DEVOIR MAISON 18

Vous traiterez au choix l'un des deux problèmes suivants, le second étant plus difficile que le premier.

▸ Problème 1 : endomorphismes nilpotents d'indice maximal.

Dans tout le problème, $\mathbf{K}$ désigne soit $\mathbf{R}$ soit $\mathbf{C}$, et E est un $\mathbf{K}$-espace vectoriel de dimension finie $n \in \mathbf{N}^*$.
Un endomorphisme $f \in \mathscr{L}(E)$ est dit **nilpotent** s'il existe $p \in \mathbf{N}$ tel que $f^p = 0_{\mathscr{L}(E)}$.
On appelle alors **indice de nilpotence** de f, et on note $\nu(f) = \min\{p \in \mathbf{N} \mid f^p = 0_{\mathscr{L}(E)}\}$.

Partie I. Quelques exemples

1. Dans cette question, on suppose que $E = \mathbf{R}_{n-1}[X]$, et on considère $f : \left| \begin{array}{ccc} \mathbf{R}_{n-1}[X] & \longrightarrow & \mathbf{R}_{n-1}[X] \\ P & \longmapsto & P' \end{array} \right.$.

- **a.** Montrer que $f \in \mathscr{L}(\mathbf{R}_{n-1}[X])$, et déterminer son image et son noyau.
- **b.** Montrer que f est nilpotent et déterminer $\nu(f)$.
- **c.** Prouver que f^2 est encore nilpotent et déterminer son indice de nilpotence.
- **d.** Soit F un sous-espace vectoriel de $\mathbf{R}_{n-1}[X]$, stable par f.
  Prouver que si $P \in F$ est de degré d (avec $0 \leqslant d \leqslant n-1$), alors $\mathbf{R}_d[X] \subset F$.
  En déduire que les seuls sous-espaces vectoriels de $\mathbf{R}_{n-1}[X]$ stables par f sont $\{0_{\mathbf{R}[X]}\}$ et les $\mathbf{R}_d[X]$, $0 \leqslant d \leqslant n-1$.

2. Dans cette question, on suppose que $(e_1, \dots, e_n)$ est une base de E, et on note f l'unique endomorphisme de E tel que $f(e_1) = 0_E$ et pour tout $k \in [\![2, n]\!]$, $f(e_k) = e_{k-1}$.
Prouver que f est nilpotent et déterminer $\nu(f)$.

Partie II. Généralités sur les endomorphismes nilpotents

3. Soient $f, g \in \mathscr{L}(E)$.

- **a.** Prouver que si f et g commutent, et que f est nilpotent, alors $f \circ g$ est nilpotent.
- **b.** Prouver que si $f \circ g$ est nilpotent, alors $g \circ f$ aussi, et que $|\nu(f \circ g) - \nu(g \circ f)| \leqslant 1$.
- **c.** On suppose f nilpotent d'indice de nilpotence p. Prouver que $\mathrm{id}_E - f$ est bijectif, et exprimer $(\mathrm{id}_E - f)^{-1}$ en fonction de $\mathrm{id}_E, f, f^2, \dots, f^{p-1}$.

4. Soit $f \in \mathscr{L}(E)$. Prouver que si f est nilpotent, alors $\mathrm{rg}(f) \leqslant n-1$. La réciproque est-elle vraie ?

Partie III. Majoration de $\nu(f)$ et caractérisations des endomorphismes nilpotents tels que $\nu(f) = \dim E$.

Dans toute cette partie, $f \in \mathscr{L}(E)$ est nilpotent, et pour tout $k \in \mathbf{N}$, on note $N_k = \mathrm{Ker}(f^k)$.

5.
- **a.** Déterminer $N_{\nu(f)}$.
- **b.** Prouver que pour tout $k \in \mathbf{N}$, $N_k \subset N_{k+1}$.
- **c.** Montrer que si $k \in \mathbf{N}$ est tel que $N_{k+1} = N_k$, alors $N_{k+1} = N_{k+2}$.
- **d.** Prouver que pour tout $k \in [\![1, \nu(f)]\!]$, $\dim N_k \geqslant k$.
- **e.** En déduire que $\nu(f) \leqslant n$, où n désigne toujours la dimension de E.

6. On suppose de plus dans cette question que $\nu(f) = n$.

- **a.** Justifier que $\dim N_{n-1} < n$. Que vaut $\dim N_n$?
- **b.** En déduire que pour tout $k \in [\![1, n-1]\!]$, $\dim N_k < \dim N_{k+1}$.
- **c.** Montrer que pour tout $i \in [\![1, n]\!]$, $\dim N_i = i$. En déduire que $\mathrm{rg}(f) = n-1$.

7. On suppose à présent que $\mathrm{rg}(f) = n-1$.

a. Soit $k \in [\![1, n]\!]$. Montrer que $\operatorname{Im} f_{|N_k} \subset N_{k-1}$, puis à l'aide du théorème du rang, prouver que $\dim N_k \leqslant 1 + \dim N_{k-1}$.

b. En déduire que $\dim N_{n-1} < n$, puis que $\nu(f) = n$.

8. Dans cette question, on suppose de nouveau que $\nu(f) = n$, et on note F un sous-espace vectoriel de E stable par f.

a. Soit $p \in [\![1, n]\!]$ et soit $x \in N_p \setminus N_{p-1}$. Montrer que $(x, f(x), \dots, f^{p-1}(x))$ est une base de N_p.

b. Soit $x \in F$. Prouver que s'il existe $p \in [\![1, n]\!]$ tel que $x \in N_p \setminus N_{p-1}$, alors $N_p \subset F$.

c. En déduire qu'il existe $p \in [\![0, n]\!]$ tel que $F = N_p$.

9. Prouver que $\nu(f) = n$ si et seulement s'il existe un nombre fini de sous-espaces vectoriels de E stables par f.

▸ Problème 2 : extensions de corps et nombres algébriques

Soit $\mathbf{L}$ un corps, et soit $\mathbf{K}$ un sous-corps de $\mathbf{L}$, c'est-à-dire un sous-anneau de $\mathbf{L}$ qui est lui-même un corps.
On peut alors munir $\mathbf{L}$ d'une structure de $\mathbf{K}$-espace vectoriel où l'addition est l'addition de $\mathbf{L}$, et où la multiplication externe est $(\lambda, x) \in \mathbf{K} \times \mathbf{L} \mapsto \lambda \cdot x$, où $\cdot$ désigne la multiplication dans $\mathbf{L}$.
Si $\mathbf{L}$ est un $\mathbf{K}$-espace vectoriel de dimension finie, on dit que $\mathbf{L}$ est une **extension finie** de $\mathbf{K}$, et on note $[\mathbf{L} : \mathbf{K}] = \dim_{\mathbf{K}} \mathbf{L}$.

Partie I. Extensions de corps

1. **Premiers exemples :**

   a. Montrer que $\mathbf{C}$ est une extension finie de $\mathbf{R}$, donner une base du $\mathbf{R}$-espace vectoriel $\mathbf{C}$ et en déduire $[\mathbf{C} : \mathbf{R}]$.
   Prouver alors qu'un sous-corps de $\mathbf{C}$ qui contient $\mathbf{R}$ est égal soit à $\mathbf{R}$, soit à $\mathbf{C}$.

   b. On rappelle que $\mathbf{Q}(\sqrt{2}) = \left\{a + b\sqrt{2},\ (a, b) \in \mathbf{Q}^2\right\}$ est un sous-corps de $\mathbf{R}$, et donc un corps.
   Montrer que $\mathbf{Q}(\sqrt{2})$ est une extension finie de $\mathbf{Q}$ et que $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

   c. On admet l'irrationalité de $\sqrt[3]{2}$, et on note $\mathbf{Q}(\sqrt[3]{2}) = \left\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2,\ (a, b, c) \in \mathbf{Q}^3\right\}$.
   On admet temporairement que $\mathbf{Q}(\sqrt[3]{2})$ est un sous-corps de $\mathbf{C}$.

   i. On suppose par l'absurde qu'il existe $P \in \mathbf{Q}[X]$, de degré 2, tel que $P(\sqrt[3]{2}) = 0$.
   Montrer que P divise $X^3 - 2$ dans $\mathbf{Q}[X]$.
   En utilisant la forme scindée de $X^3 - 2$ dans $\mathbf{C}[X]$, aboutir à une contradiction.

   ii. En déduire que $\mathbf{Q}(\sqrt[3]{2})$ est une extension finie de $\mathbf{Q}$ et donner $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}]$.

   d. Soient $p_1, \ldots, p_n$ des nombres premiers deux à deux distincts.
   Montrer que $(\ln(p_1), \ln(p_2), \ldots, \ln(p_n))$ est une famille libre du $\mathbf{Q}$-espace vectoriel $\mathbf{R}$. En déduire que $\mathbf{R}$ n'est pas une extension finie de $\mathbf{Q}$.

2. Soient $k, \mathbf{K}, \mathbf{L}$ trois corps, avec k sous-corps de $\mathbf{K}$ et $\mathbf{K}$ sous-corps de $\mathbf{L}$. On suppose que est $\mathbf{K}$ une extension finie de k et que $\mathbf{L}$ est une extension finie de $\mathbf{L}$.
   On note alors $(\alpha_1, \ldots, \alpha_n)$ une base du k-espace vectoriel $\mathbf{K}$ et $(\beta_1, \ldots, \beta_p)$ une base du $\mathbf{K}$-espace vectoriel $\mathbf{L}$.
   Montrer que $(\alpha_i \beta_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ est une base du k-espace vectoriel $\mathbf{L}$.
   En déduire que $\mathbf{L}$ est une extension finie de k et que $[\mathbf{L} : k] = [\mathbf{L} : \mathbf{K}][\mathbf{K} : k]$.

Partie II. Éléments algébriques

Dans cette partie, $\mathbf{L}$ est un corps, et $\mathbf{K}$ est un sous-corps de $\mathbf{L}$.
Pour $\alpha \in \mathbf{L}$, on note $\mathbf{K}[\alpha] = \mathrm{Vect}_{\mathbf{K}}(\alpha^n,\ n \in \mathbf{N})$ le sous-espace vectoriel du $\mathbf{K}$-espace vectoriel $\mathbf{L}$ engendré par $(\alpha^n)_{n \in \mathbf{N}}$. Un élément $\alpha \in \mathbf{L}$ est dit **algébrique sur K** s'il existe $P \in \mathbf{K}[X]$, non nul, tel que $P(\alpha) = 0$.

3. Soit $\alpha \in \mathbf{L}$. Montrer que $\mathbf{K}[\alpha] = \{P(\alpha),\ P \in \mathbf{K}[X]\}$. En déduire que $\mathbf{K}[\alpha]$ est un sous-anneau de $\mathbf{L}$.
   Montrer que c'est le plus petit (au sens de l'inclusion) sous-anneau de $\mathbf{L}$ qui contient $\mathbf{K}$ et α.

4. Soit $\alpha \in \mathbf{L}$. Montrer que α est algébrique sur $\mathbf{K}$ si et seulement si il existe $n \in \mathbf{N}$ tel que $(1, \alpha, \alpha^2, \ldots, \alpha^n)$ soit une famille liée du $\mathbf{K}$-espace vectoriel $\mathbf{L}$.

Si $\alpha \in \mathbf{L}$ est algébrique sur $\mathbf{K}$, on appelle degré de α sur $\mathbf{K}$ le plus petit entier $d \in \mathbf{N}$ tel que $(1, \alpha, \ldots, \alpha^d)$ soit liée dans le $\mathbf{K}$-espace vectoriel $\mathbf{L}$.

5. Montrer que $\alpha \in \mathbf{L}$ est algébrique de degré 1 sur $\mathbf{K}$ si et seulement si $\alpha \in \mathbf{K}$.

6. Montrer que si $\mathbf{L}$ est une extension finie de $\mathbf{K}$, alors tout élément de $\mathbf{L}$ est algébrique sur $\mathbf{K}$, de degré inférieur ou égal à $[\mathbf{L} : \mathbf{K}]$.

7. Soit $\alpha \in \mathbf{L}$, algébrique sur $\mathbf{K}$, de degré d.

   a. Montrer que $(1, \alpha, \alpha^2, \ldots, \alpha^{d-1})$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}[\alpha]$.

b. Soit $\beta \in \mathbf{K}[\alpha]$, et soit $f_\beta : \left| \begin{array}{ccc} \mathbf{K}[\alpha] & \longrightarrow & \mathbf{K}[\alpha] \\ x & \longmapsto & \beta x \end{array} \right.$.
Montrer que si $\beta \neq 0$, alors f_β est un automorphisme du $\mathbf{K}$-espace vectoriel $\mathbf{K}[\alpha]$.

c. En déduire que $\mathbf{K}[\alpha]$ est un sous-corps de $\mathbf{L}$, et que c'est le plus petit sous-corps de $\mathbf{L}$ qui contient à la fois $\mathbf{K}$ et α.

d. Montrer que $\mathbf{K}[\alpha]$ est une extension finie de $\mathbf{K}$, et déterminer $[\mathbf{K}[\alpha] : \mathbf{K}]$.

e. Montrer que $\mathbf{Q}\left(\sqrt[3]{2}\right)$ tel que défini à la question 1.c est un sous-corps de $\mathbf{C}$.

Généralement, on note $\mathbf{K}(\alpha)$ *le plus petit sous-corps de* $\mathbf{L}$ *contenant* $\mathbf{K}$ *et* α*, ce qui explique par exemple que l'on note* $\mathbf{Q}(\sqrt{2})$ *ou* $\mathbf{Q}\left(\sqrt[3]{2}\right)$ *au lieu de* $\mathbf{Q}[\sqrt{2}]$ *et* $\mathbf{Q}\left[\sqrt[3]{2}\right]$.

8. Soit $\alpha \in \mathbf{L}^*$. Montrer qu'il y a équivalence entre :

i) $\mathbf{K}[\alpha]$ est un sous-corps de $\mathbf{L}$ ii) $\alpha^{-1} \in \mathbf{K}[\alpha]$ iii) α est algébrique sur $\mathbf{K}$

Partie III. Polynôme minimal d'un élément algébrique

Dans cette partie, $\mathbf{L}$ est encore un corps et $\mathbf{K}$ est un sous-corps de $\mathbf{L}$.
On considère également $\alpha \in \mathbf{L}$ un élément algébrique de degré d sur $\mathbf{K}$.
On note $I_\alpha = \{P \in \mathbf{K}[X] \mid P(\alpha) = 0\}$. Puisque α est algébrique, $I_\alpha \neq \{0_{\mathbf{K}[X]}\}$.
On note alors $q = \min\{\deg P,\ P \in I_\alpha \setminus \{0_{\mathbf{K}[X]}\}\}$ le degré minimal d'un élément non nul de I_α.

9. Prouver que I_α contient un unique polynôme unitaire de degré q, que l'on notera dans la suite μ_α et qu'on appelle polynôme minimal de α sur $\mathbf{K}$.

10. Montrer que μ_α est irréductible dans $\mathbf{K}[X]$, et que $I_\alpha = \{\mu_\alpha Q,\ Q \in \mathbf{K}[X]\}$.

11. Justifier que $\deg \mu_\alpha = d$, le degré de α sur $\mathbf{K}$.

12. Quel est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbf{Q}$?

13. Soit $\alpha = \sqrt{2} + \sqrt{3}$. En notant que α est racine de $(X - \sqrt{2})^2 - 3 \in \mathbf{Q}(\sqrt{2})[X]$, prouver que α est algébrique sur $\mathbf{Q}$, et déterminer le degré de son polynôme minimal sur $\mathbf{Q}$.

Partie IV. Nombres algébriques (sur Q)

Dans cette partie, on dira qu'un nombre complexe est **algébrique** s'il est algébrique sur $\mathbf{Q}$.
On note $\overline{\mathbf{Q}}$ l'ensemble des nombres algébriques, de sorte que

$$\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} \mid \exists P \in \mathbf{Q}[X] \setminus \{0\}, P(\alpha) = 0\}.$$

14. Soient $\alpha, \beta \in \overline{\mathbf{Q}}$. On rappelle que $\mathbf{Q}[\alpha]$ est un corps, et on note $\mathbf{Q}[\alpha, \beta] = (\mathbf{Q}[\alpha])[\beta]$.

a. Montrer que $\mathbf{Q}[\alpha, \beta]$ est un corps, et que c'est une extension finie de $\mathbf{Q}$.

b. **Exemple** : montrer que $\mathbf{Q}[\sqrt{2}, \sqrt{3}] = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ (a, b, c, d) \in \mathbf{Q}^4\right\}$.

15. Montrer que $\overline{\mathbf{Q}}$ est un sous-corps de $\mathbf{C}$.
Il existe des nombres réels qui ne sont pas algébriques, par exemple e *et* π*, et donc* $\overline{\mathbf{Q}}$ *est un corps qui contient strictement* $\mathbf{Q}$*, mais qui n'est pas égal à* $\mathbf{C}$.

16. **a.** Soit $\mathbf{K}$ un sous-corps de $\mathbf{C}$ qui contient $\overline{Q}$.
Montrer que si $\mathbf{K}$ est une extension finie de $\overline{Q}$, alors $\mathbf{K} = \overline{Q}$.

b. En déduire que tout polynôme non constant à coefficients dans $\overline{Q}$ possède une racine dans $\overline{Q}$.
Un corps $\mathbf{K}$ *tel que tout polynôme constant de* $\mathbf{K}[X]$ *possède une racine dans* $\mathbf{K}$ *est appelé* ***algébriquement clos****. Nous savions déjà que* $\mathbf{C}$ *est algébriquement clos (c'est le théorème de d'Alembert-Gauss).*