Automorphismes de $\mathcal{S}_n$

Francinou-Gianella-Nicolas, *Oraux X-ENS, Algèbre 1*, page 69

Théorème : Soit $n \in \mathbb{N}^*$, $n \neq 6$. Alors les automorphismes de $\mathcal{S}_n$ sont intérieurs, *i.e.* de la forme $s \mapsto \sigma \circ s \circ \sigma^{-1}$, où $\sigma \in \mathcal{S}_n$.

- Soit φ un automorphisme du groupe symétrique. Nous savons que l'ensemble T des transpositions forme une parie génératrice de $\mathcal{S}_n$. L'automorphisme φ sera donc uniquement déterminé si l'on connaît les images par φ des transpositions. Pour commencer, examinons l'image d'une transposition et même l'image d'un élément quelconque de $\mathcal{S}_n$ par un automorphisme intérieur. Soit $\sigma \in \mathcal{S}_n$ et $(a_1, \ldots, a_k)$ un cycle de longueur k (on dira k-cycle). On a alors

$$\boxed{\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))} \qquad (*)$$

Un k-cycle est donc transformé en un k-cycle par tout automorphisme intérieur. En particulier, une transposition est transformée en une transposition.

Plus généralement, si s est un élément de $\mathcal{S}_n$ et $s_1, \ldots, s_k$ les cycles apparaissent dans la décomposition de s en produit de cycles à support disjoint ($s = s_1 s_2 \ldots s_k$), on obtient

$$\boxed{\sigma s \sigma^{-1} = (\sigma s_1 \sigma^{-1})(\sigma s_2 \sigma^{-1}) \ldots (\sigma s_k \sigma^{-1})} \qquad (**)$$

Pour tout i, $\sigma s_i \sigma^{-1}$ est un cycle de même longueur que s_i d'après la formule $(*)$. Si $\{a_1, \ldots, a_p\}$ est le support de s_i, $\{\sigma(a_1), \ldots, \sigma(a_p)\}$ est le support de $\sigma s_i \sigma^{-1}$. En particulier, les $\sigma s_i \sigma^{-1}$ sont des cycles à supports disjoints.

Nous allons démontrer, pour commencer, que φ transforme toute transposition en une transposition. Un automorphisme de $\mathcal{S}_n$ conserve les propriétés algébriques des éléments de $\mathcal{S}_n$. Si τ est une transposition, τ est d'ordre 2, donc $\varphi(\tau)$ est aussi d'ordre 2.Cependant, cela ne suffit pas pour affirmer que $\varphi(\tau)$ est une transposition puisqu'il existe d'autres éléménts d'ordre 2, les produits de transpositions à support disjoints (il n'y a qu'elles, puisque l'ordre d'une permutation est le *ppcm* des longueurs des cycles intervenant dans sa décomposition en produit de cycles à supports disjoints). Notons T_k l'ensemble des permutations de $\mathcal{S}_n$ qui sont produit d'exactement k transpositions à supports disjoints (pour $2k \leq n$). On a en particulier $T_1 = T$.

D'après la relation $(**)$, chaque ensemble T_k est une classe de conjugaisn de $\mathcal{S}_n$. L'image par φ d'une classe de conjugaison est encore une classe de conjugaison (car $\varphi(\sigma \circ \tau \circ \sigma^{-1}) = \varphi(\sigma) \circ \varphi(\tau) \circ \varphi(\sigma)^{-1}$). L'ensemble $\varphi(T_1)$ est donc l'un des T_k.

On va montrer par un argument de cardinalité que, pour $n \geq 6$, on ne peut pas avoir $\varphi(T_1) = T_k$, avec $k \neq 1$. Pour cela, on va calculer le cardinal de T_k. On a $|T_1| = \binom{n}{2} = \frac{n}{n-1}2$, car une transposition est déterminée par son support. Pour $k \geq 2$, on a $|T_k| = \dfrac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}}{k!}$: on choisit les supports des k transpositions et on divise par $k!$ car l'ordre n'importe pas. En simplifiant, il vient

$$|T_k| = \frac{n(n-1)\ldots(n-2k+1)}{2^k k!}$$

Nous allons montrer que si $n \geq 6$, l'équation $|T_k| = |T_1|$, c'est-à-dire

$$k! 2^k = (n-2)(n-3)\ldots(n-2k+1)$$

n'a pas de solutions k strictement supérieure à 1 (avec $2k \leq n$).

En effet, pour $k = 2$, on obtient $(n-2)(n-3) = 4$, équation qui n'a pas de solution dans $\mathbb{N}$. Et pour $k \geq 3$, il vient $\binom{n-k}{k}(n-2)\ldots(n-k+1) = 2^{k-1}$, ce qui ne peut arriver que si $n-k+1 = n-2$ (sinon le terme de gauche a un facteur impair), soit $k = 3$. Mais on a alors $(n-2)\binom{n-3}{3} = 4$ qui entraîne $n = 6$, cas qui est écarté. On a donc $\varphi(T_1) = T_1$.

- On a donc $\varphi(T) = T$. On va s'intéresser aux images des transpositions $(1,k)$ pour $k \in \{2,\dots,n\}$. Celles-ci suffisent à générer $\mathcal{S}_n$. Il existe a_1 et a_2 distincts tels que $\varphi((1,2) = (a_1, a_2)$. De même, il existe a et b distincts tels que $\varphi((1,3)) = (a,b)$. Comme $(1,2)$ et $(1,3)$ ne commutent pas, (a_1, a_2) et (a,b) non plus, ce qui nécessaite $\{a_1, a_2\} \cap \{a, b\} \neq \emptyset$. On peut supposer que $a = a_1$ et on note $a_3 = b$. On a donc $\varphi((1,3)) = (a_1, a_3)$. L'injectivité de φ assure que $a_2 \neq a_3$.

  Montrons par récurrence sur $i \in \{2,\dots,n\}$ que $\varphi((1,i))$ s'écrit (a_1, a_i) où a_i est distinct des a_k pour $k < i$. C'est vrai pour $i = 2$ te 3. Supposons $i > 3$. Alors $\varphi((1,i))$ est une transposition dont le support rencontre celui de $\varphi((1,k)) = (a_1, a_k)$ pour $2 \leq k \leq i-1$ (par hypothèse de récurrence), car $(1,i)$ et $(1,k)$ ne commutent pas (la démonstration est la même que pour $i = 3$). Si a_1 n'était pas dans le support de $\varphi((1,i))$, $i_2 \geq 2$, cela ne peut se produire que si $i = 4$. Dans ces conditions $\varphi((1,4)) = (a_2, a_3) = (a_1, a_3)(a_2, a_1)(a_1, a_3) = \varphi((3,1)(1,2)(1,3))$ et par injectivité, on a $(1,4) = (3,1)(1,2)(1,3)$, ce qui est faux.

  Donc a_1 est dans le support de $\varphi((1,i))$. Cette dernière s'écrit (a_1, a_i) et par injectivité de φ, a_i est bien distincts des a_k pour $k < i$.

- On se retrouve donc avec n élémnts de $\{1,\dots,n\}$, $a_1,\dots,a_n$ deux à deux distincts tels que $\varphi((1,i)) = (a_1, a_i)$ pour tout $2 \leq i \leq n$. Si on considère la permutation σ qui à $i \in \{1,\dots,n\}$ associe a_i, on a d'après la remarque préliminaire

$$\sigma \circ (1,i) \circ \sigma^{-1} = (a_1, a_i)$$

  Autrement dit, φ coïncide avec l'automorphisme intérieur $\varphi_\sigma : s \mapsto \sigma \circ s \circ \sigma^{-1}$ sur l'ensemble des transpositions $(1,i)$ avec $2 \leq i \leq n$. Comme φ est un morphisme et que les $(1,i)$ forment un système générateur de $\mathcal{S}_n$, on a $\varphi = \varphi_\sigma$.