

KOLOBARJI

števila	naravna (0, 1, 2, 3, ...)	...	$\mathbb{N}$
	cela (poz in neg)	...	$\mathbb{Z}$
	racionalna, realna, kompleksna	...	$\mathbb{Q}, \mathbb{R}, \mathbb{C}$
polinomi	...	...	s celimi, realnimi, kompleksnimi koef. ...
vektori	...	...	cela števila, realna, kompleksna
matrice	...	...	(kvadratne matrice)
funkcije (npr. realne, kompleksne)	...	...	

seštevanje in odštevanje

števila, polinomi, (odštevanje v $\mathbb{N}$ ni def.)
vektori

množenje in deljenje

števila, polinomi, (deljenje ni vedno def.)
vektori skalarni (npr. vektorji), vektorji (samo $\mathbb{R}^3$ in $\mathbb{R}^7$)

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 3 & -1 & 5 \\ 7 & -2 & 4 \end{pmatrix} \leftrightarrow \text{predstavitelja } A: \mathbb{R}^3 \rightarrow \mathbb{R}^3 \text{ pri neki izbrani bazi}$$

$$A, B \quad A \cdot B \leftrightarrow \text{kompozicija lin. funkcij}$$

$$A:B = A \cdot B^{-1} \quad B^{-1} \text{ je definirana, ko je } \det B \neq 0$$

$$f: X \rightarrow \mathbb{R} \quad (f \pm g)(x) = f(x) \pm g(x)$$

$$(a, b) \times (c, d) = (ad - bc, 0)$$

$$(a, b, c) \times (d, e, f) = (bf - ce, cd - af, ae - bd)$$

Za neko operacijo (obrazloži) rečeno, da je množenje, če distributivna
če $\times$ seštevanje $a \times (b + c) = a \times b + a \times c$

Vselej velja seštevanje in odštevanje

obrazloži pravila komutativnost, asociativnost, nevtralni in nasprotni element

Kolobar K je množica, v kateri lahko seštevanje in množenje

$(K, +, \cdot)$; pri tem veljajo naslednje lastnosti:

seštevanje: komutativno, asociativno, obstaja ničla 0,
obstojaajo nasprotni elementi ($a \mapsto -a$),
torej lahko odštevanje (abelova grupa)

množenje: nimamo zahtev, niti ne ugotavljamo s seštevanjem
- distributivnost $a \cdot (b+c) = a \cdot b + a \cdot c$
 $(a+b) \cdot c = a \cdot c + b \cdot c$

dodatna lastnost množenja $\leadsto$ podtip kolobarja

množenje je komutativno $\leadsto$ komutativen kolobar
asociativno $\leadsto$ asociativen kolobar
ima enoto $\leadsto$ kolobar z enoto / unitalen kolobar
 $\neq 0$ so obrnjeni $\leadsto$ kolobar z deljenjem

Večinoma bomo obravnavali kolobarje, ki so asociativni
in imajo enoto. Po navadi enakovrednosti:

kolobar $\equiv$ asociativni kolobar z enoto.

$$(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c})$$

Kolobarji, ki imajo vse štiri lastnosti bomo rekli obseg.

1. trdnjava: obseg = asoc., unitalen kolobar z deljenjem
polje = komutativni obseg

2. trdnjava: obseg = kom., asoc., unitalen kolobar z deljenjem
"nekomutativni obseg" = algebra z deljenjem

Primeri

- cela števila $\mathbb{Z}$, komutativni (asociativni, z enoto)
- soda števila $2\mathbb{Z}$, kom., asoc., ni enote, ni inverzov
- racionalna števila $\mathbb{Q}$, obsegi
tudi: $\mathbb{R}, \mathbb{C}$
- polinomi s koef.
v $\mathbb{Z}$, v $\mathbb{Q}$, v $\mathbb{R}$ $k_0 + k_1x + k_2x^2 + \dots + k_nx^n$ "porednje" lastnosti (asoc., kom., z) K
 $K[x], K[x, y]$ $K[x, y] := (K[x])[y]$ $k_{0,0} + k_{1,0}x + k_{0,1}y + k_{1,1}xy + \dots$ $(1+x) \cdot ? = 1$
 $x^i y^j$
- matrice $n \times n$, $M_n(K)$ asociativnost (če je K asociativen) ni komutativen
enota (če je v K enota)
- vektorski prostori $\mathbb{R}^3$ ($\mathbb{R}^3 + \times$)

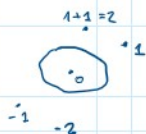
- vektorski $\sim \mathbb{R}^3$ ($\mathbb{R}^3, +, \cdot$)
 enota (če je v K enota)
 m' asoc.
 ni komutativno
 ni enota

- funkcije $f: \mathbb{R} \rightarrow \mathbb{R}$
 $\{ \text{vse funkcije } f: \mathbb{R} \rightarrow \mathbb{R} \} \supseteq \{ \text{vse } f: \mathbb{R} \rightarrow \mathbb{R} \} \supseteq \{ \text{odvedljive } f: \mathbb{R} \rightarrow \mathbb{R} \}$
 $\hookrightarrow$ podholobar
 $(K, +, \cdot)$, $L \subseteq K$, ki je
 holobar za $+$,
 $L \subseteq K$ **podholobar**

- podmnožice X , operaciji $\cup$ in $\cap$:
 $(2^X, \cup, \cap)$ ni holobar $A \cup B = \emptyset$ $\cup$ ni invertor,
 $\hookrightarrow$ kolonova množica X vendar $A + B := (A - B) \cup (B - A)$ 
 $A + A = \emptyset$
 holobar komutativ, asociativ, enota je X , ni invertor. Bode-ov holobar

K holobar brez enote

$K \cup \{1, -1, 2, -2, 3, -3, \dots\}$



$\mathbb{Z} \times K = \{(n, a) \mid n \in \mathbb{Z}, a \in K\}$

poslednje $(m, a) + (n, b) := (m+n, a+b)$ lastnosti se ohranjajo
 $(m, a) \cdot (n, b) := (m \cdot n, a \cdot b)$

Kaj je enota? $(n, a) \cdot (0, b) = (0, ab) \neq (0, b)$

$K = \mathbb{R}[x]$, $(3, 1 + 2x)$

$(1, a) \leftrightarrow 1 + a$

$(2, a) \leftrightarrow (1+1) + a$

$(n, a) \leftrightarrow n \cdot 1 + a$

$$(n \cdot 1 + a)(m \cdot 1 + b) = \underbrace{n \cdot m \cdot 1}_{(1+1+\dots+1)} + \underbrace{nb + ma + ab}_{b+b+\dots+b}$$

pravilna def. množenja

$$(n, a) \cdot (m, b) := (nm, nb + ma + a \cdot b)$$

$$(1, 0) \cdot (n, a) = (n, a)$$

$(\mathbb{Z} \times K, +, \cdot)$ je holobar z enoto, ki vsebuje K

$$\begin{aligned} a, b &\mapsto a \cdot b \\ n \in \mathbb{Z}, a & \\ ma &= \underbrace{a + \dots + a}_m \end{aligned}$$

$$\begin{aligned} (n \cdot 1 + a)(m \cdot 1 + b) &= \dots \\ \underbrace{(1+\dots+1)}_n \cdot \underbrace{(1+\dots+1)}_m &= (nm) \cdot 1 \\ &= \underbrace{(nm) \cdot 1}_\mathbb{Z} + \underbrace{nb + ma + a \cdot b}_K \end{aligned}$$

$$1, 1'$$

$$1 = 1 \cdot 1' = 1'$$

Kaj se zgodi, če dodamo enoto holobarju, ki že ima enoto?

Kolobar K (asociativni + enoto)

prvačeno s komutativnost,

vsaj en element + obratljiv.

Primeri: $\mathbb{Z}$, polinomi $\mathbb{R}[x]$, funkcije $\mathbb{R} \rightarrow \mathbb{R}$

$$\frac{a}{1} \cdot \frac{1}{a} = \frac{a}{a}$$

$$\frac{a}{a} = 1$$

$a, b \in \mathbb{Z}$ $\frac{a}{b}, \frac{c}{d}, \dots$ $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$
 $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

$$0 \cdot x \neq 1$$

Priznamo, da bodo "ulomki" elementov K tvorili obseg.

$$\frac{a+a}{b+b} = \frac{a}{b} \quad \frac{a+a}{b+b} - \frac{a}{b} = \frac{(a+a) \cdot b - a(b+b)}{(b+b) \cdot b} = \frac{0}{(b+b) \cdot b} \leftrightarrow 0$$

še več, za $k \in \mathbb{Z}$ $\frac{ka}{kb} = \frac{a}{b}$

šč več, za $c \in K$ $\frac{c \cdot a}{c \cdot b} = \frac{a}{b}$

$(K \times K - \{0\}) / \sim$
ulomki

$$\frac{a}{b} \sim \frac{a \cdot c}{b \cdot c}, c \in K - \{0\}$$

$$\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow a \cdot b' = a' \cdot b$$

$\sim$ je ekvivalenčna relacija

reflektivnost $\frac{a}{b} \sim \frac{a}{b}$ (uporabimo $c=1$) $a \cdot b = b \cdot a$

simetričnost $\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow \frac{a'}{b'} \sim \frac{a}{b}$ $a \cdot b' = a' \cdot b$

transitivnost $\frac{a}{b} \sim \frac{a'}{b'} \wedge \frac{a'}{b'} \sim \frac{a''}{b''} \Rightarrow \frac{a}{b} \sim \frac{a''}{b''}$ $a \cdot b' = a' \cdot b$ in $a' \cdot b'' = b' \cdot a'' \Rightarrow a \cdot b'' = a'' \cdot b$

$\sim \mathbb{Z} \quad b \cdot b' = 0 \quad b=0 \text{ ali } b'=0$

$\sim \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$$\frac{1}{2} + \frac{4}{3} = \frac{1 \cdot 3 + 2 \cdot 4}{2 \cdot 3} = \frac{11}{6} = 0$$

$a, b \in K \quad a \cdot b = 0 \quad b \cdot x = 1$ Ali obstaja tak x ?

če: $b \cdot x = 1 \Rightarrow a \cdot (b \cdot x) = a \cdot 1 = a$

$$0 = 0 \cdot x = (a \cdot b) \cdot x$$

če $a, b \in K - \{0\}$, $a \cdot b = 0$, pravimo, da sta a in b delitelj nič.

Teh se nikoli ne da domiši $\leadsto$
ne morejo nastopati kot imenovalec ulomkov v K

$\rightarrow K$ je kolobar brez deliteljev nič, če $a, b \in K$ velja $a \cdot b = 0$,
potem je $a = 0$ ali $b = 0$.

(drugače povedano $a, b \in K - \{0\} \Rightarrow a \cdot b \in K - \{0\}$)

K kolobar brez del. nič $\leadsto (K \times K - \{0\}) / \sim$
je obseg; pravimo mu obseg ulomkov na K

$((K \times K - \{0\}) / \sim, +, \cdot)$ je obseg

Primeri

• $\mathbb{Z} \leadsto$ obseg ulomkov $= \mathbb{Q}$

• polinomi nad K : ali so komutativni kolobar brez del. nič?

K brez del. nič $\Leftrightarrow K[x]$ brez del. nič $(a_0 + a_1x)(b_0 + b_1x) = a_0b_0 + a_0b_1x + a_1b_0x + a_1b_1x^2$

(opazimo: v obeh so vsi elementi $\neq 0$ obratljivi, zato im. deliteljev nič)

$\mathbb{R}[x]$ je kolobar brez del. nič, vendar ni obseg $\leadsto$

Kaj je obseg ulomkov?

$\mathbb{R}(x) = \left\{ \frac{p(x)}{q(x)} \mid q \neq 0 \right\}$ je obseg
ulomkov na $\mathbb{R}[x]$

K kolobar brez deliteljev nič. Kaj je obseg ulomkov na $K[x]$?

D.N.

v $\mathbb{Z}_n$:

• $f: \mathbb{R} \rightarrow \mathbb{R}$