Automorphismes intérieurs de S_n

Léo Gayral

2017-2018

ref : Perrin – Cours d'algèbre – p.31

Définition 1 (Automorphime intérieur)**.** Soit $\phi \in \mathrm{Aut}\,(G)$ un isomorphisme. On dit que l'automorphisme ϕ est intérieur s'il correspond à une action par conjugaison dans G, autrement dit si $\exists h \in G, \forall g \in G, \phi(g) = hgh^{-1}$.

Lemme 1. Soit $\phi \in \mathrm{Aut}\,(S_n)$. Si ϕ envoie les transpositions sur des transpositions, alors ϕ est intérieur.

Démonstration.
On sait que la famille $\{\tau_i := (1\ i), 2 \leq i \leq n\}$ engendre le groupe S_n. Il suffit donc de montrer que les images de toutes ces transpositions peuvent être obtenues par une même action par conjugaison pour conclure que ϕ est intérieur.

$\phi(\tau_2)$ et $\phi(\tau_3)$ sont par hypothèse des permutations. De plus, $\tau_2\tau_3$ est un 3-cycle, donc son image $\phi(\tau_2\tau_3) \neq \mathrm{id}$ est un élément d'ordre 3. Cela signifie que les deux permutations agissent sur un entier α_1 en commun. On pose alors $\alpha_2 \neq \alpha_3$ tels que $\phi(\tau_2) = (\alpha_1\ \alpha_2)$ et $\phi(\tau_3) = (\alpha_1\ \alpha_3)$. On peut suivre un raisonnement similaire pour $4 \leq i \leq n$. Si on compare τ_i et τ_2, on en déduit que leurs images ont élément en commun ; il en va de même pour τ_i et τ_3.

Si $\phi(\tau_i)$ n'agit pas sur α_1 alors $\phi(\tau_i) = (\alpha_2\ \alpha_3)$: ceci implique $\phi(\tau_2\tau_3\tau_i) = (\alpha_1\ \alpha_2)(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_3) = (\alpha_1\ \alpha_3) = \phi(\tau_3)$, d'où $\tau_i = \tau_3\tau_2\tau_3 = (2\ 3)$ par injection, ce qui est impossible.

Pour tout $2 \leq i \leq n$ on a donc un entier α_i tel que $\phi(\tau_i) = (\alpha_1\ \alpha_i)$. Comme ϕ est un automorphisme, les α_i sont deux à deux tous distincts ; en posant $\alpha : i \mapsto \alpha_i$ on définit bien un élément $\alpha \in S_n$.

On a alors $\phi(\tau_i) = \alpha\tau_i\alpha^{-1}$, donc l'automorphisme ϕ est intérieur. □

Remarque 1. L'ensemble des transpositions est une des classes de conjugaison de S_n. Plus généralement, une classe de conjugaison de S_n est entièrement décrite par la famille $(r_i)_{1\leq i\leq n}$, où r_i est le nombre de i-cycles d'un élément de la classe.

Or tout automorphisme $\phi \in \mathrm{Aut}\,(G)$ préserve les classes de conjugaison. On va donc chercher à caractériser les classes de conjugaison de S_n par leur cardinal.

Lemme 2. Soit $\mathcal{C}$ la classe de conjugaison décrite par la famille $(r_i)_{1\leq i\leq n}$. On montre la relation :

$$\#\mathcal{C} = \frac{n!}{\prod\limits_{i=1}^{n} r_i! \times i^{r_i}}$$

sur le cardinal de $\mathcal{C}$. En particulier, on retrouve bien le fait qu'il y a $\frac{n(n-1)}{2}$ transpositions dans S_n ($r_1 = n-2$, $r_2 = 1$ et $r_i = 0$ pour $i \geq 3$).

Démonstration.
L'action de groupe $S_n \curvearrowright \mathcal{C}$ par conjugaison est transitive. Comme il n'y a qu'une seule orbite, la formule des classes donne donc $\#\mathcal{C} = \frac{\#S_n}{\#\mathrm{Stab}(\alpha)}$ avec $\alpha \in \mathcal{C}$ quelconque.

On veut montrer que $\#\mathrm{Stab}(\alpha) := \#\{\sigma \in S_n, \sigma\alpha\sigma^{-1} = \alpha\} = \prod\limits_{i=1}^{n} r_i! \times i^{r_i}$. Or un i-cycle peut s'écrire, à conjugaison près, de i façons différentes, en conjuguant par une puissance dudit-cycle pour changer son « premier » élément. On peut de plus permuter sans contraintes les r_i i-cycles de α : pour le « premier » i-cycle de α on a r_i i-cycles possibles à l'arrivée, puis i choix possibles une fois le cycle choisi. Par récurrence, on peut donc choisir $(r_i \times i) \times ((r_i - 1) \times i) \times \cdots = r_i! \times i^{r_i}$ façons de stabiliser les i-cycles de α. En multipliant ces termes, en stabilisant tous les cycles disjoints de α, on obtient le résultat voulu. □

Théorème 1. Si $n \neq 6$, tout automorphisme de S_n est intérieur.

Démonstration.
Soit $\phi \in \mathrm{Aut}(S_n)$. L'image par ϕ d'une transposition reste un élément d'ordre 2. On veut donc montrer que si cet élément n'est pas une transposition mais un *produit* de k transpositions (à supports disjoints), alors le cardinal de $\mathcal{C}$ sa classe de conjugaison ne correspond pas.

Supposons donc que ϕ n'est pas intérieur, qu'il ne préserve pas les permutations. Autrement dit, $k \geq 2$ (ce qui implique directement $n \geq 4$). On a

$\binom{n}{2} = \#\mathcal{C} = \frac{n!}{(n-2k)!k!2^k}$ ssi $(n-2)! = 2^{k-1}k!(n-2k)!$ ssi $\frac{2k-3}{k} \times \binom{n-2}{2k-2} \times (2k-5) \times \cdots \times 1 = 1$.

Si $k > 3$, alors $\frac{2k-3}{k} > 1$. On a donc $2 \leq k \leq 3$. Pour $k = 2$, on veut l'égalité $\binom{n-2}{2} = 2$, $(n-2)(n-3) = 4$, ce qui est impossible. Pour $k = 3$, on veut $\binom{n-2}{4} = 1$, ce qui n'est possible que pour les valeurs binomiales aux « bords », d'où $4 = n - 2$, autrement dit $n = 6$. $\square$

Remarque 2. Il existe effectivement des automorphismes de S_6 non intérieurs. On peut par exemple prouver son existence en étudiant les $5 - Sylow$ de S_5, où bien l'action $PGL_2(\mathbb{F}_5) \curvearrowright P^1(\mathbb{F}_5)$.

On peut également trouver une construction explicite d'un tel morphisme sur `www2u.biglobe.ne.jp/~nuida/m/doc/OutS6.pdf`.