Calculatrices interdites. L'exercice et le problème sont indépendants.

Exercice

1) Soit u une suite à valeurs réelles strictement positives. Vérifions les axiomes des normes.
   - Pour tout $P = \sum_{k\in\mathbb{N}} a_k X^k$, $\boxed{N_u = \sum_{k\in\mathbb{N}} u_k|a_k| \geqslant 0}$.
   - Soit $P = \sum_{k\in\mathbb{N}} a_k X^k$, tel que $N_u(P) = 0$. La somme définissant $N_u(P)$ étant une somme de termes positifs, on obtient que pour tout entier naturel k, $u_k|a_k| = 0$. Comme de plus, $u_k \neq 0$, on en déduit que $a_k = 0$. Finalement, $\boxed{P = 0_E}$.
   - Soit $P = \sum_{k\in\mathbb{N}} a_k X^k$ et $\lambda \in \mathbb{R}$,
   $$N_u(\lambda P) = \sum_{k\in\mathbb{N}} u_k|\lambda a_k| = |\lambda| \sum_{k\in\mathbb{N}} u_k|a_k| = \boxed{|\lambda| N_u(P)}$$
   - Soit $P = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q = \sum_{k\in\mathbb{N}} b_k X^k$.
   Pour tout entier k, $u_k|a_k + b_k| \leqslant u_k|a_k| + u_k|b_k|$. En faisant la somme on obtient alors que $\boxed{N_u(P+Q) \leqslant N_u(P) + N_u(Q)}$.

   On a bien montré que N_u était une norme.
2) On procède par double implication
   - $\boxed{\Rightarrow}$ On suppose qu'il existe une constante $C \in \mathbb{R}_+^*$ telle que $N_u \leqslant CN_v$. Soit k un entier naturel, on sait que $N_u(X^k) = u_k$ et $N_v(X^k) = v_k$. On en déduit que $0 \leqslant u_k \leqslant Cv_k$. Cela montre que $\boxed{u_n = \underset{n\to+\infty}{O}(v_n)}$.
   - $\boxed{\Leftarrow}$ On suppose que $u_n = \underset{n\to+\infty}{O}(v_n)$. Il existe donc $C \in \mathbb{R}_+^*$ tel que pour tout entier n, $\left|\frac{u_n}{v_n}\right| \leqslant C$ et donc $u_n \leqslant Cv_n$ car u et v sont à valeurs positives.
   Soit $P = \sum_{k\in\mathbb{N}} a_k X^k$ on a alors
   $$N_u(P) = \sum_{k\in\mathbb{N}} u_k|a_k| \leqslant \sum_{k\in\mathbb{N}} Cv_k|a_k| = CN_v(P)$$
   C'est-à-dire $\boxed{N_u \leqslant CN_v}$.

   On en déduit que N_u et N_v sont équivalentes si et seulement si $u_n = \underset{n\to+\infty}{O}(v_n)$ et $v_n = \underset{n\to+\infty}{O}(u_n)$.
3) a) $P = \sum_{k\in\mathbb{N}} a_k X^k$. Soit $t \in [0,1]$,
   $$|P(t)| = \left|\sum_{k\in\mathbb{N}} a_k\right| \leqslant |\sum_{k\in\mathbb{N}} |a_k| = N_{\underline{1}}(P)$$
   On en déduit que $N(P) = \sup_{t\in[0,1]} |P(t)| \leqslant N_{\underline{1}}(P)$.

   On peut donc poser $\boxed{K = 1}$.

   b) Montrons que les normes N et $N_{\underline{1}}$ ne sont pas équivalentes. Pour cela nous allons montrer qu'il n'existe pas de constante $C \in \mathbb{R}_+^*$ telle que $N_{\underline{1}} \leqslant CN$. Il suffit pour ce faire d'exhiber une suite (P_n) telle que $\frac{N_{\underline{1}}(P_n)}{N(P_n)}$.

Posons $P_n = (X-1)^n$.
Pour $t \in [0,1]$, $|t-1| \in [0,1]$ et donc $|P_n(t)| = |(t-1)|^n \in [0,1]$. De plus, $|P_n(0)| = 1$ donc $N(P_n) = 1$.
Maintenant, par la formule du binôme de Newton,

$$P_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} X^k$$

Cela nous donne

$$N_{\underline{1}}(P_n) = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Finalement, $\frac{N_{\underline{1}}(P_n)}{N(P_n)} = 2^n \underset{n\to+\infty}{\longrightarrow} +\infty$. Les normes N et $N_{\underline{1}}$ ne sont pas équivalentes.

4) a) On utilise les formules d'interpolation de Lagrange. Comme $a_1, \ldots, a_{d+1}$ sont deux à deux distincts, on sait qu'il existe des polynômes $L_1, \ldots, L_{d+1}$ tels que pour tout $(i,j) \in [\![1, d+1]\!]^2$, $L_i(a_j) = \delta_{ij}$. Précisément pour tout $i \in [\![1, d+1]\!]$,

$$L_i = \frac{\prod_{j\neq i}(X - a_j)}{\prod_{j\neq i}(a_i - a_j)}$$

Soit $P \in \mathbb{R}_d[X]$. Considérons Q le polynôme de $\mathbb{R}_d[X]$ défini par $Q = \sum\limits_{i=1}^{d+1} P(a_i) L_i$. Par construction, pour tout $i \in [\![1, d+1]\!]$, $Q(a_i) = P(a_i)$; les polynômes P et Q qui sont de degré au plus d coïncident sur $d+1$ points deux à deux distincts, ils sont donc égaux.

b) On a vu à la question 3.a) que pour tout $P \in \mathbb{R}[X]$, $N(P) \leqslant N_{\underline{1}}(P)$. La propriété est donc aussi vraie sur $\mathbb{R}_d[X]$.
En utilisant ce qui précède,

$$\begin{aligned} N_{\underline{1}}(P) &= N_{\underline{1}}\Big(\sum_{i=1}^{d+1} P(a_i) L_i\Big) \\ &\leqslant \sum_{i=1}^{d+1} |P(a_i)| N_{\underline{1}}(L_i) \\ &\leqslant \left(\sum_{i=1}^{d+1} N_{\underline{1}}(L_i)\right) N(P) \end{aligned}$$

On peut alors poser $K = \left(\sum\limits_{i=1}^{d+1} N_{\underline{1}}(L_i)\right)$ qui est une constante qui ne dépend pas de P. On a bien $\boxed{N_{\underline{1}} \leqslant KN}$; les deux normes sont équivalentes.

Problème

I. Matrices compagnons et endomorphismes cycliques

1) On a $\chi_M = \det(XI_n - M) = \det\left((XI_n - M)^T\right) = \det(XI_n - M^T) = \chi_{M^T}$ donc

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

Ainsi $\mathrm{sp}(M) = \mathrm{sp}\left(M^T\right)$ et donc $\boxed{M \text{ et } M^T \text{ ont même spectre}}$

2) Procédons par double implication
— $\boxed{\Leftarrow}$ On suppose que M est diagonalisable. ce qui nous fournit $P \in GL_n(\mathbb{K})$ et $D \in \mathscr{M}_n(\mathbb{K})$ diagonale telles que $M = PDP^{-1}$
donc $M^T = (P^{-1})^T D^T P^T = \left(P^T\right)^{-1} DP^T$
d'où M^T est diagonalisable
— $\boxed{\Rightarrow}$ On suppose que M^T est diagonalisable.
Pour montrer que M est diagonalisable, on utilise l'implication précédente en remarquant que $M = \left(M^T\right)^T$.

On a bien montré que $\boxed{M^T \text{ est diagonalisable si et seulement si } M \text{ est diagonalisable}}$

Remarque : On peut aussi remarquer que les polynômes annulateurs de M sont les polynômes annulateurs de M^T. Cela implique que $\pi_M = \pi_{M^T}$ et donc

$$\begin{aligned} M \text{ diagonalisable} &\iff \pi_M \text{ scindé à racines simples} \\ &\iff \pi_{M^T} \text{ scindé à racines simples} \\ &\iff M^T \text{ diagonalisable} \end{aligned}$$

I.B. Matrices compagnons

3) Montrons par récurrence sur $n \in \mathbb{N}^*$ pour montrer que $\chi_{C_Q} = Q$.
— $\boxed{\mathrm{I}}$: Pour $n = 1$, on a $C_Q = (-a_0)$ donc $\chi_{C_Q} = |X + a_0| = X + a_0 = Q$.
— $\boxed{\mathrm{C}}$: Soit $n \geqslant 2$, on suppose la propriété $n-1$ et on la montre n. On a

$$\chi_{C_Q} = \begin{vmatrix} X & \cdots & \cdots & 0 & a_0 \\ -1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & X & a_{n-2} \\ 0 & \cdots & 0 & -1 & X + a_{n-1} \end{vmatrix}$$

En développant selon la première ligne on obtient alors

$$\chi_{C_Q} = X \begin{vmatrix} X & \cdots & \cdots & 0 & a_1 \\ -1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & X & a_{n-2} \\ 0 & \cdots & 0 & -1 & X + a_{n-1} \end{vmatrix} + (-1)^{n+1} a_0 \begin{vmatrix} -1 & * & \cdots & \cdots & * \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & * \\ 0 & \cdots & \cdots & 0 & -1 \end{vmatrix}$$

En utilisant l'hypothèse de récurrence pour calculer le premier terme on a donc

$$\chi_{C_Q} = X(X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_2 X + a_1) + (-1)^{n+1} a_0 (-1)^{n-1} = Q$$

— $\boxed{\text{C}}$: La propriété est vraie pour tout entier $n \in \mathbb{N}^*$.

Remarque : On peut aussi faire une démonstration directe (sans récurrence) en développant selon la dernière colonne.

4) On a $(C_Q)^T = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & & 0 & 1 \\ -a_0 & -a_1 & \dots & & -a_{n-1} \end{pmatrix}$.

Comme $\chi_{{C_Q}^T} = \chi_{C_Q} = Q$, les valeurs propres de $(C_Q)^T$ sont les racines de Q.

Soit $\lambda \in \mathbb{K}$ tel que $Q(\lambda) = 0$; déterminons l'espace propre $E_\lambda(C_Q^T)$.

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

$$C_Q{}^T X = \lambda X \iff \left\{ \begin{array}{rcl} x_2 & = & \lambda x_1 \\ x_3 & = & \lambda x_2 \\ & \vdots & \\ x_n & = & \lambda x_{n-1} \\ -a_0 x_1 - \cdots - a_{n-1} x_n & = & \lambda x_n \end{array} \right.$$

Donc

$$C_Q{}^T X = \lambda X \iff \left\{ \begin{array}{rcl} x_2 & = & \lambda x_1 \\ x_3 & = & \lambda^2 x_1 \\ & \vdots & \\ x_n & = & \lambda^{n-1} x_1 \\ (-a_0 - a_1\lambda - \cdots - a_{n-1}\lambda^{n-1}) x_1 & = & \lambda^n x_1 \end{array} \right.$$

FInalement

$$C_Q{}^T X = \lambda X \iff \left\{ \begin{array}{l} \forall i \in [\![2; n]\!],\ x_i = \lambda^{i-1} x_1 \\ Q(\lambda) x_1 = 0 \end{array} \right.$$

Comme $Q(\lambda) = 0$; $\boxed{\dim\left(E_\lambda\left(C_Q{}^T\right)\right) = 1,\ E_\lambda\left(C_Q{}^T\right) = \text{vect}(X_\lambda) \text{ où } X_\lambda = \begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}}$

I.C. Endomorphismes cycliques

5) On procède par double implication

— $\boxed{\Rightarrow}$ On suppose que f est cyclique.
Ceci nous fournit $x_0 \in E$ tel que $\mathscr{B} = (x_0, f(x_0), \dots, f^{n-1}(x_0))$ soit une base de E
Il existe alors $(\lambda_0, \lambda_1, \dots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $f^n(x_0) = \sum\limits_{i=0}^{n-1} \lambda_i f^i(x_0)$
On peut poser $Q = X^n + \sum\limits_{i=0}^{n-1} (-\lambda_i) X^i \in \mathbb{K}[X]$ de sorte que Q est unitaire de degré n et $\mathsf{Mat}_{\mathscr{B}}(f) = C_Q$

— $\boxed{\Leftarrow}$ On suppose qu'il existe une base $\mathscr{B} = (e_0, e_1, \dots e_{n-1})$ de E dans laquelle la matrice de f est de la forme C_Q, où Q est un polynôme unitaire de degré n
Ainsi $\forall i \in [\![0; n-2]\!],\ f(e_i) = e_{i+1}$ donc $(e_0, f(e_0), f^2(e_0), \dots, f^{n-1}(e_0))$ est une base de E et donc f est cyclique

6) On suppose f cyclique. On procède par double implication.

— $\boxed{\Rightarrow}$ On suppose que f est diagonalisable. On en déduit que χ_f est scindé sur $\mathbb{K}$.
D'après la question précédente, il existe une base $\mathscr{B}$ telle que la matrice de f dans la base $\mathscr{B}$ soit de la forme C_Q (où Q est le polynôme caractéristique de f d'après ce qui précède).
La matrice C_Q est donc diagonalisable, ainsi que C_Q^T d'après la question 2).
Comme on sait que les espaces propres de C_Q^T sont de dimension 1 d'après la question 4), cela implique que C_Q^T a n valeurs propres distinctes. Donc $\chi_{C_Q^T} = \chi_{C_Q} = \chi_f$ a toutes ses racines simples.

— $\boxed{\Leftarrow}$ Si χ_f est scindé et a toutes ses racines simples, le nombres de racines de χ_f est égal à n la dimension de E. Cela implique que f a n valeurs propres, il est donc diagonalisable.

7) On suppose que f est cyclique.
Soit $(\lambda_0, \dots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $\sum\limits_{i=0}^{n} \lambda_i f^i = 0_{\mathscr{L}(E)}$.
Comme f est cyclique, il existe $x_0 \in E$ tel que $\mathscr{B} = (x_0, f(x_0), \dots, f^{n-1}(x_0))$ soit une base de E (c'est donc en particulier une famille libre).
Or $\sum\limits_{i=0}^{n} \lambda_i f^i(x) = 0_{\mathscr{L}(E)}(x) = 0_E$ donc $\lambda_0 = \dots = \lambda_{n-1} = 0$.
Alors $\boxed{(\mathrm{Id}, f, f^2, \dots, f^{n-1}) \text{ est libre dans } \mathscr{L}(E)}$.
Notons d le degré de π_f. Comme $(\mathrm{Id}, f, f^2, \dots, f^{n-1})$ est libre $\mathscr{L}(E)$, $d \geqslant n$.
De plus d'après le théorème de Cayley-Hamilton, χ_f est annulateur de f d'où $\pi_f \mid \chi_f$ or ce sont des polynômes non nuls donc

$$d = \deg(\pi_f) \leqslant \deg(\chi_f) = n$$

Finalement $n = d$ d'où $\boxed{\text{le polynôme minimal de } f \text{ est de degré } n}$

Remarque : On s'est autorisé ici à utiliser le théorème de Cayley-Hamilton car cette question ne sert pas dans la preuve donnée plus bas de ce théorème.

I.D. Application à une démonstration du théorème de Cayley-Hamilton

8) On note $N_x = \{m \in \mathbb{N}^* \ ; \ (f^i(x))_{0 \leqslant i \leqslant m-1} \text{ libre}\}$.
On sait que $1 \in N_x$ car $x \neq 0_E$ et que $\forall m \geqslant n,\ m \notin N_x$ car $\dim E = n$
Ainsi N_x est une partie de $\mathbb{N}^*$ non vide majorée par $n-1$ donc elle admet un plus grand élément que l'on note $p \in \mathbb{N}^*$.
Ainsi la famille $(f^i(x))_{0 \leqslant i \leqslant p-1}$ est libre et la famille $(f^i(x))_{0 \leqslant i \leqslant p}$ est liée. Il existe de ce fait $(\lambda_0, \dots, \lambda_p) \in \mathbb{K}^{p+1} \setminus \{(0, \dots, 0\}$ tels que

$$\lambda_0 x + \lambda_1 f(x) + \dots + \lambda_p f^p(x) = 0_E$$

De plus, $\lambda_p \neq 0$ car sinon cela contredit la liberté de la famille $(f^i(x))_{0 \leqslant i \leqslant p-1}$. Il suffit de poser pour tout $i \in [\![0, p-1]\!]$, $\alpha_i = \frac{\lambda_i}{\lambda_p}$.

9) Posons, $F = \mathrm{Vect}(x, f(x), f^2(x), \dots, f^{p-1}(x))$.
Soit $i \in [\![0, p-2]\!]$, $f(f^i(x)) = f^{i+1}(x) \in F$. D'autre part,

$$f(f^{p-1}(x)) = f^p(x) = -\alpha_0 x - \dots - \alpha_{p-1} f^{p-1}(x) \in F$$

Par linéarité, $\boxed{F \text{ est stable par } f}$.

10) Notons $\check{f}$ l'endomorphisme induit par f sur F. Notons qu'avec les notations précédentes, la famille $\mathscr{B} = (x, , f(x), f^2(x), \dots, f^{p-1}(x))$ est une base de F puisqu'elle l'engendre par définition de F et qu'elle est libre par définition de p. Cela montre que $\check{f}$ est un endomorphisme cyclique de F. Précisément, si on note $Q = X^p + \alpha_{p-1}X^{p-1} + \cdots + \alpha_0$, la matrice de $\check{f}$ dans la base $\mathscr{B}$ est C_Q ce qui implique en particulier que $\chi_{\check{f}} = Q$.
On sait alors que $\chi_{\check{f}}$ divise χ_f et donc Q divise χ_f.

11) On commence par remarquer que si $x = 0_E$, $\chi_f(f)(x) = 0_E$.
Maintenant, si $x \neq 0_E$, on peut appliquer les résultats des questions 8, 9 et 10 pour le vecteur x. On obtient (en reprenant les notations de ces questions) que $\chi_{\check{f}}$ divise χ_f. On peut donc trouver un polynôme R tel que $\chi_f = R \times \chi_{\check{f}}$. En particulier,

$$\chi_f(f)(x) = (R \times \chi_{\check{f}})(f)(x) = R(f)\left(\chi_{\check{f}}(f)(x)\right)$$

Or, par définition (toujours en reprenant les notations des questions précédentes),

$$\chi_{\check{f}}(f)(x) = f^p(x) + \alpha_{p-1}f^{p-1}(x) + \cdots + \alpha_1 f(x) + \alpha_0 x = 0_E$$

Finalement,

$$\chi_f(f)(x) = R(f)(0_E) = 0_E$$

Cela montre que $\boxed{\chi_f(f) = 0_{\mathscr{L}(E)}}$.

II. Endomorphismes commutants, décomposition de Frobenius

12) $C(f)$ est une $\boxed{\text{sous-algèbre}}$ de $\mathscr{L}(E)$ car :
- $C(f)$ est un sous-espace vectoriel de $\mathscr{L}(E)$ comme noyau de l'endomorphisme $g \mapsto f\circ g - g\circ f$ de $\mathscr{L}(E)$.
- $C(f)$ contient id_E
- pour tous $g, h \in C(f)$, $f \circ g \circ h = g \circ f \circ h = g \circ h \circ f$ donc $g \circ h \in C(f)$.

II.A. Commutant d'un endomorphisme cyclique

On suppose que f est cyclique et on choisit un vecteur x_0 dans E tel que $(x_0, f(x_0), \dots, f^{n-1}(x_0))$ est une base de E.

Soit $g \in C(f)$, un endomorphisme qui commute avec f.

13) Il existe $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ de $\mathbb{K}$ tels que

$$\boxed{g(x_0) = \sum_{k=0}^{n-1} \lambda_k f^k(x_0)}$$

car $g(x_0) \in E$ et car $(x_0, \dots f^{n-1}(x_0))$ engendre E.

14) Soit $h = \sum_{k=0}^{n-1} \lambda_k f^k$.
Par hypothèse, g et h coïncident en x_0. De plus h commute avec f car c'est un polynôme en f, et g commute avec f par hypothèse. Par récurrence immédiate, g et h commutent avec toutes les puissances de f.
Pour tout $k \in \mathbb{N}$,

$$g(f^k(x_0)) = f^k(g(x_0) = f^k(h(x_0)) = h(f^k(x_0))$$

Donc g et h coïncident sur la famille $(x_0, \dots, f^{n-1}(x_0))$. Cette famille engendrant E et g et h étant linéaires, elles coïncident sur E.

Ainsi $\boxed{g = h \in \mathbb{K}[f]}$.

15) Par la question précédente, pour tout $g \in C(f)$ il existe un polynôme $R \in \mathbb{K}_{n-1}[X]$ tel que $g = R(f)$. La réciproque est évidente car tout polynôme en f commute avec f.

III.B. Décomposition de Frobenius

On note d le degré de π_f.

16) Soit $x \in E$. On note $I_{f,x} = \{P \in \mathbb{K}[X] / \; P(f)(x) = 0\}$.

a) $I_{f,x}$ est un sous-espace vectoriel de $\mathbb{K}[X]$ comme noyau de l'application linéaire $P \mapsto P(f)(x)$.

De plus pour tout $P \in \mathbb{K}[X]$ et tout $Q \in I_{f,x}$,

$$(PQ)(f)(x) = [P(f) \circ Q(f)](x) = P(f)(0_E) = 0_E$$

donc $PQ \in I_{f,x}$.

Ainsi $I_{f,x}$ est un $\boxed{\text{idéal}}$ de $\mathbb{K}[X]$, donc il existe un unique polynôme unitaire ou nul $\pi_{f,x}$ tel que $\boxed{I_{f,x} = \pi_{f,x}\mathbb{K}[X]}$.

$\pi_{f,x}$ divise π_f car π_f appartient à $I_{f,x}$ car $\pi(f)(x) = 0_{\mathscr{L}(E)}(x) = 0_E$.

Comme π_f n'est pas nul, $\pi_{f,x}$ ne l'est pas non plus. Donc il est $\boxed{\text{unitaire}}$.

b) Si $(x, f(x), \dots, f^{d_x-1}(x))$ était liée, il existerait des scalaires non tous nuls $\lambda_0, \dots, \lambda_{d_x-1} \in \mathbb{K}$ tels que $\lambda_0 x_0 + \ldots + \lambda_{d_x-1} f^{d_x-1}(x_0) = 0_E$ et donc le polynôme $P = \lambda_0 + \lambda_1 X + \ldots + \lambda_{d_x-1} X^{d_x-1}$ serait un polynôme non nul mais de degré au plus $d_x - 1$ appartenant à $I_{f,x}$ donc multiple de $\pi_{f,x}$, ce qui est impossible.

Donc $\boxed{(x, f(x), \dots, f^{d_x-1}(x)) \text{ est libre}}$.

17) a) On raisonne par l'absurde.

Soient $F_1, \dots, F_r$ des sous-espaces vectoriels de E tels qu'aucun des sous-espaces F_i ne contienne tous les autres.

Donc $r \geqslant 2$.

Posons $G = F_1 \cup \ldots \cup F_r$ et supposons que G est un sev de E.

Comme $F_2 \cup \ldots \cup F_r$ n'est pas inclus dans F_1, il existe x dans $F_2 \cup \ldots \cup F_r$ tel que $x \notin F_1$. On a donc $x \in G \setminus F_1$.

Supposons que $F_1 \not\subset F_2 \cup \ldots \cup F_r$. Il existe alors $y \in F_1 \setminus (F_2 \cup F_r)$. Pour tout $\lambda \in \mathbb{K}$, $x + \lambda y$ appartient à G car G est stable par combinaison linéaire, et $x + \lambda y$ n'appartient pas à F_1 car sinon $x = (x + \lambda y) - \lambda y$ appartiendrait à F_1 comme combinaison linéaire d'éléments de F_1.

Donc pour tout $\lambda \in \mathbb{K}$, il existe $i_\lambda \in [\![2, r]\!]$ tel que $x + \lambda y \in F_{i_\lambda}$.

Comme $\mathbb{K}$ est infini et $[\![2, r]\!]$ est fini, il existe deux scalaires distincts λ et μ tels que $i_\lambda = i_\mu$.

$F_{i_\lambda} \ni (x + \lambda y) - (x + \mu y) = (\lambda - \mu) y$, donc $y = \frac{1}{\lambda - \mu}(\lambda - \mu) y \in F_{i_\lambda}$, ce qui est contradictoire.

Donc $F_1 \subset F_2 \cup \ldots \cup F_r$, et ainsi $G = F_2 \cup \ldots \cup F_r$. De plus aucun des sous-espaces $F_2, \dots, F_r$ ne contient tous les autres car un tel sous-espace serait égal à G donc contiendrait également F_1.

En réitérant le raisonnement, on prouve successivement que $G = F_3 \cup \ldots \cup F_r$, etc... jusqu'à $G = F_r$, et ainsi F_r contient $F_1 \dots, F_{r-1}$, ce qui est contradictoire.

Donc $\boxed{G \text{ n'est pas un sev de } E \text{ lorsqu'aucun des } F_i \text{ ne contient tous les autres}}$.

b) L'ensemble des diviseurs unitaires de π_f est fini (notant $P_1, \ldots, P_k$) les diviseurs irréductibles de π_f et $m_1, \ldots, m_k$ leurs multiplicités dans π_f, les diviseurs unitaires irréductibles de π_f sont les polynômes de la forme $P_1^{\alpha_1} \ldots P_k^{\alpha_k}$ avec $(\alpha_1, \ldots, \alpha_k) \in [\![0, m_1]\!] \times \ldots \times [\![0, m_k]\!]$).
Donc l'ensemble A=$\{\pi_{f,x}, x \in E\}$ est fini comme sous-ensemble d'un ensemble fini. Notons-le $\{Q_1, \ldots, Q_p\}$. Pour tout $x \in E$, il existe $Q \in A$ tel que $\pi_{f,x} = Q$, et on a $Q(f)(x) = \pi_{f,x}(f)(x) = 0_E$.
Donc $E = \cup_{Q \in A} \ker Q(f)$. Comme A est fini, il existe $Q \in A$ tel que $E = \ker Q(f)$. Or il existe $x_1 \in E$ tel que $Q = \pi_{f,x_1}$.
On a ainsi $E = \ker \pi_{f,x_1}(f)$ donc $\pi_{f,x_1}(f) = 0_{\mathscr{L}}$ et ainsi π_f divise π_{f,x_1}.
Comme par ailleurs π_{f,x_1} divise π_f ces deux polynômes sont associés (et même égaux car unitaires). Donc $\boxed{d_{x_1} = d}$.

On considère un élément x_1 de E tel que $d_{x_1} = d_x$.
On pose $e_1 = x_1$, $e_2 = f(x_1)$, $\ldots$, $e_d = f^{d-1}(x_1)$ et $E_1 = \text{Vect}(e_1, e_2, \ldots, e_d)$.

18) $E_1 \subset \{P(f)(x_1) /\ P \in \mathbb{K}[X]\}$. Réciproquement, pour tout $P \in \mathbb{K}[X]$, notant Q et R le quotient et le reste de la division euclidienne de P par π_f, comme $Q\pi_f$ annule f, on a :

$$P(f)(x_1) = (0_{\mathscr{L}(E)} + R(f))(x_1) = R(f)(x_1) \in E_1$$

car R est de degré au plus $d - 1$.
Ainsi $f(E_1) = \{(XP)(f)(e_1),\ P \in \mathbb{K}[X]\} \subset \{S(f)(e_1),\ S \in \mathbb{K}[X]\} = E_1$.
Donc $\boxed{E_1 \text{ est stable par } f}$.

On note ψ_1 l'endomorphisme induit par f sur le sous-espace vectoriel E_1,

$$\psi_1\ :\ \begin{cases} E_1 \to E_1 \\ x \mapsto f(x) \end{cases}$$

19) $E_1 = Vect(x_1, f(x_1), \ldots, f^{d-1}(x_1)) = Vect(x_1, \psi_1(x_1), \ldots, \psi_1^{d-1}(x_1))$.
De plus $(x_1, \psi_1(x_1), \ldots, \psi_1^{d-1}(x_1))$ est libre par la question 16)b) et car $d_{x_1} = d$. C'est donc une base de E_1. Donc $\boxed{\psi_1 \text{ est cyclique}}$.
Si $d = n$ alors comme $(x_1, f(x_1), \ldots, f^{d-1}(x_1))$ est libre de longueur n, c'est une base de E, donc $f = \psi_1$ donc f est $\boxed{\text{cyclique}}$.

On complète, si nécessaire, $(e_1, e_2, \ldots, e_d)$ en une base $(e_1, e_2, \ldots, e_n)$ de E. Soit Φ la d-ième forme coordonnée qui à tout vecteur x de E associe sa coordonnée suivant e_d. On note $F = \{x \in E /\ \forall i \in \mathbb{N},\ \Phi(f^i(x)) = 0\}$.

20) Soit $x \in F$. Pour tout $i \in \mathbb{N}$. $\Phi(f^i(f(x))) = \Phi(f^{i+1}(x) = 0$.
Donc $f(x) \in F$.
Ainsi $\boxed{F \text{ est stable par } f}$.
Soit $x \in E_1 \cap F$. Comme $x \in F$, il existe $\lambda_1, \ldots, \lambda_d \in \mathbb{K}$ tels que

$$x = \lambda_1 x_1 + \ldots + \lambda_d f^{d-1}(x_1)$$

Comme $x \in F$, on a $0 = \Phi(x) = \lambda_d$, puis $0 = \Phi(f(x) = \lambda_{d-1}$, etc... jusqu'à $0 = \Phi(f^{d-1}(x) = \lambda_1$.
Donc $x = 0_E$.
Ainsi $\boxed{E_1 \text{ et } F \text{ sont en somme directe}}$.

Soit Ψ l'application linéaire de E dans $\mathbb{K}^d$ définie, pour tout $x \in E$, par

$$\Psi(x) = (\Phi(f^i(x)))_{0 \leqslant i \leqslant d-1} = (\Phi(x), \Phi(f(x)), \ldots, \Phi(f^{d-1}(x)))$$

21) Soit Ψ_1 la restriction de Ψ à E_1.
$\ker \Psi_1 = E_1 \cap \ker \Psi \subset E_1 \cap F = \{0_E\}$ donc Ψ_1 est injective.
De plus E_1 et $\mathbb{K}^d$ ont même dimension d.
Donc $\boxed{\Psi_1 \text{ est un isomorphisme}}$.

22) Montrer que $E = E_1 \oplus F$. Soit x dans E. Posons $y = \Psi_1^{-1}(\Psi(x))$. Alors y appartient à E_1 et

$$\Psi(y) = \Psi_1(y) = \Psi(x)$$

donc $\Psi(x-y) = 0_{\mathbb{K}^d}$.
Posons $z = x - y$. Montrons que $z \in F$.
Soit $i \in \mathbb{N}$. Montrons que $\Phi(f^i(z)) = 0$.
Notons R le reste de la division euclidienne de X^i par π_f. Alors $f^i = R(f)$ donc

$$f^i(z) \in Vect(z, f(z), \ldots, f^{d-1}(z))$$

et ainsi

$$\Phi(f^i(z)) \in Vect(\Phi(z), \Phi(f(z)), \ldots, \Phi(f^{d-1}(z))) = Vect(0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}}) = 0_K$$

Ainsi $z \in F$ donc $x = y + z \in E_1 + F$.
Donc $E = E_1 + F$. Comme E_1 et F sont en somme directe,

$$\boxed{E = E_1 \oplus F}$$

23) On procède par récurrence forte sur la dimension de E.
Le résultat est trivial si E est de dimension 1 car pour x vecteur non nul de E, (x) engendre E.
Soit $n \geqslant 2$. Supposons le résultat à démontrer vrai en dimension $1, 2, \ldots, n-1$. Soit E un $\mathbb{K}$-espace vectoriel de dimension n et f un endomorphisme de E.
Soient E_1 et F comme dans les questions précédentes.
Si $F = \{0_E\}$ alors $E = E_1$ donc f est cyclique.
Sinon, notant $\check{f}$ l'endomorphisme de F induit par f, on sait par hypothèse de récurrence que F s'écrit $E_2 \oplus \ldots \oplus E_r$ avec ....
De plus, $\pi_{\check{f}} = ppcm(\pi_{\psi_2}, \ldots, \pi_{\psi_r}) = \pi_{\psi_2}$.
Enfin, $\pi_{psi_1} = \pi_f = ppcm(\pi_{\psi_1}, \pi_{\check{f}}) = ppcm(\pi_{\psi_1}, \pi_{\psi_2})$ donc π_{ψ_2} divise π_{ψ_1}.
On a donc $E = E_1 \oplus E_2 \ldots \oplus E_r$ et $\pi_{\psi_r} | \pi_{\psi_{r-1}} | \ldots | \pi_{\psi_2} | \pi_{\psi_1}$.
Donc la propriété à démontrer est vraie en dimension n.
$\boxed{\text{Par récurrence forte, elle est vraie en toute dimension non nulle}}$.

III.C. Commutant d'un endomorphisme quelconque

24) D'après la question 15), si f est un endorphisme cyclique d'un espace de dimension n alors $C(f) = \mathbb{K}_{n-1}(f)$ et d'après la question 7), $\mathbb{K}_{n-1}(f)$ est de dimension n.
Soit f un endomorphisme quelconque d'un espace E de dimension n.
Reprenons les notations de la question 23).
L'application de $C(\psi_1) \times C(\psi_2) \times \ldots C(\psi_r)$ qui à $(g_1, \ldots, g_r)$ associe l'unique endomorphisme de E qui stabilise $E_1, \ldots, E_r$ et qui induit sur ces sous-espaces les endomorphismes $g_1, \ldots, g_r$ est linéaire injective et à valeurs dans $C(f)$.
Donc $\boxed{\dim C(f) \geqslant} \dim(C(\psi_1) \times C(\psi_2) \times \ldots C(\psi_r) = \dim C(\psi_1) + \ldots + \dim C(\psi_r) = \dim E_1 + \ldots + \dim E_r = \boxed{n}$.

25) Soit f est un endomorphisme non cyclique. Alors, dans les notations de la question 23), on a $r \geqslant 2$ car sinon $d = n$ donc par la question 19), f est cyclique.

Dans les notations précédentes, soit g un endomorphisme de E stabilisant $E_1, E_2, \ldots, E_r$ et induisant sur E_1 l'endomorphisme nul g_1 et sur $E_2, \ldots, E_r$ des éléments non nul $g_2, \ldots, g_r$ de $C(\psi_2), \ldots, C(\psi_r)$, par exemple $g_2 = id_{E_2}, \ldots, g_r = id_{E_r}$.

Si g s'écrivait $P(f)$ pour un certain polynôme P, alors P serait divisible par $\pi_{\psi_1} = \pi_f$, mais pas par π_{ψ_2}, ce qui est absurde car π_{ψ_2} divise π_{ψ_1}.

Ainsi $C(f)$ n'est pas inclus dans $\mathbb{K}[f]$.

Par contraposée, $\boxed{\text{si } C(f) = K[f] \text{ alors } f \text{ est cyclique}}$.