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

Studiju kurss

Polinomu algebra

4.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

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

1. Pamatfakti par $\mathbb{C}$

1.1. Motivācijas

1.1.1. Algebra

Algebriskā motivācija - reālo skaitļu kopā $\mathbb{R}$ nevar atrisināt pat tādu vienkāršu algebrisku vienādojumu kā

$$x^2 + 1 = 0,$$

tāpēc ir vēlams paplašināt gredzenu $\mathbb{R}$ līdz kādam lielākam gredzenam, kurā šādi vienādojumi būtu atrisināmi.

1.1.2. Ģeometrija

Ģeometriskā motivācija - reālo skaitļu kopa atbilst taisnes punktiem, bet taisne atrodas plaknē, tāpēc vēlams paplašināt $\mathbb{R}$ tā, lai lielākā gredzena elementi atbilstu plaknes punktiem.

Izrādās, ka abas motivācijas var apmierināt vienlaicīgi.

1.2. Paplašinājuma modeļi

1.2.1. 1.modelis - komplekso skaitļu plakne

Apskatīsim plakni ar Dekarta koordinātu sistēmu. Tā kā katram plaknes punktam var savstarpēji viennozīmīgi piekārtot tā Dekarta koordinātes - reālu skaitļu pāri, tad plakne identificēt ar $\mathbb{R}$ Dekarta kvadrātu

$$\mathbb{R}^2 = \{(x, y) | x \in \mathbb{R}, y \in \mathbb{R}\}.$$

Definēsim divas bināras operācijas kopā $\mathbb{R}^2$ šādā veidā:

- $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ (vektoru saskaitīšana),
- $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$ (kaut kas jauns).

Var pārbaudīt, ka $(\mathbb{R}^2, +, \cdot)$ ir lauks, kurā 0 ir elements $(0, 0)$ un 1 ir elements $(1, 0)$. Šo lauku apzīmē ar $\mathbb{C}$ un sauc par *komplekso skaitļu lauku*.

Elementi formā $(x, 0)$ veido apakšgredzenu, kas ir izomorfs ar $\mathbb{R}$. Elementu $(x, 0)$ identificēsim ar x. Tādējādi $\mathbb{C}$ var uzskatīt par $\mathbb{R}$ paplašinājumu, kas apmierina ģeometrisko motivāciju - $\mathbb{R} < \mathbb{C}$.

Var redzēt, ka elements $i = (0, 1)$ apmierina vienādojumu

$$x^2 + 1 = 0.$$

Redzam, ka

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1)(y, 0) = x + iy,$$

šo pierakstu parasti arī izmanto.

1.2.2. 2.modelis - antisimetriskās matricas

Apzīmēsim ar $\mathcal{C}$ reālo antisimetrisko 2×2 matricu kopu, kuras elementi ir formā

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Matricām ir definēta saskaitīšana un reizināšana.

Var pārbaudīt, ka $(\mathcal{C}, +, \cdot)$ ir lauks, kurā 0 ir nulles matrica

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

un 1 ir vienības matrica

$$E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

$\mathcal{C}$ satur apakšgredzenu $\mathcal{R}$, kura elementi ir matricas formā

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

Tādējādi, var uzskatīt, ka $\mathcal{C}$ ir $\mathbb{R}$ paplašinājums.

Ievērosim, ka matrica

$$I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

apmierina matricu vienādojumu

$$I^2 + E_2 = 0.$$

Tādējādi $\mathcal{C}$ var interpretēt kā $\mathbb{R}$ paplašinājumu, kas apmierina vienu no motivācijām.

1.3. Pamatfakti

1.3.1. Aritmētiskās operācijas

Komplekso skaitļu operācijas ir definētas sādā veidā:

- $(x_1 + iy_1) \pm (x_2 + iy_1) = (x_1 + x_2) \pm i(y_1 + y_2)$,
- $(x_1 + iy_1) \cdot (x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)$,
- $$\frac{x_1 + iy_1}{x_2 + iy_2} = \frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2} + i\frac{x_2y_1 - x_1y_2}{x_2^2 + y_2^2}$$

Ja $z = x + iy$, tad $x = \mathcal{R}e(z)$, $y = \mathcal{I}m(z)$, $\bar{z} = x - iy$ (*kompleksi saistītais skaitlis*). Redzam, ka $z\bar{z} = x^2 + y^2 = |z|^2 \geq 0$. Redzam, ka $|z| = 0 \Leftrightarrow z = 0$.

Komplekso skaitļu kopā nav dabiska reālo skaitļu salīdzināšanas $\leq$ (pilna sakārtojuma) analoga.

1.3.2. Polārie parametri un trigonometriskā forma

Par $z = x + iy$ *moduli* sauc lielumu $|z| = r = \sqrt{x^2 + y^2}$.

Par $z = x + iy$ *argumentu* $\arg(z)$ sauc saistītās polārās sistēmas koordināti φ, kas apmierina sakarības

$$\begin{cases} x = r\cos\varphi \\ y = r\sin\varphi. \end{cases}$$

Redzam, ka

$$z = r\cos\varphi + ir\sin\varphi = r(\cos\varphi + i\sin\varphi)$$

(kompleksā skaitļa *trigonometriskā forma*).

Redzam, ka $\arg(z)$ ir noteikts ar precizitāti līdz 2π daudzkārtnim.

1.3.3. Īpašības

1.1. teorēma. Kompleksajiem skaitļiem izpildās šādas īpašības:

1. $|z_1 + z_2| \leq |z_1| + |z_2|$,
2. $|z_1 z_2| = |z_1||z_2|$,
3. $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$,
4. $$|\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|},$$
5. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ un $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ (kompleksā saistīšana ir gredzenu homomorfizms),
6. ja $f \in \mathbb{C}[X]$, tad $\overline{f(z)} = \overline{f}(\overline{z})$, kur $\overline{f}$ ir polinoms ar kompleksi saistītiem koeficientiem salīdzinājumā ar f.

PIERĀDĪJUMS Tieša pārbaude. ■

1.1. piezīme. No teorēmas seko *Muavra formula*:

$$\Big(r(\cos\varphi + i\sin\varphi)\Big)^n = r^n(\cos n\varphi + i\sin n\varphi).$$

1.2. piezīme. No teorēmas seko n-tās kārtas saknes aprēķināšanas formula. Ja

$$z = r(\cos\varphi + i\sin\varphi),$$
$$w = \rho(\cos\psi + i\sin\psi)$$

un $w^n = z$, tad

$$\begin{cases} \rho^n = r \\ n \cdot \psi = \varphi. \end{cases}$$

Tādējādi

$$\begin{cases} \rho = \sqrt[n]{r} \\ \psi = \frac{\varphi + 2\pi k}{n}. \end{cases}$$

Dažādas ψ vērtības iegūsim, ja k vietā liksim visu atlikumu klašu mod n pārstāvjus, piemēram, kopas $\{0, ..., n-1\}$ elementus.

Apkopojot iegūstam šādu rezultātu:

$$\sqrt[n]{z} = \sqrt[n]{|z|}\Big(\cos(\frac{\varphi + 2\pi k}{n}) + i\sin(\frac{\varphi + 2\pi k}{n})\Big)$$

1.3.4. Eksponenciālā forma

Eksponentfunkciju var vispārināt uz $\mathbb{C}$ - definēt funkciju $f(z) = e^z$ ar šādām īpašībām:

- ja $z \in \mathbb{R}$, tad funkcija sakrīt ar klasisko eksponentfunkciju,
- $e^{z_1+z_2} = e^{z_1}e^{z_2}$,
- $e^{z_1 z_2} = (e^{z_1})^{z_2}$.

Var pierādīt *Eilera formulu*:

$$e^{i\varphi} = \cos\varphi + i\sin\varphi,$$

kur $\varphi \in \mathbb{R}$.

Kompleksos skaitļus var uzdot *eksponenciālajā formā*

$$z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}$$

.

1.4. $\mathbb{C}$ algebriskais slēgtums

Lauku k sauksim par *algebriski slēgtu*, ja katrs polinoms $f \in k[X]$ sadalās lineāros reizinātājos.

Citas ekvivalentas definīcijas:

- tikai lineārie polinomi ir nedalāmi gredzenā $k[X]$;
- katram polinomam $f \in k[X]$ ir vismaz viena sakne;
- katram polinomam $f \in k[X]$ sakņu multiplicitāšu skaits ir vienāds ar $\deg(f)$.

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.

1.2. 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.

■

2. Polinomu faktorizācija virs $\mathbb{C}$ un $\mathbb{R}$

2.1. Faktorizācija virs $\mathbb{C}$

2.1. teorēma. (*algebras pamatteorēma*) Tā kā $\mathbb{C}$ ir algebriski slēgts lauks, tad katrs $f \in \mathbb{C}[X]$ sadalās lineāros reizinātājos.

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

2.2. Faktorizācija virs $\mathbb{R}$

2.2. 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 $\mathbb{C}$:

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

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 (ja būtu reālas saknes, tas būtu pretrunā ar to $\mathbb{C}[X]$ ir VFG).

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

$$f(X) = (X-a_1)^{\alpha_1}...(X-a_k)^{\alpha_k}(X^2+p_1X+q_1)^{\beta_1}...(X^2+p_lX+q_l)^{\beta_l}.$$

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

■

2.2. piemērs. Sadalīt nedalāmos reizinātājos X^6-1 virs $\mathbb{R}$. Redzam, ka

$$X^6-1 = (X^2-1)(X^4+X^2+1) = (X-1)(X+1)\underbrace{(X^4+X^2+1)}_{\text{grūti}} =$$

$$(X^3-1)(X^3+1) = (X-1)(X+1)(X^2+X+1)(X^2-X+1).$$

2.3. Precīzās formulas polinomu saknēm, kuru pakāpe nepārsniedz 4

2.3.1. $\deg(f) = 3$ (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 sakarība starp α un β - 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

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

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

2.3.2. $\deg(f) = 4$ (Ferrari-Euler formulas) (neobligātā patstāvīgā lasīšana)

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

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

1.solis - lineārā substitūcija.
Veiksim substitūciju

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

un pārveidosim vienādojumu:

$$(Y-u)^4 + a(Y-u)^3 + b(Y-u)^2 + c(Y-u) + d =$$
$$Y^4 + (-4u+a)Y^3 + (-3au+b+6u^2)Y^2 +$$
$$(3au^2 - 2bu - 4u^3 + c)Y + (u^4 + d - cu - au^3 + bu^2) = 0$$

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 pakāpes, 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

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

3. 4.mājasdarbs

3.1. Obligātie uzdevumi

4.1 Attēlojiet kompleksajā plaknē apgabalu, kas apmierina nosacījumu

$$|z - i| < 1.$$

4.2 Atrisiniet kompleksajos skaitļos vienādojumu

$$z^4 + 4 = 0.$$

4.3 Sadaliet nedalāmajos reizinātājos polinomu $X^8 - 1$ virs $\mathbb{C}$ un virs $\mathbb{R}$.

4.4 Izmantojot Kardano formulas atrisiniet kompleksos skaitļos vienādojumu

$$X^3 + 12X^2 + 45X + 50 = 0.$$

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

4.5 Atrodiet $LKD(X^m + 1, X^n + 1)$ virs $\mathbb{C}$, kur $m, n \in \mathbb{N}$.