

K #5

3. ag dra 1) $f = x^4 + 2x^3 - x^2 - 4x - 2$

$g = x^4 + x^3 - x^2 - 2x - 2$

$$\begin{array}{r|l} x^4 + 2x^3 - x^2 - 4x - 2 & \\ -x^4 + x^3 - x^2 - 2x - 2 & \\ \hline x^3 & -2x \end{array} = q_1(x)$$

$$\begin{array}{r|l} x^4 + x^3 - x^2 - 2x - 2 & \\ -x^4 & -2x^2 \\ \hline x^3 + x^2 - 2x - 2 & \\ -x^3 & -2x \\ \hline x^2 & -2 \end{array}$$

$$\begin{array}{r|l} x^3 - 2x & \\ -x^3 + 2x^2 & \\ \hline 2x^2 - 2 & \\ -2x^2 + 2x & \\ \hline 2x & \\ -2x & \\ \hline 0 & \end{array} = q_2(x)$$

$$\begin{array}{r|l} 2x^2 - 2 & \\ -2x^2 + 2x & \\ \hline 2x & \\ -2x & \\ \hline 0 & \end{array} = q_3(x)$$

$$\begin{array}{r|l} 2x & \\ -2x & \\ \hline 0 & \end{array} = q_4(x)$$

$$f_1(x)$$

$r_1(x)$	$r_2(x)$
$x^3 - 2x$	$x^2 - 2$
$x^3 - 2x$	x

$= q_2(x)$

$r_3(x) = 0$

$$\Rightarrow d(f(x), g(x)) = x^2 - 2 = d$$

~~$$f(x) = g(x) \cdot q_1(x) + r_1(x)$$~~

$$r_2(x) = g(x) - r_1(x) q_2(x) =$$

$$= g(x) - (f(x) - g(x) q_1(x)) q_2(x) =$$

$$= g(x) - f(x) q_2(x) + g(x) q_1(x) q_2(x)$$

$$r_2(x) = -q_2(x) f(x) + (q_1(x) q_2(x) + 1) g(x)$$

$$d = u f + v g$$

$$\Rightarrow u = -q_2(x) = -x - 1$$

$$v = (x+1)(1) + 1 = x+2$$

$$x^2 - 2 = \underbrace{(x-1)}_u f + \underbrace{(x+2)}_v g$$

3. $I = (13 + 5\sqrt{6}) \triangleleft \mathbb{Z}[\sqrt{6}]$

$\mathcal{I}(\mathbb{Q}) \cap \mathbb{Z}[\sqrt{6}] = \{c + d\sqrt{6} \mid c, d \in \mathbb{Z}, 19 \mid (5c - 13d)\} = J : I = J$

$\mathbb{Z}[\sqrt{6}]/I \cong \mathbb{Z}_{19}$

$\mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6} \mid a, b \in \mathbb{Z}\}$

$I = \{(13 + 5\sqrt{6})(a + b\sqrt{6}) \mid a, b \in \mathbb{Z}\} = \{13a + 13\sqrt{6}b + 5\sqrt{6}a + 30b \mid a, b \in \mathbb{Z}\}$

~~$\{ (13 + 5\sqrt{6})a + (13\sqrt{6} + 30)b \mid a, b \in \mathbb{Z} \}$~~
 $= \{(13a + 30b) + (5a + 13b)\sqrt{6} \mid a, b \in \mathbb{Z}\}$

$(IC) \text{ } \cancel{13a + 30b} + \cancel{(5a + 13b)}\sqrt{6} \in I$

$5 \cdot (13a + 30b) - 13 \cdot (5a + 13b) =$
 $= 65a + 150b - 65a - 169b = -19b \Rightarrow 19 \mid -19b \in I$
 $\Rightarrow I \subseteq J$

$(JCI) \text{ } \text{Если } B \in J \text{ и } B = c + d\sqrt{6}$
 $\Rightarrow 19 \mid (5c - 13d)$

Получим $a, b \in \mathbb{Z} : \begin{cases} 13a + 30b = c \\ 5a + 13b = d \end{cases}$

$\Rightarrow 19b = 13d - 5c$

$19 \mid 13d - 5c$

$\Rightarrow b \in \mathbb{Z}$

$$5a + 13(13d - 5c) = d$$

$$5a = -168d + 65c$$

$$93a + 30(13d - 5c) = d$$

$$13a = 151c - 390d$$

$$\Rightarrow 3a + 2(-168d + 65c) = 151c - 390d$$

$$3a = 21c - 54d$$

$$a = 7c - 18d$$

$$\Rightarrow a \in \mathbb{Z}$$

$$\Rightarrow J \subseteq I \Rightarrow I = J$$

$$D(2). \mathbb{Z}[\sqrt{6}]/I \cong \mathbb{Z}_9$$

~~Ker~~

$$\text{Преположим } \varphi: \mathbb{Z}[\sqrt{6}] \rightarrow \mathbb{Z}_9$$

$$\text{Ker } \varphi = I = \{a + b\sqrt{6} \mid \varphi(a + b\sqrt{6}) = \bar{0}\}$$

$$\text{Im } \varphi = \mathbb{Z}_9 = \{ \bar{z} \in \mathbb{Z}_9 \mid \bar{z} \in \mathbb{Z}_9 \}$$

$$= \{ \varphi(z) \mid z \in \mathbb{Z}[\sqrt{6}] \}$$

~~q~~

$$\text{Тогда предположим } \varphi(a + b\sqrt{6}) = \overline{5a - 13b} \pmod{19}$$

$$\bullet \varphi(a + b\sqrt{6}) + \varphi(c + d\sqrt{6}) = \overline{5a - 13b} + \overline{5c - 13d} =$$

$$= \overline{5(a+c) - 13(b+d)} = \varphi(a + b\sqrt{6}) + \varphi(c + d\sqrt{6})$$

$$\begin{aligned} \varphi(a+b\sqrt{6}) \varphi(c+d\sqrt{6}) &= (5a-13b)(5c-13d) = \\ &= 25ac - 65ad - 65bc + 169bd = \cancel{5(5ac - 13ad - 13bc + 33bd)} \\ &= 5(5ac - 13ad - 13bc + 33bd) \end{aligned}$$

$$\begin{aligned} \varphi((a+b\sqrt{6})(c+d\sqrt{6})) &= \varphi(ac + ad\sqrt{6} + bc\sqrt{6} + bd\sqrt{6}) = \\ &= \varphi((ac+6bd) + (ad+bc)\sqrt{6}) = \\ &= 5ac + 30bd - 13ad - 13cb \end{aligned}$$

Тогда $f(\alpha) = K \cdot \varphi(\alpha)$, где $\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta)$, $\varphi(\alpha)\varphi(\beta) = 5\varphi(\alpha\beta)$, $3\alpha, \beta \in \mathbb{Z}_6$

$$f(\alpha) = K \cdot \varphi(\alpha+\beta) = K\varphi(\alpha) + K\varphi(\beta) = f(\alpha) + f(\beta)$$

$$f(\alpha\beta) = K \varphi(\alpha\beta)$$

$$f(\alpha)f(\beta) = K\varphi(\alpha) \cdot K\varphi(\beta) = 5K^2 \varphi(\alpha\beta)$$

$$\Rightarrow K = 5K^2$$

$$K(5K - 1) = 0 \quad (K \neq 0)$$

$$5K - 1 = 0$$

$$5K = 1$$

$$K = 5$$

$$\Rightarrow f(\alpha) = 5(5a-13b) \text{ e ханангд.}$$

$$\text{Im } f \subseteq \mathbb{Z}_{19}$$

$$f(1+0\sqrt{6}) = 5 \Rightarrow \text{Im } f \supseteq \mathbb{Z}_{19} \Rightarrow \text{Im } f = \mathbb{Z}_{19}$$

$$\text{Ker } f = I$$

$$\Rightarrow \mathbb{Z}[\sqrt{6}] / I \cong \mathbb{Z}_{19}$$

Zagada 3) R u S su nprilazni

$\therefore \mathcal{D}(\mathcal{D}) R \times S$ ne e nulle

Poredno R ~~ne~~ ima nule $\neq e_i \Rightarrow \exists \Gamma \in R$

$$(\Gamma, 0_S) \in R \times S \text{ u } (\Gamma, 0_S) \neq (0_R, 0_S)$$

Ustavljeno za $(0_R, S) \in R \times S$

Čeka ga razmišljanje:

$$(\Gamma, 0_S) \cdot (0_R, S) = (0_R, 0_S) \quad / \cdot (\Gamma, 0_S)^{-1}$$

pa znamo, da $(\Gamma, 0_S)^{-1}$ e definisano

~~$\neq \mathcal{D} R \times S$ ne e odrazak nula gl. na $\mathcal{D} S$~~

$$(\Gamma, 0_S)^{-1} (\Gamma, 0_S) (0_R, S) = (0_R, 0_S)$$

$$(0_R, S) = (0_R, 0_S)$$

Otpornost $c \ S \neq 0 \Rightarrow (\Gamma, 0_S)$ ima def. el.

$\Rightarrow R \times S$ ne e nulle

• Fleksa $K \triangleleft R \times S, \mathcal{D}(D) \ni I, J \triangleleft S, K = I \times J$

Fleksa $I = \{i \in R \mid \exists j; : (i, j) \in K\}$, uzl. gon. $\in I \triangleleft R$

u analognom $\in gon. za J$

• Fleksa $(a, b), (a', b') \in K$, moraba ~~a~~ $a, a' \in I$

$(a, b) - (a', b') = (a - a', b - b')$, ^{$\in K$ (zajedno $\in gon.$)} kamo $a - a' \in I$ (analogno)

• Fleksa $(a, b) \in K$ u $(c, d) \in R \times S$

$(a, b)(c, d) = (ac, bd) \in K \Rightarrow ac \in I$ za $\forall c \in R$

$(c, d)(a, b) = (ca, db) \in K \Rightarrow ca \in I$ za $\forall c \in R$

$\Rightarrow I \triangleleft R$

analogno za J , gon. $\in J \triangleleft S$

lem je bogami samo $I \times J = K$

$$(I \times J) \subseteq K \quad \text{Kako } i \in I \text{ u } j \in J \Rightarrow \exists s: (i, s) \in K \text{ u} \\ \exists r: (r, j) \in K$$

$$\text{Kako } (i, s), (r, j) \in K \Rightarrow (i, s) + (r, j) = (i+r, s+j) \in K$$

$$(K \subseteq I \times J) \quad \text{Kako } (i, j) \in K \Rightarrow i \in I \text{ u } j \in J \\ \Rightarrow K \subseteq I \times J$$

$$\Rightarrow I \times J = K$$

~~Ne postoji bez gen. za neposredno dokazivanje~~

| Treb. opreznosti pri primeni u mat. 1.)
za neposredno dokazivanje