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

Studiju kurss

Polinomu algebra

3.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

Lekcijas mērķis - apgūt pamatfaktus par polinomu faktorizāciju, nedalāmo polinomu īpašībām, polinomu sadalīšanu lināros faktoros, atvasinājuma izmantošanu polinomu faktorizācijā.

1. Polinomu faktorizācija

1.1. Pamatfakti

Gredzena $R[X]$ nedalāmos elementus sauc par nedalāmiem polinomiem.

Polinomu sauksim par *normalizētu*, ja tā vecākais koeficients ir vienāds ar 1.

1.1. teorēma. Ja k ir lauks, tad polinomu gredzenā $k[X]$ ir bezgalīgi daudz nedalāmu normalizētu polinomu.

PIERĀDĪJUMS

1.apakšgadījums. Ja k ir bezgalīgs lauks, tad visi lineārie polinomi $X - a$, $a \in k$, veido nedalāmu normalizētu polinomu kopu.

2.apakšgadījums. Ja k ir galīgs lauks, tad pierādījums ir līdzīgs pirmskaitļu kopas bezgalīguma pierādījumam. Pieņemsim pretējo: eksistē tikai galīgs skaits nedalāmu normalizētu polinomu $p_1, ..., p_k$. Apskatīsim polinomu

$$f = p_1 ... p_k + 1.$$

Tā kā $deg(f) > 0$, tad tam eksistē vismaz viens nedalāms dalītājs p_l. p_l nevar piederēt kopai $\{p_1, ..., p_k\}$, jo šādā gadījumā būtu spēkā dalāmība $p_l | f - p_1 ... p_k$ un sekotu, ka $p_l | 1$, tātad p_l būtu invertējams. Ir iegūta pretruna, jo pēc pieņēmuma kopa $\{p_1, ..., p_k\}$ satur visus nedalāmos polinomus. ■

1.2. teorēma. Ja k ir galīgs lauks, tad gredzenā $k[X]$ nedalāmu polinomu pakāpes nav ierobežotas.

PIERĀDĪJUMS Ja k ir galīgs lauks, tad katram $n \in \mathbb{N}$ eksistē galīgs skaits polinomu, kuru pakāpē ir vienāda ar n. Tā kā nedalāmu polinomu kopa ir bezgalīga, tad to pakāpes nevar būt ierobežotas. ■

1.2. Polinoma saturs

Vienkāršākā ar polinomu faktorizāciju saistītā darbība ir kopīgo reizinātāju iznešana.

Ja R ir gredzens, kurā visām elementu apakškopām eksistē LKD, tad par polinoma $f(X) \in R[X]$ *saturu* sauksim tā koeficientu LKD, to apzīmēsim ar $cont(f)$.

Ja $cont(f)$ ir invertējams elements gredzenā R, tad f sauksim par *primitīvu polinomu*.

1.1. piemērs. Normalizēts polinoms ir primitīvs polinoms. Visi polinomi ar koeficientiem laukā ir primitīvi.

Jebkuru polinomu f var izteikt formā

$$f = cont(f) f_0,$$

kur f_0 ir primitīvs polinoms.

1.2. piemērs. Ja $2X + 4 \in \mathbb{Z}[X]$, tad $f(X) = 2(X + 2)$.

1.3. teorēma. (Gausa lemma) Dots, ka R ir VFG, $f, g \in R[X]$. Tad ir spēkā satura multiplikatīvā īpašība:

$$cont(fg) \sim cont(f)cont(g).$$

PIERĀDĪJUMS

Reducēšana uz speciālgadījumu.

Ja $f = cont(f)f_0$ un $g = cont(g)g_0$, tad

$$cont(fg) \sim cont(f)cont(g)\underbrace{cont(f_0g_0)}_{?}.$$

Redzam, ka pietiek pierādīt, ka primitīvu polinomu reizinājums ir primitīvs polinoms.

Speciālgadījums - f un g ir primitīvi polinomi, jāpierāda, ka fg ir primitīvs polinoms. Pierādījums no pretējā.

Ir doti primitīvi polinomi

$$f(X) = \sum_{i=0}^{n} a_i X^i,$$

$$g(X) = \sum_{j=0}^{m} b_j X^j.$$

Pieņemsim, ka $cont(fg)$ nav invertējams, tātad eksistē nedalāms elements $p \in R[X]$ tāds, ka $p|cont(fg)$. Seko, ka p dala katru fg koeficientu.

Pieņemsim, ka k ir mazākais indekss, kuram $p \nmid a_k$, un l ir mazākais indekss, kuram $p \nmid b_l$. Tādi indeksi eksistē, jo pretējā gadījumā visi f un g koeficieni dalītos ar p, un tie nebūtu primitīvi polinomi.

Apskatīsim koeficientu pie X^{k+l} reizinājumam fg, tas ir vienāds

ar

$$\underbrace{\sum_{i=0}^{k+l} a_i b_{k+l-i}}_{\text{dalās ar } p} = \underbrace{(a_0 b_{k+l} + \ldots + a_{k-1} b_{l+1})}_{\text{dalās ar } p} + a_k b_l + \underbrace{(a_{k+1} b_{l-1} + \ldots + a_{k+l} b_0)}_{\text{dalās ar } p}.$$

Redzam, ka $p | a_k b_l$. Tā ir pretruna, jo seko, ka $p | a_k$ vai $p | b_l$.

■

1.3. Lineārie polinomi un saknes

1.3.1. Bezout teorēma

Pieņemsim, ka ir doti gredzeni $R \subseteq S$.

Teiksim, ka elements $a \in S$ ir nekonstanta polinoma $f \in R[X]$ *sakne*, ja

$$f(a) =_S 0.$$

Polinoma f sakņu kopu apzīmēsim, ar $\mathcal{V}(f)$.

1.4. teorēma. Ja R ir integrāls gredzens, tad visiem $f, g \in R[X]$ izpildās

$$\mathcal{V}(fg) = \mathcal{V}(f) \cup \mathcal{V}(g)$$

PIERĀDĪJUMS $\mathcal{V}(f) \cup \mathcal{V}(g) \subseteq \mathcal{V}(fg)$.

Ja $f(a) = 0$ vai $g(a) = 0$, tad $f(a)g(a) = 0$.

$\mathcal{V}(fg) \subseteq \mathcal{V}(f) \cup \mathcal{V}(g)$.

Ja $f(a)g(a) = 0$, tad $f(a) = 0$ vai $g(a) = 0$, jo R ir integrāls gredzens.

■

1.5. teorēma. (Bezout) $a \in R$ ir polinoma $f(X) \in R[X]$ sakne tad un tikai tad, ja $(X-a)|f(X)$.

PIERĀDĪJUMS Izdalīsim $f(X)$ ar $X-a$:

$$f(X) = q(X)(X-a) + r(X),$$

kur $deg(r(X)) < deg(X-a) = 1$. Redzam, ka $deg(r(X)) = 0$ vai $r(X) = 0$, tāpēc $r(X) = r_0$ - konstants polinoms.

Atradīsim r_0. Ja $X = a$, tad

$$f(a) = q(a)(a-a) + r_0,$$

tātad $r_0 = f(a)$ un

$$f(X) = q(X)(X-a) + f(a).$$

Redzam, ka $f(a) = 0$ tad un tikai tad, ja $f(X) = q(X)(X-a)$ jeb $(X-a)|f(X)$.

■

1.1. piezīme. No Bezout teorēmas seko, ka kvadrātisks vai kubisks polinoms f ir nedalāms tad un tikai tad, ja f nav saķņu.

Teiksim, ka elements $a \in R$ ir nekonstanta polinoma $f \in R[X]$ *k-kārtīga sakne*, ja

$$(X-a)^k | f(X) \text{ un } (X-a)^{k+1} \nmid f(X).$$

Citiem vārdiem sakot

$$f(X) = (X-a)^k g(X), \text{ kur } LKD(g(X), (X-a)) = 1.$$

1.6. teorēma. Ja gredzena R dažādi elementi $a_1, ..., a_m$ ir polinoma $f(X) \in R[X]$ saknes ar kārtām $k_1, ..., k_m$, tad

$$f(X) = (X-a_1)^{k_1} ... (X-a_m)^{k_m} g(X),$$

kur $g(a_i) \neq 0$ visiem $1 \leq i \leq m$.

PIERĀDĪJUMS Izmantosim matemātisko indukciju pēc m.

Indukcijas bāze.

Ja $m = 1$, tad apgalvojums seko no vairākkārtīgas saknes definīcijas.

Indukcijas solis.

Pieņemsim,ka apgalvojums ir spēkā, ja sakņu skaits ir vienāds vai mazāks kā $m-1$ un pierādīsim, ka tas ir spēkā, ja sakņu skaits ir vienāds ar m. Tātad

$$f(X) = (X-a_1)^{k_1}...(X-a_{m-1})^{k_{m-1}}h(X).$$

Tā kā $a_m \neq a_i$, $1 \leq i \leq m-1$, tad $h(a_m) = 0$, tādējādi

$$f(X) = (X-a_1)^{k_1}...(X-a_{m-1})^{k_{m-1}}(X-a_m)^u g(X),$$

kur $g(a_m) \neq 0$. Tā kā m ir k_m-kārtīga sakne, tad $u = k_m$ un viss ir pierādīts.

■

1.2. piezīme. Nekonstanta polinoma sakņu kārtu summa nevar pārsniegt polinoma pakāpi.

1.3.2. Polinomu interpolācija

1.3. piezīme. Ja divi polinomi f un g ar pakāpi n pieņem vienādas vērtības pēc $n+1$ substitūcijas ar dažādiem elementiem $a_1, ..., a_{n+1}$, tad tie ir vienādi. Tiešām, ja $h = f - g$, tad $deg(h) \leq n$. Pēc pieņēmuma $h(a_1) = ... = h(a_{n+1}) = 0$, tātad h ir vismaz $n+1$ dažāda sakne - pretruna, ja h nav vienāds ar 0.

1.4. piezīme. Polinomu ar pakāpi n var viennozīmīgi noteikt, ja ir zināmas tā vērtības $n+1$ punktos.

1.7. teorēma. (Lagranža interpolācijas formula) Dots, ka k ir lauks. Ja ir doti $n+1$ dažādi k elementi $a_0, ..., a_n$ un $n+1$ k elementi $b_0, ..., b_n$, tad eksistē viens un tikai viens polinoms $f(X) \in k[X]$ tāds, ka

$$f(a_i) = b_i \text{ visiem } 0 \leq i \leq n.$$

Polinoms f var tikt atrasts pēc šādas formulas:

$$f(X) = \sum_{i=0}^{n} b_i \frac{(X-a_0)...(X-a_{i-1})(X-a_{i+1})...(X-a_n)}{(a_i-a_0)...(a_i-a_{i-1})(a_i-a_{i+1})...(a_i-a_n)}$$

PIERĀDĪJUMS

Vienīgums.

Ja eksistē divi polinomi f un g tādi, ka

$$f(a_i) = g(a_i) = b_i \text{ visiem } 0 \leq i \leq n,$$

tad polinomam $h(X) = f(X) - g(X)$ pakāpe nav lielāka kā n un tam ir $n+1$ dažāda sakne $a_0, ..., a_n$. Seko, ka $h(X) = 0$.

Eksistence.

Jāveic formulas tieša pārbaude. ■

1.3. piemērs. Atradīsim polinomu $f \in \mathbb{F}_5[X]$,kura pakāpe ir vienāda ar 2, un kuram izpildās nosacījumi

$$f(1) = 2,$$
$$f(2) = 1,$$
$$f(3) = 3.$$

Saskaņā ar Lagranža interpolācijas formulu

$$f(X) = 2\frac{(X-2)(X-3)}{(1-2)(1-3)} + 1\frac{(X-1)(X-3)}{(2-1)(2-3)} + 3\frac{(X-1)(X-2)}{(3-1)(3-2)} =$$
$$= (X-2)(X-3) - (X-1)(X-3) - (X-1)(X-2) =$$
$$= -X^2 + 2X + 1 = 4X^2 + 2X + 1$$

1.4. Polinomu atvasināšana un tās pielietojumi faktorizācijā

1.4.1. Pamatfakti

Par polinoma

$$f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$$

(formālo) atvasinājumu sauksim polinomu

$$f'(X) = \sum_{i=1}^{n} a_i i X^{i-1} \in R[X]$$

Atvasinājumu var apzīmēt arī šādi: $f'(X) = (Df)(X)$.

Var definēt arī augstāku kārtu atvasinājumus.

1.4. piemērs. $(a_0 + a_1 X)' = a_1$.

$(X^p)' = 0$ gredzenā $\mathbb{F}_p[X]$.

1.8. teorēma.

1. $(af + bg)' = af' + bg'$,
2. $(fg)' = f'g + fg'$,
3. $(f^n)' = nf^{n-1}f'$.

PIERĀDĪJUMS Ir zināms no matemātiskās analīzes kursa.
■

1.4.2. Vairākkārtīgās saknes kritērijs

1.9. teorēma. Dots, ka k, K ir lauki, $k \subseteq K$. Polinomam

$$f(X) \in k[X]$$

elements $a \in K$ ir vairākkārtīga sakne tad un tikai tad, ja

$$f(a) = 0 \text{ un } f'(a) = 0.$$

PIERĀDĪJUMS Izdalīsim $f(X)$ ar $(X-a)^2$:

$$f(X) = q(X)(X-a)^2 + r(X),$$

kur $deg(r(X)) < 2$.

$r(X)$ izdalīsim ar $(X-a)$:

$$r(X) = q_1(X)(X-a) + r_1,$$

kur $deg(r_1) < 1$.

Apvienojot abus rezultātus vienā vienādībā, iegūsim

$$f(X) = q(X)(X-a)^2 + q_1(X)(X-a) + r_1.$$

Ievērosim, ka

$$f'(X) = (q(X)(X-a)^2 + q_1(X)(X-a) + r_1)' =$$
$$= q'(X)(X-a)^2 + q(X)\cdot 2(X-a) + q_1'(X)(X-a) + q_1(X).$$

Ja elements $a \in K$ ir vairākkārtīga sakne, tad $f(a) = 0$ un $f'(a) = 0$.

Ja elements $a \in K$ ir vairākkārtīga sakne, tad

$$f(X) = q(X)(X-a)^2,$$

tātad $q_1(X) = 0$ un $r_1 = 0$. Redzam, ka $f(a) = 0$ un $f'(a) = 0$.

Ja $f(a) = 0$ un $f'(a) = 0$, tad elements $a \in K$ ir vairākkārtīga sakne.

Ja $f(a) = 0$ un $f'(a) = 0$, tad $q_1(a) = 0$ un $r_1 = 0$. Tātad $(X - a)|q_1(X)$ un

$$f(X) = q_2(X)(X - a)^2$$

un a ir vairākkārtīga sakne.

■

1.4.3. Polinoma kvadrātbrīvās faktorizācijas atrašana

Teiksim, ka laukam k *harakteristika (raksturojums)* ir vienāda ar pozitīvu pirmskaitli χ, ja $\chi \cdot 1 = 0$. Ja nekādam naturālam skaitlim N neizpildās $N \cdot 1 = 0$, teiksim, ka lauka harakteristika ir vienāda ar 0. Lauka k harakteristiku apzīmē ar $char(k)$.

1.5. piemērs. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ - lauki ar harakteristiku 0.
$\mathbb{F}_q$ - lauks ar harakteristiku q.

Šajā sadaļā pētīsim polinomus virs laukiem k ar harakteristiku 0.

Ja $p \in k[X]$ ir nedalāms polinoms, kuram izpildās

$$p^k | f,$$
$$p^{k+1} \nmid f,$$

tad p sauksim par f k-kārtīgu nedalāmu dalītāju (faktoru).

Redzam, ka katru polinomu f var viennozīmīgi, ar precizitāti līdz kārtībai un invertējamiem reizinātajiem, izteikt formā

$$f = p_1^{k_1} ... p_m^{k_m}$$

1.10. teorēma. Ja p ir k-kārtīgs nedalāms dalītājs polinomam $f \in k[X]$, tad tas ir $k-1$-kārtīgs dalītājs polinomam f'.

PIERĀDĪJUMS Ir dots, ka

$$f = p^k g,$$

kur $LKD(p, g) = 1$.

Redzam, ka

$$f' = kp^{k-1}p'g + p^k g' = p^{k-1}(kp'g + pg').$$

Redzam, ka $p^{k-1}|f$. Jāpierāda, ka $p \nmid (kp'g + pg')$.

Ja $p|(kp'g + pg')$, tad $p|kp'g$.

Bet $p \nmid g$, jo $LKD(p, g) = 1$ un $p \nmid p'$, jo $deg(p) > deg(p')$.

No tā, ka $k[X]$ ir VFG seko, ka $p \nmid (kp'g + pg')$. ■

1.11. teorēma. (Kvadrātbrīvās faktorizācijas formula) Ja

$$f = p_1^{k_1} ... p_m^{k_m},$$

tad

$$\frac{f}{LKD(f, f')} = p_1 ... p_m.$$

PIERĀDĪJUMS no iepriekšējās teorēmas zinām, ka

$$f' = p_1^{k_1 - 1} ... p_m^{k_m - 1} h,$$

kur $p_i \nmid h$. Seko, ka

$$LKD(f, f') = p_1^{k_1 - 1} ... p_m^{k_m - 1}.$$

Izdalot f ar $LKD(f, f')$, iegūsim vēlamo formulu. ■

1.6. piemērs. Atradīsim polinoma

$$f(X) = X^5 - X^4 - 2X^3 + 2X^2 + X - 1 \in \mathbb{Q}[X]$$

faktorizāciju.

Atrodam $f'(X) = 5X^4 - 4X^3 - 6X^2 + 4X + 1$.
Atrodam $LKD(f, f') = X^3 - X^2 - X + 1$.
Atrodam

$$\frac{f}{LKD(f, f')} = X^2 - 1 = (X - 1)(X + 1).$$

Dalot f vairākas reizes ar $X - 1$ un $X + 1$, iegūsim faktorizāciju

$$f(X) = (X - 1)^3(X + 1)^2.$$

2. 3.mājasdarbs

2.1. Obligātie uzdevumi

3.1 Sadaliet doto polinomu nedalāmos reizinātājos virs dotā lauka:

(a) $f(X) = X^6 + 27$, virs $\mathbb{Q}$, virs $\mathbb{R}$,
(b) $f(X) = X^5 - X$, virs $\mathbb{F}_5$.

3.2 Atrodiet visus nedalāmos polinomus

(a) ar pakāpi 4 virs $\mathbb{F}_2$,
(b) ar pakāpi 3 virs $\mathbb{F}_3$,
(c) ar pakāpi 2 virs $\mathbb{F}_5$.

3.3 Pierādiet, ka polinomam

$$f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{F}_2[X]$$

eksistē lineārs dalītājs tad un tikai tad, ja

$$a_0 = 0 \text{ vai } \sum_{i=0}^{n-1} a_i = 0.$$

3.4 Nosakiet saknes a kārtu dotajā polinomā f:

(a) $f(X) = X^4 - X^3 - X + 1$, $a = 1$, virs $\mathbb{Q}$,

(b) $f(X) = X^3 + X + 1$, $a = 1$, virs $\mathbb{F}_3$,

3.5 Atrodiet polinomu $f(X) \in \mathbb{F}_3[X]$ ar šādu definējošo īpašību:

$$f(0) = 1, f(1) = 2, f(2) = 2.$$

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

3.6 Izpētiet, kādos gadījumos polinoms $f \in \mathbb{F}_p[X]$ atbilst injektīvai funkcijai $\mathbb{F}_p \to \mathbb{F}_p$, un kādos - neinjektīvai. Kāda ir saistība starp funkcijas grafa struktūru un polinoma struktūru?