Université de Bordeaux **2024-2025**
Semestre 7 **Modules, Algèbre commutative**

Corrigé de l'examen

Exercice 1

(1) Quels sont les facteurs invariants du groupe fini $(\mathbf{Z}/16\,\mathbf{Z}) \times (\mathbf{Z}/12\,\mathbf{Z}) \times (\mathbf{Z}/2024\,\mathbf{Z})$?
(2) Trouver une base adaptée pour le groupe abélien $L = \mathbf{Z}\,v_1 + \mathbf{Z}\,v_2 + \mathbf{Z}\,v_3 \subset \mathbf{Z}^3$ avec $v_1 = (-2, 1, 1)$, $v_2 = (1, -2, 1)$ et $v_3 = (1, 1, -2)$.
(3) Donner la structure du groupe abélien de type fini $G = \mathbf{Z}^3/(\mathbf{Z}(4, 8, 10) + \mathbf{Z}(6, 2, 0))$.
(4) Construire une matrice $M \in \mathsf{SL}_3(\mathbf{Z})$ dont la première ligne est $(6, 11, 5)$.
(5) Donner les invariants de similitude de la matrice :

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

(les composantes blanches correspondent à des zéros). Quel est son polynôme minimal ?

Solution : (1) Posons $G = (\mathbf{Z}/16\,\mathbf{Z}) \times (\mathbf{Z}/12\,\mathbf{Z}) \times (\mathbf{Z}/2024\,\mathbf{Z})$. On a $16 = 2^4$, $12 = 2^2 \times 3$ et $2024 = 2^3 \times 353$ donc

$$\begin{aligned} G &\simeq (\mathbf{Z}/16\,\mathbf{Z}) \times (\mathbf{Z}/4\,\mathbf{Z}) \times (\mathbf{Z}/3\,\mathbf{Z}) \times (\mathbf{Z}/8\,\mathbf{Z}) \times (\mathbf{Z}/253\,\mathbf{Z}) \\ &\simeq (\mathbf{Z}/4\,\mathbf{Z}) \times (\mathbf{Z}/8\,\mathbf{Z}) \times (\mathbf{Z}/16\,\mathbf{Z}) \times (\mathbf{Z}/3\,\mathbf{Z}) \times (\mathbf{Z}/253\,\mathbf{Z}) \\ &\simeq (\mathbf{Z}/4\,\mathbf{Z}) \times (\mathbf{Z}/8\,\mathbf{Z}) \times (\mathbf{Z}/12144\,\mathbf{Z}) \end{aligned}$$

en vertu du théorème des restes chinois : les facteurs invariants de G sont $(4, 8, 12144)$.
(2) On a $v_1 + v_2 + v_3 = (0, 0, 0)$ donc $L = \mathbf{Z}\,v_1 + \mathbf{Z}\,v_2$. Par ailleurs, on a $v_2 - v_1 = 3e_2$ avec $e_2 = (1, -1, 0)$. Posons alors $e_1 = v_1$ et $e_3 = (0, 0, 1)$. On a $\det(e_1, e_2, e_3) = 1$, de sorte que (e_1, e_2, e_3) est une base de $\mathbf{Z}^3$, et $L_1 = \mathbf{Z}\,e_1 \oplus 3\,\mathbf{Z}\,e_2$.
(3) Posons $v_1 = (6, 2, 0) = 2e_1$ avec $e_1 = (3, 1, 0)$ et $v_2 = (4, 8, 10)$. On a $v_1 + v_2 = 10e_2$ avec $e_2 = (1, 1, 1)$, donc $\Lambda = \mathbf{Z}\,v_1 + \mathbf{Z}\,v_2 = 2\,\mathbf{Z}\,e_1 + 10\,\mathbf{Z}\,e_2 \subset \mathbf{Z}^3$. Posons $e_3 = (1, 0, 0)$. La famille (e_1, e_2, e_3) est une base adaptée à Λ, et on a $G = \mathbf{Z}^3/\Lambda \simeq (\mathbf{Z}/2\,\mathbf{Z}) \oplus (\mathbf{Z}/10\,\mathbf{Z}) \oplus \mathbf{Z}$.
(4) On a bien $\mathsf{pgcd}(6, 11, 5) = 1$. On applique l'algorithme : posons $X = (6 \quad 11 \quad 5)$. On a $\left(\begin{smallmatrix} 11 & 5 \\ 2 & 1 \end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$, de sorte que $X = (6 \quad 1 \quad 0)M_1$ avec $M_1 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 11 & 5 \\ 0 & 2 & 1 \end{smallmatrix}\right) \in \mathsf{SL}_3(\mathbf{Z})$. On a $\left(\begin{smallmatrix} 6 & 1 \\ -5 & 1 \end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$, de sorte que $(6 \quad 1 \quad 0) = (1 \quad 0 \quad 0)M_2$ avec $M_2 = \left(\begin{smallmatrix} 6 & 1 & 0 \\ 5 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in \mathsf{SL}_3(\mathbf{Z})$. Cela implique $X = (1 \quad 0 \quad 0)M_2M_1$: la matrice $M = M_2M_1 = \left(\begin{smallmatrix} 6 & 11 & 5 \\ 5 & 11 & 5 \\ 0 & 2 & 1 \end{smallmatrix}\right) \in \mathsf{SL}_3(\mathbf{Z})$ convient.
(5) Le $K[X]$-module associé est isomorphe à

$$(K[X]/\langle X^3\rangle) \times (K[X]/\langle X^2\rangle) \times (K[X]/\langle (X-1)^4\rangle) \times (K[X]/\langle (X-1)^2\rangle) \times (K[X]/\langle X-2\rangle).$$

En réordonnant les facteurs et en utilisant le théorème des restes chinois, il est isomorphe à

$$((K[X]/\langle X^2(X-1)^2\rangle) \times (K[X]/\langle X^3(X-1)^4(X-2)\rangle)$$

ce qui montre que les facteurs invariants (*i.e.* les invariants de similitude de la matrice) sont

$$(X^2(X-1)^2, X^3(X-1)^4(X-2)$$

et que le polynôme minimal de la matrice est $X^3(X-1)^4(X-2)$.

Exercice 2

Soient A un anneau principal, M un A-module libre de rang fini, et $(e_1, \dots, e_r)$ des éléments de M qui sont linéairement indépendants, et tels que le quotient $M/\langle e_1, \dots, e_r\rangle$ soit sans torsion. Montrer qu'on peut compléter $(e_1, \dots, e_r)$ en une base de M sur A.

Solution : Notons N le sous-module de M engendré par $\{e_1, \dots, e_r\}$. Le A-module M/N est de type fini (comme quotient d'un module de type fini), et sans torsion par hypothèse : il est donc libre de rang fini puisque A est principal. Notons $\pi\colon M \to M/N$ la surjection canonique, et soient $e_{r+1}, \dots, e_n \in M$ tels que $(\pi(e_{r+1}), \dots, \pi(e_n))$ soit une base de M/N. Si $m \in M$, il existe $a_{r+1}, \dots, a_n \in A$ uniques tels que $\pi(m) = \sum_{k=r+1}^{n} a_k \pi(e_k)$. L'élément $m' = m - \sum_{k=r+1}^{n} a_k e_k$ appartient donc à $\mathsf{Ker}(\pi) = N$: il existe $a_1, \dots, a_r \in A$ uniques tels que $m' = \sum_{k=1}^{r} a_k e_k$. Cela montre qu'il existe $a_1, \dots, a_n \in A$ uniques tels que $= \sum_{k=1}^{n} a_k e_k$, *i.e.* que $(e_1, \dots, e_n)$ est une base de M.

Exercice 3

Posons $A = \mathbf{Z}[\sqrt{5}] \subset K = \mathbf{Q}(\sqrt{5})$. Si $x, y \in \mathbf{Q}$ et $z = x + y\sqrt{5} \in K$, posons $N(z) = x^2 - 5y^2$.
(1) Montrer que si $z_1, z_2 \in K$, on a $N(z_1 z_2) = N(z_1)N(z_2)$.
(2) Soit $z \in A$. Montrer que $z \in A^\times \Leftrightarrow N(z) \in \{\pm 1\}$.
(3) Montrer qu'il n'existe aucun élément $z \in A$ tel que $N(z) \in \{\pm 2\}$.
(4) En déduire que 2 et $1 + \sqrt{5}$ sont irréductibles dans A. Sont-ils premiers [indication : construire soigneusement un isomorphisme d'anneaux $\mathbf{Z}[X]/\langle X^2 - 5\rangle \xrightarrow{\sim} A$] ?
(5) L'anneau A est-il factoriel ?
(6) L'idéal $I = \langle 2, 1 + \sqrt{5}\rangle \subset A$ est-il principal ?

Solution : (1) Soit σ l'automorphisme du corps K caractérisé par $\sigma(\sqrt{5}) = -\sqrt{5}$: on a $N(z) = z\sigma(z)$, donc $N(z_1 z_2) = z_1 z_2 \sigma(z_1 z_2) = z_1 z_2 \sigma(z_1)\sigma(z_2) = N(z_1)N(z_2)$ pour tous $z_1, z_2 \in K$.
(2) Si $z = x + y\sqrt{5} \in K$ avec $x, y \in \mathbf{Q}$, on a $z \in A \Leftrightarrow x, y \in \mathbf{Z}$. Cela implique que $z \in A \Rightarrow N(z) \in \mathbf{Z}$. En particulier, si $z \in A^\times$, alors $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$ avec $N(z), N(z^{-1}) \in \mathbf{Z}$, ce qui implique que $N(z) \in \mathbf{Z}^\times = \{\pm 1\}$. Réciproquement, si $z \in A$ est tel que $N(z) \in \{\pm 1\}$, alors $z^{-1} = N(z)^{-1}\sigma(z) \in A$, ce qui montre que $z \in A^\times$.
(3) Soient $x, y \in \mathbf{Z}$ et $z = x + y\sqrt{5} \in A$. Supposons $x^2 - 5y^2 = N(z) = \pm 2$: modulo 5, cela implique que ± 2 est un carré dans $\mathbf{Z}/5\mathbf{Z}$, ce qui n'est pas (les carrés de $\mathbf{Z}/5\mathbf{Z}$ sont $\overline{0}$, $\overline{1}$ et $\overline{4}$).
(4) • Soient $z_1, z_2 \in A$ tels que $z_1 z_2 = 2$: on a $N(z_1)N(z_2) = N(2) = 4$. Comme on a $N(z_1) \notin \{\pm 2\}$ en vertu de la question précédente, on a $N(z_1) \in \{\pm 1\}$ ou $N(z_2) \in \{\pm 1\}$, soit encore $z_1 \in A^\times$ ou $z_2 \in A^\times$ (*cf* question (2)), ce qui montre que 2 est irréductible dans A. L'argument est exactement le même pour $1 + \sqrt{5}$ parce que $N(1 + \sqrt{5}) = -4$.

• On dispose du morphisme $f\colon \mathbf{Z}[X] \to \mathbf{Q}(\sqrt{5})$ d'évaluation en $\sqrt{5}$. Par définition, on a $A = \mathsf{Im}(f)$. On a $X^2 - 5 \in \mathsf{Ker}(f)$. Par ailleurs, comme $X^2 - 5$ est unitaire, on dispose de la division euclidienne par $X^2 - 5$ dans $\mathbf{Z}[X]$. Si $P \in \mathsf{Ker}(f)$, il existe $Q, R \in \mathbf{Z}[X]$ uniques tels que $P = (X^2 - 5)Q + R$ et $\deg(R) < 2$. Écrivons $R = aX + b$ avec $a, b \in \mathbf{Z}$: on a $a\sqrt{5} + b = 0$. Comme $\sqrt{5} \notin \mathbf{Q}$, cela implique que $a = b = 0$, *i.e.* $P \in \langle X^2 - 5\rangle$. Finalement, on a $\mathsf{Ker}(f) = \langle X^2 - 5\rangle$: le morphisme f se factorise à travers un isomorphisme $\widetilde{f}\colon \mathbf{Z}[X]/\langle X^2 - 5\rangle \xrightarrow{\sim} A$, qui envoie la classe $\overline{X}$ de X sur $\sqrt{5}$. Ce dernier induit un isomorphisme $\mathbf{Z}[X]/\langle 2, X^2 - 5\rangle \xrightarrow{\sim} A/\langle 2\rangle$. Comme $\mathbf{Z}[X]/\langle 2, X^2 - 5\rangle \simeq \mathbf{F}_2[X]/\langle (X+1)^2\rangle$ n'est pas intègre, 2 n'est pas premier dans A. De même, comme $\widetilde{f}(1 + \overline{X}) = 1 + \sqrt{5}$, l'isomorphisme $\widetilde{f}$ induit un isomorphisme $\mathbf{Z}[X]/\langle X + 1, X^2 - 5\rangle \xrightarrow{\sim} A/\langle 1 + \sqrt{5}\rangle$. Comme $\mathbf{Z}[X]/\langle X + 1, X^2 - 5\rangle \simeq \mathbf{Z}/4\,\mathbf{Z}$ n'est pas intègre, $1 + \sqrt{5}$ n'est pas premier dans A.
(5) L'anneau A contient des éléments qui sont irréductibles mais pas premiers : il n'est pas factoriel.
(6) Supposons I principal : il existe $\alpha \in A$ tel que $I = \langle\alpha\rangle$. Observons que $I \neq A$ (parce que $A/I \simeq \mathbf{Z}[X]/\langle 2, 1+X, X^2-5\rangle \simeq \mathbf{F}_2$, ou bien en observant que si $x, y \in \mathbf{Z}$, l'élement $x+y\sqrt{5}$ appartient à I si et seulement si x et y ont même parité). On a en particulier $\alpha \mid 2$ dans A, donc $N(\alpha) \mid N(2) = 4$. Comme $\alpha \notin A^\times$ (parce que $I \neq A$), on a $N(\alpha) \notin \{\pm 1\}$. Par ailleurs, on sait que $N(\alpha) \notin \{\pm 2\}$ (*cf* question (3)). On a donc nécessairement $N(\alpha) \in \{\pm 4\}$. En écrivant $2 = \alpha\beta$ avec $\beta \in A$, cela implique que $N(\beta) \in \{\pm 1\}$, de sorte que α et 2 sont associés dans A : on a $I = \langle 2\rangle$. Il en résulte que $2 \mid 1 + \sqrt{5}$ dans A, *i.e.* que $\frac{1+\sqrt{5}}{2} \in A$, ce qui n'est pas. On a donc une contradiction : l'idéal I n'est pas principal.

Exercice 4 (bonus)

Soit A un anneau principal.

(1) Soient $x, y \in A \setminus \{0\}$. Posons $d = \mathsf{pgcd}(x, y)$ et écrivons $x = dx'$ et $y = dy'$. Montrer que si $f \in \mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle)$, alors $f(1) \in \langle y'\rangle/\langle y\rangle$.

(2) En déduire que $\mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle) \simeq A/\langle d\rangle$.

Soit M, M_1 et M_2 des A-modules.

(3) Montrer que $\mathsf{Hom}_A(M, M_1 \times M_2) \simeq \mathsf{Hom}_A(M, M_1) \times \mathsf{Hom}_A(M, M_2)$.

(4) Montrer de même que $\mathsf{Hom}_A(M_1 \times M_2, M) \simeq \mathsf{Hom}_A(M_1, M) \times \mathsf{Hom}_A(M_2, M)$.

On suppose désormais M de type fini et de torsion. Notons $x_1 \mid \cdots \mid x_n$ ses facteurs invariants.

(5) En utilisant tout ce qui précède, montrer que $\mathsf{End}_A(M) \simeq \bigoplus_{i=1}^{n} (A/\langle x_i\rangle)^{2(n-i)+1}$.

Solution : (1) Écrivons $f(1) = \alpha \mod \langle y\rangle$, avec $\alpha \in A$. On a $xf(1) = f(x) = 0$ dans $A/\langle y\rangle$, *i.e.* $x\alpha \in \langle y\rangle$, soit $x'\alpha \in \langle y'\rangle$: comme $\mathsf{pgcd}(x', y') = 1$, on a donc $\alpha \in \langle y'\rangle$, et donc $f(1) \in \langle y'\rangle/\langle y\rangle$.
(2) D'après la question précédente, on dispose de l'application

$$\begin{aligned} \Phi\colon \mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle) &\to \langle y'\rangle/\langle y\rangle \\ f &\mapsto f(1) \end{aligned}$$

C'est une application A-linéaire. Si $\alpha \in y'A$, notons $f_\alpha\colon A \to A/\langle y\rangle$ l'application composée

$$A \xrightarrow{\alpha} A \to A/\langle y\rangle$$

(où la première application est la multiplication par α et la deuxième la surjection canonique). On a $f_\alpha(x) = x\alpha \mod yA$, donc $f_\alpha(x) = 0$ vu que $x\alpha = x'd\alpha \in \langle y\rangle$ puisque

$\alpha \in y'A \Rightarrow d\alpha \in \langle y\rangle$. L'application f_α se factorise donc via une application A-linéaire $\widetilde{f_\alpha} \in \mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle)$. L'application $\alpha \mapsto f_\alpha$ est A-linéaire, nulle sur $\langle y\rangle$: il en est de même de $\alpha \mapsto \widetilde{f_\alpha}$. Cette dernière se factorise donc en une application A-linéaire

$$\Psi\colon \langle y'\rangle/\langle y\rangle \mapsto \mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle)$$
$$\alpha + yA \mapsto \widetilde{f_\alpha}$$

On a $\Phi\circ\Psi = \mathsf{Id}_{y'A/\langle y\rangle}$, et $\Psi\circ\Phi = \mathsf{Id}_{\mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle)}$, ce qui implique que Φ est un isomorphisme. Comme $\langle y'\rangle/\langle y\rangle \simeq A/\langle d\rangle$, on a donc $\mathsf{Hom}_A(A/\langle x\rangle, A/\langle y\rangle) \simeq A/\langle d\rangle$.
(3) Évident.
(4) Soit $f \in \mathsf{Hom}_A(M_1\times M_2, M)$. Notons $\iota_1\colon M_1 \to M_1\times M_2$ (resp. $\iota_2\colon M_2 \to M_1\times M_2$) l'application définie par $\iota_1(x) = (x,0)$ (resp. $\iota_2(x) = (0,x)$). Les applications ι_1 et ι_2 sont A-linéaires : il en est de même de $f_1 = f\circ\iota_1\colon M_1 \to M$ et $f2 = f\circ\iota_2\colon M_2 \to M$. On dispose donc de l'application

$$\Xi\colon \mathsf{Hom}_A(M_1\times M_2, M) \to \mathsf{Hom}_A(M_1, M)\times \mathsf{Hom}_A(M_2, M)$$
$$f \mapsto (f_1, f_2)$$

Elle est A-linéaire. Pour tout $x = (x_1, x_2) \in M_1\times M_2$, on a $x = \iota_1(x_1) + \iota_2(x_2)$, donc $f(x) = f(\iota_1(x_1)) + f(\iota_2(x_2))$, ce qui montre que $f = f_1\circ\pi_1 + f_2\circ\pi_2$ où $\pi_1\colon M_1\times M_2 \to M_1$ (resp. $\pi_2\colon M_1\times M_2 \to M_2$) est la première (resp. deuxième) projection. Cela montre que Ξ est un isomorphisme (d'application réciproque donnée par $\Xi^{-1}(f_1, f_2) = f_1\circ\pi_1 + f_2\circ\pi_2$).
(5) On a $M = \bigoplus_{i=1}^{n} A/\langle x_i\rangle$. D'après les questions (3) et (4), on a donc

$$\mathsf{End}_A(M) = \mathsf{Hom}_A(M,M) = \bigoplus_{1\le i,j\le n} \mathsf{Hom}_A(A/\langle x_i\rangle, A/\langle x_j\rangle)$$

Comme $\mathsf{Hom}_A(A/\langle x_i\rangle, A/\langle x_j\rangle) \simeq A/\langle \mathsf{pgcd}(x_i, x_j)\rangle$ et $\mathsf{pgcd}(x_i, x_j) = x_{\min(i,j)}$, on en déduit que

$$\mathsf{End}_A(M) \simeq \bigoplus_{1\le i,j\le n} A/\langle x_{\min(i,j)}\rangle \simeq \Big(\bigoplus_{i=1}^{n} A/x_iA\Big)\oplus\Big(\bigoplus_{1\le i<j\le n} (A/\langle x_i\rangle)^2\Big) \simeq \bigoplus_{i=1}^{n} (A/\langle x_i\rangle)^{2(n-i)+1}$$