Corrigé majoritairement dû Édouard Lucas (Lycée Michelet, Vanves) pour la partie Centrale.
Les parties II.B et IV n'étaient pas dans le sujet Centrale, mais sont tirées d'un sujet ENTPE 1996.
La partie IV du sujet initial Centrale utilisait la théorie des espaces euclidiens.

I. Matrices compagnons et endomorphismes cycliques

I.A.

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

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

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

2. $\underline{\Leftarrow :}$ On suppose que M est diagonalisable. ce qui nous fournit $P \in GL_n(\mathbb{K})$ et $D \in \mathcal{M}_n(\mathbb{K})$ diagonale telles que $M = PDP^{-1}$
donc $M^\top = \left(P^{-1}\right)^\top D^\top P^\top = \left(P^\top\right)^{-1} DP^\top$
d'où $M^\top$ est diagonalisable
$\underline{\Rightarrow :}$ On suppose que $M^\top$ est diagonalisable.
Pour montrer que M est diagonalisable, on utilise l'implication précédente en remarquant que $M = \left(M^\top\right)^\top$.
On a bien montré que $\boxed{M^\top \text{ est diagonalisable si et seulement si } M \text{ est diagonalisable}}$

I.B. Matrices compagnons

3. On montre que $\chi_{C_Q} = Q$ par récurrence sur $\deg(Q) = n \geqslant 2$

Initialisation : On suppose que $\deg(Q) = 2$ ainsi $Q = X^2 + a_1X + a_0$ et $C_Q = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$

On a $\chi_{C_Q} = X^2 - \mathrm{tr}(C_Q)X + \det(C_Q) = X^2 + a_1X + a_0$ ce qui prouve l'initialisation

Hérédité : Soit l'entier $n \geqslant 2$. On suppose la propriété vraie pour tout polynôme unitaire de degré n.
On considère $Q(X) = X^{n+1} + a_nX^n + \cdots + a_0$ où les $a_i \in \mathbb{K}$. On a en développant par rapport à la première ligne :

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

Je note $R = X^n + a_nX^{-1} + \cdots + a_1$ et on a $\chi_{C_Q} = X\chi_{C_R} + a_0(-1)^{2n+2}$
Par hypothèse, on a $\chi_{C_R} = R$ donc $\chi_{C_Q} = XR + a_0 = Q$

Conclusion : On a montré par récurrence que la propriété était vraie pour tout polynôme unitaire de degré $\geqslant 2$
En particulier $\boxed{Q \text{ est le polynôme caractéristique de } C_Q}$

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

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

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

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

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

Notez bien que le "ainsi" concerne toute l'équivalence !

Comme λ est racine de Q, alors $\boxed{\dim\left(E_\lambda\left({C_Q}^{\top}\right)\right) = 1,\ E_\lambda\left({C_Q}^{\top}\right) = \mathrm{vect}(X_\lambda) \text{ où } X_\lambda = \begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}}$

I.C. Endomorphismes cycliques

5. **$\Rightarrow$:** On suppose que f est cyclique.
   Ceci nous fournit $x_0 \in E$ tel que $\mathcal{B} = \left(x_0, f(x_0), \ldots, f^{n-1}(x_0)\right)$ soit une base de E
   Il existe alors $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $f^n(x_0) = \sum_{i=0}^{n-1} \lambda_i f^i(x_0)$
   Je pose alors $Q = X^n + \sum_{i=0}^{n-1} (-\lambda_i) X^i \mathbb{K}[X]$
   de sorte que Q est unitaire de degré n et $\mathcal{M}_{\mathcal{B}}(f) = C_Q$

   $\Leftarrow$: 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 $\forall i \in [\![0, n-2]\!],\ f(e_i) = e_{i+1}$
   donc $(e_0, f(e_0), f^2(e_0), \ldots, f^{n-1}(e_0))$ est une base de E et donc f est cyclique

   $\boxed{\text{$f$ est cyclique si et seulement s'il existe une base $\mathcal{B}$ de E dans laquelle la matrice de f est de la forme C_Q où Q est un polynôme unitaire de degré n}}$

6. **$\Leftarrow$:** On suppose que χ_f est scindé sur $\mathbb{K}$ et a toutes ses racines simples.
   Ainsi $|\mathrm{sp}(f)| = \deg(\chi_f) = \dim E$
   donc f est diagonalisable d'après le cours

$\Leftarrow$ **:** On suppose que f est diagonalisable. Comme f est cyclique,
ceci nous fournit $\mathcal{B}$ une base de E et $Q \in \mathbb{K}[X]$ unitaire de degré n tel que $\mathcal{M}_{\mathcal{B}}(f) = C_Q$ d'après 5.
Ainsi C_Q est diagonalisable et il en est de même pour ${C_Q}^{\top}$ d'après 2
Ainsi $\mathbb{K}^n = \displaystyle\bigoplus_{\lambda \in \mathrm{sp}(f)} E_\lambda\left({C_Q}^{\top}\right)$ d'où $n = \displaystyle\sum_{\lambda \in \mathrm{sp}\left({C_Q}^{\top}\right)} \dim\left(E_\lambda\left({C_Q}^{\top}\right)\right)$
or on a $\forall \lambda \in \mathrm{sp}\left({C_Q}^{\top}\right),\ \dim\left(E_\lambda\left({C_Q}^{\top}\right)\right) = 1$ d'après 4 donc $\left|\mathrm{sp}\left({C_Q}^{\top}\right)\right| = n$
or d'après 1 : $\mathrm{sp}\left({C_Q}^{\top}\right) = \mathrm{sp}\left(C_Q\right) = \mathrm{sp}\left(f\right)$
donc f admet n valeurs propres distinctes dans $\mathbb{K}$
donc χ_f est scindé sur $\mathbb{K}$ et a toutes ses racines simples

Ainsi $\boxed{f \text{ est diagonalisable si et seulement si } \chi_f \text{ est scindé sur } \mathbb{K} \text{ et a toutes ses racines simples}}$

7. On suppose que f est cyclique.
Soit $(\lambda_0, \ldots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $\displaystyle\sum_{i=0}^{n} \lambda_i f^i = 0_{\mathcal{L}(E)}$. Montrons $\forall i \in [\![0, n-1]\!],\ \lambda_i = 0$
Comme f est cyclique, ceci nous fournit $x \in E$ tel que $\mathcal{B} = (x, f(x), \ldots, f^{n-1}(x))$ soit une base de E
donc $\displaystyle\sum_{i=0}^{n} \lambda_i f^i(x) = 0_{\mathcal{L}(E)}(x) = 0_E$
ainsi $\forall i \in [\![0, n-1]\!],\ \lambda_i = 0$ car $\mathcal{B}$ est libre
Alors $\boxed{(\mathrm{Id}, f, f^2, \ldots, f^{n-1}) \text{ est libre dans } \mathcal{L}(E)}$

Je note d le degré de π_f. D'après le cours on a $d = \dim\left(\mathbb{K}[f]\right)$.
Or $(\mathrm{Id}, f, f^2, \ldots, f^{n-1})$ est libre dans $\mathbb{K}[f]$ donc $d \geqslant n$
de plus d'après Cayley-Hamilton, on a χ_f est annulateur de f
d'où $\pi_f \mid \chi_f$ or ce sont des polynômes non nuls ainsi on a $d = \deg\left(\pi_f\right) \leqslant \deg\left(\chi_f\right) = n$
ainsi $n = d$ d'où $\boxed{\text{le polynôme minimal de } f \text{ est de degré } n}$

*On ne se sert pas de cette question pour montrer le théorème de Cayley-Hamilton dans le paragraphe **I.D** qui suit.*

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

8. On note $N_x = \left\{m \in \mathbb{N}^* \;\middle|\; \left(f^i(x)\right)_{0 \leqslant i \leqslant m-1} \text{ libre}\right\}$.
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 N_x admet un plus grand élément $p \in \mathbb{N}^*$.
Ainsi la famille $\left(f^i(x)\right)_{0 \leqslant i \leqslant p-1}$ est libre et la famille $\left(f^i(x)\right)_{0 \leqslant i \leqslant p}$ est liée

$$\boxed{\begin{array}{l}\text{On a bien l'existence de } p \in \mathbb{N}^* \text{ et de } (\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \in \mathbb{K}^p \text{ tels que la famille} \\ (x, f(x), f^2(x), \ldots, f^{p-1}(x)) \text{ est libre et } \alpha_0 x + \alpha_1 f(x) + \cdots + \alpha_{p-1} f^{p-1}(x) + f^p(x) = 0\end{array}}$$

9. On a $f\left(\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))\right) = \mathrm{Vect}(f(x), f^2(x), f^3(x), \ldots, f^p(x))$ car f linéaire
or $f^p(x) = -\alpha_0 x - \alpha_1 f(x) + \cdots - \alpha_{p-1} f^{p-1}(x) \in \mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$
d'où $f\left(\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))\right) \subset \mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$
Ainsi $\boxed{\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x)) \text{ est stable par } f}$

10. Je note alors $\tilde{f}$ l'endomorphisme induit par f sur $\text{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$
D'après ce qui précède $\mathcal{B} = \big(x, f(x), f^2(x), \ldots, f^{p-1}(x)\big)$ est une base de $\text{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$
On remarque que $\mathcal{M}_{\mathcal{B}}(\tilde{f}) = C_Q$ en notant $Q = \alpha_0 + \alpha_1 X + \cdots + \alpha_{p-1}X^{p-1} + X^p$
d'où $\chi_{\tilde{f}} = Q$ or $\chi_{\tilde{f}} | \chi_f$ car $\tilde{f}$ induit par f
On a montré que $\boxed{X^p + \alpha_{p-1}X^{p-1} + \cdots + \alpha_0 \text{ divise le polynôme } \chi_f}$
11. En reprenant les notations précédentes, on a $Q(f)(x) = 0$ et il existe $P \in \mathbb{K}[X]$ tel que $PQ = \chi_f$
Ainsi $\chi_f(f) = P(f) \circ Q(f)$ donc $\chi(f)(x) = P(f)\left[Q(f)(x)\right] = P(f)(0) = 0$ car $P(f)$ linéaire
On a ainsi montré que : $\forall x \in E,\ \chi(f)(x) = 0$
or $\chi(f) \in \mathcal{L}(E)$ d'où $\boxed{\chi_f(f) \text{ est l'endomorphisme nul}}$

II. Etude des endomorphismes cycliques

II.A. Endomorphismes cycliques nilpotents

12. $\Rightarrow$ **:** On suppose f cyclique alors $\deg(\pi_f) = n$ d'après 7
De plus d'après le cours, $\chi_f = X^n$ car f nilpotente
or $\pi_f | \chi_f$ selon Cayley-Hamilton et π_f est unitaire par définition
donc $\pi_f = X^n$
ainsi $f^n = 0$ et $\forall i \in [\![0, n-1]\!],\ f^i \neq 0$
d'où $r = n$
$\Leftarrow$ **:** On suppose que $r = n$ donc $f^n = 0$ et $f^{n-1} \neq 0$
Ceci nous fournit $x \in E$ tel que $f^{n-1}(x) \neq 0$
Soit $\lambda_0, \ldots, \lambda_{n-1} \in \mathbb{K}$ tels que $\displaystyle\sum_{i=0}^{n-1} \lambda_i f^i(x) = 0.$
On montre que $\forall i \in [\![0, n-1]\!],\ \lambda_i = 0$
On suppose, par l'absurde, que la propriété est fausse
Je note alors j le minimum de $\{i \in [\![0, n-1]\!] \mid \lambda_i \neq 0\}$
Ainsi $0 = f^{n-1-j}\left(\displaystyle\sum_{i=0}^{n-1} \lambda_i f^i(x)\right) = f^{n-1-j}\left(\displaystyle\sum_{i=j}^{n-1} \lambda_i f^i(x)\right) = \lambda_j f^{n-1}(x) + \displaystyle\sum_{i=j}^{n-1} \lambda_i f^{n-1+i-j}(x)$
Or $\forall i \geqslant p,\ f^i(x) = 0$ donc $\lambda_j f^{n-1}(x) = 0$ et $\lambda_j \neq 0$
d'où $f^{n-1}(x) = 0$ ce qui est absurde
Ainsi $(x, f(x), \ldots, f^{n-1}(x))$ est une famille libre composée de n vecteurs de E et $\dim E = n$
donc $(x, f(x), \ldots, f^{n-1}(x))$ est une base de E
donc f est cyclique.
On a montré que $\boxed{f \text{ est cyclique si et seulement si } r = n}$
On remarque que la matrice compagnon associée est unique car les coefficients de cette matrices sont donnés par ceux du polynôme caractéristique.
On sait que si f est cyclique et nilpotente, alors $\chi_f = X^n$

ainsi $\boxed{\text{la matrice compagnon de } f \text{ dans ce cas est } \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 1 & \ddots & & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})}$

II.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 $\boxed{F_k = \mathrm{Ker}((f-\lambda_k \mathrm{Id}_E)^{m_k}) \text{ est stable par } f}$
On a $\chi_f(X) = \displaystyle\prod_{k=1}^{p} (X-\lambda_k)^{m_k}$ et les polynômes $(X-\lambda_k)^{m_k}$ sont deux à deux premiers entre eux
Alors selon le lemme de décomposition des noyaux, on a
$$\mathrm{Ker}\,(\chi(f)) = \mathrm{Ker}((f-\lambda_1 \mathrm{Id}_E)^{m_1}) \oplus \cdots \oplus \mathrm{Ker}((f-\lambda_p \mathrm{Id}_E)^{m_p}) = F_1 \oplus \cdots \oplus F_p$$
de plus selon Cayley-Hamilton, $\chi_f(f) = 0$ et donc $\mathrm{Ker}\,(\chi(f)) = E$
d'où $\boxed{E = F_1 \oplus \cdots \oplus F_p}$

14. Soit $x \in F_k$. On a $(f-\lambda_k \mathrm{Id})^{m_k}(x) = 0$
Pour tout $y \in F_k$, on a $(f-\lambda_k \mathrm{Id})(y) = \varphi_k(y) \in F_k$
ainsi pour tout $p \in \mathbb{N}$, $(f-\lambda_k \mathrm{Id})^p(x) = \varphi_k^p(x)$ par récurrence immédiate sur p
donc $\varphi_k^{m_k}(x) = 0$, comme c'est vrai pour tout $x \in F_k$, on conclut que $\boxed{\varphi_k \text{ est un endomorphisme nilpotent de } F_k}$

15. D'après le cours, l'indice de nilpotence de φ_k, endomorphisme de F_k est majoré par $\dim F_k$
ainsi $\boxed{\nu_k \leqslant \dim(F_k)}$

16. Je note $P = \displaystyle\prod_{i=1}^{p} (X-\lambda_i)^{\nu_i}$. Soit $k \in [\![1,p]\!]$. Soit $x \in F_k$.
On a $P(f) = \left[\displaystyle\prod_{\substack{i=1 \\ i\neq k}}^{p} (X-\lambda_i)^{\nu_i}(f) \right] \circ (f-\lambda_k \mathrm{Id})^{\nu_k}$
donc $P(f)(x) = \left[\displaystyle\prod_{\substack{i=1 \\ i\neq k}}^{p} (X-\lambda_i)^{\nu_i}(f) \right] \left(\varphi_k^{\nu_k}(x)\right) = \left[\displaystyle\prod_{\substack{i=1 \\ i\neq k}}^{p} (X-\lambda_i)^{\nu_i}(f) \right] (0) = 0$
donc $P(f)$ coïncide avec l'endomorphisme nul sur chaque F_k et $E = F_1 \oplus \cdots \oplus F_p$ d'après 13
donc $P(f) = 0$
Je note d le degré de P comme P est unitaire alors $(\mathrm{Id}, f, f^2, \ldots, f^d)$ est liée
donc $d \geqslant n$ car $(\mathrm{Id}, f, f^2, \ldots, f^{n-1})$ est libre
or $d = \displaystyle\sum_{i=0}^{p} \nu_i$ d'où $n \leqslant \displaystyle\sum_{i=0}^{p} \nu_i$
On remarque à l'aide de la question 14 que $\nu_k \leqslant m_k$ pour tout $k \in [\![1,p]\!]$
donc $n \leqslant \displaystyle\sum_{k=0}^{p} \nu_k \leqslant \sum_{i=0}^{p} m_k = n$
ainsi les inégalités sont des égalités et $\boxed{\text{pour tout } k \in [\![1,p]\!], \text{ on a } \nu_k = m_k}$

17. Comme $E = F_1 \oplus \cdots \oplus F_p$ d'après 13 et $\forall k \in [\![1,p]\!]$, $\nu_k \leqslant \dim F_k$ d'après 15

on a donc avec la question précédente $n = \displaystyle\sum_{k=1}^{p} \nu_k \leqslant \sum_{k=1}^{p} \dim(F_k) = n$

Comme à la question précédente, on obtient : $\boxed{\forall k \in [\![1,p]\!],\ \nu_k = m_k = \dim(F_k)}$

φ_k est un endomorphisme nilpotent de F_k d'indice $\nu_k = m_k = \dim(F_k)$

donc selon 12, φ_k est nilpotent et cyclique.

ceci nous fournit une base $\mathcal{B}_k$ de F_k tel que $\mathcal{M}_{\mathcal{B}_k}(\varphi_k) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 1 & 0 & \ddots & & & \vdots \\ 0 & 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{m_k}(\mathbb{C})$

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

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

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 $E = F_1 \oplus \cdots \oplus F_p$

ainsi $\boxed{\mathcal{B} = (u_1, \ldots, u_n) \text{ est une base de } E \text{ dans laquelle } f \text{ a une matrice diagonale par blocs de formes voulues}}$

Remarque : pour la suite on peut démontrer que pour une telle base on a nécessairement :

$$\forall k \in [\![1,p]\!],\ (f - \lambda_k \mathrm{Id})^{m_k}(u_{m_1+\cdots+m_{k-1}+1}) = 0 \text{ puis}$$

$$\forall k \in [\![1,p]\!],\ \forall i \in [\![1,m_k]\!],\ u_{m_1+\cdots+m_{k-1}+i} \in F_k$$

On peut aussi supposer que l'on travaille avec la base choisie.

18. Pour $k \in [\![1,p]\!]$, on a $u_{m_1+\cdots+m_{k-1}+1} \in F_k$

ainsi $\forall i \in \mathbb{N},\ f^i(u_{m_1+\cdots+m_{k-1}+1}) \in F_k$ car F_k stable par f

puis pour tout $P \in \mathbb{C}[X]$, on a $P(f)(u_{m_1+\cdots+m_{k-1}+1}) \in F_k$ car F_k est stable par combinaison linéaire.

Et ainsi $P(f)(x_0) = \displaystyle\sum_{k=1}^{p} P(f)(u_{m_1+\cdots+m_{k-1}+1})$ est la décomposition de $P(f)(x_0)$ sur $F_1 \oplus \cdots \oplus F_p$

Soit $Q \in \mathbb{C}[X]$. On a donc $Q(f)(x_0) = 0 \iff \forall k \in [\![1,p]\!],\ Q(f)(e_k) = 0$

Je note $e_k = u_{m_1+\cdots+m_{k-1}+1}$ et on a $\mathcal{B}_k = (e_k, \varphi_k(e_k), \ldots, \varphi_k^{m_k-1}(e_k))$ est une base de F_k

On a vu que la matrice de φ_k dans cette base est $C_{X^{m_k}}$

donc $\pi_{\varphi_k} = X^{m_k}$ car φ_k est cyclique et nilpotent et $\dim(F_k) = m_k$ selon 12

$$\forall k \in [\![1,p]\!],\ (f - \lambda_k \mathrm{Id})^{m_k}(u_{m_1+\cdots+m_{k-1}+1}) = 0 \text{ puis}$$

$$\forall k \in [\![1,p]\!],\ \forall i \in [\![1,m_k]\!],\ u_{m_1+\cdots+m_{k-1}+i} \in F_k$$

Par ailleurs on montre facilement que

$$\forall P \in \mathbb{C}[X], P(\varphi_k) = 0 \Longleftrightarrow P(\varphi_k)(e_k) = 0$$

car $P(\varphi_k)$ commute avec tout φ_k^i et que $\left(\varphi_k^i(e_k)\right)_{0\leqslant i<m_k}$ est une base de F_k.
Par ailleurs on a $Q(\varphi_k) = 0 \Longleftrightarrow X^{m_k}|Q$ (nilpotent et cyclique)
donc $Q(f)(e_k) = 0 \Longleftrightarrow Q(\varphi_k + \lambda_k \mathrm{Id}_{F_k})(e_k) = 0 \Longleftrightarrow X^{m_k}|Q(X+\lambda_k)$
ainsi $Q(f)(e_k) = 0 \Longleftrightarrow (X-\lambda_k)^{m_k}|Q(X)$
donc comme les $(X-\lambda_k)^{m_k}$ sont deux à deux premiers entre eux,
on a finalement $\boxed{Q(f)(x_0) = 0 \Longleftrightarrow \prod_{k=1}^{p}(X-\lambda_k)^{m_k}|Q}$

19. Soit $(\lambda_i)_{0\leqslant i\leqslant n-1} \in \mathbb{K}^n$ tel que $\sum_{i=0}^{n-1}\lambda_i f^i(x_0) = 0$ Je note $Q = \sum_{i=0}^{n-1}\lambda_i X^i$ de sorte que $Q(f)(x_0) = 0$
ainsi $\prod_{k=1}^{p}(X-\lambda_k)^{m_k}|Q$ d'après la question précédente or $\deg(Q) \leqslant n-1 < n = \deg\left(\prod_{k=1}^{p}(X-\lambda_k)^{m_k}\right)$
donc Q est le polynôme nul et ainsi $\forall i \in [\![0,n-1]\!],\ \lambda_i = 0$
donc $\left(f^i(x_0)\right)_{0\leqslant i\leqslant n-1}$ est une famille libre de n vecteurs de E et $n = \dim E$
d'où $\left(f^i(x_0)\right)_{0\leqslant i\leqslant n-1}$ est une base de E ce qui justifie que $\boxed{f \text{ est cyclique}}$

II.C.

20. Classique : $\lambda \mapsto \det(P_1 + \lambda P_2)$ est une application polynomiale associé à un polynôme P et tel que $P(\mathrm{i}) \neq 0$. Donc P n'est pas le polynôme nul et ne peut donc pas être nul sur $\mathbb{R}$.
On a donc $\lambda \in \mathbb{R}$ tel que $Q_0 = Q_1 + \lambda Q_2 \in GL_n(\mathbb{R})$ et $AQ_0 = AQ_1 + \lambda AQ_2 = Q_1B + \lambda Q_2 B = Q_0 B$ car, par unicité des parties réelle et imaginaire, $A(Q_1 + \mathrm{i}Q_2) = (Q_1 + \mathrm{i}Q_2)B$ donne $AQ_1 = Q_1 B$ et $AQ_2 = Q_2 B$.
Ainsi $\boxed{A \text{ et } B \text{ sont semblables dans } \mathcal{M}_n(\mathbb{R}).}$

21. En considérant la matrice de $M \in \mathcal{M}_n(\mathbb{R}) \subset \mathcal{M}_n(\mathbb{C})$ de f dans une base quelconque de E. Comme $\left(\mathrm{Id}, f, \ldots, f^{n-1}\right)$, est $\mathbb{R}$-libre, $\left(I_n, M, \ldots, M^{n-1}\right)$ l'est, donc est $\mathbb{C}$-libre car les matrices sont réelles. Soit $g \in \mathcal{L}(\mathbb{C}^n)$ dont la matrice dans la base canonique est M, alors $\left(\mathrm{Id}, g, \ldots, g^{n-1}\right)$ est $\mathbb{C}$-libre et la partie précédente permet de conclure que g est cyclique, et donc d'après I.C, M est semblable dans $\mathcal{M}_n(\mathbb{C})$ à une matrice compagnon : il s'agit nécessairement à celle associé au polynôme $\chi_f \in \mathbb{R}[X]$ donc elle est à cœfficients réels.
La question précédente et de nouveau la partie I.C permettent alors de conclure que $\boxed{f \text{ est cyclique.}}$

III. Endomorphismes commutants, décomposition de Frobenius

22. L'application $g \longmapsto f\circ g - g\circ f$ est un endomorphisme de $\mathcal{L}(E)$ dont le noyau est $C(f)$
Ainsi $C(f)$ est un sous-espace vectoriel de $\mathcal{L}(E)$

De plus, soit 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 $\circ$ et il est clair que $\mathrm{Id} \in C(f)$
Ainsi $\boxed{C(f) \text{ est une sous-algèbre de } \mathcal{L}(E)}$

III.A. Commutant d'un endomorphisme cyclique

23. On a $g(x_0) \in E$ et $(x_0, f(x_0), \dots, f^{n-1}(x_0))$ est une base de E.

    d'où $\boxed{\text{l'existence de } \lambda_0, \lambda_1, \dots, \lambda_{n-1} \text{ de } \mathbb{K} \text{ tels que } g(x_0) = \sum_{k=0}^{n-1} \lambda_k f^k(x_0)}$

24. Il suffit d'établir que les applications linéaires g et $\sum_{k=0}^{n-1} \lambda_k f^k$ coïncident sur la base $(x_0, f(x_0), \dots, f^{n-1}(x_0))$.

    On montre par récurrence immédiate que $\forall i \in \mathbb{N},\ g \in C\left(f^i\right)$

    Soit $i \in [\![0, n-1]\!]$. En utilisant 21 et le fait que l'algèbre $\mathbb{K}[f]$ est commutative

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

    donc $g = \sum_{k=0}^{n-1} \lambda_k f^k$ et $\boxed{g \in \mathbb{K}[f]}$

25. On vient d'établir le sens direct (avec un polynôme de degré $\leqslant n-1$)

    La réciproque vient du fait que $\mathbb{K}[f]$ est une algèbre commutative et que $\mathbb{K}_{n-1}[X] \subset \mathbb{K}[X]$ et $f \in \mathbb{K}[f]$.

    On conclut que

$$\boxed{g \in C(f) \text{ si et seulement s'il existe un polynôme } R \in \mathbb{K}_{n-1}[X] \text{ tel que } g = R(f)}$$

III.B. Décomposition de Frobenius

26. On suppose que $G = F_1 \cup \cdots \cup F_r$ est un sous espace de E.

    Par l'absurde, je suppose qu'aucun des sous-espaces F_i ne contient tous les autres.

    Ainsi $r \geqslant 2$ et $G \neq \{0\}$.

    Méthode 1 : Quitte à réduire le nombre, on peut supposer qu'aucun F_i n'est inclus dans la réunion des autres. Cela nous fournit $x_1 \in F_1$ qui n'est dans aucun des F_i pour $i \geqslant 2$.

    Sinon, $F_1 \neq G$ et on peut aussi trouver $y \in G \setminus F_1$.

    Pour tout scalaire λ, on a $y + \lambda x_1 \notin F_1$ (car sinon $y \in F_1$) et ainsi $y + \lambda x_1 \in F_2 \cup \cdots \cup F_r$.

    La droite affine $y + \mathbb{K}x_1$ est donc incluse dans $F_2 \cup \cdots \cup F_r$ et contient une infinité d'éléments

    car $\mathbb{K}$ est infini et $t \in \mathbb{K} \mapsto y + tx_1$ est injective car $x_1 \neq 0$

    Ceci nous fournit $j \in [\![2, r]\!]$ et $\lambda \neq \lambda'$ dans $\mathbb{K}$ tel que $y + \lambda x_1 \in F_j$ et $y + \lambda' x_1 \in F_j$

    donc $x_1 \in F_j$ (par combinaison linéaire) ce qui est absurde

    Méthode 2 : Comme G est un $\mathbb{K}-$espace vectoriel de dimension finie, on peut munir G d'une norme.

    De plus les notions topologiques sur G sont indépendantes du choix de la norme car $\dim G < +\infty$.

    Comme les F_i sont des sous-espaces de G de dimensions finies, ce sont des fermés de G.

    Soit $i \in [\![1, r]\!]$. Comme $F_i \neq G$, cela nous fournit $e \in G \setminus F_i$.

    Soit $x \in F_i$. On a alors : $\forall p \in \mathbb{N}^*,\ x + \frac{1}{p}e \notin F_i$

    Pour toute boule B_x centré en x, il existe $p_0 \in \mathbb{N}^*,\ x + \frac{1}{p_0}e \in B_x$ car $\left(x + \frac{1}{p_0}e\right)_{p \geqslant 1}$ converge vers x

    Ainsi relativement à G, les F_i sont des fermés d'intérieurs vides.

    Donc pour $i \in [\![1, r]\!]$, $\Omega_i = G \setminus F_i$ un ouvert dense dans G

On pose $V_i = \bigcap_{j=1}^{i} \Omega_j$

On montre par récurrence finie que les V_i $(1 \leqslant i \leqslant r)$ sont des ouverts non vides de G

Pour l'initialisation c'est évident car $V_1 = \Omega_1$ est dense dans G.

Pour l'hérédité, on suppose pour $i < r$ que V_i est un ouvert non vide

on a $V_{i+1} = V_i \bigcap \Omega_{i+1}$ est un ouvert (intersection de deux ouverts) et non vide car $V_i \neq \emptyset$ et Ω_{i+1} dense

donc $V_r \neq \emptyset$ et $V_r = G \setminus \left(\bigcup_{j=1}^{r} F_j \right) = \emptyset$ ce qui est absurde

Ainsi $\boxed{\text{l'un des sous-espaces } F_i \text{ contient tous les autres}}$

Remarque : Pour $r = 2$, il existe une preuve classique purement algébrique. Pour le cas général, la preuve doit utiliser le fait que $\mathbb{K}$ est infini.

En effet, si je prend $K = \mathbb{Z}/2\mathbb{Z}$, $E = \mathbb{K}^2$, $F_1 = \mathrm{Vect}\left((1,0)\right)$, $F_2 = \mathrm{Vect}\left((0,1)\right)$ et $F_3 = \mathrm{Vect}\left((1,1)\right)$.

On a $E = F_1 \bigcup F_2 \bigcup F_3$ et pourtant aucun des sous-espaces F_i ne contient tous les autres.

27. Soit $x \in E$ On considère l'application $\varphi_x : P \in \mathbb{K}[X] \longmapsto P(f)(x) \in E$.

Comme $I_x = \{P \in \mathbb{K}[X] / \ P(f)(x) = 0\}$ est le noyau de l'application linéaire φ_x,

I_x un sous groupe de $(\mathbb{K}[X], +)$

Pour $P \in I_x$ et $Q \in \mathbb{K}[X]$, on a $QP \in I_x$

car $(QP)(f)(x) = (Q(f) \circ P(f))\,(x) = Q(f)\,(P(f)(x)) = 0$ car $Q(f) \in \mathcal{L}(E)$

d'où I_x est un idéal de $\mathbb{K}[X]$ comme $\pi_f \in I_x$, cet idéal est non réduit à $\{0\}$

ce qui nous fournit $\pi_{f,x} \in \mathbb{K}[X]$ unitaire (donc non nul) tel que $I_x = (\pi_{f,x}) = \{\pi_{f,x} P \mid P \in \mathbb{K}[X]\}$

On remarque que : $\forall x \in E,\ \pi_{f,x} | \pi_f$

Si 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 $\alpha_i \in \mathbb{N}^*$.

Alors le nombre de diviseurs unitaires de π_f est $\prod_{k=1}^{N} (\alpha_i + 1)$

Ainsi l'ensemble $\{\pi_{f,x} \mid x \in E\}$ est fini de cardinal noté r où $r \in [\![1, \prod_{k=1}^{N} (\alpha_i + 1)]\!]$

On peut donc choisir $u_1, \ldots u_r \in E$, tel que $\{\pi_{f,x} \mid x \in E\} = \{\pi_{f,u_i} \mid i \in [\![1, r]\!]\}$

Ainsi $E = \bigcup_{i=1}^{r} \ker(\pi_{f,u_i}(f))$ car $\forall x \in E,\ x \in \ker(\pi_{f,x}(f))$

La question 24 nous fournit $i_0 \in [\![1, r]\!]$ tel que $\ker(\pi_{f,u_{i_0}}(f)) = E$

On note $x_1 = u_{i_0}$ et on a $\ker(\pi_{f,x_1}(f)) = E$

On remarque que $\pi_{f,x_1}(f) = 0_{\mathcal{L}(E)}$ donc $\pi_f | \pi_{f,x_1}$

or $\pi_{f,x_1} | \pi_f$ et ce sont des polynômes unitaires

donc $\pi_{f,x_1} = \pi_f$ Finalement

$$\forall P \in \mathbb{K}[X],\ P(f)(x_1) = 0 \Longleftrightarrow \pi_f | P$$

en faisant comme en 19, on montre que $\boxed{(x_1, f(x_1), \ldots, f^{d-1}(x_1)) \text{ est libre}}$

28. En faisant comme en 9, on montre que $\boxed{E_1 \text{ est stable par } f}$
De plus, on a $E_1 = \{P(f)(x_1)/\ P \in \mathbb{K}_{d-1}[X]\} \subset \{P(f)(x_1)/\ P \in \mathbb{K}[X]\}$
Soit $P \in \mathbb{K}[X]$. Comme $\pi_f \neq 0$,
le théorème de la division euclidienne nous fournit Q et $R \in \mathbb{K}[X]$ tels que $\begin{cases} P = Q\pi_f + R \\ \deg(R) < d = \deg(\pi_f) \end{cases}$
On a alors $P(f)(x_1) = [Q(f) \circ \pi_f(f)]\,(x_1) + R(f)(x_1) = R(f)(x_1) \in \{T(f)(x_1)/\ T \in \mathbb{K}_{d-1}[X]\}$
On conclut que $\boxed{E_1 = \{P(f)(x_1)/\ P \in \mathbb{K}[X]\}}$

29. D'après ce qui précède $\mathcal{B} = (e_1, e_2, \ldots, e_d)$ est une base de E_1.
De plus on a $\mathcal{M}_{\mathcal{B}}(\psi_1) = C_{\pi_f}$ matrice compagnon du π_f polynôme unitaire de degré $d = \dim(E_1)$
alors d'après 5, $\boxed{\psi_1 \text{ est cyclique}}$

30. Pour $i \in \mathbb{N}$, on note $F_i = \operatorname{Ker}\left(\Phi \circ f^i\right)$ ainsi $F = \bigcap_{i\in\mathbb{N}} F_i$ est bien un sous-espace de E
De plus, on a pour $i \geqslant 1$, $f(F_i) \subset F_{i-1}$ donc
$$f(F) \subset f\left(\bigcap_{i\in\mathbb{N}^*} F_i\right) \subset \bigcap_{i\in\mathbb{N}^*} f\left(F_i\right) \subset \bigcap_{i\in\mathbb{N}^*} F_{i-1} = F$$
d'où $\boxed{F \text{ est stable par } f}$
Soit $u \in E_1 \cap F$.
Comme $u \in E_1$, cela nous fournit $\lambda_1, \ldots, \lambda_d \in \mathbb{K}$ tels que $u = \sum_{k=1}^{d} \lambda_k e_k$
or $\Phi(x) = \lambda_d$ et $\Phi(f^0(x)) = 0$ car $u \in F$, donc $\lambda_d = 0$ d'où $u = \sum_{k=1}^{d-1} \lambda_k e_k$
puis $f(u) = \sum_{k=1}^{d-1} \lambda_k e_{k+1}$ et donc $\lambda_{d-1} = 0$ et $f(u) = \sum_{k=1}^{d-2} \lambda_k e_{k+1}$
En réitérant le procédé, on trouve $\lambda_{d-2} = \ldots = \lambda_1 = 0$
donc $u = 0$
L'autre inclusion étant évidente, on a $E_1 \cap F = \{0\}$ d'où $\boxed{E_1 \text{ et } F \text{ sont en somme directe}}$

31. Je note Ψ_1 l'application linéaire induite par Ψ entre E_1 et $\mathbb{K}^d$.
Soit $x \in \operatorname{Ker}(\Psi_1)$.
On a $x \in E_1$ et $\Phi(x) = \Phi(f(x)) = \cdots = \Phi(f^{d-1}(x)) = 0$.
En faisant comme à la question précédente, on obtient $x = 0$
L'autre inclusion étant évidente, on a $\operatorname{Ker}(\Psi_1) = \{0\}$
Ainsi Ψ_1 est une application linéaire injective entre E_1 et $\mathbb{K}^d$ or $\dim(E_1) = d = \dim(\mathbb{K}^d)$
En utilisant le théorème du rang, on obtient que Ψ_1 est surjective puis bijective
Ainsi $\boxed{\Psi \text{ induit un isomorphisme entre } E_1 \text{ et } \mathbb{K}^d}$

32. De la question précédente, on montre que Ψ est surjective de E vers $\mathbb{K}^d$ et que $\ker(\Psi) \bigcap E_1 = \{0\}$.
Ainsi $\dim\left(E_1\right) = d = \operatorname{rg}\left(\Psi\right)$ et $\dim(E) = \dim\left(\ker(\Psi)\right) + \operatorname{rg}(\Psi) = \dim\left(\ker(\Psi)\right) + \dim\left(E_1\right)$
donc $E = E_1 \oplus \operatorname{Ker}(\Psi)$
On a $\operatorname{Ker}\Psi = \bigcap_{i=0}^{d-1} F_i$ (les F_i sont introduits en 28) on a donc $F \subset \operatorname{Ker}\Psi$

Soit $x \in \operatorname{Ker}(\Psi)$. Montrons que $x \in F$

Soit $i \in \mathbb{N}$. Il suffit d'établir que $\Phi(f^i(x)) = 0$

Le théorème de la division euclidienne nous fournit Q et $R \in \mathbb{K}[X]$ tel que $\deg(R) < d$ et $X^i = Q\pi_f + R$.

On peut écrire $R = \sum_{k=0}^{d-1} a_k X^k$. On a comme en 26 et car Φ est linéaire

$$\Phi(f^i(x)) = \Phi(0) + \Phi(R(f)(x)) = 0 + \sum_{k=0}^{d-1} a_k \Phi\left(f^k(x)\right) = 0$$

ainsi $F \supset \operatorname{Ker}\Psi$ d'où $F = \operatorname{Ker}\Psi$

on conclut que $\boxed{E = E_1 \oplus F}$

33. **Préambule :** Avant de commencer la construction par récurrence, on remarque que dans ce qui précède le polynôme minimal de f est celui de ψ_1 et donc que $\forall x \in F, \pi_{\psi_1}(f)(x) = 0$

Initialisation : On prend E_1, F et ψ_1 comme ci dessus.

On a E_1 stable par F et ψ_1 cyclique.

On pose $P_1 = \pi_f = \pi_{\psi_1}$, $G_1 = F$ de sorte que $E_1 \oplus G_1 = E$

On a $\forall x \in G_1,\ P_1(f)(x) = 0$

Hérédité : Soit $k \in \mathbb{N}^*$.

On suppose avoir l'existence de k sous-espaces vectoriels de E, notés $E_1, \dots, E_k$ et G_k tous stables par f, tels que

— $E = E_1 \oplus \cdots \oplus E_k \oplus G_k$;

— pour tout $1 \leqslant i \leqslant k$, l'endomorphisme ψ_k induit par f sur le sous-espace vectoriel E_i est cyclique ;

— si on note P_i le polynôme minimal de ψ_i, alors P_{i+1} divise P_i pour tout entier i tel que $1 \leqslant i \leqslant k-1$

— $\forall x \in G_k,\ P_k(f)(x) = 0$

Si $\dim G_k = 0$, on s'arrête et on pose $r = k$

Sinon, on applique 24 à 30 à l'endomorphisme induit par f sur G_k

On obtient alors E_{k+1}, G_{k+1} sous espaces stables par f et le polynôme P_{k+1} tels que

— $E = E_1 \oplus \cdots \oplus E_{k+1} \oplus G_{k+1}$;

— l'endomorphisme ψ_{k+1} induit par f sur le sous-espace vectoriel E_{k+1} est cyclique ;

— si on note P_{k+1} le polynôme minimal de ψ_{k+1}, alors P_{k+1} divise P_k

— $\forall x \in G_{k+1},\ P_{k+1}(f)(x) = 0$

On a ainsi la construction voulue au rang k.

Conclusion : Cette construction algorithmique s'arrête car à chaque étape $\dim(E_k) \leqslant 1$ et donc $r \leqslant \dim(E)$. car $(\dim G_k)_k$ est une suite à valeurs dans $\mathbb{N}$ strictement décroissante.

On obtient ainsi le résultat voulu.

On en déduit qu'il existe r sous-espaces vectoriels de E, notés $E_1, \dots, E_r$, tous stables par f, tels que : — $E = E_1 \oplus \cdots \oplus E_r$; — pour tout $1 \leqslant i \leqslant r$, l'endomorphisme ψ_i induit par f sur le sous-espace vectoriel E_i est cyclique ; — si on note P_i le polynôme minimal de ψ_i, alors P_{i+1} divise P_i pour tout entier i tel que $1 \leqslant i \leqslant r-1$.

III.C. Commutant d'un endomorphisme quelconque

34. Je reprends les notations de la questions précédente pour la décomposition de Frobenius de f.
Je note Λ l'application telle que pour $(g_1,\dots,g_r)\mathcal{L}(E_1)\times\cdots\times\mathcal{L}(E_r)$, on a $\Lambda(g_1,\dots,g_r)$ défini sur E par $\Lambda(g_1,\dots,g_r)(x)=g_1(x_1)+\cdots g_r(x_r)$ où $x=\sum_{k=1}^{r}x_k$ et les $x_k\in E_k$
Ainsi définie, Λ est linéaire de $\mathcal{L}(E_1)\times\cdots\times\mathcal{L}(E_r)$ à valeurs dans $\mathcal{L}(E)$
De plus on montre facilement que Λ est injective et que $\Lambda\left(C(\psi_1)\times\cdots\times C(\psi_r)\right)\subset C(f)$
Ainsi $\dim\left(C(f)\right)\geqslant\dim\left(C(\psi_1)\times\cdots\times C(\psi_r)\right)=\dim\left(C(\psi_1)\right)+\cdots+\dim\left(C(\psi_r)\right)$
or pour $i\in[\![1,r]\!]$, en notant $n_i=\dim E_i$ on a $C(\psi_i)=\mathrm{Vect}(\psi_i^0,\psi_i^1,\dots,\psi_i^{n_i-1})$ d'après 23 du **III.A**
Comme ψ_i est cyclique alors $(\psi_i^0,\psi_i^1,\dots,\psi_i^{n_i-1})$ est libre d'après 7
donc $\dim\left(C(\psi_i)\right)=n_i=\dim\left(E_i\right)$ d'où
$$\dim\left(C(\psi_1)\right)+\cdots+\dim\left(C(\psi_r)\right)=\dim\left(E_1\right)+\cdots+\dim\left(E_r\right)=\dim\left(E_1\oplus\cdots\oplus E_r\right)=\dim(E)=n$$
Ainsi $\boxed{\text{la dimension de } C(f) \text{ est supérieure ou égale à } n}$

35. On note $d=\deg\left(\pi_f\right)$. D'après le cours, on a $\dim\left(\mathbb{K}[f]\right)=d$
or $\mathbb{K}[f]=C(f)$ et $\dim C(f)\geqslant n$ donc $d\geqslant n$.
Or on a $\pi_f|\chi_f$ comme conséquence de Cayley-Hamilton ainsi $d\leqslant n$
donc $d=n$
Or en reprenant les notations précédentes, on a $\dim(E_1)=d=n$
Donc $E_1=E$ et $\psi_1=f$ or ψ_1 est cyclique
ainsi $\boxed{f \text{ est cyclique}}$

IV p-Cycles

IV.A –

36. Pour tout $j\in[\![0,p-1]\!]$, $f^p\left(f^j(x_0)\right)=f^j\left(f^p(x_0)\right)=f^j(x_0)$ et donc, par linéarité et le fait que $\left(x_0,f(x_0),\dots,f^{p-1}(x_0)\right)$ soit génératrice de E, $\boxed{f^p=\mathrm{Id}.}$
37. $\mathcal{E}$ est une partie de $\mathbb{N}^*$ non vide : elle contient 1 car $x_0\neq 0$ car $E\neq\{0_E\}$, et majorée par $\dim E$ donc $\boxed{\mathcal{E}\text{ admet un maximum.}}$
38. Par maximalité de m, $\left(x_0,f(x_0),\dots,f^{m-1}(x_0)\right)$ libre et $\left(x_0,f(x_0),\dots,f^{m}(x_0)\right)$ est liée donc $f^m(x_0)\in\mathrm{Vect}\left(x_0,f(x_0),\right.$.
Puis, par récurrence, $\boxed{\text{pour tout } k\geqslant m,\ f^k(x_0)\in\mathrm{Vect}\left(x_0,f(x_0),\dots,f^{m-1}(x_0)\right).}$
Comme $\left(x_0,f(x_0),\dots,f^{p-1}(x_0)\right)$ est génératrice de E, $\left(x_0,f(x_0),\dots,f^{m-1}(x_0)\right)$ engendre aussi E : c'en est une base.
Finalement, $m=n=\dim E$ et $\boxed{f \text{ est cyclique.}}$

Le nombre de valeurs propres est le degré du polynôme minimal de f. Or si $P=\sum_{k=0}^{d}a_kX^k$ avec $P(f)=0$ et $d<m$, alors $P(f)(x_0)=0=a_0x_0+\cdots+a_df^d(x_0)$ et donc $a_0=\cdots=a_d=0$ car $\left(x_0,f(x_0),\dots,f^{n-1}(x_0)\right)$ est libre et donc $P=0$.
Ainsi, $\deg\pi_f\geqslant n$ et comme $\pi_f|\chi_f$, $\deg\pi_f\leqslant n$.
Finalement $\boxed{f \text{ a exactement } \deg\pi_f=n=\dim E \text{ valeurs propres distinctes.}}$
On aurait aussi pu utiliser le fait que le polynôme scindé simple X^p-1 annule f qui est donc diagonalisable et que les sous-espaces propres sont des droites (vu l'étude sur les matrices compagnons.)

IV.B –

39. f étant un n-cycle, elle est annulée par le polynôme scindé simple $X^n - 1$ qui est nécessairement son polynôme caractéristique (et son polynôme minimal).
Donc sa matrice compagnon qui est aussi sa matrice dans la base $\left(x_0, f(x_0), \dots, f^{n-1}(x_0)\right)$ est $\boxed{C = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ (0) & & 1 & 0 \end{pmatrix}.}$

Si $k \in [\![1, n]\!]$, $\boxed{CU_k = \begin{pmatrix} \overline{\omega}^{nk} \\ \overline{\omega}^{k} \\ \vdots \\ \overline{\omega}^{(n-1)k} \end{pmatrix} = \begin{pmatrix} 1 \\ \overline{\omega}^{k} \\ \vdots \\ \overline{\omega}^{(n-1)k} \end{pmatrix} = \overline{\omega}^{-k} U_k = \omega^k U_k.}$

40. On calcule, pour $1 \leqslant k, \ell \leqslant n$, en remarque que $\overline{\omega} = \omega^{-1}$,

$$\left(M\overline{M}\right)_{k,\ell} = \sum_{j=1}^{n} m_{k,j}\overline{m_{j,\ell}} = \sum_{j=1}^{n} \overline{\omega}^{kj}\omega^{j\ell} = \sum_{j=1}^{n} \omega^{j(k-\ell)} = \sum_{j=1}^{n} \left(\omega^{k-\ell}\right)^j.$$

Donc si $k = \ell$, $\left(M\overline{M}\right)_{k,k} = n$, et si $k \neq \ell$, $\left(M\overline{M}\right)_{k,\ell} = \omega^{k-\ell}\dfrac{1-\omega^{n(k-\ell)}}{1-\omega^{k-\ell}} = 0$ car $\omega^n = 0$.

Finalement, $M\overline{M} = nI_n$ donc $\boxed{M \text{ inversible d'inverse } \frac{1}{n}\overline{M}.}$

41. En remarque que l'endomorphisme canoniquement associé à C est l'application $(x_0, \dots, x_n) \mapsto (x_n, x_1, \dots, x_{n-1})$ on obtient les puissances de C et on arrive à $A = a_0 I_n + a_1 C + \cdots + a_{n-1}C^{n-1} = P(C)$ où $\boxed{P = \sum_{k=0}^{n-1} a_k X^k.}$

Or C est diagonalisable car son polynôme caractéristique est celui de f soit $X^n - 1$ scindé à racines simple (ou parce que f est cyclique.) Ses valeurs propres sont les racines n^{e} de l'unité soit les $\overline{\omega}^k$ pour $k \in [\![1, n]\!]$ et la question 39 montre que U_k est un vecteur propre associé à $\overline{\omega}^k$. Ces vecteurs constituant les colonnes de M, il s'agit de la matrice de passage de la base canonique vers cette base de vecteurs propres.
Ainsi, $C = MDM^{-1}$ avec $D = \operatorname{diag}\left(\omega, \omega^2, \dots, \omega^n = 1\right)$
Alors $A = P\left(MDM^{-1}\right) = MP(D)M^{-1}$ donc $\boxed{A \text{ est diagonalisable}}$ et comme

$$P(D) = \operatorname{diag}\left(P(\omega), P\left(\omega^2\right), \dots, P(\omega^n)\right),$$

$\boxed{\operatorname{sp}A = \{P(z),\ z \in \mathbb{U}_n\} \text{ et } (U_1, \dots, U_n) \text{ en est une base de vecteurs propres.}}$

– FIN –