Uvod v teorijo grup

Operacija na množici $S \neq \emptyset$

$\star : S \times S \longrightarrow S$

- $\star$ je asociativna ko $\forall a,b,c.\ (a \star b) \star c = a \star (b \star c)$
- $\star$ je komutativna $\forall a,b.\ a \star b = b \star a$

Definicija: $(S, \star)$ je polgrupa, če je $\star$ asociativna

Definicija: Naj bo S množica z operacijo $\star$. Pravimo da je $e \in S$ enota oz. nevtralni element, ko $\forall a.\ ea = ae = a$

Velja: če $\exists$ enota, potem je ena sama

Definicija: Polgrupa z enoto je monoid

Definicija: S naj bo množica z operacijo $\star$ in enota e. Naj bo $x \in S$

a) $l \in S$ je levi inverz, če velja $lx = x$

b) $d \in S$ je desni inverz, če $x \star d = x$

c) $y \in S$ je inverz, če $x \star y = y \star x = e$

$$l = le = l(ed) = (l \star e) \star d = e \star d = d$$

Definicija: $x \in S$ je obrnljiv, če $\exists$ inverz za x

Definicija: Naj bo S z operacijo $\star$ monoid in je vsak element obrnljiv, potem je S grupa

Če je $\star$ komutativna je abelova

Zgledi:

1.) $(\mathbb{Z}, +)$ abelova grupa

2) X neprazna množica

$Sim(X) = \{f : X \rightarrowtail\!\!\!\twoheadrightarrow X\}$ množica vseh bijektivnih preslikav

operacija: kompozitum $\circ$

asociativnost, enota, inverz

$(Sim(X), \circ)$ je simetrična grupa množice X

Poseben primer: X je končna $X = \{1, 2, \dots, n\}$

$Sim(X) = Sim\{1, \dots, n\} = S_n$

.... Simetrična grupa reda n

Ponovitev o permutacijah

(elementi S_n)

- Vsaka permutacija je produkt (kompozitum) disjunktnih ciklov

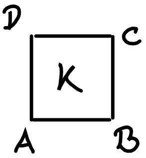
- cikli dolžine 2 je transpozicija

- vsaka permutacija $\sigma \in S_n$ je produkt transpozicij. Teh transpozicij je vedno sodo ali vedno liho mnogo

  $$\operatorname{sgn} = \begin{cases} 1 & : \sigma \text{ je produkt sodo mnogo transpozicij} \\ -1 & \sigma \text{ je produkt liho mnogo transpozicij} \end{cases}$$

- $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma)$

Zgled: Simetrije kvadrata

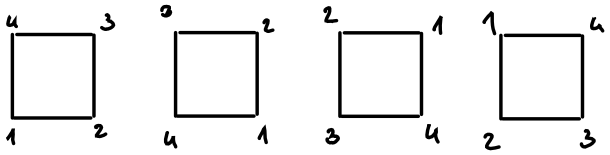


= izometrije $f:\mathbb{R}^2 \to \mathbb{R}^2$, da je $f_*(K)=K$

$f|_K : K \to K$ je bijekcija

Preverimo da je množica simetrij grupa za kompozitum

Simetrija slika oglišča v oglišča
↳ permutacija oglišč

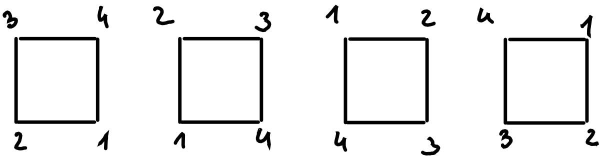


id = r^4

r: rotacija za $90°$ okoli središča (1 2 3 4)

r^2

r^3



z - zrcaljenje čez fiksno os simetrije

rz zr^3

r^2z zr^2

r^3z zr

$z^2 = id$

(1 2)(3 4)

$r^3z = zr$

$rzr = 1$

Torej vsak kompozitum r-jev in z-jev je oblike $r^n z^m$

$\{id, r, r^2, r^3, rz, r^2z, r^3z\}$

Trdimo: kvadrat ima kvečjemu 8 simetrij

Simetrija je določena s sliko oglišča 1 in informacija ali smo naredili zrcaljenje ali ne

slike 1: 4 možnosti   zrcaljenje (da/ne) 2 možnosti

$4 \cdot 2 = 8$ manj kot 8 možnosti

$D_{2\cdot 4} = \{id, r, r^2, r^3, zr, zr^2, zr^3\}$

Diederska grupa moči 8

Splošna simetrasija :

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

$$D_{2\cdot n} = \{1, r, \ldots, r^{n-1}; z, zr^2, \ldots zr^{n-1}\}$$

Diederska grupa moči $2n$

Velja $zr = r^{n-1}z$

Če je $(S, \star)$ monoid naredimo množico

$S^* := \{$ obrnljivi elementi iz $S\}$

S^* je grupa za $\star$

$e \in S^* \Rightarrow S^* \neq \emptyset$

Ali je S^* zaprta za operacijo

$x, y \in S^*$

$(x \star y)^{-1} = y^{-1} \star x^{-1}$ DN dokaži

$(x \star y) \star (y^{-1} \star x^{-1}) = x \star (e) \star (x^{-1}) = e$ ✓

Vsak $x \in S^*$ ima inverz $\in S^*$ ∎

NPR: $S = (\mathbb{R}^{n \times n}, \cdot)$

$S^* = \{A \in \mathbb{R}^{n \times n}; \det A \neq 0\} = GL_n(\mathbb{R})$

splošna linearna grupa $n \times n$ matrik

Direktni produkt grup

$G_1, \dots, G_n$ naj bodo grupe z operacijami $①, ②, ③, \dots ⓝ$

$G_1 \times G_2 \times \dots \times G_n$ vpeljemo operacijo $\star$

$$(g_1, \dots, g_n) \star (h_1, \dots, h_n) =$$

$$(g_1 ① h_1, g_2 ② h_2, \dots, g_n ⓝ h_n)$$

DN: to je grupa

Oznake:

	operacija	enota	inverz x	potenca x
grupa	$\cdot$	1	x^{-1}	x^n
abelova grupa	$+$	0	$-x$	nx

Podgrupe

Def: Naj bo G grupa, $H \subseteq G$ $H \neq \emptyset$

H je podgrupa grupe G, če je H grupa za isto operacijo

Trditev: Naslednje trditve so ekvivalentne

1) $H \leq G$
2) $\forall x, y \in H: xy^{-1} \in H$
3) H je zaprta za množenje in invertiranje

Dokaz:

$2 \Rightarrow 3$

$1 \in H$

· Izberemo $x \in H$ $y = x$

$xx^{-1} = 1 \in H$

Naj bo $x \in H$ poljuben

$x^{-1} \in H$

$1 \cdot x^{-1} \in H$

Izberemo $y \in H$

$y^{-1} \in H$

$x \cdot (y^{-1})^{-1} \in H \Rightarrow xy \in H$

Posledica: Naj bo G končna grupa
Naj bo $H \neq 0$ $H \leq G$

Potem je H podgrupa $\Leftrightarrow$ H je zaprta za množenje

Primer:

Določimo vse podgrupe v $(\mathbb{Z}, +)$

- $\{0\}$ trivialna podgrupa
- $\mathbb{Z}$

$H \leq \mathbb{Z}$ brez škode za splošnos H ni trivialna

H gotova vsebuje vsaj eno naravno število

Naj bo n najmanjše naravno število v H

Trdimo $H = n\mathbb{Z} = \{nk \,;\, k \in \mathbb{Z}\}$

Ker je H zaprta za invertiranje, je $n\mathbb{Z} \subseteq H$

Vzemimo poljuben $m \in H$

$m = kn + r \qquad 0 \leq r < n$

$r = \underbrace{m}_{\in H} - \underbrace{kn}_{\in H} \in H \qquad r < n$

$\Rightarrow r = 0 \Rightarrow m = kn \Rightarrow m \in n\mathbb{Z}$

Primer

1) $GL_n(\mathbb{R})$ – obnljive $n \times n$ matrike
je grupa za množenje matrik

$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$ ....specialna linearna grupa

$SL_n(\mathbb{R})$

2) $O(n) = \{A \in GL_n(\mathbb{R}) : AA^T = A^T A = I\}$

3) $SO(n) = \{A \in O(n) : \det(A) = 1\}$

Trditev: Naj bosta $K, K \leqslant G$

Potem tudi $H \cap K \leqslant G$

Enako za preseke poljubnih družin podmnožic

Definicija: Naj bosta $HK \subseteq G$

$HK = \{h \cdot k : h \in H, k \in K$

produkt grup

Opomba:

HK ni vedno grupa

$G = S_3$

$H = \{id, (1,2)\}$

$K = \{id, (1,3)$

$HK = \{id, (1\,2), (1\,3), (1\,3\,2)$

$(1\,3\,2)(1\,3\,2) = (1\,2\,3) \notin HK$

Trditev: Naj bosta $H, K \leq G$. Če velja

$HK = KH$

potem je HK podgrupa

Dokaz:

$a, b \in HK$

$a = h_1 k_1 \quad h_1 \in H \; k_1 \in K$

$b = h_2 k_2 \quad h_2 \in H \; k_2 \in K$

$$ab^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 \underbrace{\underbrace{k_1 k_2^{-1}}_{\in K} \underbrace{h_2^{-1}}_{\in H}}_{\in KH = HK} = \underbrace{\underbrace{h_1 h_3}_{\in H} \underbrace{k_3}_{\in K}}_{\in HK}$$

✓

■

Trditev: Naj bo $H \leq G$, $a \in G$. Potem je

$$aHa^{-1} = \{aha^{-1}, h \in H\}$$

Potem je to tudi podgrupa

Dokaz: $x, y \in aHa^{-1}$

$$x = ah_1a^{-1} \qquad y = ah_2a^{-1}$$

$$x \cdot y^{-1} = ah_1a^{-1}(ah_2a^{-1})^{-1} =$$

$$= ah_1a^{-1}a^{-1}h_2^{-1}a = a\underbrace{h_1h_2^{-1}}_{\in H}a$$

$\blacksquare$

DN: Naj bo G grupa

1) $Z(G) = \{g \in G ;\ gx = xg \quad \forall x \in G\}$

je podgrupa v G (center grupe G

2) Naj bo $a \in G$. Potem je $C_G(a) = \{g \in G ; ga = ag\}$

podgrupa v G (centralizator elementa

a v G)

Odsek podgrup in Lagrangeov izrek

Naj bo G grupa in H podgrupa G
Vpeljemo relacijo na G

$$a \sim b \iff a^{-1}b \in H$$

Trditev: relacija je ekvivalenca

Naj bo G končna grupa

G/H je tudi končna

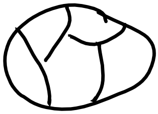
moč množice označimo z $|G:H|$ indeks podgrupe H v grupi G

Izrek: Če je G končna grupa in H podgrupa v G potem je $|G| = H \cdot |G:H|$

To je Lagrangeev izrek

Dokaz: $|G:H| = r$

$$G/H = \{a_1H, a_2H, \ldots, a_rH\}$$



$$|G| = |a_1H_1| + |a_2H_2| + \ldots + |a_rH|$$

Dokazati moramo, da je $|a_iH| = |H|$

$$\varphi: H \longrightarrow a_iH$$
$$h \longmapsto a_ih$$

φ je očitno surjektivna

injektivnost

$$\varphi(h_1) = \varphi(h_2)$$
$$a_ih_1 = a_ih_2$$
$$a_i^{-1}/ \quad h_1 = h_2$$

∎

Posledica: Naj bo G končna grupa in $H \leq G$. Potem $|H| \leq |G|$

Naj bo G abelova

Vpeljemo operacijo na G/H

$$(a+H)+(b+H)=(a+b)+H$$

Ali je ta operacija dobro definirana

$a+H=a'+H$ $\quad a^{-1}a'\in H$ $\quad a'-a\in H$

$b+H=b'+H$ $\quad b^{-1}b'\in H$ $\quad b'-b\in H$

Dokažemo $(a'+b')-(a+b)\in H$

komutativnost

$$a'+b'-a-b=(a'-a)-(b-b')\in H$$

G/H je abelova grupa za to operacijo

Generatorji grup, ciklične grupe

Definicija: Naj bo G grupa in X podmnožica v G. Potem označimo z $\langle X \rangle$ najmanjšo podgrupo, v G, ki vsebuje množico X.
Tej podgrupi pravimo <u>podgrupa generirana z množico X</u>

Zakaj je to smiselno?

$$\langle X \rangle = \bigcap_{X \subseteq A} A$$

Oznaka: če je $X = \{x_1, \ldots, x_n\}$ potem pišemo

$$\langle \{x_1, \ldots, x_n\} \rangle = \langle x_1, \ldots, x_n \rangle$$

Če je $G = \langle x_1, \ldots, x_n \rangle$ potem je G končno generirana grupa.

Če $\exists x \in G$. da je $G = \langle x \rangle$, pravimo da je G ciklična grupa

Kako izgledajo elementi $\langle X \rangle$?

$x_1, x_2 \in X \Rightarrow x_1^{-1} x_2 \in \langle X \rangle$

Očitno (DN)

$S = \{ x_{i_1}^{\pm 1} \cdot x_{i_2}^{\pm 1} \cdot \ldots \cdot x_{i_r}^{\pm 1} \; ; x_{i_j} \in X \} \subseteq \langle X \rangle$

Trditev: $\langle X \rangle = S$

Dokaz: $S \supseteq \langle X \rangle$

Naj bo $x \in \langle X \rangle$. $x = x \in S$

(Vzamemo produkt enega elementa x

$a, b \in S$

$a = x_{i_1}^{\pm 1} \cdot \ldots \cdot x_{i_r}^{\pm 1} \qquad x_{i_j} \in X$

$b = x_{k_1}^{\pm 1} \cdot \ldots \cdot x_{k_s}^{\pm 1} \qquad x_{i_j} \in X$

$a^{-1} \cdot b = x_{i_1}^{\mp 1} \cdot \ldots \cdot x_{i_r}^{\mp 1} \cdot x_{k_1}^{\pm 1} \cdot \ldots \cdot x_{k_s}^{\mp 1}$

Posledica: $a \in G$

$$\langle a \rangle = \{ a^n ; n \in \mathbb{N} \}$$

Pimeri:

$\mathbb{Z} = \langle 1 \rangle \qquad n \in \mathbb{Z} \Rightarrow n = n \cdot 1$

$\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle$

Trdimo $\mathbb{Z} = \langle 2, 3 \rangle$

(vsaki dve tuji števili generirata $\mathbb{Z}$

Def: Naj bo G grupa in $a \in G$.
Najmanjšemu naravnemu številu n, za katerega velja $a^n = 1$ pravimo red elementa a.
Če tak n ne obstaja pravimo, da ima a neskončen red

Primeri:

1. $\mathbb{Z}$; 1 ima neskončen red $(n \cdot 1)$
2. $\mathbb{Z}_n$ $1 + n\mathbb{Z}$ ima red n $k(1 + n\mathbb{Z}) = k + n\mathbb{Z}$

Trditev: Naj bo G grupa, $a \in G$
Potem je red elementa a enak n
$\Leftrightarrow$ $|\langle a \rangle| = n$

Dokaz:
$\Rightarrow$ Naj bo red $a = n$

Trdimo: $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$ in vsi
našteti elementi so paroma različni

$\supseteq$ ok
$\subseteq$ Naj bo $k \in \mathbb{Z}$ $k = mn + ost$ $0 \leq r \leq n-1$
$a^k = a^{mn+r} = (\underbrace{a^n}_{1})^m \cdot a^r = a^r$

Recimo da obstajata $0 \leq k < l \leq n-1$
$a^k = a^l \ / a^{-k}$
$1 = a^{l-k}$ $l-k < n$ kar je v protislovju
z predpostavko.

$\Leftarrow$ Recimo da $|\langle a \rangle| = n$
Potem ima a končen red
Po prejšnjem sklepu ima
$\langle a \rangle = \{1, a, \dots, a^{m-1}\}$
Sledi: $m = n$

DN: $(\mathbb{Q},+)$ ni končno generirana

Posledica: Naj bo G končna grupa

1) $\forall a \in G.$ red a deli $|G|$

2) $\forall a \in G.$ $a^{|G|} = 1$

3) $|G|$ je praštevilo $\Rightarrow$ G je ciklična

Dokaz:

1) red $a = n$ $(n < \infty$ ker je G končna$)$

$|\langle a \rangle| = n$. Po Lagrangevem izreku $n \mid |G|$

2) Naj bo red $a = n$

Po 1) je $|G| = k \cdot n$

$$a^{|G|} = a^{kn} = (a^n)^k = 1$$

3) Naj bo $|G| = p$, $a \in G - \{1\}$ po 2)

$a^p = 1$

red a deli p, red $a \neq 1$ sledi $a = p \Rightarrow$

$$\langle a \rangle = \{\underbrace{1, \dots, a^{p-1}}_{p}\}$$

Sledi: $G = \langle a \rangle$

Uvod v teorijo kolobarjev, obsegov, polj in algeber

Def: Naj bo K neprazna množica z operacijama $+$, $\cdot$
Pravimo, da je K (oziroma $(K, +, \cdot)$) kolobar, če:

1) $(K, +)$ je abelova grupa
   (enota: 0 inverz a: $-a$)

2) $(K, \cdot)$ je monoid (kolobar ima vedno enoto za množenje: 1
   (enica kolobarja K)

3) $a(b+c) = ab + ac$ in $(a+b)c = ac + bc$
   za $\forall a, b, c \in K$

Če je $\cdot$ komutativna je K komutativen

Zgledi:

- $(\mathbb{Z}, +, \cdot)$ komutativen kolobar
- $(2\mathbb{Z}, +, \cdot)$ (ni enote za množenje)
  Komutativen klbr (rng)
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ so komutativni kolobarji
- $\mathbb{R}^{n \times n}$ je kolobar
- $X \subseteq \mathbb{R}$

  $\mathbb{R}^X = \{f : X \to \mathbb{R}\}$

  seštevanje in množenje po točkah

  $\mathbb{R}^X$ je komutativen kolobar

Homomorfizem:

Homomorfizem grup: $f(a)+f(b)=f(a+b)$

Homomorfizem kolobarjev:

$f(a)+f(b)=f(a+b)$

$f(a)\cdot f(b)=f(a\cdot b)$

$f(1)=1$

zakaj moramo to definirati

$f: \mathbb{R} \longrightarrow \mathbb{R}^{2\times 2}$

$f(x)=\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ $\quad f(x+y)=f(x)+f(y)$

$f(x\cdot y)=f(x)\cdot f(y)$

$f(1)$ ni enota v tem kolobarju

Homomorfizem algeber $f: A \longrightarrow B$

- f je homomorfizem kolobarjev in
- linearna preslikava

Opomba: če je $f: A \to B$ izomorfizem

potem je f^{-1} izomorfizem

potem $A \cong B$

a je fiksen

$f(g) = aga^{-1}$ (konjugiranje)

f je avtomorfizem grup

notranji avtomorfizem

$\mathrm{Inn}\, G = \{ f_a ; f_a(g) = aga^{-1} \}$

K komutativen kolobar

$ev_a : K[X] \to X$ evalvacija

$p \mapsto p(a)$

$N \leq G$ je **Podgrupa edinka**, če

$\forall a \in G.\ aNa^{-1} \subseteq N$

$aNa^{-1} = \{ana^{-1};\ n \in N\}$

(Boljše ime bi bila normalna podgrupa)

Oznaka: $N \triangleleft G$

Primeri:

$\{1\} \triangleleft G \qquad G \triangleleft G$

Grupe v katerih sta to edini edinki se imenujejo enostavne grupe

Če je G abelova je vsaka podgrupa edinka

(obstajajo tudi nekomutativne kjer to velja)

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

Vpeljemo množenje kvaternionov

Kvaternionska grupa. Vsaka grupa je edinka

Trditev: ekvivalentne

1. $N \trianglelefteq G$
2. $\forall a \in G \quad aN \subseteq Na$
3. $\forall a \in G \quad aN = Na$
4. $\forall a \in G \quad aNa^{-1} = N$

G grupa. Recimo $|G:H| = 2$

Trdimo $H \triangleleft G$

imamo dva leva odseka podgrupe H

$\forall a \in G \quad aH = Ha$

BŠZS $a \notin H$

$1 \cdot H = H$

$aH \neq H$

$G = H \cup aH$ disjunktna unija

$aH = G/H$

Desni odseki:

Lahko je videti, da imamo ~~samo~~ natanko dva desna odseke

H in Ha

$G = H \cup Ha$ disjunktna unija

$Ha = G/H$

Torej $Ha = aH$

Primer

S_n,

$A_n = \{$sode permutacije u $S_n\}$

$A_n \leq S_n \quad |S_n : A_n| = 2 \Rightarrow A_n \trianglelefteq S_n$

2) $D_{2n} = \{id, r, r^2, \ldots, r^{n-1}, z, rz, \ldots, r^{n-1}z\}$

$\langle r \rangle = \{id, r, \ldots, r^{n-1}\}$

$|D_{2n} : \langle r \rangle| = \frac{2n}{n} = 2$

$\langle r \rangle \trianglelefteq D_{2n}$

Trditev: Naj bo G grupa

(1) če je $H \leq G$ in $N \triangleleft G$

$$HN = NH \leq G$$

(2) če sta N, M podgrupi edinki v G

potem je $NM = MN \triangleleft G$

Dokaz:

1) $\forall h \in H$

$hN = Nh \Rightarrow HN = NH$ očitno

$HN = NH \Rightarrow$ je podgrupa (smo že dokazali!)

2) NM je podgrupa

$g \in G$

$gNMg^{-1} \in NM$

$gNg^{-1}gMg^{-1} \in N \cdot M$

Izrek:

Naj bo G grupa $N \triangleleft G$

Potem je na G/N s predpisom ← kvocientna/fakterska grupa

$(aN)(bN) = (ab)N$

dobro definirana operacija

s to operacijo postane množica G/N grupa

Preslikava $\pi : G \longrightarrow G/N$, dana s predpisom

$\pi(g) = gN$ epimorfizem grup

$\ker \pi = N$

Dokaz:

dobra definiranost

če $aN = a'N$ in $bN = b'N \Rightarrow (ab)N = (a'b')N$

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}\underbrace{a^{-1}a'}_{\in N \text{ ker } aN = a'N} b b^{-1} b'$$

$$\underbrace{\underbrace{b^{-1} a^{-1} a' b}_{\in N} \underbrace{b^{-1} b'}_{\in N \text{ ker } bN = b'N}}_{\in N}$$

G/N je grupa

asociativnost pihaja iz G

enota: $1 \cdot N = N$

inverz aN: $(aN)^{-1} = a^{-1}N$

π je homomorfizem

$\pi(gh) = (gh)N = gN \cdot hN = \pi(g) \cdot \pi(h)$

$g \in \ker \pi \Leftrightarrow \pi g = 1 \cdot N \Leftrightarrow gN = N \Leftrightarrow g \in N$

Izrek: (1. izrek o izomorfizmu)

Naj bo $\rho: G \to H$ homomorfizem grup.

Potem je $\ker\rho \trianglelefteq G$. Velja

$$G/\ker\rho \cong \mathrm{im}\,\rho$$

Dokaz: $\ker\rho$ je podgrupa v G

Vzemimo $g \in G$, $x \in \ker\rho$

$gxg^{-1} \in \ker\rho$

$$\rho(gxg^{-1}) = \rho(g)\underbrace{\rho(x)}_{=1}\rho(g^{-1}) = 1$$

Definiramo $\psi: G/\ker\rho \to \mathrm{im}\,\rho$

$$\psi(g\ker\rho) := \rho(g)$$

Dobro definiranost

$\underbrace{g\ker\rho = g'\ker\rho}$ želimo videti $\rho(g) = \rho(g')$

$\Downarrow$

$g^{-1}\cdot g' \in \ker\rho$

$\rho(g^{-1}\cdot g') = 1$

$\rho(g^{-1})\cdot\rho(g') = 1$

$\rho(g') = \rho(g)$

ψ je homomorfizem

$\psi((g\ker\rho)(g'\ker\rho)) =$

$= \psi(g\cdot g'\ker\rho) = \rho(g\cdot g') = \rho(g)\cdot\rho(g') =$

$= \psi(g\ker\rho)\psi(g'\ker\rho)$

ψ je očitno epimorfizem

ψ je monomorfizem

$g\ker\rho \in \ker\psi$

$\psi(g\ker\rho) = 1$

$\rho(g) = 1$

$g \in \ker\rho \Rightarrow 1\cdot\ker\rho$

$\ker\psi$ je trivialen ker

$\ker\psi = \{1\cdot\ker\rho\}$

$\blacksquare$

Opomba: Edinke so jedra
1. homomorfizmov

2. Naj bo $\rho: G \to H$ homomorfizem

Naj bo $N \lhd G$, recimo da $N \subseteq \ker\rho$

Potem je $\psi: G/N \longrightarrow H$ dana s predpisom $\psi(gN) := \psi(g)$ dobro definiran homomorfizem grup

Pravimo da je ψ induciran s ρ

shematično:

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\pi"] & H \\ G/N \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

kanonični epimorfizem

Ta diagram komutira

$$\psi \circ \pi(g) = \psi(\pi g) = \psi(gN) = \rho(g)$$

Izrek: (2. izrek o izomorfizmu)

Naj bo G grupa, $H \leq G$ $N \trianglelefteq G$

Potem je:

1) $N \cap H \trianglelefteq H$

2) $N \trianglelefteq HN$

3) $HN/N \cong H/N \cap H$

Ideja Dokaza:

1), 2) DN

3) Definiramo $f: H \to HN/N$

$f(h) := hN$

f je epimorfizem

$\ker f = H \cap N$

Uporabimo prvi izrek o izomorfizmu

$H/\ker f \cong \operatorname{im} f$

$H/N \cap H \cong HN/N$

Izrek (3. izrek o izomorfizmu)

Naj bo G grupa $N, M \lhd G$ $M \subseteq N$

1) $M \lhd N$

2) $N/M \lhd G/M$

3) $(G/M)/(N/M) \cong G/N$

Ideja dokaza

$\rho : G/M \to G/N$

$\rho(gM) = gN$

ρ je dobro definiran epimorfizem

$\ker \rho = N/M$

Uporabimo 1. izrek o izomorfizm

$$(G/M)/(N/M) = G/N$$

Lema: Naj bo $\varphi : G \to H$ homomorfizem grup

1) če je $K \leq G \Rightarrow \varphi_*(K) \leq H$

2) če je $K \trianglelefteq G$ in φ surjektiven $\Rightarrow \varphi_*(K) \trianglelefteq H$

3) $L \leq H \Rightarrow \varphi^*(L) \trianglelefteq G$

4) $L \trianglelefteq H \Rightarrow \varphi^*(L) \trianglelefteq G$

Dokaz:

zožitev φ na K

1) $\varphi(K) = \operatorname{im} \varphi|_K$ je podgrupa v H

2) $\varphi : G \twoheadrightarrow H$

$\underline{\varphi(K) \trianglelefteq H}$

$x \in \varphi(K) \quad h \in H$

$\underline{h x h^{-1} \in \varphi(K)}$

$x = \varphi(k) \; ; \; k \in K$

$h = \varphi(g) \quad g \in G$ surjektivnost

$h x h^{-1} = \varphi(\underbrace{g k g^{-1}}_{\in K}) \in \varphi(K)$

3) $x, y \in \varphi^*(L)$

$\exists a, b \in L.\; a = \varphi(x), b = \varphi(y)$

$\underbrace{a b^{-1}}_{\in L} = \varphi(\underbrace{x y^{-1}}_{\in \varphi^*(L)}) \in L$

4) $x \in \varphi^*(L) \quad \exists a \in L : a = \varphi(x)$

$g \in G$

$\underline{g x g^{-1} \in \varphi^*(L)}$

$\underbrace{\varphi(g) a \varphi(g^{-1})}_{\in L} = \varphi(\underbrace{g x g^{-1}}_{\in \varphi^*(L)})$

Izrek: (Korespondenčni izrek)

Naj bo G grupa in $N \triangleleft G$

a) Podgrupe v G/N so natanko oblike H/N kjer je $H \leq G$ $N \subseteq H$

b) Podgrupe edinke v G/N so natanko oblike K/N kjer je K $K \triangleleft G$ $N \subseteq K$

Dokaz a)

DN $H/N \leq G/N$

Obratna smer

Naj bo L poljubna podgrupa v G/N

$\pi : G \longrightarrow G/N$ kanonični epimorfizem
$(g \longmapsto gN)$

$H = \pi^*(L)$ je poljubni podgrupa v G

$N = \ker \pi \Rightarrow N \subseteq H$

$\pi_*(\pi^*(L)) = L$, ker je π surjektiven

Uporaba:

① G poljubna grupa, $a \in G$

$\langle a \rangle$

Trditev: $\langle a \rangle \cong \begin{cases} \mathbb{Z} & ; \text{reda} = \infty \\ \mathbb{Z}_n & \text{reda} = n \end{cases}$

Dokaz:

Recimo da reda $= \infty$

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow A \\ n &\longmapsto a^n \end{aligned}$$

φ je homomorfizem

je sur, je inj

$\ker \varphi = \{0\}$

Recimo da reda $= n$

$$\begin{aligned} \varphi : \mathbb{Z}_n &\longrightarrow \langle a \rangle \\ n &\longmapsto a^n \end{aligned}$$

je epi: $\operatorname{im} \varphi = \langle a \rangle$

$m \in \ker \varphi \Leftrightarrow a^m = 1 \Leftrightarrow m | n$

$\ker \varphi = m\mathbb{Z}$

1 izrek o izomorfizmu $\mathbb{Z}/\ker \varphi \cong \operatorname{im} \varphi$

$\mathbb{Z}/m\mathbb{Z} \cong \langle a \rangle$

② Podgrupe v $\mathbb{Z}_n$

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

Po korespondenčnem izreku je $\forall$ podgrupa v $\mathbb{Z}_n$ oblike $H/n\mathbb{Z}$, kjer je $H \leq \mathbb{Z}$, $n\mathbb{Z} \subseteq H$

$H = k\mathbb{Z}$ $\quad k | n \quad n = k \cdot d$

Podgrupe v $\mathbb{Z}_n$: $\underline{k\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_d}$

Ideja dokaza: $\varphi : k\mathbb{Z} \xrightarrow{DN} \mathbb{Z}_d$ φ je epimorfizem in $\ker\varphi = n\mathbb{Z}$

(3)

Trditev: Naj bo G grupa netrivialna

G nima pravih netrivialnih podgrup

$\Leftrightarrow$ $\exists p$ praštevilo, da je $G \cong \mathbb{Z}_p$

Dokaz:

($\Leftarrow$) $H \subseteq \mathbb{Z}_p$ Lagrangeov izrek: $|H| \mid |\mathbb{Z}_p|$

$|H| \mid p \Rightarrow |H| = 1$ ali $|H| = p$

$\Rightarrow H = \{0 + p\mathbb{Z}\}$ ali $H = \mathbb{Z}_p$

($\Rightarrow$)

$a \in G$ $a \neq 1$

$\langle a \rangle$ je netrivialna grupa

Po predpostavki je $\langle a \rangle$ cela grupa.

G je ciklična

Dve možnosti: $G \cong \mathbb{Z}$ (ni da, ker ima $\mathbb{Z}$ veliko podgrup) ali $G \cong \mathbb{Z}_n$

Po prejšnji trditvi (2) sledi če je n sestavljeno število, potem ima G prave netrivialne podgrupe

Torej je n praštevilo

4. Izrek: (Cauchyjev izrek za abelove grupe)

Naj bo G končna abelova grupa. Naj bo p praštevilo da $p \mid |G|$. $\Rightarrow$

Potem v G $\exists a \in G$. $\text{red } a = p$

Lema: Naj bo G grupa, $N \triangleleft G$, $a \in G$ $\text{red } a = n$

Potem red $aN \in G/N$ deli n

Dokaz leme: $\pi : G \to G/N$

$$\pi(a^n) = \pi(a)^n = (aN)^n$$

$$\overset{\shortparallel}{1} \qquad \overset{\shortparallel}{1}$$

Torej $\text{red } aN \mid n$ ∎

Dokaz: z indukcijo po moči $n = |G|$

baza indukcije:

$|G| = p \Rightarrow G \cong \mathbb{Z}_p$ $\quad 1 + p\mathbb{Z}$ ima red p

Recimo da $|G| > p$

po 3 ima G pravo netrivialno podgrupo recimo N (ker je G abelova so vse podgrupe edinke)

$|G| = |N| \cdot |G/N|$ lagrange

$p \mid |N|$ ali $p \mid |G/N|$

1. možnost $p \mid |N|$

po indukcijski predpostavki

N vsebuje element reda p $\Rightarrow$

G vsebuje element reda p

2. možnost $p \mid |G/N|$

je tudi abelova in $|G/N| < |G|$

po indukcijski predpostavki

G/N vsebuje aN reda p

$\text{red } aN \mid \text{red } a$

$$\text{red } a = p \cdot k$$

$$a^{pk} = 1$$

$$(a^k)^p = 1$$

Torej $\exists$ element da $\text{red} = p$ ∎

⑤ $\varphi : S_n \longrightarrow (\{-1, 1\}, \cdot)$

$\varphi(\pi) = \operatorname{sgn}(\pi)$

φ je homomorfizem

$\ker\varphi = \{\pi \in S_n \,;\, \operatorname{sgn}\pi = 1\} = A_n \qquad A_n \triangleleft S_n$

1. izrek o izomorfizmu $\quad S_n/A_n = \mathbb{Z}_2$

⑥ F naj bo polje

$\varphi : Gl_n(F) \longrightarrow F^*$

$\varphi(A) = \det A$ je homomorfizem

$\ker\varphi = \{A \in Gl_n(F) : \det A = 1\} = Sl_n(F)$

Torej $Sl_n(F) \triangleleft Gl_n(F)$

1. izrek o izomorfizmu $\quad Gl_n(F)/Sl_n(F) \cong F^*$

(7.) G_1, G_2 grupi

$G_1 \times G_2$ je tudi grupa

$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$

$\tilde{G}_1 = \{(g_1, 1) : g_1 \in G_1\}$ je podgrupa v $G_1 \times G_2$

$\tilde{G}_1 \triangleleft G_1 \times G_2$

$(h_1, h_2)(g_1, 1)(h_1, h_2)^{-1} =$

$= (h_1 g_1, h_2)(h_1, h_2)^{-1} =$

$= (h_1 g_1 h_1^{-1}, 1) \in \tilde{G}_1$

$\tilde{G}_1 \cong G_1$

$(g_1, 1) \longmapsto g_1$

$G_1 \times G_2 / \tilde{G}_1 \cong G_2$

$\rho : G_1 \times G_2 \longrightarrow G_2$

$\rho : (g_1, g_2) \longmapsto g_2$ je epimorfizem

$\ker \rho = \tilde{G}_1$

(8) $\mathrm{Inn}\, G = \{ \varphi_a : G \to G \; ; \varphi_a(g) = aga^{-1} \}$

konjugiranje z elementom a
(Notranji avtomorfizmi)

Opazimo: $(\varphi_a)^{-1} = \varphi_{a^{-1}}$

$\varphi_a \circ \varphi_b = \varphi_{ab}$

Z drugimi besedami: imamo homomorfizem

$\Phi : G \to \mathrm{Inn}\, G$ $\quad$ Φ je surjektiven

$\Phi(a) = \varphi_a$

Ker je Φ surjektiven je po 1. izreku o izomorfizmu $\mathrm{Inn}\, G \cong G/\ker\Phi$

$\ker \Phi = \{ a \in G : \varphi_a = id_a \}$

$\varphi_a = id_a \Leftrightarrow \varphi_a(g) = g \quad \forall g \in G$

$\Leftrightarrow aga^{-1} = g \quad \forall g \in G$

$\Leftrightarrow ag = ga \quad \forall g \in G$

$\Leftrightarrow a \in Z(G)$

center (elementi, ki komutirajo z vsemi)

Torej $G/Z(G) \cong \mathrm{Inn}\, G$

Opomba
$\mathrm{Inn}\, G$ je podgrupa v avtomorfizmih

DN: $\mathrm{Inn}\, G \triangleleft \mathrm{Aut}\, G$

$\mathrm{Out}\, G = \dfrac{\mathrm{Aut}\, G}{\mathrm{Inn}\, G}$ ... grupa zunanjih avtomorfizmov

(niso dejanski avtomorfizmi)

Kvocientni kolobarji in algebre

K naj bo kolobar

Pozabimo na množenje

K za seštevanje je abelova grupa

Če je $I \leq K$ za seštevanje, lahko naredimo abelovo grupo K/I : $(a+I)$

operacija: $(a+I)+(b+I) = (a+b)+I$

na K/I bi radi vpeljali množenje

$(a+I)\cdot(b+I) = (ab+I)$

ali to deluje?

Definicija: Naj bo K kolobar in $I \subseteq K$ $I \neq \emptyset$. Pravimo da je I <u>ideal</u> če velja

a) $(I,+)$ je podgrupa v $(K,+)$
$\forall a,b \in I \quad a-b \in I$

b) $\forall a \in I . \forall x \in K . \; xa \in I$

c) $\forall a \in I . \forall x \in K . \; ax \in I$

Opomba:

1. Pogoj b) lahko pišemo v obliki: $KI \subseteq I$
Prav tako pogoj c) $IK \subseteq I$

2. Če I zadošča pogojema a) in b) pravimo da je I levi ideal
če iz dadeša a) in c) je desni ideal
V času idealnom rečemo obojestranski ideal

Zgledi:

(1) Vsak kolobar ima vsaj dva ideala $\{0\}$, K sta vedno ideala

Kolobarjem ki imajo le ta dva ideala pravimo enostavni kolobarji

K kolobar

I je <u>ideal</u> v K, če

I_1: $\forall a,b \in I \,.\, a-b \in I$ (je podgrupa za +)

I_2: $\forall a \in I\ \forall x \in K\ ax, xa \in I$

Zgledi:

$aK = \{ax;\ x \in K$ je desni ideal v K

če je K komutativen, je $aK = Ka$ obojestranski ideal v K.

Pravimo mu <u>glavni ideal</u> v K generiran z a (vsak ideal v K ki vsebuje a, vsebuje aK)

K nekomutativen: Najmanjši Ideal, ki vsebuje a

$KaK = \{$vse končne vrste $\sum x_i a y_i$ $x_i, y_i \in K$

Ideal v $\mathbb{Z}$:

podgrupe: $n\mathbb{Z}$ vse avtomatično ideal.

$\mathbb{R}^{2\times 2}$

$\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a,b \in \mathbb{R}\right\}$ je desni ideal, ni levi

$\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; a,b \in \mathbb{R}\right\}$ je levi in ne desni ideal

DN: $\mathbb{R}^{n\times n}$ je enostaven kolobar

Opomba: Naj bo A algebra nad poljem $\mathbb{F}$

Ideal: I_2, namesto I_1 podprostor v A-ju

Trdimo $I_1 + I_2 \Rightarrow$ podprostor v A

$\alpha \in \mathbb{F}$ $\quad a \in I$

$$\alpha a = \alpha(1\cdot a) = \underset{\in A}{(\alpha \cdot 1)} \cdot \underset{\in I}{a} \in I$$

Namesto podprostor lahko rečemo abelova podgrupa

Trditev: Naj bo K kolobar in I ideal. Potem je K/I z operacijama

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)\cdot(b+I)=(a\cdot b)+I$$

je kolobar. Pravimo mu kvocientni (faktorski) kolobar.

Dokaz:

+ je dobro definirano (vemo iz grup)

$\cdot$ je dobro definirano

Recimo da $a+I=a'+I$ in $b+I=b'+I$

Dokazujemo $(ab)+I=(a'b')+I$

$$a-a'\in I \quad b-b'\in I$$

$$ab-a'b'=ab-a'b+a'b-a'b'=$$

$$=\underbrace{\underbrace{(a-a')}_{\in I}b}_{\in I}+\underbrace{a'\underbrace{(b-b')}_{\in I}}_{\in I}$$

$$\in I$$

Lastnosti kolobarja izhajajo iz tega da je K kolobar.

Ničla v K/I: $0+I$

enica v K/I: $1+I$

Trditev: Naj bo I ideal v K
Če I vsebuje nek obrnljiv element kolobarja K, potem $I = K$

Dokaz:

Recimo da je $u \in I$ obrnljiv. $x \in K$ poljuben

$$x = \underbrace{x u^{-1}}_{\in K} \cdot \underbrace{u}_{\in I} \in I$$

Torej $K = I$

Opomba: V prejsnji trditvi je dovolj da je I levi (ali desni) ideal

Trditev: Naj bosta I, J ideala v K

a) $I \cap J$ je tudi ideal v K

b) $I \cdot J = \{$vse končne vsote $\sum x_i y_i \quad x_i \in I \; y_j \in J\}$ je tudi ideal

c) $I + J$ je ideal

Dokaz:

a) DN

b) • IJ je očitno podgrupa za seštevanje

• $\sum x_i y_i \quad x_i \in I \quad y_i \in J$

$x \in K \qquad x \sum x_i y_i = \sum \underbrace{(x x_i)}_{\in I} \underbrace{y_i}_{\in J} \in I \cdot J$

Izrek: (1. izrek o izomorfizmu)

Naj bo $\varphi: K \to L$ homomorfizem kolobarjev. Potem je $\ker\varphi$ ideal v K in velja $K/\ker\varphi \cong \operatorname{im}\varphi$

Dokaz:

$\ker\varphi \triangleleft K$

$(\ker\varphi, +)$ je podgrupa v $(K, +)$

$a \in \ker\varphi \quad x \in K$

$\varphi(ax) = \varphi(a)\varphi(x) = 0 \cdot \varphi(x) = 0 \Rightarrow ax \in \ker\varphi$

Podobno xa

$\psi: K/\ker\varphi \to \operatorname{im}\varphi$

$\psi(x + \ker\varphi) := \varphi(x)$

je dobro definiran izomorfizem kolobarjev

$\blacksquare$

Izrek: (2. izrek o izomorfizmu)

Naj bosta I in J ideala v K. Potem je

$$(I+J)/J \cong I/I\cap J$$

Izrek: (3 izrek o izomorfizmu)

Naj bodo I, J, L ideali v K, $I \subseteq J \subseteq L$

$$(L/J)/(I/J) \cong L/I$$

Izrek: (Korespondenčni izrek)

a) Podkolobarji v K/I so natanko oblike L/I, kjer je L podkolobar v K, ki vsebuje I

b) Ideali v K/I so natanko oblike J/I, kjer je J ideal v K, ki vsebuje I

Definicija: Naj bo M ideal v kolobarju K. Pravimo da je M maksimalen ideal v K, če med M in K ni nobenega drugega ideala $\neq K$

$$I \triangleleft K, \; M \subseteq I \subseteq K \Rightarrow I = M \lor I = K$$

Izrek: Naj bo K komutativen kolobar, $M \triangleleft K$. Potem je M maksimalen ideal $\Leftrightarrow K/M$ je polje

Opomba: Komutativnost je nujna: $\mathbb{R}^{2\times 2}$ (ničelni ideal je maksimalen kolobar)

Dokaz:

($\Rightarrow$) Izberemo poljuben $a+M \in K/M$ neničeln $a+M \neq 0+M$

$M + \underbrace{aK}_{\text{ideal, ker je } K \text{ komutativen}}$ je ideal (vsota dveh idealov je ideal DN)

$M \subsetneq M+aK \subseteq K$

Zaradi maksimalnosti je $M+aK = K$

Med drugim $\exists k \in K . \exists m \in M . \; 1 = m + ak$

$1 - ak \in M$

$1+M = ak+M = (a+M)(k+M)$

Torej je $(a+M)$ obrnljiv v K/M

($\Leftarrow$)

Naj bo $I \triangleleft K \quad M \subsetneq I \subseteq K$

$\exists a \in I \setminus M$, ki ni v M

$a+M \neq 0+M$

Po predpostavki je K/M polje, torej $\exists x \in K$ $(a+M)(x+M) = 1+M$

$$\underset{\in I}{ax} - 1 \in M \Rightarrow ax - 1 \in I$$

Sledi: $1 \in I \Rightarrow I = K$

$\blacksquare$

Izrek: Naj bo K poljubni kolobar. Potem je $\forall$ pravi ideal v K vsebovan v nekem maksimalnem idealu

Dokaz uporabi Zornovo lemo:

X naj bo delno urejena množica

Veriga v X: $Y \subseteq X$. $\forall a,b \in Y$. $a \leq b \vee b \leq a$

Zgornja meja neke podmnožice Y:

$m \in X$. $y \leq m$. $\forall y \in M$

Maksimalen element množice X: tak $m \in X$, da $\forall a \in X$. $m \not\leq a$

Zornova lema: Naj bo X delno urejena množica: Če ima $\forall$ veriga v X zgornjo mejo, potem X vsebuje maksimalen element

---

Dokaz: $I \triangleleft K$, $I \neq K$

$\mathcal{S}$ naj bodo vsi pravi ideali v K, ki vsebujejo I

$\mathcal{S} \neq \emptyset$, ker $I \in \mathcal{S}$

$\mathcal{S}$ lahko delno uredimo z inkluzijo

Vzemimo poljubno verigo $\mathcal{V}$ v $\mathcal{S}$

$\mathcal{U} = \bigcup_{J \in \mathcal{V}} J$ Trdimo $\mathcal{U} \in \mathcal{S}$

$\mathcal{U}$ je ideal v K

- $a,b \in \mathcal{U}$. $\exists J_1, J_2 \in \mathcal{V}$. $a \in J_1$, $b \in J_2$

  BŠZS. $J_1 \subseteq J_2$ (ker je $\mathcal{V}$ veriga)

  $a-b \in J_2 \subseteq \mathcal{U}$

- $a \in \mathcal{U}$, $x \in K$, $\exists J \in \mathcal{V}$. $a \in J$

  $ax, xa \in J \subseteq \mathcal{U}$

- $\mathcal{U} \neq K$

  če $\mathcal{U} = K \Rightarrow 1 \in \mathcal{U} \Rightarrow \exists J \in \mathcal{V}. 1 \in J. \Rightarrow J = K$

  $\divideontimes$

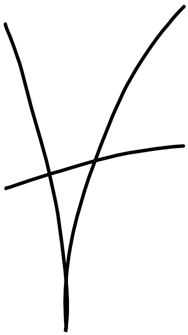
Po Zornovi lemi $\mathcal{S}$ vsebuje maksimalen element M

$M \triangleleft K$ $M \neq K$ $I \subseteq M$

M je maksimalen ideal v K

Recimo $\exists N \triangleleft K$. $M \subsetneq N \subsetneq K$. N je pravi ideal v K, ki vsebuje I, torej $N \in \mathcal{S}$ $\divideontimes$

Zapiski od Urške na discordu



Od zadnjič

$|G| = mn$ $\quad m, n$ sta si tuji:

$H = \{x \in G;\ mx = 0\}$

$K = \{x \in G;\ nx = 0\}$

$G = H + K$

$\exists a, b \in \mathbb{Z}.\ am + bn = 1$

$x = 1 \cdot x = (am + bn)x = amx + bnx$

~~damx~~ $m(bnx) = b\underbrace{mn}_{=|G|}x = 0$

$\Rightarrow bnx \in H$

$\Rightarrow amx \in G$ $\qquad G = H \oplus K$

$|H| = m \quad |K| = n$

$mn = |G| = |H| \cdot |K|$

Ker sta m in n tuji je dovolj premisliti

$\forall p \in \mathbb{P}.\ p \nmid m \Rightarrow p \nmid |H| \wedge p \nmid |K|$

Recimo da $p \nmid m$ in recimo da $p \mid |H|$

Po Cauchyjevem izreku grupa H vsebuje element y reda p

$y \neq 0 \quad py = 0;\ my = 0$

m in p sta tuja. $\exists c, d \in \mathbb{Z}.$

$cm + dp = 1$

$y = 1y = (cm + dp)y = \underbrace{cmy}_{0} + \underbrace{dpy}_{0} = 0$

$\times$

Primer: G abelova grupa moči $6 = 2 \cdot 3$

$G = H \oplus K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$

$|H| = 2 \quad |K| = 3 \Rightarrow H \cong \mathbb{Z}_2 \wedge K \cong \mathbb{Z}_3$

Edina abelova grupa moči 6

DN: m, n tuji $\Rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Opomba: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4$, ker ima

$\mathbb{Z}_4$ element reda 4 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ pa ne

Posledica: Naj bo G končna abelova

$$|G| = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

$$H_i := \{ x \in G \,;\, p_i^{e_i} x = 0$$

$$G = H_1 \oplus H_2 \oplus \ldots \oplus H_n$$

in $|H_i| = p_i^{e_i}$

Definicija: $|G| = p^n$; $p \in \mathbb{P}$ pravimo da je G <u>p-grupa</u>

Torej: $\forall$ končne abelova grupa je vsota p-grup (za različne praštevila)

Dovolj je torej obravnavati končne abelove p-grupe

Lema 1: Naj bo G netrivialna končna abelova p-grupa
Potem velja: G je ciklična $\Leftrightarrow$ G vsebuje natanko eno podgrupo moči p

Dokaz: $|G| = p^m$

$(\Longrightarrow)$ če je G ciklična in ima moč p^m

$\Rightarrow G \cong \mathbb{Z}_{p^m}$

Podgrupe: $p^k \cdot \mathbb{Z}_{p^m}$; $k \leq m$

Edina, ki ima moč p je $p^{m-1}\mathbb{Z}_{p^m}$

$(\Longleftarrow)$ indukcija po moči

$|G| = p$: očitno ima v tem primeru samo eno podgrupo

Recimo da to trditev velja za vse p-grupe moči $< p^m$

Naj bo N edina podgrupa v G, ki ima moč p

$\underline{N = \{x \in G; px = 0\}}$

$N \subseteq \{\dots\}$ saj ima N moč p

če ima $x \in G$ red p je $\langle x \rangle$ podgrupa moči p

zato je $N = \langle x \rangle$; torej $x \in N$

Oglejmo si

$\varphi: G \longrightarrow G$

$\varphi(x) = px$

φ je homomorfizem grup

$\ker \varphi = N$

$G/N \cong \operatorname{im} \varphi$ je podgrupa v G

G/N je p-grupa netrivialne

ker jo lahko gledamo kot podgrupo v G ima še vedno natanko eno podgrupo moči p

Po indukcijski predpostavki je G/N ciklična

$G/N = \langle a+N \rangle \quad a \notin N$

$\forall x \in G . \exists k \in \mathbb{Z} \quad x+n = k(a+N) = ka+N$

$x - ka \in N$

$\cancel{ka} \in N \quad x = ka+n \quad n \in N$

$G = \langle a \rangle + N$

$\langle a \rangle$ je netrivialna ciklična p-grupa

to ej $\langle a \rangle$ vsebuje element reda p;

$\langle b \rangle$ ima moč $p \Rightarrow \langle b \rangle = N$

$\langle b \rangle \leq \langle a \rangle \Rightarrow N \leq \langle a \rangle$

$\Rightarrow G = \langle a \rangle$ ■

Lema: Naj bo G končna abelova p-grupa. Naj bo C tista ciklična podgrupa v G, ki ima največjo možno moč.

Potem $\exists$ podgrupa $K \leq G$, da je

$G = C \oplus K$

Dokaz: Če je G ciklična $\Rightarrow$ $C = G$, $K = \{0\}$

Recimo da G ni ciklična. $|G| = p^m$ $m > n$

Indukcija po moči $|G|$

Po prejšnji lemi ima G vsaj dve podgrupi moči p

C ima po prejšnji lemi natanko eno podgrupo moči p

Zato $\exists$ podgrupa moči p v G ki ni vsebovana v C. označimo jo z N

Opazimo $C \cap N < N$ $|N| = p$

Torej $C \cap N = \{0\}$

2. izrek o izomorfizmu:

$HN/N \cong H/N \cap H$

$\frac{C+N}{N} \cong \frac{C}{C\cap N} \cong C$

$\frac{C+N}{N}$ je ciklična podgrupa v G/N

ima največjo moč med cikličnimi podgrupami grupe G/N in ima največjo moč med cikličnimi

$|G/N| < |G|$

Po indukcijski predpostavki $\exists K \leq G$

$N \subseteq K$ da je

$G/N = \frac{C+N}{N} \oplus \frac{K}{N}$ *

$G = C \oplus K$

iz * sledi

$x \in G$: $x + N \in G/N$

$x + N = (y+N) + (k+N) =$ $y \in C+N$

$= (y+k)+N =$ $k \in K$

$= y + k + n$ $n \in N$

$y + n \in C + N$

$G = C + \underset{K}{\underset{\cap}{N + K}} \Rightarrow$ ~~$C+K$~~ $G = C + K$

$C \cap K = \{0\}$

$x \in C \cap K$ $x \neq 0$

$x \notin N$ ker $C \cap N = \{0\}$

$x + N \in \frac{C+N}{N} \cap \frac{K}{N} = \{0 + N\}$, ker je to druga direktna vsota

$\Rightarrow$ ~~$\not$~~ $x \in N$ $\cancel{}$

Posledica: $\forall$ končna abelova p-grupa je direktna vsota cikličnih p-grup

Posledica: Vsaka končna abelova grupa je direktna vsota cikličnih grup katerih moči so potence praštevil

Kako vidimo ali: dva razcepa abelovih grup na direktni vsoti cikličnih p_i-grup predstavljata isto grupo do izomorfizma natančno

$G, \bar{G}$ končni abelovi grupi $\varphi: G \to \bar{G}$ izomorfizem

$|G| = |G| = p_1^{e_1} \dots p_k^{e_k}$

$G = H_1 \oplus \dots \oplus H_k \qquad |H_i| = p_i^{e_i}$

$\bar{G} = \bar{H}_1 \oplus \dots \oplus \bar{H}_k \qquad |\bar{H}_i| = p_i^{e_i}$

$H_1 = \{x \in G : p_1^{e_1} = 0\}$

$\bar{H}_1 = \{x \in G : p_1^{e_1} = 0\}$

$\varphi|_{H_1} : H_1 \longrightarrow \bar{H}_1$

$x \in H_1 \quad p_1^{e_1} \varphi(x) = \varphi(p_1^{e_1} x) = 0$

ker $|H_1| = |\bar{H}_1|$ sledi $H_1 \cong \bar{H}_1$

Problem izomorfnosti končnih abelovih grup se zato zreducira na to kdaj sta dve končni abelovi p-grupi izomorfni.

Izrek: Naj bosta G in $\tilde{G}$ končni abelovi p-grupi

$$G \cong \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_m}}$$

$$\tilde{G} \cong \mathbb{Z}_{p^{l_1}} \oplus \mathbb{Z}_{p^{l_2}} \oplus \ldots \oplus \mathbb{Z}_{p^{l_n}}$$

predpostavimo

$k_1 \geq \ldots \geq k_m$

$l_1 \geq \ldots \geq l_n$

Recimo da $G \cong \tilde{G} \Rightarrow k_i = l_i$ in $m = n$

Dokaz: $f: G \to \tilde{G}$ $|G| = |\tilde{G}|$

$$p^{k_1 + k_2 + \ldots k_m} = p^{l_1 + l_2 + \ldots l_n}$$

Torej $k_1 + k_2 + \ldots k_m = l_1 + l_2 + \ldots l_n$

Po indukciji na r

$G \cong \mathbb{Z}_p$ in $\tilde{G} = \mathbb{Z}_p$

Recimo da velja za vse grupe moči p^s ser

$pG = \{p \cdot g \cdot g \in G\}$

$\nwarrow$ ubistvu podenoa

$pG \leq G$ $pg_1 - pg_2 = p(g_1 - g_2)$

izpeskuljamo lahko ker je abelova

$f/_{pG}: pG \to p\tilde{G}$

$f(pg) = p(fg)$

$f/_{pG}$ je izomorfizem

$$G = \underbrace{\mathbb{Z}_{p^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_{m'}}}}_{k_j \geq 2} \oplus \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{m - m'}$$

$$G = \mathbb{Z}_{p^{l_1}} \oplus \ldots \mathbb{Z}_{p^{l_{n'}}} \oplus \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{n - n'}$$

$$pG = p\mathbb{Z}_{p^{k_1}} \oplus \ldots p\mathbb{Z}_{p^{k_{m'}}} \oplus \underbrace{p\mathbb{Z}_p \oplus \ldots \oplus p\mathbb{Z}_p}_{=0,\text{ ker } p \cdot n = 0 \vee \mathbb{Z}_p}$$

$$\cong \mathbb{Z}_{p^{k_1 - 1}} \oplus \ldots \mathbb{Z}_{p^{k_{m'} - 1}}$$

$$p\tilde{G} = \mathbb{Z}_{p^{l_1 - 1}} \oplus \ldots \mathbb{Z}_{p^{l_{n'} - 1}}$$

pG sta izomorfni in imata manjšo moč kot G

Po indukcijski predpostavki dobimo

$m' = n'$

$k_i - 1 = l_i - 1$

$k_i = l_i$

Torej

$$G = \mathbb{Z}_{p^{k_1}} \oplus \ldots \mathbb{Z}_{p^{k_{m'}}} \oplus \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{m - m'}$$

$$\tilde{G} = \mathbb{Z}_{p^{k_1}} \oplus \ldots \mathbb{Z}_{p^{k_{m'}}} \oplus \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{n - m'}$$

$|G| = p^{k_1 + k_2 + \ldots k_{m'} + m - m'}$

$|\tilde{G}| = p^{k_1 + \ldots k_{m'} + n - m'}$

$\Rightarrow n = m$

Torej je izrek dokazan

Torej vsaka ~~abelova~~ končna abelova grupa

Povzetek: Vsaka končna abelova grupa je izomorfna direktni vsoti cikličnih podgrup, ki so p-grupe za nekatera različna praštevila

$$G = \bigoplus_i \mathbb{Z}_{p_1^{k_i}} \bigoplus_j \mathbb{Z}_{p_1^{l_j}} \; \ldots\ldots$$

Zapis je enoličen do vrstnega reda direktnih sumandov natanko

Vis abelske grupper med 4032

$4032 = 2^4 \cdot 3^3$

2^4: $\mathbb{Z}_{2^4}$, $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_2$, $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2}$, $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

5

3^3: $\mathbb{Z}_{3^3}$, $\mathbb{Z}_{3^2} \oplus \mathbb{Z}_3$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

3

Giv i 15

Na podoben način kot končno gen.

končne generirane
končno generirane ciklične
abelove grupe

Izrek:
Naj bo G končno generirana abelova grupa. Potem je $G \cong \mathbb{Z}^n \oplus K$, pri čemer je K končna abelova grupa

Če je $G \cong \mathbb{Z}^n \oplus K \cong \mathbb{Z}^m \oplus L$

$\Rightarrow m = n \ \wedge K \cong L$

$(\mathbb{Z}^n = \overbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}^{n})$

Ideja dokaza:

G abelova grupa ⇍ končen red

$T(G) = \{g \in G;\ |g| < \infty\}$

$T(G)$ je podgrupa v G

$mg = 0 \qquad g, h \in T(G)$

$nh = 0$

$m \cdot n(g-h) = mng - mnh = 0 - 0 = 0$

$T(G)$.... torzijska podgrupa v G

za G pravimo da je brez torzije, če je $T(G) = \{0\}$

$G/T(G)$ je končno generirana abelova grupa brez torzije

$G = \langle x_1, \ldots x_n \rangle \Rightarrow G/T(G) = \langle x_1 + T(G), \ldots, x_n + T(G) \rangle$

Recimo da $g + T(G)$ ima končen red $\Rightarrow g \in T(G)$

$(\forall g \in G/T(G).\ g + T(G) = 0 + T(g))$

$\Downarrow$

$\exists n,\ n(g + T(G)) = 0 + T(G)$

$ng + T(G) = 0 + T(G)$

Sledi: $ng \in T(G) \Rightarrow$

$\exists m.\ m(ng) = 0$

$(mn) \cdot g = 0 \Rightarrow g$ ima končen red torej $g \in T(G)$

Izkaže se: če je G končno generirana abelova grupa brez torzije, potem je $G \cong \mathbb{Z}^n$ za nek n

Brez dokaza

Trditev: $\forall$ končno generirana abelova grupa je direktna vsota neke končnogenerirane abelove grupe brez torzije in neke končne abelove grupe

Dokaz: G naj bo končno generirana abelova $G/T(G)$ je k.g abelova brez torzije

$G/T(G) \cong \mathbb{Z}^n$

$e_i = (0, \ldots 0, \overset{i}{1}, 0, \ldots 0) \in \mathbb{Z}^n$

Vsak element $\mathbb{Z}^n$ lahko na enoličen ~~način~~ način zapišemo kot $\alpha_1 e_1 + \ldots + \alpha_n e_n$ $\mathbb{Z}^n$ ima bazo zato ima tudi $G/T(G)$ bazo

$f_1 + T(G), f_2 + T(G), \ldots, f_n + T(G)$

$f_i \in G \quad f_i \notin T(G)$

Naredimo $H = \langle f_1, f_2, \ldots, f_n \rangle$

Dokažemo lahko da so $f_1 \ldots f_n$ baza za H

$H \longrightarrow \mathbb{Z}_n$

$f_i \longrightarrow e_i$ je izomorfizem grup

trdim da je $G = H \oplus T(G)$

Ker je $H \cong \mathbb{Z}_n$ nima elementov končnega reda. Zato je $H \cap T(G) = \{0\}$

$G = H + T(G)$

$g \in G \Rightarrow g + T(G) \in G/T(G)$

$g + T(G) = \alpha_1 (f_1 + T(G)) + \ldots + \alpha_n (f_n + T(G)) \quad \alpha_i \in \mathbb{Z}$

$g + T(G) = \alpha_1 f_1 + \ldots + \alpha_n f_n + T(G)$

Torej $g = \underbrace{\alpha_1 f_1 + \ldots + \alpha_n f_n}_{\in H} + \underset{\in T(G)}{t} \,;\, t \in T(G)$

~~Dokazali~~ ~~smo~~

Dokazati moramo še, da je

$T(G)$ končna grupa.

$$G = H \oplus T(G)$$

$$T(G) \cong G/H$$ abelova ✓

G/H je kvocient končnogenerirane grupe je končno generirana

$T(G)$ je končnogenerirana grupa v kateri ima $\forall$ element končen red

$T(G) = \langle t_1, \dots, t_k \rangle \qquad m_i t_i = 0$

$t \in T(G)$

$t = \alpha_1 t_1 + \dots + \alpha_k t_k$ (ni baza, ampak vseeno lahko tako zapišemo (neenolično) ker je abelova

$0 \leq \alpha_i < m_i$

Za vse α_i imamo končnomnogo možnosti, zato imamo končno mnogo možnosti za t

$\Rightarrow T(G)$ končna

KONČNE GRUPE

delovanja grup

Definicija: Naj bo G grupa in X neprazna množica. Grupa G <u>DELUJE</u> na množici X <u>($G \curvearrowright X$)</u>, če $\exists$ preslikava (<u>DELOVANJE</u>)

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto g \cdot x \quad (\text{samo oznaka})$$

za katero veljata:

1) $g(h \cdot x) = (gh) \cdot x \quad \forall g, h \in G$

2) $1 \cdot x = x \qquad 1 \in G$

Opomba: Definirali smo levo delovanje grupe G na X. Podobno lahko definiramo desno delovanje

$$X \times G \longrightarrow X$$
$$(x, g) \longmapsto x \cdot g$$

1') $(x \cdot h) \cdot g = x (h \cdot g)$

2') $x \cdot 1 = x$

Recimo da imamo levo delovanje $G \curvearrowright X \quad (g,x) \mapsto g \cdot x$

Potem lahko definiramo desno delovanje

$$X \times G \longrightarrow X$$

$$(x,g) \longmapsto g^{-1}x \quad = x*$$

Zakaj: 1) velja

$$(x * h) * g = g^{-1}(x * h) = g^{-1}(h^{-1} * x) =$$

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

$$x * (h \cdot g)$$

Opomba: Naj G deluje na X

$\mathrm{Sym}\, X = \{X \rightarrowtail\!\!\!\twoheadrightarrow X\}$

Delovanje porodi homomorfizem grup

$$\Phi : G \longrightarrow \mathrm{Sym}\, X$$

$$\Phi(g)(x) = g \cdot x \qquad g \mapsto (x \mapsto g \cdot x)$$

Φ je homomorfizem

$$\Phi(g \cdot h)(x) = (g \cdot h)x = g(h \cdot x) =$$

$$g \cdot \Phi(h)(x) = \Phi(g)(\Phi(h)(x)) =$$

$$\Phi(g)\Phi(h)(x)$$

Obratno: Če imamo homomorfizem

$\Phi : G \longrightarrow \mathrm{Sym}\, X$ potem $G \curvearrowright X$

s predpisom $g \cdot x = \Phi(g)(x)$

Opomba: Zakaj je $\rho: X \longrightarrow X$, $\rho(x) = g \cdot x$ bijekcija?

surj:

$$\rho(g^{-1}x) = g \cdot g^{-1}x = x$$

inj:

$$\rho(x) = \rho(y)$$
$$gx = gy$$

$$x = 1 \cdot x = g^{-1} \cdot g x = g^{-1}(gx) = g^{-1}(gy) = y$$

Recimo da imamo delovanje G na X

$$\Phi : G \longrightarrow \mathrm{Sym}\, X$$

$\ker\Phi$ imenujemo jedro delovanja

Pravimo, da je delovanje zvesto če je jedro trivialno ($\ker\Phi = \{1\}$)

Če je delovanje zvesto:

$$\begin{array}{c} G/\ker\Phi \cong \mathrm{im}\,\Phi \\ \cong \\ G \end{array}$$

G je izomorfna neki podgrupi $\mathrm{Sym}\, X$

Pravimo da se G vloži v $\mathrm{Sym}\, X$

Primeri delovanj

1) Trivialno delovanje

$$g\cdot x = x \quad \text{za } \forall g\in G.\ \forall x\in X$$

2) Grupa G deluje na G z levim množenjem

$$G\times G \longrightarrow G$$
$$(g,h) \longmapsto g\cdot h$$

imamo homomorfizem

$$\Phi : G \longrightarrow \mathrm{Sym}\, G$$
$$\Phi(g)(h) = g\cdot h$$

$$g\in\ker\Phi \Leftrightarrow \Phi_g = id_G \Leftrightarrow \forall h\in G.\ g\cdot h = h$$

$$\Leftrightarrow g = 1$$

levo regularno delovanje

Cayleyjev izrek:

Množenje z leve je torej zvesto delovanje

$\Rightarrow$ $\forall$ grupa G se vloži v $\mathrm{Sym}\, G$

V posebnem: G končna. $|G| = n$

G se vloži v $\mathrm{Sym}\, G \cong \mathrm{Sym}\{1,\dots,n\} = S_n$

3) G deluje na G

$$G \times G \longrightarrow G$$
$$(g, h) \longmapsto g h g^{-1}$$

DN: To je delovanje

$$g(h \cdot x) = g(h x h^{-1}) = g h x h^{-1} g^{-1}$$
$$(gh)x = g h x (gh)^{-1} = g h x h^{-1} g$$

4) $H \leq G$; G/H množica levih odsekov H v G

G deluje na G/H

$$G \times G/H \longrightarrow G/H$$
$$g \cdot (xH) = (gx)H$$

Dobra definiranost ?

Recimo $xH = yH \Rightarrow gxH = gyH$

$\downarrow$

$x^{-1}y \in H$

Oglejmo si $(gx)^{-1} g y = x^{-1} g^{-1} g y = x^{-1} y \in H$

DN: To je delovanje

5) Recimo da G deluje na X

Y naj bo neprazna množica

$$Y^X = \{f : X \to Y\}$$

G deluje na Y^X

$$G \times Y^X \to Y^X$$

$$(g, f) \longmapsto g \cdot f = (x \longmapsto f(g^{-1}x))$$

(izkaže se da je potrebno g^{-1} da deluje

To ni res delovanje

$$\cancel{(1,f)} \quad 1 \cdot f(x) = f(1^{-1}x) = f(x) \quad \checkmark$$

$$(g(hf))(x) = hf(g^{-1}x) =$$

$$f(h^{-1}g^{-1}x) = f((g \cdot h)^{-1}x) = (g \cdot h) \cdot f(x) + 1$$

DN: $G \curvearrowright X$ $\quad G \curvearrowright Y$

$(g, x) \longrightarrow gx \qquad (g, y) \longmapsto gy$

Potem $G \curvearrowright Y^X$

$$(g, f) = g \cdot f$$

$$g \cdot f(x) = g \cdot f(g^{-1}x)$$

6) V nejloa vektorski prostor

$GL(V)$ ....vsi automorfizmi prostora V

$$GL(V) \cdot V \longrightarrow V$$

$$(A, v) \longmapsto Av$$

To je delovanje

7) K komutativen kolobar z 1

$K[x_1, \dots, x_n]$

S_n deluje na $K[x_1 \dots x_n]$

$$\sigma \cdot p(x_1 \dots x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

To je delovanje

Orbite stabilizatorji, fiksne točke delovanj

Def: Naj grupa G deluje na množici X

1) Za $x \in X$ je <u>ORBITA</u> elementa x množica

$$G \cdot x = \{ g \cdot x \,;\, g \in G \}$$

2) Za $x \in X$ je <u>stabilizator</u> točke X množica $G_x = \{ g \in G ;\ gx = x$

3) Za $g \in G$ je <u>množica fiksnih točk</u> g-ja

$$X^g = \{ x \in X ;\ gx = x \} = \mathrm{fix}(g)$$

4) <u>fiksne točke</u> delovanja (<u>invariante</u>)

$$X^G = \bigcap_{g \in G} X^g = \{ x \in X ;\ \forall g \in G .\ gx = x \}$$

Lema: Naj G deluje na X

Recimo da $g \cdot x = y$

Potem je $x = g^{-1} \cdot y$

Dokaz:

$$x = 1 \cdot x = g^{-1}(g x) = g^{-1} y$$

Trditev: Naj G deluje na X

Potem je $G_x \leq G$

Dokaz:

$1 \in G_x$ torej $G_x \neq \emptyset$

$g, h \in G_x$ $\qquad gx = x = hx$

$$(gh^{-1})x = g \cdot (\underbrace{h^{-1}x}_{\text{lema}}) = g \cdot x = x$$

$\blacksquare$

Trditev: Naj G deluje na X. Na X vpeljemo relacijo $x, y \in X$: $x \sim y \Leftrightarrow \exists\, g \in G.\ y = gx$

Potem je $\sim$ ekvivalenčna relacija na X in ekvivalenčni razred elementa x je njegova orbita Gx

Dokaz

Refleksivnost $1x = 1$

simetričnost $gx = y \Rightarrow x = g^{-1}y$

tranzitivnost $gx = y \wedge hy = z \Rightarrow h \cdot gx = z$

Ekvivalenčni razredi za

$$[x] = \{y \in X : y \sim x\} = \{y \in X.\ \exists g \in G.\ y = gx\} =$$

$$= Gx$$

Oznake: Kvocientno množico po zg. relaciji označimo $X/G = X/\sim =$

$$= \{G \cdot x ; x \in X\}$$

X/G je prostor orbit

Delovanju, ki ima eno samo orbito pravimo <u>tranzitivno delovanje</u>

Zgled

1) Naj G deluje na G z levim množenjem

$x \in G$: $Gx = \{gx ; g \in G\} = G$

$h \in G \Rightarrow h = h \cdot x^{-1} \cdot x$

Tranzitivno delovanje

$G_x = \{g \in G . gx = x\} = \{1\}$

$\Downarrow$

$g = 1$

$G^g = \{x \in G ; gx = x\} = \begin{cases} \emptyset & ; g \neq 1 \\ G & ; g = 1 \end{cases}$

② G naj deluje na G s konjugiranjem

$$G \times G \longrightarrow$$
$$(g,h) \longmapsto g * h = ghg^{-1}$$

$x \in G$

$G_x = \{g \in G; g * x = x\} = \{g \in G; gxg^{-1} = x\}$

$= \{g \in G, gx = xg\} =: C_G(x)$

... centralizator elementa x v G

orbita x-a $G * x = \{g * x; g \in G\} =$

$= \underbrace{\{gxg^{-1} : g \in G\}}_{} = Cl_G(x)$

konjugirani razred elementa x v G

$g \in G$

$G^g = \{x \in G . g * x = x\} = \{x \in G, gx = xg\} = C_G(g)$

$G^G = \bigcap_{g \in G} G^g = \bigcap_{g \in G} C_G(g) = Z(G)$

3) $H \leq G$: G deluje na G/H

Orbita xH

$G(xH) = \{ g \cdot xH ; g \in G \} = G$

tranzitivne delovanje

Fiksne točke (invariante) delovanja

$K[x_1 \dots, x_n]^{S_n}$ = tisti polinomi, ki jih

$\{ p : \forall \sigma \in S_n ,\ \sigma \cdot p(x_1 \dots x_n) = p(x_1 \dots x_n) \} =$

$\{ p(x_1 \dots x_n) : \forall \sigma \in S_n\ p(x_{\sigma(1)} \dots x_{\sigma(n)}) \} =$

simetrični polinomi

$x_1 + x_2 + x_3$

$x_1 x_2 + x_2 x_3 + x_1 x_3$

Izrek o orbiti in stabilizatorju

Naj grupa G deluje na množici X

a) $\forall x \in X.\ |\underbrace{G\cdot x}_{\text{orbita}}| = |\underbrace{G : G_x}_{\text{indeks stabilizatorja}}|$ (deluje tudi za neskončne grupe)

b) G končna grupa $\Rightarrow |G| = |Gx| \cdot |G_x|$

Dokaz:

a) Iščemo bijekcijo med množicama Gx in G/G_x

$\alpha : Gx \longrightarrow G/G_x$

$\alpha : g\cdot x \longmapsto g\cdot G_x$

Ali je α dobro definirana

$\underline{gx = hx \Rightarrow g\cdot G_x = h\,G_x}$

$gx = hx$

$h^{-1}g\,x = x$

$h^{-1}g$ stabilizira $x \Rightarrow h^{-1}g \in G_x$

$\Rightarrow h\,G_x = g\,G_x$

α očitno surjektivna

$\underline{\alpha \text{ injektivna}}$

$gG_x = hG_x \Rightarrow h^{-1}g \in G_x \Rightarrow$

$h^{-1}g\,x = x$

$gx = hx$ ✓

■

b) direktna posledica

Izrek

Naj grupa G deluje na X, X končna množica. Potem obstajajo elementi $x_1, \dots, x_r \in X - X^G$ ← tisti x_i ki jih vsi g-ji postijo pri miru

$$|X| = |X^G| + \sum |G : G_{x_i}|$$

Dokaz: Množica X je disjunktna unija nekih orbit delovanja.

$x \in X^G \Rightarrow |Gx| = 1$

vsaka fiksna točka ima enoelementno orbito

Ostali elementi imajo orbite večje od ~~enega~~ ena

recimo da jih je r (ker je G končna)

Torej $|X| = |X^G| + |Gx_1| + \dots |Gx_r|$

orbite z 1 elementom

vse ostale orbite

x_i-ji so predstavniki različnih orbit velikosti več kot 1

$$|X| = |X^G| + |G : Gx_1| + \dots |G : G_{x_r}| =$$

$$= |X^G| + \sum_{i=1}^{r} |G : G_{x_i}|$$

Posledica:

Naj bo G končna p-grupa, ki deluje na končni množici X.

Potem velja

$$|X| \equiv |X^G| \bmod p$$

Dokaz:

Po prejšnjem izreku lahko napišemo

$$|X| = |X^G| + \sum_{i=1}^{r} |G : G_{x_i}| \quad x_i \text{ niso fiksne točke}$$

Ker x_i niso fiksne točke, $G_{x_i} \neq G$

G_{x_i} je prava podgrupa $|G : G_{x_i}| = \frac{|G|}{|G_{x_i}|}$

je deljiv s p

sledi: $p \mid (|X| - |X^G|)$

$\blacksquare$

Izrek (Burnsidova lema)

Naj končna grupa G deluje na končno množico

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

Dokaz: Izračunamo moč množice $\{(g,x)\in G\times X;\ gx=x\}$ na dva načina

$$|\{(g,x)\in G\times X;\ gx=x\}| =$$

$$= \sum_{x\in X}|\{g\in G;\ gx=x\}| = \sum_{x\in X}|G_x| =$$

$$= \sum_{x\in X}\frac{|G|}{|G_x|} = |G|\cdot\sum_{x\in X}\frac{1}{|G_x|} =$$

$$= |G|\sum_{\underset{\text{orbite}}{\sigma\in X/G}}\sum_{x\in\sigma}\frac{1}{|G_x|} = |G|\cdot\sum_{\sigma\in X/G}\underbrace{\sum_{x\in\sigma}\frac{1}{|\sigma|}}_{1} =$$

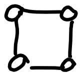
$$= |G|\cdot\sum_{\sigma\in X/G}1 = |G|\cdot|X/G|$$

drugi način

$$|\{(g,x)\in G\times X;\ gx=x\}| =$$

$$\sum_{g\in G}\{gx=x\} = \sum_{g\in G}|X^g|$$

Primer:

 barvamo oglišča z n barvami

 je isto barvanje

št barvanj glede na to identifikacijo

X.... množica vseh barv □ z n barvami

$|X| = n^4$

r...rotacija za $90°$

$G = \{id, r, r^2, r^3\}$

G deluje na X $\quad |X/G| = ?$

$$|X/G| = \frac{1}{4}\left(|X^{id}| + |X^{r}| + |X^{r^2}| + |r^3|\right)$$

$|X^{id}| = |\{$tista barvanja, ki jih id pusti na miru$\}|$

$= |X| = n^4$

n barv

$|X^{r}| = |\{r$ za $90°$ pusti na miru$\}| = n$

Podobno $|X^{r^3}| = n$

$|X^{r^2}| = n^2$

$$|X/G| = \frac{1}{4}\left(n^4 + 2n + n^2\right)$$

Razredna formula in Cauchyjev izrek

Posledica: Razredna formula

Naj bo G končna grupa

Potem obstajajo $x_1, \dots, x_r \in X - Z(G)$

da velja $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(x_i)|$

$$C_G(x_i) = \{ g \in G \;\; g x_i = x_i g \}$$

Dokaz: direktna uporaba splošne formule ko $G \curvearrowright G$ s konjugiranjem

$$G \times G \longrightarrow G$$

$$(g, x) \longmapsto g x g^{-1}$$

$\blacksquare$

Posledica: Naj bo G končna p-grupa. Potem je $Z(G) \neq \{1\}$

Dokaz: BŠZS G ni abelova

$$\exists\, x_1, \ldots, x_r \in G - Z(G)$$

$$|G| = |Z(G)| + \sum_{i=1} |G : C_G(x_i)|$$

$C_G(x_i) \neq G$, ker potem bi x_i bil v centru

Zato $p \,\big|\, |G : C_G(x_i)|$

Torej mora biti $p \,\big|\, |Z(G)|$

$\blacksquare$

Posledica: Naj bo G grupa moči p^2. Potem je G abelova

Dokaz: Naj bo G nekomutativna grupa moči p^2. Sledi: $|Z(G)| = p$

$|G/Z(G)| = p$ torej je ciklična

$$G/Z(G) = \{1Z(G), xZ(G), \ldots, x^{p-1}Z(G)\}$$

$$G = Z(G) \amalg xZ(G) \amalg \ldots \amalg x^{p-1}Z(G)$$

Vzemimo $a, b \in G$

$a \in x^i Z(G)$ $b \in x^j Z(G)$

$a = x^i \cdot z_1$ $b = x^j \cdot z_2$

$ab = x^i z_1 \cdot x^j z_2$ z_1 in z_2 sta v centru

torej $ab = x^i \cdot x^j z_1 \cdot z_2 = x^j x^i z_1 z_2 =$

$= x^j z_2 x^i z_1 = ba$ ker sta potenci istega elementa

torej je G abelova

■

Izrek (Cauchyjev izrek)

Naj bo G končna grupa in naj praštevilo p deli $|G|$. Potem v G obstaja element reda p.

Dokaz:

Za abelove grupe smo izrek že dokazali.

Indukcija po $|G|$

$|G| = p$: je ciklična torej ✓

Naj bo G grupa moči n in naj izrek velja za vse grupe manjših moči

BŠZS G ni abelova. Uporabimo razredno formulo

$$n = |G| = Z(G) + \sum_{i=1}^{r} |G : C_G(x_i)| \quad x_i \notin Z(G)$$

Recimo da $p \mid |Z(G)|$

$\Downarrow$

Abelova grupa

Potem po Cauchyjevem izreku za abelove grupe center vsebuje element reda p ✓

Lahko predpostavim da $p \nmid Z(G)$

Po razredni formuli

$$\exists i.\ p \nmid |G : C_G(x_i)| = \frac{|G|}{|C_G(x_i)|}$$

Sledi: $p \mid |C_G(x_i)|$

$C_G(x_i)$ je prava podgrupa in je manjša od $|G|$

po indukcijski predpostavki $C_G(x_i)$ vsebuje element red p

■