

Algèbre I — Master 1

Séance 4 — Modules libres et présentations

Bases, matrices et forme normale de Smith

But. Passer de la description intrinsèque d'un module au calcul par générateurs, relations et matrices, puis établir la forme normale de Smith sur un anneau principal.

Table des matières

1 Modules libres	1
1.1 Construction et propriété universelle	1
1.2 Rang	2
2 Générateurs, relations et présentations	2
3 Sous-modules d'un module libre sur un PID	2
4 Forme normale de Smith	3
4.1 Principe de l'algorithme	3
4.2 Exemple complet	3
5 Compléments	3
5.1 Modules stablement libres	3
5.2 Idéaux de Fitting	4
5.3 Anneaux non commutatifs	4
À retenir	4

1. Modules libres

1.1. Construction et propriété universelle

Soit A un anneau et I un ensemble. On note

$$A^{(I)} = \bigoplus_{i \in I} Ae_i = \{(a_i)_{i \in I} \mid a_i = 0 \text{ sauf pour un nombre fini de } i\}.$$

Définition 1.1. Un A -module F est *libre de base* $(e_i)_{i \in I}$ si tout $x \in F$ s'écrit de manière unique $x = \sum_{i \in I} a_i e_i$, avec une famille (a_i) à support fini.

Proposition 1.2 (Propriété universelle). *Pour tout A -module M , l'application*

$$\text{Hom}_A(A^{(I)}, M) \longrightarrow M^I, \quad f \longmapsto (f(e_i))_i$$

est une bijection. Ainsi, toute application de l'ensemble I vers M se prolonge de manière unique en un morphisme $A^{(I)} \rightarrow M$.

Démonstration. À une famille (m_i) on associe $f((a_i)) = \sum_i a_i m_i$. La somme est finie, et l'unicité vient de ce que les e_i engendrent $A^{(I)}$. $\square$

Une famille (x_i) dans M est *libre* si toute relation finie $\sum a_i x_i = 0$ impose $a_i = 0$; c'est une *base* si elle est libre et génératrice.

Exemple 1.3. A^n est libre de base canonique. L'idéal $(2, T) \subset \mathbb{Z}[T]$ est de type fini mais n'est pas libre de rang 1 : s'il était engendré par un élément, cet élément diviserait à la fois 2 et T , donc serait une unité, ce qui donnerait $(2, T) = A$. Sur un anneau général, « de type fini » ne signifie donc pas « libre ».

1.2. Rang

Sur un anneau commutatif non nul, si $A^m \simeq A^n$, alors $m = n$. En effet, choisissons un idéal maximal $\mathfrak{m}$ et tensorisons — ou, plus élémentairement, réduisons les matrices — modulo $\mathfrak{m}$: on obtient un isomorphisme entre espaces vectoriels $(A/\mathfrak{m})^m \simeq (A/\mathfrak{m})^n$.

Définition 1.4. Le *rang* d'un module libre de type fini F est l'entier n tel que $F \simeq A^n$.

2. Générateurs, relations et présentations

Définition 2.1. Une *présentation finie* d'un A -module M est une suite

$$A^m \xrightarrow{u} A^n \longrightarrow M \longrightarrow 0.$$

Les vecteurs de la base de A^n sont les générateurs et les colonnes de la matrice de u sont les relations. Autrement dit, $M \simeq \text{Coker}(u)$.

Tout module de présentation finie est de type fini. La réciproque est vraie si A est noethérien : pour une surjection $A^n \twoheadrightarrow M$, le noyau est alors de type fini.

Exemple 2.2. Le groupe abélien

$$M = \langle x, y \mid 6x = 0, 2x + 4y = 0 \rangle$$

est le conoyau de la matrice $\begin{pmatrix} 6 & 2 \\ 0 & 4 \end{pmatrix} : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$. Changer les générateurs correspond à une opération inversible sur les lignes ; changer les relations, à une opération inversible sur les colonnes.

Après choix de bases, un morphisme $A^n \rightarrow A^m$ est représenté par une matrice $B \in M_{m,n}(A)$. Deux matrices B, B' présentent des modules isomorphes si

$$B' = QBP, \quad Q \in \text{GL}_m(A), \quad P \in \text{GL}_n(A).$$

Les multiplications par P et Q sont engendrées par les opérations élémentaires : permutation de deux lignes ou colonnes, multiplication par une unité, et ajout d'un multiple d'une ligne ou colonne à une autre.

3. Sous-modules d'un module libre sur un PID

Dans la suite, A est un anneau principal.

Théorème 3.1. *Tout sous-module N d'un module libre A^n est libre de rang au plus n . Si N est de type fini, il possède une base $(f_1, \dots, f_r)$ avec $r \leq n$.*

Démonstration. On raisonne par récurrence sur n . Le cas $n = 0$ est clair. Soit $p : A^n \rightarrow A$ la dernière projection. L'image $p(N)$ est un idéal, donc $p(N) = (d)$. Si $d = 0$, on applique l'hypothèse de récurrence à $N \subset A^{n-1}$. Sinon, choisissons $v \in N$ avec $p(v) = d$. Pour tout $x \in N$, écrivons $p(x) = ad$; alors $x - av \in N \cap A^{n-1}$. Ainsi

$$N = (N \cap A^{n-1}) \oplus Av.$$

L'hypothèse de récurrence conclut. La somme est directe car $p(av) = ad$ et A est intègre. $\square$

Remarque 3.2. Sur $A = \mathbf{k}[X, Y]$, l'idéal (X, Y) est un sous-module de A , mais il n'est pas libre : un sous-module d'un module libre n'est donc pas toujours libre hors du cadre principal.

4. Forme normale de Smith

Théorème 4.1 (Smith). Soit A un PID et $B \in M_{m,n}(A)$. Il existe $Q \in GL_m(A)$ et $P \in GL_n(A)$ tels que

$$QBP = \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_r \\ \hline & & & 0 \end{pmatrix}, \quad d_1 \mid d_2 \mid \cdots \mid d_r,$$

où les d_i sont non nuls. Ils sont uniques à multiplication par des unités près.

4.1. Principe de l'algorithme

Si $B \neq 0$, les coefficients engendrent un idéal principal (d) . Par des opérations élémentaires et l'identité de Bézout, on fait apparaître un générateur d en position $(1, 1)$. Si un coefficient de la matrice restante n'est pas divisible par d , une nouvelle combinaison de lignes et colonnes remplace le pivot par un diviseur strict. La condition noethérienne interdit de poursuivre indéfiniment. On arrive ainsi à un pivot divisant tous les coefficients ; on annule sa ligne et sa colonne, puis on raisonne par récurrence. Une dernière correction assure $d_i \mid d_{i+1}$.

L'unicité peut se lire sur les *idéaux déterminantiels* : l'idéal engendré par les mineurs d'ordre s est

$$(d_1 d_2 \cdots d_s).$$

4.2. Exemple complet

Considérons

$$B = \begin{pmatrix} 2 & 4 & 4 \\ 6 & 6 & 12 \end{pmatrix} : \mathbb{Z}^3 \rightarrow \mathbb{Z}^2.$$

Effectuons successivement

$$L_2 \leftarrow L_2 - 3L_1, \quad C_2 \leftarrow C_2 - 2C_1, \quad C_3 \leftarrow C_3 - 2C_1, \quad L_2 \leftarrow -L_2.$$

On obtient

$$\begin{pmatrix} 2 & 4 & 4 \\ 6 & 6 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 4 \\ 0 & -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

Par conséquent,

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

La résolution directe des équations $B(x, y, z)^t = 0$ donne $y = 0$ et $x = -2z$, donc

$$\text{Ker}(B) = \mathbb{Z}(-2, 0, 1).$$

On vérifie aussi $d_1 = \text{gcd des coefficients} = 2$ et $d_1 d_2 = \text{gcd des mineurs d'ordre 2} = 12$.

5. Compléments

5.1. Modules stablement libres

Un module P est *stablement libre* s'il existe r, s tels que $P \oplus A^r \simeq A^s$. Il n'est pas toujours libre. En revanche, le théorème de Quillen–Suslin affirme que tout module projectif de type fini sur $\mathbf{k}[T_1, \dots, T_n]$ est libre.

5.2. Idéaux de Fitting

Pour une présentation $A^m \xrightarrow{B} A^n \rightarrow M \rightarrow 0$, l'idéal de Fitting $\text{Fitt}_i(M)$ est engendré par les mineurs d'ordre $n - i$ de B . Ces idéaux ne dépendent pas de la présentation. Sur un PID, ils retrouvent les produits $d_1 \cdots d_s$ et donc l'unicité de la forme de Smith.

5.3. Anneaux non commutatifs

Certains anneaux non commutatifs ne vérifient pas la propriété du rang invariant : on peut avoir $A^m \simeq A^n$ avec $m \neq n$. Cette pathologie explique pourquoi l'hypothèse commutative apparaît dans la définition générale du rang.

À retenir

- Un module libre est caractérisé par la possibilité de prolonger arbitrairement une application définie sur sa base.
- Une présentation finie est une matrice ; son conoyau est le module défini par les générateurs et relations.
- Sur un PID, tout sous-module d'un module libre est libre.
- La forme de Smith transforme une matrice en une diagonale $d_1 \mid \cdots \mid d_r$ et calcule explicitement noyau et conoyau.