

1) Naj bo K polje in $K[V]$ $K[x]$ -algebra, podana s
 $K[x] \rightarrow K[V]$
 $x \mapsto v^2$

$$\sum n_i x^i \mapsto \sum n_i v^{2i}$$

(Algebra:

- Kolobar
- $K[x]$ -modul
- $\lambda(x \cdot y) = (\lambda x) \cdot y = x \cdot (\lambda y)$

a) Pokaži, da je $K[V]$ prosti $K[x]$ -modul in $K[V] \cong K[x][t]/(t^2 - x)$.

b) Pokaži $B := K[V] \otimes_{K[x]} K[V] \cong K[V, W]/(V^2 - W^2)$.

c) Naj bo $\text{char} K \neq 2$. Pokaži, da B ni cel kolobar, nima (neničelnih) nilpotentov in $B \cong \{(f, g) \in K[V] \times K[V] ; f(a) = g(a)\}$.

d) Naj bo $\text{char} K = 2$. Poišči (neničelni) nilpotenti v B .

a) $K[V] \cong \bigoplus_{\text{nekaj kopij}} K[x]$

$$\lambda_0 + \lambda_1 v + \lambda_2 v^2 + \dots + \lambda_n v^n = \left(\begin{matrix} \text{ } \\ \text{ } \end{matrix} \right) \cdot \underbrace{\hspace{2cm}}_{\substack{\uparrow K[x] \\ \text{neodvisen od} \\ \lambda_0, \lambda_1, \dots}} + \left(\begin{matrix} \text{ } \\ \text{ } \end{matrix} \right) \cdot \underbrace{\hspace{2cm}}_{\substack{\uparrow K[x] \\ \text{neodvisen od} \\ \lambda_0, \lambda_1, \dots}} + \dots$$

diehtna?

$$x \cdot 1 = v^2$$

$$x \cdot v = v^3$$

$$x^2 \cdot v = v^5$$

$$(1+x) \cdot 1 = 1 + v^2$$

$$\Rightarrow \lambda_0 + \lambda_1 v + \lambda_2 v^2 + \dots + \lambda_n v^n = (\lambda_0 + \lambda_2 x + \dots) \cdot 1 + (\lambda_1 + \lambda_3 x + \dots) \cdot v$$

Direktna:

$$(N_0 + N_1 x + \dots) \cdot 1 \stackrel{?}{=} (\lambda_0 + \lambda_1 x + \dots) \cdot v$$

$$N_0 + \underbrace{N_1}_{\text{sodi}} v^2 + \dots = \lambda_0 v + \underbrace{\lambda_1}_{\text{lihi}} v^3 + \dots$$

$$N_i = \lambda_i = 0$$

✓

$$\text{Torej: } K[v] \cong K[x] \oplus K[x]$$

(Preverimo, da je homomorfizem modulov)

$$K[v] \cong K[x][T] / (T^2 - x)$$

baza:
 $\{1, v\}$

baza:
 $\{1, T\}$

$$a_0 + a_1 v \mapsto a_0 + a_1 T$$

Preveriti bi morali, ali ohranja množenje ...

Boljše:

$$K[x][T] \xrightarrow[\varphi]{K\text{-alg.}} K[v]$$

$K[x, T]$

$$\begin{aligned} x &\mapsto v^2 \\ T &\mapsto v \end{aligned}$$

$$\begin{aligned} (\sum \mu_i X^i) (\sum \nu_{j_k} X^{j_k} T^k) &\mapsto (\sum \mu_i v^{2i}) \cdot (\sum \nu_{j_k} v^{2j_k} v^k) \\ &\stackrel{?}{=} (\sum \mu_i X^i) (\sum \nu_{j_k} v^{2j_k} v^k) \end{aligned}$$

Vidimo: $T^2 - X \in \ker \varphi$

$$\begin{aligned} \sum \nu_{j_k} X^{j_k} T^k &= (\sum \lambda_i X^i) + (\sum \mu_\ell X^\ell) T \mapsto 0 \quad ? \\ &\mapsto \sum \lambda_i v^{2i} + \sum \mu_\ell v^{2\ell+1} \stackrel{?}{=} 0 \end{aligned}$$

Liki in sodi koeficienti se sestajajo v 0

$$\Rightarrow \lambda_i = \mu_i = 0$$

b) Hitro:

$$\begin{aligned} K[V] \otimes K[X][T]/(T^2 - X) &\cong \frac{(K[V] \otimes_{K[X]} K[X])[T]}{(T^2 - X)} \\ &\cong \frac{K[X][T]}{(T^2 - X)} \\ &\cong \frac{K[X][T]}{(T^2 - X)} \end{aligned}$$

Postopoma:

$$\phi: K[V] \otimes_{K[X]} K[V] \rightarrow K[V, W]/(V^2 - W^2)$$

$$\sum \mu_i \underbrace{(x_i(w))}_{K[V]} \otimes \underbrace{y_i(v)}_{K[V]} \mapsto \sum \mu_i x_i(v) y_i(w)$$

Univerzalna lastnost:

$$\begin{array}{ccc} A & \xrightarrow[\text{hom.}]{\varphi} & C \\ B & \xrightarrow[\text{hom.}]{\psi} & \end{array} \rightsquigarrow \begin{array}{ccc} A \otimes B & \rightarrow & C \\ a \otimes b & \mapsto & \varphi(a) \psi(b) \end{array}$$

Tudi za produkt $\otimes$ in koprodukt $\coprod$

Torej:

$$K[v] \xrightarrow{\varphi} K[v, w]/(v^2 - w^2) \\ v \mapsto v$$

$$K[v] \xrightarrow{\psi} K[v, w]/(v^2 - w^2) \\ v \mapsto w$$

Torej imamo dobro definirano ϕ

$$\psi: K[v, w] \longrightarrow K[v] \otimes_{K[x]} K[v] \\ \sum \lambda_{ij} v^i w^j \\ v \mapsto v \otimes 1 \\ w \mapsto 1 \otimes v$$

$$\text{Želimo: } (v^2 - w^2) \subseteq \ker \psi$$

$$\text{Torej bo: } K[v, w]/(v^2 - w^2) \xrightarrow{\tilde{\psi}} K[v] \otimes K[v]$$

$$\begin{aligned} \psi(v^2 - w^2) &= v^2 \otimes 1 + 1 \otimes v^2 \\ &= x \cdot 1 \otimes 1 - 1 \otimes x \cdot 1 \\ &= 1 \otimes x - 1 \otimes x \\ &= 0 \end{aligned}$$

$$\phi \circ \tilde{\psi} = \text{id} \quad ?$$

Vstavimo $v, w \dots$

$$\phi(\hat{\Psi}(v)) = \phi(v \otimes 1) = v \cdot 1 = v$$

$$\phi(\hat{\Psi}(w)) = \phi(1 \otimes w) = 1 \cdot w = w$$

$$\tilde{\Psi}(\phi(f \otimes g)) = \tilde{\Psi}(f(v) \cdot g(w)) = \underbrace{f(v \otimes 1)}_{f(v) \otimes 1} \cdot \underbrace{g(1 \otimes w)}_{1 \otimes g(w)} = f \otimes g$$

$$c) K[v, w]/(v-w)(v+w)$$

$$\text{CRT: } I+J = A \text{ algebra} \Rightarrow \frac{A}{I+J} \cong \frac{A}{I} \times \frac{A}{J}$$

$$\begin{aligned} I &= (v-w) \\ J &= (v+w) \end{aligned}$$

$$I+J = (v-w, v+w) = (v, w)$$

$$\begin{aligned} \text{Posplošen CRT: } \frac{A}{I \cap J} &\cong \{ (f, g) \in \frac{A}{I} \times \frac{A}{J} ; \overbrace{f=g}^c \pmod{I+J} \} \\ &\subseteq \frac{A}{I} \times \frac{A}{J} \end{aligned}$$

(velja vedno)

$$\begin{aligned} A &\rightarrow C \\ a &\mapsto (a \pmod{I}, a \pmod{J}) \end{aligned}$$

$$I \cap J \stackrel{\vee}{=} (v^2 - w^2)$$

$$(\geq) \checkmark$$

$$\begin{pmatrix} v-w \\ w-v \end{pmatrix} \mid \begin{pmatrix} f \\ f \end{pmatrix} \stackrel{\text{UFD}}{\Rightarrow} (v-w)(v+w) \nmid f$$

$$\cong \{ (f, g) \in K[v, w]/(v-w) \times K[v, w]/(v+w) ; f=g \pmod{I+J} \}$$

$$K[v, w]/(v-w) \cong K[y]$$

$$f(v, w) \xrightarrow{\text{"}v=w\text{"}} g(y, y)$$

$$f \equiv g \pmod{(v, w)} \stackrel{?}{\iff} f(a) = g(a)$$

$$\begin{aligned} \sum \mu_i v^i &\equiv \mu_0 \pmod{(v, w)} \\ \sum \lambda_{ij} w_j &\equiv \lambda_0 \pmod{(v, w)} \end{aligned}$$

$$K[v, w]/(v, w) \subseteq K$$

$$\lambda_0 + \sum_{i+j>0} \lambda_{ij} v^i w^j \mapsto \lambda_0$$

$$d) B \cong K[v, w]/(v^2 - w^2)$$

$$\text{char } K = 2 \Rightarrow v^2 - w^2 = (v - w)^2$$

$$\Rightarrow (v - w)^2 = 0 \pmod{v^2 - w^2}$$

$$\Rightarrow v - w \text{ nilpotent}$$

$$v - w \text{ stropnje } 1$$

$$v - w \text{ neničeln}$$

12.10.

1) Naj bo X množica in $R = \mathcal{P}(X)$ kolobar vseh podmnožic množice X , kjer je $A+B = (A \setminus B) \cup (B \setminus A)$ in $AB = A \cap B$.

a) Pokaži, da je neprazna družina $I \subseteq \mathcal{P}(X)$ ideal v R natanko tedaj, ko je zaprta za podmnožice in končne unije.

$$(\Leftrightarrow) \underline{A, B \in I} \Rightarrow \underline{A+B \in I}$$

$$\begin{aligned} A \setminus B &\subseteq A \in I \\ B \setminus A &\subseteq B \in I \end{aligned}$$

$$A+B = A \setminus B \cup B \setminus A \in I$$

$$\underline{A \in I, B \in \mathcal{P}(X)} \Rightarrow \underline{B \cdot A \in I}$$

$$B \cdot A = A \cap B \in I$$

$$(\Rightarrow) \underline{A \in I, B \subseteq A} \Rightarrow \underline{B \in I}$$

$$B \subseteq A$$

$$B = A \cap B = B \cdot A \in I$$

$$\underline{A, B \in I} \Rightarrow \underline{A \cup B \in I}$$

$$A \cup B = (A+B) \cup (A \cap B)$$

$\downarrow$
 $+$

$A+B$ in $A \cap B$ disjunktni

$$\text{Za } X \cap Y = \emptyset \text{ je } X \cup Y = X + Y$$

b) Določi glavni ideal (A) in ideal (A, B) za $A, B \in X$.
 Skleparj, da je vsak končno generiran ideal v R glavni.

$$(A) = A \cdot R = \{A \cdot B; B \in R\} = \{A \cap B; B \in R\} = P(A)$$

$$\underline{(A, B) = P(A \cup B)}$$

$$(\Leftarrow) A \cup B \in (A \cap B) \text{ po (a)}$$

$$\Rightarrow P(A \cup B) \subseteq (A, B)$$

$$(\Rightarrow) C \in (A, B)$$

$$C = \underbrace{A^1 \cdot A}_{\mathbb{R}} + \underbrace{B^1 \cdot B}_{\mathbb{R}} \subseteq A \cup B$$

$$\text{Dovolj: } A \in (A \cup B) \text{ in } B \in (A \cup B)$$

$$\Rightarrow C \in P(A \cup B)$$

$$(A_1, \dots, A_n) = (A_1, A_2) + (A_3, \dots, A_n)$$

$$= (A_1 \cup A_2, A_3, \dots, A_n)$$

$$= \dots$$

$$= (A_1 \cup \dots \cup A_n)$$

c) Naj bo X neskončna. Pokaži, da končne podmnožice množice X tvorijo ideal v $\mathcal{P}(X)$, ki ni končno generiran.

$$I \neq P(A) \text{ za nek } A \in P(X)$$

$$\Rightarrow A \text{ mora biti končno generiran}$$

$$\Rightarrow I \text{ neskončen, } P(A) \text{ pa končen}$$

$$\Rightarrow I \text{ ideal po (a)}$$

d) Kolobar je Boolov, če so vsi njegovi elementi idempotenti. Pokaži, da je vsak končen Boolov kolobar izomorfen $P(S)$ za neko končno množico S . Poišči neskončen Boolov kolobar, ki ni izomorfen nobenemu $P(S)$.

$R = \{a_1, \dots, a_n\}$ Boolov kolobar

$$a_i^2 = a_i$$

$$|P(S)| = 2^k \text{ v vsakem primeru}$$

$$n = 2^k \text{ za nek } k$$

$$e \in R$$

$$I = (e)$$

$$J = (1-e)$$

$$I + J = R$$

$$I \cdot J = 0$$

$$\text{CRT: } R/IJ \cong R/I \times R/J$$

$$R \cong R/(e) \times R/(1-e)$$

$$\cong R \cdot (1-e) \oplus R \cdot e$$

$$|R| = |R \cdot (1-e)| + |R \cdot e|$$

$$|R \cdot (1-e)|, |R \cdot e| < |R|$$

$\vdots$

Naletimo na Boolov kolobar z dvema elementoma. To je $\mathbb{Z}_2$.

$$\Rightarrow R \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{k\text{-krat}}$$

$$\Rightarrow n = 2^k$$

$$S = [k] = \{1, \dots, k\}$$

$$R = \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2 \cong P(S)$$

$P(S)$ je končen Boolov kolobar ($A \cdot A = A \cap A = A$), zato po primerjavi moči izomorfnost sledi.

Neskončen Boolov kolobar, ki ni izomorfen $P(S)$?

$$R = \{a \in \mathbb{Z}_2^{\mathbb{N}} \mid \text{končno mnogo } a_i \text{ neničelnih} \\ \text{ali končno mnogo } a_i \text{ ničelnih}\}$$

R seveda Boolov

$$\text{končen} < |R| < |\mathbb{R}| \Rightarrow R \text{ števno neskončen}$$

$P(S)$ pa ne more biti števno neskončen

2) Naj bo A kolobar in $A[[x]]$ kolobar formalnih potenčnih vrst $f = \sum_{n \geq 0} a_n x^n$, $a_n \in A$.

a) Pokaži, da je f obrnljiv v $A[[x]]$ natanko tedaj, ko je a_0 obrnljiv v A .

$$(\Rightarrow) \sum a_n x^n \text{ obrnljiv}$$

$$1 = (\sum a_n x^n)(\sum b_k x^k)$$

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

$$= a_0 b_0 + x \underbrace{(a_1 b_0 + a_0 b_1)}_{=0} + x^2 \underbrace{(a_0 b_2 + a_1 b_1 + a_2 b_0)}_{=0} + \dots$$

$\Rightarrow a_0$ obrnljiv

$(\Leftarrow) a_0$ obrnljiv

$$a_1 \cdot \frac{1}{a_0} + b_1 a_0 = 0$$

$$b_1 = -a_1 \cdot \frac{1}{a_0^2}$$

Izrazimo b_2 , ker je a_0 obrnljiv

?

b) Naj bo k polje. Pokaži, da je vsak nenulni ideal v $k[[x]]$ enak (x^n) za nek $n \geq 0$.

$$I \triangleleft k[[x]]$$

$$\text{st}(\sum a_i x^i) := \min \{i; a_i \neq 0\}$$

$$(x^n) = \{f(x) x^n; f(x) \in k[[x]]\}$$

$$n := \min_{f \in I \setminus \{0\}} \text{st } f$$

$$\underline{I = (x^n)}$$

$$(\subseteq) f \in I$$

$$f = \sum a_i x^i$$

$$= (a_m + a_{m+1}x + \dots) x^m$$

$$\stackrel{m \geq n}{=} (a_m + a_{m+1}X + \dots) X^{m-n} \cdot X^n \in (X^n)$$

$$(\Rightarrow) \text{Dovolj: } \underline{X^n \in I}$$

$$\exists f \in I : \text{st } f = n$$

$$f = (a_n + a_{n+1}X + \dots) \cdot X^n, \quad a_n \neq 0$$

$$\Rightarrow X^n = \underbrace{(a_n + a_{n+1}X + \dots)^{-1}}_{\substack{\text{obrnljiv po (a)}, \\ \text{saj } a_n \neq 0}} \cdot f \in I$$

c) Naj bo K polje s $\text{char } K \neq 2$. Pokaži, da ima $1+x$ kvadratni koren v $K[[X]]$ in zanj poišči eksplisitno formulo. Kaj se zgodi, če je $\text{char } K = 2$.

$$\sqrt{1+X} \stackrel{\text{Taylor}}{=} \sum_{n=0}^{\infty} \binom{1/2}{n} \cdot X^n$$

$$\binom{1/2}{n} = \frac{\frac{1}{2} \cdot (\frac{1}{2}-1) \cdots (\frac{1}{2}-n+1)}{n!}$$

$$\text{char } K \neq 2 \Rightarrow \frac{1}{2} \text{ definirana}$$

$$\text{Ampak: } n \geq \text{char } K \Rightarrow n! = 0 \quad \therefore$$

(v $R[[X]]$ deluje)

$$\sqrt{1+X} = \sum a_i X^i$$

$$1+X = \sum a_i X^i \cdot \sum a_j X^j$$

$$= a_0^2 + X(a_1 a_0 \cdot 2) + X^2(a_2 a_0 \cdot 2 + a_1^2) + X^3(2a_3 a_0 + 2a_2 a_1) + \dots$$

$$a_0 = 1$$

$$a_1 a_0 = \frac{1}{2} \Rightarrow a_1 = \frac{1}{2}$$

$$a_2 \cdot 2 + \frac{1}{4} = 0 \Rightarrow a_2 = -\frac{1}{4 \cdot 2} = -\frac{1}{8}$$

$$2a_3 a_0 + 2a_2 a_1 = 0 \Rightarrow 2a_3 = \frac{1}{8} \Rightarrow a_3 = \frac{1}{16}$$

Faktorji iz fakultete se poznašajo

$\Rightarrow$ Dobimo lahko vse člene

3) Naj bo R kolobar in $e, e' \in R$ idempotenta.

a) Pokaži, da je $(e)^2 = (e)$.

$$(a) \cdot (c) = (ac)$$

$$(a, b) \cdot (c, d) = [(a) + (b)][(c) + (d)] = (ac, ad, bc, bd)$$

$$\Rightarrow (e)^2 = (\overset{\text{idempotent}}{e^2}) = (e)$$

b) Naj bo $A = (a)$ glavni ideal z $A^2 = A$. Pokaži, da je $A = (t)$ za nek idempotent t . Pokaži, da iz $(e) = (e')$ sledi $e = e'$.

$$(a) = (t), \quad t^2 = t$$

$$\begin{aligned} (\subseteq) (a)^2 &= (a) \\ \parallel \\ (a^2) \end{aligned}$$

$$a \in (a^2) \Rightarrow ka^2 = a \quad \text{za nek } k \in R$$

$$(\text{Vedno: } a^2 \in (a))$$

$$ka^2 = a \quad / \cdot k$$

$$\Rightarrow (ka)^2 = (ka)$$

$$\Rightarrow k \cdot a \text{ idempotent}$$

$$k \cdot a \in (a)$$

$$(\supseteq) a = k \cdot a^2 = a \cdot (ka) \in (ka)$$

$$\underline{(e) = (e')} \Rightarrow \underline{e = e'}$$

DN

19.10.

1) Naj bo p praštevil.

a) Zapiši $\mathbb{F}_p[x]$ in $\mathbb{Z}[i]$ kot kvocienta $\mathbb{Z}[x]$.

b) Pokaži $\mathbb{F}_p[x]/(x^2+1) \cong \mathbb{Z}[i]/(p)$.

c) Za katere p je zgornji kolobar polje? Za katere pa vsebuje nenulne idempotente?

d) Če je polje, pokaži da ni izomorfno $\mathbb{Z}/n$ za nek n .

$$a) \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$$

$$\begin{aligned} \varphi: \mathbb{Z}[x] &\longrightarrow \mathbb{F}_p[x] \\ \sum a_i x^i &\longmapsto \sum (a_i \bmod p) x^i \end{aligned}$$

$$\ker \varphi = \{ \text{polinomi, katerih vsi koeficienti so večkratniki } p \}$$
$$= (p)$$

$$\Rightarrow \mathbb{F}_p[x] \cong \mathbb{Z}[x]/(p)$$

$$\psi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$$

$$\sum a_j x^j \mapsto \sum a_j i^j$$

$$x^2 + 1 \in \ker \psi$$

$$f \in \ker \psi$$

$$x^2 + 1 \mid f$$

$$f = \sum a_j x^j$$

$$\psi(t) = \sum a_j i^j = 0$$

$$\begin{aligned}
 &= \sum_{j \equiv 0 \pmod 4} a_j + \sum_{j \equiv 1 \pmod 4} a_j i - \sum_{j \equiv 2 \pmod 4} a_j - \sum_{j \equiv 3 \pmod 4} a_j i \\
 &= \left(\sum_{j \equiv 0 \pmod 4} a_j - \sum_{k \equiv 2 \pmod 4} a_k \right) + \left(\sum_{j \equiv 1 \pmod 4} a_j - \sum_{k \equiv 3 \pmod 4} a_k \right) i
 \end{aligned}$$

$$\Rightarrow \ker \psi = (x^2 + 1)$$

Alternativno:

$$\overline{\Psi}: \mathbb{Z}[x]/(x^2+1) \rightarrow \mathbb{Z}[i]$$

$$f \in \mathbb{Z}[x]/(x^2+1)$$

Če je $\ker \psi = (x^2 + 1)$, potem je to izomorfizem, in obratno.

$$f = \sum a_j x^j + (x^2+1) = b_0 + b_1 x + (x^2+1)$$

$$x^2 = -1 \pmod{(x^2+1)}$$

$$x^3 = x^2 \cdot x = -x \pmod{(x^2+1)}$$

$$f \mapsto b_0 + b_1 i = 0 \quad \forall \mathbb{Z}[i]$$

$$\Leftrightarrow b_0, b_1 = 0$$

$$\Rightarrow f = 0 \in \ker \Psi$$

$$b) \mathbb{F}_p[x]/(x^2+1) \stackrel{3. \text{ i. i. }}{=} \frac{\mathbb{Z}[x]/(p)}{(x^2+1)} \stackrel{3. \text{ i. i. }}{\cong} \frac{\mathbb{Z}[x]}{(p, x^2+1)} \cong \frac{\mathbb{Z}[x]/(x^2+1)}{(p)} \cong \mathbb{Z}[i]/(p)$$

3. izrek o izomorfizmu:

$$\frac{R/I}{J/I} \cong R/J$$

$$\frac{R/(a_1, a_2, \dots)}{(b_1, b_2, \dots)} \cong R/(a_1, a_2, \dots, b_1, b_2, \dots)$$

c) $\mathbb{Z}[i]/(p)$ polje

$$\Leftrightarrow x^2+1 \text{ nerazcepen v } \mathbb{F}_p[x]$$

$$\Leftrightarrow \text{nima ničel v } \mathbb{F}_p[x]$$

$$\Leftrightarrow -1 \text{ ni kvadrat v } \mathbb{F}_p[x]$$

$\mathbb{F}_p^x$ ciklično

$$\mathbb{F}_p^x \cong \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_k), \quad n_k | \dots | n_1$$

$$x^{n_1} - 1 \text{ vse elemente v } \mathbb{F}_p$$

Ampak ima samo n_1 ničel



$\Rightarrow \mathbb{F}_p^\times$ cikliččen

Kdaj je -1 kvadrat v $\mathbb{F}_p[x]$?

$$\mathbb{F}_p^\times = \overset{\text{cikliččen}}{\mathbb{Z}/(p-1)} = \langle g \rangle = \{1, g, \dots, g^{p-2}\}$$

$$0 \leq k \leq p-2$$

$$x^2 = -1$$

$$x = g^k$$

$$x^2 = g^{2k} \stackrel{\sim}{\iff} g^{\frac{p-2}{2}} = -1$$

$$2k = \frac{p-1}{2} \pmod{p-1}$$

$$k = \frac{p-2}{4}$$

$$k = \frac{p-2}{4} + \frac{p-2}{2}$$

$$\text{Resljivo} \iff p \equiv 2 \pmod{4}$$

- $p \equiv 3 \pmod{4}$

$$\mathbb{F}_2/(x^2+1) \dots (x^2+1)^2 = (x+1)^2$$

$x+1$ nilpotent

- $p \equiv 1 \pmod{4}$

$$\mathbb{F}_p[x]/(x^2+1)$$

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

$$\mathbb{F}_p[x]/(x^2+1) \cong \mathbb{F}_p[x]/(x-a) \times \mathbb{F}_p[x]/(x+a) \cong \mathbb{F}_p \times \mathbb{F}_p$$

Nima nilpotentov

d) DN

2) Za kolikojne $\mathbb{Z}/(2)[x]$, $\mathbb{R}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_{(2)} = \{\frac{a}{b} \in \mathbb{Q} ; b \text{ lih}\}$, $\mathbb{Z}[\frac{1}{15}]$, $\mathbb{Z}/(15)$, $\mathbb{R} \times \mathbb{R}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}[x]/(x^2)$, $\mathbb{Q}[x]$, $\mathbb{Q}[i]$:

- Opisi max ideale in enote (obrnljive elemente).

- Koliko praiidealov, ki niso max, imajo?

i) $\mathbb{Z}/(2)[x] = \mathbb{F}_2[x]$

Max ideali:

(†), $f = \sum a_i x^i$ nerazcepen

npr. $x+1$, x , x^2+x+1 , ...

Enote:

$\mathbb{Z}/(2)[x]^{\times} = \{1\}$
cel

Praideali:

$$I \neq R \Leftrightarrow R/I \text{ cel koloban}$$

$$fg \in I \Rightarrow f \in I \text{ ali } g \in I$$

(0) praideal in max ideal

$$(f) = (gh)$$

$$\frac{\mathbb{Z}/(2)[x]}{(f)} \text{ cel ?}$$

$$g \cdot h = 0, \quad g, h \neq 0$$

Dругih praidealov ni

ii) $R[x]$

Vsi ideali:

$$(0), (x^n), n \in \mathbb{N}_0$$

Max ideali:

$$(x)$$

$$E_{\text{note}} \Leftrightarrow a_{(0)} \neq 0$$

Praideali:

(0) praideal in max ideal

(x) praideal in max ideal

$$x \cdot x \in (x^2), \quad x \notin (x^2)$$

Dругih prasidealov ni

$$\text{iii) } \mathbb{Z}[[x]]$$

Max ideali:

(x, p) je en max ideal

$$\text{Enota} \Leftrightarrow a_0 = \pm 1$$

$I = (f_1, f_2, \dots)$ maksimalen

$$\underline{I + (x) \neq \mathbb{Z}[[x]]}$$

$$\text{Denimo: } I + (x) = \mathbb{Z}[[x]]$$

$$\Leftrightarrow 1 = \underbrace{f}_I + x \underbrace{g}_{\mathbb{Z}[[x]]}$$

$\Rightarrow$ Konstantni člen (f) je 1

$$\Rightarrow I = \mathbb{Z}[[x]]$$

$$\text{---} \times \text{---} \quad (I \text{ max})$$

$$\Rightarrow x \in I$$

$\Rightarrow (x, p)$ edini max ideal

Prasideali:

(0) , maksimalni, (x) , (x^2-6) , ... (neskončno jih je)

npr. $(x-6)$ pa ni praidéal

$$iv) \mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \in \mathbb{Q} ; b \text{ lih} \right\}$$

Max ideali:

$$\left\{ \frac{a}{b} \in \mathbb{Q} ; a \text{ sod, } b \text{ lih} \right\} = (2) \quad \text{edini max ideal}$$

$$\mathbb{Z}_{(2)}^\times = \left\{ \frac{a}{b} \in \mathbb{Q} ; a \text{ lih, } b \text{ lih} \right\}, \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

To sledi iz tega, da so vsi ostali elementi obrnljivi

Vsi ideali:

$$(0), (2), (4), (8), \dots$$

Praideali:

$$(0), (2) \quad \text{sta edina}$$

$$v) \mathbb{Z} \times \mathbb{Z}$$

Vsi ideali:

$$\mathbb{Z} \times 0, 0 \times \mathbb{Z}, n\mathbb{Z} \times m\mathbb{Z}, n, m \in \mathbb{Z}$$

Natančneje:

$$I \times J = \{(a, b) ; a \in I, b \in J\}$$

$$I, 0 \triangleleft \mathbb{Z}$$

Max ideali:

$$p\mathbb{Z} \times \mathbb{Z}, \mathbb{Z} \times p\mathbb{Z}$$

$$\text{Veljati mora: } \frac{\mathbb{Z} \times \mathbb{Z}}{n\mathbb{Z} \times m\mathbb{Z}} \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m)$$

Prasideali:

maksimalni in (0)

