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

Studiju kurss

Polinomu algebra

8.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- vispārināt VAPG gadījumā dalīšanu ar atlikumu ar vienu vai vairākiem polinomiem,
- definēt Grobnera bāzes, apskatīt to vienkāršākās īpašības.

Lekcijas kopsavilkums:

- VAPG var definēt polinomu dalīšanu ar atlikumu izmantojot termu un polinomu leksikogrāfisko sakārtojumu,
- VAPG var definēt lietderīgu ideālu ģeneratoru kopas īpašību (Grobnera bāzes īpašību).

Svarīgākie jēdzieni: VAP redukcija, VAP dalīšana ar vienu un vairākiem dalītājiem, polinomiālas vienādojumu sistēmas seku ideāls, VAPG ideāla Grobnera bāze.

Svarīgākie fakti un metodes: redukcijas īpašības, VAP dalījuma un atlikuma eksistence, Grobnera bāze pamatīpašības.

1. Vairāku argumentu polinomu dalīšana ar atlikumu

Sākot no šīs sadaļas $R = k$ ir lauks.

1.1. Redukcija

$f, g \in k[X_1, ..., X_n]$. Ja kāds f monoms aX^μ dalās ar $\mathcal{H}(g)$, tad pārveidojumu

$$f \to f - \frac{aX^\mu}{\mathcal{H}(g)} g = \tilde{f}$$

sauksim par *redukcijas soli* un apzīmēsim ar

$$f \xrightarrow{g} \tilde{f}.$$

1.1. piemērs. $f = X_1^2 X_2 + X_2^2$, $g = X_1 X_2 - 1$.
$\tilde{f} = f - X_1 g = X_1 + X_2^2$.

1.1. teorēma.

1. Redukcijas solis

$$f \to f - \frac{aX^\mu}{\mathcal{H}(g)} g = \tilde{f}$$

samazina polinomu leksikogrāfiskajā sakārtojumā:

$$f \succ \tilde{f}.$$

2. Ja $\mathcal{H}(g)|\mathcal{H}(f)$, tad redukcijas solis

$$f \to f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} g = \tilde{f}$$

samazina polinoma vecāko termu:

$$\mathcal{H}(f) \succ \mathcal{H}(\tilde{f}).$$

PIERĀDĪJUMS

1. Redzam, ka $\mathcal{H}(f - \tilde{f}) \prec aX^\mu$, jo aX^μ saīsinās.

2. Seko no 1. ■

$f \in k[X_1, ..., X_n]$, $G = \{g_1, ..., g_m\} \subseteq k[X_1, ..., X]$.

Teiksim, ka f *reducējas uz* $\widehat{f}$ mod G (apzīmē ar $f \xrightarrow{G} \widehat{f}$), ja $\exists$ redukcijas soļu virkne

$$f \xrightarrow{g_{i_1}} f_1 \xrightarrow{g_{i_2}} f_2 ... \xrightarrow{g_{i_l}} f_l = \widehat{f}.$$

Jebkuru (pabeigtu) redukcijas rezultātu apzīmēsim ar $\overline{f}^G$.

1.2. piemērs. $f = X_1^2 X_2 + X_2^2$, $g_1 = X_1 X_2 - 1$, $g_2 = X_2 + 1$.
$f \xrightarrow{g_1} X_1 + X_2^2 \xrightarrow{g_2} X_1 - X_2 \xrightarrow{g_2} X_1 + 1 = \overline{f}^{\{g_1, g_2\}}$.

1.2. Viens dalītājs

Ja ir doti divi VAP f un g, tad var vispārināt viena argumenta polinomu dalīšanas procedūru, ko var pamatot divos veidos:

- var atņemt no dalāmā f dalītāja g daudzkārtņus tā, lai atlikums būtu pēc iespējas mazāks leksikogrāfiskajā sakārtojumā;
- var veikt maksimāli garu f redukcijas soļu virkni ar g.

Dabiski ir izvēlēties šādu algoritmu: katrā solī veikt reducēt lielāko f termu, kas dalās ar $\mathcal{H}(g)$.

1.3. piemērs. Izdalīsim $X_1^3X_2 + X_1^2 + X_1X_2$ ar $X_1X_2 + X_2^2$ virs $\mathbb{Q}$ vai $\mathbb{R}$. Iegūsim, ka

$$d = X_1^2 - X_1X_2 + X_2^2 + 1,$$
$$r = X_1^2 - X_2^4 - X_2^2.$$

1.2. teorēma. $f, g \in k[X_1, ..., X_n]$, $f \neq 0, g \neq 0$. Tad $\exists$ tieši viens polinomu pāris (d, r), kuram izpildās nosacījumi

1. $f = dg + r$;
2. $r = 0$ vai neviens r terms nedalās ar $\mathcal{H}(g)$.

PIERĀDĪJUMS
Eksistence
Algoritms.

Doti $f, g \in k[X_1, ..., X_n]$. Sākotnēji definēsim

$$\begin{cases} r_t = f, \\ d_t = 0. \end{cases}$$

A. Atradīsim vecāko r_t termu $a_\mu X^\mu$, kas dalās ar $\mathcal{H}(g)$:
ja tāds neeksistē, tad apstājamies,
ja eksistē, tad veiksim vienu redukcijas soli, definēsim

$$\begin{cases} r_t := r_t - \frac{a_\mu X^\mu}{\mathcal{H}(g)} g, \\ d_t := d_t + \frac{a_\mu X^\mu}{\mathcal{H}(g)}. \end{cases}$$

B. Ja $r_t = 0$, tad apstājamies, ja nē, tad ejam uz A.

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc $\forall$ A tipa soļa izpildes r_t samazinās leksikogrāfiskajā sakārtojumā.

Algoritma darba rezultātā iegūtais $r_t = r$, $d_r = d$ un

$$f - r = dg.$$

Vienīgums Pieņemsim, ka

$$f = dg + r = \tilde{d}g + \tilde{r},$$

kur r un $\tilde{r}$ apmierina teorēmas nosacījumu.

$\Longrightarrow$ $r - \tilde{r} = g(\tilde{d} - d)$ $\Longrightarrow$ $\mathcal{H}(g)|\mathcal{H}(r - \tilde{r}) \vee \ g = 0.$

$g = 0$ $\Longrightarrow$ $r = \tilde{r}.$

$\mathcal{H}(g)|\mathcal{H}(r - \tilde{r})$ $\Longrightarrow$ vismaz viens no r vai $\tilde{r}$ termiem dalās ar $\mathcal{H}(g)$

$\Longrightarrow$ redukciju var turpināt attiecībā uz r vai $\tilde{r}$ - pretruna. ■

1.3. Vairāki dalītāji

Dots viens dalāmais f un vairāki dalītāji $g_1, ..., g_m$.

Var veikt vairākus redukcijas soļus, iespējams, ar dažādiem dalītājiem, katrs redukcijas solis samazina atlikumu leksikogrāfiskajā sakārtojumā $\Longrightarrow$ redukcijas process apstāsies pēc galīga soļu skaita.

1.3. teorēma. $\{f, g_1, g_2, ..., g_m\} \subseteq R[X]$, $f \neq 0$, $g_i \neq 0$.
Tad $\exists$ polinomu virkne $(d_1, d_2, ..., d_m, r)$:

1. $f = d_1 g_1 + d_2 g_2 + ... + d_m g_m + r$;
2. $r = 0$ vai neviens r terms nedalās ar $\mathcal{H}(g_i)$ $\forall$ i.

PIERĀDĪJUMS Sākot ar f veiksim redukcijas izmantojot $g_1, .., g_m$ tik ilgi, kamēr redukcijas ir iespējamas - kamēr kārtējās redukcijas rezultāts satur monomus, kas dalās ar kādu $\mathcal{H}(g_i)$:

$$f \dashrightarrow \underbrace{f - c_1 g_{i_1}}_{r_1} \dashrightarrow \underbrace{(f - c_1 g_{i_1}) - c_2 g_{i_2}}_{r_2} \dashrightarrow ...$$

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc katras redukcijas izpildes atlikums samazinās leksikogrāfiskajā sakārtojumā.

Savelkot līdzīgos locekļus, iegūsim, ka

$$f - \sum_{i=1}^{m} d_i g_i = r,$$

kur $r = 0$ vai neviens r monoms nedalās ne ar kādu $\mathcal{H}(g_i)$. ■

r sauc par f *atlikumu* vai *redukciju* mod $(g_1, ..., g_m)$.

1.1. piezīme. Reducijas algoritmu var standartizēt vairākos veidos. Piemēram, katrā redukcijas solī izvēlamies leksikogrāfiski lielāko reducējamo monomu un mazāko reducējošo polinomu g_i.

1.4. piemērs. Atradīsim $X^4 + Y^4$ redukciju mod $(XY + 1, X^2 + Y)$ virs $\mathbb{Q}$ vai $\mathbb{R}$ (definējot $X \succ Y$).

1. Reducējam ar g_2: $r_1 := f - X^2 g_2 = -X^2 Y + Y^4$.
2. Reducējam ar g_1: $r_2 := r_1 - (-X)g_1 = X + Y^4$
3. Jāapstājas, jo X un Y^4 nedalās ne ar XY, ne ar X^2.

Tādējādi

$$r = X + Y^4 = f - X^2 g_2 - (-X)g_1$$

vai

$$\underbrace{X^4+Y^4}_{f} = \underbrace{(-X)}_{d_1}\underbrace{(XY+1)}_{g_1} + \underbrace{X^2}_{d_2}\underbrace{(X^2+Y)}_{g_2} + \underbrace{(X+Y^4)}_{r}.$$

Mainot dalītāju kārtību, mainīsies rezultāts:

$$X^4+Y^4 = (X^2-Y)(X^2+Y) + 0\cdot(XY+1) + \underbrace{(Y^4+Y^2)}_{=r}.$$

1.2. piezīme. Dalīšanas rezultāts (atlikums) ir atkarīgs no dalītāju kārtības.

2. Grobnera bāzes

2.1. Motivācija

$R = k[X_1, ..., X_n]$ ideāli - kopas formā

$$\langle f_1, ..., f_m \rangle = \{ f \in R | f = \sum_i a_i f_i, \text{ kur } a_i \in R \}.$$

2.1. piezīme. Ideālus var uzskatīt par lineāru apakštelpu analogiem gredzenos.

Ir lietderīgi risināt šādas problēmas par $k[X_1, ..., X_n]$ ideāliem:

- noteikt, vai dotais polinoms pieder dotajam ideālam I,
- atrast ērtu dotā ideāla I ģeneratoru kopu (*ideāla bāzi*), citiem vārdiem sakot, izteikt I formā $\langle a_1, ..., a_m \rangle$,
- atrast polinoma atlikumu (redukciju) mod I standarta formā.

2.1. piemērs. Ir dota polinomiālu vienādojumu sistēma

$$\begin{cases} f_1(X_1, ..., X_n) = 0 \\ ... \\ f_m(X_1, ..., X_n) = 0. \end{cases}$$

Ja virkne $(a_1, ..., a_n) \in k^n$ apmierina sistēmu, tad tā apmierina arī jebkuru vienādojumu

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

Šādu vienādojumu kreisās puses var interpretēt kā ideāla elementus. Ideālu $I = \langle f_1, f_2, ..., f_m \rangle$ sauc par dotās vienādojumu sistēmas *seku ideālu*.

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

- $\Big(1 \in I\Big) \implies \Big(1 = 0\Big) \implies$ sistēmai nav atrisinājumu,
- $f(X_i) \in I \implies$ sistēma vienkāršojas, jo, lai atrastu X_i, ir jāatrisina vienādojums $f(X_i) = 0$.

Polinomiālu vienādojumu sistēmas parādās daudzās situācijās:

- analītiskajā un algebriskajā ģeometrijā, pielietojumi - GPS, robotu projektēšanā un ģeometrijas teorēmu pierādīšanā,
- diferenciālvienādojumu risināšanā,
- grafu teorijā (diskrētu objektu īpašības var iekodēt poliomiālu vienādojumu sistēmu formā),
- kriptogrāfijā - *polinomiālās kriptosistēmas.*

2.2. piezīme. Šīs problēmas ir viegli risināmas gredzenā $k[X]$:

- noteikt, vai dotais polinoms pieder ideālam - katrs ideāls ir galvenais ideāls formā $\langle g \rangle \implies \Big(f \in \langle g \rangle \iff [f]_g = 0 \Big)$,
- atrast labu (piemēram, minimālu) dotā ideāla veidotājelementu kopu (*ideāla bāzi*) - $I = \langle g_1, ..., g_n \rangle \implies I = \langle LKD(g_1, ..., g_n) \rangle$,
- atrast polinoma atlikumu mod I standarta formā - ir jāatrod $atl(f, g)$, $\deg(atl(f, g)) \leq \deg(g) - 1$.

2.3. piezīme. Šīs problēmas ir viegli risināmas, ja sākotnējie I ģeneratori ir lineāri polinomi - jāpielieto Gausa metode.

Pārejot uz vairāku argumentu polinomiem rodas grūtības:

- nav skaidrs, kā meklēt atlikumu mod I, jo redukcija nav noteikta viennozīmīgi VAP gadījumā;
- nav skaidrs, kā pārbaudīt, vai dotais polinoms f pieder ideālam $I = \langle f_1, ..., f_m \rangle$: ja mēģināt izteikt f formā $\sum_{i=1}^{m} g_i f_i$, tad cik augstas var būt g_i pakāpes?
- ideālam var eksistēt daudz dažādu bāzu (var domāt par analoģiju ar lineārajām telpām).

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

2.2. Definīcija

2.4. piezīme. Iepriekš tika definēta polinoma $f \in k[X_1, ..., X_n]$ atlikuma atrašanas operācija, ja ir dota kopa $G = \{g_1, ..., g_m\}$. Tas ir

pirmais tuvinājums polinoma atlikumam mod $I = \langle g_1, ..., g_m \rangle$.

Trūkumi:

- polinoma redukcija ir atkarīga no redukcijas soļu kārtības,
- atlikums var būt atšķirīgs no 0, ja polinoms pieder ideālam $\langle g_1, ..., g_m \rangle$.

2.2. piemērs. $f = XY^2 - X$, $g_1 = XY + 1$, $g_2 = Y^2 - 1$, 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 $f \in \langle g_1, g_2 \rangle$.

Šajā gadījumā problēma ir tur, ka

$$-X - Y = f - Y \cdot g_1 = (-Y)g_1 + X \cdot g_2 \in \langle g_1, g_2 \rangle,$$

bet neviens no $-X - Y$ monomiem nedalās ne ar vienu no $\mathcal{H}(g_i)$.

Šo problēmu var risināt, mēģinot atrast labāku ideāla bāzi, kuras elementu vecākie termi ir pēc iespējas mazāki -

vislabāk būtu, ja jebkuram ideāla elementam varētu vienmēr samazināt vecāko termu veicot redukcijas soli ar kādu ģeneratoru (bāzes elementu). Tas ir iespējams tad un tikai tad, ja jebkura ideāla elementa vecākais terms dalās ar kāda ģeneratora vecāko termu.

Šādā gadījumā jebkuru ideāla elementu varētu garantēti noreducēt līdz 0.

$I \subseteq k[X_1, ..., X_n]$ - ideāls.

$\mathcal{G} = \{g_1, ..., g_m\} \subseteq I$ sauc par *I Grobnera bāzi (GB)* $\mathcal{G}(I)$, ja

- $\mathcal{G} \subseteq I$,
- $\forall\ j: \ g_j \neq 0$,

- $f \in I,\ f \neq 0 \implies \exists\ i : \mathcal{H}(g_i) | \mathcal{H}(f)$ - f vecāko termu var samazināt ar vismaz vienu redukcijas soli izmantojot kādu $\mathcal{G}$ elementu.

2.3. piemērs. $I = \langle X, Y \rangle$. $\{X, Y\}$ ir GB.

$I = \langle XY+1, Y^2-1 \rangle$. $\{XY+1, Y^2-1\}$ nav I GB. $f = -X-Y \in I$ vecākais loceklis $\mathcal{H}(f) = -X$ nedalās ne ar $\mathcal{H}(XY+1) = XY$, ne $\mathcal{H}(Y^2-1) = Y^2$. Citiem vārdiem sakot, $-X-Y$ nav iespējams noreducēt līdz 0 izmantojot doto ģeneratoru kopu.

2.5. piezīme. GB ģeometriskā interpretācija: I elementu vecāko termu kopa $\mathcal{M}$, tās "stūri".

2.3. Pamatīpašības

Pierādīsim, ka Grobnera bāzes atrisina visas ideālu problēmas, kas tika minētas agrāk.

2.1. teorēma. $I \subseteq k[X_1, ..., X_n]$ - ideāls.

1. $\mathcal{G}(I) = \{g_1, ..., g_m\}$ ir I ģeneratoru kopa:
$$I = \langle g_1, ..., g_m \rangle.$$
2. $\forall\ f \in k[X_1, ..., X_n]$ redukcija mod $\mathcal{G}(I)$ $\overline{f}^{\mathcal{G}(I)}$ nav atkarīga no redukcijas soļu kārtības.
3. $f \in I \iff \overline{f}^{\mathcal{G}(I)} = 0.$

PIERĀDĪJUMS

1. $f \in I \implies \exists \gamma_1 \in \mathcal{G}(I)$ tāds, ka $\mathcal{H}(\gamma_1)|\mathcal{H}(f)$, tāpēc
$$f_1 = f - \frac{\mathcal{H}(f)}{\mathcal{H}(\gamma_1)}\gamma_1 = f - h_1\gamma_1 \in I.$$

Redzam, ka $\mathcal{H}(f_1) \prec \mathcal{H}(f)$.

$f_1 \in I \implies \exists\ \gamma_2 \in \mathcal{G}(I)$ tāds, ka $\mathcal{H}(\gamma_2)|\mathcal{H}(f_1)$. Definēsim
$$f_2 = f_1 - \frac{\mathcal{H}(f_1)}{\mathcal{H}(\gamma_2)}\gamma_2 = f_1 - h_2\gamma_2 = f - h_1\gamma_1 - h_2\gamma_2 \in I.$$

Redzam, ka $\mathcal{H}(f_2) \prec \mathcal{H}(f_1) \prec \mathcal{H}(f)$.

Turpinot šo procesu, pēc galīga skaita redukcijas soļu iegūsim $f_l = 0$, jo polinomiem f_i ar katru redukcijas soli vecākie termi kļūst leksikogrāfiski stingri mazāki, un šāda polinomu virkne ir galīga.

$$\Longrightarrow \quad f_l = f - \sum_{i=1}^{l} h_i \gamma_i = 0 \quad \Longrightarrow \quad f = \sum_{i=1}^{l} h_i \gamma_i .$$

$\Longrightarrow$ patvaļīgs $f \in I$ ir izsakāms kā $\mathcal{G}(I)$ elementu γ_1, γ_2,..., γ_l lineāra kombinācija ar koeficientiem no $k[X_1, ..., X_n]$.

2. Pieņemsim, ka f var reducēt divos veidos:

$$\begin{cases} f = a_1 g_1 + ... + a_m g_m + r, \\ f = b_1 g_1 + ... + b_m g_m + \hat{r}. \end{cases} \Longrightarrow$$

$$r - \hat{r} = (b_1 - a_1) g_1 + ... + (b_m - a_m) g_m \in I.$$

$$\begin{cases} r - \hat{r} \neq 0 \\ \mathcal{G}(I) \text{ ir } GB \end{cases} \Longrightarrow \exists\, i : \ \mathcal{H}(g_i) | \mathcal{H}(r - \hat{r}) \Longrightarrow$$

vismaz viens no r vai $\hat{r}$ termiem dalās ar $\mathcal{H}(g_i)$. Tas ir pretrunā ar redukcijas algoritmu, jo to varētu turpināt attiecībā uz r vai $\hat{r}$.

3. $\overline{f}^{\mathcal{G}(I)} = 0 \implies f = a_1 g_1 + ... + a_m g_m \implies f \in I.$

Otrādi, pieņemsim, ka redukcijas algoritma rezultātā ir iegūta vienādība

$$f = a_1 g_1 + ... + a_m g_m + r.$$

$$f \in I \implies r = \underbrace{f}_{\in I} - \underbrace{a_1 g_1 - .. - a_m g_m}_{\in I} \in I.$$

$$\begin{cases} r \in I \\ r \neq 0 \end{cases} \implies \exists\ g_i : \mathcal{H}(g_i) | \mathcal{H}(r).$$

Tas ir pretrunā ar redukcijas algoritmu, jo to varētu turpināt attiecībā uz r. ■

3. 8.mājasdarbs

3.1. Obligātie uzdevumi

8.1 Atrast f redukciju mod g, ja

(a) $f = X^3 + XY^2 + Y^3$, $g = X - Y$, virs $\mathbb{Q}$, $X \succ Y$,

(b) $f = X^6 + X^2Y^2Z^2 + Y^4Z^2$, $g = XYZ + 1$, virs $\mathbb{F}_2$, $X \succ Y \succ Z$.

8.2 Atrast vismaz vienu f redukciju mod (g_1, g_2), ja

(a) $f = X^3 + XY^2 + Y^3$, $g_1 = X + Y$, $g_2 = Y + 1$, virs $\mathbb{Q}$, $X \succ Y$,

(b) $f = X^3 + Y^3 + Z^3$, $g_1 = X + Y + Z$, $g_2 = Y + Z$, virs $\mathbb{F}_2$, $X \succ Y \succ Z$.

8.3 Dots $I = \langle f \rangle \in k[X_1, ..., X_n]$. Pierādīt, ka $\{f\}$ ir $\mathcal{G}(I)$.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

8.4 Dots ideāls $I \subseteq k[X_1, ..., X_n]$ un $\mathcal{G}(I)$ $\mathcal{F}$. Pierādīt, ka redukcija mod $\mathcal{F}$ ir gredzenu homomorfisms

$$\pi_I : k[X_1, ..., X_n] \to k[X_1, ..., X_n]/I :$$

(a) $\overline{f}^{\mathcal{F}} = \overline{g}^{\mathcal{F}} \iff f \equiv g (\text{mod } I)$;

(b) $\overline{f+g}^{\mathcal{F}} = \overline{f}^{\mathcal{F}} + \overline{g}^{\mathcal{F}}$;

(c) $\overline{fg}^{\mathcal{F}} = \overline{\overline{f}^{\mathcal{F}} \overline{g}^{\mathcal{F}}}^{\mathcal{F}}$