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

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

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* $q_N \geq 2$.

Solution. a) i) *Montrer que la suite* (r_n) *est strictement décroissante puis nulle.*
On a $r_n \geq 0$ si $n \geq 2$. Puis $r_n = 0$ ou $r_{n+1} < r_n$. Si $r_2 > 0$, alors r_n est strictement décroissante jusqu'au moment où elle s'annule.
Quelle est cette suite pour $a = 465$ *et* $b = 185$ *?*
On a

$$\begin{aligned} 465 &= 2 \cdot 185 + 95 \\ 185 &= 1 \cdot 95 + 90 \\ 95 &= 1 \cdot 90 + 5 \\ 90 &= 18 \cdot 5 + 0 \end{aligned}$$

On déduit alors que $q_0 = 2, q_1 = 1, q_2 = 1, q_3 = 18$.

ii) *Montrer que* $d = r_N = \text{pgcd}(a, b)$.
On a $(a, b) = (b, a - \lambda b)$ donc $(r_{i-1}, r_i) = (r_i, r_{i+1})$ et finalement $(a, b) = (r_0, r_1) = (r_N, 0) = r_N$.

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

ii) $a = 465$ *et* $b = 185$.
On a

$$\begin{array}{rrcl} & 465 & = & 1 \cdot 465 + 0 \cdot 185 \\ & 185 & = & 0 \cdot 465 + 1 \cdot 185 \\ (L_1 - 2L_2) & 95 & = & 1 \cdot 465 - 2 \cdot 185 \\ (L_2 - L_3) & 90 & = & -1 \cdot 465 + 3 \cdot 185 \\ (L_3 - L_4) & 5 & = & 2 \cdot 465 - 5 \cdot 185 \\ (L_4 - 18L_5) & 0 & = & -37 \cdot 465 + 93 \cdot 185 \end{array}$$

c) i) *Montrer que pour tout i, on a* $\begin{pmatrix} r_{i+1} & u_{i+1} & v_{i+1} \\ r_i & u_i & v_i \end{pmatrix} = \begin{pmatrix} -q_i & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_i & u_i & v_i \\ r_{i-1} & u_{i-1} & v_{i-1} \end{pmatrix}$
Simple identité matricielle.

ii) *En déduire que* $u_{i+1}v_i - u_i v_{i+1} = \pm 1$.
De $\begin{pmatrix} u_{i+1} & v_{i+1} \\ u_i & v_i \end{pmatrix} = \begin{pmatrix} -q_i & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} u_i & v_i \\ u_{i-1} & v_{i-1} \end{pmatrix}$ on déduit l'égalité des determinants des deux côtés. Et ce déterminant vaut -1 si $i = 0$

iii) *Montrer que les suites (u_i) et (v_i) sont de signe alterné et croissantes en valeur absolue (On supposera ici que $0 < b < a$).*
Par récurrence, puisque $(-1)^{i+1}u_{i+1} = (-1)^{i-1}u_{i-1} + (-1)^i q_i u_i$ et $q_i \geq 1$, on déduit que $|u_i|$ est croissante strictement.

iv) *En déduire que les solutions de $ua + vb = 0$ sont de la forme $k(u_{N+1}, v_{N+1}), k \in \mathbb{Z}$.* On a d'après la question 3, $\begin{vmatrix} r_{N+1} & u_{N+1} \\ r_N & u_N \end{vmatrix} = \pm \begin{vmatrix} r_1 & u_1 \\ r_0 & u_0 \end{vmatrix}$, soit $u_{N+1} = \pm b/d$ et $v_{N+1} = \pm a/d$. Les solutions de $ua+vb = 0$ sont de la forme $\lambda(-b/d, a/d)$. En effet, une solution existe (u_{N+1}, v_{N+1}) et si $ua+vb = 0$ alors a divise vb donc a/d divise vb/d donc divise v (car a/d et b/d sont premiers entre-eux).

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

Solution. a) Soit u et v tels que $un + vm = d$. On considère la matrice $L = \begin{pmatrix} u & v \\ -m/d & n/d \end{pmatrix}$ et on a $L \cdot \begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$. L est de déterminant 1. On a $L \begin{pmatrix} 0 \\ m \end{pmatrix} = \begin{pmatrix} mv \\ nm/d \end{pmatrix} = \begin{pmatrix} 0 \\ nm/d \end{pmatrix} + vm/dL \cdot \begin{pmatrix} n \\ m \end{pmatrix}$. Donc $\begin{pmatrix} 0 \\ nm/d \end{pmatrix}$ et $\begin{pmatrix} d \\ 0 \end{pmatrix}$ sont dans $L(nA \times mA)$. Par conséquent $L(nA \times mA) = dA \times nm/dA$.

b) Considérons la matrice $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$, dont l'image est $nA \times mA$. En faisant des opérations élémentaires sur les lignes et les colonnes de $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$, on obtient

$$\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \sim \begin{pmatrix} n & 0 \\ un & m \end{pmatrix} \sim \begin{pmatrix} n & 0 \\ un + vm & m \end{pmatrix} \sim \begin{pmatrix} 0 & -nm/d \\ d & m \end{pmatrix} \sim \begin{pmatrix} 0 & -nm/d \\ d & 0 \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & nm/d \end{pmatrix}.$$

c) On trouve $\phi = \begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}$.

Exercice 4. (1) 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 :

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

Solution. (i) On fait l'algorithme d'Euclide étendu en commençant par les divisions euclidiennes successives :

$$\begin{aligned} 255 &= 1 \times 141 + 114 \quad (E_1) \\ 141 &= 1 \times 114 + 27 \quad (E_2) \\ 114 &= 4 \times 27 + 6 \quad (E_3) \\ 27 &= 4 \times 6 + 3 \quad (E_4) \\ 6 &= 2 \times 3 + 0 \quad (E_5) \end{aligned}$$

ce qui donne $\text{pgcd}(255, 141) = 3$. Pour trouver une solution de l'équation on remonte les égalités en éliminant tous les restes, on calcule $4 \times (E_3) - (E_4)$

$$4 \times 114 = 17 \times 27 - 3$$

puis $17 \times (E_2) - (4 \times (E_3) - (E_4))$

$$17 \times 141 = 21 \times 114 + 3$$

et $21 \times (E_1) - (17 \times (E_2) - (4 \times (E_3) - (E_4)))$

$$21 \times 255 = 38 \times 141 - 3$$

d'où la solution $(-21, 38)$:

$$(-21) \times 255 + 38 \times 141 = 3.$$

(ii) Le module en question est le noyau de l'application linéaire

$$f : \mathbb{Z}^2 \to \mathbb{Z}$$

$$(x, y) \mapsto 255x + 141y.$$

On va diagonaliser cette application dont la matrice est $(255, 141)$ pour trouver facilement son noyau. Remarquons que la solution précédente nous donne la relation

$$(-21) \times 3 \times 85 + 38 \times 3 \times 47 = 3.$$

On fait un changement de base au départ en utilisant la matrice

$$M = \begin{pmatrix} -21 & -47 \\ 38 & 85 \end{pmatrix}$$

qui vérifie $\det(M) = 1$ qui est donc inversible d'inverse

$$M^{-1} = \begin{pmatrix} 85 & 47 \\ -38 - 21 & \end{pmatrix}.$$

On obtient alors $(255, 141)M = (3, 0)$. Le noyau de $(3, 0)$ est engendré par $(0, 1)$ donc celui de $(255, 141)$ par $M(0, 1) = (-47, 85)$. On peut remarquer qu'on a en fait pas besoin de la solution de l'algorithme d'Euclide étendu mais seulement du pgcd.
(iii) Les solutions forment un espace affine d'espace direction donné par le sous-module précédent. Elle sont donc de la forme

$$(x, y) = (-21, 38) + n(-47, 85) \quad n \in \mathbb{Z}.$$

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^{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 $\begin{pmatrix} 1 & 3 & 2 \\ 2 & 0 & 2 \\ -2 & 6 & 0 \\ 3 & 3 & 4 \end{pmatrix}$.

Solution. a) *Vérifier que $X'_i = XR_i$.*
Identité matricielle bien connue...

b) i) *Montrer qu'une une opération élémentaire ne modifie pas l'image de X*
$\operatorname{Im} X$ est engendré par les X_i et donc aussi par les X'_i.

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 $X' = X \cdot R$.*
Si $X' = XR$ alors $R = IR$. Multiplier à doite par R reveient à modifier les colonnes de X qui deviennent XR_i. Les colonne de I sont donc $R_i = I_i + \lambda I_j$, dont le déterminant est clairement 1. Idem pour la transposition, avec changement de signe.

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 :*
Il suffit de montrer, que pour un vecteur ligne $X = (a_1, \ldots, a_m)$, on peut trouver R de déterminant 1 telle que $XR = (d, 0, \ldots, O)$.
Remarquons alors, que dans ce cas, $d = \operatorname{pgcd}(a1, \ldots, a_n)$. En effet $d = \sum_i a_i R_{i,1}$ est dans l'idéal engendré par les a_i donc engendré par leur pgcd. Réciproquement, puisque R est inversible d'inverse R', on a $a_i = dR_{i,1}$ donc d divise a_i et donc d divise leur pgcd. Si $ua_1 + va_2 = d$, alors la matrice R égale à l'identité,sauf le premier bloc 2×2 égal à $\begin{pmatrix} u & -a_2/d \\ v & a_1/d \end{pmatrix}$ satisfait $XR = (d, 0, a_3, \ldots, a_n)$. On recommence ensuite avec la première et la troisième coordonnée jusqu'à arriver à $(*, 0, \ldots, 0)$. On a alors $XR = \begin{pmatrix} \bullet & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \end{pmatrix}$

c) i) *Montrer que il existe une matrice R de déterminant 1 telle que $X' = X \cdot R$ est échelonnée.* On peut transformer la première ligne de X en une ligne $(*, 0, \ldots 0)$. Si $* = 0$, alors on échelonne la sous-matrice formée des $n-1$ dernières lignes de X en multipliant à droite par une matrice de déterminant 1. Sinon, on échelonne la sous-matrice de X formée des $n-1$ dernières lignes et des $m-1$ dernières colonnes, en multipliant à droite par une matrice de déterminant 1 qui n'agira que sur les dernières colonnes.

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.*
Les r colonnes non-nulles de X' sont échelonnées donc libres. Elles engendrent l'image de X' donc celle de X car $X'_i = XR_i$ est combinanison des X_i et réciproquement. C'est une base de $\operatorname{Im} X$. Les $m-r$ dernières colonnes de R s'envoient sur le noyau de X, elles en forment une base. En effet, elles sont libres comme sous famille d'une base (les colonnes de R). Et si $V = v_1R_1 + \ldots + v_mR_m \in \ker X$, alors $XV = v_1X'_1 + \ldots + v_rX'_r = 0$ et $v_1 = \cdots = v_r = 0$. Donc $\ker X$ est engendré par les $R_i, i > r$.

iii) *Soit X une matrice et I la matrice identité $m \times m$. Montrer que si $X' = X \cdot R$, alors* $\begin{pmatrix} X \\ I \end{pmatrix} \cdot R = \begin{pmatrix} X' \\ R \end{pmatrix}$. Identité matricielle

d) *Déterminer image et noyau de la matrice* $\begin{pmatrix} 1 & 3 & 2 \\ 2 & 0 & 2 \\ -2 & 6 & 0 \\ 3 & 3 & 4 \end{pmatrix}$

On part de $\begin{bmatrix} 1 & 3 & 2 \\ 2 & 0 & 2 \\ -2 & 6 & 0 \\ 3 & 3 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Après échelonnement, on trouve $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 2 & -4 & 0 \\ 1 & 2 & 0 \\ 2 & 2 & 3 \\ 1 & 0 & 1 \\ -2 & -1 & -3 \end{bmatrix}$. On déduit une base de

$\operatorname{Im} X : \begin{bmatrix} 1 & 0 \\ 3 & 6 \\ 2 & 2 \\ 0 & 0 \end{bmatrix}$. Une base de $\ker X : \begin{bmatrix} 3 \\ 1 \\ -3 \end{bmatrix}$.

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 ?

Solution. a) *Trouver une base du noyau et d'un supplémentaire du noyau de X.*

On part de $\begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 2 & 1 & 4 & -1 & 1 \\ 1 & -1 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$. On obtient après échelonnement, $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 & 2 \\ -1 & -1 & 0 & -2 & -1 \\ 0 & 0 & 1 & 0 & 1 \\ 3 & 2 & -1 & 3 & 3 \end{bmatrix}$. Donc

une base du noyau est $\begin{bmatrix} 2 & 0 \\ 1 & 2 \\ -2 & -1 \\ 0 & 1 \\ 3 & 3 \end{bmatrix}$ et d'un suppélemntaire est $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 1 \\ 3 & 2 & -1 \end{bmatrix}$

b) *Trouver des formes lineaires telles que $x = \sum_{i=1}^{5} \lambda_i(x) E_i$.*

Les λ_i sont donnés par les lignes de $R^{-1} = \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 2 & 1 & 4 & -1 & 1 \\ 1 & -1 & 2 & 1 & 1 \\ -1 & 0 & -3 & 0 & -1 \\ -1 & 1 & -2 & 0 & -1 \end{bmatrix}$.

c) *Peut-on extraire de $(X_1, \dots, X_5)$, une base de l'image ?*
$\operatorname{Im} X = \mathbb{Z}^3$. On remarque que la première, troisième et conquième colonne de X forme une famille de déterminant 1 donc base de $\mathbb{Z}^3$.

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.

Solution. On échelonne $\begin{bmatrix} 4 & 3 & 2 & 1 \\ 5 & 6 & 7 & 8 \\ 12 & 11 & 10 & 9 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. On obtient $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 8 & 9 & 0 & 0 \\ 9 & 8 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & -3 & -2 \\ 1 & 2 & 2 & 1 \end{bmatrix}$ On déduit qu'un base des solutions est donnée par $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -3 & -2 \\ 2 & 1 \end{bmatrix}$.

Pour le second système, on cherche X tel que $AX \in \operatorname{Im} \begin{bmatrix} 8 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix}$. C'est à dire la projection dur $\mathbb{Z}^4$ du noyau de $\begin{bmatrix} 4 & 3 & 2 & 1 & 8 & 0 & 0 \\ 5 & 6 & 7 & 8 & 0 & 2 & 0 \\ 12 & 11 & 10 & 9 & 0 & 0 & 6 \end{bmatrix}$. On échelonne $\begin{bmatrix} 4 & 3 & 2 & 1 & 8 & 0 & 0 \\ 5 & 6 & 7 & 8 & 0 & 2 & 0 \\ 12 & 11 & 10 & 9 & 0 & 0 & 6 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$, et on obtient $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 4 & 3 & 2 & 3 & 4 \\ 1 & 2 & 4 & 6 & 5 \\ -1 & -1 & -1 & -2 & -2 \\ -18 & -18 & -23 & -37 & -37 \\ -8 & -8 & -9 & -16 & -16 \end{bmatrix}$

Le noyau de $\begin{bmatrix} 4 & 3 & 2 & 1 & 8 & 0 & 0 \\ 5 & 6 & 7 & 8 & 0 & 2 & 0 \\ 12 & 11 & 10 & 9 & 0 & 0 & 6 \end{bmatrix}$ est donc

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3 & 4 & 6 & 0 \\ 6 & 5 & 4 & 8 \\ -2 & -2 & -2 & -1 \\ -37 & -37 & -37 & -32 \\ -16 & -16 & -16 & -12 \end{bmatrix}$$ dont la projection est engendrée par $R := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3 & 4 & 6 & 0 \\ 6 & 5 & 4 & 8 \end{bmatrix}$, qui en est une base.
On remarque que $R_1 - R_3$ et $R_2 - R_3$ forme un base des solutions du système précédent.

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 $p_1^5 p_2^4$?

Solution. Il faut les rendre normalisés. C'est à dire sous la forme $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_r Z$ où $d_1 | \cdots | d_r$. On utilse l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/nm/d\mathbb{Z}$. On a donc $\mathbb{Z}/48\mathbb{Z} = \mathbb{Z}/48\mathbb{Z}$. Puis avec une notation évidente, $(2,24) = (2,24)$. $(3,16) \simeq (1,48) \simeq (48)$. $(4,12)$, $(6,8) \simeq (2,24)$, $(2,2,12)$, $(2,3,8) \simeq (2,1,24) \simeq (2,24)$, $(2,4,6) \simeq (2,2,12)$, $(2,2,2,6)$, $(2,2,3,4) \simeq (2,2,1,12) \simeq (2,2,12)$, $(2,2,2,2,3) \simeq (2,2,2,6)$. Cette décomposition est unique, puisque d_r est l'exposant du groupe.

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.

Solution.

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 $X_1 = (1,-1,2,1)$, $X_2 = (3,1,2,1)$, $X_3 = (3,5,2,3)$.

Solution.

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

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

Solution. (i) On effectue les multiplications suivantes pour diagonaliser la matrice :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ -701 & & \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Toutes les matrices qui interviennent ont un déterminant 1 ou -1 et sont donc inversibles dans $\mathbb{Z}$. La dernière matrice est donc équivalente à M et ses facteurs invariants sont $0|1|3$.
(ii) Le module N est le quotient terme à terme de Z^3 par $(0) \times \mathbb{Z} \times 3\mathbb{Z}$. On a donc

$$N \simeq \mathbb{Z} \times (0) \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Il reste à déterminer une base du noyau. D'après la matrice diagonale, il est clair que le noyau est isomorphe à $\mathbb{Z}$. De plus dans la nouvelle base (celle de la matrice diagonale), le noyau est engendré par $(0, 0, 1)$.
Dans la base de départ, le noyau est donc engendré par

$$\begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}.$$

(iii) On utilise la même méthode

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 1 \\ 0 & -5 & -3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ -701 & & \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 9 & 8 \end{pmatrix} \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 9 \end{pmatrix}.$$

Toutes les matrices qui interviennent ont un déterminant 1 et sont donc inversibles dans $\mathbb{Z}$. La dernière matrice est donc équivalente à M et ses facteurs invariants sont $1|1|9$.
Le module N est le quotient terme à terme de Z^3 par $\mathbb{Z} \times \mathbb{Z} \times 9\mathbb{Z}$. On a donc

$$N \simeq (0) \times (0) \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/9\mathbb{Z}.$$

Il reste à déterminer une base du noyau. D'après la matrice diagonale, il est clair que le noyau est isomorphe à (0).

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

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

Solution. On diagonalise la matrice correspondante

$$\begin{pmatrix} 4 & 2 & 3 \\ 5 & 8 & 11 \end{pmatrix}$$

on a

$$\begin{pmatrix} 1 & 0 \\ -51 & \end{pmatrix} \begin{pmatrix} 4 & 2 & 3 \\ 5 & 8 & 11 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -3 \\ 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & 0 & 1 \\ 0 & 1 & 0 \\ 15 & 0 & -8 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ainsi dans la nouvelle base le sous-module est engendré par $(1, 0, 0)$ et dans celle de départ il est engendré par

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -3 \\ 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & 0 & 1 \\ 0 & 1 & 0 \\ 15 & 0 & -8 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ -29 \\ 22 \end{pmatrix}.$$

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

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

Solution. On met la matrice M sous forme diagonale : en multipliant à gauche par

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2-X & 1 & 0 \\ -201 & & \end{pmatrix}$$

et à droite par

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3-X & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

on obtient

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & (X-3)(X-6) & 0 \\ 0 & 0 & X-3 \end{pmatrix}.$$

Les invariants de similitude de M sont donc $1 \mid X-3 \mid (X-3)(X-6)$ la matrice M est donc semblable à

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

On met la matrice M' sous forme diagonale : en multipliant à gauche par

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2-X & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -X & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et à droite par

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2-X & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & (X-1)^2 \\ 0 & 0 & -1 \end{pmatrix}$$

on obtient

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-1)^2(X-2) \end{pmatrix}.$$

Les invariants de similitude de M sont donc $1 \mid 1 \mid (X-1)^2(X-2)$ la matrice M est donc semblable à

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

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 μ 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 $p = a^2 + b^2$).

Solution. (i) Soit $x \in L$ et $a \in \mathbb{Z}$ tels que $ax = 0$, alors comme $x \in L \subset \mathbb{Z}^n$, on a $a = 0$ ou $x = 0$ donc L est bien sans torsion.
On considère alors les facteurs invariants de L qui sont des idéaux $(d_1), \cdots, (d_k)$ de $\mathbb{Z}$ tels que $d_1 | d_2 | \cdots | d_k$ et

$$L \simeq \bigoplus_{i=1}^{k} \mathbb{Z}/(d_i).$$

Comme L est sans torsion, tous les d_i sont nuls et donc $L \simeq \mathbb{Z}^k$ est libre.
(ii) Soient $(e_i)_{1 \le i \le n}$ et $(f_i)_{1 \le i \le n}$ deux base de L comme $\mathbb{Z}$-module. On peut passer de l'une à l'autre par une matrice M inversible sur $\mathbb{Z}$ c'est-à-dire dont le déteminant $\det(M)$ est un inversible de $\mathbb{Z}$. On a dont $\det(M) = \pm 1$.
Mais alors on a pour tout i, $f_i = Me_i$ donc la matrice (f_i) formée par les f_i écrits en colonne est $(M(e_i))$ donc

$$\det(f_i) = \det(M) \det(e_i)$$

et comme $\det(M) = \pm 1$, on a le résultat.
(iii) On a vu au (i) que $L \simeq \mathbb{Z}^k$ et k est le rang de L. Comme L est un réseau on a $k = n$, donc $L \simeq \mathbb{Z}^n$. Pour étudier $\mathbb{Z}^n/L$, on identifie L à $\mathbb{Z}^n$ et on note M la matrice correspondant à l'inclusion de L dans $\mathbb{Z}^n$. On a alors la suite exacte :

$$0 \to \mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^n \to \mathbb{Z}^n/L \to 0$$

et L est l'image de M. On réduit alors la matrice M sous forme diagonale ce qui donne les facteurs invariants de $\mathbb{Z}^n/L$. On a alors que M est équivalente à une matrice de la forme

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix}.$$

Ainsi on voit que $\mathbb{Z}^n/L \simeq \oplus_i (\mathbb{Z}/d_i\mathbb{Z})$ donc

$$\mathrm{card}(\mathbb{Z}^n/L) = \prod_{i=1}^{n} d_i.$$

Par ailleurs, l'écriture de M sous forme diagonale signifie qu'il existe une base (e_i) de $\mathbb{Z}^n$ dont les images sont les $(d_i e_i)$. Ces $(d_i e_i)$ forment une base de l'image de M c'est-à-dire une base de L. On peut donc calculer le volume de L grâce à cette base. On a donc

$$\mathrm{vol}(L) = |\det(d_i e_i)| = \left(\prod_{i=1}^{n} d_i \right) |\det(e_i)|.$$

Il reste à vérifier que $|\det(e_i)| = 1$, mais (e_i) est une base de $\mathbb{Z}^n$ donc la matrice (e_i) est inversible dans $\mathbb{Z}$ et son déterminant est ± 1.
(iv.a) Supposons par l'absurde que $B \to \mathbb{R}^n/2L$ est injective. Alors $(B+l)_{l \in 2L}$ forment une famille disjointe. Soit $(e_1, \cdots, e_n)$ une base de $2L$. Quitte à faire un changement de variable qui envoie (e_i) sur la base canonique (et

multiplie la mesure de Lebesgue par $1/vol(2L)$, on peut supposer que e_i est la base canonique). Soit $r = \text{diam}(B)$. Soit N un entier. On a

$$\mu(\bigcup_{(k_1,\cdots,k_n)\in\mathbb{Z}^n,|k_i|\leq N} B + (k_1,\cdots,k_n)) = (2N+1)^n\mu(B)$$

mais

$$\bigcup_{(k_1,\cdots,k_n)\in\mathbb{Z}^n,|k_i|\leq N} B + (k_1,\cdots,k_n) \subset [-N-r, N+r]^n.$$

On en déduit que $\mu(B) \leq \left(\frac{2N+2r}{2N+1}\right)^n$ et donc en faisant tendre N vers l'infini, $\mu(B) \leq 1$.
(iv.b) Comme $b \in B$, $-b \in B$. De plus comme B est convexe et que $a \in B$ et $-b \in B$, on a

$$\frac{1}{2}(a-b) \in B.$$

Par ailleurs, on a vu que $a - b \in 2L$ donc

$$\frac{1}{2}(a-b) \in L.$$

Ainsi

$$\frac{1}{2}(a-b) \in B \cap L$$

et cet élément est non nul car $a \neq b$.
(v) Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1$ et cyclique. Soit w un générateur de ce groupe. On a $y^{p-1} = 1$ et $y^n \neq 1$ pour $n < p-1$.
De plus, si $p \equiv 1 \pmod 4$, alors il existe $k \in \mathbb{N}$ tel que $p - 1 = 4k$. Soit alors $u = y^k$. On a alors $u^4 = y^{4k} = y^{p-1} = 1$, alors que $u^m = y^{mk} \neq 1$ si $m < 4$. L'élément u est d'ordre 4.
(vi) Calculons le volume du réseau L de l'énoncé : un élément de L s'écrit (a, b) avec $a \in \mathbb{Z}$ et $b = ua + kp$ avec $k \in \mathbb{Z}$. Les couples $(1, u)$ et $(0, p)$ sont libres et dans L. Par ailleurs, un élément $(a, b) \in L$ s'écrit $(a, b) = (a, au + kp) = a(1, u) + k(0, p)$ donc ces vecteurs forment une base de L. Ainsi on a

$$\text{vol}(L) = \left|\det \begin{pmatrix} 1 & 0 \\ u & p \end{pmatrix}\right| = p.$$

Soit maintenant B une boule de rayon r tel que

$$\pi r^2 > 4p \quad \text{et} \quad r^2 < 2p.$$

Ceci est possible car $\frac{4}{\pi} < 2$, on peut par exemple prendre $r = \sqrt{\frac{3}{2}}$. D'après la question (v), il existe alors un élément non nul $(x, y) \in B \cap L$. On a $y \equiv ux \pmod p$ donc

$$x^2 + y^2 \equiv x^2 + u^2x^2 \equiv x^2(1 + u^2) \equiv 0 \ (\bmod p)$$

car u est d'ordre 4 donc u^2 est d'ordre 2, c'est-à-dire $u^2 \equiv -1 \pmod p$. Mais alors on a que p divise $x^2 + y^2$ et

$$0 < x^2 + y^2 \leq r^2 < 2p$$

car (x, y) est non nul et dans B. Ceci impose que

$$x^2 + y^2 = p$$

donc p est somme de deux carrés.

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).

Solution. Montrons que M est sans torsion, le théorème de structure des modules sur les anneaux principaux ($\mathbb{Z}$ est principal et même euclidien) nous dira que M est alors libre. Comme M est un sous-module de $\mathbb{Z}^3$ qui est sans torsion, il est sans torsion et donc libre. Comme M est un sous-module de $\mathbb{Z}^3$, il est de rang inférieur à trois. Pour montrer qu'il est de rang 3, il suffit d'exhiber trois vecteurs de M linéairement indépendants. Or $(2, 0, 0)$, $(0, 2, 0)$ et $(0, 0, 2)$ sont dans M et linéairements indépendants (dans $\mathbb{Z}^3$ donc a fortiori dans M).

(ii) Soit $u_1 = (1,-1,0)$, $u_2 = (1,0,-1)$ et $u_3 = (2,0,0)$, montrons que (u_1,u_2,u_3) forme une base de M. Commençons par montrer que la famille est libre : c'est le cas sur $\mathbb{Q}$ donc a fortiori sur $\mathbb{Z}$. Montrons qu'elle est génératrice : soit $u = (x,y,z) \in M$, sur $\mathbb{Q}$ on a alors $u = -yu_1 - zu_2 + \frac{x+y+z}{2}u_3$ qui est bien à coefficients entiers car $2|x+y+z$.
(iii) Considérons l'application $\varphi : \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z}$ donnée par $(x,y,z) \mapsto Cl(x+y+z)$. Elle est surjective (par exemple $(1,0,0)$ s'envoie sur $Cl(1)$) et on noyau est exactement M. Elle induit donc un isomorphisme entre $\mathbb{Z}^3/M$ et $\mathbb{Z}/2\mathbb{Z}$ qui est évidement simple (il y a 2 éléments 0 et 1, si un sous-module est strict, il ne contient qu'un élément : 0).

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 $\mathbb{Z}^3$?

Solution. Supposons que M ait un supplémentaire N dans L. On a alors $L/M \simeq N$ et $N \subset L$. Comme L est sans torsion il en est de même de N et donc de L/M.
Réciproquement, supposons que L/M est sans torsion. Le théorème de structure nous dit alors que L/M est libre de rang disons r engendré par une base $(Cl(e_1),\cdots,Cl(e_r))$ avec $e_i \in L$. Notons alors N le sous-A-modulede L engendré par les e_i et montrons que N est un supplémentaire de M. Soit $x = \sum_i a_i e_i \in M \cap N$, alors $Cl(x) = \sum_i a_i Cl(e_i) = 0$ dans L/M car $x \in M$. Mais alors on a pour tout i, $a_i = 0$ donc $x = 0$. Ainsi $M \cap N = (0)$. Soit maintenant $x \in L$, on a alors $Cl(x) = \sum_i a_i Cl(e_i)$ dans L/M car $(Cl(e_i))$ est une base de L/M. Mais alors $Cl(x - \sum_i a_i e_i) = 0$ donc $x - \sum_i a_i e_i = m \in M$ et $x = m + \sum_i a_i e_i \in M + N$. On a constuit un supplémentaire de M.
Dans l'exercice 16 M n'a pas de supplémentaire car $\mathbb{Z}^3/M = \mathbb{Z}/2\mathbb{Z}$ est de torsion.

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.

Solution. (i) D'après le théorème de structure, on sait qu'il existe des entiers $d_1|d_2|\cdots|d_r$ tel que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$. On voit alors qu'il existe un élément d'ordre d_r (par exemple $(0,\cdots,0,1)$). Par ailleurs on a pour tout élément x, $d_r \cdot x = 0$ donc l'ordre de tout élément divise d_r.

(ii) On utilise encore le théorème de structure. On a les $d_i \geq 2$ précédents. Il faut alors que $\prod_{i=1}^{r} d_i = 16$. On a alors les cas suivants
Si $r = 4$ et $d_1 = d_2 = d_3 = d_4 = 2$, dans ce cas $G \simeq (\mathbb{Z}/2\mathbb{Z})^4$.
Si $r = 3$ et $d_1 = d_2 = 2$ et $d_3 = 4$, dans ce cas $G \simeq (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}$.
Si $r = 2$ et $d_1 = d_2 = 4$, dans ce cas $G \simeq (\mathbb{Z}/4\mathbb{Z})^2$.
Si $r = 2$ et $d_1 = 2$ et $d_3 = 8$, dans ce cas $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.
Si $r = 1$ et $d_1 = 16$, dans ce cas $G \simeq \mathbb{Z}/16\mathbb{Z}$.

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.

Solution. (i) C'est le théorème de structure des modules de type fini sur un anneau principal.
(ii) D'après la question précédente, M est le quotient de A^s par $(d_1)\oplus\cdots\oplus(d_s)$. Notons $(e-1,\cdots,e_s)$ la base canonique de A^s. Il suffit de montrer que le morphisme u_i défini sur A^s par $u_i(e_j)=0$ pour $1\leq j<s$ et $u_i(e_s)=m_i$ a un noyau contenant $(d_1)\oplus\cdots\oplus(d_s)$. Cependant, soit $x_j=d_je_j$. Les x_j pour $1\leq j\leq s$ engendrent $(d_1)\oplus\cdots\oplus(d_s)$ et si $j<s$, on a $u_i(x_j)=0$, donc $x_j\in\ker u_i$. Par aillerus $u_i(e_s)=d_sm_i$. Mais $d_i|d_s$ donc $d_sm_i=0$ et on a le résultat.
(iii) Pour tout i, on peut écrire

$$u(m_i)=\sum_{j=1}^{s}a_{i,j}m_j.$$

Comme u commute avec tout endomorphisme, il commute avec les u_i de la question (i). On a alors

$$u(m_i)=u(u_i(m_s))=u_i(u(m_s))=u_i(\sum_{j=1}^{s}a_{s,j}m_j)=a_{s,s}m_i.$$

Ainsi pour tout i on a $u(m_i)=a_{s,s}m_i$ et comme les m_i engendrent, on a pour tout $m\in M$, $u(m)=a_{s,s}m$.
(iv) Maintenant on suppose seulement que u est additif. Soit $a\in A$ et $\mu_a:M\to M$ la multiplication par a. On a

$$u(am)=u(\mu_a(m))=\mu_a(u(m))=au(m),$$

donc u est linéaire et on applique le (iii).
(v) Considérons E comme $k[X]$-module grâce à u : $P(X)\cdot e=P(u)(e)$. Les endomorphismes de E comme $k[X]$-module sont les endomrphismes v tels que $v\circ P(u)=P(u)\circ v$ autrement dit ce sont les endomorphismes qui commutent à u. Un endomrophisme w qui commute à tous les endomorphisme commutant à u est donc un élément du centre de $\mathrm{End}_{k[X]}(E)$. De plus w étent k-linéaire il est additif (mais pas a priori $k[X]$-linéaire). C'est donc un élément de la forme $w(m)=P(X)\cdot m$ (cf. (iv)), on encore de la forme $P(u)(m)$ c'est à dire un polynôme en 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 $D(a_1,\cdots,a_n)$.

Solution. (i) On se place sur le $k[X]$-module libre de rang n : $k[X]^n$. On considère alors l'application $k[X]$-linéaire $X\mathrm{id}-M$ dont on sait qu'elle est semblable à une matrice diagonale. Mais alors l'application $k[X]$-linéaire $X\mathrm{id}-{}^tM$ a pour matrice exactement la transposée de la précédente, elle est donc semblable à la même matrice diagonale que la précédénte. Les invariants de similitude de M et ${}^tM$ sont donc les mêmes et M et ${}^tM$ sont semblables.
(ii) Commençons par le cas $r=2$. Soient U et V des polynômes tels que $UP_1+VP_2=1$. On calcule le produit suivant

$$\begin{pmatrix}\mathrm{Id}_n & 0\\ =-VP_2\cdot\mathrm{Id}_n & \mathrm{Id}_n\end{pmatrix}\cdot\begin{pmatrix}\mathrm{Id}_n & \mathrm{Id}_n\\ 0 & \mathrm{Id}_n\end{pmatrix}\cdot\begin{pmatrix}P_1\cdot\mathrm{Id}_n & 0\\ 0 & P_2\cdot\mathrm{Id}_n\end{pmatrix}\cdot\begin{pmatrix}U\cdot\mathrm{Id}_n & -P_2\cdot\mathrm{Id}_n\\ V\cdot\mathrm{Id}_n & P_1\cdot\mathrm{Id}_n\end{pmatrix}$$

elle est équivalente à la matrice diagonale $D(P_1\cdot\mathrm{Id}_n,P_2\cdot\mathrm{Id}_n)$ car les autres matrices sont inversibles (le déterminant de la dernière est $UP_1+VP_2=1$ par définition de U et V). Par ailleurs ce produit vaut $D(\mathrm{Id}_n,P_1P_2\cdot\mathrm{Id}_n)$.
Supposons que la propriété est vraie au rang $r-1$. Alors la matrice diagonale par blocs $D(P_1\cdot\mathrm{Id}_n,\cdots,P_{r-1}\cdot\mathrm{Id}_n,P_r\cdot\mathrm{Id}_n)$ est équivalente à $D(\mathrm{Id}_n,\cdots,\mathrm{Id}_n,\prod_{i=1}^{r-1}P_i\cdot\mathrm{Id}_n,P_r\cdot\mathrm{Id}_n)$. Mais comme $\prod_{i=1}^{r-1}P_i$ et P_r sont premier entre eux on peut réappliquer le résultat du cas $r=2$ à ces deux blocs et la matrice est bien équivalente à ce qu'on cherchait.
(iii) Notons $P_1,\cdots,P_r$ les invariants de similitude de M. On a donc $P_m|\cdots|P_1$ et on sait (cf. cours) que P_1 est le polynôme minimal μ_M de M et que le polynôme caractéristique de M, χ_M est $P_1\cdots P_r$.
Supposons que toutes les valeurs propres de M sont distinctes, alors on a $P_1=\mu_M=\chi_M=P_1\cdots P_r$. Ainsi on a $P_1=\mu_M=\chi_M$ et $P_i=1$ pour $i>1$. C'est ce que dit le (ii) avec $n=1$, et les $P_i=X-a_i$ deux à deux premiers entre eux car les a_i sont tous distincts. Ceci ne fonctionne plus dans le cas général.

Dans le cas général, notons $\lambda_1, \cdots, \lambda_r$ les valeurs propres de M et notons α_i les multiplicités de ces valeurs propres. On peut supposer que l'on a $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_r$. Il s'agit donc de trouver une matrice de la forme $D(P_1, \cdots, P_s, 1 \cdots, 1)$ avec $1|P_s| \cdots |P_1$ qui est équivalente à la matrice $D((X-\lambda_1)\cdot \mathrm{Id}_{\alpha_1}, \cdots, (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_r})$. Montrons que les invariants de similitude sont les

$$P_k = \prod_{\alpha_j \geq k} (X - \lambda_j).$$

Remarquons tout d'abord qu'on a bien $1|P_s| \cdots |P_1$ et que le polynôme P_i apparaît $\alpha_i - \alpha_{i-1}$ fois (avec pour convention $\alpha_0 = 0$) et le polynôme 1 apparaît $n - \alpha_r$ fois. On raisonne par récurrence sur le nombre r de valeurs propres. Nous réécrivons la matrice diagonale par blocs $D((X-\lambda_1)\cdot \mathrm{Id}_{\alpha_1}, \cdots, (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_r})$ sous la forme

$$D((X-\lambda_1)\cdot \mathrm{Id}_{\alpha_1}, (X-\lambda_2)\cdot \mathrm{Id}_{\alpha_1} \cdots, (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_1}, (X-\lambda_2)\cdot \mathrm{Id}_{\alpha_2-\alpha_1}, \cdots (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_r-\alpha_1}).$$

D'après le (ii) cette dernière matrice est équivalente à

$$D(\mathrm{Id}_{r\alpha_1}, P_1 \cdot \mathrm{Id}_{\alpha_1}, (X-\lambda_2)\cdot \mathrm{Id}_{\alpha_2-\alpha_1}, \cdots, (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_r-\alpha_1}).$$

On constate alors que la matrice $D((X-\lambda_2)\cdot \mathrm{Id}_{\alpha_2-\alpha_1}, \cdots, (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_r-\alpha_1})$ n'a plus que $r-1$ valeurs propres. On peut donc appliquer l'hypothèse de récurrence, ses invariants de similitude étant exactement les $P_{\alpha_1+1}, \cdots, P_r$ et 1 qui apparaît $n - \alpha_r - r\alpha_1$ fois. La matrice de départ $D((X-\lambda_1)\cdot \mathrm{Id}_{\alpha_1}, \cdots, (X-\lambda_r)\cdot \mathrm{Id}_{\alpha_r})$ est donc équivalente à

$$D(\mathrm{Id}_{r\alpha_1}, P_1 \cdot \mathrm{Id}_{\alpha_1}, \mathrm{Id}_{n-\alpha_r-r\alpha_1}, P_{\alpha_1+1}, \cdots, P_s) = D(\mathrm{Id}_{n-\alpha_r}, P_1, \cdots, P_{\alpha_1}, P_{\alpha_1+1}, \cdots, P_s)$$

car P_1 apparaît α_1 fois.

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 $\dim_k C(M) \geq n$.

Solution. (i) On considère le morphisme $C(M) \to C(A)$ défini par $N \mapsto PNP^{-1}$. On commence par vérifier qu'il est bien à valeurs dans $C(A)$. En effet, on a

$$A \cdot PNP^{-1} = PMP^{-1} \cdot PNP^{-1} = PMNP^{-1} = PNMP^{-1} = PNP^{-1} \cdot PMP^{-1} = PNP^{-1} \cdot A.$$

Ce morphisme a un morphisme réciproque $C(A) \to C(M)$ défini par $R \mapsto P^{-1}RP$, ce qui nous donne l'isomorphisme recherché.
Remarquons que ce résultat nous permet de dire que pour déterminer le commutant d'une matrice, il suffit de déterminer celui d'une matrice dans sa classe de similitude et donc en particulier de sa réduite de Jordan.
(ii) Notons $M = (m_{i,j})$ on a alors $m_{i,i} = a$ pour $i \in [1,n]$, $m_{i,i+1} = 1$ pour $i \in [1, n-1]$ et $m_{i,j} = 0$ dans les autres cas. Soit $(a_{i,j}) = A \in C(M)$. On peut alors calculer les produits $AM = (b_{i,j})$ et $MA = (c_{i,j})$. On a alors

$$b_{i,j} = \sum_{k=1}^{n} a_{i,k}m_{k,j} = aa_{i,j} + a_{i,j-1} \text{ et } c_{i,j} = \sum_{k=1}^{n} m_{i,k}a_{k,j} = aa_{i,j} + a_{i+1,j}$$

avec pour convention que $a_{i,j}$ est nul si $i < 0$, si $j < 0$, si $i > n$ et si $j > n$. On voit alors que $A \in C(M)$ si et seulement si on a $a_{i,j-1} = a_{i+1,j}$.

On va considérer les diagonales de A c'est-à-dire les termes de la forme $a_{i,j}$ avec $j = i+k+1$, $k \in \mathbb{Z}$. On a alors $a_{i,i+k} = a_{i+1,i+k+1}$ ce qui signifie que les différentes diagonales de A sont constantes. Par ailleurs si $k < 0$ c'est-à-dire si $j < i$, alors on a $0 = a-k, 0 = a_{-k+1,1}$ donc toutes les sous-diagonales sont nulles. La matrice A est donc de la forme

$$A = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ 0 & x_1 & x_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & x_3 \\ \vdots & 0 & \ddots & x_1 & x_2 \\ 0 & \cdots & \cdots & 0 & x_1 \end{pmatrix}.$$

Notons $C(x_1, \cdots, x_n)$ une telle matrice. On vérifie aisément que les matrices $C(x_1, \cdots, x_n)$ sont dans $C(M)$. On a ainsi montré que $C(M)$ est l'ensemble des matrices de la forme $C(x_1, \cdots, x_n)$. Il est donc de dimension exactement n.

(iii) Pour calculer le commutant de M, on a vu à la question (i) qu'il suffit de s'intéresser à celui de sa réduite de Jordan. On considère donc une matrice diagonale par blocs, forme de jordan de M : $J(M) = D(J(a_1, n_1), \cdots, J(a_r, n_r))$ avec $n = \sum_{k=1}^{r} n_k$. D'après la question (ii), les matrices diagonales par blocs

$$D(C(x_{1,1}, \cdots, x_{1,n_1}), \cdots, C(x_{r,1}, \cdots, x_{r,n_r}))$$

sont dans le commutant de $J(M)$. On voit donc que le commutant est de dimension au moins $\sum_{k=1}^{r} n_k = n$.

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

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

Solution. (i) Il existe une matrice de $Gl_n(A)$ de première colonne $v = {}^t(v_1, \cdots, v_n)$ fixée si et seulement si on peut compléter cette colonne v en une base de A^n c'est-à-dire si A^n/Av est un A-modulelibre. D'après l'exercice 17, il faut et il suffit que A^n/Av soit sans torsion, c'est-à-dire que les coordonnées de v soient premières entre elles.

Pour conclure, on choisit alors $v = ax$ avec $a \in K$ et $v \in A^n$ tel que ses coordonnées soient premières entres elles.

(ii) Soit M une matrice carrée d'ordre n à coefficients dans K. Si la première colonne de M n'est pas nulle, il existe d'après la première question un élément non nul $a_1 \in K$ et une matrice $U_1 \in GL_n(A)$ tels que $U_1^{-1}M$ ait ${}^t(a_1, 0, \cdots, 0)$ comme première colonne. Posons $M_1 = U_1^{-1}M$. Si la première colonne de M est nulle, on pose $a_1 = 0$, $U_1 = \mathrm{Id}_n$ et $M_1 = M$. On écrit alors M_1 par blocs :

$$M_1 = \begin{pmatrix} a_1 & L_1' \\ 0 & M' \end{pmatrix}$$

où M' est carrée de taille $n-1$. Par récurrence, on peut écrire $M' = U'T'$ avec $U' \in GL_{n-1}(A)$ et $T' \in M_{n-1}(K)$ triangulaire supérieure. Posons alors

$$U = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix} \quad \text{de sorte que} \quad T = U^{-1}M_1 = \begin{pmatrix} a_1 & L_1' \\ 0 & T' \end{pmatrix}$$

est triangulaire supérieure. Finalemant $M = U_1M_1 = U_1UT$ est le produit d'une matrice U_1U de $GL_n(A)$ et d'une matrice triangulaire supérieure de $M_n(K)$.

(iii) On a

$$M = \frac{1}{420}\begin{pmatrix} 210 & 420 & -105 \\ 168 & 840 & 280 \\ 315 & 60 & -420 \end{pmatrix}.$$

La première colonne est $\frac{1}{20}\,{}^t(10,8,15)$ et la matrice

$$U_1 = \begin{pmatrix} 10 & 0 & 1 \\ 8 & 1 & 0 \\ 15 & 2 & 0 \end{pmatrix}$$

appartient à $GL_3(\mathbb{Z})$. Son inverse est

$$U_1^{-1} = \begin{pmatrix} 0 & 2 & -1 \\ 0 & -15 & 8 \\ 1 & -20 & 10 \end{pmatrix}.$$

On a

$$420U_1^{-1}M = \begin{pmatrix} 21 & 1620 & 980 \\ 0 & -12120 & -7560 \\ 0 & -15780 & -9905 \end{pmatrix}.$$

Les coefficients 12120 et 15780 on t pour pgcd 60. Une fois divisés par 60, ils deviennent 202 et 263 et une relation de Bézout est

$$-202 \times 69 + 263 \times 53 = 1.$$

On pose alors

$$U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -202 & 53 \\ 0 & -263 & 69 \end{pmatrix}$$

d'où

$$420U_2^{-1}U_1^{-1}M = \begin{pmatrix} 21 & 1620 & 980 \\ 0 & 60 & 3325 \\ 0 & 0 & 12530 \end{pmatrix}.$$

Finalement on a $M = UT$ avec

$$U = U_2U_1 = \begin{pmatrix} 10 & -263 & 69 \\ 8 & -202 & 53 \\ 15 & -404 & 106 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} \frac{1}{20} & \frac{27}{7} & \frac{7}{3} \\ 0 & \frac{1}{7} & \frac{95}{12} \\ 0 & 0 & \frac{179}{60} \end{pmatrix}.$$

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.

Solution. (i) Comme $\lambda_i \neq \lambda_j$ pour $i \neq j$, les $(X-\lambda_i)$ sont deux-à-deux premiers entre eux. Le lemme chinois nous donne donc l'isomorphisme

$$K[X]/(P_j) \simeq \bigoplus_{i=1}^{j} K[X]/(X-\lambda_i).$$

Ainsi on voit que

$$M \simeq \bigoplus_{j=1}^{k} \left(\bigoplus_{i=1}^{j} K[X]/(X-\lambda_i) \right)^{\oplus(n_j - n_{j+1})} = \bigoplus_{i=1}^{k} \left(\bigoplus_{j=i}^{k} K[X]/(X-\lambda_i) \right)^{\oplus(n_j-n_{j+1})}$$

$$= \bigoplus_{i=1}^{k} \Big(K[X]/(X-\lambda_i) \Big)^{\oplus \sum_{j=i}^{k}(n_j-n_{j+1})} = \bigoplus_{i=1}^{k} \Big(K[X]/(X-\lambda_i) \Big)^{\oplus(n_i-n_{k+1})} = M'.$$

(ii) Comme les invariants de similitude sont les mêmes pour deux matrices semblables, il suffit de traiter le cas d'une matrice f diagonale. La matrice du $K[X]$-module associé est alors $f - X\mathrm{Id}$ qui est également diagonale. Notons λ_i les valeurs propres de f et supposons que la multiplicité de λ_i est n_i avec (quitte à renuméroter les valeurs propres) :

$$n_1 \geq n_2 \geq \cdots \geq n_k \geq 1.$$

On voit alors que le $K[X]$-module associé à f est isomorphe à M'. Mais alors d'après la question précédente, il est également isomorphe à M. Cependant on a la relation de divisibilité suivante entre les polynômes P_j :

$$P_1 | \cdots | P_k.$$

Ainsi les invariants de similitude de f sont les P_j avec multiplicité $n_j - n_{j+1}$.
(iii) Si F est diagonalisable dans $\overline{K}$, on vient de voir que ses invariants de similitude sont les P_j. Ce sont aussi les invariants de similitude sur le corps K. Ils sont évidement sans facteur carré sur $\overline{K}$.
Réciproquement si tous les invariants de similitude de F sont sans facteur carré dans $\overline{K}$. Notons Q_j ces invariants de similitude et notons x_j leur multiplicité. Comme on est dans $\overline{K}$ qui est algébriquement clos, les polynômes Q_j sont scindés à racines simples. De plus on a la condition

$$Q_1 | \cdots | Q_k.$$

On peut donc écrire

$$Q_j = (X-\lambda_1)\cdots(X-\lambda_{r_j})$$

où les λ_i sont tous distincts (car Q_j est sans facteur carré). Si on note n_i le nombre de facteurs invariants Q_j où λ_i apparaît, on voit que les facteurs invariants de F sont les P_j avec multiplicicté $n_j - n_{j+1}$.
Le $K[X]$-module associé à F est donc isomorphe à M et donc aussi à M'. Il est donc isomorphe à celui d'une matrice diagonale ce qui signifie que F est diagonalisable.
Il reste la dernière équivalence. Si tous les facteurs invariants sont sans facteur carré, le polynôme minimal (qui est le plus grand facteur invariant) est aussi sans facteur carré.
Réciproquement si le polynôme minimal est sans facteur carré, comme c'est le plus grand des facteurs invriants, les autres le divisent et sont a fortiori sans facteur carré.
(iv) Nous montrons que M est monogène c'est-à-dire engendré par un seul élément. En effet, soit $m \in M$ un élément non nul, et soit M' le sous-module de M engendré par m. Il n'est pas nul (il contient $m \neq 0$), comme M est simple c'est donc M tout entier et M est engendré par m.
(v) On vient de voir que M est engendré par un seul élément, ceci nous donne une surjection

$$K[X] \to M.$$

Notons I son noyau, c'est un idéal de $K[X]$ qui est principal donc $I = (P)$ pour un polynôme P. On a alors que $M \simeq K[X]/(P)$.
Supposons que $P = QR$ et considérons le sous-module engendré par $Cl(Q)$ la classe de Q dans M, il est soit nul soit égal à tout M. S'il est nul c'est que $Cl(Q) = 0$ c'est-à-dire que P divise Q. On a alors $Q = PS$ et $P = PSR$ donc $RS = 1$ et R est inversible. Si par contre il est non nul c'est que $Cl(Q)$ engendre M donc en particulier $Cl(1) = A \cdot Cl(Q)$ et donc $1 = AQ + BP$. Les polynômes P et Q sont premiers entre eux donc P divise R, on a $R = PS$ et $P = QPS$ donc $1 = QS$ et Q est inversible. On a donc soit Q soit R inversible donc P est irréductible.
Réciproquement si P est irréductible et $M = K[X]/(P)$, montrons que M est simple. Soit M' un sous-module non nul de M, alors il existe $Cl(Q) \neq 0$ dans M'. Mais alors comme P est irréductible et P ne divise pas Q, il sont premiers entre eux donc il existe A et B tels que

$$AP + BQ = 1.$$

Ainsi si $Cl(R) \in M'$, on a $Cl(R) = Cl(APR + BQR) = BR \cdot Cl(Q) \in M'$. On a donc $M' = M$ et M est simple.
L'annulateur de $K[X]/(P)$ est exactement l'idéal (P) donc P est bien un générateur de l'annulateur.
(vi) Soient M et M' deux $K[X]$-modules simples. On peut donc les écrire sous la forme $K[X]/(P)$ et $K[X]/(Q)$ respectivement avec P et Q des polynômes irréductibles. Un élément $f \in \mathrm{Hom}_{K[X]}(M, M')$ correspond à la donnée d'un morphisme f de $K[X]$ dans M' dont le noyau contient P. Il suffit donc de se donner l'image $Cl(R) = f(1)$ de 1 telle que $0 = f(P) = P \cdot Cl(R) = Cl(PR)$. Il suffit donc de se donner R tel que Q divise PR.
On a alors deux solutions : si P et Q ne sont pas associés (c'est-à-dire si $M \not\simeq M'$), ils sont premiers entre eux (car irréductibles), on a donc Q divise R et $f(1) = 0$ donc le morphisme est nul. Si par contre P et Q sont associés (c'est-à-dire $M \simeq M'$), alors pour tout R on a que Q divise PR. Ainsi tous les R conviennent et l'ensemble des morphismes est donné par l'ensembles des classes $Cl(R)$. C'est exactement M' ou encore M c'est-à-dire $A/\operatorname{Ann}(M)$.
(vii) Si F est diagonalisable dans $\overline{K}$, alors on a vu (i) que $(\overline{K}[X]^n, F)$ est isomorphe à $M' \otimes_K \overline{K}$ qui est clairement somme directe de modules simples car les $X - \lambda_i$ sont irréductibles.
Réciproquement, si le module $(\overline{K}[X]^n, F)$ est semi-simple, alors il est somme directe de modules simples qui sont de la forme

$$\overline{K}[X]/(X - \lambda_i)$$

car $\overline{K}$ est algébriquement clos. Si on note n_i le nombre de fois où λ_i apparaît, on voit que $(\overline{K}[X]^n, F)$ est isomorphe à $M' \otimes_K \overline{K}$, il a donc les mêmes facteurs invariants et F est diagonalisable.
(viii) Soit M semi-simple, il est somme directe de modules simples donc il peut s'écrire sous la forme

$$M \simeq \bigoplus_{i=1}^{k} \Big(K[X]/(Q_i)\Big)^{n_i}$$

où les Q_i sont irréductibles deux-à-deux premiers entre eux. On peut alors calculer le module

$$\operatorname*{End}_{K[X]}(M) = \bigoplus_{1 \leq i,j \leq k} \operatorname*{Hom}_{K[X]}\left(\Big(K[X]/(Q_i)\Big)^{n_i}, \Big(K[X]/(Q_j)\Big)^{n_j}\right).$$

On a d'après (vi)

$$\operatorname*{End}_{K[X]}(M) = \bigoplus_{i=1}^{k} \Big(K[X]/(Q_i)\Big)^{n_i^2}.$$

On a donc

$$\dim_K \left(\operatorname*{End}_{K[X]}(M)\right) = \sum_{i=1}^{k} n_i^2 \deg(Q_i).$$

Il reste à exprimer les facteurs invariants selon les Q_i, mais en supposant que les n_i sont décroissants (quitte à renuméroter les Q_i) et en remplaçant $X - \lambda_i$ par Q_i dans la preuve de (i), on obtient que M est isomorphe à

$$\bigoplus_{i=1}^{k} \Big(K[X]/(P_i)\Big)^{n_i - n_{i+1}}$$

où $P_i = Q_1 \cdots Q_i$. Les P_i sont les facteurs invariants de M avec multiplicité $n_i - n_{i+1}$. On voit alors que

$$\deg(Q_i) = \deg(P_i) - \deg(P_{i-1})$$

ce qui nous donne

$$\dim_K \left(\operatorname*{End}_{K[X]}(M) \right) = \sum_{i=1}^{k} (n_i^2 - n_{i+1}^2) \deg(P_i).$$

(ix) Rappelons que le communtant de F correspond exactement aux endomorphismes de $(K[X]^n, F)$. Si F est telle que $(K[X]^n, F)$ est semi-simple, alors la dimension du commutant est

$$\sum_{i=1}^{k} (n_i^2 - n_{i+1}^2) \deg(P_i).$$

Remarquons que l'on a $n_i^2 - n_{i+1}^2 = (n_i - n_{i+1})(n_i + n_{i+1}) > n_i - n_{i+1}$ si $i < k$ et $n_k^2 - n_{k+1}^2 = n_k^2 \geq n_k$ avec égalité si et seumement si $n_k = 1$. Ainsi, on a que la dimension du commutant est au moins

$$\sum_{i=1}^{k} (n_i - n_{i+1}) \deg(P_i) = n$$

avec égalité si et seulement si $\deg(P_i) = 0$ pour $i < k$ et $n_k = 1$. Les facteurs invariants sont alors 1 avec la multiplicité $n - 1$ et P_n (le polynôme minimal) avec la multiplicité 1.
Si de plus $(\overline{K}[X]^n, F)$ est semi-simple, c'est-à-dire F diagonalisable, la dernière condition signifie que toutes les valeurs propres sont distinctes.

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 $P|Q$.

Solution. (i) Il suffit de calculer son déterlinant qui vaut $3 \times 51 + 6 \times 18 = 261$ et est non nul.
(ii) On réduit la matrice sous forme diagonale en la multipliant de la manière suivante :

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 18 \\ -6 & 51 \end{pmatrix} \begin{pmatrix} 1 & -6 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 87 \end{pmatrix}$$

ainsi $3|87$ et $\mathrm{Coker}(m) = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/87\mathbb{Z}$.
(iii) On a

$$\mathrm{Im}(m) = \mathrm{Im}\left(\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 3 & 0 \\ 0 & 87 \end{pmatrix} \right)$$

ainsi un élément de $\mathrm{Im}(m)$ s'écrit sous la forme $(3x, 87y - 6x)$. L'élément $(3, t)$ est dans l'image si et seulement si $x = 1$ et $t = 87y - 6$ c'est-à-dire si et seulement si $t \equiv -6 \pmod{87}$.
(iv) On considère l'idéal (X, Y) et on montre qu'il n'est pas principal. En effet, sinon il serait engendré par un unique élément $P \in k[X, Y]$ et on aurait alors P divise X et Y donc P serait de degré 0 en Y et en X. Le polynôme P serait une constante et (X, Y) serait égal à (0) ou à $k[X, Y]$ ce qui n'est pas le cas.
(v) Si c'était le cas, alors on aurait $M = k[X, Y]/(P) \oplus k[X, Y]/(Q) \simeq k[X, Y]/(X) \oplus k[X, Y]/(Y)$. Mais $\mathrm{Ann}(M) = (Q) = (XY)$ et on peut supposer $Q = XY$. Comme P divise Q, on a P qui est associé à 1, X, Y ou XY. Si $P = 1$, on regarde $M/(X, Y)M$ qui vaut à droite $k \oplus k$alors qu'il vaut à gauche k. Si $P = X($ ou symétriquement $P = Y$), alors on regarde $M/(X)M$ qui vaut à gauche $k[X, Y]/(X) \oplus k[X, Y]/(X)$ alors qu'à droite il vaut $k[X, Y]/(X) \oplus k[X, Y]/(X, Y)$. Dans le terme de gauche Y n'annule aucun élément (la multiplication par Y est injective) alors que dans le terme de droite Y annule la classe de $(0, 1)$. On raisonne de

la même fâon si $P = Y$. Si enfin, $P = XY$, on regarde $M/(X)M$ qui vaut à gauche $k[X,Y]/(X) \oplus k[X,Y]/(X)$ alors qu'à droite il vaut $k[X,Y]/(X) \oplus k[X,Y]/(X,Y)$. On conclue comme précédement.
Un autre moyen de conclure rapidement est de dire que l'idéal des mineurs des deux matrices sont identiques. On doit donc avoir $(P) = (P,Q) = (X,Y)$ ce qui est impossible car on a vu à la question précédente que (X,Y) n'est pas principal.