7. Dokazati da $\mathbb{Z}[x]/(6) \cong \mathbb{Z}_6[x]$.

(6) = svi polinomi kod kojih su koeficijenti djeljivi sa 6

ideal generisan sa 6

$$I = \langle 6 \rangle = \{ \sum x_i \cdot 6 \mid x_i \in R \} = \{ x \cdot 6 \mid x \in \underset{\mathbb{Z}[x]}{\underset{\parallel}{R}} \}$$

$$f : \mathbb{Z}[x] \to \mathbb{Z}_6[x]$$

$$f(a_0 + \dots + a_n x^n) = \overline{a_0} +_6 \dots +_6 \overline{a_n} x^n, \quad \overline{a_i} = a_i \pmod 6$$

Npr.

$$7 + 6x + 8x^2 \xrightarrow{f} \overline{1} + \overline{2} x^2$$

$$g_1(x) = a_0 + \dots + a_n x^n$$
$$g_2(x) = b_0 + \dots + b_m x^m, \quad m \leq n$$

$$f(g_1(x) + g_2(x)) = f((a_0 + b_0) + \dots + (a_m + b_m) x^m + \dots + (a_n + \overset{0}{\overset{\parallel}{b_n}}) x^n) =$$

$$= \overline{(a_0 + b_0)} +_6 \dots +_6 \overline{(a_m + b_m)} x^m +_6 \dots +_6 \overline{(a_n + b_n)} x^n =$$

$$= (\overline{a_0} +_6 \overline{b_0}) +_6 \dots +_6 (\overline{a_n} +_6 \overline{b_n}) x^n =$$

$$= (\overline{a_0} +_6 \dots +_6 \overline{a_n} x^n) + (\overline{b_0} +_6 \dots +_6 \overline{b_n} x^n) = f(g_1(x)) +_6 f(g_2(x))$$

Analogno, $f(g_1(x) \cdot g_2(x)) = f(g_1(x)) \cdot_6 f(g_2(x))$

$$g_1(x) = \sum_{i=0}^{n} a_i x^i \quad , \quad g_2(x) = \sum_{j=0}^{m} b_j x^j$$

$$g_1(x) \cdot g_2(x) = \sum_{k=0}^{n+m} c_k x^k \quad , \quad c_k = \sum_{s=0}^{k} a_s b_{k-s}$$

$$L = f(g_1(x) \cdot g_2(x)) = \sum_{k=0}^{n+m} \overline{c_k} x^k \qquad \overline{c_k} = \sum_{s=0}^{k} \overline{a_s} \cdot \overline{b_{k-s}}$$

$$D = f(g_1(x)) \cdot f(g_2(x)) = \left(\sum_{i=0}^{n} \overline{a_i} x^i\right) \cdot \left(\sum_{j=0}^{m} \overline{b_j} x^j\right)$$

$$= \left(\sum_{k=0}^{n+m} d_k x^k\right)$$

$$d_k = \sum_{s=0}^{k} \overline{a_s} \cdot \overline{b_{k-s}} \quad \Rightarrow \quad \overline{c_k} = d_k$$

$$\boxed{L = D}$$

R - prsten , $a \in R$

$\uparrow$

komutativan

$$I = \langle a \rangle = \{ ra \mid r \in R \} \trianglelefteq R$$

$$I = \langle x^2+1 \rangle = \{ p \mid x^2+1 \mid p \}$$

1. Neka je ideal I generisan sa polinomom $p(x)$ u prstenu $F[x]$, F je polje. Dokazati da se polinomi $f(x)$ i $g(x)$ nalaze u istoj faktor klasi prstena akko

$$f(x) \underset{\uparrow}{\equiv} g(x) \pmod{p(x)}$$

daju isti ostatak pri dijeljenju sa $p(x)$

$\boxed{(\Leftarrow)}$

$$f(x) = q_1(x)\,p(x) + r(x)$$

$$g(x) = q_2(x)\,p(x) + r(x)$$

$$f(x) - g(x) = \underbrace{p(x)\big(q_1(x) - q_2(x)\big)}_{\in I}$$

$$f(x) - g(x) \in I \xrightarrow{\text{podgrupa}} g(x) - f(x) \in I$$

$$\underline{f(x) \in g(x) + I} \qquad \underline{g(x) \in f(x) + I}$$

$\Rightarrow$ f i g su u istoj klasi

$\boxed{(\Rightarrow)}$ $f(x) + I = g(x) + I$

$$f(x) = q_1(x)\cdot p(x) + r_1(x), \quad \deg(r_1) < \deg(p)$$

$$g(x) = q_2(x)\,p(x) + r_2(x), \quad \deg(r_2) < \deg(p)$$

$$\underbrace{q_1(x)p(x)}_{\in I} + r_1(x) + I = \underbrace{q_2(x)p(x)}_{\in I} + r_2(x) + I$$

$r_1(x) - r_2(x) \in I$

$\deg(r_1 - r_2) < \deg(p)$

$p(x) \mid (r_1(x) - r_2(x)) \Rightarrow r_1(x) - r_2(x) = p(x) z(x)$

$< \deg(p(x))$ $\underline{\deg}$ $\geq \deg p(x)$

$\Rightarrow r_1(x) - r_2(x) = 0$

$r_1(x) = r_2(x)$

$\underline{I}$ | F - polje, $p \in F[x]$

$I = \langle p \rangle$ - ideal gen. sa p

Tada je $F[x]/_I$ polje akko je p nesvodljiv u $F[x]$

(2.) Formirati multiplikativnu tablicu za $\mathbb{Z}_2[x]/_{x^3+1}$.

	$\bar{1}+I$	$\bar{1}x+I$	$\bar{1}x^2+I$	$\bar{1}+x$	$\bar{1}+x^2$	$x+x^2$	$\bar{1}+x+x^2$
$\bar{1}+I$	$1+I$	$x+I$	x^2+I	$1+x$	$1+x^2$	$x+x^2$	$1+x+x^2+I$
$x+I$	$x+I$	x^2	$1+I$	$x+x^2$	$x+1$	$1+x^2$	$1+x+x^2+I$
x^2+I	x^2	$1+I$	$x+I$	$1+x^2$	x^2+x	$1+x$	$1+x+x^2+I$
$\bar{1}+x$	$1+x$	$x+x^2$	$1+x^2+I$	$1+x^2+I$	x^2+x+I	$1+x+I$	$\bar{0}+I$
$\bar{1}+x^2$	$1+x^2$						
$x+x^2$	$x+x^2$					x^2+x	$\bar{0}+I$
$\bar{1}+x+x^2$	$1+x+x^2$						

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

	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	1	$\bar{2}=\bar{0}$

$x \cdot x^2 = x^3$

$x^3 : (x^3+1) = 1$

$\underline{-x^3 \pm 1}$

$-1 \equiv \bar{1}$

$(x+x^2)(x+x^2) \equiv x^2+x^3+x^3+x^4 \equiv x^2+\bar{1}+\bar{1}+x =$

$= x^2+\bar{0}+x =$

$= x^2+x$

$x^4 : (x^3+1) = x$

$\underline{-x^4 \pm x}$

$-x \equiv -\bar{1}\cdot x \equiv \bar{1}x$

x^3+1 je svodljiv

$\bar{0} \to \bar{1}$

$\bar{1} \to \boxed{\bar{0}}$ zad. 1. prošle vježbe

Euklidov algoritam

a, b

$b : a = g_1 (r_1)$

$\uparrow \quad \uparrow$

nep. ost.

$a : r_1 = g_2 (r_2)$

$r_1 : r_2 = g_3 (r_3)$

$\vdots$

$r_k : r_{k+1} = g_{k+2} (0)$

$\boxed{g_{k+1} (r_{k+1})}$ → NZD za a i b

$24 : 16 = 1 \ (\boxed{8})$ → NZD(24, 16)

$16 : 8 = 2 \ (0)$

3. Za polinome $f(x) = \bar{2}x^3 + \bar{2}x^2$, $g(x) = \bar{1}x^4 + \bar{2}x^2 + \bar{1}x$ iz $\mathbb{Z}_3[x]$ naći NZD, i prikazati taj polinom u obliku $\underbrace{d(x) = q(x)f(x) + h(x)g(x)}_{\text{slično kao 4. za domaćeg}}$

I/

$g(x) : f(x) = (\bar{1}x^4 + \bar{2}x^2 + \bar{1}x) : (\bar{2}x^3 + \bar{2}x^2) = \bar{2}x^1 + \bar{1}$

$\bar{1}x^4 + \bar{1}x^3$

$-x^3 + \bar{2}x^2 + \bar{1}x$

$\bar{2}x^3$

$\bar{2}x^3 + \bar{2}x^2$

$\bar{1}x$

$\cdot 3$	$\bar{1}$	$\cdot \bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

II/ $(\bar{2}x^3 + \bar{2}x^2) : (\bar{1}x) = \bar{2}x^2 + \bar{2}x$

$\vdots$

$0 \Rightarrow NZD(f, g) = \bar{1}x = d(x)$

$g(x) = f(x)(\bar{2}x + \bar{1}) + \bar{1}x = d(x)$

$d(x) = g(x) - (\bar{2}x + \bar{1})f(x) =$

$= g(x) + (\bar{1}x + \bar{2})f(x)$

$$\boxed{d(x) = (\bar{1}x + \bar{2})f(x) + g(x)\cdot\bar{1}}$$

4. $f(x) = \bar{1}x^4 + \bar{1}x^3 + \bar{1}x + \bar{2}$
$g(x) = \bar{1}x^4 + \bar{2}$ $\Big\} \in \mathbb{Z}_3[x]$

$nzd(f,g) = ?$

I/
$f(x) : g(x) = (\cancel{\bar{1}x^4} + \bar{1}x^3 + \bar{1}x + \cancel{\bar{2}}) : (\bar{1}x^4 + \bar{2}) = \bar{1}$
$\cancel{\bar{1}x^4} + \cancel{\bar{2}}$
$\bar{1}x^3 + \bar{1}x = r_1(x)$

II/
$(\cancel{\bar{1}x^4} + \bar{2}) : (\bar{1}x^3 + \bar{1}x) = \bar{1}x$
$-(\cancel{\bar{1}x^4} + \bar{1}x^2)$
$r_2(x) = \bar{2}x^2 + \bar{2}$

III/
$(\cancel{\bar{1}x^3} + \cancel{\bar{1}x}) : (\bar{2}x^2 + \bar{2}) = \bar{2}x$
$\cancel{\bar{1}x^3} + \cancel{\bar{1}x}$
0

$$\boxed{nzd(f,g) = \bar{2}x^2 + \bar{2}}$$

$f(x) = g(x) \cdot \bar{1} + (\underbrace{\bar{1}x^3 + \bar{1}x}_{r_1})$

$g(x) = \bar{1}x \cdot (\underbrace{\bar{1}x^3 + \bar{1}x}_{r_1}) + (\underbrace{\bar{2}x^2 + \bar{2}}_{r_2})$

$d = r_2$

$d(x) = g(x) + \bar{2}x(\underbrace{\bar{1}x^3 + \bar{1}x}_{r_1 = \bar{1}f - \bar{1}g = f + \bar{2}g})$

$d(x) = g(x) + \bar{2}x(f(x) + \bar{2}g(x)) =$
$= \underbrace{\bar{2}x}_{p(x)} f(x) + g(x)(\underbrace{\bar{1} + \bar{1}x}_{q(x)})$

5. Naći multiplikativni inverz u $\mathbb{Z}_5[x]/I$,

$I = \langle \underbrace{\bar{1}x^2+\bar{1}x+\bar{1}}_{p} \rangle$ za element $(\bar{1}x^2+\bar{2})+I$.

Pretpostavimo da je $\bar{1}x^2+\bar{1}x+\bar{1}$ nerastavljiv, pa na osnovu T. slijedi da je $\mathbb{Z}_5[x]/I$ polje, tj. svaki nenulti element ima inverz.

$$\left.\begin{array}{l} p(\bar{0}) = \bar{1} \\ p(\bar{1}) = \bar{3} \\ p(\bar{2}) = \bar{2} \\ p(\bar{3}) = \bar{3} \\ p(\bar{4}) = \bar{1} \end{array}\right\} \text{p nema nule} \Rightarrow \text{p nije svodljiv}$$

(zad. 1. prošle vj.)

$$(\cancel{\bar{1}x^2}+\bar{1}x+\bar{1}) : (\bar{1}x^2+\bar{2}) = \bar{1}$$
$$\underline{\cancel{\bar{1}x^2}+\bar{2}}$$
$$\bar{1}x^2+\bar{4} = r_1(x)$$

$$(\cancel{\bar{1}x^2}+\bar{2}) : (\bar{1}x^2+\bar{4}) = \bar{1}x+\bar{1}$$
$$\underline{\cancel{\bar{1}x^2}+\bar{4}x}$$
$$\bar{4}x^2+\bar{2}$$
$$\underline{\bar{1}x+\bar{4}}$$
$$\bar{3} = r_2(x)$$

$$(\cancel{\bar{1}x}+\bar{4}) : (\bar{3}) = \bar{2}x+\bar{3}$$
$$\underline{\cancel{\bar{1}x}}$$
$$\cancel{\bar{4}}$$
$$\underline{\cancel{\bar{4}}}$$
$$0$$

$p(x) = \bar{1}\, q(x) + r_1(x)$

$q(x) = r_1(x)\cdot(\bar{1}x + \bar{1}) + \bar{3} \,/\, \bar{2}$

$\bar{2}\, q(x) = (\bar{2}x + \bar{2})\, r_1(x) + \bar{1}$

$\bar{1} = \bar{2}\, q(x) + (\bar{3}x + \bar{3})\cdot(p(x) + \bar{4}\, q(x))$

$\bar{1} = (\bar{3}x + \bar{3})\, p(x) + q(x)\cdot(\bar{2}x + \bar{4})$

$\bar{1} + I = \underbrace{(\bar{3}x + \bar{3})\, p(x)}_{\in I} + q(x)(\bar{2}x + \bar{4}) + I \quad \left[\begin{array}{l} x \in G,\ G \text{ gr.} \\ x + G = G \end{array}\right]$

$\bar{1} + I = \underbrace{q(x)(\bar{2}x + \bar{4}) + I}$

$= (q(x) + I)\cdot(\bar{2}x + \bar{4} + I)$

mult. inverz za $q(x)$

6. U polju $\mathbb{Q}[x]/I$, I je ideal gen. sa $x^3 + 2x + 1$. Odrediti mult. inv. za $(x^2 + 1) + I$.

$\left.\begin{array}{l} p(1) = 1^3 + 2\cdot 1 + 1 = 4 \\ p(-1) = -1 - 2 + 1 = -2 \end{array}\right\} \Rightarrow p(x)$ je nesvodljiv nad $\mathbb{Q}$

$(ax^2 + bx + c + I)(x^2 + 1 + I) = 1 + I$

$ax^4 + bx^3 + (a+c)x^2 + bx + c + I = 1 + I$

$\cancel{x^3} : (x^3 + 2x + 1) = 1$

$\cancel{x^3} + 2x + 1$

$-2x - 1$

$$\cancel{x^4} : (x^3 + 2x + 1) = x$$
$$\underline{\cancel{x^4} + 2x^2 + x}$$
$$-2x^2 - x$$

$$\Rightarrow a(-2x^2 - x) + b(-2x - 1) + (a+c)x^2 + bx + c + I = 1 + I$$

$$x^2(-2a + a + c) + x(-a - 2b + b) + c - b + I = 1 + I$$

$$\underbrace{x^2(-a+c) + x(-a-b) + c - b}_{} + I = \underbrace{1}_{} + I$$

morajo biti jednake
jer su manjeg stepena od 3

$$\left.\begin{aligned} -a + c &= 0 \\ -a - b &= 0 \\ c - b &= 1 \end{aligned}\right\} \Rightarrow \boxed{\left(\frac{x^2}{2} - \frac{x}{2} + \frac{1}{2} + I\right)}$$

<u>II način.</u>

$$(\cancel{x^3} + 2x + 1) : (x^2 + 1) = x$$
$$\underline{\cancel{x^3} + x}$$
$$x + 1$$

$$(\cancel{x^2} + 1) : (x + 1) = x - 1$$
$$\underline{\cancel{x^2} + x}$$
$$\underline{-\cancel{x} + 1}$$
$$\underline{-\cancel{x} - 1}$$
$$2$$

$$\underline{(x + 1) : 2} = \frac{1}{2}x + \frac{1}{2}$$
$$0$$

$p(x) = x\,q(x) + r_1(x)$

$q(x) = r_1(x)(x-1) + 2$

$$2 = q(x) - (x-1)\big(p(x) - x\,q(x)\big) =$$
$$= q(x) - (x-1)\,p(x) + x(x-1)\,q(x) =$$
$$= -(x-1)\,p(x) + q(x)\left(1 + x^2 - x\right) \Big/ \cdot \frac{1}{2}$$

$$\underset{+I}{1} = \underbrace{\frac{-x+1}{2}\,p(x)}_{\in I} + \underbrace{q(x)\left(\frac{x^2}{2} - \frac{x}{2} + \frac{1}{2}\right)}_{\text{invert}}\ {}_{+I}$$

7. $f(x) = x^5 + 3x^4 + x^3 + 4x^2 - 3x - 1$

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

a) Ispitati djeljivost f sa g u $\mathbb{Z}$ (X)

b) U $\mathbb{Z}_5$ (✓)

b)
$$\left(\cancel{x^5} + \bar{3}x^4 + \cancel{x^3} + \bar{4}x^2 + \bar{2}x + \bar{4}\right) : \left(x^2 + x + \bar{1}\right) = x^3 + \bar{2}x^2 + \bar{3}x + \bar{4}$$
$$\cancel{x^5} + x^4 + \cancel{x^3}$$
$$\cancel{\bar{2}x^4} + \bar{4}x^2 + \bar{2}x + \bar{4}$$
$$-\left(\cancel{\bar{2}x^4} + \bar{2}x^3 + \bar{2}x^2\right)$$
$$\cancel{\bar{3}x^3} + \bar{2}x^2 + \bar{2}x + \bar{4}$$
$$\cancel{\bar{3}x^3} + \bar{3}x^2 + \bar{3}x$$
$$\cancel{\bar{4}x^2} + \cancel{\bar{4}x} + \cancel{\bar{4}}$$
$$\cancel{\bar{4}x^2} + \cancel{\bar{4}x} + \cancel{\bar{4}}$$
$$0$$