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

Studiju kurss

Polinomu algebra

1.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.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*,
- polinomiem var definēt dalīšanu ar atlikumu.

Svarīgākie jēdzieni: gredzens, komutatīvs gredzens, unitārs gredzens, integrāls gredzens, lauks, skaitļu gredzeni, matricu gredzeni, funkciju gredzeni, apakšgredzens, gredzenu homomorfisms un izomorfisms, gredzena paplašinājums ar elementu, polinomiāla funkcija, viena argumenta polinomu gredzens, polinoma koeficienti, locekļi (termi), monomi, vecākais loceklis, pakāpe, substitūcija, polinomu dalāmība, redukcija ar polinomu, polinomu dalījums un dalīšanas atlikums.

Svarīgākie fakti un metodes: invertējamie elementi veido grupu, polinomi veido gredzenu, polinoma pakāpes īpašības, polinomu gredzenā ir lineāras telpas struktūra, redukcija samazina reducējamā polinoma pakāpi, polinomu dalīšana ar atlikumu.

1. Gredzeni - atkārtojums no skaitļu teorijas kursa

1.1. Pamatdefinīcijas

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

$$(x, y) \mapsto x + y \text{ (\textit{aditīvā operācija, saskaitīšana})},$$

$$(x, y) \mapsto xy \text{ (\textit{multiplikatīvā operācija, reizināšana})},$$

kas apmierina šādas īpašības:

- attiecībā uz operāciju $+$ R ir komutatīva grupa:
  - asociativitāte:
  $$(a + b) + c = a + (b + c),$$
  - eksistē neitrālais elements 0 : $\forall\ a$ izpildās
  $$a + 0 = 0 + a = a,$$

- katram a eksistē inversais elements $-a$:

$$a + (-a) = (-a) + a = 0,$$

- komutativitāte: $a + b = b + a$,

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

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

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

Gredzenus apzīmēsim ar pierakstu $(R, +, \cdot)$.

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. $\begin{cases} a \notin \mathcal{U}(R) \\ b \in R \end{cases} \implies ab, ba \notin \mathcal{U}(R).$

PIERĀDĪJUMS
1. Jāpārbauda grupas aksiomas.

2. $ab \in \mathcal{U}(R) \implies \exists\ x \in R:\ (ab)x = 1 \implies a(bx) = 1 \implies$ $a \in \mathcal{U}(R)$ - 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* - $\mathcal{M}(n, R)$, 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 reizinājumu:

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

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):
  - ja $a \in S$ un $b \in S$, tad $a + b \in S$;
  - $0 \in S$;
  - ja $a \in S$, tad $-a \in S$,
- tā ir slēgta atiecībā uz reizināšanu: $a \in S$, $b \in S \implies ab \in S$.

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.

2. Polinomu teorijas pamatfakti

2.1. Motivācijas un naivā definīcija

2.1.1. Gredzenu paplašinājumi

Visi gredzeni ir komutatīvi un unitāri.

R - gredzens, $S \leq R$. $\forall\ t \in R$ definēsim apakšgredzena S *paplašinājumu ar* t - kopu

$$S[t] = \{b \in R | b = a_0 + a_1 t + a_2 t^2 + ... + a_n t^n\}.$$

Citiem vārdiem sakot, $S[t]$ ir mazākais apakšgredzens, kas satur S un t. Redzam, ka divu $S[t]$ elementu

$$a(t) = a_0 + a_1 t + a_2 t^2 + ... + a_n t^n,$$
$$b(t) = b_0 + b_1 t + b_2 t^2 + ... + b_n t^n$$

summa un reizinājums ir definēti šādā veidā:

$$a(t) + b(t) = (a_0 + b_0) + (a_1 + b_1)t + (a_2 + b_2)t^2 + ... + (a_n + b_n)t^n,$$
$$a(t) \cdot b(t) = (a_0 b_0) + (a_1 b_1 + a_0 b_1)t + (a_2 b_0 + a_1 b_1 + a_0 b_2)t^2 + ...$$

Lietderīgi ir pētīt gredzenu $S[t]$ uzskatot t par ārēju elementu, kas neapmierina nekādas sakarības.

2.1.2. Polinomiālas funkcijas

Ja funkcija $f : R \to R$ ir uzdota veidā

$$f(t) = f_0 + f_1 t + f_2 t^2 + ... + f_n t^n,$$

tad sauksim to par *polinomiālu funkciju*. Visu polinomiālu funkciju kopu apzīmēsim ar $\mathcal{P}ol(R, R)$. Kopā $\mathcal{P}ol(R, R)$ var definēt gredzena struktūru kā aprakstīts iepriekšējā punktā un pētīt šo jauno gredzenu.

2.2. Viena argumenta polinomi

2.2.1. Pamatdefinīcijas

R - komutatīvs unitārs gredzens, R^* - tā elementu bezgalīgu virkņu kopu, kurās ir tikai galīgs skaits nenulles elementu - virknes formā $(a_0, a_1, ..., a_n, 0, 0, ...)$.

Virknes $f \in R^*$ i-to elementu var apzīmēt ar f_i.

Kopā R^* definēsim divas bināras operācijas $+$ un $\cdot$ šādā veidā. Ja

$$f = (f_0, f_1, ..., f_n, 0, ...),$$
$$g = (g_0, g_1, ..., g_n, 0, ...),$$

tad

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, ..., f_n + g_n, 0, ...),$$

$$f \cdot g = (h_0, h_1, h_2, ...), \text{ kur } h_k = \sum_{i=0}^{k} f_i g_{k-i}.$$

2.1. piemērs. $h_0 = f_0 g_0$, $h_1 = f_0 g_1 + f_1 g_0$, $h_2 = f_0 g_2 + f_1 g_1 + f_2 g_0$.

2.1. teorēma. Kopa R^* ar definētajām operācijām veido komutatīvu gredzenu ar vieninieku $(1, 0, \ldots)$ un nulli $(0, 0, \ldots)$.

PIERĀDĪJUMS Patstāvīgajam darbs, lasīt papildmateriālu. Ir jāpārbauda visas komutatīvā gredzena aksiomas. ■

$$\begin{cases} f = (f_0, 0, \ldots) \\ g = (g_0, 0, \ldots) \end{cases} \Longrightarrow \begin{cases} f + g = (f_0 + g_0, 0, \ldots) \\ fg = (f_0 g_0, 0, \ldots) \end{cases} \Longrightarrow$$

elementi formā $(a, 0, \ldots)$ veido apakšgredzenu $R_0 \simeq R$, tāpēc R_0 var identificēt ar R.

Apzīmēsim ar X elementu $(0, 1, 0, \ldots)$. Redzam, ka

$$X^2 = (0, 0, 1, 0, \ldots),$$

$$X^3 = (0, 0, 0, 1, 0, \ldots), \ldots,$$

$$aX^n = (\underbrace{0, \ldots, 0}_{n \text{ nulles}}, a, 0, \ldots),$$

$$a_0 + a_1X + a_2X^2 + ... + a_nX^n = (a_0, a_1, ..., a_n, 0, ...).$$

$(R^*, +, \cdot)$ sauc par *viena argumenta polinomu gredzenu virs* R, apzīmē kā $R[X]$. Parasti polinomus mēs rakstīsim formā

$$a_nX^n + a_{n-1}X^{n-1} + ... + a_1X^1 + a_0.$$

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

Simbola X vietā var lietot jebkuru citu simbolu: $R[X] \simeq R[Y]$ visiem simboliem 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 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* $\deg(f)$.

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

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

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

2.2.2. Polinoma pakāpe un tās īpašības

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

2.1. piezīme. Definēsim

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

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

1. $\deg(f+g) \le \max(\deg(f), \deg(g))$;
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.

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

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

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 $f, g \in \mathcal{U}(R)$.

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

2.2.3. 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, $f \rightarrow -f$,
- reizināšanas ar skalāru īpašības

- $\lambda(f+g) = \lambda f + \lambda g$,
- $(\lambda + \mu) f = \lambda f + \mu g$,
- $1 \cdot f = f$,
- $(\lambda\mu) f = \lambda(\mu f)$.

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. ■

2.2.4. 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

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

2.2.5. 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 $f = hg$.

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

Dalāmības īpašības - līdzīgas veselo skaitļu dalāmības īpašībām.

2.2.6. Dalīšana ar atlikumu

R ir IG, $f, g \in R[X]$, $\deg(f) \geq \deg(g)$ un g vecākais koeficients ir invertējams. Definēsim operāciju polinomu kopā - *f redukciju ar g:*

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

2.4. piemērs.
$\mathcal{R}_{X+1}(X^2+1) = (X^2+1) - X(X+1) = -X+1.$

2.4. teorēma. $\deg\Big(\mathcal{R}_g(f)\Big) < \deg(f).$

PIERĀDĪJUMS

$$\begin{cases} \mathcal{H}(f) = a_n X^n \\ \mathcal{H}(g) = b_m X^m, n \geq m \end{cases} \implies \frac{\mathcal{H}(f)}{\mathcal{H}(g)} = \frac{a_n}{b_m} X^{n-m}.$$

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

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

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

2.5. teorēma. (*viena argumenta polinomu dalīšana ar atlikumu*) R ir IG, $f, g \in R[X]$ 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

q un r eksistence.

Veiksim pēctecīgi redukcijas $\mathcal{R}_g$ sākot ar f, tik ilgi, kamēr redukcija ir definēta. Iegūsim polinomu virkni

$$f \to \mathcal{R}_g(f) \to \mathcal{R}_g^2(f) \to \dots \to \mathcal{R}_g^l(f), \text{ kur } \deg \mathcal{R}_g^l(f) < \deg g.$$

Ir spēkā polinomiālu vienādību sistēma

$$\begin{cases} \mathcal{R}_g(f) = f - q_1 g \\ \mathcal{R}_g^2(f) = \mathcal{R}_g(f) - q_2 g \\ \dots \\ \mathcal{R}_g^l(f) = \mathcal{R}_g^{l-1}(f) - q_l g. \end{cases}$$

Saskaitot vienādību kreisās un labās puses, iegūsim

$$\sum_{i=1}^{l} \mathcal{R}_g^i(f) = f + \sum_{i=1}^{l-1} \mathcal{R}_g^i(f) + \sum_{i=1}^{l} q_i g \implies$$

$$\underbrace{\mathcal{R}_g^l(f)}_{=r} = f - g \underbrace{\sum_{i=1}^{l} q_i}_{=q} \implies$$

$$f = qg + r, \text{ kur } \deg r < \deg g.$$

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

$$f = qg + r = q'g + r' \implies (q - q')g = r' - r.$$

Zinām, ka $\deg(r' - r) < \deg(g)$.

$$\deg\Big((q - q')g\Big) = \deg(q - q') + \deg(g) < \deg(g) \implies$$
$$\deg(q - q') = -\infty \implies \begin{cases} q = q', \\ r = r'. \end{cases} \quad \blacksquare$$

2.5. piemērs. $f = X^5 + X^2 + 1$, $g = X^2 + X + 1$ virs $\mathbb{Z}$.
$\mathcal{R}_g(f) = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} \cdot g = f - X^3 \cdot g = -X^4 - X^3 + X^2 + 1;$
$\mathcal{R}_g^2(f) = \mathcal{R}_g(f_1) = f_1 - (-X^2) \cdot g = 2X^2 + 1;$

$\mathcal{R}_g^3(f) = \mathcal{R}_g(f_2) = f_2 - 2 \cdot g = -2X - 1.$
$\mathcal{R}_g^4(f)$ nav definēts, jo $\deg\left(\mathcal{R}_g^3(f)\right) < \deg(g)$.

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

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

Vēlams izmantot dalīšanu "ar stūrīti".

Izdalot šos pašus polinomus virs $\mathbb{F}_2$ iegūsim

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

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 X - kopa, $\mathcal{P}(X)$ - tā apakškopu kopa. Pierādīt, ka $(\mathcal{P}(X), \Delta, \cap)$ ir gredzens, atrast aditīvo neitrālo elementu, aditīvā inversā elementa atrašanas operāciju, multiplikatīvo neitrālo elementu, multiplikatīvi invertējamos elementus.

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

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

1.5 Izdalīt polinomus:

a) $X^4 + X + 1$ ar $X + 1$ virs $\mathbb{Z}$,
b) $X^6 + X^4 + X^3 + X^2 + X$ ar $X^4 + X + 1$ virs $\mathbb{F}_2$,
c) $X^n + X^{n-1} + X$ ar $X^2 + 1$ virs $\mathbb{F}_2$, katram $n \geq 2$.

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.