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

Studiju kurss

Polinomu algebra

2.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis - LKD, MKD, Eiklīda algoritma jēdzienus polinomu gredzenu gadījumā.

Lekcijas kopsavilkums:

- polinomiem var definēt dalīšanu ar atlikumu.
- polinomu gredzenos virs lauka var izmantot Eiklīda algoritmu.

Svarīgākie jēdzieni: redukcija ar polinomu, polinomu dalījums un dalīšanas atlikums, LKD un MKD patvaļīgos gredzenos.

Svarīgākie fakti un metodes: redukcija samazina reducējamā polinoma pakāpi, polinomu dalīšana ar atlikumu, nedalāmo elementu īpašības, GFG piemēri, Eiklīda algoritms polinomu gredzenos, secinājumi no Eiklīda algoritma.

1. Polinomu dalīšana ar atlikumu

1.1. Redukcija

R ir IG, $f, g \in R[X]$, $\deg(f) \geq \deg(g)$ un g vecākais koeficients ir invertējams.

Definēsim operāciju polinomu kopā - *f redukciju ar g:*

$$(f, g) \mapsto \mathcal{R}_g(f) = f - \left(\frac{\mathcal{H}(f)}{\mathcal{H}(g)}\right) \cdot g.$$

1.1. piemērs. $\mathcal{R}_{X+1}(X^2+1) = (X^2+1) - X(X+1) = -X+1.$

1.1. teorēma. $\deg\Big(\mathcal{R}_g(f)\Big) < \deg(f).$

PIERĀDĪJUMS

$$\begin{cases} \mathcal{H}(f) = a_n X^n \\ \mathcal{H}(g) = b_m X^m, n \geq m \end{cases} \Longrightarrow \frac{\mathcal{H}(f)}{\mathcal{H}(g)} = \frac{a_n}{b_m} \cdot X^{n-m}.$$

$$\mathcal{H}(\mathcal{R}_g(f)) = \mathcal{H}\Big(f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)}g\Big) = \mathcal{H}\Big(f - \frac{a_nX^n}{b_mX^m}g\Big) =$$

$$\mathcal{H}\Big(f - \frac{a_n}{b_m}X^{n-m}(b_mX^m + ...)\Big) = \mathcal{H}(\underbrace{a_nX^n + ...}_{=f} - a_nX^n - ...).$$

Redzam, ka locekļi ar X^n saīsinās, tāpēc apgalvojums ir spēkā. ■

1.2. Teorēma par polinomu dalīšanu

1.2. teorēma. (*viena argumenta polinomu dalīšana ar atlikumu*) R ir IG, $f, g \in R[X]$ un g vecākais koeficients ir invertējams. Tad eksistē tieši viens polinomu pāris $d, r \in R[X]$:

1. $f = dg + r$,
2. $\deg(r) < \deg(g)$.

PIERĀDĪJUMS

d un r eksistence

Veiksim pēctecīgi redukcijas $\mathcal{R}_g$ sākot ar f, tik ilgi, kamēr redukcija ir definēta. Iegūsim polinomu virkni

$$f \to \mathcal{R}_g(f) \to \mathcal{R}_g^2(f) \to ... \to \mathcal{R}_g^l(f), \text{ kur } \deg \mathcal{R}_g^l(f) < \deg g.$$

Ir spēkā polinomiālu vienādību sistēma

$$\begin{cases} \mathcal{R}_g(f) = f - d_1 g \\ \mathcal{R}_g^2(f) = \mathcal{R}_g(f) - d_2 g \\ ... \\ \mathcal{R}_g^l(f) = \mathcal{R}_g^{l-1}(f) - d_l g. \end{cases}$$

Saskaitot vienādību kreisās un labās puses, iegūsim

$$\sum_{i=1}^{l} \mathcal{R}_g^i(f) = f + \sum_{i=1}^{l-1} \mathcal{R}_g^i(f) - \sum_{i=1}^{l} d_i g \implies$$

$$\underbrace{\mathcal{R}_g^l(f)}_{=r} = f - g \underbrace{\sum_{i=1}^{l} d_i}_{=q} \Longrightarrow$$

$$f = dg + r, \text{ kur } \deg r < \deg g.$$

d un r vienīgums

Pieņemsim, ka eksistē divi polinomu pāri $(d, r), (d', r')$:

$$f = dg + r = d'g + r' \Longrightarrow (d - d')g = r' - r.$$

Zinām, ka $\deg(r' - r) \leq \max\Big(\deg r', \deg(-r)\Big) < \deg(g)$.

$$\deg\Big((d - d')g\Big) = \deg(d - d') + \deg(g) < \deg(g) \Longrightarrow$$

$$\deg(d - d') = -\infty \Longrightarrow \begin{cases} d = d', \\ r = r'. \end{cases} \quad \blacksquare$$

1.2. piemērs. $f = X^5 + X^2 + 1$, $g = X^2 + X + 1$ virs $\mathbb{Z}$.

$$\mathcal{R}_g(f) = f - \left(\frac{\mathcal{H}(f)}{\mathcal{H}(g)}\right) \cdot g = f - X^3 \cdot g = -X^4 - X^3 + X^2 + 1;$$
$$\mathcal{R}_g^2(f) = \mathcal{R}_g(f_1) = f_1 - (-X^2) \cdot g = 2X^2 + 1;$$
$$\mathcal{R}_g^3(f) = \mathcal{R}_g(f_2) = f_2 - 2 \cdot g = -2X - 1.$$

$\mathcal{R}_g^4(f)$ nav definēts, jo $\deg\left(\mathcal{R}_g^3(f)\right) < \deg(g)$.

Rezultātā iegūsim

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

Vēlams izmantot dalīšanu "ar stūrīti".

Izdalot šos pašus polinomus virs $\mathbb{F}_2$ iegūsim

$$X^5 + X^2 + 1 = (X^3 + X^2)(X^2 + X + 1) + 1.$$

1.3. Hornera shēma (metode)

Dots polinoms $f \in R[X]$, $f = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$.

Redzam, ka

$$f = a_0 + X(a_1 + X(a_2 + X(...(a_{n-1} + X a_n)...)))$$

Izmantojot polinomu dalīšanu, var redzēt, ka f var iegūt kā polinomu p_n, kur polinomu virkne $\{p_i\}$, $0 \leq i \leq n$, tiek iegūta pēc šāda algoritma (*Hornera shēma*):

- $p_0 = a_n$,
- $p_i = a_{n-i} + X p_{i-1}$.

1.3. piemērs. $f = X^3 - 2X^2 + 4X - 3$.

- $p_0 = 1$,
- $p_1 = -2 + X$,
- $p_2 = 4 + X(-2 + X) = X^2 - 2X + 4$,
- $p_3 = f = -3 + X(X^2 - 2X + 4) = X^3 - 2X^2 + 4X - 3$.

2. LKD un MKD polinomu gredzenos

2.1. Kopīgie dalītāji un daudzkārtņi vispārīgos gredzenos

2.1.1. Dalītāji

$a \in R$ sauc par $\{b_1, ..., b_m\} \subseteq R$ *kopīgu dalītāju*, ja $\forall\ i: \ a \Big| b_i$. $\{b_1, ..., b_n\}$ dalītāju kopu apzīmē ar $D(b_1, ..., b_n)$.

Īpatnība patvaļīgos gredzenos: argumentu reizināšana ar invertējamiem elementiem nemaina kopīgo dalītāju kopu.

2.1. piemērs. $R = \mathbb{R}[X]$, $D(X, X^2) = \{cX \Big| c \in \mathbb{R}\backslash\{0\}\} = D(aX, X^2)$.

2.1. teorēma. R - IG. Tad

$$D(b_1, b_2) = D(ub_1, b_2),\ \forall\ u \in \mathcal{U}(R).$$

PIERĀDĪJUMS

$$\begin{cases} x \mid b_1 \\ x \mid b_2 \end{cases} \Longrightarrow \begin{cases} x \mid ub_1 \\ x \mid b_2 \end{cases}$$

$$\begin{cases} x \mid ub_1 \\ x \mid b_2 \end{cases} \Longrightarrow \begin{cases} ub_1 = qx \\ x \mid b_2 \end{cases} \Longrightarrow \begin{cases} b_1 = u^{-1}qx \\ x \mid b_2 \end{cases} \Longrightarrow \begin{cases} x \mid b_1 \\ x \mid b_2 \end{cases}$$

■

Par kopas $\{b_1, ..., b_m\}$ *lielāko kopīgo dalītāju (LKD)* sauksim to kopīgo dalītāju, kurš dalās ar jebkuru šīs kopas kopīgo dalītāju. Citiem vārdiem sakot, $d \in D(b_1, ..., b_n)$ ir LKD, ja

$$d' \in D(b_1, ..., b_n) \Longrightarrow d' \mid d.$$

2.1. piezīme. LKD ir noteikts ar precizitāti līdz asociācijai (argumentiem b_i un rezultātam):

$d = LKD(a, b) \Longrightarrow ud = LKD(a, b)$, kur $u \in \mathcal{U}(R)$.

Var izmainīt LKD definīciju tā, lai tas būtu viennozīmīgi noteikts. Piemēram, polinomu gredzenu gadījumā var pieprasīt, lai vecākais koeficients būtu vienāds ar 1.

2.2. piemērs. $\mathbb{Z}[X]$, $LKD(2X+2, X^2-1) \sim X+1$.

2.2. teorēma. R - IG.

1. $\forall\, b \in R:\ LKD(b,0) \sim b.$
2. $\forall\, a,b \in R:\ a|b \implies D(a,b) = D(a)$ un $LKD(a,b) \sim a.$
3. $\forall\, a,b,k \in R:$

$$D(a,b) = D(a-kb,b) \text{ un } LKD(a,b) \sim LKD(a-kb,b).$$

PIERĀDĪJUMS Tāds pats kā $\mathbb{Z}$ gadījumā. ■

2.1.2. Daudzkārtņi

$c \in R$ sauc par $\{b_1, ..., b_m\} \subseteq R$ *kopīgu daudzkārtni*, ja $\forall\ i$ izpildās $b_i \big| c$. $b_1, ..., b_n$ daudzkārtņu kopu apzīmē ar $M(b_1, ..., b_n)$.

Par kopas $\{b_1, ..., b_m\}$ *mazāko kopīgo daudzkārtni (MKD)* sauc to kopīgo daudzkārtni, kurš dala jebkuru šīs kopas kopīgo daudzkārtni. Citiem vārdiem sakot, c ir mazākais kopīgais daudzkārtnis, ja

$$c' \in M(b_1, ..., b_n) \implies c \big| c'.$$

2.2. piezīme. MKD ir noteikts ar precizitāti līdz asociācijai:
$c = MKD(a, b) \iff uc = MKD(a, b)$, kur $u \in \mathcal{U}(R)$.

2.3. piemērs. $\mathbb{Z}[X]$, $MKD(2X + 2, X^2 - 1) \sim 2(X^2 - 1)$.

2.2. Eiklīda algoritms polinomu gredzenos virs laukiem

2.2.1. Algoritms

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

Rīkojamies tāpat kā $\mathbb{Z}$ gadījumā:

- sākam ar polinomu pāri (f, g) kā ar pirmo pāri $(f, g) = (f_0, g_0)$, izmantojam matricas - $\left[\frac{f}{g}\right]$,
- veicam šādus soļus: ja ir iegūts pāris (f_i, g_i), $\deg f_i < \deg g_i$, tad izdalam g_i ar f_i: iegūstam vienādību $g_i = d_i f_i + r_i$, aizvietojam pāri (f_i, g_i) ar $(f_i, g_i - d_i f_i) = (f_i, r_i)$, kur $\deg r_i < \deg f_i$, matricu terminos - veicam REP3 $\left[\frac{f_i}{g_i}\right] \rightarrow \left[\frac{f_i}{r_i}\right]$,
- atkārtojam aizvietošanu tik ilgi, kamēr atlikums nav 0.

Dalīšana vienmēr ir iespējama, jo koeficienti ir invertējami. Iegūsim dalīšanas atlikumu (polinomu) virkni $r_1, r_2, ..., r_{n-1}, 0$ ar īpašību

$$\deg(r_1) > \deg(r_2) > ... > \deg(r_{n-1}).$$

Virkne, kuras elementi ir $\deg(r)$, kad r mainās algoritma izpildes gaitā, ir stingri dilstoša virkne, tāpēc šī algoritma realizācijā soļu skaits ir galīgs.

2.3. piezīme. r vietā var ievietot jebkuru elementu ur, kur $u \in \mathcal{U}(k[X])$.

2.4. piemērs. $R = \mathbb{Q}[X]$. $f = X^3 - 5X + 2$, $g = X^2 - X - 2$.

1. $f = (X+1)g + (-2X+4)$,
   $(f, g) \to (-2X+4, g)$ vai $(f, g) \to (X-2, g)$,
2. $g = (-\frac{1}{2}X - \frac{1}{2})(-2X+4) + 0$,
   $(g, -2X+4) \to (-2x+4, 0)$

2.2.2. Eiklīda algoritma saistība ar LKD

2.3. teorēma. k - lauks. Pieņemsim, ka tiek realizēts Eiklīda algoritms gredzenā $k[X]$ ar sākuma datiem (f, g), $g \nmid f$, tiek veikti n soļi, pēdējais nenulles atlikums ir r_{n-1}.

1. $D(f, g) = D(r_{n-1})$.
2. $LKD(f, g) \sim r_{n-1}$.

PIERĀDĪJUMS Tāds, pats kā $\mathbb{Z}$ gadījumā. ■

2.5. piemērs. $\mathbb{Q}[X]$. $f = X^3 - 5X + 2$, $g = X^2 - X - 2$.
Redzam, ka $LKD(f, g) \sim -2X + 4 \sim X - 2$.

2.2.3. Secinājumi no Eiklīda algoritma

2.4. teorēma. k - lauks.

1. $\forall \{f,g\} \subseteq k[X] \; \exists \; LKD(f,g)$.
2. $\forall \{f,g\} \subseteq k[X] \; \exists \; \{u,v\} \subseteq k[X]$:
$$LKD(f,g) = uf + vg.$$
($LKD(f,g)$ ir f un g $k[X]$-*lineāra kombinācija*)
3. $\forall \{f_1, ..., f_n\} \subseteq k[X] \; \exists \; \{u_1, ..., u_n\} \subseteq k[X]$:
$$LKD(f_1, ..., f_n) = \sum_{i=1}^{n} u_i f_i.$$
4. $$\begin{cases} a \Big| bc \\ LKD(a,b) \sim 1 \end{cases} \Longrightarrow a \Big| c.$$
5. $\forall \{a,b\} \subseteq k[X] \; \exists \; MKD(a,b) : \; MKD(a,b) \sim \dfrac{ab}{LKD(a,b)}$.

PIERĀDĪJUMS

1. Seko no Eiklīda algoritma.

2. Pierādījums līdzīgs $\mathbb{Z}$ gadījumam: jāapskata visas Eiklīda algoritma dalīšanas un jāizsaka LKD kā sākotnējo elementu lineāra kombinācija. Algoritms līdzīgs $\mathbb{Z}$ Blankinšipa algoritmam.

3. Izmantot indukciju ar parametru n.

Pieņemsim, ka apgalvojums ir patiess visām kopām, kurās ir ne vairāk kā $n-1$ elementi. Pierādīsim, ka tad tas ir patiess kopai $\{a_1, ..., a_n\}$.

$$LKD(f_1, ..., f_{n-1}, f_n) = LKD(\underbrace{LKD(f_1, ..., f_{n-1})}_{=b}, f_n) =$$

$$wb + u_n f_n = w \sum_{i=1}^{n-1} v_i f_i + u_n f_n = \sum_{i=1}^{n-1} (wv_i) f_i + u_n f_n.$$

4. $\begin{cases} bc = qa \\ 1 = xa + yb \end{cases} \Longrightarrow c = cxa + cyb =$

$$= acx + y \underbrace{bc}_{qa} = a(cx + yq) \implies a \mid c.$$

5. Pierādījums līdzīgs $\mathbb{Z}$ gadījumam. ■

2.4. piezīme. Ja ir doti vairāki polinomi, tad to LKD var atrast pēctecīgi.

Piemēram, ja ir doti 3 polinomi $f_1(X)$, $f_2(X)$, $f_3(X)$, tad no sākuma atrod

$$d_{12}(X) = LKD(f_1(X), f_2(X)),$$

pēc tam

$$LKD(d_{12}, f_3) = LKD(f_1(X), f_2(X), f_3(X)).$$

2.3. Eiklīda algoritma pielietojums - polinomiālu vienādojumu sistēmu risināšana ar vienu nezināmo

2.3.1. Polinomiālas vienādojumu sistēmas

Vienādojumu sistēmu

$$\begin{cases} f_1(X) = 0 \\ ... \\ f_n(X) = 0 \end{cases}, f_i \in R[X],$$

sauc par *polinomiālu vienādojumu sistēmu (PVS) ar vienu nezināmo.*

2.3.2. PVS seku vienādojumi

R - gredzens. Dota PVS P

$$\begin{cases} f_1(X) = 0 \\ ... \\ f_n(X) = 0 \end{cases}, f_i \in R[X].$$

Vienādojumu $g(X) = 0$ sauc par P *seku vienādojumu*, ja $\forall$ P atrisinājums t apmierina vienādojumu $g(t) = 0$:

$$\begin{cases} f_1(X) = 0 \\ \ldots \\ f_n(X) = 0 \end{cases} \Longrightarrow g(X) = 0.$$

2.6. piemērs. Vienkārša seku vienādojumu konstrukcija - kāpināšana naturālā pakāpē: $f(X) = 0 \Longrightarrow f^n(X) = 0.$

2.5. teorēma. Ir dota PVS P un tās seku vienādojums $g(X) = 0.$

Tad $\{\ \mathrm{P} \iff \begin{cases} \mathrm{P} \\ g(X) = 0 \end{cases}$

PIERĀDĪJUMS Ja t apmierina PVS P, tad t apmierina arī papildināto PVS $\begin{cases} \mathrm{P} \\ g(X) = 0 \end{cases}$, pēc seku vienādojuma definīcijas.

Ja t apmierina papildināto PVS $\begin{cases} \mathrm{P} \\ g(X) = 0 \end{cases}$, tad t apmierina arī

PVS P, kas satur mazāk vienādojumu. ■

2.3.3. PVS seku vienādojumu iegūšanas metode

2.6. teorēma. R - gredzens. Ja ir dota PVS

$$\begin{cases} f_1(X) = 0 \\ \ldots \\ f_n(X) = 0 \end{cases}, f_i \in R[X],$$

tad jebkuru divu polinomu f_i, f_j dalīšanas atlikums definē seku vienādojumu.

PIERĀDĪJUMS Pieņemsim, ka

$$f_i(X) = d(X)f_j(X) + r(X).$$

Pieņemsim, ka t ir PVS atrisinājums. Tad

$$\begin{cases} f_i(t) = 0 \\ f_j(t) = 0 \end{cases} \implies f_i(t) = d(t)f_j(t) + r(t) \implies r(t) = 0.$$

■

2.3.4. PVS risināšanas metode

Veicot redukcijas, agri vai vēlu iegūsim LKD.

2.7. teorēma. k - lauks. Dota PVS

$$\begin{cases} f_1(X) = 0 \\ \ldots \\ f_n(X) = 0 \end{cases}, f_i \in k[X].$$

Apzīmēsim $LKD\Big(f_1(X), f_2(X), ..., f_n(X)\Big)$ ar $D(X)$. Tad

$$\begin{cases} f_1(X) = 0 \\ \ldots \\ f_n(X) = 0 \end{cases} \iff \{\ D(X) = 0.$$

PIERĀDĪJUMS Seku vienādojumu pievienošanas rezultātā tiek iegūta ekvivalenta sistēma.

Sākotnējās PVS atrisinājumi apmierina visus seku vienādojumus.

Viens no seku vienādojumiem ir vienādojums

$$LKD\Big(f_1(X), ..., f_n(X)\Big) = D(X) = 0,$$

tātad

$$\begin{cases} f_1(X) = 0 \\ ... \\ f_n(X) = 0 \end{cases} \Longrightarrow \left\{ \; D(X) = 0. \right.$$

$$\forall \;\; i \;\; D(X) \Big| f_i(X) \; \Longrightarrow$$

$$\left\{ \; D(X) = 0 \right. \quad \Longrightarrow \begin{cases} f_1(X) = 0 \\ ... \\ f_n(X) = 0 \end{cases}$$

■

PVS risināšanas metode: atrast PVS polinomu LKD $D(X)$, atrisināt vienādojumu $D(X) = 0$.

3. 2.mājasdarbs

3.1. Obligātie uzdevumi

2.1 Izdalīt polinomus:

a) $X^4 + X + 1$ ar $X + 1$ virs $\mathbb{Z}$,
b) $2X^4 - 3X^3 + 5X^2 - 1$ ar $X^2 - 3$ virs $\mathbb{R}$,
c) $X^6 + X^4 + X^3 + X^2 + X$ ar $X^4 + X + 1$ virs $\mathbb{F}_2$,
d) $X^n + X^{n-1} + X$ ar $X^2 + 1$ virs $\mathbb{F}_2$, katram $n \geq 2$.

2.2 Atrast $LKD(f, g)$ un izteikt to lineāras kombinācijas veidā, atrast $MKD(f, g)$.

(a) $f = X^3 - X^2 - 3X + 3$, $g = X^2 - 1$, virs $\mathbb{Q}[X]$,
(b) $f = X^4 + X^2 + 1$, $g = X^3 + 1$, virs $\mathbb{F}_2[X]$,
(c) $f = X^3 + X + 1$, $g = X^3 + 2$, virs $\mathbb{F}_3[X]$.

2.3 Dotajiem polinomiem $f, g \in \mathbb{Q}[X]$ atrast tādus polinomus a un b, lai izpildītos vienādība $a(X)f(X) + b(X)g(X) = 1$:

(a) $f(X) = X^3$, $g(X) = (1 - X)^3$,
(b) $f(X) = X^2$, $g(X) = (1 - X)^4$.

2.4 Atrisināt PVS.

(a) $\begin{cases} X^3 - 2X^2 - 3X + 1 = 0 \\ X^4 + X^2 - 2X - 1 = 0 \end{cases}$, virs $\mathbb{Q}$.

(b) $\begin{cases} X^4 - X^3 - X^2 + 7X - 6 = 0 \\ X^4 + 2X^3 + X^2 - 4 = 0 \\ X^5 + 2X^4 - X - 2 = 0 \end{cases}$, virs $\mathbb{Q}$.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.5 Visiem naturāliem n un m polinomiem $f(X) = X^n$ un $g(X) = (1 - X)^m$ virs $\mathbb{Q}[X]$ atrast tādus polinomus a un b, lai izpildītos vienādība $a(X)f(X) + b(X)g(X) = 1$.

2.6 k - lauks, $f, g \in k[X]$, $d = LKD(f, g)$. Pierādīt, ka $\exists$ viennozīmīgi noteikti $a, b \in k[X]$:

(a) $d = af + bg$;
(b) $\deg a < \deg g - \deg d$,
(c) $\deg b < \deg f - \deg d$.

Izstrādāt algoritmu a un b atrašanai.