

Sous-groupes distingués de S_n :

Références: [Rem]

Énoncé:

Th 1: A_n est engendré par les 3-cycles

Th 2: Pour $n \geq 5$ les sous-groupes distingués de S_n sont $\{Id\}$, A_n et S_n .

Étapes:

(E1) A_n est engendré par les 3-cycles

↳ se ramener à $\tau_1 \circ \tau_2$ est un produit de 3-cycles

(E2) Mg si $H \triangleleft S_n$ contient un 3-cycle alors $H = A_n$.

(E3) $H \triangleleft S_n$, $H \neq S_n$, $H \neq \{Id\}$ prendre $\sigma \in H \setminus \{Id\}$, et $(x y)$ tq $(x y)$ et σ ne commutent pas

Lemme: $\forall \sigma \in S_n \setminus \{Id\} \exists \tau$ une transpo tq $\sigma \circ \tau \neq \tau \circ \sigma$.

Poser $\tilde{\sigma} = (x y) \sigma (x y) \sigma^{-1} \in H$ Mg $\tilde{\sigma} = (x y) (\sigma(x) \sigma(y))$ et $\tilde{\sigma} \neq Id$. si $\sigma(x) = y$ ou $\sigma(y) = x$ $\tilde{\sigma}$ est un 3-cycle.

Sinon prendre $z \notin \{x, y, \sigma(x), \sigma(y)\}$ et avec $(\sigma(y) z)$

mq $(x y) (\sigma(x) z) \in H$, mq $\tilde{\sigma} \circ (x y) \circ (\sigma(x) z)$ est dans H et un 3-cycle.

① Générateurs de A_n : ($n \in \mathbb{N}^*$)

On sait que $A_n = \ker(\varepsilon)$ (ε : morphisme signature)

Donc $\varepsilon: S_n \rightarrow \{+1, -1\}$ étant surjective on a:

$$\#(S_n/A_n) = \#\{\pm 1\} = 2 \quad [S_n, A_n] = 2 \text{ et}$$

$$\#(A_n) = \frac{\#(S_n)}{2} = \frac{n!}{2}$$

$$\triangleright \#(A_2) = \frac{2!}{2} = 1, \quad A_2 = \{\text{id}_E\}$$

$$\triangleright \#(A_3) = \frac{3!}{2} = 3 \quad \text{or } (1\ 2\ 3) \in A_3 \text{ car } \varepsilon(123) = 1$$

Comme $(1\ 2\ 3)$ est d'ordre 3 on a alors

$$A_3 = \langle (1\ 2\ 3) \rangle = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

$\triangleright n \geq 3$: mg A_n est engendré par les 3-cycles.

On sait que $\forall \sigma \in A_n, \varepsilon(\sigma) = 1$

Et comme S_n est engendré par les transpositions,

il existe $\tau_1, \dots, \tau_r$ des transpositions telles que $\sigma = \tau_1 \dots \tau_r$.

Comme $\varepsilon(\sigma) = \varepsilon(\tau_1 \dots \tau_r) = (-1)^r$ on en déduit $r \in 2\mathbb{N}$.

Donc pour mg σ est produit de 3-cycles il suffit de mg le produit de deux transpositions est un produit de 3-cycles.

Soit τ_1, τ_2 deux transpositions de S_n

$\triangleright$ Si $\tau_1 \circ \tau_2 = \text{id}_E$, pour n'importe quel 3-cycle γ ,

$$\tau_1 \circ \tau_2 = \gamma^3$$

▷ Si $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) \neq \emptyset$ alors $\exists (x, y, z) \in [1; n]^3$

tel que $\tau_1 = (x \ y)$ et $\tau_2 = (x \ z)$.

on a alors $(x \ y)(x \ z) = (x \ z \ y)$.

▷ Si $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) = \emptyset$ alors $\exists (x, y, z, t) \in [1; n]^4$

tel que $\tau_1 = (x \ y)$, $\tau_2 = (z \ t)$ donc

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

Donc A_n est bien engendré par les 3-cycles.

(E2) les sous-groupes distingués de S_n sont $\{id\}$, S_n et A_n .

Si $H \triangleleft S_n$ alors $\forall \sigma \in S_n, \forall \tau \in H, \sigma \circ \tau \circ \sigma^{-1} \in H$. Pour mq

$H = A_n$ il suffit alors de mq H contient un 3-cycle

et que les conjugués des 3-cycles sont exactement

les 3-cycles.

Lemme : Le conjugué d'un r -cycle est un r -cycle. Plus

précisément, si γ est un r -cycle, $\forall \sigma \in S_n$

$$\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(x_1) \dots \sigma(x_r))$$

Réciproquement, deux r -cycles γ_1 et γ_2 sont conjugués

dans S_n . $\exists \sigma \in S_n$ tel que $\gamma_2 = \sigma \circ \gamma_1 \circ \sigma^{-1}$.

Preuve du lemme :

Soit $\gamma = (x_1 \dots x_r)$ un r -cycle, soit $\sigma \in \mathfrak{S}_m$.

Mq $\sigma \circ \gamma \circ \sigma^{-1}$ est un r -cycle.

On cherche donc $\tilde{\gamma}$, r -cycle, tel que $\sigma \circ \gamma = \tilde{\gamma} \circ \sigma$.

Analyse:

On pose $\tilde{\gamma} = (y_1 \dots y_r)$.

$\forall k \in [1; r], (\sigma \circ \gamma)(x_k) = \sigma(x_{k+1})$

Et $(\tilde{\gamma} \circ \sigma)(x_k) = \tilde{\gamma}(\sigma(x_k)) = \sigma(x_{k+1})$

Synthèse: on pose $\tilde{\gamma} = (\sigma(x_1) \dots \sigma(x_r))$

Mq $\sigma \circ \gamma = \tilde{\gamma} \circ \sigma$

$\forall x \in \{x_1 \dots x_r\}$ on a $(\sigma \circ \gamma)(x) = (\tilde{\gamma} \circ \sigma)(x)$ par construction de $\tilde{\gamma}$.

$\forall x \in E \setminus \{x_1 \dots x_r\}, (\sigma \circ \gamma)(x) = \sigma(x)$

et comme $x \notin \{x_1 \dots x_r\}, \sigma(x) \notin \text{Supp}(\tilde{\gamma})$

donc $(\tilde{\gamma} \circ \sigma)(x) = \tilde{\gamma}(\sigma(x)) = \sigma(x)$.

Conclusion: $\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(x_1) \dots \sigma(x_r))$ est un r -cycle.

Réciproquement, soient γ_1 et γ_2 deux r -cycles. Mq ils

sont conjugués dans $\mathfrak{S}_m$, i.e. il existe $\sigma \in \mathfrak{S}_m$ tq

$\sigma \circ \gamma_1 \circ \sigma^{-1} = \gamma_2$ i.e. $\sigma \circ \gamma_1 = \gamma_2 \circ \sigma$

Analyse:

Soit $\varphi: E \setminus \{x_1 \dots x_r\} \rightarrow E \setminus \{y_1 \dots y_r\}$ une bijection.

$\forall x \in E \setminus \{x_1 \dots x_r\}, \varphi(x) \notin \text{Supp}(\gamma_2)$ donc $\gamma_2(\varphi(x)) = \varphi(x)$

$$\text{et } (\sigma \circ \gamma_1)(x) = \sigma(x)$$

on pose alors $\sigma(x) = \varphi(x)$ sur $E \setminus \{x_1, \dots, x_r\}$.

$$\text{D'autre part, } \forall k \in [1; r], (\sigma \circ \gamma_1)(x_k) = \sigma(x_{k+1})$$

$$\text{et } \gamma_2(\sigma(x_k)) = (\sigma \circ \gamma_1)(x_k) = \sigma(x_{k+1})$$

$$\text{on pose alors } \sigma(x_k) = y_k \quad \forall k \in [1; r]$$

Synthèse :

$$\text{Si } x \in \{x_1, \dots, x_r\}, \exists k \in [1; r] \text{ tq } x = x_k$$

$$\text{et } \sigma(x_k) = y_k \text{ donc } (\sigma \circ \gamma_1)(x_k) = \sigma(x_{k+1}) = y_{k+1}$$

$$\text{et } (\gamma_2 \circ \sigma)(x_k) = \gamma_2(y_k) = y_{k+1}$$

$$\text{et } \forall x \in E \setminus \{x_1, \dots, x_r\}, (\sigma \circ \gamma_1)(x) = \sigma(x) = \varphi(x)$$

$$\text{et } (\gamma_2 \circ \sigma)(x) = \gamma_2(\varphi(x)) = \varphi(x)$$

$$\uparrow$$

$$\varphi(x) \in E \setminus \{y_1, \dots, y_r\}$$

②.2 Supposons que γ_1 un 3-cycle, soit dans H .

$$\text{Alors } \forall \tilde{\gamma} \in \tilde{G}_m \text{ 3-cycles, } \exists \sigma \in \tilde{G}_m \text{ tq } \underline{\sigma \circ \gamma \circ \sigma^{-1}} = \tilde{\gamma}$$

$$\in H \text{ car } H \triangleleft \tilde{G}_m$$

$$\text{donc } \{3\text{-cycles}\} \subset H$$

$$\text{donc } A_m \subset H$$

$$\text{or } \#(H) \mid \#(\tilde{G}_m) \text{ (Lagrange) donc } \#(H) \mid n!$$

$$\text{donc } \exists p \in \mathbb{N} \quad p \#(H) = n!$$

$$\text{et comme } A_m \subset H \text{ alors } \frac{n!}{2} \mid \#(H)$$

donc $\exists q \in \mathbb{N}$ tq $\frac{q n!}{2} = \#(H)$.

donc $p q \frac{n!}{2} = n!$ i.e. $p q = 2$ donc $p = 2$ et $q = 1$

ou $q = 2$ et $p = 1$

donc $\#(H) = n!$ ou $\#(H) = \frac{n!}{2}$

or $H \neq \mathbb{S}_n$ donc $\#(H) = \frac{n!}{2} = \#(A_n)$ donc $H = A_n$.

(2.3) Mq $\exists \gamma \in \mathbb{S}_n$ un 3-cycle tel que $\gamma \in H$.

Soit $\sigma \in H \setminus \{\text{id}\}$, on veut construire un 3-cycle à partir de σ . Comme $H \triangleleft \mathbb{S}_n$, pour toute transposition τ de $\mathbb{S}_n$, $\tau \circ \sigma \circ \tau^{-1} \in H$ donc $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} \in H$.

On pose $\tilde{\sigma} = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$. $\tilde{\sigma}$ est-elle un 3-cycle?

On pose $\tilde{\sigma} = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$. $\tilde{\sigma}$ est-elle un 3-cycle?

Si $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = \text{id}$ alors $\tau \circ \sigma = \sigma \circ \tau$.

Lemme: pour $n \geq 3$, $\forall \sigma \in \mathbb{S}_n \exists \tau \in \mathbb{S}_n$ une transposition

telles que $\tau \circ \sigma \neq \sigma \circ \tau$ $\hookrightarrow \sigma \neq \text{id}_E$

Soit $x \in E$ tq $\sigma(x) \neq x$. On pose $y = \sigma(x)$.

Soit $z \in E \setminus \{x, y\}$. $(\sigma \circ (\tau \circ \tau^{-1}))(x) = \sigma(x) = y$.

$$((\tau \circ \tau^{-1}) \circ \sigma)(x) = x$$

Donc il suffit de prendre τ tq $\tau \circ \sigma \neq \sigma \circ \tau$

et $\tilde{\sigma} \neq \text{id}_E$. On note $\tau = (x \ y)$

$$\tilde{\sigma} = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (x \ y) \circ \sigma \circ (x \ y) \circ \sigma^{-1}$$

$$(\sigma \circ (x \ y) \circ \sigma^{-1})(\sigma(x)) = \sigma(y) \text{ et } (\sigma \circ (x \ y) \circ \sigma^{-1})(\sigma(y)) = \sigma(x)$$

et $\forall z \in E$ tq $\sigma^{-1}(z) \notin \{x, y\}$

$$(\sigma \circ (x \ y) \circ \sigma^{-1})(z) = \sigma(\sigma^{-1}(z)) = z$$

$$\text{donc } \sigma \circ (x \ y) \circ \sigma^{-1} = (\sigma(x) \ \sigma(y))$$

$$\text{donc } \tilde{\sigma} = (x \ y) \circ (\sigma(x) \ \sigma(y))$$

donc $\tilde{\sigma}$ est produit de deux transpositions.

Si $\sigma(x) = y$, comme $\tilde{\sigma} \neq \text{id}_E$, $\sigma(y) \neq x$ (et $\sigma(y) \neq y$)

$$\text{donc } \tilde{\sigma} = (x \ y)(y \ \sigma(y))$$

donc $\tilde{\sigma} = (x \ y \ \sigma(y))$ est un 3-cycle.

Même chose $\sigma(y) = x$, avec $\sigma(x) \neq y$ $\sigma(x) \neq x$.

donc comme $\tilde{\sigma} \in H$, H contient un 3-cycle, $\Delta_n = H$.

Si $\sigma(x) \notin \{x, y\}$ et $\sigma(y) \notin \{x, y\}$

Soit $z \in E \setminus \{x, y, \sigma(x), \sigma(y)\}$ (ok car $n \geq 5$)

$$\tilde{\sigma} = (x \ y)(\sigma(x) \ \sigma(y)) \in H \text{ donc}$$

$$(z \ \sigma(y)) \tilde{\sigma} (z \ \sigma(y)) \in H$$

$$\text{or } \underbrace{(z \ \sigma(y))}_{\in \tilde{G}_m} \underbrace{(x \ y)(\sigma(x) \ \sigma(y))}_{\in H} \underbrace{(z \ \sigma(y))}_{\in \tilde{G}_m} = \underbrace{(x \ y)(\sigma(x) \ z)}_{\in H}$$

$$\text{donc } (x \ y)(\sigma(x) \ \sigma(y))(x \ y)(\sigma(x) \ z) \in H$$

$$\text{or } (x \ y)(\sigma(x) \ \sigma(y))(x \ y)(\sigma(x) \ z) = (\sigma(x) \ z \ \sigma(y)) \quad \square$$

Compléments :

Théorème 1 : G_m est engendré par les cycles [Rem 45]

Soit $\sigma \in G_m \setminus \{\text{id}_E\}$. Soit $O_1, \dots, O_r$ les σ -orbites deux-à-deux distinctes de σ , et $p \leq r$ tel que $O_p, \dots, O_r$ sont réduites à un point.

on a alors $E = \bigcup_{k=1}^r O_k$

On note $\forall k \in [1; r], \gamma_k$ tq $\gamma_k(x) = \sigma(x)$ si $x \in O_k$
 $\gamma_k(x) = x$ si $x \notin O_k$

on a bien $\gamma_k \in S(E)$. Si O_k est réduite à un point alors $\gamma_k = \text{id}_E$, sinon :

$$\begin{aligned} \forall x \in O_k, \quad \text{orb}_{\gamma_k}(x) &= \{ \gamma_k^m(x); m \in \mathbb{Z} \} \\ &= \{ \sigma^m(x); m \in \mathbb{Z} \} = \text{orb}_{\sigma}(x) = O_k. \end{aligned}$$

Donc γ_k a une seule orbite non réduite à un point, O_k .

Donc γ_k est un cycle.

$$\text{Mq } \sigma = \prod_{k=1}^r \gamma_k$$

$\forall x \in E, \exists ! k_0 \in [1; r]$ tq $x \in O_{k_0}$.

$$(\gamma_r \circ \dots \circ \gamma_1)(x) = \gamma_r(\dots(\gamma_1(x))\dots)$$

et $\forall j \neq k_0, \gamma_j(x) = x$ et $\sigma(x) \in O_{k_0}$ donc $\gamma_j(\sigma(x)) = \sigma(x)$.

$$\begin{aligned} \text{Donc } \gamma_r(\dots(\underbrace{\gamma_{k_0}(x)}_{= \sigma(x)})\dots) &= \sigma(x) \\ &\in O_{k_0} \end{aligned}$$

Cette décomposition est unique à ordre près.

Soit $\sigma = \prod_{k=1}^r \gamma_k$ et $\sigma = \prod_{k=1}^p \delta_k$ deux décompositions

en produit de cycles à supports disjoints de σ . On

note Θ_k les supports des γ_k et $\mathcal{Q}_k$ les supports des δ_k .

Soit $k \in \llbracket 1; r \rrbracket$, $\Theta_k = \text{orb}_\sigma(x)$, et $\exists k' \in \llbracket 1; p \rrbracket$ tq

$\text{orb}_\sigma(x) = \mathcal{Q}_{k'}$. Donc $\forall x \in \Theta_k$, $\gamma_k(x) = \delta_{k'}(x)$ et

$\forall x \notin \Theta_k$, $\gamma_k(x) = x = \delta_{k'}(x)$ donc $\gamma_k = \delta_{k'}$ et on

a unicité à ordre près.

De plus, l'ordre de σ est $\mu = \text{ppcm}_{k \in \llbracket 1; r \rrbracket} (\text{ord}(\gamma_k))$ où $\text{ord}(\gamma_k)$ est l'ordre de γ_k . (facile à vérifier).