Izbrana poglavja iz matematike

Napisal Jure Pustoslemšek po zapiskih predavanj prof. dr. Petarja Pavešiča

Junij 2020

1 Abstraktna algebra: kolobarji in obsegi

Definicija 1.1 (Kolobar). *Kolobar je množica, kateri smo priredili notranji operaciji seštevanja in množenja, ki zadostujeta spodnjim kriterijem. Eksplicitno ga lahko zapišemo kot* $(K, +, \cdot)$.

Pri seštevanju velja komutativnost in asociativnost obstaja ničla 0 in za vsak $a \in K$ *obstaja nasprotni element* $(-a) \in K$, *torej lahko vedno odštevamo.*

$$\forall a, b \in K : a + b = b + a$$

$$\forall a, b, c \in K : (a + b) + c = a + (b + c)$$

$$\forall a \in K \exists (-a) \in K : a + (-a) = a - a = 0$$

Pri množenju nimamo dodatnih zahtev, wazen uglašenosti s seštevanjem - distibutivnost.

$$\forall a, b, c \in K : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Rečeno drugače, kolobar je grupa za seštevanje in zaprta za množenje.

Če ima množenje kakšno dodatno lastnost, to lastnost običajno izpostavimo

Množenje je asociativno	$\rightarrow$	asociativni kolobar
Množenje je komutativno	$\rightarrow$	komutativni kolobar
Množenje ima enoto	$\rightarrow$	kolobar z enoto
Vsak $a \neq 0 \in K$ ima inverz a^{-1}	$\rightarrow$	kolobar z deljenjem

Literatura velikokrat v definiciji kolobarja zahteva tudi asociativnost in obstoj enote, zato bomo v nadaljevanju privzeli, da z izrazom "kolobar" mislimo na asociativen kolobar z enoto, komutativnost in deljenje pa bomo izrecno navedli.

Definicija 1.2 (Obseg). *Kolobarju, v katerem je množenje asociativno, komutativno in ima enoto ter ima operacijo deljenja, rečemo* ***obseg****.*

1.1 Kolobarji

Zgled 1.3. *Če dani kolobar nima enote, mu jo lahko dodamo:*
K kolobar brez enote
Če dodamo 1, smo prisiljeni dodati tudi $-1, 2, -2, 3, -3, ...$
Rešitev: na $\mathbb{Z} \times K$ vpeljemo:

$$(n, a) + (m, b) := (n + m, a + b)$$

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

Ničla je $(0, 0)$, nasprotni element je $-(m, a) = (-m, -a)$, enota je $(1, 0)$. Če je K komutativen oz. asociativen, je to tudi $\mathbb{Z} \times K$.

Kaj pa, če imamo kolobar, v katerem nekateri elementi nimajo inverza, ampak bi jih želeli dodati? Poskusimo to storiti na takšen način, kot smo v osnovni šoli definirali racionalna števila s celimi števili, in sicer z uvedbo ulomkov.

Naj bo K kolobar z enoto. Za $a, b \in K, b \neq 0$ vpeljemo simbole $\frac{a}{b}$, s katerimi računamo

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

Pojavi se težava: lahko se zgodi, da je $bd = 0$, čeprav $b \neq 0$ in $d \neq 0$. Tega pri številih nismo vajeni vendar:

Zgled 1.4 (Matrike)**.**

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

Zgled 1.5 ($\mathbb{Z}_{12}$: ostanki po modulu 12)**.**

$$2 \cdot 6 = 0$$

$$3 \cdot 8 = 0$$

Definicija 1.6 (Delitelj niča)**.** *V kolobarju K je $0 \neq a \in K$ **delitelj niča**, če obstaja tak $b \neq 0$, da je $a \cdot b = 0$.*

Trditev 1.7. *Delitelj niča nima inverza.*

Dokaz. Če za $a \in K$ obstajata takšna neničelna $b, c \in K$, da velja

$$a \cdot b = 0 \text{ in } c \cdot a = 1$$

dobimo protislovje

$$b = 1 \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$$

□

Definicija 1.8 (Celi kolobar)**.** ***Celi kolobar*** *je komutativni kolobar, v katerem ni deliteljev niča. Ekvivalentno, v celem kolobarju iz* $a \cdot b = 0$ *sledi* $a = 0$ *ali* $b = 0$.

Naj bo K celi kolobar. Tvorimo **kolobar ulomkov** $\overline{K}$: elementi so ulomki $\frac{a}{b}$, vendar $\frac{a}{b} \equiv \frac{c}{d}$, če je $ad = bc$ (ulomke lahko krajšamo). Definiramo operaciji kot prej:

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

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

Preverimo lahko, da je $\overline{K}$ obseg.

Zakaj moramo enačiti sorazmerne ulomke?

Zaradi definicije operacij: $\frac{a}{b} - \frac{ka}{kb} = \frac{kab-kab}{kb^2} = 0$, torej mora veljati $\frac{ka}{kb} \equiv \frac{a}{b}$.

Opomba. *Z nekaj truda lahko vpeljemo ulomke tudi pri nekomutativnih kolobarjih in kolobarjih z deliterlji niča. Takrat dobimo kolobarje ulomkov, ki niso obsegi.*

Delitelj niča ne more biti obrnljiv, obrnljiv element pa ni delitelj niča. Ali je lahko element kolobarja niti obrnljiv niti delitelj niča?

Zgled 1.9. $\mathbb{Z}$ *nima deliteljev niča, obrnljiva pa sta le* 1 *in* -1.

Zgled 1.10. $\mathbb{Z}_{12}$

- *Delitelji niča:* $0, 2, 3, 4, 6, 8, 9, 10$
- *Obrnljivi:* $1, 5, 7, 11$

V končnih kolobarjih ni drugih možnosti, kar pove naslednji znameniti izrek.

Izrek 1.11 (Wedderburnov izrek)**.** *Končen kolobar brez deliteljev niča je obseg.*

Dokaz. Naj bo K končen kolobar brez deliteljev niča. Dokazati moramo, da so vsi elementi $K - \{0\}$ obrnljivi.

Za poljuben $a \in K - \{0\}$ definiramo funkcijo

$$l_a : K \to K$$

$$l_a(x) := a \cdot x$$

Recimo, da za neka $x, y \in K$ velja $l_a(x) = l_a(y)$. Potem je $ax = ay$, torej $a(x - y = 0)$. Ker K nima deliteljev niča, sledi $x = y$. Torej je l_a injektivna in ker slika iz K v K, tudi bijektivna.

Ker je $l_a(K) = K$, je $l_a(b) = a \cdot b = 1$ za nek $b \in K$. Ponovimo razmislek za $d_a(x) := x \cdot a$ in dobimo, da je $d_a(c) = a \cdot c = 1$ za nek $c \in K$. Iz $c = c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$ sledi $c = b = a^{-1}$. K je torej kolobar z deljenjem. Če je K komutativen, je obseg.

Dokaz komutativnosti zahteva nekaj dodatne teorije grup, zato ga ne bomo natančno navedli. Ideja je, da je center $Z(K)$ (tj. elementi K, ki komutirajo z vsemi elementi K) obseg, celoten K pa je vektorski prostor nad $Z(K)$. Iz primerjave multiplikativnih grup lahko izpeljemo, da je K 1-razsežen vektorski prostor nad $Z(K)$, torej $K = Z(K)$. □

Posledica 1.12. *$\mathbb{Z}_n$ je obseg $\Leftrightarrow$ n je praštevilo.*

Definicija 1.13 (Karakteristika kolobarja)**.** ***Karakteristika*** *kolobarja K je najmanjši $n \in \mathbb{N}$, za katerega velja, da je $n \cdot a = a + ... + a = 0$. Zapišemo jo kot $char(K) = n$ ali $charK = n$. Če tak n ne obstaja, potem pišemo $char(K) = 0$.*

Trditev 1.14. *Naj bo K kolobar.*

a) Če $1 \in K$, potem je $char(K) =$ red enote $=$ min n, da je $n \cdot 1 = 0$.

b) Če K nima deliteljev niča, potem je $char(K)$ praštevilo ali 0.

Dokaz (a). Naj bo n red enote, torej je $n \cdot 1 = 0$. Potem za vsak $a \in K$ velja:

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

Iz tega sledi, da je $charK \leq n$. Ker je red 1 enak n, je $charK \geq n$, torej $charK = n$. □

Dokaz (b). Denimo, da je $charK = k \cdot l$ za $k, l > 1$. Potem je $0 = k \cdot l \cdot 1 = k \cdot l$. Ker v K ni deliteljev niča, je $k \cdot 1 = 0$ ali $l \cdot 1 = 0$, zato je po (a) $charK < k \cdot l$. Protislovje. □

Definicija 1.15. *Naj bosta K, L kolobarja.*

$f : K \to L$ je ***homomorfizem kolobarjev****, če velja:*

$$f(a + b) = f(a) + f(b)$$

$$f(a \cdot b) = f(a) \cdot f(b)$$

za poljubna $a, b \in K$.

Bijektivnemu homomorfizmu rečemo **izomorfizem**.

Poglejmo nekaj primerov homomorfizmov:

Zgled 1.16. *$\mathbb{Z} \xrightarrow{mod\ n} \mathbb{Z}_n$ je homomorfizem (dokaz ponovi korake dokaza, da je $\mathbb{Z}_n$ kolobar).*

Zgled 1.17. *Konjugiranje* $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ *je izomorfizem kolobarjev.*

Zgled 1.18. *Za poljuben* $a \in \mathbb{R}$ *definiramo* $f_a : \mathbb{Z}[x] \to \mathbb{R}$ *s predpisom* $f_a(p) = p(a)$

$$f_a(p+q) = (p+q)(a) = p(a) + q(a) = f_a(p) + f_a(q)$$

$$f_a(p+q) = (p \cdot q)(a) = p(a) \cdot q(a) = f_a(p) \cdot f_a(q)$$

Zgled 1.19. $a \mapsto \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ *je homomorfizem* $\mathbb{R} \to M_2(\mathbb{R})$.

Zgled 1.20. *Splošneje* $f_a : \mathscr{C}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ *s predpisom* $f_a(g) := g(a)$ *je tudi homomorfizem kolobarjev.*

Zgled 1.21. $a \mapsto \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$ *<u>ni</u> homomorfizem* $\mathbb{R} \to M_2(\mathbb{R})$ *(ohranja seštevanje, ne pa množenja).*

Zgled 1.22. *Preslikava* $\mathbb{C} \to M_2(\mathbb{R})$ *s predpisom* $a + bi \mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ *je homomorfizem.*

Zgled 1.23. $a \mapsto a^p$ *je homomorfizem* $\mathbb{Z}_p \to \mathbb{Z}_p$ *(p praštevilo).*

Trditev 1.24. *Za homomorfizem* $f : K \to L$*:*

a) $f(a) = 0$*; sledi iz* $f(0) = f(0+0) = f(0) + f(0)$

b) $f(-a) = -f(a)$*; sledi iz* $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$

c) V splošnem ne zahtevamo $f(1) = 1$*; če to velja, pravimo, da je homomorfizem* ***unitalen***

d) Če je f *unitalen homomorfizem in a obrnljiv, je* $f(a)$ *obrnljiv*