

Aucun document ou appareil électronique n'est autorisé.

Vous devez **justifier toutes vos réponses**. La note tiendra compte de la qualité et de la concision de la rédaction. Vous pouvez utiliser tous les résultats du cours. Ces résultats doivent être cités correctement.

**Exercice 1.** Les trois questions de cet exercice sont indépendantes les unes des autres.

(1) On considère  $S := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\} \subset M_2(\mathbb{Z})$ .

a. Est-ce que  $S$  est un sous-anneau de  $M_2(\mathbb{Z})$ ?

b. Est-ce que  $S$  est un idéal de  $M_2(\mathbb{Z})$ ?

(2) Qu'est-ce qu'un anneau intègre?

*Il n'est pas nécessaire de rappeler la définition d'anneau.*

(3) Dans cette question, on considère un anneau  $A$  non trivial.

a. Montrer que  $A$  est à division si et seulement si  $\forall x \in A \setminus \{0\}, \exists y \in A, xy = 1$ .

b. Montrer que  $A$  est à division si et seulement si  $\forall x \in A \setminus \{1\}, \exists y \in A, x + y = xy$ .

*Indice : on pourra utiliser la question a.*

**Exercice 2.**

Soit  $n \in \mathbb{Z}$ . On considère  $A := \left\{ \begin{pmatrix} a & b \\ nb & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \subset M_2(\mathbb{Z})$ .

(1) Montrer que  $A$  est un sous-anneau de  $M_2(\mathbb{Z})$ .

On note  $M := \begin{pmatrix} 0 & 1 \\ n & 0 \end{pmatrix} \in M_2(\mathbb{Z})$  et on définit  $\varphi : \mathbb{Z}[X] \rightarrow M_2(\mathbb{Z})$  par  $\varphi(P) = P(M)$ ,

i.e. si  $P = a_0 + a_1X + a_2X^2 + \dots + a_dX^d \in \mathbb{Z}[X]$  alors  $\varphi(P) = a_0I_2 + a_1M + a_2M^2 + \dots + a_dM^d \in M_2(\mathbb{Z})$ .

(2) Montrer que  $\varphi$  est un morphisme d'anneaux.

(3) Montrer que  $\text{Im}(\varphi) = A$ .

(4) Montrer que  $\text{Ker}(\varphi) = (X^2 - n)$ .

(5) Montrer que  $\varphi$  induit un isomorphisme  $\mathbb{Z}[X]/(X^2 - n) \rightarrow A$ .

**Exercice 3.**

PARTIE I : CENTRE D'UN ANNEAU.

On définit le *centre* d'un anneau  $A$  par  $C(A) := \{x \in A : \forall a \in A, xa = ax\}$ .

(1) Soit  $A$  un anneau. Montrer que  $C(A)$  est un sous-anneau de  $A$ .

(2) Le centre d'un anneau est-il nécessairement un idéal?

PARTIE II : TOUT ANNEAU  $A$  VÉRIFIANT  $\forall x \in A, x^3 = x$  EST COMMUTATIF.

Dans toute cette partie, on considère un anneau  $A$  vérifiant  $\forall x \in A, x^3 = x$ .

(3) a. Montrer que  $\forall x \in A, \forall n \in \mathbb{N} \setminus \{0\}, x^n \in \{x, x^2\}$ .

b. En déduire que 0 est le seul nilpotent de  $A$ .

*On rappelle qu'un élément  $x \in A$  est nilpotent s'il existe  $n \in \mathbb{N} \setminus \{0\}$  tel que  $x^n = 0$ .*

(4) Soit  $e$  un idempotent de  $A$ , i.e. vérifiant  $e^2 = e$ .

a. Soit  $a \in A$ . On pose  $b := ea(1 - e)$  et  $c := (1 - e)ae$ .

Montrer que  $b$  et  $c$  sont nilpotents.

b. En déduire que  $e \in C(A)$ .

(5) Dédurre de la question précédente que  $\forall x \in A, x^2 \in C(A)$ .

(6) a. Montrer que  $\forall x \in A, 2x \in C(A)$ .

b. Montrer que  $\forall x \in A, 3x \in C(A)$ .

*Indice pour les questions (6)a. et (6)b. : étant donné  $x \in A$ , on pourra considérer  $(x + 1)^2$  et  $(x + 1)^3$ .*

(7) Conclure.

**Solution de l'exercice 1.**

- (1) a.  $S$  n'est pas un sous-anneau de  $M_2(\mathbb{Z})$  puisque  $I_2 \notin S$ .  
 b. On a  $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin S$  alors que  $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in S$ .  
 Donc  $S$  n'est pas un idéal de  $M_2(\mathbb{Z})$ .

(2) Un anneau intègre est un anneau non trivial, commutatif et sans diviseur de zéro.

- (3) a. Supposons que  $A$  soit à division. Soit  $x \in A \setminus \{0\}$ .  
 Alors il existe  $y \in A$  tel que  $xy = yx = 1$ , en particulier  $xy = 1$ .

Réciproquement, supposons que  $\forall x \in A \setminus \{0\}, \exists y \in A, xy = 1$ .

Soit  $x \in A \setminus \{0\}$ . Par hypothèse, il existe  $y \in A$  tel que  $xy = 1$ .

Si  $y = 0$  alors  $xy = 1 \neq 0$  donc  $y \neq 0$ . Donc, par hypothèse, il existe  $z \in A$  tel que  $yz = 1$ .

Alors  $z = 1 \cdot z = xyz = x \cdot 1 = x$ . Donc  $xy = yx = 1$  et  $x \in A^*$ .

Ainsi  $A$  est un anneau non trivial donc tous les éléments non nuls sont inversibles, i.e.  $A$  est un anneau à division.

- b. Supposons que  $A$  soit à division.

Soit  $x \in A \setminus \{1\}$  alors  $x - 1 \neq 0$ . Donc il existe  $z \in A$  tel que  $z(x - 1) = (x - 1)z = 1$ .

Posons  $y := zx$  alors  $xy = xzx = (1 + z)x = x + zx = x + y$ .

Réciproquement, supposons que  $\forall x \in A \setminus \{1\}, \exists y \in A, x + y = xy$ .

Soit  $x \in A \setminus \{0\}$ . Alors  $1 - x \neq 1$ .

Donc, par hypothèse, il existe  $y \in A$  tel que  $1 - x + y = (1 - x)y = y - xy$ . D'où  $1 = x - xy = x(1 - y)$ .

On a montré que  $\forall x \in A \setminus \{0\}, \exists z \in A, xz = 1$ . Ainsi  $A$  est à division d'après la question précédente.

**Solution de l'exercice 2.**

- (1) •  $I_2 = \begin{pmatrix} 1 & 0 \\ n0 & 1 \end{pmatrix} \in A$ .  
 • Soient  $\begin{pmatrix} a & b \\ nb & a \end{pmatrix}, \begin{pmatrix} c & d \\ nd & c \end{pmatrix} \in A$  alors  $\begin{pmatrix} a & b \\ nb & a \end{pmatrix} - \begin{pmatrix} c & d \\ nd & c \end{pmatrix} = \begin{pmatrix} a - c & b - d \\ n(b - d) & a - c \end{pmatrix} \in A$  et  
 $\begin{pmatrix} a & b \\ nb & a \end{pmatrix} \begin{pmatrix} c & d \\ nd & c \end{pmatrix} = \begin{pmatrix} ac + bnd & ad + bc \\ n(ad + bc) & ac + bnd \end{pmatrix} \in A$ .  
 Donc  $A$  est un sous-anneau de  $M_2(\mathbb{Z})$ .

- (2) •  $\varphi(1) = I_2$   
 • Soient  $P = \sum_k a_k X_k, Q = \sum_k b_k X_k \in \mathbb{Z}[X]$ .  
 Alors  $\varphi(P) + \varphi(Q) = \sum_k a_k M^k + \sum_k b_k M^k = \sum_k (a_k + b_k) M^k = (P + Q)(M) = \varphi(P + Q)$  et

$$\varphi(P)\varphi(Q) = \left( \sum_k a_k M^k \right) \left( \sum_k b_k M^k \right) = \sum_k \left( \sum_{\substack{i,j \geq 0 \\ i+j=k}} a_i b_j \right) M^k = (PQ)(M) = \varphi(PQ).$$

Donc  $\varphi$  est un morphisme d'anneaux.

- (3) Soit  $\begin{pmatrix} a & b \\ nb & a \end{pmatrix} \in A$  alors  $\varphi(a + bX) = aI_2 + bM = \begin{pmatrix} a & b \\ nb & a \end{pmatrix}$ . Donc  $A \subset \text{Im}(\varphi)$ .

Soit  $N \in \text{Im}(\varphi)$ . Alors il existe  $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$  tel que  $N = \varphi(P)$ .

Alors  $N = \sum_{k=0}^d a_k I_2 M^k \in A$  puisque  $a_k I_2, M \in A$  et que  $A$  est un anneau. Donc  $A = \text{Im}(\varphi)$ .

- (4) Soit  $P \in (X^2 - n)$  alors il existe  $Q \in \mathbb{Z}[X]$  tel que  $P = (X^2 - n)Q(X)$ .  
 Puis  $\varphi(P) = (M^2 - nI_2)Q(M) = (nI_2 - nI_2)Q(M) = 0Q(M) = 0$ . Donc  $(X^2 - n) \subset \text{Ker}(\varphi)$ .

Réciproquement, soit  $P \in \text{Ker}(\varphi)$ . Puisque le coefficient dominant de  $X^2 - n$  est  $1 \in \mathbb{Z}^*$ , par division euclidienne, il existe  $Q \in \mathbb{Z}[X]$  et  $\alpha, \beta \in \mathbb{Z}$  tels que  $P = (X^2 - n)Q(X) + \alpha X + \beta$ .

Puis  $0 = \varphi(P) = (M^2 - nI_2)Q(M) + \alpha M + \beta I_2 = 0Q(M) + \alpha M + \beta I_2 = \begin{pmatrix} \beta & \alpha \\ n\alpha & \beta \end{pmatrix}$ . Donc  $\alpha = \beta = 0$ .

Ainsi  $P = (X^2 - n)Q(X) \in (X^2 - n)$ . Donc  $(X^2 - n) = \text{Ker}(\varphi)$ .

- (5) C'est une conséquence du premier théorème d'isomorphisme appliqué à  $\varphi$ .

### Solution de l'exercice 3.

- (1) • Soit  $a \in A$  alors  $1 \cdot a = a \cdot 1 = a$ . Donc  $1 \in C(A)$ .  
 • Soient  $x, y \in C(A)$ .  
 – Soit  $a \in A$  alors  $a(x - y) = ax - ay = xa - ya = (x - y)a$  puisque  $x, y \in C(A)$ .  
 On a montré que  $\forall a \in A, a(x - y) = (x - y)a$ , i.e. que  $x - y \in C(A)$ .  
 – Soit  $a \in A$  alors  $a(xy) = axy = xay = xya = (xy)a$  puisque  $x, y \in C(A)$ .  
 On a montré que  $\forall a \in A, a(xy) = (xy)a$ , i.e. que  $xy \in C(A)$ .

Donc  $C(A)$  est un sous-anneau de  $A$ .

- (2) Considérons  $A := M_2(\mathbb{R})$ . Supposons par l'absurde que  $C(A)$  soit un idéal. Puisque  $I_2 \in C(A)$ , on obtient que  $C(A) = A$ . Or  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin C(A)$  puisque  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ .  
 Donc  $C(A)$  n'est pas un idéal.

- (3) a. Soit  $x \in A$ . Montrons par récurrence que  $\forall n \in \mathbb{N} \setminus \{0\}, x^n \in \{x, x^2\}$ .  
 Si  $n = 1$  alors  $x^1 = x \in \{x, x^2\}$ . Supposons le résultat vrai pour un certain  $n \in \mathbb{N} \setminus \{0\}$ .  
 • Premier cas : si  $x^n = x$  alors  $x^{n+1} = x^2 \in \{x, x^2\}$ .  
 • Second cas : si  $x^n = x^2$  alors  $x^{n+1} = x^3 = x \in \{x, x^2\}$ .

- b. Soit  $x \in A$  un élément nilpotent. Alors il existe  $n \in \mathbb{N} \setminus \{0\}$  tel que  $x^n = 0$ .

D'après la question précédente, il y a deux cas possible :

- soit  $x^n = x$  alors  $x = x^n = 0$ ;
- soit  $x^n = x^2$  alors  $x = x^3 = x \cdot x^2 = x \cdot x^n = x^2 \cdot 0 = 0$ .

Donc forcément  $x = 0$ . Et 0 est nilpotent puisque  $0^1 = 0$ .

- (4) a. On a  $b^2 = ea(1 - e)ea(1 - e) = ea(e - e^2)a(1 - e) = ea(e - e)ea(1 - e) = 0$   
 et  $c^2 = (1 - e)ae(1 - e)ae = (1 - e)a(e - e^2)ae = (1 - e)a(e - e)ae = 0$ .  
 b. Soit  $a \in A$ . Posons  $b := ea(1 - e)$  et  $c := (1 - e)ae$  comme dans la question précédente.  
 Puisque  $b$  est nilpotent, on déduit de la question précédente que  $b = 0$ , i.e.  $ea = eae$ .  
 De même, puisque  $c$  est nilpotent, on a  $c = 0$ , i.e.  $ae = eae$ .  
 Donc  $ea = eae = ae$ . Et ainsi  $e \in C(A)$ .

- (5) Soit  $x \in A$  alors  $(x^2)^2 = x^4 = x^3x = x^2$ .  
 Donc  $x^2$  est un idempotent et donc  $x^2 \in C(A)$  d'après la question précédente.

- (6) a. Soit  $x \in A$  alors  $2x = (x + 1)^2 - x^2 - 1 \in C(A)$  puisque  $(x + 1)^2, x^2, 1 \in C(A)$  d'après la question précédente et que  $C(A)$  est un anneau.  
 b. Soit  $x \in A$  alors  $x + 1 = (x + 1)^3 = x^3 + 3x^2 + 3x + 1 = x + 3x^2 + 3x + 1$  d'où  $3x = -3x^2 \in C(A)$  d'après la question précédente.

- (7) Soient  $x, y \in A$ . Alors  $x = 3x - 2x \in C(A)$  d'après la question précédente, puisque  $C(A)$  est un anneau. Ainsi  $xy = yx$ . Donc  $A$  est un anneau commutatif.