

Correction du DM n°4.

Problème 1

Pour tout $(a, b, c) \in \mathbb{R}^3$, on note $T(a, b, c) = \begin{pmatrix} a & b & c \\ b & a+c & b \\ c & b & a \end{pmatrix}$. On considère l'ensemble S défini par

$$S = \{T(a, b, c) \mid (a, b, c) \in \mathbb{R}^3\}$$

On pose $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

Partie I

Problème 1

Partie I

1. **SG 1** $S \subset \mathcal{M}_3(\mathbb{R})$ par définition.

SG 2 $O_3 = T(0, 0, 0) \in S$ donc $S \neq \emptyset$

SG 3 $\forall (M, M') \in S^2, \exists (a, b, c, a', b', c') \in \mathbb{R}^6$ tels que $M = T(a, b, c)$ et $M' = T(a', b', c')$

$$M - M' = \begin{pmatrix} a & b & c \\ b & a+c & b \\ c & b & a \end{pmatrix} - \begin{pmatrix} a' & b' & c' \\ b' & a'+c' & b' \\ c' & b' & a' \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & A+C & B \\ C & B & A \end{pmatrix} = T(A, B, C)$$

avec $A = a - a', B = b - b'$ et $C = c - c'$ donc $M - M' \in S$.

Conclusion : S est un sous-groupe de $\mathcal{M}_3(\mathbb{R})$

2. (a) $A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} = I + B, B^2 = I, AB = A$ et $BA = A$.

(b) $MM' = T(a, b, c) \times T(a', b', c') = \begin{pmatrix} a & b & c \\ b & a+c & b \\ c & b & a \end{pmatrix} \times \begin{pmatrix} a' & b' & c' \\ b' & a'+c' & b' \\ c' & b' & a' \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & A+C & B \\ C & B & A \end{pmatrix}$
soit $MM' = T(A, B, C)$ avec $A = aa' + bb' + cc', B = ba' + ab' + cb' + bc'$ et $C = ca' + ac' + bb'$.

(c) **SA 1** S est un sous-groupe de $\mathcal{M}_3(\mathbb{R})$.

SA 2 $I = T(1, 0, 0) \in S$

SA 3 $\forall (M, M') \in S^2, MM' \in S$ d'après la question précédente.

On remarque de plus que $MM' = M'M$.

Conclusion : S est un sous-anneau commutatif de $\mathcal{M}_3(\mathbb{R})$

(d) A n'est pas une matrice inversible sinon $AB = A \Rightarrow A^{-1}AB = A^{-1}A$ soit $B = I$ ce qui est absurde donc S n'est pas un corps

3. (a) $MM' = I \iff T(A, B, C) = I \iff \begin{cases} A = 1 & (1) \\ B = 0 & (2) \\ C = 0 & (3) \\ A + C = 1 & (4) = (1) + (3) \end{cases} \iff \begin{cases} aa' + bb' + cc' = 1 \\ ba' + ab' + cb' + bc' = 0 \\ ca' + ac' + bb' = 0 \end{cases}$
 $\iff \begin{cases} aa' + bb' + cc' = 1 & (1) \\ ba' + (a+c)b' + bc' = 0 & (2) \\ ca' + bb' + ac' = 0 & (3) \end{cases}$

D'où $(1) - (3) \iff (a-c)(a'-c') = 1$. Par conséquent, si $a = c$, il n'y a pas de solution.

$$\text{Si } a \neq c, \text{ alors } MM' = I \iff \begin{cases} (a-c)(a'-c') = 1 & (1') \\ (a-c)ba' + (b^2 - ac - c^2)b' = b & b \times (1) - c \times (2) \\ (a-c)ba' + (a^2 + ac - b^2)b' = 0 & a \times (2) - b \times (a) \end{cases}$$

$$\iff \begin{cases} (a-c)(a'-c') = 1 \\ (b^2 - (a+c)^2)b' = b \\ (a-c)ba' + (a^2 + ac - b^2)b' = 0 \end{cases}$$

Le système n'admet pas de solution si $b^2 - (a+c)^2 = 0$.

En effet, si l'égalité est vraie alors $(b^2 - (a+c)^2)b' = b \Rightarrow b = 0 \Rightarrow a+c = 0$ ce qui est exclu.

Si $b^2 - (a+c)^2 \neq 0$ alors on obtient

$$a' = \frac{b^2 - ac - a^2}{(a-c)(2b^2 - (a+c)^2)}, b' = \frac{b}{2b^2 - (a+c)^2} \text{ et } c' = \frac{-b^2 + ac + c^2}{(a-c)(2b^2 - (a+c)^2)}$$

(b) Les éléments inversibles de l'anneau S sont donc les matrices $T(a, b, c)$ qui vérifient $a \neq c$ et $b^2 - (a+c)^2 \neq 0$.

Partie II

1. M est orthogonale ssi $M \times {}^tM = {}^tM \times M = I$ ssi $M^{-1} = {}^tM$.

2. Si $M \in S$ alors $M = {}^tM$ d'où M est orthogonale ssi $M^2 = I \iff \begin{cases} a^2 + b^2 + c^2 = 1 \\ b^2 + 2ac = 0 \\ b(a+c) = 0 \end{cases}$.

3. $b(a+c) = 0 \iff b = 0$ ou $c = -a$.

Cas 1 : si $b = 0$ alors $ac = 0$ donc $a = 0$ ou $c = 0$.

- Si $a = 0$ alors $c = 1$ ou $c = -1$ soit $M = T(0, 0, 1)$ ou $M = T(0, 0, -1)$.
- Si $c = 0$ alors $a = 1$ ou $a = -1$ soit $M = T(1, 0, 0)$ ou $M = T(-1, 0, 0)$.

Cas 2 : si $b \neq 0$ alors $c = -a$ et $b^2 = 2a^2$ donc $4a^2 = 1$ soit $a = \frac{1}{2}$ ou $a = -\frac{1}{2}$.

- Si $a = \frac{1}{2}$ alors $b = \frac{1}{\sqrt{2}}$ ou $b = -\frac{1}{\sqrt{2}}$ soit $M = T\left(\frac{1}{2}, \frac{1}{\sqrt{2}}, -\frac{1}{2}\right)$ ou $M = T\left(\frac{1}{2}, -\frac{1}{\sqrt{2}}, -\frac{1}{2}\right)$.
- Si $a = -\frac{1}{2}$ alors $b = \frac{1}{\sqrt{2}}$ ou $b = -\frac{1}{\sqrt{2}}$ soit $M = T\left(-\frac{1}{2}, \frac{1}{\sqrt{2}}, \frac{1}{2}\right)$ ou $M = T\left(-\frac{1}{2}, -\frac{1}{\sqrt{2}}, \frac{1}{2}\right)$.

Réciproquement, les huit matrices sont orthogonales.

Problème 2 (facultatif)L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On définit $\sim$ la relation binaire sur $\mathbb{Z}^2$ telle que $x \sim y \Leftrightarrow x - y \in n\mathbb{Z}$

1. On a $\forall (x, y) \in \mathbb{Z}^2, x \sim y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow x \cong y[n]$. Cette relation est réflexive car $\forall x \in \mathbb{Z}, x - x = 0 = 0 \times n \in n\mathbb{Z}$, symétrique, car si $\forall (x, y) \in \mathbb{Z}^2$, tel que $x \sim y$, il existe un entier $p \in \mathbb{Z}$ pour lequel $x - y = pn$. On a donc $y_x = -pn$ et comme $-p \in \mathbb{Z}$, cela prouve que $y - x \in n\mathbb{Z}$ d'où $y \sim x$

Enfin, elle est transitive : car pour tout $(x, y, z) \in \mathbb{Z}^3$ si $x \sim y$ et $y \sim z$ alors il existe deux entiers p et q tels que $x - y = pn$ et $y - z = qn$, alors $x - z = x - y + y - z = (p + q)n$ or $p + q \in \mathbb{Z}$ ce qui prouve $x \sim z$

C'est donc une relation d'équivalence

2. Chaque entier $k \in \mathbb{Z}$ peut s'écrire $k = pn + r$ avec $r \in [0; n - 1]$ (division euclidienne par n , le reste étant r). Dans ce cas, k et r sont congrus modulo n , ainsi, k est dans la classe d'équivalence de r , i.e. n'importe quel entier est soit dans la classe de 0, soit dans celle de 1, soit dans celle de 2, etc ou enfin dans celle de $n - 1$.

De plus, toutes ces classes sont bien disjointes, en effet, si $0 \leq k < k' \leq n - 1$, alors $0 < k' - k < n$ qui n'est donc pas multiple de n , ainsi k et k' n'étant pas congrus modulo n , leurs classes sont disjointes.

Il y a donc exactement n classes, qui sont $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n - 1}$. Il faut noter que $\overline{n} = \overline{2n} = \dots = \overline{0}$ et $\overline{n + 1} = \overline{2n + 1} = \dots = \overline{1}$ etc...

3. On considère deux classes d'équivalence de $\mathbb{Z}/n\mathbb{Z}$. Alors il existe bien deux entiers a et b tels que ces classes d'équivalences soient $\overline{a}$ et $\overline{b}$. L'ennui étant le fait qu'il n'y a pas unicité : en choisissant un autre entier $a' = a + kn$, on aurait également pu dire que la première classe correspondait à $\overline{a + kn}$, idem, pour représenter la seconde classe d'équivalence, on aurait très bien pu choisir $b' = b + ln$ puisqu'après tout, $\overline{a + kn} = \overline{a}$ et $\overline{b + ln} = \overline{b}$. Décidons d'associer à ces deux classes la classe d'équivalence de $a + b$.

- En ayant choisi comme représentants a et b , on trouvera la classe d'équivalence $\overline{a + b}$
- En ayant choisi comme représentants $a' = a + kn$ et $b' = b + ln$, on trouvera la classe d'équivalence $\overline{a + b + (k + l)n}$ mais il se trouve que $a + b \cong a + b + (k + l)n[n]$ donc au final, la classe d'équivalence de $a + b$ ne dépend pas du choix d'un représentant a ou a' , ni du représentant b ou b' .

4. Si l'on a deux classes d'équivalences qui sont $\overline{a}$ et $\overline{b}$, alors $\overline{a + b} = \overline{a + b} = \overline{b + a} = \overline{b + a}$ (car $a + b = b + a$ vu que $+$ est commutative sur $\mathbb{Z}$)

5. On considère une classe d'équivalence, on décide d'un représentant $a \in \mathbb{Z}$ tel que cette classe qui est donc $\overline{a}$. On aurait également pu choisir $a' = a + pn$, et voyons ce que vaut $\omega^{a + pn}$. On a $\omega^{a + pn} = \omega^a \omega^{pn} = \omega^a (\omega^n)^p$ or $\omega^n = 1$ car ω est racine n -ème de l'unité.

Au final, que l'on choisisse comme représentant a ou a' , le résultat sera dans tous les cas ω^a , donc le choix d'un représentant de la classe d'équivalence n'a pas de conséquence sur le résultat, pour cette raison, l'application θ est bien définie.

6. On considère deux classes d'équivalences, $(\overline{k}, \overline{l}) \in (\mathbb{Z}/n\mathbb{Z})^2$, (comme dit précédemment, le choix des représentants n'a pas d'influence). On a alors

$$\theta(\overline{k + l}) = \omega^{k + l} = \omega^k \omega^l = \theta(\overline{k}) \theta(\overline{l}),$$

ce qui prouve que θ est un morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers $(\mathbb{U}_n, \times)$.

Pour prouver son injectivité, on cherche le noyau de θ . On a

$$\overline{k} \in \ker(\theta) \Leftrightarrow \theta(\overline{k}) = 1 \Leftrightarrow e^{\frac{2ik\pi}{n}} = 1 \Leftrightarrow n | k \Leftrightarrow \overline{k} = \overline{0}.$$

Donc $\ker(\theta) = \{\overline{0}\}$ ce qui prouve que θ est injective. Comme les cardinaux de $\mathbb{Z}/n\mathbb{Z}$ et de $\mathbb{U}_n$ sont tous les deux égaux à n , θ est un isomorphisme.

7. Comme pour la question 3, si l'on avait choisi $a' = a + kn$ et $b' = b + ln$, le produit $a'b'$ nous aurait donné $a'b' = ab + n(kb + la + kln)$ ce qui est congru à ab modulo n , donc au final la classe d'équivalence obtenue aurait été la même car

$$\overline{ab} = \overline{ab + n(kb + la + kln)} = \overline{a'b'}.$$

8. $+$ est une loi commutative, associative, d'élément neutre $\bar{0}$, dont chaque élément $\bar{k}$ admet pour symétrique l'élément $-\bar{k}$, ce qui garantit que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

La loi $\times$ est une loi, elle est associative car $\overline{a \times (b \times c)} = \overline{a \times bc} = \overline{abc} = \overline{ab \times c} = \overline{(a \times b) \times c}$. Elle est aussi distributive par rapport à $+$ car $\overline{a \times (b + c)} = \overline{a \times b + c} = \overline{a(b + c)}$ mais comme $a(b + c) = ab + ac$ (en utilisant les propriétés sur $\mathbb{Z}$ de ces opérations) on obtient finalement $\overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a \times b} + \overline{a \times c}$. Le produit dans l'autre sens : idem car tout commute. Enfin, $\bar{1}$ est l'élément neutre de $\times$ car pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ on a $\bar{1} \times \bar{a} = \bar{a} = \bar{a} \times \bar{1}$

- 9.
- Si n n'est pas un nombre premier, alors il s'écrit $n = ab$ avec $1 < a, b < n$ ainsi on a $\bar{a} \neq \bar{0}$ et $\bar{b} \neq \bar{0}$, mais pourtant $\bar{a} \times \bar{b} = \bar{0}$ donc dans ce cas, l'anneau $\mathbb{Z}/n\mathbb{Z}, +, \times$ n'est pas intègre.
 - Si n est premier, pour tout a non multiple de n , on a alors $k \wedge n = 1$ et donc d'après l'identité de Bézout, il existe deux entiers $(u, v) \in \mathbb{Z}^2$ tel que

$$au + nv = 1,$$

mais cela entraîne $\overline{au} = \overline{nv} = \bar{1}$ mais comme $\bar{n} = \bar{0}$ on a finalement $\overline{au} = \bar{1}$, et le produit étant commutatif, on a aussi le même résultat pour $\overline{ua}$, donc toutes les classes autre que $\bar{0}$ admettent un inverse pour la loi $\times$, ce qui correspond à dire que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps.

Conclusion si n n'est pas premier $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif non-intègre (donc pas un corps) et si n est premier, c'est un corps (donc notamment il est intègre).