Automorphismes de $\mathfrak{S}_n$

Perrin

Théorème : Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.

Pour montrer cela, on va utiliser la proposition suivante :

Prop : Soit $\phi \in \mathrm{Aut}\,\mathfrak{S}_n$, si ϕ transforme les transpositions en transpositions alors ϕ est intérieur.

Dém : On sait que le groupe $\mathfrak{S}_n$ est engendré par les transpositions. On a même que $\mathfrak{S}_n$ est engendré par les transpositions de la forme $\tau_i = (1, i)$ $i \geq 2$.
(En effet $(ij) = (1j)(1i)(1j)$)

Pour $n = 1, 2$ ok. On suppose $n \geq 3$.

Par hypothèse, pour tout $i \geq 2$ $\phi(\tau_i)$ est une transposition.

* Si $\phi(\tau_2)$ et $\phi(\tau_3)$ étaient à supports disjoints, elles commuteraient.
  Or $(12)(13) = (132) \neq (123) = (13)(12)$
  d'où $\phi((12))\phi((13)) = \phi((132)) \neq \phi((123)) = \phi((13))\phi((12))$ Absurde.
  Donc $\phi(\tau_2)$ et $\phi(\tau_3)$ ne sont pas à supports disjoints. Comme ϕ est bijective, $\phi(\tau_2) \neq \phi(\tau_3)$ donc leurs supports ont exactement un elt en commun : on le note a_1. $\phi(\tau_2) = (a_1, a_2)$, $\phi(\tau_3) = (a_1, a_3)$ avec $a_2 \neq a_3$.
  Or $\phi^{-1}((a_2\, a_3)) = \phi^{-1}((a_1 a_2)(a_1 a_3)(a_1 a_2)) = (12)(13)(12) = (2, 3)$

* Soit $i \in [\![4, n]\!]$, $\phi(\tau_2)$ et $\phi(\tau_i)$ ne commutent pas pour la même raison qu'avant donc ne sont pas à supports disjoints. De même pour $\phi(\tau_3)$ et $\phi(\tau_i)$.
  Si a_1 n'est pas dans le support de $\phi(\tau_i)$ alors a_2 et a_3 y sont et donc
  $\phi(\tau_i) = (a_2\, a_3)$ d'où $(1\, i) = \phi^{-1}(\phi(\tau_i)) = (2\, 3)$ ce qui est absurde.
  Donc a_1 est dans le support de $\phi(\tau_i)$ et il existe donc a_i tq
  $\phi(\tau_i) = (a_1\, a_i)$.

* Posons $s : i \mapsto a_i$. Si $s(i) = s(j)$ alors $\phi(\tau_i) = \phi(\tau_j)$
  d'où $\tau_i = \tau_j$ car ϕ est un automorphisme et donc $i = j$. D'où s injective.
  D'où s est bijective car définie sur ens de m̂ card. $s \in \mathfrak{S}_n$.

* Soit $i \in [\![1, n]\!]$, on pose $\gamma : \sigma \mapsto s\sigma s^{-1}$
  $\gamma(\tau_i) = s\tau_i s^{-1} = (a_1\, a_i) = \phi(\tau_i)$ pour $i \in [\![2, n]\!]$.
  $s\tau_i s^{-1}(a_1) = s\,\tau_i(1) = s(i) = a_i$ et de m̂ $s\tau_i s^{-1}(a_i) = a_1$
  et $s\tau_i s^{-1}(a_j) = a_j$ $j \neq 1, i$.

Donc ϕ et γ coïncident sur $\{\tau_i, i \in [\![2, n]\!]\}$ qui engendrent $\mathfrak{S}_n$
Donc $\phi = \gamma$ i.e. ϕ est intérieur.

Mq maintenant qu'un automorphisme de $\mathfrak{S}_n$ envoie les transposit° sur les transpositions

Dém: Soit $\Phi \in Aut\, \mathfrak{S}_n$. Si τ est une transposition,

Supposons que $\Phi \notin Int\, \mathfrak{S}_n$

$\times$ $\Phi(\tau)^2 = \Phi(\tau^2) = e$ or $\Phi(\tau) \neq e$ car automorphisme donc $\Phi(\tau)$ est d'ordre 2.

Or l'ordre d'un élément est le ppcm des longueurs des cycles apparaissant dans sa décomposition en cycles disjoints. donc $\Phi(\tau)$ est un produit de transposition à supports disjoints.

$\times$ Notons $C(\tau) = \{\sigma \in \mathfrak{S}_n, \sigma\tau\sigma^{-1} = \tau\} = \{\sigma \in \mathfrak{S}_n, \sigma\tau = \tau\sigma\}$ le centralisateur de τ.
Alors on a $\Phi(C(\tau)) = C(\Phi(\tau))$

$\to$ Soit $\sigma \in C(\tau)$, on a $\sigma\tau = \tau\sigma$ ~~et il existe~~ $\cancel{\sigma_0, \tau_0 \in \mathfrak{S}_n \text{ tq } \sigma = \Phi^{-1}(\sigma_0), \tau = \Phi^{-1}(\tau_0)}$ ~~car Φ bijectif~~. donc $\Phi(\sigma) \in C(\Phi(\tau))$

~~$\sigma\tau = \tau\sigma$ d'où $\Phi^{-1}(\sigma_0\tau_0) = \Phi^{-1}(\tau_0\sigma_0)$ d'où $\sigma_0\tau_0 = \tau_0\sigma_0$ car Φ bijectif.~~

~~d'où $\Phi(\sigma) = \sigma_0 \in C(\tau_0) = C(\Phi(\tau))$ d'où $\subset$.~~

En fait, un automorphisme envoie une classe de conj sur une classe de conj

$\to$ Soit $\sigma \in C(\Phi(\tau))$ on a $\sigma\Phi(\tau) = \Phi(\tau)\sigma$. $\exists \sigma_0 \in \mathfrak{S}_n$ tq $\sigma = \Phi(\sigma_0)$.

$\Phi(\sigma_0)\Phi(\tau) = \Phi(\tau)\Phi(\sigma_0)$ d'où $\sigma_0\tau = \tau\sigma_0$ d'où $\sigma_0 \in C(\tau)$ d'où $\sigma \in \Phi(C(\tau))$

donc $\Phi : C(\tau) \to C(\Phi(\tau))$ est une bijection (on sait déjà qu'il est inj)

$\times$ d'où $|C(\tau)| = |\Phi(C(\tau))| = |C(\Phi(\tau))|$ car Φ automorphisme.

$n \geq 2$
($n = 1$ évident)

Or $|C(\tau)| = \cancel{(n-2)!\, 1^{n-2} \times 1! \times 2!} = 2(n-2)!$ car

$\tau = (a,b)$

$\{\sigma \in \mathfrak{S}_n, \sigma\tau = \tau\sigma\} = \{\sigma \in \mathfrak{S}_n, \sigma\tau\sigma^{-1} = \tau\} = \{\sigma \in \mathfrak{S}_n, (\sigma(a), \sigma(b)) = (a,b)\}$

$\hookrightarrow$ définir σ sur les $n-2$ éléments comme on veut $\rightsquigarrow (n-2)!$ façons
et ensuite $\sigma(a) \in \{a, b\}$ $\rightsquigarrow$ 2 façons
$\to 2(n-2)!$

et $|C(\Phi(\tau))| = 2^k\, k!\, (n-2k)!$ $\Phi(\tau)$ produit de k transpositions $(a_1\, b_1) \cdots (a_k\, b_k)$ disjointes.

$\{\sigma \in \mathfrak{S}_n, \sigma\Phi(\tau)\sigma^{-1} = \Phi(\tau)\} = \{\sigma \in \mathfrak{S}_n, (\sigma(a_i), \sigma(b_i)) = (a_j, b_j) \quad i \in [\![1,k]\!], j \in [\![1,k]\!]\}$.

$\hookrightarrow$ définir σ sur les $n-2k$ autres éléments $\rightsquigarrow (n-2k)!$ façons.

$\sigma(a_1), \sigma(b_1)$ envoyé sur l'un des couples $\{(a_j, b_j)\}$: choix du couple : k.
puis $\sigma(a_1) \in \{a_j, b_j\} \to 2$.
puis $\sigma(a_2), \sigma(b_2)$ n'a plus que $k-1$ choix de couple puis 2 choix à l'intérieur.
etc $\rightsquigarrow 2^k k!$.

$n = 2 \Rightarrow k = 1$

Donc $2(n-2)! = 2^k\, k!\, (n-2k)! \iff (n-2)! = 2^{k-1}\, k!\, (n-2k)!$

$$\iff \frac{(n-2)!}{2^{k-1}\, k!\, (n-2k)!} = 1 \iff \frac{\binom{n-2}{2k-2}(2k-2)!\,\cancel{(n-2k)!}}{2^{k-1}\, k!\, \cancel{(n-2k)!}} = 1$$

$$\iff \frac{\binom{n-2}{2k-2} \times (2k-2)(2k-4) \cdots \times 2 \times (2k-3) \times (2k-5) \cdots \times 3 \times 1}{2^{k-1}\, k!} = 1.$$

$$\iff \binom{n-2}{2k-2} \times \frac{\cancel{2^{k-1}}\,(k-1)! \times (2k-3) \cdots 3 \times 1}{\cancel{2^{k-1}}\, k!} = 1$$

$$\iff \underbrace{\binom{n-2}{2k-2}}_{\in \mathbb{N}} \underbrace{(2k-3) \cdots 3 \times 1}_{\in \mathbb{N}} = k$$

Or $2k-3 \geq k \iff k \geq 3$ (dans ce cas là égalité impossible)

Donc $k \leq 3$.

× si $k=1$. Egalité vraie ← impossible car $\phi \notin Int\, \mathfrak{S}_n$ par prop.

× si $k=2$ $\binom{n-2}{2}(1) = 2 \iff \frac{(n-2)!}{(n-4)!\,2} = 2 \iff (n-2)(n-3)=4$

$$\iff n^2 - 5n + 2 = 0.$$

Or $\Delta = 25 - 4\times 2 = 17$ $n = \frac{5 \pm \sqrt{17}}{2} \notin \mathbb{N}$ d'où pas de solution entière.

× si $k=3$

$\binom{n-2}{4} 3 = 3$ d'où $\frac{(n-2)!}{(n-6)!\,4!} = 1$ d'où $(n-2)(n-3)(n-4)(n-5) = 4!$

Or pour $n \geq 7$ $(n-2)\dots(n-5) \geq 5\times 4\times 3\times 2 = 5! > 4!$

d'où $n < 7$

$n=3$: non $n=4$: non $n=5$ non $n=6$ oui

donc $n=6$. On a donc montré la contraposée du théorème

donc sauf pour peut être $n=6$, on a $k=1$ et donc ϕ envoie transposition sur transposition d'où par la proposition qu'on a montré au début, ϕ est intérieur. $\square$

Bonus:

× Cas $n=1$, $n=2$: $\mathfrak{S}_2$ est un groupe d'ordre 2, Tout automorphisme de $\mathfrak{S}_2$ envoie Id sur Id et est une bijection d'où $Aut(\mathfrak{S}_2)$ est le gpe trivial.

Donc pour $n=1, 2$, $Aut(\mathfrak{S}_n) = \{id\}$.

× $n \geq 3$, $h: \sigma \in \mathfrak{S}_n \longmapsto h_\sigma \{g \mapsto \sigma g \sigma^{-1}\} \in Int(\mathfrak{S}_n)$

h est surjective par définition de $Int(\mathfrak{S}_n)$.

Soit $\sigma \in \ker h$, $h_\sigma = id$.

Soit $i \in [\![1, n]\!]$, on note $\gamma_i = (1, 2, \dots, i-1, i+1, \dots, n)$. Supp $\gamma_i = [\![1,n]\!] \setminus \{i\}$.

$\gamma_i = h_\sigma(\gamma_i) = (\sigma(1)\ \sigma(2), \dots, \sigma(i-1), \sigma(i+1), \dots, \sigma(n))$.

d'où $[\![1,n]\!] \setminus \{i\} = \text{supp}\, \gamma_i = \text{supp}\, h_\sigma(\gamma_i) = [\![1,n]\!] \setminus \{\sigma(i)\}$ d'où $\sigma(i) = i$

d'où $\sigma = id$.

D'où $Int(\mathfrak{S}_n) \simeq \mathfrak{S}_n$ $n \geq 3$. ~~$n \neq$~~ et donc pour $n \neq 6$, $n \geq 3$ $Aut(\mathfrak{S}_n) \simeq \mathfrak{S}_n$

× Cas $n=6$: Il existe un automorphisme non intérieur. chercher idée de la démo.