

1. EKVIVALENTNOST

Binarna relacija na skupu S jeste svaki podskup S^2 . Neka je j binarna relacija na skupu S , tada kažemo da je x u relaciji sa y u oznaci x

j
y ako (x,y)

$\hat{}$
S. Neka je

j
binarna relacija na skupu S inverzna relacija relacije

j
jeste binarna relacija

j
-1
definisana sa

a
 j
-1
b
 $\hat{}$
b
 j
a, komplement relacije

j
jeste binarna relacija
 j
definisana sa

j
= S
2
/
 j
za relaciju
 j
na skupu S kažemo da je:

- refleksivna akko $\text{"}a \hat{ } S \text{ i } a \hat{ } a$

- antirefleksivna akko $a \in S \Rightarrow a \not R a$

- simetrična akko $a R b \Rightarrow b R a$

- antisimetrična akko $a R b \wedge b R a \Rightarrow a = b$

- tranzitivna akko $a R b \wedge b R c \Rightarrow a R c$

Relacija j je relacija poredka na S ako je refleksivna, antisimetrična i tranzitivna.

2. UREĐENI SKUPOVI

Za svako S na kome je definisano uređenje $\leq$ kažemo da je uređen skup i označavamo ga sa $(S, \leq)$.

Za uređenje $\leq$ u skupu S kažemo da je potpuno, ako za svako $x, y \in S$ važi samo jedan od sledećih uslova $x < y$, $x = y$, $x > y$

y
.
 U
suprotnom
ure
đ
enje
je
delimi
č
no

Neka je $(S, \leq)$ uređen skup i $A \subseteq S$. Ako postoji element $u_0 \in A$ takav da je za svako $a \in A$, $u_0 \leq a$ kažemo da je

u_0

o

najmanji element skupa A . Za podskup A uređenog skupa

$(S, \leq)$

$\leq$

) kažemo da je majoriran (ograničen odozgo) u S ako postoji m

$\hat{m}$

S takvo da je (

"

a

$\hat{a}$

A), a

$\leq m$. podskup A je minariran u S ako postoji

m

$\hat{m}$

S takvo da je (

"

a

$\hat{a}$

A),

$m \leq$

a .

Neka su S i S' dva uređena skupa, a $f: S \rightarrow S'$ preslikavanje S u S' . Za ovo preslikavanje kažemo da je monotono ako $x \leq y$ $\Rightarrow f(x) \leq f(y)$. Neka je f

izomorfizam iz S u S' . Ako je

A

$\hat{a}$

S i $A' = f(A)$ onda je element $m' = f(m)$ minimalan (maksimalan), minoranta (majoranta), najmanji (najveći), infimum (supermum).

3. MREŽE

Za uređeni skup $(S, \leq)$ kažemo da je mreža ako svaki njegov ekvivalentni podskup ima infimum i supremum. Ako je S mreža onda za $x, y, z \in S$ važi:

1. $x \wedge a = a$ $x \vee x = x$ idempotentost

2. $x \wedge y = y \wedge x$ $x \vee y = y \vee x$ komutativnost

3. $x \wedge (y \vee z) = (x \wedge y) \vee z$

$x \vee (y \wedge z) = (x \vee y) \wedge z$ asocijativnost

4. $x \wedge (x \vee y) = x = (x \wedge y) \vee x$ apsorptivnost

Mreža je distinktivna ako važi bar jedan od sl. uslova:

$(x \wedge y) \vee (y \wedge z) = y \wedge (x \vee z)$

$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

neka je S uređeni skup. Najmanji element skupa obično se naziva nula (0), onaj veći jedinica (1). Mreža S sa nulom i jedinicom naziva se mreža komplementima ako za $a \in S$ postoji x takav da je $x \wedge a = 0$ i $x \vee a = 1$.

b
 $\hat{1}$
 S takvo da važi a
 $\cup$
 $b=1, a$
 $\cup$
 $b=0$.

U distinktivnoj mreži komplement je jednoznačno određen i označavamo ga sa $\bar{a}$. Distinktivna mreža sa komplementima naziva se Bulova algebra.

4. GRUPOIDI

Binarna operacija u skupu G jeste preslikavanje f skupa $G \times G$ u skup G . Uređen par (G, f) nazivamo grupoid a kordinatni broj (G) skupa G – red grupoida. Slika $f(x, y)$ najčešće se piše u obliku proizvoda tj. $(x, y) @ x+y$ i kažemo da je $(G, 0)$ multiplikativna a $(G, +)$ aditivan grupoid.

Za elemente x, y grupoida G kažemo da su komutativni ako važi $xy=yx$. Grupoid u kome su svaka dva elementa komutativna naziva se komutativni grupoid. U grupoidu postoji najviše jedna jedinica.

Polugrupa sa jedinicom: monoid. Za element a grupoida G kažemo da je skrativ ako $ax=ay \cup xa=ya$
 $\cap$
 $x=y$. Grupoid sa skrativim elementima – grupoid je sa skraćivanjem.

Grupoid G je kvazigrupa ako za date $a, b \in G$ pošto je jedinično određeni element $x, y \in G$ takvi da
 $\cup$
 je $ax=b$
 $ya=b$. tj. (
 "
 a, b
 $\hat{1}$
 G) (
 \$

! x,y
 $\hat{I}$
 $G) ax=b$
 $\hat{U}$
 $ya=b$

Svaka kvazigrupa je grupoid sa skraćivanjem. Grupoid G grupa akko je podgrupa i kvazigrupa.

Grupoid $j(G)$ je: komutativan

grupoid sa jedinicom

polugrupa

Ako ima određenu osobinu i na G.

5. HOMOMORFIZMI I KONGRUENCIJA GRUPOIDA

$(G, \circ)$ i $(G, *)$ su dva grupoida i f preslikavanje skupa G u skup G . Za preslikavanje f kažemo da je homomorfizam grupoida G u grupoid G' ako važi: $(\forall x, y \in G) f(x) * f(y)$

Za homomorfizam kažemo da je monomorfizam ako je f injekcija a epimorfizam ako je f

surjekcija. Homomorfizam koji je monomorfizam i epimorfizam naziva se izomorfizam.

Za grupoid G' kažemo da je homomorfna slika grupoida G ako postoji epimorfizam iz G u G' . Ako je grupoid G grupoid sa skraćivanjem i kvazigrupa onda i odgovarajuću osobinu ima i svaki izomorfni grupoid G' . Neka je G grupoid i a ekvivalent na G . Ze realizaciju kažemo da je kongruencija u grupoid G ako je $a \sim b$ a saglasna sa operacijom grupoida G tj. ako $a \sim b$ i $c \sim d$ onda $ac \sim bd$.

Ako je f homomorfizam iz grupoida G u grupoid G' onda je jezgro $\ker f$ kongruencija u G koja je ekvivalentna $\sim$ na G . Ako je f homomorfizam iz grupoida G u grupoid G' onda je jezgro $\ker f$ kongruencija u G koja je ekvivalentna $\sim$ na G .

Ako je f homomorfizam iz grupoida G u grupoid G' onda su grupoidi $G/\ker f$ i G' izomorfni. Ako je f homomorfizam iz grupoida G u grupoid G' onda su grupoidi $G/\ker f$ i G' izomorfni.

6. PODGRUPE

Nepoznati podskup H grupoida G naziva se podgrupa grupoida G ako i samo ako $a, b \in H$ pa $ab \in H$. Ko je grupoid G podgrupa onda je svaki njegov podgrupoid i podpolugrupa.

Ako je G grupa sa jedinicom e i $f: G \rightarrow G'$ sledeći izrazi su ekvivalentni:

a) H je podgrupa grupe G

b) $e \in H, a, b \in H \Rightarrow a^{-1}; ab \in H$

c) $a, b \in H \Rightarrow ab^{-1} \in H$

Dokaz:

H je grupa $a, b \in H \Rightarrow ab \in H$. Neka je e jedinica grupe H . $e \in H$. a^{-1} je inverzni element za a u grupi H . Ako je a

a^{-1}

inverzni el. a u G : a

$\times$

a

1

$= e = aa^{-1}$

a^{-1}

važi pod b) e

$\hat{H}$

H . Ko a, b

$\hat{H}$

H onda a, b

a^{-1}

$\hat{H}$

H i ab

a^{-1}

$\hat{H}$

H jer važi pod a).

Ako je G grupoid i $H \leq G$ onda je H polugrupoid u G ako i samo ako je $HH \leq G$. Uslov $a, b \in H \Rightarrow ab \in H$ ekvivalentan je uslovu $HH \leq G$

$\hat{H}$

G . Neka je H neprazan podskup grupe G tada su sl. iskazi ekvivalentni:

1. H je podgrupa u G

2. $H^{-1}IH$ i $HH^{-1}H$

3. $HH^{-1}IH$

7. NORMALNE PODGRUPE

Podgrupe kod kojih je $(\forall x \in G) xH = Hx$ nazivaju se normalne podgrupe. Jednačina podgrupe $E = \{e\}$ i samo grupa G normalne su podgrupe grupe G .

Ako je G komutativna grupa onda je i svaka njena podgrupa normalna. H je normalna podgrupa grupe G ako je: $(\forall x \in G) x^{-1}Hx = H$

Dokaz:

Neka je H norm. podgrupa i tada prema:

$(\forall x \in G, xH = Hx)$ imamo

$$H = eH = (x^{-1} \cdot x)H = x^{-1}(xH) = x^{-1}Hx$$

Ako je H normalna podgrupa grupe G sa jedinicom e onda je relacija $\sim$ konvergencija u G . Ako je G grupa sa jedinicom e onda je ekvivalentnost

$\sim$ na G konvergencija u G , ako i samo ako je

a
 e
 norm. podgrupa grupe G . Neka je
 a
 konvergencija u G . Iz x
 a
 y sledi:

$$e = x^{-1} \times x \text{ a } x^{-1}y \text{ i } e = x \times x^{-1} \text{ a } yx^{-1} \text{ odnosno } x^{-1}y, yx^{-1} \hat{=} a_e$$

8. CIKLIČNE GRUPE

Neka je S podgrupa $n \in \mathbb{N}$ tada elemente $a_1, a_2, \dots$ za $a_1 = a_2 = \dots = a_n = a$ nazivamo n -ti stepen elementa
 a označavamo ga sa a^n . Ako je S
 adaptivna podgrupa umesto a

a^n
 piše na. Ako je a podskup grupe G podgrupu možemo pisati kao skup svih elemenata iz G koji
 mogu biti predstavljeni u obliku proizvoda stepena sa celim izloziocem konačnog broja
 elemenata iz G . Tako je: $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

$\ln$
 $\hat{=}$
 $\mathbb{Z}$
 $\}$

Za podgrupu $\langle a \rangle$ kažemo da je ciklična grupa generisana elementima a . Svaka ciklična grupa
 je komutativna, G je ciklična grupa: $x, y \in G; m, n \in \mathbb{Z}; x = a^m; y = a^n \Rightarrow xy = a^m a^n = a^{m+n} = a^{n+m} = yx$

Ako grupa G ima prost red onda je ona ciklična. Ako je grupa G ciklična grupa i H njena
 podgrupa onda su grupe H i G/H ciklične: $G = \langle a \rangle \quad H = \{e\} = E$

Jedinična podgrupa grupe G je ciklična grupa reda 1 sa generatorom e .

9. PRSTEN

Za algebru $(R, +, \times)$ sa dve binarne operacije $+$ i $\times$ kažemo da je prsten ako važi:

$(R, +)$ je komutativna grupa

$(R, \times)$ je polugrupa

$(a, b, c \in R), a(b+c) = ab+ac$

$$(a+b)c = ac+bc$$

Za $(R, +)$ kažemo da je adaptivna grupa, a za $(R, \times)$ da je multiplikativna grupa prstena. Umesto $(R, +, \times)$ obično se piše samo R . Ako je $(R, \times)$ komutativna polugrupa kažemo da je R komutativan prsten. Neutralni element adaptivne grupe prstena R označavamo sa 0 i nazivamo 0 prsten.

Ako je R prsten za svako $a, b, c \in R$ važe sledeće jednakosti:

$$A0=0a=0$$

$$-a(b)=a(-b)=-ab$$

$$(-a)(-b)=ab$$

$$a(b-c)=ab-ac$$

$$(a-b)c=ac-bc$$

U prstenu R važi:

$$(\text{"}a, b \in R, n \in \mathbb{Z}) \quad n(ab) = (na)b = a(nb)$$

10. KONGRUENCIJA I IDEALI PRSTENA

$(R, +, \times)$ i $(R', +, \times)$ su prsteni. Preslikavanje $f: R \rightarrow R'$ naziva se homomorfizam prstena, a ako je to preslikavanje homomorfne grupe $(R, +)$ u grupu $(R', +)$ i preslikavanje homomorfne grupe $(R, \times)$ u grupu $(R', \times)$ tj. ako važi:

$$(\text{"}x, y \in R) \quad f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$

Za homomorfizam f iz prstena R u prsten R' kažemo da je nulti ako je $f(r)=O'$, gde je O' nula prstena R' .

Ako je $f:R \rightarrow R'$ nulti epimorfizam iz prstena $(R,+, \times)$ u algebru $(R',+, \times)$ istog tipa, onda je R' prsten.

Ako je pored toga prsten R :

- Komutativan
- Prsten sa jedinicom
- Telo
- Polje

Tada odgovarajuću osobinu ima i R' . Za ekvivalentnost a u skupu R kažemo da je kongurencija u adaptivnoj grupi i u multiplikativnoj polugrupi prstena R' . Ako je

a
kongurencija u prstenu R onda je nad

a
: R
 $\otimes$
 $R/$
 a

epimorfizam i R/O je prsten, R je prsten a I je neprazan skup tog prstena.

Za I kažemo da je ideal prstena R ako je: I – podgrupa adaptivne grupe prstena R . ($\cdot x \in I$,

a

$\hat{I}$

$I)$

a

x, xa

$\hat{I}$

I. Ekvivalentnost

a

na prstenu R je kongurencija u R ako i samo ako je

a

0

ideal prstena R .

11.POLJA

Svaki konačni prsten ima konačnu karakteristiku. Neka je R prsten sa jedinicom e . R ima konačnu karakteristiku ako i samo ako postoji prirodan broj n takav da je $n \times e = 0$. Najmanji prirodan broj sa ovom osobinom je k -ka prstena R . Neka je R prsten sa jedinicom e i bez nepravilnih detalja nule. Ako R ima konačnu k -ku p , onda je p prost broj, a ako R nema konačnu k -ku, onda je jedna k -ka nula.

Ako R konačan prsten sa jedinicom e i bez netrivialnih delitelja nule, onda postoji broj p i prirodan broj k , tako da važi: $\frac{1}{2}R \frac{1}{2} = p^k$.

K -ka polja je prost broj ili nula. Ako je F konačno polje onda je $\frac{1}{2}F \frac{1}{2} = p^k$, gde je p k -ka polja. Konačna polja zovu se Galbova polja. Svako polje F je vektorski prostor nad svojim proizvoljnim podpoljem p .

12. POLINOMI

Ako $a, b \in R[x]$ onda $a+b, a-b, ab \in R[x]$ tj. $R[x]$ je podprsten prstena R . Pri tome važi:

$$\deg(a+b), \deg(a-b) \leq \max(\deg a, \deg b)$$

$$\deg(ab) \leq \deg a + \deg b$$

Ako je R prsten bez netrivialnih detalja nule, onda je $\deg(ab) = \deg a + \deg b$

Prsten $R[x]$ zove se prsten polinoma nad R po argumentu x . Elementi prstena $R[x]$ zovu se polinomi. Nula element prstena $R[x]$ zovu se koeficijenti polinoma $(a_0, a_1, a_2, \dots, a_n)$. Koeficijenti nula polinoma su svi jednaki nuli. Ako je $a, b \in R[x]$ pri čemu je $b \neq 0$ onda postoje jednoznačno određeni $q, r \in R[x]$ takvi da važe $a = qb + r$ i $\deg r < \deg b$

0

,a

1

,a

2

...a

n

). Koeficijenti nula polinoma su svi jednaki nuli. Ako je $a, b \in R[x]$ pri čemu je $b \neq 0$ onda postoje jednoznačno određeni $q, r \in R[x]$ takvi da važe $a = qb + r$ i $\deg r < \deg b$

1

F

[x] pri čemu je b

1

0 onda postoje jednoznačno određeni q,r

1

F

[x] takvi da važe $a = qb + r$ i $\deg r < \deg b$

Polinomi stepena nula su nesvodljivi. Polinom d je zajednički delitelj za a i b .

13. VEKTORSKI PROSTORI

Neka je $(V, +)$ komutativna grupa i k polje brojeva. Ako je definisano preslikavanje $(a, a) \in V \times V$ sa osobinama

a
 $(x+y)=$
 a
 $x+$
 a
 $y, ($
 a
 $+$
 b
 $)x=$
 a
 $x+$
 b
 $x,$
 a
 $($
 b
 $x)= ($
 a
 b
 $)x, 1x=x$ za svako
 a
 $,$
 b
 $\hat{I}$
 k i x, y

$\hat{V}$
 V onda V nazivamo vektorski prostor nad poljem k . Elemente skupa V nazivamo vektori, a elemente polja k skalari.

Operacija $f: V^2 \rightarrow V$ zove se sabiranje vektora, a operacija koja preslikava $k \times V$ u V zove se množenje vektora skalarom. Neutralni element grupe $(V, +)$ zove se nula vektor prostora V . Neka je V vektorski prostor nad poljem k . Ako je izraz $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$ kažemo da su vektori linearno nezavisni, a ako postoje skalari takvi da je:

$$\begin{aligned} & \frac{1}{2} \\ & a \\ & 1 \\ & \frac{1}{2} \\ & + \\ & \frac{1}{2} \\ & a \\ & 2 \\ & \frac{1}{2} \\ & + \dots + \\ & \frac{1}{2} \\ & a \\ & 4 \\ & \frac{1}{2} \\ & > \\ & 0 \text{ i važi:} \\ & a \\ & 1 \\ & x \\ & 1 \\ & + \\ & a \\ & 2 \\ & x \\ & 2 \\ & + \dots + \\ & a \\ & n \\ & x \\ & n \\ & = 0 \text{ kažemo da su vektori linearno zavisni.} \end{aligned}$$

Neprazan podskup U vektorskog prostora V je podprostor V ako iz $x, y \in U$ i $a, b \in k$ sledi $ax + by \in U$.
 Presek podprostora U

1
 $i \in U$
 2
je skup U
 1
 $\mathcal{C}$
 U
 2
, a zbir U
 1
 $+U$
 2
definisan je
sa U
 1
 $+U$
 2
=
{
 U
 1
 $+U$
 2
 $\tilde{U}$
 U
 1
 $\hat{U}$
 U
 1
, U
 2
 $\hat{U}$
 U
 2
}
.

14. BAZA VEKTORSKOG PROSTORA

Neka je V vektorski prostor. Iz svakog skupa $u=G(V)$ može se izdvojiti baza. Svaki element vektorskog prostora V može se na samo jedan način izraziti kao linearna kombinacija vektora i baze B .

Svaka baza B vektorskog prostora V jeste maksimalan linearni nezavistan podskup V . Ako vektorski prostor V ima bar jednu bazu sa konačnim brojem elemenata on se naziva konačno dimenzionalan prostor. U suprotnom prostor V je beskonačno dimenzionalan.

Broj vektora proizvoljne baze konačno dvodimenzionalnog vektorskog prostora naziva se dimenzija.

$$\dim(V_1+V_2)=\dim V_1+\dim V_2 \text{ @ } \dim(V_1 \cap V_2)$$

Svaka baza vektorskog prostora V naziva se i koordinatni sistem tog prostora.