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

Studiju kurss

Polinomu algebra

5.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

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

Lekcijas kopsavilkums:

- polinoms ar veseliem koeficientiem ir nedalāms virs $\mathbb{Z}$ tad un tikai tad, ja tas ir nedalāms virs $\mathbb{Q}$;
- ir lietderīgi pētīt polinomu redukcijas mod p;
- var faktorizēt polinomus virs $\mathbb{Z}$ vai $\mathbb{Q}$ izmantojot Kronekera algoritmu;
- racionālo skaitļu konstrukciju var vispārināt uz patvaļīgu integrālu gredzenu gadījumu, to var izmantot, lai pierādītu, ka $R[X]$ ir VFG, ja R ir VFG.

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

1.1. Ievads

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

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 $\mathbb{Z}$.

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

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

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

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

$$f\left(\frac{r}{s}\right) = 0 \implies \begin{cases} f_0 \equiv 0 (\text{mod } r) \\ f_n \equiv 0 (\text{mod } s) \end{cases} \iff \begin{cases} r | f_0 \\ s | f_n. \end{cases}$$

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

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

Apskatīsim redukcijas mod r un s. Redzam, ka

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

Ievērosim, ka

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

Tādējādi

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

■

1.2. 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

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

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

1.2.1. Satura multiplikativitāte

1.2. teorēma. (*satura multiplikatīvā īpašība, Gausa lemma*) Dots, ka R ir VFG, $f, g \in R[X]$. Tad

$$cont(fg) \sim cont(f)cont(g).$$

PIERĀDĪJUMS

Reducēšana uz speciālgadījumu.

Ja $f = cont(f)f_0$ un $g = cont(g)g_0$, tad

$$cont(fg) \sim cont(f)cont(g)\underbrace{cont(f_0g_0)}_{?}.$$

Redzam, ka pietiek pierādīt, ka primitīvu polinomu reizinājums ir primitīvs polinoms.

Speciālgadījums - f un g ir primitīvi polinomi, jāpierāda,

ka fg ir primitīvs polinoms. Pierādījums no pretējā.

Ir doti primitīvi polinomi

$$f(X) = \sum_{i=0}^{n} a_i X^i,$$

$$g(X) = \sum_{j=0}^{m} b_j X^j.$$

Pieņemsim, ka $cont(fg) \notin \mathcal{U}(R)$, tātad eksistē $p \in \mathcal{I}(R)$ tāds, ka $p|cont(fg)$. Seko, ka p dala katru fg koeficientu.

Pieņemsim, ka k ir mazākais indekss, kuram $p \nmid a_k$, un l ir mazākais indekss, kuram $p \nmid b_l$. Tādi indeksi eksistē, jo pretējā gadījumā visi f un g koeficieni dalītos ar p, un tie nebūtu primitīvi polinomi.

Apskatīsim koeficientu pie X^{k+l} reizinājumam fg, tas ir vienāds

ar

$$\underbrace{\sum_{i=0}^{k+l} a_i b_{k+l-i}}_{\text{dalās ar } p} = \underbrace{(a_0 b_{k+l} + \ldots + a_{k-1} b_{l+1})}_{\text{dalās ar } p, \text{ jo } a_0,\ldots,a_{k-1} \text{ dalās}} + a_k b_l + \underbrace{(a_{k+1} b_{l-1} + \ldots + a_{k+l} b_0)}_{\text{dalās ar } p, \text{ jo } b_0,\ldots,b_{l-1} \text{ dalās}}.$$

Redzam, ka $p|a_k b_l$. Tā ir pretruna, jo no VFG īpašības seko, ka $p|a_k$ vai $p|b_l$.

■

1.2.2. Galvenā teorēma

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

PIERĀDĪJUMS $f \notin \mathcal{I}(\mathbb{Z}[X]) \implies f \notin \mathcal{I}(\mathbb{Q}[X])$.

Ja $f \in \mathcal{I}(\mathbb{Z}[X])$, tad pieņemsim, ka $f \notin \mathcal{I}(\mathbb{Q}[X])$:

$$f = gh, \text{ kur } g, h \in \mathbb{Q}[X].$$

$f \in \mathcal{I}(\mathcal{Z}[X]) \implies cont(f) = 1 (\in \mathbb{Z})$.

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

$$g_2 h_2 = \frac{\alpha}{\beta} gh = \frac{\alpha}{\beta} f, \text{ kur } \alpha, \beta \in \mathbb{Z} \implies \alpha f = \beta g_2 h_2.$$

Izmantojot satura multiplikativitāti, redzam, ka

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

Esam ieguvuši, ka

$$\alpha = \pm\beta \implies f = \pm g_2 h_2,$$

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

1.3. Kronekera faktorizācijas algoritms

1.3.1. Ievads

Kronekera algoritms ir algoritms, ar kura palīdzību var sadalīt reizinātājos polinomus gredzenā $\mathbb{Z}[X]$, un tātad arī gredzenā $\mathbb{Q}[X]$. Tas ir *rupja spēka* vai *izsmeļošās pārlases* tipa algoritms.

Atzīmēsim šādus faktus:

- ja polinoms $f \in \mathbb{Z}[X]$ ar pakāpi n ir dalāms, tad tam eksistē dalītājs g, kura pakāpe nepārsniedz $l = [\frac{n}{2}]$ - *meklēsim šādu f dalītāju g,*
- polinoms g ar pakāpi l ir viennozīmīgi noteikts ar savām vērtībām $l+1$ punktos, šādu polinomu var atrast ar, piemēram, Lagranža interpolācijas formulas palīdzību - *pietiek zināt g vērtības $l+1$ punktos,*
- ja $f = gh$, tad $g(c)|f(c)$ visiem $c \in \mathbb{Z}$ - *izvēlēsimies $l+1$ c vērtības un pārbaudīsim visus $f(c)$ dalītājus kā iespējamās $g(c)$ vērtības.*

1.3.2. Algoritms

Ir dots polinoms $f \in \mathbb{Z}[X]$ ar pakāpi n. Apzīmēsim $[\frac{n}{2}]$ ar l.

1. Izvēlēsimies $l+1$ veselu punktu virkni $\mathcal{C} = (c_0, ..., c_l)$, piemēram, $(0, 1, ..., l)$ vai $(0, 1, -1, 2, -2, ...)$ (lai atvieglotu skaitļošanu, vēlams izvēlēties pēc iespējas mazākus skaitļus).
2. Ja kādam i izpildās $f(c_i) = 0$ (nejauši trāpījām uz f saknes), tad izdalām f ar $X - c_i$ un atgriežamies uz soli 1 ar polinomu $f/(X - c_i)$.
3. Atradīsim virkni $f(\mathcal{C}) = (f(c_0), ..., f(c_l))$.
4. Pēctecīgi apskatīsim visas virknes $\mathcal{D} = (d_0, ..., d_l)$, kur $d_i | f(c_i)$:
   (a) ar Lagranža interpolācijas formulas palīdzību konstruēsim polinomu $f_{\mathcal{D}}$, kuram izpildās nosacījums
   $$f_{\mathcal{D}}(c_i) = d_i, \forall i : 0 \leq i \leq l,$$
   (b) ja $f_{\mathcal{D}} \in \mathbb{Z}[X] \wedge \deg(f) > 0 \wedge f_{\mathcal{D}} | f \implies$ varam atkārtoti pielietot Kronekera algoritmu polinomiem $f_{\mathcal{D}}$ un $f/f_{\mathcal{D}}$,

(c) ja $f_{\mathcal{D}} \notin \mathbb{Z}[X] \vee f_{\mathcal{D}} \nmid f$ (citiem vārdiem sakot, $f/f_{\mathcal{D}} \notin \mathbb{Z}[X]$), tad pārejam uz nākamo virkni $\mathcal{D}$.

5. Ja pēc visu virkņu $\mathcal{D}$ apskatīšanas nav atrasts neviens f dalītājs, tad f ir nedalāms.

1.3. piemērs. Sadalīsim reizinātājos virs $\mathbb{Z}$ polinomu

$$f = X^4 - 4X^3 + 3X^2 + 2X - 1.$$

Ja tas ir dalāms, tad am eksistē dalītājs, kura pakāpe nepārsniedz 2.

Izvēlēsimies 3 punktu virkni $\mathcal{C} = (0, 1, 2)$.

Atradīsim $f(\mathcal{C}) = (-1, 1, -1)$.

Mums ir jāapskata 8 virknes, jo katram virknes $f(\mathcal{C})$ elementam ir 2 veseli dalītāji: $(1, 1, 1,)$, $(1, 1, -1)$, $(1, -1, 1)$, $(1, -1, -1,)$, $(-1, 1, 1,)$, $(-1, 1, -1)$, $(-1, -1, 1)$, $(-1, -1, -1)$.

1. $\mathcal{D} = (1, 1, 1)$,

$$f_{\mathcal{D}} = 1 \cdot \frac{(X-1)(X-2)}{(0-1)(0-2)} + 1 \cdot \frac{(X-0)(X-2)}{(1-0)(1-2)} + 1 \cdot \frac{(X-0)(X-1)}{(2-0)(2-1)} = 1.$$

Šajā gadījumā polinoms ir konstants.

2. $\mathcal{D} = (1, 1, -1)$,

$$f_{\mathcal{D}} = 1 \cdot \frac{(X-1)(X-2)}{(0-1)(0-2)} + 1 \cdot \frac{(X-0)(X-2)}{(1-0)(1-2)} + (-1) \cdot \frac{(X-0)(X-1)}{(2-0)(2-1)} = -X^2 + X + 1.$$

Izdalot f ar $f_{\mathcal{D}}$, iegūsim $-X^2 + 3X - 1$. Pārbaudot kvadrātvienādojumu saknes, redzam, ka $-X^2 + X + 1$ un $-X^2 + 3X - 1$ ir nedalāmi virs $\mathbb{Z}$, tāpēc uzdevums ir atrisināts un

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

Apskatīsim arī pārējos gadījumus.

3. $\mathcal{D} = (1, -1, 1)$,

$$f_{\mathcal{D}} = 1 \cdot \frac{(X-1)(X-2)}{(0-1)(0-2)} +$$

$$(-1) \cdot \frac{(X-0)(X-2)}{(1-0)(1-2)} + 1 \cdot \frac{(X-0)(X-1)}{(2-0)(2-1)} = 2X^2 - 4X + 1.$$

Šajā gadījumā $f_{\mathcal{D}} \nmid f$.

4. $\mathcal{D} = (1, -1, -1)$,

$$f_{\mathcal{D}} = 1 \cdot \frac{(X-1)(X-2)}{(0-1)(0-2)} +$$

$$(-1) \cdot \frac{(X-0)(X-2)}{(1-0)(1-2)} + (-1) \cdot \frac{(X-0)(X-1)}{(2-0)(2-1)} = X^2 - 3X + 1.$$

Šajā gadījumā rezultāts ir tāds pats kā 2.gadījumā.

5. Pārējie gadījumu atšķiras no iepriekšējiem ar zīmi, tos apskatīt nav nepieciešams.

1.4. Factorizācija mod p un tās pielietojumi

1.4.1. Gredzenu homomorfisma inducēts polinomu homomorfisms

Ja ir dots gredzenu homomorfisms $\varphi : R \to S$, tad var definēt atbilstošo polinomu gredzenu funkciju

$$\widehat{\varphi} : R[X] \to S[X],$$

$$\widehat{\varphi}\Big(\sum_{i=0}^{n} a_i X^i\Big) = \sum_{i=0}^{n} \varphi(a_i) X^i.$$

1.4. teorēma. Katram gredzenu homomorfismam φ funkcija $\widehat{\varphi}$ ir polinomu gredzenu homomorfisms.

PIERĀDĪJUMS Gredzena aksiomu pārbaude.■

1.4. piemērs. Mazāka gredzena iekļaušana lielākā ir gredzenu homomorfisms: $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$.

Ja $\varphi : R \to S$ ir injektīvs gredzenu homomorfisms, tad $\widehat{\varphi}(f)$ var identificēt ar f: polinomu $f \in R[X]$ var uzskatīt par polinomu $f \in S[X]$.

Ja $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ ir redukcija mod p, tad $\widehat{\varphi}$ sauc par polinoma redukciju mod p. Apzīmēsim $\widehat{\varphi}(f)$ ar $\overline{f}$.

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

1.5. piemērs. $f = X^3 - 3X^2 + 6X - 1$.
$p = 2$, $\overline{f} = X^3 + X^2 + 1$.
$p = 3$, $\overline{f} = X^3 - 1$.

1.4.2. Galvenā teorēma

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

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

$$f_l = \sum_{i=0}^{l} g_i h_{l-i} \implies$$

$$\overline{f}_l = \overline{\sum_{i=0}^{l} g_i h_{l-i}} = \sum_{i=0}^{l} \overline{g_i h_{l-i}} = \sum_{i=0}^{l} \overline{g}_i \overline{h}_{l-i}.$$

■

1.6. 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.

PIERĀDĪJUMS

1. Seko no iepriekšējās teorēmas. Normalizācijas nosacījums ir vajadzīgs, lai redukcija nesamazinātu f pakāpi.

2. Kontrapozīcijas likums piemērots pirmajam apgalvojumam. ■

1.6. piemērs. $f = X^4 - 3X^3 + 6X^2 + 4X + 7$.
$p = 3$, $\overline{f} = X^4 + X + 1 \in \mathcal{I}(\mathbb{F}_3[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X])$.

1.4.3. Eizenšteina kritērijs

1.7. 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

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

- pretruna. ■

1.7. 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, $p = 3$.

1.1. 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.

2. Integrāla gredzena daļu lauks un tā pielietojumi polinomu algebrā

2.1. Pamatfakti

2.1.1. Motivācijas

Racionālo skaitļu lauku $\mathbb{Q}$ var uzskatīt par veselo skaitļu pāru

$$(m, n) \sim \frac{m}{n}$$

kopu. Dažādi skaitļu pāri var atbilst vienam un tam pašam racionālam skaitlim:

$$\frac{1}{2} = \frac{2}{4} = \frac{7}{14}.$$

Racionālo funkciju lauku var uzskatīt par polinomu pāru

$$(P, Q) \sim \frac{P}{Q}$$

kopu. Dažādi polinomu pāri var atbilst vienai un tai pašai racionālai funkcijai:

$$\frac{1}{X} = \frac{X-1}{X^2-X}.$$

2.1.2. Definīcijas

Ir dots integrāls gredzens R. Apskatīsim kopu $R \times \underbrace{R^*}_{=R\setminus\{0\}}$.

Kopā $R \times R^*$ definēsim šādu attiecību:

$$(a_1, b_1) \asymp (a_2, b_2) \iff a_1 b_2 = a_2 b_1.$$

2.1. teorēma. Attiecība $\asymp$ ir ekvivalence.

PIERĀDĪJUMS
Refleksivitāte. $(a,b) \asymp (a,b)$, jo $ab = ab$.

Simetrija. $(a_1,b_1) \asymp (a_2,b_2) \implies a_1b_2 = a_2b_1 \implies$

$$(a_2,b_2) \asymp (a_1,b_1).$$

Tranzitivitāte. Ja $(a_1,b_1) \asymp (a_2,b_2)$ un $(a_2,b_2) \asymp (a_3,b_3)$, tad

$$a_1b_2 = a_2b_1,$$
$$a_2b_3 = a_3b_2.$$

Reizinot pirmo vienādību ar b_3, iegūsim

$$a_1b_2b_3 = a_2b_1b_3 = a_3b_2b_1.$$

Saīsinot abas puses ar $b_2 \implies a_1b_3 = a_3b_1$, tātad $(a_1,b_1) \asymp (a_3,b_3)$.
■

Tā kā attiecība $\asymp$ ir ekvivalence, tad tā definē kopas $R \times R^*$ sadalījumu atbilstošajās ekvivalences klasēs. Iegūto faktorkopu (ekvivalences klašu kopu) apzīmēsim ar $Q(R)$. Pāra (a, b) pārstāvēto klasi apzīmēsim ar $[a, b]$.

Kopā $Q(R)$ definēsim divas operācijas:

- saskaitīšanu: $[a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2]$,
- reizināšanu: $[a_1, b_1] \cdot [a_2, b_2] = [a_1 a_2, b_1 b_2]$.

2.2. teorēma.

1. Katram integrālam gredzenam R $(Q(R), +, \cdot)$ ir lauks.
2. Funkcija $\iota : R \to Q(R)$, kas ir definēta veidā $\iota(a) = [a, 1]$ ir injektīvs gredzenu homomorfisms.

PIERĀDĪJUMS 1. Jāpārbauda, ka operācijas nav atkarīgas no pārstāvju izvēles. Jāpārbauda visas lauka aksiomas.

Var pārbaudīt, ka $0 = [0, 1]$, $1 = [1, 1]$, $[a, b]^{-1} = [b, a]$.

2. Ja $\iota(a_1) = \iota(a_2)$, tad $a_1 = a_2$, tātad funkcija ir injektīva. Īpašības

$$\iota(a_1 + a_2) = \iota(a_1) + \iota(a_2),$$
$$\iota(a_1 a_2) = \iota(a_1)\iota(a_2)$$

seko no operāciju definīcijām. ■

2.1. piezīme. Iepriekšējās teorēmas otrais punkts nozīmē to, ka R var interpretēt kā $Q(R)$ apakšgredzenu. Šī iemesla dēļ $Q(R)$ sauc par *R daļu lauku (field of fractions)*.

2.2. piezīme. Tā kā $R \leq Q(R)$, tad var identificēt $Q(R)$ elementus formā $[x, 1]$ ar x un definēt R un $Q(R)$ operācijas šādi:

$$x + [y, z] = [x, 1] + [y, z] = [xz + y, z],$$
$$x \cdot [y, z] = [x, 1] \cdot [y, z] = [xy, z].$$

Šī pieeja ir ērtāka, it sevišķi, ja izmanto apzīmējumu $[x, y] = \frac{x}{y}$.

2.1. piemērs. $\mathbb{Q} = Q(\mathbb{Z})$.

Ja k ir lauks, tad $Q(k) \simeq k$. Gredzenu izomorfismu $\varphi : k \to Q(k)$ var izvēlēties formā

$$\varphi(a) = (a, 1).$$

2.1.3. Racionālo funkciju lauks

Ja k ir lauks, tad $Q(k[X])$ sauksim par *racionālo funkciju lauku virs* k un apzīmēsim ar $k(X)$.

$k(X)$ elementus var pierakstīt formā $[f, g]$ vai f/g. Šādos apzīmējumos f sauc par skaitītāju un g - par saucēju.

Redzam, ka

$$\frac{f}{g} = \frac{fh}{gh}, \text{ kur } h \neq 0.$$

Ja $f = f_1 w$ un $g = g_1 w$, tad

$$\frac{f}{g} = \frac{f_1}{g_1}.$$

Racionālu funkciju f/g sauksim par *nesaīsināmu*, ja

$$LKD(f, g) = 1.$$

2.3. teorēma. Racionālās funkcijas nesaīsināmais pieraksts ir noteikts viennozīmīgi ar precizitāti līdz asociācijai skaitītājā un saucējā.

PIERĀDĪJUMS Pieņemsim, ka $f/g = f_1/g_1$, kur

$$LKD(f, g) = LKD(f_1, g_1) = 1.$$

Tā kā

$$fg_1 = f_1 g,$$

tad $f|f_1$, $f_1|f$, $g|g_1$ un $g_1|g$. Redzam, ka $f \sim f_1$ un $g \sim g_1$. ■

Parasti tiek strādāts ar racionālu funkciju nesaīsināmajām formām.

2.2. Daļu lauku pielietojumi polinomu faktorizācijā

2.4. teorēma. Dots, ka R ir VFG. Ja primitīvi polinomi $f, g \in R[X]$ ir asociēti gredzenā $Q(R)[X]$, tad tie ir asociēti gredzenā $R[X]$.

PIERĀDĪJUMS Ja $f \sim g$ gredzenā $Q(R)[X]$, tad

$$f = \frac{\alpha}{\beta} g, \text{ kur } \alpha, \beta \in R \implies \beta f = \alpha g.$$

$cont(\beta f) = cont(\alpha g) \implies \alpha \sim \beta$ gredzenā R, tātad

$$\alpha = u\beta, \text{ kur } u \in U(R) \implies f = \frac{\alpha}{\beta} g = ug,$$

tātad $f \sim g$ gredzenā $R[X]$. ■

2.5. teorēma. Dots, ka R ir VFG. Ja nekonstants polinoms $f \in R[X]$ ir nedalāms gredzenā $R[X]$, tad tas ir nedalāms gredzenā $Q(R)[X]$.

PIERĀDĪJUMS Šis fakts jau tika pierādīts gadījumā, kad $R = \mathbb{Z}$. Vispārīgā gadījumā pierādījums ir tāds pats. ■

2.6. teorēma. Ja R ir VFG, tad $R[X]$ arī ir VFG.

PIERĀDĪJUMS

1.solis. Sadalījuma eksistence.

Jebkuru polinomu $f \in R[X]$ var uzrakstīt formā

$$f = cont(f) f_0,$$

kur f_0 ir primitīvs polinoms.

$cont(f)$ var viennozīmīgi sadalīt nedalāmos reizinātājos virs R.

Ar matemātiskās indukcijas metodi ar parametru $\deg(f_0)$ pierādīsim, ka f_0 var sadalīt nedalāmos reizinātājos virs R.

Indukcijas bāze. Ja $\deg(f_0) = 1$, tad f_0 ir nedalāms un noteikts viennozīmīgi ar precizitāti līdz invertējamam reizinātājam.

Indukcijas solis. Pieņemsim, ka jebkuru primitīvu polinomu f_0, kuram $\deg(f_0) < n$, var sadalīt nedalāmos reizinātājos.

Apskatīsim polinomu f_0, kuram $\deg(f_0) = n$. Ja f_0 ir dalāms, tad tā reizinātāju pakāpes ir mazākas nekā n, tāpēc saskaņā ar indukcijas pieņēmumu f_0 ir izsakāms kā nedalāmu reizinātāju reizinājums.

2.solis. Sadalījuma vienīgums.

Pietiek pierādīt vienīgumu primitīviem polinomiem, jo $cont(f)$ ir sadalāms viennozīmīgi.

Pieņemsim, ka f_0 var izteikt nedalāmu polinomu reizinājumā divos dažādos veidos:

$$f_0 = f_1 ... f_m = g_1 ... g_l.$$

Visi polinomi f_i, g_j ir nedalāmi virs $Q(R)[X]$ saskaņā ar iepriekšējo teorēmu.

Agrāk bija pierādīts, ka $k[X]$ ir VFG, ja k ir lauks. Tā kā $Q(R)[X]$ ir lauks, tad polinomam $f_0 \in Q(R)[X]$ izpildās viennozīmīgās faktorizācijas nosacījums:

- $m = l$,
- polinomiem var mainīt indeksāciju tā, ka $f_i \sim g_i$ virs $Q(R)[X]$.

No iepriekš dotas teorēmas seko, ka $f_i \sim g_i$ virs $R[X]$. Tātad sadalījums ir noteikts viennozīmīgi virs R. ■

2.3. piezīme. Tagad ir pierādīts, ka $\mathbb{Z}[X]$ ir VFG.

3. 5.mājasdarbs

3.1. 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 Izmantojot Kronekera algoritmu sadalīt polinomus nedalāmajos reizinātājos virs $\mathbb{Z}$:

(a) $2X^4 - 13X^3 + 25X^2 - 14X + 2$,
(b) $X^6 - 9X^5 + 29X^4 - 39X^3 + 17X^2 + 3X - 1$.

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

(a) $X^3 - 3X^2 + 4X - 4 \pmod 3$,
(b) $X^4 - 10X^3 + 6X^2 - 12X + 6$ (Eizenšteina kritērijs),
(c) $X^3 - X^2 - 3X + 5$ (Eizenšteina kritērijs ar nelielu nobīdi),
(d) $X^{15} - 9$.

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

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

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.6 Pierādiet pilnā apjomā algebras pamatteorēmu - $\mathbb{C}$ ir algebriski slēgts lauks.

5.7 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.