Planche n° 19. Groupe symétrique. Corrigé

n° 1 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 10 & 7 & 1 & 2 & 6 & 4 & 5 & 12 & 8 & 9 & 11 \end{pmatrix}$.

1) Les inversions de σ sont :

$\{1,4\}$, $\{1,5\}$, $\{2,3\}$, $\{2,4\}$, $\{2,5\}$, $\{2,6\}$, $\{2,7\}$, $\{2,8\}$, $\{2,10\}$, $\{2,11\}$, $\{3,4\}$, $\{3,5\}$, $\{3,6\}$, $\{3,7\}$, $\{3,8\}$, $\{6,7\}$, $\{6,8\}$, $\{9,10\}$, $\{9,11\}$, $\{9,12\}$.

Au total, il y a $2+8+5+2+3 = 20$ inversions. σ est donc une permutation paire (de signature 1).

2) $\tau_{11,12} \circ \sigma = (3\ 10\ 7\ 1\ 2\ 6\ 4\ 5\ 11\ 8\ 9\ 12)$.
Puis, $\tau_{9,11} \circ \tau_{11,12} \circ \sigma = (3\ 10\ 7\ 1\ 2\ 6\ 4\ 5\ 9\ 8\ 11\ 12)$.
Puis, $\tau_{10,8} \circ \tau_{9,11} \circ \tau_{11,12} \circ \sigma = (3\ 8\ 7\ 1\ 2\ 6\ 4\ 5\ 9\ 10\ 11\ 12)$.
Puis, $\tau_{8,5} \circ \tau_{10,8} \circ \tau_{9,11} \circ \tau_{11,12} \circ \sigma = (3\ 5\ 7\ 1\ 2\ 6\ 4\ 8\ 9\ 10\ 11\ 12)$.
Puis, $\tau_{7,4} \circ \tau_{8,5} \circ \tau_{10,8} \circ \tau_{9,11} \circ \tau_{11,12} \circ \sigma = (3\ 5\ 4\ 1\ 2\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$.
Puis, $\tau_{5,2} \circ \tau_{7,4} \circ \tau_{8,5} \circ \tau_{10,8} \circ \tau_{9,11} \circ \tau_{11,12} \circ \sigma = (3\ 2\ 4\ 1\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$.
Puis, $\tau_{1,4} \circ \tau_{5,2} \circ \tau_{7,4} \circ \tau_{8,5} \circ \tau_{10,8} \circ \tau_{9,11} \circ \tau_{11,12} \circ \sigma = (3\ 2\ 1\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12) = \tau_{1,3}$.
Par suite,

$$\boxed{\sigma = \tau_{11,12} \circ \tau_{9,11} \circ \tau_{10,8} \circ \tau_{8,5} \circ \tau_{7,4} \circ \tau_{5,2} \circ \tau_{1,4} \circ \tau_{1,3}.}$$

3) $O(1) = \{1,3,4,7\} = O(3) = O(4) = O(7)$, puis $O(2) = \{2,5,8,10\}$ puis $O(6) = \{6\}$ et $O(9) = \{9,11,12\} = O(11) = O(12)$.
σ a 4 orbites, deux de cardinal 4, une de cardinal 3 et un singleton (correspondant à un point fixe).

4) σ est donc le produit commutatif des cycles $c_1 = \begin{pmatrix} 1 & 3 & 4 & 7 \\ 3 & 7 & 1 & 4 \end{pmatrix}$, $c_2 = \begin{pmatrix} 2 & 5 & 8 & 10 \\ 10 & 2 & 5 & 8 \end{pmatrix}$ et $c_3 = \begin{pmatrix} 9 & 11 & 12 \\ 12 & 9 & 11 \end{pmatrix}$.

On a $c_1^4 = c_2^4 = \mathrm{Id}$ et $c_3^3 = \mathrm{Id}$. Or, $2005 = 4 \times 501 + 1$. Donc, $c_1^{2005} = c_1(c_1^4)^{501} = c_1$, et de même $c_2^{2005} = c_2$. Puis, $c_3^{2005} = (c_3^3)^{668} c_3 = c_3$. Puisque c_1, c_2 et c_3 commutent,

$$\sigma^{2005} = c_1^{2005} c_2^{2005} c_3^{2005} = c_1 c_2 c_3 = \sigma = (3\ 10\ 7\ 1\ 2\ 6\ 4\ 5\ 12\ 8\ 9\ 11).$$

$$\boxed{\sigma^{2005} = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 10 & 7 & 1 & 2 & 6 & 4 & 5 & 12 & 8 & 9 & 11 \end{pmatrix}.}$$

n° 2 : $(S_n, \circ)$ est engendré par les transpositions. Il suffit donc de montrer que pour $2 \leq i < j \leq n$, la transposition $\tau_{i,j}$ est produit des $\tau_{1,k}$, $2 \leq k \leq n$.

Mais $\tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i} = (i1j)(ji1)(i1j) = (1ij) = \tau_{i,j}$ ce qu'il fallait démontrer.

n° 3 : Les éléments de A_n sont les produits pairs de transpositions. Il suffit donc de vérifier qu'un produit de deux transpositions est un produit de cycles de longueur 3.
Soient i, j et k trois éléments deux à deux distincts de $\{1, ..., n\}$. $\tau_{i,k} \circ \tau_{i,j}$ est le 3-cycle : $i \to j$ $j \to k$ $k \to i$, ce qui montre qu'un 3-cycle est pair et que le produit de deux transpositions dont les supports ont en commun un singleton est un 3-cycle.

Le cas $\tau_{i,j} \circ \tau_{i,j} = \mathrm{Id} = (231)(312)$ est immédiat. Il reste à étudier le produit de deux transpositions à supports disjoints. Soient i, j, k et l quatre éléments de deux à deux distincts de $\{1, ..., n\}$.

$$\tau_{i,j} \circ \tau_{k,l} = (jikl)(ijlk) = (jilk) = (jkil)(ljik).$$

Donc, $\tau_{i,j} \circ \tau_{k,l}$ est un bien un produit de 3-cycles ce qui achève la démonstration.

n° 4 : D'après le n° 2, il suffit de montrer que pour $2 \leq i \leq n$, $\tau_{1,i}$ peut s'écrire en utilisant uniquement $\tau = \tau_{1,2}$ et $c = (2\ 3\ ...\ n\ 1)$. On note que $c^n = \mathrm{Id}$.
Tout d'abord, pour $1 \leq i \leq n-1$, étudions $\sigma = c^{i-1} \circ \tau \circ c^{n-i+1}$.

Soit $k \in [\![1, n]\!]$.

$$\tau \circ c^{n-i+1}(k) \neq c^{n-i+1}(k) \Leftrightarrow c^{n-i+1}(k) \in \{1, 2\} \Leftrightarrow k \in \{c^{-n+i-1}(1), c^{-n+i-1}(2)\} \Leftrightarrow k \in \{c^{i-1}(1), c^{i-1}(2)\}$$
$$\Leftrightarrow k \in \{i, i+1\}.$$

Donc, si $k \notin \{i, i+1\}$,

$$\sigma(k) = c^{i-1}(\tau \circ c^{n-i+1}(k)) = c^{i-1}(c^{n-i+1}(k)) = c^n(k) = k,$$

et la restriction de σ à $[\![1, n]\!] \setminus \{i, i+1\}$ est l'identité de cet ensemble. Comme σ n'est pas l'identité puisque $\sigma(i) \neq i$, σ est donc nécessairement la transposition $\tau_{i,i+1}$. On a montré que

$$\forall i \in [\![1, n-1]\!],\ c^{i-1} \circ \tau \circ c^{n-i+1} = \tau_{i,i+1}.$$

Vérifions maintenant que les $\tau_{1,i}$ sont des composés des $\tau_{j,j+1}$ ce qui achèvera la démonstration.
D'après le n° 2, $\tau_{i,j} = \tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}$, et donc bien sûr, plus généralement, $\tau_{i,j} = \tau_{k,i} \circ \tau_{k,j} \circ \tau_{k,i}$.

Par suite, $\tau_{1,i} = \tau_{1,2} \circ \tau_{2,i} \circ \tau_{1,2}$ puis, $\tau_{2,i} = \tau_{2,3} \circ \tau_{3,i} \circ \tau_{2,3}$, puis, $\tau_{3,i} = \tau_{3,4} \circ \tau_{4,i} \circ \tau_{3,4}$ ... et $\tau_{i-2,i} = \tau_{i-2,i-1} \circ \tau_{i-1,i} \circ \tau_{i-2,i-1}$. Finalement,

$$\tau_{1,i} = \tau_{1,2} \circ \tau_{2,3} \circ \ldots \circ \tau_{i-2,i-1} \circ \tau_{i-1,i} \circ \tau_{i-2,i-1} \circ \ldots \circ \tau_{2,3} \circ \tau_{1,2},$$

$$\boxed{\mathscr{S}_n \text{ est engendré par le cycle } (2\ 3\ \ldots\ n\ 1) \text{ et la transposition } \tau_{1,2}.}$$

n° 5 : Soit $(G, \times)$ un groupe. Pour x élément de G donné, on considère $\sigma_x : \begin{array}{ccc} G & \rightarrow & G \\ y & \mapsto & xy \end{array}$. σ_x est une application de G vers G et de plus $\sigma_x \circ \sigma_{x^{-1}} = \sigma_{x^{-1}} \circ \sigma_x = Id_G$. Donc, pour tout élément x de G, σ_x est une permutation de G.

Soit alors $\varphi : \begin{array}{ccc} (G, \times) & \rightarrow & (S_G, \circ) \\ x & \mapsto & \sigma_x \end{array}$. D'après ce qui précède, φ est une application. De plus, φ est un morphisme de groupes. En effet, pour $(x, x', y) \in G^3$, on a :

$$\varphi((xx'))(y) = \sigma_{xx'}(y) = xx'y = \sigma_x(f'_x(y)) = \sigma_x \circ \sigma_{x'}(y) = (\varphi(x) \circ \varphi(x'))(y),$$

et donc $\forall (x, x') \in G^2,\ \varphi(xx') = \varphi(x) o \varphi(x')$.

Enfin, φ est injectif car, pour (x, x') élément de G^2 :

$$\varphi(x) = \varphi(x') \Rightarrow \forall y \in G,\ xy = x'y \Rightarrow xe = x'e \Rightarrow x = x'.$$

φ est ainsi un isomorphisme de groupes de $(G, \times)$ sur $(\varphi(G), \circ)$ qui est un sous-groupe de $(S(G), \circ)$. $(G, \times)$ est bien isomorphe à un sous groupe de $(S(G), \circ)$.

n° 6 : Montrons d'abord par récurrence sur $l \geq 2$ que la signature d'un cycle de longueur l est $(-1)^{l-1}$.
• C'est connu pour $l = 2$ (signature d'une transposition).
• Soit $l \geq 2$. Supposons que tout cycle de longueur l ait pour signature $(-1)^{l-1}$. Soit c un cycle de longueur $l+1$.
On note $\{x_1, x_2, ..., x_{l+1}\}$ le support de c et on suppose que, pour $1 \leq i \leq l$, $c(x_i) = x_{i+1}$ et que $c(x_{l+1}) = x_1$.
Montrons alors que $\tau_{x_1,x_{l+1}} \circ c$ est un cycle de longueur l. $\tau_{x_1,x_{l+1}} \circ c$ fixe déjà x_{l+1} puis, si $1 \leq i \leq l-1$,

$$\tau_{x_1,x_{l+1}} \circ c(x_i) = \tau_{x_1,x_{l+1}}(x_{i+1}) = x_{i+1}$$

(car x_{i+1} n'est ni x_1, ni x_{l+1}), et enfin $\tau_{x_1,x_{l+1}} \circ c(x_l) = \tau_{x_1,x_{l+1}}(x_{l+1}) = x_1$. $\tau_{x_1,x_{l+1}} \circ c$ est donc bien un cycle de longueur l. Par hypothèse de récurrence, $\tau_{x_1,x_{l+1}} \circ c$ a pour signature $(-1)^{l-1}$ et donc, c a pour signature $(-1)^{(l+1)-1}$.

Montrons maintenant que si σ est une permutation quelconque de $\{1, ..., n\}$ ayant k orbites la signature de σ est $(-1)^{n-k}$.
Si σ est l'identité, σ a n orbites et le résultat est clair.
Si σ n'est pas l'identité, on décompose σ en produit de cycles à supports disjoints.
Posons $\sigma = c_1 ... c_p$ où p désigne le nombre d'orbites de σ non réduites à un singleton et donc $k - p$ est le nombre de points fixes de σ. Si l_i est la longueur de c_i, on a donc $n = l_1 + ... + l_p + (k - p)$ ou encore $n - k = l_1 + ... + l_p - p$.
Mais alors,

$$\varepsilon(\sigma) = \prod_{i=1}^{p} \varepsilon(c_i) = \prod_{i=1}^{p} (-1)^{l_i - 1} = (-1)^{l_1 + \cdots + l_p - p} = (-1)^{n-k}.$$

n° 7 :
1) a) Soient σ et σ' deux éléments de S_n. Soit $(i,j) \in [\![1,n]\!]^2$. Le coefficient ligne i, colonne j de $P_\sigma \times P_{\sigma'}$ vaut

$$\sum_{k=1}^{n} \delta_{i,\sigma(k)}\delta_{k,\sigma'(j)} = \delta_{i,\sigma(\sigma'(j))}, \text{ (obtenu pour } k = \sigma'(j))$$

et est donc aussi le coefficient ligne i, colonne j de la matrice $P_{\sigma\circ\sigma'}$. Par suite,

$$\boxed{\forall(\sigma,\sigma') \in (S_n)^2,\ P_\sigma \times P_{\sigma'} = P_{\sigma\circ\sigma'}.}$$

b) Soit $\sigma \in S_n$. D'après a), $P_\sigma P_{\sigma^{-1}} = P_{\sigma\circ\sigma^{-1}} = P_{Id} = I_n = P_{\sigma^{-1}}P_\sigma$. On en déduit que toute matrice P_σ est inversible, d'inverse $P_{\sigma^{-1}}$. Par suite, $G \subset GL_n(\mathbb{R})$.
Ensuite, G contient $P_{Id} = I_n$ et donc $G \neq \varnothing$.

Soit enfin $(\sigma,\sigma') \in (S_n)^2$.

$$P_\sigma P_{\sigma'}^{-1} = P_\sigma P_{\sigma'^{-1}} = P_{\sigma\circ\sigma'^{-1}} \in G.$$

On a montré que

$$\boxed{G \text{ est un sous-groupe de } (GL_n(\mathbb{R}),\times).}$$

Soit $\varphi : \begin{array}{ccc} S_n & \rightarrow & G \\ \sigma & \mapsto & P_\sigma \end{array}$. D'après a), φ est un morphisme de groupes. φ est clairement surjectif. Il reste à vérifier que φ est injectif.

Soit $(\sigma,\sigma') \in (S_n)^2$.

$$\begin{aligned}\varphi(\sigma) = \varphi(\sigma') \Rightarrow P_\sigma = P_{\sigma'} &\Rightarrow \forall(i,j) \in [\![1,n]\!]^2,\ \delta_{i,\sigma(j)} = \delta_{i,\sigma'(j)} \\ &\Rightarrow \forall j \in [\![1,n]\!],\ \delta_{\sigma(j),\sigma'(j)} = \delta_{\sigma(j),\sigma(j)} = 1 \Rightarrow \forall j \in]\!]1,n]\!],\ \sigma(j) = \sigma'(j) \\ &\Rightarrow \sigma = \sigma'.\end{aligned}$$

Ainsi, φ est un isomorphisme du groupe $(S_n,\circ)$ sur le groupe $(G,\times)$ et on a montré que

$$\boxed{(G,\times) \text{ est un sous-groupe de } (GL_n(\mathbb{R}),\times), \text{ isomorphe à } (S_n,\circ).}$$

2) Soit $(i,j) \in [\![1,n]\!]^2$. Le coefficient ligne i, colonne j de AP_σ vaut :

$$\sum_{k=1}^{n} a_{i,k}\delta_{k,\sigma(j)} = a_{i,\sigma(j)} \text{ (obtenu pour } k = \sigma(i)).$$

Ainsi, l'élément ligne i, colonne j, de AP_σ est l'élément ligne i, colonne $\sigma(j)$, de A, ou encore, si j est un élément donné de $[\![1,n]\!]$, la j-ème colonne de AP_σ est la $\sigma(j)$-ème colonne de A. Ainsi, si on note C_1,...,C_n les colonnes de A (et donc $A = (C_1,...,C_n)$), alors $AP_\sigma = (C_{\sigma(1)},...,C_{\sigma(n)})$. En clair, multiplier A par P_σ à droite a pour effet d'appliquer la permutation σ aux colonnes de A (puisque P_σ est inversible, on retrouve le fait que permuter les colonnes de A ne modifie pas le rang de A).

De même, le coefficient ligne i, colonne j, de $P_\sigma A$ vaut

$$\sum_{k=1}^{n} \delta_{i,\sigma(k)}a_{k,j} = \sum_{k=1}^{n} \delta_{\sigma^{-1}(i),k}a_{k,j} = a_{\sigma^{-1}(i),j},$$

(on a utilisé $\sigma(k) = i \Leftrightarrow k = \sigma^{-1}(i)$) et multiplier A par P_σ à gauche a pour effet d'appliquer la permutation σ^{-1} aux lignes de A.

n° 8 : $G = \{A_1,...,A_p\}$ est déjà une partie non vide de $GL_n(\mathbb{R})$, stable pour $\times$. Il reste à vérifier que G est stable pour le passage à l'inverse.

Soient $i \in [\![1,n]\!]$, puis $\varphi_i : \begin{array}{ccc} G & \rightarrow & G \\ A & \mapsto & A_iA \end{array}$. Puisque G est stable pour le produit, φ_i est une application de G dans G.

Montrons que φ_i est injective. Soit $(A,B) \in G^2$.

$$\varphi_(A) = \varphi_i(B) \Rightarrow A_iA = A_iB \Rightarrow A_i^{-1}A_iA = A_i^{-1}A_iB \Rightarrow A = B.$$

(On pouvait aussi se rappeler que dans un groupe, tout élément est simplifiable). Donc, φ_i est une application injective de l'ensemble **fini** G dans lui-même. On sait alors que φ_i est une permutation de G.

Par φ_i, A_i a un antécédent A dans G. $A_iA = A_i$ fournit $A_i^{-1}A_iA = A_i^{-1}A_i$ puis $A = I_n \in G$. Ainsi, G contient la matrice I_n. Ensuite, I_n a un antécédent par φ_i dans G. Donc, il existe $B \in G$ telle que $A_iB = I$. Mais alors $A_i^{-1} = B \in G$.
G est bien stable pour le passage à l'inverse et est donc un sous-groupe de $(GL_n(\mathbb{R}), \times)$.

n° 9 : (On peut noter que la matrice dans la base canonique de f_σ est P_σ).
Pour $(x_1, ..., x_n) \in E$, on pose $\varphi((x_1, ..., x_n)) = x_1 + ... + x_n$. φ est une forme linéaire non nulle sur E et H est le noyau de φ. H est donc bien un hyperplan de E.

Pour $(\sigma, \sigma') \in S_n^2$, les endomorphismes $f_\sigma \circ f_{\sigma'}$ et $f_{\sigma\circ\sigma'}$ coïncident sur la base canonique de $\mathbb{R}^n$ et donc $f_\sigma \circ f_{\sigma'} = f_{\sigma\circ\sigma'}$.

Ensuite, $(\mathscr{L}(E), +, .)$ est un espace vectoriel et donc, p est bien un endomorphisme de E. De plus,

$$p^2 = \frac{1}{n!^2}\left(\sum_{\sigma\in S_n} f_\sigma\right)^2 = \sum_{(\sigma,\sigma')\in(S_n)^2} f_\sigma \circ f_{\sigma'}.$$

Mais, $(S_n, \circ)$ est un groupe fini. Par suite, l'application $\begin{array}{ccc} S_n & \rightarrow & S_n \\ \sigma & \mapsto & \sigma\circ\sigma' \end{array}$, injective (même démarche que dans le n° 8), est une permutation de S_n. On en déduit que, pour σ' donnée, $\displaystyle\sum_{\sigma\in S_n} f_{\sigma\circ\sigma'} = \sum_{\sigma\in S_n} f_\sigma$. Ainsi, en posant $q = n!p$.

$$p^2 = \frac{1}{n!^2}\sum_{\sigma'\in S_n}\left(\sum_{\sigma\in S_n} f_{\sigma\circ\sigma'}\right) = \frac{1}{n!^2}\sum_{\sigma'\in S_n} q = \frac{1}{n!^2}.n!q = \frac{1}{n!}q = p.$$

p est donc une projection. Déterminons alors l'image et le noyau de p. Soit $i \in [\![1, n]\!]$.

$$p(e_i) = \frac{1}{n!}\sum_{\sigma\in S_n} f_\sigma(e_i) = \frac{1}{n!}\sum_{\sigma\in S_n} e_{\sigma(i)}.$$

Maintenant, il y a (bien sûr) autant de permuations σ telles que $\sigma(i) = 1$, que de permutations σ telles que $\sigma(i) = 2$,... ou de permutations σ telles que $\sigma(i) = n$, à savoir $\dfrac{n!}{n} = (n-1)!$. Donc,

$$p(e_i) = \frac{1}{n!}\frac{n!}{n}\sum_{k=1}^{n} e_k = \frac{1}{n}\sum_{k=1}^{n} e_k.$$

Posons $u = \dfrac{1}{n}\displaystyle\sum_{k=1}^{n} e_k$. D'après ce qui précède,

$$\mathrm{Im}p = \mathrm{Vect}(p(e_1), ..., p(e_n)) = \mathrm{Vect}(u).$$

Ensuite, si $x = x_1e_1 + ... + x_ne_n$ est un élément de E,

$$p(x) = 0 \Leftrightarrow \sum_{k=1}^{n} x_kp(e_k) = 0 \Leftrightarrow \left(\sum_{k=1}^{n} x_k\right)u = 0 \Leftrightarrow \sum_{k=1}^{n} x_k = 0 \Leftrightarrow x \in H.$$

Ainsi, p est la projection sur $\mathrm{Vect}(u)$ parallèlement à H.