

AUTOMORPHISMES DE $\mathfrak{S}_n$

- 101, 103, 104, 105, 108 -

—

Considérons G un groupe quelconque. Tout élément de G s'identifie à un automorphisme de G via la formule :

$$\forall g \in G, \iota(g) : x \mapsto gxg^{-1} \quad (1)$$

Un tel automorphisme est qualifié d'intérieur, et nous noterons $\text{Int}(G)$ l'ensemble des tels automorphismes. Dans ce cadre, la flèche ι correspond également à l'action de G sur lui-même par conjugaison. Ainsi, quel que soit le groupe auquel on s'intéresse, on dispose d'une suite exacte ⁽ⁱ⁾ :

$$1 \longrightarrow Z(G) \hookrightarrow G \twoheadrightarrow \text{Int}(G) \longrightarrow 1 \quad (2)$$

Ainsi, dans le cas où le groupe est de centre trivial, on obtient un isomorphisme entre G et son groupe d'automorphismes intérieurs. Dans le cas du groupe symétrique $\mathfrak{S}_n$, il se passe quelque chose d'encore plus joli : tous les automorphismes de $\mathfrak{S}_n$ se réalisent comme un automorphisme intérieur, c'est-à-dire que pour $n \geq 3$, on a un isomorphisme $\mathfrak{S}_n \cong \text{Aut}(\mathfrak{S}_n)$! Tous les automorphismes, vraiment ? Eh non, il y a (de façon superbe ou catastrophique selon les gens) un phénomène exceptionnel qui se produit lorsque $n = 6$, mettant en défaut le théorème...

Dans ce développement, nous allons démontrer ce résultat d'une façon peut-être moins classique que ce qui est généralement présenté, qui repose beaucoup plus sur la théorie des groupes et moins sur la combinatoire. **En conséquence, cette preuve n'est pas présentable dans la 190.** En contrepartie, je pense qu'elle gagne un recasage impeccable dans la 103.

Il s'agit de la preuve alternative présentée par Perrin, qui à mon sens à l'énorme avantage d'être beaucoup plus naturelle (donc facile à retenir !) que la preuve combinatoire, mais elle est certainement plus exigeante en terme de théorie. J'apprécie particulièrement le fait que le cas $n = 6$ apparaisse de lui-même au cours de la preuve, en mettant en évidence un argument de structure de $\mathfrak{S}_n$, ce qui, je trouve, ne se produit pas dans la preuve combinatoire classique.

Soit $n \in \mathbb{N}^*$. On note $\mathfrak{S}_n$ le groupe symétrique et $\mathfrak{A}_n$ le groupe alterné. On notera un k -cycle de la façon compacte habituelle :

$$\sigma = (a_1 \ a_2 \ \dots \ a_k) \quad (3)$$

Etant donné g un élément d'un groupe G , on appellera *centralisateur* de g et on notera $C(g)$ le stabilisateur de g sous l'action par conjugaison de G sur lui-même, c'est-à-dire :

$$C(g) := \{h \in G \mid hgh^{-1} = g\} \quad (4)$$

En tant que stabilisateur, c'est un sous-groupe de G . Notre objectif est de démontrer le théorème suivant :

(i). C'est la première (mais pas la dernière) fois que j'utilise une suite exacte dans ce développement. Il s'agit en effet de la présentation choisie par Perrin, et pour ma part je trouve que cela fournit une façon très agréable de voir les choses. Cela dit, on peut complètement éviter de parler de suite exacte ici, et si c'est une notion qui ne vous parle pas, je pense qu'il vaut mieux la contourner (typiquement, si ça ne vous paraît pas clair qu'une suite exacte courte donne des informations immédiates sur un noyau et un quotient).

Théorème 1 (Automorphismes de $\mathfrak{S}_n$ ([1], theo. 8.7)). *Les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs, sauf peut-être pour $n = 6$ ⁽ⁱⁱ⁾.*

Un lemme efficace ([1], prop. 8.8)

Toute la démonstration va reposer sur l'observation suivant :

Lemme 2. *Soit $\Phi \in \text{Aut}(\mathfrak{S}_n)$. Si l'image par Φ de toute transposition reste une transposition, alors Φ est intérieur.*

Démonstration. On suppose que pour toute transposition τ , $\Phi(\tau)$ est encore une transposition. Remarquons que les cas $n = 1$ et $n = 2$ sont triviaux, on supposera donc $n \geq 3$. Considérons la famille :

$$\forall i \in \llbracket 2, n \rrbracket, \tau_i := (1 \ i) \quad (5)$$

dont on sait qu'elle engendre $\mathfrak{S}_n$. Etant donnés $i \neq j$, τ_i et τ_j ne commutent pas car partagent 1 dans leurs supports. En conséquence, les transposition $\Phi(\tau_i)$ et $\Phi(\tau_j)$ ne commutent pas non plus, et nécessairement, leurs supports ne sont pas disjoints. Notons donc :

$$\Phi(\tau_2) = (\alpha_1 \ \alpha_2) \quad \Phi(\tau_3) = (\alpha_1 \ \alpha_3) \quad (6)$$

Soit $i \in \llbracket 2, n \rrbracket$. $\Phi(\tau_i)$ est nécessairement de la forme $(\alpha_1 \ \alpha_i)$ ou $(\alpha_2 \ \alpha_3)$. Montrons que le deuxième cas est exclu en supposant par l'absurde $\Phi(\tau_i) = (\alpha_2 \ \alpha_3)$ ⁽ⁱⁱⁱ⁾. On a alors :

$$\tau_2 \tau_3 \tau_i = (1 \ i \ 3 \ 2) \quad (7)$$

Mais en appliquant Φ :

$$\Phi(\tau_2) \Phi(\tau_3) \Phi(\tau_i) = (\alpha_1 \ \alpha_2)(\alpha_1 \ \alpha_3)(\alpha_2 \ \alpha_3) = (\alpha_1 \ \alpha_3) \quad (8)$$

Or Φ préserve l'ordre en tant qu'automorphisme, on a donc une contradiction. Ceci permet d'écrire :

$$\forall i \in \llbracket 2, n \rrbracket, \exists! \alpha_i \in \llbracket 1 \ n \rrbracket : \Phi(\tau_i) = (\alpha_1 \ \alpha_i) \quad (9)$$

On a ainsi construit une permutation $\alpha : i \mapsto \alpha_i$ et on a :

$$\forall i \in \llbracket 2, n \rrbracket, \alpha \tau_i \alpha^{-1} = \Phi(\tau_i) \quad (10)$$

c'est-à-dire que Φ et $\iota(\alpha)$ coïncident sur une partie génératrice de $\mathfrak{S}_n$: $\Phi = \iota(\alpha)$ et Φ est intérieur. $\square$

Grâce à ce lemme, il nous suffit de montrer que tout automorphisme de $\mathfrak{S}_n$ pour $n \neq 6$ envoie les transpositions sur les transpositions, ce qui constituera la seconde partie du développement.

(ii). Cet insolent $n = 6$, constante ridicule s'il en est, vous énerve ? Moi aussi, mais c'est la vie.
 (iii). On peut encore exclure le cas $n = 3$ car dans ce cas, τ_2 et τ_3 représentent toute la famille $(\tau_i)_i$ et il n'y a rien à montrer

Description des automorphismes de $\mathfrak{S}_n$

Soit τ une transposition et $\Phi \in \text{Aut}(\mathfrak{S}_n)$. Comme Φ préserve l'ordre des éléments de $\mathfrak{S}_n$, $\Phi(\tau)$ est d'ordre 2, et donc, lorsqu'on le décompose en un produit de cycles à support disjoints, c'est un produit de k transpositions ^(iv). Grâce au lemme, on aura prouvé que Φ est intérieur si on montre que $k = 1$. Remarquons tout d'abord que k est impair. En effet, Φ envoie les commutateurs de $\mathfrak{S}_n$ sur les commutateurs, donc envoie le groupe dérivé $D(\mathfrak{S}_n)$ dans lui-même. Puisqu'on manipule des ensembles finis, on a donc $\Phi(D(\mathfrak{S}_n)) = D(\mathfrak{S}_n)$. Mais pour $n \geq 3$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$, donc la signature de $\Phi(\tau)$ (qui est $(-1)^k$) est négative si $n \geq 3$ (et si $n \leq 2$, il va de soi que $k = 1$...). **Ainsi, cela permet de prouver d'emblée le théorème pour $n \leq 5$, et nous supposons dans toute la suite $n \geq 6$. On raisonne par contraposée, en supposant que $k \neq 1$.** Montrer le théorème revient donc à prouver que $n = 6$.

On va étudier les centralisateurs respectifs de τ et de $\Phi(\tau)$. Cela va nous donner des informations sur $\Phi(\tau)$, car Φ induit un isomorphisme $C(\tau) \cong C(\Phi(\tau))$ ^(v).

Etude du centralisateur de τ

Notons $\tau = (a \ b)$ et $F := \llbracket 1, n \rrbracket \setminus \{a, b\}$. Alors, pour $\sigma \in \mathfrak{S}_n$:

$$\sigma \in C(\tau) \iff \sigma \tau \sigma^{-1} = (\sigma(a) \ \sigma(b)) = (a \ b) \quad (11)$$

$$\iff \sigma(\{a, b\}) = \{a, b\} \quad (12)$$

$$\iff \sigma(F) = F \quad (13)$$

Ainsi, on a un morphisme surjectif bien défini :

$$\begin{aligned} r : C(\tau) &\rightarrow \mathfrak{S}(F) \cong \mathfrak{S}_{n-2} \\ \sigma &\mapsto \sigma|_F \end{aligned}$$

Et son noyau est composé des permutations qui se comportent comme l'identité sur F , c'est-à-dire $\text{Ker}(r) = \{Id, \tau\}$. Il s'agit d'un groupe d'ordre 2 ; à isomorphismes près, on a la suite exacte :

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \hookrightarrow C(\tau) \twoheadrightarrow \mathfrak{S}_{n-2} \longrightarrow 1 \quad (14)$$

Etude du centralisateur de $\Phi(\tau)$

Notons, pour $i \in \llbracket 1, k \rrbracket$, $\tau_i = (a_i \ b_i)$ les k -transpositions apparaissant dans la décomposition en produit de cycles de $\Phi(\tau)$. On considère N le sous-groupe de $\mathfrak{S}_n$ engendré par les (τ_i)

Lemme 3. N est un sous-groupe distingué de $C(\Phi(\tau))$, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$

Démonstration. Les τ_i sont à supports disjoints : ils commutent deux à deux et N est abélien. Comme ils sont tous d'ordre 2, tous les éléments de N sont d'ordre 1 ou 2, donc :

$$N \cong (\mathbb{Z}/2\mathbb{Z})^k \quad (15)$$

(iv). On utilise ici le fait que l'ordre d'une permutation est le ppcm de la longueur des cycles dans sa décomposition en produit de cycles à support disjoints

(v). Même si ça ne me paraissait pas clair au début, il suffit de l'écrire pour s'en convaincre.

De plus, comme les (τ_i) commutent et sont d'ordre 2, ils sont tous dans $C(\Phi(\tau))$, et $N < C(\Phi(\tau))$. Enfin, soit $\sigma \in C(\Phi(\tau))$. On a alors :

$$(a_1 \ b_1) \dots (a_k \ b_k) = \sigma [(a_1 \ b_1) \dots (a_k \ b_k)] \sigma^{-1} = (\sigma(a_1) \ \sigma(b_1)) \dots (\sigma(a_k) \ \sigma(b_k)) \quad (16)$$

Or le terme de droite est encore une écriture de $\Phi(\tau)$ en produit de cycles à supports disjoints. Par unicité à l'ordre près des termes, l'automorphisme $\iota(\sigma)$ réalise une permutation des (τ_i) . En particulier, $\iota(\sigma)$ envoie N sur lui-même, c'est-à-dire que $N \triangleleft C(\Phi(\tau))$. $\square$

Conclusion de l'étude

Ainsi, par l'isomorphisme $C(\tau) \cong C(\Phi(\tau))$, on obtient que $C(\tau)$ contient un sous-groupe distingué de cardinal 2^k , noté H . Comme r est un morphisme surjectif, $r(H)$ est encore distingué dans $\mathfrak{S}_{n-2}$, et $r(H)$ est de cardinal 2^l , avec $l = k$ si $H \cap \text{Ker}(r) = \{Id\}$ ou $l = k-1$ si $\text{Ker}(r) \subset H$. Comme on a supposé $k \neq 1$, cela impose $l > 1$. Or, si n était supérieur strict à 6, on a $n-2 \geq 5$, et donc on connaîtrait les sous-groupes distingués de $\mathfrak{S}_{n-2}$. Ainsi :

$$r(H) \in \{\{Id\}, \mathfrak{A}_{n-2}, \mathfrak{S}_{n-2}\} \quad (17)$$

Or, chacun de ces cas est exclu pour des raisons de cardinal. La seule valeur possible pour n est donc 6.

Références

- [1] Daniel PERRIN. *Cours d'algèbre*. Ellipses.