

## Simplicité de $A_n$ pour $n \geq 5$

On montre que  $A_n$  est simple pour  $n \geq 5$  en montrant dans un premier temps le cas  $n = 5$ , puis en s'y ramenant.

**Lemme 1.** Les 3-cycles sont conjugués dans  $A_n$  pour  $n \geq 5$ .

[PER]  
p. 15

*Démonstration.* Soient  $\alpha = (a_1 \ a_2 \ a_3)$  et  $\beta = (b_1 \ b_2 \ b_3)$  deux 3-cycles. Soit  $\sigma \in S_n$  telle que

$$\forall i \in \llbracket 1, 3 \rrbracket, \sigma(a_i) = b_i$$

On a deux possibilités pour  $\sigma$  :

- $\sigma$  est paire. Alors  $\sigma \in A_n$ , et le résultat est démontré pour  $\alpha$  et  $\beta$ .
- $\sigma$  est impaire. Comme  $n \geq 5$ , il existe  $c_1, c_2$  tels que  $c_1, c_2 \notin \{b_1, b_2, b_3\}$ . On pose alors  $\tau = (c_1 \ c_2)$ , et on a

$$(\tau\sigma)(a_1 \ a_2 \ a_3)(\tau\sigma)^{-1} = (b_1 \ b_2 \ b_3)$$

avec  $\tau\sigma$  paire. Le résultat est encore démontré pour  $\alpha$  et  $\beta$ .

□

**Lemme 2.** Le produit de deux transpositions est un produit de 3-cycles.

[ROM21]  
p. 49

*Démonstration.* Soient  $\alpha = (a_1 \ a_2)$  et  $\beta = (b_1 \ b_2)$  deux transpositions. Si  $\alpha = \beta$ , alors  $\alpha\beta = \text{id} = \sigma^3$  où  $\sigma$  désigne n'importe quel 3-cycle.

Si  $\alpha \neq \beta$ , on a deux possibilités :

- Leur support comporte un élément commun :  $a_1 = b_1 = c$ . Donc  $\alpha = (c \ a_2)$  et  $\beta = (c \ b_2)$  avec  $c, a_2, b_2$  distincts. Donc  $\alpha\beta = (a_2, c, b_2)$ .
- Leur support n'a pas d'élément commun. Dans ce cas  $a_1, a_2, a_1, b_2$  sont distincts et  $\alpha\beta = (a_1 \ a_2 \ b_1)(a_2 \ b_1 \ b_2)$ .

□

**Lemme 3.**  $A_n$  est engendré par les 3-cycles pour  $n \geq 3$ .

*Démonstration.* Soit  $\sigma \in A_n$ . Comme  $\sigma$  est paire, on peut la décomposer en un produit d'un nombre pair  $n$  de transpositions :

$$\sigma = \prod_{i=1}^{n-1} \tau_i \tau_{i+1}$$

Par le Lemme 1, chaque produit  $\tau_i \tau_{i+1}$  peut s'écrire comme un produit de 3-cycles. Donc  $\sigma$  est bien un produit de 3-cycles.

□

**Lemme 4.**  $A_5$  est simple.

*Démonstration.* Commençons par décrire les types possibles des permutations de  $A_5$  (le “type” d’une permutation désigne les cardinaux des supports des cycles apparaissant dans sa décomposition en cycles disjoints).

Type de permutation	Nombre de permutations
[1]	1
[3]	$\frac{5 \times 4 \times 3}{3} = 20$
[5]	$\frac{5 \times 4 \times 3 \times 2 \times 1}{5} = 24$
[2,2]	$\frac{1}{2} \frac{5 \times 4 \times 3 \times 2}{4} = 15$

Montrons que les permutations de type [2,2] sont conjuguées dans  $A_5$ . Soient  $\alpha = (a_1 \ b_1)(c_1 \ d_1)(e_1)$  et  $\beta = (a_2 \ b_2)(c_2 \ d_2)(e_2)$  deux permutations de type [2,2]. Il suffit de prendre  $\sigma \in A_5$  telle que  $\sigma(a_1) = a_2, \sigma(b_1) = b_2$  et  $\sigma(e_1) = e_2$  pour avoir  $\sigma \alpha \sigma^{-1} = \beta$ .

Soit  $H \triangleleft A_5$  tel que  $H \neq \{\text{id}\}$ . Montrons que  $H = A_5$ .

- Si  $H$  contient une permutation de type [2,2], alors par le Lemme 2, le Lemme 1, il les contient toutes.
- Si  $H$  contient une permutation de type [3], alors par le Lemme 1, il les contient toutes.
- Si  $H$  contient une permutation de type [5],  $\sigma = (a \ b \ c \ d \ e)$ , il contient alors le commutateur

$$\begin{aligned} (a \ b \ c) \sigma (a \ b \ c)^{-1} \sigma^{-1} &= (a \ b \ c) \sigma (c \ b \ a) \sigma^{-1} \\ &= (a \ b \ c) (\sigma(c) \ \sigma(b) \ \sigma(a)) \\ &= (a \ b \ c) (d \ c \ b) \\ &= (b \ d \ a) \end{aligned}$$

qui est un 3-cycle. Par le Lemme 1, il les contient tous.

Or,  $H$  ne peut pas vérifier qu’un seul des points précédents en vertu du théorème de Lagrange, car ni  $16 = 15 + 1$ , ni  $21 = 20 + 1$  ne divisent  $|A_5| = 60$ . Donc  $H$  vérifie au moins deux des points précédents, et ainsi  $|H| \geq 1 + 15 + 20 = 36$ . Donc  $|H| = 60$  et  $H = A_5$ .  $\square$

Si les théorèmes de Sylow sont mentionnés dans le plan, il est préférable de mentionner l’argument suivant.

[PER]  
p. 28

*Remarque 5.* Dans le raisonnement précédent, si  $H$  contient une permutation de type [5] (qui est donc d'ordre 5), alors  $H$  contient le 5-Sylow engendré par cet élément. Or, on sait par les théorèmes de Sylow que les sous-groupes de Sylow sont conjugués entre eux. Donc  $H$  contient tous les 5-Sylow et donc contient tous les éléments d'ordre 5.

**Théorème 6.**  $A_n$  est simple pour  $n \geq 5$ .

*Démonstration.* Soit  $N \triangleleft A_n$  tel que  $N \neq \{\text{id}\}$ . L'idée générale de la démonstration est de se ramener au cas  $n = 5$  à l'aide d'une permutation bien spécifique.

Soit  $\sigma \in N \setminus \{\text{id}\}$ , il existe donc  $a \in \llbracket 1, n \rrbracket$  tel que  $\sigma(a) = b \neq a$ . Soit  $c \in \llbracket 1, n \rrbracket$  différent de  $a, b$  et  $\sigma(b)$ . On pose  $\tau = \begin{pmatrix} a & c & b \\ & & \end{pmatrix} \in A_n$  (on a  $\tau^{-1} = \begin{pmatrix} a & b & c \\ & & \end{pmatrix}$ ). Soit  $\rho = \tau \sigma \tau^{-1} \sigma^{-1}$ . Par calcul :

$$\rho = \begin{pmatrix} a & c & b \\ & & \end{pmatrix} \sigma \begin{pmatrix} a & b & c \\ & & \end{pmatrix} \sigma^{-1} = \begin{pmatrix} a & c & b \\ & & \end{pmatrix} \begin{pmatrix} \sigma(a) & \sigma(b) & \sigma(c) \\ & & \end{pmatrix}$$

Notons bien que  $\rho \neq \text{id}$  (en tant que produit de 3-cycles, car  $\sigma(b) \neq c$ ). Or,  $\tau \sigma \tau^{-1} \in N$  car  $N$  est distingué et  $\sigma^{-1}$  aussi car  $N$  est un groupe, donc  $\rho \in N$ .

Notons  $\mathcal{F} = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ . Comme  $\sigma(a) = b$ ,  $|\mathcal{F}| \leq 5$ . Quitte à rajouter, au besoin, des éléments à  $\mathcal{F}$ , on peut supposer que  $|\mathcal{F}| = 5$ . On pose

$$A(\mathcal{F}) = \{\alpha \in A_n \mid \forall i \in \llbracket 1, n \rrbracket \setminus \mathcal{F}, \alpha(i) = i\}$$

le sous-groupe de  $A_n$  contenant les éléments qui laissent fixes  $\llbracket 1, n \rrbracket \setminus \mathcal{F}$ . Si on pose  $\mathcal{F} = \{a_1, a_2, a_3, a_4, a_5\}$ , on a une bijection entre  $\mathcal{F}$  et  $\llbracket 1, 5 \rrbracket$  :

$$\begin{aligned} \mathcal{F} &\rightarrow \llbracket 1, 5 \rrbracket \\ a_i &\mapsto i \end{aligned}$$

Donc  $A(\mathcal{F})$  et  $A_5$  sont deux groupes isomorphes (en effet, une permutation n'agissant que sur  $\mathcal{F}$  peut s'identifier à une permutation n'agissant que sur  $\llbracket 1, 5 \rrbracket$ ). De plus, par le Lemme 4, comme  $A_5$  est simple,  $A(\mathcal{F})$  l'est aussi.

Soit  $N_0 = N \cap A(\mathcal{F})$ .  $N_0 \triangleleft A(\mathcal{F})$ , en effet, soient  $\alpha \in N_0$  et  $\beta \in A(\mathcal{F})$  :

- $\beta \alpha \beta^{-1} \in A(\mathcal{F})$  car  $A(\mathcal{F})$  est un groupe.
- $\beta \alpha \beta^{-1} \in N$  car  $N \triangleleft A_5$ .

En particulier,  $N_0$  est distingué dans  $A(\mathcal{F})$  qui est simple. De plus,  $\rho \in N_0$  (car  $\text{Supp}(\rho) \subseteq \mathcal{F}$  et  $\epsilon(\rho) = (-1)^6 = 1$  donc  $\rho \in A(\mathcal{F})$  et par 1.,  $\rho \in N$ ). Donc  $N_0 \neq \{\text{id}\}$ , et ainsi  $N_0 = A(\mathcal{F})$ . On en déduit :

$$A(\mathcal{F}) = N \cap A(\mathcal{F}) \tag{*}$$

Finalement,  $\tau$  est un 3-cycle qui n'agit que sur  $\mathcal{F}$ , donc  $\tau \in A(\mathcal{F})$  et par (\*),  $\tau \in N$ . Or,  $\tau$  est un 3-cycle et les 3-cycles sont conjugués dans  $A_n$  (par le Lemme 1) donc  $N$  contient tous les 3-cycles. Et comme ceux-ci engendrent  $A_n$  (par le Lemme 3), on a  $N = A_n$ .  $\square$

# Bibliographie

## Cours d'algèbre

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

## Mathématiques pour l'agrégation

[ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2<sup>e</sup> éd. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.