

$$(x+y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} \quad \binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1 \cdot 2 \dots i} \text{ je večkratnik } p$$

$$\downarrow$$

$$\rightarrow = x^p + y^p$$

Osnovne lastnosti homomorfizma kolobarjev $f: K \rightarrow L$

vedno

$$\begin{cases} \bullet f(0) = 0 \\ \bullet f(-a) = -f(a) \end{cases}$$

$$f(0) = f(0+0) = f(0) + f(0) \Rightarrow f(0) = 0$$

$$0 = f(0) = f(a+(-a)) = f(a) + f(-a) \Rightarrow f(-a) = -f(a)$$

"pogoj"

$$\begin{cases} \bullet f(1) = 1 \\ \bullet \text{če je } f \text{ unitalen in } a \text{ obrnljiv, potem je } f(a^{-1}) = f(a)^{-1} \end{cases}$$

v splošnem ne velja $f(1) = 1$ (npr. pri matrikah)

Če je $f(1) = 1$, pravimo da je f **unitalen homomorfizem**

$$1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) \Rightarrow f(a) \text{ ima desni inverz}$$

podobno ima levi inverz $\Rightarrow f(a^{-1}) = (f(a))^{-1}$

Kdaj je homomorfizem $f: K \rightarrow L$ surjektiven/injektiv?

$\rightarrow$ "image", slika f

• Zaloge vrednosti: $\text{Im } f = f(K) = \{f(a) \mid a \in K\}$ je podkolobar v L

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

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

$$f \text{ je surjektiv} \Leftrightarrow \text{Im } f = L$$

$$- a, b \in K \quad f(a) = f(b) \rightsquigarrow 0 = f(a) - f(b) = f(a-b)$$

$$\rightsquigarrow a-b \in f^{-1}(0)$$

$$f^{-1}(0) \text{ je podkolobar v } K$$

$f^{-1}(0)$ je podkolebar v K

$$a, b \in f^{-1}(0)$$

$$a+b \in f^{-1}(0)$$

$$a \cdot b \in f^{-1}(0)$$

$$-a \in f^{-1}(0)$$

$$f(a+b) = f(a) + f(b) = 0 + 0 = 0$$

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

$$f(-a) = -f(a) = -0 = 0$$

$$f \text{ je injektiven} \Leftrightarrow f^{-1}(0) = \{0\}$$

$$f^{-1}(0) =: \text{Ker}(f) \leq K$$

jedro ('kernel')

$$a \in K, x \in \text{Ker } f \Rightarrow a \cdot x, x \cdot a \in \text{Ker } f$$

$$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0 = 0 \Rightarrow a \cdot x \in \text{Ker } f$$

podobno za $x \cdot a$

$\text{Ker } f$ je podkolebar K , ki ima dodatno lastnost,
da absorbira množenje z elementi K

Podkolebar s to lastnostjo imenujemo **IDEAL**

$I \leq K$ je ideal, če je $I \leq K$ in velja $K \cdot I \subseteq I, I \cdot K \subseteq I$
pičemo $I \triangleleft K$

$K' \leq K$ podkolebar

$I \triangleleft K$ ideal

Primeri

$\left. \begin{array}{l} K \text{ je ideal v } K \\ \{0\} \text{ " " v } K \end{array} \right\}$ "nepravilni" ideali

• soda števila

$$2\mathbb{Z} \triangleleft \mathbb{Z}$$

podkolebar ✓

polj. število $\cdot$ soda števila je soda števila ✓

$n\mathbb{Z} \triangleleft \mathbb{Z}$ n poljuben

• ideali v $\mathbb{Q}$

$$I \triangleleft \mathbb{Q}$$

$$\text{demonstrirajmo } I \neq \{0\} \text{ o } f x \in I$$

$$\Rightarrow I = \mathbb{Q}$$

$$\frac{p}{q} = \frac{p}{qx} \cdot x \in I$$

obsegi nimajo pravih idealov

še več, pravi ideali ne vsebujejo obrnljivih elementov

$$a = \overset{K}{\underset{\psi}{(a \cdot x^{-1})}} \cdot \overset{I}{\underset{\psi}{x}} \in I$$

$$\mathbb{R}[x] \quad I = \{a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{R}\} \triangleleft \mathbb{R}[x]$$

podmodular $\vee$

p-lj. polinom. polinom delju $\neq x$ je delju $\neq x$

alternativno

$$I = \text{Ker}(f_0) \quad (f_0(p) = p(0))$$

$$\text{Ker}(f_a) = \{\text{polinomi} : p(a) = 0\} = \text{večkratniki } (x-a)$$

Podobno: večkratniki polinoma x^2 ali x^2+1

Ali so večkratniki (x^2+1) jedro nekega homomorfizma?

$$p(x) \in \mathbb{R}[x], \quad p(x) = (x^2+1) \cdot q(x)$$

$$f_i : \mathbb{R}[x] \rightarrow \mathbb{C}$$

$$p(x) \mapsto p(i)$$

$$\left(\begin{array}{l} \text{alternativno:} \\ p(x) \mapsto \text{ostanek pri} \\ \text{deljenju z } (x^2+1). \end{array} \right)$$

$$\text{Ker}(f_i) = \text{elementi } \mathbb{R}[x], \text{ ki so večkratniki } (x-i)$$

$$= \text{večkratniki } x^2+1 \quad ; \text{ to je res, ker niste}$$

$$\text{realni polinomi (k. imajo realne) nastopajo}$$

$$\text{kot konjugirani pari } (a+bi, a-bi)$$

$$(x+i)(x-i) \text{ sta ničli } \leadsto \text{polinom je delju } (x+i)(x-i) = x^2+1$$

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$a_n, \dots, a_0 \in \mathbb{R}$$

$$z \in \mathbb{C}, \quad p(z) = 0$$

$$a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = 0$$

$$p(\bar{z}) = \underbrace{\bar{a}_n}_{a_n} (\bar{z})^n + \underbrace{\bar{a}_{n-1}}_{a_{n-1}} (\bar{z})^{n-1} + \dots + \underbrace{\bar{a}_1}_{a_1} \bar{z} + \underbrace{\bar{a}_0}_{a_0} = 0$$

Ali je ideal $n\mathbb{Z} \triangleleft \mathbb{Z}$ jedro nekega homomorfizma?

$$n\mathbb{Z} \text{ je jedro homomorfizma } \mathbb{Z} \xrightarrow{(\text{mod } n)} \mathbb{Z}_n$$

$\left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \in M_2(\mathbb{R}) \mid x, y \in \mathbb{R} \right\}$ je podkolobar; je tudi ideal?

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \cdot \begin{pmatrix} x' & 0 \\ y' & 0 \end{pmatrix} = \begin{pmatrix} xx' & 0 \\ yy' & 0 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} ax+by & 0 \\ cx+dy & 0 \end{pmatrix} \quad \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ax & bx \\ ay & by \end{pmatrix}$$

V nekomutativnih kolobarjih moramo ločiti

leve ideale, desne ideale, dvostranske ideale

$$K \cdot I \subseteq I$$

$$I \cdot K \subseteq I$$

oboje

• Jedro homomorfizma je vedno dvostranski ideal.

Posebno pomembni so ideali oblike $K \cdot x = \{kx \mid k \in K\}$,

rečemo jim **glavni ideali** (principal ideal), označimo jih (x) .

Primeri

• $\mathbb{Z}$ so vsi ideali glavni

$$I \triangleleft \mathbb{Z} \rightarrow I = \{0\}$$

če $I \neq \{0\}$, potem obstaja najmanjši pozitivni elt $x \in I$

$$\begin{array}{l} \text{--- } I = (x) \quad a \in I \quad a = k \cdot x + l, \quad k, l \in \mathbb{Z}, \quad \overset{\text{ostatek}}{l < x} \\ \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\ \quad \quad \quad I \quad \quad \quad I \end{array} \rightsquigarrow \underbrace{a - kx}_e \in I \Rightarrow l = 0 \quad a \in (x)$$

Rečemo, da je $\mathbb{Z}$ **glavnoidealni kolobar**

(principal ideal domain = PID)

↳ glavnoidealni + brez deliteljev nič

K obseg $\rightsquigarrow K[x]$ je glavnoidealni

$$I \triangleleft K[x], \text{ obstaja } p(x) : I = (p(x))$$

$$I \neq (0)$$

$$x^3 + x^2 - 1 \in I \quad \frac{1}{2}x^3 + \frac{1}{2}x^2 - \frac{1}{2} \in I$$

$p(x) :=$ polinom najnižje stopnje v I
z vodilnim koeficientom 1
("monični polinom")

$$I = (p(x))$$

$$q(x) \in I$$

$$q(x) = p(x) \cdot k(x) + l(x), \quad \text{st}(l(x)) < \text{st}(p(x))$$

$$\uparrow$$

$$\uparrow$$

$$\hookrightarrow l(x) \in I \Rightarrow l(x) = 0$$

$\hookrightarrow q(x)$ je večkratnik $p(x)$

• $\mathbb{Z}[x]$ ideal generiran z 2 in x ($(2, x)$)

(ti polinomi oblike $a_1x + a_2x^2 + \dots + a_nx^n$ | a_i sodi.)

$(2, x)$ ni glavni ideal

glavni idealni, ni obseg

podobno:

v $\mathbb{R}[x, y] = (\mathbb{R}[x])[y]$ (x, y) = $\{x p(x, y) + y q(x, y) \mid p, q \in \mathbb{R}[x, y]\}$ ni glavni.
 $\hookrightarrow$ ni glavni idealni

$\mathbb{Z}_3$

0

1

2

$$(2 + (3)) + (5 + (3)) =$$

$$(1 + (3)) + (-7 + (3)) =$$

$$(3) = 3\mathbb{Z} \quad 3\mathbb{Z} + 0$$

$$3\mathbb{Z} + 1$$

$$3\mathbb{Z} + 2$$

$I \triangleleft K$ dvostranski ideal

K razdelimo na ekvivalenčne razrede glede na I

za $a, b \in K$: $a \sim b \Leftrightarrow a - b \in I$

$\sim$ je ekvivalenčna relacija

$\sim$ razdeli K na ekvivalenčne razrede

mnostvo ekvivalenčnih razredov $K/\sim$ običajno označimo K/I