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

Studiju kurss

Polinomu algebra

7.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

Lekcijas mērķis - pārnest uz polinomu gredzeniem veselo skaitļu salīdzināmības un atlikuma klašu un to operāciju jēdzienus.

1. Atlikumu klases polinomu gredzenos

1.1. Salīdzināmības definīcija

Fiksēsim polinomu gredzenu $R[X]$, kur R ir Eiklīda gredzens. Apzīmēsim atlikumu, ko iegūst dalot f ar m, ar $atl(f, m)$.

Fiksēsim polinomu $m(X) \in R[X]$. Teiksim, ka divi polinomi $f(X)$ un $g(X)$ ir *salīdzināmi* vai *kongruenti* pēc moduļa $m(X)$, apzīmē ar pierakstu

$$f(X) \equiv g(X)(\text{mod m(X)}),$$

tad un tikai tad, ja

- $f(X) - g(X)$ dalās ar $m(X)$ **vai**

- skaitļi $f(X)$ un $g(X)$ dalījumā ar $m(X)$ dod vienādu atlikumu:

$$atl(f, m) = atl(g, m).$$

1.1. piemērs. $X^2 \equiv X^2 + 2X(\text{mod X})$, $X \equiv X + 100(\text{mod } 1)$,

1.1. teorēma. Abas salīdzināmības definīcijas ir loģiski ekvivalentas.

PIERĀDIJUMS (Tas pats pierādījums, kas bija veselo skaitļu salīdzināmības gadījumam)

Ja

$$f = q_1 m + r,$$
$$g = q_2 m + r,$$

tad $f - g = m(q_1 - q_2)$ un tāpēc $m|f - g$.

Ja

$$f = q_1 m + r_1,$$
$$g = q_2 m + r_2,$$

kur $r_1 \neq r_2$, tad

$$f - g = m(q_1 - q_2) + (r_1 - r_2).$$

Redzam, ka $r_1 - r_2 \neq 0$ un $\deg(r_1 - r_2) < \deg(m)$, tāpēc $m \nmid f - g$. ■

1.2. teorēma. Polinomu salīdzināmība pēc fiksēta moduļa $m(X)$ ir ekvivalences attiecība - ir spēkā šādas īpašības:

1. katrs polinoms f ir salīdzināms ar sevi - $f \equiv f$ (*refleksivitāte*),
2. ja $f \equiv g$, tad $g \equiv f$ (*simetrija*),
3. ja $f \equiv g$ un $g \equiv h$, tad $f \equiv h$ (*tranzitivitāte*).

PIERĀDĪJUMS (Analoģisks veselo skaitļu salīdzināmības gadījumam)

1. $m|f - f$, jo $m|0$.
2. Ja $m|f - g$, tad $f - g = qm$ un $g - f = (-q)m$, tāpēc $m|g - f$.
3. Ja $m|f - g$ un $m|g - h$, tad $f - g = qm$ un $g - h = q'm$. Saskaitot šīs vienādības, iegūsim $f - h = (q + q')m$, tāpēc $m|f - h$.

■

1.2. Salīdzināmības pēc moduļa m klases

Salīdzināmības attiecībai atbilstošā polinomu kopas sadalījuma apakškopas vai klases sauc par *atlikumu klasēm pēc moduļa* m. Katrā atlikumu klasē ir visi polinomi, kas dalījumā ar m dod vienu un to pašu atlikumu.

Polinoma f klasi pēc moduļa m (*redukciju pēc moduļa* m) apzīmēsim ar $[f]$ vai $f + mR[X]$.

Atlikumu klašu kopu pēc moduļa m parasti apzīmē ar pierakstu $R[X]/(m)$.

Atlikumu klašu sadalījums (faktorkopa) pēc moduļa m definē sirjektīvu funkciju - dabisko projekciju

$$\pi_m : R[X] \to R[X]/(m),$$
$$\pi_m : f \to [f],$$

kas katram polinomam piekārto to atlikumu klasi, kurai tas pieder.

1.2. piemērs. Pieņemsim, ka $m(X) = X$. Dots, ka

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

$$g = \sum_{i=0}^{k} b_i X^i.$$

Redzam, ka

$$atl(f, X) = a_0,$$

$$atl(g, X) = b_0.$$

Tādējādi atlikumu klases mod X ir savstarpēji viennozīmīgi saistītas ar R elementiem: $f \equiv g (\text{mod } X)$ tad un tikai tad, ja $a_0 = b_0$. Katrā atlikumu klasē mod X ir visi polinomi ar fiksētu brīvo locekli.

Apzīmēsim ar $R[X, n]$ visu to polinomu kopu, kuru pakāpe nepārsniedz n, ieskaitot nulles polinomu.

1.3. teorēma. Atlikumu klašu kopas mod m elementiem var savstarpēji viennozīmīgi piekārtot kopas $R[X, \deg(m)-1]$ elementus (kopu $R[X, \deg(m)-1]$ var izmantot kā atlikumu klašu kopas mod m pārstāvju kopu).

PIERĀDĪJUMS Tā kā dalot ar m, atlikuma pakāpe ir mazāka kā $\deg(m)$, tad katrs polinoms ir salīdzināms mod m ar tieši vienu elementu no kopas $R[X, \deg(m)-1]$. ■

1.3. piemērs. Apskatīsim $\mathbb{F}_2[X]/(X^2+X+1)$. Ir četri polinomi, kuru pakāpe nepārsniedz 1:

$$0, 1, X, X+1.$$

Tādējādi ir četras atlikumu klašu kopas pēc moduļa X^2+X+1:

$$[1], [0], [X], [X+1].$$

Apskatīsim $\mathbb{R}[X]/(X^2+1)$. Katra atlikumu klase ir viennozīmīgi izsakāma formā

$$[a+bX],$$

kur $a, b \in \mathbb{R}$.

1.3. Operācijas ar atlikumu klasēm, atlikumu klašu gredzeni

1.3.1. Polinomu gredzena operācijas un salīdzināmība pēc moduļa m

1.4. teorēma. Ja $f_1 \equiv f_2 \pmod{\text{m}}$ un $g_1 \equiv g_2 \pmod{\text{m}}$, tad

1. $f_1 + g_1 \equiv f_2 + g_2 \pmod{\text{m}}$;
2. $f_1 g_1 \equiv f_2 g_2 \pmod{\text{m}}$;
3. $f_1^n \equiv f_2^n \pmod{\text{m}}$.

PIERĀDĪJUMS (Analoģisks veselo skaitļu salīdzināmības gadījumam)

1. Saskaitīšana. Ja $m|f_1 - f_2$ un $m|g_1 - g_2$, tad saskaitot labās puses, iegūsim, ka $m|(f_1 - f_2) + (g_1 - g_2)$. Bet

$$(f_1 - f_2) + (g_1 - g_2) = (f_1 + g_1) - (f_2 + g_2),$$

tātad $m|(f_1 + g_1) - (f_2 + g_2)$ un $f_1 + g_1 \equiv f_2 + g_2 \pmod{\text{m}}$.

2. Reizināšana. Apskatīsim starpību $f_1g_1 - f_2g_2$:

$$f_1g_1 - f_2g_2 = f_1g_1 - f_1g_2 + f_1g_2 - f_2g_2 = f_1(g_1 - g_2) + g_2(f_1 - f_2).$$

Tā kā $m|f_1 - f_2$ un $m|g_1 - g_2$, tad $m|f_1g_1 - f_2g_2$.

3. Seko no 2.apgalvojuma. ■

1.3.2. Atlikumu klašu gredzeni

Fiksēsim nekonstantu polinomu $m \in R[X]$.

Par divu polinomu atlikumu klašu (pēc moduļa m) $[f]$ un $[g]$ summu $[f] + [g]$, sauksim klasi

$$[f + g] = \pi_m(f + g).$$

Par divu atlikumu klašu $[f]$ un $[g]$ reizinājumu $[f][g]$, sauksim klasi

$$[fg] = \pi_m(fg).$$

1.5. teorēma.

1. Polinomu atlikuma klašu operācijas ir definētas korekti - nav atkarīgas no pārstāvju izvēles.
2. Dabiskā projekcija π_m ir gredzenu homomorfizms - visiem polinomiem f un g ir spēkā sakarības
   (a) $\pi_m(f+g) = \pi_m(f) + \pi_m(g)$,
   (b) $\pi_m(fg) = \pi_m(f)\pi_m(g)$.
3. Polinomu atlikumu klašu kopa ar definētajām operācijām ir komutatīvs gredzens ar vieninieku, kas satur apakšgredzenu, izomorfu ar R.

PIERĀDĪJUMS 1. Korektums seko no iepriekšējā sadaļā pierādītās teorēmas: ja $[f_1] = [f_2]$ un $[g_1] = [g_2]$, tad

$$[f_1] + [g_1] = [f_2] + [g_2],$$
$$[f_1] \cdot [g_1] = [f_2] \cdot [g_2].$$

2. Tas seko no operāciju definīcijām atlikumu klasēm.

3. Tas, ka $R[X]/(m)$ ir gredzens, seko no saskaitīšanas un reizināšanas īpašībām.

Lai pierādītu, ka $R \leq R[X]/(m)$, ir jāuzrāda injektīvs gredzenu homomorfizms

$$\psi : R \to R[X]/(m).$$

Atcerēsimies, ka eksistē injektīvs gredzenu homomorfizms

$$\iota : R \to R[X],$$
$$\iota(r) = r$$

un projekcija

$$\pi : R[X] \to R[X]/(m),$$
$$\pi(f) = [f].$$

Pierādīsim, ka

$$\psi = \pi \circ \iota : R \to R[X]/(m)$$

ir injektīvs gredzenu homomorfizms.

Injektivitāte. Ja $\pi(\iota(r_1)) = \pi(\iota(r_2))$, tad $[r_1] = [r_2]$. Tā kā $\deg(m) \geq 1$, tad $r_1 = r_2$.

Homomorfizms. Seko no 2.

■

Polinomu atlikumu kopu pēc moduļa m ar tajā uzdotām saskaitīšanas un reizināšanas operācijām sauksim par *atlikumu gredzenu pēc moduļa* m un pzīmēsim ar pierakstu $R[X]/(m)$.

1.1. piezīme. Tā kā $R \leq R[X]/(m)$, tad var identificēt r un $[r]$ ($r \in R$). To mēs parasti arī darīsim.

1.4. piemērs. Aprakstīsim gredzena operācijas atlikumu gredzenā $\mathbb{F}_2[X]/(X^2 + X + 1)$. Ir četras atlikumu klašu kopas pēc moduļa $X^2 + X + 1$;

$$[1], [0], [X], [X + 1].$$

Atradīsim operāciju tabulas:

+	[0]	[1]	[X]	[X+1]
[0]	[0]	[1]	[X]	[X+1]
[1]	[1]	[0]	[X+1]	[X]
[X]	[X]	[X+1]	[0]	[1]
[X+1]	[X+1]	[X]	[1]	[0]

•	[0]	[1]	[X]	[X+1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[X]	[X+1]
[X]	[0]	[X]	[X+1]	[1]
[X+1]	[0]	[X+1]	[1]	[X]

1.5. piemērs. Aprakstīsim gredzena operācijas atlikumu gredzenā $\mathbb{R}[X]/(X^2+1)$. Katra atlikumu klase ir viennozīmīgi izsakāma formā

$$[a+bX],$$

kur $a, b \in \mathbb{R}$. Saskaitīšana:

$$[a_1 + b_1 X] + [a_2 + b_2 X] = [(a_1 + a_2) + (b_1 + b_2)X].$$

Reizināšana:

$$[a_1 + b_1 X] \cdot [a_2 + b_2 X] = [(a_1 a_2) + (a_1 b_2 + a_2 b_1)X + (b_1 b_2)X^2].$$

Ievērosim, ka

$$uX^2 + vX + w = u(X^2 + 1) + (vX + (w - u)),$$

tāpēc

$$[a_1 + b_1 X] \cdot [a_2 + b_2 X] = [(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)X].$$

Redzam, ka $\mathbb{R}[X]/(X^2 + 1) \backsimeq \mathbb{C}$, izomorfizms

$$f : \mathbb{R}[X]/(X^2 + 1) \to \mathbb{C}$$

var tikt definēts ar formulu

$$f([a + bX]) = a + ib.$$

1.4. Polinomu atlikumu gredzenu īpašības

Šajā sadaļā mēs apskatīsim tikai polinomus virs laukiem.

1.4.1. Atlikumu gredzena invertējamie elementi

1.6. teorēma. Dots, ka $m \in k[X]$ ir nekonstants polinoms.

$LKD(f,m) = 1 \iff [f] \in U(k[X]/(p))$ (f ir invertējams elements faktorgredzenā $k[X]/(m)$).

PIERĀDĪJUMS Ja $LKD(f,m) = 1$, tad eksistē polinomi $u, v \in k[X]$ tādi, ka

$$1 = uf + vm.$$

Seko, ka $uf = 1 - vm$ un

$$[uf] = [u][f] = [1].$$

Ja $[f]$ ir invertējama klase faktorgredzenā $k[X]/(m)$, tad eksistē klase [g] tāda, ka

$$[f][g] = [1] = [fg].$$

Seko, ka

$$fg - 1 = qm.$$

Ja eksistē nekonstants polinoms h tāds, ka $h|f$, $f = f_1 h$ un $h|m$, $m = m_1 h$, tad

$$1 = fg - qm = f_1 hg - qm_1 h = h(f_1 g - qm_1).$$

Esam ieguvuši pretrunu, jo h nevar dalīt 1. ■

1.7. teorēma. Dots, ka $p \in k[X]$ ir nekonstants polinoms. Zemāk dotie apgalvojumi ir ekvivalenti:

1. p ir nedalāms polinoms.
2. $k[X]/(p)$ ir lauks.
3. $k[X]/(p)$ ir integrāls gredzens.

PIERĀDĪJUMS Pierādīsim loģisko ekvivalenci ar ciklisko metodi:

$$1. \Rightarrow 2. \Rightarrow 3. \Rightarrow 1.$$

$1. \Rightarrow 2.$

Tā kā p ir nedalāms, tad katram f $LKD(f,p) = 1$ vai $p|f$. Ja $LKD(f,p) = 1$, tad $[f]$ ir invertējams elements. Ja $p|f$, tad $f = up = f - 0$ un $[f] = 0$. Ir pierādīts, ka ja atlikumu klase nav $[0]$, tad tā ir invertējama.

$2. \Rightarrow 3.$ Lauks ir integrāls gredzens.

$3. \Rightarrow 1.$ Pierādījums izmantojot kontrapozīcijas likumu. Ja p nav nedalāms, tad eksistē divi nekonstanti polinomi g un h tādi, ka $p =$

gh. Seko, ka $[gh] = [g][h] = [p] = [0]$, tāpēc $k[X]/(p)$ nav integrāls gredzens.

■

1.2. piezīme. Ja p ir nedalāms, tad lauku $K_p = k[X]/(p)$ sauc par k *paplašinājuma (paplašinošo) lauku*. Teorēmu var izmantot kā jaunu lauku konstruēšanas metodi. Polinomus gredzenā $k[X]$ var uzskatīt arī par polinomiem gredzenā $K_p[X]$.

1.4.2. Polinomu saknes atlikumu gredzenā

1.8. teorēma. Dots, ka $p(X) \in k[X]$ ir nekonstants nedalāms polinoms.

$k[X]/(p)$ satur vismaz vienu p sakni.

PIERĀDĪJUMS Pierādīsim, ka $\pi(X) = [X] \in K_p$ ir f sakne. Pieņemsim, ka

$$p(X) = \sum_{i=0}^{m} p_i X^i.$$

Redzam, ka

$$p([X]) = \sum_{i=1}^{m} p_i [X]^i = \sum_{i=1}^{m} p_i [X^i] =$$

$$\sum_{i=1}^{m} [p_i X^i] = [\sum_{i=1}^{m} p_i X^i] = [p(X)] = [0]$$

■

1.9. teorēma. Dots, ka $f(X) \in k[X]$ ir nekonstants polinoms.
Eksistē k paplašinājuma lauks, kas satur vismaz vienu f sakni.

PIERĀDĪJUMS Pieņemsim, ka p ir nedalāms f dalītājs. Definēsim $K_p = k[X]/(p)$. Saskaņā ar iepriekšējo teorēmu K_p satur vismaz vienu p, un tāpēc arī f, sakni. ■

1.4.3. Polinoma sašķeļošais lauks

Par polinoma $f \in k[X]$ *sašķeļošo lauku* sauksim k paplašinošo lauku K, kurā f sadalās lineāros reizinātājos: eksistē $a_1, ...a_n \in K$ tādi, ka

$$f(X) = (X - a_1)(X - a_2)...(X - a_n).$$

1.6. piemērs. Katram $f \in \mathbb{R}[X]$ komplekso skaitļu lauks $\mathbb{C}$ ir sašķeļošais lauks.

Polinomam $X^2 + X + 1 \in \mathbb{F}_2[X]$ lauks $\mathbb{F}_2[X]/(X^2 + X + 1)$ ir sašķeļošais lauks. Saknes ir $[X]$ un $[X + 1]$.

1.10. teorēma. Katram nekonstantam polinomam $f \in k[X]$ eksistē sašķeļošais lauks.

PIERĀDĪJUMS Pieņemsim, ka $f = \tilde{f} \cdot p_1 ... p_m$, kur $\tilde{f}$ ir lineāru polinomu reizinājums, katram p_i ir nedalāms polinoms, kuram

$$\deg(p_i) > 1.$$

Saskaņā ar iepriekš pierādītu teorēmu laukā $k[X]/(p_i)$ polinomam p_i eksistē vismaz viena sakne, tātad polinomam f virs lauka $k[X]/(p_i)$ būs vēl viens lineārs reizinātājs.

Vairākkārtīgi pielietojot šādu operāciju iegūsim k paplašinājumu virkni

$$\underbrace{k}_{k_0} \leq \underbrace{k[X]/(p_1)}_{k_1} \leq \underbrace{k_1[X]/(q_j)}_{k_2} \leq ... \leq k_l.$$

Katra paplašināšana dod vismaz vienu lineāru reizinātāju f sadalījumā, tāpēc pēc galīga skaita soļu f tiks sadalīts lineāros reizinātājos virs kāda k paplašinājuma k_l. ■

2. 7.mājasdarbs

2.1. Obligātie uzdevumi

7.1 Atrodiet saskaitīšanas un reizināšanas tabulas gredzenam

$$\mathbb{F}_2[X]/(X^3 + X + 1).$$

7.2 Aprakstiet sašķeļošo lauku polinomam f un atrodiet f saknes tajā šādos gadījumos:

(a) $f = X^3 + X + 1 \in \mathbb{F}_2[X]$;
(b) $f = X^2 + X + 1 \in \mathbb{F}_3[X]$,
(c) $f = X^2 - 2 \in \mathbb{Q}[X]$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

7.3 Pierādiet, ka $\mathbb{R}[X]/(X^2 + X + 1) \simeq \mathbb{C}$.