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

Studiju kurss

Polinomu algebra

10.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Grobnera bāzes

Uzskatīsim, ka polinomi ir definēti virs lauka k.

1.1. Pamati

1.1.1. Motivācija

Dažādās situācijās ir lietderīgi risināt problēmas, kas ir saistītas ar $R[X_1, ..., X_n]$ ideāliem:

- noteikt, vai dotais polinoms pieder dotajam ideālam,
- atrast ērtu dotā ideāla veidotājelementu kopu (*ideāla bāzi*).
- atrast polinoma atlikumu pēc dotā ideāla moduļa standarta formā.

1.1. piemērs. Pieņemsim, ka ir dota algebrisku vienādojumu sistēma

$$\begin{cases} g_1(X_1, ..., X_n) = 0 \\ g_2(X_1, ..., X_n) = 0 \\ ... \\ g_m(X_1, ..., X_n) = 0 \end{cases}$$

Ja elementu virkne $(X_1, ..., X_n)$ apmierina sistēmu, tad tā apmierina arī jebkuru vienādojumu

$$f_1 g_1 + f_2 g_2 + ... + f_m g_m = 0.$$

Šādu vienādojumu kreisās puses var interpretēt kā ideāla elementus.

Ideālu $I = (g_1, g_2, ..., g_m)$ sauc par dotās algebriskās sistēmas *seku ideālu*.

Daudzus jautājumus, kas ir saistīti ar algebrisku sistēmu risināšanu, var formulēt seku ideāla terminos:

- ja $1 \in I$ jeb $I = k[X_1, ..., X_n]$, tad sistēmai nav atrisinājumu,
- ja $f(X_i) \in I$, tad sistēma vienkāršojas, jo, lai atrastu X_i, ir jāatrisina vienādojums $f(X_i) = 0$.

1.1. piezīme. Ievērosim, ka šīs problēmas ir viegli risināmas gredzenā $k[X]$:

- noteikt, vai dotais polinoms pieder dotajam ideālam - tā kā katrs ideāls ir galvenais ideāls formā (g), tad $f \in (g) \iff atl(f, g) = 0$,
- atrast ērtu dotā ideāla veidotājelementu kopu (*ideāla bāzi*) - ja $I = (g_1, ..., g_n)$, tad $I = (LKD(g_1, ..., g_n))$,
- atrast polinoma atlikumu pēc dotā ideāla moduļa standarta formā - ir jāatrod $atl(f, g)$, atlikumu pakāpes nav lielākas par $\deg(g) - 1$.

Pārejot uz vairāku argumentu polinomiem rodas grūtības:

- nav uzreiz skaidrs, kā mēģināt meklēt atlikumu pēc dotā ideāla moduļa,

- ideālam var eksistēt daudz dažādu bāzu (var domāt par zināmu analoģiju ar lineārajām telpām, galvenie ideāli ir "viendimensionāli").

1960.gados tika izstrādāta teorija, kas atrisināja šādas problēmas - Grobnera (Grēbnera, Gröbner) bāzu teorija (1965.g, B.Buhbergers).

1.1.2. Definīcija

1.2. piezīme. Iepriekš tika definēta polinoma $f \in k[X_1, ..., X_n]$ atlikuma (redukcijas) atrašanas operācija, ja ir dota polinomu virkne $(g_1, ..., g_m)$. To var uzskatīt par pirmo tuvinājumu polinoma atlikuma atrašanai pēc moduļa $I = (g_1, ..., g_m)$.

Ja

$$f = \sum_{i=1}^{m} a_i g_i + r$$

ir redukcijas atrašanas rezultāts, tad apzīmēsim r ar $\overline{f}^{\{g_1,...,g_m\}}$.

Trūkumi:

- polinoma redukcija ir atkarīga no elementu kārtības virknē,
- atlikums var būt atšķirīgs no 0, ja polinoms pieder ideālam $(g_1, ..., g_m)$.

1.2. piemērs. Pieņemsim, ka $f = XY^2 - X$, $g_1 = XY + 1$, $g_2 = Y^2 - 1$, definēsim monomu kārtību ar nosacījumu $X \succ Y$. Izdalīsim f ar g_1

un g_2 dažādās kārtībās:

- dalot f ar (g_1, g_2), iegūsim
$$f = Y \cdot g_1 + 0 \cdot g_2 + (-X - Y);$$
- dalot f ar (g_2, g_1), iegūsim
$$f = X \cdot g_2 + 0 \cdot g_1 + 0.$$

Ievērosim, ka dalot pirmajā kārtībā, atlikums nav vienāds ar 0, bet no dalīšanas rezultāta otrajā kārtībā seko, ka $f \in (g_1, g_2)$.

Šajā gadījumā problēma ir tur, ka
$$-X - Y = f - Y \cdot g_1 = (-Y)g_1 + X \cdot g_2 \in (g_1, g_2),$$
bet neviens no $-X - Y$ monomiem nedalās ne ar vienu no g_i vecākajiem monomiem.

Šo problēmu var mēģināt risināt, mēģinot atrast labāku ideāla bāzi.

Nenulles polinomu kopu $\mathcal{F} = \{f_1, ..., f_m\}$ sauksim par ideāla $I \subseteq k[X_1, ..., X_n]$ *Grobnera bāzi (GB)*, ja

- $\mathcal{F} \subseteq I$,
- katram nenulles $f \in I$ eksistē i tāds, ka $\mathcal{H}(f)$ dalās ar $\mathcal{H}(f_i)$.

Ideāla I GB apzīmēsim ar $\mathcal{G}(I)$.

1.3. piemērs. Ja $I = (X, Y)$, tad $\{X, Y\}$ ir GB.

Ja $I = (XY + 1, Y^2 - 1)$, tad $\{XY + 1, Y^2 - 1\}$ nav I GB, jo polinomam $-X - Y \in I$ vecākais loceklis $\mathcal{H}(f) = -X$ nedalās ne ar vienu no $\mathcal{H}(XY + 1) = XY$ vai $\mathcal{H}(Y^2 - 1) = Y^2$.

1.1.3. Grobnera bāzu pamatīpašības

1.1. teorēma.

1. Ideāla GB ir tā veidotājelementu kopa (īsta bāze).
2. Jebkuram f redukcija pēc GB elementu kopas nav atkarīga no to kārtības.
3. $f \in I \iff \overline{f}^{\mathcal{G}(I)} = 0.$

PIERĀDĪJUMS Pieņemsim, ka ir dots ideāls $I \in k[X_1, ..., X_n]$ un $\mathcal{F} = \{f_1, ..., f_m\} = \mathcal{G}(I)$.

1. Ja $f \in I$, tad eksistē $g \in \mathcal{F}$ tāds, ka $\mathcal{H}(f)$ dalās ar $\mathcal{H}(g)$, tāpēc

$$\tilde{f} = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} g \in I.$$

Redzam, ka $f \succ \tilde{f}$.

Tā kā $\tilde{f} \in I$, tad eksistē $h \in \mathcal{F}$ tāds, ka $\mathcal{H}(\tilde{f})$ dalās ar $\mathcal{H}(h)$. Atkal

atņemsim no $\tilde{f}$ atbilstošu h daudzkārtni un iegūsim polinomu, kura vecākais loceklis ir stingri mazāks nekā $\tilde{f}$ vecākais loceklis.

Turpinot šo procesu pēc galīga skaita soļu iegūsim 0, jo polinomi virknē paliek ar katru pārveidojumu stingri mazāki. Seko, ka f ir izsakāms kā $\mathcal{F}$ elementu lineāra kombinācija ar koeficientiem no $k[X_1, ..., X_n]$.

2. Pieņemsim, ka f var reducēt divos veidos:

$$f = a_1 f_1 + ... + a_m f_m + r,$$
$$f = b_1 f_1 + ... + b_m f_m + \hat{r}.$$

Seko, ka

$$r - \hat{r} = (b_1 - a_1) f_1 + ... + (b_m - a_m) f_m \in I.$$

Tā kā $\mathcal{F}$ ir GB, tad $\mathcal{H}(r - \hat{r})$ dalās ar kādu $\mathcal{H}(f_i)$, tātad arī $\mathcal{H}(r)$

dalās ar kādu $\mathcal{H}(f_i)$. Tas ir pretrunā ar redukcijas algoritmu, jo to varētu turpināt attiecībā uz r.

3. $\overline{f}^{\mathcal{G}(I)} = 0 \implies f \in I$, jo šādā gadījumā $f = a_1 f_1 + ... + a_m f_m$.

Pieņemsim, ka redukcijas algoritma rezultātā ir iegūta vienādība

$$f = a_1 f_1 + ... + a_m f_m + r.$$

Ja $f \in I$, tad $r = f - a_1 f_1 - .. - a_m f_m \in I$. Ja $r \neq 0$, tad $\mathcal{H}(r)$ dalās ar kādu $\mathcal{H}(f_i)$. Tas ir pretrunā ar redukcijas algoritmu, jo to varētu turpināt attiecībā uz r. ■

1.1.4. Grobnera bāzu eksistence

Atcerēsimies, ka n-argumentu polinomu monomu pakāpes var interpretēt kā vektorus ar veselām nenegatīvām koordinātēm jeb kopas $\mathbb{N}^{*n}$ elementus.

Ja $v \in \mathbb{N}^{*n}$, tad definēsim

$$v + \mathbb{N}^{*n} = \{w \in \mathbb{N}^{*n} | w = v + u, \text{ kur } u \in \mathbb{N}^{*n}\}.$$

1.4. piemērs. $n = 2$, $v = (2, 0)$.

1.3. piezīme. Var definēt vektora *ēnu*. Katru $\mathbb{N}^{*2}$ apakškopu var nosegt ar galīga skaita vektoru ēnām.

1.2. teorēma. (Diksona lemma) Katrai kopai $\mathcal{M} \subseteq \mathbb{N}^{*n}$ eksistē galīga kopa $\{v_1, ..., v_l\} \subseteq \mathcal{M}$ tāda, ka

$$\mathbb{M} \subseteq (v_1 + \mathbb{N}^{*n}) \cup ... \cup (v_l + \mathbb{N}^{*n}).$$

(katru kopu $\mathcal{M} \subseteq \mathbb{N}^{*n}$ var pārklāt ar galīgas apakškopas elementu ēnām)

PIERĀDĪJUMS Patstāvīgs darbs.
■

1.3. teorēma. Katram ideālam $I \in k[X_1, ..., X_n]$ eksistē GB.

PIERĀDĪJUMS Definēsim

$$\mathcal{M} = \{v \in \mathbb{N}^{*n} | \text{ eksistē } f \in I : \mathcal{H}(f) = aX^v\}.$$

Saskaņā ar Diksona lemmu kopu $\mathcal{M}$ var noklāt ar galīgas apakškopas elementu ēnām: eksistē vektoru kopa $\{v_1, ..., v_l\} \subseteq \mathcal{M}$ tāda, ka

$$\mathcal{M} \subseteq (v_1 + \mathbb{N}^{*n}) \cup ... \cup (v_l + \mathbb{N}^{*n}).$$

Seko, ka

- eksistē elementi $f_i \in I$, tādi, ka $X^{v_i} | \mathcal{H}(f_i)$,
- katram $f \in I$ eksistē v_i tāds, ka

$$\mathcal{H}(f) = aX^{v_i+u} = aX^{v_i}X^u.$$

Esam ieguvušu, ka kopa $\{f_1, ..., f_l\}$ ir GB. ■

1.2. Buhbergera algoritms

1.2.1. S-polinomi

Ja $f, g \in k[X_1, ..., X_n]$, tad pieņemsim, ka

$$\mathcal{H}(f) = aX^\alpha,$$
$$\mathcal{H}(g) = bX^\beta.$$

Definēsim

$$S(f,g) = \frac{X^\gamma}{\mathcal{H}(f)} \cdot f - \frac{X^\gamma}{\mathcal{H}(g)} \cdot g,$$

kur $X^\gamma = MKD(X^\alpha, X^\beta)$.

1.5. piemērs. Ja $f = XY + 1$ un $g = Y^2 - 1$, tad

$$S(f,g) = \frac{XY^2}{XY}(XY+1) - \frac{XY^2}{Y^2}(Y^2-1) = X + Y.$$

1.2.2. Buhbergera kritērijs

1.4. teorēma. Kopa $\mathcal{F} = \{f_1, ..., f_m\}$ ir ideāla $I = (f_1, ..., f_m)$ GB tad un tikai tad, ja

$$\overline{S(f_i, f_j)}^{\mathcal{F}} = 0$$

visiem pāriem $i \neq j$.

1.2.3. Algoritms

Buhbergera algoritma īss apraksts - lai atrastu ideāla $I = (g_1, ..., g_l)$ GB, veicam šādas darbības:

- definējam sākotnējo ģeneratoru kopu kā mainīgu kopu $\mathcal{G}$,
- ja atrodam polinomu pāri $\{g_i, g_j\} \subseteq \mathcal{G}$ tādu, ka

$$s = \overline{S(g_i, g_j)}^{\mathcal{G}} \neq 0,$$

(vismaz vienai elementu kārtībai kopā $\mathcal{G}$), tad definējam

$$\mathcal{G} := \mathcal{G} \cup s,$$

- atkārtojam iepriekšējo soli tik ilgi, kamēr notiek $\mathcal{G}$ izmaiņas.

1.6. piemērs. Ja $I = (X, Y)$, tad saskaņā ar Buhbergera algoritmu nekas nav jādara, jo $S(X, Y) = 0$. Tādējādi sākotnējā veidotājelementu kopa (bāze) ir GB.

Ja $I = (\underbrace{XY + 1}_{g_1}, \underbrace{Y^2 - 1}_{g_2})$, tad saskaņā ar Buhbergera algoritmu ir jāveic šādi soļi:

1.
$$g_3 = S(f, g) = \frac{XY^2}{XY}(XY + 1) - \frac{XY^2}{Y^2}(Y^2 - 1) =$$
$$X + Y = \overline{X + Y}^{\{g_1, g_2\}} \neq 0,$$
tāpēc
$$\mathcal{G} = \{XY + 1, Y^2 - 1\} \cup \{X + Y\} = \{g_1, g_2, g_3\}.$$

2. $S(g_1, g_3) = -(Y^2 - 1)$, $S(g_2, g_3) = X + Y^3 = Y(Y^2 - 1) + (X + Y)$, tāpēc neko jaunu mēs neiegūsim un GB ir vienāda ar $\{g_1, g_2, g_3\}$.

1.5. teorēma. Buhbergera algoritms apstājas pēc galīga skaita soļu realizācijas un tā rezultāts ir GB.

PIERĀDĪJUMS Diskusija.

1.3. Reducētās Grobnera bāzes

1.3.1. Neviennozīmīgums

GB nav noteiktas viennozīmīgi.

1.7. piemērs. Jebkurai GB var pievienot jebkuru citu ideāla elementu, jaunā kopa arī būs GB.

Kopas $\{X, Y\}$ un $\{X + Y, Y\}$ ir divas dažādas ideāla $I = (X, Y)$ GB.

1.6. teorēma. Ja $\mathcal{F} = \{f_1, ..., f_m\}$ ir GB un eksistē $i : 1 \leq i \leq m-1$ tāds, ka $\mathcal{H}(f_m)$ dalās ar $\mathcal{H}(f_i)$, tad $\mathcal{F} \backslash f_m$ arī ir GB.

PIERĀDĪJUMS Izmantosim GB pamatīpašību:

$$f \in I \implies \mathcal{H}(f_j) | \mathcal{H}(f)$$

kādam j katrai GB $\mathcal{F}$.

Ja $f \in I$, tad eksistē j tāds, ka $\mathcal{H}(f_j) | \mathcal{H}(f)$. Ja $j = m$, tad

$$\mathcal{H}(f_i) | \mathcal{H}(f_j) | \mathcal{H}(f),$$

tātad $\mathcal{H}(f_i) | \mathcal{H}(f)$. ■

1.3.2. Definīcijas

Grobnera bāzi $\{f_1, ..., f_m\}$ sauksim par *reducētu Grobnera bāzi (RGB)*, ja

- nekādam indeksu pārim $i \neq j$ neviens f_i monoms nedalās ar $\mathcal{H}(f_j)$;
- katram i lauka k koeficients monomā $\mathcal{H}(f_i)$ ir vienāds ar 1.

1.8. piemērs. Ideālam (X, Y) kopa $\{X, Y\}$ ir RGB, bet $\{X + Y, Y\}$ - nav.

Ideālam $(XY + 1, Y^2 - 1)$ kopa $\{XY + 1, Y^2 - 1, X + Y\}$ nav RGB.

1.3.3. Reducētās Grobnera bāzes vienīgums

1.7. teorēma. Katram ideālam eksistē viena RGB.

1.3.4. Reducētās Grobnera bāzes atrašanas algoritms

RGB var atrast, ja Buhbergera algoritmā veic šādu modifikāciju:

- algoritma sākumā un pēc katra jauna S-polinoma redukcijas pievienošanas atmet jebkuru polinomu f_i, ja eksistē cits polinoms f_j tāds, ka $\mathcal{H}(f_i)$ dalās ar $\mathcal{H}(f_j)$,
- algoritma sākumā un pēc katra jauna S-polinoma redukcijas pievienošanas veic visas iespējamās savstarpējās redukcijas, pievieno radušos nenulles elementus.

1.9. piemērs. Ja $I = (\underbrace{XY+1}_{g_1}, \underbrace{Y^2-1}_{g_2})$, tad saskaņā ar reducēto Buhbergera algoritmu ir jāveic šādi soļi:

1.

$$g_3 = S(f,g) = \frac{XY^2}{XY}(XY+1) - \frac{XY^2}{Y^2}(Y^2-1) =$$

$$X + Y = \overline{X+Y}^{\{g_1,g_2\}} \neq 0,$$

tāpēc

$$\mathcal{G} = \{XY+1, Y^2-1\} \cup \{X+Y\} = \{g_1, g_2, g_3\}.$$

2. Tā kā $\mathcal{H}(XY+1) = XY$, un tas dalās ar $\mathcal{H}(g_3) = X$, tad $g_1 = XY+1$ ir jāizmet no $\mathcal{G}$.
3. $S(g_2, g_3) = X + Y^3 = Y(Y^2-1) + (X+Y)$, tāpēc neko jaunu mēs neiegūsim un reducētā Grobnera bāze ir vienāda ar $\{g_2, g_3\}$.

2. 10.mājasdarbs

2.1. Obligātie uzdevumi

10.1 Pierādīt, ka kopa $\{Y - X^2, Z - X^3\}$ nav GB, ja $X \succ Y \succ Z$.

10.2 Atrast $S(f, g)$, ja $X \succ Y \succ Z$:

(a) $f = X^2Z - Y^2$, $g = XYZ^2 + XZ^4$, virs $\mathbb{Q}$,
(b) $f = XY + Z^3$, $g = Z^2 + Z$, virs $\mathbb{F}_2$

10.3 Atrodiet RGB, ja $X \succ Y \succ Z$ dotajiem ideāliem:

(a) $I = (X^2Y - 1, XY^2 - X)$,
(b) $I = X^2 + Y, X^4 + 2X^2Y + Y^2 + 3$,
(c) $I = (X - Y^4, Y - Z^5)$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

10.4 Dots, ka $f, g \in k[X_1, ..., X_n]$, $LKD(\mathcal{H}(f), \mathcal{H}(g)) = 1$, koeficienti pie f un g vecākajiem koeficientiem ir 1. Pierādiet, ka

$$S(f, g) = (f - \mathcal{H}(f))g - (g - \mathcal{H}(g))f.$$