2. ALGEBARSKE STRUKTURE

2.1. Polugrupe i grupe

DEFINICIJA: $X \neq \emptyset$

$\alpha : X \times X \to X$ - binarna operacija

$(x, y) \to \alpha(x, y)$

Umjesto oznake $\alpha(x, y)$ koriste se oznake:

$x \circ y, \ x + y, \ x \cdot y, \ xy$

oduzimanje - nije binarna operacija na skupu prirodnih brojeva

→ Binarna operacija je asocijativna ako vrijedi

$$x \circ (y \circ z) = (x \circ y) \circ z \quad \forall x, y, z \in X$$

Skup X s asocijativnom binarnom operacijom zove se polugrupa

Primjer 2.1. (1) $S \neq \emptyset$

$F = \{f : S \to S\}$

$f, g \in F$

$f \circ g$ → kompozicija $\Rightarrow$ $(F, \circ)$ polugrupa

(2) $(\mathbb{R}, +)$ polugrupa

zatvorenost? $x, y \in \mathbb{R}$ $\quad x + y \in \mathbb{R}$ ✓

$(\mathbb{R}, \cdot)$ polugrupa

zatvorenost? DA

$(\mathbb{R}^+, \cdot)$ polugrupa

↳ pozitivni realni brojevi

$(\mathbb{R}^-, \cdot)$ nije polugrupa → umnožak dva negativna broja je pozitivni broj

DEFINICIJA $(X, \circ)$, $(Y, \cdot)$ polugrupe

Homomorfizam polugrupa je preslikavanje

$f: X \to Y$ za koje vrijedi

$$f(x \circ y) = f(x) \cdot f(y), \quad \forall x, y \in X$$

$\boxed{\text{Pr. 2.1}}$ (nastavak)

$(\mathbb{R}^+, \cdot)$, $(\mathbb{R}, +)$

$f: \mathbb{R}^+ \to \mathbb{R}$ $\quad f(x) = \ln x$ je hom. polugrupa

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

primjer $(M_n, +)$, $(M_n, \cdot)$ polugrupe

$\hookrightarrow$ matrica reda n

$(M_n, \cdot)$, $(\mathbb{R}, \cdot)$

preslikavanje: $f: M_n \to \mathbb{R}$

$$f(A, B) = f(A) \cdot f(B)$$

množenje matrica $\qquad$ $\hookrightarrow$ množenje realnih brojeva

$f \to$ determinanta $\Rightarrow$ hom. polugrupa

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

DEFINICIJA 2.2. $(X, \cdot)$ polugrupa

neutralni element ili jedinica je element $e \in X$ takav da je : $x \cdot e = e \cdot x = x \quad \forall x \in X$

polugrupa u kojoj postoji neutralni element - monoid

$\boxed{\text{Pr. 2.2.}}$ Primjeri monoida

(1) $(\mathbb{N}, +)$ nije monoid

$(\mathbb{N} \cup \{0\}, +)$ monoid

(2) $(\mathbb{N}, \cdot)$ monoid

↳ neutralni element 1

(3) $(M_n, +)$ monoid

↳ neutralni element nul matrica

$(M_n, \cdot)$ monoid

↳ neutralni element jedinična matrica

PROPOZICIJA 2.1. Ako u polugrupi $(X, \cdot)$ postoji neutralni element, onda je on jedinstven

DOKAZ: pretp. da postoje dva neutralna elementa (e, e')

$$\left.\begin{array}{ll} ex = xe = x \quad \forall x \in X & \rightarrow e \cdot e' = e'e = e' \\ e'x = xe' = x \quad \forall x \in X & \rightarrow e' \cdot e = e \cdot e' = e \end{array}\right\} e = e'$$

DEFINICIJA 2.3. Monoid X je grupa ako $\forall x \in X \ \exists y \in X$ takav da je $xy = yx = e$

y - inverzni element $\rightarrow y = x^{-1}$

$\rightarrow$ zbrajanje $\rightarrow x$

↳ inverz $-x$

$(\mathbb{N}, \cdot)$ nije grupa

↳ da postane grupa $\Rightarrow (\mathbb{Q}, \cdot) \rightarrow (\mathbb{Q} \setminus \{0\}, \cdot)$

problem s nulom

$(\mathbb{N}, +)$ - nije grupa $(\mathbb{Z}, +)$ - grupa

PROPOZICIJA 2.2. $(X, \cdot)$ monoid te $x \in X$

ako je x invertibilan, onda je njegov inverz jedinstven

DOKAZ: $\exists x', x''$

$x \cdot x' = x' \cdot x = e$

$x \cdot x'' = x'' \cdot x = e$

$$\left.\begin{array}{l} \underbrace{(x'' \cdot x)}_{e} \cdot x' = e \cdot x' = x' \\ x''\underbrace{(x \cdot x')}_{e} = x'' \cdot e = x'' \end{array}\right\} x' = x''$$

TEOREM 2.3. $(X, \cdot)$ grupa tada $\forall a, b \in X$

$ax = b$ i $ya = b$ imaju jedinstveno rješenje

DOKAZ $ax = b \quad / \cdot a^{-1}$

$$(a^{-1} \cdot a) \cdot x = a^{-1} b$$

$$e \cdot x = a^{-1} b$$

$$x = a^{-1} b$$

provjera: $a(a^{-1} b)$

$$= (aa^{-1}) b = eb = b$$

$\boxed{\text{Primjer 2.3}}$ $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$
grupa s obzirom na množenje

DOKAZ: zatvorenost $a + b\sqrt{2} \in G$
$c + d\sqrt{2} \in G$

$$\underbrace{(a + b\sqrt{2})}_{\neq 0}\underbrace{(c + d\sqrt{2})}_{\neq 0} = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$$

$$= \underbrace{(ac + 2bd)}_{\in \mathbb{Q}} + \underbrace{(ad + bc)}_{\in \mathbb{Q}}\sqrt{2} \in G$$

$\rightarrow$ nije $\emptyset$

asocijativnost – nasljeđuje se zbog svojstva realnih brojeva

neutralni element $\rightarrow$ $1 = 1 + 0\sqrt{2} \in G$

$\longrightarrow$

primjer (nastavak)

inverzni element od $a+b\sqrt{2} \in G$

$$a+b\sqrt{2}=x$$

$$x^{-1}=\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}}$$

$$=\frac{a-b\sqrt{2}}{a^2-2b^2}=\underbrace{\frac{a}{a^2-2b^2}}_{\in\mathbb{Q}}+\underbrace{\frac{-b}{a^2-2b^2}}_{\in\mathbb{Q}}\cdot\sqrt{2}$$

$$a^2-2b^2=0$$

$$a^2=2b^2$$

$$\frac{a^2}{b^2}=2 \Rightarrow \underbrace{\frac{a}{b}}_{\mathbb{Q}}=\underbrace{\pm\sqrt{2}}_{\not\in\mathbb{Q}}$$

kontradikcija

$\boxed{\text{zadatak}}$ Na skupu R definirana je binarna operacija $*$ na sljedeći način

$$x*y=\sqrt[3]{x^3+y^3}, \quad x,y\in R$$

dokažite da je $(R,*)$ grupa

zatvorenost : $x,y\in R \quad x*y=\sqrt[3]{x^3+y^3}\in\mathbb{R}$

asocijativnost: $(x*y)*z$ i $x*(y*z)$

$$(x*y)*z=\left(\sqrt[3]{x^3+y^3}*z\right)=\sqrt[3]{x^3+y^3+z^3}$$

$$x*(y*z)=x*\left(\sqrt[3]{y^3+z^3}\right)=\sqrt[3]{x^3+y^3+z^3}$$

neutralni element

$$x*e=e*x=x$$

$$x*e=\sqrt[3]{x^3+e^3}=x \;/^3$$

$$x^3+e^3=x^3 \Rightarrow e^3=0 \Rightarrow e=0$$

inverz $x\in\mathbb{R}$ $\quad x*y=0$

$$\sqrt[3]{x^3+y^3}=0 \rightarrow x^3+y^3=0 \rightarrow y^3=-x^3 \rightarrow y=-x$$

PRIMJER 2.4. $n \in \mathbb{N}$

Dokažimo da je K_n skup svih kompleksnih brojeva

$$K_n = \{ z \in \mathbb{C} , z^n = 1 \}$$ grupa

s obzirom na množenje kompleksnih brojeva

zatvorenost → $z_1 \in K_n$, $z_2 \in K_n$ $\quad z_1 \cdot z_2 \in K_n$

$$(z_1 \cdot z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1$$

asocijativnost → nasljeđuje se iz $\mathbb{C}$

neutralni element → $1 \in K_n$

inverz $\quad z \in K_n \to \frac{1}{z}$

$$\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = \frac{1}{1} = 1 \quad \to \left(\frac{1}{z}\right) \in K_n \quad z \neq 0$$

DEFINICIJA 2.4. Grupa $(X, \cdot)$ je komutativna ili Abelova ako je $x \cdot y = y \cdot x \quad \forall x, y \in X$

primjer 2.4 - abelova

zadatak - abelova

primjer 2.3 - abelova

množenje matrica – nije abelova

PRIMJER 2.5. $m \in \mathbb{N}$, $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$

definiramo binarnu operaciju $+_m$ na $\mathbb{Z}_m$

$x, y \in \mathbb{Z}_m \qquad x + y = q m + r, \; q \in \mathbb{Z}, \; r \in \mathbb{Z}_m$

$$x +_m y = r$$

Dokazati da je $(\mathbb{Z}_m, +_m)$ abelova grupa

zatvorenost $x, y \in \mathbb{Z}_m \quad x +_m y \in \mathbb{Z}_m$

ispunjeno po definiciji

asocijativnost $x +_m y = r$

$$(x +_m y) +_m z = s$$

$$y +_m z = t$$

$\exists\, k, l, p$ t.d. je $x + y = km + r$

$$r + z = lm + s$$

$$y + z = pm + t$$

$$x + t = x - pm + pm + t = -pm + x + y + z = -pm + km + r + z$$

$$= -pm + km + lm + s = (-p + k + l)m + s$$

$$x +_m (y +_m z) = x +_m t = s = (x +_m y) +_m z$$

neutralni element $\rightarrow \emptyset$

inverz od $k \rightarrow k +_m x = 0$

$$x = m - k$$

komutativnost $\rightarrow$ trivijalno (komutativnost zbrajanja)

$\Rightarrow$ Abelova grupa

$\boxed{\text{Primjer 2.6.}}$ $\mathbb{Z}_m \setminus \{0\}$ definiramo operaciju $\cdot_m$

$$x \cdot y = gm + r \quad , g \in \mathbb{Z}, \ r \in \mathbb{Z}_m$$

$$x \cdot_m y = r$$

$(\mathbb{Z}_m \setminus \{0\}, \cdot_m)$ je grupa $\Leftrightarrow$ m prost

$\mathbb{Z}_6 \setminus \{0\} = \{1, 2, 3, 4, 5\}$

$2 \cdot_6 3 = 0$ $\rightarrow$ nije zatvoreno

$\hookrightarrow$ 2 puta 3 modulo 6

ako je m prost onda imamo zatvorenost

- asocijativnost
- neutralni element $\rightarrow 1$
- inverz : $a \in \mathbb{Z}_m \setminus \{0\}$

$nzd(a, m) = 1$ jer je m prost

$\exists u, v$

$$au + mv = 1$$

$$a(u + tm) + m(v - ta) = 1 \qquad t \in \mathbb{Z}$$

$$z = u + tm \in \mathbb{Z}_m$$

$a \cdot_m z = 1$ tj. $z = a^{-1}$

abelova grupa

$(\mathbb{Z}_5 \setminus \{0\}, \cdot_5)$ tablica množenja:

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m : nzd(a,m) = 1\}$ - grupa

$(\mathbb{Z}_m^*, \cdot)$ - grupa

ako je p prost:

$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

PROPOZICIJA 2.4

X, Y grupe s neutralnim elementima e_x i e_y

$f: X \to Y$ homomorfizam, tada vrijedi:

(1) $f(e_x) = e_y$

(2) $f(x^{-1}) = (f(x))^{-1}, \ \forall x \in X$

<u>DOKAZ</u>:

(1) $f(e_x) = f(e_x \cdot e_x) = f(e_x) \cdot f(e_x) \quad / \cdot (f(e_x))^{-1}$

$$f(e_x) \cdot (f(e_x))^{-1} = f(e_x) \cdot \underbrace{f(e_x) \cdot (f(e_x))^{-1}}_{e_y}$$

$$e_y = f(e_x) \cdot e_y$$

$$e_y = f(e_x)$$

(2) $f(e_x) = f(x\, x^{-1}) = f(x) \cdot f(x^{-1}) = e_y$

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

$f(x^{-1}) = (f(x))^{-1}$

$\boxed{\text{PRIMJER 2.7.}}$ $S \neq \emptyset$

$$B(S) = \{ f : S \to S,\ f \text{ bijekcija} \}$$

$(B(S), \circ)$ grupa

$\circ \longrightarrow$ kompozicija

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

$B(S) = S_n$

$k(S_n) = n!$ – simetrična grupa reda n ili grupa permutacija

$$f \quad \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

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

$\downarrow$

$3! = 6$

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

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

$1 \to 3 \Rightarrow 3 \to 3$

svaka permutacija se može prikazati kao produkt disjunktnih ciklusa $(i_1, i_2, \ldots, i_r)$

tj. $f(i_1) = i_2$, $f(i_2) = i_3$, $\ldots$ $f(i_{r-1}) = i_r$, $f(i_r) = i_1$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 8 & 1 & 6 & 7 & 4 \end{pmatrix} = (1\,3\,2\,5)\,(4\,8)\,\cancel{(6)}\,\cancel{(7)}$$

$$= \underbrace{(1\,3\,2\,5)}_{\text{permutacija}}\ \underbrace{(4\,8)}_{\text{permutacija}}$$

ostali su fiksni   ostali su fiksni

$1 \to 3$ $\quad 4 \to 8 \quad 6 \to 6 \quad 7 \to 7$

$3 \to 2$ $\quad 8 \to 4$

$2 \to 5$

$5 \to 1$

disjunktni ciklusi KOMUTIRAJU !!!

$$(1\,3\,2\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 4 & 1 & 6 & 7 & 8 \end{pmatrix}$$

ciklus duljine 2 – transpozicija

svaka permutacija je produkt transpozicija

$$(i_1 i_2, \dots, i_r) = (i_1 i_2)(i_2 i_3) \cdots (i_{r-1} i_r)$$

rastav na transpozicije nije jedinstven ali broj transpozicija je uvijek iste parnosti

definira se parnost permutacije

$(1\ 3\ 2\ 5)$

$(1\ 3)\ (3\ 2)\ (2\ 5)\ (4\ 8) \to$ parna permutacija

Simetrična grupa S_n, $n \geq 3$ nije abelova

$\boxed{\text{Pr. 2.8.}}$ Komutativne grupe:

(1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$;

(2) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$; $X^* = X \setminus \{0\}$

DEFINICIJA 2.5. X grupa $Y \subseteq X$ t.d. je

$$y^{-1} \in Y \; , \; y \in Y$$

$$y \cdot y^{-1} \in Y \quad \forall \, y, y' \in Y$$

tada je Y podgrupa od X

$Y \leq X$

$a, b \in Y$

Kriterij za podgrupu

$Y \leq X$ ako $\forall a, b \in Y$ vrijedi $ab^{-1} \in Y$

DEFINICIJA 2.6. X grupa

$S \subseteq X$

presjek svih podgrupa od X koji sadrže skup S je podgrupa od X koja se naziva podgrupa generirana skupom S

To je najmanja podgrupa od X koja sadrži S

$X(S)$

Pr. 2.4. $K_n = \{ z \in \mathbb{C}, \, z^n = 1 \}$

$(K_n, \cdot) \leq (\mathbb{C}^*, \cdot)$

$a, b \in K_n \qquad ab^{-1} \in K_n$

$(ab^{-1})^n = a^n (b^n)^{-1} = 1 \cdot 1^{-1} = 1$

Pr. 2.3. Podgrupa od $(\mathbb{R}^*, \cdot)$

$\boxed{\text{Pr. 2. 9.}}$ a) $(\mathbb{Z}, +)$ grupa

$S = \{1\}$

$Y \subseteq \mathbb{Z}$

$S \subseteq Y$

$1 \in Y \Rightarrow 1+1 \in Y \to 2 \in Y \Rightarrow$

1+1 mora biti u tom skupu

$1+2 \in Y \to 3 \in Y$

↳ svi prirodni brojevi $\mathbb{N} \subset Y$

$\Rightarrow 0 \in Y$

cijeli skup $\mathbb{Z}$ mora biti unutra

$\Rightarrow Y = \mathbb{Z}$

$(\mathbb{Z}, +)$ – generiran samo jednim elementom 1

$100 = 1+1+1+\dots$

$-50 = -1+(-1)+(-1)+\dots$ inverzom generirano

↳ $-1, 1$ generatori za $\mathbb{Z}$

b) $G = \{1, -1\}$

generator → (-1)

1 nije generator!

$(-1)(-1)(-1) = -1$

$(-1)(-1) = 1$

↳ samo sa (-1) možemo dobiti sve brojeve u skupu G

DEFINICIJA 2.7. Grupa generirana s jednim elementom

↳ ciklička grupa

Primjer 2.10. a) $(\mathbb{Z}, +)$ ciklička

generatori → $-1, 1$

b) $(\mathbb{Z}_m, +_m)$ ciklička

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

↳ 1 je generator, 5 je generator $(5+5=4)$

$2+2+2=0$
$2+2+2+2=2$ 2 nije generator

generator je svaki element $a \in \mathbb{Z}_m \to (a, m) = 1$

c) $(\mathbb{Z}_p^*, \cdot_p)$ ciklička

p-prost

generator je svaki primitivni korijen modulo p

DEFINICIJA 2.8. X grupa, $Y \leq X$, $a \in X$

red podgrupe $Y \to k(Y)$

red elemenata a je red podgrupe $X(a)$ generirane elementom a

najmanji prirodan broj r (ako postoji):

$a^r = e$

↳ neutralni element u X

$\boxed{\text{Pr. 2.11.}}$ a) odredi red elemenata 6 u grupi $(\mathbb{Z}_7, +_7)$

$6x \equiv 0 \pmod 7$ $(6,7) = 1$

$\hookrightarrow$ 1 rješenje

$x = 7$

b) red od 6 u grupi $(\mathbb{Z}_9, +_9)$

$6x \equiv 0 \pmod 9$ $/ :3$ $(6,3) = 3$

$2x \equiv 0 \pmod 3$

$\hookrightarrow x \equiv 0 \pmod 3$

tj. $x = 3$

c) 6 grupa $(\mathbb{Z}_{10}, +_{10})$

$6x \equiv 0 \pmod{10}$ $/ :2$ $(6,10) = 2$

$3x \equiv 0 \pmod 5$

$x = 5$

$\boxed{\text{Pr. 2.12.}}$ $(\mathbb{Z}^*_{20}, \cdot_{20})$ nije ciklička

$\mathbb{Z}^*_{20} \rightarrow$ relativno prosti sa 20

$\mathbb{Z}^*_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\varphi(20) = 8$

$3 \rightarrow$ $3^2 = 9 \pmod{20}$

$3^3 = 7 \pmod{20}$

$3^4 \equiv 1 \pmod{20}$

podgrupa generirana sa 3 $\rightarrow$ $X(3) = \{\underset{3^1}{3}, \underset{3^2}{9}, \underset{3^3}{7}, \underset{3^4}{1}\}$

$\hookrightarrow 3^5 \rightarrow 3,\ 3^6 \rightarrow 9, \ldots$

$\searrow$

$g^1 = g$

$g^2 = 1$ $\quad X(g) = \{1, g\}$

ne možemo pokupiti sve elemente!

grupa nije ciklička!