*DAUGAVPILS UNIVERSITĀTE*
*Dabaszinātņu un matemātikas fakultāte*
*Matemātikas katedra*
*Bakalaura studiju programma “Matemātika”*

*Studiju kurss*

# Polinomu algebra

## 11.lekcija

*Docētājs: Dr. P. Daugulis*

*2008./2009.studiju gads*

# Saturs

**1. Grobnera bāzu pielietojumi** **5**
1.1. Polinomiālo vienādojumu sistēmu risināšana . . . . . . 5
1.1.1. Polinomiālo vienādojumu sistēmas seku ideāls . 5
1.1.2. Izslēgšanas ideāli . . . . . . . . . . . . . . . . . 6
1.1.3. Polinomiālas vienādojumu sistēmas risināšanas algoritms . . . . . . . . . . . . . . . . . . . . 8
1.2. Parametriskā pieraksta pārveidošana vispārīgajā (implicitizācija) . . . . . . . . . . . . . . . . . . . . . 10
1.2.1. Implicitizācijas problēma . . . . . . . . . . . . 10
1.2.2. Polinomiālās implicitizācijas algoritms . . . . . 11
1.2.3. Racionālās implicitizācijas algoritms . . . . . . 13

**2. Grobnera bāzu teorijas darbietilpīgie pierādījumi - patstāvīgā lasīšana** **16**
2.1. Diksona lemma . . . . . . . . . . . . . . . . . . . . 16
2.2. Buhbergera kritērijs . . . . . . . . . . . . . . . . . 18
2.2.1. Palīgrezultāti . . . . . . . . . . . . . . . . . . . 18

2.2.2. Kritērijs . . . . . . . . . . . . . . . . . . . . . . 24
2.3. Buhbergera algoritma pareizība . . . . . . . . . . . . . . . 31
2.4. Reducētās Grobnera bāzes vienīgums . . . . . . . . . . 32

**3. 11.mājasdarbs 35**
3.1. Obligātie uzdevumi . . . . . . . . . . . . . . . . . . . . 35
3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi 37

**Lekcijas mērķis:**

- apgūt polinomiālu vienādojumu sistēmu risināšanas algoritmu, kas izmanto Grobnera bāzes;
- ieskatīties Grobnera bāzu teorijas svarīgākajos pierādījumos.

**Lekcijas kopsavilkums:**

- polinomiālai vienādojumu sistēmai var definēt ideālu, kura Grobnera bāze sniedz būtisku informāciju par tās atrisinājumiem un iespējām izslēgt nezināmos;
- polinomiālu vienādojumu sistēmu risināšanu var izmantot, lai pārietu no līknes/virsmas parametriskā pierakstu uz vispārīgo;
- Grobnera bāzu teorijas pierādījumi ir grūti, it sevišķi Buhbergera kritērijs, var mēģināt sākt tā apgūšana ar divu ģeneratoru speciālgadījumu.

# 1. Grobnera bāzu pielietojumi

## 1.1. Polinomiālo vienādojumu sistēmu risināšana

### 1.1.1. Polinomiālo vienādojumu sistēmas seku ideāls

Pieņemsim, ka ir dota polinomiālu vienādojumu sistēma (PVS)

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

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

$$h_1 g_1 + h_2 g_2 + ... + h_m g_m = 0, \text{ kur } h_i \in k[X_1, ..., X_n].$$

Seku vienādojumu kreisās puses interpretēsim kā ideāla elementus.

Ideālu $I = \langle g_1, g_2, ..., g_m \rangle$ sauc par PVS *seku ideālu*.

Ideālam $I$ var atrast $RGB$. Izrādās, ka $RGB$ elementiem atbilstošos vienādojumus ir ērtāk risināt nekā sākotnējos vienādojumus.

Vienkāršākais $GB$ pielietojums PVS risināšanā: $1 \in \mathcal{G}(I) \implies 1 = 0 \implies$ PVS nav atrisinājumu.

### 1.1.2. Izslēgšanas ideāli

Viena no vēlmēm PVS risināšanā ir iegūt seku vienādojumus, kas ir atkarīgi no pēc iespējas mazākas nezināmo kopas - *izslēgt nezināmos*.

Par *$j$-to izslēgšanas ideālu* $I_j$ $(1 \leq j < n)$ sauc kopu

$$I \cap k[X_{j+1}, ..., X_n].$$

Redzam, ka $I_j$ elementi nav atkarīgi no nezināmajiem $X_1, ..., X_j$.

**1.1. teorēma.**

1. $\forall\, j\ I_j$ ir ideāls gredzenā $k[X_{j+1}, ..., X_n]$.
2. $\mathcal{F} = \mathcal{G}(I) \implies \mathcal{F} \cap k[X_{j+1}, ..., X_n] = \mathcal{G}(I_j)$.

PIERĀDĪJUMS

1. $f, f' \in I_j \implies f + f' \in I_j$.

$f \in I_j \wedge r \in k[X_{j+1}, ..., X_n] \implies rf \in I \wedge rf \in k[X_{j+1}, ..., X_n] \implies rf \in \underbrace{I \cap k[X_{j+1}, ..., X_n]}_{=I_j}$.

2. $f \in I_j \implies \exists\, g_l \in \mathcal{F} :\ \mathcal{H}(g_l) | \mathcal{H}(f)$.

$\mathcal{H}(g_l)$ nedalās ar $X_1, ..., X_j \implies$ neviens $g_l$ loceklis nedalās ar $X_1, ..., X_j$, jo tie visi ir mazāki nekā $\mathcal{H}(g_l)$.

Seko, ka $g_l \in \mathcal{F} \cap k[X_{j+1}, ..., X_n]$.

$\forall\ f \in I_j\ \exists\ g_l \in \mathcal{F} \cap k[X_{l+1}, ..., X_n]$ tāds, ka $\mathcal{H}(g_l)|\mathcal{H}(f) \Longrightarrow \mathcal{F} \cap k[X_{j+1}, ..., X_n] = \mathcal{G}(I_j)$. ■

**1.1. piezīme.** No teorēmas seko, ka $GB$ var saturēt elementus, kas saista tikai dažus argumentus: ja eksistē sakarības, kas saista nezināmos $X_{j+1}, ..., X_n$, tad $I_j \neq \{0\}$, un šādas sakarības noteikti parādīsies kā $GB$ elementi. Risinot PVS var būt nepieciešams mainīt argumentu kārtību - *izslēgšanas kārtību.*

### 1.1.3. Polinomiālas vienādojumu sistēmas risināšanas algoritms

Virkni $(a_l, a_{l+1}, ..., a_n) \in k^{n-l+1}$ sauksim par PVS ar $n$ nezināmajiem **P** *daļēju atrisinājumu*, ja $\exists\ (a_1, ..., a_{l-1}) : (a_1, ..., a_{l-1}, a_l, ..., a_n)$ ir **P** atrisinājums.

PVS risināšanai var izmantot šādu algoritmu:

1. Atrast seku ideāla $I$ $RGB$.

2. Risināt PVS sākot no vienādojumiem ar mazāku nezināmo skaitu: atrast daļējos atrisinājumus un mēģināt tos paplašināt līdz pilnajiem atrisinājumiem.

**1.2. piezīme.** Daļējo atrisinājumu paplašināšana ne vienmēr ir iespējama.

**1.1. piemērs.** Sistēmai

$$\begin{cases} X^2 + Y^2 + Z^2 = 1 \\ X^2 + Z^2 = Y \\ X = Z \end{cases}$$

seku ideāls ir $I = \langle X^2 + Y^2 + Z^2 - 1, X^2 + Z^2 - Y, X - Z \rangle$. Tā GB ir

$$\{X - Z, Y - 2Z^2, Z^4 + \frac{1}{2}Z^2 - \frac{1}{4}\}.$$

No sākuma atrodam $Z$, tad $Y$ un beigās $X$. Bet tā ir neveiksmīga kārtība. Labāk izvēlēties kārtību $X \succ Z \succ Y$.

Sistēmai

$$\begin{cases} X^3 - X - Y^2 = 0 \\ X^2 - Y^3 = 0 \end{cases}$$

seku ideāls ir $I = \langle X^3 - X - Y^2, X^2 - Y^3 \rangle$. Tā RGB ir

$$\{X + Y^2 + Y^4 - Y^7, Y^9 - 2Y^6 - Y^4 + Y^3\}.$$

No sākuma atrodam $Y$, tad $X$. Mainot argumentu kārtību, iegūsim vienādojumu attiecībā uz $X$ ar $\deg = 8$.

## 1.2. Parametriskā pieraksta pārveidošana vispārīgajā (implicitizācija)

### 1.2.1. Implicitizācijas problēma

Pieņemsim, ka Dekarta telpas $\mathbb{R}^n$ apakškopa ir uzdota parametriski ar sistēmu

$$\begin{cases} X_1 = \varphi_1(t_1, ..., t_m) \\ ... \\ X_n = \varphi_n(t_1, ..., t_m). \end{cases}$$

Var uzdot šādu jautājumus:

- vai koordinātes $X_1, ..., X_n$ ir saistītas ar polinomiālām sakarībām,
- kā atrast šādas sakarības.

**1.2. piemērs.** Ja

$$\begin{cases} X = X_0 + pt \\ Y = Y_0 + qt \\ Z = Z_0 + rt, \end{cases}$$

tad koordinātes saista divu lineāru vienādojumu sistēma

$$\begin{cases} \frac{X-X_0}{p} = \frac{Y-Y_0}{q} \\ \frac{X-X_0}{p} = \frac{Z-Z_0}{r} \end{cases}$$

### 1.2.2. Polinomiālās implicitizācijas algoritms

Ja funkcijas $\varphi_i$ ir polinomi, tad implicitizācijas problēmu var saistīt ar atbilstošu PVS risināšanu un nezināmo $t_1, ..., t_m$ izslēgšanu.

Izmantojot Grobnera bāzes implicitizācijas problēmu polinomiālu funkciju gadījumā var risināt saskaņā ar šādu algoritmu:

1. Definēt *implicitizācijas ideālu*
$$I = \langle f_1, ..., f_n \rangle \subseteq k[t_1, ..., t_m, X_1, ..., X_n],$$
kur $f_i = X_i - \varphi_i(t_1, ..., t_m)$.
2. Atrast $\mathcal{G}(I)$ ar leksikogrāfisko sakārtojumu, kas atbilst argumentu kārtībai $\underbrace{t_1 \succ t_2 \succ ...t_m}_{\text{parametri}} \underbrace{\succ X_1 \succ ...X_n}_{\text{koordinātes}}$.
3. Ja $\mathcal{G}(I)$ satur elementus, kas nesatur $t_1, ..., t_m$, tad ir iegūtas sakarības starp $X_1, ..., X_n$.

**1.3. piemērs.** Pieņemsim, ka telpā $\mathbb{R}^3$ līkne ir uzdota parametriski ar sistēmu
$$\begin{cases} X = t^4 \\ Y = t^3 \\ Z = t^2 \end{cases}$$

Šajā gadījumā implicitizācijas ideāls ir $I = \langle t^4 - X, t^3 - Y, t^2 - Z \rangle$.

Tā RGB ir $\mathcal{F} = \{t^2 - Z, tY - Z^2, tZ - Y, X - Z^2, Y^2 - Z^3\}$.

Redzam, ka līknes punkti apmierina divas sakarības

$$X - Z^2 = 0,$$
$$Y^2 - Z^3 = 0.$$

### 1.2.3. Racionālās implicitizācijas algoritms

Implicitizācijas problēmu var risināt ar Grobnera bāzu palīdzību arī gadījumā, kad funkcijas $\varphi_i$ ir racionālas funkcijas:

$$X_i = \varphi_i(t_1, ..., t_m) = \frac{P_i(t_1, ..., t_m)}{Q_i(t_1, ..., t_m)}.$$

Realizēsim šādu algoritmu:

1. Definēt *implicitizācijas ideālu*

$$I = \langle f_1, ..., f_n, \widehat{f} \rangle \subseteq k[Y, t_1, ..., t_m, X_1, ..., X_n],$$

kur

$$f_i = X_i Q_i - P_i, \widehat{f} = 1 - (Q_1 ... Q_n)Y.$$

2. Atrast $\mathcal{G}(I)$ ar leksikogrāfisko sakārtojumu, kas atbilst argumentu kārtībai $Y \succ \underbrace{t_1 \succ t_2 \succ ...t_m}_{\text{parametri}} \succ \underbrace{X_1 \succ ...X_n}_{\text{koordinātes}}$.

3. Ja $\mathcal{G}(I)$ satur elementus, kas nesatur $t_1, ..., t_m$, tad ir iegūtas sakarības starp $X_1, ..., X_n$.

**1.3. piezīme.** Ģenerators $\widehat{f} = 1 - (Q_1 ... Q_n)Y$ ir vajadzīgs, lai saucēji $Q_1, ..., Q_n$ nebūtu vienādi ar 0.

**1.4. piemērs.** Līkne uzdota parametriski ar sistēmu

$$\begin{cases} x = \frac{2t}{1+t^2} \\ y = \frac{1-t^2}{1+t^2}. \end{cases}$$

Implicitizācijas ideāla

$$I = \langle X(1+t^2) - 2t, Y(1+t^2) - (1-t^2), 1 - (1+t^2)g \rangle$$

GB satur ģeneratoru $X^2 + Y^2 - 1$.

# 2. Grobnera bāzu teorijas darbietilpīgie pierādījumi - patstāvīgā lasīšana

## 2.1. Diksona lemma

**2.1. teorēma.** (*Diksona lemma*) Katrai kopai $\mathcal{M} \subseteq \mathbb{N}^{*n}$ eksistē galīga apakškopa $\{\mu_1, ..., \mu_k\} \subseteq \mathcal{M}$ tāda, ka

$$\mathcal{M} \subseteq S(\mu_1) \cup ... \cup S(\mu_k).$$

(katru kopu $\mathcal{M} \subseteq \mathbb{N}^{*n}$ var pārklāt ar tās galīgas apakškopas $\{\mu_1, ..., \mu_k\}$ elementu ēnām)

PIERĀDĪJUMS Pielietosim matemātiskās indukcijas metodi ar parametru $n$.

Indukcijas bāze $n = 1 \implies \mathcal{M} \subseteq \mathbb{N}^*$. $\exists$ $\mathcal{M}$ minimālais elements $\nu_0$, tādējādi $\mathcal{M} \subseteq S(\nu_0)$.

Indukcijas solis Pieņemsim, ka apgalvojums ir patiess $\forall$ $n < m$ un pierādīsim, ka tad tas ir patiess, ja $n = m$.

Definēsim

$$\pi : \mathbb{N}^{*m} \to \mathbb{N}^{*(m-1)},$$

$$\pi(x_1, ..., x_m) = (x_1, ..., x_{m-1}).$$

Saskaņā ar indukcijas pieņēmumu kopu $\pi(\mathcal{M})$ var nosegt ar tās galīgas apakškopas elementu ēnām: $\exists \{\nu_1, ..., \nu_l\} \subseteq \pi(\mathcal{M})$ tāda, ka

$$\pi(\mathcal{M}) \subseteq S(\nu_1) \cup ... \cup S(\nu_l).$$

$\nu_i \in \pi(\mathcal{M}) \implies \exists \mu_i \in \mathcal{M} : \nu_i = \pi(\mu_i) \implies$

$$\pi(\mathcal{M}) \subseteq S\Big(\pi(\mu_1)\Big) \cup ... \cup S\Big(\pi(\mu_l)\Big).$$

Definēsim

$$\mathcal{M}_u = \{(x_1, ..., x_m) \in \mathcal{M} | x_m = u\},$$

$$\mathcal{M}_{\geq u} = \mathcal{M}_u \cup \mathcal{M}_{u+1} \cup ... = \bigcup_{w \geq u} \mathcal{M}_w.$$

Apzīmēsim ar $N$ $\mu_1, ..., \mu_l$ $m$-tās koordinātes maksimālo vērtību.

Redzam, ka $\mathcal{M} = \mathcal{M}_1 \cup ... \cup \mathcal{M}_{N-1} \cup \mathcal{M}_{\geq N}$.

Pierādīsim, ka $\forall\ \mathcal{M}_i$ un $\mathcal{M}_{\geq N}$ var nosegt ar galīgas kopas ēnām:

- $\forall i$ kopai $\mathcal{M}_i$ $m$-tā koordināte ir fiksēta, tāpēc $\mathcal{M}_i$ var identificēt ar $\mathbb{N}^{*(m-1)}$ apakškopu, saskaņā ar indukcijas pieņēmumu seko, ka $\mathcal{M}_i$ var noklāt ar galīgas apakškopas elementu ēnām,
- $\mathcal{M}_{\geq N} \subseteq S(\mu_1) \cup ... \cup S(\mu_l)$.

Apvienojot visus elementus, kuru ēnas nosedz $\mathcal{M}_i$ un $\mathcal{M}_{\geq N}$ iegūsim meklējamo galīgo nosedzošo kopu. ■

## 2.2. Buhbergera kritērijs

### 2.2.1. Palīgrezultāti

Zemāk apzīmēsim multideg$(f)$ ar mdeg$(f)$.

**2.2. teorēma.** (redukcijas īpašība) Dots, ka $\mathcal{G} = \{g_1, ..., g_m\}$.

$$\left(\overline{f}^{\mathcal{G}} = 0\right) \implies \left(f = \sum_{i=1}^{m} h_i g_i,\ \text{kur mdeg}(h_i g_i) \leq \text{mdeg}(f)\right).$$

PIERĀDĪJUMS Veiksim redukcijas soļu virkni sākot ar $f$, kuras rezultātā rodas 0. Iegūsim vienādību

$$f = \sum_{i=1}^{m} h_i g_i,$$

kur $h_i$ ir dalījumi, katrs redukcijas solis ar $g_j$ pievieno vienu termu pie $h_j$.

Pirmā redukcija, kas samazina vecāko termu, pievienos dalījumam $h_j$ termu $\tilde{h} g_j$, kuram $\mathrm{mdeg}(\tilde{h} g_j) = \mathrm{mdeg}(f)$. Visiem pārējiem termiem mdeg<mdeg($f$). ■

**2.3. teorēma.** ($S$-polinomu īpašības) Dots, ka

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

1. $\mathrm{mdeg}\Big(S(f,g)\Big) < \mathrm{mdeg}\Big(MKD(X^{\alpha}, X^{\beta})\Big)$.
2. $S(f,g) = -S(g,f)$.
3. $\alpha = \beta \implies S(f,g) = \frac{1}{a} f - \frac{1}{b} g$.

4. $S(X^{\mu} f, X^{\lambda} g) = X^{\nu} S(f,g)$, kur

$$X^{\nu} = \frac{MKD(X^{\mu}X^{\alpha}, X^{\lambda}X^{\beta})}{MKD(X^{\alpha}, X^{\beta})}.$$

PIERĀDĪJUMS

1. $S$-polinomā

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

locekļu $\frac{X^{\gamma}}{\mathcal{H}(f)} \cdot f$ un $\frac{X^{\gamma}}{\mathcal{H}(g)}$ vecākie termi ir vienādi ar $X^{\gamma}$ un saīsinās. Pāri var palikt tikai leksikogrāfiski mazāki termi.

2. Seko no $S$-polinoma definīcijas.

3. $\alpha = \beta \implies \gamma = \alpha = \beta \implies$

$$S(f,g) = \frac{X^{\alpha}}{aX^{\alpha}} f - \frac{X^{\alpha}}{bX^{\alpha}} g = \frac{1}{a} f - \frac{1}{b} g.$$

4. Ievērosim, ka $\mathcal{H}(X^\mu f) = aX^{\mu+\alpha}$ un $\mathcal{H}(X^\lambda g) = bX^{\lambda+\beta}$. Apzīmēsim $MKD(X^{\mu+\alpha}, X^{\lambda+\beta})$ ar $X^\omega$. Redzam, ka

$$S(X^\mu f, X^\lambda g) = \frac{MKD(X^{\mu+\alpha}, X^{\lambda+\beta})}{aX^{\mu+\alpha}}(X^\mu f) - \frac{MKD(X^{\mu+\alpha}, X^{\lambda+\beta})}{bX^{\lambda+\beta}}(X^\lambda g) = \frac{X^\omega}{aX^\alpha} f - \frac{X^\omega}{bX^\beta} g =$$
$$\frac{X^\omega}{X^\gamma}\left(\frac{X^\gamma}{aX^\alpha} f - \frac{X^\gamma}{bX^\beta} g\right) = \frac{X^\omega}{X^\gamma} S(f,g) = X^{\omega-\gamma} S(f,g) = X^\nu S(f,g). \blacksquare$$

**2.4. teorēma.** Dots, ka $\{f_1, f_2\} \subseteq k[X_1, ..., X_n]$. Ir spēkā $f_1$ un $f_2$ vecāko monomu vienādība:

$$\mathrm{mdeg}(f_1) = \mathrm{mdeg}(f_2) = \delta.$$

(Citiem vārdiem sakot, $\mathcal{H}(f_1) \asymp \mathcal{H}(f_2)$). Definēsim $f = c_1 f_1 + c_2 f_2$, kur $c_i \in k$. Tad

$$\Big(\mathrm{mdeg}(f) < \delta\Big) \implies \Big(\exists\, d \in k : f = d \cdot S(f_1, f_2)\Big).$$

PIERĀDĪJUMS

Pieņemsim, ka $\mathcal{H}(f_i) = a_i X^\mu$. Tā kā $\mathcal{H}(f) \prec \mathcal{H}(a_i X^\mu)$, tad $c_1 f_1 + c_2 f_2$ vecākie termi saīsinās $\Longrightarrow$ $c_1 a_1 + c_2 a_2 = 0$ $\Longrightarrow$

$$c_1 f_1 + c_2 f_2 = c_1 a_1 \frac{f_1}{a_1} + c_2 a_2 \frac{f_2}{a_2} =$$

$$c_1 a_1 \left( \frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) = \underbrace{\alpha_1 a_1}_{=d} S(f_1, f_2). \blacksquare$$

**2.5. teorēma.** Dots, ka $\{f_1, ..., f_m\} \subseteq k[X_1, ..., X_n]$:

$$\mathrm{mdeg}(f_1) = ... = \mathrm{mdeg}(f_m) = \delta.$$

Definēsim $f = \sum_1^m c_i f_i$, kur $c_i \in k$. Tad

$$\Big( \mathrm{mdeg}(f) < \delta \Big) \implies \Big( \exists\, d_{ij} \in k : f = \sum_{i,j} d_{ij} S(f_i, f_j) \Big).$$

PIERĀDĪJUMS

Pieņemsim, ka $\mathcal{H}(f_i) = a_i X^\mu$. Tā kā $\mathcal{H}(f) \prec \mathcal{H}(a_i X^\mu)$, tad lineārās kombinācijas $\sum_{i=1}^m c_i f_i$ vecākie termi saīsinās $\Longrightarrow$

$$c_1 a_1 + ... + c_m a_m = \sum_{i=1}^m c_i a_i = 0 \Longrightarrow$$

$$c_1 f_1 + ... + c_m f_m = c_1 a_1 \frac{f_1}{a_1} + ... + c_m a_m \frac{f_m}{a_m} =$$

$$c_1 a_1 \frac{f_1}{a_1} - c_1 a_1 \frac{f_2}{a_2} + c_1 a_1 \frac{f_2}{a_2} + c_2 a_2 \frac{f_2}{a_2} + ... + c_m a_m \frac{f_m}{a_m} =$$

$$c_1 a_1 \left( \frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) + (c_1 a_1 + c_2 a_2) \frac{f_2}{a_2} + ... + c_m a_m \frac{f_m}{a_m} =$$

$$c_1 a_1 S(f_1, f_2) + \underbrace{(c_1 a_1 + c_2 a_2) \frac{f_2}{a_2} + ... + c_m c_m \frac{f_m}{a_m}}_{\text{atkārtojam triku}} =$$

$$c_1a_1S(f_1,f_2)+(c_1a_1+c_2a_2)S(f_2,f_3)+\ldots+\left(\sum_{j=1}^{m-1}c_ja_j\right)S(f_{m-1},f_m)+$$

$$\underbrace{\left(\sum_{j=1}^{m}c_ja_j\right)}_{=0}\frac{f_m}{a_m}=\sum_{i,j}d_{ij}S(f_i,f_j).\blacksquare$$

### 2.2.2. Kritērijs

**2.6. teorēma.** (divu ģeneratoru gadījums) Kopa $\mathcal{G}=\{g_1,g_2\}$ ir ideāla $I=\langle g_1,g_2\rangle$ $GB$ $\iff$ $\overline{S(g_1,g_2)}^{\mathcal{G}}=0$.

PIERĀDĪJUMS

$\underline{\Longrightarrow}$

$S(g_1,g_2)\in I\ \wedge\ \mathcal{G}$ ir GB $\Longrightarrow$ $\overline{S(g_1,g_2)}^{\mathcal{G}}=0$.

$\underline{\Longleftarrow}$

Dots, ka $\overline{S(g_1,g_2)}^{\mathcal{G}}=0$. Jāpierāda, ka $\forall\ f\in I$ izpildās $\overline{f}^{\mathcal{G}}=0$.

Pieņemsim, ka $f = h_1 g_2 + h_2 g_2$. Definēsim $\delta = \max_i(\mathrm{mdeg}(h_i g_i))$.

Izvēlēsimies tādus $h_i$, lai $\delta$ ir minimāli iespējamais. Redzam, ka $\mathrm{mdeg}(f) \leq \delta$. Pierādīsim, ka $\mathrm{mdeg}(f) = \delta$.

Pieņemsim pretējo: $\mathrm{mdeg}(f) < \delta$. Ir iespējami divi gadījumi:

1. tikai vienam no polinomiem $h_1 g_1$ un $h_2 g_2$ mdeg$= \delta$, vecāko termu saīsināšanās labajā pusē nenotiek, tāpēc $\mathrm{mdeg}(f) = \delta$ - pretruna;
2. abiem polinomiem $h_1 g_1$ un $h_2 g_2$ mdeg$= \delta$, labajā pusē notiek vecāko termu saīsināšanās, apskatīsim šo gadījumu zemāk.

Sadalīsim saskaitāmos $f$ izvirzījumā šādā veidā:

$$f = h_1 g_1 + h_2 g_2 = \mathcal{H}(h_1) g_1 + \mathcal{H}(h_2) g_2 + \underbrace{\Big(h_1 - \mathcal{H}(h_1)\Big) g_1 + \Big(h_1 - \mathcal{H}(h_1)\Big) g_1}_{\mathrm{mdeg} < \delta}.$$

$$\mathrm{mdeg}(f) < \delta \implies \mathrm{mdeg}\Big(\mathcal{H}(h_1)g_1 + \mathcal{H}(h_2)g_2\Big) < \delta.$$

Apzīmēsim $\mathcal{H}(h_i) = a_i X^{\mu_i}$. Saskaņā ar palīgteorēmām

$$\mathcal{H}(h_1)g_1 + \mathcal{H}(h_2)g_2 = d \cdot S(X^{\mu_1}g_1, X^{\mu_2}g_2) = dX^{\delta-\gamma}S(g_1, g_2),$$

kur $X^\gamma = MKD(\mathcal{H}(g_1), \mathcal{H}(g_2))$.

$\overline{S(g_1, g_2)}^{\mathcal{G}} = 0 \implies S(g_1, g_2) = t_1 g_1 + t_2 g_2$, kur $\mathrm{mdeg}(t_i g_i) \leq \mathrm{mdeg}(S(g_1, g_2))$ saskaņā ar redukcijas īpašību.

Seko, ka $X^{\delta-\gamma}S(g_1, g_2) = X^{\delta-\gamma}t_1 g_1 + X^{\delta-\gamma}t_2 g_2$.

Ievērosim, ka $\mathrm{mdeg}(S(g_1, g_2)) < \gamma \implies$

$$\mathrm{mdeg}(X^{\delta-\gamma}t_i g_i) \leq \mathrm{mdeg}(X^{\delta-\gamma}S(g_1, g_2)) < \delta.$$

Seko, ka

$$\mathcal{H}(h_1)g_1 + \mathcal{H}(h_2)g_2 = dX^{\delta-\gamma}S(g_1, g_2) = d(\underbrace{X^{\delta-\gamma}t_1g_1}_{\text{mdeg}<\delta} + \underbrace{X^{\delta-\gamma}t_2g_2}_{\text{mdeg}<\delta}).$$

Ir iegūta pretruna - $f = h_1g_1 + h_2g_2$ var izteikt formā

$$f = d(\underbrace{X^{\delta-\gamma}t_1g_1}_{\text{mdeg}<\delta} + \underbrace{X^{\delta-\gamma}t_2g_2}_{\text{mdeg}<\delta}) + \underbrace{\Big(h_1 - \mathcal{H}(h_1)\Big)g_1 + \Big(h_1 - \mathcal{H}(h_1)\Big)g_1}_{\text{mdeg}<\delta},$$

kur katram loceklim labajā pusē mdeg$<\delta$, bet $\delta$ pēc pieņēmuma ir mazākā iespējamā maksimālā multipakāpe. ■

**2.7. teorēma.** (vispārīgais gadījums) Kopa $\mathcal{G} = \{g_1, ..., g_m\}$ ir ideāla $I = \langle g_1, ..., g_m\rangle$ $GB$ $\Longleftrightarrow$

$$\overline{S(g_i, g_j)}^{\mathcal{G}} = 0, \forall \text{ pāriem } i \neq j.$$

PIERĀDĪJUMS

$\underline{\Longrightarrow}$ Tā kā $S(g_i, g_j) \in I$ un $\mathcal{G}$ ir GB, tad $\overline{S(g_i, g_j)}^{\mathcal{G}} = 0$.

$\Longleftarrow$ Dots, ka $\overline{S(g_i, g_j)}^{\mathcal{G}} = 0$. Jāpierāda, ka $\forall\, f \in I$ izpildās $\overline{f}^{\mathcal{G}} = 0$.

Pieņemsim, ka $f = \sum_{i=1}^{m} h_i g_i$. Definēsim $\delta = \max_i(\mathrm{mdeg}(h_i g_i))$. Izvēlēsimies tādus $h_i$, lai $\delta$ ir minimāli iespējamais. Redzam, ka $\mathrm{mdeg}(f) \le \delta$. Pierādīsim, ka $\mathrm{mdeg}(f) = \delta$.

Pieņemsim pretējo: $\mathrm{mdeg}(f) < \delta$. Sadalīsim saskaitāmos $f$ izvirzījumā šādā veidā:

$$f = \sum_{i:\ \mathrm{mdeg}(h_i g_i)=\delta} h_i g_i + \sum_{i:\ \mathrm{mdeg}(h_i g_i)<\delta} h_i g_i =$$

$$\sum_{\mathrm{mdeg}(h_i g_i)=\delta} \mathcal{H}(h_i) g_i + \sum_{\mathrm{mdeg}(h_i g_i)=\delta} \Big(h_i - \mathcal{H}(h_i)\Big) g_i + \sum_{\mathrm{mdeg}(h_i g_i)<\delta} h_i g_i.$$

Summām

$$\sum_{\mathrm{mdeg}(h_i g_i)=\delta} \Big(h_i - \mathcal{H}(h_i)\Big) g_i \text{ un } \sum_{\mathrm{mdeg}(h_i g_i)<\delta} h_i g_i$$

multipakāpe ir stingri mazāka nekā $\delta$. Seko, ka arī

$$\mathrm{mdeg}\Big(\sum_{\mathrm{mdeg}(h_i g_i)=\delta} \mathcal{H}(h_i)g_i\Big) < \delta.$$

Apzīmēsim $\mathcal{H}(h_i) = \alpha_i X^{\mu_i}$. Saskaņā ar palīgteorēmām

$$\sum_{\mathrm{mdeg}(h_i g_i)=\delta} \mathcal{H}(h_i)g_i = \sum_{j,l} d_{jl} S(X^{\mu_j} g_j, X^{\mu_l} g_l) = \sum_{j,l} d_{jl} X^{\delta-\gamma_{jl}} S(g_j, g_l),$$

kur $X^{\gamma_{jl}} = MKD(\mathcal{H}(g_j), \mathcal{H}(g_l))$.

$\overline{S(g_j, g_l)}^{\mathcal{G}} = 0 \implies S(g_j, g_l) = \sum_{u=1}^{m} t_{jlu} g_u$, kur $\mathrm{mdeg}(t_{jlu} g_u) \leq \mathrm{mdeg}(S(g_j, g_l))$ saskaņā ar redukcijas īpašību.

Seko, ka $X^{\delta-\gamma_{jl}} S(g_j, g_l) = X^{\delta-\gamma_{jl}} \sum_{u=1}^{m} t_{jlu} g_u$.

Ievērosim, ka $\mathrm{mdeg}(S(g_j, g_l)) < \gamma_{jl} \implies$

$$\mathrm{mdeg}(X^{\delta-\gamma_{jl}} t_{jlu} g_u) \leq \mathrm{mdeg}(X^{\delta-\gamma_{jl}} S(g_j, g_l)) < \delta.$$

Seko, ka

$$\sum_{\mathrm{mdeg}(h_i g_i)=\delta} \mathcal{H}(h_i) g_i = \sum_{j,l} d_{jl} X^{\delta-\gamma_{jl}} S(g_j, g_l) = \sum_{j,l} d_{jl} X^{\delta-\gamma_{jl}} \sum_{u=1}^{m} t_{jlu} g_u,$$

kur $\forall j, l, u$ $\mathrm{mdeg}(X^{\delta-\gamma_{jl}} t_{jlu} g_u) < \delta$.

Ir iegūta pretruna - $f = \sum_{i=1}^{m} h_i g_i$ var izteikt formā

$$f = \underbrace{\sum_{j,l} d_{jl} X^{\delta-\gamma_{jl}} \sum_{u=1}^{m} t_{jlu} g_u}_{\mathrm{mdeg}<\delta} +$$

$$\underbrace{\sum_{\mathrm{mdeg}(h_i g_i)=\delta} \Big(h_i - \mathcal{H}(h_i)\Big) g_i}_{\mathrm{mdeg}<\delta} + \sum_{\mathrm{mdeg}(h_i g_i)<\delta} h_i g_i.$$

kur katram loceklim labajā pusē mdeg$< \delta$, bet $\delta$ pēc pieņēmuma ir mazākā iespējamā maksimālā multipakāpe. ■

## 2.3. Buhbergera algoritma pareizība

Dots ideāls $I \subseteq k[X_1, ..., X_n]$, $\mathcal{M}_I$ ir $I$ elementu vecāko monomu kopa. Saskaņā ar Diksona lemmu $M_I$ var noklāt ar kādas galīgas apakškopas $\mathcal{S}$ elementu ēnām.

**2.8. teorēma.** Buhbergera algoritms apstājas pēc galīga skaita soļu izpildes un tā rezultāts ir $GB$.

PIERĀDĪJUMS Apzīmēsim Buhberga algoritma gaitā maināmo $I$ ģeneratoru kopu (topošo $GB$) ar $\mathcal{G}$.

Ja algoritms ir apstājies, tad $\forall \{f_i, f_j\} \subseteq \mathcal{G}$ izpildās $\overline{S(f_i, f_j)}^{\mathcal{F}} = 0$, tāpēc saskaņā ar Buhbergera kritēriju ir iegūta GB.

Vecākais loceklis katram polinomam, kas tiek pievienots algoritma rezultātā, nedalās ne ar viena iepriekš pievienota polinoma vecāko locekli, jo tas ir redukcijas rezultāts.

Seko, ka jauna polinoma pievienošana stingri palielina $\mathcal{G}$ vecāko monomu kopas veidoto ēnu.

Pieņemsim, ka $\mathcal{G}$ (un tās ēnas) palielināšana notiek bezgalīgi. Apskatīsim visu ēnu apvienojumu $\widehat{\mathcal{S}}$. Saskaņā ar Diksona lemmu $\widehat{\mathcal{S}}$ var noklāt ar tās galīgas apakškopas $T$ ēnām. Bet katrs no $T$ elementiem tiks pievienots pēc galīga skaita soļiem. Ir iegūta pretruna.■

## 2.4. Reducētās Grobnera bāzes vienīgums

**2.9. teorēma.** *$\forall$ ideālam $I \in k[X_1, ..., X_n]$ $\exists$ viena un tikai viena $RGB$.*

PIERĀDĪJUMS Pieņemsim, ka ideālam $I$ eksistē divas $RGB$

$$\{g_1, ..., g_m\},$$

$$\{h_1, ..., h_l\}.$$

**1.solis $m = l$ un $\mathcal{H}(g_i) = \mathcal{H}(h_i)$ pēc atbilstošas pārkārtošanas.**

$\exists\ i:\ \mathcal{H}(h_i)|\mathcal{H}(g_1)$, pārkārtosim $h$-bāzes elementus tā, lai $i = 1$.

$\exists\ j:\ \mathcal{H}(g_j)|\mathcal{H}(h_1) \implies \mathcal{H}(g_j)|\mathcal{H}(g_1) \implies j = 1$. Redzam, ka

$$\mathcal{H}(g_1) \sim \mathcal{H}(h_1) \implies \mathcal{H}(g_1) = \mathcal{H}(h_1),$$

jo vecāko termu koeficienti $RGB$ ir 1.

Turpinot šo spriedumu iegūsim, ka

$$\mathcal{H}(g_2) = \mathcal{H}(h_2),$$
$$...,$$
$$\mathcal{H}(g_m) = \mathcal{H}(h_m).$$

**2.solis $g_i = h_i$.**

Apskatīsim $g_1 - h_1 \in I$. Neviens no $g_1$, $h_1$ un tāpēc arī $g_1 - h_1$ monomiem nedalās ne ar vienu no $\mathcal{H}(g_i)$, tātad $g_1 - h_1 = 0$.

Turpinot šo spriedumu, iegūsim, ka $g_i - h_i = 0$ visiem $i$.

**3.solis $RGB$ eksistence.**
Pieņemsim, ka ir dota $MGB$ $\{g_1, ..., g_m\}$.

Veiksim savstarpējās redukcijas tik ilgi, kamēr tas ir iespējams. Redukcijas apstāsies pēc galīga skaita soļu izpildes, jo katra redukcija samazina polinomus leksikogrāfiskajā sakārtojumā.

Veiksim otrā veida pārveidojumus, lai koeficienti pie vecākajiem monomiem būtu 1.

Neviena redukcija nemaina polinomu vecākos locekļus, tāpēc rezultātā tiek iegūta $RGB$. ■

# 3. 11.mājasdarbs

## 3.1. Obligātie uzdevumi

11.1 Izmantojot Grobnera bāzes tuvināti atrisināt dotās PVS virs $\mathbb{C}$. Ir atļauts tuvināti atrast viena argumenta polinomu saknes.

(a)

$$\begin{cases} X^4 + X^2 - Y^2 = 0 \\ X^2 - Y^3 = 0 \end{cases}$$

(b)

$$\begin{cases} X + Y + Z = 0 \\ XY + YZ + ZX = 0 \\ XYZ = 1 \end{cases}$$

(c)

$$\begin{cases} X^2 + Y + Z = 1 \\ X + Y^2 + Z = 1 \\ X + Y + Z^2 = 1 \end{cases}$$

11.2 Virsma telpā $\mathbb{R}^3$ ir uzdota parametriski ar sistēmu

$$\begin{cases} X = uv \\ Y = 1 - v \\ Z = u + v - uv \end{cases}$$

Atrodiet sakarības starp $X, Y, Z$ izmantojot Grobnera bāzes.

## 3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

11.4 (Neatrisināta problēma - *cyclic n-roots*) $\forall n \in \mathbb{N}$ atrisināt PVS

$$\begin{cases} X_0 + X_1 + ... + X_{n-1} = 0 \\ X_0X_1 + X_1X_2 + ... + X_{n-2}X_{n-1} + X_{n-1}X_0 = 0 \\ ... \\ \sum_{i=0}^{n-1} X_iX_{i+1 (\mathrm{mod}\ n)}...X_{i+m (\mathrm{mod}\ n)} = 0, \forall\ m < n \\ X_0X_1...X_{n-1} = 1. \end{cases}$$

11.5 Virsma telpā $\mathbb{R}^3$ ir uzdota parametriski ar sistēmu

$$\begin{cases} X = 3u + 3uv^2 - u^3 \\ Y = 3v + 3u^2v - v^3 \\ Z = 3u^2 - 3v^2 \end{cases}$$

Atrodiet sakarības starp $X, Y, Z$ izmantojot Grobnera bāzes.

11.6 Piedāvājiet algoritmu, ar kura palīdzību līknes vai virsmas vispārīgo pierakstu (PVS) var pārveidot parametriskajā pierakstā ar polinomiālām vai racionālām funkcijām.