Développement 1. Simplicité du groupe alterné $\mathfrak{A}_n$ lorsque $n \geqslant 5$

Lemme 1. Le groupe $\mathfrak{A}_5$ est simple.

Preuve Tout d'abord, comptons le nombre d'éléments du groupe $\mathfrak{A}_5$ classés selon leurs ordres : on trouve

- le neutre ;
- $15 = \frac{5\times 4}{2} \times \frac{3\times 2}{2} \times \frac{1}{2}$ éléments d'ordre 2 (ce sont les produits de deux transpositions dont les supports sont disjoints) ;
- $20 = \frac{5\times 4\times 3}{3}$ éléments d'ordre 3 (ce sont les 3-cycles) ;
- $24 = 5! - 1 - 15 - 20$ éléments d'ordre 5.

Comme énoncé, les éléments d'ordre 3 sont conjugués dans $\mathfrak{A}_5$. C'est également le cas pour les éléments d'ordre 2 puisque, si $\tau := (a\ b)(c\ d)(e)$ et $\tau' := (a'\ b')(c'\ d')(e')$ sont deux transpositions de $\mathfrak{A}_5$, alors la 3-transitivité de l'action de $\mathfrak{A}_5$ sur $[\![1,5]\!]$ assure qu'il existe une permutation $\sigma \in \mathfrak{A}_5$ telle que

$$\sigma(a) = a', \quad \sigma(b) = b' \quad \text{et} \quad \sigma(e) = e'$$

et on peut alors écrire $\tau' = \sigma\tau\sigma^{-1}$.

Soit $H \leqslant \mathfrak{A}_5$ un sous-groupe distingué non trivial. On veut montrer que $H = \mathfrak{A}_5$. S'il contient un élément d'ordre 3 (respectivement 2), alors il les contient tous d'après le précédent paragraphe. S'il contient un élément d'ordre 5, alors il contient le 5-sous-groupe de Sylow engendré par cet élément, donc tous les 5-sous-groupes de Sylow — ces derniers étant conjugués — et donc tous les éléments d'ordre 5. Comme les entiers $24+1$, $20+1$ et $15+1$ ne divisent pas $|\mathfrak{A}_5| = 60$ et grâce au théorème de Lagrange, le sous-groupe H contient au moins deux des trois types d'éléments de telle sorte que $|H| \geqslant 1 + 15 + 20 = 36$. D'où $|H| = 60$, soit $H = \mathfrak{A}_5$. ◁

Théorème 2. Soit $n \geqslant 5$ un entier. Alors le groupe $\mathfrak{A}_n$ est simple.

Preuve On suppose désormais $n > 5$. Soit $H \leqslant \mathfrak{A}_5$ un sous-groupe distingué non trivial. Soit $\sigma \in H \setminus \{\mathrm{Id}_{[\![1,n]\!]}\}$. Comme $\sigma \neq \mathrm{Id}_{[\![1,n]\!]}$, on peut trouver un élément $a \in [\![1,n]\!]$ tel que $b := \sigma(a) \neq a$. Soit $c \in [\![1,n]\!] \setminus \{a, b, \sigma(b)\}$. Considérons le 3-cycle $\tau := (a\ c\ b)$ d'inverse $\tau^{-1} = (a\ b\ c)$ et la permutation

$$\rho := \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$, l'ensemble $F := \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments. De plus, on a

$$\rho(F) = F \quad \text{et} \quad \rho|_{[\![1,n]\!]\setminus F} = \mathrm{Id}_{[\![1,n]\!]\setminus F}\,.$$

Quitte à rajouter des éléments à l'ensemble F, on peut supposer qu'il est de cardinal 5. Enfin, remarquons que $\rho \neq \mathrm{Id}$ car, comme $\sigma(b) \neq c = \tau^{-1}(b)$, on a

$$\rho(b) = \tau\sigma\tau^{-1}\sigma^{-1}(b) = \tau\sigma\tau^{-1}(a) = \tau\sigma(b) \neq \tau(c) = b.$$

Avec ces différentes remarques, le groupe alterné $\mathfrak{A}(F)$ est isomorphe à $\mathfrak{A}_5$ et se plonge dans $\mathfrak{A}_n$ par l'application $u \longmapsto \overline{u}$ où, pour chaque permutation $u \in \mathfrak{A}(F)$, on définit la permutation $\overline{u} \in \mathfrak{A}_n$ par les égalités

$$\overline{u}|_F = u \quad \text{et} \quad \overline{u}|_{[\![1,n]\!]\setminus F} = \mathrm{Id}_{[\![1,n]\!]\setminus F}\,.$$

Le groupe $H_0 := \{u \in \mathfrak{A}(F) \mid \overline{u} \in H\} = H \cap \mathfrak{A}(F)$ est distingué dans $\mathfrak{A}(F)$ et on a

$$\rho|_F \in H_0 \quad \text{et} \quad \rho|_F \neq \mathrm{Id}_F, \quad \text{c'est-à-dire} \quad \rho|_F \in H_0 \setminus \{\mathrm{Id}_F\}\,.$$

Grâce au lemme, le groupe $\mathfrak{A}(F) \simeq \mathfrak{A}_5$ est distingué ce qui impose $H_0 = \mathfrak{A}(F)$.

Soit $u_0 \in \mathfrak{A}(F)$ un 3-cycle. Alors la permutation $\overline{u} \in H$ est encore un 3-cycle. Les 3-cycles étant conjugués dans $\mathfrak{A}_n$ et le sous-groupe H étant distingué, ce dernier contient tous les 3-cycles. Enfin, comme les 3-cycles engendrent le groupe $\mathfrak{A}_n$, on en déduit $H = \mathfrak{A}_n$. ◁

Précision

Dans la preuve du lemme, on peut se passer du théorème de Sylow pour montrer que, si un sous-groupe distingué $H \triangleleft \mathfrak{A}_5$ contient un 5-cycle, alors il les contient tous.

Soient $\tau, \tau' \in \mathfrak{S}_5$ deux 5-cycles. Alors il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $\tau' = \sigma\tau\sigma^{-1}$. On suppose que $\tau \in H$. On veut montrer que $\tau' \in H$. Distinguons deux cas. Si $\sigma \in \mathfrak{A}_5$, c'est plié ! On suppose que $\sigma \notin \mathfrak{A}_5$. Notons $\tau = (a\ b\ c\ d\ e)$. Comme $\tau^2 = (a\ c\ e\ b\ d)$, en notant $\rho := (b\ c\ e\ d)$, on a $\rho\tau\rho^{-1} = \tau^2$ de telle sorte que

$$\tau' = \tilde{\sigma}\tau^2\tilde{\sigma}^{-1} \quad \text{avec} \quad \tilde{\sigma} := \sigma\rho^{-1} \in \mathfrak{A}_5.$$

Comme $\tau^2 \in H$, cela montre que $\tau' \in H$.

Application

Corollaire 3. Soit $n \geqslant 5$ un entier. Alors le seul sous-groupe distingué non trivial et propre de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.

Preuve Soit H un sous-groupe distingué de $\mathfrak{S}_n$. Alors le sous-groupe $H \cap \mathfrak{A}_n$ est distingué dans $\mathfrak{A}_n$. Grâce au théorème, on en réduit à traiter les deux points suivants.

- Si $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, alors $H \supset \mathfrak{A}_n$ et, pour des raisons d'ordre, on a $H \in \{\mathfrak{A}_n, \mathfrak{S}_n\}$.
- On suppose $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$. Alors la signature induit un isomorphisme
$$\varepsilon \colon H \longrightarrow \varepsilon(H) \subset \{\pm 1\}$$
ce qui assure l'inégalité $|H| \leqslant 2$. Raisonnons par l'absurde et supposons que $|H| = 2$. On note alors $H = \{\mathrm{Id}, \sigma\}$ avec $\sigma \in \mathfrak{A}_n \setminus \{\mathrm{Id}\}$. Pour toute permutation $\tau \in \mathfrak{S}_n$, la distinction donne $\tau\sigma\tau^{-1} \in H$ et, comme $\tau\sigma\tau^{-1} \neq \mathrm{Id}$, on en déduit $\tau\sigma\tau^{-1} = \sigma$ ce qui montre $\sigma \in \mathrm{Z}(\mathfrak{S}_n)$. Le centre de $\mathfrak{S}_n$ étant trivial, cela conduit à une contradiction. D'où $|H| = 1$, soit $H = \{\mathrm{Id}\}$. ◁

[1] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.