MAT4111
Premier semestre — 2020–2021

Fiche 7: Modules

1. On considère le $\mathbb{Z}$-module $\mathbb{Q}$.

(a) Déterminer $\mathsf{Tor}(\mathbb{Q})$.

(b) Quelles sont les familles libres maximales du $\mathbb{Z}$-module $\mathbb{Q}$?

(c) $\mathbb{Q}$ est-il un $\mathbb{Z}$-module libre ?

(d) $\mathbb{Q}$ est-il un $\mathbb{Z}$-module de type fini ?

Solution.

(a) C'est clair que $\mathsf{Tor}(\mathbb{Q}) = \{0\}$.

(b) On affirme qu'un ensemble S du $\mathbb{Z}$-module $\mathbb{Q}$ est libre si et seulement si le cardinal de S est 1 et $S \neq \{0\}$. En effet, si l'ensemble $S \subseteq \mathbb{Q}$ contient 0, il n'est pas libre. En outre, si $x = a/b$ et $x' = a'/b'$ sont deux éléments différents non nuls de S, avec $a, a', b, b' \in \mathbb{Z}$ non nuls, alors $(ba')x + (-b'a)x' = 0$, ce qui implique que S n'est pas libre. Finalement, c'est clair que toute partie $S \neq \{0\}$ de $\mathbb{Q}$ de cardinal 1 est libre, ce qui implique le résultat.

(c) L'item précédent nous dit que $\mathbb{Q}$ n'est pas un $\mathbb{Z}$-module libre, puisque le sous-module M engendré par un seul élément non nul a/b de $\mathbb{Q}$ (avec $a, b \in \mathbb{Z}$ non nuls) ne coïncide pas avec $\mathbb{Q}$ (par exemple, $1/(b^2+1) \in \mathbb{Q} \setminus M$).

(d) $\mathbb{Q}$ n'est pas un $\mathbb{Z}$-module de type fini. En effet, on suppose qu'il existe un ensemble fini $S = \{x_1, \ldots, x_n\} \subseteq \mathbb{Q}$ de générateurs non nuls de $\mathbb{Q}$. On écrit $x_i = a_i/b_i$, avec $a_i \in \mathbb{Z}$ non nul et $b_i \in \mathbb{N}^*$ premiers entre eux. Alors, $1/(1 + \prod_{i=1}^n b_i) \in \mathbb{Q} \setminus \langle S \rangle$, ce qui donne une contradiction.

2. Soit $M = \{(x, y, z) \in \mathbb{Z}^3 : x + y + z = 0 \pmod 2\}$.

(a) Montrer que M est un sous-$\mathbb{Z}$-module libre de type fini de $\mathbb{Z}^3$ et en donner une base.

(b) Décrire le quotient $\mathbb{Z}^3/M$.

Solution.

(a) On affirme que $\mathscr{B} = \{(1,-1,0), (0,1,-1), (0,0,2)\} \subseteq M$ est une base de M. C'est clair que $\mathscr{B}$ est libre, puisque $\alpha(1,-1,0)+\beta(0,1,-1)+\gamma(0,0,2) = (0,0,0)$, avec $\alpha, \beta, \gamma \in \mathbb{Z}$, équivaut à $\alpha = 0$, $\beta - \alpha = 0$ et $2\gamma - \beta = 0$, ce qui implique $\alpha = \beta = \gamma = 0$. En outre, si $(x, y, z) \in M$, *i.e.* $x + y + z \in 2\mathbb{Z}$, alors

$$(x, y, z) = x(1,-1,0) + (x+y)(0,1,-1) + \frac{x+y+z}{2}(0,0,2),$$

ce qui dit que $\mathscr{B}$ est une famille génératrice de M. Par conséquent, $\mathscr{B}$ est une base de M.

(b) On affirme que $\mathbb{Z}^3/M \simeq \mathbb{Z}/2\mathbb{Z}$. En effet, soit $\phi : \mathbb{Z}^3 \to \mathbb{Z}/2\mathbb{Z}$ le morphisme $\mathbb{Z}$-linéaire donné par $(x, y, z) \mapsto [x + y + z]$, où les crochets indiquent la classe de $x + y + z \in \mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$. Alors, ϕ est surjectif et M est le noyau de ϕ, ce qui prouve l'affirmation.

3. Soit $A = M_2(\mathbb{R})$ et E l'ensemble des matrices de A dont la première colonne est nulle.

(*a*) Montrer que E possède une structure de A-module à gauche.

(*b*) Montrer que E est un A-module à gauche de type fini mais qu'il n'est pas libre.

Solution.

(*a*) C'est clair que E est en fait un idéal à gauche de A et en particulier un sous-module à gauche de A.

(*b*) C'est clair que E est de type fini, puisque $\{E_{1,2}, E_{2,2}\}$ est une famille génératrice de E. Comme tout A-module à gauche libre de type fini M est une somme directe finie de copies de A, il a dimension (sur $\mathbb{R}$) donnée par un multiple entier de $\dim_{\mathbb{R}} A = 4$. Le module E a dimension 2 (sur $\mathbb{R}$), ce qui nous dit qu'il n'est pas libre.

4. Soient A un anneau commutatif et M un A-module. Montrer que chacune des affirmations suivantes est fausse en exhibant un contre-exemple.

(*a*) Une famille génératrice minimale de M est une base de M.

(*b*) Les familles génératrices minimales de M ont toutes la même cardinalité.

(*c*) Si M est libre alors une famille génératrice minimale de M est une base de M.

(*d*) Si M est libre alors une famille libre maximale de M est une base de M.

(*e*) Si M est libre alors tout sous-module de M est libre.

Solution.

(*a*) Prendre $A = M = \mathbb{Z}$ et la famille génératrice minimale $S = \{2, 3\}$.

(*b*) Prendre $A = M = \mathbb{Z}$ et les familles génératrices minimales $S = \{2, 3\}$ et $S' = \{1\}$.

(*c*) Considérer l'exemple dans le premier item.

(*d*) Prendre $A = M = \mathbb{Z}$ et la famille libre maximale $S = \{2\}$.

(*e*) Prendre $A = M = \mathbb{Z}/4\mathbb{Z}$ et le sous-module $2\mathbb{Z}/4\mathbb{Z}$.

5. Soit A un anneau, M un A-module et v un élément de M qui n'est pas un élément de torsion.

(*a*) Montrer que le sous-module $A.v$ possède un supplémentaire dans M si et seulement s'il existe une forme linéaire $f : M \to A$ qui envoie v sur 1.

(*b*) Montrer que si le sous-module $A.v$ possède un supplémentaire N dans M, alors

(i) Le module quotient M/N est isomorphe à A.

(ii) Le module quotient $M/A.v$ est isomorphe à N.

(*c*) Montrer qu'il existe des situations où le sous-module $A.v$ ne possède pas de supplémentaire dans M.

(*d*) Dans le cas où $A = \mathbb{Z}$ et $M = \mathbb{Z}^n$, quels sont les n-uplets v pour lesquels le sous-module $A.v$ possède un supplémentaire dans $\mathbb{Z}^n$?

(*e*) Peut-on compléter le triplet $(2, 10, 4)$ en une base de $\mathbb{Z}^3$? Le triplet $(5, 3, 6)$? Si oui, donner une telle base.

Solution.

(*a*) On suppose d'abord qu'il existe un morphisme A-linéaire $f : M \to A$ qui envoie v sur 1. Soit $N = \mathsf{Ker}(f) \subseteq M$. Alors, $N \cap A.v = \{0\}$, et $N + A.v = M$, puisque, étant donné $m \in M$, $m = (m - f(m).v) + f(m).v$ et $m - f(m).v \in N$, vu que $f(m - f(m).v) = f(m) - f(m).f(v) = f(m) - f(m) = 0$. Réciproquement, si le sous-module $A.v$ possède un supplémentaire N dans M, on peut écrire $M = N \oplus A.v$, et l'application $f : M \to A$ donnée par $m = n + a.v \mapsto a$ est un morphisme A-linéaire qui envoie v sur 1.

(*b*) (i) On considère le morphisme A-linéaire $f : M \to A$ donnée par $m = n + a.v \mapsto a$. Il est surjectif et son noyau est N. Cela implique que f induit un isomorphisme A-linéaire $\bar{f} : M/N \to A$.

(ii) On considère le morphisme A-linéaire $g : M \to N$ donnée par $m = n + a.v \mapsto n$. Il est surjectif et son noyau est $A.v$. Cela implique que g induit un isomorphisme A-linéaire $\bar{g} : M/A.v \to N$.

(*c*) Prendre $A = M = \mathbb{Z}/4\mathbb{Z}$ et le sous-module $2\mathbb{Z}/4\mathbb{Z}$.

(*d*) On affirme qu'un n-uplet $v = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ satisfait que le sous-module $\mathbb{Z}.v$ possède un supplémentaire dans $\mathbb{Z}^n$ si et seulement s'il existe une base $\mathscr{B} = \{v_1, \ldots, v_n\}$ de $\mathbb{Z}^n$ telle que $v_1 = v$. C'est clair que la condition es suffisante, puisque $N = \langle\{v_2, \ldots, v_n\}\rangle$ est un supplémentaire de $\mathbb{Z}.v$. La condition est aussi nécessaire. En effet, tout sous-module d'un $\mathbb{Z}$-module libre de type fini est libre et de type fini. Comme $\mathbb{Z}.v$ possède un supplémentaire N dans $\mathbb{Z}^n$, qui es un $\mathbb{Z}$-module libre. L'identité $\mathbb{Z}.v \oplus N \simeq \mathbb{Z}^n$ envoie la base de $\mathbb{Z}.v \oplus N$ formée par le vecteur v et une base de N dans une base de $\mathbb{Z}^n$, ce qui prouve le résultat.

(*e*) On ne peut pas compléter le triplet $v = (2, 10, 4)$ en une base de $\mathbb{Z}^3$, puisque l'image de tout morphisme $\mathbb{Z}$-linéaire $f : \mathbb{Z}^3 \to \mathbb{Z}$ est un nombre entier pair, vu que $f(2, 10, 4) = 2f(1, 5, 2)$. Par ailleurs, le triplet $(5, 3, 6)$ est partie de la base $\{(5, 3, 6), (1, 0, 1), (0, 1, 0)\}$ de $\mathbb{Z}^3$.

6. Soit A un anneau commutatif non nul. On rappelle que d'après le lemme de Krull, A possède (au moins) un idéal maximal I. Si M est un A-module, on désigne par IM le sous-module de M engendré par l'ensemble $\{b.m : b \in I, m \in M\}$.

(*a*) Soient $a \in A$ et $m \in M$. Montrer que la classe de $a.m$ dans le quotient M/IM ne dépend que de la classe de a dans A/I et de la classe de m dans M/IM. En déduire que M/IM possède une structure de A/I-espace vectoriel.

(*b*) On suppose que M est un A-module libre ; soit $(e_1, \ldots, e_n)$ une base de M. Montrer que pour tout $(a_1, \ldots, a_n) \in A^n$,

$$\sum_{i=1}^{n} a_i e_i \in IM \text{ ssi } \forall i \in \{1, \ldots, n\}, a_i \in I.$$

(*c*) En déduire que l'image d'une base de M par la projection canonique M/IM est une base de M/IM en tant que A/I-espace vectoriel.

(*d*) Soient n et p deux entiers. Montrer que A^n est isomorphe à A^p si et seulement si $n = p$.

Solution.

(*a*) Soient $a, a' \in A$ tels que $a - a' \in I$ et $m, m' \in M$ tels que $m - m' \in IM$. Alors, $am - a'm' = am - a'm + a'm - a'm' = (a - a')m + a'(m - m') \in IM$.

(*b*) C'est clair que, si $a_i \in I$ pour tout $i \in \{1, \dots, n\}$, alors $\sum_{i=1}^n a_i e_i \in IM$. Réciproquement, si $\sum_{i=1}^n a_i e_i \in IM$, alors il existe $m_1, \dots, m_\ell \in M$ et $b_1, \dots, b_\ell \in I$ tels que $\sum_{i=1}^n a_i e_i = \sum_{j=1}^\ell b_j m_j$. Comme $(e_1, \dots, e_n)$ est une base de M, on peut écrire $m_j = \sum_{i=1}^n c_{i,j} e_i$, pour tout $j = 1, \dots, \ell$. En conséquence, $\sum_{i=1}^n a_i e_i = \sum_{i=1}^n (\sum_{j=1}^\ell b_j c_{i,j}) e_i$, ce qui implique que $a_i = \sum_{j=1}^\ell b_j c_{i,j} \in I$, pour tout $i = 1, \dots, n$.

(*c*) C'est clair que l'image $(\bar{e}_1, \dots, \bar{e}_n)$ d'une base $(e_1, \dots, e_n)$ de M par la projection canonique M/IM est une famille génératrice. En outre, si $\sum_{i=1}^n \bar{a}_i \bar{e}_i = 0$, avec $\bar{a}_i \in A/I$ les classes des éléments $a_i \in A$, pour tout $i = 1, \dots, n$, alors $\sum_{i=1}^n a_i e_i \in IM$. L'item précédent nous dit que $a_i \in I$ pour tout $i \in \{1, \dots, n\}$, *i.e.* $\bar{a}_i = 0$ pour tout $i \in \{1, \dots, n\}$, ce qui nous dit que $(\bar{e}_1, \dots, \bar{e}_n)$ est libre.

(*d*) Si $n = p$, le A-module A^n est trivialement isomorphe à A^p. Réciproquement, si les A-modules A^n et A^p sont isomorphes, l'item précédent nous dit que les A/I-espaces vectoriels $(A/I)^n$ et $(A/I)^p$ sont isomorphes, ce qui implique $n = p$.

7. On considère les matrices

$$M_1 = \begin{pmatrix} 9 & 6 & -6 \\ 15 & 9 & 9 \\ 6 & 36 & 30 \end{pmatrix} \text{ et } M_2 = \begin{pmatrix} 3 & 2 & 5 \\ 4 & 6 & 8 \\ 7 & 2 & 3 \\ 4 & 2 & 6 \end{pmatrix}.$$

(*a*) Calculer les matrices réduites équivalentes.

(*b*) Soit N_1 (resp., N_2) le sous-module de $\mathbb{Z}^3$ (resp., $\mathbb{Z}^4$) engendré par les vecteurs colonnes de M_1 (resp. M_2). Trouver une base de $\mathbb{Z}^3$ (resp., $\mathbb{Z}^4$) adaptée à N_1 (resp., N_2).

(*c*) Donner un groupe isomorphe à $\mathbb{Z}^3/N_1$ puis $\mathbb{Z}^4/N_2$.

Solution.

(*a*) On rappelle que la matrice réduite équivalente d'une matrice $M \in M_{n\times m}(\mathbb{Z})$ est une matrice diagonale $D \in M_{n\times m}(\mathbb{Z})$ (*i.e.* $D_{i,j} = 0$ si $i \neq j$) telle que $D_{i,i} | D_{i+1,i+1} \neq 0$, pour tout $i = 1, \dots, r-1$ et $D_{i,i} = 0$ pour tout $i = r+1, \dots, \mathsf{min}(n, m)$, où $r = \mathsf{ran}(M)$. Elle est obtenue à partir d'une suite finie d'opérations de deux types : permutation de colonnes ou des lignes, et remplacer une colonne ou ligne C_{i_0} par $\pm C_{i_0} + \sum_{j \neq i_0} a_j C_j$, avec $a_j \in \mathbb{Z}$. Cela équivaut à écrire la *décomposition normale de Smith*

$$PMQ = D, \tag{1}$$

où $P \in M_n(\mathbb{Z})$ et $Q \in M_r(\mathbb{Z})$ sont matrices carrées unimodulaires (*i.e.* avec déterminant 1). À partir de cette décomposition, on peut écrire

$$MQ = P^{-1}D, \tag{2}$$

et les colonnes de P^{-1} nous donnent une base de $\mathbb{Z}^n$ adaptée au sous-module N engendré par les colonnes de M. Les premières r colonnes de $P^{-1}D$ nous donnent une base du sous-module N et le quotient $\mathbb{Z}^n/N$ est isomorphe à $\oplus_{i=1}^r \mathbb{Z}/D_{i,i}\mathbb{Z} \oplus \mathbb{Z}^{(n-r)}$.

Pour faire ces calculs on écrira, si $M \in M_{n\times m}(\mathbb{Z})$ est une matrice de n lignes et m colonnes :

(OP.1) $\sum_{j=1}^{n} a_j L_j \to L_{i_0}$ (resp., $\sum_{j=1}^{m} a_j C_j \to C_{i_0}$), avec $a_j \in \mathbb{Z}$ et $a_{i_0} \in \{\pm 1\}$, l'opération qui remplace la i_0-ème ligne (resp., colonne) par la ligne (resp., colonne) donnée par la somme des des j-ièmes lignes (resp., colonnes) multipliés par m_j ;

(OP.2) $L_{i_0} \leftrightarrow L_{j_0}$ (resp., $C_{i_0} \leftrightarrow C_{j_0}$) la permutation des i_0-ième et j_0-ième lignes (resp., colonnes).

Étant donnés n et $i, j \in [\![1, n]\!]$, on dénotera $E_{i,j} \in M_n(\mathbb{Z})$ la matrice carrée de n lignes et n colonnes telle que $(E_{i,j})_{h,k} = \delta_{i,h}\delta_{j,k}$, pour $h, k \in [\![1, n]\!]$, où $\delta_{a,b} = 0$ si $a \neq b$ $\delta_{a,b} = 1$ si $a = b$ est le symbole de Kronecker. On écrit aussi $\mathsf{I}_n \in M_n(\mathbb{Z})$ la matrice identité respective.

On rappelle que l'opération (OP.1) pour les lignes (resp., colonnes) sur une matrice $M \in M_{n\times m}(\mathbb{Z})$ équivaut à passer de M à $L.M$ (resp., $M.C$), où

$$L = \mathsf{I}_n + \sum_{j=1}^{n} a'_j E_{i_0,j} \in M_n(\mathbb{Z}) \left(\text{resp., } C = \mathsf{I}_m + \sum_{j=1}^{m} a'_j E_{j,i_0} \in M_m(\mathbb{Z}) \right), \tag{3}$$

et $a'_j = a_j$ si $j \neq i_0$ et $a'_{i_0} = a_{i_0} - 1$. Noter que le déterminant de L (resp., C) est a_{i_0}. En outre, l'opération (OP.2) pour les lignes (resp., colonnes) sur une matrice $M \in M_{n\times m}(\mathbb{Z})$ équivaut à passer de M à $L'.M$ (resp., $M.C'$), où

$$\begin{aligned} &L' = \mathsf{I}_n - E_{i_0,i_0} - E_{j_0,j_0} + E_{i_0,j_0} + E_{j_0,i_0} \in M_n(\mathbb{Z}) \\ &\left(\text{resp., } C' = \mathsf{I}_m - E_{i_0,i_0} - E_{j_0,j_0} + E_{i_0,j_0} + E_{j_0,i_0} \in M_m(\mathbb{Z}) \right). \end{aligned} \tag{4}$$

Noter que le déterminant de L' (resp., C') est -1. Comme on va devoir inverser la matrice P dans (1) et la matrice P est le produit de toutes les matrices (3) et (4) associées aux opérations (OP.1) et (OP.2) sur les lignes, respectivement, on va normalement commencer avec des opérations sur les colonnes, de sorte qu'il reste le minimum nécessaire d'opérations sur les lignes pour finalement réduire la matrice M donnée.

On va faire le calcul pour la matrice M_1. Dans ce cas on considère

$$\begin{pmatrix} 9 & 6 & -6 \\ 15 & 9 & 9 \\ 6 & 36 & 30 \end{pmatrix} \overset{C_1+C_3\to C_1}{\longrightarrow} \begin{pmatrix} 3 & 6 & -6 \\ 24 & 9 & 9 \\ 36 & 36 & 30 \end{pmatrix} \overset{\substack{C_2-2C_1\to C_2 \\ C_3+2C_1\to C_3}}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 24 & -39 & 57 \\ 36 & -36 & 102 \end{pmatrix}$$
$$\overset{C_2+C_3\to C_3}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 24 & -39 & 18 \\ 36 & -36 & 66 \end{pmatrix} \overset{C_2+2C_3\to C_2}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 24 & -3 & 18 \\ 36 & 96 & 66 \end{pmatrix} \overset{\substack{C_1+8C_2\to C_1 \\ C_3+6C_2\to C_3}}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 0 & -3 & 0 \\ 804 & 96 & 642 \end{pmatrix}$$
$$\overset{C_1-C_3\to C_1}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 0 & -3 & 0 \\ 162 & 96 & 642 \end{pmatrix} \overset{L_3-54L_1+32L_2\to L_3}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 642 \end{pmatrix}. \tag{5}$$

En appliquant (3) pour la dernière opération (sur les lignes) dans (5) on trouve que la matrice P dans (1) pour M_1 est

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -54 & 32 & 1 \end{pmatrix},$$

ce qui implique que

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 54 & -32 & 1 \end{pmatrix}.$$

Si l'on fait en plus le produit des matrices (3) associées aux opérations sur les colonnes dans (5), on trouve dans ce cas que (2) pour M_1 est donné par

$$\begin{pmatrix} 9 & 6 & -6 \\ 15 & 9 & 9 \\ 6 & 36 & 30 \end{pmatrix}\begin{pmatrix} -3 & -2 & -12 \\ 5 & 3 & 19 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 54 & -32 & 1 \end{pmatrix}\begin{pmatrix} 3 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 642 \end{pmatrix}.$$

On va faire maintenant le calcul pour la matrice M_2. Dans ce cas on considère

$$\begin{pmatrix} 3 & 2 & 5 \\ 4 & 6 & 8 \\ 7 & 2 & 3 \\ 4 & 2 & 6 \end{pmatrix} \xrightarrow{C_1-C_2\to C_1} \begin{pmatrix} 1 & 2 & 5 \\ -2 & 6 & 8 \\ 5 & 2 & 3 \\ 2 & 2 & 6 \end{pmatrix} \xrightarrow[C_3-5C_1\to C_3]{C_2-2C_1\to C_2} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 10 & 18 \\ 5 & -8 & -22 \\ 2 & -2 & -4 \end{pmatrix}$$

$$\xrightarrow{C_3-C_2\to C_3} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 10 & 8 \\ 5 & -8 & -14 \\ 2 & -2 & -2 \end{pmatrix} \xrightarrow{C_2-C_3\to C_2} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 2 & 8 \\ 5 & 6 & -14 \\ 2 & 0 & -2 \end{pmatrix} \xrightarrow[C_3-4C_2\to C_3]{C_1+C_2\to C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 11 & 6 & -38 \\ 2 & 0 & -2 \end{pmatrix}$$

$$\xrightarrow{C_1+C_3\to C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ -27 & 6 & -38 \\ 0 & 0 & -2 \end{pmatrix} \xrightarrow{L_3\leftrightarrow L_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \\ -27 & 6 & -38 \end{pmatrix} \xrightarrow{-L_3\to L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \\ -27 & 6 & -38 \end{pmatrix}$$

$$\xrightarrow{L_4+27L_1-3L_2+19L_3\to L_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}. \tag{6}$$

En appliquant (3) et (4) pour les trois dernières opérations (sur les lignes) de (6) on trouve que la matrice P dans (1) pour M_2 est

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 27 & -3 & 1 & -19 \end{pmatrix},$$

ce qui implique que

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -27 & 3 & -19 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Si l'on fait en plus le produit des matrices (3) associées aux opérations sur les colonnes dans (6), on trouve dans ce cas que (2) pour M_2 est donné par

$$\begin{pmatrix} 3 & 2 & 5 \\ 4 & 6 & 8 \\ 7 & 2 & 3 \\ 4 & 2 & 6 \end{pmatrix}\begin{pmatrix} -5 & 1 & -7 \\ -2 & 1 & -2 \\ 4 & -1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -27 & 3 & -19 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

(*b*) Les matrices précédentes nous disent que la base de $\mathbb{Z}^3$ adaptée à N_1 est $\{(1,0,54),(0,1,-32),(0,0,1)\}$ avec facteurs 3, -3 et 642, tandis que celle de $\mathbb{Z}^4$ adaptée à N_2 est $\{(1,0,-27,0),(0,1,3,0),(0,0,-19,-1),(0,0,1,0)\}$ avec facteurs 1, 2, 2 et 0.

(*c*) C'est clair que $\mathbb{Z}^3/N_1 \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/642\mathbb{Z}$ et $\mathbb{Z}^4/N_2 \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

8. Calculer la matrice réduite équivalente à la matrice

$$M = \begin{pmatrix} 12 & 18 & 0 \\ 0 & 4 & -2 \\ 8 & 16 & 5 \end{pmatrix}.$$

Solution. La méthode décrite dans l'exercice précédent nous permet de trouver la matrice réduite. Plus précisément,

$$\begin{pmatrix} 12 & 18 & 0 \\ 0 & 4 & -2 \\ 8 & 16 & 5 \end{pmatrix} \overset{C_2-3C_3\to C_2}{\longrightarrow} \begin{pmatrix} 12 & 18 & 0 \\ 0 & 10 & -2 \\ 8 & 1 & 5 \end{pmatrix} \overset{\substack{C_1-8C_2\to C_1 \\ C_3-5C_2\to C_3}}{\longrightarrow} \begin{pmatrix} -132 & 18 & -90 \\ -80 & 10 & -52 \\ 0 & 1 & 0 \end{pmatrix}$$
$$\overset{C_1-C_3\to C_1}{\longrightarrow} \begin{pmatrix} -42 & 18 & -90 \\ -28 & 10 & -52 \\ 0 & 1 & 0 \end{pmatrix} \overset{C_3-2C_1\to C_3}{\longrightarrow} \begin{pmatrix} -42 & 18 & -6 \\ -28 & 10 & 4 \\ 0 & 1 & 0 \end{pmatrix} \overset{\substack{C_1-7C_3\to C_1 \\ C_2+3C_3\to C_2}}{\longrightarrow} \begin{pmatrix} 0 & 0 & -6 \\ -56 & 22 & 4 \\ 0 & 1 & 0 \end{pmatrix}$$
$$\overset{L_1+L_2\to L_2}{\longrightarrow} \begin{pmatrix} 0 & 0 & -6 \\ -56 & 22 & -2 \\ 0 & 1 & 0 \end{pmatrix} \overset{\substack{C_1-28C_3\to C_1 \\ C_2+11C_3\to C_2}}{\longrightarrow} \begin{pmatrix} 168 & -66 & -6 \\ 0 & 0 & -2 \\ 0 & 1 & 0 \end{pmatrix} \overset{\substack{L_1-3L_2 \\ +66L_3\to L_1}}{\longrightarrow} \begin{pmatrix} 168 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 0 \end{pmatrix}$$
$$\overset{-L_2\to L_2}{\longrightarrow} \begin{pmatrix} 168 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix} \overset{L_1\leftrightarrow L_3}{\longrightarrow} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 168 & 0 & 0 \end{pmatrix} \overset{C_1\leftrightarrow C_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 168 & 0 \end{pmatrix} \overset{C_2\leftrightarrow C_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 168 \end{pmatrix}. \tag{7}$$

En appliquant (3) et (4) pour les opérations sur les lignes de (7) on trouve que la matrice P dans (1) pour M est

$$P = \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & 0 \\ -2 & -3 & 66 \end{pmatrix},$$

ce qui implique que

$$P^{-1} = \begin{pmatrix} -66 & -3 & 1 \\ 66 & 2 & -1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Si l'on fait en plus le produit des matrices (3) associées aux opérations sur les colonnes dans (7), on trouve dans ce cas que (2) pour M est donné par

$$\begin{pmatrix} 12 & 18 & 0 \\ 0 & 4 & -2 \\ 8 & 16 & 5 \end{pmatrix} \begin{pmatrix} -28 & -2 & 71 \\ 15 & 1 & -38 \\ -3 & 0 & 8 \end{pmatrix} = \begin{pmatrix} -66 & -3 & 1 \\ 66 & 2 & -1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 168 \end{pmatrix}.$$

Les colonnes de la première matrice dans le membre de droite nous donnent donc une base de $\mathbb{Z}^3$ adaptée au sous-module engendré par les colonnes de la première matrice du membre de gauche, avec facteurs donnés par les coefficients dans la diagonale de la dernière matrice.

9. Soit A un anneau euclidien. Montrer qu'un A-module de type fini est sans torsion si et seulement s'il est libre.

Solution. C'est clair que tout module libre est sans torsion. D'ailleurs, si A est euclidien, alors il est principal. L'exercice suit du résultat du cours qui dit précisément qu'un module de type fini sur un anneau principal est sans torsion si et seulement s'il est libre.

10. Soit L' un sous-$\mathbb{Z}$-module de $\mathbb{Z}^n$ de rang égal à n. On note B la base canonique de $\mathbb{Z}^n$ et $B' = (e'_1, \dots, e'_n)$ une base L'.

(*a*) Montrer que L/L' est de cardinal fini, égal à $|\det_B(B')|$.

(*b*) Soit $P = \{\sum_{i=1}^n x_i e'_i : x_i \in [0,1[\text{ pour tout } 1 \le i \le n\} \subseteq \mathbb{R}^n$. Quel est le nombre des éléments de $\mathbb{Z}^n$ qui appartiennent à P ?

Solution.

(*a*) Soit $M \in M_n(\mathbb{Z})$ la matrice dont la i-ème colonne est le vecteur e'_i, pour $i \in \{1, \dots, n\}$. Or, on sait qu'il existe $P, Q \in M_n(\mathbb{Z})$ matrices unimodulaires et D matrice diagonale satisfaisant $D_{i,i} | D_{i+1,i+1} \neq 0$ pour tout $i \in \{1, \dots, n-1\}$, telles que $PMQ = D$. En outre, $\mathbb{Z}^n/L \simeq \oplus_{i=1}^n \mathbb{Z}/D_{i,i}\mathbb{Z}$. Cela implique que $\mathbb{Z}^n/L \simeq \oplus_{i=1}^n \mathbb{Z}/D_{i,i}\mathbb{Z}$ est fini. En outre, son cardinal est

$$\left| \prod_{i=1}^n D_{i,i} \right| = |\det(D)| = |\det(PMQ)| = \det(P)|\det(M)|\det(Q) = |\det(M)| = |\det_B(B')|.$$

(*b*) L'inclusion de P dans $\mathbb{R}^n$ induit une bijection entre P et $\mathbb{R}^n/L$. En plus, cette identification nous donne une correspondance entre $P \cap \mathbb{Z}^n$ et $\mathbb{Z}^n/L$. En conséquence, le cardinal de $P \cap \mathbb{Z}^n$ est $|\det_B(B')|$, d'après l'item précédent.

11. Pour chacun des sous-modules M de $\mathbb{Z}^n$ suivants, donner une base adaptée de $\mathbb{Z}^n$ et déterminer la structure du quotient :

(*a*) $M = \{(x,y) \in \mathbb{Z}^2 : 3y = 2x \text{ et } y \in 4\mathbb{Z}\}$,

(*b*) $M = \mathbb{Z}.(1,1) \oplus \mathbb{Z}.(1,3)$,

(*c*) $M = \mathbb{Z}.(1,4) \oplus \mathbb{Z}.(2,2)$,

(*d*) $M = \{(x,y,z) \in \mathbb{Z}^3 : x + y + z = 0 \pmod 2\}$ (voir l'exercice **2**).

Solution. Pour tous les items on va présenter d'abord une matrice $A \in M_{n\times r}(\mathbb{Z})$ dont les colonnes donnent une base de M, où $r \le n$ est le rang de M, pour calculer après la décomposition normale de Smith $AQ = P^{-1}D$, où $P \in M_n(\mathbb{Z})$ et $Q \in M_r(\mathbb{Z})$ sont matrices unimodulaires et $D \in M_{n\times r}(\mathbb{Z})$ est la matrice diagonale satisfaisant $D_{i,i} | D_{i+1,i+1} \neq 0$ pour tout $i \in \{1, \dots, r-1\}$. La base de $\mathbb{Z}^n$ adaptée à M est donnée par les colonnes de P^{-1} et le quotient $\mathbb{Z}^n/M$ est isomorphe à $\oplus_{i=1}^r \mathbb{Z}/D_{i,i}\mathbb{Z} \oplus \mathbb{Z}^{(n-r)}$.

(*a*) Si l'on écrit $y = 4y'$, avec $y' \in \mathbb{Z}$, alors $3y = 2x$ équivaut à $x = 6y'$. En conséquence, $M = \mathbb{Z}.(6,4)$ et la matrice initiale est

$$A = \begin{pmatrix} 6 \\ 4 \end{pmatrix}.$$

Si l'on considère les opérations $L_1 - L_2 \to L_1$ et puis $L_2 - 2L_1 \to L_2$, on trouve que la décomposition normale de Smith correspondante est

$$\underbrace{\begin{pmatrix} 6 \\ 4 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} 1 \end{pmatrix}}_{Q} = \underbrace{\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}}_{P^{-1}} \underbrace{\begin{pmatrix} 2 \\ 0 \end{pmatrix}}_{D}.$$

(*b*) On prend

$$A=\begin{pmatrix}1 & 1\\ 1 & 3\end{pmatrix}.$$

Si l'on considère les opérations $C_2-C_1\to C_2$ et puis $L_2-L_1\to L_2$, on trouve que la décomposition normale de Smith correspondante est

$$\underbrace{\begin{pmatrix}1 & 1\\ 1 & 3\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}}_{Q}=\underbrace{\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}}_{P^{-1}}\underbrace{\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}}_{D}.$$

(*c*) On prend

$$A=\begin{pmatrix}1 & 2\\ 4 & 2\end{pmatrix}.$$

Si l'on considère les opérations $C_2-2C_1\to C_2$ et puis $L_2-4L_1\to L_2$, on trouve que la décomposition normale de Smith correspondante est

$$\underbrace{\begin{pmatrix}1 & 2\\ 4 & 2\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}1 & -2\\ 0 & 1\end{pmatrix}}_{Q}=\underbrace{\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}}_{P^{-1}}\underbrace{\begin{pmatrix}1 & 0\\ 0 & -6\end{pmatrix}}_{D}.$$

(*d*) On a montré dans l'exercice **2** que

$$\{(1,-1,0),(0,1,-1),(0,0,2)\}$$

est une base de M. On pose alors

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

Si l'on considère les opérations $L_2+L_1\to L_2$ et puis $L_2+L_3\to L_3$, on trouve que la décomposition normale de Smith correspondante est

$$\underbrace{\begin{pmatrix}1 & 0 & 0\\ -1 & 1 & 0\\ 0 & -1 & 2\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}}_{Q}=\underbrace{\begin{pmatrix}1 & 0 & 0\\ -1 & 1 & 0\\ 0 & -1 & 1\end{pmatrix}}_{P^{-1}}\underbrace{\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 2\end{pmatrix}}_{D}.$$

12. (*a*) Quels sont à isomorphismes près les groupes abéliens qui contiennent exactement 12 éléments ? Donner pour chaque groupe ses facteurs invariants.

(*b*) Même question avec 360 éléments.

Solution. On sait que, étant donné $n\in\mathbb{N}^*$, les groupes abéliens à n éléments (à isomorphisme près) sont en bijection avec les uplets $(d_1,\dots,d_\ell)\in\mathbb{N}^\ell$ avec $\ell\in\mathbb{N}^*$, $1<d_i|d_{i+1}$ pour tout $i=1,\dots,\ell-1$ et $\prod_{i=1}^{\ell}d_i=n$. Cette bijection associe le groupe $\oplus_{i=1}^{\ell}\mathbb{Z}/d_i\mathbb{Z}$ à chaque tel uplet $(d_1,\dots,d_\ell)$.

(*a*) C'est facile à vérifier qu'il y a précisément 2 groupes abéliens à 12 éléments (à iso-

morphisme près) : $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Les facteurs invariants respectifs sont 12, $(2, 6)$.

(*b*) C'est facile à vérifier qu'il y a précisément 6 groupes abéliens à 360 éléments (à isomorphisme près) : $\mathbb{Z}/360\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/180\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/90\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/120\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/60\mathbb{Z}$. Les facteurs invariants respectifs sont 360, $(2, 180)$, $(2, 2, 90)$, $(2, 6, 30)$, $(3, 120)$ et $(6, 60)$.