19. Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$

[Per96, §I.8, p28–29] [Rom17, §2.9, p67]

ÉNONCÉ

PROPOSITION. *Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.*

DÉVELOPPEMENT

Fixons $n \geq 5$ et commençons par démontrer le lemme suivant :

LEMME.
i) $\mathfrak{A}_n$ est le sous-groupe engendré par les trois cycles,
ii) Les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

i) Notons G le sous-groupe engendré par les 3-cycles. On vérifie que $G \subset \mathfrak{A}_n$ car tous les éléments de G ont pour signature 1.

Réciproquement, si $\sigma \in \mathfrak{A}_n$, considérons une décomposition $\prod_{i=1}^{p} \tau_i$ de σ en produit de transpositions. Comme $\mathcal{E}(\sigma) = 1$, on a nécessairement que p est pair.
Or, on remarque que pour i, j, k, ℓ distincts, on a :

$$(i\,j)(k\,\ell) = (i\,j\,k)(j\,k\,\ell) \quad \text{et} \quad (i\,j)(k\,i) = (i\,k\,j)$$

Donc le produit de deux transpositions distinctes est un 3-cycle. Donc σ s'écrit comme produit de $p/2$ 3-cycles. Ainsi $\sigma \in G$.
Finalement on a bien $G = \mathfrak{A}_n$.

ii) Les 3-cycles forment une classe de conjugaison dans $\mathfrak{S}_n$. Donc pour a, b, c distincts puis d, e, f distincts, il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(a\,b\,c)\sigma^{-1} = (d\,e\,f)$.
Si $\sigma \in \mathfrak{A}_n$, c'est bon. Sinon, comme $n \geq 5$, on peut choisir i, j distincts de a, b, c et alors $\sigma' = \sigma(i\,j)$ est un élément de $\mathfrak{S}_n$ tel que $\sigma'(a\,b\,c)(\sigma')^{-1} = (d\,e\,f)$.

Donc les 3-cycles sont bien conjugués dans $\mathfrak{A}_n$.

Soit donc H un sous-groupe distingué de $\mathfrak{A}_n$, distinct de $\{\mathrm{Id}\}$. Par le lemme, il suffit de montrer que H possède un 3-cycle.

Soit $\sigma \in H \setminus \{\mathrm{Id}\}$. Prenons a tel que $b = \sigma(a) \neq a$. Fixons un $c \notin \{a, b, \sigma(b)\}$ (possible car $n \geq 5$) et considérons le 3-cycle $\gamma = (a\,b\,c)$ puis $\sigma_2 = \sigma\gamma\sigma^{-1}\gamma^{-1}$.

On a $\sigma_2 \in H$ car $\sigma \in H$ et $\gamma\sigma^{-1}\gamma^{-1} \in H$, et on vérifie que $\sigma_2 = (b\;\sigma(b)\;\sigma(c))(a\,c\,b)$. On va décomposer σ_2 en produit de cycles à support disjoints, en remarquant que $\mathrm{Supp}(\sigma_2) \subset \{a, b, c, \sigma(b), \sigma(c)\}$ a au plus 5 éléments. En raisonnant sur le type de σ_2, seuls les cas suivants se produisent :

(1, 1, 1, 1, 1) Si $\sigma_2 = \mathrm{Id}$, cela entraîne que σ et γ commutent, ce qui est faux car $\sigma\gamma(a) = \sigma(b) \neq c = \gamma\sigma(a)$ par construction de c.

(2, 2, 1) Si $\sigma_2 = (i\,j)(k\,\ell)$, alors $\sigma_3 = (i\,j\,k\,\ell\,m)\sigma_2(i\,j\,k\,\ell\,m)^{-1}\sigma_2^{-1} \in H$ car H est distingué dans $\mathfrak{A}_n$, et on a $\sigma_3 = (i\,j\,k\,\ell\,m)(j\,i\,\ell\,k\,m)^{-1} = (i\,k\,m\,\ell\,j)$, et on se ramène au cas où le type est (5),

(3, 1, 1) Si σ_2 est un 3-cycle, c'est bon,

(5) Si $\sigma_2 = (i\,j\,k\,\ell\,m)$, alors de même $\sigma_3 = (i\,j\,k)\sigma_2(i\,j\,k)^{-1}\sigma_2^{-1} \in H$ et on a $\sigma_3 = (i\,j\,k)(j\,\ell\,k) = (i\,j\,\ell)$.

Dans tous les cas, on a donc bien trouvé un 3-cycle dans H. Ainsi $H = \mathfrak{A}_n$.

COMMENTAIRES

Que se passe-t-il pour $n < 5$?

- $\mathfrak{A}_3 = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\} \simeq \mathbb{Z}/3\mathbb{Z}$ est simple,
- $\mathfrak{A}_4 = \{\mathrm{Id}, \text{3-cycles}, \text{bi-transpositions}\}$ n'est pas simple, car le groupe des bi-transpositions est distingué dans $\mathfrak{A}_n$. De plus, les 3-cycles ne sont pas conjugués sinon on aurait $8 \mid |\mathfrak{A}_4|$, ce qui est faux.