DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Jauno matemātiķu skola

Viena argumenta polinomu algebra

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt viena argumenta polinomu teorijas pamatfaktus.

Lekcijas kopsavilkums:

- polinomiem ir spēkā vairāki veselo skaitļu īpašību analogi,
- polinomu sadalīšana reizinātājos ir grūta problēma.

Svarīgākie jēdzieni: polinoma koeficienti, locekļi, vecākais loceklis, pakāpe, polinomu dalāmība, nedalāms polinoms, polinoma saknes - vienkāršās un vairākkārtīgās, polinoma atvasinājums, kompleksie skaitļi,operācijas ar kompleksiem skaitļiem, komplekso skaitļu ģeometriskā interpretācija, komplekso skaitļu ģeometriskā forma.

Svarīgākie fakti un metodes: polinoma pakāpes īpašības, polinomu dalīšana ar atlikumu, polinomu viennozīmīgās faktorizācijas īpašība, Bezout teorēma, polinomu Lagranža interpolācijas formula, polinoma atvasinājuma īpašības, vairākkārtīgās saknes kritērijs, polinoma kvadrātbrīvās faktorizācijas atrašana, komplekso skaitļu īpašības, komplekso skaitļu algebriskais slēgtums, nedalāmie polinomi virs $\mathbb{R}$ un $\mathbb{C}$, faktorizācijas īpašības virs $\mathbb{Z}$ un $\mathbb{Q}$, faktorizācija mod p, Eizenšteina kritērijs.

1. Viena argumenta polinomi

1.1. Pamatdefinīcijas

Viena argumenta polinomus mēs rakstīsim formā

$$a_0 + a_1 X + a_2 X^2 + ... + a_n X^n.$$

Locekļu kārtība nav svarīga (komutativitātes dēļ), to izvēlēsimies tā, lai būtu ērtāk strādāt.

Visu viena argumenta polinomu kopu ar koeficientiem kādā kopā R apzīmēsim ar $R[X]$. R var būt $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ (skaitļu *gredzens*).

Polinomu kopā ir definētas šādas operācijas:

- saskaitīšana,
- reizināšana,
- kompozīcija.

Simbola X vietā var lietot jebkuru citu simbolu: $R[X] \simeq R[Y]$ visiem simboliem X,Y.

Gredzena elementus a_i sauc par polinoma *koeficientiem*.

Polinomus formā aX^m sauksim par *locekļiem (termiem)*.

Polinomus formā X^m sauksim par *monomiem*.

Polinoma koeficientu a_0 sauc par *brīvo locekli*.

Polinoma f locekli aX^m, $a \neq 0$, ar lielāko pakāpi m sauc par *vecāko locekli*, apzīmē ar $\mathcal{H}(f)$, a sauc par *vecāko koeficientu*, m sauc par polinoma *pakāpi* $\deg(f)$.

1.1. piemērs. $f = -3X^2 + 10X - 4$, $\mathcal{H}(f) = -3X^2$, $\deg(f) = 2$.

Nulles polinomam $0 = (0, 0, ...)$ pakāpi definē vienādu ar $-\infty$ (vai nedefinē vispār).

Ja $\deg(f) = 0, (1, 2, 3)$, tad f ir *konstants (lineārs, kvadrātisks, kubisks)* polinoms.

Divi polinomi ir vienādi tad un tikai tad, ja tiem ir vienādi koeficienti pie visām argumenta pakāpēm.

1.1. teorēma. Ja $f, g \in R[X]$, tad ir spēkā šādi apgalvojumi:

1. $\deg(f + g) \leq \max(\deg(f), \deg(g))$;
2. $\deg(fg) = \deg(f) + \deg(g)$;

PIERĀDĪJUMS

1. Divu polinomu summas vecākā koeficienta indekss nevar būt lielāks nekā lielākā no polinomu pakāpēm (var būt mazāks, ja koeficienti pie dažiem monomiem saīsinās).

2. Atsevišķi apskatām gadījumu, kad viens no polinomiem ir 0. Šādā gadījuma apgalvojums ir spēkā.

Pieņemsim, ka neviens no polinomiem nav 0. Polinomu reizinājuma vecākais koeficients ir polinomu vecāko koeficientu reizinājums. Ja

$$f = f_n X^n + ...,$$
$$g = g_m X^m + ...,$$

tad

$$fg = (f_n X^n + ...)(g_m X^m + ...) = (f_n g_m) X^{n+m} + ...$$

Ja R ir skaitļu gredzens, tad $f_n g_m \neq 0$ un

$$\deg(fg) = n + m = \deg(f) + \deg(g).$$

1.1.1. Dalāmība

Saka, ka $f \in R[X]$ dalās ar $g \in R[X]$ (apzīmē ar $g|f$), ja $\exists h \in R[X]$ tāds, ka $f = hg$.

1.2. piemērs. Ja $n \geq m$, tad $X^m | X^n$.

Dalāmības īpašības - līdzīgas veselo skaitļu dalāmības īpašībām.

Polinu f sauc par *nedalāmu polinomu*, ja tas nav izsakāms formā $f = gh$, kur g un h ir nekonstanti polinomi vai veseli skaitļi atšķirīgi no ± 1.

1.1.2. Dalīšana ar atlikumu

R ir skaitļu gredzens, $f, g \in R[X]$, $\deg(f) \geq \deg(g)$ un g vecākais koeficients ir invertējams. Definēsim

$$\mathcal{R}(f,g) = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} g.$$

(f *redukcija ar* g)

1.2. teorēma. $\deg\Big(\mathcal{R}(f,g)\Big) < \deg(f)$.

PIERĀDĪJUMS Pieņemsim, ka $\mathcal{H}(f) = a_n X^n$, $\mathcal{H}(g) = b_m X^m$, kur $n \geq m$.

Ievērosim, ka $\frac{\mathcal{H}(f)}{\mathcal{H}(g)}$ ir polinoms $\frac{a_n}{b_m} X^{n-m}$.

Redzam, ka

$$\mathcal{H}(\mathcal{R}(f,g)) = \mathcal{H}\Big[f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)}g\Big] = \mathcal{H}\Big[f - \frac{a_n X^n}{b_m X^m}g\Big] =$$

$$\mathcal{H}\Big[f - \frac{a_n}{b_m}X^{n-m}(b_m X^m + ...)\Big] = \mathcal{H}(\underbrace{a_n X^n + ...}_{=f} - a_n X^n - ...).$$

Redzam, ka locekļi ar X^n saīsinās, tāpēc apgalvojums ir spēkā. ■

1.3. piemērs. $f = X^5 + X^2 + 1$, $g = X^2 + X + 1$ virs $\mathbb{Z}$. Veiksim vairākas redukcijas pēctecīgi:

1.

$$f \to f_1 = \mathcal{R}(f,g) = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} \cdot g = f - X^3 \cdot g = -X^4 - X^3 + X^2 + 1;$$

2.

$$f_1 \to f_2 = \mathcal{R}^2(f,g) = \mathcal{R}(f_1,g) = f_1 - (-X^2) \cdot g = 2X^2 + 1;$$

$$f_2 \to f_3 = \mathcal{R}^3(f,g) = \mathcal{R}(f_2,g) = f_2 - 2 \cdot g = -2X - 1;$$

Redzam, ka $\mathcal{R}^4(f,g)$ nav definēts, jo deg $\Big(\mathcal{R}^3(f,g)\Big) < \deg(g)$.

Rezultātā iegūsim, ka f var izteikt summas veidā, kurā viens locekļis ir g daudzkārtnis, bet otra locekļa pakāpe ir mazāka nekā $\deg(g)$:

$$\begin{aligned} f = X^3g + f_1 = X^3g + (-X^2)g + f_2 = \\ = X^3g + (-X^2)g + 2g + (-2X - 1) = \\ = (X^3 - X^2 + 2)g + (-2X - 1). \end{aligned}$$

Izdalot šos pašus polinomus virs $\mathbb{F}_2$ (atlikumi mod 2) iegūsim

$$X^5 + X^2 + 1 = (X^3 + X^2)(X^2 + X + 1) + 1.$$

1.3. teorēma. (*viena argumenta polinomu dalīšana ar atlikumu*) Ja R ir skaitļu gredzens, $f, g \in R[X]$ un g vecākais koeficients ir invertējams, tad eksistē tieši viens polinomu pāris $q, r \in R[X]$:

1. $f = qg + r$,
2. $\deg(r) < \deg(g)$.

PIERĀDĪJUMS Pieņemsim, ka

$$f = a_n X^n + ... + a_0,$$
$$g = b_m X^m + ... + b_0,$$

kur $a_n, b_m \neq 0$ un b_m^{-1} eksistē.

q un r eksistence.

1.apakšgadījums. Ja $m > n$, tad definēsim

$$q = 0, r = f.$$

2.apakšgadījums. Ja $m \leq n$, tad izmantosim matemātisko indukciju ar indukcijas parametru $\deg(f)$.

Indukcijas bāze. Ja $n = 0$, tad definēsim

$$q = \frac{a_n}{b_m}, r = 0.$$

Indukcijas solis. Pieņemsim, ka (q, r) eksistences apgalvojums ir

spēkā, ja $\deg(f) < n$ un pierādīsim, ka tad tas ir spēkā, ja $\deg(f) = n$.

Atradīsim $\mathcal{R}(f,g) = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)}g$. Apzīmēsim $\frac{\mathcal{H}(f)}{\mathcal{H}(g)}$ ar q_0.

Redzam, ka

$$f = q_0 g + \mathcal{R}(f,g),$$

kur $\deg(\mathcal{R}(f,g)) < n = \deg(f)$.

Saskaņā ar indukcijas pieņēmumu eksistē polinomi q_1, r_1 tādi, ka

$$\mathcal{R}(f,g) = q_1 g + r_1, \text{ kur } \deg(r_1) < \deg(g) = m.$$

Tagad redzam, ka

$$f = q_0 g + \mathcal{R}(f,g) = q_0 g + (q_1 g + r_1) = (q_0 + q_1)g + r_1.$$

Varam definēt $q = q_0 + q_1$ un $r = r_1$.

q un r vienīgums.

Pieņemsim, ka eksistē divi polinomu pāri $(q, r), (q', r')$ tādi, ka

$$f = qg + r = q'g + r'.$$

Tas nozīmē, ka $(q - q')g = r' - r$.

Zināms, ka $\deg(r' - r) < \deg(g)$.

No otras puses, $\deg\Big((q - q')g\Big) = \deg(q - q') + \deg(g)$. Tā kā

$$\deg\Big((q - q')g\Big) = \deg(q - q') + \deg(g) < \deg(g),$$

tad $\deg(q - q') = -\infty \implies \begin{cases} q = q', \\ r = r'. \end{cases}$ ■

1.2. Polinomu faktorizācija

1.2.1. Pamatfaktu kopsavilkums

1.4. teorēma.

1. Ja $R = \mathbb{Z}, \mathbb{Q}$ vai $\mathbb{R}$, tad ir spēkā aritmētikas pamatteorēmas analogs: $\forall\ f \in R[X]$ ir viennozīmīgi izsakāms nedalāmu polinomu pakāpju reizinājuma formā.
2. Ja $R = \mathbb{Z}, \mathbb{Q}$ vai $\mathbb{R}$, tad ir definēts polinomu kopas LKD un MKD.
3. Ja $R = \mathbb{Q}$ vai $\mathbb{R}$, tad ir Eiklīda algoritma analogs ar visām sekām (LKD aprēķināšana, lineārās kombinācijas īpašība u.t.t)

1.3. Polinomu saknes

1.3.1. Vienkāršās saknes - Bezout teorēma

Teiksim, ka $a \in R$ ir nekonstanta polinoma $f \in R[X]$ *sakne*, ja $f(a) = 0$.

Polinoma f sakņu kopu apzīmēsim ar $\mathcal{V}(f)$.

1.5. teorēma. $\forall\ f, g \in R[X]$ izpildās

$$\mathcal{V}(fg) = \mathcal{V}(f) \cup \mathcal{V}(g).$$

PIERĀDĪJUMS

$\underline{\mathcal{V}(f) \cup \mathcal{V}(g) \overset{?}{\subseteq} \mathcal{V}(fg).}$

$f(a) = 0 \vee g(a) = 0 \implies f(a)g(a) = 0 \implies (fg)(a) = 0 \implies a \in \mathcal{V}(fg).$

$\underline{\mathcal{V}(fg) \overset{?}{\subseteq} \mathcal{V}(f) \cup \mathcal{V}(g).}$

$(fg)(a) = f(a)g(a) = 0 \implies f(a) = 0 \vee g(a) = 0$, jo R ir integrāls gredzens. ■

1.6. teorēma. *(Bezout)* $a \in \mathcal{V}(f) \iff (X - a) | f(X)$.

PIERĀDĪJUMS Izdalīsim $f(X)$ ar $X - a$:

$$f(X) = q(X)(X - a) + r(X), \text{ kur } \deg\Big(r(X)\Big) < \deg(X - a) = 1.$$

Redzam, ka $\deg\Big(r(X)\Big) = 0$ vai $r(X) = 0 \implies r(X) = r_0$ - konstants polinoms.

Atradīsim r_0. Veicot substitūciju $X = a$, iegūstam

$$f(a) = q(a)(a-a) + r_0 \implies r_0 = f(a) \implies$$

$$f(X) = q(X)(X-a) + f(a).$$

$$f(a) = 0 \iff f(X) = q(X)(X-a) \iff (X-a)|f(X). \blacksquare$$

1.1. piezīme. No Bezout teorēmas seko, ka kvadrātisks vai kubisks polinoms f virs lauks k ir nedalāms tad un tikai tad, ja $\mathcal{V}(f) = \emptyset$.

1.3.2. Vairākkārtīgās saknes

Teiksim, ka $a \in R$ ir nekonstanta polinoma $f \in R[X]$ *k-kārtīga sakne*, ja

$$(X-a)^k | f(X) \text{ un } (X-a)^{k+1} \nmid f(X).$$

Citiem vārdiem sakot

$$f(X) = (X-a)^k g(X), \text{ kur } LKD\Big(g(X), X-a\Big) = 1.$$

1.7. teorēma. Ja dažādi $a_1, ..., a_m$ ir polinoma $f(X) \in R[X]$ saknes ar kārtām $k_1, ..., k_m$, tad

$$f(X) = (X - a_1)^{k_1} ... (X - a_m)^{k_m} g(X),$$

kur $g(a_i) \neq 0$ visiem $1 \leq i \leq m$.

PIERĀDĪJUMS Izmantosim matemātisko indukciju ar indukcijas parametru m.

Indukcijas bāze.

Ja $m = 1$, tad apgalvojums seko no vairākkārtīgas saknes definīcijas.

Indukcijas solis.

Pieņemsim,ka apgalvojums ir spēkā, ja sakņu skaits ir vienāds vai mazāks kā $m - 1$ un pierādīsim, ka tas ir spēkā, ja sakņu skaits ir vienāds ar m.

Tātad

$$f(X) = (X - a_1)^{k_1} ... (X - a_{m-1})^{k_{m-1}} h(X).$$

Tā kā $a_m \neq a_i$, $1 \leq i \leq m-1$, tad $h(a_m) = 0$, tādējādi

$$f(X) = (X - a_1)^{k_1} ... (X - a_{m-1})^{k_{m-1}} (X - a_m)^u g(X),$$

kur $g(a_m) \neq 0$. Tā kā m ir k_m-kārtīga sakne, tad $u = k_m$. ■

1.2. piezīme. Nekonstanta polinoma sakņu kārtu summa nevar pārsniegt polinoma pakāpi.

1.3.3. Polinomu interpolācija

1.8. teorēma. Ja divi polinomi f un g ar pakāpi n pieņem vienādas vērtības pēc $n+1$ substitūcijas ar dažādiem elementiem $a_1, ..., a_{n+1}$, tad tie ir vienādi.

PIERĀDĪJUMS Ja $h = f - g$, tad

$$\deg(h) \leq \max(\deg(f), \deg(g)) = n.$$

Pēc pieņēmuma

$$h(a_1) = f(a_1) - g(a_1) = 0,$$
$$..., h(a_{n+1}) = f(a_{n+1}) - g(a_{n+1}) = 0,$$

tātad polinomam h ir vismaz $n+1$ dažādas saknes $a_1, ..., a_{n+1}$ - pretruna, ja h nav vienāds ar 0. ■

1.3. piezīme. Polinomu ar pakāpi n var viennozīmīgi noteikt (atrast tā koeficientus), ja ir zināmas tā vērtības $n+1$ punktos.

1.9. teorēma. (*Lagranža interpolācijas formula*) k ir $\mathbb{Q}$ vai $\mathbb{R}$. Ja ir doti $n+1$ dažādi k elementi $a_0, ..., a_n$ un $n+1$ k elementi $b_0, ..., b_n$, tad eksistē tieši viens polinoms $f(X) \in k[X]$ tāds, ka

$$f(a_i) = b_i \text{ visiem } 0 \leq i \leq n.$$

Polinoms f var tikt atrasts pēc šādas formulas:

$$f(X) = \sum_{i=0}^{n} b_i \frac{(X-a_0)...(X-a_{i-1})(X-a_{i+1})...(X-a_n)}{(a_i-a_0)...(a_i-a_{i-1})(a_i-a_{i+1})...(a_i-a_n)} =$$

$$\sum_{i=0}^{n} b_i \prod_{j \neq i} \frac{X-a_j}{a_i-a_j}.$$

PIERĀDĪJUMS

Vienīgums.

Seko no iepriekšējas teorēmas.

Eksistence.

Jāveic formulas tieša pārbaude. ■

1.4. Polinomu atvasināšana un tās pielietojumi faktorizācijā

1.4.1. Pamatfakti

Par polinoma

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

(formālo) atvasinājumu sauksim polinomu

$$f'(X) = \sum_{i=1}^{n} a_i i X^{i-1} \in R[X].$$

1.4. piemērs. $(a_0 + a_1 X)' = a_1$.

$(X^p)' = 0$ gredzenā $\mathbb{F}_p[X]$.

1.10. teorēma.

1. $(af + bg)' = af' + bg'$,
2. $(fg)' = f'g + fg'$,
3. $(f^n)' = nf^{n-1}f'$.

1.4.2. Vairākkārtīgās saknes kritērijs

1.11. teorēma. k - lauks, $f \in k[X]$. Polinomam

$$f(X) \in k[X]$$

$a \in \mathcal{V}(f)$ ir vairākkārtīga sakne $\iff \begin{cases} f(a) = 0 \\ f'(a) = 0 \end{cases}$.

PIERĀDĪJUMS
Izdalīsim $f(X)$ ar $(X-a)^2$:

$$f(X) = q(X)(X-a)^2 + r(X), \text{ kur } \deg\Big(r(X)\Big) < 2.$$

$r(X)$ izdalīsim ar $(X-a)$:

$$r(X) = q_1 \cdot (X-a) + r_1, \text{ kur } \deg(r_1) < 1.$$

Apvienojot abus rezultātus vienā vienādībā, iegūsim

$$f(X) = q(X)(X-a)^2 + q_1 \cdot (X-a) + r_1.$$

Ievērosim, ka

$$f'(X) = (q(X)(X-a)^2 + q_1 \cdot (X-a) + r_1)' = \\ = q'(X)(X-a)^2 + q(X) \cdot 2(X-a) + q_1.$$

Ja elements $a \in K$ ir vairākkārtīga sakne, tad $f(a) = 0$ un $f'(a) = 0$.

Ja elements $a \in K$ ir vairākkārtīga sakne, tad

$$f(X) = q(X)(X-a)^2,$$

tātad $q_1 = 0$ un $r_1 = 0$. Redzam, ka $f(a) = 0$ un $f'(a) = 0$.

Ja $f(a) = 0$ un $f'(a) = 0$, tad elements $a \in K$ ir vairākkārtīga sakne.

Ja $f(a) = 0$ un $f'(a) = 0$, tad $q_1 = 0$ un $r_1 = 0$. Tātad

$$f(X) = q(X)(X-a)^2$$

un a ir vairākkārtīga sakne. ■

1.4.3. Polinoma kvadrātbrīvās faktorizācijas atrašana

Šajā sadaļā pētīsim polinomus virs $k = \mathbb{Q}$ vai $\mathbb{R}$.

Ja $p \in k[X]$ ir nedalāms polinoms, kuram izpildās

$$p^{\alpha} | f,$$
$$p^{\alpha+1} \nmid f,$$

tad p sauksim par *f α-kārtīgu nedalāmu dalītāju (faktoru).*

$\forall\ f \in k[X]$ var viennozīmīgi, ar precizitāti līdz kārtībai un invertējamiem reizinātajiem, izteikt formā

$$f = p_1^{\alpha_1} ... p_m^{\alpha_m}.$$

1.12. teorēma. Ja p ir $f \in k[X]$ α-kārtīgs nedalāms dalītājs, tad p ir f' $\alpha - 1$-kārtīgs nedalāms dalītājs.

PIERĀDĪJUMS Ir dots, ka

$$f = p^{\alpha} g, \text{ kur } LKD(p, g) = 1.$$

Redzam, ka

$$f' = \alpha p^{\alpha-1} p' g + p^{\alpha} g' = p^{\alpha-1}(\alpha p' g + p g').$$

Redzam, ka $p^{\alpha-1} | f$. Jāpierāda, ka $p \nmid (\alpha p' g + p g')$.

$p|(\alpha p' g + p g') \implies p|\alpha p' g.$

$\deg(p) > \deg(p') \implies LKD(p, p') = 1.$

$LKD(p, g) = 1 \wedge \ LKD(p, p') = 1 \implies p \nmid \alpha p' g$ - pretruna.

$k[X]$ ir VFG $\implies p \nmid (kp' g + p g').$ ■

1.13. teorēma. (Kvadrātbrīvās faktorizācijas formula)

$$f = p_1^{\alpha_1} ... p_m^{\alpha_m} \implies \frac{f}{LKD(f, f')} = p_1 ... p_m.$$

PIERĀDĪJUMS No iepriekšējās teorēmas zinām, ka

$$f' = p_1^{\alpha_1 - 1} ... p_m^{\alpha_m - 1} h, \text{ kur } p_i \nmid h.$$

Seko, ka

$$LKD(f, f') = p_1^{\alpha_1 - 1} ... p_m^{\alpha_m - 1}.$$

Izdalot f ar $LKD(f, f')$, iegūsim vēlamo formulu:

$$\frac{f}{LKD(f, f')} = \frac{p_1^{\alpha_1} ... p_m^{\alpha_m}}{p_1^{\alpha_1 - 1} ... p_m^{\alpha_m - 1}} = p_1 ... p_m.$$

■

1.5. piemērs. Atradīsim polinoma

$$f(X) = X^5 - X^4 - 2X^3 + 2X^2 + X - 1 \in \mathbb{Q}[X]$$

faktorizāciju.

Atrodam $f'(X) = 5X^4 - 4X^3 - 6X^2 + 4X + 1$.

Atrodam $LKD(f, f') = X^3 - X^2 - X + 1$ izmantojot Eiklīda algoritmu.

Atrodam

$$\frac{f}{LKD(f, f')} = X^2 - 1 = (X - 1)(X + 1).$$

Dalot f vairākas reizes ar $X-1$ un $X+1$, iegūsim faktorizāciju

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

2. Pamatfakti par $\mathbb{C}$

2.1. Motivācijas

2.1.1. 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.

2.1.2. 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.

2.2. Paplašinājuma ģeometriskais 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),

- $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$ (kaut kas jauns).

Var pārbaudīt, ka $(\mathbb{R}^2, +, \cdot)$ ir lauks (izpildās visas skaitļu operāciju īpašības), 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 identisks 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.

2.3. Pamatfakti

2.3.1. 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 reālo skaitļu salīdzināšanas $\leq$ analoga.

2.3.2. 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.

2.3.3. Īpašības

2.1. 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. $$\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|},$$
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. ■

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

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

2.2. 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:

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

2.4. $\mathbb{C}$ 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 $\deg(f)$.

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

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

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

3.1. Faktorizācija virs $\mathbb{C}$

3.1. teorēma. (*algebras pamatteorēma*) Katrs $f \in \mathbb{C}[X]$ sadalās lineāros reizinātājos.

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

3.2. Faktorizācija virs $\mathbb{R}$

3.2. 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 (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. ■

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

ka

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

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

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

4.1. Ievads

$\mathbb{Z}[X]$ ir viennozīmīgās faktorizācijas gredzens.

Tā kā $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$, tad katru polinomu $f\in\mathbb{Z}[X]$ var uzskatīt par piederošu $\mathbb{Q}[X]$, $\mathbb{R}[X]$ vai $\mathbb{C}[X]$.

$f\in\mathbb{Q}[X]\implies\exists\, a\in\mathbb{Z}:\ af\in\mathbb{Z}[X]$ - a ir f koeficientu saucēju MKD daudzkārtnis.

Ja ir zināms polinoma sadalījums virs lielāka lauka, tad izmantojot viennozīmīgās faktorizācijas īpašību, var izdarīt atbilstošus secinājumus par polinoma faktorizāciju virs $\mathbb{Z}$.

4.1. piemērs. $X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3}) \in \mathcal{I}(\mathcal{Z}[X])$.

4.1. teorēma. (*Racionālās saknes tests*) Dots, ka

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

Dots, ka $LKD(r, s) = 1$, $r \neq 0$.

$f\left(\frac{r}{s}\right) = 0 \implies$

1. $f_0 \equiv 0 (\text{mod } r) \iff r | f_0$;
2. $f_n \equiv 0 (\text{mod } s) \iff s | f_n$.

PIERĀDĪJUMS

1.,2. Vienādojumu $f\left(\frac{r}{s}\right) = 0$ reizināsim ar s^n:

$$\overbrace{f_n r^n + \underbrace{f_{n-1} r^{n-1} s + \ldots + f_1 r s^{n-1}}_{\equiv 0 (\mathrm{mod}\ s)}}^{\equiv 0 (\mathrm{mod}\ r)} + f_0 s^n = 0.$$

Apskatīsim redukcijas mod r un s. Redzam, ka

$$\begin{cases} f_0 s^n \equiv 0 (\mathrm{mod}\ r) \\ f_n r^n \equiv 0 (\mathrm{mod}\ s). \end{cases}$$

Ievērosim, ka

$$LKD(r,s) = 1 \implies \begin{cases} r \in \mathcal{U}_s \\ s \in \mathcal{U}_r. \end{cases}$$

Tādējādi

$$\begin{cases} f_0 s^n \cdot (s^{-1})^n \equiv f_0 \equiv 0 \cdot (s^{-1})^n \equiv 0 (\mathrm{mod}\ r) \\ f_n r^n \cdot (r^{-1})^n \equiv f_n \equiv 0 \cdot (r^{-1})^n \equiv 0 (\mathrm{mod}\ s). \end{cases}$$ ■

4.2. piemērs. Mēģināsim faktorizēt $f = 2X^4 - 5X^3 + 6X^2 - 10X + 4$.
Ja r/s ir f sakne, tad $r|4$ un $s|2$.
Iespējamās racionālās saknes ir ± 4, ± 2, ± 1, $\pm \frac{1}{2}$.
Ar tiešu pārbaudi atrodam, ka saknes ir 2 un $\frac{1}{2}$.
Izdalot f ar $(X - \frac{1}{2})(X - 2)$, iegūstam

$$f = (X - \frac{1}{2})(X - 2)(2X^2 + 4).$$

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

Ar $\mathcal{I}(R[X])$ apzīmē $R[X]$ nedalāmo poliomu kopu.

4.2. teorēma. $f \in \mathcal{I}(\mathbb{Z}[X]) \iff f \in \mathcal{I}(\mathbb{Q}[X])$.

4.3. Factorizācija mod p un tās pielietojumi

Definēsim polinoma $f \in \mathbb{Z}[X]$ redukciju mod p.

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

4.3. piemērs. $f = X^3 - 3X^2 + 6X - 1$.

$p = 2$, $\overline{f} = X^3 + X^2 + 1$.

$p = 3$, $\overline{f} = X^3 - 1$.

4.3.1. Galvenā teorēma

4.3. teorēma. $f = gh \implies \overline{f} = \overline{g}\overline{h}$ katram pirmskaitlim p.

4.4. teorēma. $f \in \mathbb{Z}[X]$ ir normalizēts polinoms, p - pirmskaitlis.

1. $f \in \mathbb{Z}[X]$ ir dalāms $\implies$ $\overline{f} \in \mathbb{F}_p[X]$ ir dalāms $\forall p$.
2. $\exists\, p$ tāds, ka $f \in \mathbb{F}_p[X]$ ir nedalāms $\implies$ $f \in \mathbb{Z}[X]$ ir nedalāms.

4.4. piemērs. $f = X^4 - 3X^3 + 6X^2 + 4X + 7$.

$p = 3$, $\overline{f} = X^4 + X + 1 \in \mathcal{I}(\mathbb{F}_3[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X])$.

4.3.2. Eizenšteina kritērijs

4.5. teorēma. (*Eizenšteina kritērijs*) Pieņemsim, ka

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

eksistē pirmskaitlis p ar šādām īpašībām:

- $f_n \not\equiv 0 (\mathrm{mod}\ p)$.
- ja $l \neq n$, tad $f_l \equiv 0 (\mathrm{mod}\ p)$,
- $f_0 \not\equiv 0 (\mathrm{mod}\ p^2)$.

Tad $f \in \mathcal{I}(\mathbb{Z}[X])$.

PIERĀDĪJUMS Reducējot mod p, iegūsim, ka $\overline{f}(X) = X^n$.

$f = gh \in \mathbb{Z}[X] \implies \overline{f} = \overline{g}\overline{h} \in \mathbb{F}_p[X]$. Redzam, ka

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

Seko, ka

$$\begin{cases} g_0 \equiv 0 (\mathrm{mod}\ p), \\ h_0 \equiv 0 (\mathrm{mod}\ p), \end{cases} \Longrightarrow f_0 = g_0 h_0 \equiv 0 (\mathrm{mod}\ p^2)$$

- pretruna. ■

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

$X^3 - 9X + 11 = (X-1)^3 + 3(X-1)^2 - 6(X-1) + 3$ - nedalāms, $p = 3$.

4.1. piezīme. Izmantojot Eizenšteina kritēriju, var pierādīt, ka $\mathbb{Q}[X]$ (un tātad arī $\mathbb{Z}[X]$) nedalāmu polinomu pakāpes nav ierobežotas. Piemēram, katram n polinoms $X^n + 2X + 2$ ir nedalāms.

5. 6.mājasdarbs

5.1. Obligātie uzdevumi

6.1 Izmantojot Eiklīda algoritmu atrast polinomu $f(X)$ un $g(X)$ LKD un izteikt to polinomu lineāras kombinācijas veidā:

(a) $f(X) = X^3 - X^2 - 3X + 3$, $g(X) = X^2 - 1$, virs $\mathbb{Q}[X]$,
(b) $f(X) = X^4 + 2$, $g(X) = 2X^2 - 1$, virs $\mathbb{Q}[X]$,
(c) $f(X) = X + 1$, $g(X) = X^4 + X^3 + X^2 + 1$, virs $\mathbb{F}_2[X]$.

6.2 Dotajiem polinomiem f un g virs $\mathbb{Q}[X]$ atrast tādus polinomus a un b, lai izpildītos vienādība $a(X)f(X) + b(X)g(X) = 1$:

(a) $f(X) = X^3$, $g(X) = (1 - X)^3$,
(b) $f(X) = X^2$, $g(X) = (1 - X)^4$.

6.3 Sadalīt polinomus nedalāmos reizinātājos.

(a) $X^8 - 1$, virs $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$;
(b) $X^{12} - 1$, virs $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$;
(c) $X^{15} - 9$, virs $\mathbb{Q}$.