

Pour $n \geq 5$, A_n est simple

Ref: Perrin

Lemme 1: $n \geq 5$, A_n est engendré par les 3 cycles

Lemme 2: $n \geq 5$, les 3 cycles sont conjugués dans A_n .

Lemme 3: Les doubles transpositions sont conjugués dans A_5 .

plan: 1) $n = 5$

2) $n > 5$ en se ramenant au cas $n = 5$.

preuve lemme 1: Soit $\sigma \in A_n$, $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$ ou $n \equiv 0[2]$.

$$\tau_i \circ \tau_j \Rightarrow (ab)(bc) = (abc)$$

$$\Rightarrow (ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$$

preuve lemme 2: A_n agit $(n-2)$ -transitivement sur A_n , par conjugaison?

car si $(a_1, \dots, a_{n-2})$ et $(b_1, \dots, b_{n-2})$ sont deux ensembles à $n-2$ éléments $\neq$

on les complète en $2n$ -uplets: $(a_1, \dots, a_n)$, $(b_1, \dots, b_n)$ qui sont des permutations de $\{1, n\}$

Soit $\sigma \in S_n$ tq $\sigma(a_i) = b_i$

si $\sigma \in A_n$ c'est bon sinon on considère $\sigma \circ (a_{n-1}, a_n)$.

preuve lemme 3: Soient τ et τ' deux doubles transpositions.

$$\tau = (ab)(cd)(e)$$
 et $\tau' = (a'b')(c'd')(e')$

On dispose de $\sigma \in A_n$ tq

$$\begin{aligned} \sigma(a) &= a' \\ \sigma(b) &= b' \\ \sigma(e) &= e'. \end{aligned}$$

soit $\sigma^{-1} \tau \sigma = \tau'$
ou $\sigma \tau \sigma^{-1} = \tau'$

On a alors $\tau' = \sigma \tau \sigma^{-1}$.

1) A_5 a 60 éléments: 1 neutre

15 doubles transpositions

20 3 cycles

24 5-cycles

$$\begin{array}{c} \text{diagramme} \\ (a,b)(c,d) \end{array} \quad \frac{5 \times 4 \times 3 \times 2}{2^3}$$

$$(abc) = (bca) = (cab)$$

3 cycles x 3 choix: 3

$$(abcde) = (bcdea) = \dots = (eabcd)$$

5-cycles x 4 choix x 3 choix x 2 choix: 5

Soit $H \triangleleft A_5$ tq $H \neq \{1\}$.

a) D'après lemme 2, si H contient un 3-cycle, il les contient tous.

b) D'après lemme 3, si H contient une double transposition, il les contient toutes.

c) Si H contient un 5-cycle, il contient le 5-sylow engendré par celui-ci ($60 = 5 \times 12$).

Donc H contient tous les 5-sylow puisqu'ils sont conjugués, donc tous les 5-cycles.

Si H a) $|H| \geq 20 + 1 = 21$

Si H b) $|H| \geq 15 + 1 = 16$

Si H c) $|H| \geq 24 + 1 = 25$

} aucun ne donne $|A_5| = 60$

D'après Legendre ce n'est pas possible.

Donc $|H| \geq 20 + 25 + 1 = 36 \geq \frac{60}{2}$ donc $|H| = 60$

Donc $H = A_5$.

2) Posons $E = [1, n]$.

Soit $H \triangleleft A_n$ la $H \neq \{1\}$. Soit $\sigma \in H \neq 1$

On prend un commutateur $\rho = \tau \sigma \tau^{-1} \sigma^{-1}$ avec $\tau \in A_n$.

D'une part $\rho = \underbrace{(\tau \sigma \tau^{-1})}_{\substack{\in H \\ \text{car } H \triangleleft A_n}} \underbrace{\sigma^{-1}}_{\in H} \in H$.

D'autre part $\rho = \tau(\sigma \tau^{-1} \sigma^{-1})$ produit de deux éléments du type de τ .

Comme $\sigma \neq 1$, on suppose $\sigma(a) = b \neq a$. Choisissons τ partiellement.

Soit $c \in E$ tq $c \neq a, b, \sigma(b)$.

On pose τ le 3-cycle (acb) donc $\tau^{-1} = (abc)$

Donc $\rho = (acb)(\sigma(a), \sigma(b), \sigma(c))$.

Comme $b = \sigma(a)$, $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ est un $\# \leq 5$.

$\rho(F) = F$ et $\rho|_{E-F} = \text{Id}_{E-F}$.

Quitte à rajouter, on suppose, s'il y a des éléments $a \in F$, on peut supposer $|F| = 5$.

Enfin. $\rho \neq 1$ car $\rho(b) = \tau \sigma(b) \neq b$ puisque $\sigma(b) \neq \tau^{-1}(b) = c$.

Soit alors $A(F)$ l'ensemble des permutations paires de F . $A(F) \cong A_5$

qui se plonge dans A_n via $u \mapsto \bar{u}$ avec $\bar{u}|_F = u$; $\bar{u}|_{E-F} = \text{Id}_{E-F}$.

On pose $H_0 = \{u \in A(F), \bar{u} \in H\} = H \cap A(F)$

$H_0 \triangleleft A(F)$ et $\rho|_F \in H_0$ et $\rho|_F \neq \text{Id}_F$.

$A(F)$ est simple donc $H_0 = A(F)$ d'après 1).

Soit alors u un 3-cycle $u \in A(F)$, $u \in H_0$, donc $\bar{u}$ est 3-cycle dans H

Or les 3-cycles sont conjugués dans A_n d'après lemme 2, donc ils sont tous dans H

lemme 1 $\Rightarrow H = A_n$.