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

Studiju kurss

Polinomu algebra

6.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis: definēt *vairāku argumentu polinomu gredzenus (VAPG)*, to svarīgākos palīgjēdzienus.

Lekcijas kopsavilkums:

- var definēt vairāku argumentu polinomu gredzenus (VAPG),
- VAPG var definēt vairākus viena argumenta polinomu jēdzienu analogus;
- VAPG var ieviest monomu un polinomu sakārtojumu;
- VAPG ir spēkā integralitātes un VFG īpašības analoģiski viena argumenta polinomu gadījumam.

Svarīgākie jēdzieni: n-argumentu polinomu gredzens, monoms, terms, multipakāpe, pakāpe, homogēns polinoms, monomu leksikogrāfiskais sākārtojums, polinoma vecākais terms, polinoma multipakāpe, polinomu leksikogrāfiskais sakārtojums, polinomu faktorizācija.

Svarīgākie fakti un metodes: divu n-argumentu polinomu vienādība, monomu leksikogrāfiskā sakārtojuma īpašības, VAPG integralitāte un viennozīmīgā faktorizācija, pakāpju un multipakāpju īpašības, leksikogrāfiski dilstošu monomu un polinomu virkņu galīgums, vecākā terma multiplikativitātes īpašība.

1. Vairāku argumentu polinomi

1.1. Definīcijas

1.1.1. Polinomu gredzeni

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

$R[X][Y]$ elementi ir izsakāmi formā

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

$R[X][Y]$ 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 - $R[X_1, ..., X_n] = R[X_1, ..., X_{n-1}][X_n]$.

Argumentus var apzīmēt vismaz divos veidos:

- $X_1, X_2, ..., X_n$;
- $X = X_1, Y = X_2, Z = X_3, ...$

Par *n-argumentu monomu* sauc polinomu formā $X_1^{i_1}...X_n^{i_n}$.

Parasti katrā monomā argumentus raksta noteiktā kārtībā.

1.1. piemērs. $X_2X_3^4X_1^2 \dashrightarrow X_1^2X_2X_3^4$.

Par *n-argumentu polinoma locekli (termu)* sauc polinomu formā $aX_1^{m_1}...X_n^{m_n}$, $a \in R$.

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

$$\sum_{i_1=0,i_2=0,\ldots,i_n=0}^{m_1,m_2,\ldots,m_n} a_{i_1i_2\ldots i_n}X_1^{i_1}X_2^{i_2}...X_n^{i_n} = \sum_\mu a_\mu X^\mu, \text{ kur } \mu \text{ ir vektors.}$$

Divi n-argumentu polinomi ir vienādi $\iff$ tiem ir vienādi visi monomu koeficienti.

1.1.2. Pakāpe

Definēsim monoma $X^\mu = X_1^{i_1} ... X_n^{i_n}$ pakāpi $\deg(X^\mu) = |\mu|$:

$$\deg(X^\mu) = \deg(X_1^{i_1} ... X_n^{i_n}) = i_1 + ... + i_n.$$

Par terma pakāpi sauc tam atbilstošā monoma pakāpi.

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

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

1.2. piemērs. $X^2Y + Z^3$ - homogēns 3.pakāpes polinoms.

1.1.3. Monomu leksikogrāfiskais sakārtojums

VAPG monomus ir lietderīgi sakārtot noteiktā kārtībā atkarībā no to argumentu pakāpēm.

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

Definēsim *monomu leksikogrāfisko sakārtojumu*. Teiksim, ka

$$X^\mu \succ X^\lambda \overset{Def}{\iff} \mu - \lambda = (0, ..., 0, \underbrace{t}_{>0}, \underbrace{...}_{\text{jebkādi}}),$$

nuļļu virkne var būt arī tukša. Citiem vārdiem, sakot, vektoram $\mu - \lambda$ pirmais nenulles elements no kreisās malas ir pozitīvs.

Definēsim

- $X^\mu \asymp X^\lambda \overset{Def}{\iff} \mu = \lambda.$
- $X^\mu \succeq X^\lambda \overset{Def}{\iff} X^\mu \succ X^\lambda \ \vee \ X^\mu \asymp X^\lambda.$

1.4. piemērs. $X_1 \succ X_2 \succ X_3 \succ ... \succ X_n$, $X_1 X_2 \succ X_2^n$, $\forall\, n$.

1.1. teorēma. Monomu leksikogrāfiskais sakārtojums apmierina šādas īpašības:

1. $\preceq$ ir daļējs sakārtojums (refleksīvs, antisimetrisks, tranzitīvs);
2. $\preceq$ dihotomisks (jebkuri divi monomi ir salīdzināmi);
3. $1 \preceq X^\mu$ (konstantais monoms ir vismazākais),
4. $X^\lambda \preceq X^\mu \implies X^\lambda X^\nu \preceq X^\mu X^\nu$, $\forall\, \nu$ (reizināšana saglabā kārtību).

PIERĀDĪJUMS

1.

- Refleksivitāte - $X^\mu \preceq X^\mu \;\forall\, \mu$.
- Antisimetrija - $\begin{cases} X^\mu \preceq X^\lambda \\ X^\lambda \preceq X^\mu \end{cases} \implies \mu - \lambda = 0 \implies \mu = \lambda.$
- Tranzitivitāte - $\begin{cases} X^\lambda \preceq X^\mu \\ X^\mu \preceq X^\nu \end{cases} \implies$

$$\left\{\begin{array}{l} \mu-\lambda=(\underbrace{0,...,0}_{v \text{ nulles}},t,...), \\ \nu-\mu=(\underbrace{0,...,0}_{w \text{ nulles}},u,...), \end{array}\right. \Longrightarrow$$

$$\nu-\lambda=(\underbrace{0,...,0}_{\min(v,w) \text{ nulles}},w,...) \Longrightarrow X^\lambda \preceq X^\nu.$$

2. Dihotomija - jebkuri monomi ir salīdzināmi, to nosaka pirmais atšķirīgais argumentu pāris no kreisās malas.

3. $1=X^{(0,...,0)} \Longrightarrow 1 \preceq X^\mu \ \forall\ \mu.$

4. $X^\lambda \prec X^\mu \Longrightarrow \mu-\lambda=(0,...,0,t,...).$

$$\left\{\begin{array}{l} X^\lambda X^\nu = X^{\lambda+\nu} \\ X^\mu X^\nu = X^{\mu+\nu} \\ (\mu+\nu)-(\lambda+\nu)=\mu-\lambda \end{array}\right. \Longrightarrow X^\lambda X^\nu \prec X^\mu X^\nu. \blacksquare$$

Definēsim nenulles termu leksikogrāfisko sakārtojumu:

$$aX^\mu \succeq bX^\lambda \overset{Def}{\Longleftrightarrow} X^\mu \succeq X^\lambda.$$

Polinomus parasti uzdosim sakārtojot termus leksikogrāfiski dilstošā kārtībā.

1.5. piemērs. $\left(X_3^2 - X_1X_2 + X_2^3\right) \longrightarrow \left(-X_1X_2 + X_2^3 + X_3^2\right).$

Polinoma f *vecākais terms* $\mathcal{H}(f)$ - f lielākais terms leksikogrāfiskajā sakārtojumā.

Polinoma f multipakāpe multideg(f) - f vecākā terma multipakāpe.

1.6. piemērs. $X_1 \succ X_2 \succ X_3 \implies \mathcal{H}(X_2 + X_1^2X_2^2 + 3X_1^4) = 3X_1^4$, multideg$= (4,0,0)$.

$X \succ Y \succ Z \implies \mathcal{H}(Z^3 + Y^2 - X) = -X$, multideg$= (1,0,0)$.

1.1.4. Polinomu sakārtojums

Ja ir dots VAP f, tad tā termus var sakārtot dilstošā kārtībā attiecībā uz leksikogrāfisko sakārtojumu.

Monomu un termu leksikogrāfiskais sakārtojums inducē *polinomu leksikogrāfisko sakārtojumu* šādā veidā.

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

Ideja: lasām abus polinomus no kreisās malas un atrodam pirmo atšķirību.

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

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

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

1.7. piemērs.

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

1.1. piezīme. Tā kā reizināšana ar monomu saglabā monomu kārtību, tad polinoma reizināšana ar monomu saglabā tā monomu kārtību.

1.8. piemērs. $(\underbrace{X_1 + X_2^3}_{\text{dilstoša}})X_2 = \underbrace{X_1X_2 + X_2^3}_{\text{dilstoša}}$.

1.1.5. Faktorizācija un saknes

$f, g \in R[X_1, ..., X_n]$. Teiksim, ka f dalās ar g, ja $\exists\, h \in R[X_1, ..., X_n]$:

$$f = gh.$$

1.9. piemērs. $X + Y \Big| X^4 + Y^4$ virs $\mathbb{F}_2$, jo

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

$X^2 + XY + 2Y^2 \Big| X^4 + Y^4$ 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 $\mathbb{Z}$.

Elementu virkne $(a_1, ..., a_n) \in R^n$ ir nekonstanta polinoma $f \in R[X_1, ..., X_n]$ *atrisinājums*, ja

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

Vairāku argumentu polinomiem nav Bezout teorēmas analoga.

VAP virs bezgalīga lauka var būt bezgalīgi daudz atrisinājumu.

1.10. piemērs. Vienādojumam $X + Y = 0$ ir bezgalīgi daudz atrisinājumu virs $\forall$ bezgalīga lauka.

1.2. Pamatfakti

1.2.1. Integralitāte un faktorizācija

1.2. teorēma.

1. R ir IG $\Longrightarrow$ $R[X_1, ..., X_n]$ ir IG.
2. R ir VFG $\Longrightarrow$ $R[X_1, ..., X_n]$ ir VFG.

PIERĀDĪJUMS Iepriekš tika minēti šādi apgalvojumi:

- R ir IG $\Longrightarrow$ $R[X]$ ir IG,
- R ir VFG $\Longrightarrow$ $R[X]$ ir VFG.

Izmantosim matemātisko indukciju ar parametru n.

Indukcijas bāze Ja $n = 1$, tad viss ir pierādīts.

Indukcijas solis Pieņemsim, ka apgalvojumi ir pierādīti $\forall\ n < m$.

$R[X_1, ..., X_{m-1}] = \mathcal{R}$ - IG, VFG $\Longrightarrow$

$$\mathcal{R}[X_m] = R[X_1, ..., X_{m-1}][X_m] = R[X_1, ..., X_{m-1}, X_m] \text{ - } IG, VFG. \blacksquare$$

1.2. piezīme. $R[X_1, ..., X_n]$ ir VFG $\Longrightarrow$ $\exists$ LKD un MKD.

1.2.2. Pakāpes un sakārtojumi

1.3. teorēma. R ir IG.

1. $\forall f \in R[X_1, ..., X_n]$ var viennozīmīgi izteikt homogēnu polinomu summas veidā.
2. $\deg(fg) = \deg(f) + \deg(g)$.
3. $\deg(f + g) \leq \max(\deg(f), \deg(g))$.
4. $\mathrm{mdeg}(fg) = \mathrm{mdeg}(f) + \mathrm{mdeg}(g)$.
5. $\mathrm{mdeg}(f + g) \preceq \max(\mathrm{mdeg}(f), \mathrm{mdeg}(g))$.

PIERĀDĪJUMS
1. Grupēsim locekļus atkarībā no to pakāpēm.

2. Sadalīsim f un g homogēnajās daļās un apskatīsim vecāko termu reizinājumu. Tas nav nulle, jo $R[X_1, ..., X_n]$ ir IG. Tā pakāpe ir $\deg(f) + \deg(g)$.

3. Sadalīsim f un g homogēnajās daļās un apskatīsim to summas.

4. Apskatīsim vecāko termu reizinājumu.

5. Pierādījums līdzīgs viena argumenta polinomiem. ■

1.4. teorēma.

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

PIERĀDĪJUMS

1. $X^{\mu_i} \succ X^{\mu_{i+1}} \implies$ pakāpju vektoram μ_{i+1} vismaz viena koordināte ir mazāka nekā vektoram μ_i. Pakāpju vektoru koordinātes nevar būt negatīvas. Pēc galīga skaita soļiem tiks sasniegts vektors

$(0, ..., 0)$, par kuru mazākam vektoram vismaz viena koordināte ir negatīva $\Longrightarrow$ dilstoša monomu virkne nevar būt bezgalīga.

2. $f_i \succ f_{i+1} \Longrightarrow$ polinomam f_{i+1} vismaz viens monoms ir mazāks nekā polinomam f_i. Pēc galīga skaita soļiem tiks sasniegts polinoms 0, par kuru mazāks polinoms neeksistē $\Longrightarrow$ dilstoša polinomu virkne nevar būt bezgalīga. ■

1.5. teorēma. $f_1, ..., f_m \in R[X_1, .., X_n]$. 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 un g monomi ir sakārtoti dilšanas kārtībā:

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

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

$$\left\{ \begin{array}{l} f_i g_j \succ f_i g_k, \text{ ja } j < k, \\ f_i g_j \succ f_l g_j, \text{ ja } i < l \end{array} \right. \Longrightarrow \mathcal{H}(fg) = f_1 g_1 = \mathcal{H}(f)\mathcal{H}(g).$$

2.solis. Patvaļīgs reizinātāju skaits.
Izmantojam matemātisko indukciju ar parametru m.

Pieņemsim, ka apgalvojums ir spēkā visiem $m < l$. Tad

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

$$\underbrace{\mathcal{H}(f_1) ... \mathcal{H}(f_{m-1})}_{\text{indukcijas pieņēmums}} \mathcal{H}(f_l). \blacksquare$$

2. 6.mājasdarbs

2.1. Obligātie uzdevumi

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

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

6.2 Atrodiet visus termus, kas ir mazāki nekā $X_1^2X_2X_3^2$ VAPG $\mathbb{F}_2[X_1, X_2, X_3]$.

6.3 Sakārtot dotos polinomus dilstošā leksikogrāfiskajā kārtībā, uzskatot, ka $X \succ Y \succ Z$:

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

6.4 Atrodiet visus polinomus, kas ir mazāki nekā $X_1^2 + X_2X_3$ VAPG $\mathbb{F}_2[X_1, X_2, X_3]$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi