Grupa $(G, \cdot)$ je grupa, če je monoid z inverzom g^{-1} za vsak $g \in G$: $\forall g \in G. \exists g^{-1} \in G. \; gg^{-1} = g^{-1}g = 1$

Če je G grupa, sta za vsaka $a, b \in G$ enačbi $a \cdot x = b$ in $x \cdot a = b$ enolično rešljivi.

$a^{-1} \cdot / \; a \cdot x = b$
$x = a^{-1}b$

$x \cdot a = b \; / \cdot a^{-1}$
$x = ba^{-1}$

Naj bo $(S, \cdot)$ polgrupa z deljenjem. Torej sta za vsaka $a, b \in S$ enačbi $ax = b$ in $xa = b$ rešljivi. Pokaži, da je S grupa.

Če je S monoid, vzamemo $b = 1$.

$ax = 1 \Rightarrow x = b$ je desni inverz
$xa = 1 \Rightarrow x = c$ je levi inverz

$\Rightarrow a$ je obrnljiv

Pokazati moramo še, da je S res monoid.

Vzemimo $b = a$.

$ax = a$ je rešljiva.

Naj bo $x = 1_a$ rešitev, torej $a \cdot 1_a = a$.

Pokažimo, da je 1_a desna enota.

$\forall b: \; b \cdot 1_a = b$

$b \cdot a = b \cdot a \cdot 1_a$

$1_a = xb = by$
$b = z \cdot 1_a = 1_a \cdot t$

...

Pokaži, da je vsaka grupa s štirimi elenti Abelova.

$G = \{1, a, b, c\}$

$a, b \in G$
$\Rightarrow ab, ba \in G$

(i) $ab = 1 \Rightarrow a = b^{-1} \Rightarrow ba = b^{-1}b = 1 = ab$
(ii) $ab = a \Rightarrow b = 1 \Rightarrow ba = 1 \cdot a = a = ab$
(iii) $ab = b \Rightarrow a = 1 \Rightarrow ba = b \cdot 1 = b = ab$

(iv) $ab = c$

Če $ba \in \{1, a, b\}$, po (i)-(iii) velja $ab \neq c$.
Protislovje, torej $ba = c = ab$.

Dokaži, da v vsaki grupi iz $xy = 1$ sledi $yx = 1$.

$xy = 1$
$\Rightarrow$ y je desni inverz od x
$\Rightarrow$ y je inverz od x
$\Rightarrow y = x^{-1}$
$\Rightarrow yx = 1$

Dokaži, da le v Abelovi grupi iz $xyz = 1$ sledi $zyx = 1$.

Če je G Abelova: $1 = xyz = x(yz) = (yz)x = zyx$

S_3 ni Abelova grupa:

$(2\ 3)(1\ 2) = (1\ 3\ 2)$
$(1\ 2)(2\ 3) = (1\ 2\ 3)$

$(1\ 3\ 2)^{-1} = (1\ 2\ 3)$
$\quad x \quad\ y \quad\ z$
$(1\ 2\ 3)(2\ 3)(1\ 2) = id$
$\quad z \quad\ y \quad\ x$
Ampak: $(1\ 2)(2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \neq id$

Dokaži, da je grupa, v kateri za vsak $x \in G$ velja $x^2 = 1$, Abelova.

Potem velja $x = x^{-1}$ za vsak $x \in G$.

$xy = x^{-1}y^{-1} = (yx)^{-1} = yx$

Ali je enačba $x^2 = a$ rešljiva v vsaki grupi?

Ne, saj enačba $2x = 1$ v $\mathbb{Z}_2$ nima rešitve:

$0 + 0 = 0$
$1 + 1 = 0$

Ali ima v vsaki grupi enačba $x^2 = a$ največ dve rešitvi?

Ne, saj v $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ enačba $x^2 = (0,0)$ velja za vse x.

SIMETRIČNA GRUPA S_n

$\pi \in S_n$ zapišemo kot produkt disjunktnih ciklov, te cikle pa zapišemo kot produkt transpozicij.

$$(a_1\ a_2 \cdots a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_2)$$

π je soda, če je produkt sodo mnogo transpozicij, in liho, če je produkt liho mnogo transpozicij.

$\operatorname{sgn}(\sigma) = (-1)^k$, kjer je k število transpozicij

Če je σ n-cikel: $\operatorname{sgn}(\sigma) = (-1)^{n-1}$

Naj bo $\sigma \in S_n$. Potem za vsak k-cikel $(a_1 \cdots a_k) \in S_n$ velja:

$$\sigma\,(a_1 \cdots a_k)\,\sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k))$$

Temu pravimo konjugiranje cikla.

Recimo, da je $x = \sigma(a_1)$. Potem $(\sigma(a_1 \cdots a_k)\sigma^{-1})(x) = \sigma(x_2)$. Podobno iz $x = \sigma(a_i)$ sledi $(\sigma(a_1 \cdots a_k)\sigma^{-1})(x) = \sigma(a_{i+1})$.

Ker je σ injektivna, velja, da so $\sigma(a_1), \dots, \sigma(a_k)$ med sabo različni, torej je to res cikel. Negibne točke se spet slikajo same vase, torej res dobimo k-cikel.

Definicija: Permutaciji $\sigma, \sigma \in S_n$ imata **enako zgradbo disjunktnih ciklov**, če sta σ in σ^{-1} produkta disjunktnih ciklov $k_1, \dots, k_s$ $(k_1 \leq \dots \leq k_s)$.

Primer: $(1\,2\,3)(4\,5\,6)(7\,8)$ in $(4\,2\,5)(8\,1)(6\,3\,7)$ sta oba produkta ciklov $2, 3, 3$.

Dokaži, da sta σ in σ' konjugirani (obstaja $\pi \in S_n$, da je $\sigma = \pi \sigma' \pi^{-1}$) natanko tedaj, ko imata enako zgradbo disjunktnih ciklov.

($\Rightarrow$) Naj bo $\sigma = \pi \sigma' \pi^{-1} = \pi \overbrace{\sigma_1 \sigma_2 \cdots \sigma_k}^{\text{disjunktni cikli od } \sigma'} \pi^{-1}$.

$\sigma_i := (a_1^i \; a_2^i \; \cdots \; a_{\ell_i}^i)$

$\Rightarrow \sigma = (\pi(a_1^1)\,\pi(a_2^1) \cdots \pi(a_{\ell_1}^1)) \cdots (\pi(a_1^k)\,\pi(a_2^k) \cdots \pi(a_{\ell_k}^k))$

$\Rightarrow$ cikli iste dolžine.

($\Leftarrow$) Naj imata σ in σ' enako zgradbo disjunktnih ciklov.

$\sigma = (a_1^1 \; a_2^1 \cdots a_{\ell_1}^1) \cdots (a_1^k \; a_2^k \cdots a_{\ell_k}^k)$
$\sigma' = (b_1^1 \; b_2^1 \cdots b_{\ell_1}^1) \cdots (b_1^k \; b_2^k \cdots b_{\ell_k}^k)$

$$\pi := \begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_{\ell_1}^1 & a_1^2 & a_2^2 & \cdots & a_{\ell_2}^2 & \cdots & a_1^k & a_2^k & \cdots & a_{\ell_k}^k \\ b_1^1 & b_2^1 & \cdots & b_{\ell_1}^1 & b_1^2 & b_2^2 & \cdots & b_{\ell_2}^2 & \cdots & b_1^k & b_2^k & \cdots & b_{\ell_k}^k \end{pmatrix}$$

Poišči vse $\pi \in S_n$, da je $\pi(1\,2) = (1\,2)\pi$.

Iščemo $\pi \in S_n$, da je $\pi(1\,2)\pi^{-1} = (1\,2)$.

$(\pi(1)\ \pi(2)) = (1\ 2)$

$\Rightarrow (\pi(1) = 1 \text{ in } \pi(2) = 2)$ ali $(\pi(1) = 2 \text{ in } \pi(2) = 1)$

$\pi_1 = (1\ 2)\,\sigma$
$\pi_2 = (1)(2)\,\sigma$
σ permutacija na $\{3, 4, \ldots, n\}$

Takih π je $2 \cdot (n-2)!$.

$C((1\,2)) = \{\pi \in S_n \,;\ \pi(1\,2) = (1\,2)\pi\}$

~ Centralizator elementa $(1\,2)$.

Pokaži, da lahko vsak element $\pi \in S_n$ zapišemo kot produkt transpozicij oblike $(k\ k+1)$, kjer je $1 \leq k \leq n-1$.

$\pi = (i_1\ i_2)(i_3\ i_4)\cdots$

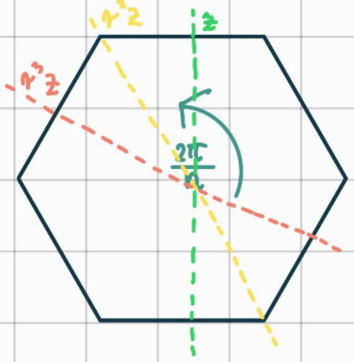
Zapišemo vsako transpozicijo v obliki:
$\tau = (i\ j)$, $i < j$

$(i\ j) = (i\ i+1)(i+1\ i+2)\cdots(j-1\ j)\cdots(i+1\ i+2)(i\ i+1)$

$\Rightarrow$ Transpozicije $(k\ k+1)$ generirajo S_n.

DIEDRSKA GRUPA D_{2n}

$|D_{2n}| = 2n$



r - rotacija za $\frac{2\pi}{n}$
z - zrcaljenje čez os simetrije

$r^n = 1$
$z^2 = 1$

$D_{2n} = \{1, r, \dots, r^{n-1}, z, rz, \dots, r^{n-1}z\}$

$zr^k = r^{n-k}z = r^{-k}z$

$n = 2$: simetrija pravokotnika, ki ni kvadrat

$D_{2\cdot 2} = \{1, a, b, ab\}$
$ab = ba$

$n = 1$: simetrija daljice

Poišči vse $x \in D_{2n}$, ki komutirajo z:

a) r

$xr = rx$

r^k komutira z r

$k \in \{0, \dots, n-1\}$

$x = r^k z$

$r^k z r = r r^k z$

$r^k r^{-1} z = r r^k z$

$r^{k-1} z = r^{k+1} z$

$k-1 \equiv k+1 \mod n$

$2 \equiv 0 \mod n$

Če $n > 2$, ne obstaja $x = r^k z$, ki komutira z r.

Če $n = 2$, je $k = 0$ ali $k = 1$.

b) z

$xz = zx$

1) $x = r^k$

$r^k z = z r^k$

$r^k z = r^{-k} z$

$k \equiv -k \mod n$

$2k \equiv 0 \mod n$

1.1) $k = 0$

1.2) $k = \frac{n}{2}$, če $n \equiv 0 \mod 2$

2) $x = r^k z$

$r^k z z = z r^k z$
$r^k z z = r^{-k} z z$
$r^k = r^{-k}$

2.1) $k = 0$
2.2) $k = \frac{n}{2}$, če $n \equiv 0 \mod 2$

PODGRUPE

G grupa
$H, K \leq G$
$H \cap K \leq G$

Dokaži: Če je $HUK \leq G$, potem je $H \subseteq K$ ali $K \subseteq H$.

Predpostavimo, da $H \not\subseteq K$. Dokazujemo $K \subseteq H$.

$\exists h \in H.\ h \notin K$
$\forall k \in K.\ k \in H$

$h, k \in HUK$
$\Rightarrow hk \in HUK$

1) $hk = h_1 \in H$
$k = h^{-1} h_1 \in H$

(zaključek za invertiranje)

2) $hk = k_1 \in K$
$h = k_1 k^{-1} \in K$

↯

Torej $K \subseteq H$.

Če je $H_1 \cup H_2 \cup H_3 \leq G$ in $H_1, H_2, H_3 \leq G$, to ne drži nujno.

$G = \{1, a, b, c\}$
$H_1 = \{1, a\}$, $H_2 = \{1, b\}$, $H_3 = \{1, c\}$

$a^2 = 1$, $b^2 = 1$, $c^2 = 1$
$ab = c$

$\Rightarrow G = D_{2 \cdot 2}$

Naj bo $H_1 \leq G_1$ in $H_2 \leq G_2$. Potem je $H_1 \times H_2 \leq G_1 \times G_2$.

Naj bo $H \leq G_1 \times G_2$. Ali je res $H = H_1 \times H_2$, kjer je $H_1 \leq G_1$ in $H_2 \leq G_2$?

Podgrupe $\mathbb{Z}_2 = \{0, 1\}$:

$\{0\}$
$\mathbb{Z}_2$

Podgrupe $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$:

$\{0\} \oplus \mathbb{Z}_2$
$\mathbb{Z}_2 \oplus \{0\}$
$\{0\} \oplus \{0\}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2$

manjka nam:
$\{(0,0),(1,1)\}$

G poljubna netrivialna grupa
$\Rightarrow \{(g,g)\,;\, g\in G\} \leq G\times G$ ~ diagonalna podgrupa

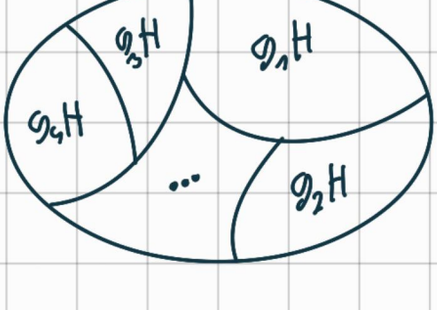
Diagonalna podgrupa ni $H_1\times H_2$, kjer $H_1\leq G_1$, $H_2\leq G_2$.

Torej trditev ne drži.

ODSEKI

$H\leq G$

gH - levi odsek
Hg - desni odsek



$$g_1H\cap g_2H=\begin{cases}\emptyset\\ g_1H\end{cases}\quad ;\ g_1H=g_2H$$

$$g_1H=g_2H \Leftrightarrow g_1^{-1}g_2\in H \Leftrightarrow g_2^{-1}g_1\in H$$

Podobno za desne odseke.

Opiši odseke:

a) grupe D_8 po podgrupi $\{1, z\}$

$$dH = \{dh;\ h \in H\}$$

$$D_8 = \{1, r, r^2, r^3, z, rz, r^2z, r^3z\}$$

$$1H = \{1, z\}$$
$$rH = \{r, rz\}$$
$$r^2H = \{r^2, r^2z\}$$
$$r^3H = \{r^3, r^4z\}$$

$$H1 = \{1, z\}$$
$$Hr = \{r, zr\} = \{r, r^3z\}$$
$$Hr^2 = \{r^2, zr^2\} = \{r^2, r^2z\}$$
$$Hr^3 = \{r^3, zr^3\} = \{r^3, rz\}$$

b) grupe U_{12} po podgrupi $\{1, -1, i, -i\}$

$$U_{12} = \{z^{12} = 1;\ z \in \mathbb{Z}\} = \{e^{\frac{\pi i k}{6}};\ k \in \{0, 1, \dots, 11\}\}$$

$$H = \{1, -1, i, -i\}$$

V Abelovih grupah: levi = desni

$$e^{\frac{i\pi}{6}}H = \{e^{\frac{i\pi}{6}}, -e^{\frac{i\pi}{6}}, ie^{\frac{i\pi}{6}}, -ie^{\frac{i\pi}{6}}\}$$
$$e^{\frac{i\pi}{3}}H = \{e^{\frac{i\pi}{3}}, -e^{\frac{i\pi}{3}}, ie^{\frac{i\pi}{3}}, -ie^{\frac{i\pi}{3}}\}$$
$$e^{\frac{i\pi}{2}}H = iH$$

c) grupe $3\mathbb{Z}$ po podgrupi $12\mathbb{Z}$

$$3\mathbb{Z} = \{3k;\ k \in \mathbb{Z}\}$$
$$H = 12\mathbb{Z} = \{12k;\ k \in \mathbb{Z}\}$$

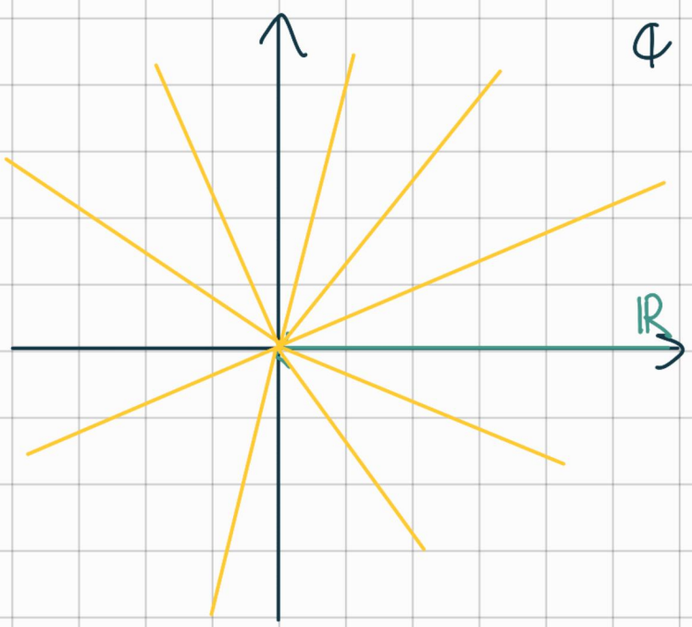
$H = \{12k;\ k \in \mathbb{Z}\}$
$3+H = \{3+12k;\ k \in \mathbb{Z}$
$6+H = \{6+12k;\ k \in \mathbb{Z}$
$9+H = \{9+12k;\ k \in \mathbb{Z}$
$12+H = \{12(1+k);\ k \in \mathbb{Z}\} = H$

Indeks podgrupe = število odsekov
$[3\mathbb{Z} : 12\mathbb{Z}] = 4$

Za končne: $[G : H] = \frac{|G|}{|H|}$

d) grupe $\mathbb{C}^*$ po podgrupi $\mathbb{R}^+$

$\mathbb{C}^* = (\mathbb{C}\setminus\{0\}, \cdot)$
$\mathbb{R}^+ = (\{r \in \mathbb{R}, r > 0\}, \cdot)$



Naj bo $z \in \mathbb{C}^*\setminus\mathbb{R}^+$. Poglejmo $z\mathbb{R}^+$. Naj bo $z = e^{i\varphi}$.

$z\mathbb{R}^+ = \{re^{i\varphi};\ r \in \mathbb{R}^+\}$, $\varphi \in [0, 2\pi]$

$[\mathbb{C}^* : \mathbb{R}^+] = \infty$

e) grupe $GL_n(\mathbb{R})$ po podgrupi $SL_n(\mathbb{R})$

$GL_n(\mathbb{R})$ – grupa obrnljivih $n \times n$ matrik nad $\mathbb{R}$
$SL_n(\mathbb{R})$ – grupa $n \times n$ matrik z determinanto 1 nad $\mathbb{R}$

Naj bo $A \in \mathbb{R}^{n\times n}$, $\det A \neq 1$.

$A \cdot SL_n(\mathbb{R}) = \{A \cdot B \,;\, B \in SL_n(\mathbb{R})\}$

Če je $C \in A \cdot SL_n(\mathbb{R})$, je $\det C = \det(A \cdot B) =$
$= \det A \cdot \det B = \det A$.

Naj bo $\det C = \det A$. Potem je $C = A \cdot A^{-1}C$.

$\det(A^{-1}C) = \frac{\det C}{\det A} = \frac{\det A}{\det A} = 1 \Rightarrow C \in A \cdot SL_n(\mathbb{R})$

$\Rightarrow A \cdot SL_n(\mathbb{R}) = \{C \in \mathbb{R}^{n\times n} \,;\, \det C = \det A\}$

$\Rightarrow GL_n(\mathbb{R}) = \bigcup_{r\in\mathbb{R}^*} r \cdot I \cdot SL_n(\mathbb{R})$

Desni odseki sovpadajo, čeprav množenje matrik ni komutativno.

$\Rightarrow SL_n(\mathbb{R})$ je podgrupa edinka v $GL_n(\mathbb{R})$.
(normal subgroup)

Naj bosta H in K končni podgrupi grupe G.

Pokaži: $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$

$HK = \{h\cdot k \,;\, h\in H, k\in K\} = \bigcup_{h\in H} hK$

V splošnem $H\cdot K$ ni podgrupa. Če je $h\cdot k = k\cdot h$ za vse $h\in H$, $k\in K$, potem $H\cdot K$ je podgrupa.

$|hK| = |K|$

Predpostavimo, da imamo m odsekov.

$\Rightarrow |HK| = m \cdot |K|$

$h_1K = h_2K \iff h_2^{-1}h_1 \in K \iff h_2^{-1}h_1 \in H \cap K$ (podgrupa)

$H \cap K \leq H$

$h_1(H\cap K) = h_2(H\cap K) \iff h_2^{-1}h_1 \in H\cap K$

Koliko je odsekov?

$[H : H\cap K] = \frac{|H|}{|H\cap K|} = m$

$\Rightarrow |HK| = \frac{|H|\cdot|K|}{|H\cap K|}$

Naj bo G končna grupa in $H \leq G$. Pokaži, da dobstajata elementa $a,b \in G$, da $a \notin H$, $b \notin H$, $ab \notin H$, vsaj ko tedaj, ko je $2 \cdot |H| < |G|$.

$2 < \frac{|G|}{|H|} = [G : H]$
$\iff$ imamo vsaj 3 odseke

($\Rightarrow$) Predpostavimo, da obstajata $a,b \in G$, da $a,b \notin H$ in $ab \notin H$. Dokazujemo, da imamo vsaj 3 odseke.

$1H$ je odsek
aH je odsek
bH je odsek
abH je odsek

Ali sovpadajo?

$1 \cdot H = aH \Leftrightarrow 1^{-1} \cdot a \in H \Rightarrow 1 \cdot H \neq aH$
$\Rightarrow 1 \cdot H \neq bH$
$\Rightarrow 1 \cdot H \neq abH$

Predpostavimo $aH = bH = abH$.

$abH = aH \Leftrightarrow a^{-1}ab \in H \Leftrightarrow b \in H \Rightarrow$ ↯

$\Rightarrow$ Imamo različne odseke: $1 \cdot H$, aH, abH

($\Leftarrow$) Predpostavimo, da imamo različne odseke H, aH, bH.

$\Rightarrow a \notin H$, $b \notin H$, $b^{-1}a \notin H$
$\Downarrow$
$b^{-1} \notin H$

$\Rightarrow H$, $b^{-1}H$, $b^{-1}aH$ odseki

$\Rightarrow a \notin H$, $b^{-1} \notin H$, $b^{-1}a \notin H$
so naši elementi

CIKLIČNE GRUPE

$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \langle 1 \rangle$
red: 1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12

$\langle 4 \rangle = \{0, 4, 8\}$

Kateri izmed elementov generirajo $\mathbb{Z}_{12}$? Tisti, ki imajo red 12:
1, 5, 7, 11

Podgrupe v $\mathbb{Z}_{12}$: $\{0\}$, $\mathbb{Z}_{12}$, $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\} = \langle 10 \rangle$,
$\langle 3 \rangle = \{0, 3, 6, 9\} = \langle 9 \rangle$, $\langle 4 \rangle = \{0, 4, 8\} = \langle 8 \rangle$, $\langle 6 \rangle = \{0, 6\}$

Lagrangev izrek: Red podgrupe deli red grupe.

V $\mathbb{Z}_{12}$ velja tudi obrat.

Pokaži, da $\mathbb{Z}_n$ vsebuje podgrupo reda k natanko tedaj, ko $k \mid n$, in da je taka podgrupa ena sama.

$n = k \cdot l$

Podgrupa reda k: $\langle l \rangle = \{0, l, 2l, \ldots, (k-1)l\}$

Zakaj je to edina podgrupa reda k?

$H < \mathbb{Z}_n$, H reda k
$H = \{h_1 = 0, \ldots, h_k\}$

$\text{red}(h_i) \mid k$

Vsi elementi v $\mathbb{Z}_n$, katerih red deli k:

$t \in \mathbb{Z}_n$: $\text{red}(t) \mid k \Leftrightarrow t \cdot k = 0$ v $\mathbb{Z}_n \Leftrightarrow$
$\Leftrightarrow n \mid tk \Leftrightarrow k \cdot l \mid t \cdot k \Leftrightarrow l \mid t$

$\Rightarrow t \in \langle l \rangle$

$\Rightarrow H \subseteq \langle l \rangle$

$\Rightarrow H = \langle l \rangle$

Vsaka podgrupa $\mathbb{Z}_n$ je ciklična.

Pokaži, da je podgrupa ciklične grupe ciklična.

$G = \langle a \rangle = \{1, a, a^{-1}, a^2, a^{-2}, \dots\}$

1) $\mathbb{Z} = \langle 1 \rangle$, a ima neskončen red

2) $G = \langle a \rangle \approx \mathbb{Z}_n$, $a^n = 1$

Podgrupe $\mathbb{Z}$: $\{0\}, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \dots$

$\mathbb{Z}$ nima drugih podgrup:

$H \leq \mathbb{Z}$, $H \neq \{0\}$

$n > 0$ in n najmanjši pozitiven element v H

Pokažimo $H = n\mathbb{Z}$

Ker $n \in H$, potem $n\mathbb{Z} \subseteq H$.

Če $k \in H$, potem $n \mid k$.

$d = \gcd(n, k)$, $d < n$

$d = \underset{\in H}{\alpha \cdot n} + \underset{\in H}{\beta \cdot k}$, $\alpha, \beta \in \mathbb{Z}$

$\Rightarrow d \in H \Rightarrow$ 

(knjiga v spletni učilnici)

Naj bo G neskončna grupa. Pokaži, da ima G neskončno mnogo podgrup.

Če ima G element neskončnega reda, potem ima podgrupo $H \cong \mathbb{Z}$, ki ima neskončno podgrup.

Če G nima elementa neskončnega reda:

$n = 1$:

$\langle 1 \rangle$ je končna
$a \in G \setminus \langle 1 \rangle$
$\langle a \rangle$ ima neskončno podgrup

$n \to n+1$:

Recimo, da imamo n končnih podgrup $A_1, \dots, A_n$.
Obstaja $a \in G \setminus (\cup A_i)$, in je $\langle a \rangle$ spet končna ima neskončno podgrup.

Določi red od $k \in \mathbb{Z}_n$.

$0 \leq k \leq n-1$

$\text{red}(0) = 1$
$\text{red}(1) = n$

$r = \text{red}\, k \iff r$ najmanjši, da $n \mid r \cdot k$

$g = \gcd(n, k)$

$n = g \cdot \alpha$
$k = g \cdot \beta$

$n \mid r \cdot k$
$g \cdot \alpha \mid r \cdot g \cdot \beta$
$\alpha \mid r \cdot \beta$

$\gcd(\alpha, \beta) = 1$

$\Rightarrow r = \alpha = \frac{n}{g} = \frac{n}{\gcd(n,k)}$

$\Rightarrow \text{red}(k) = \frac{n}{\gcd(n,k)}$

$\gcd(n,k) = 1 \Rightarrow \text{red}(k) = n$

Kdaj $k \in \mathbb{Z}_n$ generira $\mathbb{Z}_n$?

Kadar sta n, k tuji.

Kdaj je $\mathbb{Z}_n \oplus \mathbb{Z}_k$ ciklična?

Ko je $\gcd(n,k) = 1$.

$(m,h) \in \mathbb{Z}_n \oplus \mathbb{Z}_k$:

$\text{red}(m,h) = \text{lcm}(\text{red}(m), \text{red}(h))$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ni ciklična:

Nima elementa reda 4.

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$ je ciklična:

Generirana je z $(1,1)$.

$(1,1)$, $2(1,1) = (0,2)$, $3(1,1) = (1,1)$,
$4(1,1) = (0,1)$, $5(1,1) = (1,2)$

Pokaži:

a) $\text{red}(a) = \text{red}(a^{-1})$

b) $\text{red}(a) = \text{red}(bab^{-1})$

c) $\text{red}(ab) = \text{red}(ba)$

d) Ali imata v vsaki grupi elementa $a^{-1}b^{-1}$ in $a^{-1}b$ enak red kot ab?

a) $r = \text{red}\, a$
$\Rightarrow a^r = 1$

$(a^{-1})^r = (a^r)^{-1} = 1^{-1} = 1$

Dokazati moramo še, da je najmanjši.

$\text{red}(a^{-1}) \leq \text{red}(a)$

Zaradi simetrije:

$\text{red}((a^{-1})^{-1}) \leq \text{red}(a^{-1})$
$\text{red}(a) \leq \text{red}(a^{-1})$

$\Rightarrow \text{red}(a^{-1}) = \text{red}(a)$

Če je red neskončen:

$\forall n \in \mathbb{N}: a^n \neq 1$

$\text{red}(a^{-1}) = r < \infty$
$\Rightarrow \text{red}(a) \leq r$


b) $r = \text{red}\, a$
$\Rightarrow a^r = 1$

$(bab^{-1})^r = bab^{-1}bab^{-1}\cdots bab^{-1} = ba^r b^{-1} = bb^{-1} = 1$
$\Rightarrow \text{red}(bab^{-1}) \leq r$

$a = b^{-1}(bab^{-1})b$

$\text{red}(a) = \text{red}(b^{-1}(bab^{-1})b) \leq \text{red}(bab^{-1})$

Neskončni red podobno kot prej.

c) $r = \text{red}(ab)$
$\Rightarrow (ab)^r = 1$

$(ba)^r = ba\,ba\cdots ba$

$(ba)^{r+1} = baba\cdots ba = b(ab)^r a = ba$

$(ba)^{-1}(ba)^{r+1} = (ba)^r(ba)$
$(ba)^r = 1$

$\text{red}(ba) \leq \text{red}(ab)$
$\text{red}(ab) \leq \text{red}(ba)$

$\text{red}(ab) = \text{red}(ba)$

Neskončni red podobno kot prej.

d) $\text{red}(a^{-1}b^{-1}) = \text{red}((ab)^{-1}) \overset{(a)}{=} \text{red}(ab) \overset{(c)}{=} \text{red}(ba)$

$\mathbb{Z}_3$:

$a = 1, b = 2$

$\Rightarrow a + b = 0$ $\qquad -a + b = 1$
$\text{red}(a+b) = 1$ $\qquad \text{red}(-a+b) = 3$

$\Rightarrow \text{red}(a^{-1}b^{-1}) = \text{red}(ba)$
$\text{red}(a^{-1}b) \neq \text{red}(ba)$

Splošno:

$b = a^{-1}$
$\Rightarrow \text{red}(ab) = \text{red}(1) = 1$

$\Rightarrow a^{-1}b = b^2$

Vzamemo tak b, da $b^2 \neq 1$.

GENERATORJI GRUP

G je generirana z $A \subseteq G$, ko lahko vsak $g \in G$ zapišemo v obliki $g = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$, $n \geq 0$, $a_i \in A$, $\varepsilon_i = \pm 1$.

Pokaži, da je grupa $(\mathbb{R}^*, \cdot)$ generirana z intervalom $A = [-2, -1]$.

$A^2 = [1, 4]$
$A^3 = A^2 A = [-8, -1]$
$A^{-1} = [-1, -\frac{1}{2}]$
$A^{-2} = [\frac{1}{4}, 1]$

Naj bo $x \in \mathbb{R} \setminus \{0\}$.

Če je $x \geq 1$, obstaja tak $n \in \mathbb{N}$, da je $x \in [1, 2^{2n}] = A^{2n}$.

Če je $0 \leq x \leq 1$, obstaja tak $n \in \mathbb{N}$, da je $x \in [\frac{1}{2^{2n}}, 1] = A^{-2n}$.

Če je $-1 \leq x \leq 0$, obstaja tak $n \in \mathbb{N}$, da je $x \in [-1, -\frac{1}{2^{2n-1}}] = A^{-2n+1}$.

Če je $x \leq -1$, obstaja tak $n \in \mathbb{N}$, da je $x \in [-2^{2n-1}, -1] = A^{2n-1}$.

MATRIČNE GRUPE

a) Določi red podgrupe grupe $GL_2(\mathbb{Q})$, generirane z matrikama:

$$A = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{3}} \end{bmatrix}$$

b) Opiši podgrupo grupe $GL_2(\mathbb{C})$, generirane 2 matrikama:

$$A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

a) $\begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & \\ & 1 \end{bmatrix} = A^2$

$\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}\begin{bmatrix} i & \\ & 1 \end{bmatrix} = \begin{bmatrix} -i & \\ & 1 \end{bmatrix} = A^3$

$\begin{bmatrix} -i & \\ & 1 \end{bmatrix}\begin{bmatrix} i & \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} = A^4 = 1$

$B^3 = 1$

$A^{-1} = \begin{bmatrix} -i & \\ & 1 \end{bmatrix} = A^3$

Oglejmo si produkte $A^k B^m$, $k = 0,1,2,3$, $m = 0,1,2$:

A^{-k} /

$A^k B^m = A^s B^n B^{-n}$

$B^{m-n} = A^{s-k}$

$red = 1,3$ $\quad$ $red = 1,2,4$

$\Rightarrow$ Elementov je vsaj 12.

Velja: $AB = BA$

$\Rightarrow A^{\alpha_1} B^{\beta_1} A^{\alpha_2} B^{\beta_2} \cdots = A^{\alpha_1 + \alpha_2 + \cdots} B^{\beta_1 + \beta_2 + \cdots}$

Vsak element je $A^k B^m$ za vsa $k = 0,1,2,3$, $m = 0,1,2$.

$\Rightarrow$ Imamo točno 12 elementov.

b) red $A = 4$

$$A^2 = \begin{bmatrix} -1 & \\ & -1 \end{bmatrix} = -I \quad , \quad A^3 = A \cdot A^2 = -A$$
$$A^{-1} = A^3 = -A$$

$$B^2 = \begin{bmatrix} -1 & \\ & -1 \end{bmatrix} = -I \quad , \quad B^3 = B \cdot B^2 = -B$$
$$B^{-1} = B^3 = -B$$

$$AB = \begin{bmatrix} i & \\ & -i \end{bmatrix} \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} = \begin{bmatrix} & i \\ i & \end{bmatrix}$$

$$BA = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} \begin{bmatrix} i & \\ & -i \end{bmatrix} = \begin{bmatrix} & -i \\ -i & \end{bmatrix}$$

$\Rightarrow AB = -BA$

$$ABABABA\cdots = -A^2B^2ABA\cdots$$

Elementi naše grupe:

$$\underset{1}{I}, \underset{2}{-I}, \underset{4}{A}, \underset{4}{-A}, \underset{4}{B}, \underset{4}{-B}, \underset{4}{AB}, \underset{4}{-AB}$$

$\Rightarrow$ Imamo 8 elementov.

D_8 ima tudi 8 elementov. Ampak nista izomorfni.

$C = AB$: $A^2 = B^2 = C^2 = I$

$Q = \{\pm \underset{I}{1}, \pm \underset{A}{i}, \pm \underset{B}{j}, \pm \underset{AB}{k}\}$ ... kvaternionska grupa

Vse grupe reda 8:

- $\mathbb{Z}_8$
- $\mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- D_8
- Q

Vse grupe reda 6:

- $\mathbb{Z}_6$
- S_3