6. Exercices

EXERCICE 8.1. *Soient k un corps et $n \geqslant 1$ un entier. Montrer qu'il est équivalent de se donner un $k[X_1, \ldots, X_n]$-module et un k-espace vectoriel V muni de n endomorphismes $u_1, \ldots, u_n \in \mathrm{End}_k(V)$ vérifiant $u_i u_j = u_j u_i$ pour tout $1 \leqslant i, j \leqslant n$.*

EXERCICE 8.2. *Soit k un anneau à division.* [11]

(i) Montrer que tout k-module de type fini est libre.

(ii) Montrer que l'on a un isomorphisme de k-modules $k^n \simeq k^m$ si, et seulement si, $n = m$.

EXERCICE 8.3. *On rappelle que $\mathbb{H}$ désigne l'anneau des quaternions de Hamilton.*

(i) Montrer qu'il est équivalent de se donner un $\mathbb{H}$-module et un $\mathbb{R}$-espace vectoriel V muni de deux endomorphismes I et J vérifiant $I^2 = J^2 = -\mathrm{id}_V$ et $IJ = -JI$.

(ii) Montrer que si l'on a $I, J \in \mathrm{M}_n(\mathbb{R})$ avec $I^2 = J^2 = -\mathrm{I}_n$ et $IJ = -JI$, alors $n \equiv 0 \bmod 4$.

On rappelle qu'un corps k est dit *de caractéristique* 0 si pour tout entier $n \geqslant 1$ on a $n.1 \in k^\times$.

EXERCICE 8.4. *Soient k un corps, $V = k[t]$ le k-espace vectoriel des polynômes en t, $u : V \to V$, $P \mapsto P'$, l'application de dérivation (k-linéaire), et $M = V_u$ le $k[X]$-module associé.*

(i) Montrer que M n'est pas de type fini.

(ii) On suppose k de caractéristique 0*. Montrer que tous les sous-modules N de M avec $N \neq M$ sont monogènes.*

EXERCICE 8.5. (Algèbre de Weyl) *Soient k un corps et V le k-espace vectoriel $k[X]$. On note W_k le sous anneau de $\mathrm{End}_k(V)$ engendré par $k\,\mathrm{id}_V$ et les endomorphismes x et y définis par $x(P) = XP$ et $y(P) = P'$. On verra V comme un W_k-module. Dans les questions (i) et (iii) on suppose k de caractéristique* 0.

(i) Montrer que les seuls sous-modules de V sont $\{0\}$ et V.

(ii) Déterminer $yx - xy$ dans l'anneau W_k.

(iii) Soit M un W_k-module de k-espace vectoriel sous-jacent de dimension finie. Montrer $M = \{0\}$.

(iv) On suppose maintenant $k = \mathbb{Z}/p\mathbb{Z}$. Montrer que (i) et (iii) sont en défaut.

On rappelle que si A est un anneau non nécessairement commutatif, un idéal à gauche (resp. à droite, resp. bilatère) de A est un sous-groupe additif $I \subset A$ tel que pour tout $a \in A$ et tout $x \in I$ on a $ax \in I$ (resp. $xa \in I$, resp ax et $xa \in I$). Un idéal à gauche (resp. à droite) de A est dit principal s'il est de la forme Aa (resp. aA) pour un certain $a \in A$.

11. C'est-à-dire, un anneau non nul dans lequel tout élément non nul est inversible.

EXERCICE 8.6. *Soit A un anneau. Montrer que tout idéal bilatère de* $\mathrm{M}_n(A)$ *est de la forme* $\mathrm{M}_n(I)$ *avec I un idéal bilatère de A.*

EXERCICE 8.7. (Idéaux de $\mathrm{M}_n(k)$) *Soient k un corps, V un k-espace vectoriel de dimension finie n et $A = \mathrm{End}_k(V)$. On se propose de déterminer les idéaux à droite, et les idéaux à gauche, de l'anneau A. Pour $W \subset V$ un sous-espace de V on note $I_W \subset A$ le sous-ensemble des $u \in A$ avec $W \subset \ker u$, et $J_W \subset A$ le sous-ensemble des $u \in A$ avec $\mathrm{Im}\, u \subset W$.*

(i) Montrer que I_W est un idéal à gauche principal de A.

(ii) Montrer que $W \mapsto I_W$ est une bijection décroissante entre sous-espaces de V et idéaux à gauche de A.

(iii) Montrer que J_W est un idéal à droite principal de A.

(iv) Montrer que $W \mapsto J_W$ est une bijection croissante entre sous-espaces de V et idéaux à droite de A.

EXERCICE 8.8. *Déterminer le nombre d'idéaux à gauche de l'anneau* $\mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ *pour p un nombre premier.*

Si $(A, +, \cdot)$ est un anneau, son anneau *opposé* est l'anneau $(A, +, \star)$ avec $x \star y = yx$ (justifier que c'est bien un anneau !). On le note A^{opp}. Si A est commutatif, on a bien sûr $A = A^{\mathrm{opp}}$. Si M est un A-module on notera $\mathrm{End}_A(M)$ l'anneau des endomorphismes A-linéaires de M (pour $+$ et $\circ$).

EXERCICE 8.9. (Sur l'anneau opposé) *Soient A un anneau et $n \geqslant 1$ un entier.*

(i) Montrer que l'on a un isomorphisme d'anneaux $\mathrm{M}_n(A)^{\mathrm{opp}} \simeq \mathrm{M}_n(A^{\mathrm{opp}})$.

(ii) (suite) Qu'en déduire si A est commutatif ?

(iii) Montrer que $u \mapsto u(1)$ induit un isomorphisme d'anneaux $\mathrm{End}_A(A) \xrightarrow{\sim} A^{\mathrm{opp}}$.

(iv) Plus généralement, soient M un A-module libre de rang n et $e_1, \ldots, e_n$ une base de M. Pour $u \in \mathrm{End}_A(M)$ on note $\mathrm{Mat}_e u = (u_{i,j}) \in \mathrm{M}_n(A)$ l'élément déterminé par les relations $u(e_j) = \sum_{i=1}^n u_{i,j} e_i$, pour $1 \leqslant j \leqslant n$. Montrer que

$$\mathrm{End}_A(M) \to \mathrm{M}_n(A^{\mathrm{opp}}), u \mapsto \mathrm{Mat}_e u,$$

est un isomorphisme d'anneaux.

EXERCICE 8.10. *Soient V le k-espace vectoriel $k^{(\mathbb{N})}$ et $A = \mathrm{End}_k(V)$.*

(i) Montrer que les A-modules A et A^2 sont isomorphes.

(ii) Montrer que les k-algèbres A et $\mathrm{M}_2(A)$ sont isomorphes.

On rappelle la notion d'idéaux équivalents introduite dans l'Exercice 7.9.

EXERCICE 8.11. (Idéaux équivalents, partie II) *Soit A un anneau commutatif intègre de corps de fractions K.*

(i) Montrer que deux idéaux de A sont équivalents si, et seulement si, ils sont isomorphes en tant que A-modules.

(ii) Soit M un idéal fractionnaire *de K, c'est-à-dire un sous-A-module de K tel qu'il existe $a \in A$ non nul avec $aM \subset A$. Montrer que M est isomorphe à un idéal de A.*

(iii) Soit M un sous-A-module de type fini d'un K-espace vectoriel de dimension 1. Montrer que M est isomorphe à un idéal de A.

EXERCICE 8.12. *Soit $d \in \mathbb{Z}$ non carré. Notons $\mathrm{S}_2(d)$ l'ensemble des matrices $S \in \mathrm{M}_2(\mathbb{Z})$ avec $S^2 = d\mathrm{I}_2$. Le groupe $\mathrm{GL}_2(\mathbb{Z})$ agit par conjugaison sur $\mathrm{S}_2(d)$ et on notera $\mathrm{Cl}(d)$ l'ensemble de ses orbites (classes de conjugaison).*

(i) Montrer $\mathrm{S}_2(d) \neq \varnothing$.

(ii) Soit $S \in \mathrm{M}_2(\mathbb{Z})$. Vérifier $S \in \mathrm{S}_2(d) \iff \mathrm{tr}\, S = 0$ et $\det S = -d$.

(iii) Montrer qu'il existe des bijections entre :

(a) $\mathrm{Cl}(d)$,

(b) classes d'isomorphisme de structures de $\mathbb{Z}[\sqrt{d}]$-modules sur $\mathbb{Z}^2$,

(c) classes d'équivalence d'idéaux non nuls de $\mathbb{Z}[\sqrt{d}]$.

(iv) En déduire des représentants de $\mathrm{Cl}(d)$ pour $d = -2, -1, 2$.

(v) On suppose que l'entier d est un carré modulo $n \in \mathbb{Z}$, et $|\mathrm{Cl}(d)| = 1$. Montrer que $\pm n$ est de la forme $a^2 - db^2$ avec $a, b \in \mathbb{Z}$.

(vi) En considérant l'idéal $(2, \sqrt{-3} + 1)$ de $\mathbb{Z}[\sqrt{-3}]$, exhiber deux éléments de $\mathrm{S}_2(-3)$ non conjugués.

L'exercice suivant fait suite au précédent.

EXERCICE 8.13. *Soit $d \in \mathbb{Z}$ non carré. Pour $a, b, c \in \mathbb{Z}$ on pose*

$$[a, b, c] := \begin{bmatrix} b & c \\ a & -b \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

On a donc $[a, b, c] \in \mathrm{S}_2(d) \iff b^2 + ac = d$ (auquel cas a et c sont non nuls).

(i) Montrer que $[a, b, c]$ est $\mathrm{GL}_2(\mathbb{Z})$-conjugué à

$$[-a, b, -c], \ [c, -b, a], \ [a, b + a, c - a - 2b] \text{ et } [a, b - a, c - a + 2b].$$

(ii) Soit $[a, b, c] \in \mathrm{S}_2(d)$. Montrer que $[a, b, c]$ est $\mathrm{GL}_2(\mathbb{Z})$-conjugué à $[a', b', c']$ avec $2|b| \leqslant a \leqslant |c|$, puis l'inégalité $1 \leqslant a \leqslant 2\sqrt{|d|/3}$.

(iii) En déduire que les ensembles de la question (iii) de l'Exercice 8.12 sont finis.

(iv) Redémontrer la principalité de $\mathbb{Z}[\sqrt{d}]$ pour $d = -2, -1, 2$.

(v) Montrer les égalités

$$\mathrm{Cl}(3) = \{\overline{[1, 0, 3]}\}, \ \mathrm{Cl}(-3) = \{\overline{[1, 0, -3]}, \overline{[2, 1, -2]}\} \text{ et } \mathrm{Cl}(5) = \{\overline{[1, 0, 5]}, \overline{[2, 1, 2]}\}.$$

(vi) En déduire que $\mathbb{Z}[\sqrt{3}]$ est principal, mais pas $\mathbb{Z}[\sqrt{5}]$.

EXERCICE 8.14. *Pour $N \geqslant 1$ on note $\Gamma(N)$ le sous-groupe des matrices $M \in \mathrm{SL}_2(\mathbb{Z})$ telles que $M \equiv \mathrm{I}_2 \bmod N$.*

(i) Montrer que $\Gamma(N)$ est un sous-groupe distingué d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$.

(ii) Montrer que $\Gamma(2)$ *est engendré par* $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ *et* $-\mathrm{I}_2$.

(iii) (suite) Montrer qu'on ne peut pas supprimer $-\mathrm{I}_2$ *dans cet énoncé.*

(iv) Montrer qu'il existe un isomorphisme de groupes $\Gamma(N)/\Gamma(N^2) \simeq (\mathbb{Z}/N\mathbb{Z})^3$. *(On pourra utiliser le (ii) de l'exercice précédent).*

(v) En déduire que pour $N > 2$*, le groupe* $\Gamma(N)$ *n'est pas engendré par* $-\mathrm{I}_2$ *et deux transvections.*

Exercice 8.15. (L'exemple de Bass-Milnor-Serre) *Soient* $A = \mathbb{R}[\cos t, \sin t]$ *l'anneau*[12] *des polynômes trigonométriques* 2π*-périodiques sur* $\mathbb{R}$*. On se propose de montrer que l'élément*

$$\begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \in \mathrm{SL}_2(A)$$

n'est pas un produit de transvections. On verra $G = \mathrm{SL}_2(\mathbb{R})$ *comme le fermé de* $\mathrm{M}_2(\mathbb{R})$ *défini par* $\det = 1$*. On note* B *le sous-groupe des matrices triangulaires supérieures de* G*, et on pose* $K = \mathrm{SO}_2(\mathbb{R})$.

(i) Montrer que K *et* B *sont homéomorphes à* S^1 *et* $\mathbb{R}^2$ *respectivement.*

(ii) Montrer que la multiplication de G *induit un homéomorphisme* $K \times B \simeq G$.

(iii) Montrer, ou admettre, qu'il n'existe pas d'application continue

$$f : [0,1]^2 \to \mathrm{S}^1, (s,t) \mapsto f(s,t),$$

avec $f(0,t) = e^{2i\pi t}$ *et* $f(1,t) = f(s,0) = f(s,1) = 1$ *pour tout* $s, t \in [0,1]$.

(iv) Conclure.

Exercice 8.16. *Soient* A *un anneau principal,* $n \geqslant 2$ *et* $a_1, \dots, a_n \in A$ *premiers entre eux dans leur ensemble.*

(i) En considérant une forme linéaire adéquate $A^n \to A$, $(x_i) \mapsto \sum_{i=1}^n b_i x_i$*, montrer que le vecteur* $(a_1, \dots, a_n) \in A^n$ *se complète en une base de* A^n.

(ii) En déduire qu'il existe un élément de $\mathrm{SL}_n(A)$ *de première ligne* $(a_1, \dots, a_n)$.

L'exercice suivant généralise substantiellement l'Exercice 7.8.

Exercice 8.17. *Soit* $M \simeq \mathbb{Z}^n$ *un groupe abélien libre de rang fini, et soit* $u : M \to M$ *une application* $\mathbb{Z}$*-linéaire injective. Montrer que* $u(M)$ *est un sous-groupe d'indice fini* $|\det u|$ *de* M.

Exercice 8.18. *Soient* k *un corps,* V *un* k*-espace vectoriel de dimension finie* $n \geqslant 1$*,* $u \in \mathrm{End}_k(V)$*,* e *une base de* V *et* $M = \mathrm{Mat}_e u \in \mathrm{M}_n(k)$*. On se propose de montrer que les invariants de similitude de* u *sont les facteurs invariants non inversibles de la matrice* $M - X1_n$ *vue comme élément de* $\mathrm{M}_n(k[X])$.

(i) On suppose d'abord $M = \mathrm{C}(P)$ *avec* $P \in k[X]$ *unitaire de degré* n*. Montrer que les facteurs invariants de* $\mathrm{C}(P) - X1_n \in \mathrm{M}_n(k[X])$ *sont* $\sim 1, 1, \dots, 1, P$.

(ii) Conclure.

12. Cet anneau a déjà été étudié dans l'Exercice 7.18.