Пример

$G \mid S \equiv$ група дејствује на скуп S.

Посматрамо дејство групе G на скуп G, дакле $G \mid G$.

$$\boxed{g \longrightarrow \alpha_g}$$ ← хомоморфизам G на S_G

$$\alpha_g : G \to G$$

$$\alpha_g(x) = g^{-1} x g \quad \text{(конјугација)}$$

Пример

Претпоставимо да група G дејствује на скуп X, $G \mid X$.

Уведимо релацију $\equiv$ на скуп X, на начин

$$x \equiv y \iff \exists g \in G, \text{ тако да } y = x^g \quad (x, y \in X)$$

Лако је показати да је $\equiv$ заправо релација еквиваленције.

Скуп X се последично може представити као дисјункта унија класа еквиваленције.

Дефиниција

Ако G, група, дејствује на скуп X, онда скуп

$$\mathcal{O}(x) = \{ x^g \mid g \in G \}, \quad x \in X$$

називамо **орбитом** елемента x у односу на дато дејство групе G на X.

Заправо, $\mathcal{O}(x)$ је класа еквиваленције елемента x у односу на релацију дату у претходном примеру.

За дато $x \in X$, скуп

$$G_x = \{ g \in G \mid x^g = x \}$$

називамо **стабилизатор** елемента x у односу на дато дејство.

! Лако се показује да је G_x група, односно подгрупа групе G.

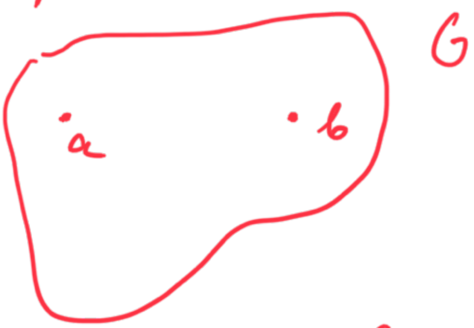
Пример

Посматрајмо дејство групе G на саму себе, $G \mid G$, на начин

$$g \longrightarrow \tau_g, \quad g \in G$$

$$\tau_g(a) = ga, \quad a \in G.$$

За $a \in G$, шта је $\mathcal{O}(a)$?



Да ли постоји $g \in G$, тако да

$$ga = b$$

Наравно $g = ba^{-1}$, што значи да

$$\tau_{ba^{-1}}(a) = b$$

Дакле, $\mathcal{O}(a) = G$.

Стабилизатор G_a, за $a \in G$ је $\{1\}$, јер $a = \tau_g(a) = ga \Rightarrow g = 1$.

<u>Дефиниција</u>

Кажемо да група G дејствује <u>транзитивно</u> на скуп X ако за дато дејство важи да је за $x \in X$ произвољно

$$\mathcal{O}(x) = X.$$

<u>пример</u>

Нека група G дејствује на саму себе конјугацијом.

За дато $a \in G$,

$$\mathcal{O}(a) = \{ g^{-1} a g \mid g \in G \}$$

$= [a]$ (класа конјугације елемента a)

С друге стране, за $a \in G$

$$G_a = \{ g \in G \mid g^{-1} a g = a \}$$

$$= \{ g \in G \mid ag = ga \}$$

$= C_G(a)$ (централизатор елемента a у групи G)

<u>задатак</u>

Нека група G дејствује на себе конјугацијом. Претпоставимо за $a, b \in G$, да постоји $g \in G$, тако да $g^{-1} a g = b$.

Испитати однос G_a и G_b.

(централизатори су конјуговани)

([illegible])

<u>Пример</u>

Свака група G дејствује на $\mathrm{Sub}(G)$ конјугацијом.

Наиме, за $a \in G$ посматрамо

$$\pi_a : H \to a^{-1} H a, \quad H \in \mathrm{Sub}(G).$$

$$a \to \pi_a$$

Шта је стабилизатор за $H \in \mathrm{Sub}(G)$?

$$G_H = \{a \in G \mid a^{-1} H a = H\}$$
$$= \{a \in G \mid aH = Ha\}$$

$\equiv$ нормализатор подгрупе H у G

$\equiv N_G(H)$.

<u>Последица</u>

Ако G дејствује на скуп X, онда је, за коначан скуп X,

$$|X| = \sum_{i \in I} |\mathcal{O}(x_i)|,$$

где је x_i, $i \in I$ скуп различитих представника дисјунктних орбита.

Теорема

Ако G дјелује на скуп X и $x \in X$,

онда је

$$|\mathcal{O}(x)| = [G : G_x]$$

доказ

Означимо са $G : G_x$ скуп свих

лијевих косета G_x у G.

Успостављамо бијекцију

$$f : G : G_x \longrightarrow \mathcal{O}(x)$$

$$f(gG_x) \longrightarrow x^g, \quad g \in G.$$

доказати:

- f је добро дефинисано
- f је инјекција
- f је сурјекција

Посљедица

Ако коначна група G дјелује на скуп X,

онда је број елемената у свакој орбити,

$\mathcal{O}(x)$, $x \in X$, дјелитељ $|G|$.

доказ: директна посљедица претходне и

Лагранжове теореме.

Последица

Ако коначна група G дејствује на скуп G, онда је број „конјугата" елемента $x \in G$ једнак индексу његовог централизатора, односно

$$|[x]| = |G : C_G(x)|.$$

Последица

Ако коначна G дејствује на $Sub(G)$ конјугацијом, онда је број „конјугата" $H \in Sub(G)$ једнак $|G : N_G(H)|$.

Теорема (Коши)

Нека је G коначна група, а p прост број такав да $p \mid |G|$.
Онда постоји $g \in G$, тако да $ord(g) = p$.

доказ

Нека је $|G| = p \cdot m$, $m \in \mathbb{N}$.
Доказ изводимо индукцијом по m.
За $m = 1$, тврђење је тривијално.
Нека је $m > 1$.
За $x \in G$ знамо да је

За $x \in G$, знамо да је

$$|[x]| = |G : C_G(x)|,$$ где

$C_G(x)$ централизатор елемента x у групи G.

Нека је $x \notin Z(G)$. ($Z(G) \equiv$ центар групе).

Онда је $|C_G(x)| < |G|$.

Уколико $p \mid |C_G(x)|$, онда по индуктивној претпоставци, постоји елемент групе $C_G(x)$ реда p.

Нека је $p \nmid |C_G(x)|$.

На основу Лагранжове теореме

$$|G| = |G : C_G(x)| \cdot |C_G(x)|$$

Дакле, закључујемо да

$$p \mid |G : C_G(x)|.$$

Посматрајући дејство групе G на саму себе конјугацијом

$$|G| = \sum_{i \in I} |[x_i]|$$

Ако је $x_i \in Z(G)$, онда $[x_i] = \{x_i\}$.

То значи

$$|G| = |Z(G)| + \sum_{j\in J} |[x_j]|$$

при чему $x_j \notin Z(G)$, $j \in J$.

С друге стране

$$|[x_j]| = |G : C_G(x_j)|,$$

па онда

$$\boxed{|G| = |Z(G)| + \sum_{\substack{j\in J \\ x_j \notin Z(G)}} |G : C_G(x_j)|}$$

једначина класа групе G.

Претпоставимо да $p \nmid |C_G(x_j)|$ за $j \in J$, односно $x_j \notin Z(G)$.

Онда, за свако $j \in J$, $p \mid |G : C_G(x_j)|$, $x_j \notin Z(G)$.

То значи да $p \mid \sum_{\substack{j\in J \\ x_j \notin Z(G)}} |G : C_G(x_j)|$

Закључујемо да $p \mid |Z(G)|$.

Међутим, $Z(G)$ је Абелова група, па следи да $Z(G)$ мора имати елемент реда p, на основу претходно доказане теореме.

Теорема

Ако је p прост број, а G p-група ($|G|=p^k$, $k\in\mathbb{N}$) онда $Z(G)\neq\{1\}$.

доказ

На основу једначине класа

$$|G| = |Z(G)| + \sum_{\substack{j\in J\\ x_j\notin Z(G)}} |G : C_G(x_j)|$$

Пошто је за свако $j\in J$, $|C_G(x_j)| < |G|$, а G p-група онда $|C_G(x_j)| = p^{m_j}$, $m_j \leq k-1$.

Дакле, $p \mid |G : C_G(x_j)|$ за $j\in J$

$$\Rightarrow p \mid \sum_{\substack{j\in J\\ x_j\notin Z(G)}} |G : C_G(x_j)|.$$

Пошто $p \mid |G|$, онда јасно из једначине класа следи $p \mid |Z(G)|$.

Последица

Ако је p прост број, онда је свака група реда p^2 Абелова

G, реда p, ...

<u>следи</u>

$|G| = |G:Z(G)| \cdot |Z(G)|$

за претпоставку $|Z(G)| = p$

$\Rightarrow G:Z(G)$ циклична и реда p.

{Показати да ако је $G:Z(G)$ циклична, онда G мора бити Абелова}.

Лема

Нека је G p-група, таква да $|G| = p^m$, $m \in \mathbb{N}$. Онда G садржи нормалну подгрупу реда p^k, за свако $k \le m$.

доказ

Индукција по m.

За $m=1$, тривијално.

У сваком случају, $Z(G) \neq \{1\}$.

Знамо $Z(G)$ је p-група, па постоји подгрупа $Z \le Z(G)$ реда p.

Очигледно, $Z \trianglelefteq G$.

$Z \;-\; - \; \{1\}$

$$|G/Z| = p^{m-1}$$

По индуктивној претпоставци, G/Z садржи нормалну подгрупу H^* реда p^{k-1}, за $k<m$.

По теореми о кореспонденцији, постоји $H \leq G$, тако да је $H^* = H/Z$.

Одатле следи да је $|H| = p^k$, као и чињеница да је $H \trianglelefteq G$.

Дефиниција

Група $G \neq \{1\}$ је проста, ако G нема нормалних подгрупа сем $\{1\}$ и G.

Лема

Абелова група G је проста ако и само ако је коначна и простог реда.

Доказ

Ако је G простог реда, тврђење је тривијално.

Обрнуто, нека је G проста група.

Нека је $x \in G$ произвољно. Подгрупа $\langle x \rangle$ је нормална, а пошто је G проста

$$G = \langle x \rangle.$$

Нека је x бесконачног реда.

Подгрупа $\langle x^2 \rangle \neq G$ и $\langle x^2 \rangle \neq \{1\}$.

Дакле, x не може бити бесконачног реда.

То значи $ord(x) = m$, $m \in \mathbb{N}$.

<u>Питање:</u> Да ли m може да буде сложен број?

Ако је m сложено, онда постоји прост број q тако да $q \mid m$, $q < m$.

То значи да постоји подгрупа $Q \leq \langle x \rangle$ реда q која није тривијална, а што је контрадикција.

<u>Лема</u>

Сви 3-циклуси су конјуговани у A_5.

<u>доказ</u>

Нека је $G = S_5$ (симетрична група на 5 елемената)

$\alpha = (123)$, $H = A_5$.

Колико има 3-циклуса у S_5?

$$\binom{5}{3} \cdot 2! = \frac{5 \cdot 4 \cdot \cancel{3}}{1 \cdot \cancel{2} \cdot \cancel{3}} \cdot \cancel{2} = 20.$$

$$|[\alpha]| = 20.$$

С друге стране $|[\alpha]| = \dfrac{|S_5|}{|C_{S_5}(\alpha)|}$

$$20 = \frac{120}{|C_{S_5}(\alpha)|} \Rightarrow |C_{S_5}(\alpha)| = 6.$$

Ми смо заинтересовани за

$|[\alpha]_{A_5}|$.

Знамо, $$|[\alpha]_{A_5}| = \frac{|A_5|}{|C_{A_5}(\alpha)|}$$

Међутим $C_{A_5}(\alpha) \subseteq C_{S_5}(\alpha)$.

Шта све комутира са α?

$\alpha = (123)$

$$\underbrace{id, \alpha, \alpha^2}_{\text{парне пермутације}}, \underbrace{(45), (45)\alpha, (45)\alpha^2}_{\text{непарне пермутације}}$$

$$|C_{A_5}(\alpha)| = |\{id, \alpha, \alpha^2\}| = 3.$$

$$|[\alpha]_{A_5}| = \frac{|A_5|}{|C_{A_5}(\alpha)|} = \frac{60}{3} = 20.$$

Лема

Ако је $n \geq 3$, онда је сваки елемент у A_n 3-циклус или је производ 3-циклуса.

доказ

Ако је $\alpha \in A_n$, онда је α производ парног броја транспозиција

$$\alpha = \tau_1 \tau_2 \dots \tau_{2m-1} \tau_{2m}$$

Подразумијевамо $\tau_i \neq \tau_{i+1}$, $1 \leq i \leq 2m-1$ јер у супротном $\tau_i \cdot \tau_{i+1} = id$.

Посматрамо τ_i, τ_{i+1} и закључујемо да τ_i и τ_{i+1} могу бити

- дисјунктне
- имати 1 заједнички елемент

Нека је $\tau_i = (s\,j)$, $\tau_{i+1} = (s\,k)$

Онда $\tau_i \tau_{i+1} = (s\,k\,j)$.

Ако $\tau_i = (s\,j)$, $\tau_{i+1} = (l\,k)$

онда

$$\tau_i \tau_{i+1} = \underbrace{(s\,j)(j\,l)}\underbrace{(j\,l)(l\,k)}$$

$\equiv$ производ 2 3-циклуса.

Последица

Група A_5 је генерисана 3-циклусима.

Ш

Теорема

A_5 је проста група.

доказ

Нека је $H \trianglelefteq A_5$, $H \neq \{1\}$.

Докажимо да $H = A_5$.

Пошто је H нормална, онда сви конјугати произвољног елемента $a \in H$ су у H.

То значи да ако H садржи бар један 3-циклус, онда их садржи све.

По претходној леми, ако H садржи све 3-циклусе, онда $H = A_5$.

Какви елементи, у смислу цикличне структуре, могу бити у A_5?

$(\cdot\cdot\cdot)$

$(\cdot\cdot)(\cdot\cdot)$

$(\cdot\cdot\cdot\cdot\cdot)$

Ако $\sigma = (123) \in H$, онда је доказ завршен.

Претпоставимо да

$\underbrace{(12)(34)}_{\sigma} \in H$

2. $\tau = (12)(35)$ елемент

За $\tau = (12)(35)$, елементи

$$\underbrace{(\tau \sigma \tau^{-1})}_{\in H} \underbrace{\sigma^{-1}}_{\in H} \text{ је из } H,$$

а $(\tau \sigma \tau^{-1}) \sigma^{-1} = \underbrace{(354)}_{3\text{-циклус}}$.

Ако је $\sigma = (12345) \in H$,

а $\rho = (132)$, онда

$$(\rho \sigma \rho^{-1}) \sigma^{-1} \in H$$

а $\rho \sigma \rho^{-1} \sigma^{-1} = \underbrace{(134)}_{3\text{-циклус}}$.

Дакле, у сваком случају, $H = A_5$, па је A_5 проста група.

<u>Зад</u>

Испитати да ли је A_4 проста група.