Grupoid, grupa, prsten i polje

19. septembar 2023

Neka je G neprazan skup i $* : G^2 \to G$, tj. $*$ je funkcija koja svakom uređenom paru $(a, b) \in G^2$ dodeljuje element $c \in G$ pri čemu je $c = *(a, b)$. Tako definisano preslikavanje naziva se *binarna operacija na skupu G*.

Umesto $c = *(a, b)$ uobičajeno je da se koristi oznaka $c = a * b$ i kaže se da je *skup G snabdeven operacijom $*$.*

Na skupu prirodnih brojeva $\mathbb{N}$ sabiranje $+$ jeste binarna operacija, jer je zbir dva prirodna broja prirodan broj, dok oduzimanje $-$ nije binarna operacija na skupu prirodnih brojeva, jer npr. $6 - 17 \notin \mathbb{N}$.

Ako se umesto skupa prirodnih brojeva $\mathbb{N}$ posmatra na primer skup celih brojeva $\mathbb{Z}$ onda su i sabiranje i oduzimanje binarne operacije na skupu $\mathbb{Z}$.

$(G, *)$, gde je $*$ binarna operacija na skupu G, naziva se *grupoid*.

Grupoid $(G, *)$ je *asocijativan* ako za svako $a, b, c \in G$ važi

$$a * (b * c) = (a * b) * c.$$

Grupoid $(G, *)$ je *komutativan* ako za svako $a, b \in G$ važi

$$a * b = b * a.$$

Ako postoji element $e \in G$ takav da je za svako $a \in G$

$$a * e = e * a = a$$

kaže se da grupoid $(G, *)$ ima *neutralni element* e.

Ako u grupoidu $(G, *)$ postoji neutralni element e i ako za $a \in G$ postoji $a^{-1} \in G$ takav da je

$$a * a^{-1} = a^{-1} * a = e$$

kaže se da je a^{-1} *inverzni element* za element a u odnosu na binarnu operaciju $*$.

Ako je grupoid $(G, *)$ asocijativan, onda nema potrebe za korišćenjem zagrada, tj. redosled izvršavanja operacija ne utiče na rezultat, tako da

$$a * (b * c) = (a * b) * c = a * b * c.$$

Ako u grupoidu $(G, *)$ postoji neutralni element onda je on jedinstven. Ako za element $a \in G$ postoji inverzni element a^{-1} on je takođe jedinstven.

Ako je $(G, *)$ grupoid i operacija $*$ je asocijativna, onda se algebarska struktura $(G, *)$ naziva *asocijativni grupoid* ili *polugrupa*.

Asocijativni grupoid $(G, *)$ je *grupa* ako u skupu G postoji neutralni element za operaciju $*$ i za svaki element iz G postoji njemu inverzni element u odnosu na operaciju $*$. Ako je pri tome $(G, *)$ komutativni grupoid, grupa $(G, *)$ je *komutativna* ili *Abelova* grupa.

Grupoid, grupa, prsten i polje

$(\mathbb{N}, +)$, gde je sa $+$ označena operacija sabiranja je asocijativni grupoid, dok je $(\mathbb{N}, \cdot)$ gde je sa $\cdot$ označena operacija množenja asocijativni grupoid sa neutralnim elementom $e = 1$.

$(\mathbb{R}, +)$ i $(\mathbb{R} \setminus \{0\}, \cdot)$, gde su sa $+$ i $\cdot$ označene operacije sabiranja i množenja redom su primeri komutativnih grupa.

Neka je posmatrana binarna operacija u skupu G operacija sabiranja $+$. Ako za binarnu operaciju $+$ postoji neutralni element onda se on označava sa 0 i naziva se *nula*. Ako u $(G,+)$ postoji nula i ako za element a postoji inverzni element onda se on naziva *suprotni element* elementa a i označava se sa $-a$. Ako je $(G,+)$ grupa, onda se ona naziva *aditivna* grupa.

Neka je posmatrana binarna operacija u skupu G operacija množenja $\cdot$. Ako za binarnu operaciju $\cdot$ postoji neutralni element onda se on naziva *jedinica*. Ako u $(G,\cdot)$ postoji jedinica i ako za element a postoji inverzni element onda se on označava sa a^{-1}. Ako je $(G,\cdot)$ grupa, onda se ona naziva *multiplikativna* grupa.

Neka su $(G, \bullet)$ i $(H, \star)$ grupe. Funkcija $f : G \to H$ takva da za svako $a, b \in G$ važi

$$f(a \bullet b) = f(a) \star f(b)$$

naziva se *homomorfizam* grupe $(G, \bullet)$ u grupu $(H, \star)$. Bijektivni homomorfizam grupe $(G, \bullet)$ u grupu $(H, \star)$ naziva se *izomorfizam*.
Primer izomorfizma grupe $((0, \infty), \cdot)$ u grupu $(\mathbb{R}, +)$ je funkcija $f(x) = \ln x$.
Neka su binarne operacije $\bullet$ i $\star$ definisane na nepraznom skupu G.
Binarna operacija $\star$ je *distributivna* u odnosu na binarnu operaciju $\bullet$ ako za svako $a, b, c \in G$ važi

$$a \star (b \bullet c) = (a \star b) \bullet (a \star c) \qquad \text{i} \qquad (a \bullet b) \star c = (a \star c) \bullet (b \star c).$$

U skupu realnih brojeva operacija množenja $\cdot$ je distributivna u odnosu na operaciju sabiranja $+$, dok obrnuto nije tačno, tj. operacija sabiranja $+$ nije distributivna u odnosu na operaciju množenja $\cdot$.

$(G, \bullet, \star)$ naziva se *prsten* ako je $(G, \bullet)$ komutativna grupa, operacija $\star$ je asocijativna i operacija $\star$ je distributivna u odnosu na binarnu operaciju $\bullet$.

$(G, \bullet, \star)$ je *polje* ako je $(G, \bullet, \star)$ prsten i $(G \setminus \{e\}, \star)$ komutativna grupa, gde je e neutralni element za operaciju $\bullet$.

Na primer, $(\mathbb{Z}, +, \cdot)$, gde je $\mathbb{Z}$ skup celih brojeva, je prsten, a $(\mathbb{Q}, +, \cdot)$ i $(\mathbb{R}, +, \cdot)$ gde su $\mathbb{Q}$ i $\mathbb{R}$ skupovi racionalnih i realnih brojeva, redom, su polja, a $+$ i $\cdot$ su operacije sabiranja i množenja. $(\mathbb{Z}, +, \cdot)$ nije polje jer npr. za $k \in \mathbb{Z} \setminus \{0, \pm 1\}$ ne postoji $k^{-1} \in \mathbb{Z} \setminus \{0\}$ takvo da je $k \cdot k^{-1} = 1$.