2.7 Automorphismes de $\mathfrak{S}_n$ (104, 105, 108) [18],[11]

Quand on regarde les groupes, il est naturel de regarder plusieurs choses : son action sur des ensembles naturels, s'il est isomorphe à d'autres groupes connus ou encore sa structure interne : les sous-groupes distingués, les centralisateurs, les classes de conjugaisons ou encore les automorphismes (notamment pour connaître les structures de produit semi-directs). Je propose ici d'étudier les automorphismes de $\mathfrak{S}_n$. On en connaît déjà quelques uns : les automorphismes intérieurs. En fait, pour $n \neq 6$, ce sont les seuls !

Théorème 2.19. Soit $n \in \mathbb{N}$. Si $n \neq 6$, alors $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Démonstration. Si $n \in \{0, 1, 2\}$, le résultat est clair (dans tous ces cas, le seul automorphisme est l'identité, qui est bien intérieur). Prenons alors $n \geqslant 3$. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ est intérieur, disons $\varphi = \mathrm{Int}_{\sigma_0}$, alors φ préserve les types cycliques :

$$\varphi\left(\begin{pmatrix} i_1 & \dots & i_k \end{pmatrix}\right) = \sigma_0 \circ \begin{pmatrix} i_1 & \dots & i_k \end{pmatrix} \circ \sigma_0^{-1} = \begin{pmatrix} \sigma_0(i_1) & \dots & \sigma_0(i_k) \end{pmatrix}.$$

En particulier, il envoie une transposition sur une autre transposition. En réalité, cela caractérise les automorphismes intérieurs de $\mathfrak{S}_n$!

Lemme 2.20. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si l'image de toute transposition par φ est une transposition, alors φ est intérieur.

Démonstration du lemme. On se base ici sur le fait que les transpositions $\tau_i = \begin{pmatrix} 1 & i \end{pmatrix}, i \in [\![2, n]\!]$ engendrent le groupe $\mathfrak{S}_n$. Regardons alors $\varphi(\tau_i)$. On sait que c'est une transposition par hypothèse. De plus, pour $i \neq j$, τ_i et τ_j ne commutent pas étant donné qu'elles ont un support différent mais pas disjoint. Ainsi $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas non plus. Elles ont donc un unique élément en commun dans leur support. En posant alors :

$$\varphi(\tau_2) = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix}$$

avec $\alpha_1 \neq \alpha_2 \in [\![1, n]\!]$. On peut donc supposer :

$$\varphi(\tau_3) = \begin{pmatrix} \alpha_1 & \alpha_3 \end{pmatrix}$$

avec $\alpha_3 \notin \{\alpha_1, \alpha_2\}$ (possible car on a supposé $n \geqslant 3$). Si $n = 3$, on a alors construit une permutation :

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix}$$

et Int_α coïncide avec φ sur τ_2 et τ_3 qui engendrent $\mathfrak{S}_3$, ce qui conclut. On va alors généraliser cette situation au cas $n \geqslant 4$. Montrons que les $\varphi(\tau_i)$, pour $i \geqslant 4$ ont également α_1 dans leur support. Si $i_0 \geqslant 4$ est tel que $\varphi(\tau_{i_0})$ n'a pas α_1 dans son support, il possède alors α_2 dans son support car il ne commute pas avec $\varphi(\tau_2)$. Par le même argument, il possède aussi α_3 dans son support : $\varphi(\tau_{i_0})$ ne commute pas avec $\varphi(\tau_3)$. Ainsi, puisque $\varphi(\tau_{i_0})$ est une transposition et que $\alpha_2 \neq \alpha_3$, on a découvert qui était $\varphi(\alpha_{i_0})$!

$$\varphi(\tau_{i_0}) = \begin{pmatrix} \alpha_2 & \alpha_3 \end{pmatrix}.$$

Ainsi :

$$\varphi(\tau_2)\varphi(\tau_3)\varphi(\tau_{i_0}) = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} \circ \begin{pmatrix} \alpha_1 & \alpha_3 \end{pmatrix} \circ \begin{pmatrix} \alpha_2 & \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_3 \end{pmatrix} = \varphi(\tau_3),$$

et donc en composant par φ^{-1}, on a :

$$\begin{pmatrix} 1 & i_0 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & i_0 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \quad \textbf{ABSURDE !!}$$

Ainsi, on a :

$$\forall i \in [\![4, n]\!],\ \exists! \alpha_i \in [\![1, n]\!], \quad \varphi(\tau_i) = \begin{pmatrix} \alpha_1 & \alpha_i \end{pmatrix}.$$

De plus, par injectivité de φ, les α_i sont tous distincts. Ainsi, on a :

$$\{\alpha_1, \ldots, \alpha_n\} = [\![1, n]\!],$$

de sorte que l'on a défini une permutation :

$$\alpha = \begin{pmatrix} 1 & \cdots & n \\ \alpha_1 & \cdots & \alpha_n \end{pmatrix}$$

vérifiant :

$$\forall i \in [\![2, n]\!], \quad \mathrm{Int}_\alpha(\tau_i) = \varphi(\tau_i).$$

Ainsi, étant donné que les τ_i engendrent $\mathfrak{S}_n$:

$$\varphi = \mathrm{Int}_\alpha$$

ce qui conclut la preuve de ce lemme ! □

Reste à montrer, en vertu de ce lemme, que pour $n \neq 6$, les transpositions sont envoyées par φ sur des transpositions. Comment le montrer ? Si τ est une transposition, alors on a bien que $\varphi(\tau)$ est d'ordre 2 mais ça pourrait être un produit de plusieurs transpositions à supports disjoints... Cependant, une transposition et un produit de plusieurs transpositions n'ont pas les mêmes propriétés algébriques. En particulier elles n'ont pas forcément les mêmes centralisateurs !

Proposition 2.21. Si $\sigma \in \mathfrak{S}_n$ est de type cyclique $(k_1, \ldots, k_n)$ avec $(k_1, \ldots, k_n) \in \mathbb{N}^n$ tels que :

$$\sum_{i=1}^{n} i k_i = n,$$

(i.e. σ s'écrit, dans sa décomposition en produits de cycles à supports disjoints comme le produits de k_1 1-cycles, de k_2 2-cycles, etc.) alors, en notant $Z(\sigma)$ le centralisateur de σ, c'est-à-dire :

$$Z(\sigma) = \left\{ \tau \in \mathfrak{S}_n \;\middle|\; \tau \circ \sigma \circ \tau^{-1} = \sigma \right\},$$

alors :

$$|Z(\sigma)| = \prod_{i=1}^{n} k_i! i^{k_i}.$$

Démonstration. Soient $\sigma \in \mathfrak{S}_n$ s'écrivant sous la forme :

$$\left(j_{1,1}^{(1)}\right) \cdots \left(j_{1,k_1}^{(1)}\right) \left(j_{1,1}^{(2)} \quad j_{2,1}^{(2)}\right) \cdots \left(j_{1,k_2}^{(2)} \quad j_{2,k_2}^{(2)}\right) \cdots \left(j_{1,1}^{(n)} \quad \cdots \quad j_{n,1}^{(n)}\right) \cdots \left(j_{1,k_n}^{(n)} \quad \cdots \quad j_{n,k_n}^{(n)}\right)$$

avec $\left\{ j_{1,1}^{(1)}, \ldots, j_{1,k_1}^{(1)}, j_{1,1}^{(2)}, \ldots, j_{2,k_2}^{(2)}, \ldots, j_{n,k_n}^{(n)} \right\} = [\![1, n]\!]$ et $\tau \in Z(\sigma)$. On a alors :

$$\begin{array}{rcl} \tau\sigma\tau^{-1} & = & \left(\tau\left(j_{1,1}^{(1)}\right)\right) \cdots \left(\tau\left(j_{1,k_1}^{(1)}\right)\right) \left(\tau\left(j_{1,1}^{(2)}\right) \quad \tau\left(j_{2,1}^{(2)}\right)\right) \cdots \left(\tau\left(j_{1,k_2}^{(2)}\right) \quad \tau\left(j_{2,k_2}^{(2)}\right)\right) \\ \cdots & & \left(\tau\left(j_{1,1}^{(n)}\right) \quad \cdots \quad \tau\left(j_{n,1}^{(n)}\right)\right) \cdots \left(\tau\left(j_{1,k_n}^{(n)}\right) \quad \cdots \quad \tau\left(j_{n,k_n}^{(n)}\right)\right) \\ & = & \sigma. \end{array}$$

Pour déterminer le cardinal de $Z(\sigma)$, on peut déterminer le nombre de choix possibles pour les images de τ :

— $\tau\left(j_{1,1}^{(1)}\right)$ doit appartenir à $\left\{j_{1,1}^{(1)},\ldots,j_{1,k_1}^{(1)}\right\}$ par unicité de la décomposition en produits de cycles à supports disjoints. Ainsi, il y a k_1 choix possibles pour $\tau\left(j_{1,1}^{(1)}\right)$. Il n'y en aura alors plus que k_1-1 pour $\tau\left(j_{1,2}^{(1)}\right)$, k_1-2 pour $\left(j_{1,3}^{(1)}\right)$,etc. On a donc au total $k_1!$ choix possibles pour les images dans les 1-cycles.

— L'image $\tau\left(j_{1,1}^{(2)}\right)$ doit être placée dans un des k_2 2-cycles (k_2 possibilités) et doit être égal à l'un des 2 entiers apparaissant dans ce cycle : 2 possibilités. L'image de $j_{2,1}^{(2)}$ est alors imposée et doit être égal à l'autre entier apparaissant dans ce cycle : 1 possibilité. Ainsi, l'image de $j_{1,2}^{(2)}$ doit être placé dans l'un des k_2-1 cycles restants et doit être égal à l'un des deux entiers apparaissant dans ce cycle : $2(k_2-1)$ possibilités. Là encore, on a donc que l'image de $j_{2,2}^{(2)}$ est imposée, etc. On a donc au total $2k_2\times 2(k_2-1)\times\ldots 2\times 1=2^{k_2}k_2!$ choix possibles pour les images dans les 2-cycles.

— De manière générale, l'image de $j_{1,1}^{(l)}$ doit être placée dans un des k_l l-cycles et doit être égale à l'un des l entiers apparaissant dans ce cycle. Les images de $j_{2,1}^{(l)},\ldots,j_{l,1}^{(l)}$ sont alors imposées : $j_{2,1}^{(l)}$ doit être égal à $\sigma\left(\tau\left(j_{1,1}^{(l)}\right)\right)$, $j_{3,1}^{(l)}$ doit être égal à $\sigma^2\left(\tau\left(j_{1,1}^{(l)}\right)\right)$, etc. Il y a donc lk_l possibilités pour les images de $j_{1,1}^{(l)},\ldots,j_{l,1}^{(l)}$. Ensuite, l'image de $j_{1,2}^{(l)}$ doit être placée dans l'un des k_l-1 l-cycles restants et doit être égale à l'un des l entiers y apparaissant. Les images de $j_{2,2}^{(l)},\ldots,j_{l,2}^{(l)}$ sont alors imposées, etc. D'où $l(k_l-1)$ choix possibles au total pour les images de $j_{1,2}^{(l)},\ldots,j_{l,2}^{(l)}$, etc. On obtient au final $lk_l\times l(k_l-1)\times\ldots\times l\times 1=l^{k_l}k_l!$ choix possibles pour les images de $j_{1,1}^{(l)},\ldots,j_{l,k_l}^{(l)}$.

D'où la formule :

$$|Z(\sigma)|=\prod_{i=1}^{n}k_i!i^{k_i}.$$

□

On va utiliser cette formule pour exhiber la condition $n\neq 6$. Étant donné que φ est un automorphisme, on a, pour toute transposition τ :

$$\varphi\left(Z(\tau)\right)=Z\left(\varphi(\tau)\right).$$

D'où :

$$|Z(\tau)|=|\varphi\left(Z(\tau)\right)|=|Z\left(\varphi(\tau)\right)|.$$

Ainsi, d'après la formule plus haut, et en notant k le nombre de transpositions apparaissant dans l'écriture en produits de cycles à supports disjoints de $\varphi(\tau)$, on a :

$$2(n-2)!=2^k k!(n-2k)!,$$

i.e.

$$\begin{aligned}1&=\binom{n-2}{2k-2}\frac{(2k-2)!}{2^{k-1}k!}\\&=\binom{n-2}{2k-2}\frac{(2k-2)(2k-4)\ldots(4)(2)\times(2k-3)(2k-5)\ldots(3)(1)}{k(2k-2)(2k-4)\ldots(4)(2)}\\&=\binom{n-2}{2k-2}\frac{(2k-3)(2k-5)\ldots(3)(1)}{k}.\end{aligned}$$

Cette égalité ne peut avoir lieu si $k\geqslant 4$, car dans ce cas-là :

$$\frac{(2k-3)(2k-5)\ldots(3)(1)}{k}>1.$$

Reste donc à traiter les cas $k=2$ ou $k=3$ et à les exclure également. Si $k=2$, on a à résoudre en n :

$$\binom{n-2}{2}\frac{1}{2}=1$$

i.e.

$$\binom{n-2}{2} = 2.$$

Le seul coefficient binomial valant 2 est le coefficient binomial $\binom{2}{1}$. Il n'y a donc pas de solutions. Si $k = 3$, on doit alors avoir :

$$\binom{n-2}{4} = 1$$

qui a lieu uniquement pour $n = 6$. Ainsi, si $n \neq 6$, il n'y a pas de solutions et donc $k = 1$: les transpositions sont envoyées sur des transpositions et la preuve est terminée ! $\square$