

Simplicité du groupe alterné $\mathfrak{A}_n$ pour $n = 3$ ou $n \geq 5$

Référence :

- Jean-Etienne Rombaldi : *Algèbre et Géométrie*, pages 49, 50-51 et 65

Couplé avec les leçons : 103, 104, 105, 108

Théorème :

Le groupe alterné $\mathfrak{A}_n$ est simple lorsque $n = 3$ ou $n \geq 5$.

Lemmes :

- Lemme 1 : Soient $(\tau_1, \tau_2) \in \mathfrak{S}_n$ deux transpositions, alors $\tau_1\tau_2$ est un produit de 3-cycles.
- Lemme 2 : Pour $n \geq 5$, les 3-cycles engendrent $\mathfrak{A}_n$.
- Lemme 3 : Pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Preuve :

1) *Preuve du Lemme 1* :

Soient $(\tau_1, \tau_2) \in \mathfrak{S}_n$, on distingue trois cas suivant les supports de ces transpositions :

- si $\tau_1 = \tau_2$, alors $\tau_1\tau_2 = id = \gamma^3$, pour n'importe quel 3-cycle $\gamma \in \mathfrak{S}_n$.
- si leur intersection est restreinte à un singleton, i.e. $\text{Supp}(\tau_1) \cap \text{Supp}(\tau_2) = \{x\}$,
on a alors $y, z \in \llbracket 1, n \rrbracket \setminus \{x\}$ avec $y \neq z$ tels que $\tau_1 = (xy)$ et $\tau_2 = (xz)$.
Ainsi $\tau_1\tau_2 = (xy)(xz) = (xzy)$ un 3-cycle.
- si $\text{Supp}(\tau_1) \cap \text{Supp}(\tau_2) = \emptyset$,
on a alors $x, y, z, t \in \llbracket 1, n \rrbracket$ tous distincts tels que $\tau_1 = (xy)$ et $\tau_2 = (zt)$.
On obtient $\tau_1\tau_2 = (xy)(zt) = (xy)(yz)(yz)(zt) = (xyz)(yzt)$ un produit de deux 3-cycles.

2) *Preuve du Lemme 2* :

Soit $n \geq 5$. On sait que les transpositions engendrent $\mathfrak{S}_n$ donc engendrent aussi $\mathfrak{A}_n$.

Soit $\sigma \in \mathfrak{A}_n$, il existe $r \in \mathbb{N}^n$ et $(\tau_i)_{1 \leq i \leq r}$ tels que $\sigma = \prod_{i=1}^r \tau_i$

Or pour tout $i \in \llbracket 1, r \rrbracket$, on a $\epsilon(\tau_i) = -1$ et $\epsilon(\sigma) = 1$ donc $(-1)^r = 1$.

Par conséquent, r est pair ($\neq 0$). En regroupant deux par deux les transpositions de la décomposition de σ , on a un produit de 3-cycles d'après le Lemme 1. Finalement, les 3-cycles engendrent tous les éléments de $\mathfrak{A}_n$.

3) *Preuve du Lemme 3 :*

Soient $n \geq 5$ et $\gamma = (x_1 x_2 x_3), \gamma' = (x'_1 x'_2 x'_3)$ deux 3-cycles de $\mathfrak{A}_n$.

On sait que γ et γ' sont conjugués dans $\mathfrak{S}_n$. Il existe donc $\sigma \in \mathfrak{S}_n$ tel que pour $i \in \{1, 2, 3\}$, $\sigma(x_i) = x'_i$ et $\gamma' = \sigma \gamma \sigma^{-1}$.

— Si $\sigma \in \mathfrak{A}_n$, on a fini.

— Sinon, on considère $x_4, x_5 \in \llbracket 1, n \rrbracket \setminus \{x_1, x_2, x_3\}$ et $\sigma' := \sigma(x_4 x_5) \in \mathfrak{A}_n$ (car de signature 1). On a alors bien pour tout $i \in \{1, 2, 3\}$, $\sigma'(x_i) = x'_i$ et on se ramène au cas précédent.

4) *Preuve du théorème :*

Pour $n = 3$, $\mathfrak{A}_3$ est d'ordre 3 donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ (d'après la structure des "petits" groupes) qui est donc simple.

Soient $n \geq 5$ et $H \neq \{id\}$ un sous-groupe distingué de $\mathfrak{A}_n$. Montrons que H contient un 3-cycle.

Soient $\sigma \in H \setminus \{id\}$ et $\gamma = (xzy) \in \mathfrak{A}_n$ tels que $\sigma(x) = y$ et $z \notin \{x, y, \sigma^{-1}(x)\}$.

On remarque que $\gamma \sigma(x) = \gamma(y) = x$ et $\sigma \gamma(x) = \sigma(z) \neq x$ donc γ et σ ne commutent pas. On considère leur commutateur : $\sigma' := \sigma \gamma \sigma^{-1} \gamma^{-1} \neq id$

Puisque $\sigma \in H$ et H est un sous-groupe distingué de $\mathfrak{A}_n$, on a $\gamma \sigma^{-1} \gamma^{-1} \in H$ donc $\sigma' \in H$.

Et on a

$$\sigma' = (\sigma \gamma \sigma^{-1}) \gamma^{-1} = (\sigma(x) \sigma(z) \sigma(y)) (y z x) = (y \sigma(z) \sigma(y)) (y z x) \neq id$$

σ' est produit de deux 3-cycles qui agissent sur $F := \{x, y, z, \sigma(y), \sigma(z)\}$ avec $|F| \leq 5$. Dans $\mathfrak{S}(F)$, σ' se décompose en produit de cycles à supports disjoints (*la "même" que dans $\mathfrak{S}_n$*). Puisque σ' est de signature 1 et agit sur au plus 5 éléments, nous n'avons que trois possibilités : σ' est soit un (i) 3-cycle, soit (ii) un produit de deux transpositions à supports disjoints, soit (iii) un 5-cyle.

— (i) Si σ' est un 3-cycle, alors H contient un 3-cycle.

— (ii) Si $\sigma' = (x_1 x_2)(x_3 x_4)$ alors on prend $x_5 \in \llbracket 1, n \rrbracket \setminus \{x_1, x_2, x_3, x_4\}$ et on considère $\rho := (x_1 x_2 x_5) \in \mathfrak{A}_n$.

Alors (*par le même raisonnement que précédemment*) $\sigma'' := \sigma' \rho (\sigma')^{-1} \rho^{-1} \in H \setminus \{id\}$

On a $\sigma'' = (\sigma' \rho (\sigma')^{-1}) \rho^{-1} = (\sigma'(x_1) \sigma'(x_2) \sigma'(x_5)) (x_5 x_2 x_1) = (x_2 x_1 x_5) (x_5 x_2 x_1) = (x_1 x_2 x_5)$

Donc H contient un 3-cycle.

— (iii) Si $\sigma' = x_1 x_2 x_3 x_4 x_5$, alors on considère $\rho = (x_1 x_2 x_3)$ et

$\sigma'' = (\sigma' \rho (\sigma')^{-1}) \rho^{-1} = (\sigma'(x_1) \sigma'(x_2) \sigma'(x_3)) (x_3 x_2 x_1) = (x_2 x_3 x_4) (x_3 x_2 x_1) = (x_1 x_4 x_2) \in H$

Dans tous les cas, H contient un 3-cyle et est stable par conjugaison. Par le Lemme 3 il contient donc tous les 3-cycles et par le Lemme 2, $H = \mathfrak{A}_n$. Ainsi les seuls sous-groupes distingués de $\mathfrak{A}_n$ sont $\{id\}$ et lui-même, c'est un groupe simple.

□