Chapitre 8

Modules sur les anneaux principaux

Le premier but de ce chapitre est d'introduire la notion de module sur un anneau A (une notion introduite par Dedekind [1] en 1871). Pour faire court, « les modules sont aux anneaux ce que les espaces vectoriels sont aux corps ». L'algèbre linéaire, dite A-linéaire, fait sens de manière intéressante dans cette généralité, et a de très nombreuses applications.

Par exemple, un groupe abélien est strictement la même chose qu'un $\mathbb{Z}$-module, et certaines constructions étudiées au chapitre 3 sont plus naturelles de ce point de vue "additif". En guise d'autre exemple important, il est équivalent d'étudier les classes d'isomorphisme de $k[X]$-modules, disons avec k un corps, et les classes de similitudes d'endomorphismes des k-espaces vectoriels. De plus, les idéaux d'un anneau sont ses sous-modules, et c'est d'ailleurs pour étudier les idéaux que Dedekind a introduit les modules. Enfin, comme nous le verrons plus tard, la notion de module fournit un langage particulièrement adapté à la théorie des représentations.

Dans une première partie, nous développons en l'illustrant le vocabulaire de base de la théorie des modules. Pour l'essentiel, l'anneau A n'y est pas nécessairement commutatif. On montre par exemple que tout sous-module d'un module de type fini sur un anneau noethérien est encore de type fini. On montre aussi que le *rang* d'un A-module libre est bien défini si A est commutatif. En dépit des ressemblances avec la théorie des espaces vectoriels, il faut prendre garde que la plupart des propriétés les plus élémentaires des espaces vectoriels sont en défaut en général pour les modules, comme l'existence des suppémentaires ou certaines propriétés des familles libres et génératrices. L'exemple des $\mathbb{Z}$-modules, bien qu'encore trop simple, est un bon exemple à avoir en tête en première approche.

Dans une seconde partie, nous étudions en détail la structure des modules de type fini sur un anneau principal. Nous suivons une approche matricielle, qui est complémentaire à l'approche par prolongement de caractères mise en avant pour les $\mathbb{Z}$-modules au Chapitre 3. Le théorème principal, dans le cas particulier des $\mathbb{Z}$-modules, se réduit au théorème de structure des groupes abéliens finis ou de type fini. Dans le cas des $k[X]$-modules, il conduit à la notion d'invariants de similitude, et contient par exemple théorie de la réduction de Jordan. Il est assez satisfaisant d'englober dans un même énoncé deux résultats en apparence aussi différents.

1. Voir R. Dedekind, *Theory of algebraic integers*, Cambridge Math. Lib.

1. Modules sur un anneau

1.1. La notion de A-module.

DÉFINITION 1.1. *Soit A un anneau. Un A-module est la donnée d'un groupe abélien*[2] *$(M,+)$ et d'une application $A\times M\to M$, $(a,m)\mapsto a.m$, telle que pour tout $a,a'\in A$ et tout $m,m'\in M$ on ait :*

(M1) $a.(m+m')=a.m+a.m'$,
(M2) $(a+a').m=a.m+a'.m$,
(M3) $a.(a'.m)=(aa').m$,
(M4) $1.m=m$.

On n'a pas supposé A commutatif car cela n'est pas nécessaire. Étant donnés A un anneau, M un groupe abélien et $A\times M\to M,(a,m)\mapsto a.m$ une application quelconque, et comme dans le cas des actions de groupes, on peut reformuler les axiomes (M1)–(M4) en terme des *translations*

$$\mathrm{L}_a : M\to M, m\mapsto a.m.$$

En effet, si on note $(\mathrm{End}_{\mathbb{Z}}(M),+,\circ)$ l'anneau des des applications $\mathbb{Z}$-linéaires $M\to M$ (pour l'addition $+$ des fonctions et la composition $\circ$), on constate que la propriété (M1) se traduit en $\mathrm{L}_a\in\mathrm{End}_{\mathbb{Z}}(M)$ pour tout $a\in A$, et que les axiomes (M2), (M3) et (M4) disent exactement que $A\to\mathrm{End}_{\mathbb{Z}}(M), a\mapsto \mathrm{L}_a$, est un morphisme d'anneaux.

Voici quelques exemples suffisamment intéressants pour justifier ce chapitre.

EXEMPLE 1.2. (i) L'anneau A lui-même peut être vu comme un A-module via l'application $A\times A\to A,(a,b)\mapsto ab$.

(ii) (*Espaces vectoriels*) Si $A=k$ est un corps, un A-module est (par définition) la même chose qu'un k-espace vectoriel.

(iii) ($\mathbb{Z}$-*modules*) Tout groupe abélien M est muni d'une, et une seule, structure de $\mathbb{Z}$-module. En effet, $\mathbb{Z}\times M\to M,(n,m)\mapsto nm$, convient. D'autre part, (M2) montre que pour $m\in M$ alors $\mathbb{Z}\to M, n\mapsto n.m$ est un morphisme de groupes, envoyant 1 sur m par (M4), et donc n sur nm pour tout $n\in\mathbb{Z}$.

EXEMPLE 1.3. (*Polynômes d'endomorphismes*) Soient k un corps, V un k-espace vectoriel et u un endomorphisme de V. L'application $k[X]\times V\to V$, $(P,v)\mapsto P(u)(v)$, est une structure de $k[X]$-module sur le groupe abélien V. En effet, on a $P(u)\in\mathrm{End}(V)$ pour tout $P\in k[X]$, donc (M1). On a aussi

$$(P+Q)(u)=P(u)+Q(u),\ \ (PQ)(u)=P(u)\circ Q(u)\ \text{ et } 1(u)=\mathrm{id}_V$$

dans $\mathrm{End}(V)$, et donc (M2), (M3) et (M4). On note V_u ce $k[X]$-module.

EXEMPLE 1.4. (*Une variante entière sur un exemple*) Soient $d\in\mathbb{Z}$ non carré et $X\in\mathrm{M}_n(\mathbb{Z})$ avec $X^2=d\,1_n$. Alors

$$\mathbb{Z}[\sqrt{d}]\times\mathbb{Z}^n\to\mathbb{Z}^n,(a+b\sqrt{d},v)\mapsto(a+bX)v,$$

est une structure de $\mathbb{Z}[\sqrt{d}]$-module sur $\mathbb{Z}^n$. Elle est bien définie car $1,\sqrt{d}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\sqrt{d}]$. La vérification des axiomes est encore immédiate.

2. Dans ce chapitre, tous les groupes abéliens seront notés additivement.

EXEMPLE 1.5. (*Restriction des scalaires*) Soient $f : A \to B$ un morphisme d'anneaux (par exemple, l'inclusion d'un sous-anneau) et M un B-module. Alors $A \times M \to M, a \mapsto f(a).m$, est une structure de A-module sur M appelé *restriction des scalaires de M à A* (ou mieux à f, pour être plus précis). Par exemple, si M est un $k[X]$-module, sa restriction au morphisme $k \to k[X], \lambda \mapsto \lambda$, est un k-espace vectoriel. Si on note V ce k-espace vectoriel, et si on pose $u : V \to V, v \mapsto X.v$, alors u est k-linéaire et on constate que l'on a $M = V_u$.

NOTATION : Comme pour les groupes et les actions de groupes, on notera souvent $(a, m) \mapsto am$ (plutôt que $a.m$) une loi de A-module.

1.2. Sous-modules. Toutes les constructions que l'on a faites en théorie des groupes abéliens admettent un enrichissement naturel en théorie des modules.

DÉFINITION 1.6. *Soient A un anneau et M un A-module. Un sous-module de M est un sous-groupe $N \subset M$ tel que $an \in N$ pour tout $a \in A$ et $n \in N$. C'est un A-module pour la loi induite $(a, n) \mapsto an$.*

EXEMPLE 1.7. *(i) Les sous-modules du A-module A sont ses idéaux. On parle aussi* d'idéaux à gauche*, si A n'est pas commutatif.*

(ii) Quand A est un corps (resp. $A = \mathbb{Z}$), un sous-module d'un A-module est simplement un sous-espace vectoriel (resp. sous-groupe).

(iii) Les sous-modules du $k[X]$-module V_u sont les sous-espaces vectoriels de V stables par l'endomorphisme u de V.

(iv) Soient M un A-module et $M_1, \ldots, M_n$ des sous-modules de A. Alors la somme $M_1 + \cdots + M_n$ et l'intersection $\cap_{i=1}^n M_i$ des sous-groupes M_i de M sont des sous-A-modules de M.

(v) Si les M_i, $i \in I$, sont des A-modules, alors le groupe abélien produit $\prod_{i\in I} M_i$ est un A-module pour $a.(m_i) = (am_i)$. De même, la somme directe externe de $\oplus_{i\in I} M_i$ des groupes abéliens M_i est un sous A-module de $\prod_{i\in I} M_i$ (éléments dont toutes les coordonnées sauf un nombre fini sont nulles). En particulier, A^I et $A^{(I)}$ sont des A-modules de manière naturelle.

1.3. Applications A-linéaires. La notion de morphisme adéquate pour les modules est la suivante :

DÉFINITION 1.8. *Soient M et N des A-modules. Un morphisme de M vers N, aussi appelé* application A-linéaire*, est une application $f : M \to N$ vérifiant $f(m + m') = f(m) + f(m')$ et $f(am) = af(m)$ pour tout $a \in A$ et $m, m' \in M$.*

L'observation 1.2 (ii) s'étend en disant que tout morphisme de groupes abéliens est automatiquement un morphisme des $\mathbb{Z}$-modules associés. En guise de second exemple, regardons maintenant ce qu'est un morphisme de $k[X]$-modules.

EXEMPLE 1.9. Soient k un corps, V_1 et V_2 deux k-espaces vectoriels, ainsi que u_1 et u_2 des endomorphismes de V_1 et V_2. Pour $i = 1, 2$ on note M_i le $k[X]$-module $(V_i)_{u_i}$. Vérifions qu'un morphisme $M_1 \to M_2$ est exactement une application k-linéaire $f : V_1 \to V_2$ telle que $f \circ u_1 = u_2 \circ f$. En effet, si f est un morphisme, on a $f(v + v') = f(v) + f(v')$ (additivité), $f(\lambda v) = \lambda f(v)$ pour $\lambda \in k$ (prendre $a = \lambda \in k[X]$) et $f(u_1(v)) = u_2(f(v))$ (prendre $a = X \in k[X]$), et donc

$f \circ u_1 = u_2 \circ f$. Réciproquement, ces deux propriétés impliquent manifestement $f(P(u_1)(v)) = P(u_2)f(v)$ pour tout $P \in k[X]$ (considérer les monômes X^k puis conclure par linéarité).

Isomorphismes. Un morphisme bijectif entre deux A-modules est appelé *isomorphisme*, auquel cas son inverse est aussi un morphisme. La composée de deux (iso-)morphismes est encore un (iso-)morphisme. On dit que deux A-modules sont isomorphes s'il existe un isomorphisme entre eux.

EXEMPLE 1.10. Soient V un k-espace vectoriel, a et b deux endomorphismes de V, et V_a et V_b les $k[X]$-modules associés. *Alors V_a et V_b sont isomorphes si, et seulement si, les endomorphismes a et b sont semblables.*

Ainsi, il est équivalent de classifier les $k[X]$-modules à isomorphisme près, disons de k-espace vectoriel sous-jacent de dimension finie n, et de déterminer les classes de similitude d'éléments de $\mathrm{M}_n(k)$.

À ce stade du cours, la proposition suivante est immédiate.

PROPOSITION 1.11. *(i) (Image et noyau) Si M et N sont des A-modules, et $u : M \to N$ est A-linéaire, alors les sous-groupes* $\operatorname{Im} u$ *et* $\ker u$ *sont des sous-A-modules de N et M respectivement.*

(ii) (Quotient par un sous-module) Si N est un sous-A-module de M, il existe une unique structure de A-module sur le groupe quotient M/N telle que la projection canonique $\pi : M \to M/N$ est A-linéaire.

(iii) Pour toute application A-linéaire $u : M \to N$, et pour tout sous-A-module $K \subset \ker u$, l'application quotient $\overline{u} : M/K \to N$ est A-linéaire. Elle est injective si $K = \ker u$, un isomorphisme si en outre $N = \operatorname{Im} u$.

La structure de A-module sur le groupe quotient M/N évoquée au (ii) est bien entendu $(a, m + N) \mapsto am + N$. Le A-module M/N ainsi définit s'appelle *A-module quotient de M par N*.

1.4. Modules monogènes. Pour $m \in M$, on pose $A\,m = \{am \mid a \in A\}$ (*sous-A-module de M engendré par m*) : c'est le plus petit sous-module de M contenant m.

DÉFINITION 1.12. *Un A-module M est dit* monogène *si on a $M = Am$ pour un certain $m \in M$.*

Par exemple, un $\mathbb{Z}$-module monogène est un groupe monogène, un k-espace vectoriel est monogène s'il est de dimension $\leqslant 1$. Considérons A comme A-module comme dans l'Exemple 1.7 (i), lui aussi est monogène ($A = A.1$). Plus généralement, si I est un idéal (=sous-module) de A, le A-module quotient A/I est encore monogène, engendré par la classe de 1 : on a $a.(1 + I) = a + I$ pour tout $a \in A$.

PROPOSITION 1.13. *Tout A-module monogène M est isomorphe à A/I pour un certain idéal (à gauche I) de A.*

DÉMONSTRATION — Soit $m \in M$ avec $M = Am$. L'application $f : A \to M,\ a \mapsto am$, est manifestement A-linéaire, et par hypothèse surjective. Son noyau I est un idéal de A (car un sous-module !) et f induit donc un isomorphisme de A-modules $A/I \simeq M$. □

Exemple 1.14. Pour $A = \mathbb{Z}$ on retrouve bien sûr la classification des groupes abéliens monogènes. Considérons maintenant k un corps et étudions les $k[X]$-modules $M = k[X]/I$, avec I idéal de $k[X]$. Si I est nul, on a $M \simeq k[X]$. En particulier, le k-espace vectoriel sous-jacent est de dimension infinie, avec pour base les X^i pour $i \geqslant 0$. Si I est non nul, on a $I = (P)$ pour un unique polynôme unitaire $P \in k[X]$, disons de degré n. Dans ce cas, la division euclidienne par P assure que tout élément de M est représenté par un unique $Q \in k[X]$ avec $\deg Q < n$. Autrement dit, le k-espace vectoriel sous-jacent à M possède pour base les classes des n éléments $1, X, \ldots, X^{n-1}$. Posons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Comme $XX^{n-1} \equiv -a_{n-1}X^{n-1} - \cdots - a_1X - a_0 \bmod P$, l'endomorphisme de multiplication par X dans cette base a pour matrice

$$\mathrm{C}(P) := \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix} \quad \text{(matrice compagnon de } P\text{)}.$$

1.5. Modules de type fini. Soient $e_1, \ldots, e_n \in M$ des éléments de M. On dispose de l'application A-linéaire

$$u : A^n \to M,\ (a_i) \mapsto \sum_{i=1}^{n} a_i e_i.$$

On dit que $e = \{e_i\}$ est une *famille génératrice* de M si u est surjective, *i.e.* $M = Ae_1 + \cdots + Ae_n$. On dit que e est *libre* si u est injective. On dit enfin que e est une base si elle est libre et génératrice, ou ce qui revient au même, si u est un isomorphisme.

Définition 1.15. *Un A-module est dit* de type fini *s'il possède une famille finie génératrice. Un A-module est dit libre de rang n s'il possède une base à n éléments.*

Par exemple, la famille d'éléments e_i de A^n définis par $(e_i)_j = \delta_{i,j}$ (symbole de Kronecker), est une base à n éléments du A-module A^n ("base canonique"). Par définition, M est donc libre de rang n si, et seulement si, il est isomorphe à A^n. Par conventions, le A-module nul $\{0\} = A^0$ est libre de base la famille vide.

Remarque 1.16.
(i) Il est clair que si $u : M \to N$ est A-linéaire surjective, et si M est de type fini, alors N l'est aussi. En effet, si $M = \sum_{i=1}^{n} Ae_i$ alors $N = u(M) = \sum_{i=1}^{n} A\,u(e_i)$. En particulier, *tout quotient d'un module de type fini est encore de type fini.*
(ii) En revanche, il n'est pas vrai en général qu'un sous-module d'un module de type fini est de type fini. Par exemple, A est toujours de type fini comme module sur lui-même, mais ses sous-modules sont de type fini si, et seulement si, A est noethérien.
(iii) Il n'est pas vrai en général qu'un sous-module d'un module libre : considérer A non principal et $M = A$.

La théorie des $\mathbb{Z}$-modules nous a déjà mise en garde sur le fait que lorsque A n'est pas un corps ces notions ne se comportent pas aussi bien en général que dans le cas des espaces vectoriels. Donnons toutefois deux énoncé positifs très utiles.

THÉORÈME 1.17. *Soit M un module de type fini sur un anneau noethérien. Alors tout sous-module de M est de type fini.*

DÉMONSTRATION — Soit N un sous-module de M. On veut montrer qu'il est de type fini. On procède par récurrence sur le cardinal minimal r d'une famille génératrice de M. On peut supposer M non nul. Considérons d'abord le cas $r = 1$ (M monogène). On a donc $M = Ae$ avec $e \in M$. On constate que $I = \{x \in A \mid xe \in N\}$ est un idéal de A, et aussi $N = Ie$. Mais I est un idéal de A, donc il est de la forme $Af_1 + \cdots + Af_r$ avec $f_i \in A$. On a donc $N = Af_1e + Af_2e + \cdots + Af_re$: il est de type fini.

Supposons maintenant $r > 1$ et écrivons $M = A\,m_1 + \ldots + A\,m_r$ et posons $M' = A\,m_1 + \ldots + A\,m_{r-1}$. On regarde la projection canonique

$$\pi : M \to M/M', m \mapsto m + M',$$

qui est A-linéaire de noyau M'. Le A-module M/M' est manifestement engendré par la classe de m_r, donc monogène. Par le cas $r = 1$, le sous-module $\pi(N)$ de M/M' est donc de type fini, disons engendré par les éléments $\pi(n_1), \cdots, \pi(n_s)$ avec $n_i \in N$. On a alors

$$N = N \cap M' + \sum_{i=1}^{s} A\,n_i.$$

En effet, l'inclusion $\supset$ est claire. Pour l'autre, on constate que pour $n \in N$, on a $\pi(n) \in \pi(N)$ et donc $\pi(n) = \sum_{i=1}^{s} a_i\pi(n_i)$ pour certains $a_1, \ldots, a_s \in A$, puis $n - \sum_{i=1}^{s} a_i\,n_i \in (\ker \pi) \cap N = M' \cap N$, et donc $n \in N' + M' \cap N$. Pour conclure, on constate que M' est engendré par $\leqslant r - 1$ éléments, et que $N \cap M'$ en est un sous-module, donc finiment engendré par récurrence. □

THÉORÈME 1.18. *Soient A un anneau commutatif non nul et m, n des entiers $\geqslant 0$. Les A-modules A^m et A^n sont isomorphes si, et seulement si, on a $m = n$. En particulier, toutes les bases d'un A-module libre de rang fini ont même cardinal.*

L'énoncé est inexact si A n'est pas commutatif : pour $A = \mathrm{End}_k(k^{(\mathbb{N})})$ on a $A \simeq A^2$ (voir l'Exercice 8.10).

DÉMONSTRATION — (On utilise quelques résultats du Complément §9 Chap. 7). Soient M un idéal maximal de A et k le corps quotient A/M. On regarde la projection naturelle $f : A^m \to k^m$, $(a_i) \mapsto (a_i \bmod M)$. Si $e_1, \ldots, e_n$ est une famille génératrice du A-module A^m, alors les $f(e_i)$ forment une famille génératrice du k-espace vectoriel k^m. On a donc $n \geqslant m$ par la théorie des espaces vectoriels. Ainsi, le cardinal d'une famille génératrice minimale du A-module A^m est m. Cela démontre le théorème. □