2 Autour du groupe symétrique

2.1 Automorphismes de $\mathfrak{S}_n$

Leçons concernées : 101, 103, 104, 105, 108

Théorème 1. *Si $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs.*

Proposition 2. *Si $n = 6$, $\mathrm{Int}(\mathfrak{S}_6)$ est un sous-groupe d'indice 2 de $\mathrm{Aut}(\mathfrak{S}_6)$.*

Preuve : Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Regardons naturellement l'image des transpositions. L'image d'une transposition est un élément d'ordre 2 de $\mathfrak{S}_n$, il peut s'agir d'une transposition ou d'un produit de transpositions à support disjoint.

Lemme 3. *Soit $\sigma \in \mathfrak{S}_n$ un élément d'ordre 2, il est produit de $k \geqslant 1$ transpositions à support disjoint. Sa classe de conjugaison $\mathcal{O}$ est de cardinal :*

$$\mathrm{Card}(\mathcal{O}) = \frac{n!}{2^k k!(n-2k)!}$$

Preuve du lemme : Soit $\sigma \in \mathfrak{S}_n$ d'ordre 2 et $\mathcal{O}$ sa classe de conjugaison. Comme $\mathfrak{S}_n$ agit transitivement dessus, il suffit de connaître le cardinal du stabilisateur de σ, ie de son commutateur $C(\sigma)$, en effet, on a

$$\mathrm{Card}(\mathcal{O}) = \frac{n!}{\mathrm{Card}(C(\sigma))}$$

On écrit $\sigma = c_1 \circ ... \circ c_k$ sa décomposition en produit de cycles à support disjoints deux à deux. Comme σ est d'ordre 2, on en déduit que la longueur de chaque c_i est 2, donc $c_1, ..., c_k$ sont des transpositions. On écrit $c_i = \begin{pmatrix} a_i & b_i \end{pmatrix}$ et $F = [\![1, n]\!] \setminus \{a_1, ..., a_n, b_1, ..., b_n\}$ l'ensemble des points fixes de σ.
On a $\theta \in C(\sigma)$ si, et seulement si,

$$\theta \circ \sigma \theta^{-1} = \sigma \quad \Longleftrightarrow \quad \{c_1, ..., c_k\} = \left\{\theta \circ c_1 \circ \theta^{-1}, ..., \theta \circ c_k \circ \theta^{-1}\right\}$$

Cela se produit si, et seulement si, il existe $f \in \mathfrak{S}_n$ et $g \in \mathfrak{S}(F)$ tels que :

1. $\forall i, \theta \circ c_i \circ \theta^{-1} = c_{f(i)}$, ie $\left(\theta(a_i) = a_{f(i)} \text{ et } \theta(b_i) = b_{f(i)}\right)$ ou symétriquement.
2. $\forall x \in F, \sigma(x) = g(x)$.

On construit ainsi une bijection entre $C(\sigma)$ et $\mathfrak{S}_k \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathfrak{S}(F)$. On en déduit que

$$\mathrm{Card}\big(C(\sigma)\big) = k! \cdot 2^k \cdot (n-2k)! \qquad \text{et} \qquad \mathrm{Card}(\mathcal{O}) = \frac{n!}{2^k k!(n-2k)!}$$

□

Lemme 4. *On définit pour $k, n \geqslant 1$ tel que $2k \leqslant n$, $\alpha(k,n) = \dfrac{(n-2)!}{(n-2k)!2^{k-1}k!}$. Alors, on a*

$$\alpha(k,n) = 1 \Longleftrightarrow (k = 1 \text{ et } n \geqslant 2) \quad \text{ou} \quad (k,n) = (3,6)$$

Preuve du lemme : On a

$$\begin{aligned}\alpha(k,n) &= \frac{\binom{n-2}{n-2k}(2k-2)!}{2^{k-1}k!} \\ &= \binom{n-2}{n-2k} \frac{\prod_{j=0}^{k-2}(2j+1)}{k}\end{aligned}$$

- Si $k \geqslant 4$, $\displaystyle\prod_{j=0}^{k-2}(2j+1) \geqslant 2k-3 > k$, donc $\alpha(k,n) > 1$.
- Si $k = 2$, $\alpha(2,n) = \dfrac{1}{2}\dbinom{n-2}{n-4} = \dfrac{(n-2)(n-3)}{4}$. Et on ne peut pas avoir $\alpha(2,n) = 1$ car le produit de deux entiers consécutifs ne donne jamais 4.
- Si $k = 3$, on a $\alpha(3,n) = \dbinom{n-2}{n-6} = \dbinom{n-2}{4}$. Si $n \geqslant 7$, on a $\alpha(3,n) > 1$. (Pour $n \leqslant 5$, $\alpha(k,n)$ n'est pas défini, pas besoin d'étudier ce cas). □

L'image de toute transposition est une transposition si $n \neq 6$. Si τ est une transposition, alors φ induit une bijection entre la classe de conjugaison de τ et la classe de conjugaison de $\varphi(\tau)$. Si $\varphi(\tau)$ est produit de k transpositions, cela donne l'égalité de cardinal des classes :

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

Ainsi, si $n \neq 6$, on a nécessairement $k = 1$ et donc $\varphi(\tau)$ est toujours une transposition.

On note $\tau_i = \begin{pmatrix} 1 & i \end{pmatrix}$, les τ_i engendrent $\mathfrak{S}_n$. Par le résultat précédent, $\varphi(\tau_i)$ est une transposition et si $i \neq j$, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas.
Si on note $\varphi(\tau_2) = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix}$, alors $\varphi(\tau_3) = \begin{pmatrix} \alpha_1 & \alpha_3 \end{pmatrix}$ avec $\alpha_3 \neq \alpha_2$ car φ est injective. Plus généralement, on en déduit que $\varphi(\tau_i) = \begin{pmatrix} \alpha_1 & \alpha_i \end{pmatrix}$ avec tous les α_i distincts. En effet, on ne peut pas avoir $\varphi(\tau_i) = \begin{pmatrix} \alpha_2 & \alpha_3 \end{pmatrix}$ car sinon $\begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_3 \end{pmatrix} \begin{pmatrix} \alpha_2 \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_3 \end{pmatrix}$, ce qui donne par φ^{-1} : $\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & i \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}$, ce qui n'est pas possible.
On construit ainsi une permutation $\alpha \in \mathfrak{S}_n$ tel que

$$\alpha \tau_i \alpha^{-1} = \begin{pmatrix} \alpha_1 & \alpha_i \end{pmatrix} = \varphi(\tau_i)$$

Et donc, on a

$$\forall \sigma \in \mathfrak{S}_n, \varphi(\sigma) = \alpha \circ \sigma \circ \alpha^{-1}$$

□

Preuve de la proposition : On montre que si $n \geqslant 5$ et si on trouve un sous-groupe d'indice n H tel que H n'est le stabilisateur d'aucun $i \in [\![1, n]\!]$, alors il existe un automorphisme qui n'est pas intérieur.
H agit par translation à gauche sur $E = \mathfrak{S}_n/H$. On a donc un morphisme de groupe

$$\varphi : \mathfrak{S}_n \longrightarrow \mathfrak{S}(\mathfrak{S}_n/H) \simeq \mathfrak{S}_n$$

Il est injectif car $\mathrm{Ker}(\varphi) = \bigcap_{a \in G} aHa^{-1} \subset H$. En lisant les sous-groupes distingués de $\mathfrak{S}_n$, on se rend compte que pour des raisons de cardinalité, nécessairement, $\mathrm{Ker}(\varphi) = 1$.
Alors, $\varphi(H) = \mathrm{Stab}(\overline{1})$. En numérotant les éléments de $\mathfrak{S}_n/H$, on a alors un isomorphisme naturel $\mathfrak{S}(\mathfrak{S}_n/H) \overset{\psi}{\simeq} \mathfrak{S}_n$ tel que $\psi \circ \varphi(H) = \psi(\mathrm{Stab}(\overline{1})) = \mathrm{Stab}(1)$.
Alors, $\psi \circ \varphi$ est un automorphisme de $\mathfrak{S}_n$ qui envoie H sur $\mathrm{Stab}(1)$ qui ne sont pas conjugués, donc $\psi \circ \varphi$ n'est pas intérieur.

Afin de conclure, on exhibe un sous-groupe d'indice 5 de $\mathfrak{S}_6$ qui n'est pas un stabilisateur. Il suffit pour cela qu'il agisse transitivement sur $[\![1, 6]\!]$.
On observe que $PGL_2(\mathbb{F}_5)$ agit transitivement et fidèlement sur la droite projective à 6 éléments $\mathbb{P}(\mathbb{F}_5^2)$, cela identifie $PGL_2(\mathbb{F}_5)$ a un sous-groupe de $\mathfrak{S}_6$ qui agit transitivement sur $[\![1, 6]\!]$. □

Références :

- D. Perrrin, Cours d'algèbre.
- RMS 128-3 (2017-2018).

Stratégie de présentation : Le calcul du cardinal de la classe de conjugaison doit être correctement effectué : selon la taille du tableau, on peut envisager d'aller jusqu'à formaliser la bijection comme cela a été fait ici, sinon il faut "bien parler".
Pour la présentation du lemme 4, il sera important d'essayer de ne pas se limiter à des lignes de calculs afin de favoriser la lisibilité.
La proposition se place à un niveau moins élémentaire que le théorème du développement. C'est une façon possible d'élever le niveau de la présentation.