Groupes d'automorphismes des groupes symétriques

Étienne AFFALOU

04/09/2024

L'objectif de ce document est de prouver le résultat suivant.

Théorème Soit n un entier naturel non nul. On suppose que $n \neq 6$. Alors, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Idée de la preuve : Tout d'abord, on a bien entendu $\mathrm{Int}(\mathfrak{S}_n) \subset \mathrm{Aut}(\mathfrak{S}_n)$.
Il suffit donc de montrer $\mathrm{Aut}(\mathfrak{S}_n) \subset \mathrm{Int}(\mathfrak{S}_n)$. Pour cela, on utilise les deux lemmes ci-dessous.

Lemme 1 Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$.
On suppose que l'image de toute transposition de $\mathfrak{S}_n$ par φ est encore une transposition. Alors, $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.

Preuve du lemme 1 : Pour tout entier $i \in \{2, \cdots, n\}$, on note $\tau_i = (1, i)$ la transposition qui échange 1 et i.
Si $(i, j) \in \{2, \cdots, n\}^2$ est tel que $i \neq j$, on a $\tau_i\tau_j \neq \tau_j\tau_i$, et donc $\varphi(\tau_i)\varphi(\tau_j) \neq \varphi(\tau_j)\varphi(\tau_i)$.
Par hypothèse, $\forall i \in \{2, \cdots, n\}$, $\varphi(\tau_i)$ est une transposition. Posons par exemple $\varphi(\tau_2) = (\alpha_1, \alpha_2)$ avec $\alpha_1 \neq \alpha_2$.
Comme $\varphi(\tau_2)$ ne commute pas avec $\varphi(\tau_3)$, les supports de $\varphi(\tau_2)$ et de $\varphi(\tau_3)$ ne sont pas disjoints.
Quitte à échanger α_1 et α_2, on peut donc supposer $\varphi(\tau_3) = (\alpha_1, \alpha_3)$ avec $\alpha_1 \neq \alpha_3$ et $\alpha_2 \neq \alpha_3$.
En fait, $\forall i \in \{2, \cdots, n\}$, $\varphi(\tau_i) = (\alpha_1, \alpha_i)$ où $\{\alpha_1, \cdots, \alpha_n\} = \{1, \cdots, n\}$.
Effectivement, une situation où $\exists i \in \{4, \cdots, n\}$ tel que $\varphi(\tau_i) = (\alpha_2, \alpha_3)$ est impossible étant donné que comme

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

on aurait $(1, 2)(1, 3)(1, i) = (1, 3)$ en passant à φ^{-1} ce qui est faux. Ce style d'argument tient encore si on cherche à trouver un $i \in \{2, \cdots, n\}$ tel que α_1 n'appartient pas au support de $\varphi(\tau_i)$. Les α_i sont nécessairement distincts par injectivité de φ. Notre automorphisme φ envoie donc les transpositions de la forme $(1, i)$ pour $i \in \{2, \cdots, n\}$ sur des transpositions de la forme (α_1, α_i) avec $\{\alpha_1, \cdots, \alpha_n\} = \{1, \cdots, n\}$.
L'application $\alpha : \{1, \cdots, n\} \to \{1, \cdots, n\}$ définie par $\forall i \in \{1, \cdots, n\}, \alpha(i) = \alpha_i$ est bien définie et est une bijection par ce qui précède. Autrement dit $\alpha \in \mathfrak{S}_n$ et de plus, $\forall i \in \{1, \cdots, n\}$, on a

$$\alpha\tau_i\alpha^{-1} = \alpha(1, i)\alpha^{-1} = (\alpha(1), \alpha(i)) = (\alpha_1, \alpha_i) = \varphi(\tau_i).$$

Ainsi, φ coïncide avec un automorphisme intérieur sur les τ_i. Mais les τ_i engendrent $\mathfrak{S}_n$ donc φ est intérieur.

Lemme 2 Soit $\sigma \in \mathfrak{S}_n$ un élément d'ordre 2. Notons $C(\sigma) = \{\tau \in \mathfrak{S}_n, \tau\sigma\tau^{-1} = \sigma\}$ le centralisateur de σ.
Alors, σ est produit de k transpositions à supports disjoints avec $k \in \mathbb{N}^*$, et $|C(\sigma)| = 2^k k!(n - 2k)!$.

Preuve du lemme 2 : La permutation σ est d'ordre 2 donc en la décomposant en produit de cycles à supports disjoints, on obtient que ces cycles sont nécessairement des transpositions. Ainsi, comme $\sigma \neq id$ pour une raison d'ordre, σ est produit de k transpositions à supports disjoints avec $k \in \mathbb{N}^*$.
Remarquons que dans toute la suite, on a $n \geqslant 2k$ étant donné qu'on dispose de k transpositions à supports disjoints.
Dans la suite, on note $\sigma = \tau_1 \cdots \tau_k$ avec $\forall i \in \{1, \cdots, k\}$, $\tau_i = (a_i, b_i)$ où $|\{a_1, \cdots, a_k, b_1, \cdots, b_k\}| = 2k$ et notons $F = \{1, \cdots, n\} \setminus \{a_1, \cdots, a_k, b_1, \cdots, b_k\}$ l'ensemble des points fixes de σ.
Comptons le nombre de permutations τ qui appartiennent au centralisateur de σ. Commencons par noter que $\tau \in C(\sigma)$

si et seulement si $\{\tau\tau_i\tau^{-1}, i \in \{1,\cdots,k\}\} = \{\tau_1,\cdots,\tau_k\}$ (il suffit d'intercaler des $\tau^{-1}\tau$).
Pour construire une telle permutation τ, on commence par choisir $f \in \mathfrak{S}_k$ telle que $\forall i \in \{1,\cdots,k\}, \tau\tau_i\tau^{-1} = \tau_{f(i)}$ ou bien $\tau\tau_{f(i)}\tau^{-1} = \tau_i$ (ce n'est pas la même chose). Pour cette première étape, on a $k!$ choix pour f, et 2^k choix pour la place de f soit au total $k!2^k$ possibilités pour cette première étape. Reste à prendre en compte le fait que l'image des points fixes de σ est libre, ce qui laisse $(n-2k)!$ possibilités.
Finalement, on a $2^k k!(n-2k)!$ possibilités pour le choix de τ, d'où le résutat annoncé.

Preuve du théorème : Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$.
Par le lemme 1 et l'idée de la preuve, il suffit de montrer que l'image par φ d'une transposition est une transposition.
Soit donc $\tau \in \mathfrak{S}_n$ une transposition. Montrons que $\varphi(\tau)$ est une transposition.
Comme τ est une transposition, $\varphi(\tau)$ est d'ordre 2 et le lemme 2 assure l'existence de $k \in \mathbb{N}^*$ tel que $\varphi(\tau)$ est produit de k transpositions à supports disjoints. Montrons que $k = 1$.
Pour cela, en reprenant les notations du lemme 2, montrons que $\varphi(C(\tau)) = C(\varphi(\tau))$.

- Soit $\sigma \in \varphi(C(\tau))$. On a donc $\sigma = \varphi(\sigma_0)$ avec $\sigma_0 \in \mathfrak{S}_n$ qui vérifie $\sigma_0\tau\sigma_0^{-1} = \tau$.
  En appliquant φ à cette égalité, on obtient $\varphi(\sigma_0)\varphi(\tau)\varphi(\sigma_0)^{-1} = \varphi(\tau)$ et donc $\sigma\varphi(\tau)\sigma^{-1} = \varphi(\tau)$.
  Autrement dit, $\sigma \in C(\varphi(\tau))$. Ainsi, on a l'inclusion $\varphi(C(\tau)) \subset C(\varphi(\tau))$.
- Soit $\sigma \in C(\varphi(\tau))$. On a donc $\sigma\varphi(\tau)\sigma^{-1} = \varphi(\tau)$. On applique φ^{-1} pour obtenir $\varphi^{-1}(\sigma)\tau\varphi^{-1}(\sigma)^{-1} = \tau$.
  Notant $\sigma_0 = \varphi^{-1}(\sigma)$, on a bien $\sigma_0 \in C(\tau)$ et $\sigma = \varphi(\sigma_0)$. De cette façon, $\sigma \in \varphi(C(\tau))$. D'où $C(\varphi(\tau)) \subset \varphi(C(\tau))$.

En particulier, ces deux ensembles étant finis, on a l'égalité des cardinaux $|\varphi(C(\tau))| = |C(\varphi(\tau))|$.
Mais φ est bijective, et donc $|\varphi(C(\tau))| = |C(\tau)|$. Ainsi, $|C(\tau)| = |C(\varphi(\tau))|$.
Utilisons la seconde partie du lemme 2 sur τ et sur $\varphi(\tau)$ pour obtenir $2(n-2)! = 2^k k!(n-2k)!$. Ainsi,

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

Remarquons que si $k > 3$, on a $2k-3 > k$ et donc le numérateur ne peut pas égaler le dénominateur k et l'égalité est impossible. Reste le cas où $k = 2$ et le cas où $k = 3$.

- Supposons que $k = 2$. Dans ce cas, l'égalité devient $4 = (n-2)(n-3)$ ce qui est impossible (en effet, $4 = 2\times 2$ ou $4 = 1\times 4$ sont les seules factorisations possibles de 4).
- Supposons que $k = 3$. Notons tout d'abord que $n \geqslant 6$ étant donné qu'on dispose de 3 transpositions à supports disjoints. Appliquer l'égalité précédente à $k = 3$ fournit $1 = (3\times(n-2)!)/(3\times 4!\times(n-6)!)$.
  On a donc $24 = (n-2)(n-3)(n-4)(n-5)$. L'égalité est vraie seulement quand $n = 6$, et donc $n = 6$.
  Cela contredit l'hypothèse $n \neq 6$ et donc le cas $k = 3$ est également impossible.

Ce qui précède prouve que k vaut nécessairement 1. Ainsi, $\varphi(\tau)$ est une transposition et le lemme 1 permet de conclure.

Remarque : Le théorème étant évident dans le cas $n = 1$, à chaque fois que l'on a parlé de transposition, il était implicite que $n \geqslant 2$.

Références :

- Cours d'algèbre, *Daniel Perrin*
- Automorphismes de $\mathfrak{S}_n$, version de *Sylvain* `https://agreg-maths.fr/users/109`
- Automorphismes de $\mathfrak{S}_n$, version de *Pandou* `https://agreg-maths.fr/users/44692`