Références :
Cours d'algèbre, Daniel Perrin

Théo. *Pour $n \neq 6$, tout automorphisme de $\mathcal{S}_n$ est intérieur.*

Prop. *Soit $\phi \in Aut(\mathcal{S}_n)$, si ϕ transforme les transpositions en transpositions, alors ϕ est intérieur.*

Démonstration.
On sait que le groupe $\mathcal{S}_n$ est engendré par les transpositions. On a même que $\mathcal{S}_n$ est engendré par les transpositions de la forme $\tau_i = (1\ i)$ pour $i \geq 2$.

En effet, pour $i, j \in [\![1, n]\!]$, $(i\ j) = (1\ j)(1\ i)(1\ j)$.

Par hypothèse, on a donc que, pour tout $i \geq 2$, $\phi(\tau_i)$ est une transposition.
De plus, pour $i, j \in [\![2, n]\!]$ tels que $i \neq j$, τ_i et τ_j ne commutent pas, donc $\phi(\tau_i)$ et $\phi(\tau_j)$ ne commutent pas. Ainsi, ces deux transpositions ne sont pas disjointes.
Si on pose $\phi(\tau_2) = (\alpha_1\ \alpha_2)$, on peut supposer, quitte à renuméroter que $\phi(\tau_3) = (\alpha_1\ \alpha_3)$. On peut donc écrire $\phi(\tau_i) = (\alpha_1\ \alpha_i)$ pour $i > 3$ avec $\{\alpha_1, ..., \alpha_n\} = \{1, ..., n\}$.
En effet, s'il existait $i \in [\![2, n]\!]$ tel que $\phi(\tau_i) = (\alpha_2, \alpha_3)$, comme

$$(\alpha_1\ \alpha_2)(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_3) = (\alpha_1\ \alpha_3)$$

On aura, en appliquant ϕ^{-1},

$$(1\ 2)(1\ 3)(1\ i) = (1\ 3),$$

or $(1\ 2)(1\ 3)(1\ i) = (1\ i\ 3\ 2)$.
Les α_i sont distincts sinon ϕ ne serait pas injective. Posons maintenant

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

On a donc que, pour tout $i \in [\![2, n]\!]$,

$$i_\alpha(\tau_i) = \alpha\tau_i\alpha^{-1} = (\alpha_1\ \alpha_i) = \phi(\tau_i)$$

Ainsi, i_α et ϕ coïncident sur les (τ_i) qui engendrent $\mathcal{S}_n$. Ainsi, on a $\phi = i_\alpha$ et donc ϕ est bien intérieur. □

Lemme. Soit $s \in \mathcal{S}_n$, on suppose que $n = k_1 + 2k_2 + ... + nk_n$ avec $k_i \in \mathbb{N}$ et que s est le produit de $k_1 + ... + k_n$ cycles disjoints (k_1 1-cycles, k_2 2-cycles,..., k_n n-cycles).
Alors, si $c(s)$ est le centralisateur de s, on a

$$|c(s)| = \prod_{i=1}^{n} k_i! i^{k_i}.$$

Démonstration. Un i-cycle peut s'écrire de i manières différentes. Ainsi, pour un i-cycle choisi, il y a i éléments dans son centralisateur. Pour trouver, le cardinal du centralisateur d'un produit de k_i i-cycles, il faut tout d'abord choisir un i-cycle. On a donc k_i choix puis i éléments dans le centralisateur. On choisit ensuite un deuxième i-cycle, on a $k_i - 1$ choix possibles et i éléments dans le centralisateur. Ainsi, le centralisateur d'un produit de k_i i-cycles a $k_i! i^{k_i}$ éléments. On fait ce raisonnement pour les cycles de toutes les longueurs de s et on obtient le résultat. □

Démonstration. Soit ϕ un automorphisme de $\mathcal{S}_n$. Si τ est une transposition, $\phi(\tau)$ est d'ordre 2, alors $\phi(\tau)$ est donc produit de k transpositions disjoints. Par ailleurs, on a $\phi(c(\tau)) = c(\phi(\tau))$.

Soit $\tau \in \mathcal{S}_n$. Soit $\sigma \in c(\tau)$. On a donc $\sigma\tau = \tau\sigma$. Il existe $\sigma_0, \tau_0 \in \mathcal{S}_n$ tels que $\sigma = \phi^{-1}(\sigma_0)$ et $\tau = \phi^{-1}(\tau_0)$. Ainsi, $\phi^{-1}(\sigma_0\tau_0) = \phi^{-1}(\tau_0\sigma_0)$ et donc $\sigma_0\tau_0 = \tau_0\sigma_0$. Par conséquent, $\phi(\sigma) = \sigma_0 \in c(\tau_0)$, ie, $\sigma \in \phi^{-1}(c(\tau_0))$. On a donc $c(\tau) \subset \phi^{-1}(c(\phi(\tau)))$ ie $\phi(c(\tau)) \subset (c(\phi(\tau)))$.

Soit $\tau \in \mathcal{S}_n$.
Si $\sigma \in c(\phi(\tau))$ alors $\sigma\phi(\tau) = \phi(\tau)\sigma$.
Il existe $\sigma_0 \in \mathcal{S}_n$ tel que $\sigma = \phi(\sigma_0)$.

$$\phi(\sigma_0)\phi(\tau) = \phi(\tau)\phi(\sigma_0) \text{ ie } \phi(\sigma_0\tau) = \phi(\tau\sigma_0) \text{ ie } \sigma_0\tau = \tau\sigma_0$$

Ainsi, on a $\sigma_0 \in c(\tau)$ ie $\phi^{-1}(\sigma) \in c(\tau)$ ie $\sigma \in \phi(c(\tau))$ d'où l'égalité.

Ainsi, on a $|c(\tau)| = |\phi(c(\tau))| = |c(\phi(\tau))|$. D'après le lemme précédent, on a

$$\begin{cases} |c(\tau)| = (n-2)! \times 1^{n-2} \times 1! \times 2^1 = 2(n-2)! \\ |c(\phi(\tau))| = (n-2k)! \times 1^{n-2k} \times k!2^k = 2^k k!(n-2k)! \end{cases}$$

On obtient donc l'égalité

$$\begin{aligned} 2(n-2)! = 2^k k!(n-2k)! &\Leftrightarrow (n-2)! = 2^{k-1}k!(n-2k)! \\ &\Leftrightarrow \frac{(n-2)!}{2^{k-1}k!(n-2k)!} = 1 \\ &\Leftrightarrow \frac{\binom{n-2}{2k-2} \times (2k-2)!(n-2k)!}{2^{k-1}k!(n-2k)!} = 1 \\ &\Leftrightarrow \frac{\binom{n-2}{2k-2} \times (2k-2)!}{2^{k-1}k!} = 1 \\ &\Leftrightarrow \frac{\binom{n-2}{2k-2} \times (2k-2) \times (2k-4) \times \ldots \times 2 \times (2k-3) \times (2k-5) \times \ldots \times 3 \times 1}{2^{k-1}k!} = 1 \\ &\Leftrightarrow \frac{\binom{n-2}{2k-2} \times 2^{k-1}(k-1)! \times (2k-3) \times (2k-5) \times \ldots \times 3 \times 1}{2^{k-1}k!} = 1 \\ &\Leftrightarrow \frac{\binom{n-2}{2k-2} \times (2k-3) \times (2k-5) \times \ldots \times 3 \times 1}{k} = 1. \end{aligned}$$

Or $2k - 3 > k$ si et seulement si $k > 3$. Ainsi, on a $k \leq 2$.

- Si $k = 1$ alors OK
- Si $k = 2$ alors
$$\frac{\binom{n-2}{2}}{2} = 1 \Leftrightarrow \frac{(n-2)!}{(n-4)!2} = 2 \Leftrightarrow (n-2)(n-3) = 4 \Leftrightarrow n^2 - 5n + 2 = 0.$$
  On a $\Delta = 17$ donc ce trinôme n'a pas de solution entière. Absurde.
- Si $k = 3$, alors
$$\binom{n-2}{4} = 1 \Leftrightarrow (n-2)(n-3)(n-4)(n-5) = 4! \Leftrightarrow n = 6.$$

On a donc montré que si $n \neq 6$, ϕ transforme les transpositions en transpositions. D'après la proposition, on obtient donc le résultat. $\square$

Leçons possibles : 101 - 104 - 105 - 108