DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Jauno matemātiķu skola

Vairāku argumentu polinomu algebra

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt vairāku argumentu polinomu (VAP) teorijas pamatfaktus.

Lekcijas kopsavilkums:

- vairāku argumentu polinomiem piemīt īpašības analoģiskas viena argumentu polinomu gadījumam,
- var pētīt speciāla veida polinomus, kas nemainās mainot vietām argumentus - simetriskos polinomus.

Svarīgākie jēdzieni: n-argumentu polinoms, VAP monoms, VAP terms, monoma multipakāpe, VAP pakāpe un multipakāpe, VAP vecākais terms, homogēns VAP, monomu leksikogrāfiskais sakārtojums, VAP leksikogrāfiskais sakārtojums, VAP atrisinājumi, reducijas solis, permutācija, permutācijas sadalījums ciklos, simetrisks polinoms (SP), elementārs SP,

Svarīgākie fakti un metodes: VAP pakāpes, multipakāpes un integralitātes īpašības, redukcijas soļa īpašības, divu VAP dalīšana ar atlikumu, VAP dalīšana ar vairākiem VAP, SP īpašības, SP pamatteorēma, elementarizācijas algoritms.

1. Vairāku argumentu polinomi

1.1. Definīcijas

1.1.1. Polinomu gredzeni

Ir dots skaitļu gredzens R ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ vai $\mathbb{C}$).

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 $R[X,Y]$.

Atkārtojot 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 $\mu = (i_1, i_2, ..., i_n)$ sauc par *multipakāpi*. Šādā pierakstā

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

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

1.1.2. 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.

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

1.1.3. Monomu sakārtojums

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

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

Definēsim *monomu leksikogrāfisko sakārtojumu*. Teiksim, ka

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

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

Definēsim

$$X^{\mu} \asymp X^{\lambda} \overset{Def}{\Longleftrightarrow} \mu = \lambda.$$

Definēsim

$$X^\mu \succeq X^\lambda \overset{Def}{\Longleftrightarrow} X^\mu \succ X^\lambda \ \vee \ X^\mu \asymp X^\lambda.$$

1.3. piemērs. $X_1 \succ X_2 \succ X_3 \succ ... \succ X_n$, $X_1 X_2 \succ X_2^5$.

Definēsim termu leksikogrāfisko sakārtojumu:

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

Polinomus parasti uzdosim sakārtojot termus leksikogrāfiski dilstošā.

1.4. 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 $\mathrm{multideg}(f)$ sauc tā vecākā terma multipakāpi.

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

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

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

1.1.5. 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 dalītāju, to sauc par nedalāmu.

1.7. piemērs. $X+Y|X^4+Y^4 \bmod 2$, jo

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

$X^2+XY+2Y^2|X^4+Y^4 \bmod 3$, 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.

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

1.2. Pamatfakti

Gredzenu sauc par integrālu gredzenu, ja tajā nav *nulles dalītāju*:

$$ab = 0 \implies a = 0 \text{ vai } b = 0.$$

Visas skaitļu kopas ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) ir integrāli gredzeni.

1.2.1. Integralitāte un faktorizācija

1.1. teorēma.

1. R ir integrāls gredzens $\implies$ $R[X_1, ..., X_n]$ ir integrāls gredzens.
2. R ir VFG (viennozīmīgās faktorizācijas gredzens) $\implies$ $R[X_1, ..., X_n]$ ir VFG.

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

1.2.2. Pakāpes un sakārtojumi

1.2. teorēma. R ir integrāls gredzens (piemēram, skaitļu gredzens $\mathbb{Z}$, $\mathbb{Q}$ vai $\mathbb{R}$).

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

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. ■

1.3. 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.

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

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

2. Vairāku argumentu polinomu dalīšana ar atlikumu

Sākot no šīs sadaļas $R = \mathbb{Q}$, $\mathbb{R}$ vai $\mathbb{C}$.

2.1. Redukcija

Doti VAP $f, g \in k[X_1, ..., X_n]$. Ja kāds f monoms aX^μ dalās ar $\mathcal{H}(g)$, tad pārveidojumu

$$f \to f - \frac{aX^\mu}{\mathcal{H}(g)} g = \tilde{f}$$

sauksim par *redukcijas soli* un apzīmēsim ar

$$f \xrightarrow{g} \tilde{f}.$$

2.1. piemērs. $f = X_1^2 X_2 + X_2^2$, $g = X_1 X_2 - 1$.
$\tilde{f} = f - X_1 g = X_1 + X_2^2$.

2.1. teorēma.

1. Redukcijas solis

$$f \to f - \frac{aX^\mu}{\mathcal{H}(g)} g = \tilde{f}$$

samazina polinomu leksikogrāfiskajā sakārtojumā:

$$f \succ \tilde{f}.$$

2. Ja $\mathcal{H}(g)|\mathcal{H}(f)$, tad redukcijas solis

$$f \to f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} g = \tilde{f}$$

samazina polinoma vecāko termu:

$$\mathcal{H}(f) \succ \mathcal{H}(\tilde{f}).$$

PIERĀDĪJUMS

1. Redzam, ka $\mathcal{H}(f - \tilde{f}) \prec aX^\mu$, jo aX^μ saīsinās.

2. Seko no 1. ■

2.2. Viens dalītājs

Ja ir doti divi VAP f un g, tad var vispārināt viena argumenta polinomu dalīšanas procedūru, ko var pamatot divos veidos:

- var atņemt no dalāmā f dalītāja g daudzkārtņus tā, lai atlikums būtu pēc iespējas mazāks leksikogrāfiskajā sakārtojumā;
- var veikt maksimāli garu f redukcijas soļu virkni ar g.

Dabiski ir izvēlēties šādu algoritmu: katrā solī veikt redukciju ar lielāko f termu, kas dalās ar $\mathcal{H}(g)$.

2.2. 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

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

2.2. teorēma. Ja $f, g \in k[X_1, ..., X_n]$ ir nenulles polinomi, tad eksistē viennozīmīgi noteikts polinomu pāris (d, r), kuram izpildās nosacījumi

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

2.3. Vairāki dalītāji

Dots viens dalāmais f un vairāki dalītāji $g_1, ..., g_m$. Var veikt vairākus redukcijas soļus, iespējams, ar dažādiem dalītājiem, katrs redukcijas solis samazina atlikumu, tāpēc redukcijas process apstāsies pēc galīga soļu skaita.

2.3. 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. $f = d_1g_1 + d_2g_2 + ... + d_mg_m + r$;
2. $r = 0$ vai neviens r terms nedalās ar $\mathcal{H}(g_i)$ katram i.

PIERĀDĪJUMS

Veiksim redukcijas soļus formā $r_t \to r_t + c_ig_i$, izvēloties lielāko r_t termu un mazāko i.

Algoritms.

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

$$\begin{cases} r_t = f, \\ d_{1t} = d_{2t} = ... = d_{mt} = 0. \end{cases}$$

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

$$\begin{cases} r_t := r_t - \frac{a_\mu X^\mu}{\mathcal{H}(g_i)} g_i, \\ d_{it} := d_{it} + \frac{a_\mu X^\mu}{\mathcal{H}(g_i)}. \end{cases}$$

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

Algoritma darba rezultātā iegūtais r_t ir vienāds ar r, $d_i = d_{it}$ un

$$r_t = f - (d_1 g_1 + ... + d_m g_m) = r.$$

Algoritms apstāsies pēc galīga skaita soļu izpildes, jo pēc katra A tipa soļa izpildes r_t samazinās leksikogrāfiskajā sakārtojumā. ■

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

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

1. $\begin{cases} r_t := f - X^2 g_2 = -X^2Y + Y^4 \\ d_{1t} = 0 \text{ (nemainās)} \\ d_{2t} = X^2 \end{cases}$

2. $\begin{cases} r_t := f_t - (-X)g_1 = X + Y^4 \\ d_{1t} = -X \\ d_{2t} = X^2 \text{ (nemainās)} \end{cases}$

Jāapstājas, jo X un Y^4 nedalās ne ar XY, ne ar X^2.

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:

$$X^4+Y^4 = (X^2-Y)(X^2+Y) + 0\cdot(XY+1) + \underbrace{(Y^4+Y^2)}_{=r}.$$

2.1. piezīme. Dalīšanas rezultāts ir atkarīgs no dalītāju kārtības.

2.2. piezīme. Polinoma dalīšana ar sakārtotu dalītāju virkni ir redukcijas speciālgadījums.

3. 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 $f = aX^\mu + ...$

3.1. Definīcijas

3.1.1. Permutācijas

Par kopas A *permutāciju* sauc bijektīvu funkciju

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

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

3.1. 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* - $\sigma \rightsquigarrow \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$
- *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

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

Katrai permutācijai σ eksistē *inversā permutācija* σ^{-1}, kas ir definēta ar nosacījumu

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

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 $\sigma(a_i) = a_{i+1 \bmod n}$,
- vai arī $|A| = 1$ (un kopas A vienīgais elements a apmierina vienādību $\sigma(a) = a$).

3.1. teorēma. (permutācijas sadalījums ciklos) Katrai galīgas kopas A permutācijai σ eksistē viennozīmīgi noteikts A sadalījums apakškopās $A_1, ..., A_m$ tāds, ka $\forall\ i$ σ 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.

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

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

3.1.2. Permutāciju grupas darbība polinomu gredzenā

$f \in k[X_1, ..., X_n]$ sauksim par *simetrisku polinomu (SP)*, ja veicot jebkādu argumentu permutāciju, f nemainās. Visu SP kopu apzīmēsim ar $k[X_1, , , ., X_n]^S$.

3.3. 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 - $X_1^2X_2$, $X + 2Y$.

3.1.3. Elementārie simetriskie polinomi

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 $m \le n$.

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

$$n = 2 \implies \begin{cases} e_1(X_1, X_2) = X_1 + X_2 \\ e_2(X_1, X_2) = X_1X_2 \end{cases}$$

$$n = 3 \implies \begin{cases} e_1(X_1, X_2, X_3) = X_1 + X_2 + X_3, \\ e_2(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3, \\ e_3(X_1, X_2, X_3) = X_1X_2X_3. \end{cases}$$

3.2. piezīme. Atverot iekavas izteiksmei

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

iegūsim

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

3.2. Simetrisko polinomu īpašības

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

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

3.2. teorēma. Simetriska polinoma vecākais terms ir monotons.

3.3. teorēma.

1. $\forall\ n\ k[X_1, ..., X_n]^S$ ir slēgta attiecībā uz saskaitīšanu un reizināšanu ar skaitļiem.
2. $\forall\ n\ k[X_1, ..., X_n]^S$ ir slēgta sttiecībā uz reizināšanu.

3.4. teorēma. (simetrisko polinomu pamatteorēma) $\forall\ f \in k[X_1, ..., X_n]^S$ 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

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

3.3. piezīme. Ir pierādīts, ka $k[X_1, ..., X_n]^S = k[e_1, ..., e_n]$.

3.4. piezīme. Simetrisko polinomu pamatteorēmu izmanto vienādojumu sistēmu un nevienādību risināšanā.

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

Var izmantot algoritmu, kas ir dots teorēmas pierādījumā.

3.5. 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. $f_2 \to f_3 = f_2 - 2e_2^2$.

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

4. 7.mājasdarbs

4.1. Obligātie uzdevumi

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

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

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

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

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

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

7.5 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) $\left[\prod_{i<j\leq n}(X_i - X_j)\right]^2$, ja $n \in \{2, 3\}$.

7.6 c_1, c_2, c_3 ir vienādojuma

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

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