Algèbre I — Master 1

Séance 5 — Modules de type fini sur un PID

Théorème de structure, groupes abéliens et endomorphismes

But. Déduire de la forme de Smith une classification complète des modules de type fini sur un anneau principal, puis l'appliquer aux groupes abéliens et aux endomorphismes.

Table des matières

1 Torsion et partie libre **1**

2 Théorème de structure **1**
2.1 Décomposition primaire 2

3 Groupes abéliens de type fini **2**

4 Les k$[T]$-modules et les endomorphismes **3**
4.1 Forme de Jordan 3

5 Compléments **3**
5.1 Cayley–Hamilton par les modules 3
5.2 Décomposition de Fitting 4
5.3 Modules non finiment engendrés 4

À retenir **4**

1. Torsion et partie libre

Soit A un PID et $K = \mathrm{Frac}(A)$.

Définition 1.1. Pour un A-module M, son sous-module de torsion est

$$M_{\mathrm{tors}} = \{m \in M \mid am = 0 \text{ pour un certain } a \neq 0\}.$$

Le module est de torsion si $M = M_{\mathrm{tors}}$, et sans torsion si $M_{\mathrm{tors}} = 0$. Son rang est

$$\mathrm{rg}_A(M) = \dim_K(K \otimes_A M).$$

Dans un domaine, la torsion forme bien un sous-module. Si M est de type fini, M_{tors} est annulé par un même élément non nul : il suffit de multiplier les annulateurs d'une famille génératrice.

Exemple 1.2. Pour $M = \mathbb{Z}^2 \oplus \mathbb{Z}/12\mathbb{Z}$, on a $M_{\mathrm{tors}} = \mathbb{Z}/12\mathbb{Z}$ et $\mathrm{rg}_{\mathbb{Z}}(M) = 2$. Le module $\mathbb{Q}$ est sans torsion comme $\mathbb{Z}$-module, mais n'est ni libre ni de type fini.

2. Théorème de structure

Théorème 2.1 (Facteurs invariants)**.** *Tout A-module de type fini M est isomorphe à*

$$A^r \oplus A/(d_1) \oplus \cdots \oplus A/(d_s), \qquad d_1 \mid d_2 \mid \cdots \mid d_s,$$

où les d_i sont non nuls et non inversibles. L'entier r et les classes des d_i modulo multiplication par une unité sont uniques.

Existence. Choisissons une surjection $A^n \twoheadrightarrow M$. Son noyau N est libre de rang fini, donc le morphisme $N \hookrightarrow A^n$ est représenté par une matrice. Sa forme de Smith est diagonale de coefficients $d_1 \mid \cdots \mid d_s$. Le conoyau est exactement $A^{n-s} \oplus \bigoplus_i A/(d_i)$; on omet les coefficients inversibles, dont le quotient est nul. □

Le rang est r. Le produit $d_1 \cdots d_s$ engendre le premier idéal de Fitting non nul ; l'ensemble des idéaux déterminantiels fournit l'unicité de tous les facteurs. On peut aussi caractériser d_s comme un générateur de l'annulateur de la partie de torsion.

2.1. Décomposition primaire

Écrivons chaque d_i comme produit de puissances d'irréductibles. Le théorème chinois donne

$$A/(d_i) \simeq \bigoplus_{p^a \| d_i} A/(p^a).$$

On obtient une autre forme de la classification.

Théorème 2.2 (Diviseurs élémentaires)**.** *Tout module de torsion de type fini sur A est somme directe de modules $A/(p^a)$, où p est irréductible. Les puissances p^a, avec multiplicité, sont uniques à association près.*

Pour un irréductible p, la composante p-primaire est

$$M_{(p)} = \{m \in M \mid p^N m = 0 \text{ pour un certain } N\}.$$

On a $M_{\text{tors}} = \bigoplus_p M_{(p)}$.

3. Groupes abéliens de type fini

En prenant $A = \mathbb{Z}$, on obtient :

Théorème 3.1. *Tout groupe abélien de type fini est isomorphe à*

$$\mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}, \qquad d_1 \mid \cdots \mid d_s.$$

Il est fini si et seulement si $r = 0$, et son ordre est alors $d_1 \cdots d_s$.

Exemple 3.2 (Passage des composantes primaires aux facteurs invariants)**.** Considérons

$$M = \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}.$$

La décomposition primaire est

$$M \simeq (\mathbb{Z}/4 \oplus \mathbb{Z}/2) \oplus (\mathbb{Z}/3 \oplus \mathbb{Z}/9).$$

En alignant les puissances croissantes de 2 et de 3, on trouve

$$M \simeq \mathbb{Z}/(2\cdot 3)\mathbb{Z} \oplus \mathbb{Z}/(4\cdot 9)\mathbb{Z} = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z}.$$

L'ordre 216 et l'exposant 36 se lisent immédiatement.

Exemple 3.3 (Calcul à partir d'une présentation)**.** Pour la matrice de la séance précédente $B = \left(\begin{smallmatrix} 2 & 4 & 4 \\ 6 & 6 & 12 \end{smallmatrix}\right)$, Smith donne

$$\operatorname{Coker}(B) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Ainsi les générateurs x, y soumis aux trois relations données par les colonnes de B définissent un groupe d'ordre 12, d'exposant 6, non cyclique.

4. Les $\mathbf{k}[T]$-modules et les endomorphismes

Soit V un $\mathbf{k}$-espace vectoriel de dimension finie et $u \in \mathrm{End}_{\mathbf{k}}(V)$. Faisons agir T par u. Le $\mathbf{k}[T]$-module V est de type fini et de torsion : pour tout v, la famille $v, u(v), \dots, u^n(v)$ est liée, et un même polynôme annule V.

Le théorème de structure donne

$$V \simeq \mathbf{k}[T]/(P_1) \oplus \cdots \oplus \mathbf{k}[T]/(P_s), \qquad P_1 \mid \cdots \mid P_s.$$

Proposition 4.1. *Dans cette décomposition, le polynôme minimal de u est P_s et son polynôme caractéristique est $P_1 \cdots P_s$.*

En effet, l'annulateur du module est (P_s), tandis que sur $\mathbf{k}[T]/(P)$, la matrice de T dans la base $1, T, \dots, T^{d-1}$ est la matrice compagnon de P, de polynôme caractéristique P.

Exemple 4.2 (Forme rationnelle)**.** Sur $\mathbb{Q}$, prenons

$$P = T^3 - 2, qquadC(P) = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Le $\mathbb{Q}[T]$-module associé est $\mathbb{Q}[T]/(T^3-2)$. Le polynôme minimal et le polynôme caractéristique sont tous deux $T^3 - 2$. Cette matrice ne se diagonalise pas sur $\mathbb{Q}$, mais sa forme compagnon est déjà une forme canonique rationnelle.

4.1. Forme de Jordan

Supposons $\mathbf{k}$ algébriquement clos. Les irréductibles sont $T - \lambda$; la décomposition en diviseurs élémentaires devient

$$V \simeq \bigoplus_{\lambda, a} \mathbf{k}[T]/((T-\lambda)^a).$$

Dans la base $1, (T-\lambda), \dots, (T-\lambda)^{a-1}$, l'action de T est un bloc de Jordan $J_a(\lambda)$. On retrouve donc la forme normale de Jordan.

Exemple 4.3. Pour un nilpotent N ayant les blocs $J_3(0) \oplus J_1(0)$,

$$V \simeq \mathbf{k}[T]/(T^3) \oplus \mathbf{k}[T]/(T).$$

Les dimensions $\dim \ker N = 2$, $\dim \ker N^2 = 3$, $\dim \ker N^3 = 4$ permettent de retrouver les tailles 3 et 1 : les accroissements successifs comptent les blocs de taille au moins j.

Exemple 4.4 (Dépendance du corps)**.** La rotation réelle $R = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ a polynôme minimal $T^2 + 1$. Sur $\mathbb{R}$, le module est simple et R n'a pas de valeur propre. Après extension à $\mathbb{C}$, $T^2 + 1 = (T - i)(T + i)$ et la représentation se décompose en deux droites propres.

5. Compléments

5.1. Cayley–Hamilton par les modules

Dans une base, V possède une présentation par la matrice $TI - [u]$ sur $\mathbf{k}[T]$. L'adjointe donne

$$\mathrm{adj}(TI - [u])(TI - [u]) = \det(TI - [u])I.$$

En évaluant en $T = u$, on obtient $\chi_u(u) = 0$. Le théorème de Cayley–Hamilton apparaît donc comme une relation dans le $\mathbf{k}[T]$-module V.

5.2. Décomposition de Fitting

Pour $u \in \mathrm{End}_{\mathbf{k}}(V)$ et $N \gg 0$,

$$V = \mathrm{Ker}(u^N) \oplus \mathrm{Im}(u^N).$$

L'endomorphisme est nilpotent sur le premier facteur et inversible sur le second. C'est le cas particulier associé aux facteurs T et aux facteurs premiers à T dans la décomposition primaire.

5.3. Modules non finiment engendrés

La finitude est essentielle : le groupe $\mathbb{Q}/\mathbb{Z}$ est de torsion, mais il ne se décompose pas en somme finie de groupes cycliques. Sa composante p-primaire est le groupe de Prüfer $\mathbb{Z}[1/p]/\mathbb{Z}$.

À retenir

- Sur un PID, un module de type fini est la somme d'une partie libre et de modules cycliques de torsion.
- Les facteurs invariants et les diviseurs élémentaires sont deux écritures équivalentes et uniques.
- On obtient la classification des groupes abéliens de type fini.
- Pour $A = \mathbf{k}[T]$, la classification devient celle des endomorphismes : forme rationnelle, puis forme de Jordan sur un corps algébriquement clos.