

Automorphisme de S_n

Geoffrey Deperle

Leçons associées :

- 101 : Groupe opérant sur un ensemble. Exemples et applications.
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients.
- 104 : Groupes finis. Exemples et applications.
- 105 : Groupes de permutation d'un ensemble fini.
- 108 : Exemples de parties génératrices d'un groupe.
- 190 : Méthodes combinatoires, problème de dénombrement.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Pour $n \neq 6$, tout automorphisme de S_n est intérieur.*

Idee générale : Un automorphisme de S_n préserve seulement les propriétés algébriques (ordre d'un élément, commutation) mais pas forcément les propriétés géométriques liées à l'action naturelle sur $\{1, \dots, n\}$. Pour des raisons de cardinal, quand $n \neq 6$, les propriétés géométriques seront également conservées.

Lemme 1. *Soit $\varphi \in \text{Aut}(S_n)$, si φ transforme toute transposition en transposition alors φ est intérieur.*

Preuve du lemme : Soit φ un tel automorphisme,

S_n est engendré par les transpositions $(\tau_i)_{i \in \llbracket 2, n \rrbracket}$ avec pour tout $i \geq 2$, $\tau_i = (1 i)$.

Comme les τ_i ne commutent pas, il en va de même pour les $\varphi(\tau_i)$ donc le support des transpositions $\varphi(\tau_i)$ ne sont pas deux à deux disjoints.

Notons $\varphi(\tau_2) = (\alpha_1 \alpha_2)$, alors $\varphi(\tau_3)$ est de la forme $\varphi(\tau_3) = (\alpha_1 \alpha_3)$ et de même pour $i \geq 3$, $\varphi(\tau_i)$ ne commute pas avec les $\varphi(\tau_j)$ pour $j < i$ donc $\varphi(\tau_i)$ est de la forme $\varphi(\tau_i) = (\alpha_1 \alpha_i)$.

Les α_i sont deux à deux disjoints donc $\{\alpha_1, \dots, \alpha_n\} = \llbracket 1, n \rrbracket$ et $\alpha : i \mapsto \alpha_i$ est une permutation vérifiant pour tout $i \in \llbracket 1, n \rrbracket$, $\alpha \tau_i \alpha^{-1} = (\alpha_1 \alpha_i) = \varphi(\tau_i)$ donc φ est un automorphisme intérieur. \square

Soit φ un automorphisme de S_n , il envoie les classes de conjugaison sur des classes de conjugaison donc il envoie les transpositions sur une classe de conjugaison constitué d'éléments d'ordre 2. Dénombrons le cardinal de chaque classe de conjugaison :

Lemme 2. Soit Ω une classe de conjugaison de S_n et $\sigma \in \Omega$, supposons que la décomposition en cycle à support disjoint de σ possède k_i cycle de longueur i , alors

$$\text{Card}(\Omega) = \frac{n!}{\prod_{i=1}^n k_i! i^{k_i}}$$

Preuve du lemme : Le groupe S_n agit transitivement sur Ω par conjugaison donc

$$\text{Card}(\Omega) = \frac{\text{Card}(S_n)}{\text{Card}(\text{Stab}(\sigma))}$$

Or, comme $\tau(a_1 \dots a_i) \tau^{-1} = (\tau(a_1) \dots \tau(a_i))$, $\tau \in \text{Stab}(\sigma)$ si et seulement si

- τ permute les cycles de même longueur : $k_i!$ possibilités.
- τ réalise une permutation cyclique sur chaque cycle donc il y a : $\underbrace{i \times \dots \times i}_{k_i \text{ fois}} = i^{k_i}$ possibilités

Donc $\text{Card}(\text{Stab}(\sigma)) = \prod_{i=1}^n k_i! i^{k_i}$ d'où le résultat. □

Preuve du théorème : Les classes de conjugaison constituées d'éléments d'ordre 2 sont les classes de conjugaison de produit de k transpositions.

Par l'absurde, si φ est un automorphisme non intérieur, il existe $k \geq 2$ tel que le cardinal de l'ensemble des transpositions est égal au cardinal de l'ensemble des produits de k transpositions. D'où d'après le lemme 2 :

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

Or,

$$\begin{aligned} \frac{n!}{2(n-2)!} = \frac{n!}{2^k k! (n-2k)!} &\iff \frac{(n-2)!}{2^{k-1} k! (n-2k)!} = 1 \\ &\iff \frac{\binom{n-2}{2k-2} (2k-2)!}{2^{k-1} k!} = 1 \\ &\iff \frac{\binom{n-2}{2k-2} (2k-3)(2k-5)}{k} = 1 \end{aligned}$$

- Si $k > 3$, on a $2k-3 > k$ donc absurde.
- Si $k = 2$, on a $\frac{1}{2} \binom{n-2}{2} \iff (n-2)(n-3) = 4$ ce qui est absurde car deux entiers consécutifs ne peuvent être pairs tous les deux.
- Si $k = 3$, $\binom{n-2}{4} = 1$ donc $n = 6$. □

Remarque 1. On peut montrer qu'il existe bien des automorphismes non intérieurs dans S_6 .

Références

- [1] Daniel PERRIN. *Cours d'algèbre*. Ellipses, 1996.