



DEVOIR SURVEILLÉ 1

Donné le : 25-9-2026

De 13h00 à 17h00

Durée : 3 heures

Année : 2026-2027

Classe : MP*

La clarté et la précision de la rédaction seront prises en compte dans l'appréciation de la copie.

PROBLÈME

OBJET DU PROBLÈME

On étudie la périodicité (éventuelle) de la suite $1, a, a^2, \dots$ des puissances successives d'un élément d'un anneau, notamment dans le cas d'anneaux de matrices finis.

- **Le préliminaire** comporte des questions dont les résultats peuvent être utilisés dans la suite du problème et d'autres questions indépendantes des parties I et II.
- **La partie I** étudie le cas particulier des éléments a tels que $a^2 = a$.
- **La partie II** établit quelle forme peut prendre la périodicité envisagée.

NOTATIONS

Dans tout le problème, « entier » signifie « entier naturel ». Les anneaux considérés ici seront toujours supposés unitaires et non triviaux (c'est-à-dire ayant au moins deux éléments) ; l'addition en sera notée $+$, la multiplication $\cdot$ (ou omise), les éléments neutres de l'addition et de la multiplication seront notés respectivement 0 et 1 (sauf mention spéciale, notamment $\bar{0}$ et $\bar{1}$ pour le cas de l'anneau $\mathbb{Z}/n\mathbb{Z}$, où $n \in \mathbb{N}^*$). Les anneaux ne seront pas supposés commutatifs, en général.

Si a est un élément d'un anneau R et m un entier non nul, on notera (comme d'habitude) a^m pour le produit de m facteurs égaux à a . On conviendra de plus que a^0 est 1 pour tout a dans R (même nul). De la sorte les formules suivantes sont valables pour tout a dans R et tous m, n dans $\mathbb{N}$:

$$(a^m)(a^n) = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

L'ensemble des éléments inversibles d'un anneau R sera noté $\mathfrak{U}(R)$.

Si R est un anneau commutatif et r un entier non nul, on notera $\mathcal{M}_r(R)$ l'anneau des matrices carrées $r \times r$ à coefficients dans R (les opérations étant définies de la même manière dans le cas d'un anneau commutatif quelconque que dans celui d'un corps), on notera dans ce cas 0_r et I_r la matrice nulle et la matrice identité correspondantes (pour éviter la confusion avec les éléments 0 et 1 de R).

PRÉLIMINAIRE

1. Soit $\mathbb{K}$ un sous-corps du corps $\mathbb{C}$. On considère $(\mathcal{A}, +, \times, .)$ une $\mathbb{K}$ -algèbre de dimension finie non nulle N et $u \in \mathcal{A}$.
 - (a) On note $I_u = \{P \in \mathbb{K}[X] / P(u) = 0\}$. Justifier qu'il existe un et un seul polynôme unitaire $\pi_u \in \mathbb{K}[X]$ tel que $I_u = \pi_u \mathbb{K}[X] = \{\pi_u P / P \in \mathbb{K}[X]\}$. On dit que π_u est le polynôme minimal de u .
 - (b) Montrer que si $u \in \mathcal{A}$ alors pour tout polynôme $P \in \mathbb{K}[X]$, on a $P(u) = 0$ si et seulement si π_u divise P .
 - (c) On suppose ici que $\mathcal{A} = \mathcal{M}_n(\mathbb{K})$ et M une matrice de projecteur.
 - i. Préciser π_M .
 - ii. Calculer $\sum_{k=0}^N \frac{M^k}{k!}$ pour tout $N \in \mathbb{N}$.
 - (d) On suppose ici que $\mathcal{A} = \mathcal{M}_n(\mathbb{K})$ avec $n \geq 2$ et que M est une matrice de $\mathcal{M}_n(\mathbb{K})$ tel que $\text{rg}(M) = 1$.
 - i. Montrer qu'il existe deux matrices U, V de $\mathcal{M}_{n,1}(\mathbb{K}) \setminus \{0\}$ tel que $M = UV^\top$ et en déduire que $M^2 = \text{Tr}(M)M$.
 - ii. Déterminer π_M .
 - iii. Calculer $\sum_{k=0}^N \frac{M^k}{k!}$ pour tout $N \in \mathbb{N}$.
2. Soit R un anneau fini et commutatif. Prouver que R est intègre si et seulement si R est un corps.
(Indication : Pour $x \in R \setminus \{0\}$, on pourra considérer la famille d'éléments de R , $(x^k)_{k \geq 1}$.)
3. Soit $n \in \mathbb{N}^*$. Justifier que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.
4. On admet que si R_1, R_2, R_3 sont des anneaux alors les anneaux $R_1 \times R_2 \times R_3$ d'une part et $(R_1 \times R_2) \times R_3$ d'autres part sont isomorphes.
 - (a) Que proposez vous comme isomorphisme de $R_1 \times R_2 \times R_3$ vers $(R_1 \times R_2) \times R_3$? (on ne demande pas de preuve).
 - (b) Rappeler sans démonstration le lemme des restes chinois pour les anneaux $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ avec $(m, n) \in (\mathbb{N}^*)^2$ et $m \wedge n = 1$.
 - (c) Soient $(m, n, s) \in (\mathbb{N}^*)^3$ tel que $m \wedge n = n \wedge s = s \wedge m = 1$. Montrer que les anneaux $\mathbb{Z}/(mns)\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ sont isomorphes.
5. Soit R un anneau commutatif et Soit $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{M}_2(R)$.
 On pose $\tau = \text{Tr}(M) = a + d$ et $\delta = \det(M) = ad - bc$.
 Montrer par un calcul direct que l'on a : $M^2 = \tau M - \delta I_2$.

PARTIE I

Pour tout anneau R , on pose $\mathcal{J}(R) = \{x \in R; x^2 = x\}$. On notera que 0 et 1 sont des éléments de $\mathcal{J}(R)$.

1.
 - a. Montrer que, si R est un anneau intègre, alors $\mathcal{J}(R)$ est réduit à $\{0, 1\}$.
 - b. Montrer que, si p est un entier premier et a un entier non nul, alors $\mathcal{J}(\mathbb{Z}/p^a\mathbb{Z})$ est réduit à $\{\bar{0}, \bar{1}\}$.
 - c. Soit R un anneau quelconque : montrer que, si a est un élément de $\mathcal{J}(R)$, alors $1 - a$ en est un aussi, et en déduire que le cardinal de $\mathcal{J}(R)$, s'il est fini, est un entier pair.

- d. Montrer que, si R est commutatif, alors $\mathcal{J}(R)$ est stable par multiplication. À quelle condition a-t-on l'équivalence : $\forall x \in R, \quad x \in \mathcal{J}(R) \Leftrightarrow -x \in \mathcal{J}(R)$?
2. a. On suppose que $\mathbb{K}$ est un corps ; montrer que la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans $\mathcal{J}(\mathcal{M}_2(\mathbb{K}))$ si, et seulement si, $M = 0_2$ ou $M = I_2$ ou $\begin{cases} a + d = 1 \\ ad = bc \end{cases}$.
- b. Calculer le cardinal de $\mathcal{J}(\mathcal{M}_2(\mathbb{Z}/p\mathbb{Z}))$ lorsque p est un nombre premier.
3. On suppose que p et q sont des nombres premiers distincts.
- a. Justifier que les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes et rappeler, sans démonstration, l'expression de l'isomorphisme naturel f de $\mathbb{Z}/pq\mathbb{Z}$ vers $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
- b. En déduire les cardinaux de $\mathcal{J}(\mathbb{Z}/pq\mathbb{Z})$ et de $\mathcal{J}(\mathcal{M}_2(\mathbb{Z}/pq\mathbb{Z}))$.
4. Soit R un anneau quelconque ; on définit sur $\mathcal{J}(R)$ une relation binaire $\preceq$ par :

$$x \preceq y \quad \text{si et seulement si} \quad xy = yx = x.$$

Par ailleurs, deux éléments a, b de R sont dits orthogonaux si et seulement si on a : $ab = ba = 0$.

- a. Montrer que $\preceq$ est une relation d'ordre, admettant 0 comme minimum et 1 comme maximum.
- b. On pose :

$$\mathcal{S}(R) = \{x \in \mathcal{J}(R); 0 \text{ est le seul minorant strict de } x \text{ pour } \preceq\}.$$

Montrer que 1 est dans $\mathcal{S}(R)$ si et seulement si $\mathcal{J}(R)$ est réduit à $\{0, 1\}$.

- c. Montrer que, pour tout a non nul dans $\mathcal{J}(R)$, il y a équivalence entre :
- (i) a n'est pas dans $\mathcal{S}(R)$;
 - (ii) il existe deux éléments non nuls b, c dans $\mathcal{J}(R)$ tels que $a = b + c$ et b et c sont orthogonaux.
- d. On dit que R vérifie la condition (★) si, et seulement si, il n'existe pas de suite infinie dans $\mathcal{J}(R)$ qui soit strictement décroissante pour $\preceq$. Montrer que, si R vérifie la condition (★), alors tout élément non nul de $\mathcal{J}(R)$ qui n'est pas dans $\mathcal{S}(R)$ s'écrit comme somme finie d'éléments de $\mathcal{S}(R)$ deux à deux orthogonaux.
5. On garde les notations de la question précédente et on suppose en outre, dans cette question, que R a la propriété (C) suivante :

$$(C) \quad \forall (a, b) \in (\mathcal{J}(R))^2, \quad ab = ba.$$

- a. Montrer que deux éléments distincts de $\mathcal{S}(R)$ sont nécessairement orthogonaux. En déduire que toute somme d'éléments distincts de $\mathcal{S}(R)$ est dans $\mathcal{J}(R)$.
- b. Montrer que, si $b_1, \dots, b_n$ sont des éléments distincts de $\mathcal{S}(R)$, alors $\{b_1, \dots, b_n\}$ est exactement l'ensemble des éléments de $\mathcal{S}(R)$ qui minorent $b_1 + \dots + b_n$ (pour $\preceq$).
- c. En déduire que, si R vérifie de plus la condition (★), on a les assertions suivantes :
- (i) la décomposition obtenue en 4.d. est unique ;
 - (ii) $\mathcal{S}(R)$ est fini ;
 - (iii) $\mathcal{J}(R)$ est fini ;
 - (iv) $\mathcal{J}(R)$ muni de la loi $\cdot$ est isomorphe à l'ensemble des parties de $\mathcal{S}(R)$ muni de l'intersection ;
 - (v) $(\mathcal{J}(R), \cdot)$ est isomorphe à un produit $(\mathbb{Z}/2\mathbb{Z}, \cdot)^n$, où n est un entier qu'on précisera.
- d. Que peut-on dire du cardinal de $\mathcal{J}(R)$ lorsqu'on suppose que R est un anneau commutatif fini ? Ce résultat s'étend-il au cas non commutatif ?
- e. Application : déterminer les entiers ≤ 60 dont les images dans $\mathbb{Z}/60\mathbb{Z}$ constituent les éléments de $\mathcal{J}(\mathbb{Z}/60\mathbb{Z})$ et ceux de $\mathcal{S}(\mathbb{Z}/60\mathbb{Z})$.
- Indication :** On peut appliquer 4.c) du préliminaire.

PARTIE II

Pour tout anneau R , on pose $\mathcal{P}(R) = \{x \in R, \exists m \in \mathbb{N}, \exists n \in \mathbb{N}^*, x^{m+n} = x^m\}$. On définit comme suit deux applications μ, π de $\mathcal{P}(R)$ dans $\mathbb{N}$: pour a dans $\mathcal{P}(R)$, $\mu(a)$ est le plus petit entier m tel qu'il existe n non nul avec $a^{m+n} = a^m$, et $\pi(a)$ est le plus petit entier n non nul tel que $a^{\mu(a)+n} = a^{\mu(a)}$. On note $x \mid y$ la relation « x divise y » (dans $\mathbb{N}$ ou $\mathbb{Z}$).

1. a. Montrer que, si a est dans $\mathcal{P}(R)$ et que $a^{\mu(a)+r} = a^{\mu(a)+r'}$ où r, r' sont deux entiers positifs ou nuls strictement inférieurs à $\pi(a)$, alors r et r' sont égaux.
- b. Montrer que, pour a dans $\mathcal{P}(R)$ et m, n entiers avec n non nul, il y a équivalence entre :
 - (i) $a^{m+n} = a^m$
 - (ii) $\mu(a) \leq m$ et $\pi(a) \mid n$.

- c. Soit a dans R et k un entier non nul ; montrer que a^k est dans $\mathcal{P}(R)$ si, et seulement si, a est dans $\mathcal{P}(R)$ et montrer que, dans ce cas, on a les relations :

$$\mu(a^k) \leq \mu(a) \leq k\mu(a^k), \quad \pi(a^k) \mid \pi(a) \text{ et } \pi(a) \mid k\pi(a^k).$$

- d. Montrer que a est dans $\mathcal{P}(R)$ si, et seulement si, il existe k non nul tel que a^k est dans $\mathcal{P}(R)$; précisément, montrer que, si a est dans $\mathcal{P}(R)$ et k est un entier non nul, alors a^k est dans $\mathcal{P}(R)$ si, et seulement si, k vérifie :

$$\mu(a) \leq k \text{ et } \pi(a) \mid k.$$

En déduire que, si a est dans $\mathcal{P}(R)$, le plus petit entier k non nul tel que a^k est dans $\mathcal{P}(R)$ vérifie :

$$\sup(\mu(a), \pi(a)) \leq k \leq \mu(a) + \pi(a).$$

- e. Soit a un élément de $\mathcal{P}(R)$; montrer que a est inversible si, et seulement si, $\mu(a)$ est égal à 0. Montrer que, dans ce cas, $a^{-1} = a^{\pi(a)-1}$, et que $\pi(a)$ est exactement l'ordre de a en tant qu'élément du groupe multiplicatif $\mathfrak{U}(R)$.
- f. Montrer que, si R est fini, alors $\mathcal{P}(R) = R$ tout entier ; obtenir, pour a dans R , un majorant de la valeur de $\mu(a) + \pi(a)$ en fonction du cardinal de R .
2. a. Montrer que, si b et c sont deux éléments orthogonaux de R (c'est-à-dire $bc = cb = 0$), alors, pour tout entier n non nul, on a : $(b+c)^n = b^n + c^n$. En déduire que, si b et c sont dans $\mathcal{P}(R)$ et sont orthogonaux, alors $b+c$ est dans $\mathcal{P}(R)$ et on a :

$$\mu(b+c) \leq \sup(\mu(b), \mu(c)) \quad \text{et} \quad \pi(b+c) \mid \text{ppcm}(\pi(b), \pi(c)).$$

- b. Soit b un élément de $\mathcal{P}(R)$ tel que $\mu(b) \leq 1$; montrer que, pour tout entier k non nul, on a :

$$(b+1-b^{\pi(b)})^k = b^k + (1-b^{\pi(b)})^k = b^k + 1 - b^{\pi(b)}.$$

En déduire que $b+1-b^{\pi(b)}$ est dans $\mathfrak{U}(R)$ et que $\pi(b)$ est un diviseur du cardinal de $\mathfrak{U}(R)$ si celui-ci est fini.

- c. On pose : $\mathcal{N}(R) = \{x \in R; \exists m \in \mathbb{N}^*, x^m = 0\}$. Montrer que, si c est dans $\mathcal{N}(R)$, alors $1-c$ est dans $\mathfrak{U}(R)$; en déduire que, dans ce cas, $\mu(c)$ est inférieur ou égal au cardinal de $\mathfrak{U}(R)$ (si celui-ci est fini).
- d. Soit a un élément quelconque de $\mathcal{P}(R)$ et k un entier non nul tel que a^k est dans $\mathcal{P}(R)$; on pose :

$$b = a^{k+1} \quad \text{et} \quad c = a(1-a^k).$$

Montrer que b et c sont orthogonaux et appartiennent à $\mathcal{P}(R)$, que $\mu(b) \leq 1$ et que c est dans $\mathcal{N}(R)$. En déduire que, si le cardinal de $\mathfrak{U}(R)$ est un entier fini N , on a :

$$\mu(a) \leq N \quad \text{et} \quad \pi(a) \mid N.$$

Que dire de la majoration ainsi obtenue de $\pi(a)$ par N dans le cas où R est un corps fini ?