

Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 4

Na prethodnom času

- Funkcije

Grupoidi i grupe

Rešavanje jednačina 1

Reši jednačinu $x + 4 = 2$.

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)

$$x + (4 + (-4)) = -2$$

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: $(\{1, 2, \dots, 12\}, +)$. 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!**

$$x + 4 = 2$$

$$(x + 4) + (-4) = 2 + (-4)$$

$$(x + 4) + 8 = 2 + 8$$

$$(x + 4) + 8 = 10$$

$$x + (4 + 8) = 10$$

$$x + 12 = 10$$

$$x = 10$$

Ovo nije broj iz skupa! Probajmo sa 8

Unazad za 4 je isto kao unapred za 8

Treba nam da zbir bude iz skupa (zatvorenost)

Treba nam (asocijativnost)

Treba nam (inverzni element)

Treba nam (neutralni element)

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?

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

$$g \circ x = h$$

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

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

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

$$i_d \circ x = g^{-1} \circ h$$

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

Mora sa leve strane! Da li je inverzna od g bijekcija? Da.

Da li je kompozicija desno bijekcija (zatvorenost)? Da.

Treba nam (asocijativnost)

Treba nam (inverzni element)

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 $\star : G^2 \rightarrow G$, 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 $\star : G^2 \rightarrow G$, 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 $\star : G^2 \rightarrow G$, 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 $\star : G^2 \rightarrow G$, 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) $(\{-1, 0, 1\}, +)$

Kejljeva 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 $\star : G^2 \rightarrow G$, 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) $(\{-1, 0, 1\}, +)$

Kejljeva 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 $\star : G^2 \rightarrow G$, 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 $\star : G^2 \rightarrow G$, 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) $(\{-1, 0, 1\}, +)$

Kejljeva 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 $\star : G^2 \rightarrow G$, 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) $(\{-1, 0, 1\}, +)$

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} x \star y = x \star z &\Rightarrow x' \star (x \star y) = x' \star (x \star z) \Rightarrow (x' \star x) \star y = (x' \star x) \star z \Rightarrow \\ e \star y = e \star z &\Rightarrow y = z \end{aligned}$$

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

$$\begin{aligned} x \star y = x \star z &\Rightarrow x' \star (x \star y) = x' \star (x \star z) \Rightarrow (x' \star x) \star y = (x' \star x) \star z \Rightarrow \\ e \star y = e \star z &\Rightarrow y = z \end{aligned}$$

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.

Aditivna i multiplikativna notacija

Često se pojavljuju grupe sa aditivnom $(G, +)$ i multiplikativnom $(G, \cdot)$ 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 multiplikativne notacije za grupu $(G, \cdot)$ kositićemo sledeće oznake

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

O teoriji grupa i jedan primer

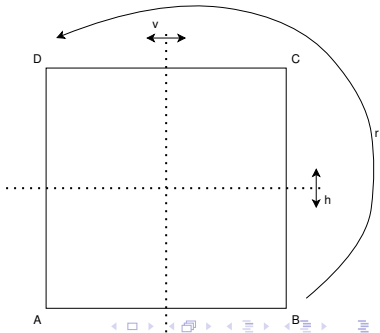
Malo kasnije videćemo da je svaka grupa zapravo neka grupa permutacija (Kejljeva teorema), a permutacije možemo zamisliti i kao simetrije. Zapravo, teorija grupa se i bavi prirodom raznih simetrija. Sledi primer.

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

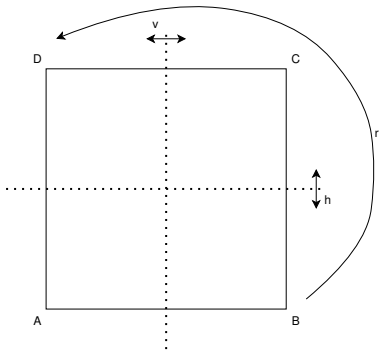
Date funkcije preslikavaju temena kvadrata na sledeći način

1. $i = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$

$$2. \quad r = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

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

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

- Zatvorenost:** U tablici se pojavljuju samo elementi iz zadatog skupa $\{i, r, h, v\}$.
- Asocijativnost:** Kompozicija je asocijativna operacija (rađeno kod funkcija).
- Neutralni element:** je i , njegova vrsta i kolona su jednake sa graničnom vrstom i kolonom.
- Inverzni elementi:** i se pojavljuje jednom u svakoj vrsti i koloni i simetrično je raspoređen u odnosu na glavnu dijagonalu. Imamo:
 $i^{-1} = i, r^{-1} = r, h^{-1} = h, v^{-1} = v$.
- 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 $(\mathbb{Q} \setminus \{0\}, \cdot)$ 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 $x \star e' = x$. Izancelacije 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 $x \in G$ definižemo koset xH sa $xH = \{xh \mid h \in H\}$.

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:

- Korak 1:** je $eH = \{e \cdot h \mid h \in H\} = H$. Neka je $e = g_0$
- Korak 2:** uzmimo bilo koje $g_1 \in G$ koje nije iz H . Dobijamo drugi koset g_1H
- Korak $i + 1$:** uzmemo bilo koje $g_i \in G$ koje nije iz $H \cup g_1H \cup \dots \cup g_{i-1}H$. Dobijamo $i + 1$ -ti koset g_iH
- 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_0H	g_1H	g_2H
g_3H	$\dots$	$\dots$
$\dots$	$\dots$	$\dots$
$\dots$	$\dots$	$g_{k-1}H$

Napomena

Treba pokazati za ove kosete da:

- Različiti koseti imaju prazne preseke*
- 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

$$x = g_i h_i = g_j h_j$$

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

$$g_i h_i h_j^{-1} = g_j$$

Pošto je $(H, \cdot)$ grupa imamo $h_i h_j^{-1} \in H$, 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 $g_0H, g_1H, \dots, g_{k-1}H$ iz konstrukcije različitih koseta imaju isti broj elemenata kao $g_0H = H$.

Dokaz

Pošto je koset $g_iH = \{g_ih \mid h \in H\}$, vidimo da koset ima tačno elemenata koliko i H ako su svi elementi g_ih , za $h \in H$, različiti. Pretpostavimo suprotno, da postoje h_1 i h_2 takvi da je $h_1 \neq h_2$ i $g_ih_1 = g_ih_2$. 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 $H, g_1H, \dots, g_{k-1}H$ koseti iz prethodne konstrukcije. Na osnovu leme Disjunktni koseti imamo $|G| = |H| + |g_1H| + \dots + |g_{k-1}H|$, a na osnovu leme Koseti su iste veličine i pretpostavke $|H| = n$, sledi $m = kn$.

Primer

Naći sve podgrupe Klajnovе 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

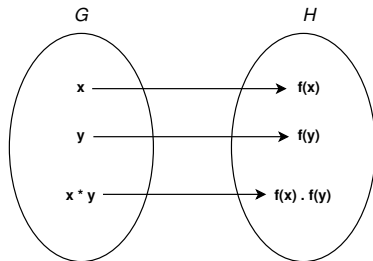
Homomorfizmi i izomorfizmi

Homomorfizmi i izomorfizmi

Definicija (Homomorfizam)

Neka su $(G, \star)$ i $(H, \cdot)$ grupoidi. Za funkciju $f : G \rightarrow H$ kažemo da je homomorfizam ako za sve $x, y \in G$ važi

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



Definicija

Bijektivni homomorfizam zove se **izomorfizam**, i tada se grupoidi zovu **izomorfni**

Primeri

1. Jedan homomorfizam grupe $(\mathbb{R}, +)$ u grupu $(\mathbb{R}^+, \cdot)$ jeste $g(x) = 1$, jer je $g(x + y) = g(x) \cdot g(y) = 1$
2. Jedan izomorfizam grupe $(\mathbb{R}, +)$ u grupu $(\mathbb{R}^+, \cdot)$ jeste $f(x) = e^x$, jer je $e^{x+y} = e^x \cdot e^y$
3. Jedan izomorfizam grupe $(\mathbb{R}^+, \cdot)$ u grupu $(\mathbb{R}, +)$ jeste $f(x) = \ln x$, jer je $\ln(x \cdot y) = \ln x + \ln y$

Osobine izomorfizama

Teorema (Inverzna funkcija od izomorfizma)

Neka je $f : G \rightarrow H$ izomorfizam grupoida $(G, \star)$ u grupoid $(H, \cdot)$. Tada je f^{-1} izomorfizam grupoida $(H, \cdot)$ u grupoid $(G, \star)$.

Teorema

Neka je $f : G \rightarrow H$ izomorfizam grupoida $(G, \star)$ u grupoid $(H, \cdot)$. Tada

1. Ako u G postoji neutralni element e_G , tada i u H postoji neutralni element e_H i važi $f(e_G) = e_H$;
2. Ako je $(G, \star)$ asocijativan (komutativan), tada je to i $(H, \cdot)$;
3. Ako G ima neutralni element e_G i ako za neko $x \in G$ postoji inverzni element x' , tada je $f(x')$ inverzni element od $f(x)$ u H .

Dokaz poslednje teoreme

Dokaz

1. Ako za sve $x \in G$ važi $x \star e_G = e_G \star x = x$, tada je $f(x \star e_G) = f(e_G \star x) = f(x)$, a pošto je f homomorfizam i $f(x) \cdot f(e_G) = f(e_G) \cdot f(x) = f(x)$. Pošto je f bijekcija, za sve $y \in H$ imamo jedno $x \in G$ takvo da je $f(x) = y$, pa imamo da za sve $y \in H$ važi $y \cdot f(e_G) = f(e_G) \cdot y = y$, tj. $f(e_G)$ jeste neutralni element u $(H, \cdot)$, a zbog njegove jedinstvenosti sledi $f(e_G) = e_H$.
2. Kako je f izomorfizam, važi: $(x \star y) \star z = x \star (y \star z)$ akko $f((x \star y) \star z) = f(x \star (y \star z))$ akko $(f(x) \cdot f(y)) \cdot f(z) = f(x) \cdot (f(y) \cdot f(z))$. Slično se dokazuje komutativnost.
3. Neka je $x \star x' = x' \star x = e_G$. Tada je $f(x \star x') = f(x' \star x) = f(e_G)$, odnosno $f(x) \cdot f(x') = f(x') \cdot f(x) = e_H$, odakle zaključujemo da je $f(x')$ inverzni element za $f(x)$.

Primer

Na skupu $\{1, a, b, c\}$ definišemo operaciju $\cdot$ na sledeći način: 1 je neutralni element, $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$ i $bc = cb = a$. Dokazati da je $(\{1, a, b, c\}, \cdot)$ Abelova grupa.

Primer

Na skupu $\{1, a, b, c\}$ definišemo operaciju $\cdot$ na sledeći način: 1 je neutralni element, $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$ i $bc = cb = a$. Dokazati da je $(\{1, a, b, c\}, \cdot)$ Abelova grupa.

Rešenje. Levo dajemo Kejlijevu tablicu za $(\{1, a, b, c\}, \cdot)$, a desno za Klajnovu grupu $(\{i, r, h, v\}, \circ)$

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$\circ$	i	r	h	v
i	i	r	h	v
r	r	i	v	h
h	h	v	i	r
v	v	h	r	i

Možemo proveriti da je $f = \begin{pmatrix} i & r & v & h \\ 1 & a & b & c \end{pmatrix}$ izomorfizam iz $(\{i, r, h, v\}, \circ)$ u grupoid $(\{1, a, b, c\}, \cdot)$, a to znači da obe strukture imaju iste osobine. Pošto je $(\{i, r, h, v\}, \circ)$ Abelova grupa, to je i $(\{1, a, b, c\}, \cdot)$. (Zapravo, to su samo dve interpretacije Klajnove grupe.)

Reprezentacije grupa: Kejljeva teorema

Teorema (Kejljeva)

Svaka grupa $(G, \cdot)$ izomorfna je sa nekom podgrupom grupe permutacija skupa G , tj. podgrupom grupe $Sym\ G = (\{f \mid f : G \xrightarrow[na]{1-1} G\}, \circ)$.

Dokaz

*Tražena funkcija je $\Psi : G \rightarrow Sym\ G$, koja svakom elementu iz G dodeljuje po jednu permutaciju iz $Sym\ G$, a definisana je sa $\Psi(a) = \sigma_a$, za sve $a \in G$. Funkcije $\sigma_a : G \rightarrow G$ definisane su sa $\sigma_a(x) = a \cdot x$, za sve $x \in G$. **Prvo bi trebalo pokazati da je σ_a bijekcija.***

Ako uzamemo skup svih ovakvih σ_a funkcija dobijamo

$$H = \{\sigma_a \mid a \in G \wedge \sigma_a : G \xrightarrow[na]{1-1} G \wedge (\forall x \in G) \sigma_a(x) = a \cdot x\}$$

Sada treba pokazati da je $(H, \circ)$ grupa i da je $\Psi : G \rightarrow H$ definisana sa $\Psi(a) = \sigma_a$ izomorfizam.

Prvi deo dokaza koji nedostaje

Prvo bi trebalo pokazati da je $\sigma_a : G \rightarrow G$ definisana sa $\sigma_a(x) = a \cdot x$, za sve $x \in G$, bijekcija:

1. Iz zatvorenosti operacije $\cdot$ na G sledi da σ_a jeste funkcija iz G u G ;
2. Injektivnost: $\sigma_a(x) = \sigma_a(y) \Rightarrow ax = ay \Rightarrow x = y$ jer u grupi G važi zakon kancelacije;
3. Surjektivnost: treba dokazati da za svako $b \in G$ postoji neko $x \in G$ takvo da je $\sigma_a(x) = b$. Pošto važi $b = 1 \cdot b = (aa^{-1})b = a(a^{-1}b)$ i $a^{-1}b \in G$, sledi $\sigma_a(a^{-1}b) = b$.

Drugi deo dokaza koji nedostaje

$$H = \{\sigma_a \mid a \in G \wedge \sigma_a : G \xrightarrow[na]{1-1} G \wedge (\forall x \in G) \sigma_a(x) = a \cdot x\}$$

Treba pokazati da je $(H, \circ)$ grupa:

1. Zatvorenost: $(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = a \cdot b \cdot x = \sigma_{a \cdot b}(x)$, kako je za $a, b \in G$ važi $a \cdot b \in G$, sledi $\sigma_{a \cdot b}(x) \in H$;
2. Asocijativnost: $\circ$ je asocijativna operacija (videti kod funkcija);
3. Neutralni element: ako je e neutralni element grupe G , onda je $\sigma_e(x) = e \cdot x = x$ identička funkcija na G , a ona je neutralni element za kompoziciju i važi $\sigma_e \in H$;
4. Inverzni elementi: ako je a^{-1} inverzni element za a u grupi $(G, \cdot)$ tada je $\sigma_a \circ \sigma_{a^{-1}} = \sigma_{a^{-1}} \circ \sigma_a = \sigma_e$, tj. za $\sigma_a \in H$ inverzni je $\sigma_{a^{-1}} \in H$.

Treći deo dokaza koji nedostaje

$\Psi : G \rightarrow H$ definisana sa $\Psi(a) = \sigma_a$ jeste izomorfizam iz grupe $(G, \cdot)$ u grupu $(H, \circ)$:

1. Injektivnost: Ako je $\Psi(a) = \Psi(b)$, tj. $\sigma_a = \sigma_b$ imamo $a \cdot x = b \cdot x$ (za sve $x \in G$), pa iz zakona kancelacije u G sledi $a = b$;
2. Surjektivnost: sledi iz konstrukcije skupa H - za svako $\sigma_a \in H$ postoji $a \in G$ takvo da je $\Psi(a) = \sigma_a$;
3. Homomorfizam: Treba pokazati da su $\Psi(a \cdot b) = \sigma_{a \cdot b}$ i $\Psi(a) \circ \Psi(b) = \sigma_a \circ \sigma_b$ jednaki. Ovo sledi jer za svako $x \in G$ važi

$$\sigma_{a \cdot b}(x) = (a \cdot b) \cdot x = a \cdot (b \cdot x) = \sigma_a(b \cdot x) = \sigma_a(\sigma_b(x)) = (\sigma_a \circ \sigma_b)(x)$$

Kongruencije

Kongruencije

Napomena

Kongruencije smo spominjali kod deljenja celih brojeva: $x \equiv_3 y$ (kongruentno po modulu 3) akko x i y daju isti ostatak pri deljenju sa 3. Ali smo imali i kod primera sa analognim satom, samo je tamo relacija bila $\equiv_{12}$.

Definicija (Kongruencije na proizvoljnim grupoidima)

Neka je $(G, \star)$ grupoid i ρ relacija ekvivalencije na G . Kažemo da je ρ kongruencija ako za sve $x, y, u, v \in G$ važi $(x \rho u \wedge y \rho v) \Rightarrow (x \star y) \rho (u \star v)$.

Definicija kaže da se relacija "slaže" sa operacijom, tj. ako

$$(x, u) \in \rho$$

$$(y, v) \in \rho$$

—tada važi—

$$(x \star y, u \star v) \in \rho$$

Važan primer

Neka je relacija $\equiv_3$ data sa za sve $a, b \in \mathbb{Z}$ važi $a \equiv_3 b$ akko $3 \mid a - b$. Tada, $\equiv_3$ jeste kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$.

Rešenje. Kod relacija samo pokazali da je $\equiv_3$ relacija ekvivalencije (RST) na $\mathbb{Z}$. Još treba da pokažemo da se slaže sa operacijama:

- U $(\mathbb{Z}, +)$ imamo $(x \equiv_3 u \wedge y \equiv_3 v) \Rightarrow (3 \mid x - u \wedge 3 \mid y - v)$
 $\Rightarrow 3 \mid (x - u) + (y - v) \Rightarrow 3 \mid (x + y) - (u + v) \Rightarrow (x + y) \equiv_3 (u + v)$
- U $(\mathbb{Z}, \cdot)$ imamo $(x \equiv_3 u \wedge y \equiv_3 v) \Rightarrow (3 \mid x - u \wedge 3 \mid y - v)$
 $\Rightarrow (3 \mid xy - uy \wedge 3 \mid uy - uv)$ (pomnožimo redom sa y i u)
 $\Rightarrow 3 \mid (xy - uy) + (uy - uv) \Rightarrow 3 \mid xy - uv \Rightarrow xy \equiv_3 uv$

Napomena

Isto bismo dokazali i da je $\equiv_n$ kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$, za sve $n \geq 2$.

Faktor grupoid

Znamo da relacija ekvivalencije vrši particiju skupa na kom je definisana i šta je faktor skup. Npr. na $\mathbb{Z}$ smo relacijom $\equiv_3$ dobili faktor skup $\mathbb{Z}_3 = \{C_0, C_1, C_2\}$. Kongruencijom na faktor skupu grupoida dobijamo nov grupoid.

Teorema

Neka je ρ kongruencija na grupoidu $(G, \cdot)$ i neka je G/ρ faktor skup. Tada je $(G/\rho, \star)$ grupoid, gde je operacija $\star$ definisana sa $C_x \star C_y = C_{x \cdot y}$ za sve $C_x, C_y \in G/\rho$.

Dokaz

Ako su $x, y \in G$, jasno da je $x \cdot y \in G$, jer je $(G, \cdot)$ grupoid. Pitanje koje se ovde postavlja je sledeće: ako uzmemo $u \in C_x$ i $v \in C_y$, znamo da je $C_x = C_u$ i $C_y = C_v$, tj. $(C_x, C_y) = (C_u, C_v)$, ali da li je i $C_x \star C_y = C_u \star C_v$? Ovo će slediti jer je ρ kongruencija:

$$(C_x, C_y) = (C_u, C_v) \Rightarrow (C_x = C_u \wedge C_y = C_v) \Rightarrow (x \rho u \wedge y \rho v) \Rightarrow (x \cdot y) \rho (u \cdot v) \Rightarrow C_{x \cdot y} = C_{u \cdot v}$$

Ponovo onaj važan primer

Kod relacija smo rekli da, pošto je svaka klasa ekvivalencije određena bilo kojim svojim elementom, pisaćemo $\mathbb{Z}_3 = \{C_0, C_1, C_2\} = \{0, 1, 2\}$.

Pošto je $\equiv_3$ kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$, dobijamo nove faktor grupoide $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$, gde su operacije definisane sa $C_x +_3 C_y = C_{x+y}$ i $C_x \cdot_3 C_y = C_{x \cdot y}$. Npr. $2 +_3 2 = 1$ i $2 \cdot_3 2 = 1$.

Ponovo onaj važan primer

Kod relacija smo rekli da, pošto je svaka klasa ekvivalencije određena bilo kojim svojim elementom, pisaćemo $\mathbb{Z}_3 = \{C_0, C_1, C_2\} = \{0, 1, 2\}$.

Pošto je $\equiv_3$ kongruencija grupe $(\mathbb{Z}, +)$ i polugrupe $(\mathbb{Z}, \cdot)$, dobijamo nove faktor grupoide $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$, gde su operacije definisane sa $C_x +_3 C_y = C_{x+y}$ i $C_x \cdot_3 C_y = C_{x \cdot y}$. Npr. $2 +_3 2 = 1$ i $2 \cdot_3 2 = 1$.

Sada možemo da crtamo Keijjeve tablice grupoida $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$

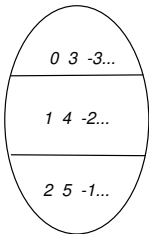
$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Proverom osobina dobijamo da je $(\mathbb{Z}_3, +_3)$ Abelova grupa, a $(\mathbb{Z}_3, \cdot_3)$ komutativan monoid. Npr. asocijativnost operacije $+_3$ sledi iz

$$(C_x +_3 C_y) +_3 C_z = C_{x+y} +_3 C_z = C_{(x+y)+z} = C_{x+(y+z)} = C_x +_3 C_{y+z} = C_x +_3 (C_y +_3 C_z)$$

I dalje u vezi važnog primera

Faktor skup $\mathbb{Z}_3$

Isto kao što smo dobili grupoide $(\mathbb{Z}_3, +_3)$ i $(\mathbb{Z}_3, \cdot_3)$, možemo dobiti grupoide $(\mathbb{Z}_n, +_n)$ i $(\mathbb{Z}_n, \cdot_n)$ (na vežbama ćemo o njihovim osobinama).

Da bi olakšali notaciju, često ćemo umesto $(\mathbb{Z}_n, +_n)$ i $(\mathbb{Z}_n, \cdot_n)$ pisati samo $(\mathbb{Z}_n, +)$ i $(\mathbb{Z}_n, \cdot)$, jer je iz konteksta jasno da su operacije "sabiranje po modulu n " i "množenje po modulu n ".

Ciklične grupe

Red elemenata grupe

Setimo se da smo red grupe definisali kao broj elemenata grupe. Takođe smo za multiplikativnu notaciju definisali $x^k = x \cdot x^{k-1}$.

Definicija (Red elementa)

Neka je $(G, \cdot)$ grupa, e neutralni element i $x \in G$. Red elementa x je najmanji $k \in \mathbb{N}$ takav da je $x^k = e$.

Primer

1. U Klajnovoj grupi $\{1, a, b, c\}$, smo imali $a^2 = b^2 = c^2 = 1$, pa su a, b, c svi reda 2 (neutralni je u svakoj grupi reda 1);
2. U grupi $(\mathbb{Z}_3 \setminus \{0\}, \cdot)$ imamo $2^2 = 1$, pa je element 2 reda 2;
3. U grupi $(\mathbb{Z}_3, +)$ reda 3 (primeti aditivnu notaciju) imamo $1 + 1 + 1 = 3 \cdot 1 = 0$, $2 + 2 + 2 = 3 \cdot 2 = 0$, pa su 1 i 2 reda 3.

Ciklične grupe

Teorema

Neka je $(G, \cdot)$ konačna grupa sa neutralnim elementom e i neka je element $x \in G$ reda k . Tada je $H = \{x^n \mid n \in \mathbb{N}\} = \{e, x, x^2, \dots, x^{k-1}\}$ nosač podgrupe.

Posledica

Neka je $(G, \cdot)$ grupa reda m . Tada red svakog elementa $x \in G$ deli red grupe i $x^m = e$.

Definicija (Ciklične grupe)

Grupa $(G, \cdot)$ reda n je ciklična ako postoji element $x \in G$ reda n .

Primeri cikličnih grupa: Sve grupe prostog reda, $(\mathbb{Z}_n, +)$, ...