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

Studiju kurss

Polinomu algebra

5.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

Lekcijas mērķis - apgūt pamatfaktus par polinomu faktorizāciju virs $\mathbb{R}$ un $\mathbb{C}$.

1. Faktorizācija virs $\mathbb{C}$ un $\mathbb{R}$

1.1. $\mathbb{C}$ algebriskās īpašības

Lauku k sauksim par *algebriski slēgtu*, ja katrs polinoms $f \in k[X]$ sadalās lineāros reizinātājos. Citiem vārdiem sakot, tikai lineārie polinomi ir nedalāmi gredzenā $k[X]$.

1.1. piemērs. $\mathbb{R}$ nav algebriski slēgts, jo polinoms x^2+1 ir nedalāms.
Katram pirmskaitlim p lauks $\mathbb{F}_p$ nav algebriski slēgts.

1.1. teorēma. (*algebras pamatteorēma*) $\mathbb{C}$ ir algebriski slēgts lauks.

PIERĀDĪJUMS Aprakstīsim tikai pierādījuma galvenos soļus un palīgrezultātus.

Palīgrezultāti no matemātiskās analīzes.

A Ja $f : \mathbb{C} \to \mathbb{C}$ ir polinomiāla funkcija, tad f ir nepārtraukta.

B Ja $g : \mathbb{C} \to \mathbb{R}$ ir nepārtraukta funkcija, tad tā pieņem savu minimālo vērtību katrā ierobežotā slēgtā $\mathbb{C}$ apakškopā.

C Ja $f : \mathbb{C} \to \mathbb{C}$ ir polinomiāla funkcija, tad eksistē $r \in \mathbb{R}$ tāds, ka

$$|f(z)| > |f(0)|$$

visiem $z : |z| > r$.

D Ja $f : \mathbb{C} \to \mathbb{C}$ ir polinomiāla funkcija, tad eksistē $z_0 \in \mathbb{C}$, kurā $|f(z)|$ pieņem savu minimālo vērtību.

E Ja $f : \mathbb{C} \to \mathbb{C}$ ir nekonstanta polinomiāla funkcija un $|f(u)| \neq 0$, tad eksistē $t \in \mathbb{C}$ tāds, ka

$$|f(t)| < |f(u)|.$$

Pierādījuma kopsavilkums.

Pieņemsim, ka $f \in \mathbb{C}[X]$. Saskaņā ar palīgrezultātu **D** eksistē $z_0 \in \mathbb{C}$, kurā $|f(z)|$ pieņem minimālo vērtību:

$$|f(z_0)| \leq |f(z)| \text{ visiem } z \in \mathbb{C}.$$

Ja $|f(z_0)| \neq 0$, tad saskaņā ar palīgrezultātu **E** eksistē $w_0 \in \mathbb{C}$ tāds, ka

$$|f(w_0)| < |f(z_0)|,$$

kas ir pretruna.

■

1.2. piemērs. Sadalīt reizinātājos polinomu $X^3 - 1$.

1.2. Polinomu faktorizācija virs $\mathbb{R}$

1.2. teorēma. Polinomu gredzena $\mathbb{R}[X]$ nedalāma elementa pakāpe nepārsniedz 2.

PIERĀDĪJUMS Tā kā $\mathbb{R} \subset \mathbb{C}$, tad polinomu $f \in \mathbb{R}[X]$ var uzskatīt par elementu gredzenā $\mathbb{C}[X]$.

Pieņemsim, ka polinoms f ir sadalīts lineāros reizinātājos virs $\mathbb{C}$:

$$f(X) = u(X - z_1)...(X - z_n).$$

Ja $z \in \mathcal{V}(f)$, tad $f(z) = 0$ un $\overline{f(z)} = 0$. Tā kā f koeficienti ir reāli skaitļi, tad

$$\overline{f} = f$$

un

$$\overline{f(z)} = \overline{f}(\overline{z}) = f(\overline{z}) = 0.$$

Redzam, ka $\overline{z} \in \mathcal{V}(f)$. Tādējādi, ja $\mathcal{V}(f)$ satur kompleksu sakni z, tad tā satur arī pāri $\{z, \overline{z}\}$.

Esam ieguvuši šādu f sakņu kopas aprakstu:

$$\mathcal{V}(f) = \{ \underbrace{a_1, ..., a_k}_{\text{reālās saknes}} , \underbrace{z_1, \overline{z_1}, ..., z_l, \overline{z_l}}_{\text{kompleksās saknes}} \}$$

Mēģināsim apvienot kompleksos lineāros reizinātājus tā, lai iegūtu polinomus ar reāliem koeficientiem. Ievērosim, ka

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} \in \mathbb{R}[X]$$

ir nedalāms elements polinomu gredzenā $\mathbb{R}[X]$, jo tam nav reālu sakņu.

Apvienojot visus kompleksi saistītos pārus, iegūsim $f \in \mathbb{R}[X]$ sadalījumu nedalāmos reizinātājos, kas ir noteikts viennozīmīgi:

$$f(X) = (X - a_1)^{\alpha_1} ... (X - a_k)^{\alpha_k} (X^2 + p_1 X + q_1)^{\beta_1} ... (X^2 + p_l X + q_l)^{\beta_l}.$$

Tā kā f bija patvaļīgs, tad secinām, ka nedalāmi polinomi gredzenā $\mathbb{R}[X]$ var ar pakāpi 0, 1 vai 2.

■

2. Faktorizācija virs $\mathbb{Z}$ un $\mathbb{Q}$

Tika minēts fakts bez pierādījuma - $\mathbb{Z}[X]$ ir VFG.

Tika definēts polinoma saturs - koeficientu LKD. Tika minēts fakts - satura multiplikatīvā īpašība.

2.1. Faktorizācijas virs $\mathbb{Z}$ un $\mathbb{Q}$ ir ekvivalentas

2.1. teorēma. Polinoms $f \in \mathbb{Z}[X]$ ir nedalāms virs $\mathbb{Z}$ tad un tikai tad, ja tas ir nedalāms virs $\mathbb{Q}$.

PIERĀDĪJUMS Ja f ir dalāms virs $\mathbb{Z}$, tad tas ir dalāms virs $\mathbb{Q}$.

Ja f ir nedalāms virs $\mathbb{Z}$, tad pieņemsim, ka tas ir dalāms virs $\mathbb{Q}$:

$$f = gh,$$

kur $g, h \in \mathbb{Q}[X]$. Tā kā f ir nedalāms, tad $cont(f) = 1$.

Reizināsim katru no polinomiem g un h ar atbilstošiem veseliem skaitļiem (kopsaucējiem) tā, lai tie pārvērstos par primitīviem polinomiem virs $\mathbb{Z}$:

- Polinomu g reizinām ar tādu veselu skaitli n, lai $g_1 = ng \in \mathbb{Z}[X]$,
- g_1 izdalām ar $cont(g_1)$, iegūstam primitīvu polinomu

$$g_2 = \frac{1}{cont(g_1)} g_1 \in \mathbb{Z}[X],$$

- to pašu varam izdarīt ar h - h reizinām ar tādu veselu skaitli m, lai $h_1 = mh \in \mathbb{Z}[X]$,
- h_1 izdalām ar $cont(h_1)$, iegūstam primitīvu polinomu $h_2 \in \mathbb{Z}[X]$.

Redzam, ka

$$g_2 h_2 = \frac{\alpha}{\beta} gh = \frac{\alpha}{\beta} f,$$

kur $\alpha, \beta \in \mathbb{Z}$. Citiem vārdiem sakot,

$$\alpha f = \beta g_2 h_2.$$

Izmantojot satura multiplikativitāti, redzam, ka

$$cont(\alpha f) = cont(\alpha) \cdot 1 = cont(\alpha) = cont(\beta g_2 h_2) = cont(\beta) \cdot 1 \cdot 1 = cont(\beta).$$

Esam ieguvuši, ka $\alpha = \pm\beta$. Seko, ka

$$f = \pm g_2 h_2,$$

kas ir pretrunā ar pieņēmumu, ka f ir nedalāms. ■

2.2. Factorizācija mod p un tās pielietojumi

Ja ir dots polinoms

$$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X],$$

tad ir lietderīgi pētīt tā *redukciju* $\overline{f}$ *mod* p kur p ir pirmskaitlis:

$$\overline{f}(X) = \sum_{i=0}^{n} (a_i \bmod p) X^i \in \mathbb{Z}[X],$$

2.2. teorēma. Ja $f \in \mathbb{Z}$ ir dalāms polinoms un $f = gh$, tad katram pirmskaitlim p polinoms $\overline{f} \in \mathbb{F}_p[X]$ ir izsakāms veidā $\overline{f} = \overline{g}\overline{h}$.

PIERĀDĪJUMS Seko no tā, ka redukcija mod p ir gredzenu homomorfizms $\mathbb{Z} \to \mathbb{F}_p$. Jāpārbauda labās un kreisās puses koeficientu vienādība. ■

2.1. piezīme. No teorēmas seko, ka ja f ir dalāms normalizēts polinoms (vecākais koeficients ir vienāds ar 1), tad tas ir dalāms katram p.

2.3. teorēma. (Eizenšteina kritērijs) Pieņemsim, ka

$$f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X],$$

kuram eksistē pirmskaitlis p ar šādām īpašībām:

- $p \nmid a_n$.
- ja $k \neq n$, tad $p | a_k$,
- $p^2 \nmid a_0$.

Tad f ir nedalāms virs $\mathbb{Z}$.

PIERĀDĪJUMS Reducējot mod p, iegūsim, ka

$$\overline{f}(X) \equiv X^n (\text{mod } p).$$

Ja

$$f(X) = g(X)h(X)$$

gredzenā $Z[X]$, tad

$$\overline{f}(X) = \overline{g}(X)\overline{h}(X)$$

gredzenā $\mathbb{F}_p[X]$. Redzam, ka

$$\overline{g}(X) = X^k,$$
$$\overline{h}(X) = X^{n-k}.$$

Seko, ka

$$g_0 \equiv 0 (\text{mod } p),$$
$$h_0 \equiv 0 (\text{mod } p),$$

tātad $a_0 = g_0 h_0 \equiv 0 (\text{mod } p^2)$ - pretruna.

■

2.1. piemērs. Polinoms $X^4 - 3X^2 + 6X - 3 \in \mathbb{Z}[X]$ ir nedalāms, jo visi koeficienti, izņemot vecāko, dalās ar 3, bet brīvais loceklis nedalās ar $3^2 = 9$.

3. Faktorizācijas algoritmi

3.1. Precīzās formulas polinomu saknēm, kuru pakāpe nepārsniedz 4

3.1.1. $deg(f) = 2$

Dots polinoms $f(X) = X^2+aX+b \in \mathbb{C}[X]$. Risināsim vienādojumu

$$X^2 + aX + b = 0.$$

1.solis - lineārā substitūcija.
Veiksim substitūciju

$$X \to Y = X + u$$

un pārveidosim vienādojumu:

$$(Y - u)^2 + a(Y - u) + b =$$

$$Y^2 + (-2u + a)Y + (u^2 - au + b) = 0$$

Redzam, ka ņemot $u = \frac{a}{2}$, iegūsim vienādojumu formā

$$Y^2 + p = 0.$$

2.solis - kvadrātsaknes atrašana un pāreja uz sākotnējo nezināmo.

Redzam, ka

$$Y = \sqrt{-p}.$$

Ja tiek fiksēta kāda konkrēta $\sqrt{-p}$ vērtība, tad ir divas saknes: $\sqrt{-p}$ un $-\sqrt{-p}$.

Atrodam X pēc formulas $X = Y - \frac{a}{2}$.

3.1.2. $deg(f) = 3$ (del Ferro-Tartaglia-Cardano formulas)

Dots polinoms $f(X) = X^3 + aX^2 + bX + c \in \mathbb{C}[X]$. Risināsim vienādojumu

$$X^3 + aX^2 + bX + c = 0.$$

1.solis - lineārā substitūcija.
Veiksim substitūciju

$$X \to Y = X + u$$

un pārveidosim vienādojumu:

$$(Y-u)^3 + a(Y-u)^2 + b(Y-u) + c =$$
$$Y^3 + (-3u+a)Y^2 + (3u^2 - 2au + b)Y + (-u^3 + au^2 - bu + c) = 0$$

Redzam, ka ņemot $u = \frac{a}{3}$, iegūsim vienādojumu formā

$$Y^3 + pY + q = 0.$$

2.solis - brīva parametra ieviešana.
Meklēsim Y formā

$$Y = \alpha + \beta,$$

ievietosim vienādojumā un iegūsim

$$(\alpha+\beta)^3 + p(\alpha+\beta) + q = (\alpha+\beta)(3\alpha\beta+p) + (\alpha^3+\beta^3+q) = 0.$$

3.solis - brīvības izmantošana redukcijai uz kvadrātvienādojumu.

Izmantojot brīvību, kas radās ieviešot vienu brīvības pakāpi, varam pieprasīt, ka izpildās vienādība

$$3\alpha\beta + p = 0.$$

Attiecībā uz α un β iegūsim sistēmu

$$\begin{cases} \alpha\beta = -\frac{p}{3} \\ \alpha^3 + \beta^3 = -q. \end{cases}$$

vai sekojošu sistēmu (ar, iespējams, lielāku atrisinājumu kopu)

$$\begin{cases} \alpha^3\beta^3 = -\frac{p^3}{27} \\ \alpha^3 + \beta^3 = -q. \end{cases}$$

4.solis - sākotnējo nezināmo atrašana.
Atrisināsim sistēmu attiecībā uz α un β:

$$\begin{cases} \alpha^3 = \frac{-q+\sqrt{q^2+\frac{4p^3}{27}}}{2} \\ \beta^3 = \frac{-q+\sqrt{q^2-\frac{4p^3}{27}}}{2}. \end{cases}$$

Redzam, ka

$$Y = \alpha + \beta = \sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}} + \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2}}.$$

Kuba saknes ir jāizvēlas tā, lai izpildītos nosacījums

$$\alpha\beta = -\frac{p^3}{27}.$$

Kompleksajiem skaitļiem eksistē trīs kuba saknes, tā kā šķiet, ka vajadzētu rasties deviņām saknēm. Īstenībā ir trīs atrisinājumi.

3.1.3. $deg(f) = 4$ (Ferrari-Euler formulas)

1.solis - lineārā substitūcija.

Dots polinoms $f(X) = X^4 + aX^3 + bX^2 + cX + d \in \mathbb{C}[X]$. Risināsim vienādojumu

$$X^4 + aX^3 + bX^2 + cX + d = 0.$$

Veiksim substitūciju

$$X \to Y = X + u$$

un pārveidosim vienādojumu:

$$\begin{aligned}(Y-u)^3 4 + a(Y-u)^3 + b(Y-u)^2 + c(Y-u) + d = \\ Y^4 + (-4u+a)Y^3 + (-3au + b + 6u^2)Y^2 + \\ (3au^2 - 2bu - 4u^3 + c)Y + (u^4 + d - cu - au^3 + bu^2) = 0\end{aligned}$$

Redzam, ka ņemot $u = \frac{a}{4}$, iegūsim vienādojumu formā

$$Y^4 + pY^2 + qY + r = 0.$$

2.solis - brīvo parametru ieviešana.
Meklēsim Y formā

$$Y = \alpha + \beta + \gamma,$$

ievietosim vienādojumā un iegūsim

$$4(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + (\alpha^2 + \beta^2 + \gamma^2)^2 + p(\alpha^2 + \beta^2 + \gamma^2) + r +$$
$$(\alpha\beta + \alpha\gamma + \beta\gamma)(4(\alpha^2 + \beta^2 + \gamma^2) + 2p) + (\alpha + \beta + \gamma)(8\alpha\beta\gamma + q) = 0.$$

3.solis - brīvības izmantošana redukcijai uz kubisko vienādojumu.

Izmantojot brīvību, kas radās ieviešot divas brīvības pakāpi, varam pieprasīt, ka izpildās sistēma ar diviem nosacījumiem:

$$\begin{cases} \alpha^2+\beta^2+\gamma^2=-\frac{p}{2} \\ \alpha\beta\gamma=-\frac{q}{8}. \end{cases}$$

Ja sistēma izpildās, tad vienādojums vienkāršojas:

$$\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2=\frac{p^2-4r}{16}.$$

Attiecībā uz α, β un γ esam ieguvuši sistēmu

$$\begin{cases} \alpha^2+\beta^2+\gamma^2=-\frac{p}{2} \\ \alpha\beta\gamma=-\frac{q}{8} \\ \alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2=\frac{p^2-4r}{16} \end{cases}$$

vai sekojošu sistēmu (ar, iespējams, lielāku atrisinājumu kopu)

$$\begin{cases} \alpha^2+\beta^2+\gamma^2 = -\frac{p}{2} \\ \alpha^2\beta^2\gamma^2 = \frac{q}{64} \\ \alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2 = \frac{p^2-4r}{16}. \end{cases}$$

Palīgrezultāts - Vieta formulas kubiskajiem vienādojumiem.

$$f = X^3 + a_2X^2 + a_1X + a_0 = (X-z_1)(X-z_2)(X-z_3),$$

tad un tikai tad, ja

$$a_2 = -(z_1+z_2+z_3),$$
$$a_1 = z_1z_2 + z_1z_3 + z_2z_3,$$
$$a_0 = -z_1z_2z_3$$

No iegūtās sistēmas attiecībā uz $\alpha^2, \beta^2, \gamma^2$ seko, ka tie ir kubiskā vienādojuma

$$Z^3 + \frac{p}{2}Z^2 + \frac{p^2 - 4r}{16}Z - \frac{q}{64} = 0$$

saknes.

4.solis - sākotnējo nezināmo atrašana.
Atrisināsim iegūto kubisko vienādojumu.
Atradīsim α, β, γ tā, lai izpildītos sākotnējais nosacījums

$$\alpha\beta\gamma = -\frac{q}{8}.$$

4. 5.mājasdarbs

4.1. Obligātie uzdevumi

5.1 Dots, ka polinoms $f \in \mathbb{Q}[X]$ ir nedalāms. Pierādīt, ka vienādojumam

$$f(z) = 0$$

nav vairākkārtīgu kompleksu sakņu.

5.2 Pierādiet, ka dotie polinomi ir nedalāmi virs $\mathbb{Z}$:

(a) $X^4 - 10X^3 + 6X^2 - 12X + 6$,
(b) $X^3 + 18X^2 - 12X - 6$,
(c) $X^{15} - 9$.

5.3 Atrodiet visus polinomus $f \in \mathbb{C}[X]$, kas apmierina funkcionālo vienādojumu

$$f(X^2) + f(X)f(X+1) = 0.$$

4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.4 Nosakiet, vai zemāk dotie polinomi ir dalāmi:

(a) $X^n \pm X \pm 1 \in \mathbb{Z}[X]$,

(b) $X^n + tX \pm 1 \in \mathbb{Z}[X]$, ja $|t| \geq 3$,

(c) $X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Z}[X]$, kur p ir pirmskaitlis.