

Chapitre 8

Modules sur les anneaux principaux

8.1 Sous-modules d'un module libre

Théorème 8.1.1. *Tout sous-module d'un module libre sur un anneau principal est libre.*

8.2 Modules de type fini

Définition 8.2.1. Un module est de type fini si et seulement s'il admet une partie génératrice finie.

Définition 8.2.2. Le rang d'un A -module de type fini est le maximum des cardinaux des parties libres.

Théorème 8.2.3. *Soit A un anneau commutatif non nul et M un A -module qui admet une base finie de cardinal n , alors toutes les bases ont le même cardinal et celui-ci est égal au rang de M .*

Corollaire 8.2.4. *Un sous-module d'un module de type fini sur un anneau principal est de type fini.*

8.3 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 libre de type fini. Si $B = (b_1, \dots, b_m)$ est une base de L et si $F = (f_1, \dots, f_n)$ est une partie génératrice de N , on

dit que la matrice $P = ([f_j]_B)$ est une matrice de présentation de M : $M \approx A^m / \text{Im}(P) = \text{coker}(P)$.

On obtient un module isomorphe en multipliant, à gauche ou 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. Elle va permettre d'obtenir une présentation diagonale essentiellement unique.

Définition 8.3.1. Une matrice $D = (d_{ij})_{i \leq m, j \leq n}$ est de forme normale de Smith si et seulement si :

$d_{ij} = 0$ pour $i \neq j$, et

pour $i < \min(m, n)$, d_{ii} divise $d_{i+1, i+1}$.

Théorème 8.3.2. 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 de Smith.

Lemme 8.3.3. 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 $UPV = \begin{pmatrix} \delta & 0 \\ 0 & Q \end{pmatrix}$, où le coefficient $\delta \in A$ divise tous les coefficients de la matrice Q .

Un algorithme conduisant à la forme donnée dans le lemme consiste à appliquer à la matrice P la première des opérations suivantes (instruction « switch ... case ... »), et à répéter tant que le coefficient $P_{1,1}$ ne divise pas tous les autres ou qu'il existe un coefficient non nul $P_{1,j}$, $j > 1$, ou $P_{i,1}$, $i > 1$. Chaque passage conduisant soit à remplacer $P_{1,1}$ par un diviseur strict, soit à faire apparaître un coefficient nul en plus dans la première ligne ou la première colonne, on obtient la forme souhaitée en un nombre fini de passages.

Cas 1 S'il existe un coefficient $P_{1,j}$, $j > 1$, non divisible par $P_{1,1}$, alors on calcule une relation de Bezout : $uP_{1,1} + vP_{1,j} = \text{PGCD}(P_{1,1}, P_{1,j}) = \delta$, puis on multiplie à droite par une matrice inversible, dont l'effet sur les colonnes est :

$$C_1 \leftarrow uC_1 + vC_j, \quad C_j \leftarrow wC_1 + tC_j,$$

$$(w = \frac{-P_{1,j}}{\delta}, t = \frac{P_{1,1}}{\delta}).$$

Cas 2 S'il existe un coefficient $P_{i,1}$, $i > 1$, non divisible par $P_{1,1}$, alors on calcule une relation de Bezout : $uP_{1,1} + vP_{i,1} = \text{PGCD}(P_{1,1}, P_{i,1}) = \delta$, puis on multiplie à gauche par une matrice inversible, dont l'effet sur les lignes est :

$$L_1 \leftarrow uL_1 + vL_i, \quad L_i \leftarrow wL_1 + tL_i,$$

$$(w = \frac{-P_{i,1}}{\delta}, t = \frac{P_{1,1}}{\delta}).$$

Cas 3 S'il existe un coefficient $P_{1,j}$, $j > 1$, non nul (divisible par $P_{1,1}$), on annule $P_{1,j}$ en multipliant par la matrice élémentaire correspondant à

$$C_j \leftarrow C_j - \frac{P_{1,j}}{P_{1,1}} C_1 .$$

Cas 4 S'il existe un coefficient $P_{i,1}$, $i > 1$, non nul (divisible par $P_{1,1}$), on annule $P_{i,1}$ en multipliant par la matrice élémentaire correspondant à

$$L_i \leftarrow L_i - \frac{P_{i,1}}{P_{1,1}} L_1 .$$

Cas 5 S'il existe un coefficient $P_{i,j}$, $i > 1$, $j > 1$, non divisible par $P_{1,1}$, alors on fait apparaître $P_{i,j}$ en position $(i, 1)$ en multipliant à droite par la matrice élémentaire correspondant à

$$C_1 \leftarrow C_1 + C_j,$$

puis on applique le cas 2.

Smith

last edited on November 16, 2011 08:48 AM by admin

File... Action... Data... sage ☒ Typeset

```
P = matrix(ZZ, 4, [3,0,5,-6,0,-3,8,1,4,5,5,6,2,2,8,9])
```

P

$$\begin{pmatrix} 3 & 0 & 5 & -6 \\ 0 & -3 & 8 & 1 \\ 4 & 5 & 5 & 6 \\ 2 & 2 & 8 & 9 \end{pmatrix}$$

```
[D,U,V]=P.smith_form()
```

D,U,V

$$\left(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 25 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ -1 & 1 & -1 & 0 \\ 5 & -4 & 3 & -1 \end{pmatrix}, \begin{pmatrix} 13 & -34 & -33 & -120 \\ -10 & 26 & 25 & 91 \\ -4 & 11 & 11 & 41 \\ 3 & -8 & -8 & -30 \end{pmatrix} \right)$$

U*P*V

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 25 \end{pmatrix}$$

8.4 Résultats de structure

Définition 8.4.1. Un module est cyclique si et seulement s'il est engendré par un élément.

Remarque 8.4.2. Sur un anneau principal A , un module cyclique est isomorphe soit à A , soit à un quotient $A/(a)$.

Théorème 8.4.3. *Tout module de type fini sur un anneau principal est isomorphe à une somme directe de modules cycliques.*

18/11/2011

Théorème 8.4.4. Soit M un module de type fini sur un anneau principal, alors M contient un sous-module libre L tel que :

$$\begin{array}{ccc} L \oplus \text{Tors}(M) & \rightarrow & M \\ (x, y) & \mapsto & x + y \end{array}$$

est un isomorphisme. (On dit que M est somme directe interne de L et $\text{Tors}(M)$.)

Remarque 8.4.5. L n'est pas unique comme sous-module de M , mais son rang est fixé : c'est celui de M .

Théorème 8.4.6. Si un module de type fini sur un anneau principal est sans torsion, alors il est libre.

Théorème 8.4.7. Deux modules de type fini sur un anneau principal sont isomorphes si et seulement s'ils ont le même rang et si leurs torsions sont isomorphes.

Théorème 8.4.8. Soit M un module non nul, de torsion et de type fini sur un anneau principal A , alors il existe une suite d'éléments non inversibles de A croissante pour la divisibilité : $a_1 | a_2 \dots | a_n \neq 0$, a_1 non inversible, telle que M est isomorphe à :

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

Définition 8.4.9. Les éléments de la suite obtenue dans le théorème précédent sont appelés les facteurs invariants.

Théorème 8.4.10. Deux modules de torsion de type fini sur un anneau principal A sont isomorphes si et seulement s'ils ont les mêmes facteurs invariants (à multiplication par des inversibles près).

Remarque 8.4.11. Les $\mathbb{Z}$ -modules de torsion de type fini sont les groupes abéliens finis. Le théorème contient la classification des groupes abéliens finis : ils se décomposent en produit de groupes cycliques et sont classifiés par la suite de leurs facteurs invariants.

8.5 Modules primaires

Définition 8.5.1. 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 8.5.2. Lorsque p et q sont associés, les sous-modules M_p et M_q sont les mêmes.

Proposition 8.5.3. *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 8.5.4. Deux modules de torsion de type fini sont isomorphes si et seulement si leurs composantes primaires sont isomorphes.

Structure des modules primaires

Théorème 8.5.5. *Soit A un anneau principal et M un A -module de type fini p -primaire. Il existe une unique suite croissante d'entiers : $0 < \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_n$ telle que M est isomorphe à :*

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

8.6 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 :

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

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, croissante pour la division : $(P_1, \dots, P_m)$. Le polynôme P_m est le polynôme minimal.

Proposition 8.6.1. *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

$$P = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$$

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 8.6.2. *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 8.6.3. *Deux endomorphismes d'un espace vectoriel de dimension finie sont conjugués si et seulement s'ils ont les mêmes facteurs invariants.*

Exercice 8.6.4. Dans le cas où le polynôme minimal est produit de facteurs de degré 1 (scindé), retrouver la forme de Jordan classique.

8.7 Modules de présentation finie et idéaux de Fitting

Définition 8.7.1. Soit A un anneau commutatif. Un A -module M est de présentation finie s'il est isomorphe au conoyau d'une application linéaire $P : A^n \rightarrow A^m : M \approx A^m / \text{Im}(P)$. On dit que P est une (matrice de) présentation de M .

Remarque 8.7.2. Dans le cas noethérien tout module de type fini est de présentation finie.

Théorème 8.7.3. *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 ou suppression d'une colonne nulle.*

Définition 8.7.4. Soit A un anneau commutatif et P une matrice à m lignes et n colonnes. Pour $0 \leq k$, le k -ième idéal de Fitting de P est l'idéal F_k engendré par les mineurs d'ordre $m - k$ si $m - k < n$ et est égal à A sinon.

Remarque 8.7.5. Les idéaux de Fitting forment une suite croissante d'idéaux.

Exercice 8.7.6. Décrire les idéaux de Fitting d'une matrice sous forme normale de Smith.

Théorème 8.7.7. *Les idéaux de Fitting d'un module M de présentation P ne dépendent pas de P .*

Définition 8.7.8. Les idéaux de Fitting d'un module M de présentation finie sur un anneau commutatif A sont ceux d'une présentation.

Proposition 8.7.9. *Soit A un anneau principal.*

a) Un module de type fini sur A est de torsion si et seulement si son idéal de Fitting $F_0(M)$ est non nul.

b) Pour un A -module M de type fini et de torsion, de facteurs invariants $d_1|d_2|\dots|d_m$, le module de Fitting $F_k(M)$ est engendré par le produit $o_k = d_1d_2\dots d_{m-k}$.

25/11/2011

8.8 Classification des sous-modules d'un module libre sur un anneau principal

Théorème 8.8.1 (Base adaptée). *Soient M un module libre de rang m sur un anneau principal A , et N un sous-module de rang n .*

a) Il existe une suite $(a_1, \dots, a_n)$ de A croissante pour la division, et une base $B = (b_1, \dots, b_m)$ de M telles que $(a_1b_1, \dots, a_nb_n)$ est une base de N .

b) La suite $(a_1, \dots, a_n)$ 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 aux inversibles près.

Remarque. Ici on peut avoir $a_1 = 1$.

Proposition 8.8.2. *Soient P une matrice dont les colonnes engendrent le sous-module N de A^m et $D = UPV$ une réduction à la forme normale de Smith. Alors les colonnes de U^{-1} forment une base adaptée.*