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

Studiju kurss

Polinomu algebra

8.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.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.

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

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

$R[X][Y]$ 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:

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

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

Parasti katrā monomā argumentus raksta noteiktā kārtībā.

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

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, to sauc par *multipakāpi.* Šādā pierakstā

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

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

1.2.2. Diskrēti ģeometriskā interpretācija

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

Viena argumenta polinomi -

- koeficientu virknes,
- viendimensionālu nosvērtu vektoru (punktu) kopas.

Divu argumentu polinomi -

- koeficientu tabulas,
- divdimensionālu nosvērtu vektoru (punktu) kopas.

Operāciju interpretācija:

- saskaitīšana - vektoru svaru summēšana,

- reizināšana ar termu aX^μ - nobīde par vektoru μ un svaru reizināšana ar a:

$$aX^\mu \cdot bX^\lambda = (ab)X^{\mu+\lambda},$$

- reizināšana ar polinomu f - reizināšanu ar f termiem rezultātu svaru summēšana.

1.1. piemērs. Reizināšana ar $X + Y$.

1.2.3. Pakāpe

Par monoma $X^\mu = X_1^{i_1}...X_n^{i_n}$ pakāpi $\deg(X^\mu)$, $|\mu|$ sauc tā argumentu pakāpju summu

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

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. $X^2Y + Z^3$ ir homogēns 3.pakāpes polinoms.

1.2.4. Monomu sakārtojums

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

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

Definēsim *monomu leksikogrāfisko sakārtojumu*. Teiksim, ka

$$X^{\mu} \succ X^{\lambda} \rightleftarrows \mu - \lambda = (0, ..., 0, \underbrace{\alpha}_{>0}, \underbrace{...}_{\text{jebkādi}}),$$

kur $\alpha > 0$, locekļi, kas seko pēc α, var būt jebkādi, nulļu virkne var būt arī tukša. Citiem vārdiem, sakot, vektoram $\mu - \lambda$ pirmais nenulles elements no kreisās malas ir pozitīvs.

Definēsim

$$X^{\mu} \asymp X^{\lambda} \leftrightarrows \mu = \lambda.$$

Definēsim

$$X^\mu \succeq X^\lambda \leftrightarrows X^\mu \succ X^\lambda \ \vee \ X^\mu \asymp X^\lambda.$$

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

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

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

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

1.1. teorēma. Leksikogrāfiskais sakārtojums ir monomiālais sakārtojums.

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

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

$$\mu - \lambda = (\underbrace{0, ..., 0}_{s \text{ nulles}}, t, ...),$$

$$\nu - \mu = (\underbrace{0, ..., 0}_{s-r \text{ nulles}}, u, ...),$$

tādējādi $\nu - \lambda = (\underbrace{0, ..., 0}_{s-r \text{ nulles}}, w, ...) \implies X^\lambda \preceq X^\nu$.

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

Reizināšana saglabā kārtību.

$X^\lambda \prec X^\mu \implies \mu - \lambda = (0, ..., 0, t, ...)$. Monomu reizināšana atbilst to pakāpju vektoru saskaitīšanai, tāpēc $X^\lambda X^\nu = X^{\lambda+\nu}$ un $X^\mu X^\nu = X^{\mu+\nu} \implies (\mu+\nu)-(\lambda+\nu) = \mu-\lambda \implies X^\lambda X^\nu \prec X^\mu X^\nu$. ■

Definēsim termu leksikogrāfisko sakārtojumu:

$$aX^\mu \succeq bX^\lambda \rightleftarrows X^\mu \succeq X^\lambda.$$

Polinomus uzdosim sakārtojot termus leksikogrāfiski.

1.5. piemērs. $X \succ Y \succ Z$.

$$\Big(Z^2 - XY + Y^3\Big) \longrightarrow \Big(-XY + Y^3 + Z^2\Big).$$

Par polinoma f *vecāko termu* $\mathcal{H}(f)$ sauksim tā lielāko termu leksikogrāfiskajā sakārtojumā.

Par polinoma f multipakāpi multideg(f) sauc tā vecākā terma multipakāpi.

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$= (1,0,0)$.

1.2.5. Polinomu sakārtojums

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

Monomu un termu leksikogrāfiskais sakārtojums inducē *polinomu leksikogrāfisko 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 $1 \leq i < l$,
- $f_l \succ g_l$.

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

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

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

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.

1.8. 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 $\mathbb{Z}$.

Teiksim, ka 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 Bezū teorēmas analoga.

VAP virs bezgalīga lauka var būt bezgalīgi daudz atrisinājumu.

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

1.3. Pamatfakti

1.3.1. Integralitāte un faktorizācija

1.2. teorēma.

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

PIERĀDĪJUMS Iepriekš tika pierādīti šādi apgalvojumi:

- R ir integrāls gredzens $\Longrightarrow$ $R[X]$ ir integrāls gredzens,
- 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 $\forall\ n < m$.

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 $R[X_1, ..., X_{m-1}]$ tam ir integrāls un VFG saskaņā ar indukcijas pieņēmumu. ■

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

1.3.2. Pakāpes un sakārtojumi

1.3. teorēma. R ir integrāls gredzens.

1. Katru $f \in R[X_1, ..., X_n]$ var vienozīmīgi 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. $\mathrm{mdeg}(f + g) \leq \max(\mathrm{mdeg}(f), \mathrm{mdeg}(g))$.

PIERĀDĪJUMS

1. Grupēsim locekļus atkarībā no to pakāpēm.

2. Sadalīsim f un g homogēnajās daļās un apskatīsim vecāko daļu reizinājumu. Tas nav nulle, jo $R[X_1, ..., X_n]$ ir integrāls gredzens. 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 $a_1X^{\mu_1} \succ a_2X^{\mu_2} \succ \ldots$ 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 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 λ, par kuru mazākam vektoram vismaz viena koordināte ir negatīva, X^λ 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 monoms 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 un g monomi ir sakārtoti dilšanas kārtībā:

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

Tad

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

un

- $f_i g_j \succ f_i g_k$, ja $j < k$,
- $f_i g_j \succ f_l g_j$, ja $i < l$.

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

2.solis. Patvaļīgs reizinātāju skaits.

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

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

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

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

$$I = \langle X_1, X_2 \rangle.$$

Pierādīsim, ka I nav galvenais ideāls. Pieņemsim pretējo: $I = \langle f \rangle \implies X_1 = qf \implies f = uX_1 \implies X_2 \notin I$ - pretruna. ■

1.4. piezīme. Var pierādīt, ka katram ideālam $I \subseteq R[X_1, ..., X_n]$ eksistē galīga ģeneratoru kopa:

$$I = \langle a_1, ..., a_m \rangle.$$

2. 8.mājasdarbs

2.1. Obligātie uzdevumi

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

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

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

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

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

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

8.6 Pierādīt, ka zemāk dotās attiecības ir monomiālie sakārtojumi:

(a) $X^\lambda \lessdot X^\mu \rightleftarrows \Big(|\lambda| < |\mu|\Big) \vee \Big(|\lambda| = |\mu| \wedge \lambda \prec \mu\Big)$ (*graduētais leksikogrāfiskais sakārtojums*, *grlex*),

(b) $X^\lambda \lhd X^\mu \rightleftarrows \Big(|\lambda| < |\mu|\Big) \vee$

$$\Big(|\lambda| = |\mu| \ \wedge \ \mu - \lambda = (..., -t, 0, ..., 0)\Big)$$

(*apgrieztais graduētais leksikogrāfiskais sakārtojums*, *grevlex*).