Javorina Stojanović (Beograd)

NEŠTO IZ TEORIJE GRUPA

Poznati su nam, više ili manje, skupovi brojeva: skup prirodnih brojeva, celih brojeva, racionalnih brojeva i realnih brojeva. Znamo i neka svojstva ovih skupova u odnosu na osnovne računske operacije, kao i svojstva tih operacija u ovim skupovima. Sada ćemo razmatrati neka pitanja koja se postavljaju u vezi s datim skupom M i proizvoljnom operacijom koja je definisana u tom skupu.

Ako su a i b ma koja dva prirodna broja, njihov zbir $a+b$ takođe je prirodan broj. Ovo svojstvo skupa prirodnih brojeva, kao što znamo, naziva se svojstvo zatvorenosti u odnosu na sabiranje i izražava:

$$Ako\ a \in N\ i\ b \in N,\ onda\ a+b \in N.$$

Proizvod ma koja dva prirodna broja takođe je prirodan broj. Znači, skup prirodnih brojeva poseduje svojstvo zatvorenosti i u odnosu na množenje; matematički:

$$Ako\ a \in N\ i\ b \in N,\ onda\ a \cdot b \in N.$$

Ovo je u skladu sa definicijom:

Dati skup M je zatvoren u odnosu na neku operaciju $*$ ako je za svako a, b iz M rezultat $a * b$ definisan i nalazi se kao element u skupu M.

Da li je skup N zatvoren u odnosu na oduzimanje? Kao što znamo, oduzimanje u skupu prirodnih brojeva je definisano samo kada je umanjenik veći od umanjioca. U slučaju kada su a i b elementi skupa N takvi da je $a<b$ razlika $a-b \notin N$. To znači da skup N nije zatvoren u odnosu na oduzimanje.

Skup celih brojeva $C=\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ je zatvoren u odnosu na sabiranje, jer je zbir ma koja dva cela broja takođe ceo broj.

Za skup M koji je zatvoren u odnosu na neku operaciju — kaže se da je *grupoid* u odnosu na tu operaciju.

Tako se, na primer, kaže da je skup C grupoid u odnosu na sabiranje, a da skup N nije grupoid u odnosu na oduzimanje.

Grupoid se može označiti kao uređen par $(M, *)$; na primer:

$$(N,+),\ (C,+),\ (N,\cdot).$$

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

T_1

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

T_2

Tablicom T_1 definisana je operacija $+_7$ (sabiranje po modulu 7). Primećujemo da je za bilo koja dva elementa a i b iz skupa $A=\{0, 1, 2, 3, 4, 5, 6\}$ rezultat $a +_7 b$ takođe elemenat tog skupa. Dakle, skup A je grupoid u odnosu na operaciju $+_7$.

Rezultat $a +_7 b$ za svako a, b iz A određuje se kao ostatak pri deljenju zbira $a+b$ sa 7.

Mada nam sabiranje po modulu 7 izgleda neobično i nepoznato, mi se s njim često srećemo, Ako je danas petak (peti dan u sedmici), posle 6 dana će biti četvrtak (četvrti dan u sedmici). Ovo se saglašava sa $5 +_7 6=4$.

Tablicom T_2 definisana je operacija $\cdot_7$ (moženje po modulu 7).

Rezultat $a \cdot_7 b$ za bilo koja dva elementa a, $b \in A$ određuje se kao ostatak pri deljenju proizvoda $a \cdot b$ sa 7.

Za svaka dva elementa a, b iz A rezultat $a \cdot_7 b \in A$. Prema tome skup A je grupoid i u odnosu na operaciju $\cdot_7$.

Odrediti da li je grupoid u odnosu na množenje skup: a) $A=\{\ldots, -3, -2, -1\}$; b) $B=\{\text{svi parni brojevi}\}$.

Odrediti da li je zatvoren u odnosu na sabiranje skup: a) $M=\{\ldots, -2, -1, 1, 2, \ldots,\}$; b) $P=\{\text{neparni brojevi veći od } 5\}$.

U skupu $S=\{0,1\}$ definisane su operacije $+_2$ i $\cdot_2$ sledećim tablicama:

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Odrediti da li je grupoid uređen par: a) $(\{0, 1\}, +_2)$; b) $(\{0,1\}, \cdot_2)$.

Poznato nam je da za operaciju sabiranje važi zakon asocijacije koji izražavamo ovako:

Za svaka tri broja a, b, c važi: $(a+b)+c=a+(b+c)$.

Za množenje takođe važi zakon asocijacije:

Za svaka tri broja a, b i c važi: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

Konstatovali smo da je $(N,+)$ grupoid, a sada možemo reći da je $(N,+)$ *asocijativni grupoid* ili *polugrupa* jer je operacija $+$ asocijativna u skupu N. Isto tako je i $(N,\cdot)$ polugrupa jer je skup N zatvoren u odnosu na operaciju množenje, a ova operacija je asocijativna u skupu N. Skup C je takođe polugrupa u odnosu na sabiranje i množenje.

Skup C je polugrupa u odnosu na sabiranje jer su istinita oba iskaza:

I Skup C je grupoid u odnosu na operaciju $+$.

II Operacija $+$ je asocijativna u skupu C.

Iz istih razloga je skup C polugrupa i u odnosu na množenje.

Skup celih brojeva je grupoid prema operaciji $-$ ali nije polugrupa, jer ova operacija nije asocijativna:

$$(a-b)-c\neq a-(b-c).$$

Dati skup M je polugrupa u odnosu na operaciju $*$, *tj. kraće* $(M,*)$ *je polugrupa, ako važi:*

I *Skup M je grupoid u odnosu na operaciju* $*$.

II *Operacija* $*$ *je asocijativna u skupu M.*

Da li je skup $B=\{\text{svi racionalni brojevi izuzev } 0\}$ polugrupa prema operaciji deljenje?

Odrediti da li je skup $S=\{0,1\}$ polugrupa: a) u odnosu na operaciju $+_2$; b) u odnosu na operaciju $\cdot_2$.

U vezi sa skupom C i operacijom $+$ setimo se sledećeg:

III Skup C sadrži (elemenat) broj 0 koji je neutralan u odnosu na operaciju $+$. To znači da za svaki broj $a\in C$ važi: $a+0=0+a=a$.

IV Za svaki broj $a\in C$ postoji njemu suprotan (iznverzan) broj $-a\in C$ takav da je: $a+(-a)=0$.

Pošto su istiniti iskazi od I do IV, kaže se da skup C čini *grupu* u odnosu na operaciju $+$.

U skupu C operacija $+$ ima svojstvo komutacije, tj. za svaka dva broja $a, b\in C$ važi $a+b=b+a$.

Zbog toga se kaže da skup C čini *komutativnu grupu* u odnosu na operaciju $+$.

Dati skup M čini grupu u odnosu na operaciju $*$ [kraće $(M, *)$ je grupa] ako su ispunjeni sledeći zahtevi:

Skup M je polugrupa u odnosu na operaciju $*$ (ispunjeni su zahtevi I i II iz definicije polugrupe).

III U skupu M postoji jedan i samo jedan element n takav da za svako $a \in M$ važi: $a * n = n * a = a$.

Elemenat n se naziva neutralni (identični) element u odnosu na operaciju $*$.

IV U skupu M svakom elementu a odgovara jedan i samo jedan element a' takav da je: $a * a' = a' * a = n$.

Element a' naziva se inverzijom od a.

Grupa $(M, *)$ je komutativna ako operacija $*$ ima svojstvo komutacije u skupu M, tj. ako za svako $a, b \in M$ važi: $a * b = b * a$.

$\oplus$	a	v
a	a	a
v	a	v

T_3

Tablica T_3 definiše operaciju $\oplus$ (mešanje) u skupu $T = \{a, v\}$, gde je a alkohol a v — voda. Odrediti da li skup $\{a, v\}$ čini grupu u odnosu na operaciju $\oplus$.

I Skup T je zatvoren u odnosu na operaciju $\oplus$ jer se kao rezultat mešanja uvek dobija element iz T.

II Operacija $\oplus$ je asocijativna u skupu T; na primer:

$$(a \oplus v) \oplus a = a \oplus (v \oplus a).$$

III Skup T sadrži neutralan element u odnosu na operaciju $\oplus$; to je v.

IV Element a nema sebi inverzan element u odnosu na operaciju $\oplus$; ne postoji element iz T koji bi mešanjem sa akloholom dao vodu.

Pošto IV uslov nije ispunjen, skup $\{a, v\}$ nije grupa u odnosu na operaciju $\oplus$.

Da li je skup $A = \{0, 1, 2, 3, 4, 5, 6\}$ grupa u odnosu na operaciju $+_7$?

I Skup A je, kao što smo već konstatovali, grupoid u odnosu na $+_7$.

II Operacija $+_7$ ima svojstvo asocijacije u skupu A; na primer: $(5 +_7 6) +_7 4 = 5 +_7 (6 +_7 4)$.

Slično važi i za ostale slučajeve.

III U skupu A postoji neutralan element u odnosu na operaciju $+_7$, a to je broj 0.

IV U skupu A svakom elementu a odgovara inverzan element a' takav da je: $a +_7 a' = a' +_7 a = 0$.

Ovo se lako zaključuje na osnovu tablice, jer u svakom horizontalnom i svakom vertikalnom redu postoji element 0. Da bismo, na primer, odredili element inverzan broju 4 dovoljno je da u horizontalnom redu koji počinje brojem 4 pronađenmo broj 0 i da onda pročitamo kojim brojem počinje vertikalan red koji sadrži (taj) broj 0. Tako zaključujemo da je izverzija od 4 broj 3 (vidi tablicu T_1).

Na osnovu ovoga možemo reći da skup A čini grupu u odnosu na operaciju $+_7$.

Primetimo još da je operacija $+_7$ komutativna u skupu A; za svako $a, b \in A$ važi: $a +_7 b = b +_7 a$.

Ovo se lako zapaža na osnovu toga što je tablica T_1 simetrična u odnosu na njenu glavnu dijagonalu (onu koja povezuje levi gornji ugao sa desnim donjim uglom tablice).

Prema tome, skup A čini komutativnu (Abelovu) grupu u odnosu na operaciju $+_7$.

Odrediti zašto nije grupa: a) $(0, 1, 2, 3, \ldots ; +)$; b) $(N ; \cdot)$.

Sačini tablicu i pokaži da skup $\{1, 3, 7, 9\}$ čini komutativnu grupu u odnosu na operaiciju $\cdot_{10}$ (množenje po modulu 10). Rezultat $a \cdot_{10} b$ određuje se kao ostatak pri deljenju proizvoda $a \cdot b$ sa 10.

Pokazali smo da je skup C komutativna grupa u odnosu na operaciju $+$ i da je polugrupa u odnosu na operaciju $\cdot$.

Poznato nam je da su ove dve operacije povezane zakonom distribucije množenja prema sabiranju, koji izražavamo:

Za svaka tri broja a, b i c važi: $a(b+c) = ab + ac$.

Na osnovu svega ovoga kaže se da skup C čini *prsten* ili *kolo* u odnosu na operacije $+$ i $\cdot$; kraće: uređena trojka $(C, +, \cdot)$ je prsten ili kolo.

Dati skup M čini prsten ili kolo u odnosu na operacije $*$ i $\ominus$ [$(M, *, \ominus)$ je prsten] ako važe sledeća tvrđenja:

I Skup M je komutativna (Abelova) grupa u odnosu na operaciju $*$.

II Skup M je polugrupa u odnosu na operaciju $\ominus$.

III U skupu M operacija $\ominus$ je distributivna prema operaciji $*$. O redosledu operacija treba voditi računa.

Da li je, $(C, \cdot, +)$ prsten?

I $(C, \cdot)$ nije grupa (nema inverzni element) pa samim tim nije ni komutativna grupa.

III Operacija $+$ nije distributativna u odnosu na operaciju $\cdot$, tj. $a+(b\cdot c)\neq(a+b)\cdot(a+c)$.

Prema tome uređena trojka $(C, \cdot, +)$ nije kolo.

Da li je skup $A=\{0, 1, 2, 3, 4, 5, 6\}$ prsten u odnosu na operacije $+_7$ i $\cdot_7$?

I Poznato je da skup A čini komutativnu grupu u odnosu na operaciju $+_7$.

II Uređen par $(A, \cdot_7)$ je grupoid. Pošto se može utvrditi da je operacija $\cdot_7$ asocijaivna znači da je $(A, \cdot_7)$ polugrupa.

III Može se dokazati da je u skupu A operacija $\cdot_7$ distiributivna u odnosu na $+_7$; na primer $(5+_7 6)\cdot_7 4=(5\cdot_7 4)+_7(6\cdot_7 4)$.

Kako su ispunjena sva tri tvrđenja, kažemo da uređena trojka $(\{0, 1, 2, 3, 4, 5, 6\}, +_7, \cdot_7)$ čini prsten.

Pokazati da je skup $S=\{0,1\}$ prsten u odnosu na operacije $+_2$ i $\cdot_2$.

Ispitajno da li je skup racionalnih brojeva Q prsten u odnosu na operacije $+$ i $\cdot$.

I Skup Q je komutativna grupa u odnosu na operaciju $+$. Zaista:

1. Skup Q je grupoid u odnosu na operaciju $+$.
2. Operacija $+$ je asocijativna u skupu Q.
3. Broj 0 je neutralan element u odnosu na operaciju $+$.
4. Svaki broj q iz skupa Q ima sebi suprotan (inverzan) broj $(-q)$ takav da je $q+(-q)=0$.
5. Operacija $+$ je komutativna u skupu Q.

II Skup Q je polugrupa prema operaciji množenje, jer važi:

1. Skup Q je grupoid u odnosu na operaciju $\cdot$.
2. U skupu Q operacija $\cdot$ je asocijativna.

III U skupu Q operacija $\cdot$ je distributivna prema operaciji $+$.

Prema tome skup racionalnih brojeva čini prsten u odnosu na operacije $+$ i $\cdot$.

Uređen par $(Q,.)$ je polugrupa; ali, da li je možda i grupa? Ispitajmo da li je ispunjen i III i IV zahtev za grupu.

III U skupu Q postoji neutralan (identični) element u odnosu na operaciju množenje. To je, kao što znamo, broj 1. Dakle, za svako $q\in Q$, $q\cdot 1=1\cdot q=1$.

IV Postoji li za svaki broj $q \in Q$ njemu inverzan broj q' takav da je $q \cdot q' = q' \cdot q = 1$?

Na prvi pogled bi se reklo da postoji, jer na primer: broju $\frac{3}{4}$ inverzan broj je $\frac{4}{3}$; broju -5 inverzan je $-\frac{1}{5}$; . . . .

Ali šta je sa brojem 0? Ima li on sebi inverzan broj? Jasno je da inverzija od 0 ne postoji, jer u tom slučaju bi postojao broj a takav da je $a \cdot 0 = 0 \cdot a = 1$ što, naravno, nije tačno.

Iz ovoga sledi da skup racionalnih brojeva nije grupa u odnosu na operaciju $\cdot$ jer 0 nema sebi inverzan element. Međutim, ako se iz skupa Q isključi 0, onda u novom skupu $\{Q \backslash 0\}$ za svaki element postoji njemu inverzan element. Jasno je da ostali zahtevi za grupu koji su važnili u skupu Q važe i u skupu $\{Q \backslash 0\}$. Dakle, skup $\{Q \backslash 0\}$ čini grupu u odnosu na operaciju $\cdot$.

Videli smo da je uređena trojka $(Q, +, \cdot)$ prsten i da je $(\{Q \backslash 0\}, \cdot)$ grupa. Na osnovu ovoga kaže se da skup Q čini *polje* ili *telo* u odnosu na operacije $+$ i $\cdot$.

Dati skup M čini polje ili telo u odnosu na operacije $*$ i $\ominus$ [kraće: uređena trojka $(M, *, \ominus)$ je polje] *ako su ispunjeni sledeći zahtevi*:

I *Uuređena trojka $(M, *, \ominus)$ je prsten.*

II *Uređen par $(\{M \backslash 0\}, \ominus)$ je grupa.*

Ako pogledamo pažljivije sadržaj ovih zahteva, onda možemo reći sledeće:

Dati skup M čini polje ili telo u odnosu na operacije $*$ i $\ominus$ ako važi:

1. Skup M je komutativna grupa u odnosu na operaciju $*$.
2. Skup $\{M \backslash 0\}$ je grupa u odnosu na operaciju $\ominus$.
3. U skupu M operacija $\ominus$ je distributivna prema operaciji $*$.

Da li je skup $A = \{0, 1, 2, 3, 4, 5, 6\}$ polje u odnosu na operacije $+_7$ i $\cdot_7$?

1. Skup A je komutativna grupa u odnosu na operaciju $+_7$ (što smo pokazali ranije).

2. Skup $\{A \backslash 0\}$ čini grupu u odnosu na operaciju $\cdot_7$. Zaista:

I skup $\{A \backslash 0\}$ je grupoid u odnosu na $\cdot_7$.

II U skupu $\{A \backslash 0\}$ operacija $\cdot_7$ je asocijativna.

III U skupu $\{A \backslash 0\}$ postoji jedan i samo jedan element neutralan u odnosu na $\cdot_7$ To je broj 1.

IV U skupu $\{A\backslash 0\}$ svaki element a ima sebi inverzan element a' takav da: $a \cdot_7 a' = a' \cdot_7 a = 1$.

Tako je inverzija od 4 broj 2, jer je $4 \cdot_7 2 = 1$.

3. U skupu A operacija $\cdot_7$ je distributivna prema operaciji $+_7$.

Prema tome uređena trojka $(A, +_7, \cdot_7)$ čini polje.

Pokazati da skup realnih brojeva R čini polje u odnosu na operacije $+$ i $\cdot$.
Pokazati da je uređena trojka $(\{0,1\}, +_2, \cdot_2)$ polje.

Статијата прв пат е објавена во списанието Математички лист на ДМ на Србија