

Simplicité de $\mathcal{A}_m$ pour $m=3, m \geq 5$.

[BER] p 275

Recanages: 104, ~~102~~, 105, 108, 103

Proposition: $m \geq 3$

$\mathcal{A}_m$ est engendré par chacune des familles suivantes:

- (i) les produits de deux transpositions;
- (ii) les 3-cycles.

Preuve:

(i) $\mathcal{A}_m$ est engendré par les transpositions.

$\sigma \in \mathcal{A}_m$ si, et seulement si $\varepsilon(\sigma) = 1$, i.e. : σ est un produit d'un nombre pair de transposition.

En particulier, $\mathcal{A}_m$ est engendré par les produits de 2 transpositions.

(ii) Il suffit de montrer que les produits de 2 transpositions sont des 3-cycles.

Soient $\tau_1, \tau_2 \in \mathcal{A}_m$ deux transpositions.

→ Si $\text{supp}(\tau_1) = \text{supp}(\tau_2)$, $\tau_1 = \tau_2$ et $\tau_1 \tau_2 = \text{Id}$ donc ok.

→ Si $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) = \{a\}$, alors $\tau_1 = (ab)$ et $\tau_2 = (ac)$ et $\tau_1 \tau_2 = (ba)(ac) = (bac)$ donc ok!

→ Si $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) = \emptyset$. Alors en notant $\tau_1 = (ab)$ et $\tau_2 = (cd)$, on a:
 $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$

Proposition:

Soit $m \geq 5$.
 Les 3-cycles sont conjugués dans $\mathcal{A}_m$

Preuve:

Soient $\sigma = (i j k)$ et $\sigma' = (l m n)$.

Les 3-cycles étant conjugués dans $\mathcal{A}_m$, il existe $\tau_1 \in \mathcal{A}_m$ tel que $\sigma' = \tau_1 \sigma \tau_1^{-1}$.

Si $\tau_1 \in \mathcal{A}_m$, c'est fini.

Si non, on considère (de) avec $d, e \in \mathcal{A}_m \setminus \{l, m, n\}$ et on pose $\tau_2 = (de)\tau_1$.

Alors $\varepsilon(\tau_2) = 1$ donc $\tau_2 \in \mathcal{A}_m$ et finalement:

$$\tau_2 \sigma \tau_2^{-1} = (de)(lmn)(de)^{-1} = (lmn)(de)(de)^{-1} = (lmn) = \sigma'$$

↑
 supports disjoints
 donc commutent

Théorème:

Soit $m \geq 3$, $\mathcal{A}_m$ est simple pour $m \neq 4$.

Preuve:

Si $m=3$, $\mathcal{A}_3$ est d'ordre 3 donc cyclique puis simple de façon immédiate.

Si $m=4$, $\mathcal{A}_4$ admet pour sous-groupe strict distingué le groupe de Klein.

Supposons $m \geq 5$. Soit $H \triangleleft \mathcal{A}_m$, $H \neq \{\text{Id}\}$. On va montrer que $H = \mathcal{A}_m$.

On commence par remarquer 4 points :

(1) Si H contient un 3-cycle, $H = \mathcal{U}_n$.

Si H contient un 3-cycle, il contient tous les 3-cycles car ils sont tous conjugués dans $\mathcal{U}_n$ par la même proposition 2 et H étant distingué, il est stable par conjugaison.

Alors H contenant tous les 3-cycles, par la proposition 1, $H \supset \mathcal{U}_n$ et enfin $H = \mathcal{U}_n$.

(2) Si $\sigma \in H$ et $\tau \in \mathcal{U}_n$, $[\sigma, \tau] \in H$.

En effet $[\sigma, \tau] = \underbrace{\sigma \tau \sigma^{-1}}_{\in H} \underbrace{\tau^{-1}}_{\in H \text{ car } H \triangleleft \mathcal{U}_n} \in H$.

(3) Si H contient un produit de deux transpositions à supports disjoints, $H = \mathcal{U}_n$.

Soit $\sigma = (ab)(cd) \in H$. Puisque $n \geq 5$, il existe $e \in [1, n] \setminus \{a, b, c, d\}$, et on pose $\tau = (cde)$ et on a :

$$\tau \sigma \tau^{-1} = (ab)(de) \quad \text{puis} \quad [\sigma, \tau] = (ab)(cd)(ab)(de) \\ = (ab)(ab)(cd)(de) \quad \text{car } (ab) \text{ et } (cd) \text{ commutent} \\ = (cde) \in H \text{ par (2)} \quad \text{car leurs supports sont disjoints.}$$

Par (1), $H = \mathcal{U}_n$.

(4) Soit $\sigma \in H$, s'il existe $F \subset [1, n]$ tq $\#F = 3$ et $\#(\sigma(F) \cup F) = 4$, $H = \mathcal{U}_n$.

On pose τ telle que $\text{supp}(\tau) = F$, alors τ est un 3-cycle et $\tau \in \mathcal{U}_n$.

Ensuite, on a $\text{supp}(\sigma \tau \sigma^{-1}) = \sigma(\text{supp}(\tau)) = \sigma(F) \neq F = \text{supp}(\tau)$ donc $\sigma \tau \sigma^{-1} \neq \tau$.

Puis $\sigma' = [\sigma, \tau] \neq \text{Id}$. De plus, $\text{supp}(\sigma') \subset \text{supp}(\sigma \tau \sigma^{-1}) \cup \text{supp}(\tau^{-1}) = \sigma(F) \cup F$ et $\sigma' \in H$.

Alors nécessairement, σ' est un 3-cycle et par (1), $H = \mathcal{U}_n$, ou σ' est un produit de deux transpositions à supports disjoints et par (3), $H = \mathcal{U}_n$. Si σ' est une transposition ou un 4-cycle, $\#(\sigma') = 2$, donc

Soit $\sigma \in H$ on considère sa décomposition en produit de cycles à supports disjoints et on repère deux cas : $\rightarrow$ cette décomposition contient que des 3-cycles. S'il n'y en a qu'un, par (1) $H = \mathcal{U}_n$. Supposons qu'il y ait au moins deux 3-cycles (abc) et (def) on pose $\tau = (ad)(be) \in \mathcal{U}_n$, on a $\sigma \tau \sigma^{-1} = (be)(cf)$ puis $[\sigma, \tau] = (be)(cf)(abc)(ad) \in H$ par (2) puis par (3) $H = \mathcal{U}_n$.

$\rightarrow$ La décomposition ne contient pas que des 3-cycles. Alors :

$\rightarrow$ S'il y a un k -cycle $(abcd \dots)$ pour $k \geq 4$, on pose $F = \{a, b, c\}$ qui vérifie (*) pour σ et par (4), $H = \mathcal{U}_n$.

$\rightarrow$ S'il n'y a pas de k -cycle pour $k \geq 4$, il y a au moins une transposition (ab) et puis une dérivée en (bcd) . On pose alors $F = \{a, b, c\}$ qui vérifie (*) pour σ et par (4), $H = \mathcal{U}_n$. □

Lemme : $\sigma, \tau \in \mathcal{G}_m$. $\text{supp}(\sigma \tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau)$.

Preuve : $\text{Fix}(\sigma \tau) \supset \text{Fix}(\sigma) \cap \text{Fix}(\tau)$ donc $\text{supp}(\sigma \tau) = E / \text{Fix}(\sigma \tau) \subset E / (\text{Fix}(\sigma) \cap \text{Fix}(\tau)) = E / \text{Fix}(\sigma) \cup E / \text{Fix}(\tau) = \text{supp}(\sigma) \cup \text{supp}(\tau)$. De Morgan.

Lemme : Deux permutations à supports disjoints commutent.

Supposons $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$.

Si $a \in \text{supp}(\sigma)$, $\sigma(a) \neq a$ et $\tau(a) = a$ donc $\sigma(\tau(a)) = \sigma(a)$.

Dans l'autre sens, on a que $\sigma(a) \notin \text{supp}(\tau)$ et $\tau(\sigma(a)) = \sigma(a)$ donc de !

De la même façon, si $a \in \text{supp}(\tau)$, σ et τ commutent.

Enfin si $a \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$, $\sigma(\tau(a)) = \sigma(a) = a = \tau(a) = \sigma(\tau(a))$