Simplicité de $\mathcal{A}_n$ (où $n \geqslant 5$)

- Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie.*

Lemme 1 : Si $n \geqslant 3$, alors $\mathcal{A}_n$ est engendré par les 3-cycles.

Démonstration. Notons G le sous-groupe engendré par les 3-cycles.
On a bien $G \subset \mathcal{A}_n$ (tous les éléments de G ont pour signature 1).
Soit $\sigma \in \mathcal{A}_n$. Comme $\mathfrak{S}_n$ est engendré par les transpositions alors σ s'écrit comme produit d'un nombre **pair** de transpositions (car $\varepsilon(\sigma) = 1$). Or pour tous $i, j, k, \ell \in [\![1, n]\!]$ distincts,

$$(i\ j)(i\ k) = (i\ k\ j) \qquad \text{et} \qquad (i\ j)(k\ \ell) = (i\ j\ k)(j\ k\ \ell)$$

Donc, le produit de 2 transpositions distinctes est un produit de 3-cycles. Par conséquent, σ s'écrit comme un produit de 3-cycles. Ainsi, $\sigma \in G$. D'où $G = \mathcal{A}_n$. □

Lemme 2 : Si $n \geqslant 5$ alors les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Démonstration. Les 3-cycles sont une classe de conjugaison dans $\mathfrak{S}_n$.
Prenons $(a\ b\ c)$ et $(d\ e\ f)$ deux 3-cycles de $\mathcal{A}_n$.
Donc il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f)$. Si $\sigma \in \mathcal{A}_n$, alors c'est fini.
Supposons que $\sigma \notin \mathcal{A}_n$. Comme $n \geqslant 5$ alors il existe $i, j \notin \{a, b, c\}$ distincts.
On pose $\sigma' = \sigma(i, j) \in \mathcal{A}_n$ et $\sigma'(a\ b\ c)\sigma'^{-1} = (d\ e\ f)$.
Finalement, deux 3-cycles quelconques sont conjugués dans $\mathcal{A}_n$. □

Si $n \geqslant 5$ alors $\mathcal{A}_n$ est simple (i.e. les sous-groupes distingués de $\mathcal{A}_n$ sont $\{\mathrm{Id}\}$ et $\mathcal{A}_n$).

Démonstration. Soit $H \lhd \mathcal{A}_n$ tel que $H \neq \{\mathrm{Id}\}$. Montrons que $H = \mathcal{A}_n$.
Grâce aux lemmes, il suffit de montrer que H possède un 3-cycle. Soit $\sigma \in H \backslash \{\mathrm{Id}\}$.
Alors il existe $a, b \in [\![1, n]\!]$ distincts tels que $\sigma(a) = b$.
Comme $n \geqslant 5$ alors il existe $c \notin \{a, b, \sigma(b)\}$. On pose $\gamma = (a\ b\ c)$ et $\sigma_2 = \sigma\gamma\sigma^{-1}\gamma^{-1}$.
Comme $\gamma \in \mathcal{A}_n$ et $\sigma \in H$ (donc $\sigma^{-1} \in H$) alors $\gamma\sigma^{-1}\gamma^{-1} \in H$ car $H \lhd \mathcal{A}_n$.
Donc le produit $\sigma_2 = \sigma\gamma\sigma^{-1}\gamma^{-1} \in H$. De plus,

$$\sigma_2 = \sigma(a\ b\ c)\sigma^{-1}(a\ c\ b) = (\sigma(a)\ \sigma(b)\ \sigma(c))(a\ c\ b) = (b\ \sigma(b)\ \sigma(c))(a\ c\ b)$$

Donc le support de σ_2 a au plus 5 éléments et $\varepsilon(\sigma_2) = 1$. Il n'y a donc que 4 possibilités :

- $\sigma_2 = \mathrm{Id}$ i.e. $\sigma\gamma = \gamma\sigma$, ce qui est impossible car $\sigma\gamma(a) = \sigma(b) \neq c = \gamma(b) = \gamma\sigma(a)$.
- σ_2 est un 3-cycle. Donc H possède un 3-cycle, ce qui conclut la démonstration.
- σ_2 est le produit de 2 transpositions à supports disjoints : $\sigma_2 = (i\ j)(i\ k)$.
  Prenons $m \notin \{i, j, k, \ell\}$ (licite car $n \geqslant 5$) et posons

$$\sigma_3 = \underbrace{\sigma_2}_{\in H}\ \underbrace{(i\ j\ m)\sigma_2^{-1}(i\ m\ j)}_{\in H \lhd \mathcal{A}_n} = (j\ i\ m)(i\ m\ j) = (i\ j\ m) \in H$$

- σ_2 est un 5-cycle : $\sigma_2 = (i\ j\ k\ \ell\ m)$. On pose

$$\sigma_3 = \underbrace{(i\ j\ k)\sigma_2(i\ k\ j)}_{\in H \lhd \mathcal{A}_n}\ \underbrace{\sigma_2^{-1}}_{\in H} = (i\ j\ k)(j\ \ell\ k) = (i\ j\ \ell) \in H$$

Donc dans tous les cas on trouve un 3-cycle appartenant à H. D'où la simplicité de $\mathcal{A}_n$. □

Remarque.

- $\mathcal{A}_1$ et $\mathcal{A}_2$ sont triviaux donc simples. $\mathcal{A}_3 = \{\mathrm{Id}, (1\ 2\ 3), (1\ 3\ 2)\} \simeq \mathbb{Z}/3\mathbb{Z}$ donc simple.
- $D = \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ le groupe des bi-transpositions est distingué dans $\mathcal{A}_4$, donc il n'est pas simple.
- C'est un résultat fondamental dans la théorie de Galois : $\mathfrak{S}_n$ *est résoluble ssi* $n \leqslant 4$. Si $n \geqslant 5$, la suite $\{\mathrm{Id}\} \lhd \mathcal{A}_n \lhd \mathfrak{S}_n$ est de Jordan-Hölder i.e. les quotients successifs sont des groupes simples.
  Or un groupe fini est résoluble ssi toute suite de Jordan-Hölder a pour quotient uniquement des nombres premiers.
  $\forall n \geqslant 5,\ \mathcal{A}_n$ n'est pas d'ordre premier donc $\mathcal{A}_n/\{\mathrm{Id}\}$ non plus, ainsi $\mathfrak{S}_n$ n'est pas résoluble.
  Pour $n \in \{1, 2, 3\}$, c'est immédiat et pour $n = 4$, $\{\mathrm{Id}\} \lhd D \lhd \mathcal{A}_n \lhd \mathfrak{S}_n$ convient.
  Ainsi les équations polynômiales de degré $\geqslant 5$ ne sont pas résolubles par radicaux (car l'extension de corps associé à un groupe de Galois est isomorphe à $\mathfrak{S}_n$ qui n'est pas résoluble).

Proposition : $\mathfrak{S}_n$ est engendré par les transpositions.

Démonstration. Montrons qu'une permutation est un produit de cycles. Soit $\sigma \in \mathfrak{S}_n$.

- Existence : $[\![1, n]\!] = \bigsqcup_{k=1}^{r} \mathcal{O}_k$ (partition d'orbites). Posons $c_k(i) = \begin{cases} i & \text{si } i \notin \mathcal{O}_k \\ \sigma(i) & \text{si } i \in \mathcal{O}_k \end{cases}$

c_k est un cycle de longueur $\ell_k = \dim \mathcal{O}_k$. Comme les supports des cycles c_k sont disjoints alors $\forall i \in [\![1, n]\!], \exists! k$ tel que $i \in \mathcal{O}_k$ et $c_1 \circ \cdots \circ c_r(i) = c_k(i) = \sigma(i)$. Donc $\sigma = c_1 \circ \cdots \circ c_r$.

- Unicité : Si $\sigma = \tau_1 \circ \cdots \circ \tau_p$. Ainsi, $\mathrm{Supp}(\sigma) = \bigsqcup_{i=1}^{r} \mathrm{Supp}(c_i) = \bigsqcup_{j=1}^{p} \mathrm{Supp}(\tau_j)$.

Ainsi, $\forall k \in [\![1, n]\!],\ \exists! i \in [\![1, r]\!],\ \exists! j \in [\![1, p]\!],\ k \in \mathrm{Supp}(c_i)$ et $k \in \mathrm{Supp}(\tau_j)$. Quitte à renuméroter, on peut supposer $k \in \mathrm{Supp}(c_1) \cap \mathrm{Supp}(\tau_1)$. Donc $\sigma(k) = c_1(k) = \tau_1(k)$ et $\forall N,\ \sigma^N(k) = c_1^N(k) = \tau_1^N(k)$. Donc $c_1 = \tau_1$. En reproduisant ce raisonnement, on obtient $r = p$ et $\forall i \in [\![1, r]\!],\ c_i = \tau_i$.

- Montrons à présent qu'un cycle est un produit de transpositions.

Soit $(x_1, x_2, \ldots, x_r)$ un cycle. $(x_1, x_2, \ldots, x_r) = (x_1, x_2)(x_2, x_3) \ldots (x_{r-1}, x_r)$.

□

Proposition : Tous les 3-cycles sont conjugués dans $\mathfrak{S}_n$.

Démonstration. Soit $\sigma = (x_1\ \ x_2\ \ x_3)$. Soit $\tau \in \mathfrak{S}_n$. Posons $\sigma'' = (\tau(x_1)\ \ \tau(x_2)\ \ \tau(x_3))$.

- Si $x \notin \{x_1, x_2, x_3\}$, alors $\sigma(x) = x$ et $\tau(x) \notin \{\tau(x_1), \tau(x_2), \tau(x_3)\}$, donc $\sigma''(\tau(x)) = \tau(x)$.

Ainsi, $\tau \circ \sigma(x) = \sigma'' \circ \tau(x)$.

- Si $x = x_k$ alors $\tau(\sigma(x)) = \tau(\sigma(x_k)) = \tau(x_{k+1})$ et $\sigma''(\tau(x)) = \sigma''(\tau(x_k)) = \tau(x_{k+1})$. □

Dénombrement des éléments de $\mathcal{A}_5$ ($60 = \frac{5!}{2}$ en tout) :

- le neutre
- $15 = 5 \times \frac{1}{2}\binom{4}{2}$ bitranspositions : on se donne un point fixe (5 possibilités) puis 2 parmi les 4 restants pour former une transposition (l'autre sera déterminée automatiquement). Comme les deux transpositions commutent alors on divise par 2.
- $20 = 2 \times \binom{5}{3}$ cycles de longueur 3 : pour $i, j, k \in [\![1, 5]\!]$, on peut former deux 3-cycles différents $(i\ j\ k)$ et $(i\ k\ j)$.
- $24 = 4 \times 3 \times 2$ cycles de longueur 5 : il n'y a pas de points fixes donc il y a 4 choix pour l'image de 1, 3 pour celle de 2, 2 pour celle de 3.