

Dans la suite nous utiliserons la propriété suivante.

Lemme. Si $(u_0, u_1, \dots, u_{n-1})$ est un cycle pour f , alors pour tout $i \in \llbracket 0, n-1 \rrbracket$ et tout $k \in \mathbb{N}$,

$$f^k(u_i) = u_{i \oplus k}$$

où $i \oplus k$ est le reste de la division euclidienne de $i + k$ par n .

Démonstration. C'est évident pour $k = 0$ et $k = 1$. Soit $k \in \mathbb{N}$. Supposons la propriété vérifiée pour k . Pour tout $i \in \llbracket 0, n-1 \rrbracket$,

$$f^{k+1}(u_i) = f(f^k(u_i)) = f(u_{i \oplus k}) = u_{(i \oplus k) \oplus 1} = u_{i \oplus (k \oplus 1)} = u_{i \oplus (k+1)}$$

Partie I

1. Soit $(u_0, \dots, u_{n-1})$ un cycle pour f . Soient $0 \leq i < j \leq n-1$. Supposons que $u_i = u_j$. On a alors

$$f^{n-j}(u_i) = f^{n-j}(u_j)$$

$$u_{i \oplus (n-j)} = u_{j \oplus (n-j)}$$

Remarquons que $i \oplus (n-j) = i + n - j \in \llbracket 1, n-1 \rrbracket$ et $j \oplus (n-j) = 0$. On a donc

$$u_{i+n-j} = u_0$$

Contradiction puisque pour tout $p \in \llbracket 1, n-1 \rrbracket$, $u_p \neq u_0$.

2. La famille (u_0, u_1) est de cardinal $2 = \dim E$. Supposons que cette famille est liée. Tout d'abord, $u_0 \neq 0$. Sinon, pour tout $k \in \llbracket 0, n-1 \rrbracket$, $u_k = f^k(u_0) = 0$. Ce n'est pas possible car la famille $(0)_{0 \leq k \leq n-1}$ n'est pas génératrice de E . Il existe donc $\lambda \in \mathbb{R}$ tel que $u_1 = \lambda u_0$. Mais alors, pour tout $k \in \llbracket 0, n-1 \rrbracket$, $u_k = f^k(u_0) = \lambda^k u_0$. Ici encore, on a une impossibilité car la famille $(\lambda^k u_0)_{0 \leq k \leq n-1}$ est de rang 1.
3. On a $f^n(u_0) = u_0$ et $f^n(u_1) = u_1$. Les endomorphismes f^n et id_E coïncident sur la base (u_0, u_1) de E . On a donc, par linéarité, $f^n = \text{id}_E$.

Soit $k \in \llbracket 1, n-1 \rrbracket$. On a $f^k(u_0) = u_k \neq u_0$. Les endomorphismes f^k et id_E diffèrent en au moins un vecteur, donc $f^k \neq \text{id}_E$.

4. Soient $m, n \geq 2$. Supposons que f est cyclique d'ordre m et aussi cyclique d'ordre n . Par exemple, $m \leq n$. Par I.3, comme f est cyclique d'ordre m , $f^m = \text{id}_E$. Toujours par I.3, pour tout $k \in \llbracket 1, n-1 \rrbracket$, $f^k \neq \text{id}_E$, et donc $m \notin \llbracket 1, n-1 \rrbracket$. Ainsi, $m = n$.
5. Soit $f = -\text{id}_E$. On a $f \neq \text{id}_E$ et $f^2 = \text{id}_E$. Cependant, pour tout $u_0 \in E$, $u_1 = f(u_0) = -u_0$. La famille (u_0, u_1) n'est donc pas génératrice de E , et donc f n'est pas cyclique d'ordre 2.
6. Soit $f \in \mathcal{L}(E)$. Montrons que f est cyclique d'ordre 2 si et seulement si f est une symétrie par rapport à une droite.

($\Rightarrow$) Supposons que f est cyclique d'ordre 2. On a $f^2 = \text{id}_E$ donc f est une symétrie. De plus, $f \neq \text{id}_E$ et comme nous l'avons vu au I.5, $f \neq -\text{id}_E$. Donc, f est une symétrie par rapport à une droite.

($\Leftarrow$) Supposons que f est la symétrie par rapport à la droite $D = \langle u \rangle$ parallèlement à la droite $D' = \langle u' \rangle$, où u et u' sont deux vecteurs de E non colinéaires. Posons $u_0 = u + u'$ et $u_1 = f(u_0)$. On a

$$u_1 = f(u) + f(u') = u - u'$$

- La famille (u_0, u_1) est clairement libre. Comme elle est de cardinal 2, elle est génératrice.
- On a $f(u_0) = u_1$ et $f(u_1) = f(u) - f(u') = u + u' = u_0$.
- Enfin, $u_1 \neq u_0$.

Ainsi, f est cyclique d'ordre 2 et (u_0, u_1) est un cycle pour f .

7. Soient u_0 et u_1 les deux premiers vecteurs d'un cycle pour f . La famille $\mathcal{B} = (u_0, u_1)$ est une base de E . Posons $f(u_1) = au_0 + bu_1$ où $a, b \in \mathbb{R}$. La matrice de f dans la base $\mathcal{B}$ est alors $A_{a,b}$.
8. De $f^n = \text{id}_E$ on déduit $A_{a,b}^n = I_2$ et donc $(\det A_{a,b})^n = \det I_2 = 1$. Or, $\det A_{a,b} = -a$. On a donc $(-a)^n = 1$.
 - Si n est impair, alors $a = -1$.
 - Si n est pair, alors, *a priori*, $a = \pm 1$.
9. Facilement,

$$A_{a,b}^2 = aI_2 + bA_{a,b}$$

Par l'isomorphisme $\text{mat}_{\mathcal{B}}$,

$$f^2 = a\text{id}_E + bf$$

10. Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E . Supposons que dans ces bases, les matrices de f sont $A_{a,b}$ et $A_{\alpha,\beta}$. On a donc

$$f^2 = a\text{id}_E + bf = \alpha\text{id}_E + \beta f$$

et donc

$$(a - \alpha)\text{id}_E + (b - \beta)f = 0$$

On vérifie facilement que les multiples de id_E (les homothéties) ne sont pas cycliques. Ainsi, la famille (id_E, f) est libre dans l'espace vectoriel $\mathcal{L}(E)$ et donc $a - \alpha = b - \beta = 0$.

11. (a) Montrons que f est cyclique d'ordre 2 si et seulement si $a = 1$ et $b = 0$.

($\Rightarrow$) Supposons que f est cyclique d'ordre 2. On a

$$f^2 = \text{id}_E = 1\text{id}_E + 0f$$

et donc $a = 1$ et $b = 0$.

($\Leftarrow$) Supposons $a = 1$ et $b = 0$. Soit $\mathcal{B} = (u_0, u_1)$ une base dans laquelle $\text{mat}_{\mathcal{B}}f = A_{a,b}$. On a $f(u_0) = u_1$ et $f(u_1) = u_0$. Les autres propriétés de cyclicité sont immédiates (base). De là, f est cyclique d'ordre 2 et $\mathcal{B}$ est un cycle pour f .

- (b) Montrons que f est cyclique d'ordre 3 si et seulement si $a = b = -1$.

($\Rightarrow$) Supposons que f est cyclique d'ordre 3. Par I.8, $a = -1$. On a donc

$$f^2 = -\text{id}_E + bf$$

De là,

$$\text{id}_E = f^3 = -f + bf^2 = -f + b(-\text{id}_E + bf) = -b\text{id}_E + (b^2 - 1)f$$

Comme (id_E, f) est libre, il vient $b = -1$.

($\Leftarrow$) Supposons que $a = b = -1$. Soit $\mathcal{B} = (u_0, u_1)$ une base de E dans laquelle la matrice de f est $A_{a,b}$. Posons aussi $u_2 = f(u_1)$. On a

$$u_2 = -u_0 - u_1$$

De là,

$$f(u_2) = -f(u_0) - f(u_1) = -u_1 - u_2 = u_0$$

On vérifie ensuite facilement toutes les propriétés de cycle pour (u_0, u_1, u_2) . Ainsi, f est cyclique d'ordre 3.

12. Soit $\mathcal{B} = (e_1, e_2)$ la base canonique de $\mathbb{R}^2$. Posons $u_0 = e_1$, $u_1 = g(u_0)$ et $u_2 = g(u_1)$. On a facilement

$$\begin{aligned} u_0 &= (1, 0) \\ u_1 &= (1, 1) \\ u_2 &= (-2, -1) \end{aligned}$$

De plus, $g(u_2) = u_0$. La famille $\mathcal{G} = (u_0, u_1, u_2)$ est clairement de rang 2, donc génératrice. De plus, $u_1, u_2 \neq u_0$. Ainsi, g est cyclique d'ordre 3 et $\mathcal{G}$ est un cycle pour g . Enfin, par I.11, $a = b = -1$.

Partie II

1. (a) Le discriminant de P est $\Delta = b^2 + 4a$. Comme P a une racine double, $\Delta = 0$, c'est à dire $b^2 = -4a$. Par I.8, $a = \pm 1$. Or, $b \in \mathbb{R}$, donc $b^2 \neq -4$. Donc $a = -1$. De là, $b^2 = 4$ donc $b = \pm 2$.
- (b) On a $U = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$. De là, $U^2 = 0$ et donc pour tout $k \geq 2$, $U^k = 0$. Comme U et I_2 commutent on a alors, par le binôme de Newton,

$$A_{a,b}^n = (I_2 + U)^n = I_2 + nU \neq I$$

Contradiction. Ainsi, $b \neq 2$.

- (c) Soit $V = A + I_2$. On a $V = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$. De là, $V^2 = 0$ et donc pour tout $k \geq 2$, $V^k = 0$. Comme V et I_2 commutent on a alors, par le binôme de Newton,

$$A_{a,b}^n = (-I_2 + V)^n = (-1)^n(I_2 - nV) \neq I$$

Contradiction (un peu moins évidente, laissée au lecteur). Ainsi, $b \neq -2$.

- (d) Le polynôme P n'a pas de racine double.
2. Remarquons que par les relations coefficients-racines, $\alpha + \beta = b$ et $\alpha\beta = -a$.

- (a) On a

$$(f - \alpha \text{id}_E) \circ (f - \beta \text{id}_E) = f^2 - (\alpha + \beta)f + \alpha\beta \text{id}_E = f^2 - bf - a \text{id}_E$$

Or, $f^2 = a \text{id}_E + bf$, d'où le résultat.

- (b) Facilement, βid_E n'est pas cyclique (les deux premiers vecteurs d'un éventuel cycle seraient liés), donc $f \neq \beta \text{id}_E$. Soit $x \in E$ tel que $f(x) \neq \beta x$. Soit $y = f(x) - \beta x$. On a $y \neq 0$ et

$$(f - \alpha \text{id}_E)(y) = 0$$

Ainsi, $\ker(f - \alpha \text{id}_E) \neq \{0\}$, donc $f - \alpha \text{id}_E$ n'est pas injectif.

- (c) Voir question précédente.

- (d) Soit $u \neq 0$ tel que $f(u) = \alpha u$. On a $f^n(u) = \alpha^n u$. Or, $f^n = \text{id}_E$. Ainsi,

$$\alpha^n u = u$$

Or, $u \neq 0$, donc $\alpha^n = 1$ d'où $\alpha = \pm 1$.

- (e) On a $\alpha = \pm 1$, $\beta = \pm 1$ et $\alpha \neq \beta$. Donc $\{\alpha, \beta\} = \{-1, 1\}$.

Dans la suite, nous prenons $\alpha = 1$ et $\beta = -1$.

(f) Il suffit de prouver que (u, v) est libre. Soient $a, b \in \mathbb{R}$ tels que

$$(1) \quad au + bv = 0$$

En appliquant f , il vient

$$(2) \quad au - bv = 0$$

En additionnant (1) et (2), on obtient $2au = 0$. Or, $u \neq 0$, donc $a = 0$. De même, on soustrait et on obtient $b = 0$.

(g) On a $f \neq \text{id}_E$ et $f \neq -\text{id}_E$. De plus, $f^2(u) = u$ et $f^2(v) = -f(v) = v$. Les endomorphismes f^2 et id_E coïncident sur la base (u, v) donc, par linéarité, $f^2 = \text{id}_E$. Ainsi, f est une symétrie par rapport à une droite donc, par I.8, f est cyclique d'ordre 2.

3. Supposons $n \geq 3$. Par II.1, P n'a pas de racine double. Par II.2, P n'a pas deux racines distinctes. Donc, P n'a pas de racine réelle. Ou, si l'on préfère, P a deux racines non réelles distinctes (conjuguées).

Allons un peu plus loin. On a

$$\Delta = b^2 + 4a < 0$$

et donc $a < 0$. Or, $a = \pm 1$, donc $a = -1$. De là,

$$b^2 < 4$$

donc $b \in]-2, 2[$. On peut donc poser

$$b = 2 \cos \theta$$

où $\theta \in]0, \pi[$. Les racines de P sont alors $e^{\pm i\theta}$. Effectuons la division euclidienne de $X^n - 1$ pour obtenir

$$X^n - 1 = PQ + \alpha X + \beta$$

En « évaluant » en f , on obtient

$$0 = \alpha f + \beta \text{id}_E$$

Par la liberté de la famille (id_E, f) , on en déduit $\alpha = \beta = 0$. Ainsi, P divise $X^n - 1$ et donc $e^{i\theta}$ est racine de $X^n - 1$, c'est à dire une racine n ème de l'unité.

On peut aller encore plus loin et montrer qu'en munissant E d'un produit scalaire judicieux, f est alors une rotation de E d'angle $\frac{2k\pi}{n}$ où $k \in \llbracket 1, n-1 \rrbracket$ est premier avec n .