

Titre : Simplicité du groupe alterné

Recasages : 103, 104, 105, 108

Thème : Théorie des groupes, calculatoire

Références : Ulmer - *Théorie des Groupes* (p. 53)

Théorème 1. *Pour $n \geq 5$, le groupe alterné \mathfrak{A}_n est simple.*

Soit $N \trianglelefteq \mathfrak{A}_n$ un sous-groupe distingué non trivial, nous allons montrer que $N = \mathfrak{A}_n$. Nous allons utiliser à de nombreuses reprises un résultat calculatoire sur le groupe symétrique :

Lemme 2. *Soit $(i_1 i_2 \cdots i_k)$ un k -cycle de \mathfrak{S}_n et $\rho \in \mathfrak{S}_n$, alors*

$$\rho(i_1 i_2 \cdots i_k)\rho^{-1} = (\rho(i_1) \rho(i_2) \cdots \rho(i_k))$$

Démonstration. Soit $a \in \llbracket 1, n \rrbracket$, alors

- Si $a \notin \{\rho(i_1), \dots, \rho(i_k)\}$, alors $\rho^{-1}(a) \notin \{i_1, \dots, i_k\}$ et

$$\rho(i_1 i_2 \cdots i_k)\rho^{-1}(a) = \rho(\rho^{-1}(a)) = a$$

- Si $a = \rho(i_p)$ pour un $p \in \llbracket 1, n \rrbracket$, alors

$$\rho(i_1 i_2 \cdots i_k)\rho^{-1}(a) = \rho(i_1 i_2 \cdots i_k)i_p = \rho(i_{p+1})$$

avec la convention $i_{k+1} = i_1$.

□

Ce lemme nous apprend en particulier que tous les k -cycles sont conjugués dans \mathfrak{S}_n , montrons que pour $n \geq 5$, les 3-cycles sont conjugués dans \mathfrak{A}_n : Soient σ et σ' deux 3-cycles, il existe $\rho \in \mathfrak{S}_n$ tel que $\rho\sigma\rho^{-1} = \sigma'$.

- Si $\rho \in \mathfrak{A}_n$, il n'y a rien à montrer.
- Si $\rho \notin \mathfrak{A}_n$, on peut (comme $n \geq 5$) choisir $a, b \notin \text{Supp}(\sigma)$, on pose $\tilde{\rho} := \rho(a b)$ et on a

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

avec $\rho(a b) \in \mathfrak{A}_n$.

Donc si N contient un 3-cycle, il les contient tous. Or, les 3-cycles engendrent \mathfrak{A}_n , donc $N = \mathfrak{A}_n$.

Soit $1 \neq \sigma \in N$, on considère la décomposition de σ en produit de cycles à supports disjoints, on a l'un des cas suivants :

- A. σ contient un cycle de longueur $n \geq 4$.
- B. σ contient un ou plusieurs 3-cycles.
- C. σ est un produit d'un nombre pair de transpositions.

Nous allons conclure dans chacun de ces cas que $N = \mathfrak{A}_n$:

- A. On pose $\sigma = (i_1 i_2 i_3 i_4 \cdots) \prod c_i$, on considère $c = (i_1 i_2 i_3) \in \mathfrak{A}_n$ et on a

$$\begin{aligned} [c, \sigma] &= c\sigma c^{-1}\sigma^{-1} = (c(i_1) c(i_2) c(i_3) c(i_4) \cdots) \left(\prod c_i \right) (i_1 i_2 i_3 i_4 \cdots)^{-1} \left(\prod c_i \right)^{-1} \\ &= (i_2 i_3 i_1 i_4 \cdots) (\cdots i_4 i_3 i_2 i_1) \\ &= (i_1 i_2 i_4) \end{aligned}$$

Qui est un élément de N car celui-ci est distingué, donc N contient un 3-cycle et $N = \mathfrak{A}_n$.

- B. 1. Si σ contient un seul 3-cycle, alors $\sigma = (i_1 \ i_2 \ i_3) \prod \tau_i$ où τ_i sont des transpositions (ce ne sont pas des k -cycles pour $k \geq 3$ par le cas précédent). On a alors $\sigma^2 = (i_1 \ i_3 \ i_2) \in N$ qui est donc égal à \mathfrak{A}_n .
2. Si σ contient plusieurs 3-cycles, on écrit $\sigma = (i_1 \ i_2 \ i_3)(i'_1 \ i'_2 \ i'_3) \prod c_i$, on considère $c = (i'_1 \ i'_2 \ i_3)$, on a alors

$$\begin{aligned}
[c, \sigma] &= (c(i_1) \ c(i_2) \ c(i_3))(c(i'_1) \ c(i'_2) \ c(i'_3)) \left(\prod c_i \right) (i'_1 \ i'_2 \ i'_3)^{-1} (i_1 \ i_2 \ i_3)^{-1} \left(\prod c_i \right)^{-1} \\
&= (i_1 \ i_2 \ i'_1)(i'_2 \ i_3 \ i'_3)(i'_3 \ i'_2 \ i'_1)(i_3 \ i_2 \ i_1) \\
&= (i_1 \ i_2 \ i'_1)(i'_2 \ i'_1)(i_3 \ i'_3)(i_3 \ i_2 \ i_1) \\
&= (i_1 \ i_2 \ i'_1 \ i'_2)(i'_3 \ i_3 \ i_2 \ i_1) \\
&= (i_1 \ i'_3 \ i_3 \ i'_1 \ i'_2)
\end{aligned}$$

Donc N contient un 5-cycle et est égal à \mathfrak{A}_n par le cas A.

- C. 1. Si σ est un produit de deux transpositions $\sigma = (i_1 \ i_2)(i_3 \ i_4)$, comme $n \geq 5$, on peut prendre $i_5 \notin \text{Supp}(\sigma)$ et $c = (i_1 \ i_2 \ i_5)$, on a alors

$$\begin{aligned}
[c, \sigma] &= (c(i_1) \ c(i_2))(c(i_3) \ c(i_4))(i_1 \ i_2)(i_3 \ i_4) \\
&= (i_2 \ i_5)(i_3 \ i_4)(i_1 \ i_2)(i_3 \ i_4) \\
&= (i_2 \ i_5)(i_1 \ i_2) \\
&= (i_5 \ i_2 \ i_1)
\end{aligned}$$

Donc N contient un 3-cycle et est égal à \mathfrak{A}_n .

2. Si σ est un produit d'au moins 4 transpositions, on a $(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)(i_7 \ i_8) \prod c_i$. On pose $c = (i_2 \ i_3)(i_4 \ i_5)$ et on a

$$\begin{aligned}
[c, \sigma] &= (c(i_1) \ c(i_2))(c(i_3) \ c(i_4))(c(i_5) \ c(i_6))(c(i_7) \ c(i_8))(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)(i_7 \ i_8) \\
&= (i_1 \ i_3)(i_2 \ i_5)(i_4 \ i_6)(i_7 \ i_8)(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)(i_7 \ i_8) \\
&= (i_1 \ i_3)(i_5 \ i_2)(i_2 \ i_1)(i_6 \ i_4)(i_4 \ i_3)(i_5 \ i_6) \\
&= (i_1 \ i_3)(i_5 \ i_2 \ i_1)(i_6 \ i_4 \ i_3)(i_5 \ i_6) \\
&= (i_3 \ i_1 \ i_5 \ i_2)(i_4 \ i_3 \ i_6 \ i_5) \\
&= (i_1 \ i_5 \ i_4)(i_2 \ i_3 \ i_6)
\end{aligned}$$

Donc $[c, \sigma]$ contient des 3-cycles, et $N = \mathfrak{A}_n$ par le cas A. Ceci termine la preuve.