ENSAI - Session 2000

ÉPREUVE DE MATHÉMATIQUE I - ALGÈBRE - 4 heures

$$f \text{ cyclique} \iff \exists p \in \mathbf{N}^*,\ \exists a \in E \ / \ \begin{cases} \text{les vecteurs } a, f(a), \ldots, f^{p-1}(a) \text{ sont 2 à 2 distincts,} \\ C_a^p = \{a, f(a), \ldots, f^{p-1}(a)\} \text{ engendre } E, \\ f(C_a^p) \subset C_a^p. \end{cases}$$

Remarque : la dernière condition équivaut à : $\exists\, j \in [\![0; p-1]\!] \ / \ f^p(a) = f^j(a)$.

PARTIE I

1. Comme $h^2(a) = h(a)$ et les éléments de C_a^p sont distincts, nécessairement $1 \leq n \leq p \leq 2$.

- Si $n = 1$, alors h est soit l'application nulle ($\mathrm{Im}\, h = \{0\}$), soit l'application identique ($\mathrm{Im}\, h = E$). Seule l'identité est cyclique, d'ordre 1 et un cycle est $\{a\}$ avec $a \in E$ et $a \neq 0$.

- Si $n = 2$, alors $p = 2$ et pour que $\{a, h(a)\}$ soit un cycle, il faut et il suffit que $\big(a, h(a)\big)$ soit une base de E
(car $h^2(a) = h(a)$).
Dans le cas où h est l'application nulle ou l'application identique, h ne vérifie pas cette condition.
Le cas où $\dim(\mathrm{Im}\, h) = 1$, c'est à dire h est un projecteur sur une droite, alors h est cyclique d'ordre 2 et $\forall\, a \in E \setminus \big(\mathrm{Im}\, h \cup \mathrm{Ker} h\big)$, $C_a^2 = \{a, h(a)\}$ est un cycle de h.

2.a. On a $\forall\, k \in [\![1; n-1]\!]$, $f(e_k) = e_{k+1}$, d'où l'on déduit facilement que $f^k(e_1) = e_{k+1}$ pour $k = 1...n-1$.
$C_{e_1}^n = \{e_1, e_2, \ldots, e_n\}$ est une partie génératrice de E formée d'éléments distincts.
De plus $f^n(e_1) = f^{n-1}(e_1) \in C_{e_1}^n$, donc f est cyclique d'ordre n et $C_{e_1}^n$ est un cycle de f.

Comme $f(e_{n-1}) = f(e_n) = e_n$, f n'est pas injective, donc $\dim(\mathrm{Ker} f) \geq 1$, d'où d'après le théorème du rang, $\mathrm{rg}(f) \leq n-1$. D'autre part, les $n-1$ premières colonnes sont linéairement indépendantes de façon évidente, d'où $\mathrm{rg}(f) \geq n-1$.

Finalement, $\mathrm{rg}(f) = n-1$ et $\dim(\mathrm{Ker} f) = 1$.

A étant triangulaire inférieure, on lit ses valeurs propres sur la diagonale : ce sont 0 d'ordre $n-1$ et 1 d'ordre 1 lorsque $n \geq 2$ (la valeur de A pour $n = 1$ étant imprécise).
On sait que le sous-espace propre relatif à la valeur propre simple 1 est nécessairemant de dimension 1.
Ainsi, f est diagonalisable si et seulement si $\mathrm{Ker} f$ est de dimension $n-1$, c'est à dire $n = 2$.

b. Posons $a = \sum_{i=1}^{n} e_i$. On a $g(a) = -\sum_{i=1}^{n} g(e_i) = -(e_2 + \cdots + e_n) + a = e_1$, $g^2(a) = e_2$, $\ldots$, $g^n(a) = e_n$.
Ainsi $C_a^{n+1} = \{a, g(a) \ldots, g^n(a)\} = \{a, e_1, e_2, \ldots, e_n\}$ est une partie génératrice de E formée d'éléments distincts.
De plus, $g^{n+1}(a) = g\big(g^n(a)\big) = g(e_n) = -a$, donc C_a^{n+1} est un cycle de g et g est cyclique d'ordre $n+1$.
On ne change pas le rang d'un système de vecteurs en les permutant. En considérant les vecteurs colonnes de B, on voit que $\mathrm{rg}(B) = \mathrm{rg}\{a, e_2, \ldots, e_n\} = n$ (matrice triangulaire).
Le calcul classique du polynôme caractérististique de B (matrice Compagnon) donne :

$$P_f = \begin{vmatrix} X & 0 & \ldots & 0 & 1 \\ -1 & \ddots & \ddots & \vdots & \vdots \\ & \ddots & \ddots & 0 & 1 \\ & (0) & \ddots & X & 1 \\ & & & -1 & 1+X \end{vmatrix} = \begin{vmatrix} 0 & 0 & \ldots & 0 & Q \\ -1 & \ddots & \ddots & \vdots & \vdots \\ & \ddots & \ddots & 0 & 1 \\ & (0) & \ddots & X & 1 \\ & & & -1 & 1+X \end{vmatrix}$$

(en effectuant $L_1 \longleftarrow L_1 + \sum_{i=2}^{n} X^{i-1} L_i$)

avec $Q = 1 + X + \cdots + X^{n-2} + X^{n-1}(1+X)$.

En développant ce dernier déterminant par rapport aux éléments de la première ligne, on obtient :

$$P_f = (-1)^{n+1} Q \det(-I_{n-1}) = Q = 1 + X + \cdots + X^n.$$

P_f admet n racines distinctes qui sont les racines $(n+1)^e$ de l'unité autres que 1, donc g est diagonalisable d'après une condition suffisante.

Remarque : d'après le théorème de Cayley-Hamilton, P_f est un polynôme annulateur de f, donc $(X-1)P_f = X^{n+1} - 1$ annule aussi g, donc $g^{n+1} = id$ en accord avec le résultat du II.1.

3.a. Dans l'espace vectoriel E de dimension n, toute famille génératrice a au moins n éléments, donc $p = \mathrm{Card}(C_a^p) \leq n$.

b. $C_a^p = \{a, f(a), \ldots, f^{p-1}(a)\}$ engendre E, donc $\mathrm{rg}(C_a^p) = n$ et $\mathrm{Im}\, f$ est engendré par les images par f des éléments de C_a^p, donc $\mathrm{rg}(f) = \mathrm{rg}\big(f(a), \ldots, f^p(a)\big) \leq \mathrm{rg}\big(a, f(a), \ldots, f^{p-1}(a)\big) \leq n-1$.

4. L'existence de m résulte du fait qu'une famille libre a au plus n éléments. De plus $m \leq p$ car $m \leq n \leq p$.

a. Montrons par récurrence sur k que $f^k(a) \in \mathrm{Vect}(\mathcal{F})$ pour $k \geq m$.

Par définition de m, $\begin{cases} \mathcal{F} = \big(a, f(a), \ldots, f^{m-1}(a)\big) & \text{est libre} \\ \big(a, f(a), \ldots, f^{m-1}(a), f^m(a)\big) & \text{est liée.} \end{cases}$

On sait que $f^m(a)$ peut s'écrire comme combinaison linéaire des éléments de $\mathcal{F}$, donc $f^m(a) \in \mathrm{Vect}(\mathcal{F})$.

Supposons que $f^k(a) \in \mathrm{Vect}(\mathcal{F})$.

Ainsi $f^k(a)$ peut s'écrire $\sum_{i=0}^{m-1} \lambda_i . f^i(a)$, donc $f^{k+1}(a) = \sum_{i=0}^{m-1} \lambda_i . f^{i+1}(a) = \lambda_{m-1} . f^m(a) + \sum_{i=0}^{m-2} \lambda_i . f^{i+1}(a)$ qui est dans $\mathrm{Vect}(\mathcal{F})$ comme somme d'éléments de $\mathrm{Vect}(\mathcal{F})$.

b. Il en résulte que $E = \mathrm{Vect}(a, \ldots, f^{p-1}(a)) = \mathrm{Vect}(a, \ldots, f^{m-1}(a))$, donc $(a, \ldots, f^{m-1}(a))$ libre et génératrice de E est une base de E, ce qui impose $m = n$.

Donc $\mathcal{F} = \big(a, f(a), \ldots, f^{n-1}(a)\big)$ est une base de E.

Remarque : dans la base $\mathcal{F}$, f est représentée par une matrice Compagnon.

c. On sait que Π_f divise P_f et que $d^o(P_f) = n$.

Raisonnons par l'absurde en supposant que $r = d^o(\Pi_f) < n$.

Π_f peut s'écrire $\sum_{i=0}^{r} \alpha_i X^i$ et puisque Π_f annule f, on a : $\sum_{i=0}^{r} \alpha_i f^i = 0_{\mathcal{L}(E)}$, donc en particulier $\sum_{i=0}^{r} \alpha_i f^i(a) = 0_E$.

Il s'agit d'une combinaison linéaire d'éléments de $\mathcal{F}$ qui est libre. Nécessairement tous les coefficients sont nuls, ce qui contredit le fait que $d^o(\Pi_f) \geq 1$.

En résumé, P_f et Π_f sont unitaires, de même degré n et Π_f divise P_f, donc $\Pi_f = P_f$.

5. On suppose que f est bijectif et que C_a^p est un cycle de f.

On sait qu'il existe $j \in [\![0; p-1]\!]$ tel que $f^j(a) = f^p(a)$.

Supposons $j \neq 0$: en composant par $(f^{-1})^j$, on obtient $f^{p-j}(a) = a$ avec $1 \leq p-j < p$, ce qui contredit que les éléments de C_a^p sont distincts.

Ainsi $j = 0$ et donc $f^p(a) = a$.

6. $A = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$. $P_f = X^2 - (\mathrm{tr}A)\, X + \det A = X^2 - b\, X - a$. $A^2 = \begin{pmatrix} a & ab \\ b & a + b^2 \end{pmatrix}$.

On suppose que 1 n'est pas valeur propre de f, c'est à dire $\underline{a+b\neq 1}$.

Supposons que f soit cyclique d'ordre 2 et soit $\{v,f(v)\}$ un cycle d'ordre 2 de f.
Par définition, $f^2(v)\in\{v,f(v)\}$.

- Si $\underline{f^2(v)=v}$, comme $v\neq 0$, alors v est un vecteur propre de f^2 relativement à la valeur propre 1.
Or $P_{f^2}=X^2-(\mathrm{tr}A^2)\,X+\det A^2=X^2-(2a+b^2)\,X+a^2$.
On a donc $1-(2a+b^2)+a^2=0$, c'est à dire $(a-1)^2-b^2=0$, d'où $a-1=\pm b$, donc $\underline{a-b=1}$ puisque $a+b\neq 1$.
Donc $b=a-1$, $A=\begin{pmatrix}0 & a\\ 1 & a-1\end{pmatrix}$ et $A^2=\begin{pmatrix}a & a(a-1)\\ a-1 & a+(a-1)^2\end{pmatrix}$.
$v=(x,y)$ est vecteur propre de f^2 pour la valeur propre 1 si et seulement si $(a-1)\,x+a\,(a-1)\,y=0$.
. Si $a=1$, alors $A=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ a pour valeur propre 1 et -1, donc ne convient pas selon l'énoncé.
Cependant, dans ce cas, f est cyclique d'ordre 2 et a pour cycle $C^2_{e_1}$ puisque $f(e_1)=e_2$ et $f^2(e_1)=e_1$.
. Si $a\neq 1$, alors on obtient $v=\lambda\,(a,-1)$ avec $\lambda\in\mathbf{C}^*$ et on trouve que $f(v)=-v$, donc $\{v,f(v)\}$ n'est pas un cycle.

- Si $\underline{f^2(v)=f(v)}$, alors f n'est pas bijective sinon on aurait $f(v)=v$ et 1 serait valeur propre de f.
Alors $a=-\det(f)=0$ et $v\in\mathrm{Ker}(f^2-f)$. $A=\begin{pmatrix}0 & 0\\ 1 & b\end{pmatrix}$ et $A^2=\begin{pmatrix}0 & 0\\ b & b^2\end{pmatrix}$
$v=(x,y)\in\mathrm{Ker}(f^2-f)\iff (b-1)\,x+b\,(b-1)\,y=0$.
. Si $b\neq 1$, alors $v=\lambda(b,-1)$ et $f(v)=0$, donc $\{v,f(v)\}$ n'engendre pas E.
. Si $b=1$, alors $f(e_2)=e_2$, donc 1 est valeur propre de f.
Cependant, $A^2=A$ et $\mathrm{Ker}(f^2-f)=\mathbf{C}^2$.
En prenant par exemple $v=(1,1)$, alors $f(v)=(0,2)$ et $f^2(v)=f(v)$, donc $\{v,f(v)\}$ est un cycle d'ordre 2.

Bilan : avec la condition "1 n'est pas valeur propre de f", il n'y a pas de solution.
Cependant $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ et $\begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}$ sont associés à des endomorphismes cycliques d'ordre 2.

7. On suppose $\theta\notin\pi\mathbf{Z}$ sinon r serait égale à $\pm id$ qui ne sont pas cycliques de façon immédiate.
Condition nécessaire : Supposons r cyclique d'ordre p et soit C^p_a un cycle d'ordre p de r.
Comme $\det r=1$, r est bijectif, donc $r^p(a)=a$ d'après 5.
Comme $a\neq 0$, 1 est valeur propre de r^p.
r^p a pour matrice $\begin{pmatrix}\cos(p\theta) & -\sin(p\theta)\\ \sin(p\theta) & \cos(p\theta)\end{pmatrix}$ et a pour valeurs propres $e^{ip\theta}$ et $e^{-ip\theta}$.
Donc nécessairement $p\theta\in 2\pi\mathbf{Z}$, donc $\underline{\theta\in 2\pi\mathbf{Q}}$.

Réciproque Supposons θ de la forme $2\pi\dfrac{q}{p}$ avec $p\geq 2$ et $p\wedge q=1$. Alors $r^p=id$.
Considérons $a=(1,0)$. On a $r(a)=(\cos\theta,\sin\theta)$ et $\begin{vmatrix}1 & \cos\theta\\ 0 & \sin\theta\end{vmatrix}=\sin\theta\neq 0$ car $\theta\notin\pi\mathbf{Z}$. Donc $\{a,r(a)\}$ est une base de $\mathbf{C}^2$. A fortiori, la famille $\big(a,r(a),\ldots,r^{p-1}(a)\big)$ engendre E. Puisque $r^p(a)=a$, pour avoir un cycle, il suffit de s'assurer que tous les éléments sont deux à deux distincts.
Supposons $r^k(a)=r^\ell(a)$ avec $0\leq k\leq\ell\leq p-1$. En considérant leurs affixes, on obtient que $e^{ik\theta}=e^{i\ell\theta}$, d'où $e^{i(\ell-k)\theta}=1$, donc $2\pi(\ell-k)\dfrac{q}{p}\in 2\pi\mathbf{Z}$, donc $(\ell-k)q\in p\mathbf{Z}$, c'est à dire p divise $(\ell-k)\,q$. Comme $p\wedge q=1$, d'après le théorème de Gauss, p divise $\ell-k$. Or $0\leq\ell-k<p$, donc $\ell=k$.
Ainsi $k\longmapsto r^k(a)$ est injective de $[\![0;p-1]\!]$ dans $\mathbf{C}$ et donc C^p_a est un cycle pour r et $\underline{r\text{ est cyclique}}$.

PARTIE II

Caractérisation des endomorphismes cycliques inversibles

1. On suppose que $f \in GL(E)$ et que C_a^p est un cycle pour f.

a. D'après I.5, $f^p(a) = a$. $\quad \forall\, k \in [\![0; p-1]\!],\ f^p\big(f^k(a)\big) = f^k\big(f^p(a)\big) = f^k(a)$.
Ainsi f^p et id coïncident sur une partie génératrice de E, donc sont égales, d'où $\underline{f^p = id}$.
(*L'implication* $(f^p(a) = a \Longrightarrow f^p = id)$ *reste valable si* $f \notin GL(E)$.)

f annule donc le polynôme $X^p - 1 = \prod_{k=0}^{p-1}(X - e^{2ik\pi/p})$ scindé dans $\mathbf{C}[X]$ à racines simples, donc $\underline{f \text{ est diagonalisable}}$.

b. Comme Π_f divise tout polynôme annulateur de f, $\Pi_f = P_f$ divise $X^p - 1$.
Raisonnons par l'absurde en supposant qu'il existe $k < p$ tel que Π_f divise $X^k - 1$.
Alors $X^k - 1$ annule aussi f, donc $f^k = id$. En particulier $f^k(a) = a$ avec $1 \le k \le p-1$, ce qui contredit que les éléments de C_a^p sont distincts.
Ainsi p est le plus petit des entiers $k \ge 1$ tel que P_f divise $X^k - 1$.

2. Réciproque.

a. Π_f divise P_f et P_f divise $X^p - 1 = \prod_{k=0}^{p-1}(X - \omega_k)$ avec $\omega_k = e^{2ik\pi/p}$.
Notons $A = \{k \in [\![0; p-1]\!] \ / \ (X - w_k) \text{ divise } \Pi_f\}$ et $B = \{k \in [\![0; p-1]\!] \ / \ (X - w_k) \text{ divise } P_f\}$.
On a $\Pi_f = \prod_{k\in A}(X - \omega_k)$, $\quad P_f = \prod_{k\in B}(X - \omega_k)$ et $\quad A \subset B$.
Le théorème de décomposition des noyaux donne :

$$E = \mathrm{Ker}\big(\Pi_f(f)\big) = \bigoplus_{k\in A} \mathrm{Ker}(f - \omega_k.id) \quad \text{et} \quad E = \mathrm{Ker}\big(\Pi_f(f)\big) = \bigoplus_{k\in B} \mathrm{Ker}(f - \omega_k.id).$$

Comme chaque w_k pour $k \in B$ est racine simple de P_f, alors $\dim \mathrm{Ker}(f - \omega_k.id) = 1$.
Il en résulte que A et B ont exactement n éléments, donc $A = B$ et par suite $\underline{\Pi_f = P_f}$.

b. f est diagonalisable car admet n valeurs propres distinctes ou encore parce que E est somme directe des sous-espaces propres de f.

c. Notons $\lambda_1, \ldots, \lambda_n$ les n valeurs propres de f et soit $\mathcal{V} = (v_1, \ldots, v_n)$ une base de vecteurs propres de f avec $f(v_k) = \lambda_k.v_k$ pour $k = 1....n$.
Si $x = \sum_{n=1}^{n} x_i.v_i$, alors $f^k(x) = \sum_{i=1}^{n} x_i.f^k(v_i) = \sum_{i=1}^{n} x_i(\lambda_i)^k.v_i$.

La matrice de la famille $\big(x, f(x), \ldots, f^{n-1}(x)\big)$ dans la base $\mathcal{V}$ est $M = \begin{pmatrix} x_1 & x_1\lambda_1 & \ldots & x_1\lambda_1^{n-1} \\ x_2 & x_2\lambda_2 & \ldots & x_2\lambda_2^{n-1} \\ \vdots & \vdots & & \vdots \\ x_n & x_n\lambda_n & \ldots & x_n\lambda_n^{n-1} \end{pmatrix}$.

$\det(M) = \big(\prod_{i=1}^{n} x_i\big)\, V_n(\lambda_1, \ldots, \lambda_n)$ où V_n est un déterminant de Vandermonde non nul car les λ_i sont deux à deux distincts.
Comme les x_i sont non nuls, $\det M \neq 0$ et par suite $\underline{\big(x, f(x), \ldots, f^{n-1}(x)\big) \text{ est une base de } E}$.

d. Puisque P_f est de degré n et divise $X^p - 1$, alors $n \le p$ et donc la famille $\big(x, f(x), \ldots, f^{p-1}(x)\big)$ engendre aussi E.
Comme $f^p(x) = \sum_{i=1}^{n} x_i(\lambda_i)^p.v_i = \sum_{i=1}^{n} x_i.v_i = x$ car les λ_i sont des racines p^e de l'unité, on en déduit que C_x^p est stable par f.
Il reste à montrer que tous les éléments de C_x^p sont $\underline{\text{distincts}}$.

Raisonnons par l'absurde en supposant qu'il existe k et ℓ distincts dans $[\![0;p-1]\!]$ tels que $k<\ell$ et $f^k(x)=f^\ell(x)$.
f étant bijective par hypothèse, on peut composer par $(f^{-1})^k$, ce qui donne $f^{\ell-k}(x)=x$.
Posons $q=\ell-k$. On a $q\geq 1$ et $f^q(x)=x$, donc $\displaystyle\sum_{i=1}^{n} x_i(\lambda_i)^q.v_i=\sum_{i=1}^{n} x_i.v_i$. Comme $\mathcal{V}$ est une base et les $x_i\neq 0$, on obtient que $\forall\, i=1..n,\ \lambda_i^q=1$. Ainsi tous les facteurs $X-\lambda_i$ de la décomposition de P_f en facteurs premiers sont des facteurs de X^q-1, donc P_f divise X^q-1 avec $1\leq q<p$, ce qui contredit l'hypothèse faite sur f.
En résumé, C_x^p est un cycle de f et f est cyclique.

3. Soit $A=\begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix}$ et $B=A+I_3$.

a. $B^2=3\,B$, donc $(A+I_3)^2=3\,(A+I_3)$, d'où $A^2-A-2\,I_3=0$.
Donc le polynôme $Q=X^2-X-2$ annule f. De plus, c'est le polynôme minimal car $A+I_3\neq 0$ et $A-2\,I_3\neq 0$.

b. Comme $A\,(A-I_3)=2\,I_3$, A et f sont inversibles.
Si f était cyclique d'ordre p, alors, d'après II.1.b, $\Pi_f=X^2-X-2=(X+1)\,(X-2)$ diviserait X^p-1, ce qui est faux.
f n'est donc pas cyclique.

PARTIE III

Caractérisation des endomorphismes cycliques non inversibles

1. On suppose que C_a^p est un cycle de f et que f n'est pas inversible.

a. D'après I.3.b, $\mathrm{rg}(f)\geq n-1$, donc d'après le théorème du rang, $\dim(\mathrm{Ker}f)\leq 1$.
Or $f\notin GL(E)$, donc f est non injective : $\dim(\mathrm{Ker}f)\geq 1$.
Ainsi $\dim(\mathrm{Ker}f)=1$.

b. Si l'on avait $f^p(a)=a$, on montrerait comme au II.1.a. que $f^p=id$ et par suite f serait inversible.
Donc $f^p(a)\neq a$.
Comme $f^p(a)\in C_a^p$, $\exists\, j\in[\![1;p-1]\!]\ /\ f^p(a)=f^j(a)$.

c. $\forall\, k\in[\![0;p-1]\!]$, $f^j\big(f^k(a)\big)=f^k\big(f^j(a)\big)=f^k\big(f^p(a)\big)=f^p\big(f^k(a)\big)$, donc $f^j=f^p$ puisqu'elles prennent les mêmes valeurs sur les éléments d'une partie génératrice.

d. f étant non injective, 0 est valeur propre de f. Notons j l'ordre de multiplicité de 0 dans P_f : $1\leq j\leq n$.
P_f se factorise donc en $P_f=X^j\,Q$ avec $Q(0)\neq 0$.
Or f annule le polynôme $X^p-X^j=X^j\,(X^{p-j}-1)$, donc $\Pi_f(=P_f)$ divise $X^j\,(X^{p-j}-1)$, d'où Q divise $(X^{p-j}-1)$.

Dans la suite, on s'intéresse à une réciproque.

2. Si Q est constant, alors $Q=1$ d'après les coefficients dominants et $j=n$.
Ainsi $P_f=\Pi_f=X^n$, donc par définition du polynôme minimal, $f^n=0$ et $f^{n-1}\neq 0$, autrement dit, f est nilpotent d'indice n.

On vérifie facilement que si $a \notin \mathrm{Ker}(f^{n-1})$, alors la famille $\big(a, f(a), \ldots, f^{n-1}(a)\big)$ est libre, donc c'est une base et par suite, une famille génératrice de E.
On constate alors que $C_a^{n+1} = \{a, f(a), \ldots, f^{n-1}(a), 0_E\}$ est un cycle de f.

3.a. f annule $\Pi_f = X^j\,Q$ et $X^q - 1$ est un multiple de Q, donc f annule le polynôme $X^j\,(X^p - 1)$.
Or X^j et $X^p - 1$ n'ont pas de facteurs communs irréductilbes dans $\mathbf{C}[X]$, donc sont premiers entre eux.
Le théorème de décomposition des noyaux donne alors : $\underline{E = \mathrm{Ker}(f^j) \oplus \mathrm{Ker}(f^q - id)}$.

b. Sachant que le noyau de tout polynôme en f est stable par f, on en déduit immédiatement que $E_1 = \mathrm{Ker}(f^j)$ et $E_2 = \mathrm{Ker}(f^q - id)$ $\underline{\text{sont stables par } f}$.
On peut donc considérer les endomorphismes f_1 et f_2 induits par f sur E_1 et E_2.

4.a. Pour montrer que f_2 est cyclique d'ordre q, on se ramène au résultat obtenu au II.2.
- $\forall\, x \in E_2 = \mathrm{Ker}(f^q - id)$, $f^q(x) = x$, d'où $f_2^q(x) = x$, donc $f_2^q = id_2$ et $\underline{f_2 \in GL(E_2)}$.

- On sait que P_{f_2} divise $P_f = X^j\,Q$, et comme $0 \notin \mathrm{Sp}(f_2)$, P_{f_2} est premier avec X^j, donc, d'après le théorème de Gauss, P_{f_2} divise Q qui divise $X^q - 1$, donc $\underline{P_{f_2} \text{ divise } X^q - 1}$.
Par suite, les zéros de P_{f_2} dans $\mathbf{C}$ sont tous d'ordre 1 : on sait qu'alors $\underline{\Pi_{f_2} = P_{f_2}}$.

- Supposons qu'il existe $k \in [\![1; p-1]\!]$ tel que P_{f_2} divise $X^k - 1$. Comme f_2 annule P_{f_2}, a fortiori, f_2 annule $X^k - 1$, donc $f_2^k = id_2$.
Tout élément $x \in E$ se décompose en $x = x_1 + x_2$ avec $x_1 = E_1$ et $x_2 \in E_2$, donc $f^j(x_1) = 0_E$ et $f^k(x_2) = x_2$.
Ainsi $\big[f^j \circ (f^k - id)\big](x) = (f^k - id)\big(f^j(x_1)\big) + f^j\big((f^k - id)(x_2)\big) = 0_E$.
On vient donc de montrer que $f^j \circ (f^k - 1) = 0$, donc $\Pi_f = X^j\,Q$ divise $X^j\,(X^k - 1)$, donc Q divise $X^k - 1$ ce qui contredit l'hypothèse faite sur Q.
Donc on peut conclure que $\underline{f \text{ est cyclique d'ordre } q}$.
Si $C_{a_2}^q$ est un cycle de f_2, alors $a_2 \in E_2$, donc $f_2^q(a_2) = a_2$.
Il en résulte que la suite $\big(f^j(a_2), \ldots, f^{j+q-1}(a_2)\big)$ se déduit de la suite $\big(a_2, \ldots, f^{q-1}(a_2)\big)$ par permutation circulaire, donc est elle-même génératrice de E_2.

5.a. En se plaçant dans une base adaptée à la somme directe $E = E_1 \oplus E_2$, f est représentée par une matrice diagonale par blocs $A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ et l'on sait que A_1 et A_2 sont des matrices associées à f_1 et f_2 respectivement.
On obtient $\underline{P_f} = \det(XI_n - A) = \det(XI_u - A_1)\,\det(XI_v - A_2) = \underline{P_{f_1}\,P_{f_2}}$.
Donc $P_{f_1}\,P_{f_2} = X^j\,Q$. Or f_1 est nilpotent d'indice $\leq j$. En notant $u = \dim(E_1)$, alors $P_{f_1} = X^u$ et puisque 0 n'est pas racine de P_{f_2} et de Q, on a nécessairement $j = u$. Ainsi $\underline{\dim(E_1) = j}$.

b) Si l'on avait $f_1^{j-1} = 0$, en reprenant un calcul effectué au III.4.a, on trouverait que le polynôme $X^{j-1}\,(X^q - 1)$ annule f, par suite $\Pi_f = X^j\,Q$ diviserait $X^{j-1}\,(X^q - 1)$, ce qui est impossible.

c) En considérant $\underline{a_1 \in E_1 \setminus \mathrm{Ker}(f_1^{j-1})}$, on vérifie facilement que $\big(a_1, f_1(a_1), \ldots, f_1^{j-1}(a_1)\big)$ est libre, donc c'est une base de E_1. Donc $\big(a_1, f(a_1), \ldots, f^{j-1}(a_1)\big)$est une base de E_1.

6. $a = a_1 + a_2$ et $f^j(a_1) = 0$, donc :
$C_{a_1+a_2}^{j+q-1} = \{a, f(a), \ldots, f^{j+q-1}(a)\}$
$= \{a_1 + a_2,\ f(a_1) + f(a_2),\ \ldots,\ f^{j-1}(a_1) + f^{j-1}(a_2),\ f^j(a_2), \ldots, f^{j+q-1}(a_2)\}$.
En considérant les projections sur E_1 ou E_2, on remarque que le rang de ces vecteurs est le même que celui de la famille $\big(a_1, f(a_1), \ldots, f^{j-1}(a_1), f^j(a_2), \ldots, f^{j+q-1}(a_2)\big)$ qui engendre $E_1 + E_2 = E$.
Donc $C_{a_1+a_2}^{j+q-1}$ $\underline{\text{engendre } E}$ et de plus ses éléments sont $\underline{\text{distincts}}$ car $a_1, f(a_1), \ldots, f^j(a_1)$ sont distincts dans E_1 et $f^j(a_2), \ldots, f^{j+q-1}(a_2)$ distincts dans E_2.
Enfin $f^{j+q}(a_1 + a_2) = f^{j+q}(a_2) = f^j(a_2)$, donc $C_{a_1+a_2}^{j+q-1}$ est $\underline{\text{stable}}$ par f.
En résumé, $\underline{C_{a_1+a_2}^{j+q-1} \text{ est un cycle de } f}$.

7. Pour $A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & -1 & 0 \\ 1 & 1 & j \end{pmatrix}$, on trouve que $\underline{P_f = X^2\,(X-j)}$ et $A^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ j & j & j^2 \end{pmatrix}$.

On vérifie que $\Pi_f = P_f$ car aucun facteur de P_f n'annule f.

Ici $Q = X - j$ qui divise $X^3 - 1$, mais pas $X - 1$ et $X^2 - 1$, donc $q = 3$ et $j = 2$.

On peut donc appliquer ce qui précède et construire un cycle C_a^4 avec a de la forme $a_1 + a_2$.

On choisit $a_1 \in E_1 = \mathrm{Ker}(f^2)$ hyperplan défini par l'équation $x + y + j\,z = 0$ et tel que $a_1 \notin \mathrm{Ker} f$, par exemple $\underline{a_1 = (j, 0, -1)}$ et $a_2 \in E_2 = \mathrm{Ker}(f^3 - id)$, par exemple $\underline{a_2 = e_3 = (0, 0, 1)}$ qui est vecteur propre de f pour la valeur propre j, donc vecteur propre de f^3 pour la valeur propre $j^3 = 1$, c'est à dire $a_2 \in \mathrm{Ker}(f^3 - id)$.

Ainsi $a = (j, 0, 0)$, $f(a) = (j, -j, j)$, $f^2(a) = (0, 0, j^2) = j^2.e_3$, $f^3(a) = (0, 0, 1) = e_3$, $f^4(a) = (0, 0, j)$ et C_a^4 est un cycle de f.

On vérifie que $f^5(a) = (0, 0, j) = f^2(a)$ comme trouvé au 6.

$* + * + * + * + * + * + *$