Les automorphismes de $\mathfrak{S}_n$

Alexis Guérin

Leçons concernées : 101, 104, 105, 108, 126, 190.

Le développement ne continent que la preuve du premier théorème et du lemme. Les autres résultats sont tout de même indispensables à connaître car ils sont sources de beaucoup de questions.

Théorème
Pour $n \neq 6$, tous les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs. En d'autres termes on a :

$$Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$$

Avant d'aborder la démonstration du théorème nous allons prouver le lemme suivant :

Lemme Soit $\varphi \in Aut(\mathfrak{S}_n)$, si φ transforme les transpositions en transpositions, alors $\varphi \in Int(\mathfrak{S}_n)$.

Preuve Si φ est un morphisme, il suffit de prouver la propriété pour un système de générateurs de $\mathfrak{S}_n$. On choisit alors le système de générateurs : $\tau_i = (1\ i+1)$ pour $i \in [\![1, n-1]\!]$. Par hypothèse, $\varphi(\tau_i)$ est aussi une transposition. De plus pour $i \neq j$ $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne sont pas à supports disjoints. En effet si c'était le cas $\varphi(\tau_i)$ et $\varphi(\tau_j)$ commuteraient, or

$$\varphi(\tau_i\tau_j) = \varphi(\tau_i)\varphi(\tau_j) = \varphi(\tau_j)\varphi(\tau_i) = \varphi(\tau_j\tau_j).$$

Donc par bijectivité de φ on aurait que $\tau_i\tau_j = \tau_j\tau_i$ ce qui est faux.
Pour $i = 1$ et $j = 2$ on peut donc noter $\varphi(\tau_1) = (a_1\ a_2)$ et $\varphi(\tau_2) = (a_1\ a_3)$ avec $a_1, a_2, a_3 \in [\![1, n]\!]$ et comme φ est un morphisme bijectif, a_1, a_2, a_3 sont différents. De plus comme τ_3 ne commute ni avec τ_1 ni avec τ_2, le support $\varphi(\tau_3)$ admet une intersection non vide avec le support de $\varphi(\tau_1)$ et celui de $\varphi(\tau_2)$. Supposons que l'on soit dans la cas où $Supp(\varphi(\tau_1)) \cap Supp(\varphi(\tau_2))Supp(\varphi(\tau_3)) = \varnothing$, alors on a obligatoirement $\varphi(\tau_3) = (a_2\ a_3)$ ainsi,

$$\varphi(\tau_1\tau_2\tau_3) = (a_1\ a_2)(a_1\ a_3)(a_2\ a_3) = (a_1\ a_3) = \varphi(\tau_2).$$

Donc par bijectivité de φ on a donc $\tau_1\tau_2\tau_3 = \tau_2$. Ce qui est absurde. On en conclut donc que $a_1 \in Supp(\varphi(\tau_3))$. Ainsi, il existe un élément $a_4 \in [\![1, n]\!]$ différent de a_1, a_2, a_3 tel que $\varphi(\tau_3) = (a_1\ a_4)$. En répétant le argument on se rend compte que pour tout $i \in [\![1, n-1]\!]$ $\varphi(\tau_i) = (a_1\ a_{i+1})$ avec a_{i+1} différent de $a_1, a_2, \dots a_i$.
On a donc obtenu une permutation $\sigma \in \mathfrak{S}_n$ définie par $\sigma(i) = a_i$ telle que pour toutes transpositions de la forme τ_i on ait $\varphi(\tau_i) = \sigma\tau_i\sigma^{-1}$. Comme $(\tau_i)_{i\in[\![1,n]\!]}$ est un système de générateurs de $\mathfrak{S}_n$, on a donc prouvé que $\varphi \in Int(\mathfrak{S}_n)$.

□

La réciproque de ce lemme est évidente. Nous pouvons maintenant passer à la preuve du théorème.

Preuve Soit $\varphi \in Aut(\mathfrak{S}_n)$. Comme l'ordre d'une permutation est une propriété algébrique alors l'image de toute transposition par un automorphisme de $\mathfrak{S}_n$ est d'ordre 2. On note

$$T_k = \{(a_1\ a_2)(a_3\ a_4)\dots(a_{2k-1}\ a_{2k}) \text{ tel que } a_i \in [\![1,n]\!]\ a_i \neq a_j \text{ si } i \neq j\}.$$

D'après le théorème **??** T_k est une classe de conjugaison de $\mathfrak{S}_n$ d'éléments d'ordre 2. Donc en utilisant le lemme **??** pour tous $k \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$ $\varphi(T_k) = T_{k'}$ avec $k' \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$. En particulier, il existe un $k_1 \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$ tel que $\varphi(T_1) = T_{k_1}$. Montrons que $k = 1$ en raisonnant par l'absurde. Pour cela nous allons calculer le cardinal des T_k par récurrence. Nous allons montrer que

$$\#T_k = \frac{n(n-1)\dots(n-2k+1)}{2^k k!}.$$

Commençons par $T_1 = \{(a_1\ a_2) \text{ tel que } a_i \in [\![1,n]\!]\ a_1 \neq a_2\}$. Nous avons n choix possibles pour a_1 et comme $a_2 \neq a_1$, nous avons $n-1$ choix possibles pour a_2. En procédant ainsi on a compté deux fois chaque transposition ($(a_1\ a_2)$ et $(a_2\ a_1)$), donc $\#T_1 = \frac{n(n-1)}{2}$.
On suppose que la propriété est vraie au rang k, prouvons la au rang $k+1$. Or

$$T_{k+1} = \{\underbrace{(a_1\ a_2)(a_3\ a_4)\dots(a_{2k-1}\ a_{2k})}_{\in T_k}(a_{2k}\ a_{2k+1}) \text{ tel que } a_i \in [\![1,n]\!]\ a_i \neq a_j \text{ si } i \neq j\}$$

Donc $\#T_{k+1} = \#T_k \times \underbrace{(n-2k)(n-2k-1)}_{\text{choix de } a_{2k} \text{ et } a_{2k+1}} \times \underbrace{\frac{1}{2}}_{\text{doublons dernière transpo}} \times \underbrace{\frac{1}{k+1}}_{\text{compte } k+1 \text{ fois même élément}}$

En utilisant l'hypothèse de récurrence on obtient donc que $\#T_{k+1} = \frac{n(n-1)\dots(n-2k-1)}{2^{k+1}(k+1)!}$. Ce qui achève la récurrence.
Or $\varphi(T_1) = T_{k_1}$ et φ est bijectif, donc on a : $\#T_1 = \#T_{k_1}$ et donc

$$2^{k_1-1}(k_1)! = (n-2)\dots(n-2k_1+1).$$

Pour $k_1 = 2$ l'équation devient : $(n-2)(n-3) = 4$, qui n'admet pas de solution sur $\mathbb{N}$ (On a un polynôme de degré 2 qui n'admet pas de racine dans entière).
Pour $k_1 > 3$, l'équation se réécrit : $(n-2)(n-3)\dots(n-k_1+1)\underbrace{\frac{(n-k_1)\dots(n-2k_1+1)}{k_1!}}_{=\binom{n-k_1}{k_1} \in \mathbb{N}} = 2^{k_1-1}$.
Or comme $(n-2)$ ou $(n-3)$ est impair par unicité de la décomposition en facteur premier, on trouve que l'équation considérée n'admet pas de solution.
Pour $k_1 = 3$ l'équation devient : $(n-2)(n-3)(n-4)(n-5) = 2^2 3! = 4!$ ce qui est équivalent à $\binom{n-2}{4} = 1$, on trouve donc $n = 6$.
Donc pour $n \neq 6$ $\varphi(T_1) = T_1$, ainsi en utilisant le lemme on conclut que si $n \neq 6$ alors $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$.

□

Corollaire Pour $n \neq 6$, $Aut(\mathfrak{S}_n) \simeq \mathfrak{S}_n$

La démonstration précédente ne nous aide pas à comprendre ce qui se passe réellement pour le cas $n = 6$. Nous allons donc un peu nous attarder sur les automorphismes de $\mathfrak{S}_6$. Dans un premier temps montrons le résultat suivant.

Propriété Pour $n \neq 4$, les propriétés suivantes sont équivalentes :

1. $Aut(\mathfrak{S}_n) \simeq Int(\mathfrak{S}_n)$
2. Les sous groupes d'indice n de $\mathfrak{S}_n$ sont tous conjugués.

Preuve Prouvons dans un premier temps que (non 2) $\Rightarrow$ (non 1).
Soit H un sous groupe d'indice n de $\mathfrak{S}_n$. On note $S(i)$ le stabilisateur de $i \in [\![1, n]\!]$ sous l'action naturelle de $\mathfrak{S}_n$ sur $[\![1, n]\!]$, donc $S(i) = \{\sigma \in \mathfrak{S}_n \mid \sigma(i) = i\}$. Alors il est immédiat que $S(i)$ est un sous groupe de $\mathfrak{S}_n$ et que comme il est isomorphe à $\mathfrak{S}_{n-1}$, il est d'indice n. Donc en particulier $S(i)$ n'est pas conjugué à H.
En remarquant que $\mathfrak{S}_n$ agit par translation à gauche sur ${}^{\mathfrak{S}_n}/_H$, on a donc un morphisme

$$\varphi : \mathfrak{S}_n \to \mathfrak{S}({}^{\mathfrak{S}_n}/_H).$$

Montrons que ce morphisme est bijectif, pour cela commençons par remarquer qu'il nous suffit de prouver l'injectivité car $\mathfrak{S}({}^{\mathfrak{S}_n}/_H) \simeq \mathfrak{S}_n$. Or, $Ker(\varphi) = \cap_{\sigma \in \mathfrak{S}_n} \sigma H \sigma^{-1}$, donc $Ker(\varphi) \subset H$, en particulier on a $\#Ker(\varphi) \leqslant \#H = (n-1)! < \frac{n!}{2}$ car $n \geqslant 5$. De plus H est un sous groupe distingué de $\mathfrak{S}_n$, donc le corollaire **??** et l'inégalité sur le cardinal de $Ker(\varphi)$ nous assure que $Ker(\varphi) = \{Id\}$. Donc φ est bien bijectif.
Dans cet isomorphisme, le stabilisateur de $H \in {}^{\mathfrak{S}_n}/_H$ est $\varphi(H)$. On considère maintenant f une bijection de ${}^{\mathfrak{S}_n}/_H$ sur $[\![1, n]\!]$ telle que $f(H) = 1$. On en déduit alors un isomorphisme

$$\psi : \sigma({}^{\mathfrak{S}_n}/_H) \to \mathfrak{S}_n.$$

tel que $\psi(\varphi(H)) = S(1)$. Or comme par hypothèse, H et $S(1)$ ne sont pas conjugués, l'automorphisme $\psi \circ \varphi$ n'est pas un automorphisme intérieur.

La réciproque (non 1) $\Rightarrow$ (non 2), se prouve rapidement une fois que l'on sait que l'image d'un sous groupe d'indice n par un automorphisme est encore un sous groupe d'indice n.

□

Remarque Dans le cas où $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$, les sous groupes d'indice n de $\mathfrak{S}_n$ sont en fait exactement les $S(i)$. En effet soit H un sous groupe d'indice n de $\mathfrak{S}_n$, alors H est conjugué à tous les $S(i)$. En utilisant le fait que $S(j) = (i\ j)S(j)(i\ j)$ et que les transpositions engendrent $\mathfrak{S}_n$, on prouve qu'il existe un $k \in [\![1, n]\!]$, tel que $H = S(k)$.

Propriété On a $Aut(\mathfrak{S}_6) \neq Int(\mathfrak{S}_6)$

Preuve D'après la propriété précédente, il suffit de construire un sous groupe d'indice 6 de $\mathfrak{S}_6$, qui n'est pas conjugué aux $S(i)$. Pour ceci, il suffit de trouver un sous groupe H qui opère transitivement sur $[\![1, 6]\!]$.
Soit k le nombre de 5-Sylow de $\mathfrak{S}_5$, d'après le troisième théorème de Sylow, $k|24$ et $k \equiv 1\ (mod\ 5)$. Donc $k = 1$ ou $= 6$. Le cas $k = 1$ est exclu par le corollaire **??**. Donc $\mathfrak{S}_5$ possède six 5-Sylow. On note X l'ensemble des 5-Sylows de $\mathfrak{S}_5$. Or $\mathfrak{S}_5$ agit sur X par conjugaison, transitivement et fidèlement. On a donc un morphisme de groupe injectif :

$$\varphi : \mathfrak{S}_5 \to \mathfrak{S}(X) \simeq \mathfrak{S}_6$$

De plus comme $\mathfrak{S}_5$ agit transitivement sur X, alors le sous groupe $\varphi(\mathfrak{S}_5)$ convient.

□

Références :

Algèbre le Grand Combat de Grégory Berhuy.
Cours d'algèbre de Daniel Perrin.