

Algèbre I — Master 1

Séance 3 — Modules

Morphismes, quotients, sommes directes et modules simples

But de la séance. Installer le langage qui unifie les groupes abéliens, les espaces vectoriels, les endomorphismes et les représentations. Nous étudierons les constructions fondamentales de la catégorie des modules, puis les notions de module simple et indécomposable.

Table des matières

1	Modules à gauche, à droite et bimodules	1
1.1	Définition	1
1.2	Premiers exemples	2
2	Morphismes de modules	3
2.1	Modules cycliques, générateurs et annulateurs	3
3	Sous-modules, quotients et théorèmes d'isomorphisme	4
3.1	Sous-modules et quotients	4
3.2	Noyau, image et conoyau	4
3.3	Deux autres théorèmes d'isomorphisme	5
4	Sommes directes et produits	5
4.1	Produit d'une famille de modules	5
4.2	Somme directe	5
4.3	Somme interne	6
5	Projecteurs et décompositions	6
6	Modules simples et indécomposables	6
6.1	Définitions et premiers exemples	6
6.2	Lemme de Schur	7
7	Compléments	7
7.1	Modules de longueur finie et Jordan–Hölder	7
7.2	Représentations de carquois	8
7.3	Algèbre de Weyl et algèbres enveloppantes	8
7.4	Modules indécomposables et idempotents	8
	À retenir	9

1. Modules à gauche, à droite et bimodules

1.1. Définition

Soit A un anneau unitaire, non nécessairement commutatif.

Définition 1.1. Un A -module à gauche est un groupe abélien $(M, +)$ muni d'une application

$$A \times M \longrightarrow M, \quad (a, m) \longmapsto am,$$

telle que, pour tous $a, b \in A$ et $m, n \in M$,

$$a(m + n) = am + an, qquad(a + b)m = am + bm, qquad(ab)m = a(bm), qquad 1_A m = m.$$

Autrement dit, faire de M un A -module à gauche revient à donner un morphisme d'anneaux

$$A \longrightarrow \text{End}_{\mathbb{Z}}(M),$$

où le produit dans l'anneau des endomorphismes est la composition.

Un A -module à droite est défini de même à l'aide d'une loi $M \times A \rightarrow M$, $(m, a) \mapsto ma$, satisfaisant notamment $(ma)b = m(ab)$. Si A^{op} désigne l'anneau opposé, dont la multiplication est $a \star b = ba$, alors

$$\{A\text{-modules à droite}\} = \{A^{\text{op}}\text{-modules à gauche}\}.$$

Lorsque A est commutatif, un module à gauche devient canoniquement un module à droite en posant $ma = am$; on parle simplement de A -module.

Définition 1.2. Soient A et B deux anneaux. Un (A, B) -bimodule est un groupe abélien M qui est à la fois un A -module à gauche et un B -module à droite, les deux actions vérifiant

$$(am)b = a(mb) \quad (a \in A, b \in B, m \in M).$$

L'anneau A est naturellement un (A, A) -bimodule par multiplication à gauche et à droite. Si $f: A \rightarrow B$ est un morphisme d'anneaux, B est un (A, B) -bimodule par $a \cdot b = f(a)b$. Les bimodules seront indispensables pour le produit tensoriel et le changement des scalaires.

1.2. Premiers exemples

Exemple 1.3 (Groupes abéliens et espaces vectoriels). Les $\mathbb{Z}$ -modules sont exactement les groupes abéliens : l'action est nécessairement donnée par

$$n \cdot m = \underbrace{m + \cdots + m}_{n \text{ fois}}$$

pour $n \geq 0$, puis par passage aux opposés pour $n < 0$. Si $\mathbf{k}$ est un corps, les $\mathbf{k}$ -modules sont exactement les espaces vectoriels sur $\mathbf{k}$.

Exemple 1.4 (Le module régulier). L'anneau A , muni de la multiplication à gauche, est un A -module noté ${}_A A$. Ses sous-modules sont exactement les idéaux à gauche de A . De même, les sous-modules de A_A sont les idéaux à droite.

Exemple 1.5 (Un endomorphisme). Soit $\mathbf{k}$ un corps. Donner à un $\mathbf{k}$ -espace vectoriel V une structure de $\mathbf{k}[T]$ -module revient à choisir un endomorphisme $u \in \text{End}_{\mathbf{k}}(V)$. À u , on associe l'action

$$P(T) \cdot v = P(u)(v).$$

Réciproquement, l'action de T sur un $\mathbf{k}[T]$ -module est un endomorphisme $\mathbf{k}$ -linéaire de l'espace vectoriel sous-jacent.

Plus généralement :

- un $\mathbf{k}[T_1, \dots, T_r]$ -module est un espace vectoriel muni de r endomorphismes qui commutent deux à deux ;
- un module sur l'algèbre libre non commutative $\mathbf{k}\langle T_1, \dots, T_r \rangle$ est un espace vectoriel muni de r endomorphismes quelconques ;
- un $\mathbf{k}[G]$ -module est une représentation linéaire du groupe G .

Exemple 1.6 (Modules quotients). Si I est un idéal à gauche de A , le groupe quotient A/I est un A -module à gauche. Si A est commutatif, tout A/I -module devient par restriction des scalaires un A -module sur lequel les éléments de I agissent par zéro.

2. Morphismes de modules

Définition 2.1. Soient M, N deux A -modules à gauche. Un *morphisme de A -modules* est une application $f: M \rightarrow N$ telle que

$$f(m + m') = f(m) + f(m'), \text{ et } f(am) = af(m).$$

On note $\text{Hom}_A(M, N)$ l'ensemble de ces morphismes.

La somme ponctuelle fait de $\text{Hom}_A(M, N)$ un groupe abélien. Si A est commutatif, c'est même un A -module pour

$$(af)(m) = af(m).$$

Dans le cas non commutatif, cette formule ne définit en général pas un morphisme A -linéaire. Enfin, $\text{End}_A(M) = \text{Hom}_A(M, M)$ est un anneau pour l'addition et la composition ; son groupe des unités est $\text{Aut}_A(M)$.

Exemple 2.2. Soient (V, u) et (W, v) les $\mathbf{k}[T]$ -modules associés à deux endomorphismes. Une application $\mathbf{k}$ -linéaire $f: V \rightarrow W$ est $\mathbf{k}[T]$ -linéaire si et seulement si le carré

$$\begin{array}{ccc} V & \xrightarrow{u} & V \\ f \downarrow & & \downarrow f \\ W & \xrightarrow{v} & W \end{array}$$

commute, c'est-à-dire si $f \circ u = v \circ f$.

2.1. Modules cycliques, générateurs et annulateurs

Si $S \subseteq M$, le *sous-module engendré* par S est

$$\langle S \rangle_A = \left\{ \sum_{i=1}^r a_i s_i \mid r \geq 0, a_i \in A, s_i \in S \right\}.$$

Le module est *de type fini* s'il admet une famille génératrice finie, et *cyclique* s'il est engendré par un seul élément.

Si $m \in M$, l'application

$$A \longrightarrow M, \quad a \longmapsto am,$$

a pour image le sous-module cyclique Am et pour noyau l'idéal à gauche

$$\text{Ann}_A(m) = \{a \in A \mid am = 0\}.$$

Le premier théorème d'isomorphisme donnera donc $Am \simeq A / \text{Ann}_A(m)$ comme A -modules à gauche.

L'*annulateur du module* est

$$\text{Ann}_A(M) = \{a \in A \mid am = 0 \text{ pour tout } m \in M\}.$$

C'est un idéal bilatère. Le module M est dit *fidèle* si $\text{Ann}_A(M) = 0$, ou de manière équivalente si le morphisme $A \rightarrow \text{End}_{\mathbb{Z}}(M)$ est injectif.

3. Sous-modules, quotients et théorèmes d'isomorphisme

3.1. Sous-modules et quotients

Définition 3.1. Une partie $N \subseteq M$ est un *sous- A -module* si c'est un sous-groupe additif et si $aN \subseteq N$ pour tout $a \in A$.

Il suffit de vérifier que N est non vide et que

$$x, y \in N, a, b \in A \implies ax + by \in N.$$

Les intersections de sous-modules sont des sous-modules. La somme d'une famille $(N_i)_{i \in I}$ de sous-modules est

$$\sum_{i \in I} N_i = \left\{ n_{i_1} + \cdots + n_{i_r} \mid r \geq 0, n_{i_j} \in N_{i_j} \right\}.$$

Si $N \subseteq M$ est un sous-module, le groupe quotient M/N possède une unique structure de A -module telle que la projection $\pi: M \rightarrow M/N$ soit A -linéaire :

$$a(m + N) = am + N.$$

Proposition 3.2 (Propriété universelle du quotient). *Si $f: M \rightarrow P$ est A -linéaire et $N \subseteq \text{Ker}(f)$, il existe un unique morphisme $\bar{f}: M/N \rightarrow P$ tel que $f = \bar{f} \circ \pi$. Il est donné par $\bar{f}(m + N) = f(m)$.*

3.2. Noyau, image et conoyau

Soit $f: M \rightarrow N$ un morphisme de A -modules. On définit

$$\text{Ker}(f) = \{m \in M \mid f(m) = 0\}, \quad \text{Im}(f) = \{f(m) \mid m \in M\},$$

qui sont des sous-modules de M et N , ainsi que le *conoyau*

$$\text{Coker}(f) = N/\text{Im}(f).$$

On a

$$f \text{ injectif} \iff \text{Ker}(f) = 0, \quad f \text{ surjectif} \iff \text{Coker}(f) = 0.$$

Le morphisme f se factorise canoniquement comme

$$M \twoheadrightarrow M/\text{Ker}(f) \xrightarrow{\bar{f}} \text{Im}(f) \hookrightarrow N.$$

Théorème 3.3 (Premier théorème d'isomorphisme). *Le morphisme induit*

$$\bar{f}: M/\text{Ker}(f) \longrightarrow \text{Im}(f), \quad m + \text{Ker}(f) \longmapsto f(m),$$

est un isomorphisme de A -modules.

Démonstration. La propriété universelle du quotient donne $\bar{f}$. Il est surjectif par définition de l'image. Si $\bar{f}(m + \text{Ker}(f)) = 0$, alors $f(m) = 0$, donc $m \in \text{Ker}(f)$ et la classe de m est nulle. Ainsi $\bar{f}$ est injectif. $\square$

Exemple 3.4. Pour $n \geq 1$, le morphisme de $\mathbb{Z}$ -modules $\mathbb{Z} \rightarrow \mathbb{Z}$, $a \mapsto na$, est injectif, son image est $n\mathbb{Z}$, et son conoyau est $\mathbb{Z}/n\mathbb{Z}$. Le premier théorème donne $\mathbb{Z} \simeq n\mathbb{Z}$ comme groupes abéliens.

3.3. Deux autres théorèmes d'isomorphisme

Proposition 3.5. Soient N, P deux sous-modules de M .

1. Il existe un isomorphisme canonique

$$(N + P)/P \simeq N/(N \cap P).$$

2. Si $N \subseteq P$, alors P/N est un sous-module de M/N et

$$(M/N)/(P/N) \simeq M/P.$$

Démonstration. Pour le premier point, on applique le premier théorème d'isomorphisme au morphisme $N \rightarrow (N + P)/P$. Pour le second, on l'applique au morphisme surjectif $M/N \rightarrow M/P$, $m + N \mapsto m + P$. $\square$

Théorème 3.6 (Correspondance des sous-modules). La projection $M \rightarrow M/N$ induit une bijection, compatible aux inclusions, entre les sous-modules de M contenant N et les sous-modules de M/N :

$$P \mapsto P/N, \quad \bar{P} \mapsto \pi^{-1}(\bar{P}).$$

4. Sommes directes et produits

4.1. Produit d'une famille de modules

Soit $(M_i)_{i \in I}$ une famille de A -modules à gauche. Le produit cartésien

$$\prod_{i \in I} M_i$$

est un A -module pour les opérations composante par composante. Les projections $p_i: \prod_j M_j \rightarrow M_i$ satisfont la propriété universelle : pour tout A -module N , l'application

$$\mathrm{Hom}_A\left(N, \prod_{i \in I} M_i\right) \longrightarrow \prod_{i \in I} \mathrm{Hom}_A(N, M_i), \quad f \mapsto (p_i \circ f)_i,$$

est une bijection.

4.2. Somme directe

La *somme directe* est le sous-module du produit formé des familles à support fini :

$$\bigoplus_{i \in I} M_i = \left\{ (m_i)_i \in \prod_i M_i \mid m_i = 0 \text{ sauf pour un nombre fini de } i \right\}.$$

Les inclusions $j_i: M_i \rightarrow \bigoplus_j M_j$ satisfont la propriété universelle : pour tout A -module N ,

$$\mathrm{Hom}_A\left(\bigoplus_{i \in I} M_i, N\right) \longrightarrow \prod_{i \in I} \mathrm{Hom}_A(M_i, N), \quad f \mapsto (f \circ j_i)_i,$$

est une bijection.

Si I est fini, somme directe et produit coïncident. Pour deux modules, on écrit $M \oplus N$; il est à la fois produit et somme, avec

$$p_M j_M = \mathrm{id}_M, \quad p_N j_N = \mathrm{id}_N, \quad p_M j_N = p_N j_M = 0, \quad j_M p_M + j_N p_N = \mathrm{id}_{M \oplus N}.$$

Pour une famille infinie de modules non nuls, l'inclusion $\bigoplus_i M_i \subseteq \prod_i M_i$ est en général stricte. Par exemple,

$$\bigoplus_{n \geq 0} \mathbb{Z} = \{(a_n) \in \mathbb{Z}^{\mathbb{N}} \mid a_n = 0 \text{ pour presque tout } n\} \subsetneq \mathbb{Z}^{\mathbb{N}}.$$

4.3. Somme interne

Soient N, P deux sous-modules de M . Le morphisme

$$N \oplus P \longrightarrow M, \quad (n, p) \longmapsto n + p,$$

a pour image $N + P$ et pour noyau $\{(x, -x) \mid x \in N \cap P\}$. Il est donc un isomorphisme sur M si et seulement si

$$M = N + P \quad \text{et} \quad N \cap P = 0.$$

Dans ce cas, on écrit $M = N \oplus P$ et l'on dit que N et P sont des *facteurs directs* de M .

5. Projecteurs et décompositions

Définition 5.1. Un *projecteur* d'un A -module M est un endomorphisme $e \in \text{End}_A(M)$ tel que $e^2 = e$.

Théorème 5.2 (Projecteurs et sommes directes). *Pour tout projecteur e de M , on a une décomposition canonique*

$$M = \text{Im}(e) \oplus \text{Ker}(e).$$

Réciproquement, une décomposition $M = N \oplus P$ définit un projecteur de M sur N parallèlement à P .

Démonstration. Pour $m \in M$,

$$m = e(m) + (m - e(m)).$$

Le premier terme appartient à $\text{Im}(e)$ et le second à $\text{Ker}(e)$, puisque $e(m - e(m)) = e(m) - e^2(m) = 0$. Si $x \in \text{Im}(e) \cap \text{Ker}(e)$, écrivons $x = e(y)$; alors $x = e(y) = e^2(y) = e(x) = 0$. La somme est donc directe.

Réciproquement, si tout m s'écrit de manière unique $m = n + p$, on pose $e(m) = n$. Cette application est A -linéaire, vérifie $e^2 = e$, et a pour image N et pour noyau P . $\square$

Corollaire 5.3. *Un sous-module $N \subseteq M$ est facteur direct si et seulement si l'inclusion $i: N \hookrightarrow M$ possède une rétraction $r: M \rightarrow N$, c'est-à-dire un morphisme tel que $r \circ i = \text{id}_N$.*

Exemple 5.4. Comme $\mathbb{Z}$ -module, $2\mathbb{Z}$ n'est pas facteur direct de $\mathbb{Z}$. En effet, une rétraction $r: \mathbb{Z} \rightarrow 2\mathbb{Z}$ vérifierait $r(2) = 2$, donc $2r(1) = 2$ et $r(1) = 1$, ce qui est impossible puisque $r(1) \in 2\mathbb{Z}$.

Exemple 5.5. Soit V un espace vectoriel. Tout sous-espace $W \subseteq V$ possède un supplémentaire, donc est facteur direct. Ce phénomène repose sur l'existence d'une base et devient faux pour les modules sur un anneau quelconque, comme le montre l'exemple précédent.

6. Modules simples et indécomposables

6.1. Définitions et premiers exemples

Définition 6.1. Un A -module S est *simple* s'il est non nul et si ses seuls sous-modules sont 0 et S .

Un A -module M non nul est *indécomposable* s'il n'existe pas de décomposition $M = M_1 \oplus M_2$ avec M_1 et M_2 non nuls.

Tout module simple est indécomposable. La réciproque est fautive : le $\mathbb{Z}$ -module $\mathbb{Z}$ est indécomposable, car ses seuls idempotents comme anneau d'endomorphismes sont 0 et 1, mais il n'est pas simple puisque $n\mathbb{Z} \subsetneq \mathbb{Z}$ pour $n \geq 2$.

Proposition 6.2. *Tout module simple est cyclique. Plus précisément, si S est simple et $0 \neq s \in S$, alors $S = As$ et*

$$S \simeq A / \text{Ann}_A(s).$$

L'idéal à gauche $\text{Ann}_A(s)$ est maximal parmi les idéaux à gauche propres de A .

Corollaire 6.3. *Si A est commutatif, les A -modules simples sont, à isomorphisme près, les modules $A/\mathfrak{m}$, où $\mathfrak{m}$ parcourt les idéaux maximaux de A .*

Exemple 6.4. Les $\mathbb{Z}$ -modules simples sont les groupes $\mathbb{Z}/p\mathbb{Z}$, pour p premier. Les $\mathbf{k}[T]$ -modules simples sont les $\mathbf{k}[T]/(P)$, où P est irréductible. Si $\mathbf{k}$ est algébriquement clos, ils sont tous de dimension 1 sur $\mathbf{k}$, avec T agissant par un scalaire.

6.2. Lemme de Schur

Théorème 6.5 (Lemme de Schur). *Soient S, T deux A -modules simples. Tout morphisme non nul $f: S \rightarrow T$ est un isomorphisme.*

Démonstration. Le noyau de f est un sous-module de S . Comme $f \neq 0$, ce noyau ne peut être S , donc il est nul et f est injectif. L'image de f est un sous-module non nul de T , donc elle est égale à T et f est surjectif. $\square$

Corollaire 6.6. *Si S est simple, tout endomorphisme non nul de S est inversible. Ainsi $\text{End}_A(S)$ est une algèbre à division.*

Corollaire 6.7 (Cas d'un corps algébriquement clos). *Supposons que A soit une $\mathbf{k}$ -algèbre, que $\mathbf{k}$ soit algébriquement clos et que S soit un A -module simple de dimension finie sur $\mathbf{k}$. Alors*

$$\text{End}_A(S) = \mathbf{k} \text{ id}_S.$$

Démonstration. Pour $u \in \text{End}_A(S)$, l'endomorphisme $\mathbf{k}$ -linéaire u possède une valeur propre $\lambda \in \mathbf{k}$. L'endomorphisme $u - \lambda \text{ id}_S$ n'est pas inversible. D'après le lemme de Schur, il est donc nul. $\square$

Remarque 6.8. L'hypothèse sur le corps est essentielle. Par exemple, la représentation réelle de dimension 2 du groupe cyclique C_4 donnée par une rotation d'angle $\pi/2$ est simple sur $\mathbb{R}$, mais son anneau d'endomorphismes est isomorphe à $\mathbb{C}$.

7. Compléments

7.1. Modules de longueur finie et Jordan–Hölder

Définition 7.1. Une *série de composition* d'un A -module M est une chaîne finie

$$0 = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$$

telle que chaque quotient M_i/M_{i+1} soit simple. Lorsqu'une telle chaîne existe, M est dit de *longueur finie*.

Théorème 7.2 (Jordan–Hölder pour les modules). *Deux séries de composition d'un même module ont la même longueur et les mêmes facteurs simples, à permutation et isomorphisme près.*

La longueur $\ell_A(M)$ est donc bien définie et additive dans les suites exactes courtes : si $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ est exacte et si deux des trois modules sont de longueur finie, alors le troisième l'est et

$$\ell_A(M) = \ell_A(M') + \ell_A(M'').$$

Par exemple, la longueur du $\mathbb{Z}$ -module $\mathbb{Z}/n\mathbb{Z}$ est le nombre de facteurs premiers de n , comptés avec multiplicité.

7.2. Représentations de carquois

Un *carquois* $Q = (Q_0, Q_1)$ est un graphe orienté. Son algèbre des chemins $\mathbf{k}Q$ a pour base les chemins orientés, y compris les chemins constants aux sommets ; le produit est la concaténation lorsqu'elle est définie, et zéro sinon. Un $\mathbf{k}Q$ -module équivaut à la donnée :

- d'un espace vectoriel V_i pour chaque sommet $i \in Q_0$;
- d'une application linéaire $V_i \rightarrow V_j$ pour chaque flèche $i \rightarrow j$.

Ainsi, les modules permettent d'étudier simultanément des systèmes d'espaces vectoriels et d'applications linéaires.

Exemple 7.3. Pour le carquois $1 \longrightarrow 2$, un module est simplement une application linéaire $f: V_1 \rightarrow V_2$. Sa décomposition en représentations indécomposables reformule la réduction de f à sa forme normale déterminée par son rang.

7.3. Algèbre de Weyl et algèbres enveloppantes

La première algèbre de Weyl est

$$A_1(\mathbf{k}) = \mathbf{k}\langle x, \partial \rangle / (\partial x - x\partial - 1).$$

Un $A_1(\mathbf{k})$ -module est un espace vectoriel muni de deux endomorphismes X, D vérifiant $DX - XD = \text{id}$. L'espace $\mathbf{k}[x]$ en est un module naturel : X agit par multiplication par x et D par dérivation.

Si $\mathfrak{g}$ est une algèbre de Lie sur $\mathbf{k}$, son algèbre enveloppante universelle $U(\mathfrak{g})$ est l'algèbre associative engendrée par $\mathfrak{g}$ avec les relations

$$xy - yx = [x, y].$$

Les représentations de $\mathfrak{g}$ sont exactement les $U(\mathfrak{g})$ -modules. Ces deux exemples illustrent le même principe que $\mathbf{k}[G]$: une théorie de représentations peut être reformulée comme une théorie de modules sur une algèbre associative.

7.4. Modules indécomposables et idempotents

Le théorème des projecteurs montre qu'un module M est indécomposable si et seulement si les seuls idempotents de $\text{End}_A(M)$ sont 0 et 1. Cela ne signifie pas que $\text{End}_A(M)$ soit une algèbre à division : cette conclusion est propre aux modules simples.

Par exemple, pour $A = \mathbf{k}[\varepsilon]/(\varepsilon^2)$, le module régulier ${}_AA$ est indécomposable, car A est local et n'a pas d'idempotent non trivial. Il n'est pourtant pas simple : (ε) est un sous-module propre non nul, et la multiplication par ε est un endomorphisme non nul mais non inversible.

À retenir

- Une structure de A -module sur M est un morphisme $A \rightarrow \text{End}_{\mathbb{Z}}(M)$; elle encode une famille d'opérateurs satisfaisant les relations de A .
- Noyaux, images, conoyaux et quotients sont encore des A -modules. Pour tout morphisme f , on a $M/\text{Ker}(f) \simeq \text{Im}(f)$.
- La somme directe représente les familles de morphismes sortant des facteurs ; le produit représente les familles de morphismes entrant dans les facteurs.
- Les décompositions en somme directe de M correspondent exactement aux projecteurs de $\text{End}_A(M)$.
- Un module simple est cyclique et indécomposable. Tout morphisme non nul entre modules simples est un isomorphisme.
- Sur un anneau commutatif, les modules simples sont les corps résiduels $A/\mathfrak{m}$.