②

Le groupe alterné est simple pour $n \neq 4$

Berhuy, page 217

Lemme Soit n un entier vérifiant $n \geq 5$.
Alors les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Soient $\sigma = (a_1\ a_2\ a_3)$ et $\sigma' = (\alpha_1\ \alpha_2\ \alpha_3)$ deux 3-cycles de $\mathcal{A}_n$.
On sait qu'alors σ et σ' sont conjugués dans $\mathfrak{S}_n$. Il existe donc $\tau \in \mathfrak{S}_n$ tel que $\sigma' = \tau\sigma\tau^{-1}$.
On a alors :

- si $\tau \in \mathcal{A}_n$, c'est terminé
- si $\tau \notin \mathcal{A}_n$, comme $n \geq 5$ on peut trouver a, b distincts de $\alpha_1, \alpha_2, \alpha_3$.

Alors en posant $\tau' = (a\ b)\tau$, on a : $\tau' \in \mathcal{A}_n$ et $\tau'\sigma\tau'^{-1} = (a\ b)(\alpha_1\ \alpha_2\ \alpha_3)(a\ b) = (\alpha_1\ \alpha_2\ \alpha_3) = \sigma'$

Donc σ et σ' sont conjugués dans $\mathcal{A}_n$.

Théorème Soit E un ensemble à n éléments avec $n \geq 3$.
Alors $\mathcal{A}_n$ est simple si et seulement si $n = 3$ ou $n \geq 5$.

- si $n = 3$, on a $|\mathfrak{S}_3| = 6$ donc $\mathcal{A}_3$ est cyclique car d'ordre 3.

Il est facile de voir qu'alors $\mathcal{A}_3$ est simple.

- si $n = 4$, le sous-groupe $H = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ est distingué dans $\mathcal{A}_4$.

Or $H \neq \{id\}$ et $H \neq \mathcal{A}_4$ donc $\mathcal{A}_4$ n'est pas simple.

- si $n \geq 5$, soit H un sous-groupe de $\mathcal{A}_n$ avec $H \neq \{id\}$

On a alors :

→ si H contient un 3-cycle alors, H étant distingué et les 3-cycles étant conjugués dans $\mathcal{A}_n$, H contient tous les 3-cycles de $\mathfrak{S}_n$. Donc $H = \mathcal{A}_n$.

→ si H contient une bi-transposition $(a\ b)(c\ d) = \sigma$, notons $\tau = (a\ b\ e)$ avec e distinct de a, b, c, d.

On a alors :

$\sigma\tau\sigma^{-1}\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in H$ car $H \triangleleft \mathcal{A}_n$

$\sigma\tau\sigma^{-1}\tau^{-1} = \sigma(\tau(c\ d)\tau^{-1})(\tau(a\ b)\tau^{-1}) = \sigma(\tau(c)\ \tau(d))(\tau(a)\ \tau(b)) = \sigma(c, d)(b\ e) = (a\ b)(b\ e) = (a\ b\ e)$

Donc H contient un 3-cycle, i.e. $H = \mathcal{A}_n$

Soit $\sigma \in H \setminus \{id\}$.

1er cas : supposons que la décomposition de σ en produits de cycles à supports disjoints ne contient que des 3-cycles

- si σ est un 3-cycle : rien à faire
- sinon, σ admet deux 3-cycles $(a\ b\ c), (d\ e\ f)$. On pose alors $\tau = (a\ d)(b\ c)$.

On a alors :

$\sigma\tau\sigma^{-1}\tau^{-1} = (\sigma(a)\ \sigma(d))(\sigma(b)\ \sigma(c))\tau^{-1} = (b\ e)(c\ f)(b\ c)(a\ d) = (c\ f)(a\ d)$

Donc $H = \mathcal{A}_n$.

2ème cas : supposons qu'il n'y a pas que 3-cycles dans la décomposition de σ

Admettons qu'il existe $F \subset [\![1, n]\!]$ avec $|F| = 3$ et $|F \cup \sigma(F)| = 4$.

Soit τ un cycle de support F alors τ est un 3-cycle et appartient alors à $\mathcal{A}_n$.

De plus :

$\text{supp}(\sigma\tau\sigma^{-1}) = \sigma(F) \neq F = \text{supp}\ \tau$ donc $\sigma\tau\sigma^{-1} \neq \tau$. Ainsi, $\sigma\tau\sigma^{-1}\tau^{-1} \in H \setminus \{id\}$.

D'où $\sigma\tau\sigma^{-1}\tau^{-1}$ est un 3-cycle ou une bitransposition.
Donc $H = \mathcal{A}_n$.

Montrons l'existence d'une telle partie F :

→ si σ contient un cycle $(a_1 \dots a_k)$ de longueur supérieure ou égale à 4 : $F = \{a_1, a_2, a_3\}$ fonctionne

→ si σ contient uniquement des 2-cycles et 3-cycles dans sa décomposition, par hypothèse il y a une transposition.
De plus, σ est de signature 1 donc il y a un nombre pair de transpositions. Il y a alors au moins deux transpositions qu'on note $(a\ b)(c\ d)$. On pose $F = \{a, b, c\}$.