Automorphismes du groupe symétrique

Jérémie Klingler – Université Lyon 1

Recasages : 101, 103, 104, 105, 108 (et 190 si c'est la dèche)

Référence : Pour la démonstration du lemme : *Cours d'algèbre*, Perrin (page 31)
Pour le reste : *Oraux X-ENS, Algèbre 1*, Francinou, Gianella, Nicolas (page 74)

Remarques préliminaires. Je préfère la version de FGN à celle de Perrin qui calcule le cardinal du centralisateur d'une permutation sans en donner la démonstration.
Attention toutefois, cette version est rédigée dans un style « annale de concours » et est donc très détaillée. Il faut donc sélectionner les morceaux que l'on souhaite détailler lors du développement.
Les points en italique sont à énoncer à l'oral.

Soit G un groupe. Un automorphisme φ de G est dit **intérieur** s'il existe $g \in G$ tel que pour tout $x \in G$, $\varphi(x) = gxg^{-1}$.

Théorème. Soit $n \in \mathbf{N}^*$. Si $n \neq 6$, alors les automorphismes du groupe $\mathcal{S}_n$ sont exactement les automorphismes intérieurs.

La démonstration se fait en deux temps. On commence par montrer qu'un automorphisme de $\mathcal{S}_n$ qui envoie les transpositions sur les transpositions est intérieur. Puis, on montre que s'il existe un automorphisme de $\mathcal{S}_n$ qui ne conserve pas les transpositions, alors $n = 6$.

Lemme. Soit $\varphi \in \mathrm{Aut}(\mathcal{S}_n)$ qui envoie les transpositions sur les transpositions. Alors φ est intérieur.

Démonstration du lemme. Soit φ un tel automorphisme.
Commençons par rappeler que $\mathcal{S}_n$ est engendré par la famille de transpositions $(\tau_i)_{2 \leq i \leq n}$, où $\tau_i := (1\, i)$.
Soit $2 \leq i \leq n$. Par hypothèse, $\varphi(\tau_i)$ est une transposition.
Si $i \neq j$, τ_i et τ_j ne commutent pas donc $\varphi(\tau_i)$ et $\varphi(\tau_j)$ non plus. Ainsi, leurs supports ne sont pas disjoints. Il existe donc $\alpha_1 \in \{1, \dots, n\}$ qui appartient à l'instersection des supports des $\varphi(\tau_i)$. [1]
Pour tout $2 \leq i \leq n$, on peut alors noter $\varphi(\tau_i) = (\alpha_1\, \alpha_i)$ avec $\alpha_i \in \{1, \dots, n\}$. En outre, comme φ est bijective (donc injective), on en déduit que les $(\alpha_i)_{1 \leq i \leq n}$ sont distincts. [2]
On peut alors définir la permutation suivante :

$$\alpha := \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix} \in \mathcal{S}_n.$$

Remarquons alors que pour tout $2 \leq k \leq n$, $i_\alpha(\tau_k) := \alpha \tau_k \alpha^{-1} = (\alpha_1\, \alpha_k) = \varphi(\tau_k)$.
Ainsi, les automorphismes φ et i_α coïncident sur les $(\tau_k)_{2 \leq k \leq n}$ qui constituent une partie génératrice de $\mathcal{S}_n$. Ainsi, ils coïncident sur $\mathcal{S}_n$ et donc $\varphi = i_\alpha$.

Démonstration du théorème. Soit $\varphi \in \mathrm{Aut}(\mathcal{S}_n)$. *On veut montrer que φ envoie les transpositions sur les transpositions.* Considérons donc $\tau \in \mathcal{S}_n$.
Comme τ est d'ordre 2, on en déduit que $\varphi(\tau)$ est également d'ordre 2. Ainsi, $\varphi(\tau)$ se décompose en produit de k transpositions à supports disjoints.

Notons T l'ensemble des transpositions dans $\mathcal{S}_n$ et T_k l'ensemble des produits de k transpositions à supports disjoints dans $\mathcal{S}_n$.

1. à savoir détailler lors d'une éventuelle question
2. si $\alpha_i = \alpha_1$, alors $\tau_i \in \operatorname{Ker}\varphi$ qui n'est donc pas trivial. Si $\alpha_i = \alpha_j$, alors $\varphi(\tau_i) = \varphi(\tau_j)$ et φ est non injectif.

On rappelle que T et T_k sont stables par conjugaison dans $\mathcal{S}_n$ [3] et sont donc les orbites respectives de τ et de $\varphi(\tau)$ par l'action de conjugaison dans $\mathcal{S}_n$. [4] Montrons alors que $\varphi(T) = T_k$.
Considérons $\tau' \in T$. Alors il existe $\sigma \in \mathcal{S}_n$ telle que $\tau' = \sigma\tau\sigma^{-1}$ et donc $\varphi(\tau') = \varphi(\sigma\tau\sigma^{-1}) = \varphi(\sigma)\varphi(\tau)\varphi(\sigma)^{-1} \in T_k$ *car T_k est stable par conjugaison.*
Réciproquement, considérons $\tau' = \sigma\varphi(\tau)\sigma^{-1} \in T_k$. Alors

$$\tau' = \varphi(\varphi^{-1}(\sigma)\tau\varphi^{-1}(\sigma^{-1})) = \varphi(\varphi^{-1}(\sigma)\tau(\varphi^{-1}(\sigma))^{-1}).$$

On a $\varphi^{-1}(\sigma)\tau(\varphi^{-1}(\sigma))^{-1} \in T$ car T est stable par conjugaison donc $\tau' \in \varphi(T)$.
Comme φ est bijective, on en déduit que $|T| = |T_k|$. Calculons alors le cardinal de T_k. On a :

$$|T_k| = \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}}{k!},$$

car il faut choisir successivement les supports des k transpositions, puis diviser par $k!$ car on peut écrire le produit de ces transpositions dans l'ordre que l'on souhaite, étant donné qu'elles commutent toutes entre elles (car elles sont à supports disjoints).
On calcule alors :

$$|T_k| = \frac{n!(n-2)!\cdots(n-2k+2)!}{2^k(n-2)!(n-4)!\cdots(n-2k)!} \cdot \frac{1}{k!} = \frac{n!}{2^k k!(n-2k)!} = \binom{n-k}{k}\frac{n(n-1)\cdots(n-k+1)}{2^k}$$

En outre, $|T| = \binom{n}{2} = \dfrac{n(n-1)}{2}$.
Si $k = 1$, on en déduit que $\varphi(T) = T$ et donc que φ envoie les transpositions sur les transpositions et est donc un automorphisme intérieur, en vertu du lemme.
Si $k = 2$, alors $|T_k| = |T|$ conduit à

$$\binom{n-2}{2}\frac{1}{2} = 1 \text{ donc } (n-2)(n-3) = 4,$$

ce qui est impossible *car le produit de deux entiers consécutifs ne peut être égal à 4.*
Supposons alors $k \geq 3$. Alors $|T_k| = |T|$ conduit à

$$\binom{n-k}{k}\frac{(n-2)\cdots(n-k+1)}{2^{k-1}} = 1 \text{ donc } \binom{n-k}{k}(n-2)\cdots(n-k+1) = 2^{k-1},$$

ce qui n'est possible que si $-k+1 = 2$ *car sinon le produit de gauche comporterait un nombre impair.*
Il en découle donc que $k = 3$ et donc $\binom{n-3}{3}(n-2) = 4$, ce qui conduit à $(n-2)(n-3)(n-4)(n-5) = 12$ et donc $n = 6$.
Par contraposée, on en déduit donc que si $n \neq 6$, alors $\varphi(T) = T$ et φ est un automorphisme intérieur d'après le lemme.

3. à savoir détailler lors des questions
4. comme T et T_k sont stables par l'action de conjugaison, ils sont inclus dans l'une de ses orbites et l'on peut alors faire le choix que l'on veut du représentant de l'orbite. Il faut être à l'aise avec son cours d'actions de groupes ici.