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

Studiju kurss

Polinomu algebra

5.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis - apgūt pamatfaktus par polinomu faktorizāciju virs $\mathbb{Z}$ un $\mathbb{Q}$.

Lekcijas kopsavilkums:

- polinoms ar veseliem koeficientiem ir nedalāms virs $\mathbb{Z}$ tad un tikai tad, ja tas ir nedalāms virs $\mathbb{Q}$;
- ir lietderīgi pētīt polinomu redukcijas mod p;
- var faktorizēt polinomus virs $\mathbb{Z}$ vai $\mathbb{Q}$ izmantojot Kronekera algoritmu.

Svarīgākie jēdzieni: polinoma redukcija mod p.

Svarīgākie fakti un metodes: $\mathbb{Z}[X]$ ir VFG un Eiklīda gredzens,

satura multiplikativitāte, faktorizācijas ekvivalence virs $\mathbb{Z}$ un $\mathbb{Q}$, racionālās saknes tests, faktorizācijas mod p īpašības, Eizenšteina kritērijs, Kronekera faktorizācijas algoritms.

1. Faktorizācija virs $\mathbb{Z}$ un $\mathbb{Q}$

1.1. Pamatfakti

1.1.1. Viennozīmīgā faktorizācija virs $\mathbb{Z}$

1.1. teorēma. $\mathbb{Z}[X]$ ir VFG.

PIERĀDĪJUMS ■

1.1.2. Skaitļu gredzenu iekļaušanas sekas

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \implies \mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X] \implies \forall\ f \in \mathbb{Z}[X]$ var uzskatīt par piederošu $\mathbb{Q}[X]$, $\mathbb{R}[X]$ vai $\mathbb{C}[X]$.

$f \in \mathbb{Q}[X] \implies \exists\ a \in \mathbb{Z}:\ af \in \mathbb{Z}[X]$ - a ir f koeficientu saucēju MKD daudzkārtnis. Papildus tam $af \sim f$ virs $\mathbb{Q}$.

Ja ir zināms polinoma sadalījums virs lielāka lauka, tad izmantojot

viennozīmīgās faktorizācijas īpašību, var izdarīt atbilstošus secinājumus par polinoma faktorizāciju virs $\mathbb{Z}$.

Naivs algoritms polinoma faktorizācijai virs $\mathbb{Z}$ vai $\mathbb{Q}$:

1. sadalīt polinomu nedalāmos reizinātājos virs $\mathbb{R}$ vai $\mathbb{C}$;
2. mēģināt apvienot vairākus nedalāmus polinomus reizinājumos tā, lai $\forall$ reizinātājs ir virs $\mathbb{Z}$ vai $\mathbb{Q}$.

1.1. piemērs. $X^2 - 3 = \underbrace{(X - \sqrt{3})(X + \sqrt{3})}_{\in \mathbb{R}[X]} \in \mathcal{I}(\mathbb{Z}[X])$.

1.2. Nedalāmība virs $\mathbb{Z}$ un $\mathbb{Q}$

$\mathbb{Z}$ gadījumā aizvietosim $\sim$ ar $= \pm$, jo $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.

1.2.1. Galvenā teorēma

1.2. teorēma. $f \in \mathbb{Z}[X]$. $f \in \mathcal{I}(\mathbb{Z}[X]) \iff f \in \mathcal{I}(\mathbb{Q}[X])$.

PIERĀDĪJUMS
■

1.2.2. Secinājumi attiecībā uz faktorizāciju

$f \in \mathbb{Z}[X]$ - faktorizācija virs $\mathbb{Q}$ ir tāda pati kā faktorizācija virs $\mathbb{Z}$, ja neskaita konstantos reizinātājus.

$f \in \mathbb{Q}[X]$ - iespējamie faktorizācijas algoritmi:

- var mēģināt faktorizēt f virs Q,

- var reizināt f ar $a \in \mathbb{Z}$: $af \in \mathbb{Z}[X]$, tad faktorizēt af virs $\mathbb{Z}$:

$$af = g_1 ... g_m \in \mathbb{Z}[X] \implies f = \frac{1}{a}(g_1 ... g_m) \in \mathbb{Q}[X].$$

1.3. Racionālās saknes tests

1.3. teorēma. *(Racionālās saknes tests)* $f(X) = \sum_{i=0}^{n} f_i X^i \in \mathbb{Z}[X]$, $LKD(r,s) = 1$, $r \neq 0$, $f\left(\frac{r}{s}\right) = 0$. Tad

1. $r \mid f_0$;
2. $s \mid f_n$.

PIERĀDĪJUMS 1., 2. Vienādību $f\left(\frac{r}{s}\right) = 0$ reizināsim ar s^n:

$$f_n \cdot \left(\frac{r}{s}\right)^n + f_{n-1} \cdot \left(\frac{r}{s}\right)^{n-1} + ... + f_1 \cdot \left(\frac{r}{s}\right) + f_0 = 0 \implies$$

$$\overbrace{\underbrace{f_n r^n + f_{n-1} r^{n-1} s + \ldots + f_1 r s^{n-1}}_{\equiv 0 (\mathrm{mod}\ s)} + f_0 s^n}^{\equiv 0 (\mathrm{mod}\ r)} = 0.$$

Apskatīsim redukcijas mod r un s:

$$\begin{cases} f_0 s^n \equiv 0 (\mathrm{mod}\ r) \\ f_n r^n \equiv 0 (\mathrm{mod}\ s). \end{cases}$$

$$LKD(r,s) = 1 \implies \begin{cases} r \in \mathcal{U}_s \\ s \in \mathcal{U}_r. \end{cases}$$

$$\implies \begin{cases} f_0 s^n \cdot (s^{-1})^n \equiv f_0 \equiv 0 \cdot (s^{-1})^n \equiv 0 (\mathrm{mod}\ r) \\ f_n r^n \cdot (r^{-1})^n \equiv f_n \equiv 0 \cdot (r^{-1})^n \equiv 0 (\mathrm{mod}\ s). \end{cases} \blacksquare$$

1.2. piemērs. Mēģināsim faktorizēt $f = 2X^4 - 5X^3 + 6X^2 - 10X + 4$.

r/s ir f sakne $\implies r|4$ un $s|2$.

Iespējamās racionālās saknes ir ± 4, ± 2, ± 1, $\pm 1/2$.

Ar tiešu pārbaudi atrodam, ka saknes ir 2 un $1/2$.

Izdalot f ar $(X-\frac{1}{2})(X-2)$, iegūstam

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

1.4. Factorizācija mod p un tās pielietojumi

1.4.1. Polinoma redukcija mod p

$p\in\mathbb{P}$, $f=\sum_{i=1}^{n}a_iX^i\in\mathbb{Z}[X]$. Par f *redukciju mod* p sauc polinomu

$$[f]_p=\sum_{i=1}^{n}[a_i]_pX^i\in\mathbb{F}_p[X],\ \text{kur } [a_i]_p \text{ ir } a_i \text{ redukcija mod } p.$$

1.3. piemērs. $f=X^3-3X^2+6X-1$.
$[f]_2=X^3+X^2+1$.
$[f]_3=X^3+2$.

$$\forall\, p:\ [(X+1)^p]_p = X^p + 1.$$

1.4.2. Galvenā teorēma

1.4. teorēma. $f, g \in \mathbb{Z}$. Tad

1. $[f+g]_p = [f]_p + [g]_p, \forall\, p \in \mathbb{P}$.
2. $[fg]_p = [f]_p[g]_p, \forall\, p \in \mathbb{P}$.

PIERĀDĪJUMS Viegli redzēt sākot no piemēriem. ■

1.5. teorēma. $f \in \mathbb{Z}[X]$ ir normalizēts polinoms.

1. $f \notin \mathcal{I}(\mathbb{Z}[X]) \implies [f]_p \notin \mathcal{I}(\mathbb{F}_p[X]), \forall\, p \in \mathbb{P}$.
2. $\exists\, p:\ [f]_p \in \mathcal{I}(\mathbb{F}_p[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X])$.

PIERĀDĪJUMS

1. Seko no iepriekšējās teorēmas:

$$f = gh \in \mathbb{Z}[\mathbb{X}] \implies [f]_p = [g]_p[h]_p \in \mathbb{F}_p[X], \forall\, p \in \mathbb{P}.$$

2. Kontrapozīcijas likums piemērots pirmajam apgalvojumam. ■

1.4. piemērs. $f = X^4 - 3X^3 + 6X^2 + 4X + 7$.

$p = 2$, $[f]_2 = X^4 + X + 1 \in \mathcal{I}(\mathbb{F}_2[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X])$.

1.4.3. Eizenšteina kritērijs

1.6. teorēma. $f = \sum_{i=0}^{n} f_i X^i \in \mathbb{Z}[X]$, $\exists\, p \in \mathbb{P}$:

- $f_n \not\equiv 0 (\mathrm{mod}\ p)$.
- $\forall\, l < n$: $f_l \equiv 0 (\mathrm{mod}\ p)$,
- $f_0 \not\equiv 0 (\mathrm{mod}\ p^2)$.

Tad $f \in \mathcal{I}(\mathbb{Z}[X])$.

PIERĀDĪJUMS Reducējot mod p, iegūsim, ka

$$[f]_p = \underbrace{[f_n]_p}_{\neq 0} X^n = cX^n.$$

$$\left\{ \begin{array}{l} f = gh \in \mathbb{Z}[X] \\ \deg(g) > 0, \deg(h) > 0 \end{array} \right. \Longrightarrow [f]_p = [g]_p[h]_p \in \mathbb{F}_p[X] \Longrightarrow$$

$$\left\{ \begin{array}{l} [g]_p = c_1 X^j, \ j > 0 \\ [h]_p = c_2 X^{n-j}, \ n - j > 0 \end{array} \right.$$

$$\Longrightarrow \left\{ \begin{array}{l} g_0 \equiv 0 (\text{mod } p), \\ h_0 \equiv 0 (\text{mod } p), \end{array} \right. \Longrightarrow f_0 \equiv g_0 h_0 \equiv 0 (\text{mod } p^2) \text{ - pretruna.}$$

■

1.5. piemērs. $X^4 - 3X^2 + 6X - 3 \in \mathcal{I}(\mathbb{Z}[X])$, jo visi koeficienti, izņemot vecāko, dalās ar $p = 3$, bet brīvais loceklis nedalās ar $3^2 = 9$.

Dažreiz var mēģināt izmantot argumenta lineāru substitūciju - nobīdi: $X^3 - 9X + 11 = (X - 1)^3 + 3(X - 1)^2 - 6(X - 1) + 3$ - nedalāms, $p = 3$.

$X^2 - 8$ nedalāmību nevar pierādīt ar Eizenšteina kritēriju ne ar kādu nobīdi.

1.1. piezīme. Izmantojot Eizenšteina kritēriju, var pierādīt, ka $\mathbb{Z}[X]$ (un tātad arī $\mathbb{Q}[X]$) nedalāmu polinomu pakāpes nav ierobežotas. Piemēram, $\forall\ n$ polinoms $X^n + 2X + 2$ ir nedalāms.

1.5. Kronekera faktorizācijas algoritms

1.5.1. Ievads

Kronekera algoritms ir algoritms, ar kura palīdzību var faktorizēt polinomus virs $\mathbb{Z}[X]$, un tātad arī virs $\mathbb{Q}[X]$.

Tas ir *rupja spēka* jeb *izsmeļošās pārlases* tipa algoritms - tiek noteikta galīga kopa, kuras visus elementus pārskatot, tiek atrisināts uzdevums.

Atzīmēsim šādus faktus:

- $f \in \mathbb{Z}[X]$, $\deg f = n$ ir dalāms $\Longrightarrow$ $\exists$ f dalītājs g : $\deg g \leq \left[\frac{n}{2}\right] = l$ - *meklēsim šādu* f *dalītāju* g,
- $\deg g \leq l \Longrightarrow$ g ir viennozīmīgi noteikts ar savām vērtībām $l+1$ punktos, šādu polinomu var atrast ar Lagranža interpolācijas formulas palīdzību - *pietiek zināt* g *vērtības* $l+1$ *punktos*,
- $f = gh \Longrightarrow g(c) \Big| f(c)\ \forall\ c \in \mathbb{Z}$ - *izvēlēsimies* $l+1$ c *vērtības un pārbaudīsim visus* $f(c)$ *dalītājus kā iespējamās* $g(c)$ *vērtības.*

1.5.2. Algoritms

$f \in \mathbb{Z}[X]$, $\deg(f) = n$. Apzīmēsim $\left[\frac{n}{2}\right]$ ar l.

1. Izvēlēsimies $l+1$ veselu punktu virkni $\mathcal{C} = (c_0, ..., c_l)$, piemēram, $(0, 1, ..., l)$ vai $(0, \pm 1, \pm 2, ...)$ (lai atvieglotu skaitļošanu, vēlams izvēlēties pēc iespējas mazākus skaitļus).

2. Ja kādam i izpildās $f(c_i) = 0$ (nejauši trāpījām uz f saknes), tad izdalām f ar $X - c_i$ un atgriežamies uz soli 1 ar polinomu $\dfrac{f}{(X - c_i)}$.

3. Atradīsim virkni $f(\mathcal{C}) = \Big(f(c_0), ..., f(c_l)\Big)$ (vēlams panākt, lai $f(\mathcal{C})$ elementi ir mazi un tiem ir maz dalītāju).

4. Pēctecīgi apskatīsim visas virknes $\mathcal{D} = (d_0, ..., d_l)$, kur $d_i \Big| f(c_i)$:

   (a) ar Lagranža interpolācijas formulas palīdzību konstruēsim polinomu $g_{\mathcal{D}}$, kuram izpildās nosacījums

   $$g_{\mathcal{D}}(c_i) = d_i, \forall i : 0 \leq i \leq l,$$

   (b) ja $\begin{cases} g_{\mathcal{D}} \in \mathbb{Z}[X] \\ \deg g_{\mathcal{D}} > 0 \\ g_{\mathcal{D}} \Big| f \text{ virs } \mathbb{Z} \end{cases} \implies$ atkārtoti pielietojam Kronekera algoritmu polinomiem $g_{\mathcal{D}}$ un $\dfrac{f}{g_{\mathcal{D}}}$,

(c) ja $g_{\mathcal{D}} \notin \mathbb{Z}[X]$ vai $g_{\mathcal{D}} \nmid f$ virs $\mathbb{Z}$, tad pārejam uz nākamo virkni $\mathcal{D}$.

5. Ja pēc visu virkņu $\mathcal{D}$ apskatīšanas nav atrasts neviens f dalītājs, tad f ir nedalāms.

1.6. piemērs. Faktorizēsim virs $\mathbb{Z}$ polinomu

$$f = X^4 - 4X^3 + 3X^2 + 2X - 1.$$

f ir dalāms $\Longrightarrow$ $\exists$ f dalītājs, kura pakāpe nepārsniedz 2.

Izvēlēsimies 3 punktu virkni $\mathcal{C} = (0, 1, 2)$.

Atradīsim $f(\mathcal{C}) = (f(0), f(1), f(2)) = (-1, 1, -1)$.

Jāapskata 8 virknes, jo $\forall$ virknes $f(\mathcal{C})$ elementam ir 2 veseli dalītāji: $(1, 1, 1,)$, $(1, 1, -1)$, $(1, -1, 1)$, $(1, -1, -1,)$, $(-1, 1, 1,)$, $(-1, 1, -1)$, $(-1, -1, 1)$, $(-1, -1, -1)$.

1. $\mathcal{D} = (1, 1, 1)$, šajā gadījumā polinoms ir konstants.

2. $\mathcal{D} = (1, 1, -1)$,

$$f_{\mathcal{D}} = 1 \cdot \frac{(X-1)(X-2)}{(0-1)(0-2)} +$$

$$1 \cdot \frac{(X-0)(X-2)}{(1-0)(1-2)} + (-1) \cdot \frac{(X-0)(X-1)}{(2-0)(2-1)} = -X^2 + X + 1.$$

$\frac{f}{f_{\mathcal{D}}} = -X^2 + 3X - 1$. Pārbaudot kvadrātvienādojumu saknes, redzam, ka $-X^2 + X + 1$ un $-X^2 + 3X - 1$ ir nedalāmi virs $\mathbb{Z}$, tāpēc uzdevums ir atrisināts un

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

2. 5.mājasdarbs

2.1. Obligātie uzdevumi

5.1 $f \in \mathbb{Q}[X]$ ir nedalāms. Pierādīt, ka vienādojumam

$$f(z) = 0$$

nav vairākkārtīgu saknļu laukā $\mathbb{C}$. (*Norādījums: izmantojiet kvadrātbrīvās faktorizācijas formulu, pierādiet, ka* $LKD(f, f') = 1$).

5.2 Faktorizēt polinomus virs $\mathbb{Q}$ izmantojot racionālo saknļu testu.

(a) $3X^2 - 5X - 2$;
(b) $24X^3 + 14X^2 - 7X - 3$;
(c) $72X^4 + 102X^3 - 37X^2 - 48X - 9$.

5.3 Izmantojot Kronekera algoritmu sadalīt polinomus nedalāmajos reizinātājos virs $\mathbb{Z}$:

(a) $2X^4 - 13X^3 + 25X^2 - 14X + 2$,
(b) $X^6 - 9X^5 + 29X^4 - 39X^3 + 17X^2 + 3X - 1$.

5.4 Pierādiet, ka dotie polinomi ir nedalāmi virs $\mathbb{Z}$:

(a) $X^3 - 2X^2 + 4X - 4 \pmod 3$,
(b) $X^4 - 10X^3 + 6X^2 - 12X + 6$ (Eizenšteina kritērijs),
(c) $X^3 - X^2 - 3X + 5$ (Eizenšteina kritērijs ar nelielu nobīdi).

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.5 (2010.g.Sanktpēterburgas Universitātes studentu konkurss, http://www.mathsoc.spb.ru/konkurs/index.html) $a, b \in \mathbb{Z}$ apmierina sakarību $a^2+ab+b^2 \equiv 0 (\mathrm{mod}\ p)$, $p \in \mathbb{P}$, $p > 3$. Pierādīt, ka $f(a,b) = (a+b)^p - a^p - b^p \equiv 0 (\mathrm{mod}\ p^3)$. (*Norādījums: pierādiet, ka $f(a,b)$ dalās ar a^2+ab+b^2, ja $p-1 \not\equiv 0 (mod\ 3)$ un dalās ar $(a^2+ab+b^2)^2$, ja $p-1 \equiv 0 (mod\ 3)$*).

5.6 Atrodiet visus polinomus $f \in \mathbb{C}[X]$, kas apmierina funkcionālo vienādojumu

$$f(X^2) + f(X)f(X+1) = 0.$$

(*Norādījums: izmantojiet* $\mathbb{C}[X]$ *VFG īpašību, meklējiet* f *formā*

$$f = a(X - c_1)...(X - c_m),$$

apskatīt gadījumus $c = 0$, $c = 1$ *u.t.t.*)

5.7 Nosakiet, vai zemāk dotie polinomi ir dalāmi:

(a) $X^n \pm X \pm 1 \in \mathbb{Z}[X]$,
(b) $X^n + tX \pm 1 \in \mathbb{Z}[X]$, ja $|t| \geq 3$,
(c) $X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Z}[X]$, kur $p \in \mathbb{P}$.

5.8 $a_1, ..., a_n$ - dažādi veseli skaitļi. Noskaidrot, vai zemāk dotie polinomi ir dalāmi virs $\mathbb{Z}$.

(a) $(X - a_1)...(X - a_n) - 1$;
(b) $(X - a_1)...(X - a_n) + 1$;
(c) $(X - a_1)^2...(X - a_n)^2 + 1$.