Osnovne algebarske strukture
3. Grupe

Borka Jadrijević

3.1 Binarna operacija. Grupoid.

Definicija 3.1 *Neka je G neprazni skup.* ***Binarna operacija*** *na skupu G je svako preslikavanje $\theta : G \times G \longrightarrow G$.*

Dakle, binarna operacija svakom uređenom paru $(a, b) \in G \times G$ pridružuje točno jedan element $c = \theta(a, b)$ koji nazivamo **rezultat** binarne operacije na paru (a, b).

$$(a, b) \in G \times G \quad \stackrel{\theta}{\longrightarrow} \quad c = \theta(a, b) \in G$$

Definicija 3.2 *Binarnom operacijom θ na nepraznom skupu G zadana je jedna* ***algebarska struktura****. Uređeni par (G, θ) koji se sastoji od nepraznog skupa G i binarne operacije θ nazivamo* ***grupoidom****.*

Primjer 3.1:

a) Neka je $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ a binarana operacija definirana kao

$$\theta(a, b) = a + b$$

koju nazivamo standardno zbrajanje. Dakle, svi ovi skupovi su uz ovu binarnu operaciju grupoidi.

b) Slično, ovi skupovi su grupoidi su i uz binarnu operaciju standardnog množenja $\theta(a,b) = a \cdot b$.

Uočimo: Npr. $(\mathbb{N},+)$ i $(\mathbb{N},\cdot)$ su različiti grupoidi;

c) Skup $\mathbb{N}$ uz standardno oduzimanje $\theta(a,b) = a - b$ nije grupoid, dok $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ to jesu;

d) Neka je S bilo koji skup i $\mathcal{P}(S) = \{A \,|\, A \subseteq S\}$ njegov partitivni skup. Tada je $\mathcal{P}(S)$ uz svaku od sljedećih operacija grupoid:

$$\begin{aligned} \theta(A,B) &= A \cup B \\ \theta(A,B) &= A \cap B \\ \theta(A,B) &= A \setminus B \end{aligned}$$

e) Neka je S bilo koji skup i $\mathcal{F}(S) = \{f \,|\, f : S \longrightarrow S\} := S^S$ (sva preslikavanja iz S u S). Na skupu S promatramo binarnu operaciju:

$$\theta(f,g) = g \circ f$$

danu sa $(g \circ f)(x) = g(f(x))$ za svaki $x \in S$.

Onda je $\left(S^S, \circ\right)$ grupoid.

Napomena: Umjesto funkcijske vrijednosti $\theta(a,b)$, rezultat binarne operacije na paru (a,b) obično pišemo

$$a+b,\ a\cdot b,\ a\circ b,\ a*b,\ldots.$$

a u apstratktnim razmatranjim obično identificiramo

$$\theta(a,b)\equiv a\cdot b\equiv ab,$$

a rezultat binarne operacije nazivamo **produktom**.

Primjer 3.2 Ako je G konačan skup i nema previše elemenata, tada se binarna operacija može zadati tablično (tablicom množenja). Npr. neka je $G=\{a,b,c,d\}$ i binarna operacija $\circ$ zadana tablično:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	b	b	b
c	c	c	c	c
d	d	c	b	a

Primjetimo: $a\circ a=a,\ \ d\circ c=b$, $c\circ d=c,\ldots$. Uočimo $d\circ c\neq c\circ d$.

Definicija 3.3 *Neka je* $(G, \cdot)$ *grupoid i* $a, b \in G$. *Ako je* $ab = ba$ *onda kažemo da* a *i* b ***komutiraju**. Nadalje, ako vrijedi*

$$ab = ba \text{ za sve } a, b \in G$$

onda kažemo da je binarna operacija ***komutativna**, tj. da je grupoid* $(G, \cdot)$ ***komutativan*** *ili* ***Abelov**.*

Primjer 3.3

- Grupoidi $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$ (uz standardno zbrajanje i množenje) su komutativni grupoidi;
- Grupoidi $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$ nisu komutativni;
- Grupoidi (u Primjeru 1, d)) $(\mathcal{P}(S), \cup)$, $(\mathcal{P}(S), \cap)$ su komutativni, dok $(\mathcal{P}(S), \setminus)$ to nije;
- Grupoid $\left(S^S, \circ\right)$ (u Primjeru 3.1, e)) i grupoid $(G, \circ)$ (u Primjeru 3.2) nije komutativan.

3.2 Asocijativnost. Polugrupa.

Definicija 3.5 *Neka je $(G, \cdot)$ grupoid. Za binarnu operaciju $\cdot$ kažemo da je* ***asocijativna*** *ako vrijedi*

$$a\,(bc) = (ab)\,c \text{ za sve } a, b, c \in G.$$

Polugrupa *ili* ***asocijativni grupoid*** *je grupoid $(G, \cdot)$ kod kojeg je binarna operacija asocijativna.*

Zakona asocijativnosti govori da ima smisla definicija produkta tri faktora

$$a\,(bc) = (ab)\,c := abc \text{ za sve } a, b, c \in G.$$

Ovo svojstvo vrijedi i za više od tri faktora.

Propozicija 3.1 *Neka je $(G, \cdot)$ polugrupa. Tada vrijedi*

$$(ab)\,cd = a\,(bc)\,d = ab\,(cd) \text{ za sve } a, b, c \in G.$$

Dokaz:

Stoga, definiramo

$$(ab)\,cd := abcd.$$

U polugrupi $(G,\cdot)$ ima smisla pojam potencije. Definiramo:

$$a^1 = a,\ a^2 = aa \text{ i induktivno } a^{n+1} = a^n a \text{ za } n \in \mathbb{N}.$$

Vrijedi:
Propozicija 3.2 *Neka je $(G,\cdot)$ polugrupa. Tada vrijedi*

$$a^m \cdot a^n = a^{m+n} \text{ i } (a^m)^n = a^{m\cdot n} \textit{ za sve } m,n \in \mathbb{N}.$$

Dokaz:

Ako je u polugrupi $(G,\cdot)$ binarna operacija komutativna, onda kažemo da je $(G,\cdot)$ ***komutativna*** ili ***Abelova*** polugrupa.

Primjer 3.5

- Grupoidi $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},+)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},+)$, $(\mathbb{C},\cdot)$ (uz standardno zbrajanje i množenje) su (komutativne) polugrupe;

- Grupoidi (u Primjeru 1, d)) $(\mathcal{P}(S), \cup)$, $(\mathcal{P}(S), \cap)$ su (komutativne) polugrupe;
- Grupoid $\left(S^S, \circ\right)$ (u Primjeru 1, e)) je (nekomutativna) polugrupa.
- Definirajmo na $\mathbb{R}$ binarnu operaciju sa

$$a * b = \min\{a, b\}$$

Tada je $(\mathbb{R}, *)$ komutativna polugrupa.

3.3 Neutralni element. Monoid.

Definicija 3.6 *Neka je $(G, \cdot)$ grupoid. Ako postoji element $l \in G$ takav da vrijedi:*

$$la = a \text{ za sve } a \in G,$$

*onda kažemo da je l **lijeva jedinica** za binarnu operaciju $\cdot$ na G.*
Slično, ako postoji $d \in G$ takav da vrijedi:

$$ad = a \text{ za sve } a \in G,$$

*onda kažemo da je d **desna jedinica** za binarnu operaciju $\cdot$ na G.*

Ako postoji $e \in G$ *takav da vrijedi:*

$$ea = ae = a \text{ za sve } a \in G,$$

onda kažemo da je e ***obostrana jedinica*** *ili samo* ***jedinica*** *ili* ***neutralni element*** *za binarnu operaciju* $\cdot$ *na* G (*ili za grupoid* $(G, \cdot)$).

Primjer 3.6

1. U grupoidu $(\mathbb{N}, +)$ nema neutralnog elementa, dok je u $(\mathbb{N}, \cdot)$ to broj 1;
2. U grupoidima $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ neutralni element je 0, dok je u $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ neutralni element 1.
3. U grupoidu $(\mathcal{P}(S), \cup)$ (u Primjeru 3.1, d)) neutralni element je $\emptyset$, dok je u grupoidu $(\mathcal{P}(S), \cap)$ neutralni element S;
4. U grupoidu $\left(S^S, \circ\right)$ (u Primjeru 1, e)) je neutralni element preslikavanje $e : S \longrightarrow S$, definirano sa $e(x) = x$ za sve $x \in S$. Ovako definirano preslikavanje e naziva se *identično preslikavanje* ili *identiteta* na S.
5. U grupoidu $(\mathcal{P}(S), \setminus)$ je desna jedinica (jedina!) $\emptyset$, dok lijevih jedinica nema;

6. Neka je na $\mathbb{N}$ dana binarna operacija s

$$a * b = a \text{ za sve } a, b \in \mathbb{N}.$$

U grupoidu $(\mathbb{N}, *)$ je desna jedinica svaki element od $\mathbb{N}$, dok lijevih jedinica nema.

Vidimo da u grupoidu može biti i samo lijevih ili samo desnih jedinica i to jedna ili više njih. Međutim vrijedi sljedeće:

Propozicija 3.3 *Neka u $(G, \cdot)$ grupoidu binarna operacija ima lijevu i desnu jedinicu. Onda su one jednake, tj. binarna operacija ima neutralni element.*

Dokaz:

Odatle specijalno slijedi: *Ako postoji bar jedna desna jedinica, ne može biti više od jedne lijeve jedinice, i obratno*.

Propozicija 3.4 *Ako grupoid $(G, \cdot)$ ima neutralni element, onda je on jedinstven.*

Dokaz:

Definicija 3.7 *Grupoid je $(G,\cdot)$ u kojem je binarna operacija asocijativna i koji ima neutralni element naziva se* ***monoid*** *ili* **kvazigrupa**. *Dakle, monoid je polugrupa s neutralnim elementom.*

Napomena: Ako je binarna operacija dodatno i komutativna onda govorimo o **komutativnom monoidu.**

Primjer 3.6

- U polugrupi $(\mathbb{N},+)$ nema neutralnog elementa, dok je u $(\mathbb{N},\cdot)$ to broj 1, pa je $(\mathbb{N},\cdot)$ (komutativni) monoid;
- Polugrupa $(\mathcal{P}(S),\cup)$ ima neutralni element $\emptyset$, dok je u polugrupi $(\mathcal{P}(S),\cap)$ neutralni element S. Dakle, $(\mathcal{P}(S),\cup)$ i $(\mathcal{P}(S),\cap)$ su (komutativni) monoidi;
- Polugrupa $\left(S^S,\circ\right)$ ima neutralni element i to je preslikavanje $e:S\longrightarrow S$, definirano sa $e(x)=x$ za sve $x\in S$. Dakle, $\left(S^S,\circ\right)$ je (nekomutativni) monoid.
- Na skupu $\mathbb{Z}_m=\{0,1,...,m-1\}$, $m\in\mathbb{N}$, definirajmo binarnu operaciju $+_m$ s

$$a+_m b=\text{ostatak pri dijeljenju } a+b \text{ s } m$$

Tada je $(\mathbb{Z}_m, +_m)$ (komutativni) monoid s neutralnim elementom $0 \in \mathbb{Z}_m$.
Tablica "množenja" za $m = 4$ je

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Slično, $(\mathbb{Z}_m, \cdot_m)$ je (komutativni) monoid s neutralnim elementom $1 \in \mathbb{Z}_m$, gdje je binarna operacija $\cdot_m$ definirana s

$$a \cdot_m b = \text{ostatak pri dijeljenju } a \cdot b \text{ s } m.$$

Tablica "množenja" za $m = 4$ je

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

3.4 Invertibilni elementi.

Definicija 3.8 *Neka je $(G,\cdot)$ grupoid koji ima neutralni element e za binarnu operaciju $\cdot$ i neka je $a \in G$ bilo koji element. Ako postoji $u \in G$ takav da vrijedi:*

$$ua = e \quad ,$$

*onda kažemo da je u **lijevi inverz** elementa a u $(G,\cdot)$.*
Slično, ako postoji $v \in G$ takav da vrijedi:

$$av = e,$$

*onda kažemo da je v **desni inverz** elementa a u $(G,\cdot)$.*
Ako postoji $x \in G$ takav da vrijedi:

$$xa = ax = e,$$

*onda kažemo da je x **obostrani inverz** ili samo **inverz** elementa a u $(G,\cdot)$. Ako za $a \in G$ postoji inverz, kažemo da je a **invertibilan element** u $(G,\cdot)$*.

Napomena: U svakom grupoidu s jedinicom ima invertibilnih elemenata. Takav je npr. sama jedinica grupoida.

Primjer 3.7

- U $(\mathbb{N}, \cdot)$ je samo neutralni element 1 invertibilan.
- U grupoidima $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ svi elementi su invertibilni.
- U $(\mathbb{Z}, \cdot)$ invertibilan su samo 1 i -1, dok su $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ invertibilni svi elementi $\neq 0$.
- U $\left(S^S, \circ\right)$ invertibilna su samo ona preslikavanja koja su bijekcije. Naime, jedino za bijekciju $f : S \longrightarrow S$ postoji inverzno preslikavanje $f^{-1} : S \longrightarrow S$ za koje vrijedi

$$f \circ f^{-1} = f^{-1} \circ f = e$$

gdje je e identiteta na S. U tom grupoidu ima, međutim, i elemenata koji imaju samo lijeve, odnosno samo desne inverze. Primjerice, za $\left(\mathbb{N}^N, \circ\right)$ i $f, g \in \mathbb{N}^N$ dane s

$$\begin{aligned} f(n) &= n + 1 \\ g(n) &= \begin{cases} n - 1, & n \geq 2 \\ 1 & n = 1 \end{cases} \end{aligned}$$

imamo

$$g \circ f = e \quad \text{i} \quad f \circ g \neq e$$

što pokazuje da je g lijevi inverz za f, a f desni inverz za g (ali obrat ne vrijedi). Dodatno, može se pokazati da f nema desnog inverza niti g lijevog.

Ako je binarna operacij a u grupoidu i asocijativna, tj. ako je $(G, \cdot)$ monoid, imamo:

Propozicija 3.5 *Neka je $(G, \cdot)$ monoid i $a \in G$ njegov element. Ako a ima lijevi i desni inverz, oni su nužno jednaki, tj. element a je invertibilan.*

Dokaz:

Odatle specijalno slijedi: *Ako u monoidu neki element ima desni inverz, ne može imati više od jednog lijevog inverza i obratno.*

Propozicija 3.6 *Neka je $(G, \cdot)$ monoid i $a \in G$ njegov element. Ako je a invertibilan, njegov inverz je jedinstven.*

Dokaz:

3.5 Grupa.

Definicija 3.9 Grupa *je monoid u kojem je svaki element invertibilan.*

Neovisno o ranijim pojmovima, grupu definiramo na ovaj način:

Definicija 3.9' *Uređeni par* $(G, \cdot)$, *gdje je* G *neprazan skup a*

$$\cdot\ : G \times G \longrightarrow G$$

binarna operacija, nazivamo ***grupa*** *ako su ispunjeni sljedeći uvjeti:*

i) *binarna operacija je asocijativna, tj. vrijedi*

$$a\,(bc) = (ab)\,c, \text{ za sve } a, b, c \in G.$$

ii) *za binarnu operaciju postoji neutralni element, tj.* $e \in G$ *sa svojstvom*

$$ea = ae = a \text{ za sve } a \in G.$$

iii) *svaki je element invertibilan, tj. za svaki* $a \in G$ *postoji* $a^{-1} \in G$ *sa svojstvom*

$$aa^{-1} = a^{-1}a = e.$$

Ako je ispunjen i dodatni zahtjev:

iv) *binarna operacija je komutativna, tj. vrijedi*

$$ab = ba \text{ za sve } a, b \in G.$$

onda kažemo da je $(G, \cdot)$ je ***komutativna*** *ili* ***Abelova*** *grupa.*

Uvjeti **i) - iii)** nazivaju se i aksiomi grupe. Taj sustav aksioma nije nezavisan, jer sadrži i tvrdnje koje se mogu dokazati. Postoji i alternativna definicija grupe koja propisuje minimalne uvjete koji karakteriziraju grupu.

Za grupu kažemo da je **konačna** ili **beskonačna**, već prema tome ima li skup G konačno ili beskonačno mnogo elemenata. Broj elemenata (kardinalni broj) skupa G nazivamo **red grupe**.

Napomena:

- Jedinstvenost neutralnog elementa u **ii)** slijedi iz Propozicije 3.4**.** Slično, jedinstvenost inverznog elementa u **iii)** slijedi iz Propozicije 3.6 budući je svaka grupa monoid.

- Apstraktnu grupu $(G, \cdot)$ (neprecizno) nazivamo "multiplikativna" grupa, a binarnu operaciju $\cdot$ "množenje". Neutralni element multiplikativne grupe obično nazivamo **jedinica** (i obično označavamo s 1).

- U Abelovoj grupi binarnu operaciju obično zapisujemo aditivno, tj. ako grupu zadamo sa $(G, +)$ onda je nazivamo "aditivna" grupa i podrazumijevamo da je Abelova. Neutralni element aditivne grupe obično nazivamo **nula** (i označavamo sa 0), a inverzni element od a označavamo sa $-a$ (umjesto a^{-1}) i nazivamo **suprotni element**.

- Obično ćemo u oznaci $(G, \cdot)$ za grupu ispuštati binarnu operaciju i govoriti jednostavno o grupi G.

Propozicija 3.7 *Neka je* $(G, \cdot)$ *grupa.*

i) *Za svaki* $a \in G$ *vrijedi*

$$\left(a^{-1}\right)^{-1} = a.$$

ii) ***(invertiranje produkta)*** *Za sve* $a, b \in G$ *vrijedi*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

iii) ***(pravilo skraćivanja)*** *Za sve* $a, b, c \in G$ *vrijedi*

$$\begin{aligned} ac &= bc \iff a = b \\ ca &= cb \iff a = b. \end{aligned}$$

Dokaz:

Propozicija 3.8 *Neka je* $(G, \cdot)$ *grupa. Tada jednadžbe*

$$ax = b \quad \text{i} \quad ya = b$$

imaju jedinstvena rješenja, za svaki $a, b \in G$.

Dokaz:

Neka je $a \in G$ bilo koji element grupe. Već smo prije (kod polugrupa) definirali pojam potencije a^n za $n \in \mathbb{N}$. U grupi možemo definirati a^n za sve $n \in \mathbb{Z}$. Definiramo

$$\begin{aligned} a^0 &:= e,\ n = 0. \\ a^n &:= \left(a^{-n}\right)^{-1},\ n < 0. \end{aligned}$$

Propozicija 3.8 *Neka je $a \in G$ bilo koji element grupe . Onda je*

i) $a^m a^n = a^n a^m = a^{m+n}$;

ii) $(a^m)^n = a^{m \cdot n}$;

za sve $m, n \in \mathbb{Z}$.

Dokaz: Slično kao Propozicija 3.2.

Primijetimo da iz **ii)**, za $m = -1$ specijalno vrijedi

$$\left(a^{-1}\right)^n = a^{-n} = (a^n)^{-1}.$$

Neka je $a \in G$ bilo koji element grupe G. Promatrajmo skup svih njegovih potencija

$$\{..., a^{-2}, a^{-1}, a^0, a^1, a^2, ...\}.$$

Ako među tim potencijama nema jednakih, kažemo da je element a **beskonačnog reda**. Ako pak među potencijama ima jednakih, ako je npr. za $k \neq l$

$$a^k = a^l,$$

onda je, prema Propoziciji 3.8,

$$a^{k-l} = e,$$

tj. postoje potencije od a koje s u jednake jedinici grupe. Kažemo u tom slučaju da je element a **konačnog reda**.

Definicija 3.10 *Neka je $n \in \mathbb{N}$ najmanji prirodni broj s gornjim svojstvom, tj. takav da je:*

1. $a^n = e$*;*

2. $a^k = e$ *i* $k \in \mathbb{N}$ *povlači* $k \geq n$*.*

Onda kažemo da je n ***red*** *elementa a.*

Napomena:

- U svakoj je grupi neutralni element jedini element reda 1;
- U konačnoj grupi svi elementi konačnog reda. No, to može biti slučaj i kod beskonačnih grupa. Grupa u kojoj su svi elementi konačnog reda naziva se **periodična**.

Propozicija 3.9 *Neka je G grupa i $a \in G$ reda n. Onda među potencijama od a ima točno n različitih, i to su*

$$e, a, a^2, ..., a^{n-1}.$$

Dokaz:

Posljedica 3.1 Neka je G grupa i $a \in G$ reda n. *Onda je $a^k = e$ ako i samo ako je k djeljiv s n.*

Dokaz:

Napomena:

- Potenciji a^n u multiplikativnoj grupi odgovara u aditivnoj: $na := a + ... + a$;
- Potenciji a^{-n} u multiplikativnoj grupi odgovara u aditivnoj: $-na := -(na)$;
- Potenciji $a^0 = e$ u multiplikativnoj grupi odgovara u aditivnoj: $0a := \mathbf{0}$ (oprez!);

Sada Propozicija 3.8 za aditivnu grupu glasi:

Propozicija 3.8' U svakoj grupi $(G, +)$ vrijede sljedeća pravila za sve $a \in G$ i $m, n \in \mathbb{Z}$.

i) $ma + na = (m + n)a;$;

ii) $m(na) = (mn)a$;

U ovom zapisu, element $a \in G$ je reda n, ako je n najmanji prirodan broj takav da je

$$na = 0.$$

Primjer 3.8

1. $(\mathbb{Z},+)$ je komutativna grupa. Neutralni element je 0, dok je $-n$ inverz od n, jer vrijedi $n+(-n)=(-n)+n=0$ za svaki $n\in\mathbb{Z}$. Slično, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ su komutativne grupe.

Napomena: Dakle, (standardno) oduzimanje je zbrajanje sa suprotnim elementom: $a+(-b):=a-b$;

2. $(\mathbb{R}\setminus\{0\},\cdot)$ je komutativna grupa. Neutralni element je 1, dok je $a^{-1}=\frac{1}{a}$ inverz od a, jer vrijedi $a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$ za svaki $a\in\mathbb{R}\setminus\{0\}$. Slično, $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$ su komutativne grupe. Zašto $(\mathbb{R},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{C},\cdot)$ nisu grupe?

3. $\left(V^3,+\right)$ je komutativna grupa.

4. $(2\mathbb{Z},+)$ je komutativna grupa.

5. Komutativni monoidi $(\mathcal{P}(S),\cup)$ i $(\mathcal{P}(S),\cap)$ nisu grupe. Zašto?

6. Jesu li $(\mathbb{Z}_m, +_m)$ i $(\mathbb{Z}_m, \cdot_m)$ (komutativni) monoidi grupe? Primjer za $m = 4$:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(\mathbb{Z}_m, +_m)$ je grupa a $(\mathbb{Z}_m, \cdot_m)$ nije. Je li $(\mathbb{Z}_m \diagdown \{0\}, \cdot_m)$ grupa?

7. Nekomutativni monoid $\left(S^S, \circ\right)$ (u Primjeru 3.1, e)) nije grupa. U tom monoidu invertibilna su samo ona preslikavanja koja su bijekcije. Naime, jedino za bijekciju

$$f : S \longrightarrow S$$

postoji inverzno preslikavanje

$$f^{-1} : S \longrightarrow S$$

za koje je vrijedi

$$f \circ f^{-1} = f^{-1} \circ f = e.$$

Neka je

$$B(S) = \left\{ f \in S^S \,|\, f \text{ je bijekcija} \right\} \subset S^s.$$

Tada je $B(S)$ s obzirom na operaciju komponiranja naslijeđenu $\circ$ iz S^S, tj. $(B(S), \circ)$ (nekomutativna) grupa. Tu grupu naivamo **grupom permutacija** od S.

8. Skup $\mathbb{R}^n = \{(\alpha_1, \alpha_2, ..., \alpha_n) \,|\alpha_i \in \mathbb{R}\}$ uz standardno koordinatno zbrajanje

$$(\alpha_1, \alpha_2, ..., \alpha_n) + (\alpha_1', \alpha_2', ..., \alpha_n') := (\alpha_1 + \alpha_1', \alpha_2 + \alpha_2', ..., \alpha_n + \alpha_n')$$

za sve $(\alpha_1, \alpha_2, ..., \alpha_n), (\alpha_1', \alpha_2', ..., \alpha_n') \in \mathbb{R}^n$ je grupa.

9. Neka je

$$P_n = \left\{ p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 \,|a_i \in \mathbb{R} \right\}$$

skup svih polinoma u jednoj varijabli x s realnim koeficijentima stupnja najviše $n-1$.

Onda je P_n uz standardno zbrajanje

$$p(x)+q(x)=$$

$$=\left(a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+...+a_1x+a_0\right)+\left(a'_{n-1}x^{n-1}+a'_{n-2}x^{n-2}+...+a'_1x+a'_0\right)$$

$$:=\left(a_{n-1}+a'_{n-1}\right)x^{n-1}+\left(a_{n-2}+a'_{n-2}\right)x^{n-2}+...+(a_1+a'_1)\,x+(a_0+a'_0)$$

za sve $p(x)\,,\,q(x)\in P_n$, grupa. Isto vrijedi i za

$$P=\bigcup_{n=1}^{\infty}P_n=\left\{p(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+...+a_1x+a_0\,\middle|\,n\in\mathbb{N},\ a_i\in\mathbb{R}\right\}.$$

10. Neka je $P=\{p,n\}=\{$par, nepar$\}$. Provjerite je li skup P uz operacije prirodnog zbrajanja $+$ i množenja $\cdot$ koje su dane s

$+$	p	n
p	p	n
n	n	p

i

$\cdot$	p	n
p	p	p
n	p	n

grupa? $(P,+)$ je komutativa grupa, dok je $(P,\cdot)$ komutativni monoid ali nije grupa.

Usporedite strukture sa skupom $\{0, 1\}$ na kojem je definirano Booleovo zbrajanje i množenje. Postoji li grupa s jednim odnosno dva elementa?

3.6 Podgrupa.

Neka je (G, θ) grupoid i $H \subseteq G$. Neka je

$$\theta\,|_{H\times H} : H \times H \to G$$

restrikcija binarne operacije θ na skup $H \times H$. Ako je

$$\theta\,(H \times H) \subseteq H,$$

onda kažemo da je skup H **zatvoren** s obzirom na operaciju θ. U tom slučaju je restrikcija

$$\overline{\theta} : H \times H \to H,$$

$$\overline{\theta}\,(a, b) = \theta\,(a, b) \quad \text{za sve} \quad (a, b) \in H \times H$$

binarna operacija na H, pa je $\left(H, \overline{\theta}\right)$ grupoid. Za taj grupoid kažemo da je **podgrupoid** od (G, θ) .

Ako $\left(H,\overline{\theta}\right)$ ima odgovarajuća dodatna svojstva, govorimo o potpolugrupi, odnosno podmonoidu, odnosno podgrupi polazne strukture (G,θ).

Kraće: Neka je $(G,\circ)$ grupoid i $H\subseteq G$. Kažemo da je skup H **zatvoren** s obzirom na operaciju $\circ$, ako za sve $a,b\in H$ vrijedi $a\circ b\in H$. U tom slučaju je $(H,\circ)$ grupoid s obzirom na operaciju $\circ$ *naslijeđenu* iz G.

Primjer 3.9

- Kako je grupoid $(\mathbb{Z},+)$ i $\mathbb{N}\subset\mathbb{Z}$, tada možemo smatrati da je $(\mathbb{N},+)$ grupoid s obzirom na operaciju $+$ naslijeđenu iz $\mathbb{Z}$;
- Kako je grupoid $(\mathbb{R},\cdot)$ i $\mathbb{Q}\subset\mathbb{R}$, tada $(\mathbb{Q},\cdot)$ možemo smatrati da je $\mathbb{Q}$ grupoid s obzirom na operaciju $\cdot$ naslijeđenu iz $\mathbb{R}$;

Primjer 3.10

- Polugrupa $(\mathbb{N},+)$ je potpolugrupa monoida $(\mathbb{N}_0,+)$;
- Monoid $(\mathbb{Z},\cdot)$ je podmonoid monoida $(\mathbb{Q},\cdot)$;

Specijalno: Neka je $(G, \circ)$ grupa, a $H \subseteq G$ podskup, koji je zatvoren u G s obzirom na množenje u grupi. Ako je podgrupoid $(H, \circ)$ grupa, onda kažemo da je to **podgrupa** od $(G, \circ)$ i pišemo $H < G$.

Primjer 3.11

- Grupa $(2\mathbb{Z}, +)$ je podgrupa grupe $(\mathbb{Z}, +)$;
- Grupa $(B(S), \circ)$ je podgrupa monoida $\left(S^S, \circ\right)$ (uz oznake od prije);
- Neka je $\mathbb{R}^+ = \{x \in \mathbb{R} \,|\, x > 0\}$. Onda je $\mathbb{R}^+ \subset \mathbb{R}$ i $(\mathbb{R}^+, \cdot)$ nije podgrupa grupe $(\mathbb{R}, +)$, jer se ne radi o istoj binarnoj operaciji.

Napomena: Svaka grupa ima podgrupe. Trivijalne podgrupe su $H = \{e\}$ i $H = G$. Ostale podgrupe od G nazivamo **prave podgrupe**. Može se pokazati da svaka beskonačna grupa ima sigurno pravih podgrupa, dok kod konačnih grupa to ne mora biti (npr. ako je red grupe prost broj).

Teorem 3.1 *Neprazan podskup $H \subseteq G$ grupe G je podgrupa od G ako i samo ako su ispunjeni sljedeći uvjeti:*

i) *za svaki $a, b \in H$ je $ab \in H$;*

ii) *za svaki $a \in H$ je $a^{-1} \in H$.*

Dokaz:

Gornja dva uvjeta možemo objediniti:

Teorem 3.2 *Neprazan podskup $H \subseteq G$ grupe G je podgrupa od G onda i samo onda ako je za svaki izbor $a, b \in H$ je $ab^{-1} \in H$.*

Dokaz:

Teorem 3.3 *Neka su $H_1, H_2 < G$ podgrupe od G . Onda je $H_1 \cap H_2$ također podgrupa od G.*

Dokaz:

Slično se vidi da je presjek bilo koje familije, konačne ili beskonačne, podgrupa od G opet podgrupa od G. Točnije, ako je I neki skup indeksa i $H_i < G$ podgrupa od G za svaki $i \in I$, onda je

$$\bigcap_{i \in I} H_i$$

podgrupa od G.

Ciklička grupa. Neka je $(G, \cdot)$ grupa. Ako je svaki $x \in G$ oblika

$$x = a^m, \ m \in \mathbb{Z}.$$

za neki $a \in G$, onda kažemo da je grupa G **ciklička**, tj. generirana jedinim elementom (kojeg nazivamo **generator** te grupe). Pišemo $G = \langle a \rangle$. Dakle,

$$\langle a \rangle = \{a^m : m \in \mathbb{Z}\}.$$

Ako je a beskonačnog reda, grupa $\langle a \rangle$ je nužno beskonačna, i nazivamo je **beskonačna ciklička grupa**. Ako je pak generator a reda n, onda je $\langle a \rangle$ konačna grupa i ima točno n elemenata, pa govorimo o **cikličkoj grupi reda** n.

Primjer 3.12 $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +_m)$ su cikličke grupe, obje generirane s elementom 1. Prva od njih je beskonačna, a druga konačna reda n.

Neka je sada G bilo koja grupa i $a \in G$ njezin element. Neka je $H = \langle a \rangle \subseteq G$. Tada je H podgrupa od G koju nazivamo **ciklička podgrupa** od G generirana s a.

3.7 Grupe permutacija. Simetrična grupa.

- Grupe permutacija igraju istaknutu ulogu u teoriji grupa, jer su njima u izvjesnom smislu reprezentirane sve moguće apstraktne grupe.

Neka je S skup i

$$B(S) = \{f : S \to S \,|\, f \text{ je bijekcija}\} \subset S^s.$$

Teorem 3.4 *Skup $B(S)$ je grupa u odnosu na kompoziciju kao binarnu operaciju.*

Dokaz:

Uočimo: Grupa $B(S)$ nekomutativna, čim S ima više od dva elementa.

Kako svaku bijekciju $f : S \rightarrow S$ nazivamo **permutacija** skupa S, tada grupu $B\left(S\right)$ nazivamo **grupa permutacija** skupa S. Također i podgrupe od $B(S)$ nazivamo grupama permutacija.

Pretpostavimo nadalje da je S **konačan skup**.

- Primijetimo da je onda preslikavanje $p : S \rightarrow S$ surjektivno, ako i samo ako je injektivno. Prema tome, svaki od tih zahtjeva je ekvivalentan činjenici da je p permutacija skupa S.
- Ako skup S ima n elemenata, možemo bez gubitka općenitosti umjesto

  $$S = \{a_1, a_2, ..., a_n\}$$

  jednostavnije pisati

  $$S = \{1, 2, ..., n\},$$

  shvaćajući te brojeve samo kao oznake, indekse elemenata iz S.

- U tom slučaju možemo permutaciju p zapisati tablično

i	1	2	$\ldots$	n
$p(i)$	$p(1)$	$p(2)$	$\ldots$	$p(n)$

odnosno (u skladu s tradicijom) kao

$$p = \begin{pmatrix} 1 & 2 & \ldots & n \\ p(1) & p(2) & \ldots & p(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix} = \begin{pmatrix} i \\ p_i \end{pmatrix}.$$

gdje su u prvom redu popisani elementi domene, a u drugom odgovarajuće vrijednosti funkcije p.

- U ovim oznakama grupovna operacija, tj. komponiranje permutacija obavlja vrlo jednostavno

$$q \circ p = \begin{pmatrix} 1 & 2 & \ldots & n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix} = \begin{pmatrix} p_1 & p_2 & \ldots & p_n \\ q(p_1) & q(p_2) & \ldots & q(p_n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \ldots & n \\ q(p_1) & q(p_2) & \ldots & q(p_n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ (q \circ p)(1) & (q \circ p)(2) & \ldots & (q \circ p)(n) \end{pmatrix} = \begin{pmatrix} i \\ (q \circ p)(i) \end{pmatrix}$$

- Identična permutacija (neutralni element!) zapisuje se kao

$$e = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

dok je inverz permutacije p u ovoj oznaci dan s

$$p^{-1} = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ 1 & 2 & ... & n \end{pmatrix}.$$

Grupu permutacija skupa $\{1, ..., n\}$ označavamo obično s

$$B(\{1, ..., n\}) = S_n$$

i nazivamo je **simetrična grupa stupnja** n.

Primjer 3.13 Neka je $S = \{1, 2, 3\}$. Tada je identična permutacija (neutralni element!)

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

Npr. imamo:

$$q \circ p = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

i

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \implies p^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

jer je

$$p^{-1} \circ p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$$p \circ p^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Propozicija 3.10 *Grupa S_n je reda $n!$, tj. ima $n!$ elemenata.*

Dokaz: Indukcijom.

Primjer 3.14 Grupa $(S_3, \circ)$ ima $|S_3| = 3! = 6$ elemenata:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Neka je $p \in S_n$ permutacija sa svojstvom da postoje međusobno različiti prirodni brojevi $i_1, i_2, ..., i_d \in \{1, 2, ..., n\}$ takvi da je

$$p(i_1) = i_2,\ p(i_2) = i_3, ..., p(i_d) = i_1$$

dok za ostale elemente iz $\{1, 2, ..., n\}$ vrijedi $p(j) = j$, $j \neq i_1, i_2, ..., i_d$. Dakle,

$$p = \begin{pmatrix} i_1 & i_2 & ... & i_{d-1} & i_d & i_{d+1} & ... & i_n \\ i_2 & i_3 & ... & i_d & i_1 & i_{d+1} & ... & i_n \end{pmatrix}$$

Kraće pišemo

$$p = \begin{pmatrix} i_1 & i_2 & ... & i_{d-1} & i_d \end{pmatrix}$$

i kažemo da je p **ciklička permutacija** ili **ciklus** duljine d.

- Svaki ciklus duljine 1 je identična permutacija e.
- Svaki ciklus duljine 2 nazivamo **transpozicija**.

Primjer 3.15 Imamo u S_6 :

$$(3) = \begin{pmatrix} 3 & 1 & 2 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e,$$

$$\begin{pmatrix} 1 & 3 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 6 & 2 & 4 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix}$$

je ciklus duljine 4, a

$$\begin{pmatrix} 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 3 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix}$$

je jedna transpozicija u S_6.

Može se pokazati da vrijedi:

- Permutacija ne mora biti ciklus, ali se uvijek može prikazati kao produkt disjunktnih ciklusa, tj. ciklusa koji ne sadrže isti prirodni broj. Npr. u S_6 je

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 6 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$$

- Svaka se permutacija može prikazati kao produkt transpozicija. Npr. u S_6 je

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}.$$

Alternirajuća grupa. Neka je dana permutacija $p \in S_n$. Svaki slučaj kad u toj permutaciji vrijedi

$$i < j \quad \text{i} \quad p(i) > p(j)$$

nazivamo **inverzija** u permutaciji p. Neka je s $I(p)$ označen ukupan broj inverzija u permutaciji p. Onda preslikavanje

$$sgn : S_n \to \{1, -1\}$$

definirano s

$$sgn(p) = (-1)^{I(p)}$$

nazivamio **parnost** ili **paritet** permutacije.

Permutaciju za koju je $sgn(p) = 1$ nazivamo **parna**, a onu za koju je $sgn(p) = -1$ **neparna**.

- Identična permutacija e je uvijek parna budući je $I(e) = 0$;

Primjer 3.16 Neka je u S_3

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{i} \quad q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Tada je

$$I(p) \;=\; 2 \Longrightarrow sgn(p) = (-1)^2 = 1 \Longrightarrow \; p \text{ je parna}$$
$$I(q) \;=\; 3 \Longrightarrow sgn(q) = (-1)^3 = -1 \Longrightarrow \; q \text{ je neparna}$$

Propozicija 3.11 *Preslikavanje* $sgn : S_n \to \{1, -1\}$ *ima ova svojstva:*

i) $sgn\,(q \circ p) = sgn\,(q) \cdot sgn\,(q)\,;$

ii) $sgn\left(p^{-1}\right) = sgn\,(p)\,,$

za sve $q, p \in S_n$.

Dokaz:

Neka je sada s A_n označen skup svih parnih permutacija u S_n. Kako je $e \in A_n$, onda je $A_n \neq \emptyset$. Štoviše vrijedi:

Teorem 3.5 *Skup* $A_n \subset S_n$ *je podgrupa od* S_n.

Dokaz:

Propozicija 3.12 *Ako je* $n > 1$*, broj parnih permutacija u* S_n *jednak je broju neparnih permutacija.*

Dokaz:

Posljedica 3.2 Uz $n > 1$ alternirnjuća grupa A_n je reda $n!/2$, tj. ima $n!/2$ elemenata.

Dokaz: