Partie I :

1. $(f-ae)\circ(f-be) = f^2-(a+b)f+abe = a^2p+b^2q-(a+b)(ap+bq)+ab(p+q) = 0$.
   Le polynôme $(X-a)(X-b)$ est scindé à racines simples. C'est un polynôme annulateur de f. f est donc diagonalisable.
2. (a) On trouve facilement $f-ae = (b-a)q$ et $f-be = (a-b)p$.
   $(f-ae)(f-be) = 0 = -(b-a)^2(p\circ q)$. Même calcul pour $q\circ p$.
   Comme $b-a \neq 0$, $pq = qp = 0$. De même
   $(f-ae)^2 = (b-a)^2q^2 = f^2-2af+a^2e = a^2p+b^2q-2a(ap+bq)+a^2(p+q)$
   p et q sont deux projecteurs.

   (b) Le spectre de f est inclus dans l'ensemble des racines d'un polynôme annulateur. Ce spectre est non vide car f est un endomorphisme d'un $\mathbb{C}$-ev et son polynôme caractéristique est scindé.
   On a donc $Sp(f) \subset \{a,b\}$ et $Sp(f) \neq \emptyset$.
   Si $Sp(f) = \{a\}$, comme f est diagonalisable, $E = E_a(f)$ et
   $\forall x \in E$, $f(x) = ax$. Donc $f = ae$ et on a $a(p+q) = ap+bq = f$ donc $(b-a)q = 0$ et comme $b \neq 0$, $q = 0$, ce qui n'est pas.
   De même si $Sp(f) = \{b\}$ on aurait $p = 0$. On a donc $S_p(f) = \{a,b\}$.

   (c) $ab \neq 0$, a et b ne sont pas nuls et 0 n'est pas valeur propre de f. f est inversible. On montre par récurrence que $\forall n \in \mathbb{N}, f^n = a^np+b^nq$.
   Cette propriété est vraie pour $n = 0$.
   Supposons la vraie pour un entier n fixé. On a alors
   $f^{n+1} = f^nf = (a^np+b^nq)(ap+bq) = a^{n+1}p+b^{n+1}q$ car $pq = qp = 0$.
   La propriété est vraie pour $n+1$, donc elle est vraie pour tout n de $\mathbb{N}$.
   Pour tout entier $n \in \mathbb{N}$:
   $(a^{-n}p+b^{-n}q)(a^np+b^nq) = p+q = e$ car $pq = qp = 0$.
   $(a^np+b^nq(a^{-n}p+b^{-n}q)) = p+q = e$
   On en déduit que $\forall n \in \mathbb{N}$, $(f^n)^{-1} = (f^{-1})^n = f^{-n} = a^{-n}p+b^{-n}q$.
   Finalement $\forall m \in \mathbb{Z}$, $f^m = a^mp+b^mq$.
3. On sait déjà que p est un projecteur. On a vu également que :
   $p = \frac{1}{a-b}(f-be)$. Donc $\ker p = \ker(f-be)$.
   De plus $p(x) = x \Leftrightarrow f(x)-bx = (a-b)x \Leftrightarrow f(x) = ax$.
   L'ensemble des vecteurs invariants par f est $\ker(f-ae)$.
   p est le projecteur sur $\ker(f-ae)$ parallèlement à $\ker(f-be)$.
   De même q est le projecteur sur $\ker(f-be)$ parallèlement à $\ker(f-ae)$.
4. On pose $F = \{xp+yq/\,(x,y) \in \mathbb{C}^2\}$.

   (a) $F = Vect(p,q)$ est un sous-espace vectoriel de $\mathcal{L}(E)$. (p,q) est une famille génératrice de F. Elle est libre car :
   $$\forall (x,y) \in \mathbb{C}^2,\ xp+yq = 0 \Rightarrow p(xp+yq) = 0 = xp^2 = xp \Rightarrow x = 0 \,\text{car}\, p \neq 0$$
   De même en composant par q on obtient $y = 0$. F est de dimension 2.
   Soit $f_1 = xp+yq$ et $f_2 = x'p+y'q$ deux éléments quelconques de F.
   $$f_1\circ f_2 = f_1f_2 = (xp+yq)(x'p+y'q) = xx'p^2+xy'pq+x'yqp+yy'q^2 = xx'p+yy'q \in F$$
   F est stable pour le produit .

(b) Soit $f_1 = xp + yq \in F$. $f_1^2 = x^2 p + y^2 q$. Comme (p, q) est libre on a :

$$f_1 \,\text{projecteur} \Leftrightarrow f_1^2 = f_1 \Leftrightarrow x^2 = x \,\text{et}\, y^2 = y$$

Il y a quatre projecteurs dans F : $0, p, q, p + q = e$.

(c) De même $f_1^2 = f$ ssi $x^2 = a$ et $y^2 = b$.
Comme x est un élément non nul il existe deux éléments de $\mathbb{C}$ distincts et opposés $\pm\delta$ vérifiant $\delta^2 = x$. De même il existe deux éléments distincts et opposés $\pm\delta'$ tels que $\delta'^2 = y$. $R(f) \cap F$ contient donc quatre éléments distincts $\delta p + \delta' q$, $\delta p - \delta' q$, $-\delta p + \delta' q$, $-\delta p - \delta' q$

5. Exemple : on pose $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$,$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

(a) $J^2 = 3J$. Par une récurrence immédiate, pour tout entier m **strictement positif** $J^m = 3^{m-1} J$. Comme $A = I + J$ et que I et J commutent on a

$$A^m = (I+J)^m = \sum_{k=0}^{m} \binom{m}{k} I^{m-k} J^k = I + \sum_{k=1}^{m} \binom{m}{k} 3^{k-1} J = I + \frac{1}{3}\left(\sum_{k=0}^{m} \binom{m}{k} 3^k - 1\right) J$$

$$A^m = I + \frac{1}{3}\left((1+3)^m - 1\right) J = \left(I - \frac{1}{3} J\right) + \frac{4^m}{3} J$$

(b) Prenons $a = 1$, $b = 4$, $A = I - \dfrac{1}{3} J$ et $B = \dfrac{1}{3} J$ on a :
$\forall m \in \mathbb{N}$, $A^m = a^m B + b^m C$.

(c) Soit f endomorphisme de $\mathbb{C}^3$ de matrice A dans la base canonique. f vérifie les hypothèses de la question précédente avec p et q de matrice B et C dans la base canonique.
Comme $f = p + 4q$ les quatre éléments de $\mathcal{R}(f) \cap F$ sont $p + 2q, p - 2q, -p + 2q, -p - 2q$.
On obtient ainsi quatre matrices M telles que $M^2 = A$. $B + 2C, B - 2C, -B + 2C, -B - 2C$. De manière explicite les solutions sont

$$\pm \frac{1}{3} \begin{pmatrix} 4 & 1 & 1 \\ 1 & 4 & 1 \\ 1 & 1 & 4 \end{pmatrix} \qquad \pm \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix}$$

Partie II

1. Soit P un polynôme quelconque de $\mathbb{C}[X]$ degré r écrit sous la forme $P = \displaystyle\sum_{m=0}^{r} a_m X^m$. On a :

$$P(f) = \sum_{m=0}^{r} a_m \left(\sum_{k=1}^{n} x_k^m p_k\right) = \sum_{k=1}^{n} \left(\sum_{m=0}^{r} a_m x_k^m\right) p_k = \sum_{k=1}^{n} P(x_k) p_k$$

2. (a) D'après la formule précédente, comme les x_k sont racines de Π, $\Pi(f) = 0$.
   Π est un polynôme annulateur de f, scindé à racines simples. f est diagonalisable.

   (b) Les polynômes L_k sont les polynômes de Lagrange associés à $x_1, ..., x_n$.
   La formule de la question 1 donne : $\forall k \in \mathbb{N}_n$, $L_k(f) = 1 \times p_k = p_k$.

   De même : $\forall (k,l) \in \mathbb{N}_n^2$, $p_k \circ p_l = L_k(f) \circ L_l(l) = (L_k L_l)(f) = \displaystyle\sum_{i=1}^{n} (L_k L_l(x_i)) p_i$.

   Si $k \neq l$ l'ensemble des racines de $L_k L_l$ est$\{x_1, ..., x_n\}$ et $p_k \circ p_l = 0$.

   Si $k = l$, $p_k^2 = \displaystyle\sum_{i=1}^{n} L_k^2(x_i) p_i = p_k$.

   (c) On sait que $S_p(f) \subset \{x_1, ..., x_n\}$, ensemble des racines d'un polynôme annulateur de f.
   On a vu que les p_i étaient des projecteurs, non nuls par hypothèse.
   Soit i fixé, il existe un vecteur non nul dans $Im(p_i)$, x qui vérifie $p_i(x) = x$ et donc pour $k \neq i$, $p_k(x) = p_k(p_i(x)) = (p_k p_i)(x) = 0$.

   Il vient, pour cet x, $f(x) = \displaystyle\sum_{k=1}^{n} x_k p_k(x) = x_i \times x$.

   x_i est valeur propre de f, et ce pour chaque i. D'où : $S_p(f) = \{x_1, ..., x_n\}$

3. f est diagonalisable, ses valeurs propres sont $x_1, ..., x_n$ donc $E = \oplus_{i=1}^{n} E_{x_i}(f)$.
   On a vu que pour i fixé et $x \in Im(p_i)$ on a $f(x) = x_i \times x$.
   Donc $Im(p_i) \subset \ker(f - x_i e)$.
   Réciproquement si $x \in \ker(f - x_i e)$:
   $f(x) = x_i \times x$ et $p_i(x) = L_i(f)(x) = L_i(x_i) \times x = x$ et $x \in Im(p_i)$. Par double inclusion on a donc $Im(p_i) = \ker(f - x_i e)$.
   Comme f est diagonalisable, $E = \oplus_{i=1}^{n} E_{x_i}(f) = \oplus_{i=1}^{n} \ker(f - x_i e) = \oplus_{i=1}^{n} Im(p_i)$.
   Soit k un entier fixé de $\{1, ..., n\}$. $\dim(\ker(p_k)) = n - \dim(Im(p_k)) = \displaystyle\sum_{i=1..n, i\neq k} \dim(Im(p_i))$.
   Cette dernière égalité est obtenue car les espaces sont en somme directe.
   Mais pour $i \neq k$ et $y \in Im(p_i)$, $p_k(y) = p_k(p_i(y))) = (p_k \circ p_i)(y) = 0$
   On a donc $Im(p_i) \subset \ker(p_k)$ pour $i \neq k$ et $\oplus_{i=1..n, i\neq k} Im(p_i) \subset \ker(p_k)$.
   On a démontré précédemment que ces deux sev avaient même dimension. La simple inclusion entraîne l'égalité.
   p_k est le projecteur sur $Im(p_k) = \ker(f - x_k e)$ parallèlement à
   $\ker(p_k) = \oplus_{i=1..n, i\neq k} Im(p_i) = V_k = \oplus_{1\leq i\leq n,\, i\neq k} \ker(f - x_i e)$.

4. On désigne par F le sous-espace de $\mathcal{L}(E)$ engendré par $\{p_1, ..., p_n\}$.

   (a) F est l'espace vectoriel engendré par les p_i. Cette famille est libre car

   $$\forall (\lambda_1, ..., \lambda_n) \in \mathbb{C}^n,\ \sum_{i=1}^{n} \lambda_i p_i = 0 \Rightarrow \forall k = 1..n, p_k \circ \left(\sum_{i=1}^{n} \lambda_i p_i \right) = 0 = \lambda_k p_k^2 = \lambda p_k$$

   Comme les p_i sont tous non nuls :

   $$\forall (\lambda_1, ..., \lambda_n) \in \mathbb{C}^n,\ \sum_{i=1}^{n} \lambda_i p_i = 0 \Rightarrow \forall k = 1..n,\ \lambda_k = 0$$

La famille est libre. $\dim(F) = n$.

(b) Soit $h = \sum_{i=1}^{n} \lambda_i p_i \in F$. On a $p_k p_l = 0$ si $k \neq l$ donc $h^2 = \sum_{i=1}^{n} \lambda_i^2 p_i$.
Compte-tenu de la liberté de la famille, $h^2 = f \Leftrightarrow \forall i, \lambda_i^2 = x_i$.
Si les x_i sont tous non-nuls on obtient 2^n choix possibles pour les λ_i et seulement 2^{n-1} si l'un des x_i est nul.
Le nombre d'éléments de $R(f) \cap F$ est donc 2^n ou 2^{n-1}.

(c) De même h est un projecteur ssi $h^2 = h$ donc ssi, pour tout i on a $\lambda_i = 1 \text{ ou } 0$. On a ainsi 2^n projecteurs définis de la manière suivante. Soit I l'ensemble des indices i de $\{1, ..., n\}$ tels que $\lambda_i = 1$ et J l'ensemble des indices j de $\{1, ..., n\}$ tels que $\lambda_j = 0$. On a $I \cap J = \emptyset$, $I \cup J = \{1, ..., n\}$ et $h = \displaystyle\sum_{i \in I} p_i$. Soit x un élément quelconque de E. $x = \displaystyle\sum_{k=1}^{n} p_k(x)$;
$h(x) = \left(\displaystyle\sum_{i \in I} p_i\right) \circ \left(\displaystyle\sum_{k=1}^{n} p_k\right)(x) = \left(\displaystyle\sum_{i \in I} p_i\right)(x)$

$$x \in Im(h) \Leftrightarrow h(x) = x = \sum_{i \in I} p_i(x) \quad \text{et} \quad x \in \ker(h) \Leftrightarrow x = \sum_{j \in J} p_j(x)$$

h est le projecteur sur $\oplus_{i \in I} \ker(f - x_i e)$ parallèlement à $\oplus_{j \in J} \ker(f - x_j e)$.

5. On suppose $n = N$.

(a) f possède $n = N = \dim(E)$ valeurs propres distinctes et comme les espaces propres sont en somme directe ils sont chacun de dimension 1. Soit $(\varepsilon_1, ..., \varepsilon_N)$ une base de vecteurs propres associés aux valeurs propres $(x_1, ..., x_N)$. Soit $g \in \mathcal{L}(E)$ tel que $g \circ f = f \circ g$. On a , pour tout i, $g(f(\varepsilon_i)) = f(g(\varepsilon_i))$. Donc $g(x_i \varepsilon_i) = f(g(\varepsilon_i)) = x_i g(\varepsilon_i)$. Le vecteur $g(\varepsilon_i)$ est élément de $E_{x_i}(f)$. Ce dernier espace est de dimension 1. Il existe donc, pour chaque i, un élément $\beta_i \in \mathbb{C}$ tel que $g(\varepsilon_i) = \beta_i \varepsilon_i$.

Soit alors y un vecteur quelconque de E, $y = \displaystyle\sum_{i=1}^{N} y_i \varepsilon_i$.

$\forall i \in \{1, .., N\}$, $p_i(y) = y_i \varepsilon_i$ et $g(y) = \displaystyle\sum_{i=1}^{N} y_i g(\varepsilon_i) = \sum_{i=1}^{N} y_i \beta_i \varepsilon_i = \sum_{i=1}^{N} \beta_i p_i(y)$.

On obtient $g = \displaystyle\sum_{i=1}^{N} \beta_i p_i \in F$.

Réciproquement si $g \in F$, il existe des éléments $\beta_1, ..., \beta_N$ de $\mathbb{C}$ tels que $g = \displaystyle\sum_{i=1}^{N} \beta_i p_i$. Pour tout i, $g(\epsilon_i) = \displaystyle\sum_{k=1}^{N} \beta_k p_k(\varepsilon_i) = \beta_i \varepsilon_i$.

La matrice de g dans la base $(\varepsilon_1, ..., \varepsilon_N)$ est diagonale, comme celle de f. Ces deux matrices commutent donc $f \circ g = g \circ f$. On a donc démontré : $\forall g \in \mathcal{L}(E)$, $g \circ f = f \circ g \Leftrightarrow g \in F$.

(b) Si $g = f^2$ alors $g \circ f = f^2 \circ f = f \circ f^2 = f \circ g$. D'après la question précédente les éléments de $R(f)$ sont dans F.

On a donc $R(f) \subset F$ et $R(f) = R(f) \cap F$, ensemble déjà étudié.

Le nombre d'éléments de $R(f)$ est 2^N si tous les x_i sont non nuls et de 2^{N-1} si l'un des x_i est nul.

6. Soit h un endomorphisme diagonalisable de E tel que $Sp(h) = \{x_1, ..., x_n\}$.
   Comme h est diagonalisable, $E = \oplus_{i=1}^n E_{x_i}(h)$. Soit pour chaque i, q_i le projecteur sur l'espace propre $E_{x_i}(h)$ parallèlement à la somme directe des autres.
   Tout élément y de E s'écrit de manière unique $y = \sum_{i=1}^n y_i$ avec, pour tout i, $y_i = q_i(y) \in E_{x_i}(h)$. Pour tout $P \in \mathbb{C}[X]$:
   $$P(h)(y) = \sum_{i=1}^n P(h)(y_i) = \sum_{i=1}^n P(x_i)y_i = \sum_{i=1}^n P(x_i)q_i(y)$$
   $P(h) = \displaystyle\sum_{i=1}^n P(x_i)q_i$ avec, en particulier, $\forall m \in \mathbb{N}$, $h^m = \displaystyle\sum_{k=1}^n x_k^m q_k$.

7. Exemple : On considère la matrice $A = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$.

   (a) $\chi_A(x) = \begin{vmatrix} -x & 1 & -1 \\ 1 & -x & -1 \\ -1 & 1 & -x \end{vmatrix} = \begin{vmatrix} -x & 1 & -1 \\ -x & -x & -1 \\ -x & 1 & -x \end{vmatrix} = \begin{vmatrix} -x & 1 & -1 \\ 0 & -x-1 & 0 \\ 0 & 0 & -x+1 \end{vmatrix}$.
   $\chi_A(x) - x(x-1)(x+1)$. Prenons $x_1 = -1, x_2 = 0, x_3 = 1$.

   (b) $L_1(X) = \dfrac{X(X-1)}{(-1) \times (-2)} = \dfrac{1}{2}(X^2 - X)$
   $L_2(X) = \dfrac{(X+1)(X-1)}{-1} = 1 - X^2$, $L_3(X) = \dfrac{(X+1)X}{2}$.
   Par calcul direct :
   $$L_1(A) = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 1 & -1 & 0 \end{pmatrix},\ L_2(A) = \begin{pmatrix} -1 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & 1 & 1 \end{pmatrix},\ L_3(A) = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

   (c) Soit M matrice quelconque de $\mathcal{M}_3(\mathbb{C})$ et f, g endomorphismes de $\mathbb{C}^3$ de matrice respective A et M dans la base canonique de $\mathbb{C}^3$.
   f vérifie les hypothèses des questions précédentes avec
   $p_1 = \frac{1}{2}(f^2 - f)$, $p_2 = Id_E - f^2$, $p_3 = \frac{1}{2}(f^2 + f)$.
   $M^= A \Leftrightarrow g^2 = f$. On est ramené à déterminer $R(f)$ qui possède ici quatre éléments $ip_1 + p_3, ip_1 - p_3, -ip_1 + p_3, -ip_1 - p_3$.
   D'où les quatre matrices solutions $\pm(iA_1 + A_3)$, $\pm(iA_1 - A_3)$
   $$\pm\begin{pmatrix} 1+i & -i & -1 \\ 1 & 0 & -1 \\ i & -i & 0 \end{pmatrix}, \quad \pm\begin{pmatrix} -1+i & -i & 1 \\ -1 & 0 & 1 \\ i & -i & 0 \end{pmatrix}$$

Partie III

Soit u un endomorphisme de E tel que $u^n = 0$ et $u^{n-1} \neq 0$.

1. (a) Comme $u^{n-1} \neq 0$ il existe un vecteur x de E tel que $u^{n-1}(x) \neq 0$. Choisissons un tel x et montrons que la famille $(x, u(x), ..., u^{n-1}(x))$ est libre.
Comme $u^n = 0$, pour $k \geq n$, $u^k = 0$.
$\forall(\alpha_0, ..., \alpha_{n-1}) \in \mathbb{C}^n, \sum_{k=0}^{n-1} \alpha_k u^k(x) = 0 \Rightarrow u^{n-1}\left(\sum_{k=0}^{n-1} \alpha_k u^k(x)\right) = 0$
$\sum_{k=0}^{n-1} \alpha_k u^k(x) = 0 \Rightarrow \alpha_0 u^{n-1}(x) = 0 \Rightarrow \alpha_0 = 0 \,\text{car}\, u^{n-1}(x) \neq 0.$
En composant successivement par $u^{n-2}, u^{n-3}, ..., u, Id_E$ on obtient successivement $\alpha_1 = ... = \alpha_{n-1} = 0$. La famille est libre.

(b) On a $u^n = 0$. Donc si P est un polynôme multiple de X^n, il existe un polynôme Q tel que $P(X) = X^n Q(X)$ et donc $P(u) = u^n \circ Q(u) = 0$.
Réciproquement soit P un polynôme annulateur de u. Effectuons la division euclidienne de P par X^n.
On peut écrire $P(X) = X^n Q(X) + R(X)$ avec $\deg(R) < n$.
On obtient $P(u) = 0 = u^n \circ Q(u) + R(u) = R(u)$.
Comme $\deg(R) < n$,il existe des éléments de $\mathbb{C}$, $\alpha_0, ..., \alpha_{n-1}$ tels que $R(X) = \sum_{k=0}^{n-1} \alpha_k X^k$. Mais $R(u) = 0$, donc en reprenant le vecteur x vu précédemment, $R(u)(x) = 0 = \sum_{k=0}^{n-1} \alpha_k u^k(x)$.
La liberté de la famille $(x, ..., u^{n-1}(x))$ entraine $\alpha_0 = ... = \alpha_{n-1} = 0$.
D'où $R = 0$ et $P = X^n Q$.
Finalement : $P(u) = 0 \Leftrightarrow X^n \,\text{divise}\, P$.

(c) Supposons que $R(u) \neq \emptyset$. Il existe $g \in \mathcal{L}(E)$ tel que $g^2 = u$. Mais alors $g^{2n} = 0$ et $g^{2n-2} = u^{n-1} \neq 0$.
Si $g^{2n-1} \neq 0$ il existe un vecteur x' tel que la famille $(x', g(x'), ..., g^{2n-1}(x'))$ soit libre.
Si $g^{2n-1} = 0$ il existe un vecteur x' tel que la famille $(x', g(x'), ..., g^{2n-2}(x'))$ soit libre. Le cardinal d'une famille libre est inférieur ou égal à la dimension de l'espace. Dans les deux cas on a $2n - 1 \leq N$.
D'où : $R(u) \neq \emptyset \Rightarrow n \leq \dfrac{N+1}{2}$.

2. (a) Le développement en série entière sur $]-1, 1[$ de $x \mapsto \sqrt{1+x} = (1+x)^{1/2}$ donne :

$$\forall x \in]-1, 1[, \sqrt{1+x} = \sum_{k=0}^{+\infty} a_k x^k \,\text{avec}\, a_0 = 1 \,\text{et pour}\, k \geq 1$$

$$a_k = \frac{(1/2)(1/2-1)...(1/2-k+1)}{k!}$$

.

(b) Utilisons le développement limité d'ordre $n-1$ de $x \mapsto \sqrt{1+x}$ en 0.
$\sqrt{1+x} =_0 \sum_{k=0}^{n} a_k x^k + o(x^n) = P_n(x) + a_n x^n + x^n \varepsilon(x)$ avec $\varepsilon(x) =_0 o(1)$.
En élevant au carré :
$1 + x =_0 P_n^2(x) + 2a_n x^n P_n(x) + a_n^2 x^{2n} + o(x^{2n})$
L'unicité du développement limité d'ordre $2n$ de $x \mapsto 1+x$ en 0 donne $1 + x = P_n^2(x) + x^n Q(x)$ avec Q fonction polynôme. Ceci montre que X^n divise $P_n^2 - X - 1$.
On prend dans la suite du problème $\omega \in \mathbb{C}$, $\omega \neq 0$ et on pose
$Q_{n,\omega} = \omega P_n\left(\dfrac{X}{\omega}\right)$.

3. (a) Prenons déjà $\omega = 1$.
Soit $Q \in \mathbb{C}_{n-1}[X]$. $Q^2 - X - 1$ est un polynôme de degré au plus $2n-2$.
Supposons que X^n divise ce polynôme. On peut écrire :
$X^n Q_1(X) = Q^2(X) - X - 1$ et donc $Q^2(0) = 1$. Donc $Q(1) = \pm 1$.
Supposons par exemple $Q(0) = 1$.
Cherchons Q sous la forme $Q(X) = 1 + \sum_{k=1}^{n-1} b_k X^k$.
$Q^2(X) = 1 + 2\sum_{k=1}^{n-1} b_k X^k + \left(\sum_{k=1}^{n-1} b_k X^k\right)^2$
Pour $n \geq 2$, la condition X^n divise $Q^2 - X - 1$ impose $2b_1 = 1$ et $b_1 = 1/2$.
De même tous les termes dans le développement de Q^2 d'ordre compris entre 2 et $n-1$ doivent être nuls.
Ceci permet de déterminer successivement et de manière unique les coefficients $b_2, ..., b_{n-1}$. On trouve par exemple en cherchant le coefficient en X^2 : $2b_2 + b_1^2 = 0 = 2b_2 + 1/4$ et $b_2 = -1/8$.
Q est déterminé de manière unique. P_n vérifie cette relation car $P_n(0) = 1$.
L'unicité donne $Q = P_n$.
Si $Q(0) = -1$, $-Q = P_n$ donc $Q = -P_n$.
Revenons au cas général $\omega \neq 0$. Soit $Q \in \mathbb{C}_{n-1}[X]$.
X^n divise $Q^2 - X - \omega^2 \Leftrightarrow \exists P_1$ tel que $Q^2(X) - X - \omega^2 = X^n P_1(X)$
X^n divise $Q^2 - X - \omega^2 \Leftrightarrow \exists P_1$ tel que $(Q/\omega)^2(X) - (X/\omega)^2 - 1 = \omega^{-2} X^n P_1(X)$
Soit Q vérifiant la propriété précédente : notons $Q_1(Y) = Q(\omega Y)/\omega$.
Pour tout $X = \omega Y$, $Q_1^2(Y) - Y^2 - 1 = \omega^{-2}(Y/\omega)^n P_1(\omega Y)$.
Donc $Q_1^2(Y) - Y - 1$ est divisible par Y^n et $Q_1(Y) = \pm P_n(Y)$ et $Q(X) = \pm \omega P_n(X/\omega)$. La réciproque se fait de même.
L'ensemble des polynômes Q de $\mathbb{C}_{n-1}[X]$ tels que X^n divise $Q^2 - X - \omega^2$ est $\{Q_{n,\omega}, -Q_{n,\omega}\}$.

(b) Comme $Q_{n,\omega}^2(X) = X + \omega^2 + X^n P_1(X)$, $Q_{n,\omega}^2(u) = u + \omega^2 e$ car $u^n = 0$.
$R(u + \omega^2 e) \neq \emptyset$.

4. On suppose $n = N$ et on prend $x \in E$ tel que la famille $(x, u(x), ...u^{n-1}(x))$ soit libre. On suppose que $g \in R(u + \omega^2 e)$.

(a) $g^2 = u + \omega^2 e \Rightarrow g \circ u = g \circ (g^2 - \omega^2 e) = (g - \omega^2 e) \circ g = u \circ g$.

(b) Notons $\varepsilon_0, ..., \varepsilon_{n-1}$ les vecteurs $x, u(x), ..., u^{n-1}(x)$ qui forment une base de E. On peut donc écrire : $g(x) = g(\varepsilon_0) = \sum_{k=0}^{n-1} c_k u^k(x) = P(u)(\varepsilon_0)$ en notant $P(X) = \sum_{k=0}^{n-1} c_k X^k$.

Comme u et g commutent, pour j entier

$$g(\varepsilon_j) = g(u^j(x)) = u^j(g(x)) = \sum_{k=0}^{n-1} c_k u^{k+j}(x) = \sum_{k=0}^{n-1} u^k(u^j(x)) = P(u)(u^j(x))$$

Les endomorphismes g et $P(u)$ sont égaux sur une base de E. Ils sont donc égaux.

Il existe bien $P \in \mathbb{C}_{n-1}[X]$ tel que $g = P(u)$.

(c) D'après les questions précédentes $R(u + \omega^2 e) = \{Q_{n,\omega}(u), -Q_{n,\omega}(u)\}$

(d) $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix} = I_4 + N$ avec $N^3 \neq 0$ et $N^4 = 0$.

$P_3(X) = 1 + X/2 - X^2/8 - X^3/16$. Les deux matrices solution sont $\pm(I_4 + N/2 - N^2/8 - N^3/16)$.

Le calcul donne

$$M = \pm \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -1/2 & 1 & 1 & 0 \\ 1/2 & -1/2 & 1 & 1 \end{pmatrix}$$

5. On suppose que $n \geq 2$ et que $R(u) \neq \emptyset$. Soit g un élément de $R(u)$. g commute avec u et est donc un polynôme en u. 0, seule valeur propre de u est racine du polynôme annulateur $P^2 - X^2$ de u. Donc $P(0) = 0$.

   D'où $g = \sum_{k=1}^{p} d_k u^k$. Prenons $t \in \mathbb{C}$. $(g + tu^{n-1})^2 = g^2 + 2gtu^{n-1} + t^2 u^{2n-2} = g^2 = u$ car $u^n = 0$. D'où une infinité d'éléments de $R(u)$.

6. (a) Par calcul les matrices qui commutent avec A sont du type

$$\begin{pmatrix} a & 0 & 0 \\ b & a & c \\ d & 0 & e \end{pmatrix} \quad (a, b, c, d, e) \in \mathbb{C}^5$$

   (b) Les matrices $M \in \mathcal{M}_3(\mathbb{C})$ telles que $M^2 = A$ commutent avec A et sont du type précédent. Par calcul on trouve

$$M = \begin{pmatrix} 0 & 0 & 0 \\ b & 0 & c \\ 1/c & 0 & 0 \end{pmatrix} \quad (b, c) \in \mathbb{C}^2,\ c \neq 0$$

Fin du corrigé