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

Studiju kurss

Polinomu algebra

6.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis - pārnest uz polinomu gredzeniem veselo skaitļu salīdzināmības un atlikuma klašu un to operāciju jēdzienus, vispārināt salīdzināmību, atlikumu klases un to operācijas uz patvaļīgiem gredzeniem.

Lekcijas kopsavilkums:

- polinomu gredzenos var definēt kongruenci pēc fiksēta polinoma moduļa, kuras īpašības ir līdzīgas veselo skaitļu kongruences īpašībām, var definēt operācijas ar atlikumu klasēm un faktorgredzenus;
- faktorgredzens mod p ir lauks tad un tikai tad, ja p ir nedalāms polinoms;

- kongruenci var vispārināt uz patvaļīgu komutatīvu gredzenu gadījumu, attīstot ideālu teoriju.

Svarīgākie jēdzieni: kongruence mod $m \in R[X]$, atlikumu klases mod m, operācijas ar atlikumu klasēm, atlikumu klašu gredzens, polinomu faktorgredzens, ideāli, operācijas ar ideāliem, ideālu ģeneratori, galvenie ideāli, galveno ideālu gredzeni, atlikumu klases mod I, operācijas ar atlikumu klasēm mod I, faktorgredzeni.

Svarīgākie fakti un metodes: kongruences mod $R[X]$ īpašības, standarta atlikumu klašu mod m pārstāvju kopa, atlikumu klašu operāciju īpašības, polionomu faktorgredzena īpašības, ideālu piemēri un speciālgadījumi, netriviāla ideāla elementu neinvertējamība, ideālu operāciju īpašības, atlikumu klašu mod I īpašības.

1. Atlikumu klases polinomu gredzenos

1.1. Salīdzināmības definīcija

$R[X]$ - Eiklīda gredzens (piemēram, ja R ir lauks). Apzīmēsim atlikumu, ko iegūst dalot $f \in R[X]$ ar $m \in R[X]$, ar $[f]_m$.

Fiksēsim $m \in R[X]$. Teiksim, ka f un g ir *salīdzināmi* vai *kongruenti* mod m, apzīmē ar pierakstu

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

tad un tikai tad, ja

- $m | f - g$ **vai**
- f un g dalījumā ar m dod vienādu atlikumu:

$$[f]_m = [g]_m.$$

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.

$$\begin{cases} f = q_1 m + r \\ g = q_2 m + r \end{cases} \Longrightarrow f - g = m(q_1 - q_2) \Longleftrightarrow m | f - g.$$

$$\begin{cases} f = q_1 m + r_1 \\ g = q_2 m + r_2, \text{ kur } r_1 \neq r_2 \end{cases} \Longrightarrow f - g = m(q_1 - q_2) + (r_1 - r_2).$$

$$\Longrightarrow r_1 - r_2 \neq 0 \text{ un } \deg(r_1 - r_2) < \deg(m) \Longrightarrow m \nmid f - g. \blacksquare$$

1.2. teorēma. Polinomu kongruence mod $m \in R[X]$ ir ekvivalences attiecība.

PIERĀDĪJUMS Analoģisks kongruencei mod $m \in \mathbb{Z}$. ■

1.2. Salīdzināmības mod m klases

1.2.1. Definīcija

Salīdzināmības attiecības klases sauc par *atlikumu klasēm mod* m.

Katrā atlikumu klasē ir visi polinomi, kas dalījumā ar m dod vienu un to pašu atlikumu.

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

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

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

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

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

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

$$\begin{cases} f = \sum_{i=0}^{n} a_i X^i, \\ g = \sum_{i=0}^{k} b_i X^i. \end{cases} \Longrightarrow \begin{cases} [f]_X = a_0, \\ [g]_X = b_0. \end{cases}$$

Tādējādi atlikumu klases mod X ir savstarpēji viennozīmīgi saistītas ar R elementiem: $[f]_X = [g]_X \iff a_0 = b_0$. Katrā atlikumu klasē mod X ir visi polinomi ar fiksētu brīvo locekli.

1.2.2. Atlikumu klašu pārstāvju kopas

Definēsim $R[X]_n = \{f \in R[X] \mid \deg f \leq n\}$.

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 mod m pārstāvju kopu).

PIERĀDĪJUMS

$$\begin{cases} [f]_m \text{ ir viennozīmīgi noteikts} \\ \deg[f]_m < \deg m \end{cases} \Longrightarrow \forall \text{ polinoms ir salīdzināms}$$

mod m ar tieši vienu elementu no kopas $R[X]_{\deg(m)-1}$. ■

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

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

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

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

1.3. Operācijas ar atlikumu klasēm, atlikumu klašu gredzeni

1.3.1. Polinomu operācijas mod m

1.4. teorēma. $\begin{cases} [f_1]_m = [f_2]_m \\ [g_1]_m = [g_2]_m \end{cases} \Longrightarrow \begin{cases} [f_1+g_1]_m = [f_2+g_2]_m \\ [f_1 \cdot g_1]_m = [f_2 \cdot g_2]_m \end{cases}$

PIERĀDĪJUMS Analoģisks $\mathbb{Z}$ salīdzināmības gadījumam.

$$\begin{cases} m|f_1 - f_2 \\ m|g_1 - g_2 \end{cases} \implies \text{saskaitot labās puses: } m|(f_1 - f_2) + (g_1 - g_2).$$

$(f_1 - f_2) + (g_1 - g_2) = (f_1 + g_1) - (f_2 + g_2) \implies m|(f_1 + g_1) - (f_2 + g_2)$
$\implies f_1 + g_1 \equiv f_2 + g_2 \pmod{m}$.

Pārējie gadījumi arī kā $\mathbb{Z}$ gadījumā. ■

1.3.2. Atlikumu klašu gredzeni

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

Par divu polinomu atlikumu klašu mod m $[f]$ un $[g]$ summu $[f] + [g]$, sauksim klasi $[f + g]$.

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

1.5. teorēma. $R[X]$ - EG, $m \in R[X]$, $\deg m > 0$.

1. Polinomu atlikuma klašu operācijas mod m ir definētas korekti - nav atkarīgas no pārstāvju izvēles.
2. $R[X]/(m)$ ar definētajām operācijām ir komutatīvs gredzens ar vieninieku (*atlikumu gredzens mod* m), kas satur apakšgredzenu, izomorfu ar R.

PIERĀDĪJUMS 1. Korektums seko no iepriekšējā sadaļā pierādītās teorēmas:

$$\begin{cases} [f_1] = [f_2] \\ [g_1] = [g_2] \end{cases} \Longrightarrow \begin{cases} [f_1 + g_1] = [f_2 + g_2] \\ [f_1 \cdot g_1] = [f_2 \cdot g_2] \end{cases} \Longrightarrow$$

$$\begin{cases} [f_1] + [g_1] = [f_2] + [g_2], \\ [f_1] \cdot [g_1] = [f_2] \cdot [g_2]. \end{cases}$$

2. Seko no tikko pierādītajām saskaitīšanas un reizināšanas īpašībām - izpildās visas aksiomas. Var redzēt, ka $[0] = [m] = 0$, $[1] = 1$.

Lai pierādītu, ka $R \le R[X]/(m)$, ir uzrādīsim injektīvu gredzenu homomorfismu

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

Pierādīsim, ka ψ ir injektīvs gredzenu homomorfisms.

Injektivitāte.
$\pi(r_1) = \pi(r_2) \implies [r_1] = [r_2]$.
$\deg(m) \geq 1 \implies r_1 = r_2$.

Homomorfisms.
Seko no 2. ■

1.1. piezīme. Bieži [] neraksta.

1.4. piemērs. Aprakstīsim operācijas atlikumu gredzenā $\mathbb{F}_2[X]/(X^2+X+1)$. Ir 4 atlikumu klašu kopas mod 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]

$\bullet$	[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]

1.4. Polinomu atlikumu gredzenu īpašības

Šajā sadaļā mēs apskatīsim tikai polinomus virs laukiem.

1.4.1. Atlikumu gredzena invertējamie elementi

1.6. teorēma. $m \in k[X]$, $\deg(m) > 0$.

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

PIERĀDĪJUMS $LKD(f,m) = 1 \implies \exists\, u, v \in k[X]$ tādi, ka

$$1 = uf + vm \implies [1] = [uf] + \underbrace{[vm]}_{=0} \implies [1] = [u][f].$$

$[f]$ ir invertējama klase faktorgredzenā $k[X]/(m) \implies$

$\exists\ [g] :\ [f][g] = [1] = [fg] \implies fg - 1 = qm.$

$\exists$ nekonstants polinoms $h:\ h|f,\ f = f_1h$ un $h|m,\ m = m_1h$, tad

$$1 = fg - qm = f_1hg - qm_1h = h(f_1g - qm_1).$$

Esam ieguvuši pretrunu, jo $h \nmid 1$. ■

1.7. teorēma. $p \in k[X]$, $\deg(p) > 0$. Zemāk dotie apgalvojumi ir ekvivalenti:

1. $p \in \mathcal{I}(k[X])$.
2. $k[X]/(p)$ ir lauks.

PIERĀDĪJUMS

<u>1. $\Longrightarrow$ 2.</u>

$p \in \mathcal{I}(k[X]) \implies \forall\ f:\ LKD(f,p) = 1\ \vee\ p|f$. Apskatīsim atsevišķi abus gadījumus.

$LKD(f,p) = 1 \implies [f] \neq 0\ \wedge [f]$ ir invertējams elements.

$p|f \implies f = up \implies [f] = [up] = [u][p] = [u][0] \implies [f] = 0.$

Ir pierādīts, ka ja atlikumu klase nav $[0]$, tad tā ir invertējama.

2. $\Longrightarrow$ 1. Pierādījums izmantojot kontrapozīcijas likumu.
$p \notin \mathcal{I}(k[X]) \Longrightarrow \exists$ divi nekonstanti polinomi g un h:

$$p = gh.$$

$\Longrightarrow [gh] = [g][h] = [p] = [0] \Longrightarrow k[X]/(p)$ nav IG, jo $\exists$ divi nulles dalītāji $[g]$ un $[h]$. ■

1.2. piezīme. $p \in \mathcal{I}(k[X])$. 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 $K_p[X]$: iekļaušana $k \longrightarrow K_p$ inducē iekļaušanu $k[X] \longrightarrow K_p[X]$.

2. Ideāli un faktorgredzeni

2.1. Ideāli

2.1.1. Definīcijas un piemēri

R - komutatīvs gredzens, $J \subseteq R$. Definēsim

$$aJ = \{r \in R | r = ax, \text{ kur } x \in J\}.$$

Kopu $I \subseteq R$ sauksim par *ideālu*, ja

1. I ir apakšgrupa attiecībā uz $+$,
2. $\forall\ r \in R: \ rI \subseteq I$ (I ir slēgta attiecībā uz reizināšanu ar R elementiem).

2.1. piemērs. $\forall$ gredzenā R ir divi izdalīti ideāli - $\{0\}$ un R. Tos sauc par triviālajiem vai neīstajiem ideāliem.

k ir lauks $\Longrightarrow$ $\forall$ ideāls ir vai nu $\{0\}$ vai k.

Gredzenā $\mathbb{Z}$ kopa $m\mathbb{Z}$ ir ideāls $\forall\ m$.

Gredzenā $R[X]$ kopa $mR[X]$ ir ideāls $\forall\ m \in R[X]$.

Ja $R = Fun(\mathbb{R}, \mathbb{R})$, tad kopa $I_a = \{f \in R | f(a) = 0\}$ ir ideāls.

2.2. piemērs. Ir dota polinomiāla vienādojumu sistēma

$$\begin{cases} f_1(X) = 0 \\ ... \\ f_m(X) = 0 \end{cases}$$

Visi polinomi formā

$$h(X) = g_1(X)f_1(X) + ... + g_m(X)f_m(X)$$

arī apmierina vienādojumu $h(X) = 0$. Visi šādi polinomi h veido ideālu - vienādojumu sistēmas *seku ideālu.*

Ideālu $I \subseteq R$ sauc par *pirmideālu*, ja

$$ab \in I \implies a \in I \ \vee \ b \in I.$$

Ideālu $I \subseteq R$ sauc par *maksimālu ideālu*, ja $\forall$ ideālam J izpildās

$$I \subseteq J \implies J = I \ \vee \ J = R.$$

2.3. piemērs. $\mathbb{Z}$ maksimālie un pirmideāli.

2.1. teorēma. R - komutatīvs gredzens, I - ideāls.

$$I \cap \mathcal{U}(R) \neq \emptyset \implies I = R.$$

(Ja ideāls satur multiplikatīvi invertējamu elementu, tad tas ir vienāds ar visu gredzenu).

PIERĀDĪJUMS $u \in \mathcal{U}(R)$, $u \in I$. Tā ka I ir ideāls, tad

$$u^{-1} \cdot u = 1 \in I.$$

$r \in R: \ r \cdot 1 = r \in rI \implies R \subseteq I.$

Bet arī $I \subseteq R \implies R = I.$ ■

2.1.2. Operācijas ar ideāliem

$I_1, ..., I_n$ - ideāli. Par to šķēlumu sauc kopu

$$I_1 \cap ... \cap I_n = \bigcap_{\alpha} I_\alpha.$$

Par ideālu summu sauc kopu

$$I_1 + ... + I_n = \sum_{i=1}^{n} I_i = \{r \in R | r = \sum_{i=1}^{n} x_i, \text{ kur } x_i \in I_i\}.$$

I - ideāls, $a \in R$. Par I *paplašinājumu ar* a $\langle I, a \rangle$ sauc kopu $\{y \in R | y = x + ar\}$, kur $x \in I$, $r \in R$.

2.4. piemērs. $R = \mathbb{Z}$, $I_1 \cap I_2$, $I_1 + I_2$.

2.2. teorēma. Ideālu šķēlums, summa un paplašinājums ir ideāls.

PIERĀDĪJUMS

Šķēlums. $x \in I_\alpha, \forall\ \alpha \implies \forall\ r \in R$ izpildās $rx \in I_\alpha$, tātad

$$rx \in \bigcap_\alpha I_\alpha.$$

Summa. $x = x_1 + x_2 + ... + x_n$, kur $x_i \in I_i \implies \forall\ r \in R$ izpildās

$$rx = \underbrace{rx_1}_{\in I_1} + \underbrace{rx_2}_{\in I_2} + ... + \underbrace{rx_n}_{\in I_n} \in \sum_{i=1}^{n} I_i.$$

Paplašinājums. $y_i = x_1 + ar_i \implies$

$$y_1 + y_2 = (x_1 + x_2) + a(r_1 + r_2) \in \langle I, a\rangle,$$

$$r'(x_i + ar_i) = \underbrace{r'x_i}_{\in I} + a(r'r_i) \in \langle I, a\rangle. \blacksquare$$

2.1.3. Ideālu ģenerēšana

R - gredzens. Kopa $aR = \langle a\rangle$ ir ideāls $\forall\ a \in R$. Tādus ideālus sauc par *galvenajiem ideāliem.*

Ja gredzenā R katrs ideāls ir galvenais, tad R sauc par *galveno ideālu gredzenu (GIG)*.

Fiksētiem elementiem $\{a_1, a_2, ..., a_n\}$ kopa

$$\{r \in R | r = a_1x_1 + a_2x_2 + ... + a_nx_n, \text{ kur } x_i \in R\} = a_1R + a_2R + ... + a_nR$$

ir ideāls, apzīmē ar $\langle a_1, a_2, ..., a_n \rangle$. Tādus ideālus sauc par *galīgi ğenerētiem ideāliem*, elementus $a_1, ..., a_n$ sauc par ideāla *ğeneratoriem*.

2.1. piezīme. Par ideāla ğeneratoru kopu var domāt kā par lineāras telpas bāzes analogu.

2.5. piemērs. Ideāls $\langle 2, X \rangle \in \mathbb{Z}[X]$ nav galvenais, to nevar izteikt formā $\langle a \rangle$. Tā kā $2 \in \langle 2, X \rangle$, tad $a = \pm 2$, bet tad $X \notin \langle 2, X \rangle$.

2.3. teorēma.

1. $\mathbb{Z}$ ir GIG.
2. k - lauks $\Longrightarrow$ $k[X]$ ir GIG.

PIERĀDĪJUMS

1. Dots ideāls $I \subseteq \mathbb{Z}$. Apskatīsim mazāko naturālo skaitli $x \in I$.

Ir skaidrs, ka $x\mathbb{Z} \subseteq I$. Ja $a \in I$, tad izdalīsim a ar x:

$$a = qx + r, \text{ kur } 0 \leq r < x.$$

$$r = \underbrace{a - qx}_{<x} \in I \Longrightarrow r = 0 \Longrightarrow a = qx \Longrightarrow I \subseteq x\mathbb{Z} \Longrightarrow x\mathbb{Z} = I.$$

2. Dots ideāls $I \subseteq k[X]$. Apskatīsim $m \in I$ ar mazāko pakāpi.

Pieņemsim, ka $f \in I$. Izdalīsim f ar m:

$$f = qm + r, \text{ kur } \deg(r) < \deg(m).$$

$$r = f - qm \in I \Longrightarrow r = 0 \Longrightarrow f = qm \Longrightarrow I \subseteq mR[X].$$

$mR[X] \subseteq I \Longrightarrow mR[X] = I.$ ■

2.2. Faktorgredzeni

2.2.1. Definīcijas

$I \subseteq R$ - ideāls. Elementi r_1 un r_2 ir salīdzināmi mod $I(r_1 \equiv r_2 (\text{mod } I))$, tad un tikai tad, ja

$$r_1 - r_2 \in I.$$

2.4. teorēma. *Salīdzināmība mod I ir ekvivalences attiecība gredzenā R.*

PIERĀDĪJUMS Līdzīgs veselo skaitļu un polinomu kongruences gadījumiem. ■

Ekvivalences klases apzīmē veidā $[a]$ vai $a + I$.
Ekvivalences klašu kopu apzīmēsim ar R/I.
Ir definēta dabiskā projekcija

$$\pi : R \to R/I, \pi(a) = [a] = a + I.$$

2.2.2. Operācijas

Operācijas ar ekvivalences klasēm:

- Saskaitīšana - $[a] + [b] = [a + b]$.
- Reizināšana - $[a][b] = [ab]$.

2.5. teorēma.

1. Ekvivalences klašu operācijas ir definētas korekti - nav atkarīgas no pārstāvju izvēles.
2. Ekvivalences klašu kopa R/I ar definētajām operācijām ir komutatīvs gredzens.

PIERĀDĪJUMS
1. Līdzīgi $\mathbb{Z}$ un $R[X]$ gadījumiem.

2. Līdzīgi $\mathbb{Z}$ un $R[X]$ gadījumiem. Aksiomu pārbaude. ■

2.6. piemērs. $\mathbb{Z}/m\mathbb{Z}$, $R[X]/(m)$.

3. 6.mājasdarbs

3.1. Obligātie uzdevumi

6.1 Aprakstiet polinomu kongruences klases dotajos gadījumos:

(a) $\mathbb{Q}[X]$, $m = a_0 \in \mathbb{Q}$;
(b) $\mathbb{Q}[X]$, $m = X^2 - 3$;
(c) $\mathbb{F}_2[X]$, $m = X^3 + X + 1$.

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

(a) Atrodiet K saskaitīšanas un reizināšanas tabulas.
(b) Atrodiet visas K primitīvās saknes: elementus $g \in \mathcal{U}(K)$, kuru kārta ir vienāda ar $|K| - 1$.

6.3 Nosakiet, vai a^{-1} eksistē dotajā faktorgredzenā, atrodiet a^{-1}, ja tas eksistē:

(a) $\mathbb{R}[X]/(X^2 + 1)$, $a = [X^4 - 1]$;
(b) $\mathbb{F}_3[X]/(X^2 + 1)$, $a = [X^2 + X + 1]$.

6.4 Nosakiet, vai dotais faktorgredzens ir lauks:

(a) $\mathbb{F}_2[X]/(X^4 + X^2 + 1)$;

(b) $\mathbb{Q}[X]/(X^2 - 2)$.

6.5 Vai visu multiplikatīvi neinvertējamo elementu kopa ir ideāls gredzenos $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{R}[X]$?

6.6 Pierādīt, ka ideāls $\langle X \rangle \subset \mathbb{Z}[X]$ ir pirmideāls, bet nav maksimāls ideāls.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

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

6.8 R - IG ar vieninieku. Pierādīt, ka $R[X]$ ir GIG tad un tikai tad, ja R ir lauks.