$\mathcal{A}_n$ est simple si $n \geq 5$

Théorème : Le groupe $\mathcal{A}_n$ est simple si $n \geq 5$.

Lemme 1 : Les 3-cycles sont conjugués dans $\mathcal{A}_5$.

Lemme 2 : Les doubles-transpositions sont conjuguées dans $\mathcal{A}_5$.

Lemme 3 : Les 3-cycles engendrent $\mathcal{A}_n$ si $n \geq 3$. Il en est de même pour les doubles transpositions.

Lemme 4 : Le groupe $\mathcal{A}_5$ est simple.

Preuve du lemme 1 : Soit (abc) et $(a'b'c')$ deux 3-cycles de $\mathcal{A}_5$. On définit $\sigma \in \mathcal{A}_5$ de sorte que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(c) = c'$. Si cette permutation est dans $\mathcal{A}_5$, on la laisse comme ça. Sinon on la multiplie avec (de) où d et e sont différents de a, b ou c. On vient ainsi de définir $\sigma \in \mathcal{A}_5$ et

$$\sigma(abc)\sigma^{-1} = (\sigma(a)\sigma(b)\sigma(c)) = (a'b'c'). \square$$

Preuve du lemme 2 : Soit $(a_1a_2)(a_3a_4)(a_5)$ et $(b_1b_2)(b_3b_4)(b_5)$ deux doubles-transposition de $\mathcal{A}_5$. On définit σ de sorte que $\sigma(a_i) = b_i$. Si $\sigma \in \mathcal{A}_5$ on la laisse comme ça, sinon on la multiplie par (a_1a_2). Dans tous les cas on a bien

$$\sigma(a_1a_2)(a_3a_4)(a_5)\sigma = (b_1b_2)(b_3b_4)(b_5). \square$$

Preuve du lemme 3 : Soit $\sigma \in \mathcal{A}_5$. On sait que $\mathcal{S}_n$ est engendré par les transpositions donc il existe $l \in \mathbb{N}$ et $\tau_1, ..., \tau_l$ des transpositions telles que

$$\sigma = \prod_{i=1}^{n} \tau_i.$$

Or $1 = \varepsilon(\sigma) = \prod_{i=1}^{n} \varepsilon(\tau_i) = (-1)^l$ donc l est pair. On vient de montrer que A_n est engendré par les doubles transpositions. Comme une double-transposition est produit de 3-cycles, les 3-cycles engendre bien $\mathcal{A}_n$:

$$(xy)(yz) = (xyz)$$
$$(xy)(zt) = (xy)(yz)(yz)(zt) = (xyz)(yzt). \square$$

Preuve du lemme 4 : Soit H un sous-groupe distingué de $\mathcal{A}_5$ différent de $\{\mathrm{Id}\}$. On sait que $\mathcal{A}_5$ est composé de Id, des double-transpositions, des 3-cycles et des 5-cycles. Si H contient une double-transposition ou un 3-cycle, les 3 premiers lemmes impliquent que $H = \mathcal{A}_5$.

Supposons donc que H contienne un 5 cycle noté σ. Comme $\#\mathcal{A}_5 = 60 = 2^2 \times 3 \times 5$ ses 5-Sylow sont de cardinal 5. Comme ils sont conjugués, H doit contenir tous les 5-cycles. En effet, soit σ' un 5-cycle. On note

S_σ (resp. $S_{\sigma'}$) le 5-Sylow qui contient σ (resp. σ'). Comme σ engendre S_σ, $S_\sigma \subset H$. Mais S_σ et $S_{\sigma'}$ sont conjugués par les théorèmes de Sylow donc $S_{\sigma'} \subset H$.

On sait qu'il y a $\dfrac{5!}{5} = 24$ 5-cycles dans $\mathcal{A}_5$ donc H possède au moins 25 éléments (avec le neutre). Mais $\#H|60$ car c'est un sous-groupe donc il faut forcément au moins un autre élément, à savoir un 3-cycle ou une double transposition. Donc $H = \mathcal{A}_5$. $\square$

Preuve du théorème : Soit $n \geq 5$ et H un sous-groupe distingué de $\mathcal{A}_n$ non réduit au neutre. L'idée va être de montrer que H contient un 3-cycle car contient un sous-groupe isomorphe à $\mathcal{A}_5$.

i) <u>Montrons qu'il existe $E \subset \{1, ..., n\}$ et $\varphi \in H$ tels que $\varphi(E) = E$ et $\varphi_{|E^c} = \text{Id}$:</u>

Par hypothèse on peut se donner $\sigma \neq \text{Id}$ et donc $a \in \{1, ..., n\}$ tel que $b := \sigma(a) \neq a$. Comme $n \geq 5$ il existe un élément $c \in \{1, ..., n\}$ différent de a, b et $\sigma(b)$. On pose alors $\tau = (acb)$ et $\varphi = \tau\sigma\tau^{-1}\sigma^{-1}$. Comme H est distingué, $\tau\sigma\tau^{-1} \in H$ et donc $\varphi \in H$. On remarque que $\varphi = (acb)(\sigma(a)\sigma(b)\sigma(c))$.

On définit maintenant $E := \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$. On a alors $\#E \leq 5$ (car $\sigma(a) = b$), $\varphi(E) = E$ et $\varphi_{|E^c} = \text{Id}$. Quitte à rajouter un élément on peut supposer $\#E = 5$.

ii) <u>Montrons que $\mathcal{A}(E)$ est un sous-groupe de H où $\mathcal{A}(E) = \{u \in \mathcal{A}_n : u(E) = E \text{ et } u_{|E^c} = \text{Id}\}$:</u>

Soit $H_0 = H \cap \mathcal{A}(E)$. Montrons que $H_0 = \mathcal{A}(E)$, ce qui permettra de conclure car H_0 est bien un sous-groupe de H. Comme $\mathcal{A}(E)$ est isomorphe à $\mathcal{A}_5$ (on projette sur E) et H_0 est distingué dans $\mathcal{A}(E)$, nécessairement $H_0 = \{\text{Id}\}$ ou $\mathcal{A}_5$. Comme φ est différente de Id, $H_0 \neq \{\text{Id}\}$ donc $H_0 = \mathcal{A}(E)$.

iii) <u>Conclusion :</u>

On vient de voir que $\mathcal{A}(E)$ est un sous-groupe de H isomorphe à $\mathcal{A}_5$ donc contient un 3-cycle, ce qui achève la preuve. $\square$

Remarques importantes :

- Avoir une idée de la preuve pour montrer que les transpositions engendrent $\mathcal{S}_n$
- Avoir en tête l'énoncé exacte des théorèmes de Sylow