Automorphismes de $\mathfrak{S}_n$: $n \neq 6 \Rightarrow \mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$

Référence : D. Perrin, *Cours d'Algèbre*, Ellipses, 1996.

Leçons concernées : 103, 104, 105, 108

Proposition 1. *Si l'image par $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ de toute transposition est une transposition, alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.*

Démonstration. Soit un tel φ. On note $\tau_i := (1i), i \geqslant 2$, dont on sait qu'elles engendrent $\mathfrak{S}_n$. On remarque que les τ_i sont non disjoints donc ne commutent pas entre eux deux à deux, donc leurs images par φ ne commutent pas entre elles deux à deux, et donc ont deux à deux une orbite non disjointe, ces images sont d'autre part des transpositions par hypothèse, et distinctes car φ est un isomorphisme. Maintenant, on note $\varphi(\tau_2) = (a_1a_2)$ et $\varphi(\tau_3) = (a_1a_3), a_3 \neq a_2$ ce qui est possible d'après la première remarque. Ensuite, on a $\varphi(\tau_4) = (a_1a_4), a_4 \neq a_3, a_2$ car sinon $\varphi(\tau_4) = (a_2a_3)$ et on écrit

$$(a_1a_2)(a_1a_3)(a_2a_3) = (a_1a_3)$$

et donc par φ^{-1},

$$(12)(13)(14) = (13)$$

ce qui est impossible. De même $\varphi(\tau_i) = (a_1a_i)$. On a trouvé une permutation a telle que $\varphi(\tau_i) = a\tau_i a^{-1}$ et donc φ et i_a coïncident sur un ensemble générateur donc sont égales. $\square$

Théorème 2. *Pour $n \neq 6$, on a $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.*

Démonstration. *Étape 1 :* on remarque tout d'abord qu'on peut supposer $n \geqslant 6$. En effet, si $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$, φ stabilise $\mathfrak{A}_n$ car $\mathfrak{A}_n = D(\mathfrak{S}_n)$ est caractéristique. L'image d'une transposition est donc impaire. D'autre part, l'image d'une transposition est d'ordre 2 donc elle se décompose en produit de k transpositions à supports disjoints, avec k impair par la première remarque. Si pour toute transposition, $k = 1$ c'est fini d'après la proposition précédente, dans le cas contraire, il y a un cas où $k \geqslant 3$ donc $n \geqslant 6$.

Étape 2 : pour $s \in \mathfrak{S}_n$, on note $c(s) := \{s' \in \mathfrak{S}_n \mid ss' = s's\}$ le centralisateur de s. Soit $\tau = (ab)$ une transposition. On a $\forall s \in \mathfrak{S}_n$, $s\tau s^{-1} = (s(a)s(b))$. Ainsi, si on note $E := \{1, \dots, n\}$ et $F = E\backslash\{a, b\}$, $s \in c(\tau) \Leftrightarrow s(\{a, b\}) = \{a, b\} \Leftrightarrow s(F) = F$. On considère alors le morphisme de groupes

$$r : \begin{array}{ccc} c(\tau) & \to & \mathfrak{S}(F) \cong \mathfrak{S}_{n-2} \\ s & \mapsto & s_{|F} \end{array}$$

qui est bien défini par l'étude précédente, de noyau $\{1, \tau\}$ et surjectif.

Étape 3 : d'autre part, si $\tau = \tau_1 \cdots \tau_k$, avec $\tau_i = (a_{2i-1}a_{2i})$, est un produit d'un nombre impair k de transpositions à supports disjoints, on a $\tau_i \in c(\tau)$. On pose $N :=< \tau_i \mid 1 \leqslant i \leqslant$

$k >$. On a $|N| = 2^k$ et donc $N \cong (\mathbb{Z}/2\mathbb{Z})^k$ et d'autre part $N \lhd c(\tau)$. En effet, soit $s \in c(\tau)$, on a $s\tau s^{-1} = \tau = (s(a_1)s(a_2)) \cdots (s(a_{2k-1})s(a_{2k}))$ donc par unicité de la décomposition en produit de cycles à supports disjoints, $s\tau_i s^{-1} = \tau_j$ pour tout i.

Étape 4 : on considère alors τ une transposition telle que son image τ' par φ soit un produit d'un nombre impair $k \geqslant 3$ de transpositions à supports disjoints. On a $c(\tau) \cong c(\tau')$ via φ, donc il existe $N' \cong (\mathbb{Z}/2\mathbb{Z})^k \lhd c(\tau)$ via φ. On a alors $r(N') \lhd \mathfrak{S}_{n-2}$ avec

$$|r(N')| = \frac{|N'|}{|\ker r \cap N'|} = 2^k \text{ ou } 2^{k-1}.$$

Or si $n \geqslant 7$, $n - 2 \geqslant 5$ et par l'étude des sous-groupes distingués de $\mathfrak{S}_m$ on trouve une absurdité par étude du cardinal. On peut alors conclure grâce à la proposition précédente. $\square$

On donne ici l'étude des sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geqslant 5$.

Proposition 3. *Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}, \mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Démonstration. On considère $H \lhd \mathfrak{S}_n$. On a $H \cap \mathfrak{A}_n \lhd \mathfrak{A}_n$, donc $H \cap \mathfrak{A}_n = \{1\}$ ou $\mathfrak{A}_n$.

Si $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, alors $H = \mathfrak{A}_n$ ou $\mathfrak{S}_n$.

Si $H \cap \mathfrak{A}_n = \{1\}$, puisque le noyau de $\varepsilon : H \to \mathbb{Z}/2\mathbb{Z}$ est $H \cap \mathfrak{A}_n$, $\varepsilon : H \to \varepsilon(H)$ est un isomorphisme, de sorte que $|H| \leqslant 2$. Si $|H| = 2$, alors $H = \{1, \sigma\}$. Mais si $\tau \in \mathfrak{S}_n$, $\tau\sigma\tau^{-1} \in H$, et comme $\sigma \neq 1$, $\tau\sigma\tau^{-1} = \sigma$, et ce pour tout $\tau \in \mathfrak{S}_n$, et donc σ est dans le centre de $\mathfrak{S}_n$, qui est trivial, d'où l'absurdité.

On justifie que le centre de $\mathfrak{S}_n$ est trivial pour $n \geqslant 3$: si $\sigma \neq 1$ est dans le centre, alors il existe $i \in [|1, n|]$ tel que $\sigma(i) = j \neq i$. Alors si on choisit $k \neq i, j$, et que l'on pose $\tau = (j\ k)$, alors $\sigma\tau(i) = j$ et $\tau\sigma(i) = k$ et donc $\sigma\tau \neq \tau\sigma$, d'où l'absurdité. $\square$