Pesteni i polja

Osnovna svojstva i primjeri

Def. Neprazan skup R, na kome su definisane dvije binarne operacije $+$ i $\cdot$ za koje važi:

I) $(R,+)$ je Abelova grupa

II) $(R,\cdot)$ je grupoid

III) Distributivnost operacija $\cdot$ u odnosu na operaciju $+$.

naziva se pesten. Skup R je nosač pesten.

Pišemo pesten R ili pesten $(R,+,\cdot)$

$T(R,+,\cdot,-,0)$ nularna

binarne operacija; unarna operacija

~~Svojstva pesten (komutativnost, asocijativnost, egzistencija jedinicnog elementa)~~ se odnose na datu operaciju.

Svaki pesten R se sastoji najmanje od jednog elementa (neutralni element 0 za sabiranje). Ako je $R=\{0\}$ - nulti prsten, $R\neq\{0\}$ - netrivijalni pesten.

Svaka Abelova grupa $(R,+)$ se može dodefinisati do pesten.

$\forall a,b\in R: ab=0$.

Osnovna svojstva:

1) $(\forall x\in R)\quad x\cdot 0=0\cdot x=0$

Zaista, $x\cdot 0 = x\cdot(0+0) = x\cdot 0 + x\cdot 0 \Rightarrow x\cdot 0=0$ ($x\cdot 0$: 0)

Slično, $0\cdot x=0$.

2) $(\forall x,y\in R)\quad x\cdot(-y)=(-x)\cdot y=-xy$

Zaista, $x+(-x)=0 \mid \cdot y$

$(x+(-x))y=0\cdot y=0$ (1)

$x\cdot y+(-x)y=0$

$\Rightarrow (-x)y=-xy$

Slično, $x\cdot(-y)=-xy$.

3) $(\forall x,y\in R)\quad (-x)\cdot(-y)=xy$

Zaista, $(-x)\cdot(-y)\overset{2)}{=}-(x\cdot(-y))\overset{2)}{=}-(-xy)=xy$.

4) $(\forall x,y,z\in R):\quad (x-y)z=xz-yz$

$$x(y-z)=xy-xz$$

Zaista, $(x-y)z=(x+(-y))z=x\cdot z+(-y)\cdot z\overset{2)}{=}x\cdot z+(-yz)=xz-yz$

Sličnо, $x(y-z)=xy-xz$.

5) $(\forall x,y\in R)(\forall n\in Z):\quad n(x\cdot y)=(nx)y=x(ny)$

Zaista, $n(xy)=\underbrace{xy+xy+\dots+xy}_{n}=(\underbrace{x+x+\dots+x}_{n})y=(nx)y$

ili $x\cdot(\underbrace{y+\dots+y}_{n})=x\cdot(ny)$

6) $(\forall x_i,y_j\in R)\quad \left(\sum_{i=1}^{n}x_i\right)\cdot\left(\sum_{j=1}^{m}y_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}x_iy_j$

$\Rightarrow$ uopšteni distributivni zakon.

7) Ako je polje R komutativno, onda važi Njutnova binomna formula: $(x+y)^n=x^n+\binom{n}{1}x^{n-1}y+\binom{n}{2}x^{n-2}y^2+\dots+\binom{n}{k}x^{n-k}y^k+\dots+y^n$

Zaista, za $n=2$ $(x+y)^2=(x+y)(x+y)=x^2+yx+xy+y^2=x^2+2xy+y^2$

Matematičkom indukcijom- $\binom{n}{k}=\frac{n!}{k!(n-k)!}$

$\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$.

Primjeri:

1) $(Z,+,\cdot)$ polje cijelih brojeva. (beskonačno)

2) $(Z_n,+,\cdot)$ polje ostataka po modulu n (konačno)

$Z_n=Z|_{\equiv}=\{0,1,2,\dots,n-1\}$

$n=p$, p-prost

$(Z_p,+,\cdot)\to$ polje (polje Galoa od p elemenata, označava se sa $GF(p)$).

3) $E \neq \emptyset$, $P(E)$ = {$X \mid X \subseteq E$}

↓ partitivni skup

$(P(E), \triangle, \cap)$ - prsten (Bulov prsten podskupova).

↓ asocijativni prsten sa 1 u kome je svaki element idempotentan.

Zaista I) $(P(E), \triangle)$ je Abelova grupa.

1) $A \triangle B = (A \setminus B) \cup (B \setminus A)$

2) Asocijativnost $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ → sami!

3) Neutralni element $\emptyset$

$A \triangle \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A$

4) $A \triangle A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset$.

Svaki element A je sam sebi suprotan.

5) $A \triangle B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \triangle A$

II) $(P(E), \cap)$ - grupoid

$A \cap B \in P(E)$, $\forall A, B \subseteq E$

III $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ → sami!

⇒ $(P(E), \triangle, \cap)$ - prsten.

Prsten je asocijativan, jer je operacija $\cap$ asocijativna.

Prsten je sa jedinicom E: $A \cap E = A = E \cap A$, $E \in P(E)$

Idempotentnost: $A \cap A = A$, $\forall A \in P(E)$.

4) R - prsten, sa $M_n(R)$ označimo skup svih kvadratnih matrica reda n sa elementima iz R.

$(M_n(R), +, \cdot)$ - prsten (Potpuni prsten kvadratnih matrica)

$A + B = (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$

$A \cdot B = (a_{ij}) \cdot (b_{ij}) = \left(\sum_{k=1} a_{ik} b_{kj} \right)$

$GL(n,R)$ – skup svih nesingularnih matrica ($\det \neq 0$)

$(GL(n,R), +, \cdot)$ – tijelo.

5) R-prsten $\iff X \neq \emptyset$ sa $R^X = \{f \mid f : X \to R\}$ skup svih funkcija

$(\forall f,g \in R^X)(\forall x \in X)$

$(f \oplus g)(x) = f(x) + g(x)$

$(f \odot g)(x) = f(x) \cdot g(x)$

$(R^X, \oplus, \odot)$ – prsten funkcija

6) $(G,+)$ aditivna Abelova grupa

$End G = \{f \mid f : G \to G\}$ – skup svih (homomorf.) endomorfizama grupe G.

$\forall f,g \in End G \quad (\forall x \in G)$:

$(f \oplus g)(x) = f(x) + g(x)$

$(f \odot g)(x) = (f \circ g)(x) = f(g(x))$

$(End G, \oplus, \odot)$ → prsten endomorfizama Abelove grupe.

$(Aut G, \oplus, \odot)$ – tijelo

7) Neka je R-prsten $R[x]$ – skup svih polinoma određenog stepena.

$R[x] = \{p \mid p(x) = a_0 + a_1 x + \dots + a_n x^n, a_i \in R\}$

$p(x) + q(x) = a_0 + a_1 x + \dots + a_n x^n + b_0 + b_1 x + \dots + b_m x^m \quad , n \leq m$

$= (a_0 + b_0) + (a_1 + b_1)x + \dots (a_n + b_n)x^n + b_{n+1} x^{n+1} + \dots + b_m x^m$

$p(x) \cdot q(x) = \underbrace{a_0 b_0}_{c_0} + (\underbrace{a_1 b_0 + a_0 b_1}_{c_1})x + (\underbrace{a_2 b_0 + a_1 b_1 + a_0 b_2}_{c_2})x^2 + \dots$

$$c_k = \sum_{i+j=k}^{n+m} a_i b_j$$

$(R[x], +, \cdot)$ → prsten polinoma.

8) Grupovi pesteu

R-pesteu

$G = \{g_1, g_2, \dots g_n\} \to$ grupa (konacna)

$RG = \{f \mid f : G \to R\}$

Na skupu RG se definisu binarne operacije $+$ i $\circ$ na sledeci nacin:

$\forall f,g \in RG, \forall x \in G:$

$(f+g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = \sum_{y \cdot z = x} f(y)\, g(z)$

$(RG, +, \cdot)$ - grupovi pesteu.

Ali, na elemente grupovog pesteua RG mozemo posmatrati kao formalne sume. $f(x) = \sum_{k=1}^{n} a_k g_k$, gde su $a_k \in R, g_k \in G$.

$$\sum_{k=1}^{n} a_k g_k + \sum_{k=1}^{n} b_k g_k = \sum_{k=1}^{n} (a_k + b_k) g_k$$

$$\sum_{k=1}^{n} a_k g_k \cdot \sum_{k=1}^{n} b_k g_k = \sum_{k=1}^{n} \Big(\sum_{g_r \cdot g_s = g_k} a_r b_s \Big) g_k$$

Primjer. $G = \langle a \rangle_3 \to$ ciklicna grupa reda 3

$G = \langle a \rangle_3 = \{a, a^2, a^3 = e\} = \{e, a, b\}$

b

$Z_5 = \{0, 1, 2, 3, 4\}$

$Z_5 G = \{re + sa + tb \mid r,s,t \in Z_5,\ e,a,b \in G\}$

$(2e + 3a + 0 \cdot b) + (4e + 2a + 3b) = (2+4)e + (3+2)a + (0+3)b$

$= 1 \cdot e + 0 \cdot a + 3b = \underline{e + 3b}$

$(2e + 3a + 0 \cdot b) \cdot (4e + 2a + 3b) = 2 \cdot 4 \cdot e \cdot e + 3 \cdot 4 \cdot a \cdot e + 0 \cdot 4 \cdot b \cdot e +$

$2 \cdot 2 \cdot e \cdot a + 3 \cdot 2 \cdot a \cdot a + 0 \cdot 2 \cdot b \cdot a + 2 \cdot 3 \cdot e \cdot b + 3 \cdot 3 \cdot a \cdot b + 0 \cdot 3 \cdot b \cdot b =$

$= 3e + 2a + 0\cdot b + 4a + 1\cdot b + 0\cdot e + 1\cdot b + 4\cdot e + 0\cdot a$

$= (3+0+4)e + (2+4+0)\cdot a + (0+1+1)\cdot b = 2e + 1\cdot a + 2b = 2e + a + 2b$

Umjesto konačne grupe G možemo razmatrati i beskonačnu grupu G. U formalnim sumama $\sum_{k \in K} a_k g_k$ treba uzeti da koeficijenti $k \in K$ (najviše konačno mnogo koeficijenata $a_k \neq 0$)
$\hat{R}$

! Svaki Bulov prsten je komutativan.

$(R, +, \cdot)$

$\forall a, b \in R, \ a\cdot b = b\cdot a$

$(a+b)^2 = a+b$ (zbog idempotentnosti)

$a^2 + ab + ba + b^2 = a+b$

$+(-a) \,/\, a + ba + ab + b = a + b \,/\, +(-b)$

$ab + ba = 0$! (1)

$ab = -ba$

Relacija (1) važi za $\forall b \in R$ pa i za $b = a$.

$a^2 + a^2 = 0$

$\boxed{a + a = 0}$ (2)

$a = -a$

$\boxed{ab = -ba = ba}$