OPERACIJA I ALGEBARSKE STRUKTURE

23. Neka je $S \neq \emptyset$. Tada preslikavanje $f: S \times S \to S$ nazivamo *binarnom operacijom f* u S. Prema definiciji preslikavanja (vidi 14) izlazi:

$$(\forall a, b \in S)(\exists! c \in S) f(a, b) = c,$$

što zapisujemo u obliku $afb = c$, gdje je a *lijevi operand*, b *desni operand*, c *rezultat operacije* sa operatorom f. Skup S sa operacijom f nazivamo *grupoidom* i označavamo sa (S, f).

24. *Grupoid* $(S, \circ)$ naziva se *grupa* ako vrijede osobine:

1° *internost*: $(\forall a, b \in S)(\exists! c \in S)\, a \circ b = c$;

2° *asocijativnost*: $(\forall a, b, c \in S)\, (a \circ b) \circ c = a \circ (b \circ c)$;

3° *egzistencija neutralnog ili jediničnog elementa*:

$$(\exists e \in S)(\forall a \in S)\, e \circ a = a = a \circ e$$

(e se naziva *neutralnim* ili *jediničnim elementom*);

4° egzistencija inverznog (simetričkog) elementa:

$$(\forall a \in S)(\exists \bar{a} \in S)\, a \circ \bar{a} = e = \bar{a} \circ a,$$

gdje je *e jedinični element* u S. Elemenat $\bar{a}$ (označava se sa a^{-1} ili $-a$) naziva se *inverznim* ili *simetričnim elementom* elementa a.
Ako pored osobina 1°–4° u grupi $(S, \circ)$ vrijedi:

5° komutativnost: $(\forall a, b \in S)\, a \circ b = b \circ a$, tada se kaže da je grupa *komutativna* ili *Abelova*.*

Neka je $(T, \circ)$ grupa i $T \subset S$, tada grupu $(T, \circ)$ nazivamo podgrupom grupe $(S, \circ)$.

* Nils Abel (1802–1829), norveški matematičar.

25. *Struktura* $(S, \circ, *)$ gdje su $\circ$ i $*$ dvije binarne interne operacije u S naziva se *prsten* ako je:

1° $(S, \circ)$ Abelova grupa;

2° operacija $*$ je asocijativna;

3° za sve $a, b, c \in S$ vrijedi

$$a * (b \circ c) = (a * b) \circ (a * c);$$

$$(b \circ c) * a = (b * a) \circ (c * a),$$

tj. lijeva i desna distributivnost operacije $*$ prema operaciji $\circ$.

26. Prsten $(S, \circ, *)$ je *tijelo* ako je $(S \setminus \{0\}, *)$ grupa, gdje je 0 neutralni element za operaciju $\circ$.

27. *Komutativno tijelo* je *polje*.
Uobičajene su oznake $(G, \cdot)$ za grupu, $(R, +, \cdot)$ za prsten, $(\Phi, +, \cdot)$ za tijelo, „0" je neutralni elemenat za adiciju $+$, „1" je neutralni elemenat za multiplikaciju.

28. *Vektorskim prostorom* ili *linearnim prostorom* nad tijelom $(\Phi, +, \cdot)$ nazivamo Abelovu grupu $X = \{x, y, \ldots\}$, u kojoj je definisano množenje s elementima iz Φ, tj.

$$(\forall x \in X)(\forall \alpha \in \Phi)\, \alpha x \in X.$$

Pri tome vrijedi:

1° $\alpha(x + y) = \alpha x + \alpha y$; 2° $(\alpha + \beta)x = \alpha x + \beta x$; 3° $\alpha(\beta x) = (\alpha \cdot \beta)x$; 4° $1x = x$ za sve elemente $\alpha, \beta \in \Phi$, $x, y \in X$. Sa 1 je označen neutralni element multiplikacije u polju Φ. Elemente iz X zovemo *vektorima*, elemente iz Φ *skalarima*, operaciju $+$ skupa X vektorsko sabiranje, operacija $(\alpha, x) \to \alpha x$ množenja vektora $x \in X$ skalarom $\alpha \in \Phi$.

29. Neka su $(A, \circ)$ i $(B, *)$ grupoidi. Ako postoji bijekcija (preslikavanje $1-1$ i *na*) $f: A \to B$ tako da vrijedi

$$(\forall x, y \in A)\, f(x \circ y) = f(x) * f(y),$$

kaže se da su grupoidi $(A, \circ)$ i $(B, *)$ *izomorfni*, a za preslikavanje f kaže se da je *izomorfizam* od A na B.
Ako je $A = B$, f se zove *automorfizam*.

ZADACI

12. Ispitati da li su slijedeće strukture grupe:

a) $S=\{1, -1, i, -i\}$ u odnosu na obično sabiranje;

b) isti skup u odnosu na množenje brojeva ($i^2=-1$);

c) $S=\{f_i(x) | i=1, 2, 3, 4\}$, gdje je

$f_1(x)=x$, $f_2(x)=\frac{1}{x}$, $f_3(x)=-x$, $f_4(x)=-\frac{1}{x}$ uz operaciju $f_i \circ f_j = f_i(f_j(x))$, i, $j=\overline{1, 4}$ (tj. $i, j \in \{1, 2, 3, 4\}$).

d) $(N, \cdot)$, $(Z, \cdot)$, $(Q, \cdot)$, $(R, \cdot)$; e) $(N, +)$, $(Z, +)$, $(Q, +)$, $(R, +)$;

f) $S=\left\{\frac{1+2m}{1+2n} \middle| m, n \in Z\right\}$ u odnosu na obično množenje;

g) $S=\left\{f: x \mapsto \frac{ax+b}{cx+d} \middle| a, b, c, d, x \in R, ad-bc=1\right\}$;

$f(x) * g(x) = f(g(x))$;

h) $(R^+, *)$, $a*b=a^b$; i) $(R^+, \odot)$, $a \odot b = a^2b^2$.

13. $S=\{f: X \to X | f \text{ je bijekcija}\}$ i

$(\forall f, g \in S) f(x) \circ g(x) = f(g(x))$. Dokazati da je $(S, \circ)$ grupa.

14. a) Neka je $nZ=\{n \cdot z | z \in Z\}$ $(n \in N)$. Ispitati da li je struktura $(nZ, +, \cdot)$ prsten, tijelo ili polje.
Isto pitanje važi i za strukture:

b) $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$; c) $(\{a+b\sqrt{2} | a, b \in Z\}, +, \cdot)$;

d) $(S, +, \cdot)$, gdje je S skup polinoma sa cijelim (realnim) koeficijentima.

15. Neka je $(G, \cdot)$ grupa. Dokazati da je:

a) $(ab)^{-1}=b^{-1}a^{-1}$; b) $(a^n)^{-1}=(a^{-1})^n$, $a^n \cdot a^m = a^{n+m}$; c) $xa=xb \Rightarrow a=b$;
d) $ax=bx \Rightarrow a=b$; e) $ax=b \Rightarrow x=a^{-1}b$; f) $xa=b \Rightarrow x=ba^{-1}$,

gdje su $a, b, x \in G$; $m, n \in Z$.

16. Dokazati da brojevi oblika $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, gdje $a, b, c \in Q$, obrazuju polje u odnosu na operacije $+$ i $\cdot$.
Naći inverzni elemenat elementa $x=1-\sqrt[3]{2}+2\sqrt[3]{4}$.

17. U prstenu $(Z, +, \cdot)$ definisane su operacije:

$a \oplus b : \stackrel{\mathrm{Df}}{=} a+b+1$;

$a \odot b : \stackrel{\mathrm{Df}}{=} ab+a+b$.

Pokazati da su $(Z, +, \cdot)$ i $(Z, \oplus, \odot)$ izomorfni prsteni.

18. Pokazati da je X vektorski prostor nad poljem Φ ako je:

a) $X=R$, $\Phi=R$ ili $X=R^n$, $\Phi=R$ $(n \in N)$ i vrijedi
$(\forall x, y \in R^n)\, x+y=(x_1+y_1, x_2+y_2, \ldots, x_n+y_n) \wedge \lambda x=(\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$,
$\lambda \in R$, $x=(x_1\ x_2, \ldots, x_n) \in R^n$.

b) $\Phi=C$, $X=C$, c) $X=C$, $\Phi=R$,

d) X je skup svih polinoma stepena $\leqq n$, $\Phi=R$.

19. Skup G čine funkcije

$f_1(x)=x$, $f_2(x)=1/x$, $f_3(x)=1-x$, $f_4(x)=1/(1-x)$, $f_5(x)=(x-1)/x$, $f_6(x)=x/(x-1)$,

a operacija $\circ$ definisana je kao u zadatku 12. c).
Napišite Kelijevu* tablicu kompozicije za grupoid $(G, \circ)$ i dokažite da je to grupa!

20. Neka je $P(S)$ partitivni skup skupa S i $\triangle$ simetrična razlika skupova. Dokazati da je $(P(S), \triangle)$ grupa.

21. Pokazati da su $(R, +)$, $(R^+, \cdot)$ grupe koje su izomorfne.
(Primjedba: $f: R \to R^+$ definisati sa $f(x)=2^x$.)

22. Dokazati da u komutativnoj grupi G vrijedi:

$(\forall a, b \in G)(\forall n \in Z)(ab)^n = a^n b^n$.

RJEŠENJA

12. a) Ne; b) da; c) da; d) $(N, \cdot)$, $(Z, \cdot)$ nisu, $(Q, \cdot)$ i $(R, \cdot)$ su grupe; e) $(N, +)$ nije grupa; f) da; g) da; h) ne; i) ne.

14. a), c) i d) prsten; b) polje.

15. a) Kako je

$$(a\cdot b)\cdot(b^{-1}a^{-1}) = a(b\cdot b^{-1})a^{-1} \quad \text{(asocijativnost)}$$
$$= a\cdot a^{-1} \quad (bb^{-1}=e)$$
$$= e$$

to je $(ab)^{-1} = b^{-1}a^{-1}$;

b) dokaz indukcijom;

c) $xa = xb \Rightarrow x^{-1}(xa) = x^{-1}(xb) \Rightarrow a = b$, pošto je $x^{-1}x = e$ za svako $x \in G$;

e) $ax = b \Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow x = a^{-1}b$.

16. $x^{-1} = \dfrac{1}{43}(5 + 9\sqrt[3]{2} - \sqrt[3]{4})$.

17. Lako se provjerava da su $(Z, +, \cdot)$ i $(Z, \oplus, \odot)$ prsteni. Ako je $f: x \mapsto x-1$, $(x \in Z)$, tada nije teško provjeriti da je

$(\forall x, y \in Z)\ f(x+y) = f(x) \oplus f(y)$, $f(x\cdot y) = f(x) \odot f(y)$ (i da je f bijekcija), tj. dati prsteni su izomorfni.

19. Kelijeva tablica operacije $\circ$ je:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Koristeći tu tablicu, lako se provjerava:

(*i*) operacija $\circ$ je interna, tj.

$(\forall i, j = \overline{1, 6})\ f_i \circ f_j = f_i(f_j(x)) \in \{f_k \mid k = \overline{1, 6}\}$;

(*ii*) $f_i \circ f_1 = f_1 \circ f_i = f_i$ za svako $i = \overline{1, 6}$, tj. f_1 je neutralni elemenat operacije $\circ$;

(*iii*) $f_i \circ f_i = f_1$, za $i = 1, 2, 3, 6$, dok je $f_4 \circ f_5 = f_5 \circ f_4 = f_1$, tj. $f_i^{-1} = f_i$ za $i = 1, 2, 3, 6$ dok je $f_4^{-1} = f_5$ i $f_5^{-1} = f_4$;

(*iv*) lako se provjerava asocijativnost, tako npr. $(f_2 \circ f_3) \circ f_6 = f_4 \circ f_6 = f_3$, $f_2 \circ (f_3 \circ f_6) = f_2 \circ f_4 = f_3$ itd. Da li je ovo Abelova grupa?