Simplicité de $\mathfrak{A}_n$

Théorème
Pour $n = 3$ ou $n \geq 5$ le groupe $\mathfrak{A}_n$ est simple.

Lemme 1
Le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.

Preuve :
On considère le produit de deux transpositions $(ij)(rs)$. Si elles ont un élément un commun le produit est soit l'identité soit un 3-cycle. Si elles n'ont pas d'élément en commun, alors :

$$(ij)(rs) = (ijr)(jrs),$$

donc le produit de deux transpositions est aussi un produit de 3-cycles. Comme une permutation paire est le produit d'un nombre pair de transpositions, le résultat en découle. $\square$

Lemme 2

1. *Si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1, ...a_p)$ et si $\tau \in \mathfrak{S}_n$ alors*

$$\tau\sigma\tau^{-1} = (\tau(a_1), ..., \tau(a_p)).$$

2. *Le groupe $\mathfrak{A}_n$ est $n-2$ transitif : si $a_1, ..., a_{n-2}$ sont distincts et $b_1, ..., b_{n-2}$ sont distincts alors il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$.*

3. *Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Preuve :

1. Si $x \notin \{\tau(a_1), ..., \tau(a_p)\}$ alors $\tau^{-1}(x) \notin \{a_1, ..., a_p\}$ et donc

$$\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$$

   Si $x = \tau(a_i)$ alors $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$.

2. On écrit

$$\{1, ..., n\} = \{a_1, ..., a_{n-2}, a_{n-1}, a_n\} = \{b_1, ..., b_{n-2}, b_{n-1}, b_n\}$$

   et on considère $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i \in [\![1, n]\!]$. Si σ est paire c'est fini, sinon on compose par (a_{n-1}, a_n).

3. Soient $\sigma = (a_1, ..., a_3)$ et $\tau = (b_1, ..., b_3)$ deux trois cycles, puisque $n \geq 5$ il existe, d'après (2), $g \in \mathfrak{A}_n$ telle que $g(a_i) = b_i$. Alors on a $\tau = g\sigma g^{-1}$ d'après (1).

$\square$

Démonstration :
Pour $n=3$, $\mathfrak{A}_n$ est cyclique d'ordre 3 et n'a pas de sous-groupe non trivial.
On suppose $n \geq 5$, et soit N un sous-groupe distingué non trivial de $\mathfrak{A}_n$. Nous allons montrer que $\mathfrak{A}_n$ contient un 3-cycle. Soit $\sigma \in N$, $\sigma \neq \mathrm{Id}$, un élément ayant le nombe maximal de points fixes. Il suffit de montrer que σ est un 3-cycle ou l'identité. On décompose $[\![1,n]\!]$ en orbites disjointes de $\langle\sigma\rangle$. Alors certaines orbites ont plus d'un élément puisque σ n'est pas l'identité. On suppose que toutes les orbites non réduites à un élément ont deux éléments. Comme σ est paire il existe au moins de telles orbites. Sur leur union σ est représentée comme un produit de deux transpositions $(ij)(rs)$. Soient $k \neq i,j,r,s$, $\tau=(rsk)$ et $\sigma'=\tau\sigma\tau^{-1}\sigma^{-1}$. Ainsi σ' est le produit d'un conjugué de σ et de σ^{-1} donc $\sigma' \in N$. Or σ' fixe i et j mais aussi les points fixes de σ distincts de k, donc σ' a plus de points fixes que σ et n'est pas l'identité car $\tau\sigma\tau^{-1} \neq \sigma$, ce qui contredit notre hypothèse.
On est donc réduit au cas où au moins une orbite de $\langle\sigma\rangle$ à plus de 3 éléments $i,j,k,\ldots$. Si σ n'est pas le 3-cycle (i,j,k), elle doit déplacer au moins deux autres éléments de $[\![1,n]\!]$ sinon σ serait une permutation impaire (i,j,k,r), ce qui est impossible. Donc σ déplace r et s en plus de i,j et k. Soit alors $\tau=(krs)$ et $\sigma'=\tau\sigma\tau^{-1}\sigma^{-1}$. Alors $\sigma' \in N$ et $\sigma'(i)=i$, ainsi σ' fixe i et tous les autres points fixes de σ, donc elle a plus de points fixes que σ et n'est pas l'identité car $\tau\sigma\tau^{-1} \neq \sigma$. Contradiction, σ est donc un 3-cycle, ce qui achève la démonstration. □

Détails supplémentaires

Le groupe $\mathfrak{A}_4$ n'est pas simple car $D(\mathfrak{A}_4)$ est un sous-groupe distingué de $\mathfrak{A}_4$ non trivial, isomorphe à V_4 :

$$D(\mathfrak{A}_4)=\{\mathrm{Id},(12)(34),(13)(24),(14)(23)\}$$

Références

- Serge Lang, *Algèbre.*
- Daniel Perrin, *Cours d'algèbre.*
- Jean-Etienne Rombaldi, *Mathématiques pour l'agrégation : Algèbre et géométrie.*