Corrigé : endomorphismes cycliques (ENTPE MP 1996)

Partie I. Matrice compagne d'un endomorphisme cyclique

Question 1. Supposons f cyclique, et considérons une base (e) définie par $e_k = f^{k-1}(x_0)$.

$f(e_n) = f^n(x_0)$ est un vecteur de E donc se décompose dans la base (e) : on pose $-f^n(x_0) = \sum_{k=0}^{n-1} a_k f^k(x_0) = \sum_{k=1}^{n} a_{k-1}e_k$, et ainsi $\mathrm{Mat}_{(e)}(f) = \mathrm{C}$.

Réciproquement, supposons l'existence d'une base (e) telle que $\mathrm{Mat}_{(e)}(f) = \mathrm{C}$. Alors pour tout $k \in [\![1, n-1]\!]$, $f(e_k) = e_{k+1}$ donc en posant $x_0 = e_1$ on a $e_k = f^{k-1}(x_0)$ pour $k \in [\![1, n]\!]$ et ainsi f est un endomorphisme cyclique.

Question 2. En développant suivant la première ligne on obtient :

$$\chi_{\mathrm{C}}(x) = \begin{vmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & \ddots & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & x & a_{n-2} \\ 0 & \cdots & 0 & -1 & x + a_{n-1} \end{vmatrix} = x\chi_{\mathrm{C}'}(x) + a_0$$

où C' désigne la matrice C amputée de sa première ligne et sa première colonne. Cette matrice C' est une matrice compagne de $\mathcal{M}_{n-1}(\mathbb{K})$, et on établit alors par récurrence que $\chi_{\mathrm{C}}(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$.

Le polynôme caractéristique étant un invariant de similitude on en déduit l'unicité de la matrice compagne associée à un endomorphisme cyclique.

Question 3. Soit $\lambda \in \mathrm{Sp}(\mathrm{C})$. Il est facile d'observer que la matrice $\mathrm{C} - \lambda \mathrm{I}_n$ est de rang $n-1$ car ses $n-1$ premières colonnes sont à l'évidence linéairement indépendantes. On en déduit que le sous-espace propre associé à la valeur propre λ est de dimension 1.

Soit X un vecteur propre associé à la valeur propre λ. Si on note $(x_1, \dots, x_n)$ ses coordonnées dans la base canonique de $\mathcal{M}_{n,1}(\mathbb{K})$ nous avons à résoudre le système $\mathrm{CX} = \lambda\mathrm{X}$. Les $n-1$ dernières lignes de ce système fournissent les relations :

$$x_k = \left(\lambda^{n-k} + a_{n-1}\lambda^{n-1-k} + \cdots + a_{k+1}\lambda + a_k\right)x_n, \qquad 1 \leqslant k \leqslant n-1$$

et la première équation $a_0 x_n + \lambda x_1 = 0$ s'écrit alors : $\chi_{\mathrm{C}}(\lambda)x_n = 0$, égalité toujours vraie puisque $\chi_{\mathrm{C}}(\lambda) = 0$.

On retrouve bien le fait que le sous-espace propre est de dimension 1, engendré par le vecteur $\mathrm{X} \in \mathcal{M}_{n,1}(\mathbb{K})$ défini par $x_n = 1$ et $x_k = \lambda^{n-k} + a_{n-1}\lambda^{n-1-k} + \cdots + a_{k+1}\lambda + a_k$ pour tout $k \in [\![1, n-1]\!]$.

Partie II. Endomorphismes nilpotents

Question 4. Soit $x_0 \in \mathrm{E}$ tel que $f^{n-1}(x_0) \neq 0_{\mathrm{E}}$. Supposons la famille $\left(x_0, f(x_0), \dots, f^{n-1}(x_0)\right)$ liée : il existe des scalaires non tous nuls $\lambda_0, \dots, \lambda_{n-1}$ tels que $\sum_{k=0}^{n-1} \lambda_k f^k(x_0) = 0_{\mathrm{E}}$.

Notons j le plus petit indice vérifiant $\lambda_j \neq 0$. En composant la relation $\sum_{k=j}^{n-1} \lambda_k f^k(x_0) = 0_{\mathrm{E}}$ par f^{n-1-j} on obtient $\lambda_j f^{n-1}(x_0) = 0_{\mathrm{E}}$, ce qui est absurde puisque $\lambda_j \neq 0$ et $f^{n-1}(x_0) \neq 0_{\mathrm{E}}$.

On en déduit que la famille $\left(x_0, f(x_0), \dots, f^{n-1}(x_0)\right)$ est libre, donc est une base puisque de cardinal n. Ainsi, f est bien un endomorphisme cyclique, et puisque $f^n(x_0) = 0$ sa matrice compagne est la matrice

$$\begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

D'après la question 2 on a $\chi_f(x) = x^n$, et d'après la question 3, $\dim(\operatorname{Ker} f) = 1$.

Question 5.

a) Si $x \in \mathrm{N}_k$ alors $f^k(x) = 0_\mathrm{E}$ donc $f^{k+1}(x) = f(0_\mathrm{E}) = 0_\mathrm{E}$ et $x \in \mathrm{N}_{k+1}$. On a donc $\mathrm{N}_k \subset \mathrm{N}_{k+1}$.
Si $x \in \mathrm{N}_{k+1}$ alors $f^{k+1}(x) = 0_\mathrm{E}$, soit aussi $f^k(f(x)) = 0_\mathrm{E}$. Ceci montre que $f(x) \in \mathrm{N}_k$, donc $f(\mathrm{N}_{k+1}) \subset \mathrm{N}_k$.

b) On a $\operatorname{Ker}\phi = \mathrm{N}_1 \cap \mathrm{N}_{k+1} \subset \mathrm{N}_1$ donc $\dim(\operatorname{Ker}\phi) \leqslant 1$, et $\operatorname{Im}\phi \subset \mathrm{N}_k$ donc $\dim(\operatorname{Im}\phi) \leqslant n_k$.
D'après le théorème du rang appliqué à ϕ, $\dim \mathrm{N}_{k+1} = \dim(\operatorname{Ker}\phi) + \dim(\operatorname{Im}\phi)$ donc $n_{k+1} \leqslant 1 + n_k$.

c) Supposons $n_k = n_{k+1}$ et montrons par récurrence sur $j \geqslant k$ que $\mathrm{N}_j = \mathrm{N}_k$.

- Si $j = k$ c'est immédiat.
- Si $j \geqslant k+1$, supposons $\mathrm{N}_{j-1} = \mathrm{N}_k$ et considérons $x \in \mathrm{N}_j$. On a $f(x) \in \mathrm{N}_{j-1}$ donc par hypothèse de récurrence, $f(x) \in \mathrm{N}_k$, et $x \in \mathrm{N}_{k+1}$.
  Mais $n_k = n_{k+1}$ et $\mathrm{N}_k \subset \mathrm{N}_{k+1}$ donc $\mathrm{N}_{k+1} = \mathrm{N}_k$, ce qui montre que $x \in \mathrm{N}_k$, puis que $\mathrm{N}_j \subset \mathrm{N}_k$. L'inclusion réciproque est évidente car $j \geqslant k$, donc $\mathrm{N}_j = \mathrm{N}_k$: la récurrence se propage.

L'inégalité obtenue à la question 5.b montre que pour tout $k \in [\![1, p]\!]$, $n_k \leqslant k$. Mais $n_p = n$ puisque $f^p = 0$, donc $p \geqslant n$.
La suite finie $n_1, n_2, \dots, n_p$ est une suite croissante de $[\![1, n]\!]$ donc si on avait $p > n$ il existerait (d'après le principe des tiroirs) $k \in [\![0, p-1]\!]$ tel que $n_k = n_{k+1}$. D'après la question précédente on aurait $\mathrm{N}_k = \mathrm{N}_p = \mathrm{E}$ donc $f^k = 0$, ce qui impliquerait $f^{p-1} = 0$, ce qui ne se peut. On en déduit que $p = n$, puis pour les mêmes raisons que $n_k = k$ pour tout $k \in [\![1, n]\!]$.

Partie III. Une caractérisation des endomorphismes cycliques

Question 6. Supposons $(\mathrm{Id}_\mathrm{E}, f, f^2, \dots, f^{n-1})$ liée : il existe des scalaires non tous nuls $\lambda_0, \dots, \lambda_{n-1}$ tels que $\displaystyle\sum_{k=0}^{n-1} \lambda_k f^k = 0$.
Appliquée au vecteur x_0 cette égalité donnerait $\displaystyle\sum_{k=0}^{n-1} \lambda_k f^k(x_0) = 0_\mathrm{E}$ et prouverait que la famille $\big(x_0, f(x_0), \dots, f^{n-1}(x_0)\big)$ est liée, ce qui ne se peut. On en déduit que la famille $(\mathrm{Id}_\mathrm{E}, f, f^2, \dots, f^{n-1})$ est libre.

Question 7.

a) les endomorphismes f et $(f - \lambda_k \mathrm{Id}_\mathrm{E})^{m_k}$ commutent donc E_k est stable par f.

b) Pour tout $x \in \mathrm{E}_k$, $(f - \lambda \mathrm{Id}_\mathrm{E})^{m_k}(x) = 0_\mathrm{E}$ donc $\phi^{m_k} = 0$.
ϕ_k est un endomorphisme nilpotent donc $\operatorname{Sp}(\phi_k) = \{0\}$. En notant $f_k : \mathrm{E}_k \to \mathrm{E}_k$ la restriction de f à E_k on en déduit que $\operatorname{Sp}(f_k) = \{\lambda_k\}$, et que le polynôme caractéristique de f_k est $(\mathrm{X} - \lambda_k)^{\dim \mathrm{E}_k}$.
Puisque $\mathrm{E} = \mathrm{E}_1 \oplus \cdots \oplus \mathrm{E}_p$ est une décomposition de l'espace en sous-espaces stables, le polynôme caractéristique de f est $\chi_f(\mathrm{X}) = \displaystyle\prod_{k=1}^{p} (\mathrm{X} - \lambda_k)^{\dim \mathrm{E}_k}$. Par unicité de la factorisation d'un polynôme on en déduit que pour tout $k \in [\![1, p]\!]$, $\dim \mathrm{E}_k = m_k$.
Si on avait $\phi_k^{m_k - 1} = 0$, le polynôme $\displaystyle\prod_{j=1}^{p} (\mathrm{X} - \lambda_j)^{m'_j}$ avec $m'_j = \begin{cases} m_j & \text{si } j \neq k \\ m_k - 1 & \text{si } j = k \end{cases}$ annulerait f. Mais ce polynôme est de degré $n-1$, et en développant on obtiendrait une relation de dépendance linéaire liant la famille $(\mathrm{Id}_\mathrm{E}, f, \dots, f^{n-1})$, ce qui ne ce peut. On a donc $\phi^{m_k - 1} \neq 0$.

c) D'après la question 4, il existe une base (b_k) de E_k pour laquelle :

$$\operatorname{Mat}_{(b_k)}(\phi_k) = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \qquad \text{et donc} \qquad \operatorname{Mat}_{(b_k)}(f_k) = \begin{pmatrix} \lambda_k & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda_k \end{pmatrix}$$

En concaténant ces bases (b_k) on obtient une base (b) de E dans laquelle la matrice associée à f est diagonale par blocs, ces blocs étant les matrices ci-dessus.

d) Soit C la matrice compagne de χ_f, (e) une base quelconque de E et g l'endomorphisme de E défini par $\operatorname{Mat}_{(e)}(g) = \mathrm{C}$.
D'après la question 2, $\chi_g = \chi_f = \displaystyle\prod_{k=1}^{p} (\mathrm{X} - \lambda_k)^{m_k}$. De plus, d'après la question 6, la famille $(\mathrm{Id}, g, g^2, \dots, g^{n-1})$ est libre donc on peut appliquer la question 7 à l'endomorphisme g : il existe une base (b') pour laquelle $\operatorname{Mat}_{(b')}(g) = \operatorname{Mat}_{(b)}(f)$.
Ceci a pour conséquence l'existence d'une base (e') pour laquelle $\operatorname{Mat}_{(e')}(f) = \mathrm{C}$ et ainsi, d'après la question 1, f est cyclique.

Question 8.

a) L'application $P : x \mapsto \det(Q_1 + xQ_2)$ est une application polynomiale de $\mathbb{R}[X]$, qui n'est pas le polynôme nul puisque $P(i) \neq 0$. Elle n'a donc qu'un nombre fini de racines réelles, et il existe $\lambda \in \mathbb{R}$ tel que $Q_1 + \lambda Q_2$ soit inversible.
Par ailleurs, l'égalité $AQ = QB$ implique, en séparant partie réelle et partie imaginaire, que $AQ_1 = Q_1B$ et $AQ_2 = Q_2B$ donc $A(Q_1 + \lambda Q_2) = (Q_1 + \lambda Q_2)B$ avec $Q_1 + \lambda Q_2 \in \mathcal{GL}_n(\mathbb{R})$, ce qui prouve que A et B sont semblables dans $\mathcal{M}_n(\mathbb{R})$.

b) Soit (e) une base quelconque de E, et $A = \mathrm{Mat}_{(e)}(f)$. La famille $(I_n, A, A^2, \dots, A^{n-1})$ est par hypothèse libre dans $\mathcal{M}_n(\mathbb{R})$, mais elle l'est aussi dans $\mathcal{M}_n(\mathbb{C})$: en effet, s'il existe $(\lambda_0, \dots, \lambda_{n-1}) \in \mathbb{C}^n$ tel que $\sum_{k=0}^{n-1} \lambda_k A^k = 0$ alors, en posant $\alpha_k = \mathfrak{Re}\,\lambda_k$ et $\beta_k = \mathrm{Im}\,\lambda_k$ et en séparant partie réelle et imaginaire on obtient $\sum_{k=0}^{n-1} \alpha_k A^k = 0$ et $\sum_{k=0}^{n-1} \beta_k A^k = 0$. La liberté dans $\mathcal{M}_n(\mathbb{R})$ de la famille $(I_n, A, \dots, A^{n-1})$ permet d'en déduire que $\alpha_k = \beta_k = 0$, donc que $\lambda_k = 0$.
La question 7 peut donc s'appliquer à l'endomorphisme $X \mapsto AX$ de $\mathbb{C}^n$, ce qui prouve que les matrices A et C, matrice compagne de χ_A, sont semblables dans $\mathcal{M}_n(\mathbb{C})$.
Puisque χ_A est un polynôme réel les matrices A et C sont à coefficients réels, et la question 8a prouve alors qu'elles sont semblables dans $\mathcal{M}_n(\mathbb{R})$, autrement dit que f est cyclique (d'après la question 1).

Partie IV. Une autre caractérisation des endomorphismes cycliques

Question 9.

a) Puisque $g(x_0) \in E$ il existe des scalaires α_k tels que $g(x_0) = \sum_{k=0}^{n-1} \alpha_k f^k(x_0)$.
Posons $h = \sum_{k=0}^{n-1} \alpha_k f^k$; nous allons montrer que les endomorphismes g et h coïncident sur la base $\big(x_0, f(x_0), \dots, f^{n-1}(x_0)\big)$ donc sont égaux :

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

et ceci car g et h commutent tous deux avec f donc avec f^k.

b) Supposons $g \in \mathscr{C}(f)$. D'après la question précédente, il existe un polynôme $R \in \mathbb{K}_{n-1}[X]$ tel que $g = R(f)$.
Réciproquement, si $g = R(f)$ il est évident que g commute avec f donc $g \in \mathscr{C}(f)$, et l'égalité $g(x_0) = R(f)(x_0)$ montre que les coefficients de R sont les coordonnées de $g(x_0)$ dans la base $\big(x_0, f(x_0), \dots, f^{n-1}(x_0)\big)$ donc sont uniques.

Question 10. Si f est cyclique, la question précédente montre que $\mathscr{C}(f) \subset \mathbb{K}_{n-1}[f] \subset \mathbb{K}[f]$. L'inclusion réciproque est évidente, donc $\mathscr{C}(f) = \mathbb{K}[f]$.

Réciproquement, supposons $\mathscr{C}(f) = \mathbb{K}[f]$. Pour montrer que f est cyclique, nous allons montrer que la famille $(\mathrm{Id}, f, \dots, f^{n-1})$ est libre.
Notons p le plus grand entier pour lequel la famille $(\mathrm{Id}_E, f, \dots, f^{p-1})$ est libre. La famille $(\mathrm{Id}_E, f, \dots, f^p)$ est liée donc il existe des scalaires non tous nuls $\alpha_0, \dots, \alpha_p$ tels que $\sum_{k=0}^{p} \alpha_k f^k = 0$. En posant $M = \sum_{k=0}^{p} \alpha_k X^k$ on obtient un polynôme non nul M de degré p tel que $M(f) = 0$.

Considérons maintenant un polynôme quelconque $P \in \mathbb{K}[X]$ et réalisons la division euclidienne de P par M : $P = MQ + R$ avec $\deg R \leqslant p - 1$. Alors $P(f) = M(f)Q(f) + R(f) = R(f)$.
Puisque $\deg R \leqslant p - 1$ ceci prouve que $\mathbb{K}[f] = \mathrm{Vect}(\mathrm{Id}, f, \dots, f^{p-1})$ et donc que $\dim \mathbb{K}[f] = \dim \mathscr{C}(f) = p$.
Nous avons admis que $\dim \mathscr{C}(f) \geqslant n$, donc $p \geqslant n$. La famille $(\mathrm{Id}_E, f, \dots, f^{n-1})$ est donc extraite de la famille $(\mathrm{Id}_E, f, \dots, f^{p-1})$, et donc libre par voie de conséquence. La partie III a prouvé dans ce cas que f est un endomorphisme cyclique.

Partie V. Cycles

Question 11.

a) Pour tout $k \in [\![0, p-1]\!]$, $f^p\big(f^k(x_0)\big) = f^k\big(f^p(x_0)\big) = f^k(x_0)$. Les endomorphismes f^p et Id_E coïncident sur une famille génératrice donc sont égaux.

b) On a $x_0 \neq 0_E$ (sinon la famille ne pourrait être génératrice) donc $1 \in \mathscr{E}$, et toute famille libre est de cardinal inférieur ou égal à n donc $\mathscr{E} \subset [\![1, n]\!]$. L'ensemble $\mathscr{E}$ est donc non vide et majoré : il possède un élément maximal m.

c) La famille $\left(x_0, f(x_0), \dots, f^m(x_0)\right)$ est liée donc il existe des scalaires $\lambda_0, \dots, \lambda_m$ non tous nuls tels que $\sum_{j=0}^{m} \lambda_j f^j(x_0) = 0_{\mathrm{E}}$. Posons $\mathrm{M} = \sum_{k=0}^{m} \lambda_k \mathrm{X}^k$; on a $\mathrm{M}(f)(x_0) = 0_{\mathrm{E}}$.

Considérons la division euclidienne de X^m par M : $\mathrm{X}^m = \mathrm{MQ} + \mathrm{R}$ avec $\deg \mathrm{R} \leqslant m-1$. On a $f^k = \mathrm{Q}(f) \circ \mathrm{M}(f) + \mathrm{R}(f)$ donc $f^k(x_0) = \mathrm{Q}(f)(\mathrm{M}(f)(x_0)) + \mathrm{R}(f)(x_0) = \mathrm{Q}(f)(0_{\mathrm{E}}) + \mathrm{R}(f)(x_0) = \mathrm{R}(f)(x_0)$ et puisque $\deg \mathrm{R} \leqslant m-1$ on a $f^k(x_0) = \mathrm{M}(f)(x_0) \in \mathrm{Vect}\left(x_0, f(x_0), \dots, f^{m-1}(x_0)\right)$.

Ceci montre que la famille $\left(x_0, f(x_0), \dots, f^{m-1}(x_0)\right)$ est génératrice ; mais par définition de m elle est aussi libre. C'est donc une base, et f est cyclique.

Question 12.

a) Puisque $f^n = \mathrm{Id}_{\mathrm{E}}$ (question 11a) on a avec les notations de la partie I : $f^n(x_0) = x_0$ et donc

$$\mathrm{C} = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & \vdots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

b) On a $\mathrm{CU}_k = \begin{pmatrix} \overline{\omega}^{nk} \\ \overline{\omega}^{k} \\ \vdots \\ \overline{\omega}^{(n-1)k} \end{pmatrix} = \omega^k \mathrm{U}_k$ donc U_k est vecteur propre de C pour la valeur propre ω^k.

Question 13. On a $(\mathrm{M}\overline{\mathrm{M}})_{ij} = \sum_{k=1}^{n} m_{ik}\overline{m}_{kj} = \sum_{k=1}^{n} \overline{\omega}^{ik}\omega^{kj} = \sum_{k=1}^{n} \omega^{k(j-i)}$.

Si $i = j$ on a donc $(\mathrm{M}\overline{\mathrm{M}})_{ii} = \sum_{k=1}^{n} 1 = n$ et si $i \neq j$, $(\mathrm{M}\overline{\mathrm{M}})_{ij} = \omega^{j-i}\dfrac{\omega^{n(j-i)}-1}{\omega^{j-i}-1} = 0$ car $\omega^n = 1$.

Nous avons prouvé que $\mathrm{M}\overline{\mathrm{M}} = n\mathrm{I}_n$ donc M est inversible et $\mathrm{M}^{-1} = \dfrac{1}{n}\overline{\mathrm{M}}$.

Question 14. Il est facile de montrer que $\mathrm{A} = \sum_{k=0}^{n-1} a_k \mathrm{C}^k = \mathrm{P}(\mathrm{C})$, où P désigne le polynôme $\mathrm{P} = \sum_{k=0}^{n-1} a_k \mathrm{X}^k$.

La question 12b montre que M est une matrice dont les colonnes forment une base de vecteurs propres de C : on a $\mathrm{C} = \mathrm{M}\begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega^n \end{pmatrix}\mathrm{M}^{-1}$ et donc $\mathrm{C}^k = \mathrm{M}\begin{pmatrix} \omega^k & & \\ & \ddots & \\ & & \omega^{nk} \end{pmatrix}\mathrm{M}^{-1}$.

Par linéarité on en déduit qua $\mathrm{A} = \mathrm{M}\begin{pmatrix} \mathrm{P}(\omega) & & \\ & \ddots & \\ & & \mathrm{P}(\omega^n) \end{pmatrix}\mathrm{M}^{-1}$. La matrice A est diagonalisable, $\mathrm{Sp}(\mathrm{A}) = \left\{\mathrm{P}(\omega), \mathrm{P}(\omega^2), \dots, \mathrm{P}(\omega^n)\right\}$ et $(\mathrm{U}_1, \dots, \mathrm{U}_n)$ forme une base de vecteurs propres de A.