M *dans* N *toute application* $f : M \longrightarrow N$ *telle que :*

1. $f(x + y) = f(x) + f(y)$ *pour tout* $x, y \in M$*,*

2. $f(ax) = af(x)$ *pour tout* $a \in A, x \in M$.

L'ensemble des A-homomorphismes se note $Hom_A(M, N)$.

Soient u et $v \in Hom_A(M, N)$ et $a \in A$. Notons par :

$$\begin{array}{rcl} u + v : M & \longrightarrow & N \\ x & \longmapsto & (u + v)(x) = u(x) + v(x) \end{array}$$

et

$$\begin{array}{rcl} au : M & \longrightarrow & N \\ x & \longmapsto & (au)(x) = au(x). \end{array}$$

$Hom_A(M, N)$ a ainsi la structure d'un A-module à travers la loi externe :

$$\begin{array}{ccc} A \times Hom_A(M, N) & \longrightarrow & Hom_A(M, N) \\ (a, u) & \longmapsto & au. \end{array}$$

Si $N = A$, $Hom_A(M, A)$ qui est l'ensemble des formes A-linéaires de M dans A s'appelle <u>le dual</u> de M.

Exemple 0.22. *1) Si N est un sous-module d'un A-module M, alors l'injection*

$$\begin{array}{rcl} i : N & \longrightarrow & M \\ x & \longmapsto & x \end{array}$$

est un A-morphisme.
2)

$$\begin{array}{rcl} M & \longrightarrow & M' \\ x & \longmapsto & 0. \end{array}$$

est un morphisme de A-modules, appelé morphisme nul.

Proposition 0.23. *Soient M et M' deux A-modules et $f \in Hom_A(M, M')$, N un sous-module de M et N' un sous-module de M'. Alors on a :*

1. *$f(N)$ est un sous-module de M', en particulier $Imf := \{f(x)/\ x \in M\}$ est un sous module de N.*
2. *$f^{-1}(N')$ est un sous-module de M, en particulier $\ker f := \{x \in M/\ f(x) = 0_N\}$ est un sous-module de M.*
3. *f est surjectif si et seulement si $Imf = M$.*
4. *f est injectif si et seulement si $\ker f = \{0\}$.*
5. *Si $f \in Hom_A(M, M')$ et $g \in Hom_A(M', M'')$ alors $g \circ f \in Hom_A(M, M'')$.*

Démonstration. Exercice.

□

Définition 0.24. *Soient M et M' deux A-modules, une application f de M dans M' est un isomorphisme de A-modules, si $f \in Hom_A(M, M')$ et s'il existe $g \in Hom_A(M', M)$ tel que $g \circ f = id_M$ et $f \circ g = id_{M'}$.*

Proposition 0.25. *1) f isomorphisme de M sur M' $\Longleftrightarrow$ $f \in Hom_A(M, M')$ et f bijectif.*
2) f isomorphisme M sur M' $\Longrightarrow$ f^{-1} isomorphisme de M' sur M.

Définition 0.26. *a) Deux A-modules M et M' sont dits isomorphes (ou A-isomorphes) s'il existe un isomorphisme de A-modules de l'un sur l'autre ; on écrit alors, symboliquement, $M \simeq M'$.*

Définition 0.27. *Soient M un A-module et N un sous-module de M. Sur le groupe quotient abelien M/N, on considère la loi de composition externe à opérateurs dans A, définie par :*

$$\begin{array}{ccc} A \times M/N & \longrightarrow & M/N \\ (a, \overline{x}) & \longmapsto & \overline{ax} = ax + N. \end{array}$$

La loi est compatible avec la relation : $x \sim y \iff x - y \in N$. En effet $x \sim y \iff x - y \in N \Longrightarrow a(x-y) \in N \Longrightarrow ax \sim ay$.
Ainsi, $\overline{x} = \overline{y} \Longrightarrow \overline{ax} = \overline{ay}, x, x' \in M$ et $a \in A$.
On peut donc poser, dans M/N, $a\overline{x} = \overline{ax}$.
M/N a une structure de A-module appelé module quotient de M par N.
L'application canonique $\pi : M \longrightarrow M/N$ est un morphisme de A-modules surjectif avec $\ker \pi = N$, appelé surjection canonique. Nous avons :

Théorème 0.28. *(Propriété universelle)*
Soient A un anneau, M et M' deux A-modules et $f \in Hom_A(M, M')$ un morphisme de modules. Si N est un sous-module de M contenu dans $\ker f$, il existe un unique homomorphisme $\widetilde{f} \in Hom(M/N, M')$ tel que $f = \widetilde{f} \circ \pi$. On a le diagramme commutatif suivant :

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "\pi"'] & M' \\ & M/N \arrow[u, "\widetilde{f}"'] \end{tikzcd}$$

Théorème 0.29. *(1er théorème d'isomorphisme)*
Soient M et M' deux A-modules et $f \in Hom_A(M, M')$. Alors on a :

$$E/Ker(f) \simeq Im(f).$$

Théorème 0.30. *(2em théorème d'isomorphisme)*
Soient N_1 et N_2 deux sous-modules d'un A-module M. Alors on a :

$$(N_1 + N_2)/N_2 \simeq N_1/(N_1 \cap N_2).$$

Corollaire 0.31. *Si $M = N_1 \oplus N_2$, alors $M/N_1 \simeq N_2$ et $M/N_2 \simeq N_1$*

Théorème 0.32. *(3em théorème d'isomorphisme)*
Soient N_1 et N_2 deux sous-modules d'un A-module M tels que $N_2 \subseteq N_1$. Alors on a :

$$M/N_1 \simeq (M/N_2)/(N_1/N_2).$$

Dans toute la suite du cours, anneau signifie anneau commutatif unitaire, sauf mention expresse du contraire.

$\boxed{0.2}$ Produit et somme de modules

Définition 0.33. *1. Soient $(M_i)_{i \in I}$ une famille de R-modules et $M = \prod_{i \in I} M_i$ le produit au sens ensembliste des M_i. On munit M d'une structure de A-module en posant :*

$$\begin{cases} (x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I} \\ \lambda (x_i)_{i \in I} = (\lambda x_i)_{i \in I} \end{cases}$$

Muni d'une telle structure, M est appelé <u>module produit</u> de la famille des modules $(M_i)_{i \in I}$.

2. *On appelle* <u>*somme directe*</u> *de la famille des modules* $(M_i)_{i\in I}$ *qu'on note* $\bigoplus_{i\in I} M_i$, *le sous module de* $M = \prod_{i\in I} M_i$, *formé des* $(x_i)_{i\in I}$ *tels que* $x_i = 0$ *sauf pour un nombre fini d'indices.*

– *Notons que lorsque* I *est fini, on a :*

$$\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i.$$

– *Pour chaque* $j \in I$, *on appelle projection canonique le* A*-morphisme surjectif :*

$$\begin{array}{rcl} P_j : \prod_{i\in I} M_i & \longrightarrow & M_j \\ (x_i)_{i\in I} & \longmapsto & x_j. \end{array}$$

On appelle injection canonique le A*-morphisme :*

$$\begin{array}{rcl} e_j : M_j & \longrightarrow & \prod_{i\in I} M_i \\ x_j & \longmapsto & (y_i)_{i\in I} \end{array}$$

avec

$$\begin{cases} y_j = x_j \\ y_i = 0 \quad \forall\, i \neq j. \end{cases}$$

Remarque 0.34. 1. *Soit* M *un* A*-module, le produit de modules où tous les facteurs sont identiques à* M *n'est autre que* M^I *(l'ensemble des applications de* I *dans* $A : I \longrightarrow A$*).*
Notation :

$$\prod_{i\in I} M_i = M^I, \bigoplus_{i\in I} M_i = M^{(I)}.$$

2. *Soient* $(M_i)_{i\in I}$, $(N_i)_{i\in I}$ *deux familles de* A*-modules et* $f_i : M_i \longrightarrow N_i$ $(i \in I)$ *une famille de morphismes. Alors :*

a) *L'application*

$$\begin{array}{rcl} f : M = \prod_{i\in I} M_i & \longrightarrow & N = \prod_{i\in I} N_i \\ (x_i)_{i\in I} & \longmapsto & (f_i(x_i))_{i\in I} \end{array}$$

est un A*-morphisme.*

b) $Ker(f) = \prod_{i\in I} Ker(f_i)$ *et* $Im(f) = \prod_{i\in I} Im(f_i)$.
Par conséquent : f *est injectif (resp., surjectif) si et seulement si* f_i *est injectif (resp., surjectif)* $\forall i \in I$.
a) et b) restent valables si on remplace le module produit par la somme directe.

Lemme 0.35. *Soit* M *un module et soit* $(N_i)_i$ *une famille de modules. Les assertions suivantes sont équivalentes :*

i) $N \simeq \prod_{i\in I} N_i$.

ii) *Il existe une famille de morphismes* $f_i : N \longrightarrow N_i$ $(i \in I)$ *tels que pour tout module* M *et toute famille de morphismes* $g_i : M \longrightarrow N_i$ $(i \in I)$, *il existe un unique* $f \in Hom_R(M, N)$ *tel que :* $f_i o f = g_i$ $\forall i \in I$.

$$\begin{tikzcd} M \arrow[rr, "g_i"] \arrow[dr, "f"'] & & N_i \\ & N \simeq \prod_{i\in I} N_i \arrow[ur, "f_i"'] & \end{tikzcd}$$

Démonstration. Supposons que $i)$ est vraie et montrons $ii)$. Si $N = \prod_{i\in I} N_i$, on considère la famille des projections canoniques $(p_i)_{i\in I}$. Pour l'existence de f prenons $f(x) = (g_i(x))_{i\in I}$ on a $p_i o f(x) = p_i(g_i(x)) = g_i(x)$ pour tout $i \in I$ et $x \in M$, d'où $p_i o f = g_i$.
unicité : Supposons qu'il existe $f' \in Hom_R(M, N)$ tel que $p_i o f' = g_i$. On a $f'(x) = (f_i'(x))_{i\in I}$,
$\begin{cases} p_i o f' = g_i \\ p_i o f = g_i \end{cases} \Longrightarrow f_i'(x) = f_i(x)$ pour tout $i \in I$, d'où $f = f'$.
Inversement, supposons que $ii)$ est vraie et montrons $i)$. D'après les hypothèses, nous avons les diagrammes commutatifs :

$$(1)\quad \begin{tikzcd} M = N \arrow[rr, "f_i"] \arrow[dr, "\exists ! f"'] & & N_i \\ & \prod_{i\in I} N_i \arrow[ur, "p_i"'] & \end{tikzcd} \qquad (2)\quad \begin{tikzcd} M = \prod_{i\in I} N_i \arrow[rr, "p_i"] \arrow[dr, "id(M)"'] & & N_i \\ & \prod_{i\in I} N_i \arrow[ur, "p_i"'] & \end{tikzcd}$$

$$(3)\quad \begin{tikzcd} M = \prod_{i\in I} N_i \arrow[rr, "p_i"] \arrow[dr, "\exists ! g"'] & & N_i \\ & N \arrow[ur, "f_i"'] & \end{tikzcd} \qquad (4)\quad \begin{tikzcd} M = N \arrow[rr, "f_i"] \arrow[dr, "id(N)"'] & & N_i \\ & N \simeq \prod_{i\in I} N_i \arrow[ur, "f_i"'] & \end{tikzcd}$$

Il en résulte d'après (1) et (3), que pour tout $i \in I$ on a :

$$\begin{cases} p_i o f = f_i & (1)\ \forall i \in I \\ f_i o g = p_i & (2). \end{cases}$$

Par conséquent, pour tout $i \in I$ on a :

$$\begin{cases} p_i o f o g = p_i \\ f_i o g o f = f_i. \end{cases}$$

D'après l'unicité de (2) et (4) on a :

$$\begin{cases} f o g = id(\prod_{i\in I} N_i) \\ g o f = id(N). \end{cases}$$

D'où, $A \simeq \prod_{i\in I} A_i$. Ce qui achève la preuve du lemme. □

On peut maintenant énoncer le théorème d'isomorphisme suivant :

Théorème 0.36. *On a l'isomorphisme :*

$$Hom_A(M, \prod_{i\in I} N_i) \cong \prod_{i\in I} Hom_A(M, N_i)$$

Démonstration. Soit

$$\begin{array}{rcl} \varphi : Hom_A(M, \prod_{i\in I} N_i) & \longrightarrow & \prod_{i\in I} Hom_A(M, N_i) \\ f & \longmapsto & (p_i o f)_{i\in I}. \end{array}$$

On peut facilement vérifier que φ est un A-morphisme. En vertu du lemme précédent, φ est bijectif. □

Corollaire 0.37. *Etant donné deux familles non vides de A-modules $(M_i)_{i\in I}$ et $(M_i')_{i\in I}$, alors*

$$(\forall i \in I, M_i' \simeq M_i) \Longrightarrow \prod_{i\in I} M_i' \simeq \prod_{i\in I} M_i.$$

Lemme 0.38. *Soient N un module et $(N_i)_{i\in I}$ une famille de modules. Les assertions suivantes sont équivalentes :*

i) $N \simeq \bigoplus_{i\in I} N_i$.

ii) *Il existe une famille de morphismes $f_i : N_i \longrightarrow N$ $(i \in I)$ tels que pour tout module M et toute famille de morphismes $g_i : N_i \longrightarrow M$ $(i \in I)$, il existe un unique $f \in Hom_A(N, M)$ tel que $fof_i = g_i$ $\forall i \in I$.*

Démonstration. Supposons que $i)$ est vraie et montrons $ii)$. Si $N \simeq \bigoplus_{i\in I} N_i$, on considère alors la famille des injections canoniques $(e_i)_{i\in I}$ et on vérifie que : $foe_i = g_i$ $\forall i \in I$ si et seulement si $f((x_i)_{i\in I}) = \sum_{i\in I} f(e_i(x))_{i\in I} = \sum_{i\in I} g_i(x_i)$. Il est possible de prendre f défini par :

$$f((x_i)_{i\in I}) = \sum_{i\in I} f(e_i(x))_{i\in I}$$

puisque les x_i sont nuls sauf pour un nombre fini.
Inversement, supposons que $ii)$ est vraie. D'après l'étude directe et par hypothèses, nous avons les diagrammes commutatifs :

$$(1)\ \begin{tikzcd} N_i \arrow[rr, "f_i"] \arrow[dr, "e_i"'] & & M = N \\ & \oplus_{i\in I} N_i \arrow[ur, "f"'] & \end{tikzcd} \qquad (2)\ \begin{tikzcd} N_i \arrow[rr, "e_i"] \arrow[dr, "e_i"'] & & M = \oplus_{i\in I} N_i \\ & \oplus_{i\in I} N_i \arrow[ur, "id(\oplus_{i\in I} N_i)"'] & \end{tikzcd}$$

$$(3)\ \begin{tikzcd} N_i \arrow[rr] \arrow[dr, "f_i"'] & & M = \oplus_{i\in I} N_i \\ & A \arrow[ur, "g"'] & \end{tikzcd} \qquad (4)\ \begin{tikzcd} N_i \arrow[rr, "f_i"] \arrow[dr, "f_i"'] & & M = N. \\ & N \arrow[ur, "id(N)"'] & \end{tikzcd}$$

Nous avons donc pour tout $i \in I$:

$$\begin{cases} foe_i = f_i \\ gof_i = e_i. \end{cases}$$

Par conséquent, on a pour tout $i \in I$:

$$\begin{cases} gofoe_i = e_i \\ fogof_i = f_i. \end{cases}$$

D'après l'unicité de $id(\oplus_{i\in I} N_i)$ et $id(N)$ on a :

$$\begin{cases} fog = id(N) \\ gof = id(\bigoplus_{i\in I} N_i). \end{cases}$$

D'où $N \simeq \bigoplus_{i\in I} N_i$. $\square$

Théorème 0.39. *On a l'isomorphisme suivant :*

$$Hom_A(\bigoplus_{i\in I} N_i, M) \cong \prod_{i\in I} Hom_A(N_i, M).$$

Démonstration. Soit

$$\begin{array}{rcl} \varphi : Hom_A(\bigoplus_{i\in I} N_i, M) & \longrightarrow & \prod_{i\in I} Hom_A(N_i, M) \\ f & \longmapsto & (foe_i)_{i\in I}. \end{array}$$

On peut vérifier facilement que φ est un A-morphisme bijectif. En effet, Soit $(g_i)_{i\in I} \in \prod_{i\in I} Hom_A(A_i, B)$, d'après le lemme précédent il existe un unique $G \in Hom_A(\bigoplus_{i\in I} N_i, M)$ tel que $G \circ e_i = g_i$ pour tout $i \in I$ i.e, $\varphi(G) = (g_i)_{i\in I} \Longrightarrow \varphi$ est bijectif. $\square$

Remarque 0.40. *Il existe des exemples où on a :*

1. $Hom_A(\prod_{i\in I} N_i, M) \ncong \bigoplus_{i\in I} Hom_A(N_i, M)$.
2. $Hom_A(\prod_{i\in I} N_i, M) \ncong \prod_{i\in I} Hom_A(N_i, M)$.
3. $Hom_A(N, \bigoplus_{i\in I} M_i) \ncong \bigoplus_{i\in I} Hom_A(N, M_i)$.
4. $Hom_A(N, \bigoplus_{i\in I} M_i) \ncong \prod_{i\in I} Hom_A(N, M_i)$.

Proposition 0.41. *Soient $(M_i)_{i\in I}$ une famille de modules et N_i un sous module de M_i pour chaque $i \in I$. On a :*

$$\frac{\oplus_{i\in I} M_i}{\oplus_{i\in I} N_i} = \oplus_{i\in I} \frac{M_i}{N_i}$$

Démonstration. L'application

$$\begin{array}{rccc} f: & \oplus_{i\in I} M_i & \longrightarrow & \oplus_{i\in I} \frac{M_i}{N_i} \\ & (x_i)_{i\in I} & \longmapsto & (x_i + N_i)_{i\in I} \end{array}$$

est un homomorphisme surjectif de modules. De plus $Ker(f) = \oplus_{i\in I} N_i$. Dés lors, le premier théorème d'isomorphisme termine la preuve. □

$\boxed{0.3}$ Suites exactes de A-modules

Définition 0.42. 1. *Une suite de A-modules et d'homomorphismes*

$$...M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} Mi + 1 \xrightarrow{f_{i+1}} ...$$

est dite <u>suite exacte en M_i</u> si $\ker f_i = Imf_{i-1}$. Cette suite est dite <u>exacte</u> si elle est exacte en chaque M_i.

2. *Une suite exacte courte est une suite exacte de la forme*

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0;$$

c'est à dire que u est injectif, v est surjectif, et $Im(u) = Ker(v)$.

Notamment on a :

Proposition 0.43. *Soit $u : M \longrightarrow N$ un morphisme de A-modules. Alors on a :*

1. *u est injectif si et seulement si la suite $0 \longrightarrow M \longrightarrow N$ est exacte.*
2. *u est surjectif si et seulement si la suite $M \longrightarrow N \longrightarrow 0$ est exacte.*
3. *u est bijectif si et seulement si la suite $0 \longrightarrow M \longrightarrow N \longrightarrow 0$ est exacte.*

Exemple 0.44. *Soit N un sous-module d'un A-module M, alors la suite*

$$0 \longrightarrow N \xrightarrow{j} M \xrightarrow{\pi} M/N \longrightarrow 0$$

où j est l'injection canonique et π la surjection canonique, est une suite exacte courte.

Proposition 0.45. *Toute suite exacte courte de A-modules à gauche*

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

est "isomorphe" à la suite exacte courte suivante

$$0 \longrightarrow Imf \xrightarrow{j} M \xrightarrow{\pi} M/Imf \longrightarrow 0$$

Autrementdit, il existe des isomorphismes de A-modules, $Imf \xrightarrow{u} N$ et $M/Imf \xrightarrow{v} P$ tels que le diagramme suivant commute.

$$\begin{array}{ccccc}
0 \longrightarrow Imf & \xrightarrow{j} & M & \xrightarrow{\pi} & M/Imf \longrightarrow 0 \\
u \downarrow & & Id_M \downarrow & & \downarrow v \\
0 \longrightarrow N & \xrightarrow{f} & M & \xrightarrow{g} & P \longrightarrow 0
\end{array}$$

donc $f \circ u = j$ et $v \circ \pi = g$.

Démonstration. On a f est injectif, g est surjectif et $Imf = \ker g$.
Soit f_1 la restriction surjective de f

$$f_1 : \begin{array}{ccc} A & \longrightarrow & Imf \\ x & \longrightarrow & f_1(x) = f(x) \end{array}.$$

Le morphisme f_1 est surjectif et il est injectif, car f est injectif, donc f_1 est un isomorphisme. On en déduit que $u = f_1^{-1}$ est un isomorphisme de Imf sur N et $f \circ u = id_{Imf} \Longrightarrow f'ou = j = id_M \circ j$. D'autre part, d'après la propriété universelle du module quotient, la condition $Imf = \ker g$ implique $\exists! v \in Hom_A(M/Imf, P)$ tel que le diagramme suivant commute

$$\begin{tikzcd}
M \arrow[r, "\pi"] \arrow[dr, "g"'] & M/Imf \arrow[d, "\exists! v"] \\
 & P
\end{tikzcd}$$

d'où $v \circ \pi = g = g \circ id_M$. De plus, $\ker g = lmf$ implique v injectif, g surjectif entraîne v surjectif, donc v est un isomorphisme de M/Imf sur P.

□

$\boxed{0.4}$ A-module libre et de type fini

0.4.1 Module de type fini

Soient M un module et S une partie de M. Le plus petit sous module de M contenant S, noté $< S >$, est exactement l'ensemble des éléments de la forme $\sum_{i=1}^{n} a_i s_i$, avec $a_i \in A$, $s_i \in S$ et $n \in \mathbb{N}^*$.

Définition 0.46. *1. Un module M est dit de type fini s'il existe une partie finie $\{x_1, \ldots, x_n\}$ de M telle que $M =< x_1, \ldots, x_n >$. Dans ce cas, nous avons :*

$$M = \sum_{i=1}^{n} Ax_i.$$

2. Un module M est dit cyclique (ou monogène) s'il existe $x \in M$ tel que $M =< x >$; c'est à dire que $M = Ax$.

Exemple 0.47. *1. Si $A = K$ est un corps, les A-modules de type fini sont les espaces vectoriels de dimension finie.*

2. A^m est un A-module de type fini.

Remarque 0.48. *Un sous module d'un A-module de type fini n'est pas nécessairement de type fini. En effet, soient $A = K[X_1, ..., X_n, ...]$, où K est un corps, $(X_i)_{i\in\mathbb{N}}$ sont des indéterminées sur K et $I :=< X_1, ..., X_n, ... >$ l'idéal de A engendré par $(X_i)_{i\in\mathbb{N}}$. L'idéal I n'est pas de type fini et pourtant A est de type fini.*

Le résultat suivant caractérise les modules de type fini.

Théorème 0.49. *Soit M un A-module. Les assertions suivantes sont équivalentes :*

1. *M est de type fini ;*
2. *Il existe $n \geqslant 1$ tel que M est isomorphe à un quotient d'un module libre de type fini $A^n(:= \underbrace{A \times A \times ... \times A}_{n fois})$.*

Démonstration. Supposons que M est de type fini engendré par $x_1, ..., x_n$: $M = \sum_{i=1}^{n} Ax_i$. Considèrons l'homorphisme :

$$\begin{array}{ccc} f : A^n & \longrightarrow & M \\ (a_1, ..., a_n) & \longmapsto & \sum_{i=1}^{n} a_i x_i. \end{array}$$

L'homomorphisme f est surjectif par construction. Par le 1er théorème d'isomorphisme on a $M = Imf \simeq A^n/Kerf$.

Inversement, supposons qu'il existe $r \in \mathbb{N}^*$ et un sous module N de A^r tels que $M \simeq A^r/N$. Si $(e_1, ..., e_r)$ est une base de A^r, alors $(e_1 + N, ..., e_r + N)$ engendre M. □

Proposition 0.50. *1. Soient M un module et N un sous module de M. Si M est de type fini, alors M/N est aussi un module de type fini.*
2. Soit $0 \to A \to^{\mu} B \to^{\nu} C \to 0$ une suite exacte de modules. Si A et C sont de type fini, alors B est aussi de type fini.

Démonstration. 1. Soit $M =< x_1, \ldots, x_n >$. Il est clair que $M/N =< \bar{x_1}, \ldots, \bar{x_n} >$, où $\bar{x_i} = x_i + N$.
2. Supposons que $A =< a_1, \ldots, a_n >$ et $C =< c_1, \ldots, c_m >$. Le morphisme ν étant surjectif, il existe $b_i \in B$ tel que $\nu(b_i) = c_i$, pour tout $i = 1, \ldots, m$. On a aussi $C =< \nu(b_1), \ldots, \nu(b_m) >$. Dés lors, on a $< \mu(a_1), \ldots, \mu(a_n), b_1, \ldots, b_m >\subseteq B$. Montrons que : $B \subseteq< \mu(a_1), \ldots, \mu(a_n), b_1, \ldots, b_m >$.

Soit $b \in B$, on a :

$$\nu(b) = \sum_{i=1}^{m} \lambda_i c_i = \sum_{i=1}^{m} \lambda_i \nu(b_i) = \sum_{i=1}^{m} \nu(\lambda_i b_i).$$

D'où $b - \sum_{i=1}^{m} \lambda_i b_i \in Ker(\nu) = Im(\mu)$ car (μ, ν) est exacte, de sorte que $b - \sum_{i=1}^{m} \lambda_i b_i = \mu(\sum_{j=1}^{n} \mu_j a_j)$ pour un certain $\mu_j \in R$. Dés lors, $b = \sum_{j=1}^{n} \mu_j \mu(a_j) + \sum_{i=1}^{m} \lambda_i b_i \in< \mu(a_1), \ldots, \mu(a_n), b_1, \ldots, b_m >$. D'où le résultat. □

Remarque 0.51. *L'hypothèse "A et C sont de type fini" est nécessaire pour avoir B de type fini dans la proposition précédente. En effet :*

1. Soient $R = K[X_1, \dots, X_n, \dots]$ l'anneau des polynômes à une infinité d'indeterminées sur un corps K, $B =< X_1, \dots, X_n, \dots >$ l'idéal engendré par $\{X_1, \dots, X_n, \dots\}$ et $A =< X_1 >$ l'idéal engendré par $\{X_1\}$.

On a A est de type fini, B n'est pas de type fini et on a la suite exacte :

$$0 \to A =< X_1 > \to B =< X_2, \dots, X_n, \dots > \to B/A \simeq < X_1, \dots, X_n, \dots > \to 0$$

où B/A n'est pas de type fini.

2. Soient B un module qui n'est pas de type fini et $C = 0$ le module nul. On a C est de type fini, B n'est pas de type fini et on a la suite exacte de A-modules :

$$0 \to A(= B) \to B \to C(= 0) \to 0.$$

Concernant les modules cycliques, on a :

Proposition 0.52. *Un module M est cyclique si et seulement si $M \simeq A/I$ pour un certain idéal I de R.*

Démonstration. Supposons que $M =< x >$. L'application :

$$\begin{array}{rcl} f : A & \longrightarrow & M \\ \lambda & \longmapsto & \lambda x \end{array}$$

est un morphisme de A-modules surjectif. Donc, $M \simeq A/\ker(f)$, où $Ker(f)$ est un idéal de R. Réciproquement, si I est un idéal de A, alors $A/I =< \overline{1} >$ est un A-module cyclique et cela achève la preuve. □

Théorème 0.53. *[Lemme de Nakayama]*
Soient I un idéal de A et $J(A)$ le radical de Jacobson de l'anneau A. Les assertions suivantes sont équivalentes :
i. $I \subseteq J(A)$;
ii. Pour tout module de type fini M tel que $IM = M$, on a $M = 0$;
iii. Pour tout module M de type fini et tout sous module N de M tel que $M = IM + N$, on a $M = N$;
iv. Pour tout module M tel que $M/IM =< \bar{x_1}, \dots, \bar{x_n} >$, on a $M =< x_1, \dots, x_n >$.

La preuve de ce théorème se base sur le lemme suivant :

Lemme 0.54. *Soient M un A-module de type fini et I un idéal de A. Si $IM = M$ alors il existe $a \in A$ tel que $(1 + a) \in I$ et $aM = 0$.*

Démonstration. Posons $M = \sum_{i=1}^{n} Ax_i$. L'égalité $IM = M$ implique que $x_i \in IM$ pour tout $i = 1, ..., n$; c'est à dire que $x_i = \sum_{j=1}^{n} a_{ij}x_j$ où $a_{ij} \in I$ et $x_j \in M$. Ainsi, on a $(-1+a_{ii})x_i + \sum_{j=1, j\neq i}^{n} a_{ij}x_j = 0$. Posons

$B = (a_{ij})_{1 \leqslant i,j \leqslant n}$ et $X = \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix}$.

On a $(B - I_n)X = 0$ où I_n est la matrice identité d'ordre n. Posons $a = det(B - I_n)$. Modulo I, on a $\overline{a} = \overline{1}$; c'est à dire que $1 + a \in I$. Il est clair que $aM = 0$ et cela termine la preuve de ce lemme. □

Preuve du théorème 0.53.

$i \Rightarrow ii$. Comme $IM = M$, alors d'après le lemme précédent, il existe $a \in A$ tel que $1+a \in I$ et $aM = 0$. Or $I \subseteq J(A)$. Dés lors, $1 + a \in J(A)$ et donc $1 - (1 + a) = -a \in U(A)$; c'est à dire que $a \in U(A)$. Ainsi $aM = 0$ et par suite $M = a^{-1}aM = a^{-1}0 = 0$. D'où ii).

$ii \Rightarrow iii$. Soient M un R-module de type fini et N un sous module de M tel que $M = IM + N$. Ainsi, le A-module M/N est de type fini et $I(M/N) = M/N$ (car $M = IM + N$). Dés lors on a $M/N = 0$; c'est à dire que $M = N$.

$iii \Rightarrow iv$. Il suffit d'appliquer iii) à $N =< x_1, \ldots, x_n >$.

$iv \Rightarrow i$. Soient $x \in I$ et $\lambda \in A$. On a : $A/IA = A/I =< \overline{1} >=< \overline{1 + \lambda x} >$, ceci implique que $A =< 1 + \lambda x >$ et $1 + \lambda x$ est donc inversible pour tout $\lambda \in A$.

Soit maintenant m un idéal maximal de A. On veut montrer que $x \in m$.
Supposons que $x \notin m$, alors $< x > +m = A$. Il existe donc $\lambda \in A$ et $a \in m$ tels que $1 = \lambda x + a$. Ainsi on a $a = 1 - \lambda x \in I$ est inversible, absurde. Donc $I \subseteq m$ pour tout idéal maximal m de A ; c'est à dire que $I \subseteq J(R)$ et cela termine la preuve du théorème. ■

0.5 A-algèbre

Définition 0.55. *A étant un annneau unitaire et commutatif, on dit que M est une A-algèbre à gauche si :*

1. *M est un anneau unitaire(éléments unité 1_M).*
2. *M est un A-module à gauche ;*
3. *$\forall (x, y) \in M \times M$, $\forall a \in A$, $a(xy) = (ax)y = x(ay)$.*

$\longrightarrow$ On définit de même, une A-algèbre à droite.
$\longrightarrow$ Une A-algèbre M est dite commutative si l'anneau M est commutatif.
$\longrightarrow$ Une A-algèbre M est dite libre si le A-module M est libre.
Donc, si K est un corps, toute K-algèbre est libre.

Exemple 0.56. 1. *Tout anneau unitaire est une $\mathbb{Z}$-algèbre.*

2. *Un anneau unitaire et commutatif A est une A-algèbre à droite et à gauche.*

Définition 0.57. *M étant une A-algèbre, une partie N de M est une sous-algèbre de M si S est à la fois un sous-anneau unitaire et un sous-A-module de M.*

Remarque 0.58. *Pour $n > 1$, $n\mathbb{Z}$ n'est pas une sous $\mathbb{Z}$-algèbre de $\mathbb{Z}$, car $1 \notin n\mathbb{Z}$.*

Définition 0.59. *Pour deux A-algèbres M et M', une application f de M dans M' est un morphisme de A-algèbres, si f est à la fois un morphisme d'anneau unitaires et un morphisme de A-modules.*

0.5.1 Module libre

Définition 0.60. *M étant un A-module. On dit qu'une partie non vide S de M est libre si pour toute partie finie T de S, la relation $\sum\limits_{s\in T} a_s s = 0$ avec les $a_s \in A$, entraîne $a_s = 0$ pour tout $s \in T$.*

Remarque 0.61.

1. *Par convention, on considère la partie vide d'un A-module quelconque, comme une partie libre.*
2. *D'après la définition 0.60., quel que soit le A-module M, $\{0\}$ n'est pas une partie libre de M.*
3. *Si S est une partie libre non vide d'un A-module M, alors $S' \subseteq S \Longrightarrow S'$ partie libre de M. Par suite, $\{0\}$ n'appartient à aucune partie libre de M.*

Définition 0.62. *Un A-module M est dit libre s'il possède une partie génératrice, libre sur A. Dans ce cas, toute partie libre et génératrice du A-module M est appelée une base de M sur A.*

Remarque 0.63. *a) Le A-module $\{0\}$ est considéré comme libre, de base l'ensemble vide.*
b) Tout K-espace vectoriel est un K-module libre.
c) Le A-module A est libre de base $\{1\}$.
d) Si A n'est pas un corps, un A-module n'est pas nécessairement libre. Par exemple, $\mathbb{Z}/6\mathbb{Z}$ en tant que $\mathbb{Z}$-module n'a pas de base. Sinon, si $\overline{x} \in \mathbb{Z}/6\mathbb{Z}$ dans une base, on a $6\overline{x} = \overline{0}$, alors que 6 n'est pas nul dans $\mathbb{Z}$.
e) Les A-modules n'ont pas les mêmes comportements que les espaces vectoriels. Un sous-module d'un A-module libre n'est pas forcément libre : soit $A = \mathbb{Z}/n^2\mathbb{Z}$ et $I = n\mathbb{Z}/n^2\mathbb{Z}$, idéal de A comme sous-module de A n'est pas libre, $n \in \mathbb{N}^*$. En effet, pour tout $x \in I$, on a $nx = 0$ avec $n \neq 0$ dans A, donc aucune partie de I ne peut être libre et donc une base de I.
(Le $\mathbb{Z}/4\mathbb{Z}$-module $\mathbb{Z}/4\mathbb{Z}$ est libre de base $\{\overline{1}\}$ mais le sous-module $2\mathbb{Z}/4\mathbb{Z}$ n'est pas libre car $\{\overline{2}\}$ est génératrice mais n'est pas libre.)

Proposition 0.64. *Soit M un A-module, les conditions suivantes sont équivalentes :*

1. *M est libre de base $X = \{x_i\}_{i\in I}$,*
2. *Tout $x \in M$ s'écrit de façon unique : $x = \sum_{i\in I} a_i x_i$, les a_i étant presque tous nuls dans A,*
3. *$M \simeq A^{(I)}$.*

Démonstration. (1) $\Longleftrightarrow$ (2), d'après la définition.
(2) $\Longleftrightarrow$ (3), on a 2) $\Longleftrightarrow M \simeq \bigoplus_{i\in I} Ax_i$, or $Ax_i \simeq A$ pour tout $i \in I$, d'où le résultat.

□

Corollaire 0.65. *M est un A-module libre de base $\{x_1, x_2, ..., x_n\}, n > 0$, si et seulement si M est isomorphe au A-module A^n.*

Remarque 0.66. *1. On a $X = \{x_i\}_{i\in I}$, donc $card(X) = card(I)$; d'où $A^{(X)} = A^{(I)}$,*

2. *Si A est un anneau unitaire, commutatif, alors toutes les bases d'un A-module libre M ont le même cardinal (que celui-ci soit fini ou non), lorsque ce cardinal est fini, il est appelé le rang de M, sinon on dit que M est libre de rang infini.*
3. *Lorsque l'anneau unitaire n'est pas commutatif, un tel A-module peut avoir des bases finies n'ayant pas le même cardinal.*
4. *Soit A un anneau principal. Alors tout idéal non nul A est libre de rang 1. En effet, soit I un idéal non nul de A, alors il existe $a \in A$ tel que $I = aA$, (a) est une base de I car A est un D.I.*
5. *Par convetion, le module $\{0\}$ est libre de rang 0.*
6. *Libre n'implique pas une base : $\{\overline{2}\}$ est une famille libre du $\mathbb{Z}$-module $\mathbb{Z}$ mais n'est pas une base. De même, famille génératrice n'implique pas une base : $\{\overline{1}\}$ est une famille génératrice du $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ mais n'est pas une base car $\overline{1}.\overline{2} = \overline{0}$ mais $\overline{2} \neq \overline{0}$.*

Exemple 0.67. *1. Soit K un corps. Tout K-espace vectoriel est un K-module libre.*
2. L'anneau des polynômes $A[X]$ est un A-module libre admettant pour base $\{1, X, X^2, X^3, \ldots\}$.
3. Le module $\mathbb{R}^n$ est un $\mathbb{R}$-module libre de type fini admettant pour base la famille $\{(1, 0, ..., 0), \ldots, (0, 0, ..., 1)\}$.

$\boxed{0.6}$ Modules Noethériens

Nous avons vu qu'en général un sous-module d'un module de type fini n'est pas de type fini. Nous allons maintenant étudier une classe de modules pour lesquels cette propriété est vérifiée.

Théorème 0.68. *Soient A un anneau et M un A-module. Les assertions suivantes sont équivalentes :*

i) *(Max) Toute famille non vide de sous modules de M admet un élément maximal (Max : condition du maximum) ;*

ii) *(C.C.A) Toute suite croissante de sous modules de M est stationnaire, (i.e, constante à partir d'un certain rang) (C.C.A : condition des chaines ascendantes) ;*

iii) *(C.F) Tout sous module de M est de type fini (C.F : condition de finitude).*

Démonstration. $i) \Longrightarrow ii)$ Soit $M_1 \subseteq M_2 \subseteq ...$ une suite de sous modules de M. D'après $i)$, $\{M_i\}_{i\in I}$ admet un élément maximal, soit M_r cet élément. Il est clair que $\forall\, n \geqslant r$, $M_n = M_r$.

$ii) \Longrightarrow i)$ Supposons qu'il existe un ensemble $\mathbb{E} \neq \emptyset$ de sous modules de M qui n'admet pas d'élément maximal.
$\star$ $\mathbb{E} \neq \emptyset$, donc il existe $M_1 \in \mathbb{E}$. Puisque $\mathbb{E}$ n'admet pas d'élément maximal, il existe $M_2 \in \mathbb{E}$ tel que $M_1 \subsetneq M_2$. De même pour M_2, il existe $M_3 \in \mathbb{E}$ tel que $M_1 \subsetneq M_2 \subsetneq M_3$. Ainsi, on construit une suite strictement croissante de sous modules de M qui n'est pas stationnaire, ce qui contredit $ii)$. D'où $i)$.

$ii) \Longrightarrow iii)$ Supposons qu'il existe un sous module N de M qui n'est pas de type fini. Soit $a_1 \in N$, alors $a_1A \subsetneq N$ (puisque N n'est pas de type fini). Donc il existe $a_2 \in N$ tel que $M_1 := Aa_1$, $M_2 := Aa_1 + Aa_2$ et $M_1 \subsetneq M_2 \subsetneq N$. De même, il existe $a_3 \in N \backslash M_2$ tel que $M_3 = Aa_1 + Aa_2 + Aa_3$ et $M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq N$. Ainsi, on construit une suite strictement croissante de sous modules de M qui n'est pas stationnaire, ce qui est absurde. D'où *iii*).

iii) $\Longrightarrow$ *ii*) Soit $M_1 \subseteq M_2 \subseteq ... \subseteq M_n \subseteq ...$ une suite croissante de sous modules de M. Soit $N := \bigcup_{j \in I} M_j$. Alors N est un sous module de M, et d'après (*iii*), N est de type fini : $N = Aa_1 + Aa_2 + ... + Aa_n$, où $a_i \in N$ et n est un entier naturel non nul. Il existe n_0 un entier naturel tel que $a_i \in M_{n_0}$ pour tout $i = 1, ..., n$. Ainsi on a $N = M_{n_0}$ et $N = M_{n_0} = M_n$ pour tout $n \geqslant n_0$. Cela termine la preuve du Théorème 0.68. □

Définition 0.69. *On dit qu'un A-module M est Noethérien s'il vérifie les conditions équivalentes du Théorème 0.68.*

Remarque 0.70. *On considère aussi dans l'autre sens la condition de minimum (Min) et celle des chaines descendantes (C.C.D) :*

(Min) Toute famille non vide de sous modules de M admet un élément minimal.

(C.C.D) Toute suite décroissante de sous modules de M est stationnaire.

Il est facile de vérifier que $(Min) \Longleftrightarrow (C.C.D)$. Un A module vérifiant l'une des deux conditions est dit un module Artinien.

Définition 0.71. *On dit que l'anneau A est noethérien s'il est noethérien comme A-module, c-à-d si tout idéal de A est de type fini.*

Exemple 0.72.
1. *Les espaces vectoriels de type fini ; c'est à dire de dimension finie, sont Noethériens.*
2. *Un groupe abelien fini est un $\mathbb{Z}$-module Noethérien.*
3. *Soit k un corps, l'anneau des polynômes $A = k[X_1, ..., X_n, ...]$ avec un nombre infini d'indéterminées n'est pas noethérien. En effet, on a la suite croissante non stationnaire d'idéaux suivante :* $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq ... \subsetneq (X_1, ..., X_n) \subsetneq ...$
4. *Tout anneau principal (et en particulier un corps) est noethérien puisque tous ses ideaux sont principaux donc de type fini.*

Théorème 0.73. *Soit A un anneau, M un A-module et N un sous-module de M. M est noethérien si et seulement si, N et M/N sont noethériens.*

Démonstration. Les sous-modules de N sont des sous-modules de M contenus dans N. Donc, N est noethérien.
D'autre part, $Q = M'/N$, où $M' = \pi^{-1}(Q)$ est un sous-module de M. M est noethérien implique que M' est de type fini, donc Q l'est aussi(car si R de type fini, alors R/S l'est aussi).
Inversement, si, N et M/N sont noethériens. Soit M' un sous-module de M, alors $M' \cap N$ est un sous-module de N donc de type fini. Nous avons $M'/(M' \cap N) \simeq (M' + N)/N$ (sous-module de M/N) or M/N est noethérien donc $M'/(M' \cap N)$ est de type fini, ce qui donne que M' est de type fini(car R et S/R de type finis $\Longrightarrow$ S de type fini). □

Corollaire 0.74. *Soit $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ une suite exacte de A-modules. Alors M est Noethérien si et seulement si L et N sont Noethériens.*

Démonstration. Imf est un sous-module de M tel que $Imf \simeq L/\ker f = L$(car f est injectif et g surjectif). Aussi, $N = Img \simeq M/\ker g = M/Imf$(car $\ker g = Imf$). On conclut à l'aide du théorème 0.73. □

Corollaire 0.75. *Soit M un A-module, et soient N et N' deux sous-modules noethériens de M tels que $M = N + N'$. Alors M est noethérien.*

Démonstration. On a une suite exacte $0 \longrightarrow N \xrightarrow{i} N + N' \xrightarrow{\pi} (N + N')/N \longrightarrow 0$. Or N est noethérien, et $(N + N')/N \simeq N'/(N \cap N')$. Comme N' est noethérien alors $(N + N')/N$, par le corollaire 0.74 $M = N' + N$ qui est noethérien. □

Corollaire 0.76. *Soient M et N des A-modules. Alors $M \oplus N$ est noethérien si et seulement si M et N sont noethériens.*

Démonstration. On utilise la suite exacte $0 \longrightarrow M \xrightarrow{q} M \oplus N \xrightarrow{p} N \longrightarrow 0$. □

Dans les anneaux noethérien, nous avons la caractérisation simple suivante des modules noethérien.

Proposition 0.77. *Soient A un anneau noethérien et M un A-module. Alors M est un A-module noetherien si et seulement s'il est de type fini.*

Démonstration. $\Longrightarrow$ Toujours vrai car M est un sous-module de M.
$\Longleftarrow$ M est de type fini donc M est isomorphe à un quotient d'un module libre de base fini : $M \simeq A^n/N$ avec N un sous-module de A^n. On a $A^n = A \oplus A \oplus ... \oplus A$, n fois, A est noethérien, donc A^n l'est, d'où M est noethérien. □

Exercice 0.78. *Soient A un anneau noethérien et S une partie multiplicative de A. Montrer que $S^{-1}A$ est noethérien.*

L'autre sens n'est pas juste.

Exercice 0.79. *A est noethérien si et seulement si tout idéal premier de A est de type fini.*

Théorème 0.80. *[Théorème de Hilbert]*

Soient A un anneau Noethérien et X une indeterminée sur A. Alors $A[X]$ est Noethérien.

Démonstration. Soit I un idéal de $A[X]$. Pour tout $n \in \mathbb{N}^*$, on pose J_n l'idéal de A engendré par les coefficients dominants des polynômes de degré inférieur ou égal à n dans I. La suite $\{J_n\}_{n \in N^*}$ est une famille croissante d'idéaux de A. Soit $J := \biguplus_n J_n$ qui est un idéal de A, et qui sera de type fini puisque A est Noethérien. Posons $J = (a_1, ..., a_r)$ et soient $f_1, ..., f_r$ les polynômes de I dont les coefficients dominants sont les a_i. Alors chaque $f_i = a_i X^{n_i} + g_i$, avec $n_i = deg(f_i)$ et $deg(g_i) \leqslant n_i - 1$.
Soit $\omega = max\{n_i/1 \leqslant i \leqslant r\}$. Soit f un élément quelconque de I, alors $f = aX^m + g$ où $m = deg(f)$ et $deg(g) \leqslant m - 1$. Par construction $a \in J$ (coefficient dominant de f), donc $a = \sum_{i=1}^r a_i u_i$ où $u_i \in A$. Si $m > \omega$, soit $f' = f - \sum_{i=1}^r u_i f_i X^{m-n_i} \in I$ (car f et $f_i \in I$). Ainsi on a $f \equiv f' mod(f_1, ..., f_r)$. Il suffit donc de traiter les polynômes de degré inférieur ou égal à ω.

Soit B le A-module des polynômes de degré inférieur à ω. Ainsi $(1, X, ..., X^{\omega})$ est une base du A-module libre de type fini B.
Comme A est Noethérien, alors B est Noethérien puisque B est un A-module de type fini. Dés lors, $I \bigcap B$ est de type fini comme idéal de B. Soit $(g_1, ..., g_s)$ un systéme générateur de $I \bigcap B$. On a $f' = \sum_{i=1}^{s} h_i g_i$, $h_i \in B \subseteq A[X]$ et $f = f' + \sum_{i=1}^{r} u_i f_i X^{m-n_i}$, d'où $f \in (g_1, ..., g_s, f_1, ..., f_r)$. Donc $I \subseteq (g_1, ..., g_s, f_1, ..., f_r)$. Or on a tous les $g_i \in I \bigcap B \subseteq I$ et tous les $f_i \in I$, par suite $(g_1, ..., g_s, f_1, ..., f_r) \subseteq I$. Dés lors on a $I = (g_1, ..., g_s, f_1, ..., f_r)$, ce qui termine la preuve du Théorème. □

Corollaire 0.81. *Soient A un anneau noethérien alors $A[X_1, ..., X_n]$ est un anneau noethérien.*

Démonstration. Par récurrence sur n et en utilisant le Théorème de Hilbert. □

Bibliographie

[1] M. F. Atiyah, I. G. Macdonald (1969), Introduction to commutative algebra, AddisonŰWesley.

[2] Josette Calais(2006), Eléments de théorie des anneaux-Anneaux commutatifs, Ellipses.

[3] Najib Mahdou(2013), Introduction à l'Algèbre Homologique, IPNPUB Fez, Morocco.