
Devoir Maison n° 25

Problème - Autour du groupe alterné

On fixe dans le problème un entier $n \geq 2$. On note $A_n = \ker(\varepsilon)$ le noyau du morphisme signature $\varepsilon : S_n \rightarrow \{\pm 1\}$ c'est-à-dire :

$$A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$$

A_n est appelé groupe alterné d'ordre n . Le but de ce problème est de donner certaines propriétés du groupe A_n et d'en déduire certaines propriétés du groupe S_n .

Partie I - Préliminaires

1. Expliciter A_2 et A_3 .
2. Justifier en une phrase que A_n est bien un sous-groupe de S_n .
3. Soit

$$\varphi: \begin{cases} A_n \longrightarrow S_n \setminus A_n \\ \sigma \longmapsto (12) \circ \sigma \end{cases}$$

Montrer que φ est bien définie et bijective.

4. En déduire le cardinal de A_n .
5. Expliciter A_4 sans justification (A_4 doit contenir l'identité, trois produits de deux transpositions, et huit 3-cycles). A_4 est-il abélien ?

On suppose dans la suite que $n \geq 3$.

Partie II - A_n et les 3-cycles

1. Montrer que les 3-cycles sont des éléments de A_n , puis qu'un produit de 3-cycles est un élément de A_n .
2. Justifier que A_n est exactement l'ensemble des permutations pouvant s'écrire comme le produit d'un nombre pair de transpositions.
3. Soient a, b, c, d quatre éléments de $\llbracket 1; n \rrbracket$ (pas forcément distincts mais avec tout de même $a \neq b$ et $c \neq d$). Montrer (en distinguant les cas selon le cardinal de $\{a; b\} \cap \{c; d\}$) que $(ab) \circ (cd)$ est un produit de 3-cycles.
4. Conclure que A_n est engendré par les 3-cycles, c'est-à-dire que A_n est exactement l'ensemble des permutations qui peuvent s'écrire comme produit de 3-cycles.

Partie III - A_n est le seul sous-groupe de S_n d'indice 2

On se donne dans cette partie un sous-groupe H de S_n d'indice 2, c'est-à-dire que $\text{card}(H) = \text{card}(S_n)/2$, et le but de cette partie est de prouver que $H = A_n$.

1. Montrer que H contient les carrés, c'est-à-dire que, pour tout $x \in S_n$, $x^2 \in H$. On pourra distinguer les cas selon que $x \in H$ ou non et, dans le dernier cas, s'intéresser à l'ensemble $xH = \{xh \mid h \in H\}$.
2. Montrer qu'un 3-cycle est un carré.
3. Conclure.

Partie IV - Simplicité de A_n pour $n \geq 5$

On suppose dans cette partie que $n \geq 5$. On rappelle (cf. exercice 34 du chapitre 18) que si G est un groupe et H un sous-groupe de G , on dit que H est distingué dans G si :

$$\forall x \in G, \forall h \in H, xhx^{-1} \in H$$

1. Montrer que, si G est un groupe, $\{e\}$ et G sont distingués dans G .

Le but de cette partie est de prouver que A_n est simple si $n \geq 5$, c'est-à-dire que A_n n'admet aucun sous-groupe distingué différent de $\{\text{Id}\}$ (il est sous-entendu qu'on parle de $\text{Id}_{\llbracket 1; n \rrbracket}$) et de lui-même. On suppose qu'il existe $H \neq \{\text{Id}\}$ un sous-groupe distingué de A_n , et on cherche à prouver que $H = A_n$. On se donne alors une permutation $\sigma \in H \setminus \{\text{Id}\}$ admettant un nombre de points fixes maximal (parmi les éléments de $H \setminus \{\text{Id}\}$).

2. Justifier l'existence de σ , puis que le support de σ a au moins trois éléments.
3. On suppose dans cette question que les cycles apparaissant dans l'écriture de σ comme produit de cycles à supports disjoints ont tous un support à deux éléments : σ est donc un produit de transpositions à supports disjoints.
 - (a) Justifier que ce produit contient au moins deux transpositions, qu'on note (ij) et (rs) avec i, j, r, s deux à deux distincts.
 - (b) Justifier l'existence d'un élément $k \in \llbracket 1; n \rrbracket$ distinct de i, j, r, s .
 - (c) On pose $\tau = (rsk)$ (attention, τ n'est pas une transposition) et $\sigma' = \sigma\tau\sigma^{-1}\tau^{-1}$. Justifier que $\sigma' \in H$.
 - (d) Soit x un point fixe de σ . Montrer que x est un point fixe de σ^{-1} .
 - (e) Calculer $\sigma'(k)$.
 - (f) Prouver que σ' a strictement plus de points fixes que σ et en déduire que l'un des cycles de σ est de longueur supérieure ou égale à 3.
4. Il existe donc i, j, k deux à deux distincts tels que $\sigma(i) = j$ et $\sigma(j) = k$. Le but de cette question est de prouver que $\sigma = (ijk)$. On raisonne par l'absurde et on suppose que ce n'est pas le cas.
 - (a) Justifier que $\sigma(k) \neq k$.
 - (b) Prouver que le support de σ contient au moins 5 éléments (on pourra s'aider de la question 3). Soient alors $r \neq s$ avec $\sigma(r) = s$ deux éléments du support de σ , distincts de i, j, k .
 - (c) Aboutir à une absurdité de même que précédemment.
5. Ainsi, $\sigma = (ijk)$. Soit $\sigma' = (i'j'k')$ un 3-cycle (pas forcément distinct de σ).
 - (a) Justifier qu'il existe $\rho \in S_n$ tel que $\rho \circ \sigma \circ \rho^{-1} = \sigma'$ (on pourra encore utiliser l'exercice 17).
 - (b) Soient r et s distincts de i, j, k . Justifier l'existence de r et s .
 - (c) À l'aide de ρ et de $\rho \circ (rs)$, prouver qu'il existe $s \in A_n$ tel que $\sigma' = s \circ \sigma \circ s^{-1}$.
 - (d) Conclure.
6. Cherchons à présent tous les sous-groupes alternés de S_n (toujours pour $n \geq 5$). Soit donc H un sous-groupe distingué de S_n .
 - (a) Justifier que $H \cap A_n$ est un sous-groupe distingué de A_n . Ainsi, d'après ce qui précède, $H \cap A_n = \{\text{Id}\}$ ou $H \cap A_n = A_n$.
 - (b) Dans le cas où $H \cap A_n = A_n$, justifier que $H = A_n$ ou $H = S_n$ (on pourra utiliser le théorème de Lagrange, cf. chapitre 18).
 - (c) Dans le cas où $H \cap A_n = \{\text{Id}\}$, prouver que $\varepsilon|_H$ est injective et donc que $\text{card}(H) \leq 2$, puis conclure que $H = \{\text{Id}\}$ (on pourra utiliser la question 3 de l'exercice 17).

Remarque : D'après le théorème de Lagrange, un groupe de cardinal premier n'admet que deux sous-groupes : $\{e\}$ et lui-même, donc A_3 (qui est d'ailleurs isomorphe à $\mathbb{Z}/3\mathbb{Z}$) est également simple. On peut montrer que A_4 n'est pas simple car l'ensemble $H = \{\text{Id}; (12)(34); (13)(24); (14)(23)\}$ est un sous-groupe distingué de A_4 (ce n'est pas compliqué à prouver, les curieux peuvent le vérifier chez eux) isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Pour la culture, le fait que A_n soit simple et le fait que les seuls sous-groupes distingués de S_n soient $\{\text{Id}\}, A_n$ et S_n , pour $n \geq 5$, sont les raisons profondes du fait qu'il est impossible de résoudre explicitement les équations de degré supérieur ou égal à 5.