



المركز القومي للأمن للتربية والتكوين

جامعة الرباط-سلا-القنيطرة



Concours d'accès au cycle de préparation à l'agrégation de Mathématiques

Session Juillet 2017

épreuve d'algèbre et de géométrie

Durée 4 heures

Le sujet comporte 5 pages, en plus de cette page de garde.

Important

L'épreuve est constituée de deux problèmes. Le candidat est invité à bien mentionner les références complètes de chaque question traitée.

Les candidats sont tenus à rendre deux copies séparées même si elles sont vierges. La première contenant la résolution du problème 1 et la seconde contenant celle du problème 2. Dans chacune des deux copies on indiquera les références du candidat et le nombre d'intercalaires utilisés.

Il sera tenu compte dans l'appréciation des copies de la rigueur de votre raisonnement, de la clarté de la rédaction et du soin apporté à la présentation de votre copie. Le candidat peut utiliser les résultats énoncés dans les questions ou parties précédentes, il veillera toutefois à mentionner la référence du résultat utilisé.

Si le candidat repère ce qu'il pense être une erreur de l'énoncé, il le signale sur sa copie en expliquant les raisons qui l'ont amené à le penser. Ceci ne doit pas l'empêcher de finir son épreuve et il a le choix d'adopter les rectifications qu'il croit nécessaires ou pas.

Les calculatrices et tout matériel électronique ainsi que les documents sont interdits lors de cette épreuve.



Problème 1

Notations

Pour un ensemble fini F , on note $\text{card}(F)$ son cardinal. Pour $n \in \mathbb{N}$ tel que $n > 1$, on note I_n l'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ et N_n l'ensemble des éléments non inversibles.

Pour a et $b \in \mathbb{Z}$, " a divise b " est noté $a|b$, ce qui équivaut à : $\exists k \in \mathbb{Z}, b = ka$. Pour a et $b \in \mathbb{Z}$, le plus grand commun diviseur dans $\mathbb{N}$ de a et b est noté $\text{pgcd}(a, b)$.

Pour $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on désigne par $\bar{a}$ la classe de a dans l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$. Si p un nombre premier les ensembles $\mathbb{Z}/p\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\}$ seront notés respectivement $\mathbb{Z}_p$ et $\mathbb{Z}_p^*$.

Soit $(G, .)$ un groupe fini d'élément neutre 1_G . Soit $a \in G$. On appelle ordre de a , s'il existe et que l'on note $w(a)$, le plus petit élément de l'ensemble $\{k \in \mathbb{N}^* \mid a^k = 1_G\}$.

Un groupe G est dit cyclique, s'il est fini et engendré par un seul élément ($G = \{a^k, k \in \mathbb{Z}\}$).

Preliminaire

1. Soit $(G, .)$ un groupe fini d'élément neutre 1_G .

(a) Montrer que pour tout élément a de G , $w(a)$ existe et que $0 < w(a) \leq \text{card}(G)$.

(b) Montrer qu'un groupe G est cyclique, si et seulement si, il existe $a \in G$ tel que $\text{card}(G) = w(a)$.

Partie 1

- 2 . Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ tels que $n > 1$. Démontrer que $\bar{a}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ si et seulement si $\text{pgcd}(a, n) = 1$.
- 3 . Soit $n \in \mathbb{N}$ tel que $n > 1$. Montrer que $(I_n, \times)$ est un groupe commutatif.
- 4 . Sans justification, énumérer, dans un tableau ayant deux rangées, les éléments de I_{10} avec leurs ordres. Ce groupe $(I_{10}, \times)$ est-il cyclique ?
- 5 . Sans justification, énumérer, dans un tableau ayant deux rangées, les éléments de I_{12} avec leurs ordres. Ce groupe $(I_{12}, \times)$ est-il cyclique ?

Partie 2

Soit $n \in \mathbb{N}$ on dit que n est primaire lorsqu'il existe un nombre premier p et $\alpha \in \mathbb{N}^*$ tels que $n = p^\alpha$.

- 6 . Soit $n \in \mathbb{N}$ tel que $n > 1$ et n ne soit pas primaire.
- (a) Établir qu'il existe deux entiers, que l'on notera n_1 et n_2 tels que $n = n_1 n_2$, $1 < n_1 < n$ et $\text{pgcd}(n_1, n_2) = 1$.
- (b) Montrer que $\text{pgcd}((n_1 + n_2), n) = 1$.
- (c) Établir également que $\overline{n_1} \notin I_n$ et $\overline{n_2} \notin I_n$.

7 . On considère p un nombre premier, $\alpha \in \mathbb{N}^*$ et $k \in \mathbb{Z}$.
Prouver que : $\bar{k} \in N_{p^\alpha} \Leftrightarrow p | k$.

8 . Soit $n \in \mathbb{N}$ tel que $n > 1$.

Démontrer que N_n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si n est primaire.

Partie 3

Soit p un nombre premier impair, un élément $x \in \mathbb{Z}_p^*$ et un carré s'il existe $y \in \mathbb{Z}_p^*$ tel que $x = y^2$.

9 . Préciser l'ensemble I_p et donner la structure de $(\mathbb{Z}_p, +, \times)$

10 . Montrer qu'il y a exactement $\frac{p-1}{2}$ carrés dans $\mathbb{Z}_p^*$.

11 . Montrer que l'ensemble des carrés dans $\mathbb{Z}_p^*$ est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \bar{1}$.

12 . En déduire que $\overline{-1}$ est un carré dans $\mathbb{Z}_p$, si et seulement si, p est congru à 1 modulo 4.

13 . En déduire qu'il existe une infinité de nombres premiers de la forme $4n + 1$.

La suite de l'épreuve est à rédiger séparément !

Problème 2

Notations

On note $\mathbb{R}$ le corps des nombres réels, $\mathbb{Z}$ l'ensemble des entiers relatifs et $\mathbb{N}$ l'ensemble des entiers naturels. Si f est une fonction d'une variable réelle, on note $D(f)$ son domaine de définition. On désigne par $\mathbb{R}[X]$ l'espace vectoriel des polynômes à coefficients dans $\mathbb{R}$ et, pour tout $m \in \mathbb{N}$, on note $\mathbb{R}_m[X]$ le sous-espace vectoriel de $\mathbb{R}[X]$ des polynômes de degré inférieur ou égal à m . Si m est non nul dans $\mathbb{N}$, on note $\mathbb{R}^m$ l'espace vectoriel réel des m -uplets à coefficients dans $\mathbb{R}$, qui est souvent identifié à l'espace vectoriel réel $\mathcal{M}_{m,1}(\mathbb{R})$ des matrices à m lignes et une colonne, et à coefficients dans $\mathbb{R}$.

Tout au long du problème, on désigne par n un entier naturel non nul. L'algèbre réelle des matrices carrées d'ordre n à coefficients dans $\mathbb{R}$ est notée $\mathcal{M}_n(\mathbb{R})$. Le groupe des matrices inversibles de $\mathcal{M}_n(\mathbb{R})$ est noté $GL_n(\mathbb{R})$ et la matrice identité de $\mathcal{M}_n(\mathbb{R})$ est notée I . Si $U \in GL_n(\mathbb{R})$, on note U^{-1} son inverse. Une matrice diagonale D est notée $\text{diag}(\lambda_1, \dots, \lambda_n)$, où $\lambda_1, \dots, \lambda_n$ sont les coefficients diagonaux de D . On rappelle que $A \in \mathcal{M}_n(\mathbb{R})$ est **diagonalisable** s'il existe $U \in GL_n(\mathbb{R})$ et

$D \in \mathcal{M}_n(\mathbb{R})$ diagonale telles que $A = UDU^{-1}$. Une telle décomposition de A est dite diagonalisation de A . Pour une matrice $A \in \mathcal{M}_n(\mathbb{R})$, on note ${}^tA$ sa transposée et $Sp(A)$ l'ensemble de toutes ses valeurs propres réelles. Le sous-ensemble de $\mathcal{M}_n(\mathbb{R})$ des matrices symétriques est notée $\mathcal{S}_n(\mathbb{R})$ et celui des matrices orthogonales est noté $\mathcal{O}_n(\mathbb{R})$. Ainsi

$$\mathcal{S}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : {}^tA = A\} \text{ et } \mathcal{O}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : {}^tAA = I\}.$$

On rappelle que $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$. Une matrice $S \in \mathcal{S}_n(\mathbb{R})$ est dite **positive** si ${}^tXSX \geq 0$ pour tout $X \in \mathbb{R}^n$. En revanche, S est dite **définie positive** si ${}^tXSX > 0$ pour tout $X \in \mathbb{R}^n \setminus \{0\}$. Le sous-ensemble de $\mathcal{S}_n(\mathbb{R})$ des matrices positives est noté $\mathcal{S}_n^+(\mathbb{R})$ et celui des matrices définies positives est noté $\mathcal{S}_n^{++}(\mathbb{R})$.

Partie : I

1. Soit $M \in \mathcal{M}_n(\mathbb{R})$ et $U \in GL_n(\mathbb{R})$. Montrer que, pour tout $P \in \mathbb{R}[X]$,
 $P(UMU^{-1}) = UP(M)U^{-1}$.
2. Soient $m \in \mathbb{N}^*$ et $a_1, \dots, a_m \in \mathbb{R}$ deux à deux distincts. Montrer que l'application :

$$\begin{aligned} \varphi: \mathbb{R}_{m-1}[X] &\longrightarrow \mathbb{R}^m \\ P &\longmapsto (P(a_1), \dots, P(a_m)) \end{aligned}$$

est un isomorphisme.

Dans la suite de cette partie, f désigne une fonction réelle d'une variable réelle et A est une matrice diagonalisable de $\mathcal{M}_n(\mathbb{R})$ telle que $Sp(A)$ est contenu dans $D(f)$.

3. On note $\Pi(A, f) = \{P \in \mathbb{R}[X] : P(\lambda) = f(\lambda), \text{ pour tout } \lambda \in Sp(A)\}$.
 - a Montrer que $\Pi(A, f)$ n'est pas vide.
 - b Soient $A = U \text{diag}(\lambda_1, \dots, \lambda_n) U^{-1}$ une diagonalisation de A et $P \in \Pi(A, f)$. Établir l'égalité

$$P(A) = U \text{diag}(f(\lambda_1), \dots, f(\lambda_n)) U^{-1}.$$

- c En déduire que si $P, Q \in \Pi(A, f)$ alors $P(A) = Q(A)$.

Autrement dit, l'ensemble $\{P(A) : P \in \Pi(A, f)\}$ contient une seule matrice notée $f(A)$ tout au long du problème.

4. Montrer que $f(A)$ est diagonalisable et que $Sp(f(A)) = \{f(\lambda) : \lambda \in Sp(A)\}$.

Partie II : Quelques exemples

Soient f et g deux fonctions réelles d'une variable réelle.

5. Soit A une matrice diagonalisable de $\mathcal{M}_n(\mathbb{R})$ telle que $Sp(A) \subset D(f) \cap D(g)$. Montrer que si $f(\lambda) = g(\lambda)$ pour tout $\lambda \in Sp(A)$ alors $f(A) = g(A)$.

Dans la suite de cette partie, on suppose que f et g sont données respectivement par $f(x) = |x|$ et $g(x) = \sqrt{x}$. En outre, soit A une matrice diagonalisable de $\mathcal{M}_n(\mathbb{R})$.

6. Démontrer que $f(A)$ existe. Dans tout ce qui suit, $f(A)$ est notée $|A|$.
 7. Montrer que si $Sp(A) \subset \mathbb{R}^+$ alors $A = |A|$.
 8. A quelle condition la matrice $g(A)$ existe-t-elle ? Dans ce cas, on note $\sqrt{A}$ au lieu de $g(A)$.
 10. Vérifier que les deux matrices $\sqrt{A^2}$ et $\sqrt{|A|}$ existent.
 11. Établir les égalités $\sqrt{A^2} = |A| = \sqrt{|A|^2}$.

Partie III

12. Soit $S \in \mathcal{S}_n(\mathbb{R})$. Montrer que $S \in \mathcal{S}_n^{++}(\mathbb{R})$ si, et seulement si, il existe $O \in \mathcal{O}_n(\mathbb{R})$ et $\lambda_1, \dots, \lambda_n \in \mathbb{R}_+^*$ tels que $S = O \text{diag}(\lambda_1, \dots, \lambda_n) O^{-1}$.
 13. Soit $S \in \mathcal{S}_n^{++}(\mathbb{R})$.
 a Vérifier que $|S| = S$.
 b Montrer que $S \in GL_n(\mathbb{R})$ et que $S^{-1} \in \mathcal{S}_n^{++}(\mathbb{R})$.
 c Justifier l'existence de $\sqrt{A}$ et montrer que $\sqrt{S} \in \mathcal{S}_n^{++}(\mathbb{R})$.
 14. Montrer que l'application $\rho: \mathcal{S}_n^{++}(\mathbb{R}) \rightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est bijective et déterminer sa réciproque ρ^{-1} .

$$\begin{array}{ccc} \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{S}_n^{++}(\mathbb{R}) \\ S & \longmapsto & \sqrt{S} \end{array}$$

 15. En déduire que $\sqrt{S^{-1}} = \sqrt{S}^{-1}$ pour tout $S \in \mathcal{S}_n^{++}(\mathbb{R})$.
 16. Soit $A \in GL_n(\mathbb{R})$.
 a Montrer que ${}^tAA \in \mathcal{S}_n^{++}(\mathbb{R})$.
 b Montrer que $A\sqrt{{}^tAA}^{-1} \in \mathcal{O}_n(\mathbb{R})$.
 17. Soient $O, U \in \mathcal{O}_n(\mathbb{R})$ et $S, T \in \mathcal{S}_n^{++}(\mathbb{R})$ telles que $OS = UT$. Établir $S^2 = T^2$.
 18. En déduire que l'application :

$$\begin{array}{ccc} \pi: \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}) \\ (O, S) & \longmapsto & OS \end{array}$$

est une bijection.

Ainsi, pour tout $A \in GL_n(\mathbb{R})$, il existe un unique couple (O, S) de $\mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$ tel que $A = OS$. Cette égalité est appelée **la décomposition polaire** de A .

19. Soient $A \in GL_n(\mathbb{R})$ et $A = OS$ sa décomposition polaire. Montrer que ${}^tAA = S^2$.

Partie IV

Un sous-groupe G de $GL_n(\mathbb{R})$ est dit **groupe polaire** si les deux conditions suivantes sont vérifiées

- (i) G est stable par transposition (c'est à dire, ${}^tA \in G$ pour tout $A \in G$).
 (ii) G est stable par racine carrée (c'est à dire, si $S \in G \cap \mathcal{S}_n^{++}(\mathbb{R})$ alors $\sqrt{S} \in G$).

20. Soit G un groupe polaire. Montrer que G est stable par décomposition polaire (c'est à dire, si $A \in G$ et $A = OS$ est sa décomposition polaire, alors $O \in G$ et $S \in G$).
 Dans la suite de cette partie, on se donne $\alpha, \beta \in \{-1, 1\}$ et $J \in \mathcal{M}_n(\mathbb{R})$ tels que ${}^t J = \alpha J$ et $J^2 = \beta I$. On considère l'ensemble

$$G = \{A \in \mathcal{M}_n(\mathbb{R}) : {}^t A J A = J\}.$$

21. Vérifier que $\det(A) \in \{-1, 1\}$ pour tout $A \in G$, où $\det(A)$ est le déterminant de A .
 22. Soit $S \in G \cap \mathcal{S}_n^{++}(\mathbb{R})$.
 a Prouver que $P(S^{-1})J = JP(S)$, pour tout $P \in \mathbb{R}[X]$.
 b Établir l'existence de $Q \in \mathbb{R}[X]$ tel que $Q(S) = \sqrt{S}$ et $Q(S^{-1}) = \sqrt{S}^{-1}$.
 c En déduire que $\sqrt{S^{-1}}J = J\sqrt{S}$.
 23. Conclure que G est polaire.

Partie V : Groupe orthogonal et compacité

24. On note $tr(A)$ la trace d'une matrice $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que l'application

$$\begin{aligned} \varphi: \mathcal{M}_n^2(\mathbb{R}) &\longrightarrow \mathbb{R} \\ (A, B) &\longmapsto tr({}^t AB) \end{aligned}$$

est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.

On note $\|\cdot\|_2$ la norme euclidienne associée à ce produit scalaire (c'est à dire $\|A\|_2 = \sqrt{tr({}^t AA)}$, pour tout $A \in \mathcal{M}_n(\mathbb{R})$).

Dans le reste du problème, $\mathcal{M}_n(\mathbb{R})$ est muni de ce produit scalaire.

25. Montrer que l'application

$$\begin{aligned} T: \mathcal{M}_n(\mathbb{R}) &\longrightarrow \mathcal{M}_n(\mathbb{R}) \\ A &\longmapsto {}^t AA \end{aligned}$$

est continue et en déduire que $\mathcal{O}_n(\mathbb{R})$ est une partie compacte de $\mathcal{M}_n(\mathbb{R})$.

26. Soit G un sous-groupe de $GL_n(\mathbb{R})$. On suppose de plus que G contient $\mathcal{O}_n(\mathbb{R})$ et que c'est une partie compacte de $\mathcal{M}_n(\mathbb{R})$. On se donne $A \in G$ et on écrit sa décomposition polaire $A = OS$.
 a Montrer que $\{S^k : k \in \mathbb{Z}\}$ est une partie bornée de $\mathcal{M}_n(\mathbb{R})$.
 b En déduire que $Sp(S) = \{1\}$ et que $S = I$.
 c Que peut-on alors dire de G ?
 27. Soit $A \in \mathcal{M}_n(\mathbb{R})$ et $(A_k)_{k \in \mathbb{N}}$ une suite de $\mathcal{M}_n(\mathbb{R})$ donnée par $A_k = A - \frac{1}{k+1}I$.
 a Montrer que $(A_k)_{k \in \mathbb{N}}$ converge vers A .
 b Établir l'existence $k_0 \in \mathbb{N}$ tel que $A_k \in GL_n(\mathbb{R})$ pour tout $k \in \mathbb{N}$ avec $k \geq k_0$.
 c En déduire qu'il existe une suite $(O_k)_{k \in \mathbb{N}}$ de $\mathcal{O}_n(\mathbb{R})$ et une suite $(S_k)_{k \in \mathbb{N}}$ de $\mathcal{S}_n^{++}(\mathbb{R})$ telles que la suite $(C_k S_k)_{k \in \mathbb{N}}$ converge vers A .
 d Justifier l'existence d'une sous-suite de $(O_k)_{k \in \mathbb{N}}$ qui converge vers $O \in \mathcal{O}_n(\mathbb{R})$.
 e En déduire qu'il existe $S \in \mathcal{S}_n^+(\mathbb{R})$ telle que $A = OS$.

FIN DE L'ÉPREUVE