DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Polinomu algebra

6.lekcija (papildmateriāls)

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

1. Lauku paplašinājumi

1.1. Polinomu saknes atlikumu gredzenā

1.1. teorēma. $p \in \mathcal{I}(k[X])$, $\deg p \geq 1$. $k[X]/(p)$ satur vismaz vienu p sakni.

PIERĀDĪJUMS Pierādīsim, ka $[X] \in K_p$ ir p sakne.
$p([X]) = \sum_{i=1}^{m} p_i[X]^i = \sum_{i=1}^{m} p_i[X^i] = \sum_{i=1}^{m}[p_i X^i] =$
$[\sum_{i=1}^{m} p_i X^i] = [p(X)] = [0]$ ■

1.2. teorēma. $f(X) \in k[X]$, $\deg(f) > 0$. Eksistē k paplašinājuma lauks, kas satur vismaz vienu f sakni.

PIERĀDĪJUMS Pieņemsim, ka p ir nedalāms f dalītājs. Definēsim $K_p = k[X]/(p)$. Saskaņā ar iepriekšējo teorēmu K_p satur vismaz vienu p, un tāpēc arī f, sakni. ■

1.2. Polinoma sašķeļošais lauks

Par $f \in k[X]$ *sašķeļošo lauku* sauksim k paplašinošo lauku K, kurā f sadalās lineāros reizinātājos: eksistē $a_1, ...a_n \in K$ tādi, ka

$$f(X) = (X - a_1)(X - a_2)...(X - a_n).$$

1.1. piemērs. $\forall\ f \in \mathbb{R}[X]$ $\mathbb{C}$ ir sašķeļošais lauks.

Polinomam $X^2 + X + 1 \in \mathbb{F}_2[X]$ lauks $\mathbb{F}_2[X]/(X^2 + X + 1)$ ir sašķeļošais lauks. Saknes ir $[X]$ un $[X + 1]$.

1.3. teorēma. $\forall\ f \in k[X] \deg(f) > 0\ \exists$ sašķeļošais lauks.

PIERĀDĪJUMS Pieņemsim, ka $f = \tilde{f} \cdot p_1...p_m$, kur $\tilde{f}$ ir lineāru polinomu reizinājums, $p_i \in \mathcal{I}(k[X]), \deg(p_i) > 1$.

Saskaņā ar iepriekš pierādītu teorēmu laukā $k[X]/(p_i)$ polinomam p_i eksistē vismaz viena sakne $\Longrightarrow$ polinomam f virs lauka $k[X]/(p_i)$ būs vēl viens lineārs reizinātājs.

Vairākkārtīgi pielietojot šādu operāciju iegūsim k paplašinājumu virkni

$$\underbrace{k}_{k_0} \leq \underbrace{k[X]/(p_1)}_{k_1} \leq \underbrace{k_1[X]/(q_j)}_{k_2} \leq ... \leq k_l.$$

Katra paplašināšana dod vismaz vienu lineāru reizinātāju f sadalījumā, tāpēc pēc galīga skaita soļu f tiks sadalīts lineāros reizinātājos virs kāda k paplašinājuma k_l. ■

2. Ideālu īpašības

2.1. teorēma.

1. $\langle f_1, ..., f_n \rangle + \langle g_1, ..., g_m \rangle = \langle f_1, ..., f_n, g_1, ..., g_m \rangle$.
2. $\langle f_1, ..., f_n \rangle \cdot \langle g_1, ..., g_m \rangle = \langle h_{11}, ..., h_{nm} \rangle$, kur $h_{ij} = f_i g_j$.

PIERĀDĪJUMS

1. $r \in \langle f_1, ..., f_n, g_1, ..., g_m \rangle \iff$

$$r = \underbrace{\alpha_1 f_1 + ... + \alpha_n f_n}_{\in \langle f_1, ..., f_n \rangle} + \underbrace{\beta_1 g_1 + ... + \beta_m g_m}_{\in \langle g_1, ..., g_m \rangle} \iff$$

$$r \in \langle f_1, ..., f_n \rangle + \langle g_1, ..., g_m \rangle.$$

2.

$$r \in \langle f_1, ..., f_n \rangle \cdot \langle g_1, ..., g_m \rangle \iff r = \sum_l \Big(\sum_i \alpha_{li} f_i \Big) \Big(\sum_j \beta_{lj} g_j \Big) =$$

$$\sum_{i,j} \underbrace{\Big(\sum_l \alpha_{li} \beta_{lj} \Big)}_{=\gamma_{ij}} \underbrace{(f_i g_j)}_{=h_{ij}} = \sum_{i,j} \gamma_{ij} h_{ij} \implies r \in \langle h_{11}, ..., h_{nm} \rangle.$$

$$r \in \sum_{i,j} \delta_{ij} h_{ij} \implies r \in \langle f_1, ..., f_n \rangle \cdot \langle g_1, ..., g_m \rangle. \blacksquare$$

2.2. teorēma. Ja k ir lauks un $\{f_1, ..., f_n\} \subset k[X]$, tad

1. $\langle f_1, ..., f_n \rangle = \langle LKD(f_1, ..., f_n) \rangle$.
2. $\sum_{i=1}^{m} \langle f_i \rangle = \langle LKD(f_1, ..., f_m) \rangle$.
3. $\bigcap_{i=1}^{m} \langle f_i \rangle = \langle MKD(f_1, ..., f_m) \rangle$.

PIERĀDĪJUMS

1. Izmantosim matemātisko indukciju ar parametru n.

Indukcijas bāze

$n = 2$, apskatīsim $I = \langle f_1, f_2 \rangle$, apzīmēsim $d = LKD(f_1, f_2)$.
No vienas puses:

$$r \in \langle f_1, f_2 \rangle \iff r = g_1 f_1 + g_2 f_2 \implies$$
$$r = g_1 h_1 d + g_2 h_2 d = (g_1 h_1 + g_2 h_2) d \implies$$
$$r \in \langle d \rangle = \langle LKD(f_1, f_2) \rangle.$$

No otras puses:

$$r \in \langle LKD(f_1, f_2) \rangle \implies r = gd = g(u_1 f_1 + u_2 f_2) \implies$$
$$r = (gu_1) f_1 + (gu_2) f_2 \in \langle f_1, f_2 \rangle.$$

Indukcijas solis

Pieņemsim, ka apgalvojums ir pierādīts $\forall\ n < m$, pierādīsim, ka tad apgalvojums ir patiess, ja $n = m$.

$$1. \implies \langle f_1, ..., f_{m-1}, f_m\rangle = \underbrace{\langle f_1, ..., f_{m-1}\rangle}_{=\langle LKD(f_1,...,f_{m-1})\rangle} + \langle f_m\rangle =$$

$$\langle LKD(LKD(f_1, ..., f_{m-1}), f_m)\rangle = \langle LKD(f_1, ..., f_n)\rangle.$$

2. seko no 1. un 2.

$$3.\ g \in \bigcap_{i=1}^{m} \langle f_i\rangle \implies g \in \langle f_i\rangle,\ \forall i \implies f_i|g \implies$$

$$MKD(f_1, ..., f_m)|g \implies g \in \langle MKD(f_1, ..., f_m)\rangle.$$

$$g \in \langle MKD(f_1, ..., f_m)\rangle \implies MKD(f_1, ..., f_m)|g \implies$$

$$f_i|g \implies g \in \bigcap_{i=1}^{m} \langle f_i\rangle.\blacksquare$$

2.1. piemērs. $\langle X^2-1, X+1\rangle = \langle X+1\rangle$.
$\langle X^2-1\rangle \cap \langle X(X+1)\rangle = \langle X(X^2-1)\rangle$.

3. Faktorgredzenu īpašības

3.1. teorēma. R ir komutatīvs unitārs gredzens, $I \subseteq R$ - ideāls.

1. R/I - integrāls gredzens $\iff$ I - pirmideāls.
2. R/I - lauks $\iff$ I - maksimāls ideāls.

PIERĀDĪJUMS

1. $\Leftarrow$

I - pirmideāls $\Longrightarrow$ $1+I \neq 0+I$ $\Longrightarrow$ faktorgredzenā R/I eksistē vienīnieks $1+I$.

$$(a+I)(b+I) = 0+I \implies ab \in I \implies a \in I \vee b \in I \implies$$
$$a+I = 0 \vee b+I = 0.$$

$\Longrightarrow$

$1 + I \neq 0 \Longrightarrow 1 \notin I \Longrightarrow I \neq R.$

Dots, ka $(a + I)(b + I) = 0 \Longrightarrow a + I = 0 \vee b + I$,

$(a + I)(b + I) = ab + I$, tātad ir dots, ka $ab \in I \Longrightarrow a \in I \vee b \in I$.

2. $\Leftarrow$

I - maksimāls ideāls $\Longrightarrow 1 + I \neq 0 + I \Longrightarrow$ faktorgredzenā R/I eksistē vieninieks $1 + I \neq 0 + I$.

$a + I \neq 0 \Longrightarrow a \notin I$. Apskatīsim ideālu $J = \langle I, a \rangle$, $I \subseteq J$. Tā kā I ir maksimāls ideāls, $a \in J$ un $a \notin I$, tad $J = R$. Seko, ka $1 \in J$ un $1 = x + ar$, kur $x \in I, r \in R$. Seko, ka

$$1 - ar = x \in I \Longrightarrow 1 \sim ar \Longrightarrow ar + I = 1 + I \Longrightarrow r = a^{-1}.$$

$\Rightarrow$

$1 + I \neq 0 \Longrightarrow 1 \notin I \Longrightarrow I \neq R$;

Dots, ka $\forall\, a \notin I$ eksistē $b = a^{-1}$:

$$(a + I)(b + I) = 1 + I,$$

jāpierāda, ka I ir maksimāls ideāls: katram ideālam J izpildās nosacījums $I \subseteq J \implies J = I \vee J = R$.

Pieņemsim, ka $\exists$ ideāls J: $I \subset J \subset R$. Izvēlēsimies $b \in J, b \notin I$. Eksistē $c = b^{-1}$:

$$(b + I)(c + I) = 1 + I \implies bc + I = 1 + I.$$

Redzam, ka $bc \sim 1 \implies 1 = bc + x$, kur $x \in I$. Seko, ka $1 \in J \implies J = R$. ■

3.1. piezīme. No teorēmas seko, ka maksimāls ideāls ir pirmideāls.

4. 6.mājasdarbs

4.1. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

6.5 Aprakstiet sašķeļošo lauku polinomam f un atrodiet f saknes tajā šādos gadījumos:

(a) $f = X^3 + X + 1 \in \mathbb{F}_2[X]$;
(b) $f = X^2 + X + 1 \in \mathbb{F}_3[X]$,
(c) $f = X^2 - 2 \in \mathbb{Q}[X]$.