Simplicité de $\mathcal{A}_n$, $n \geqslant 5$

Référence : Perrin : Cours d'algèbre p. 28, Ulmer : Théorie des groupes p. 73

Lemme 1 (p. 11)

$\mathcal{A}_n$ est engendré par les 3-cycles pour $n \geqslant 3$.

Preuve du Lemme 1

Soit $\sigma \in \mathcal{A}_n$, σ s'écrit comme un produit pair de transposition (car les transpositions engendrent le groupes des permutations et que la signature de σ est 1). Montrons que cette écriture peut se ramener à un produit de 3 cycles.

- $(a\ b)(a\ b) = Id.$
- $(a\ b)(b\ c) = (a\ b\ c)$
- $(a\ b)(a\ c) = (a\ c\ b)$
- $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$

Comme chaque cas consomme deux transpositions, nous avons ce que nous voulions. ■
Au passage, nous avons montré que les cycles d'ordre 3 sont dans $\mathcal{A}_n$.

Les éléments de $\mathcal{A}_5$

$\mathcal{A}_5$ possède 60 éléments. En effet, il y a :

- Le neutre
- 15 élements d'ordre 2 : ce sont les double transpositions disjointes (car une transposition seule a pour signature -1). Il y en a $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ (il faut diviser par 2 car comme elles sont disjointes $\tau_1\tau_2 = \tau_2\tau_1$).)
  Ou sinon on dit $\frac{5 \times 4 \times 3 \times 2}{2 \times 2 \times 2}$ (nombre de choix à inversion près pour chaque transposition (2×2) à inversion près de la transposition totale (2)).
- 20 élements d'ordre 3 : ce sont les 3-cycles. Il y en a $\frac{5 \times 4 \times 3}{3}$ (car on peut changer l'ordre des coefficients dedans). Ou sinon on dit $2\binom{5}{3} = 20$ (penser que les coefficients binomiaux ne prennent pas compte de l'ordre)
- 24 élements d'ordre 5 : $4! = 24$ 5-cycles (on fixe les 4 premiers éléments et le dernier est imposé)

Simplicité de $\mathcal{A}_5$ (Ulmer)

Preuve

Lemme 2

Rappel : $Z_G(h) = \{g \in G | ghg^{-1} = h\} = G_h$ (deuxième égalité le stabilisateur pour l'action par conjugaison).
Soit $\sigma \in \mathcal{A}_n$. Notons $\mathcal{A}_n \cdot \sigma = \{\gamma\sigma\gamma^{-1} | \gamma \in \mathcal{A}_n\}$ la classe de conjugaison (=l'orbite) de σ dans $\mathcal{A}_n$. Et $\mathcal{S}_n \cdot \sigma = \{\gamma\sigma\gamma^{-1} | \gamma \in \mathcal{S}_n\}$ la classe de conjugaison de σ dans $\mathcal{S}_n$.
→ Soit $Z_{\mathcal{S}_n}(\sigma) = Z_{\mathcal{A}_n}(\sigma) \subseteq \mathcal{A}_n$ et donc $|\mathcal{A}_n \cdot \sigma| = \frac{1}{2}|\mathcal{S}_n \cdot \sigma|$.
→ Soit $\exists \alpha \in \mathcal{S}_n \backslash \mathcal{A}_n$ tel que $\alpha\sigma = \sigma\alpha$. Alors $\mathcal{A}_n \cdot \sigma = \mathcal{S}_n \cdot \sigma$ et donc $|\mathcal{A}_n \cdot \sigma| = |\mathcal{S}_n \cdot \sigma|$.

Preuve du Lemme 2

Indication : utiliser les morphismes signatures $\varepsilon_1 : Z_{\mathcal{S}_n} \to \{\pm 1\}$ et $\varepsilon_2 : Z_{\mathcal{A}_n} \to \{\pm 1\}$ ainsi que la relation orbite-stabilisateur.
$\to$ Si ε_1 est trivial, il envoie tout sur 1. Donc $Z_{\mathcal{S}_n}(\sigma) = Z_{\mathcal{A}_n}(\sigma)$.
Relation orbite-stabilisateur (utilisée 2 fois) :

$$|\mathcal{A}_n \cdot \sigma| = \frac{|\mathcal{A}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = \frac{1}{2}|\mathcal{S}_n \cdot \sigma|$$

$\to$ Si ε_1 n'est pas trivial, $\exists \alpha \in Z_{\mathcal{S}_n}(\sigma)$ tel que $\text{sign}(\alpha) = -1$. Et $\text{Id} \in Z_{\mathcal{S}_n}$ est telle que $\text{sign}(\text{Id}) = 1$. Donc $\text{Im}(\varepsilon_1) = \{\pm 1\}$. Le théorème d'isomorphisme donne

$$\frac{|Z_{\mathcal{S}_n}(\sigma)|}{|\text{Ker}(\varepsilon_1)|} = 2$$

Mais $\text{Ker}(\varepsilon_1) = Z_{\mathcal{A}_n}(\sigma)$ donne $2\,|Z_{\mathcal{A}_n}(\sigma)| = |Z_{\mathcal{S}_n}(\sigma)|$. Donc (relation orbite-stabilisateur) :

$$|\mathcal{A}_n \cdot \sigma| = \frac{|\mathcal{A}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{2\,|\mathcal{A}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = \frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = |\mathcal{S}_n \cdot \sigma| \qquad \blacksquare$$

Pour $\sigma \in \mathcal{A}_5$, la classe de conjugaison de σ dans $\mathcal{A}_5$ est soit identique (de même taille) que la classe de conjugaison de σ dans $\mathcal{S}_5$, soit de taille moitié.
De plus, la classe de conjugaison dans $\mathcal{S}_5$ d'un cycle de n'importe quelle taille est l'ensemble des cycles de cette taille (par $\tau(a\ b\ c...)\tau^{-1} = (\tau(a)\ \tau(b)\ \tau(c)...)$).
On réunit les informations :

Type d'éléments de $\mathcal{A}_5$	Cardinal	# de la classe dans $\mathcal{S}_5$	# de la classe dans $\mathcal{A}_5$
Neutre	1	1	Impair donc 1
Double-transposition	15	15	Impair donc 15
3-cycle	20	20	Si $\gamma = (a\ b\ c)$. Avec $(d\ e) \in \mathcal{S}_5 \backslash \mathcal{A}_5$, on a $(d\ e)(a\ b\ c)(d\ e) = (a\ b\ c)$ donc $(d\ e)$ stabilise γ. D'après le **Lemme 2**, $\lvert\mathcal{A}_5 \cdot \gamma\rvert = \lvert\mathcal{S}_5 \cdot \gamma\rvert = 20$
5-cycle	24	24	D'après la formule des classes $\lvert\mathcal{A}_5 \cdot \tau\rvert\,\lvert Z_{\mathcal{A}_5}(\tau)\rvert = \lvert\mathcal{A}_5\rvert = 60$. Or $24 \nmid 60$ donc nécessairement le cardinal est de moitié : 12

Donc les tailles des classes de conjugaison dans $\mathcal{A}_5$ sont 1,12,15 ou 20. Or, un sous-groupe distingué contient l'identité et une union de classe de conjugaison (car s'il a un élément, il a sa classe de conjugaison par définition de distingué). Le cardinal d'un sous-groupe distingué de $\mathcal{A}_5$ divise 60 donc appartient à 1,2,3,4,5,6,10,12,15,20,60. Un sous-groupe distingué de $\mathcal{A}_5$ est forcément le neutre ou $\mathcal{A}_5$.

$n \geqslant 5$ quelconque (Perrin)

Preuve

Posons $E = [\![1, n]\!]$. Soit $H \lhd \mathcal{A}_n \setminus \{Id\}$. Soit $\sigma \in H \setminus \{Id\}$.

Etape 1 Construire un ensemble à 5 éléments, pour cela fabriquer à partir de σ un élément non trivial de H qui n'agisse que sur un ensemble à 5 éléments.
Comme $\sigma \neq Id$, il existe $a \in E$ tel que $b = \sigma(a) \neq a$.
Soit également $c \notin \{a, b, \sigma(b)\}$ et τ le 3-cycle $(a\ c\ b) \in \mathcal{A}_n$. Ainsi, $\tau^{-1} = (a\ b\ c)$. On pose $\rho = (\tau\sigma\tau^{-1})\sigma^{-1} \in H$ comme commutateur $\times$ un élément de H.
On a $\rho = \tau(\sigma\tau^{-1}\sigma^{-1}) = (a\ c\ b)(\sigma(a\ b\ c)\sigma^{-1}) = (a\ c\ b)\,(\sigma(a)\ \sigma(b)\ \sigma(c))$
Comme $b = \sigma(a)$, l'ensemble $F := \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\} = \text{Supp}(\rho)$ a au plus 5 éléments et $\rho|_{E\setminus F} =$

$Id_{E\setminus F}$.

Quitte a rajouter des éléments dans F, on peut supposer que $|F| = 5$.

Etape 2 Trouver un sous-groupe distingué dans cet ensemble.

Soit maintenant $\mathcal{A}(F)$ l'ensemble des permutations paires d'éléments de F. On a $\mathcal{A}(F) \cong \mathcal{A}_5$.
Considérons le morphisme i d'injection de $\mathcal{A}(F)$ dans $\mathcal{A}_n$‘

$$i : \begin{array}{ccc} \mathcal{A}(F) & \to & \mathcal{A}_n \\ u & \mapsto & \bar{u} \end{array}$$

avec $\bar{u}|_F = u$ et $\bar{u}|_{E\setminus F} = Id_{E\setminus F}$ (on a prolongé u par l'identité).

Posons $H_0 = \{u \in \mathcal{A}(F) \mid \bar{u} \in H\}$.
$H_0 \lhd \mathcal{A}(F)$ (car $H \lhd \mathcal{A}_n$, s'écrit bien).

Etape 3 Conclure

De plus, H_0 non réduit à $\{Id\}$ car $\rho|_F \in H_0$. En effet $\rho \in H$ et $\rho \neq Id$ car $\rho(b) = (\tau\sigma\tau^{-1})\sigma^{-1}(b) = (\tau\sigma\tau^{-1})(a) = \tau\sigma(b) \neq \tau(c) = b$ car $c \neq \sigma(b)$.
Comme $\mathcal{A}(F) \cong \mathcal{A}_5$ et $\mathcal{A}_5$ simple, on a $H_0 = \mathcal{A}(F)$.
Donc H_0 contient en particulier un 3-cycle, donc $\bar{u}$ est également un 3-cycle et appartient à H. H contient donc tous les 3-cycles puisque ceux-ci sont conjugués dans $\mathcal{A}_n$.
Or $\mathcal{A}_n$ est engendré par les 3-cycles, et finalement $H = \mathcal{A}_n$. ■

Bonus

Proposition

$\mathcal{A}_n$ est $(n-2)$-transitif sur $[\![1, n]\!]$ ie si on a $a_1, \ldots, a_{n-2}$ distincts et $b_1, \ldots, b_{n-2}$ distincts, il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$.

Preuve

On écrit $[\![1, n]\!] = \{a_1, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, \ldots, b_{n-2}, b_{n-1}, b_n\}$.
On considère $\tau \in \mathcal{S}_n$ telle que $\tau(a_i) = b_i$. Si τ est paire, c'est terminé. Sinon, on compose τ avec la transposition $(a_{n-1}\ a_n)$, cela nous donne σ. ■

Notes :

✓ **A l'oral**, $n = 5$: 7'40 puis 8'34. Quand on dénombre $\mathcal{A}_5$ on commence déjà le tableau. Tout : 14'16 au feutre en speedant. Développement à retravailler car dur ! En speedant 6'05 pour $\mathcal{A}_5$ et 12'40 au total. Donc on peut aller un peu plus doucement.
✓ La signature c'est $(-1)^{\text{nombre de transpositions}}$ lorsqu'on a décomposé en produit de transpositions (non forcément disjointes).