Endomorphismes cycliques

Corrigé DM 6

par David Blottière, le 6 novembre 2023 à 17h40

Extrait du sujet CentraleSupélec 1 MP 2019.

Notations et définitions

Dans tout le problème, $\mathbf{K}$ *désigne* $\mathbf{R}$ *ou* $\mathbf{C}$*,* $\mathbf{N}$ *désigne l'ensemble des entiers naturels et* n *est un entier naturel.*

On note $\mathbf{K}_n[X]$ *le sous-espace vectoriel de* $\mathbf{K}[X]$ *des polynômes de degré inférieur ou égal à* n *à coefficients dans* $\mathbf{K}$ *et, pour* $n \geqslant 1$*,* $\mathscr{M}_n(\mathbf{K})$ *la* $\mathbf{K}$*-algèbre des matrices carrées de taille* n *à coefficients dans* $\mathbf{K}$*. La matrice unité est notée* I_n *et on désigne par* $GL_n(\mathbf{K})$ *le groupe des matrices inversibles de* $\mathscr{M}_n(\mathbf{K})$*.*

Pour toute matrice A *de* $\mathscr{M}_n(\mathbf{K})$*, on note* $A^\top$ *la transposée de la matrice* A*,* $rg(A)$ *son rang,* $tr(A)$ *sa trace,* $\chi_A = \det(XI_n - A)$ *son polynôme caractéristique,* π_A *son polynôme minimal et* $sp(A)$ *l'ensemble de ses valeurs propres dans* $\mathbf{K}$*.*

Dans tout le problème, E *désigne un espace vectoriel sur le corps* $\mathbf{K}$ *de dimension finie* n *supérieure ou égale à 2, et* $\mathscr{L}(E)$ *est l'algèbre des endomorphismes de* E*. On note* f *un endomorphisme de* E*.*

On note $f^0 = Id_E$ *et* $\forall k \in \mathbf{N},\ f^{k+1} = f^k \circ f$*.*

Si $Q \in \mathbf{K}[X]$ *avec* $Q(X) = a_0 + a_1X + \cdots + a_mX^m$*,* $Q(f)$ *désigne l'endomorphisme* $a_0Id_E + a_1f + \cdots + a_mf^m$*. On note* $\mathbf{K}[f]$ *la sous-algèbre commutative de* $\mathscr{L}(E)$ *constituée des endomorphismes* $Q(f)$ *quand* Q *décrit* $\mathbf{K}[X]$*.*

De même, on utilise les notations suivantes, similaires à celles des matrices, pour un endomorphisme f *de* E *:* $rg(f)$*,* $tr(f)$*,* χ_f*,* π_f *et* $sp(f)$*.*

Enfin, on dit que f *est* <u>*cyclique*</u> *si et seulement s'il existe un vecteur* x_0 *dans* E *tel que* $(x_0, f(x_0), \dots, f^{n-1}(x_0))$ *soit une base de* E*.*

I — Matrices compagnons

Soit $M \in \mathscr{M}_n(\mathbf{K})$*.*

Q1. — Montrer que M et $M^\top$ ont même spectre.

On a :

$$\chi_M = \det(XI_n - M) = \det\left((XI_n - M)^\top\right) = \det\left(XI_n - M^\top\right) = \chi_{M^\top}$$

donc, pour tout $\lambda \in \mathbf{K}$,

$$\begin{aligned} \lambda \in \operatorname{sp}(M) &\Leftrightarrow \chi_M(\lambda) = 0 \\ &\Leftrightarrow \chi_{M^\top}(\lambda) = 0 \\ &\Leftrightarrow \lambda \in \operatorname{sp}\left(M^\top\right) \end{aligned}$$

Ainsi $\operatorname{sp}(M) = \operatorname{sp}\left(M^\top\right)$. ■

Q2. — Montrer que $M^\top$ est diagonalisable si et seulement si M est diagonalisable.

$\Longrightarrow$. On suppose que M est diagonalisable, ce qui nous fournit $P \in GL_n(\mathbf{K})$ et $D \in \mathcal{M}_n(\mathbf{K})$ 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.

$\Longleftarrow$. On suppose que $M^\top$ est diagonalisable. Pour montrer que M est diagonalisable, on utilise l'implication précédente en remarquant que $M = \left(M^\top\right)^\top$. ■

Q3. — Soit $(a_0, a_1, \dots, a_{n-1}) \in \mathbf{K}^n$ et $Q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. On considère la matrice

$$C_Q = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \dots & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & & \vdots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & -a_{n-2} \\ 0 & \dots & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Déterminer en fonction de Q le polynôme caractéristique de C_Q.

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 $C_Q = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \in \mathcal{M}_2(\mathbf{K})$. On a $\chi_{C_Q} = X^2 - \operatorname{tr} C_Q)X + \det(C_Q) = X^2 + a_1X + a_0$ ce qui prouve l'initialisation.

Hérédité. Soit un 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 $a_i \in \mathbf{K}$. On a en développant par rapport à la première ligne :

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

On 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 $\geqslant 2$. ■

Q4. — Soit λ une valeur propre de $C_Q^\top$. Déterminer la dimension et une base du sous-espace propre associé.

On a $\left(C_Q\right)^\top = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & & 0 & 1 \\ -a_0 & -a_1 & \dots & & -a_{n-1} \end{pmatrix}$ et $\chi_{C_Q^\top} = \chi_{C_Q} = Q$. Ainsi $Q(\lambda) = 0$.

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

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

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

Ainsi :

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

Comme λ est racine de Q, alors $\dim\left(E_\lambda\left(C_Q^\top\right)\right) = 1$ et $E_\lambda\left(C_Q^\top\right) = \operatorname{vect}\left(X_\lambda := \begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}\right)$. ■

II — Endomorphismes cycliques

Q5. — Montrer que f est cyclique si et seulement s'il existe une base $\mathscr{B}$ de E dans laquelle la matrice de f est de la forme C_Q, où Q est un polynôme unitaire de degré n.

$\Longrightarrow$. On suppose que f est cyclique. Ceci nous fournit $x_0 \in E$ tel que $\mathscr{B} = \left(x_0, f(x_0), \ldots, f^{n-1}(x_0)\right)$ soit une base de E Il existe alors $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in \mathbf{K}^n$ tel que :

$$f^n(x_0) = \sum_{i=0}^{n-1} \lambda_i \cdot f^i(x_0).$$

On pose alors $Q = X^n + \sum_{i=0}^{n-1} (-\lambda_i) X^i \in \mathbf{K}[X]$ de sorte que Q est unitaire de degré n et $\operatorname{Mat}_{\mathscr{B}}(f) = C_Q$.

$\Longleftarrow$. On suppose qu'il existe une base $\mathscr{B} = (e_0, e_1, \ldots e_{n-1})$ 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 $i \in [\![0, n-2]\!]$, $f(e_i) = e_{i+1}$. Donc $(e_0, f(e_0), f^2(e_0), \ldots, f^{n-1}(e_0))$ est une base de E et f est cyclique. ■

Q6. — Soit f un endomorphisme cyclique. Montrer que f est diagonalisable si et seulement si χ_f est scindé sur $\mathbf{K}$ et a toutes ses racines simples.

$\Longleftarrow$. On suppose que χ_f est scindé sur $\mathbf{K}$ et a toutes ses racines simples. Ainsi :

$$|\text{sp}(f)| = \deg(\chi_f) = \dim E$$

et f est diagonalisable d'après le cours.

$\Longrightarrow$. On suppose que f est diagonalisable. Comme f est cyclique, ceci nous fournit $\mathscr{B}$ une base de E et $Q \in \mathbf{K}[X]$ unitaire de degré n tel que $\text{Mat}_{\mathscr{B}}(f) = C_Q$ d'après 5. Ainsi C_Q est diagonalisable et il en est de même pour $C_Q^\top$ d'après 2. Ainsi :

$$\mathbf{K}^n = \bigoplus_{\lambda \in \text{sp}(f)} E_\lambda\left(C_Q^\top\right)$$

d'où :

$$n = \sum_{\lambda \in \text{sp}\left(C_Q^\top\right)} \dim\left(E_\lambda\left(C_Q^\top\right)\right)$$

or on a, pour tout $\lambda \in \text{sp}\left(C_Q^\top\right)$, $\dim\left(E_\lambda\left(C_Q^\top\right)\right) = 1$ d'après 4 donc :

$$\left|\text{sp}\left(C_Q^\top\right)\right| = n$$

Or d'après 1 :

$$\text{sp}\left(C_Q^\top\right) = \text{sp}\left(C_Q\right) = \text{sp}\left(f\right)$$

donc f admet n valeurs propres distinctes dans $\mathbf{K}$. Par suite, χ_f est scindé sur $\mathbf{K}$ et a toutes ses racines simples.
■

Q7. — Montrer que si f est cyclique, alors $(\text{Id}, f, f^2, \ldots, f^{n-1})$ est libre dans $\mathscr{L}(E)$ et le polynôme minimal de f est de degré n.

On suppose que f est cyclique.

Liberté de $(\text{Id}, f, f^2, \ldots, f^{n-1})$. Soit $(\lambda_0, \ldots, \lambda_{n-1}) \in \mathbf{K}^n$ tel que :

$$\sum_{i=0}^{n} \lambda_i \cdot f^i = 0_{\mathbf{L}(E)}.$$

Montrons que, pour tout $i \in [\![0, n-1]\!]$, $\lambda_i = 0$.
Comme f est cyclique, il existe $x \in E$ tel que $\mathscr{B} = (x, f(x), \ldots, f^{n-1}(x))$ soit une base de E donc :

$$\sum_{i=0}^{n} \lambda_i \cdot f^i(x) = 0_{\mathbf{L}(E)}(x) = 0_E.$$

Ainsi, pour tout $i \in [\![0, n-1]\!]$, $\lambda_i = 0$ car $\mathscr{B}$ est libre.

Polynôme minimal de f. On note d le degré de π_f. D'après le cours on a $d = \dim\left(\mathbf{K}[f]\right)$. Or $(\text{Id}, f, f^2, \ldots, f^{n-1})$ est libre dans $\mathbf{K}[f]$ 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 $n = d$.

N.B. : Le résultat de cette question ne sera heureusement pas appliqué dans la partie suivante.

■

III — Application à une démonstration du théorème de Cayley-Hamilton

Q8. — Soit x un vecteur non nul de E. Montrer qu'il existe un entier p strictement positif tel que la famille :

$$(x, f(x), f^2(x), \ldots, f^{p-1}(x))$$

soit libre et qu'il existe $(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \in \mathbf{K}^p$ tel que :

$$\alpha_0 \cdot x + \alpha_1 \cdot f(x) + \cdots + \alpha_{p-1} \cdot f^{p-1}(x) + f^p(x) = 0.$$

On note :

$$N_x = \left\{ m \in \mathbf{N}^* \ : \ \left(f^i(x)\right)_{0 \leqslant i \leqslant m-1} \text{ libre} \right\}.$$

On sait que $1 \in N_x$ car $x \neq 0_E$ et que, pour tout $m \geqslant n$, $m \notin N_x$ car $\dim E = n$. Ainsi N_x est une partie de $\mathbf{N}^*$ non vide majorée par $n-1$, donc N_x admet un plus grand élément $p \in \mathbf{N}^*$ (bon ordre). 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, d'où l'existence de $(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \in \mathbf{K}^p$ tel que :

$$\alpha_0 \cdot x + \alpha_1 \cdot f(x) + \cdots + \alpha_{p-1} \cdot f^{p-1}(x) + f^p(x) = 0.$$

■

Q9. — Justifier que $\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$ est stable par f.

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 :

$$f^p(x) = -\alpha_0 \cdot x - \alpha_1 \cdot f(x) + \cdots - \alpha_{p-1} \cdot f^{p-1}(x) \in \mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$$

d'où :

$$f\left(\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))\right) \subset \mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x)).$$

■

Q10. — Montrer que $X^p + \alpha_{p-1}X^{p-1} + \cdots + \alpha_0$ divise le polynôme χ_f.

On note alors $\tilde{f}$ l'endomorphisme induit par f sur $\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$. D'après ce qui précède :

$$\mathscr{B} = \left(x, f(x), f^2(x), \ldots, f^{p-1}(x)\right)$$

est une base de $\mathrm{Vect}(x, f(x), f^2(x), \ldots, f^{p-1}(x))$. On remarque que :

$$\mathrm{Mat}_{\mathscr{B}}\left(\tilde{f}\right) = C_Q$$

où $Q = \alpha_0 + \alpha_1 X + \cdots + \alpha_{p-1}X^{p-1} + X^p$. Ainsi $\chi_{\tilde{f}} = Q$. On conclut avec $\chi_{\tilde{f}} \mid \chi_f$, car $\tilde{f}$ est induit par f. ■

Q11. — Démontrer que $\chi_f(f)$ est l'endomorphisme nul.

En reprenant les notations précédentes, on a $Q(f)(x) = 0$ et il existe $P \in \mathbf{K}[X]$ 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, pour tout $x \in E$, $\chi(f)(x) = 0$. Par suite $\chi(f) = 0_{\mathscr{L}(E)}$. ■

IV — Endomorphismes cycliques nilpotents

Dans cette sous-partie, on suppose que f est un endomorphisme nilpotent de E. On note r le plus petit entier naturel tel que $f^r = 0$.

Q12. — Montrer que f est cyclique si et seulement si $r = n$. Préciser alors la matrice compagnon.

$\Longrightarrow$. 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 $\pi_f \mid \chi_f$ selon Cayley-Hamilton et π_f est unitaire par définition. Donc $\pi_f = X^n$. On en déduit $f^n = 0$ et, pour tout $i \in [\![0, n-1]\!]$, $f^i \neq 0$. D'où $r = n$.

$\Longleftarrow$. 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 $\lambda_0, \dots, \lambda_{n-1} \in \mathbf{K}$ tels que :

$$\sum_{i=0}^{n-1} \lambda_i f^i(x) = 0.$$

On montre que, pour tout $i \in [\![0, n-1]\!]$, $\lambda_i = 0$. On suppose, par l'absurde, que la propriété est fausse et on note alors j le minimum de :

$$\{i \in [\![0, n-1]\!] \,:\, \lambda_i \neq 0\}.$$

Ainsi :

$$0 = f^{n-1-j}\left(\sum_{i=0}^{n-1} \lambda_i \cdot f^i(x)\right) = f^{n-1-j}\left(\sum_{i=j}^{n-1} \lambda_i \cdot f^i(x)\right) = \lambda_j \cdot f^{n-1}(x) + \sum_{i=j}^{n-1} \lambda_i \cdot f^{n-1+i-j}(x)$$

Or, pour tout $i \geqslant p$, $f^i(x) = 0$ donc $\lambda_j \cdot f^{n-1}(x) = 0$ et $\lambda_j \neq 0$. D'où $f^{n-1}(x) = 0$ ce qui est absurde. Ainsi $(x, f(x), \dots, f^{n-1}(x))$ est une famille libre composée de n vecteurs de E et $\dim E = n$. Donc $(x, f(x), \dots, f^{n-1}(x))$ est une base de E et f est cyclique.

Matrice compagnon. Supposons f cyclique et considérons $x \in E$ tel que $f^{n-1}(x) \neq 0$. La matrice de f dans la base $(x, f(x), \dots, f^{n-1}(x))$ de E est :

$$C_{X^n} = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 & 0 \\ 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \ddots & & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \end{pmatrix}.$$

■

V — Un critère de cyclicité

Dans cette partie on suppose $\mathbf{K} = \mathbf{C}$. On suppose que $(Id, f, f^2, \dots, f^{n-1})$ est libre et on se propose de montrer que f est cyclique. On factorise le polynôme caractéristique de f sous la forme

$$\chi_f(X) = \prod_{k=1}^{p} (X - \lambda_k)^{m_k}$$

où les λ_k sont les p valeurs propres deux à deux distinctes de f et les m_k de $\mathbf{N}^*$ leurs ordres de multiplicité respectifs.

Pour $k \in [\![1, p]\!]$, on pose $F_k = \ker\big((f - \lambda_k \cdot Id_E)^{m_k}\big)$.

Q13. — Montrer que les sous-espaces vectoriels F_k sont stables et que $E = F_1 \oplus \dots \oplus F_p$.

Stabilité des F_k. Pour $k \in [\![1, p]\!]$, $(f - \lambda_k \cdot \mathrm{Id}_E)^{m_k}$ et f commutent car $\mathbf{C}[f]$ est une algèbre commutative. Donc $F_k = \ker((f - \lambda_k \cdot \mathrm{Id}_E)^{m_k})$ est stable par f.

Décomposition de E en somme directe des F_k. On a $\chi_f(X) = \prod_{k=1}^{p} (X - \lambda_k)^{m_k}$ 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 :

$$\ker\big(\chi(f)\big) = \ker((f - \lambda_1 \cdot \mathrm{Id}_E)^{m_1}) \oplus \dots \oplus \ker((f - \lambda_p \cdot \mathrm{Id}_E)^{m_p}) = F_1 \oplus \dots \oplus F_p.$$

De plus, selon Cayley-Hamilton, $\chi_f(f) = 0$ et donc $\ker\big(\chi(f)\big) = E$. Il vient $E = F_1 \oplus \dots \oplus F_p$. ■

Pour $k \in [\![1, p]\!]$, on note φ_k l'endomorphisme induit par $f - \lambda_k \cdot Id$ sur le sous-espace vectoriel F_k :

$$\varphi_k \left| \begin{array}{ccc} F_k & \longrightarrow & F_k \\ x & \longmapsto & f(x) - \lambda_k \cdot x. \end{array} \right.$$

Q14. — Justifier que φ_k est un endomorphisme nilpotent de F_k.

Soit $x \in F_k$. On a $(f - \lambda_k \cdot \mathrm{Id})^{m_k}(x) = 0$. Pour tout $y \in F_k$, on a $(f - \lambda_k \mathrm{Id})(y) = \varphi_k(y) \in F_k$. Ainsi pour tout $p \in \mathbf{N}$:

$$(f - \lambda_k \mathrm{Id})^p(x) = \varphi_k^p(x) \qquad [\text{récurrence immédiate sur } p]$$

donc $\varphi_k^{m_k}(x) = 0$. Comme c'est vrai pour tout $x \in F_k$, on conclut que φ_k est un endomorphisme nilpotent de F_k. ■

On note ν_k le plus petit entier naturel tel que $\varphi_k^{\nu_k} = 0$.

Q15. — Pourquoi a-t-on $\nu_k \leqslant \dim(F_k)$?

D'après le cours, l'indice de nilpotence de φ_k, endomorphisme de F_k est majoré par $\dim F_k$. Ainci $\nu_k \leqslant \dim(F_k)$. ■

Q16. — Montrer, avec l'hypothèse proposée, que pour tout $k \in [\![1, p]\!]$, on a $\nu_k = m_k$.

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

$$P(f) = \left[\prod_{\substack{i=1 \\ i \neq k}}^{p} (X - \lambda_i)^{\nu_i}(f) \right] \circ (f - \lambda_k \cdot \mathrm{Id})^{\nu_k}$$

donc :

$$P(f)(x) = \left[\prod_{\substack{i=1 \\ i \neq k}}^{p} (X - \lambda_i)^{\nu_i}(f) \right] \left(\varphi_k^{\nu_k}(x) \right) = \left[\prod_{\substack{i=1 \\ i \neq k}}^{p} (X - \lambda_i)^{\nu_i}(f) \right] (0) = 0.$$

Donc $P(f)$ coïncide avec l'endomorphisme nul sur chaque F_k et comme $E = F_1 \oplus \cdots \oplus F_p$ d'après 13, $P(f) = 0$. On note d le degré de P. Comme P est unitaire, $(\mathrm{Id}, f, f^2, \ldots, f^d)$ est liée donc $d \geqslant n$ car $(\mathrm{Id}, f, f^2, \ldots, f^{n-1})$ est libre.
Or

$$d = \sum_{i=0}^{p} \nu_i$$

d'où $n \leqslant \sum_{i=0}^{p} \nu_i$. On remarque, à l'aide de la question 14, que $\nu_k \leqslant m_k$, pour tout $k \in [\![1, p]\!]$.
Donc :

$$n \leqslant \sum_{k=0}^{p} \nu_k \leqslant \sum_{i=0}^{p} m_k = n$$

et les inégalités sont des égalités, i.e., pour tout $k \in [\![1, p]\!]$, on a $\nu_k = m_k$. ■

Q17. — Expliciter la dimension de F_k pour $k \in [\![1, p]\!]$, puis en déduire l'existence d'une base $\mathscr{B} = (u_1, \ldots, u_n)$ de E

dans laquelle f a une matrice diagonale par blocs, ces blocs appartenant à $\mathcal{M}_{m_k}(\mathbf{C})$ et étant de la forme :

$$\begin{pmatrix} \lambda_k & 0 & \dots & \dots & \dots & 0 \\ 1 & \lambda_k & \ddots & & & \vdots \\ 0 & 1 & \lambda_k & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \lambda_k & 0 \\ 0 & \dots & \dots & 0 & 1 & \lambda_k \end{pmatrix}.$$

Dimension des F_k. Comme $E = F_1 \oplus \cdots \oplus F_p$ d'après 13 et, pour tout $k \in [\![1,p]\!]$, $\nu_k \leqslant \dim(F_k)$ d'après 15. On a donc avec la question précédente :

$$n = \sum_{k=1}^{p} \nu_k \leqslant \sum_{k=1}^{p} \dim(F_k) = n.$$

Comme à la question précédente, on obtient, pour tout $k \in [\![1,p]\!]$, $\nu_k = m_k = \dim(F_k)$.

Existence d'une base idoine. 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 $\mathscr{B}_k$ de F_k tel que :

$$\mathrm{Mat}_{\mathscr{B}_k}(\varphi_k) = \begin{pmatrix} 0 & 0 & \dots & \dots & \dots & 0 \\ 1 & 0 & \ddots & & & \vdots \\ 0 & 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{m_k}(\mathbf{C}).$$

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

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

En concaténant les bases $\mathscr{B}_k$ pour k allant de 1 à p. On obtient une base $\mathscr{B}$ adaptée à la décomposition en somme directe $E = F_1 \oplus \cdots \oplus F_p$. Ainsi $\mathscr{B} = (u_1, \dots, u_n)$ est une base de E dans laquelle f a une matrice diagonale par blocs de formes voulues.

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

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

puis :

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

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

■

On pose $x_0 = u_1 + u_{m_1+1} + \cdots + u_{m_1+\cdots+m_{p-1}+1}$.

Q18. — Déterminer les polynômes $Q \in \mathbf{C}[X]$ tels que $Q(f)(x_0) = 0$.

Pour $k \in [\![1, p]\!]$, on a $u_{m_1+\cdots+m_{k-1}+1} \in F_k$. Ainsi, pour tout $i \in \mathbf{N}$;

$$f^i(u_{m_1+\cdots+m_{k-1}+1}) \in F_k$$

car F_k stable par f puis, pour tout $P \in \mathbf{C}[X]$, 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 :

$$P(f)(x_0) = \sum_{k=1}^{p} P(f)(u_{m_1+\cdots+m_{k-1}+1})$$

est la décomposition de $P(f)(x_0)$ sur $F_1 \oplus \cdots \oplus F_p$.
Soit $Q \in \mathbf{C}[X]$. On a donc :

$$Q(f)(x_0) = 0 \quad \Longleftrightarrow \quad \forall k \in [\![1, p]\!], \quad Q(f)(e_k) = 0.$$

On note $e_k = u_{m_1+\cdots+m_{k-1}+1}$ et on a :

$$\mathscr{B}_k = \left(e_k, \varphi_k(e_k), \ldots, \varphi_k^{m_k-1}(e_k)\right)$$

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, nilpotent et $\dim(F_k) = m_k$ selon 12.

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

puis :

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

Par ailleurs, on montre facilement que :

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

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.
De plus, $Q(\varphi_k) = 0$ si et seulement si $X^{m_k} \mid Q$ (φ_k nilpotent et cyclique) donc :

$$\begin{aligned} Q(f)(e_k) = 0 \quad &\Longleftrightarrow \quad Q(\varphi_k + \lambda_k \cdot \mathrm{Id}_{F_k})(e_k) = 0 \\ &\Longleftrightarrow \quad X^{m_k} \mid Q(X + \lambda_k) \\ &\Longleftrightarrow \quad (X - \lambda_k)^{m_k} \mid Q(X). \end{aligned}$$

Comme les $(X - \lambda_k)^{m_k}$ sont deux à deux premiers entre eux, on a finalement :

$$Q(f)(x_0) = 0 \quad \Longleftrightarrow \quad \prod_{k=1}^{p} (X - \lambda_k)^{m_k} \mid Q.$$

■

Q19. — Justifier que f est cyclique.

Soit $(\lambda_i)_{0 \leqslant i \leqslant n-1} \in \mathbf{K}^n$ tel que :

$$\sum_{i=0}^{n-1} \lambda_i \cdot f^i(x_0) = 0.$$

On note $Q = \sum_{i=0}^{n-1} \lambda_i X^i$ de sorte que $Q(f)(x_0) = 0$. Ainsi :

$$\prod_{k=1}^{p} (X - \lambda_k)^{m_k} \mid Q$$

d'après la question précédente. Ot

$$\deg(Q) \leqslant n-1 < n = \deg\left(\prod_{k=1}^{p}(X-\lambda_k)^{m_k}\right)$$

donc Q est le polynôme nul et ainsi, pour tout $i \in [\![0, n-1]\!]$, $\lambda_i = 0$. 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. Ceci justifie que f est cyclique. ■

VI — Commutant d'un endomorphisme cyclique

On appelle commutant de f l'ensemble $C(f) = \{g \in \mathscr{L}(E) \,:\, f\circ g = g\circ f\}$.

Q20. — Montrer que $C(f)$ est une sous-algèbre de $\mathscr{L}(E)$.

L'application :

$$\left|\begin{array}{ccc} \mathscr{L}(E) & \longrightarrow & \mathscr{L}(E) \\ g & \longmapsto & f\circ g - g\circ f \end{array}\right.$$

est un endomorphisme de $\mathscr{L}(E)$ dont le noyau est $C(f)$. Ainsi $C(f)$ est un sous-espace vectoriel de $\mathscr{L}(E)$. 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 $\mathrm{Id} \in C(f)$. ■

On suppose que f est cyclique et on choisit un vecteur x_0 dans E tel que $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$ est une base de E. Soit $g \in C(f)$, un endomorphisme qui commute avec f.

Q21. — Justifier l'existence de $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ de $\mathbf{K}$ tels que

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

On a $g(x_0) \in E$ et $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$ est une base de E. D'où l'existence de $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ de $\mathbf{K}$ tels que :

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

■

Q22. — Montrer alors que $g \in \mathbf{K}[f]$.

Il suffit d'établir que les applications linéaires g et $\sum_{k=0}^{n-1} \lambda_k \cdot f^k$ coïncident sur la base $(x_0, f(x_0), \ldots, f^{n-1}(x_0))$. On montre par récurrence immédiate que :

$$\forall i \in \mathbf{N}, \quad g \in C\left(f^i\right).$$

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

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

donc $g = \sum_{k=0}^{n-1} \lambda_k \cdot f^k$. Ainsi $g \in \mathbf{K}[f]$. ■

Q23. — Établir que $g \in C(f)$ si et seulement s'il existe un polynôme $R \in \mathbf{K}_{n-1}[X]$ tel que $g = R(f)$.

On vient d'établir le sens direct (avec un polynôme de degré $\leqslant n-1$). La réciproque vient du fait que $\mathbf{K}[f]$ est une algèbre commutative. ■

VII — Décomposition de Frobenius

On se propose de démontrer le théorème de décomposition de Frobenius : toute matrice est semblable à une matrice diagonale par blocs, ces blocs étant des matrices compagnons.

Q24. — Montrer que si la réunion d'un nombre fini de sous-espaces vectoriels $F_1, \dots, F_r$ de E est un sous-espace vectoriel, alors l'un des sous-espaces F_i contient tous les autres.

On suppose que $G = F_1 \cup \cdots \cup F_r$ est un sous espace de E. Par l'absurde, on suppose qu'aucun des sous-espaces F_i ne contient tous les autres. Ainsi $r \geqslant 2$ et $G \neq \{0\}$.
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 $i \geqslant 2$. Comme, $F_1 \neq G$ 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 $y + \mathbf{K} x_1$ est donc incluse dans $F_2 \cup \cdots \cup F_r$ et contient une infinité d'éléments car $\mathbf{K}$ est infini et :

$$\left|\begin{array}{ccc} \mathbf{K} & \longrightarrow & F_2 \cup \cdots \cup F_r \\ t & \longmapsto & y + t \cdot x_1 \end{array}\right.$$

est injective car $x_1 \neq 0$. Ceci nous fournit $j \in [\![2, r]\!]$ et $\lambda_1 \neq \lambda_2$ dans $\mathbf{K}$ tels que $y + \lambda_1 \cdot x_1 \in F_j$ et $y + \lambda_2 \cdot x_1 \in F_j$. Donc $x_1 \in F_j$ (par combinaison linéaire). Ce qui est absurde.

Cas $r = 2$. Pour $r = 2$, il existe une preuve classique purement algébrique.

Corps finis. Pour le cas général, la preuve doit utiliser le fait que $\mathbf{K}$ est infini. En effet, si je prend $K = \mathbb{F}_2$, $E = \mathbf{K}^2$, $F_1 = \operatorname{Vect}((1,0))$, $F_2 = \operatorname{Vect}((0,1))$ et $F_3 = \operatorname{Vect}((1,1))$. On a $E = F_1 \bigcup F_2 \bigcup F_3$ et pourtant aucun des sous-espaces F_i ne contient tous les autres. ■

On note d le degré de π_f.

Q25. — Justifier l'existence d'un vecteur x_1 de E tel que $(x_1, f(x_1), \dots, f^{d-1}(x_1))$ est libre.
Indication : pour tout x non nul de E, on pourra remarquer que $I_x = \left\{P \in \mathbf{K}[X] \,:\, P(f)(x) = 0\right\}$ est un idéal de $\mathbf{K}[X]$ engendré par un polynôme unitaire $\pi_{f,x}$ diviseur de π_f et considérer les sous-espaces vectoriels $\ker(\pi_{f,x}(f))$.

Soit $x \in E$. On considère l'application :

$$\varphi_x \left|\begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & E \\ P & \longmapsto & P(f)(x). \end{array}\right.$$

Comme :

$$I_x = \left\{P \in \mathbf{K}[X] \,:\, P(f)(x) = 0\right\}$$

est le noyau de l'application linéaire φ_x, I_x un sous-groupe de $(\mathbf{K}[X], +)$. Pour $P \in I_x$ et $Q \in \mathbf{K}[X]$, on a $QP \in I_x$ car :

$$(QP)(f)(x) = \big(Q(f) \circ P(f)\big)(x) = Q(f)\big(P(f)(x)\big) = 0$$

car $Q(f) \in \mathscr{L}(E)$, d'où I_x est un idéal de $\mathbf{K}[X]$. Comme $\pi_f \in I_x$, cet idéal est non réduit à $\{0\}$, ce qui nous fournit $\pi_{f,x} \in \mathbf{K}[X]$ unitaire (donc non nul) tel que :

$$I_x = \pi_{f,x} \mathbf{K}[X] = \left\{\pi_{f,x} P \,:\, P \in \mathbf{K}[X]\right\}.$$

On remarque que :

$$\forall x \in E, \quad \pi_{f,x} \mid \pi_f.$$

Si on écrit $\pi_f = \prod_{k=1}^{N} P_i^{\alpha_i}$ décomposition en facteurs irréductibles, où $N \in \mathbf{N}^*$, les P_i sont irréductibles unitaires et distincts deux-à-deux et enfin les $\alpha_i \in \mathbf{N}^*$.

Alors le nombre de diviseurs unitaires de π_f est $\prod_{k=1}^{N}(\alpha_i+1)$. Ainsi l'ensemble $\{\pi_{f,x} \,:\, x\in E\}$ est fini de cardinal noté r, où $1\leqslant r\leqslant \prod_{k=1}^{N}(\alpha_i+1)$. On peut donc choisir $u_1,\dots u_r\in E$, tel que :

$$\{\pi_{f,x} \,:\, x\in E\} = \{\pi_{f,u_i} \,:\, i\in [\![1,r]\!]\}.$$

Ainsi :

$$E=\bigcup_{i=1}^{r}\ker(\pi_{f,u_i}(f))$$

car, pour tout $x\in E$, $x\in\ker(\pi_{f,x}(f))$. 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 $\pi_{f,x_1}(f)=0_{\mathscr{L}(E)}$ donc $\pi_f\mid\pi_{f,x_1}$. Or $\pi_{f,x_1}\mid\pi_f$ et ce sont des polynômes unitaires donc $\pi_{f,x_1}=\pi_f$.
Finalement :

$$\big(\forall P\in\mathbf{K}[X],\quad P(f)(x_1)=0\big)\quad\Longleftrightarrow\quad \pi_f\mid P$$

en faisant comme en 19, on montre que $(x_1,f(x_1),\dots,f^{d-1}(x_1))$ est libre. ■

On pose $e_1=x_1$, $e_2=f(x_1)$, …, $e_d=f^{d-1}(x_1)$ *et* $E_1=\mathrm{Vect}(e_1,e_2,\dots,e_d)$.

Q26. — Montrer que E_1 est stable par f et que $E_1=\{P(f)(x_1) \,:\, P\in\mathbf{K}[X]\}$.

En faisant comme en 9, on montre que E_1 est stable par f. De plus, on a :

$$E_1=\{P(f)(x_1) \,:\, P\in\mathbf{K}_{d-1}[X]\}\subset\{P(f)(x_1) \,:\, P\in\mathbf{K}[X]\}.$$

Soit $P\in\mathbf{K}[X]$. Comme $\pi_f\neq 0$, le théorème de la division euclidienne nous fournit Q et $R\in\mathbf{K}[X]$ tels que

$$P=Q\pi_f+R\qquad\text{et}\qquad \deg(R)<d=\deg(\pi_f).$$

On a alors :

$$P(f)(x_1)=\big[Q(f)\circ\pi_f(f)\big](x_1)+R(f)(x_1)=R(f)(x_1)\in\{T(f)(x_1) \,:\, T\in\mathbf{K}_{d-1}[X]\}.$$

On conclut que $E_1=\{P(f)(x_1) \,:\, P\in\mathbf{K}[X]\}$. ■

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

$$\psi_1\left|\begin{array}{ccc} E_1 & \longrightarrow & E_1\\ x & \longmapsto & f(x).\end{array}\right.$$

Q27. — Justifier que ψ_1 est cyclique.

D'après ce qui précède $\mathscr{B}=(e_1,e_2,\dots,e_d)$ est une base de E_1. De plus on a :

$$\mathrm{Mat}_{\mathscr{B}}(\psi_1)=C_{\pi_f}$$

qui est la matrice compagnon du π_f polynôme unitaire de degré $d=\dim(E_1)$. D'après 5, ψ_1 est cyclique. ■

On complète, si nécessaire, $(e_1,e_2,\dots,e_d)$ *en une base* $(e_1,e_2,\dots,e_n)$ *de* E*. Soit* Φ *la* d*-ième forme coordonnée qui à tout vecteur* x *de* E *associe sa coordonnée suivant* e_d*. On note :*

$$F=\Big\{x\in E \,:\, \forall\, i\in\mathbf{N},\quad \Phi\Big(f^i(x)\Big)=0\Big\}.$$

Q28. — Montrer que F est stable par f et que E_1 et F sont en somme directe.

Pour $i \in \mathbf{N}$, on note :

$$F_i = \ker\left(\Phi \circ f^i\right)$$

ainsi $F = \bigcap_{i \in \mathbf{N}} F_i$ est bien un sous-espace de E. De plus, on a pour $i \geqslant 1$, $f(F_i) \subset F_{i-1}$ donc :

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

d'où F est stable par f.
Soit $u \in E_1 \cap F$. Comme $u \in E_1$, cela nous fournit $\lambda_1, \ldots, \lambda_d \in \mathbf{K}$ tels que :

$$u = \sum_{k=1}^{d} \lambda_k \cdot e_k$$

or $\Phi(x) = \lambda_d$ et $\Phi(f^0(x)) = 0$ car $u \in F$, donc $\lambda_d = 0$ d'où :

$$u = \sum_{k=1}^{d-1} \lambda_k \cdot e_k$$

puis :

$$f(u) = \sum_{k=1}^{d-1} \lambda_k \cdot e_{k+1}$$

et donc $\lambda_{d-1} = 0$. Ainsi :

$$f(u) = \sum_{k=1}^{d-2} \lambda_k \cdot e_{k+1}.$$

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 E_1 et F sont en somme directe. ■

Soit Ψ l'application linéaire définie par :

$$\Psi \left| \begin{array}{rcl} E & \longrightarrow & \mathbf{K}^d \\ x & \longmapsto & \left(\Phi\left(f^i(x)\right)\right)_{0 \leqslant i \leqslant d-1} = \left(\Phi(x), \Phi(f(x)), \ldots, \Phi\left(f^{d-1}(x)\right)\right). \end{array} \right.$$

Q29. — Montrer que Ψ induit un isomorphisme entre E_1 et $\mathbf{K}^d$.

On note Ψ_1 l'application linéaire induite par Ψ entre E_1 et $\mathbf{K}^d$. Soit $x \in \ker(\Psi_1)$. On a $x \in E_1$ et :

$$\Phi(x) = \Phi(f(x)) = \cdots = \Phi\left(f^{d-1}(x)\right) = 0.$$

En faisant comme à la question précédente, on obtient $x = 0$. L'autre inclusion étant évidente, on a $\ker(\Psi_1) = \{0\}$. Ainsi Ψ_1 est une application linéaire injective entre E_1 et $\mathbf{K}^d$.
Or $\dim(E_1) = d = \dim(\mathbf{K}^d)$. En utilisant le théorème du rang, on obtient que Ψ_1 est surjective puis bijective. ■

Q30. — Montrer que $E = E_1 \oplus F$.

De la question précédente, on déduit que Ψ est surjective de E vers $\mathbf{K}^d$ et que $\ker(\Psi) \bigcap E_1 = \{0\}$. Ainsi :

$$\dim(E_1) = d = \operatorname{rg}(\Psi)$$

et :

$$\dim(E) = \dim(\ker(\Psi)) + \operatorname{rg}(\Psi) = \dim(\ker(\Psi)) + \dim(E_1)$$

donc $E = E_1 \oplus \ker(\Psi)$.

On a $\ker(\Psi) = \bigcap_{i=0}^{d-1} F_i$ (les F_i sont introduits en 28) on a donc $F \subset \ker(\Psi)$.
Soit $x \in \ker(\Psi)$. Montrons que $x \in F$ Soit $i \in \mathbf{N}$. Il suffit d'établir que $\Phi(f^i(x)) = 0$. Le théorème de la division euclidienne nous fournit Q et $R \in \mathbf{K}[X]$ 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 :

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

ainsi $F \supset \ker(\Psi)$ d'où $F = \ker(\Psi)$. On conclut que $E = E_1 \oplus F$. ■

Q31. — En déduire qu'il existe r sous-espaces vectoriels de E, notés $E_1, \ldots, E_r$, tous stables par f, tels que :
(a) $E = E_1 \oplus \cdots \oplus E_r$;
(b) pour tout $1 \leqslant i \leqslant r$, l'endomorphisme ψ_i induit par f sur le sous-espace vectoriel E_i est cyclique;
(c) si on note P_i le polynôme minimal de ψ_i, alors P_{i+1} divise P_i pour tout entier i tel que $1 \leqslant i \leqslant r-1$.

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 :

$$\forall x \in F, \quad \pi_{\psi_1}(f)(x) = 0.$$

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 :

$$\forall x \in G_1, \quad P_1(f)(x) = 0.$$

Hérédité. Soit $k \in \mathbf{N}^*$. On suppose avoir l'existence de k sous-espaces vectoriels de E, notés $E_1, \ldots, E_k$ et G_k tous stables par f, tels que :
(a) $E = E_1 \oplus \cdots \oplus E_k \oplus G_k$;
(b) pour tout $1 \leqslant i \leqslant k$, l'endomorphisme ψ_k induit par f sur le sous-espace vectoriel E_i est cyclique;
(c) si on note P_i le polynôme minimal de ψ_i, alors P_{i+1} divise P_i pour tout entier i tel que $1 \leqslant i \leqslant k-1$;
(d) pour tout $x \in G_k$,$P_k(f)(x) = 0$.

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 :
(a) $E = E_1 \oplus \cdots \oplus E_{k+1} \oplus G_{k+1}$;
(b) l'endomorphisme ψ_{k+1} induit par f sur le sous-espace vectoriel E_{k+1} est cyclique;
(c) si on note P_{k+1} le polynôme minimal de ψ_{k+1}, alors P_{k+1} divise P_k ;
(d) pour tout $x \in G_{k+1}$, $P_{k+1}(f)(x) = 0$.

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

Conclusion. Cette construction algorithmique s'arrête car à chaque étape $\dim(E_k) \leqslant 1$ et donc $r \leqslant \dim(E)$. ■

VIII — Commutant d'un endomorphisme quelconque

Q32. — Montrer que la dimension de $C(f)$ est supérieure ou égale à n.

On reprend les notations de la questions précédente pour la décomposition de Frobenius de f.
On note Λ l'application définie par :

$$\Lambda \left| \begin{array}{ccc} \mathscr{L}(E_1)\times\cdots\times\mathscr{L}(E_r) & \longrightarrow & \mathscr{L}(E) \\ (g_1,\ldots,g_r) & \longmapsto & \Lambda(g_1,\ldots,g_r) \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & g_1(x_1)+\cdots g_r(x_r) \text{ où } x=\sum_{k=1}^{r} x_k \text{ et les } x_k\in E_k. \end{array}\right. \end{array}\right.$$

Ainsi définie, Λ est linéaire de $\mathscr{L}(E_1)\times\cdots\times\mathscr{L}(E_r)$ à valeurs dans $\mathscr{L}(E)$. 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 $C(\psi_i)=\operatorname{Vect}\left(\psi_i^0,\psi_i^1,\ldots,\psi_i^{n_i-1}\right)$ d'après 23. Comme ψ_i est cyclique alors $\left(\psi_i^0,\psi_i^1,\ldots,\psi_i^{n_i-1}\right)$ est libre d'après 7. Donc :

$$\dim\left(C(\psi_i)\right)=n_i=\dim(E_i)$$

d'où

$$\dim\left(C(\psi_1)\right)+\cdots+\dim\left(C(\psi_r)\right)=\dim(E_1)+\cdots+\dim(E_r)=\dim(E_1\oplus\cdots\oplus E_r)=\dim(E)=n.$$

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

Q33. — On suppose que f est un endomorphisme tel que l'algèbre $C(f)$ est égale à $\mathbf{K}[f]$. Montrer que f est cyclique.

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