Automorphismes de $\mathfrak{S}_n$

Leçons : 105, 108

Définition 1

Un automorphisme de $\mathfrak{S}_n$ de la forme $\varphi_\sigma : \tau \mapsto \sigma\tau\sigma^{-1}$ est appelé automorphisme intérieur. Le groupe des automorphismes intérieurs est noté $\mathrm{Int}(\mathfrak{S}_n)$.

Théorème 2

Si $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

On va commencer par prouver la proposition suivante :

Proposition 3

Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ envoie les transpositions sur les transpositions, alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.

Démonstration. Soit φ un tel automorphisme. On sait que $\mathfrak{S}_n$ est engendré par les transpositions $\tau_i = (1\,i)$ pour $i \geqslant 2$. Comme les τ_i ne commutent pas deux à deux, il en va de même des $\varphi(\tau_i)$ donc les $\varphi(\tau_i)$ ne sont pas à supports deux à deux disjoints.

Posons $\varphi(\tau_2) = (\alpha_1\,\alpha_2)$, alors, par exemple, $\varphi(\tau_3) = (\alpha_1\,\alpha_3)$. Comme pour $i > 3$, $\varphi(\tau_i)$ ne commute ni avec $\varphi(\tau_2)$, ni avec $\varphi(\tau_3)$, $\varphi(\tau_i)$ est de la forme $(\alpha_1\alpha_i)$. De plus, les α_i sont deux à deux distincts donc $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\}$. On a ainsi défini une permutation $\alpha \in \mathfrak{S}_n$. De plus, $\forall i \geqslant 2, \alpha\tau_i\alpha^{-1} = (\alpha_1\,\alpha_i) = \varphi(\tau_i)$, donc φ est intérieur. □

Démonstration (du théorème)**.** L'idée générale est de considérer l'action par conjugaison de $\mathfrak{S}_n$ sur lui-même. On note $c(s)$ le centralisateur d'un élément s.

Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Pour $n \geqslant 2, D(\mathfrak{S}_n) = \mathfrak{A}_n$ [1] donc comme φ préserve les commutateurs, il envoie $\mathfrak{A}_n$ sur lui-même. Ainsi, l'image d'une transposition par φ est un élément d'ordre 2 donc un produit d'un nombre d'un impair k de transpositions disjointes. Si $n < 6$, $\mathfrak{A}_n$ ne contient pas de triples transpositions donc $k = 1$ ce qui conclut. Supposons à présent $n > 6$.

Soit $\tau = (a\,b)$. Alors

$$s \in c(\tau) \Leftrightarrow s\tau s^{-1} = \tau \Leftrightarrow (s(a)s(b)) = (a\,b) \Leftrightarrow s(F) = F$$

où $F = E \setminus \{a, b\}$ et $E = [\![1, n]\!]$. Cela fournit un morphisme surjectif $\begin{array}{rccc} r : & c(\tau) & \longrightarrow & \mathfrak{S}_{n-2} \\ & s & \longmapsto & s_{|F} \end{array}$ de noyau $\{1, \tau\}$ donc $\mathfrak{S}_{n-2} \simeq c(\tau)/(\mathbb{Z}/2\mathbb{Z})$.

Supposons que $\varphi(\tau) = \tau'$ soit un produit d'un nombre impair $k \geqslant 3$ de transpositions disjointes $\tau' = (a_1\,a_2)\ldots(a_{2k-1}\,a_{2k})$. On note $\tau_i = (a_{2i-1}\,a_2 i)$. Les τ_i commutent entre eux deux à deux donc pour tout i, $\tau_i \in c(\tau)$. De plus, si $N =< \tau_1, \ldots, \tau_k >$, N est un sous-groupe distingué de $c(\tau')$: si $s \in c(\tau')$, $s\tau' s^{-1} = (s\tau_1 s^{-1})\ldots(s\tau_k s^{-1})$ donc par unicité de la décomposition en cycles à supports disjoints, $\forall i, \exists 1 \leqslant j \leqslant k : s\tau_i s^{-1} = \tau_j$. Donc $c(\tau')$ a un sous-groupe distingué N isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.

Par ailleurs $c(\tau)$ est isomorphe via φ à $c(\tau')$ donc à $c(\tau)$ de sorte qu'en composant avec r, on obtient un morphisme surjectif $f : c(\tau') \twoheadrightarrow \mathfrak{S}_{n-2}$ de noyau $\{1, \tau'\}$.

1. En effet, pour $n \geqslant 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles et ceux-ci sont deux à deux conjugués, donc si $\sigma = (abc)$ est un 3-cycle, $\sigma^2 = (acb)$ en est aussi un donc il existe $\tau \in \mathfrak{A}_n$ tel que $\sigma^2 = \tau\sigma\tau^{-1}$ donc σ est un commutateur

Par théorème d'isomorphisme, $f(N) \simeq N/(\ker(f) \cap N)$. Comme $\tau' \in N$, $\ker f \subset N$ et $f(N) \simeq (\mathbb{Z}/2\mathbb{Z})^k/(\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^{k-1}$ [2]. Or, comme $n-2 \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_{n-2}$ sont $\mathfrak{A}_{n-2}$, {id} et lui-même : par un argument de cardinalité, on conclut à une absurdité. Donc $k = 1$ et φ est intérieur.

□

Remarque.
- La preuve peut également se faire par dénombrement en calculant le cardinal du centralisateur de s produit de $k_1 + \cdots + k_n$ cycles disjoints parmi lesquels k_1 cycles d'ordre 1, ..., k_n d'ordre n, en supposant que $n = k_1 + 2k_2 + \cdots + nk_n$.
- Comme on utilise le fait que $\mathfrak{A}_n$ est le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$ pour $n \geqslant 5$, il faut aussi savoir le prouver !

Référence : Daniel PERRIN (1996). *Cours d'algèbre*. Ellipses, pp. 31-32

2. Ici, il me semble qu'il y a une imprécision dans le Perrin qui affirme que le cas $f(N) \simeq (\mathbb{Z}/2\mathbb{Z})^k$ n'est pas exclu.