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

***Studiju kurss***

# Polinomu algebra

## 9.lekcija

***Docētājs: Dr. P. Daugulis***

***2007./2008.studiju gads***

# Saturs

# 1. Vairāku argumentu polinomi

## 1.1. Motivācijas

Pieņemsim, ka $R$ ir komutatīvs gredzens ar vieninieku, $S \subseteq R$ ir tā apakšgredzens ar vieninieku. Katrai $R$ elementu virknei $t_1, ..., t_n \in R$ definēsim apakšgredzena $S$ *paplašinājumu ar elementiem* $t_1, ..., t_n$ - kopu

$$S[t_1, ..., t_n] = \{a \in R | b = \sum_{i_1, ...i_n} a_{i_1 ... i_n} t_1^{i_1} ... t_n^{i_n}\}.$$

Citiem vārdiem sakot $S[t_1, ..., t_n]$ ir mazākais apakšgredzens, kas satur $S$,$t_1, ..., t_n$. Līdzīgi kā viena argumenta polinomu gadījumā var atrast divu elementu summu un reizinājumu.

Lietderīgi ir pētīt kopu $S[t_1, ..., t_n]$ uzskatot $t_1, ..., t_n$ par ārējiem elementiem, kas neapmierina nekādas sakarības.

Ja funkcija $f : R^n \to R$ ir uzdota ar polinomiālu likumu

$$f(t_1, ..., t_n) = \sum_{i_1, ...i_n} f_{i_1 ... i_n} t_1^{i_1} ... t_n^{i_n},$$

tad sauksim to par *n-argumentu polinomiālu funkciju*. Visu polinomiālu funkciju kopu apzīmēsim ar $\mathcal{P}ol(R^n, R)$. Kopā $\mathcal{P}ol(R^n, R)$ var definēt gredzena struktūru kā aprakstīts iepriekšējos punktos un pētīt šo jauno gredzenu.

## 1.2. Definīcijas

### 1.2.1. Polinomu gredzeni

Ir dots komutatīvs gredzens ar vieninieku $R$.

Konstruēsim viena argumenta polinomu gredzenu virs $R[X]$ - iegūsim gredzenu $R[X][Y]$.

$R[X][Y]$ elementi ir izsakāmi formā

$$\sum_{j=0}^{k} b_j Y^k = \sum_{j=0}^{k} (\sum_{i=0}^{n} a_{ij} X^i) Y^k = \sum_{i=0,j=0}^{n,k} a_{ij} X^i Y^k$$

$R[X][Y]$ ar definētajām summas un reizināšanas operācijām sauc par *divu argumentu polinomu gredzenu virs* $R$ un apzīmē ar $R[X, Y]$.

Iterējot šo konstrukciju iegūst *n-argumentu polinomu gredzenu virs* $R$ - $R[X_1, ..., X_n] = R[X_1, ..., X_{n-1}][X_n]$.

Par *n-argumentu monomu* sauc polinomu formā $aX_1^{m_1}...X_n^{m_n}$. Par monoma pakāpi sauc tā argumentu pakāpju summu.

Argumentus var apzīmēt vismaz divos veidos:

- $X_1, X_2, ..., X_n$;
- $X, Y, Z, ....$

Monomu $X_1^{i_1}...X_n^{i_n}$ apzīmē arī ar $X^\mu$, kur $\mu = (i_1, i_2, ..., i_n)$ var domāt kā vektoru ar nenegatīvām koordinātēm. Šādā pierakstā polinomu

$$\sum_{i_1=0,i_2=0,...,i_n=0}^{m_1,m_2,...,m_n} a_{i_1 i_2 ... i_n} X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$$

apzīmē kā

$$\sum_{\mu} a_\mu X^\mu,$$

kur summēšanas arguments ir vektors.

Divi n-argumentu polinomi ir vienādi tad un tikai tad, ja tiem ir vienādi visi monomu koeficienti.

### 1.2.2. Ģeometriskā interpretācija

Apzīmēsim $\mathbb{N} \cup \{0\}$ ar $\mathbb{N}^*$.

Viena argumenta polinomi -

- koeficientu virknes,
- funkcijas

$$\mathbb{N}^* \to R,$$
$$i \to a_i$$

  ar galīgu definīcijas apgabalu,
- viendimensionālu nosvērtu vektoru (punktu) kopas.

Divu argumentu polinomi -

- koeficientu tabulas,
- funkcijas

$$(\mathbb{N}^*)^2 \to R,$$
$$(i,j) \to a_{ij}$$

  ar galīgu definīcijas apgabalu,
- divdimensionālu nosvērtu vektoru (punktu) kopas.

Trīs argumentu polinomi -

- trīsdimensionālas koeficientu tabulas,
- funkcijas

$$(\mathbb{N}^*)^3 \to R,$$
$$(i,j,k) \to a_{ijk}$$

  ar galīgu definīcijas apgabalu,
- trīsdimensionālu nosvērtu vektoru (punktu) kopas.

Operāciju interpretācija:

- saskaitīšana - vektoru svaru summēšana,
- reizināšana ar monomu $aX^\mu$ - nobīde par vektoru $\mu$ un svaru reizināšana ar $a$,
- reizināšana ar polinomu $f$ - reizināšanu ar $f$ monomiem rezultātu svaru summēšana.

**1.1. piemērs.** Reizināšana ar $X + Y$.

### 1.2.3. Pakāpe

Par n-argumentu polinoma $f$ pakāpi sauc maksimālo monoma pakāpi, apzīmēsim to ar $\deg(f)$.

Ja $\mu = (\mu_1, ..., \mu_n)$, tad apzīmēsim monoma $X^\mu$ pakāpi $\sum_{i=1}^{n} \mu_i$ ar $|\mu|$.

$n$-argumentu polinomu sauc par *homogēnu $m$-tās pakāpes polinomu*, ja katra monoma pakāpe ir vienāda ar $m$.

**1.2. piemērs.** $X^2Y + XY^2 + Z^3$ ir homogēns 3.pakāpes polinoms.

### 1.2.4. Monomu sakārtojums

Vairāku argumentu polinomu monomus ir lietderīgi sakārtot noteiktā kārtībā atkarībā no tajos ieejošu argumentu pakāpēm.

**1.3. piemērs.** Ja $n = 1$, tad monomi tiek kārtoti pakāpes dilšanas kārtībā.

Definēsim *monomu leksikogrāfisko sakārtojumu*. Teiksim, ka

$$aX^{\mu} \succ bX^{\lambda},$$

ja

$$\mu - \lambda = (0, ..., 0, \alpha, ...),$$

kur $\alpha > 0$ un locekļi, kas seko pēc $\alpha$, var būt jebkādi, $a \neq 0$, $b \neq 0$.

Definēsim

$$aX^{\mu} \asymp bX^{\lambda},$$

ja

$$\mu = \lambda.$$

Definēsim

$$aX^{\mu} \succeq bX^{\lambda},$$

ja $aX^{\mu} \succ bX^{\lambda}$ vai $aX^{\mu} \asymp bX^{\lambda}$.

**1.4. piemērs.** $X_1 \succ X_2$, $X_1X_2 \succ X_2^5$.

**1.1. piezīme.** Attiecību $\geqslant$ monomu kopā sauksim par *monomu sakārtojumu*, ja izpildās šādi nosacījumi:

- $\geqslant$ ir daļējs sakārtojums (refleksīvs, antisimetrisks, tranzitīvs),
- $\geqslant$ ir dihotomisks (jebkuru divi monomi ir salīdzināmi kādā kārtībā),
- $1 \leqslant X^{\mu}$ (konstantais monoms ir vismazākais),
- ja $X^{\lambda} \leqslant X^{\mu}$, tad $X^{\lambda}X^{\nu} \leqslant X^{\mu}X^{\nu}$, katram $\nu$ (reizināšana saglabā kārtību).

Mēs parasti izmantosim leksikogrāfisko sakārtojumu, kas ir monomu sakārtojuma speciālgadījums.

**1.1. teorēma.** Leksikogrāfiskais sakārtojums ir monomu sakārtojums.

PIERĀDĪJUMS
$\succeq$ **ir dihomomisks daļējs sakārtojums.**

- Refleksivitāte - $X^\mu \preceq X^\mu$ katram $\mu$.
- Antisimetrija - ja $X^\mu \preceq X^\lambda$ un $X^\lambda \preceq X^\mu$, tad $\mu - \lambda = 0$, tātad $\mu = \lambda$.
- Tranzitivitāte - ja $X^\mu \preceq X^\lambda$ un $X^\lambda \preceq X^\nu$, tad

$$\lambda - \mu = (0, ..., 0, t),$$
$$\nu - \lambda = (0, ..., 0, v),$$

tādējādi $\nu - \mu = (0, ..., 0, w)$.

- Dihotomija - jebkuri divi elementi ir salīdzināmi, to nosaka pirmais atšķirīgais elementu pāris no kreisās malas.

**Reizināšana saglabā kārtību.**

Ja $X^\lambda \preceq X^\mu$, tad $\mu - \lambda = (0, ..., 0, t)$. ■

Par polinoma $f$ *vecāko locekli* $\mathcal{H}(f)$ sauksim tā lielāko momomu.

**1.5. piemērs.** $\mathcal{H}(X_1 + X_2 + X_1^2 X_2^2 + 3X_1^4) = 3X_1^4$.

Ja definējam leksikogrāfisko sakārtojumu, kurā $X \succ Y \succ Z$, tad $\mathcal{H}(Z^3 + Y^2 - X) = -X$.

### 1.2.5. Polinomu sakārtojums

Monomu sakārtojums inducē *polinomu leksigrāfisko sakārtojumu* šādā veidā.

Pieņemsim, ka

$$f = f_1 + f_2 + ..., \text{ kur } f_i \succ f_{i+1},$$
$$g = g_1 + g_2 + ..., \text{ kur } g_i \succ g_{i+1}.$$

Definēsim $f \succ g$, ja eksistē tāds $l \geq 1$, ka

- $f_i \asymp g_i$, visiem $1 \leq i \leq l$,
- $f_l \succ g_l$.

Definēsim $f \asymp g$, ja $f$ un $g$ monomu kopas ir vienādas (ar precizitāti līdz koeficientiem).

**1.6. piemērs.**
$(X_1^2 + X_1X_2 + X_1^2) \succ (X_2^2 + X_1 + X_2^5)$.
$(X_1^2 + X_1X_2 + X_1^2 + X_2) \succ (X_1^2 + X_1X_2 + X_1^2 + 1)$.

## 1.2.6. Faktorizācija un saknes

Ja $f, g \in R[X_1, ..., X_n]$, tad teiksim, ka $f$ dalās ar $g$, ja eksistē $h \in R[X_1, ..., X_n]$ tāds, ka $f = gh$.

Ja polinomam nav neinvertējamu dalītāju, to sauc par nedalāmu.

**1.7. piemērs.** $X^4 + Y^4$ dalās ar $X + Y$ virs $\mathbb{F}_2$, jo

$$X^4 + Y^4 = (X + Y)^4.$$

$X^4 + Y^4$ dalās ar $X^2 + XY + 2Y^2$ virs $\mathbb{F}_3$, jo

$$X^4 + Y^4 = (X^2 + XY + 2Y^2)(X^2 + 2XY + 2Y^2).$$

$X^4 + Y^4$ ir nedalāms virs $\mathbb{Z}$.

Pieņemsim, ka ir doti gredzeni $R \subseteq S$.

Teiksim, ka elementu virkne $(a_1, ..., a_n) \in S$ ir nekonstanta polinoma $f \in R[X_1, ..., X_n]$ *atrisinājums*, ja

$$f(a_1, ..., a_n) =_S 0.$$

Vairāku argumentu polinomiem nav Bezū teorēmas analoga.

Vairāku argumentu polinomam virs bezgalīga lauka var būt bezgalīgi daudz atrisinājumu.

**1.8. piemērs.** Vienādojumam $X + Y = 0$ ir bezgalīgi daudz atrisinājumu.

# 1.3. Pamatfakti

## 1.3.1. Integralitāte un faktorizācija

**1.2. teorēma.**

1. Ja $R$ ir integrāls gredzens, tad katram $n$ $R[X_1, ..., X_n]$ ir integrāls gredzens.
2. Ja $R$ ir VFG, tad katram $n$ $R[X_1, ..., X_n]$ ir VFG.

PIERĀDĪJUMS Iepriekš tika pierādīti šādi apgalvojumi:

- ja $R$ ir integrāls gredzens, tad $R[X]$ ir integrāls gredzens,
- ja $R$ ir VFG, tad $R[X]$ ir VFG.

Izmantosim matemātisko indukciju.
Ja $n = 1$, tad viss ir pierādīts.
Pieņemsim, ka apgalvojumi ir pierādīti visiem $n < m$.
Seko, ka $R[X_1, ..., X_{m-1}, X_m] = R[X_1, ..., X_{m-1}][X_m]$ ir integrāls un VFG, jo koeficientu gredzens tam ir integrāls un VFG saskaņā ar indukcijas pieņēmumu. ■

**1.2. piezīme.** Tā kā $R[X_1, ..., X_n]$ ir VFG, tad tam eksistē $LKD$ un $MKD$.

### 1.3.2. Pakāpe, monomu un polinomu sakārtojums

**1.3. teorēma.** Apskatīsim $R[X_1, ..., X_n]$, kur $R$ ir integrāls gredzens

1. Jebkuru polinomu var viennozīmīgi izteikt homogēnu polinomu summas veidā.
2. $\deg(fg) = \deg(f) + \deg(g)$.

PIERĀDĪJUMS 1. Apgalvojums ir acīmredzams.

2. Sadalīsim $f$ un $g$ homogēnajās daļās un apskatīsim vecāko daļu reizinājumu. Tas nav nulle, jo $R[X]$ ir integrāls gredzens. Tā pakāpe ir $\deg(f) + \deg(g)$.

■

**1.4. teorēma.**

1. Jebkura stingri dilstoša monomu virkne $a_1X^{\mu_1} \succ a_2X^{\mu_2} \succ \ldots$ ir galīga.
2. Jebkura stingri dilstoša polinomu virkne $f_1 \succ f_2 \succ \ldots$ ir galīga.

PIERĀDĪJUMS

1. Ja $X^{\mu_i} \succ X^{\mu_{i+1}}$, tad vektoram $\mu_{i+1}$ vismaz viena koordināte ir mazāka nekā vektoram $\mu_i$. Vektoru koordinātes nevar būt negatīvas. Pēc galīga skaita soļiem tiks sasniegts vektors $\lambda$, par kuru mazākam vektoram vismaz viena koordināte ir negatīva, $X^\lambda$ ir pēdējais monoms virknē.

2. Ja $f_i \succ f_{i+1}$, tad polinomam $f_{i+1}$ vismaz viens monoms ir mazāks nekā polinomam $f_i$. Pēc galīga skaita soļiem tiks sasniegts polinoms $g$, par kuru mazāks polinoms neeksistē, $g$ ir pēdējais polinoms virknē. ■

**1.5. teorēma.** Ja $f_1, ..., f_m \in R[X_1, .., X_n]$, tad

$$\mathcal{H}(f_1 f_2 ... f_m) = \mathcal{H}(f_1)\mathcal{H}(f_2)...\mathcal{H}(f_m).$$

PIERĀDĪJUMS

**1.solis. Divi reizinātāji.**

Pierādīsim, ka

$$\mathcal{H}(fg) = \mathcal{H}(f)\mathcal{H}(g).$$

Pieņemsim, ka

$$f = f_1 + f_2 + ..., \text{ kur } f_1 = \mathcal{H}(f), f_i \succ f_{i+1},$$
$$g = g_1 + g_2 + ..., \text{ kur } g_1 = \mathcal{H}(g), g_i \succ g_{i+1}.$$

Redzam, ka

$$fg = \sum_{i,j} f_i g_j$$

un

- $f_u g_v \succ f_w g_v$, ja $u < w$,
- $f_u g_v \succ f_u g_t$, ja $v < t$.

Seko, ka

$$\mathcal{H}(fg) = f_1 g_1 = \mathcal{H}(f)\mathcal{H}(g).$$

**2.solis. Patvaļīgs reizinātāju skaits.**

Izmantojam matemātisko indukciju ar parametru $m$. Pieņemsim, ka apgalvojums ir spēkā visiem $m < l$. Tad

$$\mathcal{H}(f_1 f_2 ... f_l) = \mathcal{H}((f_1 ... f_{l-1}) f_l) = \underbrace{\mathcal{H}(f_1 ... f_{l-1})}_{\text{indukcijas pieņēmums}} \mathcal{H}(f_l) =$$

$$\mathcal{H}(f_1)\mathcal{H}(f_2)...\mathcal{H}(f_m).$$

■

### 1.3.3. Ideāli

Gredzenos $R[X_1, ..., X_n]$ ir definēti ideāli.

Būtiska atšķirība no $R[X]$ - eksistē ideāli, kas nav galvenie.

**1.6. teorēma.** Ja $n \geq 2$, tad $R[X_1, ..., X_n]$ nav GIG.

PIERĀDĪJUMS Pieņemsim, ka $n \geq 2$ un apskatīsim ideālu

$$I = (X_1, X_2).$$

Ja $I = (f)$, tad $X_1 = qf$, tātad $f = uX_1$. Bet tad $X_2 \notin I$ - pretruna. ■

Var pierādīt, ka katram ideālam polinomu gredzenā $R[X_1, ..., X_n]$ eksistē galīga ģeneratoru kopa - katrs ideāls ir galīgi ģenerēts.

Tādējādi, katru ideālu $I \subseteq R[X_1, ..., X_n]$ var uzdot formā

$$I = (a_1, ..., a_m) = \{f \in R[X_1, ..., X_n] | f = f_1 a_1 + f_2 a_2 + ... + f_m a_m,$$
$$\text{kur } f_i \in R[X_1, ..., X_n]\}.$$

# 1.4. Vairāku argumentu polinomu dalīšana ar atlikumu

## 1.4.1. Viens dalītājs

**1.7. teorēma.** Ja $f, g \in R[X]$ ir nenulles polinomi, tad eksistē polinomu pāris $(d, r)$, kuram izpildās šādi nosacījumi:

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

PIERĀDĪJUMS
**Algoritms.**

Doti divi nenulles polinomi $f, g \in R[X_1, ..., X_n]$. Definēsim

$$f_t = f.$$

A. Atradīsim vecāko $f_t$ monomu $a_\mu X^\mu$, kas dalās ar $\mathcal{H}(g)$, ja tāds neeksistē, tad apstājamies, ja eksistē, tad definēsim

$$f_t := f_t - \frac{a_\mu X^\mu}{\mathcal{H}(g)} g.$$

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

Algoritma darba rezultātā iegūtais $f_t$ ir vienāds ar $r$ un

$$f - r = dg.$$

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc katra $A$ tipa soļa izpildes ar $f_t$ izmaiņu $f_t$ samazinās polinomu sakārtojuma nozīmē - monomi, kas var dalīties ar $\mathcal{H}(g)$, paliek stingri mazāki.

■

**1.9. 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

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

## 1.4.2. Vairāki dalītāji

**1.8. teorēma.** Ja $\{f, g_1, g_2, ..., g_m\} \subseteq R[X]$ ir nenulles polinomi, tad eksistē polinomu virkne $(d_1, d_2, ..., d_m, r)$, kurai izpildās nosacījumi

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

PIERĀDĪJUMS
**Algoritms.**

Doti nenulles polinomi $f, g_1, g_2, ..., g_m \in R[X_1, ..., X_n]$. Definēsim

$$f_t = f.$$

A. Atradīsim vecāko $f_t$ monomu $a_\mu X^\mu$, kas dalās ar kādu $\mathcal{H}(g_i)$, ja tāds neeksistē, tad apstājamies, ja eksistē, tad atradīsim mazāko $i$ un definēsim

$$f_t := f_t - \frac{a_\mu X^\mu}{\mathcal{H}(g_i)} g_i.$$

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

Algoritma darba rezultātā iegūtais $f_t$ ir vienāds ar $r$ un

$$f - r = d_1 g_1 + ... + d_m g_m.$$

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc katra $A$ tipa soļa izpildes ar $f_t$ izmaiņu $f_t$ samazinās polinomu sakārtojuma nozīmē - monomi, kas var dalīties ar $\mathcal{H}(g_i)$, paliek stingri mazāki.

■

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

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

1. $f_t := f - X^2 g_2 = -X^2Y + Y^4$,

2. $f_t := f_t - (-X)g_1 = X + Y^4$. Jāapstājas.

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.

# 2. 9.mājasdarbs

## 2.1. Obligātie uzdevumi

9.1 Sakārtot dotos monomus augošā leksikogrāfiskajā kārtībā, uzskatot, ka $X \succ Y \succ Z$:

$$X^2Y, Y^3, XYZ, X^2Z^4, Y^2Z^3, 1, Z^2.$$

9.2 Ja iespējams, sakārtot dotos polinomus dilstošā leksikogrāfiskajā kārtībā, uzskatot, ka $X \succ Y \succ Z$:

$$X^2Y^2 + XY^3 + XY + Y,$$
$$X^3 + X^2Y^2 + XY^3 + Y^2,$$
$$X^2Y^2 + X^2 + XY + Y,$$
$$X^3 + X^2Y + XY^2 + Y^2.$$

9.3 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 $\mathbb{F}_2$, $X \succ Y \succ Z$.

9.4 Atrast $f$ 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 $\mathbb{F}_2$, $X \succ Y \succ Z$.

## 2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

9.5 Konstruējiet ideālu virs kāda polinomu gredzena, kuru nevar ģenerēt ar mazāk kā $m$ elementiem ($m \geq 3$).