$\boxed{1}$ Групе - основни појмови и примери

Деф Операција дужине n на скупу A је $f: A^n \to A$.

- $n=0$: f је нуларна операција
- $n=1$: f је унарна оп.
- $n=2$: f је бинарна оп.

Пример а) Сабирање је операција над $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, \dots$

б) Множење је операција над $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$

в) $-$ је унарна операција над $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$

Деф Алгебарска структура $(A, f_1, \dots, f_n) = \mathcal{A}$ је уређена $(n+1)$-торка где се A назива носач структуре $\mathcal{A}$, $f_1, \dots, f_n$ су операције над A и важи: $\#(f_i) \geq \#(f_{i+1})$, $i = \overline{1, n-1}$.

Деф Група $(G, \cdot)$ је алгебарска структура са једном бинарном операцијом на непразном скупу која испуњава сл. својства:

1. $(\forall x,y,z \in G)\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ асоцијативност
2. $(\exists e \in G)$ т.д. $(\forall x \in G)\ x \cdot e = x = e \cdot x$ неутрал
3. $(\forall x \in G)(\exists x' \in G)\ x \cdot x' = e = x' \cdot x$ инверз

Пример $(\mathbb{R}, +)$:

1. $(x+y)+z = x+(y+z)$ ✓
2. $x+0 = x = 0+x$ ✓
3. $x+(-x) = 0 = (-x)+x$ ✓

Тврђење Нека је $(G, \cdot)$ група, e - неутрал у G. Тада је неутрал јединствен.

Доказ

Пп да је $\bar{e} \in G$ т.д. $(\forall x \in G)$ важи $x \cdot \bar{e} = x = \bar{e} \cdot x$. За $(\forall x \in G)$ важи

$x \cdot e = x = e \cdot x$ $\quad (x = \bar{e}) \Rightarrow \bar{e} \cdot e = \bar{e} = e \cdot \bar{e}$

$x \cdot \bar{e} = x = \bar{e} \cdot x$ $\quad (x = e) \Rightarrow e \cdot \bar{e} = e = \bar{e} \cdot e$

$\Big\}\ e = \bar{e} \cdot e = \bar{e} \Rightarrow e = \bar{e}.$

∟

$x \in G$

Тврђење Нека је $(G,\cdot)$ група, x' инверз у G. Тада је инверз јединствен.

Доказ

Нека је $\bar{x} \in G$ т.д. $x \cdot \bar{x} = e = \bar{x} \cdot x$. Посматрамо елемент $(\bar{x} \cdot x) \cdot x' = \bar{x} \cdot (x \cdot x')$

$$\left.\begin{array}{l}(\bar{x} \cdot x) \cdot x' = e \cdot x' = x' \\ \bar{x} \cdot (x \cdot x') = \bar{x} \cdot e = \bar{x}\end{array}\right\} x' = \bar{x}$$

Тврђење Нека је $(G,\cdot)$ група, $x,y \in G$. Тада је $(xy)^{-1} = y^{-1}x^{-1}$.

Доказ

По својству инверза важи: $(xy)^{-1}xy = e = xy(xy)^{-1}$. Проверимо да ли је $y^{-1}x^{-1}$ инверз од xy: $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$

$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$.

Тврђење Нека је $(G,\circ)$ група и $x \in G$. Тада важи: $(x^{-1})^{-1} = x$.

Доказ

$$\left.\begin{array}{l}x^{-1} \text{ инверз од } x: \quad x^{-1}x = e = xx^{-1} \\ (x^{-1})^{-1} \text{ инверз од } x^{-1}: \quad (x^{-1})^{-1} x^{-1} = e = x^{-1}(x^{-1})^{-1}\end{array}\right\} x = (x^{-1})^{-1}$$

Тврђење Нека је $(G,\circ)$ група, $n \in \mathbb{N}$, $a,g \in G$. Тада је: $(gag^{-1})^n = ga^ng^{-1}$.

Доказ

- $n=0$: $(gag^{-1})^0 = e$

  $ga^0g^{-1} = gg^{-1} = e$

- $n \to n+1$: $(gag^{-1})^{n+1} = (gag^{-1})^n(gag^{-1}) \overset{\text{ИХ}}{=} (ga^ng^{-1})(gag^{-1}) = ga^n\overbrace{g^{-1}g}^{e}ag^{-1} = ga^{n+1}g^{-1}$

Тврђење Нека је $(G,\circ)$ група, $n \in \mathbb{N}$, $g \in G$. Тада: $g^{-n} = (g^n)^{-1}$

Доказ

- $n=1$: $g^{-1} = (g^1)^{-1} = g^{-1}$ ✓
- $n \to n+1$: $g^{-(n+1)} = g^{-n-1} = g^{-n} \cdot g^{-1} \overset{\text{ИХ}}{=} (g^n)^{-1} \cdot g^{-1} = (g^n \cdot g)^{-1} = (g^{n+1})^{-1}$

Тврђење Нека је $(G,\circ)$ група, $x_i \in G$, $i=\overline{1,n}$, $n \in \mathbb{N}$. Тада важи:

$$(x_1 \cdot x_2 \cdot \ldots \cdot x_r)(x_{r+1} \cdot x_{r+2} \cdot \ldots \cdot x_n) = (x_1 \cdot \ldots \cdot x_r \cdot x_{r+1} \cdot \ldots \cdot x_n) = \prod_{i=1}^{n} x_i$$

Доказ

- $n=2$: $((x_1)x_2) = (x_1 \cdot x_2)$ ✓
- $n \to n+1$: $r=n$: $(x_1 x_2 \ldots x_n)(x_{n+1}) = (x_1 x_2 \ldots x_n) x_{n+1} = (x_1 x_2 \ldots x_n x_{n+1}) = \prod_{i=1}^{n+1} x_i$

  $r<n$: $(x_1 x_2 \ldots x_r)(x_{r+1} \ldots x_{n+1}) = (x_1 x_2 \ldots x_r)(x_{r+1} \ldots x_n)(x_{n+1}) =$

  $= (x_1 x_2 \ldots x_n) x_{n+1} = (x_1 \ldots x_n x_{n+1}) = \prod_{i=1}^{n+1} x_i$

Тврђење Нека је $(G,\circ)$ група, $a,b,x \in G$. Свака ј-на облика $ax=b$ има јединствено решење у G. $x = a^{-1}b$

Доказ

Пп да је $x_1 \in G$ решење ове ј-не: $ax_1 = b \Rightarrow x_1 = a^{-1}b = x \Rightarrow x_1 = x$.

Тврђење Нека је $(G,\circ)$ група, $x \in G$, $m,n \in \mathbb{N}$. Тада: $x^n \cdot x^m = x^{n+m}$

Доказ

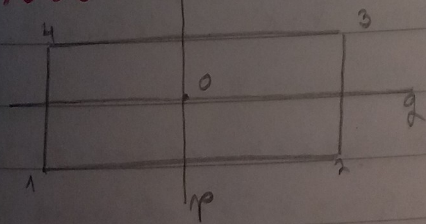
$\overbrace{(x \cdot x \cdot \ldots \cdot x)}^{n} \cdot \overbrace{(x \cdot \ldots \cdot x)}^{m} = \overbrace{(x \cdot \ldots \cdot x)}^{n+m} = x^{n+m}$

Тврђење Нека је $(G,\circ)$ група, $x \in G$, $m,n \in \mathbb{N}$. Тада: $(x^n)^m = x^{nm}$

Доказ

$\overbrace{(x^n \cdot x^n \cdot \ldots \cdot x^n)}^{m} = (x^n)^m$

* Клајнова група. Посматрамо правоугаоник. Желимо да одредимо т[…] њега ротацијама и симетријама које га […] исто. => посматрамо симетрије. Имамо сим. око $p \to \sigma_p$ и око $q \to \sigma_q$. Шта је $\sigma_p \circ \sigma_q$? То је симетрија око центра σ_0.



$\circ$	ε	σ_p	σ_q	σ_0
ε	ε	σ_p	σ_q	σ_0
σ_p	σ_p	ε	σ_0	σ_q
σ_q	σ_q	σ_0	ε	σ_p
σ_0	σ_0	σ_q	σ_p	ε

$V = \{\varepsilon, \sigma_p, \sigma_q, \sigma_0\}$, ε - идентичка транф.

- сваки елем. има инверз
- неутрал је ε
- композиција је асоц. операција
- важи комутативност

* Диедарске групе. $D_n = \{\varepsilon, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{n-1}\}$, $n \in \mathbb{N}$
    - ε - идентичко пресликавање
    - ρ^k - ротација за $k\varphi$, где је ρ ротација за φ, а $\varphi = \frac{2\pi}{n}$
    - $\sigma\rho^k$ - ротација ρ^k, а затим симетрија око праве
    - $\sigma\rho^k = \rho^{n-k}\sigma$
    - $\rho^n = \varepsilon$

Теорема (Леонардова)
Свака коначна група изометријских трансформација у равни је изоморфна тачно једној од група C_n, D_n за неко $n \in \mathbb{N}$.

[2] Подгрупе

Деф Нека су $(G, \cdot)$ и $(H, *)$ групе. Тада је $H \leq G$ ако $(\forall x, y \in H)$ важи:
$x * y = x \cdot y$, $H \subseteq G$.

Тврђење Нека је $H \leq G$, $e \in G$, $\varepsilon \in H$ неутрали. Тада је $e = \varepsilon$.

Доказ

$H \leq G \Rightarrow (\forall x, y \in H)$ $x \cdot y = x * y$. Ако је $x \in H \Rightarrow x^{-1} \in H$ јер је H група, а и $x, x^{-1} \in G$ јер је $H \leq G$. $x \cdot x^{-1} = x * x^{-1} \Rightarrow e = \varepsilon$.

∟

Тврђење Нека је $H \leq G$, $e \in G, H$ неутрал. Тада за $x \in H$ важи $\bar{x} = x^{-1}$, инверз $x^{-1} \in G$, $\bar{x} \in H$.

Доказ

$H \leq G \Rightarrow (\forall x, y \in H)$ $x \cdot y = x * y$. $x \in H \Rightarrow (\exists \bar{x} \in H)$ $x * \bar{x} = e = \bar{x} * x$. $x \in G \Rightarrow (\exists x^{-1} \in G)$
$x \cdot x^{-1} = e = x^{-1} \cdot x \Rightarrow x * \bar{x} = e = x \cdot x^{-1}$. $\bar{x} \in H \Rightarrow \bar{x} \in G \Rightarrow x \cdot \bar{x} = e = \bar{x} \cdot x \Rightarrow$
$\Rightarrow x \cdot \bar{x} = x \cdot x^{-1} = e \Rightarrow \bar{x} = x^{-1}$.

∟

Став Нека је $(G,\circ)$ група и H непразан подскуп од G. Тада је $H \leq G$ у односу на операцију $\circ$ акко $(\forall x,y\in H)$ важи $x^{-1}\cdot y\in H$.

Доказ

$\boxed{\Rightarrow}$ $H \leq G$. Тада је $x\in H \Rightarrow x^{-1}\in H$. $y\in H \Rightarrow x^{-1}\cdot y\in H$.

$\boxed{\Leftarrow}$ H је непразан подскуп од G. $h\in H$ било који. На основу услова $h^{-1}\cdot h\in H \Rightarrow e\in H$ (имамо неутрал). $x\in H$ и $e\in H \Rightarrow x^{-1}\cdot e\in H$ (имамо инверз). $x,y\in H \Rightarrow x^{-1}\in H \Rightarrow x^{-1}y\in H \Rightarrow \underbrace{(x^{-1})^{-1}\cdot y}_{x\cdot y}\in H$ (операција је затворена). Важи асоцијативност $\Rightarrow H$ је група $\Rightarrow H\leq G$.

∟

Став Нека је $H,K \leq G$. Тада:
1. $H\cap K \leq G$
2. $H\cup K\leq G \Leftrightarrow K\subseteq H$ или $H\subseteq K$

Доказ

(1.) $K,H\leq G \overset{?}{\Rightarrow} H\cap K\leq G$. Приметимо да $H\cap K\subseteq H,K$. Узмимо $x,y\in H\cap K$.

$\left.\begin{array}{l}\Rightarrow x,y\in H \Rightarrow x^{-1}\in H,\ y^{-1}\in H \Rightarrow xy^{-1}\in H \\ \Rightarrow x,y\in K \Rightarrow x^{-1}\in K,\ y^{-1}\in K \Rightarrow x,y^{-1}\in K\end{array}\right\}\ xy^{-1}\in H\cap K \Rightarrow x^{-1},y^{-1}\in H\cap K$

$H\cap K\subseteq H$ и важи $(\forall x,y\in H\cap K) \Rightarrow xy^{-1}\in H\cap K \Rightarrow H\cap K\leq H\leq G$,

$H\cap K\leq K\leq G \Rightarrow H\cap K\leq G$.

(2) $\boxed{\Leftarrow}$ $H\subseteq K \Rightarrow H\cup K = K\leq G$, $K\subseteq H \Rightarrow H\cup K = H\leq G$.

$\boxed{\Rightarrow}$ Нека је $H\cup K\leq G$. Пп, $H\not\subseteq K$. Треба доказати $K\subseteq H$. Како $H\not\subseteq K$, постоји $h\in H$ и $h\notin K$. Узмем $k\in K$ било које. $h\cdot k\in H\cup K$ (јер је $H\cup K\leq G$). $h\cdot k\in H \Rightarrow k\in H \Rightarrow h\cdot k\cdot k^{-1} = h\in K$ ↯

Дакле, $h\cdot k\notin K$ па мора бити: $h\cdot k\in H \Rightarrow h\in H \Rightarrow h^{-1}\cdot h\cdot k\in H$ ↯

∟

Став За сваки скуп $X\subseteq G$, G-група, постоји најмања подгрупа од G која садржи X као свој подскуп.

Доказ

$X\neq\emptyset \rightarrow \{e\}$ је најмања подгрупа. $H = \bigcap_{\substack{K\leq G\\ X\subseteq K}} K\leq G$ по претходном ставу.

Ако је L било која подгрупа од G т.д. $X\subseteq L$, онда се L јавља у овом пресеку па је $H\subseteq L$.

∟

$\boxed{3}$ Цикличне групе и ред елемента.

Деф Група $G \neq \{e\}$ је циклична ако $\exists a \in G$ т.д. $G = \langle a \rangle$.

Деф Елемент a је бесконачног реда ако је $a^k \neq a^l$, за $\forall k \neq l$.
У супротном, нека је $n = \min\{a^k = e,\ k > 0\}$. Тада кажемо да је a реда n. (елемента)

Деф Ако је G група (бесконачна), кажемо да је она бесконачног реда.
Ако је коначна, број елем у G, $|G|$, зовемо ред групе.

Пример $D_4 = \{\varepsilon, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$
$\omega(\rho^2) = 2$, $\omega(\rho) = 4$, $\omega(\rho^3) = 4$, $\omega(\sigma) = 2$

Став Ако је $n = \omega(a)$, онда је $G = \{e, a, \dots, a^{n-1}\}$ и међу њима нема једнаких.

Доказ

Треба доказати да је G једнако овом скупу и да у њему нема једнаких елем. $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$, $m = qn + r$, $0 \leq r < n$.
$x \in G$, $x = a^m = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r \in \{e, a, \dots, a^{n-1}\}$. Дакле, сваки елем. из G је облика a^r, $r \in \overline{1, n-1}$. Пп да ту има једнаких т.ј. $a^k = a^l$ за $k \neq l$, $k, l \in \overline{1, n-1}$. нпр. $l > k$, $a^{\omega(a)} = e$, $0 \leq k, l < n-1$,
$a^k = a^l \Rightarrow a^{l-k} = e$, $0 < l-k \leq n-1 < n \Rightarrow l \neq k \to$ сви су различити. $\llcorner$

Став Ред елемента је једнак реду групе коју тај елем. генерише.

Пример $S = \{z \in \mathbb{C},\ |z| = 1\}$, $(S, \cdot)$ - бесконачна група

Лема Нека је $n=\omega(a)$ у групи G. Тада $(\forall m\in\mathbb{Z})$: $a^m=e \iff n\mid m$.

Доказ

$\boxed{\Leftarrow}$ $m=ng \Rightarrow a^m=a^{ng}=(a^n)^g=e^g=e$

$\boxed{\Rightarrow}$ Нека је $a^m=e$, $m=gn+r$, $r\in[0,n)$. $e=a^m=a^{gn+r}=(a^n)^g\cdot a^r=a^r \Rightarrow$
$a^r=e$, $0\le r<n=\omega(a) \Rightarrow r=0 \Rightarrow m=gn \Rightarrow n\mid m$

Теорема Нека је $(G,\circ)$ група и $a\in G$. Ако је a бесконачног реда, онда је и a^m бесконачног реда, $m\neq 0$. Ако је $n=\omega(a)$, $m\neq 0$ и $m\in\mathbb{Z}$, онда је ред елем. a^m: $\omega(a^m)=\dfrac{n}{НЗД(n,m)}$.

Доказ

- $(a^m)^k=(a^m)^l$, за $k\neq l \Rightarrow a^{mk}=a^{ml}$, a бесконачног реда $\Rightarrow$
$\Rightarrow mk=ml$, $m\neq 0 \Rightarrow k=l$ ↯
- $n=\omega(a)$, $НЗД(n,m)=d$. $n=dn_1$, $m=dm_1 \Rightarrow НЗД(n_1,m_1)=1$. Треба показати да је $\omega(a^m)=\frac{n}{d}=n_1$. Дакле, треба показати:
  1° $(a^m)^{n_1}=e$: $(a^m)^{n_1}=a^{mn_1}=a^{dm_1n_1}=a^{nm_1}=(a^n)^{m_1}=e^{m_1}=e$.
  2° $(a^m)^k=e$, $k>0 \Rightarrow k\ge n_1$: $a^{mk}=e$, $n=\omega(a)\Rightarrow n\mid mk$,
  $НЗД(n_1,m_1)=1 \Rightarrow n_1\mid k \Rightarrow k\ge n_1$.
  $dn_1\mid dm_1k \Rightarrow n_1\mid m_1k$, $НЗД(n_1,m_1)=1$

Последица Ако је $n=\omega(a)$, онда је a^m генератор $\langle a\rangle$ акко $НЗД(n,m)=1$.

Став Група $\mathbb{Z}_n\times\mathbb{Z}_m$ је циклична акко $НЗД(n,m)=1$.

4 Подгрупе цикличне групе.

Теорема Свака подгрупа цикличне групе је и сама циклична.

доказ

$G=\langle a\rangle$, $H\le G$, $H=\{e\}=\langle e\rangle$ није занимљиво. $H\neq\{e\}$. Сви елем. у H су степени од a. Кди? Ако је $a^{-3}\in H$, $H\le G \Rightarrow (a^{-3})^{-1}\in H$,
$\Rightarrow$ у H мора бити позитивних степена, $\{n>0:\ a^n\in H\}\neq\emptyset$.
Непразан подскуп од $\mathbb{N}$ $\Rightarrow$ има min елемент. Нека је $r=\min\{n>0:\ a^n\in H\}$.
Тврдимо да је $H=\langle a^r\rangle$. $a^r\in H \Rightarrow \langle a^r\rangle\le H$. $x\in H$, $m=q\cdot r+r_1$, $0\le r_1<r$.
$x=a^m=a^{qr+r_1}=(a^q)^{r}\cdot a^{r_1}=\underbrace{(a^r)^q}_{\in H}\cdot a^{r_1} \Rightarrow a^{r_1}=(a^r)^{-q}\cdot x\in H$, $a^{r_1}\in H$,
$0\le r_1<r=\min\{n>0:\ a^n\in H\} \Rightarrow r_1=0$ тј $m=qr \Rightarrow x=a^m=(a^r)^q\in\langle a^r\rangle$.

Теорема Ако је G циклична група реда n и $k>0$ т.д. $k\mid n$, тада у G постоји тачно једна група реда k.

доказ

- Постоји: Користимо теорему о реду елемента. Посматрамо елем. $a^{n/k}$: $o(a^{n/k})=\dfrac{n}{НЗД(n/k,\ n)}=\dfrac{n}{\frac{n}{k}}=k$. $H=\langle a^{n/k}\rangle$, $|H|=o(a^{n/k})=k$.
- Јединственост: Нека је и $H_1\le G$ и $|H_1|=k$. На основу претходне теореме $\Rightarrow H_1=\langle a^r\rangle$, за неко r. $|H_1|=k \Rightarrow o(a^r)=k$ $\Rightarrow (a^r)^k=e \Rightarrow n\mid rk \Rightarrow (\frac{n}{k})\cdot k\mid rk \Rightarrow \frac{n}{k}\mid r$. $r=\frac{n}{k}\cdot q$, $a^r=a^{\frac{n}{k}\cdot q}=(a^{n/k})^q\in H$. $H_1=\langle a^r\rangle$, $a^r\in H \Rightarrow H_1\le H$, $|H_1|=|H|=k \Rightarrow H_1=H$.

$\boxed{5}$ Изоморфизми група. Класификација цикличних група.

Деф Нека су $(G,\circ)$ и $(H,*)$ групе. Оне су изоморфне, $G \cong H$, ако постоји бијекција $f: G \to H$ т.д. $(\forall x,y \in G): f(x \cdot y) = f(x) * f(y)$.

Став Ако је $f: G \to H$ изоморфизам, онда је и $f: H \to G$ изоморфизам.

Својства 1. e - неутрал у G, ε - неутрал у H
$f: G \to H \Rightarrow f(e) = \varepsilon$.

2. Инверз се слика у инверз: $f(x^{-1}) = \overline{f(x)}$, $x \cdot x^{-1} = e$

3. Ако је $f: G \to H$ изоморфизам и $f(g) = h \Rightarrow \omega(g) = \omega(h)$

Доказ

• Став: Нека су $h_1, h_2 \in H$. $f^{-1}(h_1 * h_2) \overset{?}{=} f^{-1}(h_1) \cdot f^{-1}(h_2)$. Пошто је f "на", $\exists g_1, g_2 \in G$ т.д.:

1) $f(g_1) = h_1$ и $f(g_2) = h_2 \Rightarrow g_1 = f^{-1}(h_1)$ и $g_2 = f^{-1}(h_2)$

2) $f(g_1 \cdot g_2) = f(g_1) * f(g_2) = h_1 * h_2$

$\overset{\text{"на"}}{\Rightarrow} f^{-1}(h_1 * h_2) = g_1 \cdot g_2 = f^{-1}(h_1) * f^{-1}(h_2)$.

• (1): $e \cdot e = e$, $f(e \cdot e) = f(e)$, $f(e * e) = f(e)$ $/ * \overline{f(e)}$ - инверз

$\Rightarrow f(e) * f(e) * \overline{f(e)} = f(e) * \overline{f(e)} \Rightarrow f(e) * \varepsilon = \varepsilon$

• (2): $f(x x^{-1}) = f(e)$, $f(x) \cdot f(x^{-1}) = e$

$x^{-1} \cdot x = e$, $f(x^{-1} x) = f(e)$, $f(x^{-1}) \cdot f(x) = \varepsilon$

$\Rightarrow$ јединственост инверза у H $f(x^{-1}) = \overline{f(x)}$

• (3): а) g бесконачног реда $\Leftrightarrow g^m \neq g^n$, $m \neq n$

-Пп да ред од h није бесконачан тј. $(\exists r,s \in \mathbb{Z})$ т.д. $r \neq s$,
а $h^r = h^s$, $f(g)^r = f(g)^s \Rightarrow f(g^r) = f(g^s)$, а f је "1-1"
$\Rightarrow g^r = g^s$. ↯ јер је $r \neq s$.

б) Нека је $\omega(g) = m$. $h^m = f(g)^m = f(g^m) = f(e) = \varepsilon \Rightarrow h$ је коначног реда и $\omega(h) \mid m$. И f^{-1} је изоморфизам, а $f^{-1}(h) = g$.
$\Rightarrow m \mid \omega(h)$, $\omega(h) > 0$
Аналогно добијамо: $\omega(g) \mid \omega(h)$

$\Rightarrow \omega(g) = \omega(h)$.

$\llcorner$

Теорема (О класификацији цикличних група)

Нека је $G \neq \{e\}$ бесконачна група. Тада је она изоморфна тачно једној од група $\mathbb{Z}_n$, за неко $n \geq 2$ или $\mathbb{Z}$.

Доказ

Ако је G бесконачно циклична, она је изоморфна са $\mathbb{Z}$.
$f: \mathbb{Z} \to G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$. $f(m) = a^m$, f је бијекција. $m \neq n \Rightarrow a^m \neq a^n$. $f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) f(l)$. $|G| = n$, $G = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$. $f: \mathbb{Z}_n \to G$ дефинисано са $f(k) = a^k$.

Теорема (Кејлијева)

Свака група G изоморфна је некој подгрупи групе S_G. од пермутација

Доказ

$G' = \{L_g \mid g \in G\}$, $L_g : G \to G$, $L_g(x) = g \cdot x$. L_g је бијекција. Важи: $L_g \circ L_h = L_{g \cdot h}$. $L_e(x) = e \cdot x = x \Rightarrow L_e$ је идентитет. $L_g \circ L_{g^{-1}} = L_{g \cdot g^{-1}} = L_e = L_{g^{-1}} \cdot L_g \Rightarrow L_g$ је бијекција: $L_g^{-1} = L_{g^{-1}}$. Према томе, $G' \subseteq S_G$. Доказујемо сада $G' \leq S_G$. Само треба показати: $L_g, L_h \in G' \Rightarrow L_g^{-1} \circ L_h \in G'$. $L_g^{-1} \cdot L_h = L_{g^{-1}} \cdot L_h = L_{g^{-1}h} \in G'$. $f: G \to G'$ дефинисана са $f(g) = L_g$. f јесте „на". $L_g = L_{g_1}$, $L_g(e) = L_{g_1}(e)$, $ge = g_1 e \Rightarrow g = g_1 \Rightarrow$ јесте „1-1". $f(g \cdot h) = L_{gh} = L_g \cdot L_h = f(g) \cdot f(h)$.

Последица Свака коначна група реда n изоморфна је некој подгрупи групе S_n.

Доказ

$|G| = n$, G изоморфна подгрупи групе $S_G \cong S_n$.

$\boxed{6}$ Директан производ група. Разлагање у директан производ.

деф Нека су $(G_1, *_1), \dots, (G_n, *_n)$ групе. Директан производ група P дефинишемо као $P := G_1 \times \dots \times G_n$ и важи: $x, y \in P$ $\quad x * y := (x_1, \dots, x_n) * (y_1, \dots, y_n) = (x_1 *_1 y_1, \dots, x_n *_n y_n)$

- неутрал: $e = (e_1, \dots, e_n)$, $e_i \in G_i$, $i = \overline{1,n}$
- инверз: $(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$
- број елем.: $|P| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$
- ред елем.: $x \in P$, $x := (x_1, \dots, x_n)$, $x_i \in G_i$, $i = \overline{1,n}$, $\omega(x) := НЗС(\omega(x_1), \dots, \omega(x_n))$

Пример $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ – није циклична група

$|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$. Редови елемената: $\omega((0,0)) = НЗС(1,1) = 1$ $\quad \omega((1,0)) = НЗС(2,1) = 2$

$\omega((0,1)) = НЗС(1,2) = 2$ $\quad \omega((1,1)) = НЗС(2,2) = 2$

Став (о разлагању на директан производ)

Нека је $(G, \circ)$ група, $H \leq G$ и $K \leq G$ за које важи:

$$\left.\begin{array}{ll} 1. & G = H \cdot K \\ 2. & (\forall h \in H)(\forall k \in K)\ hk = kh \\ 3. & H \cap K = \{e\} \end{array}\right\} \text{ Тада важи: } G \cong H \times K.$$

Доказ

Дефинишемо $f: H \times K \to G$ са $f(h,k) = h \cdot k$. Из (1) $\Rightarrow$ f је „на"; из (3) $\Rightarrow$ f је „1-1". Провера: $f(h,k) = f(h_1, k_1)$, $h_1^{-1} \backslash\ h \cdot k = h_1 \cdot k_1 \ / \cdot k^{-1}$ $\Rightarrow H \ni h_1^{-1} h = k_1 k^{-1} \in K$, $H \cap K = \{e\} \Rightarrow h_1^{-1} h = e$, $k_1 \cdot k^{-1} = e \Rightarrow h = h_1$, $k = k_1 \Rightarrow f$ је „1-1"; из (2) $\Rightarrow$ $f((h,k) \cdot (h_1, k_1)) = f(hh_1, kk_1) = hh_1 \cdot kk_1 = hk \cdot h_1 k_1 = f(h,k) \cdot f(h_1, k_1)$. Дакле, f је изоморфизам.

$\llcorner$

Став Нека је H циклична група реда m и K циклична група реда n. Тада је $H \times K$ циклична $\Leftrightarrow$ НЗД$(m,n)=1$.

Доказ

Нека је $H=\langle a\rangle=\{e,a,\dots,a^{m-1}\}$, сви a_i су различити, $o(a)=m$.

Нека је $K=\langle b\rangle=\{e,b,\dots,b^{n-1}\}$, сви b_j су различити, $o(b)=n$.

$\boxed{\Leftarrow}$ $|H\times K|=|H|\cdot|K|=m\cdot n$. Треба доказати да у $H\times K$ постоји елемент реда $m\cdot n$. Посматрамо елем. $(a,b)\in H\times K$:

$$(a,b)^{mn}=(a^{mn},b^{mn})=((a^m)^n,(b^n)^m)=(e^n,\varepsilon^m)=(e,\varepsilon).$$

Нека је сада $k>0$ т.д. је $(a,b)^k=(e,\varepsilon)$. Желимо да докажемо да је k бар $m\cdot n$: $(a^k,b^k)=(e,\varepsilon)$. $a^k=e$, $b^k=\varepsilon \Rightarrow o(a)\mid k,\ o(b)\mid k \Rightarrow$
$\Rightarrow m\mid k,\ n\mid k \Rightarrow mn\mid k \Rightarrow k\geq m\cdot n$. Ред елем. (a,b) је баш $m\cdot n$.

$\boxed{\Rightarrow}$ Доказујемо: ако је НЗД$(m,n)=d>1$, онда у $H\times K$ не постоји елем. реда $m\cdot n$. Показујемо да за $(\forall (h,k)\in H\times K)$ $(h,k)^{\frac{mn}{d}}=(e,\varepsilon)$. Дакле, за $(\forall (h,k)\in H\times K)$, $o(h,k)=\frac{mn}{d}<m\cdot n$. $(h,k)\in H\times K$, $(h,k)=(a^r,b^s)$, $r=\overline{0,m-1}$, $s=\overline{0,n-1}$. $(h,k)^{\frac{mn}{d}}=(a^r,b^s)^{\frac{mn}{d}}=(a^{\frac{rmn}{d}},b^{\frac{smn}{d}})=((a^m)^{\frac{rn}{d}},(b^n)^{\frac{sm}{d}})=(e,\varepsilon)$.

Последица Нека су $m_1,\dots,m_r$ такви да је НЗД$(m_i,m_j)=1$, $i\neq j$. Тада је
$\mathbb{Z}_{m_1}\times\dots\times\mathbb{Z}_{m_r}\cong\mathbb{Z}_{m_1\cdots m_r}$

Пример $\mathbb{D}_6\cong\mathbb{D}_3\times\mathbb{Z}_2$.

- У групи $\mathbb{D}_6$ треба наћи 1 подгрупу изоморфну са $\mathbb{D}_3$ и другу изоморфну са $\mathbb{Z}_2$, чији је пресек тривијалан, а елем. међусобно комутирају.

$H\leq\mathbb{D}_6$, $H=\{\varepsilon,\rho^2,\rho^4,\sigma,\sigma\rho^2,\sigma\rho^4\}\cong\mathbb{D}_3$
$K\leq\mathbb{D}_6$, $K=\{\varepsilon,\rho^3\}\cong\mathbb{Z}_2$

$\left.\begin{matrix} H\cdot K=\mathbb{D}_6 \text{ и} \\ ab=ba \text{ и } a\in H, b\in K \\ H\cap K=\{e\}\end{matrix}\right\}$

$\Rightarrow \mathbb{D}_6\cong H\times K$ тј. $\mathbb{D}_6\cong\mathbb{D}_3\times\mathbb{Z}_2$

Став Нека је $G \neq \{e\}$ коначна група у којој је ред сваког елемента, различит од неутрала, једнак 2. G је изоморфна директном производу цикличних група реда 2. $|G| = 2^n$, за неко n.

Доказ

- Најпре доказујемо да је група комутативна: $x, y \in G$, $x^2 = y^2 = e = (xy)^2$.
  $x^2 \cdot y^2 = e \cdot e = (xy)^2$, $x^{-1}\backslash\, xxyy = xyxy \,/y^{-1} \Rightarrow xy = yx$ ✓
- $G \neq \{e\}$, нека је $x \in G \setminus \{e\}$. Посматрамо $\langle x \rangle = \{e, x\} \cong C_2$. Нека је H максимална подгрупа од G која је изоморфна производу $\underbrace{C_2 \times \ldots \times C_2}_{k}$, за неко k. Тврдимо да је она једнака G. У супротном, нека је $y \in G \setminus H$. Посматрамо групу $K = \langle y \rangle = \{e, y\}$, тврдимо $H \cdot K \leq G$. $x, y \in H \cdot K \overset{?}{\Rightarrow} x^{-1}y \in HK$: $x = h_1 k_1$, $y = h_2 k_2$. $x^{-1}y =$
  $= k_1^{-1} h_1^{-1} h_2 k_2 \overset{\text{комут.}}{=} h_1^{-1} h_2 k_1^{-1} k_2 \in HK$. Наравно, $e = e \cdot e \in H \cdot K$ јер је $H \cdot K \neq \emptyset$. $H \subseteq H \cdot K$ (јер $H = H \cdot e$), $y \notin H$, $H \cdot K = H \cup \{h \cdot y \mid y \in H\}$.
  $\Rightarrow$ $H \cdot K$ је већа подгрупа од H, $H \cap K = \{e\}$ ($y \notin H$)
  $\Rightarrow$ имамо да је $H \cdot K \cong H \times K \cong \underbrace{C_2 \times \ldots \times C_2}_{k}$ ↯ (јер смо добили већу подгрупу од максималне)

$\llcorner$

$\boxed{7}$ Лагранжова теорема и последице

Деф. Нека је $(G,\cdot)$ група, $H \leq G$ и $x \in G$.

$xH := \{xh \mid h \in H\}$ – леви косет H у G, G/H – скуп левих косета

$Hx := \{hx \mid h \in H\}$ – десни косет H у G, $H \backslash G$ – скуп десних косета

Став Нека је $(G,\cdot)$ група, $H \leq G$, $x,y \in G$. Тада:

1. $xH = yH \Leftrightarrow x^{-1}y \in H$
2. $xH \neq yH \Rightarrow xH \cap yH = \emptyset$

Доказ

(1) $\boxed{\Rightarrow}$ $y = y \cdot e \in yH = xH \Rightarrow y = xh$ за $h \in H \Rightarrow x^{-1}y = h \in H$.

$\boxed{\Leftarrow}$ $x^{-1}y \in H$, $xH \stackrel{?}{=} yH$. $x^{-1}y = h_0$

$\boxed{\subseteq}$ $u \in xH$, $u = xh = y \cdot h_0^{-1} h \in yH$

$\boxed{\supseteq}$ $v \in yH$, $v = yh_1 = xh_0h_1 \in xH$

(2) Пп $xH \cap yH \neq \emptyset$. $z \in xH \cap yH$, $z = xh_1$, $z = yh_2$, $h_1, h_2 \in H$. $\Rightarrow x^{-1}z \in H$ и $y^{-1}z \in H \stackrel{(1)}{\Rightarrow} xH = zH$, $yH = zH \Rightarrow xH = yH$ ↯.

L

Теорема (Лагранжова)

Нека је G коначна група и $H \leq G$. Тада је $|G| = |H| \cdot [G:H]$. Ред подгрупе H дели ред групе G.

Доказ

G – коначна група $\Rightarrow$ G је коначна унија левих косета подгрупе H тј. за $x_1, \dots, x_k \in G$ важи: $G = x_1H \sqcup x_2H \sqcup \dots \sqcup x_kH$, при чему је $k = [G:H]$. $|xH| = |yH|$ за $(\forall x,y \in G)$. Ф-ја $f: xH \to yH$ је дефинисана са: $f(xh) = yh$ и задаје бијекцију између ова 2 скупа. Стога је $|G| = |H| \cdot k = |H| \cdot [G:H]$.

L

Последица 1 G - коначна група, $a \in G \Rightarrow w(a) \mid |G|$.

→ $w(a) = |\langle a \rangle|$
Лагранж: $|\langle a \rangle| \mid |G|$ $\Big\} \Rightarrow w(a) \mid |G|$

Последица 2 Свака група простог реда је циклична.

→ $a \in G \setminus \{e\} \Rightarrow w(a) \neq 1$
Посл. 1: $w(a) \mid p$ $\Big\} \Rightarrow w(a) = p \Rightarrow \langle a \rangle = G$.

Последица 3 Ако је G коначна и $a \in G \Rightarrow a^{|G|} = e$.

→ Посл. 1: $w(a) \mid |G|$
$a^m = e \iff w(a) = m$ $\Big\} \Rightarrow a^{|G|} = e$.

Деф $\Phi(n) := \{k \mid 1 \leq k < n,\ \text{НЗД}(k,n) = 1\}$ - скуп бројева до n који су узајамно прости са n.

Став $(\Phi(n), \cdot_n)$ је комутативна група, $n \geq 2$.

Доказ

$x, y \in \Phi(n) \Rightarrow x \cdot_n y := \rho(x \cdot y, n)$. Јасно је: $x \cdot_n y = y \cdot_n x$ јер је $x \cdot y = y \cdot x$. Слично, $x \cdot_n 1 = x = 1 \cdot_n x$. $\cdot_n$ је асоцијативно. Зашто сваки елем. има инверз? $x \in \Phi(n) \Rightarrow \text{НЗД}(x,n) = 1$. Безуова релација: $(\exists a, b \in \mathbb{Z})$ т.д. је $xa + nb = 1$. Нека је $\bar{a} = \rho(a,n) \Rightarrow \text{НЗД}(a,n) = 1 \Rightarrow \text{НЗД}(\bar{a},n) = 1$, $a = qn + \bar{a}$, $0 \leq \bar{a} < n$. Дакле, $\bar{a} \in \Phi(n)$. $x \cdot_n \bar{a} = \rho(x \cdot a, n)$, $xa = q_1 n + x \cdot_n \bar{a}$
$\Rightarrow 1 - x \cdot_n \bar{a} = n(b + q_1) \Rightarrow x \cdot_n \bar{a} \equiv 1 \pmod{n} \Rightarrow x \cdot_n \bar{a} = 1$.

Последица 4 (Ојлерова теорема)

Ако је $\text{НЗД}(x,n) = 1 \Rightarrow x^{\varphi(n)} \equiv 1 \pmod{n}$. $\varphi(n) := |\Phi(n)|$

→ $\bar{x} = \rho(x,n) \in \Phi(n)$. Посл. 3: у групи $(\Phi(n), \cdot)$, $\bar{x}^{\varphi(n)} = 1$.

$\underbrace{\bar{x} \cdot_n \bar{x} \cdot_n \ldots \cdot_n \bar{x}}_{\varphi(n)} = 1$ у $\Phi(n) \iff \bar{x} \cdot \bar{x} \cdot \ldots \cdot \bar{x} \equiv 1 \pmod{n}$ у $\mathbb{Z}$.

$x \equiv \bar{x} \Rightarrow x^{\varphi(n)} \equiv \bar{x}^{\varphi(n)}$, а $\bar{x}^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow x^{\varphi(n)} \equiv 1 \pmod{n}$.

Последица 6 (Мала Фермаова теорема)

Ако $p \nmid x$, p-прост $\Rightarrow x^{p-1} \equiv 1 \pmod p$

$\rightarrow$ p-прост $\Rightarrow p \nmid x \Rightarrow$ НЗД $(x,p)=1$. Посл. 4: $x^{\varphi(p)} \equiv 1 \pmod p$

$\Rightarrow x^{p-1} \equiv 1 \pmod p$ (јер p-прост $\Rightarrow \varphi(p) = p-1$).

Својства Ојлерове ф-је: 1. НЗД $(m,n)=1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ мултипликативност

2. p-прост: $\varphi(p^r) = p^r - p^{r-1}$, $r \geq 1$

Док:

Колико има бројева из скупа $\{1,2,\ldots,p^{r-1}\}$ који нису узајамно прости са p^r? Како је p прост, то је еквив. питању колико има бројева из скупа који су дељиви са p? $1p, 2p, \ldots, (p^{r-1}-1)p$, има их $(p^{r-1}-1)$. Дакле, $\varphi(p^r) = (p^r - 1) - (p^{r-1}-1) = p^r - p^{r-1}$.

$\llcorner$

Теорема Нека је $n = p_1^{w_1} p_2^{w_2} \cdot \ldots \cdot p_k^{w_k}$, $n \in \mathbb{Z}$, $k \in \mathbb{N}$. Тада $\varphi(n) = n(1-\frac{1}{p_1}) \cdot \ldots \cdot (1-\frac{1}{p_k})$.

$\boxed{8}$ Кошијева теорема. Класификација група малог реда.

Теорема (Кошијева)

Ако је G коначна група, p-прост и $p \mid |G| \Rightarrow$ у G постоји елем. реда p.

Пример Свака група реда 6 је изоморфна или групи $\mathbb{Z}_6$ или групи $\mathbb{D}_3$.

Нека је $|G|=6$. Коши: $(\exists a \in G)\ w(a) = 3$ и $(\exists b \in G)\ w(b) = 2$.

$H = \langle a \rangle = \{e, a, a^2\}$, $K = \langle b \rangle = \{e, b\} \Rightarrow H \cap K = \{e\}$; $|H \cap K| \,/\, |H| = 3$,

$|H \cap K| \,|\, |K| = 2 \Rightarrow |H \cap K| = 1$, $b \notin H \Rightarrow H \cap bH = \varnothing$, $|H \sqcup bH| = 3+3 = 6 = |G|$.

$G = H \sqcup bH = \{e, a, a^2, b, ba, ba^2\}$. $ab \in G$, $ab = ?$. $ab \notin H$ (јер би онда $b \in H$ $\lightning$).

$ab \neq b$. 1) $ab = ba$, $\langle a \rangle \cap \langle b \rangle = \{e\} \Rightarrow w(ab) = $ НЗС$(3,2) = 6 \Rightarrow$

$\Rightarrow G = \langle a, b \rangle \cong \mathbb{Z}_6$.

2) $ab = ba^2$, $a^3 = e$, $b^2 = e \Rightarrow G \cong \mathbb{D}_3$.

Пример Описати групе реда 4.

1) у G постоји елем. реда 4 $\Rightarrow G \cong \mathbb{Z}_4$

2) у G нема елем. реда 4. Ред елем. дели ред групе па сваки елем. у G, сем e, је реда 2 $\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong K$. (Клајнова група)

Пример Свака група реда 8 је изоморфна тачно једној од група:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{D}_4, \quad \mathbb{Q}_8$$

1° у G постоји елем реда 8 $\Rightarrow$ $G \cong \mathbb{Z}_8$

2° у G не постоји елем. реда 4. Тада не постоји ни елем. реда 8 јер ако је $\omega(a)=8 \Rightarrow \omega(a^2)=4$. Сви елем., осим e, су реда 2: $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

3° у G нема елем. реда 8, али има реда 4. Нека је то $a \in G$, $\omega(a)=4$. $H = \langle a \rangle = \{e, a, a^2, a^3\}$. $b \in G \setminus \langle a \rangle \Rightarrow bH \cap H = \emptyset$. $|H \sqcup bH| = 4+4 = 8 = |G|$. Дакле, $G = H \sqcup bH$ тј. $G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$.

а) $\omega(b)=2$, $ab = ?$ Пошто $b \notin H \Rightarrow ab \notin H$ и $ab \neq b$.

$ab \in \{ba, ba^2, ba^3\}$

1) $ab \overset{?}{=} ba^3$: $a = ba^2b^{-1} \Rightarrow a^2 = ba^4b^{-1} = beb^{-1} = bb^{-1} = e$ ↯

2) $ab = ba^3$, $a^4 = e$, $b^2 = e \Rightarrow$ $G \cong \mathbb{D}_4$

3) $ab = ba$, G-комутативна. $K = \langle b \rangle = \{e, b\}$. $K \cdot H = G$ ✓, $(\forall x \in K)(\forall y \in H)\ xy = yx$ ✓, $H \cap K = \{e\}$ ✓ $\Rightarrow G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_4$

б) $\omega(b)=4$, $G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$. $b^2 = ?$ $\omega(b)=4 \Rightarrow \omega(b^2)=2$, $b^2 \notin bH$ јер $b \notin H$, $\omega(a) = 4 = \omega(a^3) \Rightarrow b^2 \notin \{a, a^3\}$, $b^2 \notin \{e\} \Rightarrow b^2 = a^2$.

$ab = ?$ као и у (а), једино остају: $ab = ba$ или $ab = ba^3$.

1) $ab = ba$, G-комут., $c = ab \neq e$, $c^2 = (ab)^2 = a^2b^2$ јер је $ab = ba$. Пошто је $b^2 = a^2 \Rightarrow c^2 = a^2a^2 = e \Rightarrow \omega(c) = 2$. $L = \langle c \rangle = \{e, c\}$. $L \cap H = \{e\}$ јер $c \notin H$. $cH \cap H = \emptyset$, $G = H \sqcup cH$, $G = L \cdot H$, $L \cap H = \{e\}$ $\Rightarrow G \cong L \times H \cong \mathbb{Z}_2 \times \mathbb{Z}_4$

2) $ab = ba^3$, $a^2 = b^2$, $a^4 = e \Rightarrow$ $G \cong \mathbb{Q}_8$

$\boxed{9}$ Нормалне подгрупе и количничке групе.

Деф Нека је G група и $x, y \in G$. Елемент y је конјугован елементу x ако $(\exists g \in G)$ за који је $y = gxg^{-1}$.

Деф Нека је $H \leq G$. H је нормална, $H \triangleleft G$, ако $(\forall g \in G)$ важи $gH = Hg$.
(H је унија неких класа конјукције)

Став $H \triangleleft G \iff (\forall g \in G)\ gHg^{-1} \subseteq H$.

Доказ

$\boxed{\Rightarrow}$ $gH = Hg \ /g^{-1} \Rightarrow gHg^{-1} = H$.

$\boxed{\Leftarrow}$ $gHg^{-1} \subseteq H \ /g \Rightarrow gH \subseteq Hg$, $\forall g \in G$. Видимо да је $gH \subseteq Hg$.

Уместо g, узимамо g^{-1}. Тада: $_{g}\backslash\ g^{-1}H \subseteq Hg^{-1} \ /g \Rightarrow Hg \subseteq gH \Rightarrow gH = Hg$.

Став Свака подгрупа индекса 2 је нормална.

Доказ

$H \leq G$, $[G:H] = 2$, $|G/H| = 2$, $g \in G$.

$$\left.\begin{array}{l} 1)\ g \in H \Rightarrow gH = H = Hg \\ 2)\ g \notin H \Rightarrow H \cap gH = \emptyset \Rightarrow G = H \sqcup gH,\ H \cap Hg = \emptyset \Rightarrow G = H \sqcup Hg \end{array}\right\} \Rightarrow gH = G \setminus H = Hg.$$

Пример

1) $A_n \triangleleft S_n$
2) $\langle \rho \rangle \triangleleft D_n$
3) $G \triangleleft G$
4) $\{e\} \triangleleft G$

Деф Центар групе G, $Z(G)$, је: $Z(G) := \{x \in G \mid (\forall g \in G)\ xg = gx\}$.

Деф $[G,G]$ - подгрупа генерисана свим комутаторима. ($[G,G] \triangleleft G$).

Став $Z(G) \triangleleft G$.

Доказ

$eg = ge = g \Rightarrow e \in Z(G)$. Дакле, $Z(G) \neq \emptyset$, $g \in G$. Проверавамо да ли је подгрупа: $z_1, z_2 \in Z(G) \overset{?}{\Rightarrow} z_1^{-1} \cdot z_2 \in Z(G)$. $g \in G$ било које.

$z_1^{-1} \backslash\, z_1 g = g z_1 \,/\, z_1^{-1} \Rightarrow g z_1^{-1} = z_1^{-1} g$, $z_2 g = g z_2$.

$(z_1^{-1} z_2) g = z_1^{-1}(z_2 g) = z_1^{-1}(g z_2) = (z_1^{-1} g) z_2 = g(z_1^{-1} z_2)$

$\Rightarrow z_1^{-1} \cdot z_2 \in Z(G) \Rightarrow Z(G) \leq G$. $g \in G$, $z \in Z(G)$. Треба доказати да је $gzg^{-1} \in Z(G)$: $gzg^{-1} = zgg^{-1} = ze = z \in Z(G) \Rightarrow Z(G) \triangleleft G$.

Став Скуп свих левих косета нормалне подгрупе H, групе G чини једну групу у односу на (управо) дефинисано множење подскупова од G. Овако добијена група се зове количничка група групе G по нормалној подгрупи H.

Деф Група G је проста ако су њене једине нормалне подгрупе G и $\{e\}$.

Деф Ако су $x, y \in G$, дефинишемо комутатор елем. x и y, $[x,y]$ са:
$[x,y] := x^{-1}y^{-1}xy$.

- $xy = yx \Leftrightarrow [x,y] = e$.

Став Ако је $G \cong H$, онда је и $G^{AG} \cong H^{AG}$.

Доказ

Нека је $f: G \to H$ изоморфизам: $f([x,y]) = [f(x), f(y)] \Rightarrow f[[G,G]] \subseteq [H,H]$. Дефинишимо ф-ју $\tilde{f}: G^{AG} \to H^{AG}$ са $\tilde{f}(x[G,G]) := f(x)[H,H]$. Показаћемо да је $\tilde{f}$ добро деф. и $G/[G,G] \cong [H,H]$.

- <u>добро деф</u>: Нека је $x[G,G] = y[G,G]$. Треба доказати да је $f(x)[H,H] = f(y)[H,H]$. $\Rightarrow x^{-1}y \in [G,G] \Rightarrow f(x)^{-1}f(y) = f(x^{-1}y) \in [H,H]$
$\Rightarrow f(x)[H,H] = f(y)[H,H]$
- <u>$\tilde{f}$ је "на"</u>: Нека је $z[H,H] \in H^{AG}$. $(\exists x \in G)$ т.ј. $f(x) = z \Rightarrow \tilde{f}(x[G,G]) = f(x)[H,H] = z[H,H] \Rightarrow \tilde{f}$ је "на"

$\longrightarrow$

• $\tilde{f}$ је „1-1": Ако је $\tilde{f}(x[G,G]) = \tilde{f}(y[G,G]) \Rightarrow f(x)[H,H] = f(y)[H,H] \Rightarrow f(x^{-1}y) \in [H,H]$ тј. за неке $z_1, u_1, \dots, z_n, u_n \in H$ је $f(x^{-1}y) = [z_1,u_1]\cdots[z_n,u_n]$. Пошто је f „на" $\Rightarrow (\exists x_1, y_1, \dots, x_n, y_n \in G)$ т.д. је $f(x_1) = z_1, \dots, f(x_n) = z_n$ и $f(y_1) = u_1, \dots, f(y_n) = u_n \Rightarrow f(x^{-1}y) = [f(x_1), f(y_1)]\cdots[f(x_n), f(y_n)] = f([x_1,y_1]\cdots[x_n,y_n])$.
Пошто је f „1-1": $x^{-1}y = [x_1,y_1]\cdots[x_n,y_n] \Rightarrow x^{-1}y \in [G,G] \Rightarrow x[G,G] = y[G,G]$.

• $\tilde{f}$ се слаже са оп.: $\tilde{f}((x[G,G])(y[G,G])) = \tilde{f}(xy[G,G]) = f(xy)[H,H] = (f(x)f(y))[H,H] =$
$= (f(x)[H,H])(f(y)[H,H]) = \tilde{f}(x[G,G])\,\tilde{f}(y[G,G])$.

$\Rightarrow \tilde{f}$ је изоморфизам.

Пример $(\forall n \geq 2)$ $S_n^{Ab} \cong \mathbb{Z}_2$.

Пример $(\forall s \geq 2)$: 1. $(D_{2s})^{Ab} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

2. $(D_{2s+1})^{Ab} \cong \mathbb{Z}_2$

Став Ако је p непаран прост број, онда је свака група реда $2p$ или циклична или је изоморфна групи D_p.

Доказ

Нека је G група реда $2p \xRightarrow{\text{Коши}} (\exists x \in G)$ т.д. $\omega(x) = p$ и $(\exists y \in G)$ т.д. $\omega(y) = 2$. Како ред елем. дели ред групе, $y \notin \langle x \rangle \Rightarrow G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, \dots, x^{p-1}, y, yx, \dots, yx^{p-1}\}$. Ред елем. yx може бити 2, p или $2p$. Ако је то $2p \Rightarrow G$ је циклична. Покажимо да $\omega(yx) \neq p$. Ппс, $\omega(yx) = p$: $\langle x \rangle = e\langle x \rangle = (yx)^p\langle x \rangle = (yx\langle x \rangle)^p = (y\langle x \rangle)^p = y^p\langle x \rangle \Rightarrow y^p \in \langle x \rangle$. Како је p непаран, а $\omega(y) = 2 \Rightarrow y \in \langle x \rangle$ ↯ $\Rightarrow \omega(yx) \neq p$.
$\omega(yx) = 2$: $(yx)^2 = e \Rightarrow yxyx = e \Rightarrow yx = x^{-1}y$. Пошто је $x^p = e$ и $y^2 = e$, видимо да се изоморфизам између G и D_p може остварити придруживањем $y \mapsto \sigma$, $x \mapsto \rho$.

10 Хомоморфизми група и теореме о изоморфизмима

Деф. Нека су $(G,\cdot)$ и $(H,*)$ групе. Ф-ја $f: G \to H$ је хомоморфизам ако за $(\forall x,y \in G)$ важи: $f(x\cdot y) = f(x) * f(y)$.

- изоморфизам = хомоморфизам + бијекција
- хомоморфизам + „на" = епиморфизам

Деф. Нека је $f: G \to H$ хомоморфизам. Језгро хомоморфизма f, $\ker f$, се дефинише као: $\ker f := \{ g \in G : f(g) = e_H \}$.

Став Језгро сваког хомоморфизма $f: G \to H$ је нормална подгрупа од G.

Доказ

$f(e_G) = e_H \Rightarrow e_G \in \ker f \Rightarrow \ker f \neq \emptyset$. Пп да $x,y \in \ker f$. Треба доказати да $x^{-1}y \in \ker f$. $f(x^{-1}y) = f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H$, па $x^{-1}y \in \ker f \Rightarrow \ker f \leq G$.

$x \in \ker f$ и $g \in G$ ипо који: $f(gxg^{-1}) = f(g) * f(x) * f(g)^{-1} = f(g) * e_H * f(g)^{-1} = e_H$

$\Rightarrow g \ker f\, g^{-1} \subseteq \ker f$, $\forall g \in G \Rightarrow \ker f \triangleleft G$.

Став Хомоморфизам група $f: G \to H$ је „1-1" акко $\ker f = \{e_G\}$.
мономорфизам — тривијално језгро

Доказ

$\boxed{\Rightarrow}$ Пп да је f „1-1" и $x \in \ker f$: $f(x) = e_H = f(e_G)$. Како је f „1-1"
$\Rightarrow x = e_G \Rightarrow \ker f = \{e_G\}$.

$\boxed{\Leftarrow}$ Нека је $\ker f = \{e_G\}$. Пп да је $f(x) = f(y)$: $f(x^{-1}y) = f(x^{-1}) * f(y) =$
$= f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H \Rightarrow x^{-1}y \in \ker f = \{e_G\}$. Добијамо да је
$x = y \Rightarrow f$ је „1-1".

Деф Слика хомоморфизма $f: G \to H$, $\operatorname{Im} f$, се дефинише као:
$$\operatorname{Im} f := \{ y \in H : (\exists x \in G)\ y = f(x) \}.$$

Став Ако је $f: G \to H$ хомоморфизам, онда је $\operatorname{Im} f \leq H$.

$\to$ $e_H = f(e_G) \Rightarrow \operatorname{Im} f \neq \emptyset$. Пп да $y_1, y_2 \in \operatorname{Im} f$: $(\exists x_1, x_2)$ т.д. $f(x_1) = y_1$ и $f(x_2) = y_2$.
Тада је $y_1^{-1} * y_2 = f(x_1)^{-1} * f(x_2) = f(x_1^{-1} x_2) \in \operatorname{Im} f$.

Теорема (I о изоморфизмима)

Нека је $f: G \to H$ хомоморфизам. Тада f индукује изоморфизам $\tilde{f}: G/\ker f \to \mathrm{Im} f$ дефинисан са: $\tilde{f}(x\ker f) := f(x)$.

Доказ

- $\tilde{f}$ добро дефинисано:

  Нека је $x\ker f = y\ker f$ тј. $x^{-1}y \in \ker f$. $f(x^{-1}y) = e_H$ па је $f(x) = f(y)$
  $\Rightarrow \tilde{f}(x\ker f) = \tilde{f}(y\ker f)$.

- $\tilde{f}$ је хомоморфизам:

  $\tilde{f}((x\ker f)(y\ker f)) = \tilde{f}((xy)\ker f) = f(xy) = f(x) * f(y) = \tilde{f}(x\ker f) * \tilde{f}(y\ker f)$

  Из деф. хомом. $\tilde{f}$: $\mathrm{Im}\tilde{f} = \mathrm{Im} f$.

- $\tilde{f}$ је „1-1": Да ли је $\ker\tilde{f}$ тривијално?

  Пп да $x\ker f \in \ker\tilde{f} \Rightarrow \tilde{f}(x\ker f) = e_H \overset{деф}{\Rightarrow} x \in \ker f \Rightarrow x\ker f = \ker f$.

Теорема (II о изоморфизмима)

Нека је G група, $H \leq G$ и $K \lhd G$. Тада је $HK \leq G$, $H \cap K \lhd G$ и $HK/K \cong H/H \cap K$.

Доказ

- Треба доказати да је $HK \leq G$. Како је $e \in H \cap K \Rightarrow e = ee \in H \cap K$, па је $HK \neq \emptyset$. Пп да су $x, y \in HK \Rightarrow (\exists h, h' \in H)$ и $(\exists k, k' \in K)$ т.д. $x = hk$, $y = h'k'$. Тада је: $x^{-1}y = k^{-1}h^{-1}h'k' = k^{-1}((h')^{-1}h)^{-1}k' =$
  $= \underbrace{((h')^{-1}h)^{-1}}_{\in H}\left(\underbrace{((h')^{-1}h)}_{\in H}\underbrace{k^{-1}}_{\in K}\underbrace{((h')^{-1}h)^{-1}}_{\in H}\right)\underbrace{k'}_{\in K} \in HK$.

- Пошто је $K \lhd G \Rightarrow K \lhd HK$. Дефинишимо ф-ју $f: H \to HK/K$ са $f(h) = hK$. Пошто $f(hh') = (hh')K = (hK)(h'K) = f(h)f(h') \Rightarrow f$ је хомом.

- f је „на": Нека је xK произвољни елем. из $HK/K \Rightarrow$ за неко $h \in H$ и $k \in K$: $x = hk$. Тада је $xK = (hk)K = h(kK) = hK = f(h)$
  $\Rightarrow f$ је „на".

- језгро: $h \in H$ произвољно. Тада $h \in \ker f \Leftrightarrow f(h) = K$ (K је неутрал у HK/K).
  Пошто је $f(h) = hK \Rightarrow h \in \ker f \Leftrightarrow h \in K$ тј. $\ker f = H \cap K$.
  I тиа: $H/\ker f \cong \mathrm{Im} f$ тј. $H/H \cap K \cong HK/K$.

- $H \cap K \lhd H$ следи из чињенице да је $H \cap K$ језгро неког хомоморфизма

Теорема (III о изоморфизмима)

Нека су H и K нормалне подгрупе групе G за које је $H \leq K$.

Тада је $K/H \trianglelefteq G/H$ и $(G/H)/(K/H) \cong G/K$.

Доказ

Дефинишимо фју $f: G/H \to G/K$ са $f(gH) = gK$. Ова фја је добро деф. јер из пп да је $gH = g'H \Rightarrow g^{-1}g' \in H$, а како је $H \subseteq K$,

$\Rightarrow g^{-1}g' \in K \Rightarrow gK = g'K$.

f је епиморфизам. Одредимо језгро од f:

$gH \in \ker f \Leftrightarrow gK = K \Leftrightarrow g \in K$. Видимо да је $\ker f = K/H$.

Резултат се добија применом I теореме о изоморфизмима.

$\perp$

Став Ако је $H \leq G$ таква да $[G:H] = p$, p - најмањи прост број који дели ред групе G $\Rightarrow$ $H \trianglelefteq G$.

11 Дејства група и примери дејства. Орбита и стабилизатор.

Деф Нека је G група, $X \neq \emptyset$. Дејство групе G на скуп X је хомоморфизам $\varphi : G \to S_X$

Деф Нека је G група и $X \neq \emptyset$. Дејство G на X је свака $\theta : G \times X \to X$, за коју важи:

а) $\theta(e,x) = x$, за $\forall x \in X$ $\quad (e \cdot x)$

б) $\theta(g_1, \theta(g_2, x)) = \theta(g_1 g_2, x)$, $(\forall x \in X)(\forall g_1, g_2 \in G)$

* Ове две дефиниције су еквивалентне:

- Нека је дат хомоморфизам $\varphi : G \to S_X$. Дефинишемо $\theta : G \times X \to X$ са $\theta(g,x) := \varphi(g)(x)$. $\theta(e,x) = \varphi(e)(x) = id_X(x) = x$.
  $\theta(g_1 g_2, x) = \varphi(g_1 g_2)(x) = (\varphi(g_1)\circ\varphi(g_2))(x) = \varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1)(\theta(g_2,x)) =$
  $= \theta(g_1, \theta(g_2, x))$.
- Нека је задато $\theta : G \times X \to X$ са наведеним својствима. Дефинишемо $\varphi : G \to S_X$ са $\varphi(g)(x) = \theta(g,x)$. Зашто је $\varphi(g) \in S_X$, $\forall g$ тј. зашто је $\varphi(g)$ бијекција? $\varphi(e)(x) = \theta(e,x) = x$, $\forall x \in X$. Дакле, $\varphi(e) = id_X$.
  $\varphi(g_1 g_2) \overset{(*)}{=} \varphi(g_1)\cdot\varphi(g_2)$. $id_X = \varphi(e) = \varphi(g g^{-1}) = \varphi(g)\cdot\varphi(g^{-1})$.
  $id_X = \varphi(e) = \varphi(g^{-1} g) = \varphi(g^{-1})\cdot\varphi(g)$.
  Дакле, $\varphi(g)\cdot\varphi(g^{-1}) = id_X = \varphi(g^{-1})\,\varphi(g) \Rightarrow (\forall g \in G)$ $\varphi(g)$ је бијекција, инверз је $\varphi(g^{-1})$. Значи је $\varphi(g) \in S_X$, а $(*)$ даје хомоморфизам.
  - Доказ за $(*)$: $(\forall g_1, g_2 \in G)(\forall x \in X)$

$$\varphi(g_1 g_2)(x) = \theta(g_1 g_2, x) = \theta(g_1, \theta(g_2, x)) = \theta(g_1, \varphi(g_2)(x)) =$$
$$= \varphi(g_1)(\varphi(g_2)(x)) = (\varphi(g_1)\cdot\varphi(g_2))(x)$$

Деф G дејствује на X, $x \in X$. Орбита елемента x је:

$$\mathcal{O}(x) := \{ g \cdot x \mid g \in G \}$$

Деф G дејствује на X, $x\in X$. Стабилизатор елемента x је:

$$\Sigma_x := \{ g\in G : g\cdot x = x\}$$

Пример Нека је $X=\mathbb{R}^2$, а $G=\mathbb{Z}_2$. Тада је дејство групе G на скупу X задато са: $0\cdot(x_1,x_2)=(x_1,x_2)$, $1\cdot(x_1,x_2)=(-x_1,-x_2)$

- орбита елем. $(x_1,x_2)\in\mathbb{R}^2$ је: $\mathcal{O}((x_1,x_2)) = \{(x_1,x_2),(-x_1,-x_2)\}$

Став Нека је $X\neq\emptyset$ и G дејствује на X. Тада је $\Sigma_x \le G$, за $(\forall x\in X)$.

Доказ

$e\cdot x = x \Rightarrow e\in\Sigma_x$. $g_1,g_2\in\Sigma_x \overset{?}{\Rightarrow} g_1^{-1}g_2\in\Sigma_x$.

$g_1^{-1}\backslash\ g_1\cdot x = x \Rightarrow g_1^{-1}(g_1x)=g_1^{-1}x \Rightarrow (g_1^{-1}g_1)x = g_1^{-1}x \Rightarrow e\cdot x = g_1^{-1}x \Rightarrow$
$\Rightarrow x = g^{-1}x$.

Дакле, $g_1\cdot x = x \Rightarrow x = g_1^{-1}x$. Слично, важи и за $g_2\cdot x = x$.

$g_1,g_2\in\Sigma_x$: $(g_1^{-1}g_2)x = g_1^{-1}(g_2x)=g_1^{-1}x = x \Rightarrow g^{-1}g_2\in\Sigma_x \Rightarrow \Sigma_x\le G$.

Став G дејствује на X. Постоји бијекција између $\overset{G\cdot x}{\overset{\shortparallel}{\mathcal{O}(x)}}$ и $G/\overset{G_x}{\overset{\shortparallel}{\Sigma_x}}$.

Доказ

$f: G/\Sigma_x \to \mathcal{O}(x)$. f је бијекција између скупова $f(g\Sigma_x)=g\cdot x$.

· Добра дефинисаност: $g\Sigma_x = g_1\Sigma_x \overset{?}{\Rightarrow} g\cdot x = g_1\cdot x$. $g\Sigma_x = g_1\Sigma_x \Rightarrow$
$\Rightarrow g^{-1}g_1\in\Sigma_x \Rightarrow g\backslash (g^{-1}g_1)x = x \Rightarrow g_1x = gx$.

· f је „на": $y\in\mathcal{O}(x)\Rightarrow (\exists g\in G)\ y = g\cdot x = f(g\cdot\Sigma_x)$

· f је „1-1": $f(g\Sigma_x)=f(g_1\Sigma_x) \Rightarrow g^{-1}\backslash gx = g_1x \Rightarrow x = (g^{-1}g_1)x \Rightarrow g^{-1}g_1\in\Sigma_x$
$\Rightarrow g\Sigma_x = g_1\Sigma_x$.

Последица Ако је G коначна група која дејствује на X, онда за $\forall x\in X$:

$$|\mathcal{O}(x)| \mid |G|.$$

Доказ

$$\left.\begin{array}{l} |\mathcal{O}(x)| = |G/\Sigma_x| = [G:\Sigma_x] \\ \text{Лагранж: } |G| = |\Sigma_x|\cdot[G:\Sigma_x] \end{array}\right\} \Rightarrow |\mathcal{O}(x)| \mid |G|$$

Пример $C_4 = \langle i \rangle = \{1, i, -1, -i\}$, $C_4 \times \mathbb{C} \to \mathbb{C}$, $(\xi, z) \to \xi \cdot z$

-орбита нашег елемента z: $\mathcal{O}(z) = \{z, iz, -z, -iz\}$, $\mathcal{O}(0) = \{0\}$

Пример $G \times G/H \to G/H$, ово дејство има само 1 орбиту

$(g, aH) \to gaH$ • транзитивно дејство.

$\mathcal{O}(H) = \{gH \mid g \in G\} = G/H$

* Скуп (простор) на коме имамо дејство групе са тачно једном орбитом је хомоген скуп (простор).

Пример $H \le G$, $H \times G \to G$, $(h, g) \to hg$

$\mathcal{O}(g) = \{hg \mid h \in H\} = Hg$ десни косет

Пример $G \times G \to G$, $(g, x) \to gxg^{-1}$

$\mathcal{O}(x) = \{gxg^{-1} \mid g \in G\}$ - класа конјуговања елемента x

$\mathcal{O}(x) = \{x\} \Leftrightarrow (\forall g \in G)\ gxg^{-1} = x \Leftrightarrow (\forall g \in G)\ gx = xg \Leftrightarrow x \in Z(G)$.

Став Нека је G група реда p^n, за неко p и $n \ge 1$, која дејствује на коначном скупу X т.д. $p \mid |X|$. Тада не може постојати само 1 једночлана орбита.

Доказ

При сваком дејству групе G на скупу X, скуп X је дисјунктна унија разл. орбита: орбите су заправо класе еквиваленције $x \in \mathcal{O}(x)$.

Ако је $\mathcal{O}(x) \cap \mathcal{O}(y) \neq \emptyset \Rightarrow z \in \mathcal{O}(x) \cap \mathcal{O}(y)$, $z = g_1 \cdot x = g_2 \cdot y \Rightarrow y = (g_2^{-1} g_1) x \Rightarrow y \in \mathcal{O}(x)$; $u \in \mathcal{O}(y) \Rightarrow u = g_3 \cdot y = (g_3 g_2^{-1} g_1) \cdot x \Rightarrow u \in \mathcal{O}(x)$. Слично, $v \in \mathcal{O}(x) \Rightarrow v = g_4 \cdot x = g_4((g_2^{-1} g_1)^{-1} y) = (g_4 g_1^{-1} g_2) \cdot y \in \mathcal{O}(y)$. Дакле, $\mathcal{O}(x) = \mathcal{O}(y)$, различите орбите су дисјунктне.

$X = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \ldots \sqcup \mathcal{O}_k$. Пп да постоји тачно 1 једночлана орбита $\mathcal{O}_1$.

$|X| = |\mathcal{O}_1| + |\mathcal{O}_2| + \ldots + |\mathcal{O}_k|$, $i \ge 2$: $|\mathcal{O}_i| \neq 1$, $|\mathcal{O}_i| \mid |G| = p^n \Rightarrow$

$\Rightarrow |\mathcal{O}_i| = p^{n_i}$, $i \ge 1 \Rightarrow p \mid |\mathcal{O}_i|$. По тп, $p \mid |X| \Rightarrow p \mid 1$ ↯.

12 Доказ Кошијеве теореме

Теорема (Кошијева)

G - коначна група, $p \mid |G|$, p - прост $\Rightarrow (\exists x \in G)$ т.д. $w(x) = p$.

Доказ

- Посматрамо скуп $X = \{(g_0, g_1, \dots, g_{p-1}) \in G^p \mid g_0 \cdot g_1 \cdot \dots \cdot g_{p-1} = e\}$. $|X| = ?$
$|X| = |G| \cdot |G| \cdot \dots \cdot |G| \cdot 1 = |G|^{p-1}$. Свакако $p \mid |X|$. Посматрамо дејство $\mathbb{Z}_p$ на X: $(k, (g_0, \dots, g_{p-1})) \to (g_{k+_p 0}, \dots, g_{k+_p(p-1)})$.
- Како изгледа једночлана орбита?
$\mathcal{O}((e, \dots, e)) = \{(e, \dots, e)\}$. Нека је $\mathcal{O}((g_0, \dots, g_{p-1})) = \{(g_0, \dots, g_{p-1})\}$.
Посебно: $1 \cdot (g_0, \dots, g_{p-1}) = (g_0, \dots, g_{p-1}) \cdot (g_1, \dots, g_0) = (g_0, \dots, g_{p-1})$.
$g_0 = g_1, \; g_2 = g_1, \dots, g_0 = g_{p-1} \Rightarrow$ сви су једнаки.
Орбита је једночлана ако су сви једнаки.
- Према претходном ставу, не сме постојати тачно једна једночлана орбита. Дакле, мора постојати $g \in G$, $g \neq e$ т.д. је $(g, \dots, g) \in X$ тј. $g^p = e \Rightarrow w(g) = p$. ∎

Теорема Нека је $|G| = p^n$, p - прост и $n \geq 1$. Тада је: $Z(G) \neq \{e\}$.

Доказ

$G \times G \to G$, $(g, x) \to gxg^{-1}$. $\mathcal{O}(x) = \{x\} \Leftrightarrow x \in Z(G)$. По ставу: не може да постоји тачно 1 једночлана орбита. Једна постоји: $\mathcal{O}(e) = \{e\}$. Ако је $x \neq e$, $\mathcal{O}(x) = x \Rightarrow x \in Z(G) \setminus \{e\}$. ∎

Став Свака група реда p^2 је комутативна.

Доказ

$|G| = p^2$. Према претходном, $Z(G) \neq \{e\}$
1° $|Z(G)| = p^2 \Rightarrow G = Z(G) \Rightarrow G$ је комутативна
2° $|Z(G)| = p$, $Z(G) \trianglelefteq G$. $|G/Z(G)| = [G : Z(G)] = \frac{p^2}{p} = p$. Свака група реда p је циклична $\Rightarrow G$ је циклична, $G/Z(G) = \langle aZ(G) \rangle$.

$x, y \in G$, $xZ(G) = a^r Z(G)$, за неко $r \in [0,p)$; $yZ(G) = a^s Z(G)$, за неко $s \in [0,p)$

$x \in xZ(G) = a^r Z(G) \Rightarrow x = a^r z_1$, $z_1 \in Z(G)$

$y \in yZ(G) = a^s Z(G) \Rightarrow y = a^s z_2$, $z_2 \in Z(G)$

$$\left.\begin{aligned} x \cdot y &= a^r z_1 \cdot a^s z_2 = a^{r+s} z_1 \cdot z_2 \\ y \cdot x &= a^s z_2 \cdot a^r z_1 = a^{s+r} z_2 \cdot z_1 = a^{r+s} z_1 z_2 \end{aligned}\right\}$$ G је комутативна, па $|Z(G)| = p$ није могуће

Дакле, $G = Z(G)$.

Став Свака група реда p^2, p-прост, или је циклична или је изоморфна групи $C_p \times C_p$.

Доказ

Користимо Теорему о разл. на директан производ. Нека G није циклична, а реда је p^2. $x \in G \setminus \{e\} \Rightarrow \omega(x) = p$. $H = \langle x \rangle$, $y \in G \setminus H \Rightarrow K = \langle y \rangle$.
$H \cap K = \{e\}$ јер $|H \cap K| \mid |H| \Rightarrow |H \cap K| \in \{1, p\}$. Ако је $|H \cap K| = p$, онда је $H \cap K = H = K$ ↯. $H \cdot K = \{x^r y^s, 0 \le r < p, 0 \le s < p\}$ сви елем. су различити.

$x^{-r_1} \backslash x^r y^s = x^{r_1} y^{s_1} / y^{-s} \Rightarrow x^{-r_1 + r} = y^{s_1 - s} \in H \cap K = \{e\}$.

$x^{-r_1 + r} = e = y^{s_1 - s} \Rightarrow x^r = x^{r_1}$, $0 \le r, r_1 < p \Rightarrow r = r_1$

$\Rightarrow y^s = y^{s_1}$, $0 \le s, s_1 < p \Rightarrow s = s_1$

Пошто су сви различити, има их p^2, па је $H \cdot K = G$. Став о разл. на директан производ: $G \cong H \times K \cong C_p \times C_p$.

13 Одређивање броја орбита при дејству коначне групе на коначном скупу.

Став G дејствује на X. Ако су x и y из исте орбите, онда су Σ_x и Σ_y конјуговане подгрупе.

Доказ

Нека је $y = g.x$ (акко $g^{-1}y = x$). Тврдимо да је $\Sigma_y = g\Sigma_x g^{-1}$.

$\boxed{\subseteq}$ $h \in \Sigma_y$, посматрамо: $g^{-1}hg \in \Sigma_x$?

$(g^{-1}hg)\,x = g^{-1}(h\cdot(g.x)) = g^{-1}\cdot(h\cdot y) = g^{-1}\cdot y = x$,

$g^{-1}hg \in \Sigma_x \Rightarrow h \in g\Sigma_x g^{-1}$.

$\boxed{\supseteq}$ $h \in g\Sigma_x g^{-1}$, $h = gh'g^{-1}$, $h' \in \Sigma_x$

$hy = (gh'g^{-1})y = g.(h'.(g^{-1}.y)) = g\cdot(h'.x) = g.x = y$.

Став G дејствује на X. Ако су g и h конјуговани, онда постоји бијекција између X^g и X^h, где је $X^g := \{x \mid g\cdot x = x\}$.

Доказ

$g = khk^{-1}$, $\varphi: X \to X$, $\varphi(x) = k\cdot x$. φ-бијекција, инверз је $x \to k^{-1}\cdot x$.
Треба доказати: $\varphi[X^h] = X^g$. Нека је $x \in X^h$ тј. $h\cdot x = x$. Да ли је $k\cdot x \in X^g$? $g.(k\cdot x) = (khk^{-1})\cdot(k\cdot x) = k\cdot(h\cdot(k^{-1}\cdot(k\cdot x))) = k\cdot(h\cdot x) = k\cdot x$.
Заиста је $\varphi[X^h] \subseteq X^g$. Зашто је φ „на"? $y \in X^g$, $h\cdot(k^{-1}\cdot y) = (k^{-1}gk)\cdot(k^{-1}\cdot y) = k^{-1}(g\cdot y) = k^{-1}\cdot y$. Дакле, $k^{-1}y \in X^h$, а $\varphi(k^{-1}y) = y$, па је φ „на". Пошто је φ „1-1" $\Rightarrow$ имамо бијекцију између X^h и X^g.

Теорема Нека коначна група G дејствује на коначном скупу X. Тада је број орбита једнак: $\frac{1}{|G|}\sum_{g\in G}|X^g|$.

Доказ

$E = \{(g,x) \in G\times X \mid g.x = x\}$. Пребројаћемо елем. у E на 2 начина.

$X = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \ldots \sqcup \mathcal{O}_k$, $\mathcal{O}_i = \mathcal{O}(x_i)$, k-тражени број орбита,

• $E = \bigsqcup_{g\in G}\{g\}\times X^g$, $|E| = \sum_{g\in G}|X^g|$ →

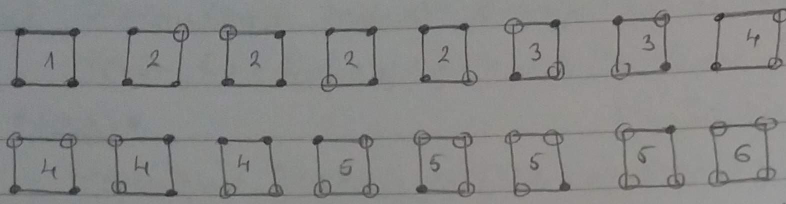
- $E = \bigsqcup_{x\in X} \Sigma_x \times \{x\}$, $|E| = \sum_{x\in X} |\Sigma_x|$

$|E| = \sum_{x\in X}|\Sigma_x| = \sum_{x\in \mathcal{O}_1} |\Sigma_x| + \dots + \sum_{x\in\mathcal{O}_k}|\Sigma_x| = |\mathcal{O}(x_1)|\cdot|\Sigma_{x_1}| + \dots + |\mathcal{O}(x_k)|\cdot|\Sigma_{x_k}| =$

$= [G:\Sigma_{x_1}]\cdot|\Sigma_{x_1}| + \dots + [G:\Sigma_{x_k}]\cdot|\Sigma_{x_k}| =$ (Лагранж) $= |G| + \dots + |G| = k\cdot|G|$

L $\sum_{g\in G}|X^g| = |E| = k\cdot|G| \Rightarrow k = \frac{1}{|G|}\sum_{g\in G}|X^g|$.

Пример Темена квадрата бојимо са 2 боје, при чему се сматра да је ротиран квадрат исти квадрат. Колико има орбита?



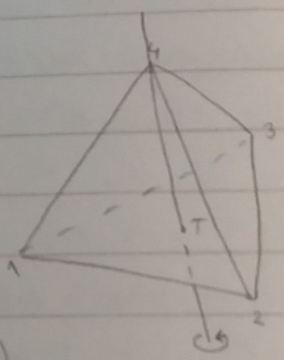
- ако су исти → припадају истој орбити

$|X| = 16$, $|X^1| = 16$, $|X^{-1}| = 2\cdot 2\cdot 1\cdot 1 = 4$, $|X^i| = 2$, $|X^{-i}| = 2$

$\Rightarrow \frac{1}{4}(16 + 4 + 2 + 2) = \frac{24}{4} = \underline{\underline{6}}$ орбита

* Група ротација правилног тетраедра:

- ε , $\underset{(1\,2\,3)}{R_{4,2\pi/3}}$, $\underset{(1\,3\,2)}{R^2_{4,2\pi/3}}$



$\left.\begin{array}{l} \bullet\ \text{идентична: } \underline{1} \\ \bullet\ \text{осе кроз темe: } \underline{4\times 2} \\ \bullet\ \text{осе кроз средишта наспр. стр: } \underline{3\times 1} \end{array}\right\} = 12 \quad (= |A_4|)$

Требају нам класе конјугације у A_4

- у A_4 (123) и (132) нису конјуговане
- Класе конјугације у A_4:

{(1)} ; {(123), (124), (134), (234)} ; {(132), (142), (143), (243)} ;
{(12)(34), (13)(24), (14)(23)}

14 Коначно генерисане слободне Абелове групе

Деф Абелова група F је *слободна Абелова група* са системом слободних генератора $[x_1, \dots, x_n]$, $x_i \in F$ ако за сваку Абелову групу A и елементе $a_1, \dots, a_n \in A$, постоји тачно један хомоморфизам $f: F \to A$ т.д. је $f(x_i) = a_i$, $\forall i$

Став Ако је F слободна Абелова група са системом слободних генератора $[x_1, \dots, x_n]$, тада из $w_1 x_1 + \dots + w_n x_n = 0$, $w_i \in \mathbb{Z}$, следи да је $w_1 = \dots = w_n = 0$.

Доказ

Докажимо да је $w_1 = 0$. $A = \mathbb{Z}$, $a_1 = 1, a_2 = 0, \dots, a_n = 0$. Тада постоји јединствен хомоморфизам $f: F \to A$ т.д. је $f(x_i) = a_i$, $\forall i$,
$f(w_1 x_1 + \dots + w_n x_n) = f(0)$. $w_1 f(x_1) + \dots + w_n f(x_n) = 0$, $w_1 a_1 + \dots + w_n a_n = 0$.
$\Rightarrow w_1 \cdot 1 + w_2 \cdot 0 + \dots + w_n \cdot 0 = 0 \Rightarrow w_1 = 0$. Слично се доказује и за остале w_i.

Став $\mathbb{Z}^n = \mathbb{Z} \times \dots \times \mathbb{Z}$ је слободна Абелова група са слободним системом генератора $[e_1, \dots, e_n]$, где су $e_1 = (1, \dots, 0)$, $e_2 = (0, 1, \dots, 0)$, $\dots$, $e_n = (0, \dots, 1)$.

Доказ

A - Абелова група, $a_1, \dots, a_n \in A$. Дефинишемо $f: \mathbb{Z}^n \to A$ са
$f(w_1, \dots, w_n) = w_1 a_1 + \dots + w_n a_n \Rightarrow f((w_1, \dots, w_n) + (w_1', \dots, w_n')) = f(w_1 + w_1', \dots, w_n + w_n') =$
$= (w_1 + w_1') a_1 + \dots + (w_n + w_n') a_n = (w_1 a_1 + \dots + w_n a_n) + (w_1' a_1 + \dots + w_n' a_n) =$
$= f(w_1, \dots, w_n) + f(w_1', \dots, w_n') \Rightarrow$ јесте хомоморфизам.
$f(e_i) = f(0, \dots, \underset{\boxed{i}}{1}, \dots, 0) = 0 \cdot a_1 + \dots + 1 \cdot a_i + \dots + 0 \cdot a_n = a_i$ ($\exists$ хомоморфизам)
Јединственост: Нека је $\varphi: F \to A$ хомоморфизам, $\varphi(e_i) = a_i$.
$\varphi(w_1, \dots, w_n) = \varphi((w_1, \dots, 0) + (0, w_2, \dots, 0) + \dots + (0, \dots, w_n)) =$
$= \varphi(w_1, \dots, 0) + \dots + \varphi(0, \dots, w_n) = w_1 a_1 + \dots + w_n a_n$
$(\varphi(w_1, 0, \dots, 0) = \varphi(w_1(1, \dots, 0)) = w_1 \varphi(1, \dots, 0) = w_1 \varphi(e_1) = w_1 a_1)$

Став Ако је F слободна и има систем слободних генератора $[x_1, \dots, x_n]$, а F' има систем слободних генератора $[x_1', \dots, x_n'] \Rightarrow F \cong F'$.

Доказ

На основу дефиниције постоји тачно 1 хомоморфизам $f: F \to F'$ и тачно 1 хомоморфизам $g: F' \to F$, за које је $f(x_i) = x_i'$ и $g(x_i') = x_i$, $\forall i$. Тада је за $\forall i)$ $(g \circ f)(x_i) = x_i$ и $(f \circ g)(x_i') = x_i'$. Како и идентични хомоморфизми id_F и $id_{F'}$ имају иста својства, то на основу јединствености закључујемо да је $g \circ f = id_F$, $f \circ g = id_{F'} \Rightarrow F \cong F'$.

$\llcorner$

* Свака слободна Абелова група са n с.г. је изоморфна са $\mathbb{Z}^n$.

Став Ако је $\mathbb{Z}^r \cong \mathbb{Z}^s \Rightarrow r = s$.

Доказ

Пт да је $r \leq s$. Приметимо да се у групи $\mathbb{Z}^s$ налазе и елементи канонске базе в.п. $\mathbb{R}^s$ тј вектори $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$. То значи да су сви наведени базни вектори целобројне линеарне комбинације од r вектора, $f(1, \dots, 0), \dots, f(0, \dots, 1)$, где је f изоморфизам који постоји по пт. То значи да тих r вектора мора генерисати простор $\mathbb{R}^s$, димензије s. Знамо да не може мање од s вектора генерисати в.п. димензије s па мора бити $r \geq s$. Пошто смо пт да је $r \leq s$, а имамо $r \geq s \Rightarrow r = s$.

$\llcorner$

Теорема Нека је F слободна Абелова група са n слободних генератора и $R \leq F$. Тада постоји с.с.г. $[x_1, \dots, x_n]$ групе F и ненегативни цели бројеви $d_1, \dots, d_n$ за које је $R = \langle d_1 x_1 \rangle \oplus \dots \oplus \langle d_n x_n \rangle$, при чему $d_i \mid d_{i+1}$, $i \in [1, n-1]$.

15 Коначно генерисане Абелове групе.

Деф Нека је A Абелова група. Она је коначно генерисана ако постоје елементи $x_1, \dots, x_n \in A$ т.д. је $A = \{ m_1 x_1 + \dots + m_n x_n \mid m_i \in \mathbb{Z} \}$.

* Ако су $B, C \leq A$: $B + C = \{ b + c \mid b \in B, c \in C \}$
  * $H, K \leq G$: $H \cdot K \leq G \Leftrightarrow HK = KH$ $\rightarrow$ за B, C ово увек важи јер су комутативне
* Ако је A генерисана елем. $x_1, \dots, x_n$, онда је $A = \langle x_1 \rangle + \dots + \langle x_n \rangle$, $\langle x_i \rangle = \{ m_i x_i \}$

Деф Сума $B + C \leq A$ је директна ако се сваки елем. из $B + C$ може на јединствен начин приказати у облику $b + c$, за $b \in B$, $c \in C$.

* $B_1 \oplus B_2 \oplus \dots \oplus B_n$ - ознака

Став Сума $B + C$ је директна акко $B \cap C = \{0\}$.

Доказ

$\boxed{\Rightarrow}$ Нека је $x \in B \cap C$, $x \in A$: $x = x + 0$, $x \in B$, $0 \in C$ или $x \in C$, $0 \in B$.

Пошто је јединствен приказ: $x = 0$ и $0 = x \Rightarrow B \cap C = \{0\}$.

$\boxed{\Leftarrow}$ Нека је $B \cap C = \{0\}$. $x \in B + C$, $x = b_1 + c_1$ и $x = b_2 + c_2$.

$b_1 + c_1 = b_2 + c_2 \Rightarrow \underbrace{b_1 - b_2}_{\in B} = \underbrace{c_2 - c_1}_{\in C} \Rightarrow (B \cap C = \{0\}) \Rightarrow b_1 - b_2 = c_2 - c_1 \in B \cap C = \{0\}$

$\Rightarrow b_1 - b_2 = 0$, $c_2 - c_1 = 0 \Rightarrow b_1 = b_2$, $c_2 = c_1$

$\llcorner$

Став Директна сума $B_1 \oplus \dots \oplus B_n \cong B_1 \times \dots \times B_n$ директном производу.

Доказ

Нека је сума $B_1 + \dots + B_n$ директна. $\varphi : B_1 \times \dots \times B_n \rightarrow A$ дефинисана са $\varphi(b_1, \dots, b_n) = b_1 + \dots + b_n$.

* φ-хомоморфизам: $\varphi((b_1, \dots, b_n) + (b_1', \dots, b_n')) = \varphi(b_1 + b_1', \dots, b_n + b_n') = (b_1 + b_1') + \dots + (b_n + b_n')$
  $= (b_1 + \dots + b_n) + (b_1' + \dots + b_n') = \varphi(b_1, \dots, b_n) + \varphi(b_1', \dots, b_n')$
* $\mathrm{Im}\,\varphi = B_1 + \dots + B_n$, $\mathrm{Ker}\,\varphi = \{ (b_1, \dots, b_n) \mid \varphi(b_1, \dots, b_n) = 0 \} = \{ (b_1, \dots, b_n) \mid b_1 + \dots + b_n = 0 \} = \{ (0, \dots, 0) \}$

I тврђ. о изом.: $B_1 \times \dots \times B_n \cong \mathrm{Im}\,\varphi = B_1 \oplus \dots \oplus B_n$.

$\llcorner$

Теорема Нека је A коначно генерисана Абелова група. Тада постоје позитивни цели бројеви $d_1, \dots, d_k$ и природан број s т.д. $d_i | d_{i+1}, \forall i$ и да је: $A \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^s$. $(d_i > 1)$

Теорема Претпоставимо да је $\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r \cong \mathbb{Z}_{e_1} \times \dots \times \mathbb{Z}_{e_\ell} \times \mathbb{Z}^s$, при чему је $d_i \geq 2$, $e_j \geq 2$, $(\forall i, j)$; $d_i | d_{i+1}$, $e_j | e_{j+1}$, $(\forall i, j)$. Тада је $k = \ell$, $d_i = e_i$, за све i, и $r = s$.

$\boxed{16}$ Комутативни прстени са јединицом. Делитељи нуле, регуларни и инвертибилни елементи.

Деф Комутативни прстен са јединицом је структура $(A, +, \cdot)$ за коју важи:
1) $(A, +)$ је Абелова група
2) $(A, \cdot)$ је комутативан моноид
3) $(\forall x, y, z \in A)$ важи: $x \cdot (y + z) = x \cdot y + x \cdot z$

* Неутрал за сабирање у комутативном прстену A означавамо са 0 и зовемо нулом прстена A.
* Неутрал за множење означавамо са 1 и зовемо јединицом прстена A.
* У сваком прстену A, за $(\forall a \in A)$ важи: $a \cdot 0_A = 0_A$

  $\rightarrow$ $a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A \overset{(1)}{\Rightarrow} 0_A = a \cdot 0_A$
* Ако би у прстену A важило: $0_A = 1_A$, добили бисмо да за $(\forall a \in A)$ важи: $a = a \cdot 1_A = a \cdot 0_A = 0_A$, па би било $A = \{0_A\}$ - нула прстен
* У сваком прстену је испуњено: $-a = (-1_A) \cdot a$

  $\rightarrow$ $a + (-1_A) \cdot a = 1_A \cdot a + (-1_A) \cdot a = a \cdot 1_A + a \cdot (-1_A) = a(1_A + (-1_A)) = a \cdot 0_A = 0_A$
* $(A, \cdot)$ је моноид, па у њој неки елем. могу имати инверз. Јасно је да то не може бити 0: $a \cdot 0 = 0 \neq 1$, $\forall a \in A$. Посматрамо оне елем. из $A \setminus \{0\}$ који имају инверз у односу на множење. Скуп њихових елем. означавамо са $U(A)$

• $(U(A), \cdot)$ је комутативна група (група инверзибилних елем. прстена)
Ако је $U(A) = A \setminus \{0\}$, прстен A је поље

Пример Комутативни прстени са јединицом:

$\mathbb{Z}$; $\mathbb{Z}_n = (\mathbb{Z}_n, +_n, \cdot_n)$; $\underbrace{\mathbb{R} \; ; \; \mathbb{Q} \; ; \; \mathbb{C}}_{\text{поља}}$

$\mathbb{Z} \to$ није поље

$\mathbb{Z}_n \to U(\mathbb{Z}_n) = \varphi(n)$

↳ поље је само ако је n-прост

Пример Прстен полинома са коеф. у неком комутативном прстену са јединицом A и неодређеном x тј. прстен $A[x] := \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in A, \forall i\}$, $n \in \mathbb{N}$

- не важи: $\deg(a b) = \deg a + \deg b$

  нпр. $\mathbb{Z}_6[x]$, $a = 2+3x$, $b = 1+2x$:

  $a \cdot b = (2+3x)(1+2x) = 2+x \quad (2 \cdot_6 3 = 0)$

Деф За елемент $a \neq 0$, комутативног прстена са јединицом A, кажемо да је прави делитељ нуле у A ако постоји $b \in A \setminus \{0\}$ т.д. је $a \cdot b = 0$.

Став У пољу нема правих делитеља нуле.

Доказ

Пт да у пољу F постоје прави делитељи нуле тј. $\exists a, b$ т.д. $a \neq 0$ и $b \neq 0$, а $a \cdot b = 0$. Како је $a \neq 0$, $(\exists a^{-1})$ за који важи $a^{-1} \cdot a = 1$. Тако добијамо да је: $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = b \; \lightning \; (b \neq 0)$.

∟

Деф Комутативни прстен са јединицом у коме нема правих делитеља нуле називамо област целих или домен.

• свако поље је домен (обрнуто не мора да важи)

Став Сваки коначан домен је поље.

Доказ

Нека је A коначан домен и да је $a \in A \setminus \{0\}$. Треба показати да a има инверз. Посматрајмо фју $L_a : A \to A$ деф са $L_a(x) = a \cdot x$, $x \in A$.
Ова фја је „1-1". Ако је $L_a(x) = L_a(y) \Rightarrow a \cdot x = a \cdot y$, па је $a \cdot (x - y) = 0$.
Пошто је A домен, а $a \in A \setminus \{0\}$, мора бити $x - y = 0$ тј. $x = y$.
Свака „1-1" фја која слика коначан скуп у њега самог мора бити сурјекција $\Rightarrow L_a$ је сурјекција па $\exists a'$ т.д. $L_a(a') = 1$ тј.
L $(\exists a' \in A)$ за које је $a' \cdot a = 1 \Rightarrow a$ има инверз.

Деф Елемент $a \in A$ је регуларан ако из $a \cdot x = a \cdot y \Rightarrow x = y$.

- инвертибилни елем. су и регуларни (обрнуто не мора да важи)

Став У сваком коначном прстену, сваки регуларан елем. је инвертибилан.

- сваки елем. у коначном прстену је делитељ нуле или инвертибилан

Деф Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ комутативни прстени са јединицом при чему је $B \subseteq A$. Ако за $(\forall x, y \in B)$ важи:
$x + y = x +' y$, $x \cdot y = x \cdot' y$ и $1_A = 1_B$, онда је B један потпрстен са јединицом прстена A.

$\boxed{17}$ Идеали у комутативном прстену са јединицом

деф Нека је A комутативан прстен са јединицом и I непразан подскуп од A. Тада је I *идеал* у A, $I \triangleleft A$, ако:

1. $(\forall x, y \in I)\ x + y \in I$
2. $(\forall a \in A)(\forall x \in I)\ a \cdot x \in I$

- $0 \in I$ за сваки идеал

деф Нека су I и J идеали прстена A.

1. $I + J := \{x + y \mid x \in I, y \in J\}$
2. $I \cdot J := \{x_1 y_1 + \ldots + x_n y_n \mid x_i \in I, y_j \in J\}$

- $I \cdot J$ - најмањи идеал који садржи све могуће производе елем. из I са елем. из J.
- Пресек 2 идеала је идеал
- унија 2 идеала је идеал акко је један од њих садржан у другом!

пример Ако је A комутативан прстен са јединицом и $a \in A$ било који, онда је: $\langle a \rangle := \{r \cdot a \mid r \in A\}$ идеал. Овај идеал се назива *главни идеал* генерисан елементом a.

$$r \cdot a + s \cdot a = (r + s) \cdot a \quad \text{и} \quad s \cdot (r \cdot a) = (sr) \cdot a$$

$$\Rightarrow \langle a \rangle \text{ је заиста идеал у прстену } A$$

пример Сваки идеал у $\mathbb{Z}$ је облика $\langle m \rangle$ за неки природан број m.

$\rightarrow$ Нека је $I \triangleleft \mathbb{Z}$. Како је $(I, +) \leq (\mathbb{Z}, +) \Rightarrow I = \langle m \rangle$.

- идеал $\langle m \rangle$ се означава и са $m\mathbb{Z}$ (скуп свих целобројних умножака бр. m)

Став а) Сваки идеал у $\mathbb{Z}$ је главни (претх. пример)

б) Сваки идеал у K (K-поље) је или $\{0\}$ или је цело K

в) Сваки идеал у $K[x]$ (прстен), K-поље, је главни.

Доказ

(а) $x \in I \Rightarrow (-1)\cdot x = -x \in I$. $I \triangleleft \mathbb{Z} \Rightarrow I$ је подгрупа од $\mathbb{Z}$. $I = \langle n \rangle$.

(б) $I \triangleleft K$ и $I \neq \{0\}$: $x \in I$, $x \neq 0$. Ако је $a \in K$ било који $\Rightarrow a \in I$.

Пошто је I-идеал и $x \in I$, $x \neq 0 \Rightarrow (\exists x^{-1})$ $\underbrace{(ax^{-1})x}_{a} \in I$.

(в) $I \triangleleft K[x]$. $I = \{0\} = \langle 0 \rangle$.

$I \neq \{0\}$, $a_0 + a_1x + \dots + a_nx^n \in I$, $a_n \neq 0$

$$a_n^{-1}(a_0 + a_1x + \dots + a_nx^n) = a_n^{-1}a_0 + a_n^{-1}a_1x + \dots + x^n \in I$$

Нека је μ монични полином најмањег степена из I. Тврдимо $I = \langle \mu \rangle$. $\mu \in I \Rightarrow \langle \mu \rangle \subseteq I$. $b \in I$: $b = g\mu + r$, $\deg r < \deg \mu$ или $r = 0$.

$r = \underbrace{b}_{\in I} - \underbrace{g\mu}_{\in I} \in I$, $\deg r < \deg \mu$. $r = r_0 + r_1x + \dots + r_tx^t \in I$, $r_t \neq 0$

$r_t^{-1}\cdot r$ - монични полином степена мањег од μ ↯

Зато је $r = 0$ и $b = g\mu \in \langle \mu \rangle$.

∟

Пример Нека је A неки комутативни прстен са јединицом и $u \in U(A)$. Тада је $\langle u \rangle = A$.

→ $I \triangleleft A$, $U(A) \cap I \neq \emptyset \Rightarrow I = A$.

Пример $A/I = \{a + I \mid a \in A\}$:
- $(a+I) + (b+I) := (a+b) + I$
- $(a+I)\cdot(b+I) := (ab) + I$

$$\left.\begin{array}{l} a+I = a_1+I \\ b+I = b_1+I \end{array}\right\} ab + I = a_1b_1 + I \Rightarrow a\cdot b - a_1\cdot b_1 = a\cdot b - a_1\cdot b + a_1\cdot b - a_1\cdot b_1 =$$
$$= \underbrace{(a-a_1)}_{\in I}\cdot b + a_1\cdot\underbrace{(b-b_1)}_{\in I} \in I$$

$(A/I, +, \cdot)$ - комутативни прстен са јединицом

$\boxed{18}$ Хомоморфизми, количнички прстени и теорема о изоморфизму

Деф Нека су $(A,+,\cdot)$ и $(B,+',\cdot')$ два комутативна прстена са јединицом. Ф-ја $f: A \to B$ је хомоморфизам прстена ако је $f(1_A)=1_B$ и ако за $(\forall x,y \in A)$ важи:

1. $f(x+y) = f(x) +' f(y)$
2. $f(x\cdot y) = f(x) \cdot' f(y)$.

Пример Ф-ја $f_n: \mathbb{Z} \to \mathbb{Z}_n$ задата са $f_n(x) := \rho(x,n)$, где је $\rho(x,n)$ означен остатак при дељењу x са n, је један хомоморфизам прстена.

- $f_n(x,n) +_n f_n(y,n) = f_n(x+y,n)$

f_n је „на", $\ker f = n\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. $n \geq 1$

Деф Нека је $f: A \to B$ хомоморфизам прстена. Језгро хомоморфизма f, $\ker f$, се дефинише са: $\ker f := \{x \in A \mid f(x) = 0_B\}$.

Став Нека је $f: A \to B$ хомоморфизам. Тада важи:

1. $\ker f \lhd A$ $\longrightarrow$ $x \in \ker f$, $a \in A$: $f(a\cdot x) = f(a)\cdot \underbrace{f(x)}_{0} = 0$
2. ако је $J \lhd B \Rightarrow f^{-1}[J] \lhd A$
3. ако је $I \lhd A$ и f је „на" $\Rightarrow f[I] \lhd B$.

Деф Нека је $I \lhd A$. На A дефинишем релацију конгруенције по модулу I са:

$a \equiv b \pmod I$ акко $a-b \in I$

Теорема (о изоморфизмима за прстене)

Нека је $f: A \to B$ хомоморфизам прстена. Тада је $\tilde{f}: A/\ker f \to \mathrm{Im} f$ задато са: $\tilde{f}(a+\ker f) := f(a)$ изоморфизам прстена.

19 Декартов производ прстена. Кинеска теорема о остацима.

Деф Нека су $(A_1,+',\cdot'),\dots,(A_n,+'',\cdot'')$ комутативни прстени са јединицом. На Декартовом производу $A=A_1\times\dots\times A_n$, задајемо структуру комутативног прстена са јединицом са:

$$(a_1,\dots,a_n)+(b_1,\dots,b_n):=(a_1+'b_1,\dots,a_n+''b_n)$$

$$(a_1,\dots,a_n)\cdot(b_1,\dots,b_n):=(a_1\cdot'b_1,\dots,a_n\cdot''b_n)$$

• $0_A=(0_{A_1},\dots,0_{A_n})$, $1_A=(1_{A_1},\dots,1_{A_n})$

Став Нека су $m_1,\dots,m_n$ позитивни цели бројеви за које је НЗД$(m_i,m_j)=1$, за све $i\neq j$. Тада је: $\mathbb{Z}/(m_1\cdots m_n)\mathbb{Z}\cong(\mathbb{Z}/m_1\mathbb{Z})\times\dots\times(\mathbb{Z}/m_n\mathbb{Z})$

Доказ

$f:\mathbb{Z}\to\mathbb{Z}/m_1\mathbb{Z}\times\dots\times\mathbb{Z}/m_n\mathbb{Z}$. $f(x)=(x+m_1\mathbb{Z},\dots,x+m_n\mathbb{Z})$.

$$x\in\ker f \iff \begin{matrix} x+m_1\mathbb{Z}=m_1\mathbb{Z}\\ x+m_2\mathbb{Z}=m_2\mathbb{Z}\\ \vdots \\ x+m_n\mathbb{Z}=m_n\mathbb{Z}\end{matrix} \iff \begin{matrix} m_1\mid x\\ m_2\mid x\\ \vdots\\ m_n\mid x\end{matrix} \iff \underbrace{\text{НЗС}(m_1,\dots,m_n)}_{= m_1\cdot m_2\cdot\ldots\cdot m_n}\mid x$$

$$\underbrace{\mathbb{Z}/m\mathbb{Z}\cong \mathrm{Im} f\le \mathbb{Z}/m_1\mathbb{Z}\times\dots\times\mathbb{Z}/m_n\mathbb{Z}}_{\text{исто}} \Rightarrow \mathrm{Im} f \text{ је све.}$$

Последица (Кинеска теорема о остацима)

Нека су $m_1,\dots,m_n$ позитивни цели бројеви који су пар по пар узајамно прости и $x_1,\dots,x_n$ произвољни цели бројеви. Тада постоји цео број x т.д.

$$x\equiv x_1 \pmod{m_1}$$

$$x\equiv x_2 \pmod{m_2}$$

$$\dots$$

$$x\equiv x_n \pmod{m_n}.$$

Ако је x' неки други цео број који задовољава наведени систем конгруенција, онда је: $x\equiv x' \pmod{m_1\cdot\ldots\cdot m_n}$.

Доказ

Из доказа претх. става следи да је f „на". То значи да за $x_1,\dots,x_n$ постоји $x\in\mathbb{Z}$ т.д.

$$\left.\begin{matrix} x+m_1\mathbb{Z}=x_1+m_1\mathbb{Z}\\ \dots \\ x+m_n\mathbb{Z}=x_n+m_n\mathbb{Z}\end{matrix}\right\} \Rightarrow \begin{matrix} x\equiv x_1 \pmod{m_1}\\ \dots\\ x\equiv x_n \pmod{m_n}\end{matrix}$$

Ако је x' други цео број који задовољава наведене конгруенције, то значи да је $f(x) = f(x')$ тј. $x - x' \in \ker f = (m_1, \dots, m_k)\mathbb{Z}$.

* $\varphi(mn) = \varphi(m)\varphi(n)$, НЗД$(m,n) = 1$

$\varphi(n) = |\Phi(n)|$, $U(\mathbb{Z}_n) = \Phi(n)$

$\boxed{\supseteq}$ $a \in \Phi(n)$, НЗД$(a,n) = 1$, $ap + nq = 1$ за неке $p, q \in \mathbb{Z}$

$a \cdot_n p = 1$, $\bar{p} = \rho(p,n)$, $\bar{a} = a$, $a \cdot_n \bar{p} = 1 \Rightarrow a \in U(\mathbb{Z}_n)$

$\boxed{\subseteq}$ $a \in U(\mathbb{Z}_n)$. $(\exists b \in \mathbb{Z}_n)$ $a \cdot_n b = 1$, $ab = 1 + nq \Rightarrow$ НЗД$(a,n) = 1$.

$d \mid a$, $d \mid n \Rightarrow d \mid 1$.

$\boxed{20}$ Инвертибилни елементи у прстену и Ојлерова теорема.

Став Ако су прстени A и B изоморфни, онда је $(U(A), \cdot) \cong (U(B), \cdot)$.

Доказ

Јасно је да се инвертибилни елем. сликају у инвертибилне. Ако је $a \in U(A)$, то значи да постоји a' т.д. $a \cdot a' = 1_A$. Тада је $f(a) \cdot f(a') = f(a \cdot a') = f(1_A) = 1_B$, па и $f(a)$ има инверз. Према томе, $f[U(A)] \subseteq U(B)$ за сваки хомоморфизам $f: A \to B$. Ако је f изоморфизам и $b \in U(B)$, то постоји $a \in A$ т.д. је $f(a) = b$. Елемент b има инверз, па је $b \cdot b' = 1_B$ за неки $b' \in B$. Елемент b' је слика неког елем. a': $f(a') = b'$. Тада је $f(a \cdot a') = f(a) \cdot f(a') = b \cdot b' = 1_B$, па како је f „1-1", мора бити $a \cdot a' = 1_A$, па a има инверз. Закључујемо да f успоставља бијекцију између $U(A)$ и $U(B)$. Како је f хомоморфизам, добијамо тражени изоморфизам.

Став Важи једнакост: $U(A_1 \times \dots \times A_n) = U(A_1) \times \dots \times U(A_n)$.

Теорема (Ојлерова)

Ако су $m_1, \dots, m_k$ пар по пар узајамно прости позитивни цели бројеви, онда је $\mathbb{Z}_{m_1 \dots m_k} \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$ и $\varphi(m_1 \dots m_k) = \varphi(m_1) \dots \varphi(m_k)$, где је φ - Ојлерова ф-ја.

Доказ →

Доказ

нзд$(m,n)=1$, $\varphi(mn) = |\Phi(mn)| = |U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}/mn\mathbb{Z})| =$

$= |U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})| = |U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})| =$

$= |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| = |U(\mathbb{Z}_m)| \cdot |U(\mathbb{Z}_n)| = |\Phi(m)| \cdot |\Phi(n)| =$

$= \varphi(m) \cdot \varphi(n).$

$\boxed{21}$ Коначне подгрупе мултипликативне групе поља. Примене.

Нисмо радили

Став Нека је A Абелова група реда m и нека за $\forall d$ који дели m постоји највише d елем. $a \in A$ за које је $da = 0$. Тада је A циклична група.

Теорема Нека је F поље и G коначна подгрупа групе $(F \setminus \{0\}, \cdot)$. Тада је G циклична група.

- свака коначна подгрупа мултипликативне групе поља је циклична.

Деф Ма који генератор групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ се зове примитивни корен модуло p.

Став Нека је r ма који прим. корен модуло p. Тада је са:
$ind_r(a) = x$ акко $r^x = a$, дефинисан изоморфизам
$ind_r : (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \to (\mathbb{Z}_{p-1}, +_{p-1})$.