1° $x - y = a_1b_1 + \dots + a_nb_n - c_1d_1 - \dots - c_nd_n =$

$= \underbrace{a_1}_{\in I_1}\underbrace{b_1}_{\in I_2} + \dots + \underbrace{a_n}_{\in I_1}\underbrace{b_n}_{\in I_2} + \underbrace{(-c_1)}_{\in I_1}\underbrace{d_1}_{\in I_2} + \dots + \underbrace{(-a_n)}_{\in I_1}\underbrace{d_n}_{\in I_2} \in I_1 \cdot I_2$

2° $x = a_1b_1 + \dots + a_nb_n \in I_1 \cdot I_2$

$r \in R$

$x \cdot r = (a_1b_1 + \dots + a_nb_n)r = (a_1b_1)r + \dots + (a_nb_n)r =$

$= \underbrace{a_1}_{\in I_1}(\underbrace{b_1r}_{\in I_2}) + \dots + \underbrace{a_n}_{\in I_1}(\underbrace{b_nr}_{\in I_2}) \in I_1 \cdot I_2$

Analogno $r \cdot x \in I_1 \cdot I_2$.

$I_1 \cdot I_2 \triangleq R$

Def: $(R_1, +, \cdot), (R_2, +, \cdot)$ – prstena

$f : R_1 \to R_2$ je homomorfizam prstena ako

$(\forall a, b \in R_1)$:

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

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

$\operatorname{Ker} f = \{ x \in R_1 \mid f(x) = 0 \}$

(7.) Ako su R_1, R_2 prstenи, $f : R_1 \xrightarrow{\text{hom.}} R_2$

Dokazati da je Ker f ideal.

? $\operatorname{Ker} f \trianglelefteq R_1$?

D| $x, y \in \operatorname{Ker} f$

$f(x) = f(y) = 0$

? $f(x-y) = 0$?

$$f(x-y) = f(x+(-y)) = f(x) + f(-y) = 0 + 0 = 0$$

$$f(-y) = -f(y) \, ?$$

$$f(y+(-y)) = f(0) = 0$$

$$-f(y) \,/\, f(y) + f(-y) = 0$$

$$f(-y) = -f(y)$$

$$\Rightarrow (\operatorname{Ker} f, +) \leq (R_1, +)$$

$x \in \operatorname{Ker} f$

$r \in R_1$

? $x \cdot r \in \operatorname{Ker} f$? $\quad (r \cdot x \in \operatorname{Ker} f)$

$$f(x \cdot r) = f(x) \cdot f(r) = 0 \cdot f(r) = 0$$

$$f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0 = 0$$

$$\Rightarrow \operatorname{Ker} f \trianglelefteq R_1$$

$$f(0+0) = f(0)$$

$-f(0) /$ $f(0) + f(0) = f(0)$

$$f(0_{R_1}) = 0_{R_2}$$

(8.) Ako su R_1, R_2 prsteni sa jedinicom, $f : R_1 \xrightarrow[\text{hom.}]{\text{surj.}} R_2$ tada $f(1_{R_1}) = 1_{R_2}$.

D| Neka je $r \in R_2$ proizvoljno. Tada $\exists x \in R_1$ t.d. $f(x) = r$.

$$f(x \cdot 1_{R_1}) = f(x) \cdot f(1_{R_1}) = \underline{r \cdot f(1_{R_1})}$$

$$\overset{\|}{f(x)} = r$$

Analogno: $\underline{r = f(1_{R_1}) \cdot r}$

$\Rightarrow$ $f(1_{R_1})$ je jedinični el. za $\cdot$ u R_2, tj. $f(1_{R_1}) = 1_{R_2}$.

(9.) Osnovna teorema o homomorfizmu prstena:

R, S - prsteni, $f : R \xrightarrow{\text{hom.}} S$

Tada je $R/_{\text{Ker} f} \cong \text{Im} f$

? $\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n$?

Scanned by TapScanner

$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$

$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$

$f: \mathbb{Z} \to \mathbb{Z}_n$

$f(x) = x \bmod n$

$f(x+y) = (x+y) \bmod n = x \bmod n + y \bmod n =$
$= f(x) +_{\bmod n} f(y)$

$f(x \cdot y) = (x \cdot y) \bmod n = x \bmod n \cdot y \bmod n =$
$= f(x) \cdot_{\bmod n} f(y)$

$\text{Ker} f = \{x \in \mathbb{Z} \mid \underbrace{f(x) = 0}_{\text{"}}\} = n\mathbb{Z}$

$x \bmod n = 0$

$\text{Im} f = \mathbb{Z}_n$

Po osn. teoremi $\Rightarrow \mathbb{Z}/\text{Ker} f \cong \text{Im} f$ tj.

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

(10.) $I, J \trianglelefteq R \Rightarrow I \cdot J \subseteq I \cap J$?

$\{a \cdot b \mid a \in I, b \in J\}$

Nekaj je $a \cdot b \in I \cdot J$ tj. $a \in I, b \in J$.

I je ideal $\Rightarrow$ $a \in R$, $b \in I$, $a \cdot b \in I$

J je ideal $\Rightarrow$ $a \in R$, $b \in J$, $a \cdot b \in J$

$\Rightarrow a \cdot b \in I \cap J$

(11.) Neka je u prstenu R ideala I_1, I_2 takvi da je $I_1 + I_2 = R$, a $I_1 \cap I_2 = \{0\}$. Dokažati da je $R \cong I_1 \times I_2$.

Dokaz: $\forall x \in R$, $x = a_1 + a_2$, $a_1 \in I_1$, $a_2 \in I_2$

Ako bi $x = a_1 + a_2$ i $x = b_1 + b_2$ onda je:

$a_1 + a_2 = b_1 + b_2$

$a_2 - b_2 = -a_1 + b_1 = 0 \in I_1 \cap I_2$

($a_2 - b_2 \in I_2$, $-a_1 + b_1 \in I_1$)

$\Rightarrow$ $a_1 = b_1$, $a_2 = b_2$ } jedinstveno predstavljanje

$f : I_1 \times I_2 \to R$

$f(a_1, a_2) = a_1 + a_2$

$f((a_1, a_2) \oplus (b_1, b_2)) = f(a_1 + b_1, a_2 + b_2) =$

$= a_1 + b_1 + a_2 + b_2 = a_1 + a_2 + b_1 + b_2 = f(a_1, a_2) + f(b_1, b_2)$

prsten

$$f((a_1,a_2)\cdot(b_1,b_2)) = f(a_1b_1, a_2b_2) =$$

$$= a_1b_1 + a_2b_2$$

$$f(a_1,a_2)\cdot f(b_1,b_2) = (a_1+a_2)(b_1+b_2) =$$

$$= a_1b_1 + \underbrace{a_1b_2} + \underbrace{a_2b_1} + a_2b_2$$

Prethodni rad. $\Rightarrow I\cdot J \subseteq I \cap J$

$I_1 \cdot I_2 \subseteq I_1 \cap I_2 = \{0\} \Rightarrow a_1b_2 = 0,\ a_2b_1 = 0$

f je hom.

"1-1" i "na" analogno kao za dir. pr. grupa

(12.) Dokazati da je $Aut(\mathbb{Q}) = \{Id_{\mathbb{Q}}\}$.

D| $f(0) = 0$ ($f: \mathbb{Q} \to \mathbb{Q}$ automorfizam prstena $\mathbb{Q}$)

$f(1) = f(1\cdot 1) = f(1)\cdot f(1)$

$a = a^2 \Rightarrow a = 0 \vee a = 1$

$\underbrace{\quad}_{\times}$

jer je bij.

$\Rightarrow f(1) = 1$

$n \in \mathbb{N}$

$f(n) = f(\underbrace{1+\cdots+1}_{n}) = n\cdot f(1) = n$

$f(-n+n) = f(0) = 0$

$f(-n) + f(n) = 0$

$f(-n) = -f(n) = -n$

$f\left(n \cdot \frac{1}{n}\right) = f(1) = 1$

$f(n) \cdot f\left(\frac{1}{n}\right) = 1$

$f\left(\frac{1}{n}\right) = \frac{1}{f(n)} = \frac{1}{n}$

$f\left(\frac{p}{2}\right) = f\left(\underbrace{\frac{1}{2} + \cdots + \frac{1}{2}}_{p}\right) = p \cdot f\left(\frac{1}{2}\right) = p \cdot \frac{1}{2} = \frac{p}{2}$

$f\left(-\frac{p}{2}\right) = -f\left(\frac{p}{2}\right) = -\frac{p}{2}$

$\Rightarrow f = Id_{\mathbb{Q}}$

Vježbe

Prsten polinoma

R - prsten

Def. Beskonačni niz elemenata $a_0, a_1, \dots, a_n$ od kojih je samo konačno mnogo njih različito od nule, nazivamo polinomom nad R.

$a_0 + a_1 x + \dots + a_n x^n$ $\qquad R[x]$

$(a_0, a_1, \dots, a_n) + (b_0, b_1, \dots, b_k) =$

$= (a_0 + b_0, a_1 + b_1, \dots)$

$(a_0, a_1, \dots, a_n) \cdot (b_0, b_1, \dots, b_m) = (c_0, c_1, c_2, \dots)$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

$$\deg(p) = \max\{ n \mid a_n \neq 0 \}$$

$\deg(p \cdot q) = \deg(p) + \deg(q)$, ako je F polje.

Def. $\alpha \in R$ je nula polinoma $p = (a_0, a_1, \dots, a_n)$ ako vrijedi:

$a_0 + a_1 \alpha + a_2 \alpha^2 + \dots + a_n \alpha^n = 0$

$p(\alpha) = 0$

T] $(R,+,\cdot)$ - komutativan prsten sa jedinicom

$(\forall p(x) \in R[x])(\exists q(x) \in R[x])$

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

T] $(R,+,\cdot)$ - komutativni, sa jedinicom

$p, q \in R[x]$

$\exists s(x), r(x) \quad p(x) = q(x)s(x) + r(x), \deg r < \deg q$

Def] Kažemo da je polinom f reducibilan (ireducibilan) nad R ako se polinom f može prikazati kao $f(x) = p(x) \cdot q(x)$, $0 < \deg p, \deg q < \deg f$.

① Polinom drugog i trećeg stepena nad poljem F je svodljiv ako ima nulu u F.

D] ($\Rightarrow$) Neka je f svodljiv.

$f = p \cdot q$

Jedan od polinoma p, q je stepena 1.

Neka je $p(x) = a_0 + a_1 x$

$p(x) = 0$

$a_0 + a_1 x = 0$

$a_1 x = -a_0 \Rightarrow x = (a_1^{-1})(-a_0)$ gde je F polje

$$p(a_1^{-1}\cdot(-a_0)) = a_0 + \underbrace{a_1\cdot a_1^{-1}}\cdot(-a_0) = a_0 - a_0 = 0 \Rightarrow$$

$$\Rightarrow \quad p(\alpha) = 0$$

$$f(x) = p(x)\cdot q(x)$$

$$f(\alpha) = p(\alpha)\cdot q(\alpha) = 0\cdot q(\alpha) = 0$$

($\Leftarrow$) Nela $\mathbb{F}$ ima nule.

$$(\exists \alpha) \quad f(\alpha) = 0$$

$$\xRightarrow{T.} f(x) = (x-\alpha)\,q(x) + \underbrace{f(\alpha)}_{=0}$$

$$f(x) = (x-\alpha)\,q(x) \Rightarrow f(x) \text{ je reducibilen}$$

$(x^2+1)^2 = (x^2+1)(x^2+1)$ - reducibilen ali nema nule!

(2.) Da li je $p(x) = \bar{1}x^3 + \bar{1}x + \bar{1} \in \mathbb{Z}_5[x]$ ireducibilen nad $\mathbb{Z}_5$?

$p(\bar{0}) = \bar{1}$
$p(\bar{1}) = \bar{3}$
$p(\bar{2}) = \bar{1}$
$p(\bar{3}) = \bar{1}$
$p(\bar{4}) = \bar{4}$

$\deg(p) = 3$

$\mathbb{Z}_5$ je polje jer je 5 prost

(zad. 1.) $\Rightarrow$ p je neireducibilen

Algoritam Kriterijum:

Polinom $f(x) = a_0 + \dots + a_n x^n$ je nesvodljiv nad $\mathbb{Q}$ ako postoji prost broj p t.d. $p \mid a_0, p \mid a_1, \dots, p \nmid a_n \wedge p^2 \nmid a_0$. ∎

(3.) Ispitati svodljivost polinoma nad poljem $\mathbb{Q}$:

a) $f(x) = x^2 + 4x + 2$

b) $f(x) = x^3 - x^2 - 4$

c) $f(x) = x^{50} + 14x - 56$

a) $2 \mid 2, \ 2 \mid 4, \ 2 \nmid 1, \ 2^2 \nmid 2 \Rightarrow f$ je nesvodljiv

I način.

$x^2 + 4x + 2 = 0$

$$x_{1,2} = \frac{-4 \pm \sqrt{16 - 8}}{2} = \frac{-4 \pm \sqrt{8}}{2} \notin \mathbb{Q}$$

T.

$\Rightarrow$ nesvodljiv

b) $f(x) = x^3 - x^2 - 4$

$\pm 1, \pm 2, \pm 4$

$f(2) = 2^3 - 2^2 - 4 = 8 - 4 - 4 = 0 \Rightarrow$ svodljiv

c) $f(x) = x^{50} + 14x - 56$

$p = 7 \qquad 7 \mid (-56), \ 7 \mid 14, \ 7 \nmid 1, \ 49 \nmid (-56)$

A.k
$\Longrightarrow$ nesvodljiv

④. Neka su r_a, r_b ostaci pri dijeljenju $p(x)$ sa $x-a, x-b$ respektivno, $a \neq b$.
Kolika je ostatak pri dijeljenju $p(x)$ sa $(x-a)(x-b)$?

$$p(x) = (x-a)\,q_1(x) + r_a = p(a)$$

$$p(a) = r_a$$

$$p(x) = (x-b)\,q_2(x) + r_b = p(b)$$

$$p(b) = r_b$$

$$p(x) = (x-a)(x-b)\,q(x) + \underbrace{r(x)}_{=mx+n}$$

$$p(a) = r_a \Rightarrow \boxed{ma + n = r_a}$$

$$p(b) = r_b \Rightarrow \boxed{mb + n = r_b}$$

$$m(a-b) = r_a - r_b \Rightarrow \boxed{m = \frac{r_a - r_b}{a-b}}$$

$$ma + n = r_a$$

$$n = r_a - ma = r_a - \frac{r_a - r_b}{a-b}\,a = \boxed{\frac{r_b a - r_a b}{a-b}}$$

$$r(x) = \frac{r_a - r_b}{a-b}\,x + \frac{r_b a - r_a b}{a-b}$$

(5) Ostaci pri dijeljenju $p(x)$ sa $x-1, x-2, x-3$ su 3, 7, 13 respektivno. Nađi ostatak pri dij. $p(x)$ sa $(x-1)(x-2)(x-3)$.

(R) $p(x) = q(x)(x-1)(x-2)(x-3) + \underbrace{ax^2+bx+c}_{\text{polinom stepena} \leq 2}$.

$p(x) = (x-1)S_1(x) + p(1)$, $p(1) = 3$

$p(1)=3$
$p(2)=7$
$p(3)=13$

$$\begin{cases} a+b+c=3 \\ 4a+2b+c=7 \\ 9a+3b+c=13 \end{cases}$$

$a=b=c=1$

R prsten

$a \in R$

$I = \langle a \rangle = \{ \sum_i x_i a y_i + r_j \cdot a + a \cdot q_k \mid x_i, y_i, r_j, q_k \in R \}$.

R komutativan

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

Ako je F polje $f(x) = a_0 + a_1 x + \dots + a_n x^n = \sum_{k=0}^{n} a_k x^k$

$f'(x) = a_1 + 2a_2 x + \dots = \sum_{k=1}^{n} k \cdot a_k x^{k-1}$

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

b) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$

c) $(\alpha f(x))' = \alpha f'(x)$

d) $(f^n(x))' = n \cdot f^{n-1}(x) \cdot f'$

$(x-1)^2 \to 1$
$2(x-1) \to 1$
} višestrukosti 2

2

Def. $\alpha \in F$ je nula polinoma $f(x) \in F[x]$ višestrukosti k ako je:
$f(\alpha) = 0,\ f'(\alpha) = 0,\ \dots,\ f^{(k-1)}(\alpha) = 0,\ f^{(k)}(\alpha) \neq 0$

(6.) Dokazati da je a nula polinoma
$f(x) = 2x^{n+1} - n(n+1)a^{n-1}x^2 + 2(n^2-1)a^n x - n(n-1)a^{n+1}$
višestrukosti 3, ako je $a \neq 0$.

$f(a) = 2a^{n+1} - n(n+1)a^{n-1}a^2 + 2(n^2-1)a^n a - n(n-1)a^{n+1} =$
$= a^{n+1}(2 - n^2 - n + 2n^2 - 2 - n^2 + n) = a^{n+1} \cdot 0 = 0$

$f'(x) = 2(n+1)x^n - n(n+1)a^{n-1} \cdot 2x + 2(n^2-1)a^n$

$f'(a) = 2(n+1)a^n - n(n+1)a^{n-1} \cdot 2a + 2(n^2-1)a^n =$
$= a^n(2n + 2 - 2n^2 - 2n + 2n^2 - 2) = a^n \cdot 0 = 0$

$f''(x) = 2n(n+1)x^{n-1} - 2n(n+1)a^{n-1}$

$f''(a) = 2n(n+1)a^{n-1} - 2n(n+1)a^{n-1} =$
$= a^{n-1}(2n^2 + 2n - 2n^2 - 2n) = a^{n-1} \cdot 0 = 0$

$f'''(x) = 2n(n+1)(n-1)x^{n-2}$

$f'''(a) = 2n(n+1)(n-1)a^{n-2} \neq 0$