Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction est un facteur important d'appréciation des copies. Les candidats sont donc invités à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

Notations et vocabulaire

On note $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls, $\mathbb{Z}$ l'anneau des entiers relatifs, $\mathbb{Q}$ le corps des nombres rationnels, $\mathbb{R}$ le corps des nombres réels, $\mathbb{C}$ le corps des nombres complexes.

Dans toute la suite de ces notations, $\mathbb{K}$ désigne un corps.

Si E est un $\mathbb{K}$-espace vectoriel de dimension finie, la dimension de E sur $\mathbb{K}$ est notée $\dim_{\mathbb{K}}(E)$ et plus simplement $\dim(E)$ s'il n'y a pas d'ambiguïté.

Si E et F sont deux $\mathbb{K}$-espaces vectoriels, on note $\mathcal{L}(E,F)$ le $\mathbb{K}$-espace vectoriel des applications linéaires de E dans F. On note $\mathcal{L}(E)$ la $\mathbb{K}$-algèbre des endomorphismes de E, $\mathrm{GL}(E)$ le groupe des inversibles de $\mathcal{L}(E)$; les éléments de $\mathrm{GL}(E)$ sont les automorphismes du $\mathbb{K}$-espace vectoriel E. L'élément neutre de $\mathrm{GL}(E)$ est l'application identique de E, notée id_E.

Si E et F sont deux $\mathbb{K}$-espaces vectoriels et u un élément de $\mathcal{L}(E,F)$, on désigne par $\mathrm{Ker}(u)$ le noyau de u et par $\mathrm{Im}(u)$ l'image de u. Si E_1 est un sous-espace vectoriel de E et si F_1 est un sous-espace vectoriel de F contenant $u(E_1)$, on note $u_{|E_1}^{|F_1}$ l'élément de $\mathcal{L}(E_1,F_1)$ défini par

$$\forall x \in E_1, \qquad u_{|E_1}^{|F_1}(x) = u(x).$$

Si $E = F$ et si E_1 est un sous-espace vectoriel de E stable par u, c'est-à-dire tel que $u(E_1) \subset E_1$, on abrège $u_{|E_1}^{|E_1}$ en $u_{|E_1}$.

Si E est un $\mathbb{K}$-espace vectoriel non nul de dimension finie et u un endomorphisme de E, on note χ_u le polynôme caractéristique de u.

Si E est un $\mathbb{K}$-espace vectoriel, une partie $\mathcal{L}$ de $\mathcal{L}(E)$ est dite *commutative* si

$$\forall (u,v) \in \mathcal{L}^2, \qquad u \circ v = v \circ u.$$

Pour (r,s) dans $\mathbb{N}^{*2}$, on note $\mathcal{M}_{r,s}(\mathbb{K})$ le $\mathbb{K}$-espace vectoriel des matrices à r lignes et s colonnes à coefficients dans $\mathbb{K}$. Pour n dans $\mathbb{N}^*$, on note $\mathcal{M}_n(\mathbb{K})$ la $\mathbb{K}$-algèbre des matrices carrées à n lignes et n colonnes à coefficients dans $\mathbb{K}$, $\mathrm{GL}_n(\mathbb{K})$ le groupe des inversibles de $\mathcal{M}_n(\mathbb{K})$; les éléments de $\mathrm{GL}_n(\mathbb{K})$

sont les matrices inversibles de $\mathcal{M}_n(\mathbb{K})$. L'élément neutre de $\mathrm{GL}_n(\mathbb{K})$ est la matrice identité de $\mathcal{M}_n(\mathbb{K})$, notée I_n.

Pour n dans $\mathbb{N}^*$ et M dans $\mathcal{M}_n(\mathbb{K})$, on note χ_M le polynôme caractéristique de M.

Si n est un élément de $\mathbb{N}^*$, une partie $\mathcal{M}$ de $\mathcal{M}_n(\mathbb{K})$ est dite *commutative* si

$$\forall (M,N) \in \mathcal{M}^2, \qquad MN = NM.$$

Si n est un élément de $\mathbb{N}^*$, on note $\mathcal{T}_n(\mathbb{K})$ le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ constitué des matrices triangulaires supérieures, $\mathcal{T}_n^0(\mathbb{K})$ le sous-espace vectoriel de $\mathcal{T}_n(\mathbb{K})$ constitué des matrices triangulaires supérieures dont la diagonale est nulle.

Deux parties $\mathcal{P}$ et $\mathcal{P}'$ de $\mathcal{M}_n(\mathbb{K})$ sont dites *conjuguées dans* $\mathrm{GL}_n(\mathbb{K})$ s'il existe P dans $\mathrm{GL}_n(\mathbb{K})$ telle que

$$\mathcal{P}' = \{PMP^{-1} \ ; \ M \in \mathcal{P}\}.$$

Un *espace euclidien* est un couple $(E, \langle\ ,\ \rangle)$ où E est un $\mathbb{R}$-espace de dimension finie et $\langle\ ,\ \rangle$ un produit scalaire euclidien sur E. On note alors $\mathcal{O}(E)$ l'ensemble des isométries de $(E, \langle\ ,\ \rangle)$, c'est-à-dire des éléments u de $\mathcal{L}(E)$ tels que

$$\forall (x,y) \in E^2, \qquad \langle u(x), u(y)\rangle = \langle x, y\rangle .$$

On rappelle que $\mathcal{O}(E)$ est un sous-groupe de $\mathrm{GL}(E)$. On note $\mathrm{SO}(E)$ le sous-groupe de $\mathcal{O}(E)$ constitué des isométries de déterminant 1.

Pour n dans $\mathbb{N}^*$, on note $\mathcal{O}_n(\mathbb{R})$ l'ensemble des matrices orthogonales de $\mathcal{M}_n(\mathbb{R})$, c'est-à-dire des matrices M de $\mathcal{M}_n(\mathbb{R})$ telles que $M^TM = I_n$, où M^T désigne la transposée de la matrice M. On rappelle que $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. On note $\mathrm{SO}_n(\mathbb{R})$ le sous-groupe de $\mathcal{O}_n(\mathbb{R})$ constitué des matrices de $\mathcal{O}_n(\mathbb{R})$ de déterminant 1.

Pour θ dans $\mathbb{R}$, on introduit la matrice $R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

On rappelle que

$$\mathrm{SO}_2(\mathbb{R}) = \{R(\theta) \ ; \ \theta \in \mathbb{R}\}.$$

Deux parties $\mathcal{P}$ et $\mathcal{P}'$ de $\mathcal{M}_n(\mathbb{R})$ sont dites *conjuguées dans* $\mathcal{O}_n(\mathbb{R})$ s'il existe P dans $\mathcal{O}_n(\mathbb{R})$ telle que

$$\mathcal{P}' = \{PMP^{-1} \ ; \ M \in \mathcal{P}\}.$$

On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1 ; on rappelle que $\mathbb{U}$ est un sous-groupe du groupe $(\mathbb{C}^*, \times)$.

Pour n dans $\mathbb{N}^*$, on désigne par $\mathbb{U}_n$ le sous-groupe de $\mathbb{U}$ dont les éléments sont les racines n-ièmes de 1.

Un nombre complexe z est une *racine de l'unité* s'il existe n dans $\mathbb{N}^*$ tel que $z \in \mathbb{U}_n$.

Si x est un nombre réel, on note $\lfloor x \rfloor$ la partie entière de x, c'est-à-dire le plus grand entier relatif inférieur ou égal à x, et $\lceil x \rceil$ la partie entière supérieure de x, c'est-à-dire le plus petit entier relatif supérieur ou égal à x.

Organisation et buts du sujet

La partie **I** fait établir quelques résultats utilisés dans les parties **II** et **III**.

Les parties **II** et **III** sont indépendantes.

La partie **II** est consacrée aux sous-algèbres commutatives de dimension maximale de $\mathcal{M}_n(\mathbb{K})$.

La partie **III** est consacrée aux sous-groupes commutatifs finis de cardinal maximal de $\mathrm{GL}_n(\mathbb{Q})$.

I. Préliminaires

I.A. Commutation et trigonalisation simultanée

Dans les questions 1 à 3, $\mathbb{K}$ est un corps.

1. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.

   a) Soient u et v deux endomorphismes de E tels que $u \circ v = v \circ u$. Démontrer que, pour tout λ dans $\mathbb{K}$, $\mathrm{Ker}(u - \lambda \mathrm{id}_E)$ est stable par v. Plus généralement, démontrer que, pour P dans $\mathbb{K}[X]$, le sous-espace vectoriel $\mathrm{Ker}(P(u))$ de E est stable par v.

   b) Soit $\mathcal{L}$ une partie commutative de $\mathcal{L}(E)$ dont tous les éléments sont des endomorphismes trigonalisables de E. On suppose qu'au moins un élément de $\mathcal{L}$ n'est pas une homothétie. Démontrer qu'il existe un sous-espace vectoriel F de E, non nul et différent de E, stable par tous les éléments de $\mathcal{L}$.

2. Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, $\mathcal{L}$ une partie commutative de $\mathcal{L}(E)$ dont tous les éléments sont des endomorphismes trigonalisables de E, F un sous-espace vectoriel de E non nul, distinct de E et stable par tous les éléments de $\mathcal{L}$.

   On note $n = \dim(E), m = \dim(F)$. On a donc $1 \leq m \leq n-1$ et $n \geq 2$. On fixe une base $(e_1, \ldots, e_m)$ de F, que l'on complète en une base $e = (e_1, \ldots, e_n)$ de E.

   a) Justifier que, pour tout élément u de $\mathcal{L}$, la matrice M_u de u dans la base e s'écrit

   $$M_u = \begin{pmatrix} A_u & B_u \\ 0 & C_u \end{pmatrix} \quad \text{où} \quad (A_u, B_u, C_u) \in \mathcal{M}_m(\mathbb{K}) \times \mathcal{M}_{m,n-m}(\mathbb{K}) \times \mathcal{M}_{n-m}(\mathbb{K}).$$

   Pour (u, v) dans $\mathcal{L}^2$, établir les relations

   $$A_u A_v = A_v A_u \qquad \text{et} \qquad C_u C_v = C_v C_u.$$

   b) Soit u dans $\mathcal{L}$. Calculer χ_u en fonction de χ_{A_u} et de χ_{C_u}. En déduire que les matrices A_u et C_u sont trigonalisables.

3. a) En raisonnant par récurrence, démontrer que, pour tout élément n de $\mathbb{N}^*$, pour tout $\mathbb{K}$-espace vectoriel E de dimension n et toute partie commutative $\mathcal{L}$ de $\mathcal{L}(E)$ dont tous les éléments sont des endomorphismes trigonalisables de E, il existe une base e de E telle que, pour tout u de $\mathcal{L}$, la matrice de u dans e appartienne à $\mathcal{T}_n(\mathbb{K})$.

   On demande de rédiger très précisément la démonstration par récurrence.

   b) Soit n un entier supérieur ou égal à 2. Expliciter un couple (A, B) de $\mathcal{T}_n(\mathbb{K})^2$ tel que $AB \neq BA$. La réciproque de la propriété démontrée dans la question a) est-elle exacte ?

   c) Soient n dans $\mathbb{N}^*$, E un $\mathbb{K}$-espace vectoriel de dimension n, $u_1, \ldots, u_n$ des endomorphismes nilpotents de E qui commutent deux à deux. Calculer $u_n \circ \cdots \circ u_1$.

4. Soient E un $\mathbb{R}$-espace vectoriel non nul de dimension finie, $\mathcal{L}$ une partie commutative de $\mathcal{L}(E)$. Démontrer qu'il existe une droite ou un plan de E stable par tous les éléments de $\mathcal{L}$.

   Indication. On pourra fixer une base e de E, considérer les matrices des éléments de $\mathcal{L}$ dans e comme des matrices complexes, justifier que ces matrices ont un vecteur propre complexe commun et décomposer ce vecteur en partie réelle et partie imaginaire.

I.B. Sous-groupes abéliens de $\mathcal{O}_2(\mathbb{R})$

5. Soit n dans $\mathbb{N}^*$.

   a) Démontrer que $\mathbb{U}_n$ est le seul sous-groupe d'ordre n de $\mathbb{U}$.

   b) Expliciter, sans détailler la vérification, un isomorphisme de groupes de $\mathbb{U}$ sur $\mathrm{SO}_2(\mathbb{R})$. Démontrer que le groupe $\mathrm{SO}_2(\mathbb{R})$ admet exactement un sous-groupe d'ordre n, que l'on note $\mathcal{R}_n$, dont on écrira les éléments.

6. a) Soit O dans $\mathcal{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$. Justifier que O est conjuguée dans $\mathcal{O}_2(\mathbb{R})$ à $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

   Déterminer le centralisateur $C(S)$ de S dans $\mathcal{O}_2(\mathbb{R})$, i.e. le sous-groupe de $\mathcal{O}_2(\mathbb{R})$ constitué des éléments de $\mathcal{O}_2(\mathbb{R})$ qui commutent à S.

   b) Démontrer que les sous-groupes commutatifs de $\mathcal{O}_2(\mathbb{R})$ sont les sous-groupes de $\mathrm{SO}_2(\mathbb{R})$ et les sous-groupes de $\mathcal{O}_2(\mathbb{R})$ conjugués dans $\mathcal{O}_2(\mathbb{R})$ à l'un des deux sous-groupes

   $$\{I_2, S\} \qquad \text{et} \qquad \{I_2, S, -I_2, -S\}.$$

7. Soit A la matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

   a) Démontrer qu'il existe P dans $\mathrm{GL}_2(\mathbb{R})$ telle que $R\left(\frac{\pi}{3}\right) = PAP^{-1}$.

   b) Démontrer que le sous-groupe $\mathcal{R}_6$ de $\mathrm{SO}_2(\mathbb{R})$, défini à la question 5.b), est conjugué dans $\mathrm{GL}_2(\mathbb{R})$ à un sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$.

II. Sous-algèbres commutatives de dimension maximale de $\mathcal{M}_n(\mathbb{K})$

Dans toute cette partie **II**, n est un élément de $\mathbb{N}^*$, $\mathbb{K}$ un corps.

Si n est pair, on écrit $n = 2m$ où $m \in \mathbb{N}^*$. L'ensemble des matrices de la forme $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$, où A parcourt $\mathcal{M}_m(\mathbb{K})$, est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$, que l'on note $\mathcal{V}_n(\mathbb{K})$. On ne demande pas de le justifier.

Si n est impair et supérieur ou égal à 3, on écrit $n = 2m+1$ où $m \in \mathbb{N}^*$. L'ensemble des matrices de la forme $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$, où A parcourt $\mathcal{M}_{m,m+1}(\mathbb{K})$ (respectivement $\mathcal{M}_{m+1,m}(\mathbb{K})$) est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$, que l'on note $\mathcal{V}_n^1(\mathbb{K})$ (respectivement $\mathcal{V}_n^2(\mathbb{K})$). On ne demande pas de le justifier.

Si n est pair, on pose

$$\mathcal{A}_n(\mathbb{K}) = \{\lambda I_n + M \ ; \ \lambda \in \mathbb{K}, \ M \in \mathcal{V}_n(\mathbb{K})\}.$$

Si n est impair et supérieur ou égal à 3, on pose, pour i dans $\{1, 2\}$,

$$\mathcal{A}_n^i(\mathbb{K}) = \{\lambda I_n + M \ ; \ \lambda \in \mathbb{K}, \ M \in \mathcal{V}_n^i(\mathbb{K})\}.$$

Pour ℓ dans $\mathbb{N}^*$, on pose $b(\ell) = \left\lfloor \frac{\ell^2}{4} \right\rfloor$.

II.A. Les sous-algèbres $\mathcal{A}_n(\mathbb{K})$, $\mathcal{A}_n^i(\mathbb{K})$

8. a) Justifier que, si n est pair, la dimension de $\mathcal{V}_n(\mathbb{K})$ est $b(n)$ et que, si n est impair supérieur ou égal à 3 et i est dans $\{1,2\}$, la dimension de $\mathcal{V}_n^i(\mathbb{K})$ est $b(n)$.

   b) Si n est pair et si M et M' sont dans $\mathcal{V}_n(\mathbb{K})$, que vaut $M'M$? Même question si n est impair supérieur ou égal à 3, si i est dans $\{1,2\}$ et si M et M' sont dans $\mathcal{V}_n^i(\mathbb{K})$.

Dans les questions 9 et 10, $\mathcal{V}$ est un sous-espace vectoriel de $\mathcal{T}_n(\mathbb{K})$ tel que

$$\forall (M, M') \in \mathcal{V}^2, \qquad M'M = 0.$$

On note $d = \dim(\mathcal{V})$ et on pose

$$\mathcal{A} = \{\lambda I_n + M \ ; \ \lambda \in \mathbb{K}, \ M \in \mathcal{V}\}.$$

9. a) Vérifier que $\mathcal{A}$ est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$. Exprimer $\dim(\mathcal{A})$ en fonction de d.

   b) Démontrer que le groupe des éléments inversibles de $\mathcal{A}$ est

   $$\mathcal{A}^\times = \{\lambda I_n + M \ ; \ (\lambda, M) \in \mathbb{K}^* \times \mathcal{V}\}.$$

   c) Démontrer que $\mathcal{V}$ est le seul idéal de la $\mathbb{K}$-algèbre commutative $\mathcal{A}$ différent de $\mathcal{A}$ et qu'il est maximal pour l'inclusion parmi les idéaux de $\mathcal{A}$ différent de $\mathcal{A}$.

10. a) Démontrer que le groupe $(\mathcal{A}^\times, .)$ est isomorphe au produit direct du groupe $(\mathbb{K}^*, \times)$ par le groupe $(\mathbb{K}^d, +)$.

    b) Soient p un nombre premier, r un élément de $\mathbb{N}^*$, $q = p^r$, $\mathbb{F}_q$ un corps de cardinal q.

    Démontrer que, si $\mathbb{K} = \mathbb{F}_q$, le groupe $(\mathcal{A}^\times, .)$ des éléments inversibles de $\mathcal{A}$ est isomorphe au produit direct du groupe $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$ par le groupe $((\mathbb{Z}/p\mathbb{Z})^{rd}, +)$.

    Indication. On rappelle que le groupe multiplicatif d'un corps fini est cyclique.

II.B. Sous-espaces vectoriels commutatifs de matrices nilpotentes

Le but de cette sous-partie **II.B** est d'établir le résultat suivant.

Théorème 1.
(i) La dimension maximale d'un sous-espace vectoriel commutatif de $\mathcal{M}_n(\mathbb{K})$ dont les éléments sont des matrices nilpotentes est $b(n)$.

(ii) Si $n \geq 4$, tout sous-espace vectoriel commutatif de $\mathcal{M}_n(\mathbb{K})$ dont les éléments sont des matrices nilpotentes et dont la dimension est $b(n)$ est conjugué dans $\mathrm{GL}_n(\mathbb{K})$ au sous-espace $\mathcal{V}_n(\mathbb{K})$ si n est pair, à l'un des deux sous-espaces $\mathcal{V}_n^1(\mathbb{K})$, $\mathcal{V}_n^2(\mathbb{K})$ si n est impair.

Soient E un $\mathbb{K}$-espace vectoriel de dimension n, $\mathcal{V}$ un sous-espace vectoriel commutatif de $\mathcal{L}(E)$ dont les éléments sont des endomorphismes nilpotents de E.

On note F le sous-espace vectoriel de E engendré par les images des éléments de $\mathcal{V}$, i.e. le sous-espace des éléments de E de la forme $\sum_{i=1}^{r} u_i(x_i)$ où r parcourt $\mathbb{N}^*$, $(u_1, \dots, u_r)$ parcourt $\mathcal{V}^r$ et $(x_1, \dots, x_r)$ parcourt E^r.

Soient S un sous-espace vectoriel supplémentaire de F dans E, Ψ l'application de $\mathcal{V}$ dans $\mathcal{L}(S, F)$ définie par

$$\forall u \in \mathcal{V}, \qquad \Psi(u) = u|_S^F.$$

L'application Ψ est linéaire ; on ne demande pas de justifier ce point.

11. a) Démontrer que l'application Ψ est injective.

    Indication. On pourra déterminer le noyau de Ψ en s'aidant de la question 3.c).

    b) Démontrer que

    $$\dim(\mathcal{V}) \leq \dim(F)\ (n - \dim(F)) \leq b(n).$$

On a ainsi établi l'item *(i)* du théorème 1.

Dans les questions 12 et 13, on suppose que $\mathcal{V}$ est de dimension $b(n)$ et que $n \geq 4$.

On note $d = \dim(S)$.

12. a) Démontrer que l'application Ψ est un isomorphisme de $\mathbb{K}$-espaces vectoriels.

    b) Démontrer que, si $n = 2m$ avec m dans $\mathbb{N}^* \setminus \{1\}$, alors $d = m$, et que, si $n = 2m + 1$ avec m dans $\mathbb{N}^* \setminus \{1\}$, alors d appartient à $\{m, m + 1\}$.

En particulier, on a donc $d \geq 2$.

13. On se propose d'établir que

    $$\forall (u, u') \in \mathcal{V}^2, \qquad u' \circ u = 0.$$

    Raisonnant par l'absurde, on suppose qu'il existe u et u' dans $\mathcal{V}$ tels que $u' \circ u \neq 0$.

    a) Justifier l'existence de x_1 dans S tel que $u' \circ u(x_1) \neq 0$.

    b) On complète x_1 en une base $(x_1, \dots, x_d)$ de S. Démontrer qu'il existe v et v' dans $\mathcal{V}$ tels que

    $$v(x_1) = u'(x_2), \quad v(x_2) = 0, \qquad v'(x_1) = 0, \quad v'(x_2) = u(x_1).$$

    c) Démontrer que v et v' ne commutent pas et conclure.

14. Établir l'item *(ii)* du théorème 1.

II.C. Sous-algèbres commutatives de $\mathcal{M}_n(\mathbb{K})$

Le but de cette sous-partie **II.C** est d'établir le résultat suivant.

Théorème 2.
(i) La dimension maximale d'une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$ est $b(n)+1$.

(ii) Si $n \geq 4$, toute sous-algèbre commutative de dimension $b(n)+1$ de $\mathcal{M}_n(\mathbb{K})$ est conjuguée dans $\mathrm{GL}_n(\mathbb{K})$ à la sous-algèbre $\mathcal{A}_n(\mathbb{K})$ si n est pair, à l'une des deux sous-algèbres $\mathcal{A}_n^1(\mathbb{K})$, $\mathcal{A}_n^2(\mathbb{K})$ si n est impair.

15. Soient n_1 et n_2 deux éléments de $\mathbb{N}^*$ tels que $n_1 \leq n_2$. Démontrer que

$$(b(n_1)+1)+(b(n_2)+1) \leq b(n_1+n_2)+1.$$

Dans la suite de cette sous-partie II.C, on pourra utiliser sans démonstration le résultat suivant.
Si r est un entier supérieur ou égal à 2, si $n_1 \leq \cdots \leq n_r$ sont des éléments de $\mathbb{N}^*$, alors

$$\sum_{i=1}^{r}(b(n_i)+1) \leq b\left(\sum_{i=1}^{r} n_i\right)+1,$$

avec égalité si et seulement si $r=2$, $n_1=n_2=1$, ou $r=2$, $n_1=1$ et $n_2=2$.

16. On suppose que $\mathbb{K}$ est algébriquement clos.

    a) Démontrer que, pour tout $\mathbb{K}$-espace vectoriel E non nul de dimension finie et toute sous-algèbre commutative $\mathcal{A}$ de $\mathcal{L}(E)$, il existe un élément r de $\mathbb{N}^*$, des sous-espaces vectoriels $E_1, \ldots, E_r$ non nuls de E vérifiant les conditions suivantes :

    - pour tout i de $[\![1,r]\!]$, E_i est stable par tout élément de $\mathcal{A}$;

    - on a $E = \bigoplus_{i=1}^{r} E_i$;

    - pour tout élément u de $\mathcal{A}$ et tout i de $[\![1,r]\!]$, l'endomorphisme $u_{|E_i}$ de E_i est de la forme $\lambda_i(u)\mathrm{id}_{E_i} + \nu_i(u)$ où $\lambda_i(u)$ est un élément de $\mathbb{K}$ et où $\nu_i(u)$ est un élément nilpotent de $\mathcal{L}(E_i)$.

    b) Établir le théorème 2 sous l'hypothèse « $\mathbb{K}$ est algébriquement clos ».

17. On ne suppose plus que $\mathbb{K}$ est algébriquement clos. Soit Ω une extension algébriquement close de $\mathbb{K}$: $\mathbb{K}$ est un sous-corps du corps algébriquement clos Ω.

    Soient $\mathcal{A}$ une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$ de dimension m, $(U_i)_{i\in[\![1,m]\!]}$ une base du $\mathbb{K}$-espace vectoriel $\mathcal{A}$, $\mathcal{A}_\Omega$ le Ω-sous-espace vectoriel de $\mathcal{M}_n(\Omega)$ engendré par $(U_i)_{i\in[\![1,m]\!]}$.

    a) Démontrer que $\mathcal{A}_\Omega$ est une Ω-sous-algèbre commutative de $\mathcal{M}_n(\Omega)$ de dimension m.

    D'après la question 16.b), on a donc $m \leq b(n)+1$.

    Dans les questions b) à d) on suppose que $m = b(n)+1$ et que $n \geq 4$.

b) Démontrer que $\mathcal{A}$ contient une matrice non inversible et non nulle.

Indication. On pourra s'intéresser à l'intersection de $\mathcal{A}$ et du sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ constitué des matrices dont la première colonne est nulle.

c) Soit M dans $\mathcal{A}$. D'après l'item *(ii)* du théorème 2 appliqué au corps algébriquement clos Ω, la matrice M s'écrit $\lambda I_n + N$ où λ est un élément de Ω et où N est une matrice nilpotente de $\mathcal{M}_n(\Omega)$. Soit C une matrice de $\mathcal{A}$ non nulle et non inversible.

Établir l'égalité $(M - \lambda I_n)C = 0$. En déduire que λ appartient à $\mathbb{K}$ et N à $\mathcal{M}_n(\mathbb{K})$.

d) Établir le théorème 2.

II.D. Cardinal maximal d'un sous-groupe abélien de $\mathrm{GL}_n(\mathbb{F}_q)$

On fixe un nombre premier p, deux éléments d et n de $\mathbb{N}^*$, avec $n \geq 4$. On pose $q = p^d$ et on note $\mathbb{F}_q$ un corps de cardinal q.

On note

$$\beta_q(n) = (q-1)\, q^{b(n)}.$$

On remarquera que, grâce à l'étude menée dans la sous-partie **II.A**, on dispose des résultats suivants, que l'on ne demande pas de justifier :

- si n est pair, le groupe des inversibles de $\mathcal{A}_n(\mathbb{F}_q)$ est un sous-groupe commutatif de $\mathrm{GL}_n(\mathbb{F}_q)$ de cardinal $\beta_q(n)$;

- si n est impair, les groupes des inversibles de $\mathcal{A}_n^1(\mathbb{F}_q)$ et $\mathcal{A}_n^2(\mathbb{F}_q)$ sont des sous-groupes commutatifs de $\mathrm{GL}_n(\mathbb{F}_q)$ de cardinal $\beta_q(n)$.

Le but de cette sous-partie **II.D** est d'établir le résultat suivant.

Théorème 3. *Supposons que $n \geq 4$.*

(i) Le cardinal maximal d'un sous-groupe abélien fini de $\mathrm{GL}_n(\mathbb{F}_q)$ est $\beta_q(n)$.

(ii) Tout sous-groupe abélien de $\mathrm{GL}_n(\mathbb{F}_q)$ de cardinal $\beta_q(n)$ est conjugué dans $\mathrm{GL}_n(\mathbb{F}_q)$ au groupe des inversibles de $\mathcal{A}_n(\mathbb{F}_q)$ si n est pair, au groupe des inversibles de $\mathcal{A}_n^1(\mathbb{F}_q)$ ou au groupe des inversibles de $\mathcal{A}_n^2(\mathbb{F}_q)$ si n est impair.

18. Soient G un sous-groupe commutatif de $\mathrm{GL}_n(\mathbb{F}_q)$, V_G le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{F}_q)$ engendré par G, d_G la dimension de ce sous-espace.

    a) Démontrer que V_G est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{F}_q)$ et que $|G| \leq q^{d_G} - 1$.

    b) On suppose que le sous-groupe G est de cardinal maximal parmi les sous-groupes commutatifs de $\mathrm{GL}_n(\mathbb{F}_q)$ et que $n \geq 4$.

    Démontrer que $d_G = b(n) + 1$, puis que $|G| = \beta_q(n)$. En déduire le théorème 3.

III. Sous-groupe abéliens finis de $\mathrm{GL}_n(\mathbb{Q})$ de cardinal maximal

Pour n dans $\mathbb{N}^*$, on pose $c(n) = 6^{\frac{n}{2}}$ si n est pair, $c(n) = 2.\,6^{\frac{n-1}{2}}$ si n est impair.

Le but de cette partie **III** est d'établir le théorème suivant.

Théorème 4. *Soit n dans $\mathbb{N}^*$.*

(i) L'ensemble des cardinaux des sous-groupes commutatifs finis de $\mathrm{GL}_n(\mathbb{Q})$ a pour maximum $c(n)$.

(ii) Deux sous-groupes de $\mathrm{GL}_n(\mathbb{Q})$ de cardinal $c(n)$ sont conjugués dans $\mathrm{GL}_n(\mathbb{Q})$.

III.A. Irréductibilité des polynômes cyclotomiques

Un nombre complexe z est dit *algébrique* si l'idéal annulateur $I_z = \{P \in \mathbb{Q}[X]\ ;\ P(z) = 0\}$ n'est pas nul. Si tel est le cas, on note Π_z le générateur unitaire de cet idéal, i.e. le polynôme minimal de z sur $\mathbb{Q}$; on rappelle que Π_z est un irréductible de l'anneau $\mathbb{Q}[X]$.

Si z est un nombre complexe, on dit que z est un *entier algébrique* s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(z) = 0$. Les entiers algébriques sont donc en particulier des nombres complexes algébriques. On note $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques.
Pour n dans $\mathbb{N}^*$, on pose

$$\mu_n = \left\{\exp\left(\frac{2ik\pi}{n}\right)\ ;\ k \in [\![1, n]\!],\ k \wedge n = 1\right\} \quad \text{et} \quad \Phi_n = \prod_{z \in \mu_n} (X - z)\,.$$

19. Soit n dans $\mathbb{N}^*$.

    a) Démontrer que μ_n est l'ensemble des éléments d'ordre n du groupe $\mathbb{U}$.

    b) Soit D_n l'ensemble des diviseurs de n dans $\mathbb{N}^*$. Établir l'égalité $X^n - 1 = \prod_{d \in D_n} \Phi_d$.

    c) Démontrer que Φ_n appartient à $\mathbb{Z}[X]$.

Dans toute la suite de cette sous-partie III.A, on pourra utiliser sans démonstration le fait que $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.

20. a) Démontrer que $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Que peut-on en déduire si a et b sont deux éléments non nuls de $\mathbb{Z}$ tels que a divise b dans $\overline{\mathbb{Z}}$?

    b) Soit z dans $\overline{\mathbb{Z}}$. Démontrer que Π_z appartient à $\mathbb{Z}[X]$.

    Indication. On pourra établir que les coefficients de Π_z sont des éléments de $\overline{\mathbb{Z}} \cap \mathbb{Q}$.

21. Si P est un élément de $\mathbb{C}[X]$ unitaire de degré d appartenant à $\mathbb{N}^*$ qui se factorise sous la forme $P = \prod_{k=1}^{d}(X - z_k)$ où les z_k sont dans $\mathbb{C}$, on pose

$$\Delta(P) = \prod_{1 \leq k < \ell \leq d} (z_\ell - z_k)^2.$$

a) Avec les notations précédentes, démontrer que

$$\Delta(P) = (-1)^{\frac{d(d-1)}{2}} \prod_{k=1}^{d} P'(z_k).$$

b) Soit n dans $\mathbb{N}^*$. Démontrer qu'il existe ε_n dans $\{-1, 1\}$ tel que $\Delta(X^n - 1) = \varepsilon_n\, n^n$.

22. a) Soient d un entier tel que $d \geq 2$, U l'élément $U = \prod_{1 \leq k < \ell \leq d} (X_\ell - X_k)$ de $\mathbb{Z}[X_1, \ldots, X_d]$.

Si σ est une permutation de l'ensemble $[\![1, d]\!]$, exprimer $U(X_{\sigma(1)}, \ldots X_{\sigma(d)})$ en fonction de la signature $\varepsilon(\sigma)$ de σ et de $U(X_1, \ldots, X_d)$.

b) Soient $\mathbb{A}$ un sous-anneau de $\mathbb{C}$, P dans $\mathbb{A}[X]$ un polynôme unitaire non constant, d le degré de P. Démontrer que $\Delta(P)$ appartient à $\mathbb{A}$.

Indication. Si $m \in [\![1, d]\!]$, soit $\Sigma_m = \sum_{1 \leq i_1 < i_2 < \cdots < i_m \leq d} X_{i_1} X_{i_2} \ldots X_{i_m}$. On pourra utiliser sans démonstration le fait suivant : si V est un élément de $\mathbb{Z}[X_1, \ldots, X_d]$ tel que, pour toute permutation σ de $[\![1, d]\!]$,

$$V(X_{\sigma(1)}, \ldots, X_{\sigma(d)}) = V(X_1, \ldots, X_d),$$

alors il existe un élément W de $\mathbb{Z}[X_1, \ldots, X_d]$ tel que $V(X_1, \ldots, X_d) = W(\Sigma_1, \ldots, \Sigma_d)$.

23. Soient n dans $\mathbb{N}^*$, z dans μ_n et p un nombre premier.

a) Démontrer que, pour P dans $\mathbb{Z}[X]$, $P(X^p) - P(X)^p$ appartient à $p\,\mathbb{Z}[X]$.

En déduire que $\Pi_z(z^p)$ appartient à $p\,\overline{\mathbb{Z}}$.

b) Démontrer que, si $\Pi_z(z^p) \neq 0$, p divise n dans $\overline{\mathbb{Z}}$.

24. a) Soit n dans $\mathbb{N}^*$. Démontrer que le polynôme Φ_n est irréductible sur $\mathbb{Q}$.

b) Soit P un polynôme non constant de $\mathbb{Q}[X]$. On suppose que les racines de P dans $\mathbb{C}$ sont des racines de l'unité et que P admet au moins une racine différente de 1. Démontrer que P admet au moins une racine de la forme $\exp(i\theta)$ avec θ dans $\left[\frac{\pi}{3}, \pi\right]$.

III.B. Sous-groupe abéliens finis de $\mathcal{O}_n(\mathbb{R})$

Soient $(E, \langle\ ,\ \rangle)$ un espace euclidien non nul, $\|\ \|$ la norme euclidienne associée à $\langle\ ,\ \rangle$. Pour u dans $\mathcal{L}(E)$, on pose

$$\|u\|_{\mathrm{op}} = \sup\{\|u(x)\|\ ;\ x \in E,\ \|x\| = 1\}.$$

L'application $u \mapsto \|u\|_{\mathrm{op}}$ est une norme sur $\mathcal{L}(E)$.

25. On suppose dans cette question 25 que E est de dimension 2 et on oriente E.

Soient θ dans $[0, 2\pi[$, r_θ la rotation d'angle θ du plan euclidien orienté ainsi défini. Exprimer le nombre réel $\|r_\theta - \mathrm{id}_E\|_{\mathrm{op}}$ en fonction de $\sin\left(\frac{\theta}{2}\right)$.

Dans la suite de cette sous-partie **III.B**, G est un sous-groupe commutatif de $\mathcal{O}(E)$.

26. Démontrer que l'on peut écrire une décomposition en somme directe orthogonale

$$E = D_1 \overset{\perp}{\oplus} \ldots \overset{\perp}{\oplus} D_k \overset{\perp}{\oplus} P_1 \ldots \overset{\perp}{\oplus} P_\ell$$

où (k, ℓ) est dans $\mathbb{N}^2$, où $D_1, \ldots, D_k$ sont des droites stables par tous les éléments de G, $P_1, \ldots, P_\ell$ des plans stables par tous les éléments de G, et où, pour tout j dans $[\![1, \ell]\!]$ et tout g de G, l'endomorphisme $g_{|P_j}$ de P_j appartient à $\mathrm{SO}(P_j)$.

Dans la suite de cette sous-partie **III.B**, on suppose que G est fini.

On pose

$$V = \bigoplus_{i=1}^{k} D_i \quad \text{et} \quad W = \bigoplus_{j=1}^{\ell} P_j.$$

On note $G_0 = \{g \in G \ ; \ g_{|V} = \mathrm{id}_V\}$. L'ensemble G_0 est un sous-groupe de G, la justification de ce point n'est pas demandée.

27. a) Démontrer que $|G|$ divise $2^k \, |G_0|$.

On suppose dans la suite de cette question 27 que $G_0 \neq \{\mathrm{id}_E\}$.

On pose $\varepsilon = \min\{\|g - \mathrm{id}_E\|_{\mathrm{op}} \ ; \ g \in G_0 \setminus \{\mathrm{id}_E\}\}$.

b) Démontrer que ε appartient à $]0, 2]$ et que, pour tout couple (g, g') d'éléments distincts de G,

$$\|g - g'\|_{\mathrm{op}} \geq \varepsilon.$$

c) Démontrer que $|G_0| \leq \left\lceil \dfrac{\pi}{\mathrm{Arcsin}\left(\frac{\varepsilon}{2}\right)} \right\rceil^{\ell}$.

28. On suppose dans cette question 28 que, pour tout g dans G, le polynôme caractéristique χ_g de g appartient à $\mathbb{Q}[X]$. Démontrer que $|G_0| \leq 6^\ell$.

III.C. Sous-groupes abéliens finis de $\mathbf{GL}_n(\mathbb{Q})$

29. Soient n dans $\mathbb{N}^*$, G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{R})$. Démontrer que G est conjugué dans $\mathrm{GL}_n(\mathbb{R})$ à un sous-groupe de $\mathcal{O}_n(\mathbb{R})$.

Indication. On pourra partir d'un produit scalaire quelconque $\langle \ , \ \rangle$ et considérer l'application

$$B \ : (x, y) \in \mathbb{R}^n \times \mathbb{R}^n \longmapsto \sum_{g \in G} \langle g(x), g(y) \rangle \, .$$

30. a) Établir le point *(i)* du théorème 4.

b) Établir le point *(ii)* du théorème 4.

Indication. On pourra admettre sans démonstration le fait suivant : deux parties de $\mathcal{M}_n(\mathbb{Q})$ conjuguées dans $\mathrm{GL}_n(\mathbb{R})$ sont conjuguées dans $\mathrm{GL}_n(\mathbb{Q})$.