Introduction à la théorie des modules

Version du 14 décembre 2017 à 18:34

Table des matières

Chapitre 1

Généralités sur les modules

1.1 La catégorie des A-modules

A est anneau unitaire, non nécessairement commutatif.

1.1.1 Objets

Définition 1.1.1. Un A-module à gauche est la donnée d'un groupe abélien $(M,+)$ et d'une loi externe $A \times M \to M$, notée $\times$ satisfaisant les conditions suivantes :

— distributivité

— distributivité

— associativité

— action de 1_A triviale

En général, on note la loi externe avec un point au lieu de $\times$, voire on omet de la noter. Les éléments de A sont appelés les *scalaires*.

Remarque 1.1.2. Il revient au même de donner une structure de A-module sur un groupe abélien M, ou de donner un morphisme d'anneaux entre A et l'anneau des endomorphismes de groupe de M.

Exercice 1.1.3. Il existe une définition de A-module à droite qui est semblable. Écrire la définition. Que devient la remarque précédente pour les modules à droite ?

Dans la suite, on parlera surtout de modules à gauche, et on écrit *module* au lieu de *module à gauche*. Si des modules à droite apparaissent, ce sera signalé. Les modules à droite ont aussi quelques avantages et apparaissent de façon naturelle dans certains contextes.

Remarque 1.1.4. Si l'anneau A est commutatif, on ne fait pas la différence entre modules à gauche et à droite et on écrit juste module.

Exercice 1.1.5 (Règles de calcul)**.** Soit M un A-module. Montrer :

— $\forall m \in M, 0_A.m = 0_M$;

— $\forall m \in M, (-1_A)m = -m$;
— $\forall a \in A, a0_M = 0_M$.

Exemple 1.1.6. Voici quelques exemples de modules.

— Le groupe abélien 0 à un élément a une unique structure de A-module. C'est le module nul.
— L'anneau A est un A-module, avec comme loi externe la multiplication de l'anneau.
— Tout groupe abélien a une unique structure de $\mathbb{Z}$-module : si $n \in \mathbb{Z}$ et $x \in M$, on est obligé de définir $n \cdot x = x + x + \ldots + x$.
— Si A est un corps, les A-modules sont exactement les A-espaces vectoriels.
— $A[X]$ est un A-module.
— Si M est un A-module et $f : B \to A$ est un morphisme d'anneaux, alors l'application

$$\times_B : B \times M \to M, (b, m) \mapsto f(b)m$$

munit M d'une structure de B-module. (Utile pour $B = Z(A)$ pour avoir un module sur un anneau commutatif par exemple.)

Exemple 1.1.7 (fondamental)**.** Soit V un K-ev, et f un endomorphisme (d'espace vectoriel) de E. Alors on définit :

$$\mu : K[X] \times V \to V, \quad (P, v) \mapsto P(f)(v),$$

où $P(f)(v)$ est le polynôme d'endomorphisme $P(f)$ appliqué au vecteur v. Exercice : vérifier que ceci munit le K-ev V d'une structure de $K[X]$-module. Cet exemple est fondamental.

Dans les exemples qui suivent, l'anneau A n'est pas commutatif.

Exemple 1.1.8. Soit G un groupe, k un corps et $A = k[G]$ l'algèbre du groupe sur k (voir les rappels sur les anneaux). Alors un A-module à gauche est la même chose qu'une k-représentation de G, c'est-à-dire un k-espace vectoriel V et une action à gauche de G sur V par automorphismes linéaires.

Exemple 1.1.9. Soit k un corps, $n \in \mathbb{N}$ et $A = M_n(k)$. Alors k^n est un A-module à gauche. Plus généralement, si V est un k-ev, alors V est un $\mathrm{End}_k(V)$-module à gauche.

Définition 1.1.10. Soit I un ensemble (fini ou infini), M un A-module, $(x_i)_{i \in I}$ une famille d'éléments de M. Une combinaison linéaire des x_i est un élément de M de la forme $\sum\limits_{i \in I} a_i x_i$, où $(a_i)_{i \in I}$ est une famille presque nulle (on dit aussi : à support fini) d'éléments de A.

1.1.2 Morphismes

Définition 1.1.11 (Morphisme)**.** Soient M et N deux A-modules. Une application $f : M \to N$ est dite A-linéaire si c'est un morphisme de groupe abélien et qu'elle est compatible avec la loi externe, autrement dit $\forall a \in A, \forall m \in M, f(am) = af(m)$.

On dit juste morphisme au lieu de : application A-linéaire, etc.

Exemple 1.1.12. Le morphisme nul.

Exercice 1.1.13. Une application $f : M \to N$ est A-linéaire ssi :

$$\forall a, b \in A, \forall m, n \in M, f(am + bn) = af(m) + bf(n).$$

On montre par récurrence que $f(\sum a_i x_i) = \sum a_i f(x_i)$.

Définition 1.1.14. On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de M dans N. Un morphisme de M dans lui-même est un endomorphisme. On note $\mathrm{End}_A(M)$ l'ensemble des endomorphismes de M.

Proposition 1.1.15. La composée de deux applications A-linéaires est A-linéaire.

Définition 1.1.16. Un diagramme de modules est la donnée de modules M_i et de morphismes $f_{ij} : M_i \to M_j$. On dit que le diagramme commute si $\forall i, j$, tous les morphismes de M_i vers M_j obtenus en composant des morphismes du diagramme sont égaux.

Exemple : triangle commutatif, carré commutatif.

Définition 1.1.17. Un morphisme $f : M \to N$ est un isomorphisme s'il existe un morphisme $g : N \to M$ tel que $f \circ g = \mathrm{Id}_N$ et $g \circ f = \mathrm{Id}_M$.

Proposition 1.1.18. Un morphisme $f : M \to N$ est un isomorphisme si et seulement s'il est bijectif.

Démonstration. La preuve est la même que pour les espaces vectoriels. Un isomorphisme est forcément bijectif vu la définition. Montrons que si un morphisme est bijectif, son application réciproque g est A-linéaire. Soient n et n' des éléments de M, et m, m' les antécédents par f, c'est-à-dire $n = g(m)$ et $m' = g(n')$. Alors, pour $a, b \in A$ on a :

$$\begin{aligned} g(an + bn') &= g(af(m) + bf(m')) \\ &= g(f(am + bm')) \quad \text{(car } f \text{ est linéaire)} \\ &= am + bm' \\ &= ag(n) + bg(n'). \end{aligned}$$

□

Exercice 1.1.19. Soit $a \in A$, et $\phi_a : M \to M, m \mapsto am$ l'homothétie de rapport a. C'est un morphisme de groupe abélien. Déterminer des conditions pour que ϕ soit : un endomorphisme ; un automorphisme.

Remarque 1.1.20 (Morphismes de A dans un A-module)**.** Un morphisme de A dans M est déterminé par l'image de 1_A. Autrement dit, l'application

$$\mathrm{Hom}_A(A, M) \to M,$$

$$f \mapsto f(1_A)$$

est une bijection.

1.1.3 Sous-objets et quotients

Définition 1.1.21. Soit M un module. Un sous-module est un sous-groupe $N \subset M$ qui est stable par la loi externe : $\forall a \in A, \forall n \in N, an \in N$.

Exemple 1.1.22. Le module nul et A sont des sous-modules de A.

Les sous-modules d'un $\mathbb{Z}$-module sont ses sous-groupes.

Les sous-modules du A-module à gauche A sont les idéaux à gauche de A.

Les sous-modules de $\mathbb{Z}$ sont les $n\mathbb{Z}$.

Si A est un corps, les sous-modules sont les sous-espaces vectoriels.

Si M est un A-module à gauche et I est un idéal à gauche de A, alors IM est un sous-module de M.

Exemple 1.1.23. Les sous-modules de (V, f) de l'exemple fondamental sont les sous-k-ev de V stables par le k-endomorphisme f.

Exemple 1.1.24. Les sous-modules d'une représentation d'un groupe sont les sous-représentations : les sous-ev stables sous l'action du groupe.

Proposition 1.1.25. Les images directes et réciproques de sous-modules par des morphismes sont des sous-modules.

Proposition–Définition 1.1.26 (Quotients)**.** Soit N un sous-module de M.

1. Il existe un module Q et un morphisme $\pi = M \to Q$ vérifiant la propriété (dite universelle) suivante (on dit aussi : « solution du problème universel suivant ») :
   Pour tout module P et tout morphisme $\phi : M \to P$ tel que $\phi(N) = 0$ (autrement dit $N \subset \operatorname{Ker}\phi$), il existe un unique morphisme $\bar{\phi} = Q \to P$ tel que $\phi = \bar{\phi} \circ \pi$.
2. Un tel couple (Q, π) est unique à unique isomorphisme près, c'est-à-dire que si $(Q', \pi' : M \to Q')$ est une autre solution du problème universel, alors il existe un unique isomorphisme $\psi : Q \to Q'$ tel que $\pi' = \psi \circ \pi$.

Démonstration. Unicité. Puis, existence : le groupe abélien quotient M/N a structure de A-module telle que la projection canonique soit A-linéaire. Le quotient muni de cette structure répond au problème. □

L'image d'un élément $x \in M$ dans le quotient est notée $x + N$. Les règles de calcul sont celles qui sont naturelles, ce qui est une traduction du fait que la projection canonique soit un morphisme de modules.

On a une correspondance entre sous-modules de M/N et sous-modules de M contenant N, via la projection canonique.

1.2 Propriétés générales, alias « $A-Mod$ est une catégorie abélienne »

1.2.1 Additivité

Proposition 1.2.1. L'ensemble $\operatorname{Hom}_A(M, N)$ est un groupe abélien pour la loi d'addition naturelle. (L'élément neutre est le morphisme nul.)

1.2.2 Produits et coproduits

Proposition–Définition 1.2.2. Soit $(E_i)_{i\in I}$ une famille de modules.

1. Il existe un module P muni d'applications $p_k : P \to E_k$, vérifiant la propriété suivante (dite propriété universelle du produit) :
   Pour tout module M muni d'applications $f_k : P \to E_k$, il existe un unique morphisme $\phi M \to P$ tel que $\forall k$, $p_k \circ \phi = f_k$.
2. Une solution de ce problème universel est unique à unique isomorphisme près

Un tel module P est appelé module produit et noté $\prod\limits_{i\in I} E_i$. Les applications $p_k : \prod E_l \to E_k$ sont les projections canoniques.

Démonstration. Unicité : □
Existence :
L'ensemble produit $\prod E_i$ est muni de la structure de A-module en définissant la somme et la multiplication externe composante par composante. Il répond au problème. □

Proposition–Définition 1.2.3. Soit $(E_i)_{i\in I}$ une famille de modules.

1. Il existe un module S muni d'applications $i_k : E_k \to S$, vérifiant la propriété suivante (dite propriété universelle de la somme directe) :
   Pour tout module M muni d'applications $f_k : E_k \to M$, il existe un unique morphisme $\phi : S \to M$ tel que $\forall k$, $phi \circ i_k = f_k$.
2. Une solution de ce problème universel est unique à unique isomorphisme près.

Un tel module P est appelé module somme directe, ou coproduit, et noté $\bigoplus\limits_{i\in I} E_i$ ou $\coprod\limits_{i\in I} E_i$. Les applications $i_k : \prod E_l \to E_k$ sont les inclusions canoniques.

Démonstration. Unicité : □
Existence : Le sous-ensemble de $\prod E_i$ des suites presque nulles est un sous-module de $\prod E_i$. Les applications $i_k : E_k \to \bigoplus E_l$ sont les inclusions canoniques. □

Remarque : dans les ouvrages de niveau M1/agreg ou inférieur, la notation $\bigoplus$ et l'appellation « somme directe » sont beaucoup plus employés que $\coprod$ et « coproduit ». Sinon, certains auteurs emploient les deux indifféremment, et d'autres distinguent les deux et réservent la notation $\bigoplus$ et le nom de somme directe au cas d'une somme directe *interne* , voir plus loin.

Proposition 1.2.4. Les propriétés universelles du produit et de la somme peuvent s'écrire sou la forme suivante :

$$\mathrm{Hom}_A(M, \prod E_i) = \prod \mathrm{Hom}_A(M, E_i),$$
$$\mathrm{Hom}_A(\bigoplus E_i, M) = \prod \mathrm{Hom}_A(E_i, M).$$

Exercice 1.2.5. Dans la proposition plus haut, préciser le sens des égalités (bijections ? isomorphismes ? de groupes ? modules ?). Ensuite, démontrer la proposition.

Notation : si tous les modules sont identiques, notations E^I et $E^{(I)}$. En particulier, on a les modules A^I et $A^{(I)}$.

1.2.3 Noyaux, Images, conoyaux, coimages

Proposition 1.2.6. Les noyaux et images de morphismes sont des A-modules. Les conoyaux et coimages aussi.

Proposition 1.2.7. Injectif ssi noyau nul, surjectif ssi $Im(f) = N$.

Proposition 1.2.8. Propriété universelle de ces objets.

Remarque : dans la mesure du possible, privilégier l'utilisation des propriétés universelles aux définitions ensemblistes, pour s'entraîner à les manipuler.

Théorème 1.2.9. Monomorphisme ssi injectif; épimorphisme ssi surjectif.

Théorème 1.2.10 (Premier théorème d'isomorphisme)**.** Soit $f : M \to N$ un morphisme. Alors f passe au quotient par $\mathrm{Ker}(f)$ et induit un isomorphisme

$$\mathrm{Coim}(f) \xrightarrow{\sim} \mathrm{Im}(f).$$

Théorème 1.2.11 (Décomposition canonique d'un morphisme)**.** Tout morphisme $f : M \to N$ s'écrit comme composée d'un épimorphisme puis d'un monomorphisme.

Démonstration. Écrire

$$M \twoheadrightarrow \mathrm{Coim}(f) \xrightarrow{\sim} \mathrm{Im}(f) \hookrightarrow N$$

□

1.3 Suites exactes, chasse au diagramme

Définition 1.3.1. Suites exactes. Morphisme de suites exactes. Isomorphisme de suites exactes.

Proposition–Définition 1.3.2. Soit $0 \to N \to M \to Q \to 0$ une suite exacte courte de modules. Alors les cinq conditions suivantes sont équivalentes :

1. isomorphe à une somme directe;
2. scindée à gauche;
3. scindée à droite;
4. la suite induite $0 \to \mathrm{Hom}(P, N) \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, Q) \to 0$ est exacte pour tout A-module P;
5. la suite induite $0 \to \mathrm{Hom}(Q, P) \to \mathrm{Hom}(M, P) \to \mathrm{Hom}(N, P) \to 0$ est exacte pour tout A-module P.

Lorsqu'elles sont vérifiées, on dit que la suite exacte courte est *scindée*.

Remarque 1.3.3. Attention, la situation est très différente en théorie des groupes (non abéliens) : dans une suite exacte de groupes non abéliens, un scindage à droite ne suffit pas à avoir un produit direct. La raison est essentiellement que l'image de la section est un groupe qui n'est pas forcément distingué.

Proposition 1.3.4. Lemme des cinq.

Exercice 1.3.5. Lemme du serpent.

Exercice 1.3.6. Lemme « 3×3 ».

1.4 Opérations sur les sous-modules

1.4.1 Sous-modules engendrés

Proposition 1.4.1. L'intersection de sous-modules est un sous-module.

Définition 1.4.2. Sous-module engendré par une partie, par une famille. Notation $\langle X \rangle$.

Théorème 1.4.3. Le module engendré par une famille est l'ensemble des combinaisons linéaires d'éléments de cette famille.

Définition 1.4.4. Module monogène. Notation $A.x$. Morphisme canonique associé à x : $f : A \to M$, $1_A \to x$, dont l'image est le sous-module Ax de M.

Si I est le noyau de ce morphisme, on en déduit que le module Ax est isomorphe à A/I.

Définition 1.4.5. Somme de sous-modules : $\sum E_i = \langle \cup E_i \rangle$.

Pour tout $i \in I$, on a le morphisme d'injection canonique $j_i : M_i \to M$. Par propriété universelle de la somme directe, on en déduit un morphisme canonique $f : \bigoplus E_i \to M$. L'image de ce morphisme est $\sum E_i$. C'est l'ensemble des combinaisons linéaires d'éléments des E_i.

Notation 1.4.6. Si M et N sont des sous-modules, on note $M + N$ leur somme.

1.4.2 Deuxième théorème d'isomorphisme

Théorème 1.4.7.

$$\frac{M}{M \cap N} \simeq \frac{M+N}{N}.$$

1.4.3 Sous-modules en somme directe et projecteurs

Proposition–Définition 1.4.8. Soit M un module et N, N' deux sous-modules. Les conditions suivantes sont équivalentes :

1. le morphisme canonique $N \coprod N' \to M$ est injectif et induit un isomorphisme $N \coprod N' \simeq N + N'$;
2. Tout élément de $N \cap N'$ admet une unique écriture de la forme $n + n'$ avec $n \in N$ et $n' \in N'$;
3. $N \cap N' = \{0\}$.

Dans ce cas, on dit que les deux sous-modules *sont en somme directe* (ou *somme directe interne*), et on préfère écrire $N \oplus N'$ plutôt que $N + N'$.

Définition 1.4.9. Somme directe interne d'une famille de sous-modules.

Définition 1.4.10. Projecteur

Propriétés

Définition 1.4.11. Famille orthogonale de projecteurs

Théorème 1.4.12. Si E est somme directe finie de sous-modules, alors on a une famille finie orthogonale de projeteurs dont la somme est l'identité.

1.4.4 Supplémentaires

Définition 1.4.13. Sommes directes à deux termes : on dit que les deux sous-modules sont supplémentaires.

0 et A sont supplémentaires dans le A-module A.

Correspondance entre couples de sous-modules supplémentaires et projecteurs. Correspondance entre les supplémentaires d'un sous-module fixé et les projecteurs d'image ce sous-module.

Tout supplémentaire de N dans M est canoniquement isomorphe à M/N ; Exemple : $2\mathbb{Z} \subset \mathbb{Z}$ n'a pas de supplémentaire.

Chapitre 2

Compléments

2.1 Modules de morphismes et dualité

2.2 Torsion

Attention, plusieurs définitions. Forcer intègre pour éviter les problèmes.
Éléments de torsion.
Modules de torsion, modules sans torsion.
Exemples.
Partie de Torsion.
Si A est intègre, c'est un sous-module.
Le quotient par la torsion n'a pas de torsion.
propriétés universelles.
p-torsion

2.3 Changement de l'anneau de base

Source : Objectif agrégation pour le minimum syndical.

Chapitre 3

Modules particuliers

Dans ce chapitre A est commutatif.
A/I est de torsion. $\mathbb{Q}/\mathbb{Z}$ est de torsion.

3.1 Familles libre et génératrices

Définitions équivalentes. Bases. Contre-exemples.

3.2 Modules de type fini

Proposition–Définition 3.2.1. Soit M un module. Les conditions suivantes sont équivalentes.

1. Il existe une famille génératrice finie $m_1, \ldots m_r$ de M.
2. Il existe un morphisme surjectif $A^r \to M$.

Lorsqu'elles sont vérifiées, on dit que le module est *de type fini*.

Exemples : A^n est de type fini. Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas de type fini. Si k est un corps, le k-module (c'est-à-dire k-ev) $k[X]$ n'est pas de type fini comme k-module. Attention, on dit cependant que c'est une *k-algèbre de type fini*! (En tant que k-algèbre, $k[X]$ est en effet engendrée par un nombre fini d'éléments, en fait juste un seul : X. Mais pas en tant que k-ev.)

Proposition 3.2.2. Soit M de type fini. Alors :

1. Tout quotient de M est de type fini.
2. Un sous-module de M n'est pas forcément de type fini.

Proposition 3.2.3. Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de modules. Si M' et M'' sont de t.f., alors M aussi.

Cette proposition est une conséquence de la proposition plus générale qui dit qu'une famille génératrice de M' et une famille génératrice de M'' fournissent une famille génératrice de M. On peut aussi appliquer le lemme des cinq dans sa version générale.

Théorème 3.2.4 (Cayley-Hamilton)**.**

Corollaire 3.2.5. Soit M un module de type fini, et $f \in \mathrm{End}_A(M)$. Si f est surjectif, il est bijectif.

3.3 Modules libres

3.3.1 Généralités sur les bases, contre-exemples

3.3.2 Théorie de la dimension pour les espaces vectoriels (admis)

Les résultats suivants sont admis. Voir Lang, Algebra, III.5 (chapitre sur les espaces vectoriels).

Théorème 3.3.1. Soit V un k-ev. Soit $\mathscr{L}$ une famille libre et $\mathscr{G} \supset \mathscr{L}$ une famille génératrice. Alors il existe une base $\mathscr{B}$ avec $\mathscr{L} \subset \mathscr{B} \subset \mathscr{G}$.

En particulier, de toute famille génératrice on peut extraire une base, et toute famille libre peut être complétée en une base.

Théorème-définition 3.3.2. Soit V un k-ev. Toutes les bases de V ont le même cardinal, que l'on appelle la *dimension* de V (en tant que k-espace vectoriel).

3.3.3 Théorie du rang pour les modules libres sur un anneau commutatif

3.3.4 Applications

à la fin, les surjections vers un module libre sont scindées

3.4 Modules de présentation finie

3.5 Modules noethériens (et artiniens)

Proposition 3.5.1.

Proposition–Définition 3.5.2. Soit M un module. On a équivalence entre les trois assertions suivantes. Un module est noethérien s'il vérifie les conditions équivalentes précédentes.

Proposition–Définition 3.5.3. Soit M un module. On a équivalence entre les deux assertions suivantes. Un module est artinien s'il vérifie les conditions équivalentes précédentes.

Proposition 3.5.4. « 2-out-of-3 » pour noethériens et artiniens.

Proposition 3.5.5. Soit M un A-module, et $f \in \mathrm{End}_A(M)$.

— Si M est noethérien et f est surjectif, f est bijectif.

— Si M est artinien et f est injectif, f est bijectif.

Chapitre 4

Modules de type fini sur les anneaux principaux