Étude de $\mathbb{K}[u]$. Polynôme minimal

1. L'espace vectoriel $\mathcal{L}(E)$ étant de dimension n^2, la famille $\left\{u^k \mid 0 \leq k \leq n^2\right\}$ est liée et en conséquence, il existe un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ tel que $P(u) = 0$. Il en résulte que l'ensemble I_u n'est pas réduit au polynôme nul. Cet ensemble étant le noyau du morphisme d'algèbres $\varphi_u : P \mapsto P(u)$, c'est un idéal de l'anneau $\mathbb{K}[X]$ et comme cet anneau est principal, il existe un unique polynôme unitaire π_u tel que $I_u = \mathbb{K}[X]\pi_u$. Ce polynôme est de degré au moins égal à 1.
2. Dire que π_u est de degré 1 équivaut à dire qu'il existe un scalaire λ tel que $\pi_u(X) = X - \lambda$ et l'égalité $\pi_u(u) = 0$ équivaut à $u = \lambda Id$, ce qui revient à dire que u est une homothétie.
3. On rappelle qu'un projecteur est un endomorphisme u de E tel que $u \circ u = u$.
   Un tel projecteur étant annulé par $X(X-1)$, son polynôme minimal est $\pi_u(X) = X$ si $u = 0$, $\pi_u(X) = X - 1$ si $u = Id$, $\pi_u(X) = X^2 - X$ dans les autres cas.
4. Soit $u \in \mathcal{L}(E)$ nilpotent d'ordre $p \geq 1$. Comme u est annulé par X^p, son polynôme minimal est un diviseur de ce polynôme, donc de la forme X^r avec $1 \leq r \leq p$. Comme $u^k \neq 0$ pour tout k compris entre 1 et $p-1$ (sinon $u^{p-1} = 0$), ce polynôme minimal est X^p.
5. Notons v la restriction de u à F. C'est un endomorphisme de F si F est stable par u. De $\pi_u(u) = 0$ dans $\mathcal{L}(E)$, on déduit que $\pi_u(v) = 0$ dans $\mathcal{L}(F)$, donc π_u est dans l'idéal annulateur de v et c'est un multiple du polynôme minimal de v.
6. Si $\lambda \in \mathbb{K}$ est une valeur propre de u et $x \in E \setminus \{0\}$ un vecteur propre associé, de l'égalité :

   $$0 = \pi_u(u)(x) = \pi_u(\lambda)\, x$$

   on déduit que $\pi_u(\lambda) = 0$, c'est-à-dire que λ est racine de π_u.
   Réciproquement si $\lambda \in \mathbb{K}$ est racine de π_u, on a alors $\pi_u(X) = (X - \lambda)Q(X)$ et avec $\pi_u(u) = (u - \lambda Id) \circ Q(u) = 0$ et le caractère minimal de π_u on déduit que $u - \lambda Id$ est non inversible ce qui équivaut à dire que $\ker(u - \lambda Id) \neq \{0\}$ et λ est une valeur propre de u.
7.
   (a) Pour tout $P \in \mathbb{K}[X]$, on a la division euclidienne $P = \pi_u Q + R$ avec $R \in \mathbb{K}_{p_u-1}[X]$ et compte tenu de $\pi_u(u) = 0$, on a $P(u) = R(u) = \displaystyle\sum_{k=0}^{p_u-1} \alpha_k u^k$ si $R(X) = \displaystyle\sum_{k=0}^{p_u-1} \alpha_k X^k$.
   Si R, S sont deux polynômes dans $\mathbb{K}_{p_u-1}[X]$ tels que $P(u) = R(u) = S(u)$, on a alors $(R-S)(u) = 0$ et π_u divise $R - S$, ce qui impose $R - S = 0$ du fait que $\deg(R-S) < \deg(\pi_u)$. Les coefficients α_k, pour k compris entre 0 et $p_u - 1$ sont donc uniquement déterminés.
   (b) L'écriture $P(u) = \displaystyle\sum_{k=0}^{p_u-1} \alpha_k u^k$ avec les coefficients α_k, pour k compris entre 0 et $p_u - 1$, uniquement déterminés, pour tout $P(u) \in \mathbb{K}[u]$ nous dit que la famille $\left(u^k\right)_{0 \leq k \leq p_u - 1}$ est une base de $\mathbb{K}[u]$ et cet espace est de dimension égale à p_u.
   (c) On peut aussi procéder comme suit : le morphisme d'algèbres $\varphi_u : P \mapsto P(u)$ est surjectif de $\mathbb{K}[X]$ sur $\mathbb{K}[u]$ de noyau $I_u = \mathbb{K}[X]\pi_u = (\pi_u)$ (idéal engendré par π_u), il induit donc un isomorphisme d'algèbres de $\dfrac{\mathbb{K}[X]}{(\pi_u)}$ sur $\mathbb{K}[u]$, donc $\dim(\mathbb{K}[u]) = \dim\left(\dfrac{\mathbb{K}[X]}{(\pi_u)}\right) = p_u$ (en utilisant le théorème de division euclidienne).
8.

(a) Par division euclidienne, tout polynôme $A \in \mathbb{K}[X]$ s'écrit $A = PQ + R$ avec $R \in \mathbb{K}_{n-1}[X]$ et $\overline{P} = \overline{R} = \sum_{k=0}^{n-1} \alpha_k \overline{X^k}$, donc $\left(\overline{X^k}\right)_{0 \leq k \leq n-1}$ est une famille génératrice de E. Dire que $\sum_{k=0}^{n-1} \alpha_k \overline{X^k} = \overline{0}$ dans E équivaut à dire que $R = \sum_{k=0}^{n-1} \alpha_k X^k$ est multiple de P, donc nul à cause des degré, ce qui revient à dire que tous les α_k sont nuls. La famille $\mathcal{B} = \left(\overline{X^k}\right)_{0 \leq k \leq n-1}$ est donc une base de E et $\dim(E) = n = \deg(P)$.

(b) Avec $u\left(\overline{X^k}\right) = \overline{X^{k+1}}$ pour $0 \leq k \leq n-2$ et :

$$u\left(\overline{X^{n-1}}\right) = \overline{X^n} = \sum_{k=0}^{n-1} a_k \overline{X^k}$$

(qui résulte de $\overline{P} = \overline{0}$), on voit que C_P est la matrice de u dans la base $\mathcal{B}$.

(c) Notons $e_k = \overline{X^{k-1}}$ pour k compris entre 1 et n. On a alors $u(e_k) = e_{k+1}$ pour $1 \leq k \leq n-1$ et $u(e_n) = \sum_{k=0}^{n-1} a_k e_{k+1}$, soit $e_k = u^{k-1}(e_1)$ pour $1 \leq k \leq n$ et :

$$\left(u^n - \sum_{k=0}^{n-1} a_k u^k\right)(e_1) = 0$$

$$\left(u^n - \sum_{k=0}^{n-1} a_k u^k\right)(e_j) = u^{j-1}\left(\left(u^n - \sum_{k=0}^{n-1} a_k u^k\right)(e_1)\right) = 0$$

pour $1 \leq j \leq n$, ce qui signifie que u est annulé par $P(X) = X^n - \sum_{k=0}^{n-1} a_k X^k$. Le polynôme π_u divise donc P. Si π_u est de degré $p < n$, alors u^p est combinaison linéaire de $Id, u, \cdots, u^{p-1}$, donc $e_{p+1} = u^p(e_1)$ est combinaision linéaire de $e_1, e_2, \cdots, e_p$, ce qui n'est pas. On a donc $p = n$ et $\pi_u = P$.

(d) Si on connait le théorème de Cayley-Hamilton (démontré plus loin), on peut dire que π_u est unitaire de degré n divisant le polynôme caractéristique lui aussi unitaire de degré n, donc ces polynômes sont égaux.
Si on veut se passer du théorème de Cayley-Hamilton, on peut calculer directement $P_u = P_{C_P}$.
En notant $P_{(a_0,\cdots,a_{n-1})}(X) = \det(XI_n - C_P)$ le polynôme caractéristique de C_P et en le développant par rapport à la première ligne, on a :

$$P_{(a_0,\cdots,a_{n-1})}(X) = \begin{vmatrix} X & \cdots & 0 & -a_0 \\ -1 & \ddots & \vdots & -a_1 \\ \vdots & \ddots & X & \vdots \\ 0 & \cdots & -1 & X - a_{n-1} \end{vmatrix} = X \cdot P_{(a_1,\cdots,a_{n-1})}(X) - a_0$$

et par récurrence $P_{(a_0,\cdots,a_{n-1})}(X) = X^p - \sum_{k=0}^{n-1} a_k X^k = P(X)$.
Un polynôme unitaire est donc polynôme minimal et polynôme caractéristique de sa matrice compagnon.

(e) L'endomorphisme u est inversible si, et seulement si, 0 n'est pas valeur propre de u, ce qui équivaut à dire que 0 n'est pas racine de $\pi_u = P$, encore équivalent à $P(0) \neq 0$.
De $P(u) = u^n - \sum_{k=0}^{n-1} a_k u^k = 0$ avec $a_0 = P(0) \neq 0$, on déduit que :

$$u\left(u^{n-1} - \sum_{k=1}^{n-1} a_k u^{k-1}\right) = a_0 Id$$

et :

$$u^{-1} = \frac{1}{a_0}\left(u^{n-1} - \sum_{k=1}^{n-1} a_k u^{k-1}\right)$$

est un polynôme en u.
Il en résulte que :

$$u^{-1}(e_1) = \frac{1}{a_0}\left(e_n - \sum_{k=1}^{n-1} a_k e_k\right)$$

et avec $u^{-1}(e_k) = u^{-1}(u(e_{k-1})) = e_{k-1}$ pour k compris entre 2 et n, on déduit que la matrice de u^{-1} dans la base $\mathcal{B}$ (à savoir C_P^{-1}) est :

$$C_P^{-1} = \begin{pmatrix} -\frac{a_1}{a_0} & 1 & \cdots & 0 \\ -\frac{a_2}{a_0} & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & 1 \\ \frac{1}{a_0} & 0 & \cdots & 0 \end{pmatrix}$$

Ce qui peut se vérifier aussi par un calcul direct.

(f) Comme $P(0) \neq 0$, l'endomorphisme u est inversible.
De :

$$P(u) = u^n - \sum_{k=0}^{n-1} a_k u^k = 0$$

on déduit, en multipliant par $(u^{-1})^n$ que :

$$Id - \sum_{k=0}^{n-1} a_k \left(u^{-1}\right)^{n-k} = 0$$

donc u^{-1} est annulé par $Q(X) = 1 - \sum_{k=0}^{n-1} a_k X^{n-k}$, ce polynôme étant de degré n puisque $a_0 \neq 0$. Donc $\pi_{u^{-1}}$ divise Q et il est de degré au plus n (ce qui est connu comme conséquence du théorème de Cayley-Hamilton). Si $\pi_{u^{-1}}$ est de degré $q < n$, on a une relation du type $(u^{-1})^q - \sum_{k=0}^{q-1} b_k (u^{-1})^k = 0$ et multipliant par u^q, celà donne $Id - \sum_{k=0}^{q-1} b_k u^{q-k} = 0$ qui contredit $\deg(\pi_u) = n$. Le polynôme $\pi_{u^{-1}}$ est donc de degré n et proportionnel à Q. Comme il est unitaire, on a $\pi_{u^{-1}} = \frac{1}{a_0} Q$, soit $\pi_{u^{-1}}(X) = \frac{1}{P(0)} X^n P\left(\frac{1}{X}\right)$.

Sous-espaces cycliques

1. Comme E est de dimension n, le système $\left(u^k(x)\right)_{0\leq k\leq n}$ est lié, ce qui se traduit par l'existence d'un polynôme non nul $P\in\mathbb{K}_n[X]$ tel que $P(u)(x)=0$. On a donc $I_{u,x}\neq\{0\}$ (on peut aussi dire que $\{0\}\neq I_u\subset I_{u,x}$). Et pour P,Q dans $I_{u,x}$ et R dans $\mathbb{K}[X]$, on a $(P-Q)(u)(x)=P(u)(x)-Q(u)(x)=0$ et $(PR)(u)(x)=R(u)(P(u)(x))=0$, donc $P-Q$ et PR sont dans $I_{u,x}$, ce qui signifie que $I_{u,x}$ est un idéal de $\mathbb{K}[X]$. L'anneau $\mathbb{K}[X]$ étant principal, il existe un unique polynôme unitaire $\pi_{u,x}$ tel que $I_{u,x}=\mathbb{K}[X]\pi_{u,x}$. Ce polynôme est de degré compris entre 1 et n (il est non constant et divise $P\in\mathbb{K}_n[X]$). Comme $I_u=\mathbb{K}[X]\pi_u\subset I_{u,x}=\mathbb{K}[X]\pi_{u,x}$, le polynôme $\pi_{u,x}$ divise π_u.
2. Il est clair que $E_{u,x}$ est un sous-espace vectoriel de E qui contient x.
   Pour tout $k\in\mathbb{N}$, on a $u\left(u^k(x)\right)=u^{k+1}(x)\in E_{u,x}$, donc $E_{u,x}$ est stable par u.
   Si F est sous-espace vectoriel de E contenant x et stable par u, on a alors $u(x)\in F$ et on vérifie par récurrence que $u^k(x)\in F$ pour tout entier $k\geq 0$, donc F contient $E_{u,x}$.
   Comme $\pi_{u,x}$ est de degré minimum dans $I_{u,x}\backslash\{0\}$, le système $\mathcal{B}_{u,x}=\left\{u^k(x)\mid 0\leq k\leq p_{u,x}-1\right\}$ est libre.
   En notant $\pi_{u,x}(X)=X^{p_{u,x}}-\sum_{k=0}^{p_{u,x}-1}a_kX^k$, de $\pi_{u,x}(u)(x)=0$, on déduit que $u^{p_{u,x}}(x)$ est dans $\mathrm{Vect}(\mathcal{B}_{u,x})$ et par récurrence sur $k\geq 0$, on vérifie que $u^{p_{u,x}+k}(x)\in\mathrm{Vect}(\mathcal{B}_{u,x})$ pour tout entier naturel k, ce qui signifie que $\mathcal{B}_{u,x}$ est un système générateur et donc une base de $E_{u,x}$.
   On a donc $\dim(E_{u,x})=p_{u,x}$.
   On peut aussi dire que tout élément de $E_{u,x}$ est de la forme $P(u)(x)$ avec $P\in\mathbb{K}[X]$. Par division euclidienne, on $P=\pi_{u,x}Q+R$ avec $R\in\mathbb{K}_{p_{u,x}-1}[X]$ et $P(u)=R(u)=\sum_{k=0}^{p_u-1}\alpha_ku^k$, un tel polynôme R étant uniquement déterminé, ce qui signifie que $\mathcal{B}_{u,x}=\left(u^k(x)\right)_{0\leq k\leq p_{u,x}-1}$ est une base de $E_{u,x}$.
   Donc $\dim(E_{u,x})=p_{u,x}=\deg(\pi_{u,x})$
3. Si x est vecteur propre de u, il existe alors un scalaire λ tel que $u(x)=\lambda x$. On a alors $u^k(x)=\lambda^kx$ pour tout entier $k\geq 0$ et $E_{u,x}$ est la droite vectorielle dirigée par x, donc $\dim(E_{u,x})=1$ et $\pi_{u,x}$ est de degré 1.
   Réciproquement si $E_{u,x}$ est de dimension 1, c'est la droite vectorielle dirigée par x (ce vecteur est non nul dans $E_{u,x}$) et en particulier il existe un scalaire λ tel que $u(x)=\lambda x$, ce qui signifie que x est un vecteur propre de u.
4. Si u est une homothétie, tout vecteur non nul de E est vecteur propre de u, donc $\dim(E_{u,x})=\deg(\pi_{u,x})=1$.
   Si $\deg(\pi_{u,x})=1$ pour tout $x\in E\setminus\{0\}$, on a alors $\dim(E_{u,x})=1$ pour tout $x\in E\setminus\{0\}$, donc tout vecteur non nul est propre. Si x,y sont deux vecteurs linéairement indépendants, il existe alors deux scalaires λ,μ tels que $u(x)=\lambda x$ et $u(y)=\mu y$, donc $u(x+y)=\lambda x+\mu y$ est colinéaire à $x+y$ (ce vecteur est vecteur propre non nul de u) et il existe un scalaire ν tel que $\lambda x+\mu y=\nu(x+y)$, ce qui entraîne $\lambda=\nu=\mu$. Il en résulte que u est une homothétie. D'où l'équivalence des trois assertions.
5. (a) Avec $\pi_{u,x}(u)(x)=u^{p_{u,x}}(x)-\sum_{k=0}^{p_{u,x}-1}a_ku^k(x)=0$, on déduit que $u^{p_{u,x}}(x)=\sum_{k=0}^{p_{u,x}-1}a_ku^k(x)$ et la matrice de $v_{u,x}$ dans la base $\mathcal{B}_{u,x}$ de $E_{u,x}$ est :
$$A_{u,x}=\begin{pmatrix}0&\cdots&0&a_0\\1&\ddots&\vdots&a_1\\\vdots&\ddots&0&\vdots\\0&\cdots&1&a_{p_{u,x}-1}\end{pmatrix}$$
   c'est-à-dire la matrice compagnon de $\pi_{u,x}$.

(b) Le polynôme minimal [resp. caractéristique] de la restriction de u à E_x est celui de la matrice compagnon $A_{u,x}$ de $\pi_{u,x}$, soit $\pi_{u,x}$.

6. Pour tout $x \in E\backslash\{0\}$ le sous espace cyclique $E_{u,x}$ étant stable par u, le polynôme caractéristique $\pi_{u,x}$ de $u_{|E_{u,x}}$ divise celui de u (facile à vérifier avec les matrices). C'est-à-dire que $P_u = Q_x \cdot \pi_{u,x}$ et $P_u(u)(x) = Q_x(u) \circ \pi_{u,x}(u)(x) = 0$, ce dernier résultat étant encore valable pour $x = 0$. On a donc $P_u(u)(x) = 0$ pour tout $x \in E$, soit $P_u(u) = 0$.

7. Le polynôme minimal divisant tout polynôme annulateur de u, on déduit du théorème de Cayley-Hamilton que π_u divise le polynôme P_u et $\deg(\pi_u) \leq \deg(P_u) = n$. L'égalité $\deg(\pi_u) = n$ équivaut à dire que $\pi_u = P_u$.

8.

(a) On procède par récurrence sur $r \geq 1$, le résultat étant évident pour $r = 1$.

Supposons le acquis jusqu'au rang $r \geq 1$ et soit $E = \bigcup_{k=1}^{r+1} F_k$, les F_k étant des sous-espaces vectoriels de E.

Si $F_{r+1} \subset \bigcup_{j=1}^{r} F_j$, on a alors $E = \bigcup_{j=1}^{r} F_j$ et c'est terminé avec l(hypothèse de récurrence.

Si $\bigcup_{j=1}^{r} F_j \subset F_{r+1}$, on a alors $E = F_{r+1}$ et c'est terminé de manière triviale.

Si aucune des hypothèses précédentes n'est vérifiée, il existe un vecteur $x \in F_{r+1} \setminus \bigcup_{k=1}^{r} F_k$ et un vecteur $y \in \bigcup_{k=1}^{r} F_k \setminus F_{r+1}$. Pour tout $\lambda \in \mathbb{K}$, le vecteur $y + \lambda x$ ne peut être dans F_{r+1} (si $y + \lambda x \in F_{r+1}$, on a alors $y = (y + \lambda x) - \lambda x \in F_{r+1}$ ce qui n'est pas), il est donc dans $\bigcup_{k=1}^{r} F_k$ et il existe un indice k_λ compris entre 1 et r tel que $y + \lambda x \in F_{k_\lambda}$. Pour $\lambda \neq \mu$ dans $\mathbb{K}$, l'égalité $k_\lambda = k_\mu$ entraîne $y + \lambda x \in F_{k_\lambda}$ et $y + \mu x \in F_{k_\mu} = F_{k_\lambda}$, donc $x = \dfrac{1}{\lambda - \mu}(y + \lambda x - (y + \mu x)) \in F_{k_\lambda}$, soit $x \in \bigcup_{k=1}^{r} F_k$, ce qui n'est pas. On a donc $k_\lambda \neq k_\mu$ pour $\lambda \neq \mu$ dans $\mathbb{K}$ et l'ensemble $\{k_\lambda \mid \lambda \in \mathbb{K}\}$ est infini contenu dans $\{1, \cdots, r\}$, ce qui est impossible.

Pour $\mathbb{K}$ fini de cardinal inférieur ou égal à r, il n'y a pas d'impossibilité. Dans ce cas, $\mathbb{K} = \bigcup_{k=1}^{q-1} \mathbb{K}x_k$ où $\mathbb{K}$ est de cardinal q et les x_k sont tous les éléments non nuls de $\mathbb{K}$.

(b) Pour tout $x \in E \setminus \{0\}$ le polynôme $\pi_{u,x}$ divise π_u puisque $\pi_u \in I_{u,x}$, donc :

$$\Phi = \{\pi_{u,x} \mid x \in E\} \subset \{\text{diviseurs unitaires de } \pi_u\}$$

et cet ensemble est fini. Notons $\Phi = \{\pi_{u,x_k} \mid 1 \leq k \leq r\}$. On a alors :

$$E = \bigcup_{k=1}^{r} \ker(\pi_{u,x_k}(u))$$

et il existe un indice k compris entre 1 et r tel que $E = \ker(\pi_{u,x_k}(u))$. Il en résulte que $\pi_{u,x_k} = \pi_u$ puisque π_{u,x_k} est un polynôme unitaire qui annule u et qui divise π_u.

9.

(a) Pour tout $P \in I_{u,x+y}$, on a $P(u)(x+y)=0$, donc $P(u)(x)=-P(u)(y) \in E_{u,x} \cap E_{u,y}$ et $P(u)(x)=P(u)(y)=0$ puisque cette intersection est réduite au vecteur non, ce qui nous dit que $P \in I_{u,x} \cap I_{u,y}$. On a donc $I_{u,x+y} \subset I_{u,x} \cap I_{u,y}$. Réciproquement si $P \in I_{u,x} \cap I_{u,y}$, on a $P(u)(x)=P(u)(y)=0$ et $P(u)(x+y)=0$, soit $P \in I_{u,x+y}$.
En définitive, on a $I_{u,x+y}=I_{u,x} \cap I_{u,y}$ avec $I_{u,x+y}=\mathbb{K}[X]\,\pi_{u,x+y}$ et $I_{u,x} \cap I_{u,y}=\mathbb{K}[X](\pi_{u,x} \vee \pi_{u,y})$ (par définition du ppcm), ce qui revient à dire que $\pi_{u,x+y}=\pi_{u,x} \vee \pi_{u,y}$ puisque ces polynômes sont unitaires.

(b) Si $P \in I_{u,x_1+\cdots+x_p}$, on a :

$$\sum_{k=1}^{p} P(u)(x_k) = P(u)\left(\sum_{k=1}^{p} x_k\right) = 0$$

donc $P(u)(x_k)=0$ pour tout k puisque $P(u)(x_k) \in E_{u,x_k}$ et ces sous-espaces sont en somme directe, ce qui nous dit que $P \in \bigcap_{k=1}^{p} I_{u,x_k}$. On a donc $I_{u,x_1+\cdots+x_p} \subset \bigcap_{k=1}^{p} I_{u,x_k}$.
Réciproquement si $P \in \bigcap_{k=1}^{p} I_{u,x_k}$, on a $P(u)(x_k)=0$ pour tout k et $P(u)\left(\sum_{k=1}^{p} x_k\right)=0$, soit $P \in I_{u,x_1+\cdots+x_p}$.
En définitive, on a $I_{u,x_1+\cdots+x_p}=\bigcap_{k=1}^{p} I_{u,x_k}$ et $\pi_{u,x_1+\cdots+x_p}=\pi_{u,x_1} \vee \cdots \vee \pi_{u,x_p}$.

(c) On vérifie facilement que pour tous vecteurs $x_1, \cdots, x_p$ dans $E \setminus \{0\}$, on a :

$$E_{u,x_1+\cdots+x_p} \subset \sum_{k=1}^{p} E_{u,x_k}$$

Soit $(y_k)_{1\leq k\leq p}$ une suite de vecteurs telle que $y_k=P_k(u)(x_k) \in E_{u,x_k}$ et $y=\sum_{k=1}^{p} y_k=0$.
En notant $Q_j=\prod_{\substack{k=1\\k\neq j}}^{p} \pi_{u,x_k}$ pour $1 \leq j \leq p$, on a :

$$0=P_j(u)(y)=\sum_{k=1}^{p} P_k(u)(Q_j(u)(x_k))=(P_jQ_j)(u)(x_j)$$

et π_{u,x_j} va diviser P_jQ_j en étant premier avec Q_j puisque les π_{u,x_k} sont deux à deux premiers entre eux. Le théorème de Gauss nous dit alors que π_{u,x_j} divise P_j et $y_j=P_j(u)(x_j)=0$.
On a donc $\sum_{k=1}^{p} E_{u,x_k}=\bigoplus_{k=1}^{p} E_{u,x_k}$ et avec la question précédente, on déduit que :

$$\pi_{u,x_1+\cdots+x_p}=\pi_{u,x_1} \vee \cdots \vee \pi_{u,x_p}=\pi_{u,x_1} \cdot \cdots \cdot \pi_{u,x_p}$$

et :

$$\begin{aligned}\dim\left(E_{u,x_1+\cdots+x_p}\right)=\deg\left(\pi_{u,x_1+\cdots+x_p}\right)&=\sum_{k=1}^{p}\deg\left(\pi_{u,x_k}\right)=\sum_{k=1}^{p}\dim\left(E_{u,x_k}\right)\\&=\dim\left(\bigoplus_{k=1}^{p} E_{u,x_k}\right)\end{aligned}$$

ce qui nous donne l'égalité $E_{u,x_1+\cdots+x_p}=\bigoplus_{k=1}^{p} E_{u,x_k}$.

(d) Pour tout $x \in E \setminus \{0\}$, on a $P^m(u)(x) = 0$, donc $\pi_{u,x}$ divise P^m et il existe un entier m_x compris entre 1 et m tel que $\pi_{u,x} = P^{m_x}$.
Si $m = 1$, on a alors $\pi_{u,x} = P = \pi_u$ pour tout $x \in E \setminus \{0\}$ et c'est terminé.
Si $m \geq 2$ et tous les m_x sont strictement inférieur à m, l'ensemble $\{m_x \mid x \in E \setminus \{0\}\}$ étant contenu dans $\{1, \cdots, m-1\}$ admet un plus grand élément r compris entre 1 et $m-1$, mais alors $P^r(u)(x) = 0$ pour tout $x \in E$ et $\pi_u = P^m$ ne peut être le polynôme minimal de u. Il existe donc $x \in E \setminus \{0\}$ tel que $\pi_{u,x} = P^m = \pi_u$.

(e) Dans le cas général, on a la décomposition en facteurs premiers unitaires $\pi_u = \prod_{k=1}^{p} P_k^{m_k}$ et le théorème de décomposition des noyaux nous dit que $E = \bigoplus_{k=1}^{p} F_k$, où les espaces $F_k = \ker\left(P_k^{m_k}(u)\right)$ sont stables par u, le polynôme minimal de la restriction de u à F_k étant $P_k^{m_k}$ (facile à vérifier). De la question précédente, on déduit que pour tout entier k compris entre 1 et r, il existe un vecteur $x_k \in F_k \setminus \{0\}$ tel que $\pi_{u_{|F_k},x_k} = \pi_{u_{|F_k}} = P_k^{m_k}$. De $P_k^{m_k}(u)(x_k) = 0$, on déduit que π_{u,x_k} divise $P_k^{m_k}$ et de $\pi_{u,x_k}\left(u_{|F_k}\right)(x_k) = 0$, on déduit que $P_k^{m_k}$ divise π_{u,x_k}, donc $\pi_{u,x_k} = P_k^{m_k}$.
Enfin comme les $\pi_{u,x_k} = P_k^{m_k}$ sont deux à deux premiers entre eux, en notant $x = \sum_{k=1}^{p} x_k$, on a $x \neq 0$ et $E_{u,x} = \bigoplus_{k=1}^{p} E_{u,x_k}$, ce qui entraîne :

$$\pi_{u,x} = \pi_{u,x_1} \vee \cdots \vee \pi_{u,x_p} = \prod_{k=1}^{p} P_k^{m_k} = \pi_u$$

Endomorphismes cycliques

1. Si $\mathcal{B}_{u,x}$ est une base de E, on a alors $E = \mathrm{Vect}(\mathcal{B}_{u,x}) \subset E_{u,x}$, donc $E = E_{u,x}$ et u est cyclique. Réciproquement, soit u est cyclique et $x \in E \setminus \{0\}$ tel que $E = E_{u,x}$. Si la famille $\mathcal{B}_{u,x}$ est liée, il existe un entier p compris entre 1 et $n-1$ tel que $u^p(x)$ soit combinaison linéaire de $x, \cdots, u^{p-1}(x)$ et en procédant par récurrence, on en déduit facilement que pour tout entier $k \geq p$, $u^k(x)$ est combinaison linéaire de $x, \cdots, u^{p-1}(x)$, ce qui entraîne que :

$$E_{u,x} = \mathrm{Vect}\left\{u^k(x) \mid k \in \mathbb{N}\right\} \subset \mathrm{Vect}\left\{u^k(x) \mid 0 \leq k \leq p-1\right\}$$

et $\dim(E_{u,x}) \leq p < n$, en contradiction avec $E = E_{u,x}$. La famille $\mathcal{B}_{u,x}$ est donc libre et c'est une base de E.

2. Si u est cyclique, il existe alors un vecteur $x \in E \setminus \{0\}$ tel que $\mathcal{B}_{u,x} = \left(u^k(x)\right)_{0 \leq k \leq n-1}$ soit une base de E et $\deg(\pi_{u,x}) = n$ (si $\deg(\pi_{u,x}) = p < n$, la famille $\left(u^k(x)\right)_{0 \leq k \leq p}$ est alors liée).
S'il existe un vecteur $x \in E \setminus \{0\}$ tel que $\deg(\pi_{u,x}) = n$, la famille $\left(u^k(x)\right)_{0 \leq k \leq n-1}$ est nécessairement libre (sinon on a un élément non nul de $I_{u,x}$ de degré strictement inférieur à n) et c'est une base de E, donc u est cyclique.

3. Soient u cyclique et $x \in E \setminus \{0\}$ tel que $\mathcal{B}_{u,x} = \left(u^k(x)\right)_{0 \leq k \leq n-1}$ soit une base de E. En écrivant que $u^n(x) = \sum_{k=0}^{n-1} a_k u^k(x)$, on voit que la matrice de u dans cette base est la matrice

de Frobenius :

$$F = \begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & \ddots & \vdots & a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & a_{n-1} \end{pmatrix}$$

C'est la matrice compagnon de $P(X) = X^p - \sum_{k=0}^{p-1} a_k X^k$ qui est le polynôme minimal et le polynôme caractéristique de u.
Réciproquement, supposons qu'il existe une base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E dans laquelle la matrice de u soit une matrice de Frobenius F. En notant $x = e_1$, on a $u^k(x) = e_{k+1}$ pour k compris entre 0 et $n-1$ et $\left(u^k(x)\right)_{0\leq k\leq n-1}$ est une base de E. Donc u est cyclique.

4. Supposons que $P_u = \pi_u$. Si $x \in E\setminus\{0\}$ est tel que $\pi_{u,x} = \pi_u$, ce polynôme $\pi_{u,x}$ est alors de degré n et la famille $\left(u^k(x)\right)_{0\leq k\leq n-1}$ est nécessairement libre, c'est donc une base et u est cyclique.
Avec la question précédente, on a vu que la condition est nécessaire.
On peut aussi dire que si u est cyclique, alors $\left(u^k(x)\right)_{0\leq k\leq n-1}$ est une base de E et le polynôme minimal π_u ne peut être de degré $p \leq n-1$, sinon la famille $\left(u^k(x)\right)_{0\leq k\leq p}$ serait liée, il est donc de degré n et égal à P_u puisqu'il le divise et est unitaire comme P_u.

5.

   (a) Si u est cyclique, on a alors $P_u = \pi_u$ avec $\pi_u(X) = \prod_{k=1}^{p}(X-\lambda_k)$ (les valeurs propres de u sont les racines de π_u et u est diagonalisable si, et seulement si, π_u est scindé à racines simples), ce qui impose $p = n$.
   Si u est diagonalisable avec n valeurs propres distinctes, son polynôme minimal est alors unitaire, de degré n et divisant le polynôme minimal P_u lui aussi unitaire de degré n, donc $\pi_u = P_u$ et u est cyclique.

   (b) Pour u cyclique, on a $\pi_u = P_u$. Si u est diagonalisable, π_u est alors scindé à racines simples et comme il est de degré n, on en déduit que u a n valeurs propres distinctes.
   Si u a n valeurs propres distinctes, il est alors diagonalisable (cyclique ou pas).

6.

   (a) Pour tout $P \in E$, on a $u^n(P) = P^{(n)} = 0$, donc u est nilpotent.
   Avec $u^0(e_{n-1}) = e_{n-1}$ et :

$$u^k(e_{n-1}) = \left(X^{n-1}\right)^{(k)} = (n-1)\cdots(n-k)\,X^{n-1-k} = \frac{(n-1)!}{(n-k-1)!}e_{n-1-k}$$

   pour k compris entre 1 et $n-1$, on déduit que la famille $\left(u^k(e_{n-1})\right)_{0\leq k\leq n-1}$ est une base de E et $E = E_{u,e_{n-1}}$, donc u est cyclique.
   Avec $u^{n-1}(e_{n-1}) = (n-1)!e_0 \neq 0$, on déduit que u est nilpotent d'indice n.

   (b) Si P est un polynôme constant, on a $u(P) = 0$ et si P est de degré $p \geq 1$, on a $\deg(u(P)) = \deg(P) - 1$, le coefficient dominant de $u(P)$ étant pa_p en désignant par a_p celui de P, donc $\deg(u^n(P)) \leq \deg(P) - n < 0$ et $u^n(P) = 0$, c'est-à-dire que u est nilpotent.
   Avec $\deg\left(u^k(e_{n-1})\right) = n-1-k$, on déduit que la la famille $\left(u^k(e_{n-1})\right)_{0\leq k\leq n-1}$ est échelonnée en degré et c'est une base de E, donc u est cyclique.
   Avec $\deg(u^{n-2}(e_{n-1})) = 1$, on déduit que $u^{n-2}(e_{n-1}) = aX+b$ avec $a \neq 0$ et $u^{n-1}(e_{n-1}) = a \neq 0$, donc u est nilpotent d'indice n.

7. Comme $u^{q-1} \neq 0$, il existe $x \in E \setminus \{0\}$ tel que $u^{q-1}(x) \neq 0$.
Si $\sum_{k=0}^{q-1} \lambda_k u^k(x) = 0$, on a alors :

$$0 = u^{q-1}\left(\sum_{k=0}^{q-1} \lambda_k u^k(x)\right) = \lambda_0 u^{q-1}(x)$$

($u^{q+k} = 0$ pour $k \geq 0$) et $\lambda_0 = 0$. Si $q = 1$, c'est fini, sinon en supposant que $\lambda_0 = \cdots = \lambda_j = 0$ pour $0 \leq j \leq q-2$, on a $\sum_{k=j+1}^{q-1} \lambda_k u^k(x) = 0$ et, en appliquant u^{q-2-j} à cette dernière égalité, on obtient $\lambda_{j+1} u^{q-1}(x) = 0$ et $\lambda_{j+1} = 0$. D'où le résultat.

8. Soit u nilpotent d'ordre q et cyclique. Il existe $x \in E$ tel que $\mathcal{B}_{u,x} = \left(u^k(x)\right)_{0 \leq k \leq n-1}$ soit une base de E et en particulier $u^{n-1}(x) \neq 0$, donc $q = n$.
Réciproquement soit u nilpotent d'ordre n. La famille $\mathcal{B}_{u,x} = \left(u^k(x)\right)_{0 \leq k \leq n-1}$ est alors une base de E et u est cyclique.

9.

   (a) La matrice A_0 étant annulée par le polynôme $X^p - 1$ qui est scindé et à racines simples dans $\mathbb{C}[X]$, est diagonalisable, ses valeurs propres étant des racines p-ème de l'unité.

   (b) Si $\lambda \in \mathbb{R}$ est une valeur propre de A_0, alors λ^p est valeur propre de $A_0^p = I_2$, donc $\lambda^p = 1$ et $\lambda \in \{-1, 1\}$. Comme on est en dimension 2, A_0 a une deuxième valeur propre réelle qui est aussi dans $\{-1, 1\}$. Cette matrice étant diagonalisable dans $\mathcal{M}_2(\mathbb{C})$, on en déduit que $A_0^2 = I_2$, ce qui n'est pas ($A_0^k \neq I_2$ pour $1 \leq k \leq p-1$ avec $p - 1 \geq 2$). Donc les valeurs propres complexes de A_0 sont non réelles.
   Les valeurs propres complexes de A_0 sont donc $\lambda = e^{\frac{2ik\pi}{p}}$ et $\overline{\lambda} = e^{-\frac{2ik\pi}{p}}$ (elles sont conjuguées puisque A_0 est réelles et racines p-èmes de l'unité puisque $A_0^p = I_2$) où k est un entier compris entre 1 et $p-1$. Comme A_0 est d'ordre p, il en est de même de λ dans $\mathbb{C}^*$ et k est premier avec p, ce qui peut se montrer comme suit : en notant $\delta = k \wedge p$, on a $p = \delta p'$, $k = \delta k'$ et $\lambda^{p'} = \left(e^{\frac{2ik'\pi}{p'}}\right)^{p'} = e^{2ik'\pi} = 1$, $\overline{\lambda}^{p'}$, donc $A_0^{p'} = I_2$ avec $1 \leq p' \leq p-1$ si $\delta \neq 1$, ce qui contredit le fait que A_0 est d'ordre p, donc $\delta = 1$.

   (c) Dire que la famille $(x, u(x))$ est liée équivaut à dire qu'il existe un réel λ tel que $u(x) = \lambda$, ce qui contredit le fait que A_0 n'a pas de valeurs propres réelles. Cette famille est donc libre et c'est une base de E.

   (d) On sait déja que la matrice de u dans la base $(x, u(x))$ est de la forme :

$$A = \begin{pmatrix} 0 & a_0 \\ 1 & a_1 \end{pmatrix}$$

   et le polynôme caractéristique de u est :

$$P_u(X) = P_A(X) = X^2 - a_1 X - a_0 = P_{A_0}(X) = X^2 - \operatorname{Tr}(A_0) + \det(A_0)$$

   ce qui nous donne :

$$a_1 = \operatorname{Tr}(A_0) = \lambda + \overline{\lambda} = 2\cos\left(\frac{2k\pi}{p}\right)$$

   et :

$$a_0 = -\det(A_0) = -\lambda \cdot \overline{\lambda} = -1$$

10. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u est de la forme :

$$F = \begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & \ddots & \vdots & a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & a_{p-1} \end{pmatrix}$$

où $P(X) = X^p - \sum_{k=0}^{p-1} a_k X^k$ est le polynôme caractéristique et minimal de u. La matrice :

$$\lambda I_n - F = \begin{pmatrix} \lambda & \cdots & 0 & -a_0 \\ -1 & \ddots & \vdots & -a_1 \\ \vdots & \ddots & \lambda & \vdots \\ 0 & \cdots & -1 & \lambda - a_{p-1} \end{pmatrix}$$

est de rang 1 puisque $\det(\lambda I_n - F) = 0$ et le déterminant de la matrice d'ordre $n-1$ extraite en supprimant la première ligne et la dernière colonne vaut $(-1)^{n-1} \neq 0$, donc l'espace propre $\ker(\lambda Id - u)$ est de dimension 1.
Cet espace propre s'obtient en résolvant le système $FX = \lambda X$, ce qui nous donne :

$$\begin{cases} \lambda x_1 - a_0 x_n = 0 \\ -x_{k-1} + \lambda x_k - a_{k-1} x_n = 0 \ \ (2 \leq k \leq n) \end{cases}$$

soit :

$$\begin{cases} x_{n-1} = (\lambda - a_{n-1}) x_n \\ x_{n-2} = \lambda x_{n-1} - a_{n-2} x_n = (\lambda^2 - a_{n-1}\lambda - a_{n-2}) x_n \\ x_{n-3} = \lambda x_{n-2} - a_{n-3} x_n = (\lambda^3 - a_{n-1}\lambda^2 - a_{n-2}\lambda - a_{n-3}) x_n \\ \vdots \\ x_1 = \lambda x_2 - a_1 x_n = (\lambda^{n-1} - a_{n-1}\lambda^{n-2} - \cdots - a_2\lambda - a_1) x_n \end{cases}$$

la première équation se traduisant par $P(\lambda) x_n = 0$. Prenant $x_n = 1$, un générateur de $\ker(\lambda Id - u)$ est le vecteur x dont les coordonnées dans la base $\mathcal{B}$ sont :

$$\left(\lambda^{n-1} - a_{n-1}\lambda^{n-2} - \cdots - a_1, \cdots, \lambda^2 - a_{n-1}\lambda - a_{n-2}, \lambda - a_{n-1}, 1\right)$$

Décomposition de Frobenius

1. Pour tout entier $k \geq 0$, on a $({}^t u)^k = {}^t u^k$ et pour tout polynôme $P \in \mathbb{K}[X]$, $P({}^t u) = {}^t(P(u))$, donc $P({}^t u) = 0$ si, et seulement, $P(u) = 0$ et $I_{{}^t u} = I_u$, $\pi_{{}^t u} = \pi_u$.
2.
   (a) Supposons qu'il existe des scalaires non tous nuls $\lambda_1, \cdots, \lambda_p$ tels que $\sum_{k=1}^{p} \lambda_k \varphi_k = 0$. En désignant par r le plus grand indice compris entre 1 et p tel que $\lambda_r \neq 0$, on a :

$$\begin{aligned} 0 &= \sum_{k=1}^{r} \lambda_k \varphi_k \left(u^{p-r}(x)\right) = \sum_{k=1}^{r} \lambda_k e_p^* \left(u^{k-1}\left(u^{p-r}(x)\right)\right) \\ &= \sum_{k=1}^{r} \lambda_k e_p^* \left(u^{p-r+k-1}(x)\right) = \sum_{k=1}^{r} \lambda_k e_p^* (e_{p-r+k}) = \lambda_r \end{aligned}$$

   ce qui est contradictoire. La famille $(\varphi_k)_{1 \leq k \leq p}$ est donc libre dans E^* et $\dim(G) = p$.

(b) On a $\dim(E_{u,x}) = \deg(\pi_{u,x}) = p$ et $\dim(G^\circ) = n - \dim(G) = n - p$.
Si $y \in E_{u,x} \cap G^\circ$, on $y = \sum_{k=1}^{p} \lambda_k e_k$ et pour tout j compris entre 1 et p :

$$0 = \varphi_j(y) = \sum_{k=1}^{p} \lambda_k \varphi_j(e_k)$$

Ce qui nous donne :

$$\varphi_1(e_k) = e_p^*(e_k) = \begin{cases} 0 \text{ si } 1 \leq k \leq p-1 \\ 1 \text{ si } k = p \end{cases} \Rightarrow \lambda_k = 0$$

$$\varphi_2(e_k) = e_p^*(u(e_k)) = e_p^*(e_{k+1}) = \begin{cases} 0 \text{ si } 1 \leq k \leq p-2 \\ 1 \text{ si } k = p-1 \end{cases} \Rightarrow \lambda_{p-1} = 0$$

et continuant ainsi de suite, on arrive à $\lambda_1 = \cdots = \lambda_p = 0$.
On a donc $E_{u,x} \cap G^\circ = \{0\}$ et $E = E_{u,x} \oplus G^\circ$.

(c) Pour k compris entre 1 et $p-1$, on a :

$${}^t u(\varphi_k) = \left({}^t u\right)^k \left(e_p^*\right) = \varphi_{k+1}$$

et pour $k = p$:

$${}^t u(\varphi_p) = \left({}^t u\right)^p \left(e_p^*\right) = e_p^* \circ u^p$$

avec u^p combinaison linéaire de $Id, u, \cdots, u^{p-1}$ (p est le degré du polynôme minimal), donc $e_p^* \circ u^p$ est combinaison linéaire de $e_p^* \circ Id = \varphi_1, e_p^* \circ u = \varphi_2, \cdots, e_p^* \circ u^{p-1} = \varphi_p$, c'est-à-dire que ${}^t u(\varphi_p) \in G$. L'espace G est donc stable par ${}^t u$.

(d) Pour $y \in G^\circ$ et $\varphi \in G$, on a $\varphi(y) = 0$ et $\varphi(u(y)) = ({}^t u)(\varphi)(y) = 0$ puisque G est donc stable par ${}^t u$, donc $u(y) \in G^\circ$ et G° est stable par u.

(e) On procède par récurrence sur $n = \dim(E) \geq 1$.
Pour $n = 1$, u est une homothétie et sa matrice est diagonale, donc de Frobenius, dans n'importe quelle base.
Supposons le résultat acquis pour les espaces de dimension comprise entre 1 et $n-1 \geq 1$ et soit $u \in \mathcal{L}(E)$ avec E de dimension $n \geq 2$.
Si u est cyclique, c'est alors terminé (son polynôme minimal est de degré n et il existe une base dans laquelle la matrice de u est la matrice compagon de π_u).
Sinon, on a une décomposition $E = E_{u,x} \oplus G^\circ$ avec $E_{u,x}, G^\circ$ stables par u, la restriction de u à $E_{u,x}$ étant cyclique. Il suffit alors d'appliquer l'hypothèse de récurrence à la restriction de u à G°, cet espace étant de dimension $n - p_u$ comprise entre 1 et $n-1$ puisque $1 \leq p_u \leq n-1$.
En écrivant que F_k est la matrice compagon de P_k, on a $P_1 = \pi_{u,x} = \pi_u$, $P_2 = \pi_v$, où v est la restriction de u à G°. De $P_1(u) = 0$, on déduit que $P_1(v) = 0$ et P_2 divise P_1.
La construction des F_k, nous montre que F_{k+1} divise F_k, pour tout k compris entre 1 et $r-1$.

Commutant d'un endomorphisme

1. Tout polynôme en u commute à u, donc $\mathbb{K}[u] \subset \mathcal{C}(u)$ et en particulier, $\mathcal{C}(u)$ est non vide.
Pour v, w dans $\mathcal{C}(u)$ et λ dans $\mathbb{K}$, on a :

$$u \circ (v + \lambda w) = u \circ v + \lambda u \circ w = v \circ u + \lambda w \circ u = (v + \lambda w) \circ u$$

donc $v+\lambda w \in \mathcal{C}(u)$ et $\mathcal{C}(u)$ est un sous-espace vectoriel de $\mathcal{L}(E)$ (on peut aussi dire que $\mathcal{C}(u)$ est le noyau de l'endomorphisme $\varphi_u : v \mapsto u\circ v - v\circ u$, c'est donc un sous-espace vectoriel de $\mathcal{L}(E)$).
D'autre part, $Id \in \mathcal{C}(u)$ et :

$$u\circ(v\circ w) = (u\circ v)\circ w = (v\circ u)\circ w = v\circ(u\circ w) = v\circ(w\circ u) = (v\circ w)\circ u$$

donc $v\circ w \in \mathcal{C}(u)$ et $\mathcal{C}(u)$ est un sous-anneau de $\mathcal{L}(E)$.
En définitive, $\mathcal{C}(u)$ est une sous-algèbre de $\mathcal{L}(E)$.

2. Soit $\mathcal{B}$ une base de diagonalisation dans laquelle la matrice de u est de la forme :

$$D = \begin{pmatrix} \lambda_1 I_{m_1} & 0 & \cdots & 0 \\ 0 & \lambda_2 I_{m_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_r I_{m_r} \end{pmatrix}$$

L'endomorphisme $v \in \mathcal{L}(E)$ de matrice :

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1r} \\ \vdots & \ddots & \vdots \\ A_{r1} & \cdots & A_{rr} \end{pmatrix}$$

dans la base $\mathcal{B}$, où $A_{ij} \in \mathcal{M}_{m_i,m_j}(\mathbb{K})$, est dans $\mathcal{C}(u)$ si, et seulement si, $AD = DA$, ce qui équivaut à :

$$\begin{pmatrix} \lambda_1 A_{11} & \cdots & \lambda_r A_{1r} \\ \vdots & \ddots & \vdots \\ \lambda_1 A_{r1} & \cdots & \lambda_r A_{rr} \end{pmatrix} = \begin{pmatrix} \lambda_1 A_{11} & \cdots & \lambda_1 A_{1r} \\ \vdots & \ddots & \vdots \\ \lambda_r A_{r1} & \cdots & \lambda_r A_{rr} \end{pmatrix}$$

soit à :

$$(\lambda_j - \lambda_i) A_{ij} = 0 \ \ (0 \leq i,j \leq r)$$

ou encore à $A_{ij} = 0$ pour $0 \leq i \neq j \leq r$.
L'espace $\mathcal{C}(u)$ est donc isomorphe à l'espace des matrices diagonales par blocs de la forme :

$$\begin{pmatrix} A_{11} & 0 & \cdots & 0 \\ 0 & A_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_{r,r} \end{pmatrix}$$

où $A_{ii} \in \mathcal{M}_{m_i}(\mathbb{K})$ et cet espace est de dimension $\displaystyle\sum_{k=1}^{r} m_k^2$.

3. Si u est cyclique, il existe alors $x \in E \setminus \{0\}$ tel que $\mathcal{B}_{u,x} = \left(u^k(x)\right)_{0\leq k\leq n-1}$ soit une base de E.
Pour $v \in \mathcal{C}(u)$, on peut alors écrire :

$$v(x) = \sum_{k=0}^{n-1} \lambda_k u^k(x) = \left(\sum_{k=0}^{n-1} \lambda_k u^k\right)(x)$$

et comme v commute à u, on a pour tout entier j compris entre 1 et $n-1$:

$$v\left(u^j(x)\right) = u^j(v(x)) = u^j\left(\sum_{k=0}^{n-1} \lambda_k u^k(x)\right) = \left(\sum_{k=0}^{n-1} \lambda_k u^k\right)\left(u^j(x)\right)$$

et $v = \sum_{k=0}^{n-1} \lambda_k u^k$ puisque ces deux endomorphismes coÏncident sur la base $\mathcal{B}_{u,x}$. On a donc $v \in \mathbb{K}[u]$. On a donc ainsi montré que $\mathcal{C}(u) \subset \mathbb{K}[u]$ et l'égalité. Il en résulte que :

$$\dim(\mathcal{C}(u)) = \dim(\mathbb{K}[u]) = \deg(\pi_u) = n$$

4. Comme $\mathcal{C}(u)$ est un sous-espace de $\mathcal{L}(E)$, on a $\dim(\mathcal{C}(u)) \leq n^2$ (pour $u = Id$, on a $\dim(\mathcal{C}(u)) = n$).
Soit $\mathcal{B}$ une base dans laquelle la matrice de u est diagonale par blocs de la forme :

$$F = \begin{pmatrix} F_1 & 0 & \cdots & 0 \\ 0 & F_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & F_r \end{pmatrix}$$

où les $F_k = C_{P_k} \in \mathcal{M}_{m_k}(\mathbb{K})$ sont des matrices de Frobenius, P_k étant un polynôme unitaire de degré m_k.
Le polynôme caractéristique de u est alors :

$$P_u(X) = P_F(X) = \prod_{k=1}^{r} P_{F_k}(X) = \prod_{k=1}^{r} P_k(X)$$

et $\sum_{k=1}^{r} \deg(P_k) = \sum_{k=1}^{r} m_k = n$.
Un endomorphisme $v \in \mathcal{L}(E)$ de matrice :

$$A = \begin{pmatrix} A_{11} & 0 & \cdots & 0 \\ 0 & A_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_{r,r} \end{pmatrix}$$

dans la base $\mathcal{B}$, où $A_{ii} \in \mathcal{M}_{m_i}(\mathbb{K})$, est dans $\mathcal{C}(u)$ si, et seulement si, chaque matrice A_{ii} est dans le commutant $\mathcal{C}(F_i) = \mathbb{K}[F_i]$ (F_i est la matrice, dans la base canonique, d'un endomorphisme cyclique de $\mathbb{K}^{m_i}$). L'ensemble $\mathcal{G}$ de ces endomorphisme est un sous-espace vectoriel de $\mathcal{L}(E)$ de dimension $\sum_{k=1}^{r} \dim(\mathcal{C}(F_k)) = \sum_{k=1}^{r} m_k = n$ et contenu dans $\mathcal{C}(u)$. On a donc $n \leq \dim(\mathcal{C}(u))$.
5. On sait déjà que si u est cyclique, alors $\mathcal{C}(u) = \mathbb{K}[u]$.
Réciproquement, si $\mathcal{C}(u) = \mathbb{K}[u]$, on a alors $n \leq \dim(\mathcal{C}(u)) = \dim(\mathbb{K}[u])$ avec $\dim(\mathbb{K}[u]) = \deg(\pi_u) \leq n$, donc $\deg(\pi_u) = n$, $\pi_u = P_u$ et u est cyclique.