Automorphismes de $\mathfrak{S}_n$

Leçons : 104 ; 105 ; 108

Références : PERRIN, *Cours d'algèbre* (p.30)

"*Ce développement permet de donner une caractérisation du nombre* 6. "David Xu [1]

Prérequis :

- la famille des $(1i)$ engendre $\mathfrak{S}_n$
- un morphisme conserve l'ordre
- existence et unicité de la décomposition en cycle à support disjoint

On rappelle la définition d'un automorphisme intérieur.

Définition 1. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. On dit que φ est intérieur s'il existe $g \in \mathfrak{S}_n$ tel que pour tout $\sigma \in \mathfrak{S}_n$, on ait $\varphi(\sigma) = g\sigma g^{-1}$.

Introduction :

Pour des groupes relativement simples comme $\mathbb{Z}/n\mathbb{Z}$, on connait le groupe des automorphismes : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. On va étudier ici les automorphismes de $\mathfrak{S}_n$ et notamment on va voir que pour tout $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont exactement les automorphismes intérieurs de $\mathfrak{S}_n$ que l'on sait très bien décrire par un élément de $\mathfrak{S}_n$ (c.f. la définition ci-desus).

Théorème 1. Si $n \neq 6$, alors les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs, i.e. $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Lemme 1. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ envoie les transpositions sur les transpositions alors φ est intérieur.

Démonstration du lemme. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ qui envoie les transpositions sur les transpositions. On sait que l'ensemble $\{\tau_i := (1, i), \forall i \in \{2, \dots, n\}\}$ engendre $\mathfrak{S}_n$. On va donc étudier l'image des transpositions par φ.

Comme φ envoie transposition sur transposition, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ sont des transpositions, mais

$$\tau_2 \circ \tau_3 = (132)$$

qui est d'ordre 3, donc $\varphi(\tau_2) \circ \varphi(\tau_3)$ est aussi d'ordre 3, donc $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ont un élément en commun, on le note α_1. On écrit donc

$$\varphi(\tau_2) = (\alpha_1\alpha_2) \quad \text{et} \quad \varphi(\tau_3) = (\alpha_1\alpha_3)$$

De plus, $\alpha_2 \neq \alpha_3$ car φ est injectif [2].

Soit $i \in \{4, \dots, n\}$, on va regarder $\varphi(\tau_i)$, par le même argument que ci-dessus, il a élément commun avec $(\alpha_1\alpha_2)$ et $(\alpha_1\alpha_3)$

1. à ne pas dire le jour de l'oral
2. car φ est un automorphisme, donc il est bijectif par définition

Par l'absurde, considérons que $\varphi(\tau_i) = (\alpha_2\alpha_3)$, on aurait alors

$$\varphi(\tau_2 \circ \tau_3 \circ \tau_i) = (\alpha_1\alpha_2)(\alpha_1\alpha_3)(\alpha_2\alpha_3) = (\alpha_1\alpha 3) = \varphi(\tau_3)$$

Par injectivité de φ, on a donc

$$\tau_i = \tau_3 \circ \tau_2 \circ \tau_3 = (13)(12)(13) = (23)$$

ce qui est impossible par définition des τ_i. Ainsi l'élément en commun est forcément α_1. On peut donc écrire

$$\forall i \in \{2, \dots, n\} \quad \varphi(\tau_i) = (\alpha_1\alpha_i)$$

où tous les α_i sont distincts par injectivité de φ.

On pose alors la permutation

$$\alpha : \begin{cases} \{1, \dots, n\} & \to & \{1, \dots, n\} \\ i & \mapsto & \alpha_i \end{cases}$$

bien défini car tous les α_i sont distincts, sont dans $\{1, \dots, n\}$ et car il y en a n.

Ainsi on a

$$\varphi(\tau_i) = \alpha^{-1} \circ \tau_i \circ \alpha$$

Ce qui conclut la preuve car φ est donc intérieur. □

Proposition 1. Soit $\sigma \in \mathfrak{S}_n$, on écrit σ comme produit de cycles à supports disjoints et on note $n = k_1 + 2k_2 + 3k_3 + \cdots + nk_n$ où k_i est le nombre de i-cycle dans la permutation σ. Alors le centralisateur [a] de σ a pour cardinal

$$|c(\sigma)| = \prod_{i=1}^{n} i^{k_i} k_i!$$

a. le centralisateur de σ est $c(\sigma) = \{g \in \mathfrak{S}_n, g\sigma g^{-1} = \sigma\}$

Démonstration de la proposition.

Étape 1 : *Commençons par le cas où σ est un cycle*

Soit $\sigma = (x_1 \dots x_r)$ un cycle. Soit g un élément de $c(\sigma)$, on a donc

$$g\sigma g^{-1} = (g(x_1) \dots g(x_r))$$

Il faut donc que g envoie les éléments du cycle sur les éléments du cycle. Pour les $(n-r)$ autres éléments, il n'y a pas de containtes, donc on a $(n-r)!$ choix possibles. De plus, g a r choix pour l'image de x_1, mais une fois cette image fixée les autres sont elles-aussi fixées. Donc il a $(n-r)!r$ choix pour g, ainsi

$$|c(\sigma)| = (n-r)!r$$

Étape 2 : *Cas général*

Soit σ une permutation. Soit g un élément de $c(\sigma)$, on a $g\sigma g^{-1}$ qui envoie les $i-$cycles sur les $i-$cycles.

Pour chaque i, il y a k_i $i-$cyles, par définition. Pour chaque $i-$cycle $c_{j,i}$, on va fixer sur quel $i-$cycle, g enverra $c_{j,i}$. On a k_i choix pour $c_{1,i}$, puis $k_i - 1$ choix pour $c_{2,i}$, jusqu'à un seul choix pour $c_{k_i,i}$. Ainsi il y a $k_i!$ pour savoir sur quel $i-$cycle, g enverra chaque $i-$cycle.

Ensuite, pour chaque $i-$cycle, il faut choisir l'image du premier élément du cycle (comme à l'étape 1). Donc, comme on a k_i $i-$cycles, on a i^{k_i} choix possibles.

On a donc $i^{k_i}k_i!$ choix pour les $i-$cycles. Il faut faire cela pour chaque i, d'où

$$|c(\sigma)| = \prod_{i=1}^{n} i^{k_i}k_i!$$

□

Démonstration du théorème. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. On veut utiliser le lemme, donc on regarde si les transpositions s'envoient sur les transpositions. Soit τ une transposition. On sait que $\varphi(\tau)$ est d'ordre 2 car τ est d'ordre 2 et qu'un automorphisme conserve l'ordre. Donc $\varphi(\tau)$ est un produit de k transpositions à supports disjoints.

On va maintenant regarder le centralisateur pour utiliser la proposition. On a $c(\varphi(\tau)) = \varphi(c(\tau))$ (preuve par double inclusion). Donc $|c(\tau)| = |\varphi(c(\tau))| = |c(\varphi(\tau))|$.

Par la proposition

$$|c(\tau)| = 1^{n-2}(n-2)! \times 2^1 1! = 2(n-2)!$$

car il y a qu'un cycle de taille 2 et $n-2$ cycles de taille 1 et

$$|c(\varphi(\tau))| = 1^{n-2k}(n-2k)! \times 2^k k! = 2^k(n-2k)!k!$$

car il y a k cycles de taille 2 et $n-2k$ cycles de taille 1.

On veut que ces deux quantités soient égales.

$$\begin{aligned}
2(n-2)! = 2^k(n-2k)!k! &\iff \frac{(n-2)!}{(n-2k)!}\frac{1}{2^{k-1}k!} = 1 \\
&\iff \binom{n-2}{2k-2}\frac{(2k-2)!}{2^{k-1}k!} = 1 \\
&\iff \binom{n-2}{2k-2}\frac{(2k-2)(2k-4)\dots 4\times 2\times (2k-3)(2k-5)\dots 3\times 1}{2^{k-1}(k-1)!k} = 1 \\
&\iff \binom{n-2}{2k-2}\frac{(2k-3)(2k-5)\dots 3\times 1}{k} = 1
\end{aligned}$$

C'est impossible si $k \geqslant 4$ car $\dfrac{(2k-3)(2k-5)\dots 3\times 1}{k} > 1$ et le coefficient binomiale est supérieur à 1, donc on regarde les cas $k=1$, $k=2$ et $k=3$.

— Si $k=1$, alors l'image de τ est une transposition.

— Si $k=2$, on a $\binom{n-2}{2}\frac{1}{2} = 1 \iff (n-2)(n-3) = 4 \iff n^2-5n+2 = 0$. Or $\Delta = 5^2 - 4\times 2 = 17$ donc les solutions ne sont pas entières. Donc le cas $k=2$ est impossible.

— Si $k=3$, on a $\binom{n-2}{4} = 1 \iff (n-2)(n-3)(n-4)(n-5) = 4! \iff n = 6$.

Ainsi si $n \neq 6$, on est forcément dans le cas $k=1$ et donc toute transposition s'envoie sur une transposition, donc, par le lemme, φ est intérieur. Ainsi

$$\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$$

□

Remarques :

Il existe bien des automorphismes de $\mathfrak{S}_6$ qui ne sont pas intérieurs.

Donc pour $n=6$ on a $\mathrm{Aut}(\mathfrak{S}_n) \neq \mathrm{Int}(\mathfrak{S}_n)$. $\mathrm{Int}(\mathfrak{S}_n)$ est d'indice 2 dans $\mathrm{Aut}(\mathfrak{S}_n)$. C'est donc bien une caractérisation. (dans le développement, on ne prouve qu'un sens)