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

Studiju kurss

Polinomu algebra

9.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt simetrisko polinomu teorijas pamatus.

Lekcijas kopsavilkums:

- var definēt īpaša veida vairāku argumentu polinomus, kas nemainās, ja tajos tiek mainīti argumenti - simetriskos polinomus,
- var definēt vairākas simetrisko polinomu klases - elementāros polinomus, pakāpju polinomus u.c.
- katru simetrisko polinomu var izteikt kā polinomu no elementārajiem polinomiem.

Svarīgākie jēdzieni:

Svarīgākie fakti un metodes:

1. Simetriskie polinomi

Šajā lekcijā apskatīsim polinomus virs lauka k. Teiksim, ka $f \in k[X_1, ..., X_n]$ satur termu aX^μ, $a \neq 0$, ja $f = aX^\mu + ...$

1.1. Definīcijas

1.1.1. Permutācijas

Par kopas A *permutāciju* sauc bijektīvu funkciju

$$\sigma : A \to A.$$

Visu n elementu kopas $\{1, ..., n\}$ permutāciju kopu apzīmē ar Σ_n.

1.1. piezīme. $|\Sigma_n| = n(n-1)(n-2)...2 \cdot 1 = n!$.

Permutācijas var uzdot šādos veidos:

- *attēlu saraksts* - $\sigma \rightsquigarrow (\sigma(1), ..., \sigma(n))$;

- *horizontālais pieraksts* - $\sigma \rightsquigarrow \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$
- *funkcionālais grafs* ar vienu vai diviem kopas eksemplāriem.

Katrā kopā A eksistē tikai viena universāli definēta permutācija - *vienības permutācija* id: $\mathrm{id}(x) = x$.

Kopā Σ_n var definēt *kompozīcijas* operāciju. Ja ir dotas divas permutācijas σ_1 un σ_2, tad to kompozīcija $\sigma_1\sigma_2$ ir definēta ar nosacījumu

$$(\sigma_1\sigma_2)(x) = \sigma_1(\sigma_2(x)), \forall x.$$

$\forall$ permutācijai σ $\exists$ *inversā permutācija* σ^{-1}:

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = \mathrm{id}\,.$$

Permutāciju $\sigma : A \to A$ sauc par *ciklisku attēlojumu* vai *ciklu*, ja

- vai nu $|A| \geq 2$ un A elementus var sakārtot virknē $(a_1,...,a_n)$ tā, ka $\sigma(a_i) = a_{i+1 \text{ mod n}}$,
- vai arī $|A| = 1$ (un kopas A vienīgais elements a apmierina vienādību $\sigma(a) = a$).

1.1. teorēma. (permutācijas sadalījums ciklos) Katrai galīgas kopas A permutācijai σ eksistē viennozīmīgi noteikts A sadalījums apakškopās $A_1, ..., A_m$ tāds, ka $\forall\ i\ \sigma$ sašaurinājums uz A_i ir cikls.

Var definēt permutācijas *ciklisko pierakstu* šādā veidā. Ja

$$A_1 = \{a_{11}, ..., a_{1n_1}\}, ..., A_m = \{a_{m1}, ..., a_{mn_m}\},$$

$$\sigma(a_{11}) = a_{12}, ..., \sigma(a_{1n_1}) = a_{11}, ...$$
$$\sigma(a_{m1}) = a_{m2}, ..., \sigma(a_{mn_m}) = a_{m1},$$

tad $\sigma = (a_{11}a_{12}...a_{1n_1})...(a_{m1}a_{m2}...a_{mn_m})$ (katrs cikls atdalīts ar iekavām). Ciklus ar garumu 1 (*fiksētos punktus*) cikliskajā pierakstā neuzrāda.

1.1. piemērs. Permutāciju $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$ var sadalīt divos ciklos $\{1,5\} \cup \{2,4,3\}$ un apzīmēt kā (15)(243).

Dažas biežāk izmantojamas permutācijas:

- *transpozīcijas* - σ : $\sigma = (ab)$;
- *involūcijas* - σ : $\sigma^2 = \mathrm{id}$.

1.2. piemērs. (12) - transpozīcija. (12)(35)(46) - involūcija, var ievērot, ka cikli ar atdalītām kopām komutē.

1.1.2. Permutāciju grupas darbība polinomu gredzenā

$\forall\, \sigma \in \Sigma_n$ un $\forall\, aX^\mu = aX_1^{\mu_1}...X_n^{\mu_n} \in k[X_1,...,X_n]$ definēsim termu $\sigma \circ (aX^\mu)$ ar šādu nosacījumu:

$$\sigma \circ (aX^\mu) = aX_{\sigma(1)}^{\mu_1},...,X_{\sigma(n)}^{\mu_n}.$$

1.3. piemērs. $(12) \circ (X_1 X_2^4 X_3^5) = X_2 X_1^4 X_3^5 = X_1^4 X_2 X_3^5,$

$\forall\ \sigma \in \Sigma_n$ un $\forall\ f = \sum_\mu a_\mu X_1^{\mu_1} ... X_n^{\mu_n} \in k[X_1, ..., X_n]$ definēsim polinomu $\sigma \circ f$ ar šādu nosacījumu:

$$\sigma \circ f = \sum_\mu \sigma \circ (a_\mu X^\mu) = \sum_\mu a_\mu X_{\sigma(1)}^{\mu_1} ... X_{\sigma(n)}^{\mu_n}.$$

Tādējādi $\forall\ \sigma$ ir definēta *σ-darbības funkcija*

$$T_\sigma : k[X_1, ..., X_n] \to k[X_1, ..., X_n],$$
$$T_\sigma(f) = \sigma \circ f.$$

1.4. piemērs.

$f = X_1 + X_2 X_3 \ \wedge\ \sigma = (23) \implies$

$\sigma \circ f = X_{\sigma(1)} + X_{\sigma(2)} X_{\sigma(3)} = X_1 + X_3 X_2 = X_1 + X_2 X_3 = f.$

$f \in k[X_1, ..., X_n]$ sauksim par *simetrisku polinomu (SP)*, ja

$$\sigma \circ f = f, \forall\ \sigma \in \Sigma_n.$$

Citiem vārdiem sakot, veicot jebkādu argumentu permutāciju, f nemainās, f ir *invariants attiecībā uz grupas* Σ_n *darbību*. Visu SP kopu apzīmēsim ar $k[X_1,,,.,X_n]^S$.

1.5. piemērs. Simetriskie monomi - $a(X_1...X_n)^m$.

Simetriskie polinomi - konstantes, $X_1+X_2, X_1X_2 \in k[X_1,X_2]$, $X^2+XY+Y^2 \in k[X,Y]$.

Nesimetriski polinomi - $X_1^2X_2$, $X+2Y$.

1.1.3. Simetrisko polinomu klases

SP sauksim par *elementāru SP*, ja tas ir izsakāms formā

$$e_m(X_1,X_2,...,X_n) = \sum_{1\le i_1<i_2<...<i_m\le n} X_{i_1}X_{i_2}...X_{i_m}.$$

Definēsim arī $e_0 = 1$. Redzam, ka $m \le n$.

1.6. piemērs. $n=1 \implies e_1(X)=X$.

$n = 2 \implies$

$$\begin{cases} e_1(X_1, X_2) = X_1 + X_2 \\ e_2(X_1, X_2) = X_1 X_2 \end{cases}$$

$n = 3 \implies$

$$\begin{cases} e_1(X_1, X_2, X_3) = X_1 + X_2 + X_3, \\ e_2(X_1, X_2, X_3) = X_1 X_2 + X_1 X_3 + X_2 X_3, \\ e_3(X_1, X_2, X_3) = X_1 X_2 X_3. \end{cases}$$

1.2. piezīme. Atverot iekavas izteiksmei

$$(X - c_1)(X - c_2)...(X - c_n),$$

iegūsim

$$X^n - e_1(c_1, ..., c_n)X^{n-1} + e_2(c_1, ..., c_n)X^{n-2} + ... + (-1)^{n+1} e_n(c_1, ..., c_n).$$

SP sauksim par *pakāpju summu SP*, ja tas ir izsakāms formā

$$p_m(X_1, X_2, ..., X_n) = \sum_{i=1}^{n} X_i^m.$$

Definēsim arī $p_0 = \sum_{i=1}^{n} 1 = n$.

1.7. piemērs. $n = 1 \implies p_m(X) = X^m$.

$n = 3 \implies p_m(X_1, X_2, X_3) = X_1^m + X_2^m + X_3^m$.

Ja $X^\mu = X_1^{\mu_1} ... X_n^{\mu_n}$, tad par μ-*monomiālo SP* m_μ (vai μ-orbītu) sauksim

$$S(X^\mu) = \sum_{\sigma \in \Sigma_n} \sigma \circ X^\mu = \sum_{\sigma \in \Sigma_n} X_{\sigma(1)}^{\mu_1} X_{\sigma(2)}^{\mu_2} ... X_{\sigma(n)}^{\mu_n}.$$

1.8. piemērs. $m_{(2,0)} = S(X_1^2) = S(X_i^2) = (n-1)! \sum_{i=1}^{n} X_i^2$.
$m_{(1,1)} = S(X_1 X_2) = 2(n-1)! \sum_{i<j}^{n} X_i X_j$.
$e_k = c \cdot S(X_1 X_2 ... X_k)$.

1.2. Simetrisko polinomu īpašības

1.2.1. Permutāciju darbības īpašības

Termu $aX^{\mu} = aX^{(\mu_1,\ldots,\mu_n)}$ sauksim par monotonu, ja

$$\mu_1 \geq \ldots \geq \mu_n.$$

1.2. teorēma. aX^{μ} ir monotons $\Longrightarrow \sigma \circ (aX^{\mu}) \preceq aX^{\mu}, \forall\, \sigma.$

PIERĀDĪJUMS Ievērosim, ka termam $\rho \circ (aX^{\mu})$ kāpinātājs pie X_i ir vienāds ar $\mu_{\rho^{-1}(i)}$ - aX^{μ} kāpinātāju pie $X_{\rho^{-1}(i)}$. Šī iemesla dēļ sākotnējo permutāciju ērtāk apzīmēt ar σ^{-1}.

Pieņemsim pretējo: $\exists \sigma^{-1} \in \Sigma_n : \sigma^{-1} \circ (aX^{\mu}) \succ aX^{\mu} \Longrightarrow$

$$\exists\, \sigma : \ (\mu_1, \ldots, \mu_n) \prec (\mu_{\sigma(1)}, \ldots, \mu_{\sigma(n)}) \Longrightarrow$$

$\exists\ i:\ \mu_{\sigma(i)} > \mu_i$ un $\mu_{\sigma(j)} = \mu_j,\ \forall\ j < i$. Tas nav iespējams, jo visi μ_l, kas ir lielāki nekā μ_i, jau ir starp elementiem $\{\mu_{\sigma(1)}, ..., \mu_{\sigma(i-1)}\}$. ■

1.2.2. Simetrisko polinomu struktūra

1.3. teorēma. Simetriska polinoma vecākais terms ir monotons.

PIERĀDĪJUMS Pieņemsim, ka SP f vecākais terms ir

$$\mathcal{H} = aX_1^{\mu_1}...X_i^{\mu_i}X_{i+1}^{\mu_{i+1}}...X_n^{\mu_n},\ \text{kur}\ \mu_i < \mu_{i+1}.$$

f ir SP $\Longrightarrow$ f satur termu $\tau \circ \mathcal{H}$, kur $\tau = (i, i+1)$. Redzam, ka

$$\tau \circ \mathcal{H} = aX_1^{\mu_1}...X_i^{\mu_{i+1}}X_{i+1}^{\mu_i}...X_n^{\mu_n} \succ \mathcal{H} - \text{pretruna.}$$ ■

1.4. teorēma. $\forall$ SP var izteikt monomiālo SP lineāras kombinācijas veidā: $f \in k[X_1, ..., X_n]^S \Longrightarrow f = \sum_\mu c_\mu S(X^\mu)$.

PIERĀDĪJUMS Pietiek pierādīt apgalvojumu homogēnam SP f.

f satur $a_1 X^{\mu_1}$ $\Longrightarrow$ f satur $a_1(\sigma \circ (X^{\mu}))$, $\forall\ \sigma$. Izvēlēsim tādu monomu $X^{\mu_1} = \sigma_1 \circ (X^{\mu})$, kas ir lielākais leksikogrāfiskajā sakārtojumā. Definēsim $f_1 = f - a_1 S(X^{\mu_1})$.

$f_1 \neq 0$ $\Longrightarrow$ f_1 satur vismaz vienu termu $a_2 X^{\mu'}$, kur $X^{\mu'} \prec X^{\mu_1}$ $\Longrightarrow$ f_1 satur $a_2(\sigma \circ (X^{\mu'}))$, $\forall\ \sigma$. Izvēlēsim tādu monomu $X^{\mu_2} = \sigma_2 \circ (X^{\mu'})$, kas ir lielākais leksikogrāfiskajā sakārtojumā. Definēsim $f_2 = f_1 - a_2 S(X^{\mu_2})$.

Turpināsim šo procesu. Tā kā lielākie atlikušie orbītu vecākie termi kļūst stingri mazāki, tad pēc galīga skaita soļiem process apstāsies un iegūsim $f_l = 0$. Seko teorēmas apgalvojums. ■

1.9. piemērs.

$$(X_1 + X_2)(X_1 + X_3)(X_2 + X_3) = X_1^2 X_2 + X_1^2 X_3 + X_1 X_2^2 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2 + 2X_1 X_2 X_2 = S(X_1^2 X_2) + \frac{1}{3} S(X_1 X_2 X_3).$$

1.2.3. Simetriskie polinomi veido apakšgredzenu

1.5. teorēma.

1. $\forall\ n\ k[X_1, ..., X_n]^S$ ir lineāra telpa.
2. $\forall\ n\ k[X_1, ..., X_n]^S$ ir $k[X_1, ..., X_n]$ apakšgredzens.

PIERĀDĪJUMS Jāpierāda, ka divu SP f un g summa un f reizinājums ar g ir SP:

$$\sigma \circ (f + g) = \sigma \circ f + \sigma \circ g = f + g, \forall \sigma,$$

$$\sigma \circ (fg) = (\sigma \circ f)(\sigma \circ g) = fg, \forall \sigma. \blacksquare$$

1.3. Simetrisko polinomu pamatteorēma

1.6. teorēma. $\forall\ f \in k[X_1, ..., X_n]^S$ var viennozīmīgi izteikt formā

$$f(X_1, ..., X_n) = g(e_1, ..., e_n), \text{ kur } g \in k[Y_1, ..., Y_n].$$

PIERĀDĪJUMS $\forall$ SP f ir homogēnu SP summa $\Longrightarrow$ pietiek pierādīt apgalvojumu, ja f ir homogēns SP.

1.solis Eksistence un algoritms.
Pierādīsim, ka $\forall\ f \in k[X_1, ..., X_n]^S\ \exists\ g \in k[Y_1, ..., Y_n]$ tāds, ka

$$f(X_1, ..., X_n) = g\Big(e_1(X_1, ..., X_n), ..., e_n(X_1, ..., X_n)\Big).$$

Pamatideja - sākot ar f veiksim "redukcijas" atņemot polinomus formā $ae_1^{\gamma_1}...e_n^{\gamma_n}$ tā, lai katra šāda "redukcija" samazinātu vecāko termu. Izrādās, ka tas vienmēr ir iespējams. Beigās iegūsim 0, tātad f ir izsakāms kā $ae_1^{\gamma_1}...e_n^{\gamma_n}$ tipa polinomu summa.

Pieņemsim, ka $\mathcal{H}(f) = aX_1^{\mu_1}...X_n^{\mu_n},$ kur $\mu_i \geq \mu_{i+1}$.

Definēsim pirmo "redukciju":

$$f_1 = f - ae_1^{\mu_1-\mu_2}e_2^{\mu_2-\mu_3}...e_n^{\mu_n} \in k[X_1, ..., X_n]^S.$$

Pierādīsim, ka $\mathcal{H}(f) \succ \mathcal{H}(f_1)$. Redzam, ka saskaņā ar vecākā terma multiplikativitātes īpašību

$$\mathcal{H}(ae_1^{\mu_1-\mu_2}e_2^{\mu_2-\mu_3}...e_n^{\mu_n}) = a\mathcal{H}(e_1^{\mu_1-\mu_2})\mathcal{H}(e_2^{\mu_2-\mu_3})...\mathcal{H}(e_n^{\mu_n}) =$$
$$a\mathcal{H}(e_1)^{\mu_1-\mu_2}\mathcal{H}(e_2)^{\mu_2-\mu_3}...\mathcal{H}(e_n)^{\mu_n} =$$
$$aX_1^{\mu_1-\mu_2}(X_1X_2)^{\mu_2-\mu_3}...(X_1...X_n)^{\mu_n} = aX_1^{\mu_1}X_2^{\mu_2}...X_n^{\mu_n} = \mathcal{H}(f).$$

Seko, ka $f_1 = f - ae_1^{\mu_1-\mu_2}e_2^{\mu_2-\mu_3}...e_n^{\mu_n}$ vecākie termi saīsinās un $\mathcal{H}(f) \succ \mathcal{H}(f_1)$.

Pieņemsim, ka $\mathcal{H}(f_1) = bX_1^{\nu_1}...X_n^{\nu_n}$, kur $\nu_i \geq \nu_{i+1}$.

Definēsim otro "redukciju":

$$f_2 = f_1 - be_1^{\nu_1-\nu_2}e_2^{\nu_2-\nu_3}...e_n^{\nu_n}.$$

Spriežot līdzīgi, iegūsim, ka $\mathcal{H}(f) \succ \mathcal{H}(f_1) \succ \mathcal{H}(f_2)$.

Turpinot, pēc galīga skaita soļiem iegūsim SP $f_l = 0$, tāpēc

$$f = ae_1^{\mu_1-\mu_2}...e_n^{\mu_n} + be_1^{\nu_1-\nu_2}...e_n^{\nu_n} + ... = g(e_1, ..., e_n) \in k[e_1, ..., e_n].$$

2.solis Vienīgums.
Pieņemsim, ka $\exists$ divi polinomi $g_1, g_2 \in k[Y_1, ..., Y_n]$ tādi, ka

$$f = g_1(e_1, ..., e_n) = g_2(e_1, ..., e_n) \implies$$

$$\widehat{g} = g_1 - g_2 \neq 0 \text{ kā polinoms.}$$

No otras puses, ievietojot $\widehat{g}$ argumentu vietā e_i, iegūsim, ka

$$\widehat{g}\Big(e_1(X_1, ..., X_n), ..., e_n(X_1, ..., X_n)\Big) = 0.$$

Katram $\widehat{g}$ monomam $aY_1^{\lambda_1} ... Y_n^{\lambda_n}$, $a \neq 0$, izpildās

$$\mathcal{H}(ae_1^{\lambda_1} e_2^{\lambda_2} ... e_n^{\lambda_n}) = aX_1^{\lambda_1}(X_1X_2)^{\lambda_2} ... (X_1X_2...X_n)^{\lambda_n} = aX_1^{\lambda_1 + ... \lambda_n} X_2^{\lambda_2 + ... + \lambda_n} ... X_n^{\lambda_n}.$$

Funkcija

$$(\lambda_1, ..., \lambda_n) \mapsto (\lambda_1 + ... + \lambda_n, \lambda_2 + ... + \lambda_n, ..., \lambda_n)$$

ir injektīva $\Longrightarrow$ dažādu $\widehat{g}(Y)$ monomu vecākie termi pēc e_i ievietošanas nevar saīsināties $\Longrightarrow$ $\mathcal{H}(\widehat{g}(e)) \neq 0$ $\Longrightarrow$ $\widehat{g}(e) \neq 0$ - pretruna. ■

1.4. Algoritmi SP izteikšanai ar elementāro SP palīdzību

SP izteikšanu ar elementāro SP palīdzību sauksim par tā *elementarizāciju*.

1.4.1. Teorēmas algoritms

Var izmantot algoritmu, kas ir dots teorēmas pierādījumā.

1.10. piemērs. Elementarizēsim $f = X_1^4 + X_2^4$:

1. $f \to f_1 = f - e_1^4 = -4X_1^3X_2 - 6X_1^2X_2^2 - 4X_1X_2^3$.
2. $f_1 \to f_2 = f_1 + 4e_1^2e_2 = 2X_1^2X_2^2$.
3. $f_2 \to f_3 = f_2 - 2e_2^2$.

$\Longrightarrow$ $f = e_1^4 - 4e_1^2 e_2 + 2e_2^2.$

1.4.2. Nenoteikto koeficientu metode

Ja $\alpha = (\alpha_1, ..., \alpha_n)$ ir pakāpju vektors, tad apzīmēsim

$$E(\alpha) = e_1^{\alpha_1} e_2^{\alpha_2} ... e_n^{\alpha_n}.$$

Katram $m \in \mathbb{N}$ visu vienādojuma

$$1 \cdot \alpha_1 + 2 \cdot \alpha_2 + ... + n \cdot \alpha_n = m$$

atrisinājumu kopu apzīmēsim ar $\mathcal{T}_m$.

Algoritmu var paātrināt šādā veidā:

1. Izteikt f kā homogēnu SP summu $f_1 + ... + f_d$.
2. $\forall$ f_i meklējam formā

$$f_i = \sum_{\tau \in \mathcal{T}_i} c_\tau E(\tau),$$

   kur koeficienti c_τ tiek atrasti liekot X_i vietā konkrētus mazus veselus skaitļu, parasti $0, \pm 1, \pm 2, ...$.

1.11. piemērs. Elementarizēsim $X_1^5 + X_2^5 \in \mathbb{Q}[X_1, X_2]$. Tas ir homogēns un vienāds ar $S(X_1^5)$. Elementarizācija ir jāmeklē formā

$$X_1^5 + X_2^5 = e_1^5 + ae_1^3e_2 + be_1e_2^2, \text{ kur } a, b \text{ - nezināmi.}$$

$$(X_1, X_2) = (1, 1) \Longrightarrow 2 = 2^5 + a \cdot 2^3 + b \cdot 2.$$
$$(X_1, X_2) = (1, 2) \Longrightarrow 1 + 2^5 = 3^5 + a \cdot 3^3 \cdot 2 + b \cdot 3 \cdot 2^2.$$

Iegūsim sistēmu

$$\begin{cases} 4a + b = -15 \\ 9a + 2b = -35 \end{cases} \Longrightarrow (a, b) = (-5, 5) \Longrightarrow$$

$$X_1^5 + X_2^5 = e_1^4 - 5e_1^3e_2 + 5e_1e_2^2.$$

2. 9.mājasdarbs

2.1. Obligātie uzdevumi

9.1 Pierādīt, ka jebkuru permutāciju var izteikt kā transpozīciju kompozīciju.

9.2 σ ir permutācija ar zināmu sadalījumu ciklos, τ ir transpozīcija. Kāds var būt sadalījums ciklos permutācijai $\tau \circ \sigma$?

9.3 Izteikt SP

$$(X_1X_2 + X_3X_4)(X_1X_3 + X_2X_4)(X_1X_4 + X_2X_3)$$

formā $\sum_\mu c_\mu S(X^\mu)$.

9.4 Izteikt dotos SP izmantojot elementāros SP:

(a) $X_1^3 + X_2^3$;
(b) $X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$;
(c) $(X_1X_2 + X_3)(X_1X_3 + X_2)(X_2X_3 + X_1)$;
(d) $\left[\prod_{i<j\le n}(X_i - X_j)\right]^2$, ja $n \in \{2, 3\}$.

9.5 c_1, c_2, c_3 ir vienādojuma

$$X^3 + 2X^2 + 3X + 4 = 0$$

saknes. Aprēķiniet $\frac{1}{c_1^2} + \frac{1}{c_2^2} + \frac{1}{c_3^2}$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

9.6 Piedāvājiet algoritmus SP izteikšanai

(a) ar pakāpju summu SP palīdzību,

(b) ar pilno homogēno SP palīdzību.