- у коначној групи G, за свако $a \in G$ важи $a^{|G|} = 1$.

Нека је p неки прост број и $a \in \mathbb{Z}$.

Имамо 2 случаја:

а) $НЗД(a, p) = 1$

б) $НЗД(a, p) = p$

Посматрамо систем остатака по модулу p, $\mathbb{Z}_p$.

У односу на модуларно сабирање $\mathbb{Z}_p$ је Абелова група.

У односу на модуларно множење, $\mathbb{Z}_p \setminus \{0\}$ Абелова група.

Дакле, у односу на посматрано $a \in \mathbb{Z}$, имамо $[a]_p \in \mathbb{Z}_p \setminus \{0\}$ или $[a]_p = 0$.

$|\mathbb{Z}_p \setminus \{0\}| = p - 1$. ($[a]_p \in \mathbb{Z}_p \setminus \{0\}$)

$[a]_p^{p-1} = 1 \iff a^{p-1} \equiv 1 \pmod{p}$

Тј. сетили смо да је $[a]_p = 0$, односно

$a \equiv 0 \pmod p \Rightarrow a^p \equiv 0 \pmod p$

$\Rightarrow a^p \equiv a \pmod p$ ∎

Лема Нека је p прост број и $a \in \mathbb{Z}$.
Онда је $a^p \equiv a \pmod p$ (Ферма)

Лема (Ојлер)
Нека су $r, m \in \mathbb{Z}$, такви да је
$\text{НЗД}(r, m) = 1$. Онда је

$$r^{\varphi(m)} \equiv 1 \pmod m.$$

Лема (Вилсон)
Цијели број p је прост ако и само ако
важи $(p-1)! \equiv -1 \pmod p$

скица $[0], [2], \ldots, [p-1]$
да у скупу $\{[2], \ldots, [p-2]\}$
сваки елемент није себи инверз
$[2] \cdot \ldots \cdot [p-2] \equiv 1 \mod p.$

- хомоморфизам
  - мономорфизам
  - епиморфизам
  - изоморфизам

- симетрична група S_n.

  Нека је A скуп од n елемената

  $S_n = \{ f : A \to A \mid f \equiv \text{бијекција} \}$

  $|S_n| = n!$

  $(S_n, \circ)$ група.

- циклична декомпозиција пермутације

- циклични структура пермутације

  пример: $\alpha = (123)(4)(5) \in S_5$

  $\text{type}(\alpha) = 1^2 3^1$ (формално)

  2 циклса дужине 1, 1 циклус дужине 3

  $\beta = (12)(345)(6)(78) \in S_8$

  $\text{type}(\beta) = 1^1 2^2 3^1$

- <u>транспозиција</u> (циклус дужине 2)

- Свака пермутација се може представити као производ транспозиција.
- $(i_1 i_2 \dots i_r) = (i_2 i_3 \dots i_r i_1) = \dots = (i_r i_1 \dots i_{r-1})$

r циклична поједнака

- Сваку пермутацију можемо представити као производ дисјунктних циклуса и то представљање је јединствено до на поредак

Пример:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$$

$$= (1\ 6)(2\ 4)(3\ 7\ 8\ 9)$$

Посматрајмо $(3\ 7\ 8\ 9) \overset{?}{=} (3\ 9)(3\ 8)(3\ 7)$

Лема Сваку пермутацију можемо представити у облику производа транспозиција. У оштем случају, то представљање није јединствено, али је за свака два представљања у облику производа транспозиција исте

Парност броја инверзија.

Лема За свако циклус $(i_1\ i_2\ \dots\ i_r) \in S_n$ важи

1) $(i_1\ i_2\ \dots\ i_r)^{-1} = (i_r\ i_{r-1}\ \dots\ i_2\ i_1)$

2) $\beta = (i_1\ i_2\ \dots\ i_r)$

$$\beta^k(i_j) = i_{(k+j) \bmod r}.$$

Пример

Колико има различитих r-циклуса у S_n?

$$\frac{\binom{n}{r} \cdot r!}{r} = \binom{n}{r} \cdot (r-1)!$$

Типови пермутација у S_4

цикличка структура	број
$(.)(.)(.)(.)$	1
$(..)(.)(.)$	6
$(...)(.)$	8
$(....)$	6
$(..)(..)$	3

Лема Ако су $\alpha, \beta \in S_n$, онда

$\alpha \beta \alpha^{-1}$ има исту цикличну структуру

као β.

Лема Пермутације β и α имају исту

цикличну структуру ако и само ако

постоји $\sigma \in S_n$ тако да

$$\beta = \sigma \alpha \sigma^{-1}$$

Пример

Нека је $\gamma = (i_1\ i_2 \dots i_r) \in S_n$, $\alpha \in S_n$.

Онда је

$$\alpha \gamma \alpha^{-1} \equiv (\alpha(i_1)\ \alpha(i_2) \dots \alpha(i_r))$$

Нека је $t = \alpha(i_j)$

$$\underbrace{\alpha \gamma \alpha^{-1}}_{\downarrow}(t) \equiv \alpha(i_{j+1})$$

$$\alpha(i_j) \to \alpha(i_{j+1})$$

$$\beta = (1\,2\,3)(1\,4)(1\,5)$$

$\alpha = (5\,2\,4)\,(1)\,(3)$

$\sigma \alpha \sigma^{-1} \equiv (\sigma(1)\ \sigma(2)\ \sigma(3))\,(\sigma(4))\,(\sigma(5))$

$\equiv (5\,2\,4)\,(1)\,(3)$

$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\,5\,3\,4)\,(2)$

Дефиниција За елементи a, b дате G кажемо да су **конјуговани**, ако постоји $c \in G$, тако да $a = c b c^{-1}$

У групи G, можемо да уведемо релацију $\sim$ (конјугације)

$a \sim b \equiv a$ и b су конјуговани

Релација $\sim$ је

- рефлексивна
- симетрична
- транзитивна

Релација конјугације је релација еквиваленције у групи G.

- Јасно је да је у Абеловој групи G за свако $a \in G$, класа конјугације

$$[a]_\sim = \{a\}.$$

- У неком смислу, класе конјугације, односно саме конјугације, мере „дефинитисаност" групе G у односу на комутативност.

Лема* Пермутације $\alpha, \beta \in S_n$ имају исту цикличну структуру ако и само ако $[\alpha]_\sim = [\beta]_\sim$, односно ако су α и β конјуговане.

Дефиниција За пермутацију $\alpha \in S_n$ кажемо да је **парна** ако је α могуће представити као производ парног броја транспозиција.

Ако је $\alpha \in S_n$, $\alpha = \beta_1 \beta_2 \dots \beta_t$, производ дисјунктних циклуса, онда

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}$$

$\operatorname{sgn}(\alpha) \in \{-1, 1\}$

Покажува се:

Лема Перумутација $\alpha \in S_n$ је парна ако и само ако $\operatorname{sgn}(\alpha) = 1$.

Дефиниција За перумутација $\alpha \in S_n$ кажеме да је **непарна** ако није парна.

$A_n = \{\alpha \in S_n \mid \operatorname{sgn}(\alpha) = 1\}$

$A_n \equiv$ сеш свих парних перумутација од S_n

Задача Докажеме да је $|A_n| = \frac{1}{2} n!$

доказ

Нека је $\tau = (12)$, а O_n сеш свих непарних перумутација.

Посмошримо $\left.\begin{array}{l} f: A_n \to O_n \\ f(\alpha) = \tau\alpha \end{array}\right\} \Rightarrow |A_n| \leq |O_n|$

$\left.\begin{array}{l} g: O_n \to A_n \\ g: \alpha \to \tau\alpha \end{array}\right\} \Rightarrow |O_n| \leq |A_n|$

$\Rightarrow |O_n| = |A_n|.$

Пример

Нека је $\alpha \in S_n$

$\text{cycle}(\alpha) = 1^{m_1} 2^{m_2} \dots n^{m_n}$

$m_i \in \mathbb{N} \cup \{0\}$.

Означимо са C_α, централизатор елемента α у S_n, односно

$$C_\alpha = \{\beta \in S_n \mid \alpha\beta = \beta\alpha \equiv \beta\alpha\beta^{-1} = \alpha\}$$

Нека је

$(i_1\ i_2 \dots i_r)$ један од r-циклуса α

$\beta\alpha\beta^{-1}(i_1\ i_2 \dots i_r) = (\beta(i_1) \dots \beta(i_r))$

Заинтересовани смо за $|C_\alpha| = ?$

Нека α има m_r циклуса дужине r.

m_r циклуса дужине r $\longrightarrow$ $m_r!$

$m_r! \cdot r^{m_r}$

r^{m_r} долази од могућности циклични
померањем r-циклуса

... n ... 0 ... 0
од тих m_r.

На основу претходног, закључујемо

$$|C_\alpha| = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdots n^{m_n} \cdot m_n!$$

Дефиниција

Нека је G група, а

$$\gamma_g : G \to G \text{ пресликавање}$$

$$\gamma_g(a) = gag^{-1}.$$

Пресликавање γ_g називамо конјугацијом.

Лема

(1) Ако је G група и $g \in G$, онда је конјугација $\gamma_g : G \to G$ изоморфизам.

(2) Слика a и $\gamma_g(a)$ имају исти ред.

Чињенице

- Центар групе G, $Z(G)$, је нормална подгрупа групе G.
- Група G је Абелова ако је $Z(G) = G$.

- $Aut(G)$ је група аутоморфизама
- $Inn(G) = \{\gamma_g \mid \gamma_g : x \to gxg^{-1}\}$

  (унутрашњи аутоморфизми)
- $Inn(G) \trianglelefteq Aut(G)$

Пример

Клајнова 4-група је подгрупа S_4

$$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$

Показује се да је $V \trianglelefteq S_4$.

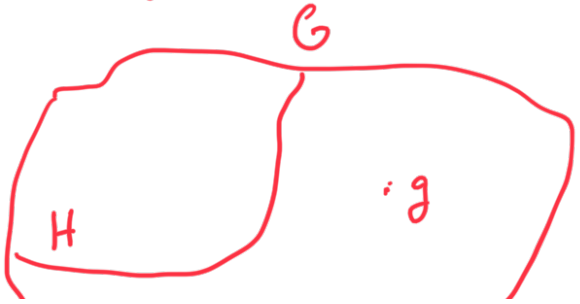
Лема

(1) Ако је H подгрупа индекса 2 у групи G, онда је $g^2 \in H$, за свако $g \in G$.

(2) Ако је H подгрупа индекса 2 у групи G, онда је $H \trianglelefteq G$.

$$G : H = \{aH \mid a \in G\}$$

(1)



$g = a \cdot h$, $h \in H$

$g^2 = ahah$

$\cancel{a}hah = \cancel{a}h,$

$hah = h,$

$a = \underbrace{h^{-1}h_1h^{-1}}_{\in H}$

12) Показать сами.