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

Leçons : 101, 103, 104, 105, 108

[Ulm], exercices 7.10-11
[Per], théorème 8.1

Théorème

Soit $n \in \mathbb{N}$, $n \geqslant 5$.
$\mathfrak{A}_n$ est simple.

Démonstration :

Étape 1 : Montrons que $\mathfrak{A}_5$ est simple.
Soit $H \triangleleft \mathfrak{A}_5$, H est réunion de classes de conjugaison dans $\mathfrak{A}_5$.
On connait les classes de conjugaison dans $\mathfrak{S}_5$, déduisons-en celles de $\mathfrak{A}_5$.

Lemme

Soit $n \in \mathbb{N}$, $G = \mathfrak{A}_n$ ou $\mathfrak{S}_n$.
On note $\sigma^G = \left\{\gamma\sigma\gamma^{-1} \middle| \gamma \in G\right\}$ et $\mathrm{Z}_G(\sigma) = \left\{\gamma \in G \middle| \gamma\sigma\gamma^{-1} = \sigma\right\}$ où $\sigma \in \mathfrak{A}_n$.
On a deux cas :
- Soit $\#\sigma^{\mathfrak{A}_n} = \dfrac{1}{2}\#\sigma^{\mathfrak{S}_n}$ et $\mathrm{Z}_{\mathfrak{A}_n}(\sigma) = \mathrm{Z}_{\mathfrak{S}_n}(\sigma)$;
- Soit $\sigma^{\mathfrak{A}_n} = \sigma^{\mathfrak{S}_n}$ et $\exists \alpha \in \mathfrak{S}_n \backslash \mathfrak{A}_n, \alpha\sigma\alpha^{-1} = \sigma$.

Démonstration :
On considère $\tilde{\varepsilon} : \left| \begin{array}{ccc} \mathrm{Z}_{\mathfrak{S}_n}(\sigma) & \to & \{\pm 1\} \\ \gamma & \mapsto & \varepsilon(\gamma) \end{array}\right.$. On a donc deux cas :
- Soit $\tilde{\varepsilon}$ est trivial, alors $\mathrm{Z}_{\mathfrak{S}_n}(\sigma) \subseteq \mathfrak{A}_n$ et par suite $\mathrm{Z}_{\mathfrak{S}_n}(\sigma) = \mathrm{Z}_{\mathfrak{A}_n}(\sigma)$.
  Par la relation orbite-stabilisateur pour l'action de conjugaison :
  $$\#\mathfrak{S}_n = \#\mathrm{Z}_{\mathfrak{S}_n}(\sigma) \times \#\sigma^{\mathfrak{S}_n} \text{ et } \#\mathfrak{A}_n = \#\mathrm{Z}_{\mathfrak{A}_n}(\sigma) \times \#\sigma^{\mathfrak{A}_n} \text{ d'où } \#\sigma^{\mathfrak{A}_n} = \frac{1}{2}\#\sigma^{\mathfrak{S}_n}.$$
- Soit $\tilde{\varepsilon}$ est non-trivial et $\mathrm{Z}_{\mathfrak{A}_n}(\sigma) = \mathrm{Ker}\ \tilde{\varepsilon}$ est d'indice 2 dans $\mathrm{Z}_{\mathfrak{S}_n}(\sigma)$.
  Ainsi, il existe $\alpha \in \mathfrak{S}_n \backslash \mathfrak{A}_n$, tel que $\alpha\sigma\alpha^{-1} = \sigma$.
  De plus, la relation orbite-stabilisateur donne ici : $\#\sigma^{\mathfrak{A}_n} = \#\sigma^{\mathfrak{S}_n}$ d'où $\sigma^{\mathfrak{A}_n} = \sigma^{\mathfrak{S}_n}$. ∎

D'après le lemme, au passage de $\mathfrak{S}_5$ à $\mathfrak{A}_5$, les classes de conjugaison sont soit conservées, soit coupées en deux. On construit alors le tableau suivant :

Classes dans $\mathfrak{S}_5$	Cardinaux dans $\mathfrak{S}_5$	Passage dans $\mathfrak{A}_5$
Id	1	Conservée car de cardinal impair
$(a\ b\ c)$	20	Conservée car $(d\ e)(a\ b\ c)(d\ e)^{-1} = (a\ b\ c)$
$(a\ b)(c\ d)$	15	Conservée car de cardinal impair
$(a\ b\ c\ d\ e)$	24	Coupée car $24 \nmid 60$ (relation orbite-stabilisateur)

Or H est réunion de classes de conjugaison, contient Id et vérifie $\#H \mid 60$ (théorème de Lagrange).
Ainsi, on conclut assez rapidement que $\#H \in \{1, 60\}$ et donc $\mathfrak{A}_5$ est simple. [1]

Étape 2 : Déduisons-en que $\mathfrak{A}_n$ est simple pour tout $n \geqslant 5$.
Soit $H \triangleleft \mathfrak{A}_n$, $H \neq \{\mathrm{Id}\}$.
Soit $\sigma \in H \backslash \{\mathrm{Id}\}$ et $a \in [\![1, n]\!]$ tel que : $a \neq \sigma(a) =: b$.

1. On peut faire autrement ici (on ne le fera pas, parce que c'est plus long même si c'est plus rigolo). $\mathfrak{A}_5$ admet 5 classes de conjugaison donc 5 caractères irréductibles : de degrés 1 (pour la représentation triviale), d_2, d_3, d_4 et d_5. On a : $60 = 1 + d_2^2 + d_3^2 + d_4^2 + d_5^2$, et on en déduit (en essayant de manière exhaustive, c'est bon hein, 59 c'est pas la mort non plus), que $d_2 = d_3 = 3$, $d_4 = 4$ et $d_5 = 5$. Soit $\mathcal{C}$ une classe de conjugaison de $\mathfrak{A}_5$. $\mathbb{1}_{\mathcal{C}}$ étant une fonction centrale, on obtient :
$$\mathbb{1}_{\mathcal{C}} = \textstyle\sum_{i=1}^5 \langle \mathbb{1}_{\mathcal{C}}, \chi_i\rangle \chi_i = \frac{1}{\#G} \sum_{i=1}^5 \sum_{g \in G} \mathbb{1}_{\mathcal{C}}(g)\overline{\chi_i(g)}\chi_i = \frac{\#\mathcal{C}}{\#G} \sum_{i=1}^5 \overline{\chi_i(\mathcal{C})}\chi_i.$$
Et donc $1 = \frac{\#\mathcal{C}}{\#G} \sum_{i=1}^5 |\chi_i(\mathcal{C})|^2$. Finalement, $\sum_{i=1}^5 |\chi_i(\mathcal{C})|^2 = \frac{\#G}{\#\mathcal{C}}$. Supposons maintenant que $\mathcal{C} \neq \{\mathrm{Id}\}$, et donc $\frac{\#G}{\#\mathcal{C}} \leqslant 5$, donc $\forall i \in [\![2, 5]\!], |\chi_i(\mathcal{C})| < 3 \leqslant \chi_i(\mathrm{Id})$. Donc $\forall i \in [\![2, 5]\!], \mathrm{Ker}\ \chi_i = \{\mathrm{Id}\}$. Donc les seuls sous-groupes distingués de $\mathfrak{A}_5$ sont $\mathfrak{A}_5$ et $\{\mathrm{Id}\}$, donc $\mathfrak{A}_5$ est simple.

Soit $c \notin \{a, b, \sigma(b)\}$, et $\tau = (a\ c\ b)$ et $\tau^{-1} = (a\ b\ c)$.
On définit $\rho = \underbrace{\tau\sigma\tau^{-1}}_{\in H}\underbrace{\sigma^{-1}}_{\in H} = \tau\left(\sigma\tau^{-1}\sigma^{-1}\right) = (a\ b\ c)(\sigma(a)\ \sigma(b)\ \sigma(c)) \in H$.
Donc supp $\rho = \{a, b, c, \sigma(b), \sigma(c)\}$, d'où # supp $\rho \leqslant 5$.
Aussi $\rho \neq \mathrm{Id}$ car $\rho(b) = \tau\sigma\tau^{-1}(a) = \tau\sigma(b) \neq b$ car $\sigma(b) \neq c = \tau^{-1}(b)$.
Soit alors $E \subseteq [\![1, n]\!]$, avec $E \supseteq$ supp ρ et $\#E = 5$.
On définit l'injection $i : \left| \begin{array}{ccc} \mathfrak{A}(E) & \to & \mathfrak{A}_n \\ u & \mapsto & \overline{u} \end{array} \right.$ où $\overline{u}_{|E} = u$ et $\overline{u}_{|E^C} = \mathrm{Id}$.
Soit $H' = i^{-1}(H)$; i est un morphisme de groupes et donc $H' \triangleleft \mathfrak{A}(E)$.
Or $\rho_{|E} \neq \mathrm{Id}$ et $\rho_{|E} \in H'$ car $\rho \in H$.
Ainsi, $H' = \mathfrak{A}(E)$ car $\mathfrak{A}(E) \simeq \mathfrak{A}_5$ est simple.
Soit alors v un 3-cycle de $\mathfrak{A}(E)$; $\overline{v} \in H$ et $\overline{v}$ est un 3-cycle de $\mathfrak{A}_n$.
Comme on l'a vu précédemment, pour $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
Donc H contient tous les 3-cycles ; mais ils engendrent $\mathfrak{A}_n$!
Finalement, $H = \mathfrak{A}_n$ et donc $\mathfrak{A}_n$ est simple. ■

Références

[Ulm] F. ULMER – *Théorie des groupes*, Ellipses, 2012.
[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.