

Problème 1

Notations et rappels

Dans tout le sujet, n désigne un entier naturel non nul et E un $\mathbb{C}$ -espace vectoriel de dimension n .

Si $M \in \mathcal{M}_n(\mathbb{C})$, on note M^T la transposée de M .

Si M est une matrice de $\mathcal{M}_n(\mathbb{C})$, on définit la suite des puissances de M par $M^0 = I_n$ et, pour tout entier naturel k , par la relation $M^{k+1} = M M^k$.

De même, si u est un endomorphisme de E , on définit la suite des puissances de u par $u^0 = \text{Id}_E$ et, pour tout entier naturel k , par la relation $u^{k+1} = u \circ u^k$.

Une matrice M est dite nilpotente s'il existe un entier naturel $k \geq 1$ tel que $M^k = 0$. Dans ce cas, le plus petit entier naturel $k \geq 1$ tel que $M^k = 0$ s'appelle l'indice de nilpotence de M .

Soit $\mathcal{B}$ une base de E , un endomorphisme de E est nilpotent d'indice p si sa matrice dans $\mathcal{B}$ est d'indice p .

On pose $J_1 = (0)$ et, pour un entier $\alpha \geq 2$, $J_\alpha = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & & & & \\ 0 & \ddots & & & \\ \vdots & \ddots & \ddots & & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_\alpha(\mathbb{C})$.

Si $A_1 \in \mathcal{M}_{n_1}(\mathbb{C})$, $A_2 \in \mathcal{M}_{n_2}(\mathbb{C})$, ..., $A_k \in \mathcal{M}_{n_k}(\mathbb{C})$, on note

$$\text{diag}(A_1, A_2, \dots, A_k) = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & & \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & A_k \end{pmatrix} \in \mathcal{M}_{n_1+n_2+\dots+n_k}(\mathbb{C}).$$

I Premiers résultats

1.1. Que peut-on dire d'un endomorphisme nilpotent d'indice 1 ?

1.2 - Réduction d'une matrice de $\mathcal{M}_2(\mathbb{C})$ nilpotente d'indice 2

On suppose que $n = 2$. Soit u un endomorphisme de E nilpotent d'indice $p \geq 2$.

1.2.1. Montrer qu'il existe un vecteur x de E tel que $u^{p-1}(x) \neq 0$.

1.2.2. Vérifier que la famille $(u^k(x))_{0 \leq k \leq p-1}$ est libre. En déduire que $p = 2$.

1.2.3. Montrer que $\text{Ker}(u) = \text{Im}(u)$.

1.2.4. Construire une base de E dans laquelle la matrice de u est égale à J_2 .

1.2.5. En déduire que les matrices nilpotentes de $\mathcal{M}_2(\mathbb{C})$ sont exactement les matrices de trace et déterminant nuls.

II - Réduction d'une matrice de $\mathcal{M}_n(\mathbb{C})$ nilpotente d'indice 2

On suppose que $n \geq 3$. Soit u un endomorphisme de E nilpotent d'indice 2 et de rang r .

2.1. Montrer que $\text{Im}(u) \subset \text{Ker}(u)$ et que $2r \leq n$.

2.2. On suppose que $\text{Im}(u) = \text{Ker}(u)$. Montrer qu'il existe des vecteurs $e_1, e_2, \dots, e_r$ de E tels que la famille $(e_1, u(e_1), e_2, u(e_2), \dots, e_r, u(e_r))$ est une base de E .

2.3. Donner la matrice de u dans cette base.

2.4. On suppose $\text{Im}(u) \neq \text{Ker}(u)$. Montrer qu'il existe des vecteurs $e_1, e_2, \dots, e_r$ de E et des vecteurs $v_1, v_2, \dots, v_{n-2r}$ appartenant à $\text{Ker}(u)$ tels que $(e_1, u(e_1), e_2, u(e_2), \dots, e_r, u(e_r), v_1, v_2, \dots, v_{n-2r})$ est une base de E .

2.5. Quelle est la matrice de u dans cette base ?

III - Valeurs propres, polynôme caractéristique, polynômes annulateurs d'une matrice nilpotente

Dans cette partie, A désigne une matrice de $M_n(\mathbb{C})$.

3.1. Montrer que, si A est nilpotente, alors 0 est l'unique valeur propre de A .

3.2. Quelles sont les matrices de $M_n(\mathbb{C})$ à la fois nilpotentes et diagonalisables ?

3.3. Montrer qu'une matrice est nilpotente si, et seulement si, son polynôme caractéristique est égal à X^n .

3.4. Montrer la réciproque de la question 3.3.

3.5. Montrer qu'une matrice triangulaire de $M_n(\mathbb{C})$ à diagonale nulle est nilpotente et qu'une matrice nilpotente est semblable à une matrice triangulaire à diagonale nulle.

3.6. Démontrer que, si A est une matrice nilpotente d'indice p , alors tout polynôme de $\mathbb{C}[X]$ multiple de X^p est un polynôme annulateur de A .

On suppose que P est un polynôme annulateur de A nilpotente. $\int_{\mathbb{C}} \frac{1}{z} dz = 0$.

3.7. Démontrer que 0 est racine de P .

3.8. On note m la multiplicité de 0 dans P , ce qui permet d'écrire $P = X^m Q$ où Q est un polynôme de $\mathbb{C}[X]$ tel que $Q(0) \neq 0$. Démontrer que $Q(A)$ est inversible puis que P est un multiple de X^p dans $\mathbb{C}[X]$.

IV - Racines carrées de matrices nilpotentes

Pour une matrice $V \in M_n(\mathbb{C})$ donnée, on dit qu'une matrice $R \in M_n(\mathbb{C})$ est une racine carrée de V si $R^2 = V$. On se propose d'étudier l'existence et les valeurs de racines carrées éventuelles de certaines matrices nilpotentes.

4.1. On note $A = \begin{pmatrix} 1 & 3 & -7 \\ 2 & 6 & -14 \\ 1 & 3 & -7 \end{pmatrix}$ et u l'endomorphisme de $\mathbb{C}^3$ canoniquement associé à A .

4.1.1. Calculer le rang de A . En déduire, sans aucun calcul, le polynôme caractéristique de A . Montrer que A est nilpotente et donner son indice de nilpotence.

4.1.2. Démontrer que A est semblable à la matrice $\text{diag}(J_2, J_1)$. Donner la valeur d'une matrice P inversible telle que $A = P \text{diag}(J_2, J_1) P^{-1}$.

On cherche à déterminer l'ensemble des matrices $R \in M_3(\mathbb{C})$ telles que $R^2 = A$. On note ρ l'endomorphisme canoniquement associé à R .

4.2.2. Démontrer que $\text{Im}(u)$ et $\text{Ker}(u)$ sont stables par ρ et que ρ est nilpotent.

4.2.3. En déduire l'ensemble des racines carrées de A . Indication : on pourra considérer $R' = P^{-1} R P$.

4.2. On se propose dans cette question d'étudier l'équation matricielle $R^2 = J_2$. Soit R une solution de cette équation. Donner

les valeurs de R^4 et R^6 , puis l'ensemble des solutions de l'équation.

4.3. En général, soit $V \in M_n(\mathbb{C})$ une matrice nilpotente d'indice p . On se propose d'étudier l'équation $R^2 = V$.

4.3.1. Montrer que, si $2p - 1 > n$, alors il n'existe aucune solution.

4.3.2. Pour toute valeur de l'entier $n \geq 3$, exhiber une matrice $V \in M_n(\mathbb{C})$, nilpotente d'indice $p \geq 2$ et admettant au moins une racine carrée.

Problème 2

On notera respectivement $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ les corps des nombres complexes, réels et rationnels, et $\mathbb{Z}$ l'anneau des entiers relatifs.

Pour un entier $n \geq 1$ on dit qu'un nombre complexe z est une racine n -ième de l'unité si $z^n = 1$, et que z est une racine de l'unité s'il existe $k \geq 1$ tel que z soit une racine k -ième de l'unité.

Pour $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ on notera $R[X]$ l'anneau des polynômes à coefficients dans R . Un polynôme non nul est unitaire si son coefficient dominant est égal à 1. Un polynôme $P \in \mathbb{Q}[X]$ est irréductible dans $\mathbb{Q}[X]$ si P n'est pas constant et si l'égalité $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ implique que Q ou R est constant.

Un nombre complexe z est appelé nombre algébrique s'il existe $P \in \mathbb{Q}[X]$ non nul tel que $P(z) = 0$. On dit que $z \in \mathbb{C}$ est un entier algébrique s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(z) = 0$.

On admet le résultat suivant.

Théorème : L'ensemble des entiers algébriques est un sous-anneau de $\mathbb{C}$.

I - Polynôme minimal d'un nombre algébrique

on fixe un nombre algébrique α . Soit

$$I(\alpha) = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}.$$

5.1. Montrer que $I(\alpha)$ est un idéal de $\mathbb{Q}[X]$, différent de $\{0\}$.

Il existe donc un unique polynôme unitaire $\Pi_\alpha \in \mathbb{Q}[X]$, appelé polynôme minimal de α , tel que

$$I(\alpha) = \{\Pi_\alpha Q \mid Q \in \mathbb{Q}[X]\}.$$

On appelle degré de α le degré du polynôme Π_α .

5.2. Montrer que α est de degré 1 si et seulement si $\alpha \in \mathbb{Q}$.

5.3. Montrer que Π_α est irréductible dans $\mathbb{Q}[X]$.

5.4. Soit $P \in \mathbb{Q}[X]$ un polynôme unitaire, irréductible dans $\mathbb{Q}[X]$. Montrer que si z est une racine complexe de P , alors P est le polynôme minimal de z .

5.6.1. Soient $A, B \in \mathbb{Q}[X]$ deux polynômes qui possèdent une racine commune dans $\mathbb{C}$. Montrer que A et B ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.

5.6.2. Montrer que les racines de Π_α dans $\mathbb{C}$ sont simples.

5.7.1. Montrer que si $\alpha \in \mathbb{Q}$ est un entier algébrique, alors $\alpha \in \mathbb{Z}$.

5.7.2. Montrer que si $\alpha \in \mathbb{C}$ est un entier algébrique alors $\Pi_\alpha \in \mathbb{Z}[X]$. *(voir l'indication)*

Indication : utiliser le théorème admis en introduction ainsi que la question 5.6.1

5.8.1. Soit $\alpha \in \mathbb{C}$ un entier algébrique de degré 2 et de module 1. Montrer que α est une racine de l'unité.

5.8.2. Montrer que $\frac{3+4i}{5}$ est un nombre algébrique de degré 2 et de module 1 mais n'est pas une racine de l'unité.

II - Polynôme réciproque

Un polynôme unitaire de degré $d \geq 1$

$$P = \sum_{i=0}^d a_i X^i \in \mathbb{C}[X]$$

est dit réciproque si $a_i = a_{d-i}$ pour $0 \leq i \leq d$.

6.1.1. Montrer qu'un polynôme $P \in \mathbb{C}[X]$ unitaire de degré d est réciproque si et seulement si $X^d P\left(\frac{1}{X}\right) = P$.

6.1.2. Soit $P \in \mathbb{C}[X]$ un polynôme unitaire réciproque. Montrer que si $z \in \mathbb{C}$ est une racine de P , alors $z \neq 0$ et $\frac{1}{z}$ est aussi une racine de P , avec la même multiplicité.

Si α est un nombre algébrique de polynôme minimal Π_α les racines complexes de Π_α différentes de α sont appelées les conjugués de α . On notera $C(\alpha)$ l'ensemble des conjugués de α . L'ensemble $C(\alpha)$ est donc vide si α est de degré 1.

6.2. Soit z un nombre algébrique de module 1 et tel que $z \notin \{-1, 1\}$. Montrer que $\frac{1}{z}$ est un conjugué de z . En déduire que Π_z est réciproque.

On note S l'ensemble des nombres réels $\alpha \in]1, +\infty[$ qui sont aussi des entiers algébriques de degré au moins 2 et qui vérifient

$$\max_{\gamma \in C(\alpha)} |\gamma| = 1.$$

Soit α un élément de S et soit $\gamma \in C(\alpha)$ de module 1.

6.2.1. Montrer que le polynôme minimal de α est réciproque et que $\frac{1}{\alpha}$ est un conjugué de α .

6.2.2. Montrer que γ n'est pas une racine de l'unité.

6.2.3. Montrer que tous les conjugués de α autres que $\frac{1}{\alpha}$ sont de module 1.

6.3. Montrer que le degré de tout élément de S est un entier pair, supérieur ou égal à 4.