Automorphismes de $\mathscr{S}_n$

Achille Méthivier

Théorème 1. *Si $n \neq 6$, alors les automorphismes de $\mathscr{S}_n$ sont intérieurs.*

Lemme 2. *Soit $\varphi \in \mathrm{Aut}(\mathscr{S}_n)$. Si φ envoie transposition sur transposition, alors φ est intérieur.*

Démonstration. On sait que $\mathscr{S}_n$ est engendré par les transpositions de la forme $\tau_i = (1, i)$ pour $i \geq 2$. Pour $i \neq j$, τ_i et τ_j ne commutent pas, et comme φ est un automorphisme (en particulier un morphismes injectif), $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas. Elle ne sont donc pas à supports disjoints. Si on pose $\varphi(\tau_2) = (\alpha_1, \alpha_2)$, on peut supposer $\varphi(\tau_3) = (\alpha_1, \alpha_3)$. On en déduit que pour tout $i > 3$, $\varphi(\tau_i) = (\alpha_1, \alpha_i)$, avec $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\}$. En effet, si ce n'était pas le cas on aurait pour un $i > 3$, $\varphi(\tau_i) = (\alpha_2, \alpha_i)$. Et comme $(\alpha_1, \alpha_2)(\alpha_1, \alpha_i)(\alpha_2, \alpha_i) = (\alpha_1, \alpha_i)$. En prenant φ^{-1}, on aurait $(12)(1i)(2i) = (1i)$ mais la permutation de gauche envoie 2 sur 1 alors que celle de droite envoie $i \neq 2$ sur 1. On en déduit en plus que les α_i sont tous distincts, sinon φ ne saurait être injective. On a donc construit une permutation $\alpha \in \mathscr{S}_n$ telle que $\alpha\tau_i\alpha^{-1} = \varphi(\tau_i)$. Donc, φ coïncide avec le morphisme intérieur i_α sur les τ_i qui engendrent $\mathscr{S}_n$, d'où $\varphi = i_\alpha$. □

Lemme 3. *Soit $s \in \mathscr{S}_n$, et supposons que $n = k_1 + 2k_2 + \cdots + nk_n$ avec $k_i \in N$ et s est produit de $k_1 + \cdots + k_n$ cycles disjoints, avec k_i cycles d'ordre i. Alors, si $c(s)$ désigne le centralisateur de $\mathscr{S}_n$, on a*

$$\#c(s) = \prod_{i=1}^{n} k_i!\, i^{k_i}.$$

Démonstration. Regardons tout d'abord le centralisateur d'un cycle de longueur i, $\alpha = (\alpha_1, \ldots, \alpha_i)$. Soit $\sigma \in c(\alpha)$,

$$\sigma\alpha\sigma^{-1} = \alpha$$
$$(\sigma(\alpha_1), \ldots, \sigma(\alpha_i)) = (\alpha_1, \ldots, \alpha_i).$$

La permutation σ est donc totalement déterminée par sa valeur $\sigma(\alpha_1) \in \{\alpha_1, \ldots, \alpha_i\}$, donc i possibilités. Regardons maintenant $\alpha = (\alpha_1^1, \ldots, \alpha_i^1) \cdots (\alpha_1^{k_i}, \ldots, \alpha_i^{k_i})$, produit de k_i cycles disjoints de longueurs i. Soit $\sigma \in c(\alpha)$,

$$\Big(\sigma(\alpha_1^1), \ldots, \sigma(\alpha_i^1)\Big) \cdots \Big(\sigma(\alpha_1^{k_i}), \ldots, \sigma(\alpha_i^{k_i})\Big) = (\alpha_1^1, \ldots, \alpha_i^1) \cdots (\alpha_1^{k_i}, \ldots, \alpha_i^{k_i}).$$

On a $\sigma(\alpha_1^1) \in \{\alpha_1^1, \ldots, \alpha_i^1\} \sqcup \cdots \sqcup \{\alpha_1^{k_i}, \ldots, \alpha_i^{k_i}\}$. Si $\sigma(\alpha_1^1) \in \{\alpha_1^k, \ldots, \alpha_i^k\}$ pour $1 \leq k \leq k_i$, cela impose $\sigma_{|\{\alpha_1^1, \ldots, \alpha_i^1\}} \in c\big((\alpha_1^k, \ldots, \alpha_i^k)\big)$. On a donc k_i choix pour $\sigma(\alpha_1^1)$ qui devient alors déterminé comme élément du centralisateur d'un des cycles et donc i choix possibles. On recommence pour $\sigma(\alpha_1^2)$ mais cette fois on a plus que $(k_i - 1)$ choix de cycles possibles et encore i choix pour un élément du centralisateur. Finalement, on a bien $k_i!\, i^{k_i}$ possibilités pour σ. On recommence pour chaque k_i, tous les cycles étant à supports disjoints, on trouve bien la formule attendue. □

Démonstration du théorème. Soit $\varphi \in \mathrm{Aut}(\mathscr{S}_n)$ et $\tau \in \mathscr{S}_n$ une transposition. Comme τ est d'ordre 2, $\varphi(\tau)$ l'est aussi et s'écrit comme produit de k transposition à supports disjoints. Soit $s \in \mathscr{S}_n$ et $\sigma \in c(s)$, alors $\varphi\left(\sigma s\sigma^{-1}\right) = \varphi(\sigma)\varphi(s)\varphi(\sigma)^{-1} = \varphi(s)$. Donc $\varphi(c(s)) \subset c(\varphi(s))$. En appliquant le même résultat à φ^{-1} et $\varphi(s)$, on a $\varphi^{-1}\big[c\big(\varphi(s)\big)\big] \subset c\big((s)\big)$, donc $\varphi(c(s)) = c(\varphi(s))$. En particulier $\#c(\tau) = \#c(\varphi(\tau))$, et τ est produit de cycles à supports disjoints : 1 cycle d'ordre 2 et $n-2$ cycle d'ordre 1. De même, $\varphi(\tau)$ est produit de k cycles d'ordres 2 et $n - 2k$ cycles d'ordres 1. Le lemme 3 donne que $2(n-2)! = 2^k k!(n-2k)!$, donc

$$2^{k-1}k! = (n-2)\cdots(n-2k+1)$$
$$\underbrace{2k(2k-2)\cdots 4}_{k-1 \text{ termes}} = \underbrace{(n-2)\cdots(n-2k+1)}_{2(k-1) \text{ termes}}.$$

Notons a le membre de droite et b le membre de gauche et supposons dans la suite $k > 1$ de telle sorte que $2(k-1) > k-1$. On a

$$n - 2 < 2k \leq n \iff 2 > n - 2k \geq 0,$$

donc, si $n - 2k \geq 2$, on a $n - 3 > 2k - 2$ et donc $a > b$.
Traitons le cas $n - 2k = 1$, donc

$$(n-2)! = 2^{\frac{n-1}{2}-1}\left(\frac{n-1}{2}\right)!,$$

et on a

$$\frac{n-1}{2} > n - 2 \iff 3 > n,$$

les cas $n = 3$ ou 4 étant exclus car $k \neq 1$ et n impair, il reste $n \geq 5$. Mais dans ce cas,

$$(n-2)\cdots\left(\frac{n-1}{2}+1\right) = 2^{\frac{n-1}{2}-1}$$

et comme il y a $n-2-\frac{n-1}{2}=\frac{n+1}{2}-1\geq 2$, dès que $n\geq 7$, le produit de gauche dans l'égalité du dessus contient au moins 3 termes et est donc divisible par 3, ce qui reste vrai dans le cas $n=5$, et aboutit à une absurdité.
Le cas $2k=n$ se traite de manière similaire puisqu'on a

$$(n-2)\cdots\left(\frac{n+1}{2}+1\right)=2^{n/2-1},$$

et le terme de gauche est divisible par 3 dès que $n\geq 10$. Il reste les cas $n=2$, 4, 6 ou 8. Le cas 2 étant exclu par l'hypothèse $k\neq 1$, on remarque que le seul cas possible est $n=6$ et $k=3$. Par hypothèse $n\neq 6$, et l'égalité est vérifiée pour $k=1$ seulement, donc $\varphi(\tau)$ est une transposition et on conclut par le lemme 1. □

I Références

— Cours d'algèbre, Daniel Perrin (page 31).