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

Studiju kurss

Polinomu algebra

1.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt viena argumenta polinomu teorijas pamatjēdzienus.

Lekcijas kopsavilkums:

- jebkuram gredzenam R var definēt tā paplašinājumu - *viena argumenta polinomu gredzenu virs* R,
- polinomam var definēt *pakāpi.*

Svarīgākie jēdzieni: gredzens, komutatīvs gredzens, unitārs gredzens, integrāls gredzens, lauks, skaitļu gredzeni, matricu gredzeni, funkciju gredzeni, apakšgredzens, gredzenu homomorfisms un izomorfisms, viena argumenta polinomu gredzens, polinoma koeficienti, locekļi (termi), monomi, vecākais loceklis, pakāpe, substitūcija, polinomu dalāmība, asociācija.

Svarīgākie fakti un metodes: invertējamie elementi veido grupu, polinomi veido gredzenu, polinoma pakāpes īpašības, dalāmības īpašības, asociācijas īpašības, polinomu gredzenā ir lineāras telpas struktūra.

1. Gredzeni - atkārtojums no skaitļu teorijas kursa

1.1. Pamatdefinīcijas

Par *gredzenu* sauc kopu R, kurā ir uzdotas divas bināras operācijas

$$(x, y) \mapsto x + y \ (\textit{aditīvā operācija, saskaitīšana}),$$
$$(x, y) \mapsto xy \ (\textit{multiplikatīvā operācija, reizināšana}),$$

kas apmierina šādas īpašības:

- operācija $\cdot$ ir asociatīva: $(ab)c = a(bc)$,
- ir spēkā kreisā un labā distributīvās īpašības:

$$a(b + c) = ab + ac,$$
$$(a + b)c = ac + bc.$$

Gredzenu sauc par

- *komutatīvu gredzenu*, ja operācija $\cdot$ ir komutatīva: $\forall\ a, b \in R$ izpildās $ab = ba$.

- *gredzenu ar vieninieku (unitāru gredzenu)*, ja $\exists$ neitrālais elements e (1) attiecībā uz reizināšanas operāciju: $\forall\, a \in R$:

$$ae = ea = a.$$

$u \in R$ - *(multiplikatīvi) invertējams*, ja $\exists\ z = a^{-1} \in R$ tāds, ka $az = za = 1$. R invertējamo elementu kopu apzīmē ar $\mathcal{U}(R)$.

1.1. teorēma.

1. $(\mathcal{U}(R), \cdot)$ ir grupa.
2. $\left\{ \begin{array}{l} a \notin \mathcal{U}(R) \\ b \in R \end{array} \right. \Longrightarrow\ ab, ba \notin \mathcal{U}(R).$

PIERĀDĪJUMS

1. Jāpārbauda grupas aksiomas.

2. $ab \in \mathcal{U}(R) \Longrightarrow \exists\, x \in R:\ (ab)x = 1 \Longrightarrow a(bx) = 1 \Longrightarrow$ $a \in \mathcal{U}(R)$ - pretruna. ■

Gredzenu sauc par

- *integrālu gredzenu (IG)*, ja tas ir komutatīvs un tajā nav *nulles dalītāju*: $ab = 0 \implies a = 0 \vee b = 0$;
- *lauku*, ja tas ir IG un $r \neq 0 \implies r \in \mathcal{U}(R)$ $(\mathcal{U}(R) = R \backslash \{0\})$.

1.1. piemērs. Skaitļu un no tiem atvasinātu objektu gredzeni:

- "pats galvenais" gredzens - $\mathbb{Z}$ (IG, bet ne lauks);
- kanoniskie skaitļu gredzeni - $\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ (lauki);
- atlikumu klašu gredzeni mod m - $\mathbb{Z}_m$;
- atlikumu klašu gredzeni mod p, kur p ir pirmskaitlis - $\mathbb{F}_p$ (lauki).

1.2. piemērs. *Matricu gredzeni* - $\mathcal{M}at(n, R)$, kur R ir komutatīvs gredzens, operācijas - matricu saskaitīšana un reizināšana (nekomutatīvi gredzeni ar vieninieku, 0 - nulles matrica, 1 - vienības matrica).

1.3. piemērs. *Funkciju gredzeni.* X - kopa, R - gredzens. $Fun(X, R)$ - visu funkciju $X \to R$ kopa. Definēsim funkciju summu un reizināju-

mu:

$$(f+g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Var pārbaudīt, ka $Fun(X, R)$ ar šādām operācijām veido gredzenu (komutatīvi gredzeni ar nulles dalītājiem).

Gredzena R apakškopu $S \subseteq R$ sauc par *apakšgredzenu* (apzīmē $S \leq R$), ja

- tā veido apakšgrupu attiecībā uz saskaitīšanu (aditīvu apakšgrupu),
- tā ir slēgta atiecībā uz reizināšanu: $a \in S$, $b \in S \implies ab \in S$,
- unitāriem gredzeniem pieprasa, ka apakšgredzens satur 1.

1.2. Gredzenu homomorfismi

$(R_1, +_{R_1}, *_{R_1})$, $(R_2, +_{R_2}, *_{R_2})$ - gredzeni. Funkciju $f : R_1 \to R_2$ sauc par *gredzenu homomorfismu*, ja tā saglabā gredzenu operācijas:

$$f(x *_{R_1} y) = f(x) *_{R_2} f(y),$$
$$f(x +_{R_1} y) = f(x) +_{R_2} f(y).$$

Gredzenu homomorfismu sauc par *gredzenu izomorfismu*, ja tas ir bijektīvs. Ja R_1 un R_2 ir izomorfi gredzeni, tad rakstīsim $R_1 \simeq R_2$.

Ja gredzeni ir izomorfi, tad var uzskatīt, ka tie atšķiras tikai ar elementu un operāciju apzīmējumiem - to operāciju tabulas ir vienādas ar precizitāti līdz elementu apzīmējumiem.

1.4. piemērs. Gredzenu homomorfismu piemēri -

- jebkura gredzena vienības attēlojums,
- mazāka skaitļu gredzena iekļaušana lielākā,
- redukcija mod m.

1.3. Dažas lietderīgas identitātes gredzenos

1.3.1. Pakāpju summa un starpība

$$a^n - b^n = (a-b) \cdot \sum_{i=10}^{n-1} a^{n-1-i} b^i = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1}).$$

$$n \equiv 1 (\text{mod } 2) \implies$$

$$a^n + b^n = (a+b) \cdot \sum_{i=0}^{n-1} (-1)^i a^{n-1-i} b^i = (a+b)(a^{n-1} - a^{n-2}b + ... + ab^{n-2} + b^{n-1}).$$

1.3.2. Kvadrātu summu reizinājums - Brahmaguptas-Fibonači vienādība

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2 = (ac+bd)^2 + (ad-bc)^2.$$

$$(a^2+mb^2)(c^2+md^2) = (ac-mbd)^2 + m(ad+bc)^2 = (ac+mbd)^2 + m(ad-bc)^2.$$

2. Polinomu teorijas pamatfakti

2.1. Pamatdefinīcijas

R - komutatīvs unitārs gredzens. Definēsim $R[X]$ kā visu formālu izteiksmju

$$a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 = \sum_{i=1}^{n} a_i X^i,$$

kur $a_i \in R, n \in \mathbb{N} \cup \{0\}$, kopu.

Var uzskatīt arī, ka $\sum_{i=1}^{n} a_i X^i = \sum_{i=1}^{\infty} a_i X^i$, kur $a_i = 0, \forall\ i \geq n \in \mathbb{N}$.

Divi polinomi ir vienādi $\iff$ tiem ir vienādi koeficienti pie visām argumenta pakāpēm.

Definēsim divas operācijas:

- $\left(\sum_{i=1}^{n} a_i X^i\right) + \left(\sum_{i=1}^{n} b_i X^i\right) = \sum_{i=1}^{n} (a_i + b_i) X^i$

- $\left(\sum_{i=1}^{n} a_i X^i\right) \cdot \left(\sum_{i=1}^{n} b_i X^i\right) = \sum_{j=1}^{n} c_j X^j$, kur $c_j = \sum_{l=0}^{j} a_l b_{j-l}$.

2.1. piemērs. $(X+1)+(X-1) = 2X$, $(X-1)(X+1) = X^2 - 1$, $\mathbb{R}[X]$.

2.1. teorēma.

1. Kopa $R[X]$ ar definētajām operācijām veido komutatīvu gredzenu ar reizināšanas neitrālo elementu 1 un saskaitīšanas neitrālo elementu 0.
2. Elementi formā $a_0 \in R \in R[X]$ veido apakšgredzenu $R_0 \simeq R$.

PIERĀDĪJUMS Patstāvīgs darbs. Ir jāpārbauda visas komutatīvā gredzena aksiomas. ■

$R[X]$ sauc par *viena argumenta polinomu gredzenu virs* R. Locekļu kārtība nav svarīga (komutativitātes dēļ), to izvēlēsimies tā, lai būtu ērtāk strādāt.

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

- Gredzena elementus a_i sauc par polinoma *koeficientiem*.
- Polinomus formā aX^m sauc par *locekļiem (termiem)*.
- Polinomus formā X^m sauc par *monomiem*.
- Polinoma locekli 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* $\deg(f)$.

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

Nulles polinomam 0 pakāpi definē vienādu ar $-\infty$.

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

2.2. Polinoma pakāpe un tās īpašības

2.1. piezīme. Definēsim

$$-\infty < n,$$
$$-\infty + n = -\infty,$$
$$-\infty + (-\infty) = -\infty.$$

2.2. teorēma. R - IG, $f, g \in R[X]$. Tad:

1. $\deg(f+g) \leq \max(\deg(f), \deg(g))$;
2. $\deg(fg) = \deg(f) + \deg(g)$;
3. $R[X]$ ir IG;
4. $f \in \mathcal{U}(R[X]) \iff \begin{cases} \deg(f) = 0 \\ f \in \mathcal{U}(R). \end{cases}$

PIERĀDĪJUMS

1. Divu polinomu summas vecākā koeficienta indekss nevar būt lielāks kā lielākā no polinomu pakāpēm (var būt mazāks, ja koeficienti

pie dažiem monomiem saīsinās).

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

Pieņemsim, ka neviens no polinomiem nav 0.

$$\begin{cases} f = f_n X^n + \dots \\ g = g_m X^m + \dots \end{cases} \Longrightarrow$$

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

R - IG $\Longrightarrow$ $f_n g_m \neq 0 \Longrightarrow$

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

3. $fg = 0 \Longrightarrow \deg(f) + \deg(g) = -\infty \Longleftrightarrow \deg(f) = -\infty$ vai $\deg(g) = -\infty \Longrightarrow f = 0$ vai $g = 0$.

4. $fg = 1 \Longrightarrow \deg(f) + \deg(g) = 0 \Longrightarrow \deg(f) = \deg(g) = 0$ un $f, g \in \mathcal{U}(R)$.

$f \in \mathcal{U}(R) \implies f \in \mathcal{U}(R[X])$, jo $\mathcal{U}(R) \subseteq \mathcal{U}(R[X])$. ■

2.3. Citas pamatīpašības

2.3.1. Lineāras telpas struktūra

k - lauks. Kopā $k[X]$ var definēt lineārās telpas operācijas:

- saskaitīšana: $(f, g) \mapsto f + g$,
- reizināšana ar k elementu (reizināšanu ar skalāru): $(\lambda, f) \mapsto \lambda f$.

2.3. teorēma. *k - lauks.*

1. *$k[X]$ ar saskaitīšanas un reizināšanas operācijām veido k-lineāru telpu.*
2. *Monomu kopa $\{1, X, X^2, ...\}$ ir $k[X]$ bāze (kanoniskā bāze).*

PIERĀDĪJUMS

1. Lineārās telpas aksiomu pārbaude:

- saskaitīšanas asociativitāte un komutativitāte,
- neitrālā un inversā elementa eksistence attiecībā uz saskaitīšanu - 0, $f \to -f$,
- reizināšanas ar skalāru īpašības

2. Var pārbaudīt, ka $\{1, X, ...\}$ ir lineāri neatkarīga kopa

$$\lambda_0 \cdot 1 + \lambda_1 X + ... + \lambda_n X^n = 0 \implies \forall\, i: \ \lambda_i = 0.$$

$\{1, X, ...\}$ ir $k[X]$ veidotājsistēma $\implies$ tā ir bāze. ■

2.3.2. Substitūcijas

$f(X) = a_n X^n + ... + a_0 \in R[X]$. $\forall\ r \in R$ elements $f(r) \in R$ tiek saukts par *substitūciju* vai *substitūcijas rezultātu* (X vietā tiek ievietots konkrēts $r \in R$).

Tādējādi $\forall\ r \in R$ ir definēta funkcija

$$\Phi_r : R[X] \to R, \text{ kur } \Phi_r(f) = f(r).$$

2.4. Dalāmība (polinomu un patvaļīgos gredzenos)

Šajā sadaļā visi gredzeni ir unitāri IG (piemēram, $R[X]$, kur R - IG).

2.4.1. Dalāmības īpašības

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

2.3. piemērs. Ja $n \geq m$, tad $X^m \mid X^n$.

Dalāmības īpašības - līdzīgas veselo skaitļu dalāmības īpašībām.

2.4. teorēma. R - IG, unitārs (piemēram, $A[X]$, kur A - IG).

1. $a \mid b_1,\ a \mid b_2,\ \ldots,\ a \mid b_n \implies a \mid (b_1 + \ldots + b_n)$.
2. $\left\{ \begin{array}{l} a \mid b \\ b \mid c \end{array} \right. \implies a \mid c.$

3. $a \mid b \implies \forall c \in R: \; a \mid bc.$

4. $\left\{ \begin{array}{l} a \mid b \\ c \mid d \end{array} \right. \implies ac \mid bd.$

5. $u \in \mathcal{U}(R) \iff u \mid 1.$

PIERĀDĪJUMS

1.-4.Pierādām līdzīgi veselo skaitļu gredzena gadījumam.

5. $u \in \mathcal{U}(R) \iff \exists\, u' \in R: \; uu' = 1 \iff u \mid 1.$ ■

2.4.2. Dalāmība un asociācija

Šajā sadaļā visi gredzeni ir unitāri IG (piemēram, $R[X]$, kur R - IG).

Ja $b \mid a$ un $a \mid b$, tad a un b sauc par *asociētiem elementiem*, apzīmē ar $a \sim b$ ($\sim$ ir binära attiecība kopā R).

2.4. piemērs. $\mathbb{Z}$ - $\pm a$. $k[X]$ - uf, kur $u \in k$, $u \neq 0$.

2.5. teorēma.

1. $\sim$ ir ekvivalences attiecība (refleksīva, simetriska, tranzitīva).
2. $a \sim b \iff \exists u \in \mathcal{U}(R) : a = ub$.

PIERĀDĪJUMS

1. Refleksivitāte $a = 1 \cdot a$.

Simetrija Seko no definīcijas.

Tranzitivitāte

$$\left\{\begin{array}{l} a\sim b \\ b\sim c \end{array}\right. \iff \left\{\left\{\begin{array}{l} a\,|\,b \\ b\,|\,a \end{array}\right. \left\{\begin{array}{l} b\,|\,c \\ c\,|\,b \end{array}\right.\right. \iff \left\{\left\{\begin{array}{l} a\,|\,b \\ b\,|\,c \end{array}\right. \left\{\begin{array}{l} c\,|\,b \\ b\,|\,a \end{array}\right.\right.$$

$$\Longrightarrow \quad a\sim c.$$

2. $a\sim b \Longrightarrow a=cb=c\underbrace{(c'a)}_{=b}=(cc')a \Longrightarrow$

$$cc'=1 \Longrightarrow c,c'\in\mathcal{U}(R).$$

$$a=ub \Longrightarrow \left\{\begin{array}{l} b\,|\,a \\ b=u^{-1}a \end{array}\right. \Longrightarrow \left\{\begin{array}{l} b\,|\,a \\ a\,|\,b \end{array}\right. \Longrightarrow a\sim b. \ \blacksquare$$

2.2. piezīme. Tā kā $\sim$ ir ekvivalence, ir definētas atbilstošās ekvivalences klases.

3. 1.mājasdarbs

3.1. Obligātie uzdevumi

1.1 Pierādīt, ka komutatīvs unitārs gredzens ir IG tad un tikai tad, ja izpildās *multiplikatīvās saīsināšanas likums*:

$$\text{ja } xy = xz \text{ un } x \neq 0, \text{ tad } y = z.$$

1.2 Atrast piemērus funkciju gredzeniem $\mathcal{F}un(X, R)$, kuros eksistē nulles dalītāji.

1.3 Pierādīt, ka gredzenā $k[X]$, kur k ir lauks, polinomi ar pakāpi 0 dala visus polinomus.

1.4 Pierādīt, ka bezgalīgā gredzenā neinvertējamu (nenulles) elementu kopa ir bezgalīga vai tukša.

1.5 Cik ir dažādu kubisko polinomu virs $\mathbb{F}_p$?

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

1.6 Nosakiet, vai dotās kopas ar dotajām operācijām ir gredzeni:

(a) $(\mathbb{Q}_p, +, \cdot)$, kur $\mathbb{Q}_p = \{m/n \in \mathbb{Q} | LKD(n, p) = 1\}$, $p \in \mathbb{P}$;

(b) $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ reālie skaitļi formā $a + b\sqrt{2}$;

(c) reālie skaitļi formā $a+b\sqrt[3]{2}$, kur $a, b \in \mathbb{Q}$, operācijas - skaitļu saskaitīšana un reizināšana;

(d) simetriskas $n \times n$ matricas ar reāliem elementiem, operācijas - matricu saskaitīšana un reizināšana.

1.7 Dots $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, $n > 0$, $a_n \neq 0$, $\forall\ i\ a_i \in \mathbb{Z}$ - nekonstants polinoms ar veseliem koeficientiem. Pierādīt, ka bezgalīgi daudziem $n \in \mathbb{Z}$ $f(n)$ ir salikts skaitlis ($f(n) = ab$, kur $|a| > 1$ un $|b| > 1$).