Simplicité de $\mathfrak{A}_n$ pour $n = 3$ et $n \geq 5$:

I Le développement

Le but de ce développement est de démontrer que le groupe $\mathfrak{A}_n$ est simple pour $n = 3$ et $n \geq 5$ (c'est-à-dire qu'il ne possède aucun sous-groupe distingué non-trivial). Pour cela, nous allons d'abord utiliser le fait que $\mathfrak{A}_n$ est engendré par les 3-cycles et que ceux-ci sont tous conjugués dans $\mathfrak{A}_n$ puis ensuite utiliser ce résultat central pour démontrer que $\mathfrak{A}_n$ est un groupe simple.

Lemme 1 : [Rombaldi, p.49]
Le produit de deux transpositions de $[\![1; n]\!]$ est un produit de 3-cycles.
Plus précisément, pour tous $x, y, z, t \in [\![1; n]\!]$ deux à deux distincts, on a :

$$(x\ y)(x\ z) = (x\ z\ y) \text{ et } (x\ y)(z\ t) = (x\ y\ z)(y\ z\ t)$$

Preuve :
Soient τ_1 et τ_2 deux transpositions de $[\![1; n]\!]$.
On raisonne par disjonction de cas sur le support des deux transpositions :
$*$ Si $\tau_1 = \tau_2$, alors $\tau_1\tau_2 = \mathrm{Id}_{[\![1;n]\!]} = \gamma^3$ pour n'importe quel 3-cycle γ.

$*$ Si $\tau_1 \neq \tau_2$, on a alors deux sous-cas à envisager :
- Si $\mathrm{Supp}(\tau_1) \cap \mathrm{Supp}(\tau_2)$ est réduit à un singleton (on peut par exemple prendre $\{x\}$ sans perte de généralités), alors $\tau_1 = (x\ y)$ et $\tau_2 = (x\ z)$ avec x, y, z trois éléments distincts de $[\![1; n]\!]$. On a alors en examinant chacun des éléments des supports :

$$\tau_1\tau_2 = (x\ y)(x\ z) = (y\ x)(x\ z) = (y\ x\ z) = (x\ z\ y)$$

- Si $\mathrm{Supp}(\tau_1) \cap \mathrm{Supp}(\tau_2) = \emptyset$, on a alors $\tau_1 = (x\ y)$ et $\tau_2 = (z\ t)$ avec x, y, z, t quatre éléments deux à deux distincts de $[\![1; n]\!]$. Ainsi en examinant chacun des éléments des supports :

$$\tau_1\tau_2 = (x\ y)(z\ t) = (x\ y)(y\ z)(y\ z)(z\ t) = (x\ y\ z)(y\ z\ t)$$

Finalement, on a bien le résultat voulu.

■

Proposition 2 : [Rombaldi, p.49]
Pour $n \geq 5$, $\mathfrak{A}_n$ est engendré par les 3-cycles.

Preuve :
Soit $n \geq 5$.
Comme $\mathfrak{S}_n$ est engendré par les transpositions, il en est de même pour $\mathfrak{A}_n$. Si l'on considère $\sigma \in \mathfrak{A}_n \setminus \{\mathrm{Id}_{[\![1;n]\!]}\}$, il existe alors $r \in \mathbb{N}^*$ et $(\tau_i)_{i\in[\![1;r]\!]}$ un r-uplet de transpositions tel que : $\sigma = \prod_{i=1}^{r} \tau_i \quad (*)$.

De plus, puisque la signature de chaque τ_i vaut -1 et celle de σ vaut 1 (car $\sigma \in \mathfrak{A}_n$), on en déduit de $(*)$ que $(-1)^r = 1$ et donc que r est un nombre pair non nul.

En regroupant ainsi deux à deux les transpositions dans $(*)$, on obtient par le lemme précédent que σ s'écrit comme un produit de 3-cycles.

■

Proposition 3 : [Rombaldi, p.65]
Pour $n \geq 5$, les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$.

Preuve :
Soient $n \geq 5$ et $\gamma = (x_1\ x_2\ x_3)$ et $\gamma' = (x'_1\ x'_2\ x'_3)$ deux 3-cycles.
On sait déjà que deux 3-cycles sont conjugués dans $\mathfrak{S}_n$. On se donne donc une permutation $\sigma \in \mathfrak{S}_n$ telle que pour tout $k \in [\![1; 3]\!]$, $\sigma(x_k) = x'_k$ et on a alors $\gamma' = \sigma\gamma\sigma^{-1}$.

On raisonne par disjonction de cas :
$*$ Si $\sigma \in \mathfrak{A}_n$, alors on a bien le résultat voulu.

$*$ Si $\sigma \notin \mathfrak{A}_n$, alors en prenant x_4, x_5 dans $[\![1; n]\!] \setminus \{x_1; x_2; x_2\}$, la permutation $\sigma' = (x_4\ x_5)\sigma$ est dans $\mathfrak{A}_n$ (car de signature égale à 1) et vérifie bien, pour tout $k \in [\![1; 3]\!]$, $\sigma'(x_k) = x'_k$. On est donc ramené au cas précédent et on a ainsi le résultat voulu.

Finalement, les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$.

■

Théorème 4 : [Rombaldi, p.50 + 51]
Pour $n = 3$ ou $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

Preuve :
$*$ Traitons tout d'abord du cas où $n = 3$:
$\mathfrak{A}_n$ est alors un groupe d'ordre 3, il est donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ d'après la structure des "petits" groupes et ainsi il est simple.

$*$ Traitons désormais du cas général où $n \geq 5$:
Soit H un sous-groupe distingué de $\mathfrak{A}_n$ différent de $\{\mathrm{Id}_{[\![1;n]\!]}\}$.
Puisque les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$ et engendrent $\mathfrak{A}_n$, il suffit de montrer que H contient un 3-cycle (car H les contiendra tous puisqu'il est stable par conjugaison en tant que sous-groupe distingué et il sera ainsi égal à $\mathfrak{A}_n$).

Soient $\sigma \in H \backslash \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$ et $\gamma = (x\ z\ y) \in \mathfrak{A}_n$ un 3-cycle (avec $y = \sigma(x)$ et $z \notin \left\{x; y; \sigma^{-1}(x)\right\}$) qui ne commute pas avec σ (car $\gamma\sigma(x) = x$ et $\sigma\gamma(x) = \sigma(z) \neq x$).

Comme H est un sous-groupe distingué de $\mathfrak{A}_n$, on en déduit alors que l'élément $\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1} = \sigma\left(\gamma\sigma^{-1}\gamma^{-1}\right)$ appartient à H. De plus, en écrivant que :

$$\sigma' = \left(\sigma(x\ z\ y)\sigma^{-1}\right)(y\ z\ x) = (\sigma(x)\ \sigma(z)\ \sigma(y))(y\ z\ x) = (y\ \sigma(z)\ \sigma(y))(y\ z\ x)$$

On voit alors que σ' est le produit de deux 3-cycles (car y, $\sigma(y)$ et $\sigma(z)$ sont deux à deux distincts par bijectivité de σ) qui agissent sur $F = \{x, y, z, \sigma(y), \sigma(z)\}$ formé d'au plus 5 éléments (tous les points de $[\![1;n]\!] \backslash F$ sont fixes).

De plus, l'égalité $\sigma' = \mathrm{Id}_{[\![1;n]\!]}$ n'a lieu que lorsque $\sigma\gamma\sigma^{-1}\gamma^{-1} = \mathrm{Id}_{[\![1;n]\!]}$, c'est-à-dire $\sigma\gamma = \gamma\sigma$. Ce qui n'est pas possible d'après la définition de γ.

Ainsi, dans $\mathfrak{S}_F$, σ' s'écrit donc comme produit de cycles à supports disjoints. Or, cette décomposition étant également celle de $\mathfrak{S}_n$ et comme $\sigma' \in \mathfrak{A}_n$, il n'y a donc que trois possibilités : σ' est soit un 3-cycles, soit un produit de deux transpositions à supports disjoints, soit un 5-cycle.
- Si σ' est un 3-cycle, alors puisque $\sigma' \in H$, on a le résultat voulu.

- Si σ' est un produit de deux transpositions à supports disjoints, alors on écrit $\sigma' = (x_1\ x_2)(x_3\ x_4)$ et, en choisissant $x_5 \in [\![1;n]\!] \backslash \{x_1; x_2; x_3; x_4\}$ et en notant $\rho = (x_1\ x_2\ x_5) \in \mathfrak{A}_n$, on vérifie que le commutateur définit par $\sigma'' = [\sigma', \rho] = \sigma'\left(\rho\left(\sigma'\right)^{-1}\rho^{-1}\right)$ (qui est dans H par le même argument que précédemment) est un 3-cycle et on obtient le résultat voulu.
En effet :

$$\begin{aligned}\sigma'' &= \left(\sigma'\rho\left(\sigma'\right)^{-1}\right)\rho^{-1} = \left(\sigma'(x_1)\ \sigma'(x_2)\ \sigma'(x_5)\right)(x_5\ x_2\ x_1)\\ &= (x_2\ x_1\ x_5)(x_5\ x_2\ x_1) = (x_1\ x_2\ x_5)\end{aligned}$$

- Dans le troisième cas, on a $\sigma' = (x_1\ x_2\ x_3\ x_4\ x_5)$ et, en notant le 3-cycle $\rho = (x_1\ x_2\ x_3) \in \mathfrak{A}_n$, on vérifie de même que le commutateur $\sigma'' = [\sigma', \rho]$ (qui est dans H) est un 3-cycle et on obtient le résultat voulu.
En effet :

$$\begin{aligned}\sigma'' &= \left(\sigma'\rho\left(\sigma'\right)^{-1}\right)\rho^{-1} = \left(\sigma'(x_1)\ \sigma'(x_2)\ \sigma'(x_3)\right)(x_3\ x_2\ x_1)\\ &= (x_2\ x_3\ x_4)(x_3\ x_2\ x_1) = (x_1\ x_4\ x_2)\end{aligned}$$

Ainsi, dans tous les cas H contient un 3-cycle, donc par la remarque préliminaire de la démonstration, on en déduit que $H = \mathfrak{A}_n$ et donc que $\mathfrak{A}_n$ est simple.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Remarque 5 :
En fait, les groupes $\mathfrak{A}_3$ et $\mathfrak{A}_4$ sont également engendrés par les 3-cycles mais ce résultat n'est pas utile dans la preuve du théorème.

II.2 Pour aller plus loin...

II.2.1 Centre de $\mathfrak{A}_n$

Proposition 6 : [Rombaldi, p.64] :
Pour $n \geq 4$, le centre de $\mathfrak{A}_n$ est réduit à $\left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.

Preuve :
Soient $n \geq 4$ et $\sigma \in \mathfrak{A}_n \backslash \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.
Il existe alors $x \in [\![1;n]\!]$ tel que $y = \sigma(x) \neq x$.
On se donne $z \in [\![1;n]\!] \backslash \left\{x; y; \sigma^{-1}(x)\right\}$ (possible car $n \geq 4$) et $\gamma = (x\ z\ y) \in \mathfrak{A}_n$.
On a alors $\gamma\sigma(x) = \gamma(y) = x$ et $\sigma\gamma(x) = \sigma(z) \neq x$, donc $\sigma\gamma \neq \gamma\sigma$ et ainsi $\sigma \notin Z(\mathfrak{A}_n)$.

Le centre de $\mathfrak{A}_n$ est donc réduit à $\left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.

■

Remarque 7 :
∗ Pour $n \in \{1; 2\}$, $\mathfrak{A}_n$ est le groupe trivial donc $Z(\mathfrak{A}_n) = \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$ et pour $n = 3$, $\mathfrak{A}_n$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et il est donc abélien et égal à son centre.
∗ Le centre de $\mathfrak{A}_n$ est en réalité le même que $\mathfrak{S}_n$.

II.2.2 Application de la simplicité de $\mathfrak{A}_n$

La simplicité de $\mathfrak{A}_n$ trouve tout son intérêt dans la théorie de Galois. En effet, il est possible de montrer que $\mathfrak{S}_n$ est le groupe de Galois de l'équation polynomiale générale de degré n et que ce n'est pas un groupe résoluble pour $n \geq 5$. Cela permet de justifier que pour $n \geq 5$, les solutions des équations polynomiales générales de degré n ne peuvent pas s'exprimer simplement en fonction des coefficients (théorème d'Abel-Ruffini).

De plus, on peut en déduire le groupe dérivé de $\mathfrak{A}_n$:

Corollaire 8 : [Perrin, p.28]
Pour $n \geq 5$, on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.

Preuve :
Soit $n \geq 5$.
On sait que le groupe dérivé est un sous-groupe distingué, donc ici $D(\mathfrak{A}_n)$ est un sous-groupe distingué de $\mathfrak{A}_n$. De plus, par le développement, $\mathfrak{A}_n$ est un groupe simple, donc $D(\mathfrak{A}_n) = \mathfrak{A}_n$ ou $D(\mathfrak{A}_n) = \mathrm{Id}_{[\![1;n]\!]}$.

Or, on sait également que le quotient $\mathfrak{A}_n/D(\mathfrak{A}_n)$ est abélien et que le groupe $\mathfrak{A}_n$ n'est pas abélien (car sinon il serait égal à son centre), on a donc $D(\mathfrak{A}_n) = \mathfrak{A}_n$.

■

Corollaire 9 : [Perrin, p.30]
Pour $n \geq 5$, le seul sous-groupe distingué de $\mathfrak{S}_n$ non trivial est $\mathfrak{A}_n$.

Preuve :
Soit $n \geq 5$.
$*$ On sait que $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ car il est d'indice 2 dans $\mathfrak{S}_n$ (et c'est même le seul !).

$*$ Soit H un sous-groupe distingué de $\mathfrak{S}_n$ non trivial.
On a alors $H \cap \mathfrak{A}_n$ qui est un sous-groupe distingué de $\mathfrak{A}_n$. Or, par le développement, on sait que $\mathfrak{A}_n$ est simple et donc $H \cap \mathfrak{A}_n$ est égal à $\mathfrak{A}_n$ ou à $\left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.
- Si $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, alors H contient $\mathfrak{A}_n$ et donc son cardinal divise $n!$ et est un multiple de $\frac{n!}{2}$. Ainsi, on a $H = \mathfrak{S}_n$ ou $H = \mathfrak{A}_n$.

- Si $H \cap \mathfrak{A}_n = \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$, alors la signature induit un isomorphisme de H sur $\varepsilon(H) \subseteq \{-1;1\}$, de telle sorte que $\mathrm{Card}(H) \leq 2$.

Or, si $\mathrm{Card}(H) = 2$ alors on a $H = \{1;\sigma\}$. Mais en considérant un élément $\rho \in \mathfrak{S}_n$, on a $\rho\sigma\rho^{-1} \in H$ (car H est un sous-groupe distingué de $\mathfrak{S}_n$ par hypothèse) et $\rho\sigma\rho^{-1} \neq \mathrm{Id}_{[\![1;n]\!]}$ (car l'élément neutre est seul dans sa classe de conjugaison) et donc $\rho\sigma\rho^{-1} = \sigma$ et ainsi σ appartient au centre de $\mathfrak{S}_n$. Or ce centre est égal au groupe trivial et on aboutit donc a une contradiction. On en déduit que H est de cardinal 1 et donc égal au groupe trivial.

Ainsi, le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.

■

Remarque 10 :
On démontre de même que le groupe dérivé de $\mathfrak{S}_n$ est égal à $\mathfrak{A}_n$.

II.3 Recasages

Recasages : 103 - 104 - 105 - 108.

III Bibliographie

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie*.

— Daniel Perrin, *Cours d'algèbre*.