UE2 Groupes et Géométrie — Université de Nice
2019-2020

LES AUTOMORPHISMES DU GROUPE SYMÉTRIQUE, $\mathcal{S}_n$, $n \geq 3$

Référence : Perrin, Cours d'algèbre, page 30.

Puisque $n \geq 3$ le centre $Z(\mathcal{S}_n)$ de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$ (Lemme 2). Par suite $\mathcal{S}_n$ agit fidèlement sur lui-même par conjugaison. Autrement dit le groupe $\mathrm{Int}(\mathcal{S}_n)$ des automorphismes intérieurs de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_n$.

L'énoncé suivant assure que sauf dans le cas exceptionnel $n = 6$ les automorphismes intérieurs sont les seuls automorphismes.

On donne ensuite un automorphisme non intérieur de $\mathcal{S}_6$.

1. Automorphismes de $\mathcal{S}_n$, $n \neq 6$

Lemme 1. *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

Lemme 2. *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.*

Démonstration. Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (Lemme 1)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

Théorème 3. *Soit $n \geq 3$. Supposons que $n \neq 6$; alors*

$$\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Int}(\mathcal{S}_n) \simeq \mathcal{S}_n.$$

Lemme 4. *Soit φ un automorphisme de $\mathcal{S}_n$ qui envoie transpositions sur transpositions. Alors φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.*

Démonstration. Les transpositions de la forme $(1\ i)$ où $2 \leq i \leq n$ engendrent $\mathcal{S}_n$. Posons $\tau_i = \varphi(1\ i)$. Remarquons que pour i et j distincts τ_i et τ_j ne commutent pas car $(1\ i)$ et $(1\ j)$ ne commutent pas. Il en résulte que les transpositions τ_i et τ_j ont exactement un élément en commun dans leur support. On peut donc écrire τ_2 et τ_3 sous la forme

$$\tau_2 = (\alpha_1\ \alpha_2) \qquad\qquad \tau_3 = (\alpha_1\ \alpha_3)$$

avec $\alpha_2 \neq \alpha_3$. Montrons que pour tout $k \geq 4$ on a $\tau_k = (\alpha_1\ \alpha_k)$ pour un certain $\alpha_k \in \{1, 2, \ldots, n\}$. En effet si α_1 n'était pas dans le support de τ_k on aurait $\tau_k = (\alpha_2\ \alpha_3)$ et

$$\tau_2 \circ \tau_k = (\alpha_1\ \alpha_2\ \alpha_3) \qquad\qquad \tau_3 \circ \tau_k = (\alpha_1\ \alpha_3\ \alpha_2)$$

seraient inverses l'un de l'autre. Mais

$$(1\ 2)(1\ k) = (2\ 1\ k)$$

n'est pas l'inverse de

$$(1\ 3)(1\ k) = (3\ 1\ k)$$

contradiction.

Notons que $\alpha\colon k \mapsto \alpha_k$ est un élément de $\mathcal{S}_n$.

L'automorphisme φ et la conjugaison par α coïncident sur les générateurs $(1\ j)$ de $\mathcal{S}_n$; ils coïncident donc sur $\mathcal{S}_n$ tout entier. □

Démonstration du Théorème 3. Soit φ un automorphisme non intérieur de $\mathcal{S}_n$. Montrons que $n = 6$.

D'après le Lemme 4 il existe une transposition τ telle que $\varphi(\tau)$ ne soit pas une transposition. Puisque $(\varphi(\tau))^2 = \mathrm{id}$, $\varphi(\tau)$ est un produit de $k \geq 2$ transpositions à supports disjoints. Désignons par $\mathrm{C}(\tau)$ le centralisateur de τ

$$\mathrm{C}(\tau) = \big\{ f \in \mathcal{S}_n \mid f \circ \tau = \tau \circ f \big\}.$$

On a

$$\mathrm{C}(\tau) = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{engendré par } \tau} \times \underbrace{\mathcal{S}_{n-2}}_{\text{permutations de support disjoint de celui de } \tau}$$

En particulier on a un morphisme surjectif

$$\psi\colon \mathrm{C}(\tau) \to \mathcal{S}_{n-2}$$

de noyau $\mathbb{Z}/2\mathbb{Z}$.

Posons $\mathrm{H} = \mathrm{C}(\varphi(\tau)) = \big\{ f \in \mathcal{S}_n \mid f \circ \varphi(\tau) = \varphi(\tau) \circ f \big\}$. Les groupes H et $\mathrm{C}(\tau)$ sont isomorphes via φ. Chacune des transpositions de la décomposition de $\varphi(\tau)$ commute avec $\varphi(\tau)$ donc H contient un sous-groupe N isomorphe à $\big(\mathbb{Z}/2\mathbb{Z}\big)^k$. De plus N est le noyau du morphisme

$$\begin{array}{ccl} \mathrm{H} & \to & \mathcal{S}_k \\ h & \mapsto & \text{permutation induite sur les } k \text{ transpositions de la décomposition de } \varphi(\tau) \end{array}$$

donc $\mathrm{N} \lhd \mathrm{H}$.

Ainsi comme $\mathrm{C}(\tau) \simeq \mathrm{H}$, $\mathrm{C}(\tau)$ contient un sous-groupe N' avec les deux propriétés suivantes :

$$\begin{cases} \mathrm{N}' \lhd \mathrm{C}(\tau) \\ \mathrm{N}' \simeq \big(\mathbb{Z}/2\mathbb{Z}\big)^k \end{cases}$$

Via ψ on obtient que $\mathcal{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $\big(\mathbb{Z}/2\mathbb{Z}\big)^k$ ou $\big(\mathbb{Z}/2\mathbb{Z}\big)^{k-1}$ suivant que $\tau \in \mathrm{N}'$ ou $\tau \notin \mathrm{N}'$.

Or les sous-groupes distingués de $\mathcal{S}_n$ sont

- $\{\mathrm{id}\}$, $\mathcal{A}_n$, $\mathcal{S}_n$ si $n \neq 4$;
- $\{\mathrm{id}\}$, $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4$, $\mathcal{S}_4$.

On en déduit les deux possibilités suivantes

- $n = 4$ car $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre à $\big(\mathbb{Z}/2\mathbb{Z}\big)^{k-1}$ avec $k = 2$;
- $n = 6$ car $\mathcal{S}_4$ contient $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons que $n = 4$. Le centralisateur d'une transposition dans $\mathcal{S}_4$ est de cardinal 4 (c'est le groupe V_4) alors que le centralisateur d'une double transposition est de cardinal 8 (en effet il divise strictement 24, est multiple strict de 4 car contient V_4 mais aussi au moins un 4-cycle) : contradiction.

Ainsi $n = 6$. □

2. Automorphismes extérieurs de $\mathcal{S}_6$, version 1

Étudions désormais les automorphismes extérieurs de $\mathcal{S}_6$.

Rappelons l'énoncé suivant :

Théorème 5. *Soit $n \geq 5$. Les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.*

Lemme 6. *L'ensemble $\mathrm{Syl}(\mathcal{S}_5)$ des 5-sous-groupes de Sylow de $\mathcal{S}_5$ est de cardinal 6.*

On numérote arbitrairement $\mathrm{Syl}(\mathcal{S}_5)$ de 1 à 6.

Lemme 7. *Faisons opérer $\mathcal{S}_5$ sur $\mathrm{Syl}(\mathcal{S}_5) \simeq \{1, 2, 3, 4, 5, 6\}$ par conjugaison. La morphisme $\mathcal{S}_5 \to \mathcal{S}_6$ ainsi obtenu est injectif. Notons G son image.*

Lemme 8. *Numérotons arbitrairement de 1 à 6 les éléments de $\mathcal{S}_6/\mathrm{G}$. Faisons opérer $\mathcal{S}_6$ sur $\mathcal{S}_6/\mathrm{G} \simeq \{1, 2, 3, 4, 5, 6\}$ par translations.*

Le morphisme $\varphi\colon \mathcal{S}_6 \to \mathcal{S}_6$ ainsi obtenu est un automorphisme.

Lemme 9. *Le groupe G n'a pas de points fixes sur $\{1, 2, 3, 4, 5, 6\}$.*

Le groupe $\varphi(\mathrm{G})$ admet un point fixe.

L'automorphisme φ n'est pas intérieur.

Démonstration du Lemme 6. On a $|\mathcal{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. L'ordre d'un élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est donc 5. Or 5 est premier donc tout élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Posons $n_5 = \#\mathrm{Syl}_5(\mathcal{S}_5)$. Les théorèmes de Sylow assurent que

$$\begin{cases} n_5 \equiv 1 \bmod 5 \\ n_5 \text{ divise } 2^3 \cdot 3 = 24 \end{cases}$$

Par conséquent n_5 appartient à $\{1, 6\}$.

Supposons que $n_5 = 1$. Alors $\mathcal{S}_5$ a un unique 5-Sylow qui est distingué : contradiction avec le fait que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$. Par suite $n_5 = 6$. □

Démonstration du Lemme 7. Soit K le noyau du morphisme de $\mathcal{S}_5$ vers $\mathcal{S}_\mathrm{G}$. Il est contenu dans le stabilisateur de chacun des éléments de $\mathrm{Syl}_5(\mathcal{S}_5)$. L'action de G sur $\mathrm{Syl}_5(\mathcal{S}_5)$ est transitive (théorème de Sylow). Il en résulte que le stabilisateur de chaque élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ a pour cardinal $\frac{120}{6} = 20$. Donc $|\mathrm{K}|$ divise 20. Puisque K est distingué dans $\mathcal{S}_5$, que $|\mathrm{K}|$ divise 20 et que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$, on obtient que $\mathrm{K} = \{\mathrm{id}\}$. □

Démonstration du Lemme 8. Soit K' le noyau du morphisme naturel de $\mathcal{S}_6$ dans $\mathcal{S}_{\mathcal{S}_6/\mathrm{G}}$. Il est contenu dans le stabilisateur des éléments de $\mathcal{S}_6/\mathrm{G}$ et en particulier dans celui de la classe triviale G qui n'est autre que G. Ainsi $|\mathrm{K}'|$ divise $|\mathrm{G}| = 120$. On a donc

$$\begin{cases} \mathrm{K}' \lhd \mathcal{S}_6 \\ |\mathrm{K}'| \text{ divise } 120 \\ \text{les sous-groupes distingués de } \mathcal{S}_6 \text{ sont } \{\mathrm{id},\, \mathcal{A}_6,\, \mathcal{S}_6\} \end{cases}$$

d'où $\mathrm{K}' = \{\mathrm{id}\}$. Autrement dit le morphisme φ est injectif. Pour des raisons de cardinalité φ est bijectif. □

Démonstration du Lemme 9. Si G avait un point fixe sur $\{1, 2, 3, 4, 5, 6\} \simeq \mathcal{S}$ cela signifierait qu'il existe un 5-sous-groupe de Sylow invariant par conjugaison, *i.e.* distingué, ce qui est absurde. Par contre $\varphi(\mathrm{G})$ a un point fixe, celui qui correspond à la classe triviale G, invariante sous l'action de G par translation.

Supposons que φ soit intérieur donc de la forme

$$\sigma \mapsto \sigma_0 \circ \sigma \circ \sigma_0$$

pour un certain σ_0. Soit p un point fixe de $\varphi(\mathrm{G})$. On aurait alors pour tout $g \in \mathrm{G}$

$$\begin{aligned} g(\sigma_0^{-1}p) &= \sigma_0^{-1}(\sigma_0(g(\sigma_0^{-1}(p)))) \\ &= \sigma_0^{-1}((\sigma_0 \circ g \circ \sigma_0^{-1})(p)) \\ &= \sigma_0^{-1}(\varphi(g)(p)) \\ &= \sigma_0^{-1}(p) \end{aligned}$$

car p est fixe sous $\varphi(\mathrm{G})$. On aboutit alors à une contradiction. □

3. Automorphismes extérieurs de $\mathcal{S}_6$, version 1

Rappel : soit G un groupe. Si H est un sous-groupe de G d'incide r, nous obtenons un morphisme de G dans $\mathcal{S}_r$ en faisant agir G sur les classes à gauche modulo H. Plus précisément si $g_1\mathrm{H}$, …, $g_r\mathrm{H}$ désignent les r classes à gauche, nous associons une permutation $\sigma \in \mathcal{S}_r$ à un élément $g \in \mathrm{G}$ en posant

$$(gg_i)\mathrm{H} = g_{\sigma(i)}\mathrm{H}$$

Notons que $i \mapsto \sigma(i)$ est une bijection : l'inverse est donné par l'action de g^{-1}.

Lemme 10. *Soit $n \geq 5$. Si* H *est un sous-groupe de $\mathcal{S}_n$ d'indice n qui agit transitivement sur $\{1, 2, \ldots, n\}$, alors le morphisme $\psi\colon \mathcal{S}_n \to \mathcal{S}_n$ associé à l'action de $\mathcal{S}_n$ sur les classes de $\mathcal{S}_n$ modulo* H *est un automorphisme non intérieur.*

Démonstration. Considérons l'action

$$\mathcal{S}_n \times \mathcal{S}_n/\mathrm{H} \to \mathcal{S}_n/\mathrm{H} \qquad\qquad (g, g_i\mathrm{H}) \mapsto g_{\sigma(i)}\mathrm{H} := (gg_i)\mathrm{H}$$

Par définition un élément g appartient à $\ker\psi$ si et seulement si

$$g \in \bigcap_{i=1}^{n} \mathrm{Stab}(g_i\mathrm{H}).$$

En particulier $\ker\psi$ est contenu dans H. Comme H est d'indice $n \geq 3$ et comme les seuls sous-groupes distingués de $\mathcal{S}_n$ sont d'indice 1 ou 2 ou n on a $\ker\psi = \{\mathrm{id}\}$. Par suite ψ est un automorphisme.

Raisonnons par l'absurde : supposons que ψ soit un automorphisme intérieur. Alors il existe $a \in \mathcal{S}_n$ tel que $\psi(\mathrm{H}) = a\mathrm{H}a^{-1}$. Ainsi $\psi(\mathrm{H})$ agit transitivement sur $\{1, 2, \ldots, n\}$. En effet soient i, j dans $\{1, 2, \ldots, n\}$; il existe par hypothèse un élément h de H tel que $h(a^{-1}(i)) = a^{-1}(j)$, donc aha^{-1} est un élément de $a\mathrm{H}a^{-1}$ qui envoie i sur j. Remarquons que si $g_i\mathrm{H} = \mathrm{H}$ est la classe de l'élément neutre modulo H, alors $\psi(\mathrm{H})$ fixe i ; en effet si $h \in \mathrm{H}$, alors

$$hg_i\mathrm{H} = h\mathrm{H} = \mathrm{H} = g_i\mathrm{H}$$

et donc n'agit pas transitivement. □

Proposition 11. *Il existe un sous-groupe* H *de* $\mathcal{S}_6$ *d'indice* 6 *qui agit transitivement sur*

$$\{1, 2, 3, 4, 5, 6\}.$$

Démonstration. Considérons l'action de $\mathrm{GL}(2, \mathbb{F}_5)$ sur les six droites du plan $(\mathbb{F}_5)^2$. Cette action est transitive. Elle devient fidèle après avoir quotienté par le sous-groupe des homothéties qui est d'ordre 4. Autrement dit cette action induit un morphisme injectif de $\mathrm{PGL}(2, \mathbb{F}_5)$ dans $\mathcal{S}_6$; l'image H de ce morphisme agit transitivement sur $\{1, 2, 3, 4, 5, 6\}$. L'ordre de $\mathrm{GL}(2, \mathbb{F}_5)$ est $24 \cdot 20 = 5! \cdot 4$. Par conséquent

$$|\mathrm{H}| = |\mathrm{PGL}(2, \mathbb{F}_5)| = 5!$$

Ainsi H est un sous-groupe d'indice 6 dans $\mathcal{S}_6$. □