# Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 7

# Na prethodnom času

- Homomorfizam i izomorfizam
- Reprezentacija Bulovih algebri
- Bulovi izrazi i EK, DNF, SDNF (dualno ED, KNF, SKNF)
- Bulove funkcije i njihova veza sa Bulovim izrazima
- Minimizacija Bulovih izraza (u obliku DNF)
- Proste implikante i MDNF
- Karnoove karte

# Grupoidi i grupe

# Rešavanje jednačina 1

Reši jednačinu $x + 4 = 2$.

# Rešavanje jednačina 1

Reši jednačinu $x + 4 = 2$.

**U kom skupu?**

# Rešavanje jednačina 1

Reši jednačinu $x + 4 = 2$. **U kom skupu?**

U $(\mathbb{N}, +)$:

$$x + 4 = 2$$

$$(x + 4) + (-4) = 2 + (-4)$$ Ovo nije prirodan broj! Probajmo sa celim.

$$(x + 4) + (-4) = -2$$ Treba nam da zbir bude ceo broj (zatvorenost)

$$x + \big(4 + (-4)\big) = -2$$ Treba nam (asocijativnost)

$$x + 0 = -2$$ Treba nam (inverzni element)

$$x = -2$$ Treba nam (neutralni element)

U $(\mathbb{N}, +)$ nema rešenja, ali u $(\mathbb{Z}, +)$ ima i to je $x = -2$.

# Rešavanje jednačina 2

Reši jednačinu $x + 4 = 2$.

**U kom skupu?**

# Rešavanje jednačina 2

Reši jednačinu $x + 4 = 2$. **U kom skupu?**

U skupu časova na analognom satu: $(\{1, 2, \ldots, 12\}, +)$. Tj. ako jednačina glasi: ako će za 4 časa naš sat da pokazuje 2, koliko je sada sati? **Nacrtati sat!**

# Rešavanje jednačina 2

Reši jednačinu $x + 4 = 2$. **U kom skupu?**

U skupu časova na analognom satu: $(\{1, 2, \dots, 12\}, +)$. Tj. ako jednačina glasi: ako će za 4 časa naš sat da pokazuje 2, koliko je sada sati? **Nacrtati sat!**

$$\begin{aligned}
x + 4 &= 2 && \\
(x + 4) + (-4) &= 2 + (-4) && \text{Ovo nije broj iz skupa! Probajmo sa 8} \\
(x + 4) + 8 &= 2 + 8 && \text{Unazad za 4 je isto kao unapred za 8} \\
(x + 4) + 8 &= 10 && \text{Treba nam da zbir bude iz skupa (zatvorenost)} \\
x + (4 + 8) &= 10 && \text{Treba nam (asocijativnost)} \\
x + 12 &= 10 && \text{Treba nam (inverzni element)} \\
x &= 10 && \text{Treba nam (neutralni element)}
\end{aligned}$$

U daljem radu ćemo ćemo u ovom skupu umesto 12 pisati 0 i ovaj skup ćemo označavati sa $\mathbb{Z}_{12}$, jer smo ovde radili sabiranje po modulu 12.

# Rešavanje jednačina 3

Reši jednačinu $x \cdot 4 = 2$. **U kom skupu?**

# Rešavanje jednačina 3

Reši jednačinu $x \cdot 4 = 2$. **U kom skupu?**

U $(\mathbb{Z}, \cdot)$:

$$x \cdot 4 = 2$$

$$(x \cdot 4) \cdot 4^{-1} = 2 \cdot 4^{-1}$$

Ovo nije ceo broj! Probajmo sa racionalnim.

$$(x \cdot 4) \cdot 4^{-1} = \frac{1}{2}$$

Treba nam da proizvod bude racionalan broj (zatvorenost)

$$x \cdot (4 \cdot 4^{-1}) = \frac{1}{2}$$

Treba nam (asocijativnost)

$$x \cdot 1 = \frac{1}{2}$$

Treba nam (inverzni element)

$$x = \frac{1}{2}$$

Treba nam (neutralni element)

U $(\mathbb{Z}, \cdot)$ nema rešenja, ali u $(\mathbb{Q}, \cdot)$ ima i to je $x = \frac{1}{2}$.

# Rešavanje jednačina 4

Reši jednačinu $g \circ x = h$.

**U kom skupu?**

# Rešavanje jednačina 4

Reši jednačinu $g \circ x = h$. **U kom skupu?**

U $(\{f \mid f : \mathbb{N} \xrightarrow[na]{1-1} \mathbb{N}\}, \circ)$:

$$g \circ x = h$$

$$(g \circ x) \circ g^{-1} = h \circ g^{-1}$$ Mora sa leve strane! Da li je inverzna od $g$ bijekcija? Da.

$$g^{-1} \circ (g \circ x) = g^{-1} \circ h$$ Da li je kompozicija desno bijekcija (zatvorenost)? Da.

$$(g^{-1} \circ g) \circ x = g^{-1} \circ h$$ Treba nam (asocijativnost)

$$i_d \circ x = g^{-1} \circ h$$ Treba nam (inverzni element)

$$x = g^{-1} \circ h$$ Treba nam (neutralni element)

Rešenje je $x : \mathbb{N} \xrightarrow[na]{1-1} \mathbb{N}$ data sa $x = g^{-1} \circ h$.

# Grupoid

## Definicija (Grupoid)

*Neka je $G \neq \emptyset$. Tada uređeni par $(G, \star)$ zovemo grupoid ako je $\star : G^2 \to G$, tj. ako je $\star$ binarna operacija skupa $G$, tj. ako je operacija* **zatvorena** *na skupu $G$.*

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

# Grupoid

## Definicija (Grupoid)

*Neka je* $G \neq \emptyset$. *Tada uređeni par* $(G, \star)$ *zovemo grupoid ako je* $\star : G^2 \to G$, *tj. ako je* $\star$ *binarna operacija skupa* $G$, *tj. ako je operacija* **zatvorena** *na skupu* $G$.

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

# Grupoid

## Definicija (Grupoid)

*Neka je $G \neq \emptyset$. Tada uređeni par $(G, \star)$ zovemo grupoid ako je $\star : G^2 \to G$, tj. ako je $\star$ binarna operacija skupa $G$, tj. ako je operacija* **zatvorena** *na skupu $G$.*

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

# Grupoid

## Definicija (Grupoid)

*Neka je* $G \neq \emptyset$. *Tada uređeni par* $(G, \star)$ *zovemo grupoid ako je* $\star : G^2 \to G$, *tj. ako je* $\star$ *binarna operacija skupa* $G$, *tj. ako je operacija* **zatvorena** *na skupu* $G$.

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

*Kejlijeva tablica za* **konačan** *par* $(\{-1, 0, 1\}, \cdot)$

| $\cdot$ | $-1$ | $0$ | $1$ |
|---|---|---|---|
| $-1$ | | | |
| $0$ | | | |
| $1$ | | | |

# Grupoid

## Definicija (Grupoid)

*Neka je $G \neq \emptyset$. Tada uređeni par $(G, \star)$ zovemo grupoid ako je $\star : G^2 \to G$, tj. ako je $\star$ binarna operacija skupa $G$, tj. ako je operacija* **zatvorena** *na skupu $G$.*

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

*Kejlijeva tablica za* **konačan** *par* $(\{-1, 0, 1\}, \cdot)$

| $\cdot$ | $-1$ | $0$ | $1$ |
|---|---|---|---|
| $-1$ | $1$ | | |
| $0$ | | | |
| $1$ | | | |

# Grupoid

## Definicija (Grupoid)

*Neka je $G \neq \emptyset$. Tada uređeni par $(G, \star)$ zovemo grupoid ako je $\star : G^2 \to G$, tj. ako je $\star$ binarna operacija skupa $G$, tj. ako je operacija* **zatvorena** *na skupu $G$.*

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

*Kejlijeva tablica za* **konačan** *par $(\{-1, 0, 1\}, \cdot)$*

| $\cdot$ | $-1$ | $0$ | $1$ |
|---|---|---|---|
| $-1$ | $1$ | $0$ | |
| $0$ | | | |
| $1$ | | | |

$$(-1) \cdot 0 = 0$$

# Grupoid

## Definicija (Grupoid)

*Neka je $G \neq \emptyset$. Tada uređeni par $(G, \star)$ zovemo grupoid ako je $\star : G^2 \to G$, tj. ako je $\star$ binarna operacija skupa $G$, tj. ako je operacija* **zatvorena** *na skupu $G$.*

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

*Kejlijeva tablica za* **konačan** *par $(\{-1, 0, 1\}, \cdot)$*

| $\cdot$ | $-1$ | $0$ | $1$ |
|---|---|---|---|
| $-1$ | $1$ | $0$ | $-1$ |
| $0$ | $0$ | $0$ | $0$ |
| $1$ | $-1$ | $0$ | $1$ |

# Grupoid

## Definicija (Grupoid)

*Neka je $G \neq \emptyset$. Tada uređeni par $(G, \star)$ zovemo grupoid ako je $\star : G^2 \to G$, tj. ako je $\star$ binarna operacija skupa $G$, tj. ako je operacija* **zatvorena** *na skupu $G$.*

## Primer

*Zaokruži slovo ispred grupoida:*

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{N}, -)$

(c) $(\mathbb{Z}, -)$

(d) $(\{-1, 0, 1\}, \cdot)$

(e) $(\{-1, 0, 1\}, +)$

*Kejlijeva tablica za* **konačan** *par $(\{-1, 0, 1\}, \cdot)$*

| $\cdot$ | $-1$ | $0$ | $1$ |
|---|---|---|---|
| $-1$ | $1$ | $0$ | $-1$ |
| $0$ | $0$ | $0$ | $0$ |
| $1$ | $-1$ | $0$ | $1$ |

# Osobine grupoida

Grupoid $(G, \star)$ je

(a) **asocijativan** ako za sve $x, y, z \in G$ važi

$$(x \star y) \star z = x \star (y \star z)$$

(b) sa **neutralnim elementom** ako postoji $e \in G$ takav da za sve $x \in G$ važi

$$x \star e = e \star x = x$$

(c) sa **inverznim elementima** ako za svako $x \in G$ postoji $x' \in G$ takav da važi (gde je $e$ neutralni element)

$$x' \star x = x \star x' = e$$

(d) **komutativan** ako za sve $x, y \in G$ važi

$$x \star y = y \star x$$

# Polugrupe, monoidi i grupe

Uređeni par $(G, \star)$ je

- **polugrupa** ako je asocijativan grupoid (zatvorenost i asocijativnost)
- **monoid** ako je asocijativan grupoid sa neutralnim elementom (zatvorenost, asocijativnost i neutralni element)
- **grupa** ako važi
  - (Z) zatvorenost
  - (A) asocijativnost
  - (N) postoji neutralni element
  - (I) postoje inverzni elementi
- **Abelova grupa** ako je komutativna grupa

Za Abelovu grupu, ako vam je lakše zapamtiti osobine su NIZAK, za grupu NIZA

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q} \backslash \{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q} \backslash \{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q} \backslash \{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{N}, -)$
(d) $(\mathbb{Z}, -)$
(e) $(\mathbb{Z}, \cdot)$
(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\setminus\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\setminus\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\setminus\{0\}, \cdot)$

# Primeri

Od sledećih struktura zaokruži slovo ispred

polugrupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

monoida:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

grupa:

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{N}, -)$

(d) $(\mathbb{Z}, -)$

(e) $(\mathbb{Z}, \cdot)$

(f) $(\mathbb{Q}\backslash\{0\}, \cdot)$

# Osobine 1/2

## Teorema (Neutralni element je jedinstven)

*Ako u grupoidu $(G, \star)$ postoji neutralni element tada je on jedinstven.*

## Dokaz

*Pretpostavimo suprotno, da u grupoidu imamo dva neutralna elementa $e'$ i $e''$. Tada dobijamo $e' \star e'' = e''$ i $e' \star e'' = e'$. Dakle, neutralni element može biti samo jedan.*

# Osobine 1/2

## Teorema (Neutralni element je jedinstven)

*Ako u grupoidu $(G, \star)$ postoji neutralni element tada je on jedinstven.*

## Dokaz

*Pretpostavimo suprotno, da u grupoidu imamo dva neutralna elementa $e'$ i $e''$. Tada dobijamo $e' \star e'' = e''$ i $e' \star e'' = e'$. Dakle, neutralni element može biti samo jedan.*

## Teorema (Inverzni elementi su jedinstveni u grupi)

*U grupi $(G, \star)$ za svaki $x \in G$ postoji jedinstven inverzni element $x' \in G$.*

## Dokaz

*Znamo da u grupi za svaki $x \in G$ postoji bar jedan inverzni element $x' \in G$.*
*Pretpostavimo sada suprotno, da u grupi za neko $x \in G$ postoje dva inverzna elementa $x'$ i $x''$. Neka je $e \in G$ neutralni element te grupe. Tada dobijamo*
*$x' = x' \star e = x' \star (x \star x'') = (x' \star x) \star x'' = e \star x'' = x''$. Dakle, za svaki $x \in G$ postoji jedinstven inverzni element.*

# Osobine 2/2

## Teorema (Zakon kancelacije u grupi)

*Ako je $(G, \star)$ grupa tada u njoj važi zakon kancelacije (skraćivanja): za sve $x, y, z \in G$ ako je $x \star y = x \star z$ ili $y \star x = z \star x$, tada je $y = z$.*

## Dokaz

$x \star y = x \star z \;\Rightarrow\; x' \star (x \star y) = x' \star (x \star z) \;\Rightarrow\; (x' \star x) \star y = (x' \star x) \star z \;\Rightarrow$

$e \star y = e \star z \;\Rightarrow\; y = z$

# Osobine 2/2

## Teorema (Zakon kancelacije u grupi)

*Ako je $(G,\star)$ grupa tada u njoj važi zakon kancelacije (skraćivanja): za sve $x,y,z \in G$ ako je $x\star y = x\star z$ ili $y\star x = z\star x$, tada je $y = z$.*

**Dokaz**

$$x\star y = x\star z \;\;\Rightarrow\;\; x'\star(x\star y) = x'\star(x\star z) \;\;\Rightarrow\;\; (x'\star x)\star y = (x'\star x)\star z \;\;\Rightarrow$$
$$e\star y = e\star z \;\;\Rightarrow\;\; y = z$$

## Teorema (Rešavanje jednačina u grupi)

*U grupi $(G,\star)$, za sve $x,y \in G$ važi*

1. $(x\star y)' = y'\star x'$;
2. *jednačina $x\star z = y$ (takođe i $z\star x = y$) ima jedinstveno rešenje.*

**Dokaz**

1. $(x\star y)\star(y'\star x') = x\star((y\star y')\star x') = x\star(e\star x') = x\star x' = e$
2. *Jedno rešenje je $z = x'\star y$. Ako bi imali dva rešenja $z_1$ i $z_2$, tada bi iz $x\star z_1 = y$ i $x\star z_2 = y$ i zakona kancelacije dobili $z_1 = z_2$.*

# Aditivna i mulitiplikativna notacija

Često se pojavljuju grupe sa aditivnom $(G, +)$ i mulitiplikativnom $(G, \cdot)$ notacijom - ove notacije ćemo koristiti kod prstena i polja.
Kod aditivne notacije za grupu $(G, +)$ kositićemo sledeće oznake

- $0$ - neutralni element zovemo nula
- $-x$ - inverzni od $x$
- $1x = x$ i $(n+1)x = nx + x$
- $0x = 0$ i $(-n)x = n(-x)$

Kod mulitiplikativne notacije za grupu $(G, \cdot)$ kositićemo sledeće oznake

- $1$ - neutralni element zovemo jednica
- $x^{-1}$ - inverzni od $x$
- $x^1 = x$ i $x^{n+1} = x^n \cdot x$
- $x^0 = 1$ i $x^{-n} = \left(x^{-1}\right)^n$

# O teoriji grupa i jedan primer

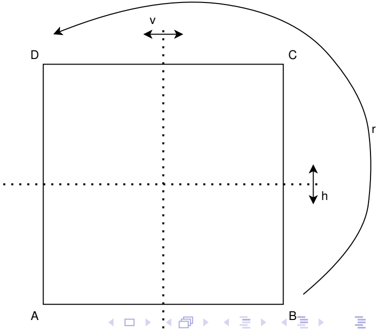
Malo kasnije videćemo da je svaka grupa zapravo neka grupa permutacija (Kejlijeva teorema), a permutacije možemo zamisliti i kao simetrije. Zapravo, teorija grupa se i bavi prirodom raznih simetrija. Sledi primer.

## Primer

*Neka je $ABCD$ kvadrat. Posmatrajmo 4 simetrije ovog kvadrata koje njegova temena $A, B, C, D$ preslikavaju ponovo u njegova temena (ukupno postoji 8 ovakvih simetrija):*

1. *$i$ rotacija za 0 stepeni*
2. *$r$ rotacija za 180 stepeni*
3. *$h$ osna simetrija u odnosu na horizontalnu osu*
4. *$v$ osna simetrija u odnosu na vertikalnu osu*

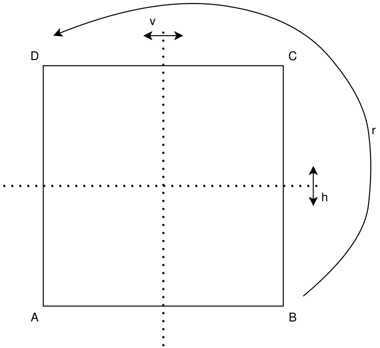
*Dokazati da je $(\{i, r, h, v\}, \circ)$ Abelova grupa.*



# Rešenje: deo 1

Date funkcije preslikavaju temena kvadrata na sledeći način

1. $i = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$
2. $r = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$
3. $h = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$
4. $v = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$



# Rešenje: deo 2

Sada za funkcije računamo kompozicije

1. $i = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$
2. $r = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$
3. $h = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$
4. $v = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$

Znamo da je $i \circ f = f \circ i = f$, za svaku funkciju $f$, pa te kompozicije nećemo pisati. Takođe, možemo da primetimo da je $r \circ r = h \circ h = v \circ v = i$, pa ni te kompozicije nećemo pisati.

1. $r \circ h = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = v$
2. $r \circ v = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = h$
3. $h \circ r = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = v$
4. $h \circ v = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = r$
5. $v \circ r = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = h$
6. $v \circ h = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = r$

# Rešenje: deo 3

Popunimo Kejlijevu tablicu i proverimo da li je $(\{i, r, h, v\}, \circ)$ Abelova grupa (NIZAK).

**Iz Kejlijeve tablice čitamo osobine:**

1. **Zatvorenost:** U tablici treba da se pojavljuju samo elementi iz zadatog skupa.
2. **Asocijativnost:** Ne vidi se iz tablice.
3. **Neutralni element:** Vrsta i kolona jednog elementa mora biti jednaka sa graničnom vrstom i kolonom.
4. **Inverzni elementi:** Neutralni element se mora pojavljivati tačno jednom u svakoj vrsti i koloni i mora biti simetrično raspoređen u odnosu na glavnu dijagonalu.
5. **Komutativnost:** Cela tablica mora biti simetrična u odnosu na glavnu dijagonalu.

| $\circ$ | $i$ | $r$ | $h$ | $v$ |
|---|---|---|---|---|
| $i$ | $i$ | $r$ | $h$ | $v$ |
| $r$ | $r$ | $i$ | $v$ | $h$ |
| $h$ | $h$ | $v$ | $i$ | $r$ |
| $v$ | $v$ | $h$ | $r$ | $i$ |

## Rešenje: deo 3

Popunimo Kejlijevu tablicu i proverimo da li je $(\{i, r, h, v\}, \circ)$ Abelova grupa (NIZAK).

1. **Zatvorenost:** U tablici se pojavljuju samo elementi iz zadatog skupa $\{i, r, h, v\}$.
2. **Asocijativnost:** Kompozicija je asocijativna operacija (rađeno kod funkcija).
3. **Neutralni element:** je $i$, njegova vrsta i kolona su jednake sa graničnom vrstom i kolonom.
4. **Inverzni elementi:** $i$ se pojavljuje jednom u svakoj vrsti i koloni i simetrično je raspoređen u odnosu na glavnu dijagonalu. Imamo: $i^{-1} = i, r^{-1} = r, h^{-1} = h, v^{-1} = v$.
5. **Komutativnost:** Tablica jeste simetrična u odnosu na glavnu dijagonalu.

| $\circ$ | $i$ | $r$ | $h$ | $v$ |
|---|---|---|---|---|
| $i$ | $i$ | $r$ | $h$ | $v$ |
| $r$ | $r$ | $i$ | $v$ | $h$ |
| $h$ | $h$ | $v$ | $i$ | $r$ |
| $v$ | $v$ | $h$ | $r$ | $i$ |

# Rešenje: deo 3

Popunimo Kejlijevu tablicu i proverimo da li je $(\{i, r, h, v\}, \circ)$ Abelova grupa (NIZAK).

1. **Zatvorenost:** U tablici se pojavljuju samo elementi iz zadatog skupa $\{i, r, h, v\}$.
2. **Asocijativnost:** Kompozicija je asocijativna operacija (rađeno kod funkcija).
3. **Neutralni element:** je $i$, njegova vrsta i kolona su jednake sa graničnom vrstom i kolonom.
4. **Inverzni elementi:** $i$ se pojavljuje jednom u svakoj vrsti i koloni i simetrično je raspoređen u odnosu na glavnu dijagonalu. Imamo: $i^{-1} = i, r^{-1} = r, h^{-1} = h, v^{-1} = v$.
5. **Komutativnost:** Tablica jeste simetrična u odnosu na glavnu dijagonalu.

| $\circ$ | $i$ | $r$ | $h$ | $v$ |
|---|---|---|---|---|
| $i$ | $i$ | $r$ | $h$ | $v$ |
| $r$ | $r$ | $i$ | $v$ | $h$ |
| $h$ | $h$ | $v$ | $i$ | $r$ |
| $v$ | $v$ | $h$ | $r$ | $i$ |

Zaključak: $(\{i, r, h, v\}, \circ)$ jeste Abelova grupa. (Inače, ova grupa ima svoje ime i zove se Klajnova grupa.)

# Podgrupoidi i podgrupe

# Podgrupoidi i podgrupe

## Definicija (Podgrupoid)

*Neka je $(G,\star)$ grupoid i $H \subseteq G$. Tada je $(H,\star)$ podgrupoid grupoida $(G,\star)$ ako je $\star$ na $H$ restrikcija operacije $\star$ iz $G$.*

## Primer

*Strukture $(\mathbb{N},\cdot)$ i $(\{-1,0,1\},\cdot)$ jesu podgrupoidi grupoida $(\mathbb{Z},\cdot)$, a $(\{-1,0,1\},+)$ i $(\mathbb{Q},\cdot)$ nisu.*

## Definicija (Podgrupa)

*Neka je $(G,\star)$ grupa i $H \subseteq G$. Tada je $(H,\star)$ podgrupa grupe $(G,\star)$ ako je $\star$ na $H$ restrikcija operacije $\star$ iz $G$ i ako je $(H,\star)$ grupa.*

## Primer

*Strukture $(\mathbb{Z},+)$ i $(\mathbb{Q},+)$ jesu podgrupe grupe $(\mathbb{R},+)$, a $(\mathbb{N},+)$ i $(\mathbb{Q}\backslash\{0\},\cdot)$ nisu.*

# Osobine podgrupa

## Teorema (Neutralni element podgrupe)

*Neka je $(G, \star)$ grupa i $(H, \star)$ jedna njena podgrupa. Ako je $e$ neutralni element grupe $(G, \star)$ tada važi $e \in H$ i $e$ je neutralni element u $(H, \star)$.*

## Dokaz

*Neka je $e \in G$ neutralni element grupe $(G, \star)$, a $e' \in H$ neutralni element grupe $(H, \star)$. Pošto je $H \subseteq G$, za sve $x \in H$ važi $x \star e = x$, ali i $x \star e' = x$. Iz kancelacije sledi $e = e'$.*

# Osobine podgrupa

## Teorema (Neutralni element podgrupe)

*Neka je $(G,\star)$ grupa i $(H,\star)$ jedna njena podgrupa. Ako je $e$ neutralni element grupe $(G,\star)$ tada važi $e \in H$ i $e$ je neutralni element u $(H,\star)$.*

## Dokaz

*Neka je $e \in G$ neutralni element grupe $(G,\star)$, a $e' \in H$ neutralni element grupe $(H,\star)$. Pošto je $H \subseteq G$, za sve $x \in H$ važi $x \star e = x$, ali i $x \star e' = x$. Iz kancelacije sledi $e = e'$.*

## Teorema (Kako se traže podgrupe)

*Neka je $(G,\star)$ grupa i $H \subseteq G$. Tada je $(H,\star)$ podgrupa grupe $(G,\star)$ akko za sve $x, y \in H$ važi $x \star y \in H$ i $x' \in H$, gde je $x'$ inverzni element od $x$.*

## Dokaz

$(\Rightarrow)$ : *sledi direktno iz definicije podgrupe.*
$(\Leftarrow)$ : *(Z): dato je $x \star y \in H$. (A): pošto je $\star$ asocijativna na čitavom $G$ onda je i na bilo kom njegovom podskupu na kom je zatvorena, tj. na $H$. (N): Iz $x \star y \in H$ i $x' \in H$ sledi $x \star x' = e \in H$ (a znamo da je neutralni jedinstven). (I): dato je $x' \in H$.*

# Plan za Lagranžovu teoremu: koseti

Broj elemenata grupe zvaćemo **red grupe**. Lagranžova teorema kaže da red podgrupe $H$ deli red grupe $G$.
**Plan:** Grupu $G$ ćemo razbiti na klase ekvivalencije, koje su sve sa istim brojem elemenata, a jedna klasa je podgrupa $H$.
Ove klase ekvivalencije su skupovi koji se zovu (levi) **koseti podgrupe** $H$.

**G**

| | | |
|---|---|---|
| e H | xH | yH |
| zH | ... | |
| | | |
| | | |

## Definicija (Koset)

*Neka je* $(H, \cdot)$ *podgrupa grupe* $(G, \cdot)$. *Za proizvoljni element* $x \in G$ *definišemo koset* $xH$ *sa* $xH = \{xh \,|\, h \in H\}$.

**Treba pokazati:**

1. Particija skupa $G$: Koseti se ili poklapaju ili ne seku i u uniji daju čitav skup $G$;
2. Svi koseti imaju isti broj elemenata kao i $H$, pa je $|G| = k \cdot |H|$, gde je $k$ broj različitih koseta.

# Samo različiti koseti

Zapravo, nećemo posmatrati sve kosete nego ćemo konstruisati samo različite kosete. Neka je $e$ neutralni element u $(G, \cdot)$, pa samim tim i u podgrupi $(H, \cdot)$. Posmatramo kosete:

1. **Korak** 1: je $eH = \{e \cdot h \,|\, h \in H\} = H$. Neka je $e = g_0$
2. **Korak** 2: uzmimo bilo koje $g_1 \in G$ koje nije iz $H$. Dobijamo drugi koset $g_1 H$
3. **Korak** $i + 1$: uzmemo bilo koje $g_i \in G$ koje nije iz $H \cup g_1 H \cup \ldots \cup g_{i-1} H$. Dobijamo $i + 1$-ti koset $g_i H$
4. Pošto $G$ ima konačno mnogo elemenata, ovih koseta ima konačno mnogo i svi elementi iz $G$ će biti u bar jednom kosetu

Skup $G$

| | | |
|---|---|---|
| $g_0 H$ | $g_1 H$ | $g_2 H$ |
| $g_3 H$ | $\cdots$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $g_{k-1} H$ |

### Napomena

*Treba pokazati za ove kosete da:*

1. *Različiti koseti imaju prazne preseke*
2. *Svi koseti imaju isti broj elemenata kao $H$*

# Različiti koseti imaju prazne preseke

## Lema (Disjunktni koseti)

*Za dva koseta iz prethodne konstrukcije* $g_iH$ *i* $g_jH$ *važi* $g_iH \cap g_jH = \emptyset$.

## Dokaz

*Neka je* $i < j$. *Na osnovu konstrukcije koseta znamo da* $g_j \notin g_iH$. *Dokaz izvodimo svođenjem na kontradikciju, pretpostavimo da postoji* $x \in g_iH \cap g_jH$. *Tada postoje* $h_i, h_j \in H$ *takvi da je*

$$x = g_ih_i = g_jh_j$$

*Množenjem ove jednakosti sa* $h_j^{-1}$ *sa desne strane dobijamo*

$$g_ih_ih_j^{-1} = g_j$$

*Pošto je* $(H, \cdot)$ *grupa imamo* $h_ih_j^{-1} \in H$, *tj. dobili smo da* $g_j \in g_iH$, *što je kontradikcija.*

# Svi različiti koseti imaju isti broj elemenata kao $H$. Lagranžova teorema

## Lema (Koseti su iste veličine)

*Svi skupovi $g_0 H, g_1 H, \ldots, g_{k-1} H$ iz konstrukcije različitih koseta imaju isti broj elemenata kao $g_0 H = H$.*

## Dokaz

*Pošto je koset $g_i H = \{g_i h \mid h \in H\}$, vidimo da koset ima tačno elemenata koliko i $H$ ako su svi elementi $g_i h$, za $h \in H$, različiti. Pretpostavimo suprotno, da postoje $h_1$ i $h_2$ takvi da je $h_1 \neq h_2$ i $g_i h_1 = g_i h_2$. Množenjem poslednje jednakosti sa $g_i^{-1}$ sa leve strane dobijamo $h_1 = h_2$, što je kontradikcija.*

# Lagranžova teorema

## Teorema (Lagranžova)

*Neka je $(G, \cdot)$ grupa reda $m$, tj. $|G| = m$ i $(H, \cdot)$ jedna njena podgrupa reda $n$, tj. $|H| = n$. Tada $n \mid m$.*

## Dokaz

*Neka su $H, g_1H, \ldots, g_{k-1}H$ koseti iz prethodne konstrukcije. Na osnovu leme Disjunktni koseti imamo $|G| = |H| + |g_1H| + \ldots + |g_{k-1}H|$, a na osnovu leme Koseti su iste veličine i pretpostavke $|H| = n$, sledi $m = kn$.*

# Primer

Naći sve podgupe Klajnove grupe $(\{i, r, h, v\}, \circ)$

| $\circ$ | $i$ | $r$ | $h$ | $v$ |
|---|---|---|---|---|
| $i$ | $i$ | $r$ | $h$ | $v$ |
| $r$ | $r$ | $i$ | $v$ | $h$ |
| $h$ | $h$ | $v$ | $i$ | $r$ |
| $v$ | $v$ | $h$ | $r$ | $i$ |

*Rešenje.* Podgrupe mogu imati $1, 2, 4$ elemenata i moraju sadržati neutralni element. Trivijalne podgrupe od 1 i 4 elementa su $(\{i\}, \circ)$ i $(\{i, r, h, v\}, \circ)$. Potencijalne podgrupe od 2 elementa su $(\{i, r\}, \circ)$, $(\{i, h\}, \circ)$ i $(\{i, v\}, \circ)$. Proverom zaključujemo da jesu podgrupe.

| $\circ$ | $i$ | $r$ |
|---|---|---|
| $i$ | $i$ | $r$ |
| $r$ | $r$ | $i$ |

| $\circ$ | $i$ | $h$ |
|---|---|---|
| $i$ | $i$ | $h$ |
| $h$ | $h$ | $i$ |

| $\circ$ | $i$ | $v$ |
|---|---|---|
| $i$ | $i$ | $v$ |
| $v$ | $v$ | $i$ |

# Šta smo danas radili

- Grupoidi
- Monoidi
- Grupe
- Abelove grupe
- Kejlijeve tablice (za konačne skupove)
- Pogrupoidi i podgrupe
- Red grupe i red podgrupe, Lagranžova teorema