À propos des automorphismes de $\mathfrak{S}_n$

Théorème. Soit $n \neq 6$ un entier $\geqslant 2$. Soit $\varphi : \mathfrak{S}_n \to \mathfrak{S}_n$ un automorphisme de groupes. Alors il existe $\sigma \in \mathfrak{S}_n$ tel que

$$\forall\, \tau \in \mathfrak{S}_n,\ \varphi(\tau) = \sigma\tau\sigma^{-1}\ .$$

Démo.

Si $1 \leqslant k \leqslant \frac{n}{2}$, on note N_k le nombre de produit de k transpositions à supports disjoints dans $\mathfrak{S}_n$.

On a $N_1 = \binom{n}{2}$, nombre de transpositions. Plus généralement :

$$N_k = \frac{\binom{n}{2}\binom{n-2}{2}\ldots\binom{n-2k+2}{2}}{k!} = \frac{n!}{(n-2k)!2^k k!}$$

pour tout $1 \leqslant k \leqslant \frac{n}{2}$.

Pour tout $\tau \in \mathfrak{S}_n$, on pose $\mathscr{C}(\tau) = \{g\tau g^{-1}\ :\ g \in \mathfrak{S}_n\}$.

Si τ est une transposition, alors $\mathscr{C}(\tau)$ est l'ensemble des transpositions. Plus généralement si τ est un produit de $k-$transpositions à supports disjoints, alors $\mathscr{C}(\tau)$ est l'ensemble des produits de $k-$transpositions à supports disjoints.

Soit τ une transposition, comme φ est un automorphisme, si τ est une transposition, alors $\varphi(\tau)$ est d'ordre 2 donc est un produit de k transpositions à supports disjoints pour un certain $k \geqslant 1$ et $2k \leqslant n$.

Or $\varphi(\mathscr{C}(\tau)) = \mathscr{C}(\varphi(\tau))$ donc puisque φ est bijective, on a :

$$\binom{n}{2} = |\mathscr{C}(\tau)| = |\varphi(\mathscr{C}(\tau)| = |\mathscr{C}(\varphi(\tau))| = N_k\ .$$

Or,

$$\forall\, k \geqslant 2,\ N_k \neq N_1$$

en effet,

i) Si $k = 2$, $n \geqslant 4$ et alors $N_k = \frac{n!}{(n-4)!8} = \binom{n}{2}\frac{(n-2)(n-3)}{4} \begin{cases} > \binom{n}{2} & \text{si } n \geqslant 5 \\ < \binom{n}{2} & \text{si } n = 4. \end{cases}$.

ii) Si $k = 3$, $n \geqslant 6$ et alors $N_k = \frac{n!}{(n-6)!48} = \binom{n}{2}\frac{(n-2)(n-3)(n-4)(n-5)}{24} > \binom{n}{2}$ si $n > 6$.

iii) Si $k > 3$, alors $n \geqslant 2k > 6$ et $N_k = \frac{n!}{(n-2k)!2^k k!} = \binom{n}{2}\binom{n-2}{2(k-1)}\frac{(2(k-1))!}{2^{k-1}k!} \geqslant \binom{n}{2}\frac{1\times 2\times\ldots\times 2(k-1)}{2\times 4\times\ldots\times(2k-2)\times k} = \binom{n}{2}\frac{1\times 3\times\ldots\times(2k-3)}{k} \geqslant \binom{n}{2}\frac{2k-3}{k} > \binom{n}{2}$.

Donc forcément $k = 1$ et $\varphi(\tau)$ est une transposition si τ est une transposition.

Soient $1 \leqslant i, j, k, l \leqslant n$ tels que $\varphi((12)) = (ij)$, $\varphi((13)) = (kl)$.

Comme $(12), (23)$ ne commutent pas, leurs images $(ij), (kl)$ non plus. Donc $\{i, j\} \cap \{k, l\}$ est un singleton. On peut donc poser $1 \leqslant \epsilon_1, \epsilon_2, \epsilon_3 \leqslant n$ tels que $\varphi((12)) = (\epsilon_1, \epsilon_2)$, $\varphi((13)) = (\epsilon_1, \epsilon_3)$.

Pour tout $i \geqslant 4$, $\varphi((1i))$ est une transposition qui ne commute pas avec $\varphi((12)) = (\epsilon_1, \epsilon_2)$ donc $\varphi((1i))$ est une transposition de la forme (ϵ_1, ϵ) ou (ϵ_2, ϵ). Comme $\varphi((1i))$ ne commute pas non plus avec $\varphi((13)) = (\epsilon_1, \epsilon_3)$, on a forcément $\varphi((1i)) = (\epsilon_1, \epsilon)$. Notons $\epsilon_i = \epsilon$.

On a donc des entiers $1 \leqslant \epsilon_1, ..., \epsilon_n \leqslant n$ tels que

$$\forall\, 2 \leqslant i \leqslant n,\, \varphi((1i)) = (\epsilon_1, \epsilon_i)\ .$$

Comme φ est injective les ϵ_i sont deux à deux distincts et $\sigma : i \mapsto \epsilon_i$ est dans $\mathfrak{S}_n$.

On vérifie facilement que :

$$\forall\, 2 \leqslant i \leqslant n,\, \varphi((1i)) = \sigma(1i)\sigma^{-1}$$

or les transpositions $(1i)$, $2 \leqslant i \leqslant n$ engendrent $\mathfrak{S}_n$ donc

$$\forall\, g \in \mathfrak{S}_n,\ \ \varphi(g) = \sigma g \sigma^{-1}\ .$$

Qed.