Automorphismes de $\mathfrak{S}_n$

[PERRIN, p 30]

ÉNONCÉ :

Théorème : Pour $n \neq 6$, $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$.

DÉVELOPPEMENT :

LEMMES :

1. Soit $\phi \in Aut(\mathfrak{S}_n)$. Si ϕ envoie chaque transposition sur une transposition, alors $\phi \in Int(\mathfrak{S}_n)$.
2. En notant $\mathcal{C}$ la classe de conjugaison décrite par la famille $(r_i)_{1\leq i\leq n}$, on a la relation :

$$Card(\mathcal{C}) = \frac{n!}{\prod_{i=1}^n r_i! \times i^{r_i}}$$

Démonstration. 1. Considérons, pour $i \in \{2, \dots, n\}$, $\tau_i = (1, i)$. Par hypothèse, on a, pour $i \in [|2, n|]$, que $\phi(\tau_i)$ 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 $\phi(\tau_j)$ non plus. Ainsi, ces deux transpositions ne sont pas disjointes. Posons $\phi(\tau_2) = (\alpha_1\ \alpha_2)$. Alors, quitte à renuméroter, on peut supposer que $\phi(\tau_1) = (\alpha_1\ \alpha_3)$. On peut donc écrire, pour $i \in [|4, n|]$, $\phi(\tau_i) = (\alpha_1, \alpha_i)$ avec $\{\alpha_1, \dots, \alpha_n\} = \{1, \dots, n\}$. En effet, s'il existait $i \in [|4, n|]$ tel que $\phi(\tau_i) = (\alpha_2\ \alpha_3)$, comme

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

On aura, en appliquant ϕ^{-1} à l'égalité :

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

or $(1\ 2) \circ (1\ 3) \circ (1\ i) = (1\ i\ 3\ 2)$.
Les $(\alpha_i)_{i\in[|1,n|]}$ sont nécessairement distincts par injectivité de ϕ. Posons alors :

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

Pour $i \in [|2, n|]$,

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

Comme les $(\tau_i)_{i\in[|2,n|]}$ engendrent $\mathfrak{S}_n$, $\phi = i_\alpha$ et ϕ est donc bien intérieur.

2. L'action de groupes : $\mathfrak{S}_n \times \mathcal{C} \longrightarrow \mathcal{C}$ par conjugaison est transitive, si bien que la formule des classes nous donne :

$$|\mathcal{C}| = \frac{|\mathfrak{S}_n|}{|Stab(\mathcal{C})|}$$

Voyons que $|Stab(\alpha)| = \prod_{i=1}^n ri! \times i^{r_i}$, $\alpha \in \mathcal{C}$ quelconque. Un i-cycle peut s'écrire, à conjugaison près, de i manière différente (en conjuguant par une puissance dudit-cycle). On peut de plus permuter sans contraintes les r_i i-cycles de α, ce qui nous donne $r_i! \times i^{r_i}$ façons de stabiliser les $i - cycles$ de α. En stabilisant tous les cycles disjoints de α, on obtient le résultat voulu.

□

Démonstration. (*théorème*) : Soit $\phi \in Aut(\mathfrak{S}_n)$ non intérieur. Il ne préserve ainsi pas le transpositions en vertu du lemme. Soit τ une telle transposition, alors $\phi(\tau)$ est un produit de k transpositions, $k \geq 2$. Ainsi, on a nécessairement $n \geq 4$. En notant $\mathcal{C}$ sa classe de conjugaison, il vient que :

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

Si $k > 3$, $\frac{2k-3}{3} > 1$ donc $2 \leq k \leq 3$. Pour $k = 2$, on a $\binom{n-2}{2} = 2$ donc $(n-2)(n-3) = 4$. Pour $k = 3$, on a $\binom{n-2}{4} = 1$ donc $4 = n-2$ donc $n = 6$.
Ainsi, les éléments de $Aut(\mathfrak{S}_n)$ conservant les classes de conjugaison nous montre que $n = 6$, d'où le résultat par contraposée. $\square$

Remarques :

- On utilise le fait que pour $\sigma, \tau \in \mathfrak{S}_n$:

$$(Supp(\sigma) \cap Supp(\tau) = \emptyset) \Rightarrow (\sigma \circ \tau \neq \tau \circ \sigma)$$

  qu'il faut donc savoir montrer.
- La famille $(r_i)_{1 \leq i \leq n}$ d'un élément $\sigma \in \mathfrak{S}_n$ s'appelle le type de σ (exemple : $\sigma = (1,2,3) \circ (6,4,5) \circ (11,10) \circ (7,9) \in \mathfrak{S}_{11}$, son type est $(1,2,2,0,\ldots,0)$). Ces derniers caractérisent les classes de conjugaison de $\mathfrak{S}_n$.
- Pour $n = 6$, $Int(\mathcal{S}_6)$ est un sous-groupe d'indice 2 de $Aut(\mathfrak{S}_6)$: il y a 360 automorphismes intérieurs de $\mathfrak{S}_6$.