

I.F Automorphismes de $\mathfrak{S}_n$ (103) (104) (105) (108)

Les quatre premiers résultats sont à mettre dans le plans mais ne font pas partie du développement.

Lemme 7: Principe de conjugaison

$\forall \sigma = (a_1, \dots, a_p) \in \mathfrak{S}$, $\forall \tau \in \mathfrak{S}_n$, on a $\tau \sigma \tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$.

Démonstration. On pose $\tau' = \tau(a_1, \dots, a_p)\tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$. Alors $\tau'(\tau(a_i)) = \tau(a_{i+1})$ pour $i < p$ et $\tau'(\tau(a_p)) = \tau(a_1)$.

Si $a \notin \{\tau(a_i) \mid i \in \llbracket 1, p \rrbracket\}$ alors $\tau^{-1}(a) \notin \{a_i \mid i \in \llbracket 1, p \rrbracket\}$ car τ est une bijection.
 $\Rightarrow \sigma$ fixe $\tau^{-1}(a) \Rightarrow \tau'(a) = \tau(\tau^{-1}(a)) = a$. ■

Proposition 8

Si σ et σ' sont conjugués alors σ et σ' ont la même décomposition en produit de cycles à supports disjoints.

Démonstration. C'est une conséquence du lemme précédent. ■

Proposition 9

Si σ et σ' ont la même décomposition en produit de cycles à supports disjoints, alors σ et σ' sont conjugués.

Démonstration. Soit $\sigma = \sigma_1 \dots \sigma_n$ et $\sigma' = \sigma'_1 \dots \sigma'_n$ avec $\sigma_i = (a_{i1} \dots a_{ip_i})$ et $\sigma'_i = (a'_{i1} \dots a'_{ip_i})$.
 Si $X = E \setminus \text{supp}(\sigma) = E \setminus \bigcup_i \text{supp}(\sigma_i)$ et $X' = E \setminus \text{supp}(\sigma') = E \setminus \bigcup_i \text{supp}(\sigma'_i)$, alors soit $f : X \rightarrow X'$ bijective et $\tau : E \rightarrow E$ tel que $\tau(a_{ij}) = a'_{ij}$ et $\tau(a) = f(a)$ si $a \notin \{a_{ij}\}$.
 Alors τ est bien défini car les σ_i sont à supports disjoints $\Rightarrow$ les a_{ij} sont deux à deux distincts.
 Alors $\tau \sigma_i \tau^{-1} = \sigma'_i$ par le principe de conjugaison.
 $\Rightarrow \tau \sigma \tau^{-1} = \tau \sigma_1 \tau^{-1} \tau \sigma_2 \tau^{-1} \dots \tau \sigma_n \tau^{-1} = \sigma'_1 \dots \sigma'_n = \sigma'$. ■

Théorème 10: Simplicité de $\mathfrak{A}_n$

Pour $n = 3$ et $n \geq 5$ le groupe $\mathfrak{A}_n$ est simple.

Démonstration. Elle est à connaître avant de faire ce développement même si je ne la rédige pas ici. ■

Théorème 11: Groupe dérivé de $\mathfrak{S}_n$

Le sous-groupe dérivé de $\mathfrak{S}_n$ est

$$D(\mathfrak{S}_n) = \mathfrak{A}_n.$$

Démonstration. On commence par remarquer que tout commutateur est de signature 1. Ainsi $D(\mathfrak{S}_n) \subseteq \mathfrak{A}_n$.
 Montrons donc l'inclusion inverse. Il suffit de démontrer que $D(\mathfrak{S}_n)$ contient une partie génératrice de $\mathfrak{A}_n$, par exemple les 3-cycles.
 Si $\sigma \in \mathfrak{A}_n$ est un 3-cycle alors il est de la forme $\sigma = (a \ b \ c)$ puis $\sigma^2 = (a \ c \ b)$ est aussi un 3-cycle. Ainsi il existe $\tau \in \mathfrak{S}_n$ tel que $\sigma^2 = \tau \sigma \tau^{-1}$ par ce qui précède. On a ainsi $\sigma = \tau \sigma \tau^{-1} \sigma^{-1}$. Donc $\sigma \in D(\mathfrak{S}_n)$. ■

Le développement à proprement parlé commence ici. La partie présentée à l'oral est constituée de la proposition et du théorème qui suivent.

Proposition 12

Soit $\varphi \in \text{Aut}(\mathfrak{S}_n)$. Si φ envoie les transpositions sur les transpositions, alors $\varphi \in \text{Int}(\mathfrak{S}_n)$.

Démonstration. Soit φ un tel automorphisme. On sait que $\mathfrak{S}_n$ est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geq 2$. Puisque les τ_i ne commutent pas deux à deux, il en est de même pour les $\varphi(\tau_i)$. Ceci entraîne que les $\varphi(\tau_i)$ ne sont pas à supports deux à deux disjoints.

On note $\varphi(\tau_2) = (\alpha_1\ \alpha_2)$ et $\varphi(\tau_3) = (\alpha_1\ \alpha_3)$ (comme il ne s'agit que de notations, on peut supposer que c'est α_1 qui est commun au support des deux transpositions images). On veut montrer que α_1 est commun au support de toutes les transpositions images des τ_i . Par suite, pour tout $i \geq 4$ les supports de $\varphi(\tau_2), \varphi(\tau_3), \varphi(\tau_i)$ ne sont pas disjoints. Donc on a $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$ ou $\varphi(\tau_i) = (\alpha_2\ \alpha_3)$.

Supposons que $\varphi(\tau_i) = (\alpha_2\ \alpha_3)$, on a alors puisque φ est un morphisme de groupe et qu'il est bijectif :

$$\varphi(\tau_2\tau_3\tau_i) = \varphi(\tau_2)\varphi(\tau_3)\varphi(\tau_i) = (\alpha_1\ \alpha_2)(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_3) = (\alpha_1\ \alpha_3) = \varphi(\tau_3)$$

Mais

$$\tau_2\tau_3\tau_i = (1\ 2)(1\ 3)(1\ i) = (1\ i\ 3\ 2) \neq \tau_3.$$

Ceci contredit donc la bijectivité de φ et ainsi ce cas est exclu.

On a donc $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$ pour tout i . On sait en outre que les α_i sont deux à deux distincts car φ est bijective. On pose alors $\alpha \in \mathfrak{S}_n$ la bijection définie par $i \mapsto \alpha_i$ et on a :

$$\forall i \geq 2, \alpha\tau_i\alpha^{-1} = (\alpha(1)\ \alpha(i)) = \varphi(\tau_i)$$

par principe de conjugaison.

Au total φ est intérieur. ■

Théorème 13: Automorphismes intérieurs de $\mathfrak{S}_n$

Pour $n \neq 6$, on a $\text{Int}(\mathfrak{S}_n) = \text{Aut}(\mathfrak{S}_n)$.

Démonstration. 1. L'inclusion $\text{Int}(\mathfrak{S}_n) \subset \text{Aut}(\mathfrak{S}_n)$ est immédiate

2. Soit alors $\varphi \in \text{Aut}(\mathfrak{S}_n)$. Montrons qu'il est intérieur.

Comme $n \geq 2$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$ et $\varphi([a, b]) = [\varphi(a), \varphi(b)]$ car φ est un morphisme. Donc $\varphi(D(\mathfrak{S}_n)) \subset D(\mathfrak{S}_n)$ mais il y a en fait égalité par cardinalité.

Ainsi, l'image d'une transposition par φ est un produit d'un nombre impair de transpositions à supports disjoints (décomposition en produits de cycles à support disjoints : les cycles sont des transpositions pour des raisons d'ordre). Notons k ce nombre.

— Si $k = 1$ alors la proposition précédente conclut la preuve.

— Supposons donc $k \geq 3$ (donc $n \geq 6$).

3. Soit $\tau = (a\ b)$ une transposition. On note $c(\tau)$ son centralisateur, i.e. $c(\tau) = \{\sigma \in \mathfrak{S}_n \mid \sigma\tau\sigma^{-1} = \tau\}$.

Si $s \in c(\tau)$ alors $s\tau s^{-1} = \tau = (s(a)\ s(b)) = (a\ b)$. On note alors $F = \llbracket 1, n \rrbracket \setminus \{a, b\}$ et on a que F est stable par s pour tout $s \in c(\tau)$. On obtient alors un morphisme de groupe surjectif

$$\begin{array}{ccc} c(\tau) & \rightarrow & \mathfrak{S}_F \cong \mathfrak{S}_{n-2} \\ \sigma & \mapsto & \sigma|_F \end{array} \quad \text{de noyau } \{\text{id}, \tau\}.$$

D'où $\mathfrak{S}_F \cong \mathfrak{S}_{n-2} \cong c(\tau)/(\mathbb{Z}/2\mathbb{Z})$.

4. Si l'on note $\tau = \underset{\tau_1}{(a_1\ a_2)} \dots \underset{\tau_k}{(a_{2k-1}\ a_{2k})}$ comme un produit de k transpositions à supports disjoints, alors les τ_i commutent et donc $\tau_i \in c(\tau)$.

Soit N le sous-groupe engendré par ces transpositions : $N := \langle \tau_1, \dots, \tau_k \rangle$. C'est un sous-groupe de $c(\tau)$.

Son cardinal est $|N| = 2^k = \sum_{i=0}^k \binom{k}{i}$ car le coefficient binomial traduit le nombre de τ_i dans le produit (les termes pouvant être permutés car les supports sont disjoints).

Tous les éléments de N sont d'ordre 2 donc $N \cong (\mathbb{Z}/2\mathbb{Z})^k$.

De plus comme pour tout $s \in c(\tau)$, $s\tau s^{-1} = (s(a_1) \ s(a_2)) \dots (s(a_{2k-1}) \ s(a_{2k})) = \tau$, alors par unicité de la décomposition en cycles à supports disjoints, $\forall i, \exists 1 \leq j \leq k : s\tau_i s^{-1} = \tau_j$. Donc N est un sous-groupe distingué de $c(\tau)$.

5. Supposons que pour toute transposition τ , $\varphi(\tau) =: \tau'$ soit un produit d'un nombre impair de transpositions $k \geq 3$.

Comme φ est un automorphisme $c(\tau) \cong c(\tau')$ est un isomorphisme de groupe. En effet :

$$\begin{aligned} c(\tau') &= \{ \sigma \in \mathfrak{S}_n \ / \ \sigma \tau' \sigma^{-1} = \tau' \} \\ &= \{ \sigma \in \mathfrak{S}_n \ / \ \sigma \varphi(\tau) \sigma^{-1} = \varphi(\tau) \} \\ &= \{ \sigma \in \mathfrak{S}_n \ / \ \varphi(\varphi^{-1}(\sigma) \tau \varphi^{-1}(\sigma^{-1})) = \varphi(\tau) \} \\ &= \{ \varphi(\tilde{\sigma}) \in \mathfrak{S}_n \ / \ \varphi(\tilde{\sigma} \tau \tilde{\sigma}^{-1}) = \varphi(\tau) \} \\ &= \{ \varphi(\tilde{\sigma}) \in \mathfrak{S}_n \ / \ \tilde{\sigma} \tau \tilde{\sigma}^{-1} = \tau \} \\ &= \varphi(c(\tau)). \end{aligned}$$

D'où $c(\tau')$ contient un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.

Il s'en suit que $\mathfrak{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^l$ avec $l = k$ ou $l = k-1$; donc $l > 0$.

Or les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n, \{\text{id}\}$ et $\mathfrak{A}_n$ pour $n \geq 5$. Ce n'est donc possible que pour $n-2 = 4$, soit $n = 6$.

6. Au total, sauf éventuellement pour $n = 6$, l'image d'une transposition est une transposition. D'où par la proposition précédente φ est intérieure. ■

En fait on peut construire pour $n = 6$ des automorphismes de $\mathfrak{S}_n$ qui ne sont pas intérieurs. Philippe Caldero a d'ailleurs fait une vidéo avec une méthode pour construire un automorphisme extérieur disponible sur Youtube.