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

***Studiju kurss***

# Polinomu algebra

## 10.lekcija

***Docētājs: Dr. P. Daugulis***

***2008./2009.studiju gads***

# Saturs

**Lekcijas mērķis:**

- apgūt Grobnera bāzu atrašanas algoritmus (neiedziļinoties pierādījumos).

**Lekcijas kopsavilkums:**

- katram ideālam eksistē Grobnera bāze, pierādījumā var tikt izmantota ģeometriskā interpretācija;
- ideālu ģeneratoru kopas un GB var pārveidot līdzīgi LVS pārveidojumiem Gausa metodē;
- ir kritērijs (Buhbergera kritērijs), ar kura palīdzību var palielināt ideāla ģeneratoru kopu, kamēr ir iegūta GB, pielietojot kritēriju ir jāveic noteiktas operācijas ar polinomu pāriem;
- izmantojot Buhbergera kritēriju un ideālu ģeneratoru kopu pārveidojumus, var iteratīvi mainīt sākotnējo ģeneratoru kopu līdz tiek iegūta GB.

# 1. Grobnera bāzu eksistence

## 1.1. Diksona lemma

Atcerēsimies, ka $n$-argumentu monomu pakāpes var interpretēt kā vektorus ar veselām nenegatīvām koordinātēm no kopas $\mathbb{N}^{*n}$.

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

$$S(\mu) = \mu + \mathbb{N}^{*n} = \{\lambda \in \mathbb{N}^{*n} | \lambda = \mu + \nu, \text{ kur } \nu \in \mathbb{N}^{*n}\}.$$

Ievērosim, ka

$$\lambda \in S(\mu) \iff X^{\lambda} = X^{\mu+\nu} = X^{\mu} \cdot X^{\nu} \iff X^{\mu} | X^{\lambda}.$$

**1.1. piemērs.** $n = 2$, $\mu = (2, 0)$.

**1.1. piezīme.** Katru $\mathbb{N}^{*2}$ apakškopu var nosegt ar galīgas vektoru kopas ēnām.

**1.1. 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 Skatīt nākamo lekciju. ■

# 1.2. Eksistences teorēma

## 1.2.1. Ideāla vecāko monomu kopa

Apzīmēsim ideāla $I$ vecāko monomu pakāpju vektoru kopu ar $\mathcal{M}_I \subseteq \mathbb{N}^{*n}$:

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

**1.2. teorēma.** $\mathcal{M}_I + \mathbb{N}^{*n} \subseteq \mathcal{M}_I$ ($\mathcal{M}_I$ ir slēgta attiecībā uz visu elementu ēnu pievienošanu).

PIERĀDĪJUMS
$\mu \in \mathcal{M}_I \implies \exists f \in I : \mathcal{H}(f) = aX^\mu$.
Seko, ka $\forall \lambda \in \mathbb{N}^{*n}$ izpildās $\underbrace{X^\lambda(aX^\mu)}_{=aX^{\mu+\lambda}} \in I \implies \mu + \lambda \in \mathcal{M}_I$. ■

### 1.2.2. Teorēma

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

PIERĀDĪJUMS

Saskaņā ar Diksona lemmu kopu $\mathcal{M}_I$ var noklāt ar galīgas apakškopas elementu ēnām: $\exists$ vektoru kopa $\{\mu_1, ..., \mu_l\} \subseteq \mathcal{M}_I$ tāda, ka

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

Seko, ka

- $\exists\ f_i \in I$, tādi, ka $\mathcal{H}(f_i) = a_i X^{\mu_i}$,
- $\forall\ f \in I\ \exists\ \mu_j$ tāds, ka

  $$\mathcal{H}(f) = aX^{\mu_j+\nu_j} = aX^{\mu_j}X^{\nu_j} \iff X^{\mu_j}|\mathcal{H}(f) \iff \mathcal{H}(f_j)|\mathcal{H}(f).$$

Seko, ka $\{f_1, ..., f_l\}$ ir GB. ■

**1.4. teorēma.** (*Hilberta bāzes teorēma*) $\forall$ ideālam $I \subseteq k[X_1, ..., X_n]$ eksistē galīga ģeneratoru kopa:

$$\exists\ g_1, ..., g_m : I = \langle g_1, ..., g_m \rangle.$$

PIERĀDĪJUMS Katram ideālam $I$ eksistē GB $\mathcal{G}(I) = \{g_1, ..., g_m\}$, kas ir $I$ galīga ģeneratoru kopa. ■

# 2. Grobnera bāzu atrašanas algoritms

## 2.1. Vienkāršie pārveidojumi

### 2.1.1. Ideāla ğeneratoru kopas elementārie pārveidojumi

**2.1. teorēma.** (*ideāla ğeneratoru kopas elementārie pārveidojumi*)

1. Ideāla ğeneratorus var mainīt vietām (pirmā veida elementārais pārveidojums).
2. $I = \langle f_1, ..., f_m \rangle \ \wedge \ f_i' = \lambda_i f_i$, kur $\lambda_i \neq 0 \implies$
$$I = \langle f_1, ..., \underbrace{f_i'}_{\uparrow\downarrow f_i}, ..., f_m \rangle.$$
(jebkuru ideāla ğeneratoru $f_i$ var aizvietot ar $\lambda_i f_i$, otrā veida elementārais pārveidojums).
3. $I = \langle f_1, ..., f_m \rangle \ \wedge \ f_i' = f_i + c_{ij} f_j \implies$
$$I = \langle f_1, ..., \underbrace{f_i'}_{\uparrow\downarrow f_i}, ..., f_m \rangle.$$

(jebkuru ideāla ģeneratoru $f_i$ var aizvietot ar $f_i + c_{ij} f_j$, trešā veida elementārais pārveidojums).

4. $I = \langle f_1, ..., f_m \rangle \ \wedge \ \{g_1, ..., g_l\} \subseteq I \implies$

$$I = \langle f_1, ..., f_m, g_1, ..., g_l \rangle.$$

(ideāla ģeneratoru kopai var pievienot jebkuru ideāla apakškopu, ceturtā veida elementārais pārveidojums).

PIERĀDĪJUMS

1. Saskaitīšana un reizināšana gredzenā $k[X_1, ..., X_n]$ ir komutatīva.

2.

$$r = \sum_{j=1, j \neq i}^{m} h_j f_j + h_i f_i \iff r = \sum_{j=1, j \neq i}^{m} h_j f_j + h_i \frac{\lambda_i}{\lambda_i} f_i \iff$$

$$r = \sum_{j=1, j \neq i}^{m} h_j f_j + \frac{h_i}{\lambda_i} (\lambda_i f_i) \iff r = \sum_{j=1, j \neq i}^{m} h_j f_j + h'_i f'_i.$$

**3.**

$$r = \sum_{u=1, u \notin \{i,j\}}^{m} h_u f_u + h_i f_i + h_j f_j \iff$$

$$r = \sum_{u=1, u \notin \{i,j\}}^{m} h_u f_u + h_i f_i + h_i c_{ij} f_j - h_i c_{ij} f_j + h_j f_j \iff$$

$$r = \sum_{u=1, u \notin \{i,j\}}^{m} h_u f_u + h_i (f_i + c_{ij} f_j) + (h_j - h_i c_{ij}) f_j \iff$$

$$r = \sum_{u=1, u \notin \{i,j\}}^{m} h_u f_u + h_i f_i' + h_j' f_j.$$

4. Jebkuru ideāla elementu $r$ var izteikt kā sākotnējo elementu

$f_1, ..., f_m$ lineāru kombināciju, jaunie elementi nav obligāti jāizmanto:

$$r = \sum_{j=1}^{m} h_j f_j \implies r = \sum_{j=1}^{m} h_j f_j + \sum_{u=1}^{l} 0 \cdot g_u.$$

■

**2.1. piezīme.** Svarīgs speciālgadījums - $f_i + c_{ij} f_j$ ir viena redukcijas soļa rezultāts. Tā kā dalīšana ar atlikumu vai redukcija ir redukcijas soļu virkne, seko, ka jebkuru ideāla ģeneratoru var aizvietot ar redukcijas rezultātu.

**2.2. piezīme.** Otrā veida elementāros pārveidojumus var izmantot, lai mainītu zīmes vai koeficientus pie lielākā monoma.

**2.1. piemērs.** $I = \langle X^2 - Y^2 - 1, X + 1 \rangle \implies$

$$I = \langle -Y^2, X + 1 \rangle = \langle Y^2, X + 1 \rangle.$$

$$I = \langle XY - 2, X \rangle \implies I = \langle -2, X \rangle = \langle 1, X \rangle \implies I = k[X, Y].$$

### 2.1.2. Grobnera bāzu elementārie pārveidojumi

**2.2. teorēma.** (*GB neviennozīmīgums*)

1. GB var pievienot jebkuru galīgu ideāla apakškopu - ja $\mathcal{F}$ ir $\mathcal{G}(I)$ un $\mathcal{F}'$ ir tāda, ka $\mathcal{F}' \subseteq I$, $\mathcal{F}' \supseteq \mathcal{F}$, $|\mathcal{F}'| < \infty$, tad $\mathcal{F}'$ arī ir $\mathcal{G}(I)$.

2. No GB var izmest elementu, kura vecākais terms dalās ar kāda cita GB elementa vecāko termu - ja $\mathcal{F}$ ir $\mathcal{G}(I)$, $f_i, f_j \in \mathcal{F}$ un $\mathcal{H}(f_j)|\mathcal{H}(f_i)$, tad $\mathcal{F}\backslash\{f_i\}$ arī ir $\mathcal{G}(I)$.

3. GB elementu var aizvietot ar redukcijas soļa un, sekojoši, arī redukcijas, rezultātu - ja $\mathcal{F}$ ir $\mathcal{G}(I)$, $f_i, f_j \in \mathcal{F}$ un $f_i' = f_i + c_{ij} f_j$ ir redukcijas soļa rezultāts, tad $\Big(\mathcal{F}\backslash\{f_i\}\Big) \cup f_i'$ arī ir $\mathcal{G}(I)$.

4. GB elementu var aizvietot ar otrā veida pārveidojuma rezultātu.

PIERĀDĪJUMS

1. Pievienojot $GB$ citus ideāla elementus, saglabāsies Grobnera bāzu definējošā īpašība.

2. Apskatīsim tos $f \in I$, kurus var ietekmēt $f_i$ izmešana no $\mathcal{G}(I)$:

$$\mathcal{H}(f_i)|\mathcal{H}(f) \wedge \ \mathcal{H}(f_j)|\mathcal{H}(f_i) \implies \mathcal{H}(f_j)|\mathcal{H}(f).$$

Seko, ka joprojām $\exists f_j \in \mathcal{G}(I)$, kuram $\mathcal{H}(f_j)|\mathcal{H}(f)$. Tātad $f_i$ izmešana no ģeneratoru kopas saglabā Grobnera bāzes definējošo īpašību.

3. $\mathcal{H}(f_j) \nmid \mathcal{H}(f_i) \implies \mathcal{H}(f_i') = \mathcal{H}(f_i) \implies$ GB definējošā īpašība saglabājas.

$\mathcal{H}(f_j)|\mathcal{H}(f_i) \implies f_i$ var izmest no $\mathcal{F}$ saskaņā ar 2. Elementu $f_i'$ var pievienot saskaņā ar 1.

4. Reizinot $GB$ elementu ar nenulles koeficientu $GB$ īpašības saglabājas. ■

**2.3. piezīme.** Vienkāršāko pārveidojumu ģeometriskā interpretācija:

- var atmest elementus, kuru vecākie termi nevar būt "stūri",
- var veikt redukcijas, jo tās samazina vecākos termus - pietuvina tos "stūriem".

Grobnera bāzi $\{f_1, ..., f_m\}$ sauksim par *minimālu Grobnera bāzi (MGB)*, ja $\forall\ i \neq j$ izpildās nosacījums $\mathcal{H}(f_i) \nmid \mathcal{H}(f_j)$.

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

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

**2.2. piemērs.** Ideālam $\langle X, Y\rangle$ kopa $\{X, Y\}$ ir $RGB$, bet $\{X + Y, Y\}$ - nav.

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

**2.3. teorēma.** Katram ideālam eksistē viena un tikai viena RGB.

PIERĀDĪJUMS Skatīt nākamo lekciju. ■

## 2.2. Buhbergera $S$-pāru kritērijs

### 2.2.1. $S$-polinomi

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

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

Definēsim $X^\gamma = MKD(X^\alpha, X^\beta)$ un

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

Citiem vārdiem sakot, reizinām $f$ un $g$ ar tādiem termiem, lai vecākie locekļi būtu vienādi un pēc iespējas mazāki - vienādi ar $f$ un $g$ vecāko locekļu $MKD$, un saīsinātos.

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

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

### 2.2.2. Motivējošs piemērs

Pieņemsim, ka $I = \langle g_1, g_2 \rangle \subseteq k[X,Y]$ un $\{g_1, g_2\}$ nav $GB$.

Kā var gadīties, ka $f = h_1 g_1 + h_2 g_2$, bet $f$ vecāko termu nevar noreducēt ne ar $g_1$, ne ar $g_2$? Meklēsim šādus $f$ ar pēc iespējas mazāku vecāko termu.

Ja $\mathcal{H}(h_1 g_1) \succ \mathcal{H}(h_2 g_2)$ vai otrādi, tad vecākie termi labajā pusē nesaīsināsies un $\mathcal{H}(f)$ dalīsies ar vecāko no tiem, tātad $f$ varēs noreducēt vismaz vienu reizi.

Seko, ka $h_1 g_1$ un $h_2 g_2$ vecākie monomi ir vienādi un termi saīsinās.

Kā panākt, ka $h_1g_1$ un $h_2g_2$ vecākie termi ir pēc iespējas mazāki un var saīsināties?

Apskatīsim $g_3 = S(g_1, g_2)$. Ja $g_3 \neq 0$, $\overline{g_3}^{\{g_1,g_2\}} \neq 0$, tad $\overline{g_3}^{\{g_1,g_2\}}$ būtu jāpievieno kā jauns $I$ ğenerators.

**2.4. piemērs.** $g_1 = XY + 1$, $g_2 = Y^2 - 1$, $g_3 = S(g_1, g_2) = X + Y$.

### 2.2.3. Kritērijs

**2.4. teorēma.** Kopa $\mathcal{G} = \{g_1, ..., g_m\}$ ir ideāla $I = \langle g_1, ..., g_m \rangle$ $GB \iff$

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

PIERĀDĪJUMS Skatīt nākamo lekciju. ■

## 2.3. Algoritmi

### 2.3.1. Buhbergera algoritms

Buhbergera sākotnējais algoritms - lai atrastu ideāla $I = \langle g_1, ..., g_l \rangle$ $GB$, veicam šādas darbības:

- definējam sākotnējo ģeneratoru kopu kā mainīgu kopu $\mathcal{G}$,
- ja atrodam tādu polinomu pāri $\{g_i, g_j\} \subseteq \mathcal{G}$, ka
$$s = \overline{S(g_i, g_j)}^{\mathcal{G}} \neq 0,$$
(vismaz vienai redukcijai mod $\mathcal{G}$), tad definējam
$$\mathcal{G} := \mathcal{G} \cup s,$$
- atkārtojam iepriekšējo soli tik ilgi, kamēr notiek $\mathcal{G}$ izmaiņas.

**2.5. piemērs.** $I = \langle X, Y \rangle$. Saskaņā ar Buhbergera algoritmu nekas nav jādara, jo $S(X, Y) = 0$. Tādējādi sākotnējā veidotājelementu kopa (bāze) ir $GB$.

$I = (\underbrace{XY+1}_{g_1}, \underbrace{Y^2-1}_{g_2})$. 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 $\{g_1, g_2, g_3\}$.

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

PIERĀDĪJUMS Skatīt nākamo lekciju. ■

### 2.3.2. Uzlabotie algoritmi

Buhbergera algoritmu var uzlabot šādos veidos:

- meklēt nevis $GB$, bet $RGB$;
- algoritma sākumā un pēc katra $S$-polinoma pievienošanas veikt visas savstarpējās redukcijas;
- izvēlēties tādus $S(f,g)$, lai $MKD(\mathcal{H}(f),\mathcal{H}(g))$ būtu pēc iespējas mazāks.

Lai atrastu ideāla $I = \langle g_1, ..., g_l \rangle$ $RGB$, veicam šādas darbības:

A (Sākotnējās ģeneratoru kopas definēšana) Definējam sākotnējo ģeneratoru kopu kā mainīgo kopu $\mathcal{G}$.

B (Sākotnējās redukcijas) Veicam visas iespējamās $\mathcal{G}$ elementu savstarpējās redukcijas.

C (Nereducējama $S$-polinoma pievienošana un redukcijas) Ja atrodam polinomu pāri $\{g_i, g_j\} \subseteq \mathcal{G}$ tādu, ka

$$s = S(g_i, g_j) \neq 0,$$

tad veicam $\mathcal{G}$ izmaiņu:

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

Veicam soli $B$. Ja notiek $\mathcal{G}$ izmaiņa, tad atkārtojam šo soli vēlreiz.

**2.6. piemērs.** $I = \langle \underbrace{XY+1}_{g_1}, \underbrace{Y^2-1}_{g_2} \rangle$. 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 $g_1 = XY+1$ var noreducēt uz $g_2$.

3. $S(g_2, g_3) = X + Y^3 = Y(Y^2-1) + (X+Y)$ - reducējas uz 0, tāpēc neko jaunu mēs neiegūsim un $RGB$ ir vienāda ar $\{g_2, g_3\}$.

# 3. 10.mājasdarbs

## 3.1. Obligātie uzdevumi

10.1 Atrast $\mathbb{N}^{*2}$ apakškopu, kuru var noklāt ar ne mazāk kā $m$ tās elementu ēnām, vai pierādīt, ka tāda apakškopa neeksistē.

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

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

(a) $I = \langle X^2Y - 1, XY^2 - X \rangle$, $X \succ Y$
(b) $I = \langle X^2 + Y, X^4 + 2X^2Y + Y^2 + 3 \rangle$, $X \succ Y$,
(c) $I = \langle X^3 + Y^3, X^2 + Y^2 \rangle$, $X \succ Y$,
(d) $I = \langle X - Y^4, Y - Z^5 \rangle$, $X \succ Y \succ Z$,
(e) $I = \langle X^2 - Z, XY - T \rangle$, $X \succ Y \succ Z \succ T$.

## 3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

10.5 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

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

10.6 Dots ideāls $I \subseteq k[X, Y]$ ar diviem ģeneratoriem. Kāds var būt $RGB$ elementu skaits kopā? Atrodiet konkrētus piemērus visos gadījumos.