Chapitre 5

Modules de type fini sur les anneaux principaux

5.1 Forme normale de Smith

Un module M de type fini sur un anneau principal A est isomorphe au quotient d'un module libre L de rang fini par un sous-module N. Ce sous-module N est de type fini. Si $B = (b_1, \ldots, b_m)$ est une base de L et si $F = (f_1, \ldots, f_n)$ une partie génératrice de N, on dit que la matrice $P = ([f_j]_B)$ est une matrice de présentation de M : $M \approx A^m/\mathrm{Im}(P) = \mathrm{coker(P)}$.
On obtient un module isomorphe en multipliant, à gauche et à droite, la matrice de présentation par une matrice inversible. La forme normale de Smith étend la réduction de Gauss au cas d'un anneau principal.

Définition 5.1.1. Une matrice $D = (d_{ij})_{i \leq m, j \leq n}$ est de forme normale si et seulement si :
$d_{ij} = 0$ pour $i \neq j$, et
pour $i < \min(m, n)$, d_{ii} divise $d_{i+1,i+1}$.

Définition 5.1.2. Une matrice est dite élémentaire lorsqu'elle est obtenue par des opérations élémentaires sur les lignes ou colonnes de la matrice identité. Les opérations élémentaires sur une matrice sont les suivantes :

permuter deux lignes (resp. deux colonnes),
ajouter un multiple d'une ligne à une autre ligne (respectivement colonne),
multiplier une ligne ou une colonne par un scalaire inversible.

Théorème 5.1.3. *a) Pour toute matrice P à m lignes et n colonnes, à coefficients dans un anneau principal A, il existe des matrices inversibles U*

et V telle que $UPV = D$ est une matrice de forme normale.
b) Dans le cas euclidien il existe des produits de matrices élémentaires U et V tels que $UPV = D$ est une matrice de forme normale.
c) Les coefficients de D sont déterminés à multiplication par un inversible près.

Corollaire 5.1.4. *Si A est un anneau euclidien, alors le groupe $GL_n(A)$ est engendré par les matrices élémentaires.*

5.2 Résultats de structure

Théorème 5.2.1. *Tout sous-module d'un module libre de rang fini sur un anneau principal est libre.*

Théorème 5.2.2. *Si un module de type fini sur un anneau principal est sans torsion, alors il est libre.*

Théorème 5.2.3. *Soit M un module de type fini sur un anneau principal, alors M contient un sous-module libre L tel que M est somme directe interne de L et* $\mathrm{Tors}(M)$.

Remarque 5.2.4. L n'est pas unique comme sous-module de M, mais son rang est fixé : c'est celui de M.

Théorème 5.2.5. *Soit M un module de torsion de type fini sur un anneau principal, alors il existe une suite d'éléments de A croissante pour la divisibilité : $a_1|a_2\dots|a_n \neq 0$, unique modulo produit par des inversibles, telle que M est isomorphe à :*

$$\bigoplus_{i=1}^{n} A/(a_i)\ .$$

Remarque 5.2.6. Les $\mathbb{Z}$-modules de torsion de type fini sont les groupes abéliens finis.

5.3 Modules primaires

Définition 5.3.1. a) Soient M un module sur un anneau principal A, et p un élément irréductible de A. Un élément v de M est p-primaire si et seulement s'il est annulé par une puissance de p :

$$\exists \alpha \in \mathbb{N}\ p^{\alpha}.v = 0\ .$$

b) Les éléments p-primaires de M forment un sous-module : le sous-module M_p des éléments p-primaires.
c) Les sous-modules M_p non triviaux sont les composantes primaires de M.

Remarque 5.3.2. Lorsque p et q sont associés, les sous-modules M_p et M_q sont les mêmes.

Proposition 5.3.3. *a) Un module de torsion de type fini a un nombre fini de composantes primaires (non triviales).*
b) Un module de torsion de type fini est somme directe de ses composantes primaires.

Remarque 5.3.4. Deux modules de torsion de type fini sont isomorphes si et seulement si leurs composantes primaires sont isomorphes.

Structure des modules primaires

Théorème 5.3.5. *Soit A un anneau principal et M un A-module de type fini p-primaire. Il existe une unique suite croissante d'entiers : $0 < \alpha_1 \leq \alpha_2 \cdots \leq \alpha_n$ telle que M est isomorphe à :*

$$\bigoplus_{i=1}^{n} A/(p^{\alpha_i}) \ .$$

5.4 Invariants de similitude d'un endomorphisme

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, et f un endomorphisme de E. Une structure de $\mathbb{K}[X]$-module est définie sur E, avec l'opération externe :

$$\begin{array}{rcl} \mathbb{K}[X] \times E & \to & E \\ (P, v) & \mapsto & P.v = P(f)(v) \end{array}$$

Le $\mathbb{K}[X]$-module E est de torsion, et sa classe d'isomorphisme est caractérisée par ses facteurs invariants : une suite de polynômes unitaires, décroissante pour la division : $(P_1, \ldots, P_m)$. Le polynôme P_1 est le polynôme minimal.

Remarque 5.4.1. Une présentation de E comme $\mathbb{K}[X]$-module est $XI - U$ où U est une matrice de f.

La matrice compagne d'un polynôme unitaire

$$P = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$$

est :

$$C(P) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Théorème 5.4.2. *L'endomorphisme f admet la suite de facteurs invariants $(P_1, \dots, P_m)$ si et seulement s'il existe une base de E dans laquelle la matrice est diagonale par blocs, avec les matrices compagnes des P_i comme blocs diagonaux.*

Corollaire 5.4.3. *Deux endomorphismes d'un espace vectoriel de dimension finie sont conjugués si et seulement s'ils ont les mêmes facteurs invariants.*

Exercice 5.4.4. Dans le cas où le polynôme minimal est produit de facteurs de degré 1 (scindé), retrouver la forme de Jordan classique.

5.5 Classification des sous-modules d'un module libre

Théorème 5.5.1 (Base adaptée)**.** *Soient M un module libre de rang n sur un anneau principal A, et N un sous-module de rang m.*
a) Il existe une suite $(a_1, \dots, a_m)$ de A croissante pour la division, et une base $B = (b_1, \dots, b_n)$ de M telles que : $(a_1 b_1, \dots, a_m b_m)$ est une base de N.
b) La suite $(a_1, \dots, a_m)$ est unique et caractérise la classe d'isomorphisme du sous-module N : deux sous-modules N et N' se correspondent par un isomorphisme de M si et seulement si leurs suites invariantes sont les mêmes.

5.6 Annexe : Modules de présentation finie

Définition 5.6.1. Soit A un anneau commutatif. Un A-module M est de présentation finie s'il est isomorphe au conoyau d'une application linéaire $P : A^n \to A^m$: $M \approx A^m/\mathrm{Im}(P)$. On dit que P est une (matrice de) présentation de M.

Remarque 5.6.2. Dans le cas noethérien tout module de type fini est de présentation finie.

Théorème 5.6.3. *Deux présentations d'un module de type fini sont reliées par une suite de transformations de l'un des types suivants :*
(i) Permutation des lignes ou des colonnes.
(ii) Transformation élémentaire sur les lignes : $L_i \leftarrow L_i + \alpha L_j$*, ou sur les colonnes :* $C_i \leftarrow C_i + \alpha C_j$*.*
(iii) Stabilisation $P \leftrightarrow \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$*.*
(iv) Ajout d'une ligne (resp. colonne nulle) ou l'inverse.