Automorphismes de S_n

↳ Ref : Perrin, p 30-33

Lemme : $(n \geq 3)$ Soit $\varphi \in Aut(S_n)$, si φ transforme les transpositions en transpositions, alors φ est un automorphisme intérieur.

Théorème : Pour $n \neq 6$, tout automorphisme de S_n est intérieur ie
$$Aut(S_n) = Int(S_n).$$

Proposition : Pour $n = 6$, $Aut(S_6) \neq Int(S_6)$.

Idée de la preuve : Les automorphismes de S_n conservent a priori seulement les propriétés algébriques des permutations (ordre des éléments, propriétés de commutations etc), mais pas forcément les propriétés géométriques, liées à l'action de S_n sur $[\![1,n]\!]$ (nombre de points fixes, cycles etc). Or le lemme nous dit que l'on va devoir travailler avec les propriétés géométriques, il va donc falloir traduire ces propriétés géométriques en propriétés algébriques (et en particulier étudier les transpositions du point de vue algébrique).

Preuve du lemme : On sait que S_n est engendré par la famille de transpositions $\{\tau_i = (1\ i),\ i \in [\![2,n]\!]\}$. Pour tout $i \in [\![2,n]\!]$, par supposition $\varphi(\tau_i)$ est une transposition. De plus, si $i \neq j$, τ_i et τ_j ne commutent pas, donc $\varphi(\tau_i)$ et $\varphi(\tau_j)$ non plus, donc ces transpositions ont des supports non disjoints.
Si l'on pose $\varphi(\tau_2) = (\alpha_1\ \alpha_2)$, on peut donc supposer $\varphi(\tau_3) = (\alpha_1\ \alpha_3)$ où $\alpha_3 \neq \alpha_2$ (nécessairement un seul élément en commun car φ automorphisme donc $\varphi(\tau_2) \neq \varphi(\tau_3)$)
Si $n=3$, ok, sinon par suite pour $i \geq 4$, $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. En effet s'il existe $i \geq 4$ tel que $\alpha_1 \notin Supp(\varphi(\tau_i))$, alors comme $Supp(\varphi(\tau_i)) \cap Supp(\varphi(\tau_j)) \neq \emptyset$ pour $j = 2,3$ alors $\varphi(\tau_i) = (\alpha_2\ \alpha_3)$. Or $(\alpha_1\ \alpha_2)(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_3) = (\alpha_1\ \alpha_3)$ donc on composant par φ^{-1}, on aurait $(1\ 2)(1\ 3)(1\ i) = (1\ 3)$ ↯ (regarder l'image de i par exc).
Donc $\forall i \geq 2$, $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$ où les α_i sont tous distincts puisque $\varphi \in Aut(S_n)$, donc $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\}$. On définit alors $\alpha : [\![1,n]\!] \longrightarrow [\![1,n]\!]$, $i \longmapsto \alpha_i$
et on a alors construit une permutation $\alpha \in S_n$ telle que $\forall i \geq 2$, $\alpha \tau_i \alpha^{-1} = (\alpha(1)\ \alpha(i)) = (\alpha_1\ \alpha_i) = \varphi(\tau_i)$
Ainsi φ coïncide avec l'automorphisme intérieur $Int\,\alpha$ associé à α sur les τ_i qui engendrent S_n, et donc $\varphi = Int\,\alpha$.

Preuve du théorème : Idée générale : on va maintenant étudier les transpositions d'un point de vue algébrique. On sait déjà qu'elles sont d'ordre 2, mais dès que $n \geq 4$, cela ne suffit plus à les caractériser. Nous allons donc étudier les centralisateurs des éléments d'ordre 2. Dans la suite, $n \geq 3$ (le thm est clair pour $n = 1,2$)

1) Etude du centralisateur d'une transposition : On va dans la suite noter pour $\tau \in S_n$, $C(\tau) = \{\sigma \in S_n \mid \sigma \tau \sigma^{-1} = \tau\}$ le centralisateur d'une permutat° τ.

Soit $\tau = (a\ b)$ une transposition de S_n, et soit $\sigma \in S_n$. On note $E = [\![1,n]\!]$ et $F = [\![1,n]\!] \setminus \{a,b\}$. Alors on a les équivalences suivantes :

$\sigma \in C(\tau) \iff \sigma\tau\sigma^{-1} = \tau \iff (\sigma(a)\ \sigma(b)) = (a\ b) \iff \sigma(\{a,b\}) = \{a,b\}$
$\iff \sigma(F) = F$.

Ainsi on a le morphisme surjectif suivant : $\pi : C(\tau) \longrightarrow \mathrm{Bij}(F) \simeq S_{n-2}$
$\sigma \longmapsto \sigma_{|F}$

De plus, $\mathrm{Ker}(\pi) = \{id, \tau\} \simeq \mathbb{Z}/2\mathbb{Z}$.

2) Etude du centralisateur d'un produit de transpositions à supports disjoints : Soit $\tau = \underbrace{(a_1\ a_2)}_{\tau_1} \circ \cdots \circ \underbrace{(a_{2k-1}\ a_{2k})}_{\tau_k}$ un produit de k transpositions à supports disjoints.

Les τ_i sont à supports disjoints, donc commutent entre elles, et donc avec σ, ainsi : $\forall i \in [\![1,k]\!]$, $\tau_i \in C(\tau)$.

Soit $N = \langle \{\tau_i,\ 1 \le i \le k\} \rangle = \left\{ \prod_{i=1}^{k} \tau_i^{\alpha_i},\ \alpha_i \in \{0,1\} \right\}$ le sous groupe engendré par les τ_i.

Alors $|N| = 2^k$ et est formé d'éléments d'ordre 2, et donc $N \simeq (\mathbb{Z}/2\mathbb{Z})^k$. De plus N est distingué dans $C(\tau)$, en effet si $\sigma \in C(\tau)$, alors $\sigma\tau\sigma^{-1} = \underbrace{(\sigma(a_1)\ \sigma(a_2))}_{\sigma\tau_1\sigma^{-1}} \circ \cdots \circ \underbrace{(\sigma(a_{2k-1})\ \sigma(a_{2k}))}_{\sigma\tau_k\sigma^{-1}} = \tau$

Donc par unicité de la décomposition en cycles à supports disjoints (à l'ordre près), la conjugaison par σ permute les τ_i ie $\forall i \in [\![1,k]\!]$, $\exists j \in [\![1,k]\!]$, $\sigma\tau_i\sigma^{-1} = \tau_j$.
Et donc $N \lhd C(\tau)$.

3) Regroupons les morceaux, en utilisant le lemme et la connaissance des sous groupes distingués de S_n.

Soit $\varphi \in \mathrm{Aut}(S_n)$, et supposons que $\varphi \notin \mathrm{Int}(S_n)$. D'après le lemme, il existe $\tau \in S_n$ une transposition telle que $\varphi(\tau) = \tau'$ ne soit pas une transposition. En revanche, puisque φ conserve l'ordre, c'est un élément d'ordre 2, et donc un produit de k transpositions à supports disjoints, avec $k > 1$ (puisque ce n'est pas une transposition). De plus pour $n \ge 3$, $D(S_n) = A_n$, et comme φ transforme un commutateur en commutateur, il fixe A_n, donc nécessairement k est impair. Ainsi k est impair et > 1, donc $k \ge 3$ et donc $n \ge 6$.

Les centralisateurs $C(\tau)$ et $C(\tau') = C(\varphi(\tau))$ sont isomorphes (via φ).
D'après le point 2), $C(\tau')$ admet un sous groupe distingué N iso à $(\mathbb{Z}/2\mathbb{Z})^k$, donc $C(\tau)$ admet un sous groupe distingué H $(= \varphi^{-1}(N))$, lui aussi iso à $(\mathbb{Z}/2\mathbb{Z})^k$.
Le morphisme π du point 1) étant surjectif, $\pi(H) \lhd \pi(C(\tau)) = \mathrm{Bij}(F)$.
Donc S_{n-2} admet un sous groupe distingué H' (iso à $\pi(H)$) tel que
* $H' \simeq (\mathbb{Z}/2\mathbb{Z})^{k-1}$ si $\tau \in H$ (par 1er thm d'iso appliqué à $\pi_{|H} : H \to \pi(H)$ de noyau $\{Id, \tau\}$
on obtient $\pi(H) \simeq H/\{Id, \tau\} \simeq (\mathbb{Z}/2\mathbb{Z})^k/(\mathbb{Z}/2\mathbb{Z})$)

* $H' \simeq (\mathbb{Z}/2\mathbb{Z})^{k \geq 3}$ sinon (avec le même argument)

Or on connait les sous groupes distingués de S_{n-2} en fonction de $n \geq 6$:

• Si $n-2 \neq 4$ ($n-2 \geq 5$ donc), les sous groupes distingués de S_{n-2} sont

	$\{Id\}$	A_n	S_n
cardinal	1	$\frac{(n-2)!}{2}$	$(n-2)!$
	×	$\neq 2^{\alpha}$ car $n-2 \geq 3$	

Donc si $n-2 \neq 4$, S_{n-2} ne peut avoir de sous groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{\alpha}$ pour $\alpha \geq 2$.

• Si $n-2=4$, ie $n=6$, les sous groupes de S_{n-2} sont

$\{Id\}$	V_4	A_4	S_4
1	4	12	24
×	✓	×	×

$\rightarrow V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 = (\mathbb{Z}/2\mathbb{Z})^{3-1}$, et on pourrait avoir $H' \simeq V_4$

Ainsi, sauf éventuellement pour $n=6$, on parvient à une contradiction. Donc pour $n \neq 6$, $Aut(S_n) = Int(S_n)$.

(Idée de) preuve de la proposition (Bonus) : Pour $n \geq 5$, montrons que s'il existe sous groupe d'indice n H tel que H n'est pas le stabilisateur d'un $i \in [\![1,n]\!]$ alors il existe un automorphisme non intérieur. En effet, soit H un tel sous groupe, alors S_n agit par translat° à gauche sur $E = S_n/H$ de cardinal n, on a donc un morphisme de groupes $\varphi : S_n \longrightarrow Bij(S_n/H) \simeq S_n$ et $Ker\,\varphi = \bigcap_{G \in S_n} GHG^{-1}$ (intersect° des $Stab(GH) = GHG^{-1}$) avec $Ker\,\varphi \subset H$ et $Ker\,\varphi$ distingué dans S_n. Donc, $Ker\,\varphi = \{Id\}$ par cardinalité (sous gp distingués : $\{Id\}$, A_n, S_n et $|Ker\,\varphi| < (n-1)! < \frac{n!}{2}$.

Donc φ est injective donc c'est un isomorphisme (grâce aux cardinaux), et $\varphi(H)$ est le stabilisateur de la classe $\bar{1} = H$.

On choisit une bijection de f de S_n/H dans $X = [\![1,n]\!]$ tel que $f(\bar{1}) = 1$, on en déduit un isomorphisme $\psi : Bij(S_n/H) \longrightarrow S_n$, $G \longmapsto fGf^{-1}$ qui envoie $\varphi(H)$ sur le stabilisateur de 1.

Ainsi $\psi \circ \varphi$ est un automorphisme de S_n qui vérifie $\psi \circ \varphi(H) = Stab(1)$, mais H et $Stab(1)$ ne sont pas conjugués (car H n'est pas un $Stab(i)$), donc $\psi \circ \varphi$ n'est pas intérieur.

Il faut donc trouver pour $n=6$, un tel H qui n'est pas un $Stab(i)$, par exemple en trouvant un H qui gère transitivement sur $[\![1,6]\!]$ (et là ça devient un peu perché)

Deux méthodes :

* Le groupe S_5 contient 6 5-Sylow : si k désigne le nbr de 5 Sylow alors $k \equiv 1 [5]$ et $k | 24$ donc $k=1$ ou 6. Mais $k=1$ impossible sinon P l'unique 5 Sylow serait distingué donc $k=6$. Si on note X l'ensemble des 5-Sylow de S_5, alors S_5 agit transitivement et fidèlement. On a donc un morphisme injectif $\varphi : S_5 \longrightarrow Bij(X) \simeq S_6$ et comme S_5 agit transitivement, $\varphi(S_5)$ convient

* On remarque que $PGL_2(\mathbb{F}_5)$ agit transitivement et fidèlement sur la droite

projective à 6 éléments $\mathbb{P}(\mathbb{F}_5^2)=\mathbb{P}^1(\mathbb{F}_5)$ cela identifie $PGL_2(\mathbb{F}_5)$ à un sous groupe de S_6 qui agit transitivement sur $[\![1,6]\!]$.
Bon idée à retenir : on regarde les 5-Sylow de S_5 ou l'action de $PGL_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$.

<u>Remarques</u> : * En fait $\mathrm{Int}(S_6)$ est un sous groupe d'indice 2 de $\mathrm{Aut}(S_6)$, en effet au vu de ce qui précède, si φ et ψ sont deux automorphismes "extérieurs" alors ils transforment tous deux la classe de conjugaison des transpositions en celle des produits de 3 transpositions à supports disjoints (et en fait échangent ces deux classes qui ont même cardinal) Donc $\psi\circ\varphi$ conserve les transpositions et donc est intérieur.

* Le théorème permet de déduire que si $n\geq 3$ et $n\neq 6$, alors $\mathrm{Aut}(S_n)\simeq S_n$, puisque si $n\geq 3$, $Z(S_n)=\{Id\}$, donc $\mathrm{Int}(S_n)\simeq S_n$, et puisque $n\neq 6$, $\mathrm{Int}(S_n)=\mathrm{Aut}(S_n)$ (et si $n=1,2$, $\mathrm{Aut}(S_n)=\{Id\}$

* On prend pour acquis la liste des sous groupes de S_n, il faut savoir le montrer : pour $n>5$, corollaire de la simplicité de A_n pour $n>5$ (cf dev correspondant), pour $n=4$, on regarde les classes de conjugaison pour déterminer les ss-grp distingués : dans S_4 il y a : $1\times\{Id\}$, 3 doubles transpo, 8 3-cycles, 6 4-cycles et 6 transpos ; alors soit on contient une transpo et on est S_4 ($1+3+6+8+6 \mid 24$ ok), soit on ne contient pas de transpo, mais on contient un 3 cycle, alors on est A_4 ($1+3+8 \mid 24$ ok), soit on ne contient ni transpo ni 3 cycle mais on contient une double transpo, alors on est V_4 ($1+3\mid 24$ ok), soit on contient rien d'autre que Id, alors bah on est $\{Id\}$ ($1\mid 24$ ok), les autres combinaisons ne fonctionnent pas au niveau des cardinaux (on pourrait imaginer avoir $\{Id\}+\{4 \text{ cycles}\}$ par ex, mais $1+6\nmid 24$ donc perdu !)

* Il existe une autre preuve, qui consiste à dénombrer le stabilisateur d'un élément dans une classe de conjugaison donnée : si σ est le produit de k_1 cycles d'ordre 1, k_2 d'ordre 2, … k_n d'ordre n ($k_1+2k_2+\dots+n k_n=n$) alors $|C(\sigma)|=\prod_{i=1}^{n} k_i!\, i^{k_i}$, en effet $\tau\in C(\sigma)$ ssi τ permute les cycles de m longueur ($k_i!$ possibilités) et τ réalise une permutat° cyclique de chaque cycle (chaque cycle de longueur i peut s'écrire de i manières différentes) (i^{k_i}).
En ensuite, on dit $|C(\tau)|=|C(\varphi(\tau))|$ donc si τ transpo et $\varphi(\tau)$ produit de k transpo, on obtient $(n-2)!\times 2=2^k k!(n-2k)!$. On bidouille et on voit que cela implique $k=1$, sauf si $n=6$ et $k=3$ (cf Perrin).

* Utilité de tout ça ? Aider à déterminer les act° de groupes sur S_n et par suite les produits semi directs impliquant S_n (super … !)
(*) la formule magique : la classe de conjugaison d'une permutat° produit de k_1 1-cycles, k_2 2-cycles … k_m m-cycles est de cardinal $\frac{n!}{[illegible]}$