

103
104
105
108

A_n est simple
pour $n \geq 5$

- Algèbre, le grand cambout, BERHUY, p 275
- Maths pour l'ingez, Rambaldi, p 49

BER 215

Def 1: Le groupe alterné, noté $A(E)$, est l'ensemble des permutations de $S(E)$ de signature 1. Il est distingué dans $S(E)$ comme noyau d'un morphisme de groupes, et est même d'indice 2.

On a : $|A(E)| = \frac{n!}{2}$

- Si $n = 2$: $S(E) = \{id, (1\ 2)\}$ donc $A(E) = \{id\}$
- Si $n = 3$: $S(E) = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

donc A_3 est cyclique engendré par $(1\ 2\ 3)$ car
 $|A_3| = \frac{3!}{2} = 3$ et le cycle $(1\ 2\ 3)$ est d'ordre 3.

BER 216

Lemme 2: Soit E un ensemble à n éléments. On suppose que $n \geq 3$. Alors $A(E)$ est engendré par chacune des familles suivantes:

- 1) les produits de deux transpositions
- 2) les 3-cycles

Dém : On sait que $S(E)$ est engendré par les transpositions. Ainsi $\forall \sigma \in S(E)$: $\sigma = \tau_1 \dots \tau_n$ où τ_i est une transposition. On a $\epsilon(\sigma) = (-1)^n$ et alors $\sigma \in A(E)$ si n est pair. Donc les éléments de $A(E)$ sont les produits d'un nombre pair de transpositions. Ainsi, les produits de deux transpositions engendrent $A(E)$.

Pour montrer 2), il suffit alors de montrer qu'un produit de deux transpositions est un produit de 3-cycles.

ROM 49

Soit τ_1 et $\tau_2 \in S(E)$ deux transpositions.

- Si elles ont le même support, $\tau_1 = \tau_2$ et donc

- $\tau_1 \tau_2 = \text{id}_E = \gamma^3$ pour n'importe quel 3-cycle.
- Si $\text{Supp}(\tau_1) \cap \text{Supp}(\tau_2) = \{x\}$, alors $\tau_1 = (x \ y)$ et $\tau_2 = (x \ z)$ avec x, y, z distincts.
Alors: $\tau_1 \tau_2 = (x \ y)(x \ z) = (y \ x)(x \ z) = (y \ x \ z) = (x \ z \ y)$
 - Si $\text{Supp}(\tau_1) \cap \text{Supp}(\tau_2) = \emptyset$, alors $\tau_1 = (x \ y)$ et $\tau_2 = (z \ t)$ avec x, y, z, t distincts.
Alors: $\tau_1 \tau_2 = (x \ y)(z \ t) = (x \ y)(y \ z)(y \ z)(z \ t)$
 $= (x \ y \ z)(y \ z \ t)$ $\square$

BER 217

Lemme 3: Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}(E)$.

Dém: Soit $\sigma = (a_1 \ a_2 \ a_3)$ et $\sigma' = (b_1 \ b_2 \ b_3)$ deux 3-cycles. Alors on veut que il existe $\gamma \in S(E)$ tel que $\gamma \sigma \gamma^{-1} = \sigma'$ (car les 3-cycles sont conjugués dans $S(E)$)

Si $\gamma \in \mathcal{A}(E)$, c'est fini.

Si non, $\varepsilon(\gamma) = -1$. Comme $n \geq 5$, il existe $c \neq d$ distincts de b_1, b_2, b_3 . On pose alors $\gamma' = (cd)\gamma$. Par construction, $\gamma' \in \mathcal{A}(E)$ car $\varepsilon(\gamma') = \varepsilon((cd)) \cdot \varepsilon(\gamma) = (-1)(-1) = 1$

Mais alors:

$$\begin{aligned} \gamma' \sigma \gamma'^{-1} &= (cd) \gamma \sigma \gamma^{-1} (cd)^{-1} \\ &= (cd) (b_1 \ b_2 \ b_3) (cd)^{-1} \\ &= (b_1 \ b_2 \ b_3) (cd) (cd) = (b_1 \ b_2 \ b_3) = \sigma' \end{aligned}$$

car $(b_1 \ b_2 \ b_3)$ et $(c \ d)$ sont à supports disjoints donc commutent.

On a le résultat annoncé. $\square$

Def 4: Un groupe est simple s'il n'a pas d'autres sous-groupes distingués que $\{\text{id}\}$ et lui-même.

BER 217 Théorème 5: Soit $n \geq 3$. Alors le groupe $A(E)$ est simple si et seulement si $n \neq 4$.

Dém:

- Si $n = 3$, alors $A(E)$ est cyclique d'ordre 3 donc est simple (on peut aussi dire que $|A(E)| = 3$ et utiliser le théorème de Lagrange).

- Si $n = 4$, on pose $E = \{a, b, c, d\}$
Soit $H = \{id_E, (ab)(cd), (ac)(bd), (ad)(bc)\}$
Alors H est un sous-groupe de A_4 . Il est distingué dans S_4 car le conjugué d'une permutation de type $(2, 2)$ est une permutation de type $(2, 2)$. Donc A_4 n'est pas simple.
(H est appelé le groupe de Klein)

Soit $n \geq 5$

- Soit $H \triangleleft A(E)$ avec $H \neq \{id_E\}$. On aq $H = A(E)$
On remarque que:

1) Si H contient un 3-cycle, alors $H = A(E)$

d'après le lemme 3

En effet, alors H contient tous les 3-cycles car ceux-ci sont conjugués dans $A(E)$ ^①, et H est un SGD dans $A(E)$. Comme $A(E)$ est engendré par les 3-cycles (d'après le lemme 2), alors $H = A(E)$.

2) Si $\sigma \in H$ et $\tau \in A(E)$, alors $\sigma\tau\sigma^{-1}\tau^{-1} = [\sigma, \tau] \in H$

En effet, comme H sous-groupe, $\sigma^{-1} \in H$ et comme il est distingué dans $A(E)$, $\tau\sigma^{-1}\tau^{-1} \in H$.

Donc $[\sigma, \tau]$ aussi.

3) Si H contient un produit de deux transpositions σ

Supports disjoints, alors H contient un 3-cycle.

En particulier $H = \mathcal{A}(E)$

En effet, soit $\sigma = (ab)(cd) \in H$ avec a, b, c, d distincts. Comme $n \geq 5$, on choisit $e \in E \setminus \{a, b, c, d\}$

Soit $\tau = (a b e)$. On a $\sigma^{-1} = (cd)(ab)$. Alors :

$$\begin{aligned}\tau \sigma^{-1} \tau^{-1} &= \tau (cd) \tau^{-1} \tau (ab) \tau^{-1} \\ &= (\tau(c) \tau(d)) (\tau(a) \tau(b)) \\ &= (cd)(be)\end{aligned}$$

$$\text{Donc : } [\sigma, \tau] = (ab)(cd)(cd)(be) = (a b e)$$

D'après 2), on a que $(a b e) \in H$ et par 1), on a que $H = \mathcal{A}(E)$.

On en conclut qu'il suffit de montrer que H contient un 3-cycle ou une double transposition à SD.

Soit $\sigma \in H \setminus \{\text{id}_E\}$ et $\sigma = \prod_{i=1}^r \sigma_i$ sa décomposition en cycles à SD.

a) Si σ_i est un 3-cycle pour tout i

• Si $n=1$, c'est OK : $H = \mathcal{A}(E)$

• Sinon si $n \geq 2$, on a $\sigma_1 = (a b c)$ et $\sigma_2 = (d e f)$

$$\text{Soit } \tau = (a d)(b e)$$

$$\text{Alors d'après 2), } \sigma' = [\sigma, \tau] \in H$$

$$\begin{aligned}\text{On : } \sigma \tau \sigma^{-1} &= (\sigma(a) \sigma(d)) (\sigma(b) \sigma(e)) \\ &= (b e)(c f)\end{aligned}$$

et alors :

$$\sigma' = (b e)(c f)(b e)(a d) = (c f)(a d) \in H$$

car à SD donc commutent

$$\text{Donc } H = \mathcal{A}(E).$$

b) Si σ_i n'est pas un 3-cycle (grosse à renommier)

On admet provisoirement l'existence de $F \subset E$ tq $|F| = 3$ et $|F \cup \sigma(F)| = 4$ (donc $\sigma(F) \neq F$)

Soit τ un cycle de support F . C'est un 3-cycle et alors $\tau \in A(E)$.

De plus, $\text{supp}(\sigma\tau\sigma^{-1}) = \sigma(F) \neq F = \text{supp}(\tau)$

Ainsi $\sigma\tau\sigma^{-1} \neq \tau$ d'où $\sigma' = [\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \neq \text{id}_E$

D'après 2), on a $\sigma' \in H$.

De plus, on a :

$\text{supp}(\sigma') \subset \text{supp}(\sigma\tau\sigma^{-1}) \cup \text{supp}(\tau^{-1}) = \sigma(F) \cup F$

Comme $|\sigma(F) \cup F| = 4$ et que $\sigma' \neq \text{id}_E$, alors :

- soit σ' est un 3-cycle donc gagné
- soit σ' est une double transposition : gagné
- soit σ' est une transposition : impossible car $\epsilon(\sigma) = 1$
- soit σ' est un 4-cycle : impossible car $\epsilon(\sigma) = 1$

Donc $H = A(E)$

On montre finalement l'existence de F

- Si $\exists \sigma_i$ tq σ_i est de longueur ≥ 4 :

$\sigma_i = (a \ b \ c \ d \ \dots)$. On pose alors $F = \{a, b, c, d\}$ et alors $|F| = 3$ et $F \cup \sigma(F) = \{a, b, c, d\}$ donc $|F \cup \sigma(F)| = 4$.

- Sinon si les σ_i ne sont que de longueur 2 ou 3
Comme on a supposé au préalable que tous les σ_i ne sont pas des 3-cycles, il existe alors au moins un 2-cycle, et comme $\epsilon(\sigma) = 1$, il y en a un autre. On prend $(a \ b)$ et $(c \ d)$.
On pose $F = \{a, b, c\}$. Alors $|F| = 3$ et $F \cup \sigma(F) = \{a, b, c, d\}$.

On a bien montré le résultat voulu. $\square$

Si $m=2$, S_2 est commutatif

Remarques:

1) On a un lemme sur le centre de $S(E)$:

ROM 56

Lemme 6: Si $n \geq 3$, alors $S(E)$ n'est pas commutatif (ie le centre est trivial)

Dém: Soit x_1, x_2, x_3 distincts dans E .

Soit $\tau_1 = (x_1 \ x_2)$ et $\tau_2 = (x_2 \ x_3)$

On a: $\tau_2 \circ \tau_1(x_1) = \tau_2(x_1) = x_1$

et $\tau_1 \circ \tau_2(x_1) = \tau_1(x_1) = x_2 \neq x_1$

Donc $\tau_2 \circ \tau_1 \neq \tau_1 \circ \tau_2$ et $S(E)$ n'est pas commutatif

2) On obtient un corollaire sur les SGO de $S(E)$:

BER 220

Corollaire 7: Soit $n \geq 2$. Si $n \neq 4$, les SGO de $S(E)$ sont $\{id_E\}$, $A(E)$ et $S(E)$

Dém: Si $m=2$, c'est OK car $A(E) = \{id\}$

Ainsi soit $n \geq 3$ et $n \neq 4$. Soit H un SGO de $S(E)$

Alors par prop, $H \cap A(E)$ est un SGO de $A(E)$

donc d'après le théorème 5, on a $H \cap A(E) = \{id_E\}$

ou bien $H \cap A(E) = A(E)$

• Si $H \cap A(E) = A(E)$, alors $A(E) \subset H$.

- Si $H \subset A(E)$, alors $H = A(E)$

- Si H contient σ_0 de signature -1 , il contient alors 2 classes à gauche modulo $A(E)$ distinctes (à savoir $A(E)$ et $\sigma_0 A(E)$) et comme $A(E)$ est d'indice 2, alors H contient $S(E)$
Donc $H = S(E)$

• Si $H \cap A(E) = \{id\}$, alors la restriction de la signature induit un morphisme injectif $H \hookrightarrow \{\pm 1\}$
Donc $|H| \leq 2$

Par l'absurde, on suppose que $|H| = 2$. Soit $\tau \in H$
tel que $\tau \neq id$. Soit $\sigma \in S(E)$ (comme
 $\sigma \tau \sigma^{-1} \in H$ et $\sigma \tau \sigma^{-1} \neq id_E$ car $\tau \neq id$,

On a $\tau \tau \tau^{-1} = \tau$. Ainsi $\tau \in Z(S(E))$. Or $n \geq 3$
donc le centre est trivial, donc $\tau = \text{id}$. Contradiction.
Ainsi $|H| = 1$ et alors $H = \{\text{id}\}$.

Attention, le résultat est faux pour $n = 4$. En effet, le
groupe de Klein est distingué dans $S(E)$ et est
distinct de $\{\text{id}\}$, $A(E)$ et $S(E)$.

- 3) Les 3-cycles ne sont pas conjugués dans A_4 car sinon
ils formeraient une orbite mais comme il y en a 8,
on aurait que $8 \nmid 12$. Contradiction.