

* Automorphismes de S_n : d'après 101, 104, 105, 108, 103

[Perin] I.8

Pour $n \neq 6$, les automorphismes de S_n sont intérieurs (i.e. $\varphi = \sigma \circ \sigma^{-1}$)

lemme:

Soit $\varphi \in \text{Aut}(S_n)$. Si φ envoie les transpositions sur des transpositions, alors φ est intérieur.

preuve du lemme: On a $n \geq 3$.

Soit $\varphi \in \text{Aut}(S_n)$ envoyant les transpositions sur des transpositions.

● Pour $i \in \{2, \dots, n\}$, notons $\tau_i = (1 \ i)$. Pour rappel, les τ_i engendrent S_n .

Soient $i, j \geq 2$.

Par hypothèse, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ sont deux transpositions. $\varphi(\tau_i) = (a \ b)$ et $\varphi(\tau_j) = (c \ d)$.

Or, τ_i et τ_j ne commutent pas donc $\varphi(\tau_i)$ et $\varphi(\tau_j)$ non plus (car $\varphi \in \text{Aut}(S_n)$).

Ainsi, les supports de $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne sont pas disjoints, disons $a = d$ de sorte que $\varphi(\tau_i) = (a \ b)$ et $\varphi(\tau_j) = (a \ c)$.

Soit maintenant $k \geq 2$, $k \notin \{i, j\}$ (s'il existe).

De la même manière que ce qu'on vient de dire, $\varphi(\tau_k)$ est une

● transposition dont le support n'est pas disjoint de ceux de $\varphi(\tau_i)$ et $\varphi(\tau_j)$.

Ainsi, 2 cas sont possibles: $\varphi(\tau_k) = (a \ d)$ avec $d \notin \{b, c\}$ (car φ bijective) ou

$\varphi(\tau_k) = (b \ c)$.

* Montrons que le cas $\ell(z) = (b\ c)$ est impossible.

On aurait alors: $\tau \circ \sigma \circ \sigma^{-1} = (a\ i)(a\ j)(i\ k) = (k\ j\ i\ 1)$

$$\text{et } \ell(\tau \circ \sigma \circ \sigma^{-1}) = \ell(\tau) \circ \ell(\sigma) \circ \ell(\sigma^{-1}) = (a\ b)(a\ c)(b\ c) = (c\ a)$$

Or ces deux éléments sont d'ordres distincts, ce qui est absurde car $\ell \in \text{Aut}(\mathcal{S}_n)$

Ainsi, on a: $\ell(z) = (a\ d)$ avec $d \notin \{b, c\}$.

En fait, on a: $\forall i \geq 2, \ell(e_i) = (a\ a_i)$ à les $a_i \in \{2, \dots, n\}$ et sont $2 \leq i \leq n$ distincts.

Posons alors $\sigma \in \mathcal{S}_n$ défini par $\sigma(1) = a, \sigma(i) = a_i$ pour $i \geq 2$.

On a alors par construction: $\ell(e_i) = \sigma \tau \sigma^{-1} \quad \forall i \geq 2$.

Comme les τ_i engendrent $\mathcal{S}_n$, cette égalité reste vraie pour tout élément de $\mathcal{S}_n$.

Ainsi: $\ell = \sigma \circ \sigma^{-1}$

preuve du théorème:

Soit $\ell \in \text{Aut}(\mathcal{S}_n)$, notre but est donc de montrer que ℓ envoie les transpositions sur des transpositions.

* Commençons par traiter les cas $n \leq 5$:

Soit τ une transposition de $\mathcal{S}_n$

$\ell(\tau)$ reste un élément d'ordre 2 donc c'est un produit de k transpositions à supports disjoints. On a donc en particulier $2k = |\text{supp}(\ell(\tau))| \leq n \leq 5$, donc $k \leq 2$

Par ailleurs, $\ell \circ \ell$ est un morphisme de groupes de $\mathcal{S}_n$ dans $\{\pm 1\}$ et il est non trivial (car $\ell \circ \ell(\ell^{-1}(\tau)) = \tau = -1$). On a donc forcément (c'est classique):

$\ell \circ \ell = \text{id}$, i.e. ℓ préserve la signature.

Ainsi, k est forcément impair et donc $k=1$. $\ell(\tau)$ est une transposition.

* Supposons donc maintenant $n \geq 6$.

On cherche à caractériser algébriquement les transpositions, pour cela on va s'intéresser aux centralisateurs (commutateurs) $c(\tau)$ du élément $\tau \in \mathcal{S}_n$.

Soit τ une transposition de $\mathcal{S}_n$: $\tau = (a\ b)$

Soit $\sigma \in c(\tau)$, on a: $\sigma \tau \sigma^{-1} = (\sigma(a)\ \sigma(b)) = \tau = (a\ b)$.

Ainsi, σ laisse stable $\{a, b\}$ et donc $F := \{ \sigma \in \mathcal{S}_n \mid \sigma \text{ laisse stable } \{a, b\} \}$ également.

On dispose donc d'un morphisme surjectif $\rho: c(\tau) \rightarrow \mathcal{S}_{n-2}$
 $\sigma \mapsto \sigma|_F$

de noyau de p est exactement $\{1, \tau\} \simeq \mathbb{Z}/2\mathbb{Z}$ donc on dispose d'une suite exacte courte:

$$1 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow c(\tau) \xrightarrow{p} S_{n-2} \rightarrow 1$$

Étudions maintenant $c(\ell(\tau))$:

D'une part, comme $\ell \in \text{Aut}(\mathfrak{S}_n)$, on a: $c(\ell(\tau)) = \ell(c(\tau)) \simeq c(\tau)$

D'autre part, $\ell(\tau)$ est d'ordre 2 donc on peut écrire $\ell(\tau) = \tau_1 \dots \tau_k$ avec $k \geq 1$ et les τ_i des transpositions à supports disjoints.

On pose $N := \langle \tau_1, \dots, \tau_k \rangle$.

On a donc $N \subseteq c(\ell(\tau))$. (car les τ_i commutent entre-eux).

De plus, si $\sigma \in c(\ell(\tau))$, alors $\tau_1 \dots \tau_k = \sigma(\tau_1 \dots \tau_k)\sigma^{-1}$

$$= (\sigma\tau_1\sigma^{-1}) \dots (\sigma\tau_k\sigma^{-1})$$

Or, les $\sigma\tau_i\sigma^{-1}$ sont des transpositions à supports disjoints et donc, par l'unicité de la décomposition en produit de cycles à support disjoints, la conjugaison par σ permute les τ_i .

Ainsi:

$$N \trianglelefteq c(\ell(\tau)) \simeq c(\tau)$$

Or, $(\mathbb{Z}/2\mathbb{Z})^k \rightarrow N$ est un isomorphisme car les τ_i commutent entre-eux et donc:

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

d'où $\tilde{N}$ ce sous-groupe.

p étant surjective, on a: $p(\tilde{N}) \trianglelefteq S_{n-2}$

En particulier, si $n \geq 7$, alors $n-2 \geq 5$ et donc on a forcément:

$$p(\tilde{N}) = \{1\}, A_{n-2} \text{ ou } S_{n-2}$$

Or, par le premier théorème d'isomorphisme, on a: $p(\tilde{N}) \simeq \tilde{N}/\ker(p)|_{\tilde{N}}$

Or, $\tilde{N} \simeq (\mathbb{Z}/2\mathbb{Z})^k$ et $\ker(p)|_{\tilde{N}} = \{1\}$ ou $\mathbb{Z}/2\mathbb{Z}$ donc:

$$|p(\tilde{N})| = 2^l \quad \text{avec } l = k \text{ ou } k-1$$

Or, ni A_{n-2} ni S_{n-2} sont de cardinal une puissance de 2 et donc:

$$p(\tilde{N}) = \{1\}. \text{ Ainsi } l = k-1 \text{ et } k=1$$

En particulier: $\ell(\tau)$ est une transposition.