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, **K** désigne soit **R** soit **C**, et E est un **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. Montrer que $\nu(f) = n$ si et seulement si $\mathrm{rg}(f) = n-1$.

8. Dans cette question, on suppose de nouveau que $v(f) = n$, 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 $v(f) = n$ si et seulement s'il existe un nombre fini de sous-espaces vectoriels de E stables par f.

▸ Problème 2 : nombres algébriques et extensions de corps

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 alors de dimension finie sur $\mathbf{K}$, 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 $p_1, \dots, p_n$ des nombres premiers deux à deux distincts.
   Montrer que $(\ln(p_1), \ln(p_2), \dots, \ln(p_n))$ 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 $(\alpha_1, \dots, \alpha_n)$ une base du k-espace vectoriel $\mathbf{K}$ et $(\beta_1, \dots, \beta_p)$ 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 $(X^n)_{n \in \mathbf{N}}$. Un élément $\alpha \in \mathbf{L}$ est dit **algébrique sur $\mathbf{K}$** 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 $(1, \alpha, \alpha^2, \dots, \alpha^n)$ 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 $(1, \alpha, \dots, \alpha^d)$ 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 $(1, \alpha, \alpha^2, \dots, \alpha^{d-1})$ 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 $\mathbf{C}$.

CORRECTION DU DEVOIR MAISON 18

▸ Problème 1 : endomorphismes nilpotents d'indice maximal

Partie I. Quelques exemples

1.a. La linéarité de f a été prouvée dans le cours[1].
Et puisque si $P \in \mathbf{R}_{n-1}[X]$, $\deg P' \leqslant n-2$, on a bien $P' = f(P) \in \mathbf{R}_{n-2}[X] \subset \mathbf{R}_{n-1}[X]$, et donc $\boxed{f \text{ est un endomorphisme de } \mathbf{R}_{n-1}[X].}$

[1] Dans le chapitre de polynômes.

Son noyau est formé des polynômes constants : $\boxed{\mathrm{Ker}(f) = \mathbf{R}_0[X].}$
Et son image est engendrée par l'image de la base canonique, c'est-à-dire

$$\mathrm{Im}(f) = \mathrm{Vect}\left(f(1), f(X), \dots, f(X^{n-1})\right) = \mathrm{Vect}\left(0_{\mathbf{R}[X]}, 1, 2X, \dots, (n-1)X^{n-2}\right) = \mathrm{Vect}\left(1, 2X, \dots, (n-1)X^{n-2}\right).$$

Mais la famille $(1, 2X, \dots, (n-1)X^{n-2})$ est formée de polynômes de degrés deux à deux distincts, elle est donc libre. Tous ces polynômes sont dans $\mathbf{R}_{n-2}[X]$, et ils sont au nombre de $n-1 = \dim \mathbf{R}_{n-2}[X]$.
Donc nous avons là une base de $\mathbf{R}_{n-2}[X]$, si bien que $\boxed{\mathrm{Im}(f) = \mathbf{R}_{n-2}[X].}$

1.b. On a donc, pour tout $k \in \mathbf{N}$, $f^k : P \mapsto P^{(k)}$.
En particulier, pour $P \in \mathbf{R}_{n-1}[X]$, $P^{(n-1)}$ est constant, et $P^{(n)}$ est nul.
Mais pour tout $P \in \mathbf{R}_{n-1}[X]$, $f^n(P) = P^{(n)} = 0_{\mathbf{R}[X]}$, si bien que $f^n = 0_{\mathscr{L}(E)}$.
Donc f est nilpotente, et $\boxed{\nu(f) \leqslant n.}$
Par ailleurs, $f^{n-1}(X^{n-1}) = (n-1)! \neq 0$, donc $f^{n-1} \neq 0_{\mathscr{L}(E)}$, et donc $\boxed{\nu(f) = n.}$

1.c. De manière générale, si $f^p = 0_{\mathscr{L}(E)}$, alors $(f^2)^p = f^{2p} = 0_{\mathscr{L}(E)}$.
Donc $\boxed{f^2 \text{ est bien nilpotent.}}$

Si n est pair, $n = 2k$, alors $(f^2)^k = f^{2k} = f^n = 0_{\mathscr{L}(E)}$ et $(f^2)^{k-1} = f^{2k-2} \neq 0_{\mathscr{L}(E)}$.
Donc $\nu(f^2)$ est égal à k, la moitié de n.
Si n est impair, $n = 2k+1$, alors $(f^2)^k = f^{2k} = f^{n-1} \neq 0_{\mathscr{L}(E)}$.
Et $(f^2)^{k+1} = f^{2k+2} = f^{n+1} = f \circ f^n = 0_{\mathscr{L}(E)}$. Et donc $\nu(f^2) = k+1 = \left\lfloor \frac{n}{2} \right\rfloor + 1$.

Remarque
Un moyen de regrouper les deux cas est de dire que
$$\nu\left(f^2\right) = \left\lfloor \frac{n+1}{2} \right\rfloor.$$

1.d. Si P est de degré d, alors P' est de degré $d-1$, P'' de degré $d-2$, etc, $P^{(d)}$ de degré 0.
Donc en particulier, $(P, P', \dots, P^{(d)})$ est une famille de polynômes de degrés deux à deux distincts, elle est libre.
Tous ces polynômes sont alors dans $\mathbf{R}_d[X]$, et il s'agit d'une famille de $d+1$ vecteurs de $\mathbf{R}_d[X]$, donc c'est $\boxed{\text{une base de } \mathbf{R}_d[X].}$

Soit à présent F un sous-espace vectoriel de $\mathbf{R}_{n-1}[X]$, stable par f, et différent de $\{0_{\mathbf{R}[X]}\}$.
Notons alors $d = \max\{\deg P, P \in F \setminus \{0_{\mathbf{R}[X]}\}\}$, et soit $P \in F$ de degré d.
On a donc trivialement $F \subset \mathbf{R}_d[X]$.
Et par stabilité de F par f, $P' = f(P) \in F$, puis $P'' = f(P') \in F, \dots, P^{(d)} \in F$.
Donc $\mathrm{Vect}(P, P', \dots, P^{(d)}) \subset F$. Or par la question précédente, $\mathrm{Vect}(P, P', \dots, P^{(d)}) = \mathbf{R}_d[X]$, si bien que $\mathbf{R}_d[X] \subset F$, et donc $F = \mathbf{R}_d[X]$.
Donc les sous-espaces vectoriels de E stables par f sont exactement $\{0_{\mathbf{R}[X]}\}$ et les $\mathbf{R}_d[X]$, $0 \leqslant d \leqslant n-1$.

Autrement dit
On considère P de degré maximal parmi les éléments de F.

2. On a donc $f^2(e_1) = f(0_E) = 0_E$, $f^2(e_2) = f(e_1) = 0_E$, et pour $i \geqslant 3$, $f^2(e_i) = f(e_{i-1}) = e_{i-2}$.

Prouvons donc par récurrence sur $i \in [\![1, n]\!]$ que pour tout $k \in [\![1, n]\!]$, $f^i(e_k) = \begin{cases} 0 & \text{si } k \leqslant i \\ e_{k-i} & \text{sinon} \end{cases}$.

Pour $i = 1$, c'est évident.
Supposons donc le résultat vrai pour f^i. Alors pour $k \leqslant i$, on a $f^{i+1}(e_k) = f(f^i(e_k)) = 0_E$.
Pour $k = i+1$, on a $f^{i+1}(e_{i+1}) = f(f^i(e_{i+1})) = f(e_1) = 0_E$.
Et pour $k > i+1$, on a $f^{i+1}(e_k) = f(f^i(e_k)) = f(e_{k-i}) = e_{k-i-1} = e_{k-(i+1)}$.
Ainsi, la propriété est héréditaire, et donc vraie pour tout $i \in [\![1, n]\!]$.

En particulier, pour tout $k \in [\![1, n]\!]$, $f^n(e_k) = 0_E$.
Donc l'endomorphisme f^n est nul sur une base, donc est nul. Ce qui prouve déjà que f est nilpotent et que $\nu(f) \leqslant n$.
Puisque par ailleurs, $f^{n-1}(e_n) = e_1 \neq 0_E$, $f^{n-1} \neq 0_{\mathscr{L}(E)}$, et donc $\boxed{\nu(f) = n.}$

Partie II. Généralités sur les endomorphismes nilpotents

3.a. Supposons donc f nilpotent avec $f^p = 0_{\mathscr{L}(E)}$.
Alors $(f \circ g)^p = f^p \circ g^p = 0_{\mathscr{L}(E)} \circ g^p = 0_{\mathscr{L}(E)}$.
Donc $\boxed{f \circ g \text{ est nilpotent}}$ et son indice de nilpotence est inférieur ou égal à celui de f.

3.b. Supposons donc que $(f \circ g)^p = 0_{\mathscr{L}(E)}$.
Alors $(g \circ f)^{p+1} = g \circ (f \circ g \circ \cdots f \circ g) \circ f = g \circ (f \circ g)^p \circ f = g \circ 0_{\mathscr{L}(E)} \circ f = 0_{\mathscr{L}(E)}$.
Donc $g \circ f$ est nilpotent, et $\nu(g \circ f) \leqslant \nu(f \circ g) + 1$.
Une fois acquise la nilpotence de $g \circ f$, on peut prouver sur le même principe que $f \circ g$ est d'indice au plus $\nu(g \circ f) + 1$.
Et donc $-1 \leqslant \nu(g \circ f) - \nu(f \circ g) \leqslant 1$ si bien que $\boxed{|\nu(g \circ f) - \nu(f \circ g)| \leqslant 1.}$

> **⚠ Attention !**
> On n'a qu'une inégalité pour l'instant : nous avons une puissance de $g \circ f$ qui est nulle, mais ne savons pas encore si nous avons trouvé la plus petite telle puissance.

3.c. Il s'agit de penser à une identité remarquable usuelle : puisque id_E et f commutent[2],

$$(\mathrm{id}_E - f) \circ \left(\sum_{i=0}^{p-1} \mathrm{id}_E^{p-1-i} f^i \right) = \mathrm{id}_E^p - f^p = \mathrm{id}_E.$$

Et de même, $(\mathrm{id}_E + f + \cdots + f^{p-1}) \circ (\mathrm{id}_E - f) = \mathrm{id}_E$.
Et donc $\boxed{\mathrm{id}_E - f \text{ est bijective, d'inverse } \mathrm{id}_E + f + \cdots + f^{p-1}.}$

Remarque *: tous les résultats prouvés dans cette question sont en fait valables[3] dans n'importe quel anneau autre que $\mathscr{L}(E)$.*

[2] Hypothèse indispensable pour appliquer la troisième identité remarquable généralisée.

[3] En remplaçant «bijectif» par «inversible» dans 3.c.

4. Nous savons que $\mathrm{rg}(f) \leqslant n$.
Si f est un endomorphisme de rang n, alors f est surjectif, et puisque nous sommes en dimension finie, est un isomorphisme.
Et en particulier, pour tout $k \in \mathbf{N}$, f^k est encore un isomorphisme et donc n'est jamais nul, si bien que f n'est pas nilpotent.
Donc si f est nilpotent, $\mathrm{rg}(f) \neq n - 1$ et donc $\boxed{\mathrm{rg}(f) \leqslant n - 1.}$

La réciproque est fausse, par exemple si H est un hyperplan de E, que D en est un supplémentaire, et que p désigne la projection sur H parallèlement à D, alors $\mathrm{rg}(p) = \dim H = n - 1$, et pour tout $k \in \mathbf{N}^*$, $p^k = p \neq 0_{\mathscr{L}(E)}$. Donc p n'est pas nilpotent.

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

5.a. Puisque $f^{\nu(f)} = 0_{\mathscr{L}(E)}$, $N_\nu(f) = \mathrm{Ker}(0_{\mathscr{L}(E)}) = E$.

5.b. Soit $k \in \mathbf{N}$, et soit $x \in N_k$. Alors $f^k(x) = 0_E$, et donc $f^{k+1}(x) = f(0_E) = 0_E$, si bien que $x \in N_{k+1}$.
On a donc bien $\boxed{N_k \subset N_{k+1}.}$

> **Remarque**
> Plus généralement, une application linéaire est nulle si et seulement si son noyau est égal à E (ou si son image est réduite au vecteur nul).

5.c. Soit $k \in \mathbf{N}$, et supposons que $N_k = N_{k+1}$. Soit alors $x \in N_{k+2}$.
On a donc $f^{k+2}(x) = 0_E \Leftrightarrow f^{k+1}(f(x)) = 0_E$.
Donc $f(x) \in \mathrm{Ker}(f^{k+1}) = N_{k+1} = N_k = \mathrm{Ker}(f^k)$.
Ce qui signifie que $f^k(f(x)) = 0_E \Leftrightarrow f^{k+1}(x) = 0_E$.
Et donc $x \in N_{k+1}$, si bien que $N_{k+2} \subset N_{k+1}$.
Puisque nous avions déjà l'inclusion réciproque, on en déduit que $\boxed{N_{k+2} = N_{k+1}.}$

5.d. Notons qu'on a déjà, pour tout $k \in \mathbf{N}$, $\dim N_k \leqslant \dim N_{k+1}$. La question précédente, nous dit que dès que deux termes consécutifs de la suite[4] $(N_k)_k$ sont égaux, alors cette suite stationne.
Puisque $f^{\nu(f)-1} \neq 0_{\mathscr{L}(E)}$, alors $N_{\nu(f)-1} \neq E = N_{\nu(f)}$.
Et par conséquent, pour tout $k \leqslant \nu(f) - 1$, $N_k \neq N_{k+1}$.
Puisque $N_k \subset N_{k+1}$, ceci signifie qu'on ne peut donc pas avoir $\dim N_k = \dim N_{k+1}$, faute de quoi ces deux espaces seraient égaux.
Et donc $\dim N_{k+1} > \dim N_k$, soit encore, puisqu'il s'agit d'entiers, $\dim N_{k+1} \geqslant \dim N_k + 1$.

[4] De sous-espaces vectoriels.

> **Rappel**
> Deux sev de même dimension, avec l'un inclus dans l'autre sont égaux.

Une récurrence facile, en notant que $\dim N_0 = \dim \mathrm{Ker}(\mathrm{id}_E) = \dim\{0_E\} = 0$, prouve que pour tout $k \in [\![1, \nu(f)]\!]$, $\boxed{\dim N_k \geqslant k.}$

5.e. En particulier $n = \dim N_{\nu(f)} \geqslant \nu(f)$.

6.a. Puisque $f^{n-1} \neq 0_{\mathscr{L}(E)}$, $\mathrm{Ker}\, f^{n-1} \neq E$, et donc $\boxed{\dim N_{n-1} < n.}$
En revanche, $f^n = 0_{\mathscr{L}(E)}$, $\mathrm{Ker}\, f^n = E$, et donc $\boxed{\dim N_n = n.}$

6.b. On a donc, comme précédemment, pour tout $k \in [\![1, n-1]\!]$, $N_k \neq N_{k+1}$, et donc $\dim N_k < \dim N_{k+1}$, soit encore $\boxed{\dim N_{k+1} \geqslant \dim N_k + 1.}$

6.c. On en déduit que pour tout $i \in [\![1, n]\!]$, $\dim N_i \geqslant \dim N_0 + i = i$.
Si l'une de ces inégalités était stricte, par exemple si on avait $\dim N_{i_0} \geqslant i_0 + 1$ avec $i_0 \in [\![1, n]\!]$ alors

$$n = \dim N_n \geqslant \dim N_{i_0} + (n - i_0) \geqslant i_0 + 1 + n - i_0 \geqslant n + 1$$

ce qui est absurde. Donc $\boxed{\text{pour tout } i \in [\![1, n]\!],\ \dim N_i = i.}$
En particulier, on en déduit que $\dim \mathrm{Ker}\, f = \dim N_1 = 1$.
Et donc par le théorème du rang, $\mathrm{rg}\, f = \dim E - \dim \mathrm{Ker}\, f = \boxed{n - 1.}$

7. Nous venons de prouver que si $\nu(f) = n$, alors $\mathrm{rg}(f) = n - 1$.

Supposons à présent que $\mathrm{rg}(f) = n - 1$, si bien[5] que $\dim \mathrm{Ker}\, f = 1$.
Alors pour tout $k \in [\![1, n]\!]$, appliquons le théorème du rang à la restriction de f à N_k. On a alors

$$\dim N_k = \dim \mathrm{Ker}\, f_{|N_k} + \dim \mathrm{Im}\, f_{|N_k}.$$

Mais $\mathrm{Im}\, f_{|N_k} \subset N_{k-1}$. En effet, si $y = f(x)$, avec $x \in \mathbf{N}_k$, alors $f^{k-1}(y) = f^k(x) = 0_E$, si bien que $y \in N_{k-1}$.
Et par ailleurs, $\mathrm{Ker}\, f_{|N_k} = \mathrm{Ker}\, f \cap N_k = \mathrm{Ker}\, f$.
On en déduit donc que $\dim N_k \leqslant \dim \mathrm{Ker}\, f + \dim N_{k-1} \leqslant 1 + \dim N_{k-1}$.
Autrement dit, les dimensions des N_k ne peuvent pas augmenter de plus d'une unité à chaque étape.
Donc $\dim N_2 \leqslant \dim N_1 + 1 \leqslant 2$, $\dim N_3 \leqslant \dim N_2 + 1 \leqslant 3$, et de proche en proche, $\dim N_{n-1} \leqslant n - 1$, si bien que $\mathrm{Ker}\, f^{n-1} \neq E$, et donc $f^{n-1} \neq \{0_{\mathscr{L}(E)}\}$.
Donc $\nu(f) \geqslant n$, et par conséquent, $\nu(f) = n$.

[5] C'est le théorème du rang.

Plus généralement
La restriction de f à un sev G a toujours pour noyau $G \cap \mathrm{Ker}\, f$.
En effet, ce noyau est formé des éléments de G qui sont annulés par f... donc qui sont dans $\mathrm{Ker}\, f$.

8.a. Soient $\lambda_0, \dots, \lambda_{p-1}$ des scalaires tels que $\lambda_0 x + \lambda_1 f(x) + \cdots + \lambda_{p-1} f^{p-1}(x) = 0_E$.
Alors en appliquant f^{p-1}, il vient

$$\lambda_0 f^{p-1}(x) + \lambda_1 f^p(x) + \cdots + \lambda_{p-1} f^{2(p-1)}(x) = f^{p-1}(0_E) = 0_E.$$

Mais puisque $x \in N_p$, $f^p(x) = 0_E$, et donc $f^{p+1}(x) = \cdots = f^{2(p-1)}(x) = 0_E$.
Donc il reste $\lambda_0 f^{p-1}(x) = 0_E$.
Or $x \notin N_{p-1} = \mathrm{Ker}(f^{p-1})$, donc $f^{p-1}(x) \neq 0_E$, et donc $\lambda_0 = 0$.
Il reste donc $\lambda_1 f(x) + \cdots + \lambda_{p-1} f^{p-1}(x) = 0_E$.
En appliquant f^{p-2}, il vient $\lambda_1 f^{p-1}(x) + \lambda_2 f^p(x) + \cdots + \lambda_{p-1} f^{2p-3}(x) = 0_E$.
Soit encore $\lambda_1 f^{p-1}(x) = 0_E$, et puisque $f^{p-1}(x)$ est toujours non nul, $\lambda_1 = 0$.
De proche en proche, on prouve que les λ_i sont tous nuls, si bien que $(x, f(x), \dots, f^{p-1}(x))$ est une famille libre.

Par ailleurs, il a été prouvé à la question 6.c que $\dim N_p = p$, et donc $(x, f(x), \dots, f^{p-1}(x))$ est une famille libre de N_p de cardinal p : c'est donc $\boxed{\text{une base de } N_p.}$

8.b. Puisque F est stable par f, et que $x \in F$, pour tout $f(x) \in F$. Donc $f^2(x) = f(f(x)) \in F$, et une récurrence immédiate prouve que pour tout $k \in [\![1, p-1]\!]$, $f^k(x) \in F$.
Donc $N_p = \mathrm{Vect}(x, f(x), \dots, f^{p-1}(x)) \subset F$.

Rappel
$\mathrm{Vect}(x, f(x), \dots, f^{p-1}(x))$ est le plus petit (au sens de l'inclusion) sous-espace vectoriel de E qui contient $x, f(x), \dots, f^{p-1}(x)$

8.c. Si $F = \{0_E\}$, alors $F = \mathrm{Ker}(\mathrm{id}_E) = N_0$.
Supposons donc $F \neq \{0_E\}$. Soit alors $A = \{i \in [\![1, n]\!] \mid \exists x \in F, x \in N_i \setminus N_{i-1}\}$.
Puisque A est une partie non vide de $\mathbf{N}$, elle possède un plus grand élément p.
Soit alors $x \in F$ tel que $x \in N_p \setminus N_{p-1}$. Alors par la question précédente, $N_p \subset F$.

Soit $x \in E$. Puisque $\{0_E\} = N_0 \subset N_1 \subset \cdots \subset N_{n-1} \subset N_n = E$, si on note $i_x = \min\{k \in [\![0,]\!] \mid x \in N_i\}$, on a $x \in N_{i_x} \setminus N_{i_x - 1}$.

Or par définition de p, $i_x \leqslant p$, donc $x \in N_{i_x} \subset N_p$.
Et donc $F \subset N_p$.

Par double inclusion, on en déduit que $\boxed{F = N_p.}$

9. Nous venons de prouver que si $\nu(f) = n$, alors f possède pour seuls sous-espaces stables les N_i, $0 \leqslant i \leqslant n$, qui sont donc en nombre fini.

Inversement, supposons que $\nu(f) < n$. Comme prouvé précédemment, $\operatorname{rg}(f) < n-1$, et donc $\dim \operatorname{Ker} f \geqslant 2$.
Soit alors (e_1, e_2) une famille libre de $\operatorname{Ker} f$, et pour tout $\lambda \in \mathbf{K}$, posons $F_\lambda = \operatorname{Vect}(e_1 + \lambda e_2)$, qui est donc de dimension 1.
Alors F_λ est stable par f puisque $F_\lambda \subset \operatorname{Ker} f$, et donc pour tout $x \in F_\lambda$, $f(x) = 0_E \in F_\lambda$.
Par ailleurs, pour $\lambda \neq \mu$, $e_1 + \lambda e_2$ et $e_1 + \mu e_2$ ne sont pas colinéaires, si bien que $e_1 + \mu e_2 \notin F_\mu$.
Et donc $F_\lambda \neq F_\mu$.
Donc les F_λ, $\lambda \in \mathbf{K}$ sont des sous-espaces stables par f, deux à deux distincts. Puisque $\mathbf{K}$ est infini, il existe donc une infinité de sous-espaces stables par f.

Plus généralement
Le même raisonnement prouve que tout sous-espace vectoriel de $\operatorname{Ker} f$ est stable par f.

Et donc $\boxed{\nu(f) = n \text{ si et seulement si il existe un nombre fini de sous-espaces de } E \text{ stables par } f.}$

▸ Problème 2 : nombres algébriques et extensions de corps

Partie I. Extensions de corps

1. Premiers exemples

1.a. Puisque tout complexe s'écrit de manière unique sous la forme $a + ib$, $(a, b) \in \mathbf{R}^2$, la famille $(1, i)$ est une base du $\mathbf{R}$-espace vectoriel $\mathbf{C}$, qui est donc une extension finie de $\mathbf{R}$, avec $[\mathbf{C} : \mathbf{R}] = 2$.
Un sous-corps de $\mathbf{C}$ contenant $\mathbf{R}$ est en particulier un sous-espace vectoriel du $\mathbf{R}$-espace vectoriel $\mathbf{C}$. Donc il est de dimension inférieur ou égale à 2.
S'il est de dimension 2, il est égal à $\mathbf{C}$ tout entier.
S'il est de dimension $1 = [\mathbf{R} : \mathbf{R}]$, il est égal à $\mathbf{R}$.

Détails
Il contient $\mathbf{R}$, et ils ont même dimension, donc ils sont égaux.

1.b. La famille $(1, \sqrt{2})$ est génératrice[6] du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\sqrt{2})$, qui est donc de dimension finie sur $\mathbf{Q}$, de dimension inférieure ou égale à 2.
Puisque $\sqrt{2} \notin \mathbf{Q}$, $\mathbf{Q}(\sqrt{2}) \neq \mathbf{Q}$, et donc $\dim_{\mathbf{Q}} \mathbf{Q}(\sqrt{2}) \neq 1$, si bien que $\boxed{[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2.}$

[6] C'est la définition même de $\mathbf{Q}(\sqrt{2})$: tous ses éléments sont des combinaisons linéaires à coefficients rationnels de 1 et de $\sqrt{2}$.

1.c.i. Notons $X^3 - 2 = QP + R$ la division euclidienne de $X^3 - 2$ par P dans $\mathbf{Q}[X]$, avec $\deg R < 1$.
Alors en évaluant cette relation en $\sqrt[3]{2}$, $R(\sqrt[3]{2}) = 0$.
Si R est de degré 1, alors il existe $(a, b) \in \mathbf{Q}^* \times \mathbf{Q}$ tels que $R = aX + b$, et alors $\sqrt[3]{2} = -\dfrac{b}{a} \in \mathbf{Q}$, ce qui est absurde.
Donc R est constant, et donc $R = 0_{\mathbf{Q}[X]}$. Et donc P divise $X^3 - 2$ dans $\mathbf{Q}[X]$.

En particulier, P divise $X^3 - 2$ dans $\mathbf{C}[X]$.
Mais ce polynôme est scindé, et ses racines sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.
Donc l'un des deux complexes $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ est racine de P.
Mais P étant à coefficients réels, s'il possède l'un pour racine, il possède l'autre[7] pour racine, et donc possède trois racines, ce qui est absurde puisque $\deg P = 2$.
Donc $\boxed{\sqrt[3]{2} \text{ n'est racine d'aucun polynôme de degré 2 à coefficients rationnels.}}$

[7] Son conjugué car $j^2 = \overline{j}$.

1.c.ii. Par définition de $\sqrt[3]{2}$, la famille $\left(1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right)$ est une famille génératrice du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}\left(\sqrt[3]{2}\right)$, qui est donc une extension finie de $\mathbf{Q}$, de degré au plus 3.
Par ailleurs, si a, b, c sont trois rationnels tels que $a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 = 0$, alors $\sqrt[3]{2}$ est racine de $P = a + bX + cX^2 \in \mathbf{Q}[X]$, ce qui par la question précédente prouve que $\deg P < 2$ (autrement dit que $c = 0$).
Si $\deg P = 1$ (donc si $b \neq 0$), alors $\sqrt[3]{2} = -\dfrac{a}{b} \in \mathbf{Q}$, ce qui est absurde, donc $b = 0$, et donc nécessairement $a = 0$.

Donc $\left(1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right)$ est une famille libre du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}\left(\sqrt[3]{2}\right)$, et donc en est une base, si bien que $\boxed{\left[\mathbf{Q}\left(\sqrt[3]{2}\right) : \mathbf{Q}\right] = 3.}$

1.d. Soient $q_1, \dots, q_n \in \mathbf{Q}$ tel que $\sum_{i=1}^{n} q_i \ln(p_i) = 0$.

Quitte à multiplier tous les q_i par le PGCD de leurs dénominateurs, on peut les supposer entiers[8].

[8] Relatifs.

Et donc $\ln\left(\prod_{i=1}^{n} p_i^{q_i}\right) = 0 \Leftrightarrow \prod_{i=1}^{n} p_i^{q_i} = 1$.

En séparant les i pour lesquels $q_i \geqslant 0$ de ceux pour lesquels $q_i < 0$, on a

$$\prod_{\substack{i=0 \\ q_i \geqslant 0}}^{n} p_i^{q_i} = \prod_{\substack{i=0 \\ q_i < 0}}^{n} p_i^{-q_i}.$$

Et alors par unicité de la décomposition en produit de facteurs premiers, $q_1 = q_2 = \cdots = q_n = 0$.

Donc la famille $(\ln(p_1), \dots, \ln(p_n))$ est une famille libre du $\mathbf{Q}$-espace vectoriel $\mathbf{R}$.
Si $\mathbf{R}$ était une extension finie de $\mathbf{Q}$, alors le cardinal des familles libres serait majoré par $[\mathbf{R} : \mathbf{Q}]$.
Mais puisqu'il existe une infinité de nombres premiers, il existe des familles libres de cardinal arbitrairement grand, si bien que $\boxed{\mathbf{R} \text{ n'est pas une extension finie de } \mathbf{Q}.}$

2. Soit $x \in \mathbf{L}$. Alors il existe $\lambda_1, \dots, \lambda_p \in \mathbf{K}$ tels que $x = \sum_{j=1}^{p} \lambda_j \beta_j$.

Mais pour tout $j \in [\![1, p]\!]$, il existe $\mu_{1,j}, \dots, \mu_{n,j} \in k$ tels que $\lambda_j = \sum_{i=1}^{n} \mu_{i,j} \alpha_i$.

Et donc $x = \sum_{j=1}^{p} \lambda_j \beta_j = \sum_{j=1}^{p} \sum_{i=1}^{n} \mu_{i,j} \alpha_i \beta_j$.

Donc la famille $(\alpha_i \beta_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ est une famille génératrice du k-espace vectoriel $\mathbf{L}$.
Ce qui prouve déjà que $\mathbf{L}$ est une extension finie de k, avec $[\mathbf{L} : k] \leqslant np$.

> **Rappel**
> La dimension d'un espace vectoriel est inférieure ou égale au cardinal de toute famille génératrice.

Prouvons à présent qu'il s'agit d'une famille libre : soient $(\mu_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ des éléments de k tels que $\sum_{i=1}^{n} \sum_{j=1}^{p} \mu_{i,j} \alpha_i \beta_j = 0$.

Alors $\sum_{j=1}^{p} \underbrace{\left(\sum_{i=1}^{n} \mu_{i,j} \alpha_i\right)}_{\in \mathbf{K}} \beta_j = 0$.

Par liberté de $(\beta_1, \dots, \beta_p)$ dans le $\mathbf{K}$-espace vectoriel $\mathbf{L}$, pour tout $j \in [\![1, p]\!]$, $\sum_{i=1}^{n} \mu_{i,j} \alpha_i = 0$.

Et par liberté de $(\alpha_1, \dots, \alpha_n)$ dans le k-espace vectoriel $\mathbf{K}$, pour tout $(i, j) \in [\![1, n]\!] \times [\![1, p]\!]$, $\mu_{i,j} = 0$.
Et donc $(\alpha_i \beta_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ est une famille libre du k-espace vectoriel $\mathbf{L}$, et donc en est une base.

Ainsi, $[\mathbf{L} : k] = \dim_k \mathbf{L} = n \times p = \dim_k \mathbf{K} \times \dim_{\mathbf{K}} \mathbf{L} = \boxed{[\mathbf{L} : \mathbf{K}] \times [\mathbf{K} : k].}$

Partie II. Éléments algébriques

3. Soit $x \in \mathbf{K}[\alpha]$. Alors il existe $n \in \mathbf{N}$ et $a_0, \dots, a_n \in \mathbf{K}$ tels que $x = \sum_{k=0}^{n} a_k \alpha^k$.

Si on note $P = \sum_{k=0}^{n} a_k X^k$, alors $x = P(\alpha)$, si bien que $x \in \{P(\alpha),\ P \in \mathbf{K}[X]\}$.

Et inversement, si $x = P(\alpha)$, avec $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{K}[X]$, alors $P(\alpha)$ est combinaison linéaire des éléments $\alpha^0, \alpha, \dots, \alpha^n$ du $\mathbf{K}$-espace vectoriel $\mathbf{L}$.
Donc $\{P(\alpha), P \in \mathbf{K}[X]\} \subset \mathbf{K}[\alpha]$. Donc par double inclusion, $\mathbf{K}[\alpha] = \{P(\alpha), P \in \mathbf{K}[X]\}$.

Soient $x, y \in \mathbf{K}[\alpha]$. Alors il existe $P, Q \in \mathbf{K}[X]$ tels que $x = P(\alpha)$ et $y = Q(\alpha)$.
Et donc $x - y = (P - Q)(\alpha) \in \mathbf{K}[\alpha]$ et $xy = (PQ)(\alpha) \in \mathbf{K}[\alpha]$.
Comme par ailleurs, $1 \in \mathbf{K}$ par définition d'un corps, $\mathbf{K}[\alpha]$ est un sous-anneau de $\mathbf{L}$.

Si A est un sous-anneau de $\mathbf{L}$ qui contient $\mathbf{K}$ et α, alors pour tout $k \in \mathbf{N}$, $\alpha^k \in A$ par stabilité de A par produit.
Et donc pour tout $k \in \mathbf{N}$ et tout $\lambda \in \mathbf{K} \subset A$, $\lambda\alpha^k \in A$.
Et donc quels que soient $a_0, \dots, a_n \in \mathbf{K}$, $a_0 + a_1\alpha + \cdots + a_n\alpha_n \in A$ par stabilité de A par somme.
Donc $\mathbf{K}[\alpha] \subset A$, si bien que $\mathbf{K}[\alpha]$ est bien le plus petit sous-anneau de $\mathbf{L}$ qui contient à la fois $\mathbf{K}$ et α.

4. Soit $\alpha \in \mathbf{L}$. Si α est algébrique sur $\mathbf{K}$, alors il existe $P \in \mathbf{K}[X]$, non nul, tel que $P(\alpha) = 0$.
Donc en notant $n = \deg P$, et $P = \sum_{k=0}^{n} a_k X^k$, avec $a_0, \dots, a_n \in \mathbf{K}$ non tous nuls, on obtient $\sum_{k=0}^{n} a_k \alpha^k = 0$, avec les a_k non tous nuls, si bien que $(1, \alpha, \dots, \alpha^n)$ est liée dans le $\mathbf{K}$-espace vectoriel $\mathbf{L}$.

Inversement, s'il existe $n \in \mathbf{N}$ tel que $(1, \alpha, \dots, \alpha^n)$ soit liée, alors il existe des scalaires $a_0, a_1, \dots, a_n \in \mathbf{K}$, non tous nuls tels que $\sum_{k=0}^{n} a_k \alpha^k = 0$.
Posons alors $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{K}[X]$, qui est non nul puisque l'un au moins des a_k est non nul.
Alors $P(\alpha) = 0$, si bien que α est algébrique sur $\mathbf{K}$.

5. Si α est algébrique de degré 1, alors $(1, \alpha)$ est liée.
Donc il existe $\lambda \in \mathbf{K}$ tel que $\alpha = \lambda 1 = \lambda \in \mathbf{K}$.

Et inversement, si $\alpha \in \mathbf{K}$, alors $\underbrace{\alpha}_{\in \mathbf{K}} + (-1)\alpha = 0$, qui est donc une combinaison linéaire[9] nulle dont les coefficients ne sont pas tous nuls. Donc $(1, \alpha)$ est liée, si bien α est algébrique de degré au plus 1.
La famille formée du seul vecteur (de $\mathbf{L}$) 1 étant libre, α est bien de degré 1.

[9] À coefficients dans $\mathbf{K}$

6. Supposons que $\mathbf{L}$ soit une extension finie de $\mathbf{K}$, et notons $d = [\mathbf{L} : \mathbf{K}]$. Soit alors $\alpha \in \mathbf{L}$. La famille $(1, \alpha, \dots, \alpha^d)$ est une famille de $\mathbf{L}$, de cardinal $d + 1 > d = \dim_{\mathbf{K}} \mathbf{L}$, donc elle est liée.
Par la question 4, α est alors algébrique sur $\mathbf{K}$, et par définition du degré de α, celui-ci est inférieur ou égal à d.

7.a. Par définition de d, $(1, \alpha, \alpha^2, \dots, \alpha^{d-1})$ est une famille libre de $\mathbf{K}[\alpha]$.
Prouvons qu'elle est génératrice.
Puisque $(1, \alpha, \dots, \alpha^d)$ est liée, il existe $\lambda_0, \dots, \lambda_d \in \mathbf{K}$, non tous nuls, tels que $\lambda_0 + \lambda_1\alpha + \cdots + \lambda_d\alpha^d = 0$.
On ne peut avoir $\lambda_d = 0$, car on aurait alors $\lambda_0 + \lambda_1\alpha + \cdots + \lambda_{d-1}\alpha^{d-1} = 0$, avec $\alpha_0, \dots, \alpha_{d-1}$ non tous nuls, ce qui contredit la liberté de $(1, \alpha, \dots, \alpha^{d-1})$.
Donc $\lambda_d \neq 0$, si bien que $\alpha^d = -\frac{1}{\lambda_d} \sum_{k=0}^{d-1} \lambda_k \alpha^k \in \mathrm{Vect}(1, \alpha, \dots, \alpha^{d-1})$.

Prouvons alors par récurrence sur n que $\alpha^n \in \mathrm{Vect}(1, \alpha, \dots, \alpha^{d-1})$.
Pour $n < d$ c'est évident, et si $n = d$, cela vient d'être fait.
Supposons $\alpha^n \in \mathrm{Vect}(1, \alpha, \dots, \alpha^{d-1})$, et soient $\lambda_0, \dots, \lambda_{d-1} \in \mathbf{K}$ tels que $\alpha^n = \lambda_0 + \lambda_1\alpha + \cdots + \lambda_{d-1}\alpha^{d-1}$.
Alors

$$\alpha^{n+1} = \underbrace{\lambda_0\alpha + \lambda_1\alpha^2 + \cdots + \lambda_{d-2}\alpha^{d-1}}_{\in \mathrm{Vect}(1,\dots,\alpha^{d-1})} + \underbrace{\lambda_d\alpha^d}_{\in \mathrm{Vect}(1,\dots,\alpha^{d-1})} \in \mathrm{Vect}(1, \alpha, \dots, \alpha^{d-1}).$$

Donc pour tout $n \in \mathbf{N}$, $\alpha^n \in \text{Vect}(1, \alpha, \dots, \alpha^{d-1})$, si bien que[10] $\text{Vect}(\alpha^n, n \in \mathbf{N}) \subset \text{Vect}\left(1, \alpha, \dots, \alpha^{d-1}\right)$.
Et donc $(1, \alpha, \dots, \alpha^{d-1})$ est génératrice de $\mathbf{K}[\alpha]$, et donc en est une base.

[10] $\text{Vect}(\alpha^n, n \in \mathbf{N})$ est le plus petit sous-espace vectoriel de $\mathbf{L}$ qui contient tous les α^n.

7.b. Soient $x, y \in \mathbf{K}[\alpha]$, et soit $\lambda \in \mathbf{K}$. Alors

$$f_\beta(\lambda x + y) = \beta(\lambda x + y) = \lambda\beta x + \beta y = \lambda f_\beta(x) + f_\beta(y)$$

donc f_β est une application $\mathbf{K}$-linéaire, et donc un endomorphisme du $\mathbf{K}$-espace vectoriel $\mathbf{K}[\alpha]$.
Par ailleurs, $\text{Ker}\, f_\beta = \{x \in \mathbf{K}[\alpha] \mid \beta x = 0\}$.
Mais puisque $\mathbf{K}[\alpha]$ est un corps, il est intègre, et donc pour $\beta \neq 0$, $\beta x = 0 \Rightarrow x = 0$.
Donc $\text{Ker}\, f_\beta = \{0\}$, et donc f est injective.

Puisque $\mathbf{K}[\alpha]$ est un $\mathbf{K}$-espace vectoriel de dimension finie, puisque f_β est injective, c'est un automorphisme.

7.c. En particulier, pour $\beta \neq 0$, f_β est surjective, donc il existe $x \in \mathbf{K}[\alpha]$ tel que $\beta x = 1$. Si l'existence d'un tel x était évidente[11] dans $\mathbf{L}$, ce que nous venons de prouver c'est que cet inverse est dans $\mathbf{K}[\alpha]$.
Donc $\mathbf{K}[\alpha]$ est un sous-anneau de $\mathbf{L}$ dans lequel tout élément non nul est inversible, c'est donc un sous-corps de $\mathbf{L}$, qui contient clairement $\mathbf{K}$ et α.

[11] C'est β^{-1}.

De plus, si k est un sous-corps de $\mathbf{L}$ qui contient $\mathbf{K}$ et α, alors c'est un sous-anneau de $\mathbf{L}$ qui contient α, et donc il contient $\mathbf{K}[\alpha]$.
Donc $\mathbf{K}[\alpha]$ est le plus petit sous-corps de $\mathbf{L}$ qui contient $\mathbf{K}$ et α.

7.d. On a déjà dit que $(1, \alpha, \dots, \alpha^{d-1})$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}[\alpha]$, donc que $[\mathbf{K}[\alpha] : \mathbf{K}] = d$.

7.e. Notons $\mathbf{Q}[\sqrt[3]{2}]$ l'anneau défini ci-dessus.
Puisque $\sqrt[3]{2}$ est algébrique sur $\mathbf{Q}$ (car racine de $X^3 - 2 \in \mathbf{Q}[X]$), $\mathbf{Q}[\sqrt[3]{2}]$ est un corps.
La famille $\left(1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right)$ est libre sur $\mathbf{Q}$, comme cela a été prouvé à la question 1.c.ii.
Par ailleurs, $\left(1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2, \left(\sqrt[3]{2}\right)^3\right)$ n'est pas libre puisque $\left(\sqrt[3]{2}\right)^3 = 2 \times 1$.
Donc le degré de $\sqrt[3]{2}$ sur $\mathbf{Q}$ est 3, de sorte que $\mathbf{Q}[\sqrt[3]{2}] = \text{Vect}\left(1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right)$, qui est bien l'ensemble $\mathbf{Q}\left(\sqrt[3]{2}\right)$ décrit à la question 1. Et donc cet ensemble est bien un sous-corps de $\mathbf{C}$.

8. L'implication *i)* $\Rightarrow$ *ii)* est évidente.
ii) $\Rightarrow$ *iii)*. Si $\alpha^{-1} \in \mathbf{K}[\alpha]$, il existe $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbf{K}[X]$ tel que $\alpha^{-1} = P(\alpha)$.
Et alors en multipliant par α, il vient $1 = \sum_{i=0}^{n} a_i \alpha^{i+1} \Leftrightarrow -1 + \sum_{i=0}^{n} a_i \alpha^{i+1} = 0$.
Donc α est racine de $-1 + \sum_{i=0}^{n} a_i X^{i+1} \in \mathbf{K}[X]$, et ce dernier polynôme est non nul puisque son coefficient constant est non nul. Donc α est algébrique sur $\mathbf{K}$.

Enfin, nous avons déjà prouvé *iii)* $\Rightarrow$ *i)*.

Partie III. Polynôme minimal d'un élément algébrique

9. L'existence d'un polynôme de degré q dans I_α découle de la définition même de q.
En divisant ce polynôme par son coefficient dominant, on obtient encore un élément de I_α, qui contient donc au moins un polynôme unitaire de degré q.

Supposons que P_1, P_2 sont deux polynômes unitaires de degré q tels que $P_1(\alpha) = P_2(\alpha) = 0$.
Alors $P_1 - P_2$ est encore dans I_α (puisque $P_1(\alpha) - P_2(\alpha) = 0$), et est de degré strictement inférieur à q.
Par définition de q, ceci signifie que $P_1 - P_2 = 0_{\mathbf{K}[X]}$, et donc $P_1 = P_2$.
Ainsi, I_α contient un unique polynôme unitaire de degré q.

Détails
Les termes de plus haut degré de P_1 et P_2 sont tous deux égaux à X^q, et donc s'annulent.

10. Supposons par l'absurde que $\mu_\alpha = PQ$, avec $P, Q \in \mathbf{K}[X]$ et $\deg P < q$.
Alors $P(\alpha)Q(\alpha) = \mu_\alpha(\alpha) = 0$. Or $\mathbf{L}$ est un corps, donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$.
On ne peut pas avoir $P(\alpha) = 0$ par définition[12] de q. Et donc $Q(\alpha) = 0$. Mais $\deg Q \leqslant q$, et encore par définition de q, $\deg Q \geqslant q$. On en déduit que $\deg Q = q$, et donc $\deg P = 0$.
Ainsi, $\mu_\alpha = PQ \Rightarrow \deg P = 0$ **ou** $\deg Q = 0$, donc $\boxed{\mu_\alpha \text{ est irréductible sur } \mathbf{K}[X].}$

[12] P ne peut pas être nul puisque μ_α ne l'est pas.

Il est évident que si $Q \in \mathbf{K}[X]$, alors $(\mu_\alpha Q)(\alpha) = 0$, et donc $\mu_\alpha Q \in I_\alpha$.
Inversement, soit $P \in I_\alpha$, et soit $P = \mu_\alpha Q + R$ la division euclidienne de P par μ_α.
Alors $0 = P(\alpha) = \mu_\alpha(\alpha)Q(\alpha) + R(\alpha) \Leftrightarrow R(\alpha) = 0$.
Or $\deg R < q$, si bien que toujours par définition de Q, $R = 0_{\mathbf{K}[X]}$. Et donc $P = \mu_\alpha Q$.

Ainsi, on a bien prouvé que $\boxed{I_\alpha = \{\mu_\alpha Q,\ Q \in \mathbf{K}[X]\}.}$

Autrement dit
Les polynômes annulateurs de α sont les multiples de son polynôme minimal.

11. Puisque α est algébrique de degré d, la famille $(1, \alpha, \dots, \alpha^d)$ est liée dans le $\mathbf{K}$-espace vectoriel $\mathbf{L}$.
Et donc il existe $a_0, a_1, \dots, a_d$ non tous nuls tels que $0 = \sum_{i=0}^{d} a_i \alpha^i$. Donc α est racine du polynôme $\sum_{i=0}^{d} a_i X^i$, qui est donc non nuls puisque ses coefficients ne sont pas tous nuls.
Et donc $\deg \mu_\alpha = q \leqslant d$.

Inversement, si $\deg \mu_\alpha = q$, alors il existe $a_0, \dots, a_q \in \mathbf{K}$, avec $a_q \neq 0$ tels que $\mu_\alpha = \sum_{i=0}^{q} a_i X^i$.
Et donc $0 = \mu_\alpha(\alpha) = \sum_{i=0}^{q} a_i \alpha^i$ est une combinaison linéaire de $1, \alpha, \dots, \alpha^q$, nulle et à coefficients non tous nuls, donc $(1, \alpha, \dots, \alpha^q)$ est liée.
Par définition du degré de α sur $\mathbf{K}$, ce degré d est inférieur ou égal à q.
Et donc $d = q = \deg \mu_\alpha$.

Remarque
Notons au passage que ceci prouve qu'il existe des polynômes irréductibles de degré 3 dans $\mathbf{Q}[X]$, ce qui n'est par exemple pas le cas dans $\mathbf{R}[X]$ ou $\mathbf{C}[X]$.
On prouverait plus généralement (mais c'est plus dur) que pour tout $n \in \mathbf{N}$, $X^n - 2$ est irréductible dans $\mathbf{Q}[X]$.

12. Puisque $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$, le degré de $\sqrt[3]{2}$ sur $\mathbf{Q}$ est égal à 3. Or $X^3 - 2$ est un polynôme unitaire de $\mathbf{Q}[X]$, de degré 3, qui annule $\sqrt[3]{2}$: c'est son polynôme minimal.

13. Il est clair que α est racine de $\left(X - \sqrt{2}\right)^2 - 3$.
Donc α est algébrique sur $\mathbf{Q}(\sqrt{2})$, de degré au plus 2.
S'il était de degré 1, cela signifierait que $\alpha \in \mathbf{Q}(\sqrt{2})$. Et alors $\sqrt{3} = \alpha - \sqrt{2} \in \mathbf{Q}(\sqrt{2})$.
Mais pour $(a, b) \in \mathbf{Q}^2$, on a $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$ est égal à 3 si et seulement si[13] $\begin{cases} a^2 + 2b^2 = 3 \\ ab = 0 \end{cases}$, système qui n'a pas de solutions rationnelles puisque $\sqrt{3} \notin \mathbf{Q}$.
Donc α est algébrique sur $\mathbf{Q}(\sqrt{2})$ de degré 2.
Autrement dit $[\mathbf{Q}(\sqrt{2})(\alpha) : \mathbf{Q}(\sqrt{2})] = 2$.
Et donc par la question 2, $[\mathbf{Q}(\sqrt{2})[\alpha] : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2})[\alpha] : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 4$.

[13] La famille $(1, \sqrt{2})$ est libre dans le $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\sqrt{2})$, ce qui signifie que l'écriture d'un élément de $\mathbf{Q}(\sqrt{2})$ sous la forme $a + b\sqrt{2}$ est unique.

Détails
C'est la question 6 : on a une extension de $\mathbf{Q}$ de dimension 4, donc tout élément de cette extension est algébrique sur $\mathbf{Q}$, de degré au plus 4.

Ceci prouve déjà que α est algébrique sur $\mathbf{Q}$ de degré inférieur ou égal à 4.

Par ailleurs, $\alpha^2 = 5 + 2\sqrt{6}$, et donc

$$\alpha^3 = (5 + 2\sqrt{6})(\sqrt{2} + \sqrt{3}) = 5\sqrt{2} + 5\sqrt{3} + 2\sqrt{12} + 2\sqrt{18} = 11\sqrt{2} + 9\sqrt{3}.$$

Et donc $\alpha^3 - 9\alpha = 2\sqrt{2}$, si bien que $\sqrt{2} = \dfrac{\alpha^3 - 9\alpha}{2}$.
Donc $\mathbf{Q}[\alpha]$ est un corps[14] qui contient $\mathbf{Q}$ et $\sqrt{2}$, donc qui contient $\mathbf{Q}(\sqrt{2})$. Comme il contient de plus α, il contient $\mathbf{Q}(\sqrt{2})[\alpha]$. Et bien entendu, $\mathbf{Q}(\sqrt{2})[\alpha]$ contient $\mathbf{Q}$ et α, donc contient $\mathbf{Q}[\alpha]$.
On a donc $\mathbf{Q}(\sqrt{2})[\alpha] = \mathbf{Q}[\alpha]$.
Donc $[\mathbf{Q}[\alpha] : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2})[\alpha] : \mathbf{Q}]$, qui vaut 4 par ce qui a été dit précédemment.
Et donc cela signifie que le polynôme minimal de α sur $\mathbf{Q}$ est de degré 4.
Ceci implique en particulier qu'aucun polynôme à coefficients rationnels de degré inférieur ou égal à 3 ne possède α pour racine.

[14] Car α est algébrique sur $\mathbf{Q}$.

En revanche, cela ne nous aide pas à calculer ce polynôme minimal, dont on pourrait prouver qu'il vaut $X^4 - 10X^2 + 1$.

Partie IV. Nombres algébriques (sur Q)

14.a. Puisque β est racine d'un polynôme non nul à coefficients dans $\mathbf{Q}$, il est racine du même polynôme, vu comme polynôme à coefficients dans $\mathbf{Q}[\alpha]$.
Et donc β est algébrique sur $\mathbf{Q}[\alpha]$, si bien que $\mathbf{Q}[\alpha,\beta]$ est un corps, à savoir le plus petit sous-corps de $\mathbf{C}$ qui contient $Q[\alpha]$ et β.
Et on a alors $\mathbf{Q}[\alpha,\beta]$ est une extension finie de $\mathbf{Q}[\alpha]$, lui-même extension finie de $\mathbf{Q}$, donc par la question 2, $\mathbf{Q}[\alpha,\beta]$ est une extension finie de $\mathbf{Q}$ et

$$[\mathbf{Q}[\alpha,\beta] : \mathbf{Q}] = [\mathbf{Q}[\alpha,\beta] : \mathbf{Q}[\alpha]][\mathbf{Q}[\alpha] : \mathbf{Q}].$$

14.b. **Exemple** : $\sqrt{3}$ est algébrique sur $\mathbf{Q}(\sqrt{2})$, et le polynôme minimal de $\sqrt{3}$ sur $\mathbf{Q}(\sqrt{2})$ divise tout polynôme annulateur de $\sqrt{2}$, et donc en particulier divise $X^2 - 3$.
Donc déjà le degré de ce polynôme annulateur est inférieur ou égal à 2.
De plus[15], $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$, donc $\sqrt{3}$ est de degré 2 sur $\mathbf{Q}(\sqrt{2})$ et donc $[\mathbf{Q}[\sqrt{2},\sqrt{3}] : \mathbf{Q}] = 4$.

[15] Ceci a été prouvé à la question 13.

Ainsi, $(1,\sqrt{3})$ est une base de$\mathbf{Q}[\sqrt{2},\sqrt{3}]$ en tant que $\mathbf{Q}(\sqrt{2})$-espace vectoriel.
Puisque $(1,\sqrt{2})$ est une base de $\mathbf{Q}(\sqrt{2})$ en tant que $\mathbf{Q}$-espace vectoriel, par la question 2, $(1,\sqrt{2}\times 1, 1\times\sqrt{3}, \sqrt{2}\times\sqrt{3})$ est une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[\sqrt{2},\sqrt{3}]$.
Donc $\boxed{\mathbf{Q}[\sqrt{2},\sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, (a,b,c,d) \in \mathbf{Q}^4\}.}$

15. Il est clair que $1 \in \overline{\mathbf{Q}}$.
Soient $\alpha,\beta \in \overline{\mathbf{Q}}$. Alors $\mathbf{Q}[\alpha,\beta]$ est un sous-corps de $\mathbf{C}$ qui contient $\mathbf{Q}[\alpha]$ (et donc α) et contient β. Donc il contient $\alpha - \beta$ et $\alpha\beta$.
Mais puisque $\mathbf{Q}[\alpha,\beta]$ est une extension finie de $\mathbf{Q}$, tous ses éléments sont algébriques sur $\mathbf{Q}$, et donc $\alpha - \beta$ et $\alpha\beta$ sont algébriques.
Donc déjà $\overline{\mathbf{Q}}$ est un sous-anneau de $\mathbf{C}$.

Enfin, si α est un nombre algébrique non nul, alors $\alpha^{-1} \in \mathbf{Q}[\alpha]$, qui est une extension finie de $\mathbf{Q}$, donc α^{-1} est algébrique sur $\mathbf{Q}$.
Donc $\boxed{\overline{\mathbf{Q}} \text{ est un sous-corps de } \mathbf{C}.}$

Remarque

Ceci nous dit que si α et β sont annulés par un polynôme à coefficients rationnels, alors il en est de même de $\alpha-\beta$ et $\alpha+\beta$, mais ne nous dit pas comment calculer de tels polynômes à partir de ceux annulant α et β.