DS 9 : un corrigé

Le barème comporte 70 points.

Partie I : polynôme minimal (sur 16 points)

1°) (sur 4 points) $I \neq \{0\}$, donc $\{\deg(P)/P \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$. Elle admet ainsi un plus petit élément, noté m. Il existe un polynôme P_0 de $I \setminus \{0\}$ de degré m.
Soit $P \in I$. Effectuons la division euclidienne de P par P_0 : il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = P_0Q + R$ avec $\deg(R) < m$.
$R = P - P_0Q \in I$ car I est un idéal, mais $\deg(R) < m$, donc $R = 0$.
Ainsi $P = P_0Q \in P_0\mathbb{K}[X]$.
On a donc montré que $I \subseteq P_0\mathbb{K}[X]$. Mais réciproquement, $P_0 \in I$ et I est un idéal, donc $P_0\mathbb{K}[X] \subseteq I$. Ainsi $I = P_0\mathbb{K}[X]$.
Quitte à diviser P_0 par son coefficient dominant, on peut supposer que P_0 est unitaire, ce qui prouve l'existence.
Pour démontrer l'unicité, supposons que P_1 soit également un polynôme unitaire tel que $I = P_1\mathbb{K}[X]$.
$P_0 \in I = P_1\mathbb{K}[X]$, donc $P_1 \mid P_0$. De même $P_0 \mid P_1$. Ainsi, P_0 et P_1 sont associés. D'après le cours, il existe $\lambda \in \mathbb{K}^*$ tel que $P_0 = \lambda P_1$. Mais P_0 et P_1 sont unitaires, donc $P_1 = P_0$, ce qui prouve l'unicité.

2°) (sur 2 points) • $\varphi_u(1) = \varphi_u(X^0) = u^0 = Id_E$.
• Soient $P = \sum_{n\in\mathbb{N}} b_nX^n \in \mathbb{K}[X]$, $Q = \sum_{n\in\mathbb{N}} c_nX^n \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

$$\diamond \quad \varphi_u(\alpha P) = \left(\sum_{n\in\mathbb{N}}(\alpha b_n)X^n\right)(u) = \sum_{n\in\mathbb{N}}(\alpha b_n)u^n = \alpha \sum_{n\in\mathbb{N}} b_nu^n = \alpha\varphi_u(P).$$

$$\diamond \quad \varphi_u(P + Q) = \left(\sum_{n\in\mathbb{N}}(b_n + c_n)X^n\right)(u) = \sum_{n\in\mathbb{N}}(b_n + c_n)u^n = \varphi_u(P) + \varphi_u(Q).$$

$\diamond \quad \varphi_u(PQ) = \left(\sum_{n\in\mathbb{N}}(\sum_{k=0}^{n}(b_{n-k}c_k))X^n\right)(u) = \sum_{n\in\mathbb{N}}(\sum_{k=0}^{n}(b_{n-k}c_k))u^n$. D'autre part, d'après les règles de calcul dans l'algèbre $L(E)$,

$\varphi_u(P)\varphi_u(Q) = \Big(\sum_{n\in\mathbb{N}} b_n u^n\Big)\Big(\sum_{n\in\mathbb{N}} c_n u^n\Big) = \sum_{p,q\in\mathbb{N}} b_p c_q u^{p+q}$, donc par sommation par paquets, $\varphi_u(P)\varphi_u(Q) = \sum_{n\in\mathbb{N}} \Big(\sum_{p+q=n} b_p c_q\Big) u^n$. Ainsi, $\varphi_u(PQ) = \varphi_u(P)\varphi_u(Q)$.

3°) (sur 3 points)
$\diamond$ $(Id_E, u, u^2, \ldots, u^{n^2})$ est une famille de cardinal n^2+1 dans $L(E)$ qui est de dimension n^2, donc elle n'est pas libre. Cette famille est donc liée.

$\diamond$ Ainsi, il existe une famille non nulle de scalaires $(\alpha_i)_{0\le i\le n^2}$ telle que $\sum_{i=0}^{n^2} \alpha_i u^i = 0$.

Si l'on pose $Q(X) = \sum_{i=0}^{n^2} \alpha_i X^i$, alors $Q \neq 0$ et $Q(u) = 0$.

$\diamond$ Posons $I = \{P \in \mathbb{K}[X] \ / \ P(u) = 0\}$. $I = \mathrm{Ker}(\varphi_u)$ et φ_u est un morphisme d'anneaux, donc d'après le cours, I est un idéal de $\mathbb{K}[X]$, non nul d'après le point précédent. Alors, d'après la première question, il existe un unique polynôme π_u dans $\mathbb{K}[X]$, de coefficient dominant égal à 1, tel que $I = \pi_u\mathbb{K}[X]$, c'est-à-dire tel que pour tout $P \in \mathbb{K}[X]$, $P \in I \Longleftrightarrow \pi_u \mid P$, ce qu'il fallait démontrer.

4°) (sur 2 points) Soit $u \in L(E)$.
$\diamond$ Supposons que $deg(\pi_u) = 0$. Alors $\pi_u = 1 = X^0$, donc $0 = \pi_u(u) = u^0 = Id_E$, donc $E = \{0\}$.
Ainsi, lorsque $E = \{0\}$, $L(E) = \{0\} = \{Id_E\}$ et $\pi_{Id_E} = 1$ et
lorsque $E \neq \{0\}$, on n'a jamais $\deg(\pi_u) = 0$.
$\diamond$ Supposons maintenant que $E \neq \{0\}$.
Supposons que $\deg(\pi_u) = 1$. Alors il existe $\lambda \in \mathbb{K}$ tel que $\pi_u = X - \lambda$,
donc $0 = \pi_u(u) = u - \lambda Id_E$, ce qui prouve que u est une homothétie.
Réciproquement, si u est une homothétie, il existe $\lambda \in \mathbb{K}$ tel que $u = \lambda Id_E$, donc u est annulé par le polynôme $X - \lambda$. Alors π_u divise $X - \lambda$, mais d'après le point précédent, $\deg(\pi_u) \ge 1$ et π_u est unitaire, donc $\pi_u = X - \lambda$ et $\deg(\pi_u) = 1$.
En conclusion, lorsque $E = \{0\}$, Id_E est l'unique élément de $L(E)$ et $\deg(\pi_{Id_E}) = 0$ et lorsque $E \neq \{0\}$, on a toujours $\deg(\pi_u) \ge 1$, avec égalité si et seulement si u est une homothétie.

5°) (sur 2 points) Posons $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
$\diamond$ On calcule $M^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & cb+d^2 \end{pmatrix}$
et $\mathrm{Tr}(M)M - \det(M)I_2 = (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} - (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, donc on obtient bien que $M^2 = \mathrm{Tr}(M)M - \det(M)I_2$.
$\diamond$ Notons $P(X) = X^2 - \mathrm{Tr}(M)X + \det(M)$. On vient de montrer que $P(M) = 0$.
Notons c la base canonique de $\mathbb{K}^2$. D'après le cours, $\mathrm{mat}(u, c) = M$, donc
$\mathrm{mat}(u^2, c) = M^2$ puis $\mathrm{mat}(P(u), c) = P(M) = 0$. Ainsi $P(u) = 0$ et π_u divise P.

D'après la question précédente, si $c = b = 0$ et $a = d$, alors u est une homothétie et $\pi_u = X - a$, mais sinon, u n'est pas une homothétie, donc $\deg(\pi_u) \geq 2$, donc $\pi_u = P = X^2 - \mathrm{Tr}(M)X + \det(M)$.

6°) (sur 3 points)

En posant $s = a_0^2 - a_1^2 - a_2^2 - a_3^2$, on calcule $M^2 = \begin{pmatrix} s & 2a_0a_1 & 2a_0a_2 & 2a_0a_3 \\ -2a_0a_1 & s & -2a_0a_3 & 2a_0a_2 \\ -2a_0a_2 & 2a_0a_3 & s & -2a_0a_1 \\ -2a_3a_0 & -2a_2a_0 & 2a_1a_0 & s \end{pmatrix}$,

donc $M^2 = 2a_0M - (a_0^2 + a_1^2 + a_2^2 + a_3^2)\, I_4$.
Premier cas. On suppose que $(a_1, a_2, a_3) = 0$. Alors $M = a_0I_4$ et $\pi_f = X - a_0$.
Deuxième cas. On suppose que $(a_1, a_2, a_3) \neq 0$. Alors M n'est pas scalaire, donc f n'est pas une homothétie et d'après la question 4, $\deg(\pi_f) \geq 2$. Alors, ce qui précède montre que $\pi_f = X^2 - 2a_0X + (a_0^2 + a_1^2 + a_2^2 + a_3^2)$.

Partie II : ordre d'un vecteur (sur 19 points)

7°) (sur 3 points) Notons $I = \{P \in \mathbb{K}[X] \;/\; P(f)(u) = 0\}$.
$0 \in I$, donc $I \neq \emptyset$. De plus, si $P, Q \in I$ et $R \in \mathbb{K}[X]$,
alors $(P + Q)(f)(u) = [P(f) + Q(f)](u) = P(f)(u) + Q(f)(u) = 0$
et $(RP)(f)(u) = (R(f) \circ P(f))(u) = R(f)[P(f)(u)] = R(f)(0) = 0$,
donc $P + Q \in I$ et $RP \in I$.
Ceci démontre que I est un idéal de $\mathbb{K}[X]$. Il est non nul car $\pi_f \in I$, donc d'après la première question, il existe un unique polynôme P_u dans $\mathbb{K}[X]$, de coefficient dominant égal à 1, tel que $I = P_u\mathbb{K}[X]$, c'est-à-dire tel que pour tout $P \in \mathbb{K}[X]$,
$P \in I \Longleftrightarrow P_u \mid P$, ce qu'il fallait démontrer.

8°)

$\diamond$ (sur 3 points) On calcule successivement que $c_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, $f\,(c_3) = \begin{pmatrix} -1 \\ 0 \\ -3 \\ -1 \end{pmatrix}$,

$$f^2\,(c_3) = -\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - 3\begin{pmatrix} -1 \\ 0 \\ -3 \\ -1 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \\ 7 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 2 \\ 0 \end{pmatrix}$$

et $f^3\,(c_3) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 2\begin{pmatrix} -1 \\ 0 \\ -3 \\ -1 \end{pmatrix} = \begin{pmatrix} -4 \\ 1 \\ -6 \\ -2 \end{pmatrix}$.

$\diamond$ Soit $(\alpha_i)_{0 \leq i \leq 3} \in \mathbb{Q}^4$ tel que $\displaystyle\sum_{i=0}^{3} \alpha_i f^i(c_3) = 0$. Alors $\begin{cases} -\alpha_1 + \alpha_2 - 4\alpha_3 & = 0 \\ -\alpha_2 + \alpha_3 & = 0 \\ \alpha_0 - 3\alpha_1 + 2\alpha_2 - 6\alpha_3 & = 0 \\ -\alpha_1 - 2\alpha_3 & = 0 \end{cases}$.

D'après la seconde équation, $\alpha_2 = \alpha_3$, d'après la dernière équation, $\alpha_1 = -2\alpha_3$, donc la première équation devient $2\alpha_3 + \alpha_3 - 4\alpha_3 = 0$, c'est-à-dire $\alpha_3 = 0$,
ainsi $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Enfin la troisième équation montre que $\alpha_0 = 0$, donc la famille $(f^i(c_3))_{0\leq i\leq 3}$ est une famille libre. Elle est de cardinal 4 et $\dim(\mathbb{Q}^4) = 4$, donc c'est bien une base de $\mathbb{Q}^4$.

◇ (sur 3 points) Soit $Q \in \mathbb{Q}[X]$ un polynôme non nul tel que $\deg(P) \leq 3$: il existe $(\alpha_i)_{0\leq i\leq 3} \in \mathbb{Q}^4$ une famille non nulle de rationnels telle que $Q(X) = \sum_{i=0}^{3} \alpha_i X^i$.

Alors $Q(f)(c_3) = \sum_{i=0}^{3} \alpha_i f^i(c_3) \neq 0$ car la famille est libre. Ainsi, P n'est pas un multiple de P_{c_3}, quel que soit $P \in \mathbb{Q}_3[X] \setminus \{0\}$. Ceci implique que $\deg(P_{c_3}) \geq 4$.

Par ailleurs, on calcule

$$f^4(c_3) = -4\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} - 6\begin{pmatrix} -1 \\ 0 \\ -3 \\ -1 \end{pmatrix} - 2\begin{pmatrix} 2 \\ 0 \\ 7 \\ 3 \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \\ 4 \\ 0 \end{pmatrix} = 4\left(-c_3 + f^2(c_3)\right),$$

donc si l'on pose $Q(X) = X^4 - 4X^2 + 4$, on a $Q(f)(c_3) = 0$. Ainsi P_{c_3} divise Q, or P_{c_3} et Q sont unitaires et $\deg(P_{c_3}) \geq 4$, donc $P_{c_3} = X^4 - 4X^2 + 4$.

9°) (sur 1 point) $\pi_f(f) = 0$, donc $\pi_f(f)(u) = 0$, ce qui prouve par définition de P_u que P_u divise π_f.

10°) (sur 2 points)

◇ D'après le cours, $S = \left\{ \sum_{i\in\mathbb{N}} \alpha_i f^i(u) \ / \ (\alpha_i)_{i\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})} \right\}$, or pour toute famille $(\alpha_i)_{i\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$ presque nulle de scalaires, $\sum_{i\in\mathbb{N}} \alpha_i f^i(u) = P(f)(u)$,
en posant $P(X) = \sum_{i\in\mathbb{N}} \alpha_i X^i$, donc $S = \{P(f)(u) \ / \ P \in \mathbb{K}[X]\}$.

◇ Soit $x \in S$. Il existe $P \in \mathbb{K}[X]$ tel que $x = P(f)(u)$.
Alors $f(x) = f(P(f)(u)) = [f \circ P(f)](u) = [XP](f)(u)$, donc $f(x) \in S$.
Ainsi, $f(S) \subset S$.

11°) (sur 3 points)

◇ Posons $s = \deg(P_u)$. Soit $(\alpha_i)_{0\leq i<s}$ une famille de scalaires telle que $\sum_{i=0}^{s-1} \alpha_i f^i(u) = 0$.

Alors $P(f)(u) = 0$, où $P(X) = \sum_{i=0}^{s-1} \alpha_i X^i$, donc P_u divise P, mais $\deg(P) < s = \deg(P_u)$, donc $P = 0$. Alors, pour tout $i \in \{0, \ldots, s-1\}$, $\alpha_i = 0$. Ainsi, la famille $(f^i(u))_{0\leq i<s}$ est une famille libre de S.

◇ Soit $x \in S$. Il existe $P \in \mathbb{K}[X]$ tel que $x = P(f)(u)$. Par division euclidienne, on peut écrire que $P = P_u Q + R$ avec $\deg(R) < s$.
Alors $x = (P_u Q + R)(f)(u) = Q(f)(P_u(f)(u)) + R(f)(u) = R(f)(u)$,

mais $\deg(R) < s$, donc $x \in \text{Vect}((f^i)_{0\leq i<s})$. Ceci prouve que $(f^i(u))_{0\leq i<s}$ est également une famille génératrice de S. C'est donc une base de S, de cardinal s,
donc $\dim(S) = s = \deg(P_u)$.

12°) (sur 4 points)
$\diamond$ Commençons par montrer que, pour tout $i \in \mathbb{N}$ et $x \in S$, $f^i(x) = g^i(x)$.
Soit $i \in \mathbb{N}$. Notons $R(i)$ l'assertion : pour tout $x \in S$, $f^i(x) = g^i(x)$.
Pour $i = 0$ et $x \in S$, $f^0(x) = Id_E(x) = x = g^0(x)$, d'où $R(0)$.
Pour $i \geq 0$, supposons $R(i)$. Soit $x \in S$. D'après $R(i)$,
$f^{i+1}(x) = f(g^i(x))$, or $g^i(x) \in S$, donc $f^{i+1}(x) = g(g^i(x)) = g^{i+1}(x)$, ce qui prouve $R(i+1)$.
$\diamond$ Par combinaison linéaire des propriétés $R(i)$, on en déduit que pour tout $x \in S$, pour tout $P(X) = \sum_{i\in\mathbb{N}} \alpha_i X^i \in \mathbb{K}[X]$, $P(f)(x) = \sum_{i\in\mathbb{N}} \alpha_i f^i(x) = \sum_{i\in\mathbb{N}} \alpha_i g^i(x) = P(g)(x)$.
$\diamond$ En particulier, avec $P = \pi_g \in \mathbb{K}[X]$ et $x = u \in S$, on a $\pi_g(f)(u) = \pi_g(g)(u) = 0$, car $\pi_g(g) = 0$, donc P_u divise π_g.
$\diamond$ Soit $i \in \mathbb{N}$.

$$\begin{aligned} P_u(g)[f^i(u)] &= P_u(f)[f^i(u)] = (P_u \times X^i)(f)[u] \\ &= (X^i \times P_u)(f)[u] = f^i(P_u(f)[u]) \\ &= f^i(0) = 0, \end{aligned}$$

donc $P_u(g)$ est un endomorphisme de S qui annule tous les vecteurs de la famille $(f^i(u))_{i\in\mathbb{N}}$. C'est une famille génératrice de S, donc $P_u(g) = 0$. Ainsi π_g divise P_u.
$\diamond$ Ainsi, les deux polynômes π_g et P_u sont associés et unitaires donc ils sont égaux.

Partie III : le polynôme minimal est l'ordre d'un vecteur (sur 5 points)

13°) (sur 1 point)
On a vu en question 8 que $(c_3, f(c_3), f^2(c_3), f^3(c_3))$ est une base de $\mathbb{Q}^4$, donc pour tout $x \in \mathbb{Q}^4$, il existe $(\alpha_0, \ldots, \alpha_3) \in \mathbb{K}^4$ tel que $x = \sum_{i=0}^{3} \alpha_i f^i(c_3) = Q(f)(c_3)$, en posant $Q(X) = \sum_{i=0}^{3} \alpha_i X^i$. Ceci prouve que (c_3) est f-génératrice.

14°) (sur 1 point) E est de dimension finie, donc E admet une base $e = (e_1, \ldots, e_n)$.
Soit $x \in E$. Il existe $(a_i)_{1\leq i\leq n} \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^{n} a_i e_i$.
Pour tout $i \in \mathbb{N}_n$, posons $Q_i(X) = a_i$.
Ainsi, pour tout $i \in \mathbb{N}_n, Q_i(f)(e_i) = (a_i Id_E)(e_i) = a_i e_i$, donc $x = \sum_{i=1}^{n} Q_i(f)(e_i)$.
Ainsi, e est une famille f-génératrice.

15°) (sur 3 points) Notons π le PPCM des polynômes $P_{e_1}, \ldots, P_{e_k}$.

$\diamond$ D'après la question 9, π_f est un multiple de chaque P_{e_i} pour $i \in \mathbb{N}_k$, donc π_f est un multiple de π.

$\diamond$ Soit $x \in E$. Il existe $(\varphi_i)_{1 \leq i \leq k} \in \mathbb{K}[X]^k$ tel que $x = \sum_{i=1}^{k} \varphi_i(f)\,[e_i]$.

Soit $i \in \mathbb{N}_k$. Il existe $R \in \mathbb{K}[X]$ tel que $\pi = R(X)P_{e_i}(X)$,
donc $\pi(f)\,[\varphi_i(f)\,[e_i]] = (RP_{e_i}\varphi_i)\,(f)\,[e_i] = (R\varphi_i)\,(f)\,[P_{e_i}(f)\,[e_i]] = (R\varphi_i)\,(f)[0] = 0$.
On en déduit que $\pi(f)[x] = 0$, pour tout $x \in E$, donc $\pi(f)$ est un polynôme annulateur de f. Ainsi, π est un multiple de π_f.
$\diamond$ Ainsi, les deux polynômes π et π_f sont associés et unitaires, donc ils sont égaux.

Partie IV : le polynôme minimal est l'ordre d'un vecteur (sur 13 points)

16°) (sur 3 points) Soit $i \in \mathbb{N}_k$. Notons $Q = P_y \prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}$. Par défnition de P_{y_i}, il suffit de montrer que $Q(f)(y_i) = 0$.

Posons $z = y - y_i = \sum_{\substack{j=1 \\ j \neq i}}^{k} y_j$: pour tout $h \in \{1, \ldots, k\} \setminus \{i\}$,
$\Big[\prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}\Big](f)(y_h) = \Big[\prod_{\substack{1 \leq j \leq k \\ j \notin \{i,h\}}} P_{y_j}\Big](f)(P_{y_h}(f)(y_h)) = 0$, donc $\Big[\prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}\Big](f)(z) = 0$, ce qui prouve que $\Big[\prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}\Big](f)(y_i) = \Big[\prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}\Big](f)(y)$,
donc $Q(f)(y_i) = Q(f)(y) = \Big[\prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}\Big](f)(P_y(f)(y)) = 0$.

17°) (sur 3 points) Pour tout $i \in \mathbb{N}_k, P_{y_i}$ et $\prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_{y_j}$ sont premiers entre eux, donc, d'après le théorème de Gauss, $P_{y_i} \mid P_y$. De plus, les P_{y_i} sont deux à deux premiers entre eux, donc $\prod_{1 \leq i \leq k} P_{y_i}$ divise P_y. D'autre part,

$$\Big(\prod_{1 \leq i \leq k} P_{y_i}\Big)(f)[y] = \sum_{j=1}^{k} \Big(\prod_{1 \leq i \leq k} P_{y_i}\Big)(f)\,[y_j] = \sum_{j=1}^{k} \Big(\prod_{\substack{1 \leq i \leq k \\ i \neq j}} P_{y_i}\Big)(f)\,[P_{y_j}(f)\,[y_j]] = 0,$$

donc, P_y divise $\prod_{1 \leq i \leq k} P_{y_i}$. Ainsi, ces deux polynômes sont associés et unitaires, donc ils sont égaux.

18°) (sur 4 points)
◇ $P_i^{\alpha_i}(f)\,[e_j] = 0$, car $e_j \in F_i = \text{Ker}\,(P_i^{\alpha_i}(f))$, donc P_{e_j} divise $P_i^{\alpha_i}$. De plus, P_i est un polynôme irréductible de $\mathbb{K}[X]$, donc il existe $\beta_j \in \{0, \ldots, \alpha_i\}$ tel que $P_{e_j} = P_i^{\beta_j}$ (tous ces polynômes sont unitaires).
◇ Pour tout $j \in \mathbb{N}_r$, $P_{e_j} \mid P_i^{\beta}$, donc, pour tout $j \in \mathbb{N}_r, P_i^{\beta}(f)\,[e_j] = 0$. Ainsi $P_i^{\beta}(f)$ annule les vecteurs d'une base de F_i, donc $F_i \subset \text{Ker}\left(P_i^{\beta}(f)\right)$.
D'autre part, $\beta \leq \alpha_i$, donc $P_i^{\alpha_i}(f) = [P_i(f)]^{\alpha_i} = [P_i(f)]^{a_i - \beta} \circ [P_i(f)]^{\beta}$,
donc $\text{Ker}\left(P_i^{\beta}(f)\right) \subset \text{Ker}\,(P_i^{\alpha_i}(f)) = F_i$. Ainsi, $\text{Ker}\left(P_i^{\beta}(f)\right) = \text{Ker}\,(P_i^{\alpha_i}(f))$.
Alors d'après le théorème de décomposition des noyaux,

$$\begin{aligned}
E &= \text{Ker}(\pi_f(f)) = \bigoplus_{j=1}^{n} \text{Ker}\left(P_j^{\alpha_j}(f)\right) \\
&= \text{Ker}\,(P_i^{\alpha_i}(f)) \bigoplus \Big(\bigoplus_{\substack{i \leq j \leq n \\ j \neq i}} \text{Ker}\left(P_j^{\alpha_j}(f)\right) \Big) \\
&= \text{Ker}\left(P_i^{\beta}(f)\right) \bigoplus \Big(\bigoplus_{\substack{i \leq j \leq n \\ j \neq i}} \text{Ker}\left(P_j^{\alpha_j}(f)\right) \Big) \\
&= \text{Ker}\Big(\Big(P_i^{\beta} \prod_{\substack{1 \leq j \leq n \\ j \neq n}} P_j^{\alpha_j}\Big)(f)\Big),
\end{aligned}$$

donc $\Big(P_i^{\beta} \prod_{\substack{1 \leq j \leq k \\ j \neq i}} P_j^{\alpha_j}\Big)(f) = 0$.

19°) (sur 3 points) Ainsi, $P_i^{\beta} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} P_j^{\alpha_j}$ est un multiple du polynôme minimal de f, c'est-à-dire de $P_i^{\alpha_i} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} P_j^{\alpha_j}$, donc $\alpha_i \leq \beta$. Or $\beta \leq \alpha_i$, donc $\alpha_i = \beta = \max\limits_{1 \leq j \leq r} \beta_j$. Ainsi, il existe $j \in \mathbb{N}_r$ tel que $\beta_j = \alpha_i$. Alors, $P_{e_j} = P_i^{\alpha_i}$.
On a donc prouvé que, pour tout $i \in \mathbb{N}_k$, il existe $y_i \in E$ tel que $P_{y_i} = P_i^{\alpha_i}$. D'après la question 17, $P_{y_1 + \cdots + y_k} = \prod_{i=1}^{k} P_i^{\alpha_i} = \pi_f$, ce qu'il fallait démontrer.

Partie V : Endomorphismes cycliques (sur 17 points)

20°) (sur 1 point) D'après la question 8, $(c_3, f(c_3), f^2(c_3), f^3(c_3))$ est une base de $\mathbb{Q}^4 = E$, donc f est cyclique.

21°) (sur 4 points)
◇ Soit $Q \in \mathbb{K}[X]$. $Q(f) \circ f = (Q(X)X)(f) = (XQ(X))(f) = f \circ Q(f)$,
donc $\{g \in L(E) \;/\; f \circ g = g \circ f\} \supset \{Q(f) \;/\; Q \in \mathbb{K}[X]\}$.
◇ Réciproquement, soit $g \in L(E)$ tel que $g \circ f = f \circ g$.

Par hypothèse, il existe $u \in E$ tel que la famille $(u, f(u), \ldots, f^{n-1}(u))$ est une base de E. On peut donc décomposer le vecteur $g(u)$ dans cette base :

il existe $(\alpha_i)_{0 \leq i \leq n-1} \in \mathbb{K}^n$ tel que $g(u) = \sum_{i=0}^{n-1} \alpha_i f^i(u)$.

Posons $Q(X) = \sum_{i=0}^{n-1} \alpha_i X^i$. Ainsi, $g(u) = Q(f)[u]$.

Soit $j \in \{0, \ldots, n-1\}$. On montre par récurrence sur j que g commute avec f^j, donc $g\left(f^j(u)\right) = f^j(g(u)) = f^j(Q(f)[u]) = \left(f^j \circ Q(f)\right)(u) = Q(f)\left(f^j(u)\right)$, donc g et $Q(f)$ coïncident sur les vecteurs d'une base de E. Ainsi, $g = Q(f)$.

22°) (sur 3 points)

$\diamond$ Supposons que f est cyclique. Ainsi, il existe $e_1 \in E$ pour lequel, pour tout $x \in E$, il existe $(\alpha_i)_{0 \leq i \leq n-1} \in \mathbb{K}^n$ tel que $x = \sum_{i=0}^{n-1} \alpha_i f^i\left(e_1\right) = Q(f)\left[e_1\right]$, où $Q = \sum_{i=0}^{n-1} \alpha_i X^i$. Ainsi, (e_1) est une famille f-génératrice. D'après la question 15, le polynôme minimal de f est égal à P_{e_1}, lequel est de degré n d'après la question 11.

$\diamond$ Réciproquement, supposons que le polynôme minimal de f est de degré n. D'après la question 19, il existe $u \in E$ tel que le polynôme minimal de f est égal à P_u. P_u est de degré n, donc toujours d'après la question 11, la famille $\left(f^i(u)\right)_{0 \leq i \leq n-1}$ est libre. De plus elle contient $n = \dim(E)$ vecteurs, donc c'est une base de E. Ainsi, f est un endomorphisme cyclique.

23°)

$\diamond$ (sur 1 point) Soit $x \in \mathrm{Ker}(P_i(f))$. On a vu que f commute avec $P_i(f)$, donc $P_i(f)(f(x)) = f(P_i(f)(x)) = f(0) = 0$. Ainsi $f(x) \in \mathrm{Ker}(P_i(f))$, ce qu'il fallait démontrer.

$\diamond$ (sur 2 points) Pour tout $x \in \mathrm{Ker}\left(P_i(f)\right)$, d'après le début de la réponse à la question 12,

$\pi_{f_i}(f)(x) = \pi_{f_i}\left(f_i\right)(x) = 0$, donc $\mathrm{Ker}\left(P_i(f)\right) \subset \mathrm{Ker}\left(\pi_{f_i}(f)\right)$.

De plus, pour tout $x \in \mathrm{Ker}\left(P_i(f)\right)$, $P_i\left(f_i\right)[x] = P_i(f)[x] = 0$, donc $P_i\left(f_i\right) = 0$. On en déduit que P_i est un multiple de π_{f_i}, donc il existe $g \in L(E)$ tel que $P_i(f) = g \circ \pi_{f_i}(f)$, donc $\mathrm{Ker}\left(\pi_{f_i}(f)\right) \subset \mathrm{Ker}\left(P_i(f)\right)$. Ainsi, $\mathrm{Ker}\left(\pi_{f_i}(f)\right) = \mathrm{Ker}\left(P_i(f)\right)$.

$\diamond$ (sur 3 points) On vient de voir que $\pi_{f_i} \mid P_i$, donc π_{f_i} est premier avec tous les P_j, pour $j \in \mathbb{N}_t \backslash \{i\}$. Ainsi, d'après le théorème de décomposition des noyaux,

$$\begin{aligned} E &= \mathrm{Ker}(\pi_f(f)) = \bigoplus_{i=1}^{t} \mathrm{Ker}(P_i(f)) \\ &= \mathrm{Ker}\left(\pi_{f_i}(f)\right) \bigoplus \bigoplus_{\substack{1 \leq j \leq n \\ i \neq j}} \mathrm{Ker}\left(P_j(f)\right) = \mathrm{Ker}\Big(\Big(\pi_{f_i} \prod_{\substack{1 \leq j \leq n \\ i \neq j}} P_j\Big)(f)\Big), \end{aligned}$$

ce qui prouve que $\pi_{f_i} \prod_{\substack{1 \leq j \leq n \\ i \neq j}} P_j$ annule f, donc que c'est un multiple de $\pi_f = P_i \prod_{\substack{1 \leq j \leq n \\ i \neq j}} P_j$.

Ainsi, π_{f_i} est un multiple de P_i. Ces deux polynômes sont donc associés et unitaires. Ils sont égaux.

24°) (sur 3 points) D'après la question 22, il suffit de montrer que, pour tout $i \in \mathbb{N}_t$, $\dim(\mathrm{Ker}(P_i(f))) = \deg(\pi_{f_i}) = \deg(P_i)$.

Pour tout $j \in \mathbb{N}_t$, notons $s_j = \deg(P_j)$. D'après la question 19 et la question 11, $s_j \leq \dim(\mathrm{Ker}(P_j(f)))$.

Soit $i \in \mathbb{N}_t$. Supposons que $s_i < \dim(\mathrm{Ker}(P_i(f)))$.

Alors $n = \dim(E) = \sum_{j=1}^{t} \dim(\mathrm{Ker}(P_j)(f)) > \sum_{j=1}^{n} s_j = \deg(\pi_f)$. Or, on suppose que f est cyclique, donc, d'après la question 22, $\deg(P) = n$. Ainsi, $n > n$, ce qui est faux.

On a donc prouvé que $\deg(P_i) = s_i = \dim(\mathrm{Ker}(P_i(f)))$, ce qui termine le corrigé.