I. Matrices compagnons et endomorphismes cycliques

(A)

1. Pour tout $\lambda \in \mathbb{K}$, $\chi_M(\lambda) = \det(\lambda I_n - M) = \det\left((\lambda I_n - M)^\top\right) = \det(\lambda I_n - M^\top) = \chi_{M^\top}(\lambda)$. Ainsi,

$$\forall \lambda \in \mathbb{K},\ \lambda \in \mathrm{sp}(M) \Leftrightarrow \chi_M(\lambda) = 0 \Leftrightarrow \chi_{M^\top}(\lambda) = 0 \Leftrightarrow \lambda \in \mathrm{sp}\left(M^\top\right).$$

Finalement, $\mathrm{sp}(M) = \mathrm{sp}\left(M^\top\right)$.

2. On suppose que M est diagonalisable ; on peut donc introduire $P \in GL_n(\mathbb{K})$ et $D \in \mathcal{M}_n(\mathbb{K})$ diagonale telles que $M = PDP^{-1}$. On a donc, $M^\top = (P^{-1})^\top D^\top P^\top = \left(P^\top\right)^{-1} DP^\top$, avec $P^\top \in GL_n(\mathbb{K})$. D'où $M^\top$ est diagonalisable.

La réciproque en découle puisque $M = \left(M^\top\right)^\top$.

(B) Matrices compagnons

3. Il existe plusieurs méthodes pour montrer que $\chi_{C_Q} = Q$.
En développant par rapport à la dernière colonne :

$$\begin{aligned}
\chi_{C_Q} &= \begin{vmatrix}
X & \dots & \dots & \dots & 0 & a_0 \\
-1 & X & \dots & \dots & 0 & a_1 \\
0 & -1 & \ddots & & \vdots & a_2 \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & & \ddots & -1 & X & a_{n-2} \\
0 & \dots & \dots & 0 & -1 & X + a_{n-1}
\end{vmatrix} \\
&= \sum_{i=0}^{n-2} (-1)^{n+i+1} a_i \begin{vmatrix} A_i & 0 \\ 0 & B_i \end{vmatrix} + (X + a_{n-1}) X^{n-1}
\end{aligned}$$

avec $A_i = \begin{vmatrix} X & 0 & \dots & 0 \\ -1 & X & 0 & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & -1 & X \end{vmatrix} \in \mathcal{M}_i(\mathbb{K})$ et $B_i = \begin{vmatrix} -1 & X & 0 & 0 \\ 0 & -1 & \ddots & 0 \\ \vdots & \ddots & \ddots & X \\ 0 & 0 & 0 & -1 \end{vmatrix} \in \mathcal{M}_{n-i+1}(\mathbb{K})$.

Donc $\chi_{C_Q} = \sum_{i=0}^{n-2} (-1)^{n+i+1}(-1)^{n-i+1} a_i X^i + a_{n-1}X^{n-1} + X^n = Q$.

On peut aussi montrer que $\chi_{C_Q} = Q$ par récurrence sur $\deg(Q) = n \geq 2$

Initialisation : On suppose que $\deg(Q) = 2$ ainsi $Q = X^2 + a_1 X + a_0$ et $C_Q = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$.
Ainsi, $\chi_{C_Q} = X^2 - \mathrm{Tr}(C_Q)X + \det(C_Q) = X^2 + a_1 X + a_0 = Q$.

Hérédité : Soit $n \geq 2$ tel que la propriété soit vraie pour tout polynôme unitaire de degré n.
On considère $Q(X) = X^{n+1} + a_n X^n + \dots + a_0$ où les $a_i \in \mathbb{K}$.
On a en développant par rapport à la première ligne :

$$\begin{aligned}
\chi_{C_Q} &= \begin{vmatrix}
X & \dots & \dots & \dots & 0 & a_0 \\
-1 & X & \dots & \dots & 0 & a_1 \\
0 & -1 & \ddots & & \vdots & a_2 \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & & \ddots & -1 & X & a_{n-1} \\
0 & \dots & \dots & 0 & -1 & X + a_n
\end{vmatrix}_{[n+1]} \\
&= X\chi_{C_R} + (-1)^{n+2} a_0 \begin{vmatrix}
-1 & X & \dots & \dots & 0 \\
0 & -1 & \ddots & & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & -1 & X \\
0 & \dots & \dots & 0 & -1
\end{vmatrix}_{[n]}
\end{aligned}$$

où $R = X^n + a_n X^{-1} + \dots + a_1$. Par hypothèse de récurrence, $\chi_{C_R} = R$, et donc $\chi_{C_Q} = XR + a_0 = Q$.

On a ainsi montré par récurrence que la propriété était vraie pour tout polynôme unitaire de degré ≥ 2.
Enfin, la dernière méthode usuelle est de faire l'opération $L_1 \leftarrow L_1 + XL_2 - X^2 L_3 + \ldots + (-1)^{n-1} L_n$.

4. Soit $\lambda \in \mathrm{Sp}(C_Q{}^\top) = \mathrm{Sp}(C_Q)$. Par définition, $\dim\left(E_\lambda(C_Q{}^\top)\right) \geq 1$.
Par ailleurs, $\dim\left(E_\lambda(C_Q{}^\top)\right) = n - \mathrm{rang}(C_Q{}^\top - \lambda I_n)$.

Or, $(C_Q)^\top - \lambda I_n = \begin{pmatrix} -\lambda & 1 & 0 & \dots & 0 \\ 0 & -\lambda & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & & 0 & 1 \\ -a_0 & -a_1 & \dots & & -\lambda - a_{n-1} \end{pmatrix}$ a une sous-matrice inversible de taille $n-1$ (en conservant les (n-1) premières lignes et $n-1$ dernières colonnes). Donc, $\text{rang}(C_Q - \lambda I_n) \geq n-1$ et $\dim\left(E_\lambda(C_Q{}^\top)\right) \leq 1$. Finalement, $\dim\left(E_\lambda(C_Q{}^\top)\right) = 1$.

Reste à en déterminer un vecteur.

Comme, $\chi_{C_Q{}^\top} = \chi_{C_Q} = Q$ ainsi $Q(\lambda) = 0$.

Soit $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$. On a :

$$(C_Q)^\top X = \lambda X \iff \begin{cases} x_2 & = \lambda x_1 \\ x_3 & = \lambda x_2 \\ \vdots & \\ x_n & = \lambda x_{n-1} \\ -a_0 x_1 & - \ldots - a_{n-1}x_n = \lambda x_n \end{cases}$$

$$\iff \begin{cases} x_2 = \lambda x_1 \\ x_3 = \lambda^2 x_1 \\ \vdots \\ x_n = \lambda^{n-1} x_1 \\ (-a_0 - a_1\lambda - \ldots - a_{n-1}\lambda^{n-1})x_1 = \lambda^n x_1 \end{cases}$$

$$\iff \begin{cases} \forall i \in [\![2, n]\!],\ x_i = \lambda^{i-1} x_1 \\ Q(\lambda) x_1 = 0 \end{cases}$$

Donc $E_\lambda\left(C_Q{}^\top\right) = \text{vect}(X_\lambda)$ où $X_\lambda = \begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}$.

(C) **Endomorphismes cycliques**

5. $\Rightarrow$ **:** On suppose que f est cyclique. On trouve ainsi $x_0 \in E$ tel que $\mathcal{B} = \left(x_0, f(x_0), \ldots, f^{n-1}(x_0)\right)$ soit une base de E. On peut donc décomposer $f^n(x_0)$ dans cette base : on pose $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $f^n(x_0) = \sum_{i=0}^{n-1} \lambda_i f^i(x_0)$.

   On pose $Q = X^n + \sum_{i=0}^{n-1}(-\lambda_i)X^i \mathbb{K}[X]$. On vérifie alors que $\mathcal{M}_\mathcal{B}(f) = C_Q$.

   $\Leftarrow$ **:** On suppose qu'il existe une base $\mathcal{B} = (e_0, e_1, \ldots e_{n-1})$ de E dans laquelle la matrice de f est de la forme C_Q, où Q est un polynôme unitaire de degré n . Ainsi pour tout $i \in [\![0, n-2]\!]$, $f(e_i) = e_{i+1}$. Ainsi $(e_0, f(e_0), f^2(e_0), \ldots, f^{n-1}(e_0)) = (e_0, e_1, \ldots e_{n-1})$ est une base de E. Finalement, f est cyclique.

6. Soit f un endomorphisme cyclique.

   Si χ_f est scindé sur $\mathbb{K}$ et a toutes ses racines simples, on sait que f est diagonalisable d'après le cours.

   Réciproquement, on suppose que f, cyclique, est diagonalisable. On sait qu'alors χ_f est scindé sur $\mathbb{K}$ et que chaque sous-espace propre a pour dimension la multiplicité de la valeur propre en question. Par ailleurs, comme f est cyclique, d'après la question **??**, chaque sous-espace propre est de dimension 1. On en déduit donc que toutes les valeurs propres sont simples. Ainsi χ_f est scindé sur $\mathbb{K}$ et a toutes ses racines simples.

7. On suppose que f est cyclique. Soit $(\lambda_0, \ldots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $\sum_{i=0}^{n} \lambda_i f^i = 0_{\mathcal{L}(E)}$.

   Comme f est cyclique, on introduit $x_0 \in E$ tel que $\mathcal{B} = \left(f^j(x_0)\right)_{0 \leq j \leq n-1}$ soit une base de E. En évaluant en x_0, on obtient : $\sum_{i=0}^{n} \lambda_i f^i(x_0) = 0_{\mathcal{L}(E)}(x_0) = 0_E$. Or $\mathcal{B}$ est libre, on en déduit que pour tout $i \in [\![0, n-1]\!]$, $\lambda_i = 0$.

   Finalement, $\left(f^j\right)_{0 \leq j \leq n-1}$ est libre dans $\mathcal{L}(E)$.

   On sait que $\dim(\mathbb{K}[f]) = d$, le degré de π_f. Comme $(\text{Id}, f, f^2, \ldots, f^{n-1})$ est libre dans $\mathbb{K}[f]$, $d \geq n$. Par ailleurs, d'après le théorème de Cayley-Hamilton, le polynôme χ_f est un polynôme annulateur ; π_f divise χ_f ; et donc $d = \deg(\pi_f) \leq \deg(\chi_f) = n$. Finalement $n = d$ et le polynôme minimal de f est de degré n.

(D) **Application à une démonstration du théorème de Cayley-Hamilton**

8. Soit x un vecteur non nul de E.
Approche 1 : On note $N_x = \left\{m \in \mathbb{N}^*,\ \left(f^i(x)\right)_{0\leq i\leq m-1} \text{ libre}\right\}$.
Comme $x \neq 0_E$, $1 \in N_x$; par aileurs N_x est majoré par $n = \dim E$; N_x admet donc un plus grand élément $p \in \mathbb{N}^*$.
Par définition, la famille $\left(f^i(x)\right)_{0\leq i\leq p-1}$ est libre et la famille $\left(f^i(x)\right)_{0\leq i\leq p}$ est liée. On peut donc introduire $(\alpha_j)_{0\leq i\leq p-1} \in \mathbb{K}^p$ tel que $\sum_{j=0}^{p-1} \alpha_j f^j(x) + f^p(x) = 0$.
Approche 2 : On note $I_x = \{P \in \mathbb{K}[X],\ P(f)(x) = 0_E\}$. On vérifie qu'il s'agit d'un idéal de $\mathbb{K}[X]$. En effet, c'est un sous-groupe pour la loi $+$, en tant que noyau de l'application linéaire $\varphi_x : P \in \mathbb{K}[X] \longmapsto P(f)(x) \in E$. De plus, pour tout $P \in I_x$ et $Q \in \mathbb{K}[X]$, on a $(QP)(f)(x) = (Q(f) \circ P(f))(x) = Q(f)(P(f)(x)) = 0_E$. Ainsi $QP \in I_x$.
Il est donc principal et engendré par un polynôme $P_x = X^p + \sum_{k=0}^{p-1} \alpha_j X^j$. Ainsi $0_E = P_x(f)(x) = f^p(x) + \sum_{k=0}^{p-1} \alpha_j f^j(x)$.
De plus si $\sum_{k=0}^{p-1} a_j f^j(x) = 0_E$, le polynôme $Q = \sum_{k=0}^{p-1} a_j X^j$ est dans I_x, donc divisible par P_x. Pour des raisons de degré, $Q = 0_{\mathbb{K}[X]}$.
Finalement, la famille $\left(f^i(x)\right)_{0\leq i\leq p-1}$ est libre.

9. Soit $F_x = \mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$. Pour tout $0 \leq j \leq p-2$, $f(f^j(x)) \in F_x$. De plus, $f\left(f^{p-1}(x)\right) = f^p(x) = -\sum_{j=0}^{p-1} \alpha_j f^j(x) \in F_x$.
Finalement, par linéarité de f, on a bien montré $f(F_x) \subset F_x$.

10. On note $\tilde{f}$ l'endomorphisme induit par f sur F_x. Comme elle est libre et génératrice, $\mathcal{B} = \left(f^i(x)\right)_{0\leq i\leq p-1}$ est une base de F_x.
On remarque que $\mathcal{M}_{\mathcal{B}}(\tilde{f}) = C_{P_x}$ en notant $P_x = \alpha_0 + \alpha_1 X + \cdots + \alpha_{p-1}X^{p-1} + X^p$. On en déduit donc que $\chi_{\tilde{f}} = P_x$. Or $\chi_{\tilde{f}}$ divise χ_f.
On peut donc conclure que P_x divise le polynôme χ_f.

11. Soit $Q \in \mathbb{K}[X]$, tel que $\chi_f = QP_x$. Or, on a $P_x(f)(x) = 0_0$. Or, $\chi_f(f) = Q(f) \circ P_x(f)$; ainsi $\chi(f)(x) = Q(f)(P_x(f)(x)) = Q(f)(0_E) = 0_E$.
On l'a montré pour $x \in E$ quelconque. Donc $\chi_f(f)$ est l'endomorphisme nul.

II. Étude des endomorphismes cycliques

(A) Endomorphismes cycliques nilpotents

12. Comme f est nilpotente, son polynôme minimal est $\mu_f = X^r$. Si f cyclique alors $\deg(\pi_f) = n$ d'après 7 et donc $r = n$.
Réciproquement, si $r = n$, alors $f^n = 0$ et $f^{n-1} \neq 0$. Ceci nous fournit $x \in E$ tel que $f^{n-1}(x) \neq 0$. Et on montre alors (méthode habituelle à développer) que $\left(f^i(x)\right)_{0\leq i\leq n-1}$ est libre, de cardinal n.
Donc f est cyclique.
Comme f est nilpotente, $\chi_f = X^n$ et la matrice compagnon est dans ce cas $\begin{pmatrix} 0 & \ldots & \ldots & \ldots & 0 & 0 \\ 1 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & 1 & \ddots & & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & 0 \\ 0 & \ldots & \ldots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$.

(B)

13. Pour $k \in [\![1,p]\!]$, $(f - \lambda_k \mathrm{Id}_E)^{m_k}$ et f commutent car $\mathbb{C}[f]$ est une algèbre commutative ; donc $F_k = \ker((f - \lambda_k \mathrm{Id}_E)^{m_k})$ est stable par f.
D'après le théorème de Cayley-Hamilton, $\chi_f(f) = 0$. Par ailleurs, les polynômes $(X - \lambda_k)^{m_k}$ sont deux à deux premiers entre eux ; d'après le théorème de décomposition des noyaux,
$$E = \ker(\chi(f)) = \bigoplus_{j=1}^{p} \ker((f - \lambda_j \mathrm{Id}_E)^{m_j}) = \bigoplus_{j=1}^{p} F_j.$$

14. Par définition, pour tout $x \in F_k$, $(f - \lambda_k \mathrm{Id})^{m_k}(x) = 0$. Or pour tout $x \in F_k$, $(f - \lambda_k \mathrm{Id})(x) = \varphi_k(x) \in F_k$; et donc (par récurrence immédiate sur p) pour tout $p \in \mathbb{N}$, $(f - \lambda_k \mathrm{Id})^p(x) = \varphi_k^p(x)$. Finalement, pour tout $x \in F_k$, $\varphi_k^{m_k}(x) = 0_E$. Comme c'est vrai pour tout $x \in F_k$, on conclut que $\varphi_k^{m_k} = 0_{\mathcal{L}(F_k)}$.
On note ν_k le plus petit entier naturel tel que $\varphi_k^{\nu_k} = 0$.

15. D'après le cours, l'indice de nilpotence de φ_k, ν_k, endomorphisme de F_k est majoré par $\dim(F_k)$.

16. On note $P = \prod_{i=1}^{p} (X - \lambda_i)^{\nu_i}$. Soit $k \in [\![1, p]\!]$. Pour tout $x \in F_k$,

$$\begin{aligned} P(f)(x) &= \left[\prod_{\substack{i=1\\ i\neq k}}^{p} (X-\lambda_i)^{\nu_i}(f)\right] \circ (f - \lambda_k \mathrm{Id})^{\nu_k}(x) \\ &= \left[\prod_{\substack{i=1\\ i\neq k}}^{p} (X-\lambda_i)^{\nu_i}(f)\right](0_E) = 0_E. \end{aligned}$$

Donc $P(f)$ coïncide avec l'endomorphisme nul sur chaque F_k ; comme $E = \bigoplus_{k=1}^{p} F_k$, $P(f) = 0_{\mathcal{L}(E)}$.

Ainsi, P est divisible par π_f qui est de degré supérieur ou égal à n, car $(\mathrm{Id}_E, f, \dots, f^{n-1})$ est libre. On en déduit que le degré de P, $d = \sum_{k=0}^{p} \nu_k \geq n$. Or d'après la question 14, pour tout $k \in [\![1, p]\!]$, $\nu_k \leq m_k$.

Finalement, $n \leq \sum_{k=0}^{p} \nu_k \leq \sum_{i=0}^{p} m_k = n$. Ainsi les inégalités sont des égalités et pour tout $k \in [\![1, p]\!]$, on a $\nu_k = m_k$.

17. On rappelle que $E = F_1 \oplus \cdots \oplus F_p$. Ainsi, $n = \sum_{k=1}^{p} \dim(F_k) \geq \sum_{k=1}^{p} \nu_k = n$ d'après ce qui précède. Comme à la question précédente, on obtient : $\forall k \in [\![1, p]\!]$, $\nu_k = m_k = \dim(F_k)$.

Ce n'est pas la méthode utilisée dans le cours, mais c'est la plus rapide étant donné ce qui a déjà été démontré.

Finalement φ_k est un endomorphisme nilpotent de F_k d'indice $\nu_k = m_k = \dim(F_k)$, donc (d'après la question 12), φ_k est nilpotent et cyclique. On peut donc introduire une base $\mathcal{B}_k$ de F_k tel que $\mathcal{M}_{\mathcal{B}_k}(\varphi_k) = \begin{pmatrix} 0 & 0 & \dots & \dots & \dots & 0 \\ 1 & 0 & \ddots & & & \vdots \\ 0 & 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{m_k}(\mathbb{C})$.

En notant f_k l'endomorphisme induit par f sur F_k, on a alors

$$\mathcal{M}_{\mathcal{B}_k}(f_k) = \begin{pmatrix} \lambda_k & 0 & \dots & \dots & \dots & 0 \\ 1 & \lambda_k & \ddots & & & \vdots \\ 0 & 1 & \lambda_k & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \lambda_k & 0 \\ 0 & \dots & \dots & 0 & 1 & \lambda_k \end{pmatrix} \in \mathcal{M}_{m_k}(\mathbb{C})$$

Finalement, en concaténant les bases $\mathcal{B}_k$ pour k allant de 1 à p, on obtient une base $\mathcal{B}$ adaptée à la décomposition en somme directe $E = F_1 \oplus \cdots \oplus F_p$ et dans laquelle f a une matrice diagonale par blocs de la forme equise.

18. Pour $k \in [\![1, p]\!]$, on note $z_k = u_{m_1 + \cdots + m_{k-1} + 1} \in F_k$. Ainsi $x_0 = \sum_{k=1}^{p} z_k$.

Pour tout polynôme $P \in \mathbb{C}[X]$, $P(f)(x_0) = 0_E$ si seulement si $\sum_{k=1}^{p} P(f)(z_k) = 0_E$. Par stabilité des F_k par f, pour tout $k \in [\![1, p]\!]$, $P(f)(z_k) = P(f_k)(z_k) \in F_k$. Comme la somme des F_k est directe, $P(f)(x_0) = 0_E$ si seulement si pour tout $k \in [\![1, p]\!]$, $P(f_k)(z_k) = 0_{F_k}$.

Soit $k \in [\![1, p]\!]$. Par construction (voir question précédente), $\mathcal{B}_k = \left(\phi_k^j(z_k)\right)_{0 \leq j \leq m_k - 1}$ est une base de F_k, avec ϕ_k un endomorphisme nilplotent cyclique. Comme $f_k = \phi_k + \lambda_k \mathrm{Id}_{F_k}$, f_k et ϕ_k commutent. Donc si $P(f_k)(z_k) = 0_{F_k}$, alors pour tout $0 \leq j \leq m_k - 1$, $P(f_k)\left(\phi_k^j(z_k)\right) = \phi_k^j\left(P(f_k)(z_k)\right) = 0_{F_k}$. Ainsi, $P(f_k)$ s'annulant sur une base, $P(f_k)$ est nul. Ainsi,

$$P(f_k)(z_k) = 0_{F_k} \Leftrightarrow P(f_k) = 0_{\mathcal{L}(F_k)} \Leftrightarrow P(\phi_k + \lambda_k \mathrm{Id}_{F_k}) = 0_{\mathcal{L}(F_k)}$$
$$\Leftrightarrow \pi_{\phi_k} = X^{\nu^k} | P(X+\lambda_k) \Leftrightarrow (X-\lambda_k)^{\nu_k} | P.$$

Finalement, les polynômes $(X-\lambda_k)^{\nu_k}$ étant premiers entre eux,

$$\begin{aligned} P(f)(x_0) = 0_E &\Leftrightarrow \forall k \in [\![1,p]\!],\ P(f_k)(z_k) = 0_{F_k} \\ &\Leftrightarrow \forall k \in [\![1,p]\!],\ (X-\lambda_k)^{\nu_k} | P \\ &\Leftrightarrow \chi_f = \prod_{k=1}^{p} (X-\lambda_k)^{\nu_k} | P. \end{aligned}$$

19. Soit $(\lambda_i)_{0 \leq i \leq n-1} \in \mathbb{K}^n$ tel que $\displaystyle\sum_{i=0}^{n-1} \lambda_i f^i(x_0) = 0$. En posant $Q = \displaystyle\sum_{i=0}^{n-1} \lambda_i X^i$, notre hypothèse s'écrit : $Q(f)(x_0) = 0$.

    D'après la question précédente, $\displaystyle\prod_{k=1}^{p} (X-\lambda_k)^{m_k}$ divise Q. Or $\deg(Q) \leq n-1 < n = \deg\left(\displaystyle\prod_{k=1}^{p} (X-\lambda_k)^{m_k}\right)$. Donc Q est le polynôme nul, *i.e.* pour tout $i \in [\![0, n-1]\!]$, $\lambda_i = 0$. Finalement, $\left(f^i(x_0)\right)_{0 \leq i \leq n-1}$ est une famille libre de n vecteurs de E et $n = \dim E$ et $\left(f^i(x_0)\right)_{0 \leq i \leq n-1}$ est une base de E. On peut donc conclure que f est cyclique.

III. Endomorphismes commutants, décomposition de Frobenius

(A) Commutant d'un endomorphisme cyclique

20. L'application $g \longmapsto f \circ g - g \circ f$ est un endomorphisme de $\mathcal{L}(E)$ dont le noyau est $C(f)$; $C(f)$ est donc un sous-espace vectoriel de $\mathcal{L}(E)$. Par ailleurs, pour tous g et $h \in C(f)$, on a $(g \circ h) \circ f = g \circ f \circ h = f \circ (g \circ h)$; ainsi $C(f)$ est stable par $\circ$; comme $\mathrm{Id} \in C(f)$, $C(f)$ est une sous-algèbre de $\mathcal{L}(E)$.
21. Comme $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$ est une base de E et $g(x_0) \in E$, il existe $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{K}$ tels que $g(x_0) = \displaystyle\sum_{k=0}^{n-1} \lambda_k f^k(x_0)$.
22. On souhaite vérifier que les applications linéaires g et $\displaystyle\sum_{k=0}^{n-1} \lambda_k f^k$ coïncident sur la base $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$. Comme g commute avec f, il commute avec tous les polynômes en f. En particulier, pour tout $i \in [\![0, n-1]\!]$, comme l'algèbre $\mathbb{K}[f]$ est commutative,

$$\begin{aligned} g\left(f^i(x_0)\right) &= f^i\left(g(x_0)\right) = f^i\left(\sum_{k=0}^{n-1} \lambda_k f^k(x_0)\right) \\ &= \sum_{k=0}^{n-1} \lambda_k f^k\left(f^i(x_0)\right). \end{aligned}$$

    Finalement, $g = \displaystyle\sum_{k=0}^{n-1} \lambda_k f^k$ et $g \in \mathbb{K}[f]$.
23. On vient de montrer que $C(f) \subset \mathbb{K}[f]$. Comme $\mathbb{K}[f]$ est une algèbre commutative, l'autre inclusion est immédiate. On a donc $C(f) = \mathbb{K}[f]$, qui admet pour base $(f^k)_{k \leq 0 \leq n-1}$. Et on a donc l'équivalence demandée.

(B) Décomposition de Frobenius

24. **Remarque :** Pour $r = 2$, la preuve est classique et générale : on suppose par exemple que F_1 ne contient pas F_2 On peut donc choisir $z \in F_2 \setminus F_1$. Ainsi pour tout $x \in F_1$, x et z sont dans $F_1 \cup F_2$ qui est un sous-espace vectoriel, donc $x + z$ également. S'il était dans F_1, on aurait $z = (z+x) - x \in F_1$, ce qui n'est pas le cas. Donc $x + z \in F_2$ et $x = (x+z) - z \in F_2$. On a donc montré $F_1 \subset F_2$.

    Pour le cas $r \geq 3$, on doit utiliser le fait que $\mathbb{K}$ est infini (ou au moins de cardinal supérieur à r). En effet, si on prend K un corps fini et $E = \mathbb{K}^d$ avec $d \geq 2$, E est fini (de cardinal p^d) et E est l'union finie des $\mathrm{Vect}(x)$ pour $x \in E \setminus \{0_E\}$ sans qu'aucune de ces droites ne contiennent toutes les autres.

    Pour montrer le résultat, on rédige une récurrence sur r. La propriété est vraie pour $r = 1$ et $r = 2$.

    Soit $r \geq 2$ tel que la propriété soit vérifiée pour $r - 1$. On suppose que $G = \displaystyle\bigcup_{j=1}^{r} F_j$ est un sous espace de E.

Si $F_r \subset G_0 = \bigcup_{j=1}^{r-1} F_j$, alors $G_0 = G$ est un sous-espace vectoriel, et par hypothèse de récurrence, il existe $k \in [\![1, r-1]\!]$ tel que $F_k = G_0 = G$. Ce F_k contient donc bien tous les autres.
On suppose que G_0 ne contient pas F_r On peut donc fixer $x \in F_r \backslash G_0$.
Si G_0 contient F_r, on a terminé.
Sinon, on peut fixer $y \in G_0 \setminus F_r$. Comme x et y sont dans le sous-espace vectoriel G, pour tout scalaire $a \in \mathbb{K}$, on a $y + ax \in G$. Mais $y + ax \notin F_r$ (car sinon $y = (y + ax) - ax \in F_r$). Ainsi, $y + ax \in G_0$: pour tout $a \in K$, on peut donc poser $k(a) \in [\![1, r-1]\!]$ tel que $y + ax \in F_{k(a)}$. Comme $\mathbb{K}$ est soit infini, soit de cardinal supérieur à r, l'application $a \mapsto k(a)$ ne peut pas être injective.
On trouve donc $j \in [\![1, r-1]\!]$ et $a \neq a'$ dans $\mathbb{K}$ tel que $y + ax \in F_j$ et $y + a'x \in F_j$. Finalement, par combinaison linéaire, $x \in F_j \subset G_0$, ce qui est absurde.
Finalement, on a bien montré par récurrence que l'un des sous-espaces F_k contient tous les autres.

25. Soit $x \in E$. On considère, comme en **??** l'application $\varphi_x : P \in \mathbb{K}[X] \longmapsto P(f)(x) \in E$, et son noyau $I_x = \{P \in \mathbb{K}[X] / \ P(f)(x) = 0\}$, qui est un idéal principal, donc de la forme $I_x = \pi_{f,x}\mathbb{K}[X]$, avec $\pi_{f,x} \in \mathbb{K}[X]$. Comme $\pi_f \in I_x$, $\pi_{f,x}$ est un diviseur π_f.
On écrit $\pi_f = \prod_{k=1}^{N} P_i^{\alpha_i}$ décomposition en facteurs irréductibles, où $N \in \mathbb{N}^*$, les P_i sont irréductibles unitaires et distincts deux à deux et enfin les $\alpha_i \in \mathbb{N}^*$. Un polynôme est un diviseur de π_f si et seulement si il s'écrit $\prod_{k=1}^{N} P_i^{\beta_i}$ avec pour tout $i \in [\![1, N]\!]$, $0 \leq \beta_i \leq \alpha_i$. Ainsi le nombre de diviseurs unitaires de π_f est $\prod_{k=1}^{N} (\alpha_i + 1)$.
Donc l'ensemble $\{\pi_{f,x}, \ x \in E\}$ est fini de cardinal noté r où $1 \leq r \leq \prod_{k=1}^{N} (\alpha_i + 1)$.
On peut donc choisir $y_1, \ldots y_r \in E$, tel que $\{\pi_{f,x}, \ x \in E\} = \{\pi_{f,y_i}, \ i \in [\![1, r]\!]\}$.
Ainsi $E = \bigcup_{x \in E} \ker(\pi_{f,x}(f)) = \bigcup_{i=1}^{r} \ker(\pi_{f,y_i}(f))$ (car $\forall x \in E, \ x \in \ker(\pi_{f,x}(f))$).
D'après la question 24, on trouve $k \in [\![1, r]\!]$ tel que $\ker(\pi_{f,y_k}(f)) = E$. Ainsi, si on note $x_1 = y_k$ et on a $\ker(\pi_{f,x_1}(f)) = E$ *i.e.* $\pi_{f,x_1}(f) = 0_{\mathcal{L}(E)}$. Finalement, $\pi_f | \pi_{f,x_1}$; comme $\pi_{f,x_1} | \pi_f$ et ce sont des polynômes unitaires, $\pi_{f,x_1} = \pi_f$.
Finalement, en reprenant l'argument classique (voir par exemple la question 19), comme π_{f,x_1} est de degré d, $(x_1, f(x_1), \ldots, f^{d-1}(x_1))$ est libre.

26. L'image de φ_{x_1} est $\{P(f)(x_1) / \ P \in \mathbb{K}[X]\}$ et est évidemment stable par f (car $XP \in \mathbb{K}[X]$ pour $P \in \mathbb{K}[X]$). Par ailleurs $\ker \varphi_{x_1} = \pi_{f,x_1} = \pi_f$ admet comme supplémentaire $\mathbb{K}_{d-1}[X]$ (par existence et unicité de la division euclidienne par π_f). Donc, φ_{x_1} réalise un isomorphisme de $\mathbb{K}_{d-1}[X]$ vers $\mathrm{Im}\varphi_{x_1}$. Ainsi, $E_1 = \{P(f)(x_1) / \ P \in \mathbb{K}_{d-1}[X]\} = \mathrm{Im}\varphi_{x_1} = \{P(f)(x_1) / \ P \in \mathbb{K}[X]\}$.

27. D'après ce qui précède $\mathcal{B} = (e_1, e_2, \ldots, e_d) = \left(\psi_1^k(x_1)\right)_{0 \leq k \leq d-1}$ est une base de E_1. Ainsi ψ_1 est cyclique.

28. Pour $i \in \mathbb{N}$, on note $F_i = \ker\left(\Phi \circ f^i\right)$; ainsi $F = \bigcap_{i \in \mathbb{N}} F_i$ est bien un sous-espace de E.
De plus, pour tout $i \geq 1$, si $x \in F_i$, $\Phi \circ f^{i-1}(f(x)) = \Phi \circ f^i(x) = 0$; ainsi $f(F_i) \subset F_{i-1}$. On a donc :

$$f(F) \subset f\left(\bigcap_{i \in \mathbb{N}^*} F_i\right) \subset \bigcap_{i \in \mathbb{N}^*} f(F_i) \subset \bigcap_{i \in \mathbb{N}^*} F_{i-1} = F.$$

Soit $y \in E_1 \cap F$. Comme $y \in E_1$, on peut l'écrire $y = \sum_{k=1}^{d} \lambda_k e_k$, avec $\lambda_1, \ldots, \lambda_d \in \mathbb{K}$. Par définition de Φ, $\Phi(x) = \lambda_d$; or $\Phi(f^0(x)) = 0$ car $y \in F$. On obtient donc $\lambda_d = 0$.
On suppose avoir montré $\lambda_d = \ldots \lambda_l = 0$, pour un certain $2 \leq l \leq d$.
Ainsi $y = \sum_{k=1}^{l-1} \lambda_k e_k = \sum_{k=1}^{l-1} \lambda_k f^{k-1}(x_1)$, et

$$f^{d-l+1}(y) = \sum_{k=1}^{l-1} \lambda_k f^{d-l+k}(x_1) = \sum_{k=1}^{l-1} \lambda_k e_{d-l+1+k}.$$

Comme $y \in F$,

$$0 = \Phi \circ f^{d-l+1}(y) = \lambda_{l-1}.$$

Finalement, on obtient, pour tout $i \in [\![1, d]\!]$ $\lambda_i = 0$, et $y = 0_E$. Ainsi $E_1 \cap F = \{0_E\}$.

29. Par linéarité de f et de Φ, Ψ est bien linéaire entre E vers $\mathbb{K}^d$.

Par définition de Ψ, $\ker \Psi = \bigcap_{k=0}^{d-1} \ker\left(\Phi \circ f^k\right)$. Or, en reprenant la démonstration de la question précédente, on n'a utilisé que des $\Phi \circ f^k$ avec $0 \leq k \leq d-1$; on a donc en fait montré que $\left(\bigcap_{k=0}^{d-1} \ker\left(\Phi \circ f^k\right)\right) \cap E_1 = \{0_E\}$, *i.e.* $\ker \Psi \cap E_1 = \{0_E\}$.

La restriction Ψ_1 de Ψ à E_1 est donc injective. Or $\dim(E_1) = d = \dim(\mathbb{K}^d)$, Ψ_1 réalise un isomorphisme entre E_1 et $\mathbb{K}^d$.

30. D'après la question précédente, Ψ est surjective de E vers $\mathbb{K}^d$ (puisqu'elle l'est de E_1 vers $\mathbb{K}^d$) ; et donc par théorème du rang, $\dim(E) - d = \dim\left(\ker(\Psi)\right)$.

Comme $\ker \Psi \cap E_1 = \{0_E\}$, $\ker(\Psi) \oplus E_1 \subset E$, et par égalité des dimensions, $E = E_1 \oplus \ker(\Psi)$.

Or $F \subset \bigcap_{k=0}^{d-1} \ker\left(\Phi \circ f^k\right) = \ker(\Psi)$.

Mais comme π_f est de degré d, $(f^k)_{0 \leq k \leq d-1}$ forme une base de $\mathbb{K}[f]$. Ainsi pour tout $i \geq d$, $f^i \in \mathrm{Vect}(f^k)_{0 \leq k \leq d-1}$, et donc $\Phi \circ f^i$ est combinaison linéaire des $\left(\Phi \circ f^k\right)_{0 \leq k \leq d-1}$. On a donc $\ker(\Psi) = \bigcap_{k=0}^{d-1} \ker\left(\Phi \circ f^k\right) \subset \ker(\Phi \circ f^i)$. Finalement $\ker \Psi \subset F$.

On a donc égalité $F = \ker \Psi$ et on conclut que $E = E_1 \oplus F$.

31. On conserve les notations ci-dessus. On a montré que ψ_1 est un endormorphisme cyclique et son polynôme minimal $\pi_{\psi_1} = \pi_{\psi_1, x_1} = \pi_{f, x_1} = \pi_f$. On note P_1 ce polynôme et $G_1 = F$.

Ainsi, $E_1 \oplus G_1 = E$, avec G_1 stable apr f. Et pour tout $x \in G_1$, $P_1(f)(x) = \pi_f(f)(x) = 0$.

Soit $k \geq 1$. On suppose avoir construit des sous espaces-vectoriels $E_1, \ldots, E_k$ et G_k tous stables par f, tels que

— $E = E_1 \oplus \cdots \oplus E_k \oplus G_k$
— pour tout $1 \leq i \leq k$, l'endomorphisme ψ_i induit par f sur le sous-espace vectoriel E_i est cyclique de polynôme minimal P_i
— pour tout $i \in [\![1, k-1]\!]$, P_{i+1} divise P_i
— $\forall x \in G_k,\ P_k(f)(x) = 0$.

Si $\dim G_k = 0$, on pose $r = k$ et on a bien le résultat souhaité ($r = 1$ si et seulement si f est cyclique et $E_1 = E$).

Sinon, on applique les questions 24 à 30 à l'endomorphisme f_k induit par f sur G_k. On note P_{k+1} le polynôme minimal de f_k. Il divise bien P_k, puisque $P_k(f_k) = O_{\mathcal{L}(G_k)}$.

On obtient alors E_{k+1} et G_{k+1} deux sous-espaces stables par f tels que $G_k = E_{k+1} \oplus G_{k+1}$, tels que l'endomorphisme ψ_{k+1} induit par f sur le sous-espace vectoriel E_{k+1} est cyclique de polynôme minimal P_{k+1} et tels que pour tout $x \in G_{k+1}$, $P_{k+1}(f)(x) = 0$. Ainsi,

— $E = E_1 \oplus \cdots \oplus E_{k+1} \oplus G_{k+1}$
— pour tout $1 \leq i \leq k+1$, l'endomorphisme ψ_i induit par f sur le sous-espace vectoriel E_i est cyclique de polynôme minimal P_i
— pour tout $i \in [\![1, k]\!]$, P_{i+1} divise P_i
— $\forall x \in G_{k+1},\ P_{k+1}(f)(x) = 0$.

On a ainsi la construction voulue au rang $k+1$.

Comme à chaque étape, le degré du polynôme minimal P_k est supérieur ou égal à 1, la dimension de E_k est supérieure ou égale à 1 ; ainsi la suite des dimensions des G_k est une suite strictement décroissante d'entiers. Au bout d'un nombre fini d'étapes, on obtient donc $\dim G_k = 0$ et on a alors $r = k$ et la décomposition souhaitée.

Remarque : On peut montrer l'unicité de la suite de polynômes $(P_1, \ldots, P_r)$ tels qu'il existe une décomposition de la forme obtenue ci-dessus. Ce sont des invariants de similitude de f.

(C) Commutant d'un endomorphisme quelconque

32. On reprend la décomposition de Frobenius de f obtenue ci-dessus (on conserve les mêmes notations).

Pour tout $k \in [\![1, r]\!]$, ψ_k est cyclique ; on a montré au **??** que son commutant $C(\psi_k) = \mathbb{K}[\psi_k]$; il s'agit donc d'un espace vectoriel de dimension $\deg(\pi_{\psi_k}) = \deg(P_k) = \dim(E_k)$.

On introduit Λ l'application linéaire qui à $(g_1, \ldots, g_r) \in \prod_{j=1}^{r} \mathcal{L}(E_j)$ associe g l'unique endomorphisme de E tel que pour tout $i \in [\![1, r]\!]$, pour tout $x \in E_i$, $g(x) = g_i(x)$. Comme $E = \bigoplus_{i=1}^{r} E_i$, Λ est bien définie, et elle est évidemment injective (puisque chaque g_i est alors l'application induite par g sur E_i).

Soit $g \in \Lambda\left(\prod_{j=1}^{r} C(\psi_j)\right)$. Ainsi pour tout $i \in [\![1, r]\!]$, g laisse stable E_i ; de plus sur E_i $g \circ f = f \circ g$. Comme $E = \bigoplus_{i=1}^{r} E_i$, on peut conclure que $g \in C(f)$. Ainsi,

$$\begin{aligned}\dim(C(f)) &\geq \Lambda\left(\prod_{j=1}^{r} C(\psi_j)\right) = \dim\left(\prod_{j=1}^{r} C(\psi_j)\right) \\ &= \sum_{j=1}^{r} \dim(C(\psi_j)) = \sum_{j=1}^{r} \dim(E_j) = n\end{aligned}$$

Ainsi la dimension de $C(f)$ est supérieure ou égale à n.

33. On note $d = \deg(\pi_f)$. Par le théorème de Cayley-Hamilton, $d = \deg(\pi_f) \leq= \deg(\chi_f) = n$.
On sait que $\dim(\mathbb{K}[f]) = d$ et on suppose que $\mathbb{K}[f] = C(f)$; donc $\dim C(f) = d \geq n$.
Comme on a montré $\dim(C(f)) = n$, on peut conclure que $d = n$. Donc avec les notations précédentes, on a $\dim(E_1) = d = n$. Donc $E_1 = E$ et $f = \psi_1$ est cyclique.