

# Kolobarji, Obsegi in Polinomi

April 22, 2008

## Definicija kolobarja

Algebrska struktura  $(K, +, \cdot)$  je **kolobar**, če velja:

1.  $(K, +)$  je Abelova grupa, njeno enoto označimo z  $0$ ;
2.  $(K, \cdot)$  je polgrupa;
3. operacija  $\cdot$  distribuira čez  $+$ , tj., za vse  $a, b, c \in K$  velja:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{in} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

Operacijam ”+” in ” $\cdot$ ” v kolobarju  $K$  rečemo **seštevanje** in **množenje**.

Kolobar  $K$  je:

- **Abelov** oz. **komutativen**, če je množenje komutativno;
- **kolobar z enico**, če je  $(K, \cdot)$  monoid oz. obstaja element  $1 \in K$  tako, da za vsak  $x \in K$  velja:

$$1 \cdot x = x \cdot 1 = x$$

## Zgledi:

- $\mathcal{T} = (\{0\}, +, \cdot)$  je najmanjši kolobar, imenujemo ga **trivialni kolobar**;
- **Kolobarji celih, racionalnih, realnih in kompleksnih števil:**

$$(\mathbb{Z}, +, \cdot), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot), \quad (\mathbb{C}, +, \cdot)$$

To so kolobarji z običajnim seštevanjem in množenjem;

- $(\mathbb{Z}_n, +_n, \cdot_n)$  je **kolobar ostankov po modulu  $n$** ;
- $(n\mathbb{Z}, +, \cdot)$  je **kolobar večkratnikov naravnega števila  $n$** ;
- $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$  je **kolobar realnih funkcij**

$$\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \rightarrow \mathbb{R}\}$$

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

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

- $\mathcal{B} = (\mathcal{P}(M), +, \cap)$  je **Boolov kolobar**

$$A + B = A \setminus B \cup B \setminus A.$$

# Delitelji ničā

Elementa  $a, b \in K \setminus \{0\}$  sta **delitelja ničā**, če je  $a \cdot b = 0$ .

**Zgleda:**

- $2 \cdot_6 3 = 0$  torej sta 2 in 3 sta delitelja ničā v  $(\mathbb{Z}_6, +_6, \cdot_6)$ .
- $f, g \in \mathbb{R}^{\mathbb{R}}$  podamo takole:

$$f(x) = \begin{cases} 0, & \text{za } x \leq 0 \\ x, & \text{sicer.} \end{cases} \quad \text{in} \quad g(x) = \begin{cases} x, & \text{za } x \leq 0 \\ 0, & \text{sicer.} \end{cases}$$

Potem za vsak  $x \in \mathbb{R}$  velja  $f(x) \cdot g(x) = 0$ . Torej,  $f$  in  $g$  sta delitelja ničā.

Kolobar  $K$  je **cel**, kadar je Abelov in je brez deliteljev ničā.

# Aditivna potenca

Aditivno  $m$ -to potenco elementa  $a$  označimo z  **$ma$** , tj.

$$ma = \underbrace{a + a + \cdots + a}_m$$

Potem pa velja:

$$(m + n)a = ma + na$$

$$m(na) = (mn)a$$

$$n(a + b) = na + nb$$

$$(mn)a \cdot b = (ma) \cdot (nb)$$

# Absorpcijski element 0

**Trditev 1** *V kolobarju je 0 absorpcijski element, tj. velja*

$$a \cdot 0 = 0 \cdot a = 0$$

**Dokaz.** Sklepamo takole:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Podobno pokažemo, da je  $0 \cdot a = 0$ . □

**Naloga 1** *Pokaži, da je 0 edini absorpcijski element.*

**Odgovor:**

**Vprašanje 1** *Naj bo  $K$  kolobar z enico. Ali je lahko  $1 = 0$ ?*

**Odgovor:**

## Operacija $-$

Označimo z  $-a$  inverz elementa  $a$  v grupi  $(A, +)$ . Operacijo " $-$ " definiramo takole

$$\mathbf{a} - \mathbf{b} := a + (-b).$$

**Trditev 2** V kolobarju  $K$  velja:

1.  $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

2.  $(-a) \cdot (-b) = a \cdot b$

3.  $a \cdot (b - c) = a \cdot b - a \cdot c$

**Dokaz.** Iz  $(-a) + a = 0$  sledi  $(-a) \cdot b + a \cdot b = 0$  in tako dobimo, da je  $(-a) \cdot b = -(a \cdot b)$ . Podobno pokažemo drugi del prve enakosti.

V dokazu trditve 2 uporabimo dvakrat trditev 1 takole:

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b.$$

Tretjo trditev pa dokažemo takole:

$$a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b - a \cdot c.$$

□

## Množica $K^*$

Naj bo  $K$  kolobar z enico. Element  $a$  je **obrnljiv**, če

$$\exists b \in K : a \cdot b = b \cdot a = 1.$$

Naj bo  $\mathbf{K}^*$  množica obrnljivih elementov kolobarja  $K$ . Opazimo, da  $0 \notin K^*$ .

**Trditev 3** Struktura  $(K^*, \cdot)$  je grupa za množenje.

# Obsegi

Kolobar  $K$  je **obseg**, če je  $K^* = K \setminus \{0\}$ , tj. vsak element iz  $K$  različen od 0, je obrnljiv.

Komutativen obseg je **polje**, tj. če v obsegu velja  $a \cdot b = b \cdot a$  za vse  $a, b$ .

**Problem 1** *Pokaži, da v poljubnem obsegu ni deliteljev nič.*

**Rešitev:**

**Izrek 4**  $(\mathbb{Z}_n, +_n, \cdot_n)$  je polje natanko takrat, ko je  $n$  praštevilo.

**Dokaz.** ( $\Leftarrow$ ) Naj bo  $n$  praštevilo. Potrebno bo pokazati, da je vsak element iz  $\mathbb{Z}_n \setminus \{0\}$  obrnljiv. To pa vemo iz DS I: enačba  $ax = 1 + yn$  je rešljiva, tako bo  $x \in \mathbb{Z}_n$  inverz za  $a$ .

( $\Rightarrow$ ) Recimo, da je  $n$  sestavljeno število. Potem, je  $n = a \cdot b$  za  $1 < a, b < n$  in od tod sledi  $a \cdot_n b = 0$  v  $\mathbb{Z}_n$ . Torej,  $a$  in  $b$  sta delitelja nič. Potem pa iz rešitve prejšnjega problema sledi, da  $\mathbb{Z}_n$  ni obseg.  $\square$

**Vprašanje 2** *Kateri kolobarji iz prvega zglada*

$\mathcal{T}$     $\mathbb{Z}$     $\mathbb{Q}$     $\mathbb{R}$     $\mathbb{C}$     $n\mathbb{Z}$     $\mathbb{Z}_n$     $\mathbb{R}^{\mathbb{R}}$     $\mathcal{B}$

*so obsegi oz. polja?*

**Odgovor:**

**Naloga 2** *V kolobarju  $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$  reši sistem enačb:*

$$3x + 8y = 7$$

$$6x + 5y = 4.$$

**Rešitev:** Dobimo tri rešitve:  $(1, 2)$ ,  $(5, 2)$ ,  $(9, 2)$ .

# Karakteristika kolobarja

Naj bo  $K$  kolobar z enico ter naj bo  $r = \text{red}(1)$  v grupi  $(K, +)$ .

**Karakteristika** kolobarja  $K$  je

$$r(K) = \begin{cases} r, & \text{če je } r \text{ končno število;} \\ 0, & \text{če } r = \infty. \end{cases}$$

**Zgledi:**  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  imajo karakteristiko 0, ker je  $n \cdot 1 \neq 0$  za vse  $n \in \mathbb{N}$ .

**Trditev 5** V kolobarju s karakteristiko  $r$  je  $r \cdot x = 0$  za vsak  $x \in K$ .

**Dokaz.** Pokažimo takole:

$$\begin{aligned} r \cdot x &= \underbrace{x + x + \cdots + x}_r = 1 \cdot x + 1 \cdot x + \cdots + 1 \cdot x \\ &= \underbrace{(1 + 1 + \cdots + 1)}_r \cdot x = (r \cdot 1) \cdot x = 0 \cdot x = 0 \end{aligned}$$

□

**Trditev 6** Naj bo  $K$  celi kolobar. Potem je karakteristika  $r(K)$  bodisi 0 ali praštevilo.

**Dokaz.** Naj bo  $r = r(K)$  sestavljeno število različno od 0, recimo  $r = a \cdot b$  za  $a, b \neq 0, 1$ . Potem je  $a \cdot b \cdot 1 = 0$  in od tod  $(a \cdot 1) \cdot (b \cdot 1) = 0$ . Ker  $a \cdot 1 \neq 0$  ter  $b \cdot 1 \neq 0$ , dobimo, da sta  $a \cdot 1$  in  $b \cdot 1$  delitelja nič, kar je protislovje.



# Izrek o končnih obsegih

**Izrek 7** *Naj bo  $F$  končen obseg. Potem velja:*

(a)  *$F$  je komutativen*

(b)  *$|F|$  je potenca praštevila*

(c) *grupa  $(F \setminus \{0\}, \cdot)$  je ciklična*

(d) *Naj bo  $F_1$  obseg in  $|F_1| = |F|$ , potem  $F_1 \cong F$ .*

Končnemu obsegu oz. polju s  $p^n$  elementi rečemo **Galoisovo polje reda  $n$**  in ga označimo z  **$\mathbf{GF}(p^n)$** .

# Polinomi

$K$  je komutativen kolobar;

$K[X]$  je množica vseh polinomov s koeficienti iz  $K$ ;

Označimo s ”+” in ”·” običajno seštevanje in množenje polinomov;

Označimo z  $\deg(p)$  stopnjo polinoma  $p(x)$ ;

**Zgled:** Če v kolobarju  $\mathbb{Z}_6[x]$  seštejemo ter zmnožimo polinoma:

$$p(x) = 2x^2 + 3 \quad \text{in} \quad q(x) = 3x + 1,$$

dobimo rezultat:

$$p(x) + q(x) = 2x^2 + 3x + 4$$

$$p(x) \cdot q(x) = 6x^3 + 2x^2 + 9x + 3 = 2x^2 + 3x + 3$$

V splošnem veljata naslednji neenakosti:

$$\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$$

$$\deg(p \cdot q) \leq \deg(p) + \deg(q)$$

V primeru, da je kolobar cel oz. brez deliteljev nič, imamo zgoraj enačaja.

**Trditev 8** *Pokaži, da je  $(K[x], +, \cdot)$  kolobar.*

**Dokaz.**

# Deljenje polinomov

**Naloga 3** Naj bosta  $f(x) = x^4 + x^3 + 2x + 2$  in  $g(x) = x^2 + 4$  polinoma iz  $\mathbb{Z}_5[x]$ . Izračunaj količnik  $q(x)$  ter ostanek  $r(x)$  pri deljenju  $f(x)$  z  $g(x)$ .

Polinoma  $q(x)$  in  $r(x)$  iz zgornjega primera imenujemo **količnik** in **ostanek** pri deljenju  $f(x)$  z  $g(x)$ .

**Opomba 1** Če je  $\deg(g) > 0$ , potem velja  $\deg(r) < \deg(g)$ !

# Evklidov izrek za polinome

**Izrek 9** Naj bo  $F$  polje in  $f(x), g(x) \in F[x]$ , kjer je  $\deg(g) > 0$ . Potem obstajata enolično določena polinoma  $q(x), r(x) \in F(x)$  tako, da velja:

$$f(x) = q(x) \cdot g(x) + r(x) \quad \text{in} \quad 0 \leq \deg(r) < \deg(g).$$

**Dokaz.** Označimo s  $q(x)$  in  $r(x)$  koeficient ter ostanek pri deljenju  $f(x)$  z  $g(x)$ . Očitno za tako podana  $q(x)$  in  $r(x)$  velja zgornja zveza.

Zdaj pokažemo, da sta  $q(x)$  in  $r(x)$  enolično določena. Če to ni res, potem obstajata  $q'(x)$  in  $r'(x)$ , za katera velja

$$f(x) = q'(x) \cdot g(x) + r'(x) \quad \text{in} \quad 0 \leq \deg(r') < \deg(g).$$

Potem sklepamo, da je

$$(q(x) - q'(x)) \cdot g(x) = r'(x) - r(x)$$

Če  $q(x) \neq q'(x)$ , potem je leva stran polinom stopnje vsaj  $\deg(g)$ , desna stran pa polinom stopnje strogo manjše od  $\deg(g)$ , kar ni možno. Torej  $q(x) = q'(x)$  in od tod  $r(x) \neq r'(x)$ .

# Ničle polinoma

Element  $\alpha \in K$  je **ničla** oz. **koren** polinoma  $p(x) = a_n x^n + \dots + a_1 x + a_0$ , če velja  $p(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$ .

**Trditev 10** Če je  $\alpha$  ničla polinoma, potem obstaja polinom  $q(x)$  tako, da je

$$p(x) = (x - \alpha)q(x).$$

**Dokaz.** Naj bo  $p(x) = a_n x^n + \dots + a_1 x + a_0$ . Ker je  $p(\alpha) = 0$ , sklepamo:

$$\begin{aligned} p(x) &= p(x) - p(\alpha) \\ &= a_n(x^n - \alpha^n) + \dots + a_1(x - \alpha). \end{aligned}$$

Iz znane zveze

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$

sklepamo, da obstaja polinom  $q(x)$  stopnje  $n - 1$ , za katerega velja

$$p(x) = (x - \alpha)q(x).$$

□

**Posledica 11** Polinom  $p(x) \in K[x] \setminus \{0\}$  stopnje  $n$  ima kvečjemu  $n$  ničel.

## (Ne)razcepni polinomi

Polinom  $p(x) \in K[x]$  je **razcepen** nad  $K[x]$ , če obstajata polinoma  $p_1(x), p_2(x) \in K[x]$  tako, da

$$p(x) = p_1(x) \cdot p_2(x) \quad \text{in} \quad 0 < \deg(p_1), \deg(p_2) < \deg(p)$$

Polinomi, ki niso razcepni, so **nerazcepni**.

**Vprašanje 3** Ugotovi, kateri od naslednjih polinomov so razcepni v  $\mathbb{Z}_2[x]$ :

- $x^2 + 1$
- $x^2 + x + 1$
- $x^3 + x + 1$
- $x^4 + x^2 + 1$

Velja: Vsak polinom stopnje 1 je nerazcepen.

**Trditev 12** Naj bo  $p(x) \in K[x]$  polinom stopnje 2 ali 3. Potem je  $p(x)$  razcepen natanko takrat, ko ima ničlo.

# Modulski polinomi

Ostanek pri deljenju polinoma  $f(x)$  s polinomom  $g(x)$  označimo z  $f(x) \bmod g(x)$ .

Naj bo  $m(x)$  polinom stopnje  $n$  – **modulski polinom**

Naj bo  $K^n[x]$  množica polinomov stopnje manjše od  $n$ , tj.

$$K^n[x] = \{p(x) \in K[x] : \deg(p) < n\}.$$

**Vprašanje 4** Naj bo  $K$  končen kolobar z  $m$  elementi. Koliko elementov ima kolobar polinomov  $K^n[x]$ ?

**Odgovor:**

Množenje  $\cdot_m$  polinomov iz  $K^n[x]$  definiramo takole

$$p(x) \cdot_m q(x) = p(x) \cdot q(x) \bmod m(x)$$

**Zgled:** Zmnoži  $f(x) = x^2 + 2$  ter  $g(x) = x^2 + x + 1$  v kolobarju polinomov nad  $\mathbb{Z}_3$  po modulu  $m(x) = x^3 + x + 1$ .



**Problem 2** *Pokaži, da je  $(K^n[x], +, \cdot_m)$  kolobar.*

**Rešitev:**

# Galoisova polja $\mathbf{GF}(p^n)$

**Izrek 13** *Kolobar  $(K^n[x], +, \cdot_m)$  nad poljem  $K$  je polje natanko takrat, ko je modulski polinom  $m(x)$  nerazcepen.*

**Zgled:** Sestavi polje  $\mathbf{GF}(4)$  tako, da vzameš  $m(x) = x^2 + x + 1$  za modulski polinom.