$\mathfrak{A}_n$ est simple pour $n \geq 5$

Chen Thomas
t.chen.thomas1[at]gmail.com

16 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104 : Groupes finis. Exemples et applications.
- 105 : Groupe des permutations d'un ensemble fini. Applications.
- 108 : Exemples de parties génératrices d'un groupe. Applications.
- 190 : Méthodes combinatoires, problèmes de dénombrement. Applications.

Références

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

[2] J.-E. Rombaldi. *Mathématiques pour l'agrégation : Algèbre & géométrie.* deBoeck Supérieur, 2021.

Lemme 1. [2] Les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$. Cela est faux pour $n = 4$.

Démonstration. Soit $(a\ b\ c), (\alpha\ \beta\ \gamma)$ deux 3-cycles de $\mathfrak{A}_n$. Dans $\mathfrak{S}_n$, ces permutations sont conjugués : il existe $\sigma \in \mathfrak{S}_n : \sigma(a\ b\ c)\sigma^{-1} = (\alpha\ \beta\ \gamma)$. Si $\sigma \in \mathfrak{S}_n$, c'est gagné. Sinon, soit d, e distincts de a, b, c dans $[\![1, n]\!]$. Alors $\sigma \circ (d\ e)$ est dans $\mathfrak{A}_n$ et

$$\sigma \circ \underbrace{(d\ e)(a\ b\ c)(d\ e)}_{=(a\ b\ c)} \sigma^{-1} = \sigma(a\ b\ c)\sigma^{-1} = (\alpha\ \beta\ \gamma)$$

donc deux 3-cycles sont conjugués dans $\mathfrak{A}_n$. Cela est faux dans $\mathfrak{A}_4$: $(1\ 2\ 3)$ et $(2\ 3\ 4)$ ne peuvent être conjugués dans $\mathfrak{A}_4$: mettons que σ soit telle que $\sigma(1\ 2\ 3)\sigma^{-1} = (2\ 3\ 4)$. Alors $\sigma(4) = 1$. En imposant $(\sigma(1)\ \sigma(2)\ \sigma(3)) = (2\ 3\ 4)$, cela impose que $\sigma \in \{(1\ 4)(2\ 3), (1\ 2\ 4), (1\ 3\ 4)\}$. Dans les trois cas, cela ne fonctionne pas. $\square$

Lemme 2. [2] Les 3-cycles engendrent $\mathfrak{S}_n$.

Démonstration. $\mathfrak{S}_n$ est engendré par les transpositions. De fait, par multiplicativité de la signature, un élément de $\mathfrak{A}_n$ est un produit pair de transpositions : soit $\sigma \in \mathfrak{A}_n$. Alors il existe $N \in \mathbb{N}$ et $(\tau_i = (a_i\ b_i))_{1 \leq i \leq 2N}$ des transpositions telles que

$$\sigma = \prod_{i=1}^{2N} \tau_i.$$

Or, pour tout $a, b, c, d \in \mathbb{N}^*$ deux à deux distincts, $(a\ b)(a\ c) = (a\ c\ b)$ et $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$ donc en regroupant par 2, on a le résultat souhaité. □

Théorème 3. *[1] $\mathfrak{A}_5$ est simple.*

Démonstration. Dénombrons les éléments de $\mathfrak{A}_5$.

- Il y a identité.
- Il y a les doubles transpositions : pour obtenir une double transposition, on choisit $\binom{5}{2}$ éléments à permuter, puis $\binom{3}{2}$ éléments à permuter, le dernier élément sera automatiquement fixé. L'ordre ne compte pas donc je divise par 2 le résultat. Il y a donc 15 doubles transpositions.
- Il y a les 3-cycles : pour obtenir un trois cycle, on choisit nos deux points fixes $\binom{5}{2}$ choix que l'on multiplie par les 2 3-cycles que l'on peut créer après ce choix. J'ai donc 20 3-cycles.
- Pas d'éléments d'ordre 4 – mais pas besoin de justifier via la suite –[1].
- Un 5-cycle est déterminé par un tirage sans remise de 5 éléments dans une urne à 5 éléments et faire tous les tirages possible donnera 5 fois un même 3-cycles : il y a donc $4! = 24$ 5 cycles.

Au total, on a donc obtenu 60 éléments donc il n'y en a pas d'autres.

Soit maintenant H un sous-groupe distingué de $\mathfrak{A}_n$ différent de $\{\mathrm{id}\}$. Par les lemmes, il suffit de montrer que H contient un 3-cycle.

Les doubles transpositions sont conjugués dans $\mathfrak{A}_5$. En effet, soit $(a\ b)(c\ d)(e)$, $(\alpha\ \beta)(\gamma\ \delta)(\eta)$ deux doubles transpositions. Soit $\sigma \in \mathfrak{S}_5$ telle que $\sigma(a) = \alpha, \sigma(b) = \beta, \sigma(e) = \eta$. Si $\sigma \in \mathfrak{A}_5$, alors puisque $\sigma(a\ b)(c\ d)(e)\sigma^{-1} = (\alpha\ \beta)(\sigma(c)\ \sigma(d))(\eta)$ ce qui signifie $(\sigma(c)\ \sigma(d)) = (\gamma\ \delta)$, alors nos deux doubles transpositions sont conjugués dans $\mathfrak{A}_5$.
Sinon, soit $\sigma' = \sigma \circ (c\ d)$. Alors $\sigma' \in \mathfrak{A}_5$ et le résultat tient toujours.

Le bloc suivant n'est pas fait dans les références et je n'en ai pas trouvé. Perrin utilise les Sylow, je l'ai évité car sans, ce n'est pas si long.

Si σ, σ' sont deux 5-cycles dans $\mathfrak{A}_5$ alors σ' est conjugué dans $\mathfrak{A}_5$ à σ ou σ^2. En effet, ils sont conjugués dans $\mathfrak{S}_5$: il existe $\tau \in \mathfrak{S}_5$ tel que $\sigma' = \tau\sigma\tau^{-1}$. Si τ est dans $\mathfrak{A}_5$, c'est gagné. Sinon, on note $\sigma = (a\ b\ c\ d\ e)$ et $\sigma^2 = (a\ c\ e\ b\ d)$ de sorte qu'on arrive à les conjuguer avec un 4-cycle : en prenant la permutation $(b\ c\ e\ d)$, on arrive à $\sigma = (b\ c\ e\ d)\sigma^2(b\ c\ e\ d)^{-1}$. Ainsi,

$$\sigma' = \tau\sigma\tau^{-1} = \underbrace{\tau(b\ c\ e\ d)}_{\in\mathfrak{A}_5}\sigma^2[\tau(b\ c\ e\ d)]^{-1}$$

Ainsi,

- Si H contient un 3-cycle, c'est terminé.
- si H contient une double transposition, il les a tous : cela fait $1 + 15 = 16 \nmid 60$ donc H doit contenir aussi un 5-cycle, disons σ. H étant un groupe, il contient σ^2 et donc par précédent, il contient tous les 5-cycles : H est donc au-moins de cardinal $1 + 15 + 24 > 30$ donc $H = \mathfrak{A}_5$.

1. Si on a un élément d'ordre 4, c'est un 4-cycle donc il est de signature -1. Ce n'est pas long mais on peut se permettre de ne pas écrire cette puce.

- Si H contient un 5-cycles, il contient son carré donc tous les 5 cycles : cela fait au moins $1+24=25 \nmid 60$ éléments donc H contient aussi une double-transposition et on est ramené à précédent.

Ainsi, $H=\mathfrak{A}_5$: $\mathfrak{A}_5$ est simple. $\square$

Théorème 4. *[1] $\mathfrak{A}_n$ est simple pour $n \geq 5$.*

Démonstration. On va se ramener à $\mathfrak{A}_5$. Pour cela, soit H un sous-groupe distingué de $\mathfrak{A}_n$ distinct de $\{\mathrm{id}\}$. Soit $\sigma \in H \backslash \{\mathrm{id}\}$. *Idée : regarder un commutateur de σ : très souvent, un commutateur n'est pas dans la classe de conjugaison.* Soit a tel que $\sigma(a) \neq b$. On note $b=\sigma(a)$. Soit c tel que $c \neq a, b, \sigma(b)$. Considérons alors $\tau=(a\ c\ b)$ et calculons $[\tau, \sigma]$. On a

$$\rho := [\tau, \sigma] = (a\ c\ b)\sigma(a\ b\ c)\sigma^{-1} = (a\ c\ b)(b\ \sigma(b)\ \sigma(c)) \in H.$$

Ainsi, $\mathrm{supp}(\rho) \subset \{a, b, c, \sigma(a), \sigma(b)\}$. Soit F qui contient ces éléments. Quitte à en rajouter, on peut supposer que F contient 5 éléments. On a par construction $\rho(F) \subset F$.

Puisque $\mathfrak{A}_F \simeq \mathfrak{A}_5$, $\mathfrak{A}_F$ est simple. Soit donc l'injection naturelle $i : \mathfrak{A}_F \to \mathfrak{A}_n$ qui à u associe $\overline{u}$ qui coïncide avec u sur F, et identité sinon. Alors $H_0 = \{u \in \mathfrak{A}_F : i(u) \in H\} = F \cap H$ est un sous-groupe distingué de F. D'ailleurs, $\rho \in H_0$ donc $H_0 \neq \{\mathrm{id}\}$. [2]Par simplicité de $\mathfrak{A}_F$, $H_0 = \mathfrak{A}_F$ donc H contient $\mathfrak{A}_F$: en particulier, H contient un 3-cycle. $\square$

2. ρ est distinct de id. En effet, $\rho(b) = \tau\sigma\tau^{-1}\sigma^{-1}(b)$. On a posé $b=\sigma(a)$ donc $\rho(b) = \tau\sigma(b)$. Si $\rho(b)=b$, alors $c = \tau^{-1}(b) = \sigma(b)$ ce qui est exclu.