MINISTÈRE DE L'ÉQUIPEMENT, DU LOGEMENT, DES TRANSPORTES ET DU TOURISME

CONCOURS COMMUN 1996
ENTPE, ENSG, ENTM, ENSTIMD
Banque de notes pour le concours EIVP

COMPOSITION DE MATHÉMATIQUES OPTION
Temps accordé : 4 heures
4 pages

Un corrigé

PREMIÈRE PARTIE : Matrice compagne d'un endomorphisme cyclique

1. Si f est cyclique, il existe un vecteur x_0 tel que la famille $\mathscr{B} = (x_0, f(x_0), ..., f^{n-1}(x_0))$ soit une base de E. Notons $(-a_0, ..., -a_{n-1})$ les coordonnées du vecteur $f^n(x_0) = f(f^{n-1}(x_0))$ dans la base $\mathscr{B}$. Dans cette base, la matrice de f est la matrice C.
Réciproquement, si $\mathscr{B} = (e_1, ..., e_n)$ est une base de E dans laquelle la matrice de f est C, posons $x_0 = e_1$. Pour $i \in [\![2, n]\!]$, on a $e_i = f(e_{i-1})$ et donc, pour $i \in [\![1, n-1]\!]$, $e_i = f^{i-1}(e_1) = f^{i-1}(x_0)$. La famille $(x_0, f(x_0), ..., f^{n-1}(x_0))$ est donc une base de E et f est cyclique.
f est cyclique si et seulement si il existe une $\mathscr{B}$ base de E telle que $Mat_{\mathscr{B}}(f) = C$.

2. Montrons par récurrence sur n que $P_C(X) = (-1)^n \left(X^n + \sum_{k=0}^{n-1} a_k X^k\right)$.

Pour $n = 1$, c'est évident : $P_C(X) = -(a_0 + X)$. Supposons le résultat vrai au rang $n-1$, montrons le au rang n. En développant par rapport à la première ligne, on a

$$P_C(X) = \begin{vmatrix} -X & 0 & \cdots & 0 & -a_0 \\ 1 & -X & & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & -X & -a_{n-2} \\ 0 & 0 & \cdots & 1 & -a_{n-1} - X \end{vmatrix} =$$

$$-X \begin{vmatrix} -X & 0 & \cdots & 0 & -a_1 \\ 1 & -X & & 0 & -a_2 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & -X & -a_{n-2} \\ 0 & 0 & \cdots & 1 & -a_{n-1} - X \end{vmatrix} - (-1)^{n+1} a_0 \begin{vmatrix} 1 & -X & \cdots & 0 \\ 0 & 1 & & 0 \\ 0 & & \ddots & \vdots \\ \vdots & \vdots & & -X \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

et donc d'après l'hypothèse de récurrence

$$P_C(X) = (-1)^n X(X^{n-1} + a_{n-1}X^{n-2} + ... + a_1) + (-1)^n a_0 = (-1)^n (X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0) = (-1)^n Q(X).$$

D'après le calcul précédent, les coefficients de la dernière colonne de la matrice C sont uniquement déterminés à partir des coefficients du polynôme caractéristique de f. La matrice compagne associée à un endomorphisme cyclique est unique.

3. Soit λ une valeur propre complexe de la matrice C, donc $\dim(\ker(C - \lambda I_n)) \geq 1$. La matrice constituée par les $n-1$ premières colonnes et $n-1$ dernières lignes de la matrice $C - \lambda I_n$ est inversible car de déterminant 1. La matrice $C - \lambda I_n$ est donc de rang $n-1$ au moins ou encore $dim(\ker(C - \lambda I_n)) \leq 1$. On a donc $\dim(\ker(C - \lambda I_n)) = 1$. Donc les sous-espaces propres de la matrice C sont donc des droites vectorielles.
Déterminons alors les sous-espaces propres de C. Soient λ une valeur propre complexe de la matrice C et $X = (x_i)_{(1 \leq i \leq n)} \in \mathscr{M}_{n,1}(\mathbb{C})$. Le système $AX = \lambda X$ est équivalent à

$$\begin{cases} x_{n-1} = (a_{n-1} + \lambda) x_n \\ x_{n-2} = a_{n-2} x_n + \lambda x_{n-1} = (a_{n-2} + a_{n-1}\lambda + \lambda^2) x_n \\ x_{n-3} = a_{n-3} x_n + \lambda(a_{n-2} + a_{n-1}\lambda + \lambda^2) x_n \\ \quad = (a_{n-3} + a_{n-2}\lambda + a_{n-1}\lambda^2 + \lambda^3) x_n \\ \cdots \\ x_1 = (a_1 + a_2\lambda + ... + a_{n-1}\lambda^{n-2} + \lambda^{n-1}) x_n \end{cases}$$

ce qui montre que $\ker(C-\lambda I_n)$ est la droite vectorielle engendrée par le vecteur

$$(a_1+a_2\lambda+...+a_{n-1}\lambda^{n-2}+\lambda^{n-1},...,a_{n-2}+a_{n-1}\lambda+\lambda^2,a_{n-1}+\lambda,1).$$

DEUXIÈME PARTIE : Endomorphismes nilpotents

4. Soit x_0 un vecteur tel que $f^{n-1}(x_0)\neq 0$. Vérifions que la famille $(x_0,f(x_0),...,f^{n-1}(x_0))$ est une base de E. Puisque $\mathrm{card}(f^i(x_0))_{0\leq i\leq n-1}=n=\dim(E)<+\infty$, il suffit de vérifier que la famille $(f^i(x_0))_{0\leq i\leq n-1}$ est libre.

Supposons par l'absurde qu'il existe $(a_0,...,a_{n-1})\neq(0,0,...,0)$ tel que

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

Soit $k=\min\{\, i\in[\![0,n-1]\!] \mid a_i\neq 0\,\}$. On a alors

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

$$\Rightarrow\sum_{i=k}^{n-1}a_if^{n+i-k-1}(x_0)=0\Rightarrow a_kf^{n-1}(x_0)=0$$

(car pour $i=k+1$, $n+i-k-1=n$ et donc $f^{n+i-k-1}(x_0)=0$) D'où $a_k=0$ (car $f^{n-1}(x_0)\neq 0$).

Ceci contredit la définition de k. La famille $(x_0,f(x_0),...,f^{n-1}(x_0))$ est donc une base de E et f est cyclique.

Si f est nilpotent d'indice n, alors f est cyclique. Puisque $f(\ f^{n-1}(x_0))=0$, la matrice de f dans la base $(x_0,f(x_0),...,f^{n-1}(x_0))$ est

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

qui est une matrice compagne et donc la matrice compagne de f. D'après la question 3), $\ker f$ est de dimension au plus 1. Mais f étant nilpotent, f n'est pas inversible et donc $\dim(\ker f)=1$.

5. (a) Soient $x\in E$ et $k\in[\![0,p-1]\!]$. $x\in N_k\Rightarrow f^k(x)=0\Rightarrow f(f^k(x))=0\Rightarrow f^{k+1}(x)=0\Rightarrow x\in N_{k+1}$. Donc, $\forall k\in[\![0,p-1]\!]$, $N_k\subset N_{k+1}$.
Soient $k\in[\![0,p-1]\!]$ et $y\in f(N_{k+1})$. Il existe $x\in N_{k+1}$ tel que $y=f(x)$. Mais alors $f^k(y)=f^k(f(x))=f^{k+1}(x)=0$ et donc $y\in N_k$. Ainsi $\forall k\in[\![0,p-1]\!]$, $f(N_{k+1})\subset N_k$.

(b) D'après la question a), φ est bien une application de N_{k+1} dans N_k, linéaire car f l'est. Le théorème du rang permet alors d'écrire

$$\begin{aligned}n_{k+1}&=\dim(N_{k+1})=\dim(\ker\varphi)+\dim(Im\varphi) &(1)\\&=\dim(\ker f\cap N_{k+1})+\dim(f(N_{k+1}))=\dim(\ker f)+\dim(f(N_{k+1}))\ \ (car\ \ker f=N_1\subset N_{k+1}) &(2)\\&=\dim(\ker f)+\dim(N_k) &(3)\\&=1+n_k(d'aprs4)). &(4)\end{aligned}$$

D'où $\forall k\in[\![0,p-1]\!]$, $n_{k+1}\leq n_k+1$.

(c) Si $n_k=n_{k+1}$ alors, puisque $N_k\subset N_{k+1}$ (d'après 5)a)), on a $N_k=N_{k+1}$.
Soit $j=k+1$. Supposons que $N_j=N_k$ et montrons que $N_{j+1}=N_k$. On a déjà $N_k=N_j\subset N_{j+1}$. Mais pour $x\in E$, $x\in N_{j+1}\Rightarrow f^{j+1}(x)=0\Rightarrow f^j(f(x))=0\Rightarrow f(x)\in N_j=N_k\longleftrightarrow f^k(f(x))=0\Rightarrow x\in N_{k+1}=N_k$. et donc, $N_{j+1}=N_k$.
On a montré par récurrence que $\forall j\geq k+1$, $N_j=N_k$.

Si $n_k = n_{k+1}$ alors $\forall j \geq k+1$, $N_j = N_k$. On a $n_p = \dim(\ker f^p) = n$ et $\forall k \in [\![0, p-1]\!]$, $n_k = n_{k+1} = 1+n_k$. Par suite, $n_{k+1} = n_k$ ou $n_{k+1} = n_k + 1$.
Maintenant, puisque $f^{p-1} \neq 0 = f^p$, $N_{p-1} \neq N_p$ et le début de la question montre que $\forall k \in [\![0, p-1]\!]$, $n_{k+1} = n_k + 1$.
Par suite, $\forall k \in [\![1, p]\!]$, $n_k = n_1 + (k-1) = k$ ce qui reste vrai pour $k = 0$. En particulier, $p = np = n$. On a montré que $p = n$ et $\forall k \in [\![0, n]\!]$, $n_k = k$.

TROISIÈME PARTIE : Une caractérisation des endomorphismes cycliques

6. f est cyclique donc il existe un vecteur x_0 tel que la famille $(x_0, f(x_0), ..., f^{n-1}(x_0))$ soit une base de E. Soit $(a_0, ..., a_{n-1}) \in \mathbb{C}^n$. $a_0 Id + a_1 f + ... + a_{n-1} f^{n-1} = 0 \Rightarrow \forall x \in E, a_0 x + a_1 f(x) + ... + a_{n-1} f^{n-1}(x) = 0 \Rightarrow a_0 x_0 + a_1 f(x_0) + ... + a_{n-1} f^{n-1}(x_0) = 0 \Rightarrow a_0 = a_1 = ... = a_{n-1} = 0$ (car la famille $(x_0, f(x_0), ..., f^{n-1}(x_0))$ est libre). Donc, si f est un endomorphisme cyclique, la famille $(Id, f, ..., f^{n-1})$ est libre.

7. (a) $(f - \lambda_k I)^{m_k}$ est un polynôme en f et donc commute avec f. On sait alors que $E_k = \ker(f - \lambda_k I)^{m_k}$ est stable par f.
Les polynômes $(X - \lambda_k)^{m_k}$ sont deux à deux premiers entre eux. D'après le théorème de décomposition des noyaux,

$$\ker(P_f(f)) = E1 \oplus ... \oplus E_p.$$

Mais d'après le théorème de Cayley-Hamilton, $P_f(f) = 0$ et donc $\ker(P_f(f)) = E$. Finalement,

$$\forall k \in [\![1, p]\!], \ \ f(E_k) \subset E_k \text{ et } E = E_1 \oplus ... \oplus E_p.$$

(b) Puisque f laisse stable E_k, φ_k est bien un endomorphisme de E_k. Par définition de E_k, on a pour tout vecteur x élément de E_k, $(f - \varphi_k I)^{m_k}(x) = 0$ ou encore $\varphi_k^{m_k}(x) = 0$. D'où

$$\varphi_k^{m_k} = 0.$$

Notons f_k la restriction de f à E_k (on a donc $f_k = \varphi_k Id_{E_k} + \varphi_k$). Puisque le polynôme $(X - \lambda_k)^{m_k}$ est annulateur de f_k, λ_k est l'unique valeur propre de f_k (f_k admettant au moins une valeur propre puisque $\mathbb{K} = \mathbb{C}$ et que $E_k \neq \{0\}$). Par suite, le polynôme caractéristique de f_k est $(X - \lambda_k)^{dim(E_k)}$. On sait alors que ce polynôme divise le polynôme caractéristique de f ce qui montre que $\dim(E_k) = m_k$.
Maintenant, si pour un entier $k \in [\![1, p]\!]$ on a $\dim(E_k) < m_k$, alors $\displaystyle\sum_{j=1}^{p} \dim(E_j) < \sum_{j=1}^{n} m_j = n$, ce qui contredit le fait que $E = E_1 \oplus ... \oplus E_p$. Finalement,

$$\forall k \in [\![1, p]\!], \ \ \dim(E_k) = m_k.$$

Montrons que $\varphi_k^{m_k - 1} \neq 0$. Supposons par l'absurde que $\varphi^{m_k - 1} = 0$ et considérons le polynôme $Q = (X - \lambda_k)^{m_k - 1} \displaystyle\prod_{j \neq k} (X - \lambda_j)^{m_j}$ si $p = 2$ ou $Q = (X - \lambda_k)^{m_k - 1} = (X - \lambda_1)^{n-1}$ si $p = 1$.
Pour $i \in [\![1, p]\!]$, on a $Q(f_i) = 0$ (des polynômes en f commutent) et donc $Q(f) = 0$. Mais Q est un polynôme non nul de degré $(m_{k-1}) + \displaystyle\sum_{j \neq k} m_j = \sum_{j=1}^{p} m_j - 1 = n - 1$. L'égalité $Q(f) = 0$ fournit alors une combinaison linéaire nulle à coefficients non tous nuls de la famille $(Id, f, f^2, ..., f^{n-1})$ ce qui contredit la liberté de cette famille. Donc $\varphi_k^{m_k - 1} \neq 0$.

(c) φ_k est donc un endomorphisme nilpotent de E_k, d'indice $m_k = \dim E_k$. D'après la question 4), il existe une base B_k de E_k dans laquelle la matrice de φ_k est la matrice compagnon de format m_k

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

ou encore dans laquelle la matrice de f_k est

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

Soit $B = B_1 \cup ... \cup B_k$. D'après la question 7)a), $E = E_1 \oplus ... \oplus E_p$ et donc B est une base de E et la matrice de f dans cette base a la forme désirée.

(d) Il s'agit de vérifier que la matrice précédente est semblable à une matrice compagne qui ne peut être, d'après la question 2), que la matrice compagne de P_f.
Soit donc C la matrice compagne de P_f et g l'endomorphisme de matrice C dans une base donnée de E. Le polynôme caractéristique de g est celui de f à savoir $\prod_{k=1}^{p}(X-\lambda_k)^{m_k}$ et d'autre part, g est cyclique d'après la question 1).
D'après la question 6), la famille $(Id, g, ..., g^{n-1})$ est libre et d 'après la question 7), il existe une base de E dans laquelle la matrice de g est la matrice diagonale par blocs du 7). C est donc semblable à cette matrice ce qui montre que f est cyclique. si $(Id, f, ..., f^{n-1})$ est une famille libre, f est cyclique.

8. (a) $\det(Q_1 + \lambda Q_2)$ est un polynôme en λ, non nul car $\det(Q_1 + iQ_2) = \det Q \neq 0$ et admet donc un nombre fini de racines. $\mathbb{R}$ étant infini, il existe au moins un réel λ_0 tel que $\det(Q_1 + \lambda_0 Q_2) \neq 0$ ou encore tel que la matrice $P = Q_1 + \lambda_0 Q_2$ soit une matrice réelle inversible.

$$\{ \lambda \in \mathbb{R} \mid Q_1 + \lambda Q_2 \in \mathbf{G}\,\mathbf{L}_n(\mathbb{R}) \} \neq \varnothing.$$

Maintenant, en posant $P = Q_1 + \lambda_0 Q_2$,

$$\begin{aligned} A = QBQ^{-1} &\Rightarrow AQ = QB \Rightarrow AQ_1 + iAQ_2 = Q_1B + iQ_2B && (5)\\ &\Rightarrow AQ_1 = Q_1B \text{ et } AQ_2 = Q_2B(\text{ identification des parties réelles et imaginaires }) && (6)\\ &\Rightarrow A(Q_1 + \lambda_0 Q_2) = (Q_1 + \lambda_0 Q_2)B && (7)\\ &\Rightarrow AP = PB \Rightarrow A = PBP^{-1} && (8) \end{aligned}$$

D'où A et B sont semblables dans $\mathscr{M}_n(\mathbb{R})$.

(b) Soit A la matrice de f dans une base donnée de E. D'après la question 7), A est semblable dans C à une matrice compagne. Mais A est réelle, et donc cette matrice compagne est réelle. Ces deux matrices réelles sont semblables dans $\mathscr{M}_n(\mathbb{C})$ et donc, d'après la question a), dans $\mathscr{M}_n(\mathbb{R})$. Par suite, il existe une base de E dans laquelle la matrice de f est une matrice compagne. D'après la question 1), f est cyclique. Conclusion : si $\mathbb{K} = C$ ou $\mathbb{K} = \mathbb{R}$, f est cyclique si et seulement si la famille $(Id, f, ..., f^{n-1})$ est libre.

QUATRIÈME PARTIE : Une autre caractérisation des endomorphismes cycliques

9. (a) Soit $g \in C(f)$. Puisque la famille $(x_0, f(x_0), ..., f^{n-1}(x_0))$ est une base de E, on peut poser

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

Posons encore

$$h = \sum_{k=1}^{n-1} a_k f^k$$

de sorte que l'on a déjà $g(x_0) = h(x_0)$. Plus généralement, pour $j \in [\![0, n-1]\!]$, $g(f^j(x_0)) = f^j(g(x_0))$ (puisque g est dans $C(f)$)

$$= f^j(h(x_0)) = h(f^j(x_0))$$

(puisque h est un polynôme en f et donc commute avec f^j).
Ainsi, les endomorphismes g et h coïncident sur une base de E et donc sont égaux. Par suite, $g \in \mathbb{K}[f]$.
En résumé, $C(f) \subset \mathbb{K}[f]$. Comme on a toujours $\mathbb{K}[f] \subset C(f)$, on a montré que si f est cyclique, $C(f) = \mathbb{K}[f]$.

(b) Soit $g \in \mathscr{L}(E)$. S'il existe $R \in \mathbb{K}_{n-1}[X]$ tel que $g = R(f)$ alors g est dans $C(f)$.
Réciproquement, si g est dans $C(f)$, d'après la question a), il existe un polynôme $P \in \mathbb{K}[X]$ tel que $g = P(f)$. La division euclidienne de P par P_f fournit un polynôme Q et un polynôme R de degré au plus $n-1$ tels que $P = QP_f + R$. Par suite,

$$g = P(f) = Q(f)_circP_0(f) + R(f) = R(f)$$

d'après le théorème de Cayley-Hamilton. g est donc bien de la forme $R(f)$ où R est un polynôme de degré au plus $n-1$.

$$C(f) = \mathbb{K}_{n-1}[f].$$

10. Supposons f non cyclique. D'après la question 7), la famille $(Id, f, ..., f^{n-1})$ est liée et, en écrivant une relation de dépendance, on voit qu'il existe un entier $p \in [\![0, n-1]\!]$ tel que $f^p \in \mathrm{Vect}(Id, f, ..., f^{p-1})$.
Mais alors, par récurrence, pour $k \geq p$, $f^k \in \mathrm{Vect}(Id, f, ..., f^{p-1})$ (en effet, si pour $k \geq p$, $f^k \in \mathrm{Vect}(Id, f, ..., f^{p-1})$ alors $f^{k+1} \in \mathrm{Vect}(f, ..., f^p) \subset \mathrm{Vect}(Id, f, ..., f^{p-1})$). Par suite, $C(f) = \mathbb{K}[f] = \mathrm{Vect}(f^k)_{k\in\mathbb{N}} = \mathrm{Vect}(Id, f, ..., f^{p-1})$ et en particulier, $\dim(\mathbb{K}[f]) = p < n$. Ceci contredit le résultat admis dans le préambule de l'énoncé à savoir $\dim(C(f)) = n$. On a montré que si $C(f) = \mathbb{K}[f]$ alors f est cyclique. Finalement, f est cyclique si et seulement si $C(f) = \mathbb{K}[f]$.

CINQUIÈME PARTIE : Cycles

11. (a) Pour $k \in [\![0, p-1]\!]$, $f^p(f^k(x_0)) = f^k(f^p(x_0)) = f^k(x_0) = I(f^k(x_0))$. Par suite, les endomorphismes f^p et I coïncident sur une famille génératrice de E et donc $f^p = I$.

(b) $\mathscr{E}$ est un sous-ensemble de $\mathbb{N}$, non vide (car x_0 est nécessairement non nul de sorte que $k = 1$ est dans $\mathscr{E}$) et majoré par n (car le cardinal d'une famille libre de E est majoré par la dimension de E). E admet donc un plus grand élément que l'on note m.

(c) Par définition de m, la famille $(x_0, f(x_0), ..., f^{m-1}(x_0))$ est libre et la famille $(x_0, f(x_0), ..., f^m(x_0))$ est liée. Par suite,

$$f^m(x_0) \in \mathrm{Vect}(x_0, f(x_0), ..., f^{m-1}(x_0)).$$

De plus, si pour $k \geq m$, $f^k(x_0) \in \mathrm{Vect}(x_0, f(x_0), ..., f^{m-1}(x_0))$ alors

$$f^{k+1}(x_0) \in \mathrm{Vect}(f(x_0), ..., f^m(x_0)) \in \mathrm{Vect}(x_0, f(x_0), ..., f^{m-1}(x_0)).$$

On a montré par récurrence que $\forall k \geq m$, $f^k(x_0) \in \mathrm{Vect}(x_0, f(x_0), ..., f^{m-1}(x_0))$.
La famille $(x_0, f(x_0), ..., f^{m-1}(x_0))$ est déjà libre dans E. Vérifions que cette famille est génératrice de E. On a déjà $m \leq n \leq p$ (car la famille $(x_0, f(x_0), ..., f^{m-1}(x_0))$ est libre dans E et la famille $(x_0, f(x_0), ..., f^{p-1}(x_0))$ est génératrice de E). De plus, pour $k \geq m$, $f^k(x_0) \in \mathrm{Vect}(x_0, f(x_0), ..., f^{m-1}(x_0))$.
Donc, $E = \mathrm{Vect}(x_0, f(x_0), ..., f^{p-1}(x_0)) = \mathrm{Vect}(x_0, f(x_0), ..., f^{m-1}(x_0))$ et la famille $\left(x_0, f(x_0), ..., f^{m-1}(x_0)\right)$ est une base de E. On en déduit que $m = n$ et que f est cyclique.
Le polynôme $X^p - 1$ est annulateur de f, non nul à racines simples dans $\mathbb{C}$ (car sans racine commune avec sa dérivée pX^{p-1}). Donc, f est diagonalisable. Par suite, l'ordre de multiplicité de chacune de ses valeurs propres est exactement la dimension du sous-espace propre associé. Mais, f étant cyclique, les sous-espaces propres de f sont d'après la question 3) de dimension 1. Finalement, f admet n valeurs propres simples ou encore n valeurs propres deux à deux distinctes. Notons que ces valeurs propres sont à choisir parmi les racines du polynôme $X^p - 1$ et sont donc des racines p-ièmes de l'unité. f admet n valeurs propres deux à deux distinctes.

12. Si $p = n$, la matrice de f dans la base $(x_0, f(x_0), ..., f^{n-1}(x_0))$ est

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

C est une matrice compagne et donc la matrice compagne de f. Soit alors $k \in [\![1, n]\!]$.

$$CU_k = \begin{pmatrix} \overline{w}^{nk} \\ \overline{w}^{k} \\ \vdots \\ \overline{w}^{k(n-1)} \end{pmatrix} = \frac{1}{\overline{w}^k} \begin{pmatrix} \overline{w}^{nk} \\ \overline{w}^{k} \\ \vdots \\ \overline{w}^{k(n-1)} \end{pmatrix} = w^k U_k.$$

13. Le coefficient ligne k, colonne l de la matrice $M\overline{M}$ vaut

$$\sum_{j=1}^{n} \overline{w}^{kj} w^{jl} = \sum_{j=1}^{n} w^{-kj} w^{jl} = \sum_{j=1}^{n} \left(w^{(l-k)}\right)^j$$

Maintenant, $w^{l-k} = 1 \Leftrightarrow l - k \in n\mathbb{Z}$. Mais, puisque $1 \leq k \leq n$ et $1 \leq l \leq n$, on a $-(n-1) \leq l - k \leq n - 1$. Mais alors, le seul multiple de n compris entre $-(n-1)$ et $n-1$ étant 0, $w^{l-k} = 1 \Leftrightarrow k = l$. On a donc deux cas :

• Premier cas. Si $k = l$,

$$\sum_{j=1}^{n} \overline{w}^{kj} w^{jl} = n.$$

• Deuxième cas. Si $k \neq l$,

$$\sum_{j=1}^{n} \overline{w}^{kj} w^{jl} = 0$$

Ainsi, le coefficient ligne k, colonne l de la matrice $M\overline{M}$ vaut $n\delta_{k,l}$. On en déduit que $M\overline{M} = nI_n$ ou encore que M est inversible et

$$M^{-1} = \frac{1}{n}\overline{M}$$

14. On note que $A = a_0 I_n + a_1 C + a_2 C^2 + \dots + a_{n-1} C^{n-1} = Q(C)$ où $Q = a_0 + a_1 X + \dots + a_{n-1} X^{n-1}$. D'après les questions 11)c) et 12), f (ou C) a n valeurs propres deux à deux distinctes à savoir les w^k, $1 \leq k \leq n$, une base de vecteurs propres associée étant $(U_1, \dots, U_n)$ et est donc diagonalisable. La matrice dans la base canonique de $\mathscr{M}_{n,1}(\mathbb{C})$ de la famille $(U_1, \dots, U_n)$ étant M, on a plus précisément $C = MDM^{-1}$ où $D = \operatorname{diag}(1, w, w^2, \dots, w^{n-1})$. Mais alors,

$$A = Q(C) = MQ(D)M^{-1} = M \operatorname{diag}(Q(1), Q(w), Q(w^2), \dots, Q(w^{n-1}))M^{-1}.$$

Ainsi, A est diagonalisable, $\operatorname{Sp}(A) = \left\{ Q(1), Q(w), Q(w^2), \dots, Q(w^{n-1}) \right\}$ où $Q = a_0 + a_1 X + \dots + a_{n-1} X^{n-1}$ et une base de vecteurs propres de A est $(U_1, U_2, \dots, U_n)$.

• • • • • • • • •