

EP1 2025 : matrices d'ordre fini

Exercice préliminaire 1

1. Analyse : soit $\varphi : \mathbf{K}[X] \rightarrow \text{End}(E)$ un morphisme de $\mathbf{K}$ -algèbres qui envoie X sur u . Alors un polynôme $P = \sum_{k=0}^d a_k X^k$ est nécessairement envoyé sur $\sum_{k=0}^d a_k u^k$, d'où l'unicité d'un tel morphisme.
- Synthèse : pour tout $P = \sum_{k=0}^d a_k X^k \in \mathbf{K}[X]$, on pose $\theta_u(P) = \sum_{k=0}^d a_k u^k$. On vérifie que l'application θ_u ainsi définie est bien linéaire; de plus, pour tout $(i, j) \in \mathbf{N}^2$, on a

$$\theta_u(X^i X^j) = \theta_u(X^{i+j}) = u^{i+j} = u^i \circ u^j = \theta_u(X^i) \circ \theta_u(X^j).$$

Comme les applications $(P, Q) \mapsto \theta_u(P \times Q)$ et $(P, Q) \mapsto \theta_u(P) \circ \theta_u(Q)$ sont bilinéaires sur $\mathbf{K}[X] \times \mathbf{K}[X]$ et coïncident en les (X^i, X^j) , on a pour tout $(P, Q) \in \mathbf{K}[X] \times \mathbf{K}[X]$, $\theta_u(P \times Q) = \theta_u(P) \circ \theta_u(Q)$.

Enfin – selon la tradition française – on vérifie que $\theta_u(1) = \text{Id}_E$, ce qui prouve que θ_u est un morphisme d'algèbres.

2. Notons $n = \dim E$. L'espace vectoriel $L(E)$ est de dimension n^2 .
- La famille d'endomorphismes $(\text{Id}_E, u, u^2, \dots, u^{n^2})$, qui est de cardinal $n^2 + 1$ est donc nécessairement liée. Il existe des scalaires $a_0, a_1, \dots, a_{n^2}$ non tous nuls tels que $a_0 \text{Id}_E + a_1 u + \dots + a_{n^2} u^{n^2} = 0$. Posons $P = \sum_{k=0}^{n^2} a_k X^k$; alors $P \neq 0$ et $\theta_u(P) = 0$, donc θ_u n'est pas injectif.
3. Le noyau $\ker \theta_u$ du morphisme d'algèbres θ_u est un idéal non nul de $\mathbf{K}[X]$ qui est un anneau principal. Il existe donc un unique polynôme unitaire μ_u qui engendre cet idéal. On a alors $P \in \ker \theta_u$ si et seulement s'il existe $Q \in \mathbf{K}[X]$ tel que $P = Q\mu_u$.
4. La famille $(\text{Id}_E, u, \dots, u^{d-1})$ est libre. En effet, si $a_0, a_1, \dots, a_{d-1}$ sont des scalaires tels que $a_0 \text{Id}_E + a_1 u + \dots + a_{d-1} u^{d-1} = 0$, alors le polynôme $P = \sum_{k=0}^{d-1} a_k X^k$ est annulateur de u et de degré strictement inférieur à $d = \deg \mu_u$. On en déduit que $P = 0$, i. e., $a_0 = a_1 = \dots = a_{d-1} = 0$.
- La famille $(\text{Id}_E, u, \dots, u^{d-1})$ est génératrice. En effet, soit $v \in \mathbf{K}[u]$; par définition de $\mathbf{K}[u]$, il existe $P \in \mathbf{K}[X]$ tel que $v = P(u)$. Écrivons la division euclidienne de P par μ_u : $P = Q\mu_u + R$ avec $\deg R < \deg \mu_u$. Comme θ_u est un morphisme d'algèbres, on obtient en évaluant en u que $P(u) = Q(u) \circ \mu_u(u) + R(u) = R(u)$. Donc $P(u) \in \text{Vect}(\text{Id}_E, u, \dots, u^{d-1})$.

Exercice préliminaire 2

5. Soit $k \in \llbracket 1, n \rrbracket$. On écrit $\mathbf{Z}/n\mathbf{Z} = \{\bar{1}, \dots, \overline{n-1}, \bar{n} = \bar{0}\}$. L'élément $\bar{k} \in \mathbf{Z}/n\mathbf{Z}$ est inversible si et seulement s'il existe $\bar{u} \in \mathbf{Z}/n\mathbf{Z}$ tel que $\bar{k}\bar{u} = \bar{1}$, ce qui en relevant dans $\mathbf{Z}$ équivaut à l'existence de $u \in \mathbf{Z}$ et de $v \in \mathbf{Z}$ tels que $uk + vn = 1$. Par le théorème de Bézout, c'est équivalent à ce que k et n soient premiers entre eux.
6. Soit p un nombre premier et $\alpha \in \mathbf{N}^*$. Un entier $k \in \llbracket 1, p^\alpha \rrbracket$ n'est pas premier avec p^α si et seulement si k est un multiple de p (puisque p est premier). Les multiples de p de l'intervalle entier $\llbracket 1, p^\alpha \rrbracket$ sont de la forme $k = mp$ avec $1 \leq m \leq p^{\alpha-1}$, il y en a donc $p^{\alpha-1}$. Par passage au complémentaire, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

7. Soit n un entier tel que $\varphi(n) \leq 2$. Les diviseurs premiers de n doivent être inférieurs ou égaux à 3 puisque si p est premier, $\varphi(p) = p-1$. Écrivons $n = 2^\alpha 3^\beta$ avec $\alpha, \beta \in \mathbf{N}$. Si $\alpha \geq 1$ et $\beta \geq 1$, alors $\varphi(n) = 2^{\alpha-1} \cdot 3^{\beta-1} \cdot 2$, ce qui force $\alpha = \beta = 1$. On a donc $n = 6$. Si $\alpha \geq 1$ et $\beta = 0$, $\varphi(n) = 2^{\alpha-1}$, ce qui force $\alpha \leq 2$; on a donc $n = 4$ ou $n = 2$. Si $\alpha = 0$ et $\beta \geq 1$, on a $\varphi(n) = 3^{\beta-1} \cdot 2$, ce qui force $\beta = 1$. On a donc $n = 3$. Enfin, le cas $\alpha = \beta = 0$ donne $n = 1$.

En résumé, les entiers n tels que $\varphi(n) \leq 2$ sont parmi 1, 2, 3, 4 et 6 et réciproquement ces entiers conviennent.

—— I. Décomposition de $X^n - 1$ en irréductibles ——

8. Les racines de $X^n - 1$ sont les ω_n^k , $k \in \llbracket 0, n-1 \rrbracket$. Ce sont les n racines n -ièmes de l'unité qui sont 2 à 2 distinctes. On a donc $X^n - 1 = \prod_{k=0}^{n-1} (X - \omega_n^k)$ et $X^n - 1$ est à racines simples.
9. (a) Les seuls réels de module 1 sont 1 et -1 ; 1 est une racine n -ième de l'unité pour tout $n \in \mathbf{N}$ et -1 est une racine n -ième de l'unité si et seulement si n est pair.
- (b) On trouve $P_\theta = (X - e^{i\theta})(X - e^{-i\theta}) = X^2 - 2 \cos(\theta)X + 1 \in \mathbf{R}[X]$. Comme $\theta \notin \pi\mathbf{Z}$, $e^{i\theta}$ et $e^{-i\theta}$ sont non réels donc P_θ est irréductible dans $\mathbf{R}[X]$.
- (c) Supposons n impair; alors $X^n - 1$ admet 1 comme unique racine réelle; les autres racines sont les ω_n^k , $k \in \llbracket 1, n-1 \rrbracket$ qui sont 2 à 2 conjuguées puisque $X^n - 1$ est à coefficients réels. D'après le calcul de la question précédente, on a

$$X^n - 1 = (X - 1) \prod_{k=1}^{(n-1)/2} (X^2 - 2 \cos(2k\pi/n)X + 1).$$

Dans le cas n pair, 1 et -1 sont racines, ce qui correspond à $k = 0$ et $k = n/2$, et on a

$$X^n - 1 = (X - 1)(X + 1) \prod_{k=1}^{n/2-1} (X^2 - 2 \cos(2k\pi/n)X + 1).$$

10. (a) Soit $m \in \mathbf{N}^*$; ω_n^m est une racine primitive n -ième de l'unité si et seulement si ω_n^m engendre le groupe multiplicatif $\mathbf{U}_n$, ce qui équivaut à $\omega_n \in \langle \omega_n^m \rangle = \{\omega_n^{mk}, k \in \mathbf{Z}\}$. Ainsi, ω_n^m est une racine primitive n -ième si et seulement s'il existe $k \in \mathbf{Z}$ tel que $\omega_n^{km} = \omega_n$, ce qui équivaut à $1 - km \in n\mathbf{Z}$, ou encore à l'existence d'entiers k et ℓ tels que $1 = km + n\ell$. Par le théorème de Bézout, cela équivaut à $m \wedge n = 1$.
- (b) Par division euclidienne de m par n , on peut se restreindre à $m \in \llbracket 1, n \rrbracket$. On conclut alors par la question précédente et la définition de $\varphi(n)$.
11. (a) Soit $z \in \mathbf{U}_n$. En notant d l'ordre de z dans le groupe $\mathbf{U}_n$, qui divise n par le théorème de Lagrange, on a $z \in A_d$; réciproquement, si $z \in A_d$ pour un d divisant n , alors en écrivant $n = md$, on a $z^n = (z^d)^m = 1$, donc $z \in \mathbf{U}_b$. L'union est disjointe par unicité de l'ordre d'un élément dans un groupe. En effet, A_d est l'ensemble des éléments d'ordre d .

On en déduit

$$X^n - 1 = \prod_{z \in \mathbf{U}_n} (X - z) = \prod_{d|n} \prod_{z \in A_d} (X - z) = \prod_{d|n} \Phi_d.$$

- (b) On a $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$. De $X^4 - 1 = \Phi_4 \Phi_2 \Phi_1 = \Phi_4(X^2 - 1)$, on déduit que $\Phi_4 = X^2 + 1$. On a $X^5 - 1 = \Phi_5 \Phi_1$, donc $\Phi_5 = X^5 + X^4 + X^3 + X^2 + X + 1$. Enfin, $X^6 - 1 = \Phi_6 \Phi_3 \Phi_2 \Phi_1$, donc $X^6 - 1 = \Phi_6(X^3 - 1)(X + 1)$, puis $\Phi_6 = \frac{X^3 + 1}{X + 1} = X^2 - X + 1$.
- (c) Écrivons $B = X^m + \sum_{k=0}^{m-1} b_k X^k$ où les b_k sont entiers.

Soit H_n l'énoncé : pour tout polynôme $A \in \mathbf{Z}[X]$ de degré inférieur strictement à n , il existe $Q, R \in \mathbf{Z}[X]$ tels que $A = BQ + R$ et $\deg R < m$.

On montre le résultat par récurrence sur n . L'énoncé H_m est vrai, il suffit de poser $Q = 0$ et $R = A$. Soit $n \geq m$ et supposons H_n . Montrons H_{n+1} . Soit $A \in \mathbb{Z}[X]$ de degré strictement inférieur à $n + 1$. Notons $A = \sum_{k=0}^n a_k X^k$ et posons $A_1 = A - a_n X^{n-m} B$. Alors on a $A_1 \in \mathbb{Z}[X]$ et $\deg A_1 < n$ donc on peut appliquer l'hypothèse de récurrence à A_1 . Il existe $Q_1, R_1 \in \mathbb{Z}[X]$ tels que $A_1 = BQ_1 + R_1$ avec $\deg R_1 < m$. En posant $Q = Q_1 + a_n X^{n-m}$, on a alors $A = BQ + R_1$, avec $Q \in \mathbb{Z}[X]$ et $\deg R_1 < m$ ce qui prouve H_{n+1} .

D'après le principe de récurrence, pour tout $n \geq m$, H_n est vraie, ce qui conclut.

(d) On prouve le résultat par récurrence forte sur n .

Pour $n = 1$, on a $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.

Supposons le résultat vrai pour tout entier $d < n$ et montrons que $\Phi_n(X) \in \mathbb{Z}[X]$. Par hypothèse, le polynôme $P = \prod_{d|n, d \neq n} \Phi_d(X)$ est élément de $\mathbb{Z}[X]$. On a la relation $X^n - 1 = \Phi_n(X)P(X)$ et par ailleurs, la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$ (possible parce que P est unitaire, voir question précédente) s'écrit $X^n - 1 = PQ + R$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg R < \deg P$. On en déduit la relation $R(X) = P(X)(\Phi_n(X) - Q(X))$, qui implique $\Phi_n = Q$, sinon $\deg R \geq \deg P$. Finalement, $\Phi_n \in \mathbb{Z}[X]$.

—— 2. Un lemme sur les matrices d'ordre fini ——

12. Le polynôme $X^r - 1$ est annulateur de A . Sur $\mathbb{C}$, $X^r - 1$ est scindé simple donc par théorème A est diagonalisable sur $\mathbb{C}$ et le spectre de A est inclus dans les racines de $X^r - 1$ qui sont des racines de l'unité.
13. Comme $X^r - 1$ est annulateur de A , on a $\mu_A \mid X^r - 1$. Or le polynôme $X^r - 1$ est à racines simples, donc μ_A est de la forme $\mu_A = P_1 \cdots P_q$ où les P_j sont irréductibles et 2 à 2 distincts (sinon μ_A admettrait une racine multiple dans $\mathbb{C}$).

—— 3. Endomorphismes cycliques ——

14. On procède par récurrence sur la dimension n .

Initialisation, $n = 1$. On a $P = X + a_0$, $C_P = (-a_0)$, donc $\chi_{C_P} = X + a_0 = P$.

Soit $n \geq 1$; supposons que pour tout polynôme unitaire P de degré n , on a $\chi_{C_P} = P$.

Soit $P = X^{n+1} + a_n X^n + \cdots + a_1 X + a_0$ un polynôme unitaire de degré $n + 1$. On développe le déterminant $\det(XI_{n+1} - C_P)$ selon la première colonne; le premier cofacteur vaut, par hypothèse de récurrence, $X(X^n + a_n X^{n-1} + \cdots + a_2 X + a_1)$ et le second vaut

$$\begin{vmatrix} 0 & \cdots & \cdots & a_0 \\ -1 & X & & a_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & X + a_n \end{vmatrix}$$

que l'on calcule en développant par rapport à sa première ligne. On trouve $(-1)^{n+1} a_0 (-1)^{n-1} = a_0$ (mineur triangulaire).

En définitive, $\chi_{C_P} = X(X^n + a_n X^{n-1} + \cdots + a_2 X + a_1) + a_0 = X^{n+1} + a_n X^n + \cdots + a_1 X + a_0$, ce qui prouve l'hypothèse au rang $n + 1$. Par le principe de récurrence, l'hypothèse est vraie pour tout $n \geq 1$.

15. (a) On commence par démontrer que I_x est un idéal de $\mathbb{K}[X]$.

Le polynôme nul appartient à I_x , et si $P, Q \in I_x$, $(P - Q)(u)(x) = P(u)(x) - Q(u)(x) = 0$, donc $(I_x, +)$ est un sous-groupe de $(\mathbb{K}[X], +)$.

Soit $P \in I_x$ et $Q \in \mathbb{K}[X]$. Puisque θ_u est un morphisme d'algèbres, on a $(PQ)(u)(x) = P(u) \circ Q(u)(x) = Q(u) \circ P(u)(x) = Q(u)(0) = 0$. Donc $PQ \in I_x$.

Ainsi, I_x est un idéal de l'anneau $\mathbf{K}[X]$ qui est principal, donc I_x admet un unique générateur unitaire μ_x . De plus, $\mu_u \in I_x$, donc $\mu_x \mid \mu_u$.

- (b) Les polynômes $P_i^{m_i}$ sont premiers entre eux et μ_u est annulateur de u . D'après le lemme des noyaux

$$E = \bigoplus_{i=1}^q \ker P_i^{m_i}(u).$$

De plus, les endomorphismes $P_i^{m_i}(u)$ sont des polynômes en u , donc ils commutent avec u . On en déduit que les noyaux $\ker P_i^{m_i}(u)$ sont stables par u .

- (c) Pour tout $i \in \llbracket 1, q \rrbracket$, $P_i^{m_i}$ annule u_i , donc $\mu_{u_i} \mid P_i^{m_i}$. Le polynôme P_i étant irréductible, les diviseurs de $P_i^{m_i}$ sont de la forme $P_i^{\alpha_i}$ avec $\alpha_i \leq m_i$.

S'il existe i tel que $\mu_{u_i} = P_i^{\alpha_i}$ avec $\alpha_i < m_i$, alors le polynôme $P = P_i^{\alpha_i} \prod_{j \neq i} P_j^{m_j}$ est annulateur de u (par la décomposition du lemme des noyaux obtenue en 15(a)), non nul, et de degré strictement inférieur à $\deg \mu_u$, ce qui est absurde. Donc pour tout i , $\mu_{u_i} = P_i^{m_i}$.

Supposons par l'absurde que pour tout $x \in N_i$, $\mu_x \neq \mu_{u_i}$. Alors pour tout $x \in N_i$, $\mu_x \mid P_i^{m_i-1}$, ce qui entraîne $P_i^{m_i-1}(u_i)(x) = 0$. Le polynôme $P_i^{m_i-1}$ est alors annulateur de u_i , ce qui contredit le fait que $\mu_{u_i} = P_i^{m_i}$. Ainsi, il existe $x_i \in N_i$ tel que $\mu_{x_i} = P_i^{m_i} = \mu_{u_i}$.

Posons $x = \sum_{i=1}^q x_i$ et montrons que $\mu_x = \mu_u$. Soit $P \in I_x$; alors

$$0 = P(u)(x) = P(u)(x_1) + \cdots + P(u)(x_q)$$

et pour tout i , $P(u)(x_i) \in N_i$. Or $E = \bigoplus_{i=1}^q N_i$, donc on peut en déduire que pour tout $i \in \llbracket 1, q \rrbracket$, $P(u)(x_i) = 0$. On en déduit que $\mu_{x_i} = P_i^{m_i}$ divise P , et comme les $P_i^{m_i}$ sont premiers entre eux, $\mu_u = \prod_{i=1}^q P_i^{m_i}$ divise P . On conclut que $\mu_u = \mu_x$ puisque d'après 15a), $\mu_x \mid \mu_u$.

16. Supposons i); notons $u^k(x_0) = a_0 x_0 + a_1 u(x_0) + \cdots + a_{k-1} u^{k-1}(x_0)$ les coordonnées de $u^k(x_0)$ dans la base $\mathcal{B} = (x_0, u(x_0), \dots, u^{k-1}(x_0))$. On vérifie que la matrice de u dans $\mathcal{B}$ est C_P où $P = -a_0 - a_1 X - \cdots - a_{k-1} X^{k-1}$. On a prouvé ii).

Supposons ii); notons $\mathcal{B} = (x_0, x_1, \dots, x_{k-1})$. Par définition d'une matrice compagnon, en considérant les $k-1$ premières colonnes de $\text{Mat}_{\mathcal{B}}(u)$, on a $(x_0, x_1, \dots, x_{k-1}) = (x_0, u(x_0), \dots, u^{k-1}(x_0))$, d'où i).

Supposons i); alors le degré de μ_u vaut k . En effet, si $\deg \mu_u = d < k$, la famille $(\text{Id}_E, u, \dots, u^k)$ est liée, donc la famille $(x_0, u(x_0), \dots, u^k(x_0))$ est également liée, ce qui est absurde puisque $(x_0, u(x_0), \dots, u^{k-1}(x_0))$ est une base de E . D'après le théorème de Cayley-Hamilton, μ_u divise χ_u et ils sont tous les deux unitaires et de degré k , donc on conclut que $\chi_u = \mu_u$, d'où iii).

Supposons iii); d'après 15(c), il existe $x \in E$ tel que $\mu_x = \mu_u$. Comme $\mu_u = \chi_u$, on a donc que $\deg \mu_x = \deg \mu_u = \deg \chi_u = k$; ainsi, la famille $(x, u(x), \dots, u^{k-1}(x))$ est libre, et comme elle est de cardinal k , c'est une base de E , ce qui prouve i).

17. Tout polynôme en u commute avec u , donc $\mathbf{K}[u] \subseteq \text{Com}(u)$.

Réciproquement, soit $v \in \text{Com}(u)$. L'endomorphisme u étant cyclique, il existe un vecteur $x_0 \in E$ tel que $\mathcal{B} = (x_0, u(x_0), \dots, u^{k-1}(x_0))$ soit une base de E . Soit $a_0, \dots, a_{k-1}$ les coordonnées du vecteur $v(x_0)$ dans $\mathcal{B}$. On a donc $v(x_0) = a_0 x_0 + a_1 u(x_0) + \cdots + a_{k-1} u^{k-1}(x_0)$. On montre que $v = \sum_{i=0}^{k-1} a_i u^i$, ce qui prouvera que $v \in \mathbf{K}[u]$. Pour cela, il suffit de vérifier que les endomorphismes v et $w = \sum_{i=0}^{k-1} a_i u^i$ coïncident sur la base $\mathcal{B}$. Soit $j \in \llbracket 0, k-1 \rrbracket$; on a $w(u^j(x_0)) = u^j(w(x_0)) = u^j(v(x_0)) = v(u^j(x_0))$ car v et u^j commutent, d'où le résultat.

18. (a) Soit $x \in E$. Pour tout $P \in \mathbf{K}[X]$, $u(P(u)(x)) = (XP)(u)(x)$, donc E_x est stable par u .

Fixons $x \neq 0$. Le vecteur x étant non nul, il existe un entier k tel que la famille $(x, u(x), \dots, u^k(x))$ soit libre. Soit d le plus grand entier tel que $(x, u(x), \dots, u^d(x))$ soit libre.

Alors la famille $(x, u(x), \dots, u^{d+1}(x))$ est liée, donc il existe un polynôme annulateur non nul A de v de degré au plus $d+1$. Soit $y = P(u)(x)$ un élément de E_x . En effectuant la division euclidienne de P en

$\mathbb{K}[X]$ par A , on prouve que la famille $(x, u(x), \dots, u^d(x))$ est génératrice. Donc $(x, u(x), \dots, u^d(x)) = (x, v(x), \dots, v^d(x))$ est une base de E_x , ce qui prouve que v est cyclique.

Par ailleurs, μ_u est annulateur de v par restriction. Donc $\mu_v \mid \mu_u$, et comme μ_u est irréductible, on a $\mu_v = \mu_u$. On en déduit que $\dim E_x = \deg \mu_v = \deg \mu_u$.

- (b) Si $x = 0$, on a $E_x = \{0\}$ donc $E_x \cap F = \{0\}$.

Supposons que $x \neq 0$ et que $E_x \cap F \neq \{0\}$ et montrons que $E_x \subseteq F$. Soit v l'endomorphisme induit par u sur E_x , qui est de dimension au moins 1. D'après la question précédente, v est cyclique et $\chi_v = \mu_v = \mu_u$. Soit $y \in E_x \cap F \setminus \{0\}$. Alors $E_y \subseteq E_x$ car E_x contient y et E_x est stable par u . Le polynôme caractéristique de l'endomorphisme induit par v sur E_y divise $\chi_v = \pi_u$ et son degré est au moins 1, donc par irréductibilité de π_u , il est égal à π_u . On en déduit que $\dim E_y = \deg \pi_u = \dim E_x$, donc $E_x = E_y$. Or $E_y \subseteq F$, puisque F contient y et F est stable par u . On conclut que $E_x \subseteq F$.

- (c) On considère les familles de vecteurs $(x_1, \dots, x_p)$ telles que la somme $\sum_{i=1}^p E_{x_i}$ est directe. Il existe au moins la famille constituée du seul vecteur $x_1 = 0$. Soit p et $(x_1, \dots, x_p)$ tels que $\dim \bigoplus_{i=1}^p E_{x_i}$ soit maximale; montrons que $E = \bigoplus_{i=1}^p E_{x_i}$ pour un tel p . Raisonnons par l'absurde : si $F = \bigoplus_{i=1}^p E_{x_i}$ n'est pas égal à E , alors il existe $x \in E \setminus F$ et par conséquent, $E_x \not\subseteq F$. L'espace F étant stable par u , on déduit de la question précédente que $E_x \cap F = \{0\}$. La somme $F + E_x$ est donc directe et $\dim \bigoplus_{i=1}^p E_i \oplus E_x > p$, ce qui contredit la définition de p .

19. (a) Avec les notations de la question 15(b), on a $E = \bigoplus_{i=1}^q N_i$ où $N_i = \ker P_i(u)$. Le polynôme minimal de u_i , l'endomorphisme induit par u sur N_i est égal à P_i d'après 15(c). D'après la question précédente, pour tout $i \in \llbracket 1, q \rrbracket$, il existe des vecteurs $(x_1, \dots, x_{p_i})$ de N_i tels que $N_i = \bigoplus_{k=1}^{p_i} E_{x_k}$. On a donc

$$E = \bigoplus_{i=1}^q \bigoplus_{k=1}^{p_i} E_{x_k}.$$

Fixons $i \in \llbracket 1, q \rrbracket$. Comme $E_x = \{0\}$ si $x = 0$, on peut sans restriction supposer que chacun des vecteurs x_k précédents est non nul. On rappelle que u_i est l'endomorphisme induit par u sur $\ker P_i(u)$. Le polynôme minimal de u_i étant égal à P_i , il est irréductible et on a par Q18(a) que les induits $u_{i,k}$ de u_i sur les E_{x_k} sont cycliques. Il existe donc une base $\mathcal{B}_{x_k}$ de E_{x_k} telle que la matrice de cet induit $u_{i,k}$ soit la matrice compagnon d'un certain polynôme (Q16) qui n'est autre que son polynôme minimal. Le polynôme minimal de $u_{i,k}$ divise celui de u_i , donc est égal à P_i (puisque $E_{x_k} \neq \{0\}$). Dans une base $\mathcal{B}_i$ de N_i obtenue en concaténant les bases $\mathcal{B}_{x_k}$, la matrice de u_i est de la forme $\text{Diag}(C_{P_i}, \dots, C_{P_i})$ avec p_i blocs.

Enfin, dans une base $\mathcal{B}$ obtenue en concaténant les bases $\mathcal{B}_i$, la matrice de u est diagonale par blocs de la forme

$$\text{Diag}(C_{P_1}, \dots, C_{P_1}, \dots, C_{P_q}, \dots, C_{P_q}).$$

- (b) La matrice de u dans $\mathcal{B}$ est diagonale par blocs, donc χ_u est le produit des $\chi_{C_{P_i}}$. De plus, le polynôme caractéristique des matrices compagnons C_{P_i} est égal à P_i , donc

$$\chi_u = P_1^{\ell_1} \cdots P_q^{\ell_q}.$$

——— 4. Matrices complexes ou réelles d'ordre fini ———

20. (a) Le polynôme $X^n - 1$ est annulateur de A et scindé à racines simples dans $\mathbf{C}$. On en déduit que A est diagonalisable et que ses valeurs propres sont parmi les racines de $X^n - 1$, donc sont des racines n -ièmes de l'unité.
- (b) Notons $D = \text{Diag}(\lambda_1, \dots, \lambda_k)$. La matrice A étant diagonalisable, il existe $P \in \text{GL}_k(\mathbf{C})$ telle que $A = PDP^{-1}$ et les matrices A et D ont le même ordre. Pour tout $m \in \mathbf{N}$, $D^m = \text{Diag}(\lambda_1^m, \dots, \lambda_k^m)$ donc $D^m = I_k$ si et seulement si pour tout $j \in \llbracket 1, k \rrbracket$, $n_j \mid m$. On en déduit que l'ordre de A est $\text{ppcm}(n_1, \dots, n_k)$.
- (c) Soit $r \in \mathbf{N}^*$. D'après la question précédente, il suffit de considérer par exemple la matrice $A = \text{Diag}(\omega_r, 1, \dots, 1)$.
21. Le polynôme caractéristique de R_θ est $P_\theta = X^2 - 2X \cos(\theta) + 1 = (X - e^{i\theta})(X - e^{-i\theta})$ et c'est aussi son polynôme minimal, sinon R_θ serait diagonale, égale à $\pm I_2$, ce qui est impossible puisque ses valeurs propres $e^{\pm i\theta}$ sont non réelles. Comme $\chi_{R_\theta} = \mu_{R_\theta}$, on en déduit avec Q16 que R_θ est cyclique, donc semblable à une matrice compagnon. Les coefficients de son polynôme caractéristique étant $a_0 = 1$ et $a_1 = -2 \cos(\theta)$, R_θ est semblable à $\begin{pmatrix} 0 & -1 \\ 1 & 2 \cos \theta \end{pmatrix}$.
22. Soit $A \in \text{GL}_k(\mathbf{R})$ une matrice d'ordre fini. Il existe donc $n \in \mathbf{N}^*$ tel que μ_A divise $X^n - 1$ dans $\mathbf{R}[X]$. Les éventuelles valeurs propres réelles de A sont ± 1 puisque ce sont les racines de l'unité réelles (Q9(a)). Les éventuelles valeurs propres non réelles sont des racines n -ièmes de l'unité de la forme $e^{i\theta_j}$ avec $n\theta_j \in 2\pi\mathbf{Z}$, donc $\theta_j \in 2\pi\mathbf{Q}$ et elles viennent par paires avec leur conjugué donc fournissent un facteur P_{θ_j} . De plus, on a vu en Q13 que μ_A est sans facteurs carrés, d'où la forme annoncée.

$$\mu_A = (X - 1)^{\varepsilon_1} (X + 1)^{\varepsilon_2} P_{\theta_1} \cdots P_{\theta_q},$$

où $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, $P_{\theta_i} = X^2 - 2 \cos(\theta_i)X + 1$ et $\theta_i \in 2\pi\mathbf{Q} \setminus \pi\mathbf{Z}$.

23. Soit $A \in \text{GL}_k(\mathbf{R})$. Supposons que A est semblable à une matrice diagonale par blocs de la forme

$$D = \text{Diag}(I_{k_1}, -I_{k_2}, R_{\theta_1}, \dots, R_{\theta_1}, \dots, R_{\theta_q}, \dots, R_{\theta_q}),$$

où $\theta_j \in 2\pi\mathbf{Q}$. Il existe un entier m tel que pour tout j , $m\theta_j \in 2\pi\mathbf{Z}$. On vérifie alors que $D^{2m} = I_k$, donc A est d'ordre fini.

Réciproquement, supposons A d'ordre fini. D'après la question précédente et Q19, en notant $\chi_A = (X - 1)^{k_1} (X + 1)^{k_2} P_{\theta_1}^{\ell_1} \cdots P_{\theta_q}^{\ell_q}$, A est semblable à une matrice de la forme

$$D = \text{Diag}(I_{k_1}, -I_{k_2}, R_{\theta_1}, \dots, R_{\theta_1}, \dots, R_{\theta_q}, \dots, R_{\theta_q}),$$

et les tailles des matrices imposent que $k = k_1 + k_2 + 2(\ell_1 + \cdots + \ell_q)$.

24. Soit A une matrice d'ordre fini. Les calculs par blocs montrent que l'ordre de A est le ppcm des ordres des matrices qui apparaissent dans les blocs. L'ordre de I_{k_1} est 1, l'ordre de $-I_{k_2}$ est 2, et pour tout m , $R_{\theta_j}^m = R_{m\theta_j}$, donc R_{θ_j} est d'ordre le plus petit entier m tel que $m\theta_j \in 2\pi\mathbf{Z}$, à savoir b_j . Finalement, l'ordre de A est $\text{ppcm}(2, b_1, \dots, b_q)$ si $k_2 > 0$ et $\text{ppcm}(b_1, \dots, b_q)$ si $k_2 = 0$.
25. D'après la question précédente, et en remarquant que $R_{2\pi} = I_2$ et $R_\pi = -I_2$, A est d'ordre fini si et seulement si A est semblable à une matrice R_θ , ou bien, dans le cas où $\text{Spec } A = \{-1, 1\}$, si A est semblable à la matrice $\text{Diag}(1, -1)$.
26. Soit $r \in \mathbf{N}^*$; il suffit de considérer $A = R_{2\pi/r}$ qui est d'ordre r .

27. (a) La symétrie, la bilinéarité et le caractère positif proviennent directement de $\langle \cdot, \cdot \rangle$.
 Soit $u \in \mathbf{R}^2$; supposons que $(u, u)_G = \frac{1}{|G|} \sum_{A \in G} \langle Au, Au \rangle = 0$. Alors tous les $\langle Au, Au \rangle$ sont nuls, en particulier pour $A = I_2$, ce qui donne $\langle u, u \rangle = 0$, donc $u = 0$.
 Soit $B \in G$ et $u, v \in \mathbf{R}^2$. On a $(Bu, Bv)_G = \frac{1}{|G|} \sum_{A \in G} \langle ABu, ABv \rangle$; l'application $A \mapsto AB$ étant une bijection de G , on conclut que $(Bu, Bv)_G = (u, v)_G$.
- (b) La matrice S est symétrique définie positive. Elle est donc congruente à I_2 , i.e., il existe $P \in GL_2(\mathbf{R})$ telle que $S = P^T P$ (considérer une base orthonormée pour le produit scalaire $(\cdot, \cdot)_G$).
 Soit $A \in G$; pour tout $u, v \in \mathbf{R}^2$ on a par la question précédente, $(Au)^T S(Av) = u^T S v$, soit $u^T (A^T S A - S) v = 0$, ce qui implique que $S = A^T S A$. En effet, si une matrice M vérifie que pour tout u, v , $u^T M v = 0$, en fixant v et en posant $u = M v$, on obtient $M v = 0$. En remplaçant S par $P^T P$, ceci se réécrit $(P A P^{-1})^T (P A P^{-1}) = I_2$, donc $P A P^{-1} \in \mathcal{O}_2(\mathbf{R})$.
28. Soit G un sous-groupe fini de $SO_2(\mathbf{R})$ d'ordre n . Tout élément $A \in G$ est une matrice de rotation telle que $A^n = I_2$ (théorème de Lagrange) donc son angle est de la forme $\frac{2k\pi}{n}$. Ceci montre l'inclusion entre G et le groupe engendré par la rotation $R_{2\pi/n}$ d'angle $\frac{2\pi}{n}$. Ces deux groupes sont de cardinal n , donc $G = \langle R \rangle \cong \mathbf{Z}/n\mathbf{Z}$.
29. Par stabilité d'un groupe pour sa loi interne, on a $\{I_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\} \subseteq D_n$.
 Pour montrer l'autre inclusion, on montre d'abord que $AB = BA^{-1}$, ce que l'on peut vérifier par un simple calcul matriciel, sachant que $A^{-1} = R_{-\frac{2\pi}{n}}$.
 On montre ensuite par récurrence sur k que pour tout $k \in \llbracket 0, n \rrbracket$, $A^k B = BA^{-k} = BA^{n-k}$ puisque $A^n = I_2$. Sachant que $B^2 = I_2$, tout élément de $\langle A, B \rangle$ s'écrit sous la forme A^k ou bien $A^k B = BA^{n-k}$. Ceci montre l'inclusion $D_n \subseteq \{I_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\}$.
 On conclut que $D_n = \{I_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\}$.
30. (a) Le déterminant induit un isomorphisme $G/(G \cap SO_2(\mathbf{R})) \cong \{-1, 1\}$ car G contient un élément de déterminant 1 (la matrice I_2) et un élément de déterminant -1 (G n'est pas inclus dans $SO_2(\mathbf{R})$).
 (b) Puisque $G \not\subseteq SO_2(\mathbf{R})$, il existe dans G un élément de déterminant -1 , i.e., une matrice de symétrie axiale de la forme
- $$S_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}.$$
- (c) La matrice S_θ est une matrice de symétrie axiale orthogonale, donc elle est diagonalisable *via* une matrice de passage orthogonale $P \in \mathcal{O}_2(\mathbf{R})$, et ses valeurs propres sont 1 et -1 . Quitte à changer la première colonne de P en son opposé, on peut supposer que $P \in SO_2(\mathbf{R})$.
- (d) Le sous-groupe $G \cap SO_2(\mathbf{R})$ est cyclique (d'après Q28). Notons n son ordre. Il est d'indice 2 dans G d'après Q30(a), donc $|G| = 2n$. Le groupe G contient $R_{2\pi/n}$ et un élément S_θ ; comme G est un groupe, il contient aussi les éléments $R_{2\pi/n}^k, S_\theta R_{2\pi/n}^k$ pour $k \in \llbracket 0, n-1 \rrbracket$. Le groupe $SO_2(\mathbf{R})$ étant commutatif, on peut écrire $R_{2\pi/n} = P R_{2\pi/n} P^{-1}$, et par ailleurs $S_\theta = P B P^{-1}$, donc $G = P D_n P^{-1}$, i.e., G est conjugué au groupe diédral D_n .

— 5. Matrices rationnelles d'ordre fini —

31. Le polynôme minimal de A divise $X^n - 1$ et la décomposition en irréductibles de $X^n - 1$ dans $\mathbf{Q}[X]$ est $X^n - 1 = \prod_{d|n} \Phi_d$ (on a admis que les polynômes cyclotomiques sont irréductibles sur $\mathbf{Q}$). De plus, μ_A est sans facteurs carrés puisque $\mathbf{Q}$ est de caractéristique nulle. Il existe donc $d_1, \dots, d_q$ des diviseurs 2 à 2 distincts de n tels que $\mu_A = \Phi_{d_1} \cdots \Phi_{d_q}$.
32. Découle de Q19.

33. (a) D'après Q16, Le polynôme minimal de C_{Φ_d} est Φ_d . On a $X^d - 1 = \prod_{j|d} \Phi_j$, donc $X^d - 1$ est annulateur de C_{Φ_d} . Ainsi, l'ordre de C_{Φ_d} divise d . Si c'était un diviseur strict d' de d , le polynôme minimal Φ_d , qui est irréductible sur $\mathbf{Q}$, serait l'un des facteurs irréductibles de $X^{d'} - 1 = \prod_{j|d'} \Phi_j$, ce qui est impossible puisque $d' < d$.
- (b) Si A est semblable à une telle matrice diagonale par blocs, comme chaque bloc est d'ordre fini (égal à d_j), A est d'ordre fini égal à $\text{ppcm}(d_1, \dots, d_q)$.
Réciproquement, si A est d'ordre fini, d'après Q32 A est semblable à une matrice diagonale par blocs de matrices $C_{\Phi_{d_j}}$ dont l'ordre est d_j , donc l'ordre de A est $\text{ppcm}(d_1, \dots, d_q)$. De plus, le degré de Φ_{d_j} est égal à $\varphi(d_j)$, donc en considérant les tailles des matrices blocs, on a la relation

$$k = \sum_{j=1}^q m_j \varphi(d_j).$$

- (c) Comme vu précédemment, son ordre est égal à $\text{ppcm}(d_1, \dots, d_q)$.
- (d) On prend $k = 4$. Comme $\text{ppcm}(3, 4) = 12$, on considère la matrice $A = \text{Diag}(C_{\Phi_3}, C_{\Phi_4})$. Or $\Phi_3 = X^2 + X + 1$, donc $C_{\Phi_3} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, et $\Phi_4 = X^2 + 1$, donc $C_{\Phi_4} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. La matrice

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

convient.

- (e) L'égalité $k = \sum_{j=1}^q m_j \varphi(d_j)$ montre que les $\varphi(d_j)$ sont inférieurs ou égaux à k donc

$$\text{ppcm}(d_1, \dots, d_q) \leq \text{ppcm}\{m, \varphi(m) \leq k\}.$$

34. (a) On cherche les matrices d'ordre fini de taille 2; une telle matrice est semblable à une matrice diagonale par blocs de matrices compagnons de polynômes cyclotomiques.
Deux cas se présentent : soit il n'y a qu'un seul bloc compagnon de taille 2, alors le polynôme cyclotomique associé est de degré 2, et d'après l'exercice préliminaire 2, on a $\varphi(n) = 2$ si et seulement si $n = 3, 4, 6$. De plus, on a vu en Q11(b) que $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$ et $\Phi_6 = X^2 - X + 1$. Les matrices compagnons correspondantes sont

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

qui sont respectivement d'ordre 3, 4 et 6.

Dans l'autre cas, il y a deux blocs compagnons de taille 1, ce qui donne les matrices diagonales

$$I_2, -I_2, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

d'ordre respectivement 1, 2 et 2. Ces matrices ont des polynômes minimaux 2 à 2 distincts, deux d'entre elles ne peuvent être dans la même classe de conjugaison.

- (b) Un sous-groupe fini de $\text{GL}_2(\mathbf{Q})$ est *a fortiori* un sous-groupe fini de $\text{GL}_2(\mathbf{R})$, donc d'après Q30 est cyclique ou isomorphe à un groupe diédral.

Cas cyclique : la question précédente a montré que les ordres possibles pour une matrice d'ordre fini de $\text{GL}_2(\mathbf{Q})$ sont 1, 2, 3, 4 ou 6 ce qui donne les cas $\{I_2\}$, $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$ et $\mathbf{Z}/6\mathbf{Z}$.

Cas diédral : si $G \cong D_n$, alors G contient un sous-groupe cyclique de cardinal n , donc n vaut 1, 2, 3, 4 ou 6. On peut écarter le cas $n = 1$ qui redonne $G \cong \mathbf{Z}/2\mathbf{Z}$. On réalise effectivement un tel groupe en prenant pour G le groupe engendré par $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et l'une des matrices de la question précédente.

—— 6. Matrices d'ordre fini dans $GL_2(\mathbf{Z}/p\mathbf{Z})$ ——

35. Se donner une matrice $M \in GL_2(\mathbf{Z}/p\mathbf{Z})$ revient à choisir une première colonne C_1 non nulle, soit $p^2 - 1$ possibilités, et une deuxième colonne C_2 qui n'est pas dans $\text{Vect}(C_1)$, soit $p^2 - p$ possibilités. Au total, il y a $(p^2 - 1)(p^2 - p)$ éléments dans $GL_2(\mathbf{Z}/p\mathbf{Z})$.
36. D'après Cayley-Hamilton, le polynôme minimal μ_M de M est de degré d au plus égal à 2. Le morphisme d'algèbres surjectif $P \mapsto P(M)$ a pour noyau $\mu_M \mathbf{Z}/p\mathbf{Z}[X]$, d'où l'isomorphisme

$$(\mathbf{Z}/p\mathbf{Z})[X]/\mu_M(\mathbf{Z}/p\mathbf{Z})[X] \cong \mathbf{Z}/p\mathbf{Z}[M].$$

On en déduit que $|\mathbf{Z}/p\mathbf{Z}[M]| = p^d \leq p^2$

37. Soit $M \in GL_2(\mathbf{Z}/p\mathbf{Z})$ et notons r son ordre. Alors les r matrices $I_2, M, M^2, \dots, M^{r-1}$ sont des éléments distincts de $(\mathbf{Z}/p\mathbf{Z}[M])^*$, qui est de cardinal $p^2 - 1$. Donc $r \leq p^2 - 1$.
38. (a) Le polynôme minimal de M étant de degré 2, on a $\chi_M = \mu_M$, si bien que M est cyclique d'après Q16. On sait alors par Q17 que le commutant de M est $(\mathbf{Z}/p\mathbf{Z})[M]$, donc $\text{Stab}(M) = (\mathbf{Z}/p\mathbf{Z})[M] \cap GL_2(\mathbf{Z}/p\mathbf{Z})$.
- (b) Supposons que M n'admet pas de valeurs propres dans $\mathbf{Z}/p\mathbf{Z}$. Les éléments de $(\mathbf{Z}/p\mathbf{Z})[M]$ sont de la forme $aM + bI_2$ avec $a, b \in \mathbf{Z}/p\mathbf{Z}$. Une telle matrice est non inversible si $a = 0$ et $b = 0$ (c'est la matrice nulle) ou si $a \neq 0$ et $-\frac{b}{a}$ est une valeur propre de M , ce qui est exclu ici. Donc toutes les matrices $aM + bI_2$ sont inversibles sauf la matrice nulle. Il y en a $p^2 - 1$.
- (c) Supposons que M admettent une unique valeur propre λ dans $\mathbf{Z}/p\mathbf{Z}$. Une matrice $aM + bI_2$ est non inversible si elle est nulle ou si $-\frac{b}{a} = \lambda$. En choisissant a non nul ($p - 1$ possibilités), la valeur de b est nécessairement $-a\lambda$. Il y a donc $p - 1$ telles matrices plus la matrice nulle, soit p matrices non inversibles dans $(\mathbf{Z}/p\mathbf{Z})[M]$. Donc $|\text{Stab}(M)| = p^2 - p$.
39. D'après Q37, l'ordre d'une matrice de $GL_2(\mathbf{Z}/3\mathbf{Z})$ est majoré par $3^2 - 1 = 8$ et doit diviser le cardinal de $GL_2(\mathbf{Z}/3\mathbf{Z})$ qui est 48 d'après Q35. Les seules possibilités sont 1, 2, 3, 4, 6 et 8.
40. (a) En caractéristique 3, $X^6 - 1 = (X^2 - 1)^3 = (X - 1)^3(X + 1)^3$, donc $X^6 - 1$ est scindé dans $\mathbf{Z}/3\mathbf{Z}$.
- (b) Soit M une matrice d'ordre 6. Alors son polynôme minimal divise $X^6 - 1$ qui est scindé, donc M est trigonalisable. Si M est diagonalisable, alors M est semblable à $\pm I_2$ ou à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ qui sont d'ordre 1 ou 2. On en déduit que M n'est pas diagonalisable.

Si M a une unique valeur propre, elle est semblable à $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ ou $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On a $B^3 = I_2$ donc B ne convient pas et A bien d'ordre 6 puisque $A^n = \begin{pmatrix} (-1)^n & n(-1)^{n-1} \\ 0 & (-1)^n \end{pmatrix}$.

Réciproquement, une matrice semblable à A est d'ordre 6.

- (c) Déterminer le nombre de matrices d'ordre 6 revient à calculer $|\text{Stab}(A)|$. D'après Q38(c), son cardinal est $3^2 - 3 = 6$. Il y a donc par la formule des classes rappelée en début de partie, $\frac{48}{6} = 8$ matrices d'ordre 6.
41. On a $X^3 - 1 = (X - 1)^3$, donc une matrice d'ordre 3 est trigonalisable. On voit rapidement que M est d'ordre 3 si et seulement si M est semblable à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Le stabilisateur de cette matrice est de cardinal $3^2 - 3 = 6$ d'après Q38(c), il y a donc $\frac{48}{6} = 8$ matrices d'ordre 3.

42. (a) On a $X^8 - 1 = (X^4 - 1)(X^4 + 1) = (X - 1)^2(X + 1)^2(X^4 + 1)$. Le polynôme $X^4 + 1$ n'a pas de racines dans $\mathbf{Z}/3\mathbf{Z}$. En recherchant une décomposition de $X^4 + 1$ sous la forme $(X^2 + aX + b)(X^2 + a'X + b')$ où $a, b, a', b' \in \mathbf{Z}/3\mathbf{Z}$, on trouve rapidement que $X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$ et les deux trinômes sont irréductibles car sans racines dans $\mathbf{Z}/3\mathbf{Z}$. La décomposition en irréductibles dans $\mathbf{Z}/3\mathbf{Z}[X]$ est

$$X^8 - 1 = (X - 1)^2(X + 1)^2(X^2 + X + 2)(X^2 + 2X + 2).$$

- (b) Une matrice de $GL_2(\mathbf{Z}/3\mathbf{Z})$ est d'ordre 8 si et seulement si son polynôme minimal divise $X^8 - 1$ et ne divise pas $X^4 - 1$. Ce polynôme étant de degré 2 (sinon $M = \lambda I_2$ qui est d'ordre au plus 3), les seules possibilités sont $X^2 + X - 1$ et $X^2 - X - 1$.
- (c) On peut exhiber une matrice d'ordre 8 en considérant les matrices compagnons

$$C_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ ou } C_2 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

- (d) Leurs stabilisateurs sont de cardinal $3^2 - 1 = 8$ d'après Q38(c), il y a donc $\frac{48}{8} = 6$ matrices semblables à C_1 et aussi 6 matrices semblables à C_2 , ce qui donne au total 12 matrices d'ordre 8.

43. On montre de même qu'une matrice M est d'ordre 4 si et seulement si son polynôme minimal est $X^2 + 1$ qui n'a pas de racines dans $\mathbf{Z}/3\mathbf{Z}$. Une matrice d'ordre 4 est par exemple

$$C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

et il y a $3^2 - 1 = 8$ matrices semblables à C , donc $\frac{48}{8} = 6$ matrices d'ordre 4 dans $GL_2(\mathbf{Z}/3\mathbf{Z})$.

44. (a) Une matrice d'ordre 2 autre que $-I_2$ a pour polynôme minimal $X^2 - 1$, donc est diagonalisable avec pour spectre $\{-1, 1\}$.
- (b) Le stabilisateur de M est l'ensemble des matrices de la forme $aM + bI_2$ qui sont inversibles. Une telle matrice n'est pas inversible si elle est nulle ou si $\frac{b}{a} = \pm 1$. Ce sont les matrices $M \pm I_2$ et $\pm M + I_2$, il y a donc 5 matrices non inversibles de cette forme, et $|\text{Stab}(M)| = 9 - 5 = 4$. Par la formule des classes, il y a $\frac{48}{4} = 12$ matrices semblables à M . En rajoutant $-I_2$, cela fait 13 éléments d'ordre 2.