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

**Proposition 1.** *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

*Démonstration.*

Notons $G$ le sous-groupe de $\mathfrak{S}_n$ engendré par les 3-cycles. On a tout d'abord que $G \subseteq \mathfrak{A}_n$ car les 3-cycles ont pour signature 1 donc tous les éléments de $G$ aussi.

Réciproquement, soit $\sigma \in \mathfrak{A}_n$. Considérons un décomposition $\prod_{i=1}^{p} \tau_i$ de $\sigma$ en produit de transpositions. Comme $\sigma$ est de signature 1, on a nécessairement que $p$ est pair. Or, pour $i, j, k, l \in [\![1, n]\!]$ distincts, on a :

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l) \quad \text{et} \quad (i\ j)(k\ i) = (i\ k\ j)$$

Donc le produit de deux transpositions est un 3-cycle, et $\sigma$ s'écrit comme un produit de $\frac{p}{2}$ 3-cycles. Ainsi, $\sigma \in G$. Finalement, on a bien que $G = \mathfrak{A}_n$. □

**Proposition 2.** *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

*Démonstration.*

Les 3-cycles forment une classe de conjugaison dans $\mathfrak{S}_n$. Donc, pour $a, b, c \in [\![1, n]\!]$ distincts et $d, e, f \in [\![1, n]\!]$ distincts, il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f)$. Si $\sigma \in \mathfrak{A}_n$, c'est bon. Sinon, comme $n \geqslant 5$, on peut choisir $i, j \in [\![1, n]\!]$ distincts de $a, b, c$. Alors $\sigma' = \sigma(i\ j)$ un élément de $\mathfrak{A}_n$ tel que $\sigma'(a\ b\ c)\sigma'^{-1} = (d\ e\ f)$.
Les 3-cycles sont donc bien conjugués dans $\mathfrak{A}_n$. □

**Théorème 3.** *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

*Démonstration.*

Soit $H$ un sous-groupe distingué non trivial de $\mathfrak{S}_n$. Par la Proposition 1, il suffit que $H$ contienne les 3-cycles. Par la Proposition 2, il suffit que qu'il n'en continent qu'un. Montrons donc que $H$ contient un 3-cycle.

Soit $\sigma \in H \setminus \{Id\}$. Prenons $a \in [\![1, n]\!]$ tel que $b = \sigma(a) \neq a$. Fixons $c \in [\![1, n]\!]$ distinct de $a, b, \sigma(b)$. C'est possible puisque $n \geqslant 5$. Considérons de plus le 3-cycle $\gamma = (a\ b\ c)$ puis $\sigma_2 = \sigma\gamma\sigma^{-1}\gamma^{-1}$.

On a $\sigma_2 \in H$ car $\sigma \in H$ et $\gamma\sigma^{-1}\gamma^{-1} \in H$. On a également que $\sigma_2 = (b\ \sigma(b)\ \sigma(c))(a\ c\ b)$. On va décomposer $\sigma_2$ en produit de cycles à supports disjoints, en remarquant que $\operatorname{supp}(\sigma_2) \subseteq \{a, b, c, \sigma(b), \sigma(c)\}$ a au plus 5 éléments. Puisque $\sigma_2$ a pour signature 1, en raisonnant sur le type de $\sigma_2$, on peut avoir :

- $[1, 1, 1, 1, 1]$ Si $\sigma_2 = Id$, cela entraîne que $\sigma$ et $\gamma$ commutent, ce qui est faux car $\sigma\gamma(a) = \sigma(b) \neq c = \gamma\sigma(a)$.
- $[2, 2, 1]$ Si $\sigma_2 = (i\ j)(k\ l)$, alors $\sigma_3 = (i\ j\ k\ l\ m)\sigma_2(i\ j\ k\ l\ m)^{-1}\sigma_2^{-1} \in H$ car $H$ est distingué dans $\mathfrak{A}_n$, et on a $\sigma_3 = (i\ j\ k\ l\ m)(j\ i\ l\ k\ m)^{-1} = (i\ k\ m\ l\ j)$, et on se ramène au cas où le type est $[5]$.
- $[3, 1, 1]$ Si $\sigma_2$ est un 3-cycle, c'est bon.
- $[5]$ Si $\sigma_2 = (i\ j\ k\ l\ m)$, alors de même $\sigma_3 = (i\ j\ k)\sigma_2(i\ j\ k)^{-1}\sigma_2^{-1} \in H$, et $\sigma_3 = (i\ j\ k)(j\ l\ k) = (i\ j\ l)$.

Dans tous les cas, on a donc bien trouvé un 3-cycle dans $H$. Ainsi $H = \mathfrak{A}_n$. □

## Références

[Per96] Daniel Perrin. *Cours d'Algèbre.* Ellipses, 1996