DS2 VAJE 14

1. $(\mathbb{Z}_{pq}, +, \cdot)$ $\quad p, q$ PRAŠTEVILI.

POIŠČI VSE IDEALE IN KVOCIENTNE KOLOBARJE.

$$\langle x \rangle \subseteq \mathbb{Z}_{pq}$$

PODKOLOBAR GENERIRAN Z x

$$\langle x \rangle = \mathbb{Z}_{pq} \iff x \text{ TUJ } pq$$

$$\langle p \rangle = \{0, p, 2p, \dots, (q-1)p\}$$
$$\langle q \rangle = \{0, q, 2q, \dots, (p-1)q\}$$

$$\langle p, q \rangle = \mathbb{Z}_{pq}$$

$\langle p \rangle$ IDEAL ?

PODKOLOBAR ✓

$$\underset{\in \mathbb{Z}_{pq}}{x} \cdot \underset{\langle p \rangle}{y} \overset{?}{\in} \langle p \rangle$$

$$\underset{\mathbb{Z}_{pq}}{x} \cdot \underset{\langle p \rangle}{(y p)} = \underset{\langle p \rangle}{(x \cdot y) \cdot p}$$

JE IDEAL ✓

PODOBNO $\langle q \rangle$ JE IDEAL.

$$\mathbb{Z}_{pq} / \langle p \rangle$$

ODSEKI:

$$0 + \langle p \rangle = \{0, p, \dots, (q-1)p\}$$
$$1 + \langle p \rangle = \{1, p+1, \dots\}$$
$$2 + \langle p \rangle = \quad \vdots$$
$$\vdots$$
$$p-1 + \langle p \rangle$$
$$p + \langle p \rangle =$$
$$= \{p, 2p, \dots, 0\} = \langle p \rangle$$

mod p

$$(x + \langle p \rangle) + (y + \langle p \rangle) = (x+y) + \langle p \rangle$$
$$(x + \langle p \rangle) \cdot (y + \langle p \rangle) = (x \cdot y) + \langle p \rangle$$

mod p

$$\mathbb{Z}_{pq} / \langle p \rangle \cong \mathbb{Z}_p$$

$$f : \mathbb{Z}_p \to \mathbb{Z}_p / \langle p \rangle \qquad f(x) = x + \langle p \rangle$$

2. $K = \mathbb{Z}_4[x]$

POIŠČI VSE DELITELJE NIČA IN OBRNLJIVE EL. STOPNJE ≤ 1.

- $(a_1x+a_0)\cdot(b_nx^n+b_{n-1}x^{n-1}+\dots+b_0)=0$

$$a_1b_nx^{n+1}+(a_1b_{n-1}+a_0b_n)x^n+\dots+a_0b_0=0$$

$$\Rightarrow a_1b_n=0 \quad (\text{v } \mathbb{Z}_4)$$

$$\Rightarrow a_0b_0=0 \quad (\text{v } \mathbb{Z}_4)$$

$$\Rightarrow a_1\in\{0,2\} \qquad a_0\in\{0,2\}$$

$$a_0=a_1=0$$

$2x\cdot 2=0$ $\Rightarrow$ $2x \rightarrow$ JE DELITELJ 0

$(2x+2)\cdot 2=0$ $\quad$ $2x+2$

$2\cdot 2=0$ $\quad$ 2

- $(a_1x+a_0)(b_nx^n+\dots+b_0)=1$

$$a_1b_nx^{n+1}+\dots+a_0b_0=1$$

$\Rightarrow a_1b_n=0$ $\Leftarrow$ a_1 DELITELJ NIČA

$a_0\cdot b_0=1$ $\Leftarrow$ a_0 OBRNLJIV

$a_1 \in \{0, 2\}$, $a_0 \in \{1, 3\}$

1 ✓ $\qquad (2x+1)(2x+1) = 4x^2 + 4x + 1$

3 ✓ $\qquad = 1$ ✓

$(2x+3)(2x+3) = 4x^2 + 12x + 9$

$= 1$ ✓

3. $K = \mathbb{Z}_3[x]$

$I = \{ p(x)(x^2+2x+2) \mid p(x) \in K \}$

$= \langle x^2+2x+2 \rangle$

I IDEAL:

GRUPA ZA SEŠT.: $p_1(x) \cdot (x^2+2x+2)$

INVERZI: $-p(x)$ ✓ $\qquad + \; p_2(x) \cdot (x^2+2x+2)$

$= ((p_1+p_2)(x)) \cdot (x^2+2x+2)$

$$\underset{\substack{\uparrow \\ K}}{g(x)} \cdot \underbrace{p(x)(x^2+2x+2)}_{\in I} =$$

$$= (g(x) \cdot p(x)) \cdot (x^2+2x+2) \in I$$

K/I EL. SO OBLIKE $g(x)+I$

ČE $g(x) \in I \Rightarrow g(x)+I = I$

ZA POLJUBEN $g(x)$:

$$g(x) = (x^2+2x+2)p(x) + r(x)$$

$$g(x)+I = r(x) + (x^2+2x+2)p(x) + I$$

$$= r(x) + I$$

$\Rightarrow$ ODSEKI: $r(x)+I$

STOPNJE < 2

$\Rightarrow I,\ 1+I,\ 2+I,\ x+I,\ x+1+I,$
$x+2+I,\ 2x+I,\ 2x+1+I,\ 2x+2+I$

KAKO SEŠTEVAMO, MNOŽIMO?

$$(r_1(x)+I) + (r_2(x)+I) = (\underbrace{r_1(x)+r_2(x)}_{\text{ST.} < 2})+I$$

$$(r_1(x)+I)(r_2+I) = r_1(x)\cdot r_2(x) + I$$

ST. LAHKO 2

$$r_1(x)\cdot r_2(x) = p(x)\cdot(x^2+2x+2) + r_3(x)$$

$$r_1(x)r_2(x)+I = r_3(x)$$

RAČUNAMO:

$$x+I$$

$$(x+I)^2 = x^2+I = x+1+I$$

$$x^2 : x^2+2x+2 = 1$$

$$-x^2-2x-2$$

$$\boxed{x+1}$$

$$(x+I)^3 = x\cdot(x+1)+I = x^2+x+I$$

$$= x+1+x+I = 2x+1+I$$

$$(x+I)^4 = x\cdot(2x+1)+I = 2x^2+x+I$$

$$= 2\cdot(x+1)+x+I = 2+I$$

$$\vdots$$

$$(x+I)^8 = I$$

JE OBSEG

4.

$$K = \mathbb{Z}_5[x]$$

RAZCEPI: $x^4 + x^2 + 3x + 1 = p(x)$

$p(0) = 1 \Rightarrow 0$ NI NIČLA

$p(1) = 1 \Rightarrow 1$ NI NIČLA

$p(2) = 1 + 4 + 1 + 1 = 2 \Rightarrow 2$ NI NIČLA

$p(3) = 1 + 4 + 4 + 1 = 0 \Rightarrow 3$ JE NIČLA

$p(4) = 1 + 1 + 2 + 1 = 0 \Rightarrow 4$ JE NIČLA

$\Rightarrow (x-4)(x-3)$ DELI $p(x)$

$$\begin{gathered}(x-4)(x-3) \\ \| \\ x^2 - 7x + 12 = x^2 + 3x + 2\end{gathered}$$

$$\begin{array}{l}(x^4 + x^2 + 3x + 1) : (x^2 + 3x + 2) = x^2 + 2x + 3 \\ -x^4 - 3x^3 - 2x^2 \\ \quad 2x^3 + 4x^2 + 3x + 1 \\ \quad -2x^2 - 6x^2 - 4x \\ \qquad 3x^2 + 4x + 1 \\ \qquad\quad 0\end{array}$$

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

ALI IMA $\underset{g(x)}{\underbrace{x^2+2x+3}}$ NIČLE?

$$g(3) = 4+1+3 = 3 \neq 0$$
$$g(4) = 1+3+3 = 2 \neq 0$$

$\Rightarrow$ x^2+2x+3 JE NERAZCEPEN!

5. PREVERI, DA

$$f(x) = x^4+x+1$$

NI RAZCEPEN NAD $\mathbb{Z}_2$ (V $K = \mathbb{Z}_2[x]$).

NIČLE: $f(0) = 1 \neq 0$

$f(1) = 1+1+1 = 1 \neq 0$

$\Rightarrow$ NIMA LINEARNIH ČLENOV

$$(x^2+ax+b)\cdot(x^2+cx+d) = f(x)$$
$$\| $$
$$x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd$$

$a+c = 0$ $\Rightarrow a = c$

$b+d+ac = 0$ $ac = 0$ $a=0$ $c=0$

$$ad + bc = 1 \quad \Rightarrow \quad 0 + 0 = 1$$

$$bd = 1 \quad \Rightarrow b = 1 \quad d = 1$$

$\Rightarrow f(x)$ NERAZCEPEN

6. $K = \mathbb{Z}_3[x]$ $\qquad I_1 = \langle x^2 + 2x + 2 \rangle$

K / I_1 JE POLJE (3. NAL)

$$I_2 = \langle x^2 + 2x + 1 \rangle = \{ p(x) \cdot (x^2 + 2x + 1) \mid p(x) \in K \}$$

K / I_2 POLJE ?

ČE KOLOBAR KONČEN:

(KOLOBAR OBSEG $\Leftrightarrow$ KOLOBAR CEL)

NIMA DELITELJEV NIČA

ALI IMA K/I_2 DELITELJE NIČA?

$$\left(p_1(x)+I_2\right)\cdot\left(p_2(x)+I_2\right) = 0+I_2$$

ST. ≤ 1

$$p_1(x)\cdot p_2(x) + I_2 = 0 + I_2$$

$$\underbrace{p_1(x)\cdot p_2(x)}_{\text{ST} \leq 1} = g(x)\cdot\underbrace{(x^2+2x+1)}_{\text{ST. } 2} + \underbrace{r(x)}_{=0}$$

$$\Rightarrow x^2+2x+1 = p_1(x)\cdot p_2(x)$$

ALI $\underbrace{x^2+2x+1}_{= i_2(x)}$ JE RAZCEPEN?

LINEARNI ČLENI $\Leftrightarrow$ NIČLE

$i_2(0) = 1 \neq 0$ $\qquad$ $i_2(2) = 9 = 0$

$i_2(1) = 1 \neq 0$ $\qquad$ $\Rightarrow$ 2 JE NIČLA

$$x^2+2x+1 = (x-2)(x-2)$$

$\Rightarrow$ JE RAZCEPEN

$\Rightarrow$ $\mathbb{Z}_3[x] / \langle x^2+2x+1 \rangle$ NI CEL

$$\left((x-2)+I_2\right) \cdot \left((x-2)+I_2\right) = 0+I_2$$

$\Rightarrow$ NI POLJE