# TD n°6.

## 1 Modules sur les anneaux principaux

### 1.1 Calculs matriciels

**Exercice 1.** Soit $A$ un anneau principal. Soit $f : A^n \to A^m$ un morphisme de modules. Montrer que $\ker f$ admet un supplémentaire dans $A^n$.

**Exercice 2. Algorithme d'Euclide étendu et relation de Bézout**
Soit $a > b > 0$ deux entiers naturels. On considère les suites $(r_i), (q_i)$ définies par

$$\left\{ \begin{array}{lcll} r_0 & = & a, & \\ r_1 & = & b, & \end{array} \right. , \quad \left\{ \begin{array}{lcll} r_{i-1} & = & r_i q_i + r_{i+1} & si \quad r_i \neq 0, \\ r_{i+1} & = & q_{i+1} = 0 & si \quad r_i = 0. \end{array} \right.$$

où $(q_i, r_{i+1})$ est le quotient et le reste de la division euclidienne de $r_{i-1}$ par $r_i$.

a) i) Montrer que la suite $(r_n)$ est strictement décroissante puis nulle. Quelle est cette suite pour $a = 465$ et $b = 185$ ?

ii) Soit $N = \max\{p \in \mathbb{N}, r_p > 0\}$. Montrer que $d = r_N = \text{pgcd}(a, b)$.

b) Aux suites $(r_n)$ et $(q_n)$ on associe deux autres suites $(u_n), (v_n)$ définies par
$$u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1, u_{i+1} = u_{i-1} - u_i q_i, \ v_{i+1} = v_{i-1} - v_i q_i.$$

i) Montrer que pour tout $i$, on a $r_i = u_i a + v_i b$. Montrer que $\text{pgcd}(a, b) = u_N a + v_N b$.

ii) Calculer les suites $(r_n), (u_n), (v_n)$ pour $a = 465$ et $b = 185$.

c) i) Montrer que pour tout $i$, on a

$$\begin{pmatrix} r_{i+1} & u_{i+1} & v_{i+1} \\ r_i & u_i & v_i \end{pmatrix} = \begin{pmatrix} -q_i & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_i & u_i & v_i \\ r_{i-1} & u_{i-1} & v_{i-1} \end{pmatrix}$$

ii) En déduire que $u_{i+1} v_i - u_i v_{i+1} = \pm 1$.

iii) Montrer que les suites $(u_i)$ et $(v_i)$ sont de signe alterné et croissantes en valeur absolue (On supposera ici que $0 < b < a$).

iv) En déduire que les solutions de $ua + vb = 0$ sont de la forme $k(u_{N+1}, v_{N+1}), k \in \mathbb{Z}$.

v) En déduire les solutions de $ua + vb = d$.

vi) Montrer que $(u_N, v_N)$ est l'unique ( ?) solution de $ua + vb = d$ vérifiant $|u| \leq |b/2d|$, $|v| \leq |a/2d|$. *on pourra remarquer que* $q_N \geq 2$.

**Exercice 3.** Soit $n$ et $m$ des éléments de $A$ euclidien. On note $d = (n, m)$ et soit $u$ et $v$ des éléments de $A$ tels que $un + vm = d$.

a) Trouver une matrice de $\text{SL}_2(A)$ telle que $L(nA \times mA) = dA \times \frac{nm}{d} A$.

b) Montrer que les matrices $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$ et $\begin{pmatrix} d & 0 \\ 0 & \frac{nm}{d} \end{pmatrix}$ sont équivalentes dans $\text{SL}_2(A)$.

c) Déterminer un isomorphisme $\phi$ de $\mathbb{Z}^2$ tel que $\phi(12\mathbb{Z} \times 18\mathbb{Z}) = 6\mathbb{Z} \times 36\mathbb{Z}$.

**Exercice 4.** (i) Calculer $\text{pgcd}(255, 141)$ et donner une solution $(x, y) \in \mathbb{Z}^2$ de l'équation suivante :

$$255x + 141y = \text{pgcd}(255, 141).$$

(ii) Déterminer une base du sous-$\mathbb{Z}$-module de $\mathbb{Z}^2$ défini par l'équation $255x + 141y = 0$.
(iii) Donner toutes les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation suivante :

$$255x + 141y = \text{pgcd}(255, 141).$$

**Exercice 5. Échelonnement de matrices en colonnes**
Soit $X$ une matrice $n \times m$ à coefficients dans un anneau principal $A$. On note $X_i$ la $i^{\text{e}}$ colonne de $X$

a) On appelle opération élémentaire (sur les colonnes de $X$) une transformation de la forme $X_i \mapsto X_i + \lambda X_j$ pour un certain couple $i, j$ et $\lambda \in A$, ou encore $(X_i, X_j) \mapsto (X_j, -X_i)$.
   i) Montrer qu'une une opération élémentaire ne modifie pas l'image de $X$.
   ii) Montrer que si $X'$ est le résultat de l'opération élémentaire, alors il existe une matrice $m \times m$ $R$ de déterminant 1, telle que $X' = X \cdot R$.
   iii) Montrer qu'il existe une matrice carrée $m \times m$, $R$, de déterminant 1, telle que les $m-1$ denières coordonnées de la première ligne de $XR$ sont nulles.

b) La hauteur $h(U)$ d'un vecteur $U$ de $M_{n,1}(A)$ est l'entier $n-i$ où $i$ est le plus grand entier tel que $U_j = 0$ pour tout $j \leq i$ (le vecteur nul est le seul vecteur de hauteur nulle).
   Une matrice $X$ de $M_{n,m}(A)$, vecteurs colonnes $X_1, \cdots, X_m$ est dite échelonnée (en colonnes) s'il existe $k$ tel que
   $$h(X_1) > h(X_2) > \cdots > h(X_k) > h(X_{k+1}) = \cdots = h(X_{k+m}) = 0$$
   On note $r(X) = \max\{i, h(X_i) > 0\}$.
   i) Montrer que il existe une matrice $R$ de déterminant 1 telle que $X' = X \cdot R$ est échelonnée.
   ii) Donner en fonction des colonnes de $R$ et de $X'$, une base du noyau de $X$, une base de l'image de $X$ et une base d'un supplémentaire du noyau de $X$.
   iii) Soit $X$ une matrice et $I$ la matrice identité $m \times m$. Montrer que si $X' = X \cdot R$, alors $\begin{pmatrix} X \\ I \end{pmatrix} \cdot R = \begin{pmatrix} X' \\ R \end{pmatrix}$.
   iv) Déterminer image et noyau de la matrice $\begin{pmatrix} 1 & 3 & 2 \\ 2 & 0 & 2 \\ -2 & 6 & 0 \\ 3 & 3 & 4 \end{pmatrix}$.

**Exercice 6.** a) Trouver une base du noyau et d'un supplémentaire du noyau de $X$ (dans $\mathbb{Z}^5$) : $(E_1, E_2, E_3, E_4, E_5)$

$$X = \begin{pmatrix} 1 & -2 & 3 & 1 & 2 \\ 2 & 1 & 4 & -1 & 1 \\ 1 & -1 & 2 & 1 & 1 \end{pmatrix}$$

b) Trouver des formes lineaires telles que $x = \sum_{i=1}^{5} \lambda_i(x) E_i$.
c) Peut-on extraire de $(X_1, \ldots, X_5)$, une base de l'image ?

**Exercice 7.** Résoudre le système

$$\begin{cases} 4x_1 + 3x_2 + 2x_3 + x_4 = 0 \\ 5x_1 + 6x_2 + 7x_3 + 8x_4 = 0 \\ 12x_1 + 11x_2 + 10x_3 + 9x_4 = 0 \end{cases},$$

puis

$$\begin{cases} 4x_1 + 3x_2 + 2x_3 + x_4 = 0 \ (\mod 8) \\ 5x_1 + 6x_2 + 7x_3 + 8x_4 = 0 \ (\mod 2) \\ 12x_1 + 11x_2 + 10x_3 + 9x_4 = 0 \ (\mod 6) \end{cases}.$$

Il suffit de calculer une certaine image réciproque.

**Exercice 8. Calcul d'une suite normalisée**
Parmi les groupes suivants, lesquels sont isomorphes ? $\mathbb{Z}_{48}$, $\mathbb{Z}_2 \times \mathbb{Z}_{24}$, $\mathbb{Z}_3 \times \mathbb{Z}_{16}$, $\mathbb{Z}_4 \times \mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. SI $p_1$ et $p_2$ sont de nombres premiers distincts, quel est le nombre de classes d'équivalences de groupes abéliens d'ordre $p_1^5 p_2^4$ ?

**Exercice 9.** Soit $F$ le sous-$\mathbb{Z}$-module de $\mathbb{Z}^4$ engendré par $X_1 = (6, 12, -12, 18)$, $X_2 = (15, 0, 30, 15)$, $X_3 = (10, 10, 0, 20)$.

a) Déterminer une base de $F$. Quelle est le rang de $F$ ?
b) Montrer que $(X_1, X_2)$ est une famille libre. $(X_1, X_2)$ peut-elle être complétée en une base de $F$ ?
c) Trouver dans $F$ un vecteur dont les coordonnées ont un pgcd égal à 3.

**Exercice 10.** a) Déterminer image et noyau de $A = \begin{pmatrix} 6 & 3 & 6 & -1 \\ 2 & 5 & 6 & -1 \\ 8 & 11 & 15 & -1 \end{pmatrix}$.

b) Résoudre $Ax = \begin{pmatrix} 8 \\ 4 \\ 1 \end{pmatrix}$.

c) Résoudre $AX = A$.

d) Le vecteur $(5, 3, 4, 3)$ est-il combinaison linéaire à coefficients entiers de $X_1 = (1, -1, 2, 1)$, $X_2 = (3, 1, 2, 1)$, $X_3 = (3, 5, 2, 3)$.

**Exercice 11.** (i) Donner les facteurs invariants de la matrice

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

(ii) Déterminer le module $N$ obtenu par la présentation

$$\mathbb{Z}^3 \xrightarrow{M} \mathbb{Z}^3 \to N \to 0.$$

Donner une base du noyau de la matrice $M$.
(iii) Même questions avec

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 9 & 8 \end{pmatrix}.$$

**Exercice 12.** (i) Donner une base du sous-module de $\mathbb{Z}^3$ défini par les équations

$$\begin{cases} 4x + 2y + 3z = 0 \\ 5x + 8y + 11z = 0 \end{cases}$$

**Exercice 13.** Sur un corps $k$ (de caractéristique 0), donner les invariants de similitude des matrices

$$M = \begin{pmatrix} 3 & -1 & 2 \\ 0 & 2 & 2 \\ 0 & -2 & 7 \end{pmatrix} \text{ et } M' = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 0 & 2 \end{pmatrix}.$$

**Exercice 14.** Soit $A$ un anneau principal. Donner les facteurs invariants de

$$M = J(a, n) = \begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & 0 & \ddots & a & 1 \\ 0 & \cdots & \cdots & 0 & a \end{pmatrix}.$$

## 1.2 $\mathbb{Z}$-modules et réseaux

**Exercice 15.** (i) Soit $L$ un sous-$\mathbb{Z}$-module de $\mathbb{Z}^n$. Montrer que $L$ est toujours sans torsion et donc libre.
(ii) On dit que $L$ est un réseau s'il est de rang $n$. Supposons que $L$ est un réseau et soit $(e_i)_{1 \leq i \leq n}$ une base de $L$. On appelle volume de la base $(e_i)$ l'entier

$$\mathrm{vol}(e_i) = |\det(e_i)|.$$

Montrer que le volume est indépendant de la base. On l'appelle volume du réseau et on le note

$$\mathrm{vol}(L).$$

(iii) Montrer que $\mathrm{vol}(L) = \mathrm{Card}(\mathbb{Z}^n/L)$.
(iv) Soit $B$ une partie convexe, symétrique (si $a \in B$, alors $-a \in B$) et bornée de $\mathbb{R}^n$. Supposons que

$$\mu(B) > 2^n \mathrm{vol}(L)$$

où $\mu$ est la mesure de Lebesgue. on va montrer que $B$ contient un élément non nul de $L$.
(iv.a) Montrer qu'il existe deux éléments distincts $a$ et $b$ dans $B$ tels que $a-b \in 2L$ (on pourra se ramener au cas où $2L = \mathbb{Z}^n$ via une application linéaire inversible).
(iv.b) Conclure en étudiant $\frac{1}{2}(a-b)$.
(v) On rappelle que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, montrer que si $p \equiv 1 \pmod 4$ alors il existe $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre 4.
(vi) En considérant le réseau

$$L = \{(a,b) \in \mathbb{Z}^2 \ / \ b \equiv ua \pmod p\}$$

montrer que $p$ est toujours somme de deux carrés (c'est-à-dire $p = a^2 + b^2$).

**Exercice 16.** On considère l'ensemble $M$ des triplets $(x,y,z) \in \mathbb{Z}^3$ tels que $x+y+z$ est pair.
(i) Montrer que $M$ est un sous-$\mathbb{Z}$-module libre de type fini et de rang 3 de $\mathbb{Z}^3$.
(ii) Donner une base de $M$ sur $\mathbb{Z}$.
(iii) Montrer que $\mathbb{Z}^3/M$ est un $\mathbb{Z}$-module simple (c'est-à-dire que ses seuls sous-modules sont (0) et lui-même).

**Exercice 17.** Soit $A$ un anneau principal et $L$ un $A$-modulelibre de rang fini. Soit $M$ un sous-$A$-modulede $L$. Montrer que $M$ possède un supplémentaire dans $L$ si et seulement si $L/M$ est sans torsion.
Application, dans l'exercice 16, $M$ a-t-il un supplémentaire dans $\mathbb{Z}^3$ ?

**Exercice 18.** (i) Soit $G$ un groupe abélien fini (donc un $\mathbb{Z}$-module fini), montrer qu'il existe un élément de $G$ dont l'ordre est multiple de l'ordre de tout élément de $G$.
(ii) Déterminer tous les groupes abéliens d'ordre 16.

## 1.3 Invariants de similitude d'un endomorphisme

**Exercice 19.** Soit $A$ un anneau principal et $M$ un $A$-modulede type fini.
(i) Justifier l'existence d'éléments $m_i$ (pour tout $1 \leq i \leq s$) de $m$ d'annulateurs $d_1|d_2|\cdots|d_s$, tels que

$$M \simeq \bigoplus_{i=1}^{s} Am_i.$$

(ii) Soit $i \in \{1, \cdots, s\}$, montrer qu'il existe $u_i \in \mathrm{End}_A M$ tel que

$$u_i(m_1) = \cdots = u_i(m_{s-1}) = 0, \text{ et } u_i(m_s) = m_i.$$

(iii) Soit $u \in \mathrm{End}_A M$ qui commute à tout autre élément de $\mathrm{End}_A M$, montrer qu'il existe $a \in A$ tel que $u(m) = am$ pour tout $m \in M$.
(iv) Soit $u : M \to M$ une application additive telle que pour tout $v \in \mathrm{End}_A M$, on ait $u \circ v = v \circ u$. Montrer que $u$ est une homothétie $m \mapsto am$ pour $a \in A$.
(v) Soit $k$ un corps commutatif, soit $E$ un $k$-espace vectoriel de dimension finie et $u \in \mathrm{End}_k E$. Montrer que tout endomorphisme de $E$ qui commute à tout endomorphisme commutant à $u$ est un polynôme en $u$.
*Indice* : on pourra utiliser la structure de $k[X]$-module sur $E$ définie par $u$.

**Exercice 20.** (i) Soit $M$ une matrice de taille $n \times n$ à coefficients dans un corps $k$. Montrer que $M$ est semblable à sa transposée.
(ii) Soient $(P_i)_{1 \leq i \leq r}$ polynômes deux à deux premiers entre eux, montrer que la matrice carrée de taille $nr$ diagonale par blocs $D(P_1 \cdot \mathrm{Id}_n, \cdots, P_r \cdot \mathrm{Id}_n)$ est équivalente à la matrice $D(\mathrm{Id}_{(r-1)n}, \prod_{i=1}^{r} P_i \cdot \mathrm{Id}_n)$.
(iii) Donner les invariants de similitude d'une matrice diagonale $D(a_1, \cdots, a_n)$.

**Exercice 21.** Soit $M$ une matrice carrée de taille $n$ à coefficients dans un corps $k$, on définit son commutant par :

$$C(M) = \{N \in M_n(k) \ / \ MN = NM\}.$$

C'est un sous-espace vectotiel de $M_n(k)$.
(i) Soit $A$ une matrice carrée de taille $n$ telle que $A = PMP^{-1}$ avec $P$ une matrice inversible. Montrer que l'on a $C(A) = PC(M)P^{-1}$.
(ii) Déterminer $C(M)$ lorsque $M \in M_n(k)$ est

$$M = J(a,n) = \begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & 0 & \ddots & a & 1 \\ 0 & \cdots & \cdots & 0 & a \end{pmatrix}.$$

(iii) Montrer que pour toute matrice $M$, on a $\dim_k C(M) \geq n$.

**Exercice 22.** Soit $A$ un anneau principal et $K$ son corps des fractions.
(i) Soit $x$ un élément non nul de $K^n$. Montrer qu'il existe une matrice dans $GL_n(A)$ dont la première colonne est proportionnelle à $x$ (on pourra utiliser l'exercice 17).
(ii) Montrer que toute matrice carrée d'ordre $n$ à coefficiens dans $K$ est produit d'une matrice de $GL_n(A)$ et d'une matrice triangulaire de $M_n(K)$ (raisonner par récurrence).
(iii) Application numérique : $A = \mathbb{Z}$ et

$$M = \begin{pmatrix} \frac{1}{2} & 1 & -\frac{1}{4} \\ \frac{2}{5} & 2 & \frac{2}{3} \\ \frac{3}{4} & \frac{1}{7} & -1 \end{pmatrix}.$$

**Exercice 23.** Soit $n$ un entier strictement positif, on se donne une partition $n = n_1 + \cdots + n_k$ avec $n_1 \geq n_2 \geq \cdots \geq n_k$.
On posera $n_{k+1} = 0$. On se donne des scalaires $\lambda_1 \neq \cdots \neq \lambda_k$ d'un corps $K$. Soit $P_j$ le polynôme

$$P_j(X) = (X - \lambda_1) \cdots (X - \lambda_j)$$

pour tout $j \in [1, k]$.
(i) Montrer que le $K[X]$-module

$$M = \bigoplus_{j=1}^{k} (K[X]/(P_j))^{n_j - n_{j+1}}$$

est isomorphe à

$$M' = \bigoplus_{j=1}^{k} (K[X]/(X - \lambda_j))^{n_j}.$$

On note $\bar{K}$ un corps algébriquement clos contenant $K$.
(ii) Calculer les invariants de similitude d'une matrice diagonalisable de $M_n(\bar{K})$ en fonction des valeurs propres et de leur multiplicité.
(iii) Montrer qu'une matrice carrée $F \in M_n(K)$ est diagonalisable dans $\bar{K}$ si et seulemet si tous les invariants de similitude sont sans facteurs carrés. Montrer que ceci est équivalent au fait que le polynôme minimal est sans facteur carré.
On dit qu'un module non nul est simple si ses seuls sous-modules sont (0) et lui-même. Un module est dit semi-simple s'il est somme directe de modules simples.
(iv) Montrer que tout $K[X]$-module simple est de type fini.
(v) Montrer que les $K[X]$-modules simples de $M$ sont les modules isomorphes à $K[X]/(P)$ avec $P$ irréductible. Montrer que $P$ est un générateur de $\mathrm{Ann}(M)$.
(vi) Soit $M$ et $M'$ deux $K[X]$-modules simples. Montrer que l'on a

$$\mathrm{Hom}_{K[X]}(M, M') = \begin{cases} (0) & \text{si } M \not\simeq M' \\ A/\mathrm{Ann}(M) & \text{si } M \simeq M'. \end{cases}$$

(vii) Montrer qu'une matrice $F \in M_n(K)$ est diagonalisable dans $\bar{K}$ si et seulement si le $K[X]$-module associé ($\bar{K}^n$ muni de la multiplication $X \cdot v = F \cdot v$) est semi-simple.
(viii) Soit $M$ semi-simple sur $K[X]$. Calculer la dimension sur $K$ de $\mathrm{End}_{K[X]}(M)$ en fonction du degré des facteurs invariants de $M$.
(ix) Calculer la dimension sur $K$ du commutant d'une matrice $F \in M_n(K)$ telle que le $K[X]$-module associé est semi-simple.

**Exercice 24.** Soit $m$ l'endomorphisme de $\mathbb{Z}^2$ de matrice

$$\begin{pmatrix} 3 & 18 \\ -6 & 51 \end{pmatrix}.$$

(i) Montrer que $m$ est injective.
(ii) Déterminer $a$ et $b$ dans $\mathbb{N}^*$ tels que $a|b$ et $\mathrm{Coker}(m) \simeq \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$.
(iii) À quelle condition l'élément $(3, t)$ appartient-t-il à $\Im(m)$.
(iv) Montrer que $A = \mathbb{R}[X, Y]$ n'est pas principal.
(v) Montrer que la matrice

$$\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} \in M_2(A)$$

n'est pas équivalente à une matrice

$$\begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix} \in M_2(A)$$

telle que $P|Q$.