IRMFMF 2025-02-25

def: kolobar $(K,+,\cdot)$: $(K,+)$ abelova grupa
in distributivnost

obseg je unitalni asociativni komutativni kolobar z obrnljivimi neničelnimi elementi.

DANES:
Delitelji niča in karakteristika kolobarja.
kolobarji pri IPM so vedno asociativni z enoto.

[Delitelji niča]

def.: $a \neq 0$ je delitelj niča, če $\exists b \neq 0 \ni: ab = 0$.

primeri: • $f, g : X \to \mathbb{R}$
za $f(x) = x + |x|$ in $g(x) = x - |x|$

$$(f \cdot g)(x) = x^2 - |x|^2 = 0$$

• $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

• 2 v $\mathbb{Z}_4$: $2 \cdot_4 2 = 0$

• 2 v $\mathbb{Z}_6$: $2 \cdot_6 3 = 0$

• v $\mathbb{Z}_{m \cdot n}$ sta m in n delitelja niča

• X, $(2^X, \nabla, \cap)$ boolov kolobar

$A \cap (X - A) = \emptyset$

vsi elementi, razen $\emptyset$ in X (enota za $\cap$), so delitelji niča

Trditev: če je K kolobar brez deliteljev niča, je tudi: $K[x]$ brez deliteljev niča.

Dokaz: naj bosta $p(x)$ in $q(x)$ poljubna neničelna elementa.

$p(x) = a_n x^n + \dots$, $a_n \neq 0$ $\qquad$ $q(x) = b_m x^m + \dots$, $b_m \neq 0$

$p(x)\,q(x) = \underline{a_n b_m}\, x^{n+m} + \dots$

$\hookrightarrow$ neničelno $\Rightarrow$ $p(x)q(x)$ je neničelno.

Trditev: $a \in K$ ne more biti hkrati obrnljiv in delitelj niča.

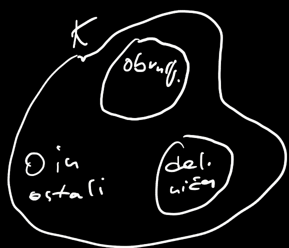
Dokaz: PDDRAA a je tak element. let $b \neq 0$ tak, da $ab = 0$.

let c tak, da $ca = 1$.

tedaj produkt

$$
\begin{aligned}
(ca)b &= c(ab) \\
1 \cdot b &= c \cdot 0 \\
1 \cdot b &= 0 \\
b &= 0 \quad \text{↯}
\end{aligned}
$$

V $\mathbb{Z}$ ni deliteljev niča, obrnljiva sta le 1 in -1. Ni torej nujno, da je element bodisi obrnljiv bodisi je delitelj niča.



Trditev: Če $a \neq 0$ ni delitelj niča, iz $ax = ay$ sledi $x = y$.

Pravilo krajšanja.

Dokaz:
$$ax = ay$$
$$ax - ay = 0$$
$$a(x-y) = 0$$
$$x - y = 0$$
$$x = y$$

Izrek (Wedderburn): let K končen (komutativen) kolobar brez deliteljev niča je obseg.

Dokaz: $K = \{x_1, \dots, x_n\}$

$\forall a \neq 0 \rightarrow \{ax_1, \dots, ax_n\}$ so vsi različni, sicer bi iz $ax_i = ax_j$ sledilo $x_i = x_j$.

eden izmed ___ je 1, eden izmed ___ je 1.

$\Rightarrow \exists x_i \ni: \; ax_i = 1 = x_i a \Rightarrow x_i$ je inverz a

Opomba: izrek velja brez predpostavljene komutativnosti. Tedaj bi podobno prišli $a x_i = 1 = x_j a$.

$x_i = x_j$, kajti $\underbrace{(x_i a)}_{1} x_j = x_i \underbrace{(a x_j)}_{1}$

$1 \cdot x_j = x_i \cdot 1 \Rightarrow x_j = x_i$

Težje pa je dokazati, da je množenje komutativno (ampak velja).

Če je $(K,+,\cdot)$ kolobar z inverzi vseh neničelnih elementov, je $K \setminus \{0\}$ grupa za množenje. To je multiplikativna grupa kolobarja K. Če je K obseg, je njegova multiplikativna grupa abelova (po definiciji).

Ulomki. let K kom. kolobar brez deliteljev niča - (a,b) $\frac{a}{b}$, $b \neq 0$.

$K \times (K - \{0\})$ ulomki.

Def: $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$

refl simetr ✓

tranz: $\frac{a}{b} \sim \frac{c}{d}$, $\frac{c}{d} \sim \frac{e}{f}$

$ad = bc$ $\qquad$ $cf = de$

$$adf = bcf = bde$$

$$\Downarrow$$

$$(af)d = (be)d$$

$$\Downarrow$$

$$af = be \Rightarrow \frac{a}{b} \sim \frac{e}{f} \quad ✓$$

$\Rightarrow$ relacija je ekvivalenčna.

$$\operatorname{Frac}(K) := K \times K - \{0\} \big/ \sim$$ ekvivalenčni razredi

na $\operatorname{Frac}(K)$ vpeljemo $+$ in $\cdot$:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

definicija je dobra $\Rightarrow$ neodvisna od izbire predstavnikov ekv. razredov.

Trditev: V $\operatorname{Frac}(K)$ so vsi neničelni elementi obrnljivi! — ničelni elementi so oblike $\frac{0}{b}$.

Dokaz: $\frac{a}{b} \cdot \frac{b}{a} = 1 \in \operatorname{Frac}(K)$

Trditev: Če je K komutativni ~~kolobar~~ doseg brez deliteljev niča, je $\operatorname{Frac}(K) := \left(K \times K \setminus \{0\} \big/ \sim, +, \cdot \right)$ obseg — obseg ulomkov za kolobar K.

Primeri:

- $\mathbb{Z}$, $\operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$
- $K \longrightarrow \operatorname{Frac}(K)$ — vedno obstaja taka f-ja.
  $a \longmapsto \frac{a}{1}$ je injektivna.

na naraven način lahko gledamo na K kot na „$\subseteq$" $\operatorname{Frac}(K)$. — gre za bolj kolobarjev — „podkolobar" v $\operatorname{Frac}(K)$ ob upoštevanju zgornje identifikacije

- $\mathbb{R}[x]$ niso obseg, so pa kom. kol. brez del. niza.
racionalne f-je (z realnimi koeficienti) so pa $\mathrm{Frac}(\mathbb{R}[x])$.
↳ oznaka $\mathbb{R}(x)$

- K kolobar brez deliteljev niča. $K[x]$ je tudi kolobar brez deliteljev niča. Velja
$$\mathrm{Frac}(K[x]) = \mathrm{Frac}(K)(x)$$
↳ $\mathrm{Frac}(\mathbb{Z}[x]) = \mathbb{Q}(x)$

- za K obseg pa velja $\mathrm{Frac}(K) = K$.

upoštevanje tisto zgornjo identifikacijo, ki je kar tudi surjektivna, kajti $\frac{a}{b} = \frac{ab^{-1}}{1}$

[KARAKTERISTIKA KOLOBARJA]

oglejmo si K in 1:

$$1,\ 1+1,\ 1+1+1,\ \dots$$

↳ lahko se tu pojavi 0, lahko pa ne.

označimo $\underbrace{1+\dots+1}_{n\text{-krat}} =: n1$ to ni •

Def.: karakteristika K je

$\mathrm{char}(K) := \min n \in \mathbb{N} \ \exists: n1 = 0$, če pa tak $n \not\exists$, pa je $\mathrm{char}(K) := 0$

če je $\mathrm{char}\, K \neq 0 \Rightarrow \forall a \in K$ velja $\mathrm{char}(K)a = 0$

$$\underbrace{a + \cdots + a}_{\mathrm{char}(K)\text{-krat}} = a \cdot \underbrace{(1 + \cdots + 1)}_{\mathrm{char}(K)\text{-krat}} = a \cdot 0 = 0$$

primeri:

- $\mathrm{char}\, \mathbb{Z} = \mathrm{char}\, \mathbb{Q} = \mathrm{char}\, \mathbb{R} = 0$
- $\mathrm{char}\, \mathbb{Z}_n = n$
- $\mathrm{char}(2^X, \triangledown, \cap) = 2$
- $\mathrm{char}(K[x]) = \mathrm{char}(K)$
- $\mathrm{char}\, M_n(K) = \mathrm{char}\, K$

Trditev: če je K kolobar brez deliteljev niča, je $\mathrm{char}(K) = 0$ ali $\mathrm{char}(K) =$ praštevilo.

Dokaz: če je $\mathrm{char}(K) = m \cdot n$ za $m, n > 1$, velja $\underset{\neq 0}{m1} \cdot \underset{\neq 0}{n1} = (m \cdot n)1 = 0$, torej

$\Rightarrow m1$ ali $n1$ sta delitelja niča $\times$

Trditev: Če kolobar K vsebuje kot podkolobar nek obseg $F \subseteq K$, potem je K vektorski prostor nad F.

Dokaz:

po definiciji vektorskega prostora.

Def.: V je vektorski postor nad obsegom $F \iff (V,+)$ abelova grupa

$\wedge$ množenje s skalarji:
$F \times V \to V$ $\wedge$

$\forall u, v \in V,\ a, b \in F$:

$1 \cdot v = v \ \wedge\ (a+b) \cdot v = av + bv \ \wedge$
$a \cdot (v+w) = av + aw \ \wedge$
$(a \cdot b) \cdot v = a \cdot (b \cdot w)$

Trditev: let K kolobar in $\operatorname{char} K = p$. tedaj

$\{0, 1, 1+1, 1+1+1, \ldots \underbrace{1+\ldots+1}_{p-1\text{-krat}}\} \subseteq K$.

so vsi različni.

ta množica je $\mathbb{Z}_p$.

$\Rightarrow K$ je V.P. nad $\mathbb{Z}_p$.

Posebej, če je K končen, potem $|K| = p^{\dim_{\mathbb{Z}_p} K}$.