

Exercice I

- 1) Soit u et v dans G^2 . L'endomorphisme $u \circ v$ appartient à G donc $(u \circ v)^2 = \text{id}_E$ ce qui implique que $(u \circ v) = (u \circ v)^{-1} = v^{-1} \circ u^{-1}$. En remarquant que l'on a aussi $u = u^{-1}$ et $v = v^{-1}$ on obtient

$$u \circ v = v^{-1} \circ u^{-1} = v \circ u$$

- 2) Soit $u \in G$. Par définition, les éléments de G sont des symétries vectorielles. On sait alors que les valeurs propres appartiennent à $\{\pm 1\}$. Plus précisément :
- Si $u = \text{id}_E$ (la symétrie par rapport à E en entier et parallèlement à $\{0\}$) la seule valeur propre est 1. Dans ce cas u est diagonalisable.
 - Si $u = -\text{id}_E$ (la symétrie par rapport à $\{0\}$ et parallèlement à E en entier) la seule valeur propre est -1 . Dans ce cas u est diagonalisable.
 - Sinon $F = \text{Ker}(u - \text{id}_E)$ et $G = \text{Ker}(u + \text{id}_E)$ sont des sous-espaces vectoriels non triviaux de E tels que $E = F \oplus G$ et u est la symétrie par rapport à F parallèlement à G . En particulier, le spectre de u est $\{-1, 1\}$ et u est diagonalisable.

- 3) Soit u et v deux éléments de G .

- a) Comme u et v commutent (question 1), d'après le cours les sous-espaces propres de u sont stables par v .
- b) Considérons, v_+ et v_- les endomorphismes induits par v sur $E_1(u)$ et $E_{-1}(u)$ respectivement. Ils vérifient encore que $v_+^2 = \text{id}_{E_1(u)}$ et $v_-^2 = \text{id}_{E_{-1}(u)}$. Cela implique que v_+ et v_- sont des symétries et sont donc diagonalisables.

Il existe donc une base \mathcal{B}_+ de $E_1(u)$ telle que $\text{Mat}_{\mathcal{B}_+}(v_+)$ est diagonale. L'endomorphisme u_+ induit par u sur $E_1(u)$ est $\text{id}_{E_1(u)}$, sa matrice dans toute base est diagonale.

De même il existe une base \mathcal{B}_- de $E_{-1}(u)$ dans laquelle la matrice de v_- est diagonale ainsi que celle de $u_- = -\text{id}_{E_{-1}(u)}$.

On considère alors la base \mathcal{B} de E obtenue en concaténant les deux bases \mathcal{B}_+ et \mathcal{B}_- . Les matrices $\text{Mat}_{\mathcal{B}}(u)$ et $\text{Mat}_{\mathcal{B}}(v)$ sont diagonales.

- 4) Procédons par récurrence sur l'entier r pour montrer que pour tout $r \geq 1$, $\mathcal{P}(r)$ où $\mathcal{P}(r) : \ll$ Pour tout u_1, \dots, u_r des symétries de E qui commutent deux à deux, il existe une base \mathcal{B} tel que pour tout i compris entre 1 et r , $\text{Mat}_{\mathcal{B}}(u_i)$ sont diagonales \gg .

— Initialisation : Le cas $r = 1$ est évident et le cas $r = 2$ a été traité dans la question 3.

— Soit $r \geq 2$, on suppose $\mathcal{P}(r)$ et on montre $\mathcal{P}(r+1)$. On considère u_1, \dots, u_{r+1} des symétries de E qui commutent deux à deux.

L'endomorphisme u_{r+1} est une symétrie. Notons $E_+ = \text{Ker}(u_{r+1} - \text{id}_E)$ et $E_- = \text{Ker}(u_{r+1} + \text{id}_E)$. Ces s.e.v. sont supplémentaires dans E .

Comme ci-dessus, u_1, \dots, u_r commutent à u_{r+1} donc E_+ et E_- sont stables par u_1, \dots, u_r . On note $u_{i,+}$ et $u_{i,-}$ les endomorphismes induits par u_i sur E_+ et E_- respectivement. Ce sont encore des symétries et elles commutent deux à deux.

De ce fait, d'après $\mathcal{P}(r)$, il existe une base \mathcal{B}_+ de E_+ telle que les matrices des endomorphismes $u_{1,+}, \dots, u_{r,+}$ dans la base \mathcal{B}_+ soient diagonales. Comme $u_{r+1,+} = \text{id}_{E_+}$, sa matrice dans cette base est aussi diagonale.

De même, il existe une base \mathcal{B}_- de E_- telle que les matrices des endomorphismes $u_{1,-}, \dots, u_{r+1,-}$ dans la base \mathcal{B}_- soient diagonales.

En concaténant les bases \mathcal{B}_+ et \mathcal{B}_- , on obtient une base \mathcal{B} de E telle que les matrices des endomorphismes u_1, \dots, u_r, u_{r+1} dans la base \mathcal{B} soient diagonales. Cela prouve $\mathcal{P}(r+1)$.

— Conclusion : pour tout $r \in \mathbf{N}^*$, $\mathcal{P}(r)$ est vrai.

5) Soit $p \in \mathbf{N}$ tel qu'il existe p éléments u_1, \dots, u_p de G deux à deux distincts. D'après la question précédente, il existe une base \mathcal{B} telle que toutes les matrices $M_i = \text{Mat}_{\mathcal{B}}(u_i)$ soient diagonales. Comme de plus les spectres des éléments de G sont inclus dans $\{\pm 1\}$ les éléments diagonaux de ces matrices sont inclus dans $\{\pm 1\}$. Comme il n'y a que 2^n matrices diagonales dans $\mathcal{M}_n(\mathbf{K})$ dont les coefficients diagonaux valent -1 ou 1 (une telle matrice est uniquement déterminée par n -uplet de ses coefficients diagonaux), et comme $u \mapsto \text{Mat}_{\mathcal{B}}(u)$ est injective, on a $p \leq 2^n$.

Ainsi toute partie finie de G contient au plus 2^n éléments.

On en déduit que G est fini et que $\text{Card}(G) \leq 2^n$.

6) Pour tout entier n , on identifie, $\text{GL}_n(\mathbf{K})$ avec $\text{GL}(\mathbf{K}^n)$.

Soit p et q deux entiers non nuls distincts. Par symétrie, on peut supposer $p < q$. Supposons par l'absurde qu'il existe un isomorphisme de groupes $\varphi : (\text{GL}_q(\mathbf{K}), \times) \rightarrow (\text{GL}_p(\mathbf{K}), \times)$. On considère le sous-groupe H de $\text{GL}_q(\mathbf{K})$ composé des matrices diagonales ayant des 1 ou -1 sur la diagonale :

$$H = \left\{ \left(\begin{array}{cccc} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varepsilon_q \end{array} \right), (\varepsilon_1, \dots, \varepsilon_q) \in \{\pm 1\}^q \right\}$$

On vérifie que H est un sous-groupe de $\text{GL}_q(\mathbf{K})$ dont tous les éléments sont des symétries. De plus son cardinal est 2^q . Maintenant, $\varphi(H)$ est un sous-groupe de $\text{GL}_p(\mathbf{K})$ qui est aussi de cardinal 2^q car φ est bijective. On pour tout $x \in \varphi(H)$, il existe $h \in H$ tel que $x = \varphi(h)$ et on a

$$x^2 = (\varphi(h))^2 = \varphi(h^2) = \varphi(I_q) = I_p$$

On en déduit que le cardinal de $\varphi(H)$ est inférieur ou égal à 2^p ce qui est absurde.

Finalement $(\text{GL}_q(\mathbf{K}), \times)$ et $(\text{GL}_p(\mathbf{K}), \times)$ ne sont pas isomorphes.

Exercice II

1) Soit $j \in \llbracket 1, n \rrbracket$,

$$f_\sigma(e_j) = \sum_{i=1}^n P_\sigma[i, j] e_i = 1 \cdot e_{\sigma(j)} = e_{\sigma(j)}$$

2) Pour tout $j \in \llbracket 1, n \rrbracket$, $f_\sigma \circ f_{\sigma'}(e_j) = f_\sigma(e_{\sigma'(j)}) = e_{\sigma(\sigma'(j))} = f_{\sigma \circ \sigma'}(e_j)$.

Comme (e_1, \dots, e_n) est une base, $f_\sigma \circ f_{\sigma'} = f_{\sigma \circ \sigma'}$ donc $P_\sigma P_{\sigma'} = P_{\sigma \circ \sigma'}$.

En particulier $P_\sigma P_{\sigma^{-1}} = P_{\sigma \circ \sigma^{-1}} = P_{id} = I_n$ (où id est l'identité de $\llbracket 1, n \rrbracket$). Donc $P_{\sigma^{-1}}$ est inverse à droite de P_σ . Comme P_σ est une matrice carrée, elle est inversible et son inverse est $P_{\sigma^{-1}}$;

3) Supposons σ et σ' conjuguées. Soit $\tau \in S_n$ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$.

Alors $P_{\sigma'} = P_\tau P_\sigma (P_\tau)^{-1}$ donc P_σ et $P_{\sigma'}$ sont semblables.

4) a) Notons $\gamma_1, \dots, \gamma_p$ les cycles de la décomposition de σ en cycles à supports disjoints, l_1, \dots, l_p leurs longueurs. Choisissons i_1 dans le support de γ_1, \dots, i_p dans le support de γ_p .

Soient enfin j_1, \dots, j_q les points fixes de σ .

Dans la base $(e_{i_1}, e_{\sigma(i_1)}, \dots, e_{\sigma^{l_1-1}(i_1)}, \dots, e_{i_p}, \dots, e_{\sigma^{l_p-1}(i_p)}, e_{j_1}, \dots, e_{j_q})$ la matrice de f_σ est dia-

gonale par blocs avec p blocs diagonaux de la forme : $\begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & & \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$ et $q = c_1(\sigma)$ blocs

égaux à (1) et de polynôme caractéristique $X - 1$.

Un bloc de la première forme de taille l_k a pour polynôme caractéristique

$$\begin{vmatrix} X & \dots & \dots & 0 & -1 \\ -1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \\ 0 & \dots & 0 & -1 & X \end{vmatrix} = (-1)^{l_k+1}(-1) \begin{vmatrix} -1 & X & & \\ 0 & \ddots & \ddots & \\ \vdots & & \ddots & X \\ 0 & \dots & 0 & -1 \end{vmatrix} + (-1)^{2l_k} X \begin{vmatrix} X & \dots & \dots & 0 \\ -1 & \ddots & & \\ 0 & \ddots & \ddots & \\ 0 & \dots & -1 & X \end{vmatrix}$$

par développement selon la dernière colonne.

Les matrices obtenues étant triangulaires, on obtient

$$(-1)^{l_k+2+l-k-1} + X^k = X^k - 1$$

Ainsi $\chi_{P_\sigma} = \prod_{k=1}^n (X^k - 1)^{c_k(\sigma)}$.

b) Soit $m \in \llbracket 1, n \rrbracket$. Montrer que $\sum_{m|k} c_k(\sigma) = \sum_{m|k} c_k(\sigma')$.

Posons $z = e^{\frac{2i\pi}{m}}$. z est racine simple de $X^k - 1$ si $m|k$ et n'est pas racine sinon.

Comme P_σ et $P_{\sigma'}$ sont supposées semblables, elles ont même polynôme caractéristique, donc z a même ordre de multiplicité dans ces deux polynômes.

Ainsi $\sum_{m|k} c_k(\sigma) = \sum_{m|k} c_k(\sigma')$.

c) On procède par récurrence forte descendante sur m .

$$c_n(\sigma) = \sum_{n|k} c_k(\sigma) = \sum_{n|k} c_k(\sigma') = c_n \sigma'$$

Soit $m \in \llbracket 1, n-1 \rrbracket$. Supposons que $\forall k \in \llbracket m+1, n \rrbracket \quad c_k(\sigma) = c_k(\sigma')$.

Comme $c_m(\sigma) + \sum_{m|k, k>m} c_k(\sigma) = c_m(\sigma') + \sum_{m|k, k>m} c_k(\sigma')$ on en déduit que $c_m(\sigma) = c_m(\sigma')$.

Ainsi

$$\forall m \in \llbracket 1, n \rrbracket, \quad c_m(\sigma) = c_m(\sigma')$$

d) Soit $\gamma = (a_1, \dots, a_p)$ et $\tau \in S_n$.

Pour tout $i \in \llbracket 1, p-1 \rrbracket$, $\tau \circ \gamma \circ \tau^{-1}(\tau(a_i)) = \tau(a_{i+1})$

$\tau \circ \gamma \circ \tau^{-1}(\tau(a_p)) = \tau(a_1)$

et pour $i \in \llbracket 1, n \rrbracket \setminus \{\tau(a_1), \dots, \tau(a_p)\}$, $\tau \circ \gamma \circ \tau^{-1}(i) = \tau \circ \gamma(j)$ avec $j \notin \{a_1, \dots, a_p\}$ donc $\tau \circ \gamma \circ \tau^{-1}(i) = \tau(j) = i$

Ainsi $\tau \circ \gamma \circ \tau^{-1}$ est le cycle $(\tau(a_1), \dots, \tau(a_p))$.

e) En déduire que σ et σ' sont conjuguées.

Notons $(a_1, \dots, a_{p_1}) \circ (a_{p_1+1}, \dots, a_{p_2}) \circ \dots \circ (a_{p_{q-1}+1}, \dots, a_{p_q})$ avec $p_q = n$ la décomposition en cycles à supports disjoints de σ . Par abus, on fait intervenir chaque point fixe x de σ par un facteur (x) dans cette décomposition (bien que les 1-cycles n'existent pas).

Soit $(b_1, \dots, b_{p_1}) \circ (b_{p_1+1}, \dots, b_{p_2}) \circ \dots \circ (b_{p_{q-1}+1}, \dots, b_{p_q})$ celle de σ' , avec des cycles de même longueur aux mêmes positions que dans la décomposition de σ , ce qui est possible par la question précédente et car des cycles à supports disjoints commutent.

Soit τ la permutation telle que $\forall i \in \llbracket 1, n \rrbracket$, $\tau(a_i) = b_i$.

Alors

$$\begin{aligned} \tau \circ \sigma \circ \tau^{-1} &= \tau \circ (a_1, \dots, a_{p_1}) \circ \tau^{-1} \circ \tau \circ (a_{p_1+1}, \dots, a_{p_2}) \circ \tau^{-1} \circ \dots \circ \tau \circ (a_{p_{q-1}+1}, \dots, a_{p_q}) \circ \tau^{-1} \\ &= (b_1, \dots, b_{p_1}) \circ (b_{p_1+1}, \dots, b_{p_2}) \circ \dots \circ (b_{p_{q-1}+1}, \dots, b_{p_q}) \\ &= \sigma' \end{aligned}$$

Donc σ et σ' sont conjugués.