Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$

ÉNONCÉ :

Simplicité de $\mathfrak{A}_n$:
Le groupe alterné $\mathfrak{A}_n$ est simple dès que $n \geq 5$.

DÉVELOPPEMENT :

Montrons d'abord deux points résumés dans le lemme qui suit.

LEMME : Soit $n \geq 5$, alors

- $\mathfrak{A}_n$ est exactement le sous-groupe de $\mathfrak{S}_n$ engendré par les 3-cycles.
- Les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Démonstration.

• Notons G le sous-groupe engendré par les 3-cycles. Il est clair que $\mathfrak{A}_n \subset G$.
Réciproquement, soit $\sigma \in \mathfrak{A}_n$ et considérons une décomposition en produit de transpositions $\sigma = \tau_1 \circ \dots \tau_p$ où les $(\tau_i)_{1\leq i\leq p}$ sont distincts deux à deux. Le morphisme signature envoyant σ sur 1, on a nécessairement que p est pair.
En remarquant que pour x, y, z et t deux à deux distincts, on a :

$$(x\ y) \circ (z\ t) = (x\ y\ z) \circ (y\ z\ t) \quad \text{et} \quad (x\ y) \circ (z\ x) = (x\ z\ y)$$

Ainsi, σ s'écrit comme produit d'au plus p 3-cycles. Donc $\sigma \in G$.

• Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ b_3)$ deux trois cycles et $g \in \mathfrak{S}_n$ tel que, pour $i \in \{1, \dots, 3\}$, $g(a_i) = b_i$. Si $g \in \mathfrak{A}_n$, c'est terminé. Sinon, on considère $f := g \circ (x\ y) \in \mathfrak{A}_n$ où $x, y \notin \{a_1, a_2, a_3\}$. □

<u>Revenons-en au théorème</u>.
Considérons un sous-groupe H non trivial de $\mathfrak{A}_n$ (*i.e.* $H \neq \{Id\}$) et soit $\sigma \in H \setminus \{Id\}$. On considère le 3-cycle $\gamma = (x\ z\ y) \in \mathfrak{A}_n$ avec $y = \sigma(x)$ ne commutant pas avec σ.
On pose $\sigma' = \sigma \circ \gamma \circ \sigma^{-1} \circ \gamma^{-1} \in H$ car ce dernier est distingué. En remarquant que

$$\sigma' = (y\ \sigma(z)\ \sigma(y))\sigma(y\ z\ x)$$

est un produit de deux 3-cycles agissant sur $F := \{x, y, z, \sigma(y), \sigma(z)\}$ qui est un ensemble formé d'au plus 5 éléments et fixant tous les autres points.
$\sigma' \neq Id$ car σ et τ ne commutent pas.
Dans $\mathfrak{S}(F)$, la permutation σ' s'écrit comme produit de cycles de supports disjoints qui est la même que dans $\mathfrak{S}_n$. Or, comme $\sigma' \in \mathfrak{A}_n$, il n'y a que 3 possibilités :

- <u>σ' est un 3-cycle</u> : Terminé
- <u>σ' est un produit de 2 transpositions de supports disjoints</u> :
  On a $\sigma' = (x\ y) \circ (z\ t)$. En choisissant $a \in E \setminus \{x, y, z, t\}$, on a :
  $$\sigma" = (x\ a) \circ \sigma' \circ (x\ a) \circ (\sigma')^{-1} = ((x\ a) \circ \sigma' \circ (x\ a)^{-1}) \circ (\sigma')^{-1} \in H$$
  avec $\sigma" = (x\ a\ y)$ et c'est terminé.
- <u>σ' est un 5-cycle</u> :
  Soit $\sigma' = (x\ y\ z\ t\ w)$ et
  $$\sigma" = (x\ y) \circ \sigma' \circ (x\ y) \circ (\sigma')^{-1} = ((x\ y) \circ \sigma' \circ (x\ y)^{-1}) \circ (\sigma')^{-1} \in H$$
  avec $\sigma" = (x\ y\ z)$ et c'est terminé.

Remarques :

- Le développement est relativement court si maîtrisé : il faut prendre le temps de bien expliquer ce que l'on fait.
- $\mathfrak{A}_3$ est trivialement simple quant à $\mathfrak{A}_4$, il n'est pas simple car $D(\mathfrak{A}_4) = \{Id, (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\}$ est distingué, non trivial.
- $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60 (on utilise les théorèmes de SYLOW).
- Il faut connaître et savoir montrer des applications telles que :
  — Les seuls sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geq 5$ sont les triviaux et $\mathfrak{A}_n$.
  — $D(\mathfrak{A}_n) = \mathfrak{A}_n$, $n \geq 5$.
  — Un sous-groupe de $\mathfrak{S}_n$ d'indice n, $n \geq 3$, est isomorphe à $\mathfrak{S}_{n-1}$.