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

Studiju kurss

Polinomu algebra

3.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

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

Lekcijas kopsavilkums:

- eksistē bezgalīgi daudz nedalāmu normalizētu poliomu ar lauka koeficientiem, var gadīties, ka to pakāpes nav ierobežotas;
- katrai polinoma f saknei atbilst viens f lineārs dalītājs, un otrādi;
- n-tās pakāpes polinoms ir viennozīmīgi noteikts ar tā vērtībām $n+1$ punktos;
- izmantojot polinomu formālo atvasināšanu, var atrast to vairākkārtīgās saknes un kvadrātbrīvo sadalījumu reizinātājos.

1. Polinomu faktorizācija

1.1. Pamatfakti

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

Polinomu $f \in k[X]$ sauksim par *normalizētu*, ja tā vecākais koeficients ir vienāds ar 1. Katrai asociācijas klasei ir tieši viens normalizēts pārstāvis.

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.

$p_l \in \{p_1, ..., p_k\} \implies p_l | f - p_1 ... p_k \implies p_l | 1$. 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 pakāpe 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 koeficientu kopīgo dalītāju atdalīšana izmantojot distributīvo īpašību - *kopīgo reizinātāju iznešana.*

Ja $f = f_1 + f_2 + ... + f_m$ un $\exists\ a$ tāds, ka $\forall\ i$ izpildās $a|f_i$ vai $f_i = ag_i$, tad saskaņā ar distributīvo īpašību

$$f = a(g_1 + g_2 + ... + g_m).$$

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 $cont(f) \in \mathcal{U}(R)$, 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. Polinomu saknes

1.3.1. Vienkāršās saknes - Bezout teorēma

Teiksim, ka elements $a \in R$ ir nekonstanta polinoma $f \in R[X]$ *sakne*, ja $f(a) = 0$.

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

1.3. 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

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

$f(a) = 0 \vee g(a) = 0 \implies f(a)g(a) = 0 \implies (fg)(a) = 0 \implies a \in \mathcal{V}(fg).$

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

$(fg)(a) = f(a)g(a) = 0 \implies f(a) = 0 \vee g(a) = 0$, jo R ir integrāls gredzens.

■

1.4. teorēma. (*Bezout*) $a \in \mathcal{V}(f) \iff (X - a)|f(X)$.

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

$$f(X) = q(X)(X - a) + r(X), \text{ kur } \deg\Big(r(X)\Big) < \deg(X - a) = 1.$$

Redzam, ka $\deg\Big(r(X)\Big) = 0$ vai $r(X) = 0 \implies r(X) = r_0$ - konstants polinoms.

Atradīsim r_0. Veicot substitūciju $X = a$, iegūstam

$$f(a) = q(a)(a - a) + r_0 \implies r_0 = f(a) \implies$$

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

$$f(a) = 0 \iff f(X) = q(X)(X - a) \iff (X - a)|f(X). \blacksquare$$

1.1. piezīme. No Bezout teorēmas seko, ka kvadrātisks vai kubisks polinoms f virs lauks k ir nedalāms tad un tikai tad, ja $\mathcal{V}(f) = \emptyset$.

1.3.2. Vairākkārtīgās saknes

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

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

1.5. 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 ar indukcijas parametru 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 $u = k_m$. ■

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

1.3.3. Polinomu interpolācija

1.6. teorēma. 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.

PIERĀDĪJUMS Ja $h = f - g$, tad

$$\deg(h) \leq \max(\deg(f), \deg(g)) = n.$$

Pēc pieņēmuma

$$h(a_1) = f(a_1) - g(a_1) = 0,$$
$$..., h(a_{n+1}) = f(a_{n+1}) - g(a_{n+1}) = 0,$$

tātad polinomam h ir vismaz $n+1$ dažādas saknes $a_1, ..., a_{n+1}$ - pretruna, ja h nav vienāds ar 0. ■

1.3. piezīme. Polinomu ar pakāpi n var viennozīmīgi noteikt (atrast tā koeficientus), ja ir zināmas tā vērtības $n+1$ punktos.

1.7. teorēma. (*Lagranža interpolācijas formula*) 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:

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

PIERĀDĪJUMS

Vienīgums.

Seko no iepriekšējas teorēmas.

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. k - lauks, $f \in k[X]$. Polinomam

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

$a \in \mathcal{V}(f)$ ir vairākkārtīga sakne $\iff f(a) = 0 \wedge f'(a) = 0$.

PIERĀDĪJUMS

Izdalīsim $f(X)$ ar $(X-a)^2$:

$$f(X) = q(X)(X-a)^2 + r(X), \text{ kur } \deg\Big(r(X)\Big) < 2.$$

$r(X)$ izdalīsim ar $(X-a)$:

$$r(X) = q_1 \cdot (X-a) + r_1, \text{ kur } \deg(r_1) < 1.$$

Apvienojot abus rezultātus vienā vienādībā, iegūsim

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

Ievērosim, ka

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

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 $q_1 = 0$ 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 $q_1 = 0$ un $r_1 = 0$. Tātad

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

un a ir vairākkārtīga sakne. ■

1.5. piemērs.

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 $char(k)$.

1.6. piemērs. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ - lauki ar harakteristiku 0.
$\mathbb{F}_p$ - lauks ar harakteristiku p.

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

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

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

Tā kā $k[X]$ ir VFG, tad katru $f \in k[X]$ var vienozīmīgi, ar precizitāti līdz kārtībai un invertējamiem reizinātajiem, izteikt formā

$$f = p_1^{\alpha_1} ... p_m^{\alpha_m}.$$

1.10. teorēma. Ja p ir $f \in k[X]$ α-kārtīgs nedalāms dalītājs un $\alpha \not\equiv 0(\text{mod } char(k))$, tad p ir f' $\alpha - 1$-kārtīgs nedalāms dalītājs.

PIERĀDĪJUMS Ir dots, ka

$$f = p^{\alpha} g, \text{ kur } LKD(p, g) = 1.$$

Redzam, ka

$$f' = \alpha p^{\alpha-1} p' g + p^{\alpha} g' = p^{\alpha-1}(\alpha p' g + p g').$$

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

$p|(\alpha p' g + p g') \implies p|\alpha p' g.$

$\deg(p) > \deg(p') \implies LKD(p, p') = 1.$

$LKD(p,g)=1 \wedge\ LKD(p,p')=1 \implies p \nmid \alpha p'g$ - pretruna.

$k[X]$ ir VFG $\implies p \nmid (kp'g+pg')$. ■

1.7. piemērs.

1.11. teorēma. (Kvadrātbrīvās faktorizācijas formula)

$$f=p_1^{\alpha_1}...p_m^{\alpha_m} \wedge \alpha_i \not\equiv 0(\text{mod } char(k)), \forall\ i \implies$$
$$\frac{f}{LKD(f,f')}=p_1...p_m.$$

PIERĀDĪJUMS No iepriekšējās teorēmas zinām, ka

$$f'=p_1^{\alpha_1-1}...p_m^{\alpha_m-1}h, \text{ kur } p_i \nmid h.$$

Seko, ka

$$LKD(f,f')=p_1^{\alpha_1-1}...p_m^{\alpha_m-1}.$$

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

$$\frac{f}{LKD(f, f')} = \frac{p_1^{\alpha_1} ... p_m^{\alpha_m}}{p_1^{\alpha_1 - 1} ... p_m^{\alpha_m - 1}} = p_1 ... p_m.$$

■

1.4. piezīme. Nosacījums $\alpha_i \not\equiv 0 (\mathrm{mod}\ char(k))$ jeb $char(k) \nmid \alpha_i$ izpildās, piemēram, šādos divos gadījumos:

- $char(k) = 0$,
- $char(k) > \deg(f)$.

1.8. 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 $LKD(f, f') = X^3 - X^2 - X + 1$ izmantojot Eiklīda algoritmu.

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

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

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?

3.7 Pamatojiet *Ņūtona interpolācijas formulu.* Dots lauks k. Ja ir doti $n+1$ dažādi k elementi $a_0, ..., a_n$ un $n+1$ k elementi $b_0, ..., b_n$, tad $f(X) \in k[X]$, kas apmierina nosacījumus

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

var tikt meklēts formā

$$\begin{aligned} f(X) = c_0 + c_1(X - a_0) + c_2(X - a_0)(X - a_1) + ... \\ + c_n(X - a_0)...(X - a_{n-1}) = \\ c_0 + \sum_{i=1}^{n} c_i \prod_{j=1}^{i} (X - a_{j-1}). \end{aligned}$$

Mēģiniet atrast c_k kā funkciju no a_i un b_i, $0 \leq i \leq n$.