Exercice I

1) Soit u et v dans G^2. L'endomorphisme $u \circ v$ appartient à G donc $(u \circ v)^2 = \mathrm{id}_E$ 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 $u = \mathrm{id}_E$ (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 $u = -\mathrm{id}_E$ (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 $F = \mathrm{Ker}(u - \mathrm{id}_E)$ et $G = \mathrm{Ker}(u + \mathrm{id}_E)$ 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 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 $v_+^2 = \mathsf{id}_{E_1(u)}$ et $v_-^2 = \mathsf{id}_{E_{-1}(u)}$. Cela implique que v_+ et v_- sont des symétries et sont donc diagonalisables. Il existe donc une base $\mathscr{B}_+$ de $E_1(u)$ telle que $\mathsf{Mat}_{\mathscr{B}_+}(v_+)$ est diagonale et une base $\mathscr{B}_-$ de $E_{-1}(u)$ telle que $\mathsf{Mat}_{\mathscr{B}_-}(v_-)$ est diagonale.
      On considère alors la base $\mathscr{B}$ de E obtenue en concaténant les deux bases $\mathscr{B}_+$ et $\mathscr{B}_-$. Les matrices $\mathsf{Mat}_{\mathscr{B}}(u)$ et $\mathsf{Mat}_{\mathscr{B}}(v)$ sont diagonales.

4) Procédons par récurrence sur l'entier r pour montrer que pour tout $r \geqslant 1$, $\mathscr{P}(r)$ où $\mathscr{P}(r)$: « Pour tout $u_1, \ldots, u_r$ des symétries de E qui commutent deux à deux, il existe une base $\mathscr{B}$ tel que pour tout i compris entre 1 et r, $\mathsf{Mat}_{\mathscr{B}}(u_i)$ sont diagonales ».
   — Initialisation : Le cas $r = 1$ est évident et le cas $r = 2$ a été traité dans le question 3.
   — Soit $r \geqslant 2$, on suppose $\mathscr{P}(r)$ et on montre $\mathscr{P}(r+1)$. On considère $u_1, \ldots, u_{r+1}$ des symétries de E qui commutent deux à deux.
   Si $u_{r+1} = \mathrm{id}_E$ ou $-\mathrm{id}_E$, on est ramené au cas de r endomorphismes.
   Dans les autres cas, l'endomorphisme u_{r+1} est une symétrie, il est donc diagonalisable. Notons E_+ et E_- ses espaces propres.
   Comme ci-dessus, $u_1, \ldots, u_r$ commutent à u_{r+1} donc E_+ et E_- sont stables par u. 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 $\mathscr{P}(r)$, il existe une base $\mathscr{B}_+$ de E_+ telle que les matrices des endomorphismes $u_{1,+}, \ldots u_{r,+}$ dans la base $\mathscr{B}_+$ soient diagonales. De même, il existe une base $\mathscr{B}_-$ de E_- telle que les matrices des endomorphismes $u_{1,-}, \ldots u_{r,-}$ dans la base $\mathscr{B}_-$ soient diagonales. En concaténant les base $\mathscr{B}_+$ et $\mathscr{B}_-$, on obtient une base $\mathscr{B}$ de E telle que les matrices des endomorphismes $u_1, \ldots u_r, u_{r+1}$ dans la base $\mathscr{B}$ soient diagonales. Cela prouve $\mathscr{P}(r+1)$.
   — Conclusion : pour tout $r \in \mathbf{N}^*$, $\mathscr{P}(r)$ est vrai.

5) Posons $p = 2^n$. Supposons par l'absurde que l'on peut trouver $p+1$ éléments $u_1, \ldots u_{p+1}$ de G deux à deux distincts. D'après la question précédente, il existe une base $\mathscr{B}$ telle que toutes les matrices $M_i = \mathsf{Mat}_{\mathscr{B}}(u_i)$ 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 $2^n = p$ matrices diagonales dans $\mathscr{M}_n(\mathbf{K})$ dont les coefficients diagonaux valent -1 ou 1 (une telle matrice

est uniquement déterminée par n-uplet de ses coefficients diagonaux), il existe i et j compris entre 1 et $p+1$ tels que $M_i = M_j$ ce qui est absurde car les endomorphismes étaient supposés deux à deux distincts.

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

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

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 $\varphi : (\mathsf{GL}_q(\mathbf{K}), \times) \to (\mathsf{GL}_p(\mathbf{K}), \times)$. On considère le sous-groupe H de $\mathsf{GL}_q(\mathbf{K})$ composé des matrices diagonales ayant des 1 ou -1 sur la diagonale :

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

On vérifie que H est un sous-groupe de $\mathsf{GL}_q(\mathbf{K})$ dont tous les éléments sont des symétries. De plus son cardinal est 2^q. Maintenant, $\varphi(H)$ est un sous-groupe de $\mathsf{GL}_p(\mathbf{K})$ 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 $(\mathsf{GL}_q(\mathbf{K}), \times)$ et $(\mathsf{GL}_p(\mathbf{K}), \times)$ ne sont pas isomorphes.

Exercice II

1) Soit $j \in [\![1, n]\!]$,

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

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

Comme $(e_1, \ldots, e_n)$ 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 $[\![1, n]\!]$). 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 $\gamma_1, \ldots, \gamma_p$ les cycles de la décomposition de σ en cycles à supports disjoints, $l_1, \ldots, l_p$ leurs longueurs. Choisissons i_1 dans le support de γ_1, ..., i_p dans le support de γ_p.

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

Dans la base $(e_{i_1}, e_{\sigma(i_1)}, \ldots, e_{\sigma^{l_1-1}(i_1)}, e_{i_2}, \ldots, e_{\sigma^{l_p-1}(i_p)}, e_{j_1}, \ldots, e_{j_q})$ la matrice de f_σ est diagonale par blocs avec p blocs diagonaux de la forme : $\begin{pmatrix} 0 & \ldots & \ldots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & & \\ 0 & \ldots & 0 & 1 & 0 \end{pmatrix}$ 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 $m \in [\![1,n]\!]$. 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 $m \in [\![1,n-1]\!]$. Supposons que $\forall k \in [\![m+1,n]\!] \quad c_k(\sigma) = c_k(\sigma')$.
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

$$\forall m \in [\![1,n]\!], \quad c_m(\sigma) = c_m(\sigma')$$

d) Soit $\gamma = (a_1, \dots, a_p)$ et $\tau \in S_n$.
Pour tout $i \in [\![1,p-1]\!]$, $\tau \circ \gamma \circ \tau^{-1}(\tau(a_i)) = \tau(a_{i+1})$
$\tau \circ \gamma \circ \tau^{-1}(\tau(a_p)) = \tau(a_1)$
et pour $i \in [\![1,n]\!] \setminus \{\tau(a_1), \dots, \tau(a_p)\}$, $\tau \circ \gamma \circ \tau^{-1}(i) = \tau \circ \gamma(j)$ avec $j \notin \{a_1, \dots, a_p\}$ donc $\tau \circ \gamma \circ \tau^{-1}(i) = \tau(j) = i$
Ainsi $\boxed{\tau \circ \gamma \circ \tau^{-1} \text{ est le cycle } (\tau(a_1), \dots, \tau(a_p)).}$

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 $\forall i \in [\![1,n]\!]$, $\tau(a_i) = b_i$.
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.