Développement : Automorphismes de $\mathfrak{S}_n$

RM

2022-2023

Référence :

1. Oral à l'agrégation de mathématiques

Énoncé :

Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.

Définition 1 : Soit G un groupe et φ un endomorphisme de G. On dit que φ est un automorphisme intérieur de G s'il existe $a \in G$ tel que $\varphi(x) = axa^{-1}$ pour tout $x \in G$, et qu'il est extérieur sinon. On note $Int(G)$ l'ensemble des automorphismes intérieurs de G.

Lemme 2 : Soit G un groupe et φ un automorphisme de G. Alors l'image par φ d'une classe de conjugaison est une classe de conjugaison.

Démonstration : Soit x un élément de G, et soit C_x sa classe de conjugaison. Soit $y \in C_x$: il existe $a \in G$ tel que $y = axa^{-1}$. Comme φ est un morphisme, on a alors $\varphi(y) = \varphi(a)\varphi(x)\varphi(a)^{-1} \in C_{\varphi(x)}$ et par conséquent $\varphi(C_x) \subseteq C_{\varphi(x)}$.
Soit $y \in C_{\varphi(x)}$: il existe $a \in G$ tel que $y = a\varphi(x)a^{-1}$. On pose $b = \varphi^{-1}(a)$ de sorte que $\varphi(bxb^{-1}) = a\varphi(x)a^{-1} = y$, et donc $y \in \varphi(C_x)$. Ainsi, on a donc $\varphi(C_x) = C_{\varphi(x)}$, ce qui prouve le résultat.

Théorème (Admis) 3 : Deux permutations sont conjuguées si et seulement si elles ont le même nombre de cycles de chaque longueur.

Résolution :

Lemme : Soit $\varphi \in Aut(\mathfrak{S}_n)$. Si φ transforme transposition en transposition, alors $\varphi \in Int(\mathfrak{S}_n)$.

Démonstration : Comme φ est un morphisme, il suffit de montrer que φ est intérieur sur un ensemble de générateurs de $\mathfrak{S}_n$ pour montrer que $\varphi \in Int(\mathfrak{S}_n)$. On choisit alors la famille génératrice formée par les transpositions $\tau_i = (1, i)$ pour $i \in [\![2\,;n]\!]$. Par hypothèse, $\varphi(\tau_i)$ est aussi une transposition pour tout $i \in [\![2\,;n]\!]$. De plus, pour tout $i, j \in [\![2\,;n]\!]$ distincts, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne sont pas à supports disjoints. En effet, si c'était le cas, alors elles commuteraient et on aurait donc

$$\varphi(\tau_i\tau_j) = \varphi(\tau_i)\varphi(\tau_j) = \varphi(\tau_j)\varphi(\tau_i) = \varphi(\tau_j\tau_i)$$

ce qui entraînerait $\tau_i\tau_j = \tau_j\tau_i$ par bijectivité de φ, ce qui est faux.
Il existe donc $a_1 \in [\![1\,;n]\!]$ qui appartient au support de $\varphi(\tau_2)$ et $\varphi(\tau_3)$. On introduit alors les éléments $a_2, a_3 \in [\![1\,;n]\!]$ tels que $\varphi(\tau_2) = (a_1, a_2)$ et $\varphi(\tau_3) = (a_1, a_3)$.
Comme $\varphi(\tau_2)$ et $\varphi(\tau_3)$ sont des transpositions et que φ est bijective, on a de plus que a_1, a_2, a_3 sont deux à deux distincts.

En effet, comme $\tau_2 \neq \tau_3$, alors $\varphi(\tau_2) \neq \varphi(\tau_3)$ et donc $a_2 \neq a_3$. Comme τ_2 et τ_3 ne sont pas l'identité, alors $\varphi(\tau_2)$ et $\varphi(\tau_3)$ non plus. Donc $a_1 \neq a_2$ et $a_1 \neq a_3$, et donc on a bien que $a_1 \neq a_2 \neq a_3$.

De même, comme τ_4 ne commute ni avec τ_3 ni avec τ_2, alors le support de $\varphi(\tau_4)$ possède une intersection non vide avec le support de $\varphi(\tau_2)$ et $\varphi(\tau_3)$. Supposons par l'absurde que l'intersection des supports de $\varphi(\tau_2)$,$\varphi(\tau_3)$ et $\varphi(\tau_4)$ soit vide, ce qui revient à dire que $\varphi(\tau_4) = (a_2, a_3)$.

En effet,

$$supp(\varphi(\tau_2)) \cap supp(\varphi(\tau_3)) \cap supp(\varphi(\tau_4)) = \{a_1, a_2\} \cap \{a_1, a_3\} \cap \{a_2, a_3\} = \emptyset$$

et l'intersections et vide si et seulement si $\varphi(\tau_4) = (a_2, a_3)$.

On a alors l'égalité

$$\varphi(\tau_2\tau_3\tau_4) = (a_1, a_2)(a_1, a_3)(a_2, a_3) = (a_1, a_3) = \varphi(\tau_3).$$

Par injectivité de φ, on a donc $\tau_2\tau_3\tau_4 = \tau_3$, ce qui est faux. Ainsi, a_1 appartient nécessairement au support de $\varphi(\tau_4)$ et par conséquent il existe $a_4 \in [\![1\,;n]\!]$ différent de a_1, a_2, a_3 tel que $\varphi(\tau_4) = (a_1, a_4)$. On répète le même argument pour montrer que pour tout $i \in [\![2\,;n]\!]$, il existe $a_i \in [\![1\,;n]\!]$ tel que $\varphi(\tau_i) = (a_1, a_i)$. Par bijectivité de φ, on montre comme avant que tous les a_i sont distincts et on a donc construit une permutation $\sigma : i \mapsto a_i$ qui vérifient, pour tout $i \in [\![1\,;n]\!]$, $\sigma\tau_i\sigma^{-1} = (a_1, a_i) = \varphi(\tau_i)$. Comme les τ_i engendrent $\mathfrak{S}_n$, on a donc $\varphi(x) = \sigma x\sigma^{-1}$ pour tout $x \in \mathfrak{S}_n$, d'où $\varphi \in Int(\mathfrak{S}_n)$. □

La condition suffisante que l'on vient de prouver est en fait aussi nécessaire. En effet, si φ est un automorphisme intérieur, alors il stabilise toutes les classes de conjugaison. D'après le théorème 3, l'ensemble T_1 des transpositions est une classe de conjugaison, et on a donc $\varphi(T_1) = T_1$.

Démonstration (Théorème) : L'ordre est une propriété algébrique, donc l'image de toute transposition par $\varphi \in Aut(\mathfrak{S}_n)$ est un élément d'ordre 2, mais pas nécessairement une transposition à priori. On note alors T_k l'ensemble des permutations de $\mathfrak{S}_n$ qui sont produits d'exactement k transpositions à support disjoint. D'après le Théorème 3, T_k est une classe de conjugaison de $\mathfrak{S}_n$ pour tout $k \in [\![1\,;\lfloor n/2 \rfloor]\!]$ (en effet, il ne peut y avoir plus de $\lfloor n/2 \rfloor$ transpositions à support disjoint pour un élément de $\mathfrak{S}_n$).

D'après le Lemme précédent, il suffit de montrer que $\varphi(T_1) = T_1$ pour conclure. D'après le Lemme 2, $\varphi(T_1)$ est une classe de conjugaison d'éléments d'ordre 2, donc il existe $k \in \mathbb{N}$ tel que $\varphi(T_1) = T_k$ (car tous les élément de T_k sont d'ordre 2).

Supposons par l'absurde que $k > 1$ et montrons que c'est impossible par cardinalité lorsque $n \neq 6$. D'une part, on a

$$|T_1| = \binom{n}{2} = \frac{n(n-1)}{2}.$$

D'autre part, pour créer une permutation de T_k, il suffit de choisir les supports des k transpositions. Puisque les supports sont disjoints, alors les transpositions commutent et leur ordre n'importe pas. Ainsi, on en déduit

$$|T_k| = \frac{\binom{n}{2}\binom{n-2}{2}...\binom{2-2(k-1)}{2}}{k!} = \frac{n(n-1)...(n-2k+1)}{2^k k!}.$$

Par bijectivité de φ, on a donc $|T_1| = |\varphi(T_1)| = |T_k|$, d'ou l'égalité suivante :

$$(n-2)...(n-2k+1) = 2^{k-1}k!.$$

Montrons que cette équation diophantienne n'admet une solution que dans le cas $n = 6$: • Pour $k = 2$: l'équation se réécrit $(n-2)(n-3) = 4$, qui n'admet pas de solution dans $\mathbb{N}$.

• Pour $k > 3$: on réécrit $(n-2)(n-3)...(n-k+1)\binom{n-k}{k} = 2^{k-1}$. Cependant, on a nécessairement soit $(n-2)$, soit $(n-3)$, qui est impair, donc il n'existe pas de solution pour $k > 3$.

• Pour $k = 3$: $(n-2)(n-3)(n-4) = 2^3 \times 3$ qui admet pour unique solution $n = 6$.

Ainsi, pour $n \neq 6$, la seule solution est $k = 1$ et donc $\varphi(T_1) = T_1$, d'où $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$ d'après le Lemme. □

Corollaire 4 : Pour $n \neq 2, 6$, le groupe $Aut(\mathfrak{S}_n)$ est isomorphe à $\mathfrak{S}_n$ et tous les automorphismes sont intérieurs.

Démonstration : On vient de montrer que tous les morphismes de $\mathfrak{S}_n$ sont intérieurs. dE plus pour tout groupe G, $G/Z(G)$ est isomorphe à $Int(G)$ par l'application

$$\begin{array}{rccc} \varphi : & G & \to & Int(G) \\ & x & \mapsto & (u \mapsto xux^{-1}) \end{array} .$$

Il est clair qu'il s'agit d'un morphisme de groupe et que $Ker(\varphi) = Z(G)$. On conclut en quotientant par $Z(G)$, qui est trivial, que $\mathfrak{S}_n$ est isomorphe à $Int(\mathfrak{S}_n) = Aut(\mathfrak{S}_n)$. □

> À voir dans le livre les programmes sage qui peuvent se révéler intéressant.
> De plus, on peut trouver la structure exact de $Aut(\mathfrak{S}_6)$ qui est la suivante :
>
> $$Aut(\mathfrak{S}_6) \cong Int(\mathfrak{S}_6) \rtimes \mathbb{Z}/2\mathbb{Z}$$