

# Algebra 2

9. november 2024

## 1 Uvod v teorijo grup

### 1.1 Uvod v teorijo grup

**Definicija 1.1.** Naj bo  $S$  neprazna množica. *Operacija na množici*  $S$  je preslikava  $*$  :  $S \times S \rightarrow S$ ,  $(a, b) \mapsto a * b$ . Operacija  $*$  je *asociativna*, če  $\forall a, b, c \in S. (a * b) * c = a * (b * c)$ . Operacija  $*$  je *komutativna*, če  $\forall a, b \in S. a * b = b * a$ .

**Definicija 1.2.** Neprazna množica  $S$  skupaj z operacijo  $*$  je *polgrupa*, če je operacija  $*$  asociativna.

**Definicija 1.3.** Naj bo  $S$  množica z operacijo  $*$ . Pravimo, da je  $e \in S$  *enota* (oz. *neutralni element*) za operacijo  $*$ , če  $\forall x \in S. e * x = x * e = x$ .

**Trditev 1.1.** Če v množici  $S$  obstaja enota za operacijo  $*$ , potem je ena sama.

**Definicija 1.4.** Polgrupa z enoto je *monoid*.

**Definicija 1.5.** Naj bo  $S$  množica z operacijo  $*$  in  $e \in S$  enota. Naj bo  $x \in S$ .

- Element  $l \in S$  je *levi inverz* elementa  $x$ , če  $l * x = e$ .
- Element  $d \in S$  je *desni inverz* elementa  $x$ , če  $x * d = e$ .
- Element  $y \in S$  je *inverz* elementa  $x$ , če  $x * y = y * x = e$ .

**Trditev 1.2.** Če je  $S$  monoid,  $x \in S$ ,  $l$  levi inverz  $x$  ter  $d$  desni inverz  $x$ , potem  $l = d$ .

**Definicija 1.6.** Pravimo, da je element  $x \in S$  *obrnljiv*, če obstaja inverz od  $x$ .

**Definicija 1.7.** Naj bo  $S$  z operacijo  $*$  monoid. Pravimo, da je  $S$  *grupa*, če je vsak element iz  $S$  obrnljiv. Če je operacija  $*$  komutativna, pravimo, da je  $S$  *Abelova grupa*.

V grupah ponavadi uporabljamo *multiplikativni zapis*: operacija:  $\cdot$ , enota:  $1$ , inverz od  $x$ :  $x^{-1}$ , potenca:  $x^n$ .

V Abelovih grupah uporabljamo *aditivni zapis*: operacija:  $+$ , enota:  $0$ , inverz od  $x$ :  $-x$ , potenca:  $nx$ .

Multiplikativni zapis	Aditivni zapis (Abelova grupa)
$G$ ima natanko eno enoto	$G$ ima natanko en ničeln element
Vsak element iz $G$ ima natanko en inverz	Vsak element iz $G$ ima natanko en nasprotni element
$(x^{-1})^{-1} = x$	$-(-x) = x$
$(xy)^{-1} = y^{-1}x^{-1}$	$-(x + y) = -x - y$
$x^{m+n} = x^m x^n$	$(m + n)x = mx + nx$
$(x^m)^n = x^{mn}$	$n(mx) = (nm)x$
V splošnem $(xy)^n \neq x^n y^n$	$n(x + y) = nx + ny$
$xy = xz \Rightarrow y = z$	$x + y = x + z \Rightarrow y = z$ (pravila krajšanja)
$yx = zx \Rightarrow y = z$	
$xy = 1 \Rightarrow yx = 1$	

Tabela 1: Lastnosti računanja v grupah

*Zgled.* Nekaj primerov grup.

1.  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot)$  so Abelove grupe.
2. Naj bo  $X$  neprazna množica. Definiramo  $\text{Sim}(X) = \{\text{vse bijektivne preslikave } f : X \rightarrow X\}$ .  $(\text{Sim}(X), \circ)$  je grupa, imenujemo jo *simetrična grupa* množice  $X$ .  
V posebnem primeru, ko je  $X$  končna dobimo  $\text{Sim}(\{1, 2, \dots, n\}) = S_n$ . Torej običajne permutacije.

**Zgled** (Simetrije kvadrata). Simetrije kvadrata  $K$  so izometrije  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ , da je  $f(K) = K$ .

Primeri simetriji:  $r$  - rotacija za  $90^\circ$  okoli središča kvadrata,  $z$  - zrcaljenje čez fiksno os simetrije ter kompozicije  $r$  in  $z$ . Iz geometrije lahko vidimo, da je  $zr = r^3z$ . To pomeni, da je vsak kompozitum  $r$  in  $z$  oblike  $r^kz$ .

Kvadrat ima kvečjemu 8 simetriji, ker je vsaka simetrija določena s sliko oglišča 1 in informacijo, ali smo naredili zrcaljenje ali ne. Dobimo množico simetriji  $D_{2,4} = \{\text{id}, r, r^2, r^3, z, rz, r^2z, r^3z\}$ .  $D_{2,4}$  je *diedrska grupa moči 8*.

**Zgled** (Diedrska grupa moči  $2n$ ). Imamo naslednje simetrije pravilnega  $n$ -kotnika:

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

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

Množica vseh simetriji je  $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, z, rz, r^2z, \dots, r^{n-1}z\}$ .  $D_{2n}$  je *diedrska grupa moči  $2n$* .

**Zgled** (Monoid  $\rightarrow$  Grupa). Naj bo  $(S, *)$  monoid. Definiramo  $S^* = \{\text{obrnljive elementi iz } S\}$ , potem  $S^*$  je grupa za  $*$ .

**Primer.** Naj bo  $S = (\mathbb{R}^{n \times n}, \cdot)$ ,  $S^* = \{A \in \mathbb{R}^{n \times n} \mid \det A \neq 0\} = \text{GL}_n(\mathbb{R})$ .  $\text{GL}_n(\mathbb{R})$  je *splošna linearna grupa  $n \times n$  matrik*.

**Zgled** (Direktni produkt grup). Naj bodo  $G_1, G_2, \dots, G_n$  grupe z operacijami  $*_1, *_2, \dots, *_n$ . Na množice  $G_1 \times G_2 \times \dots \times G_n$  vpeljamo operacijo  $(g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n)$ . Potem  $(G_1 \times G_2 \times \dots \times G_n, *)$  je grupa.

## 1.2 Ponovitev o permutacijah

**Izrek 1.3.** Vsaka permutacija je produkt disjunktih ciklov.

**Definicija 1.8.** Cikli dolžine 2 so *transpozicije*.

**Trditev 1.4.** Vsaka permutacija  $\pi \in S_n$  je produkt transpozicij. Teh transpozicij je vedno sodo mnogo ali vedno liho mnogo.

**Definicija 1.9.** Permutacija je *soda* (oz. *liha*), če je produkt sodo (oz. liho) mnogo transpozicij.

**Definicija 1.10.** Znak permutacije je  $\text{sgn}(\pi) = \begin{cases} 1; & \pi \text{ je soda} \\ -1; & \pi \text{ je liha} \end{cases}$ .

**Trditev 1.5.**  $\text{sgn}(\pi\rho) = \text{sgn}(\pi) \cdot \text{sgn}(\rho)$ .

## 1.3 Podgrupe

**Definicija 1.11.** Naj bo  $G$  grupa in  $H \subseteq G$ ,  $H \neq \emptyset$ .  $H$  je *podgrupa grupe  $G$* , če je  $H$  za isto operacijo tudi grupa. Oznaka  $H \leq G$ .

**Opomba.** Očitno o podgrupah:

1. Naj bo  $G$  grupa. Vedno velja:  $\{1\} \leq G$  in  $G \leq G$ .
2. Če je  $H \leq G$ , potem (nujno!)  $1 \in H$ , kjer 1 je enota v  $G$ .

**Opomba.** Pri monoidih se enota ne deduje nujno, npr.  $(\mathbb{Z}, \cdot)$  in  $(\{0\}, \cdot)$ .

**Trditev 1.6.** Naj bo  $G$  grupa,  $H \subseteq G$ ,  $H \neq \emptyset$ . 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.** Definicija podgrupe. □

**Posledica 1.6.1.** Naj bo  $G$  končna grupa in  $H \subseteq G$ ,  $H \neq \emptyset$ . Velja:

$$H \leq G \Leftrightarrow H \text{ je zaprta za množenje.}$$

**Dokaz.** Ker je  $G$  končna, ko potenciramo  $x \in H$ , ena izmed potenc zagotovo ponovi. □

**Opomba.** V končnih grupih ni potrebno preverjati zaprtost za invertiranje.

**Primer.** Primeri podrgup.

1. Vse prave podgrupe v grupi  $(\mathbb{Z}, +)$  so oblike  $n\mathbb{Z}$ ,  $n \in \mathbb{N}$ .
2. Definiramo  $\text{SL}_n(\mathbb{R}) = \{A \in \text{GL}_n(\mathbb{R}) \mid \det A = 1\}$ . Potem  $\text{SL}_n(\mathbb{R}) \leq \text{GL}_n(\mathbb{R})$ .  $\text{SL}_n(\mathbb{R})$  imenujemo *specialna linearna grupa*.
3. Definiramo  $\text{O}(n) = \{A \in \text{GL}_n(\mathbb{R}) \mid AA^T = A^T A = I\}$ . Potem  $\text{O}(n) \leq \text{GL}_n(\mathbb{R})$ .
4. Definiramo  $\text{SO}(n) = \{A \in \text{O}(n) \mid \det A = 1\}$ . Potem  $\text{SO}(n) \leq \text{O}(n)$ . Grupo  $\text{SO}(n)$  imenujemo *specialne ortogonalne matrike*.

**Trditev 1.7.** Naj bosta  $H$  in  $K$  podgrupi grupe  $G$ . Potem  $H \cap K \leq G$ . Enako velja za preseke poljubnih družin podgrup.

*Dokaz.* Karakterizacija podgrupe. □

**Definicija 1.12.** Naj bosta  $H, K \leq G$ . Definiramo  $HK = \{hk \mid h \in H, k \in K\}$ . Temu pravimo *produkt podgrup*.

*Zgled.*  $HK$  ni nujno podgrupa v  $G$ . Vzemimo  $G = S_3$ ,  $H = \{\text{id}, (1\ 2)\}$ ,  $K = \{\text{id}, (1\ 3)\}$ .

**Trditev 1.8.** Naj bosta  $H, K \leq G$ . Če velja  $HK = KH$ , potem je  $HK \leq G$ .

*Dokaz.* Karakterizacija podgrupe in definicija produkta podgrup. □

*Opomba.* Ni nujno, da produkt podgrup  $HK$  komutativen. Torej ni nujno vsak element  $hk \in HK$  se da zapisati kot  $k'h' \in KH$  za neki  $k' \in K$  in  $h' \in H$ .

**Definicija 1.13.** Naj bo  $H \leq G$ ,  $a \in G$ . Definiramo množico  $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ . Potem  $aHa^{-1} \leq G$ . Temu se reče *konjugiranje podgrupe  $H$  z elementom  $a$* .

*Dokaz.* Karakterizacija podgrupe. □

**Trditev 1.9.** Naj bo  $G$  grupa.

1. Definiramo  $Z(G) = \{y \in G \mid \forall x \in G. yx = xy\}$ . Potem  $Z(G) \leq G$ . Tej grupi pravimo center grupe  $G$ .
2. Naj bo  $a \in G$ . Definiramo  $C_G(a) = \{y \in G \mid ya = ay\}$ . Potem  $C_G(a) \leq G$ . Tej podgrupi pravimo centralizator elementa  $a$  v  $G$ .

*Dokaz.* Karakterizacija podgrupe. □