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

Studiju kurss

Polinomu algebra

1.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Ievads **4**

2. Gredzeni - atkārtojums no skaitļu teorijas kursa **6**
2.1. Pamatdefinīcijas 6
2.2. Gredzenu homomorfizmi 12

3. Polinomu teorijas pamatfakti **14**
3.1. Motivācijas 14
3.1.1. Gredzenu paplašinājumi 14
3.1.2. Polinomiālas funkcijas 15
3.2. Viena argumenta polinomi 16
3.2.1. Pamatdefinīcijas 16
3.2.2. Substitūcijas 25
3.2.3. Dalāmība 26
3.2.4. Dalīšana ar atlikumu 26
3.3. Viena argumenta pakāpju rindas (patstāvīgā lasīšana) 33

4. 1.mājasdarbs 37

1. Ievads

Studiju kurss "POLINOMU ALGEBRA"

Docētājs - Pēteris Daugulis, Ph.D., DU vadošais pētnieks
Tālr.: katedras telefons,
E-pasts: pdk@ru.lv

Webvieta lekciju materiāliem, mājasdarbiem un citai informācijai:
http://www.de.dau.lv/matematika/daugulis-pa/daugulis-pa.html

Pārbaudes formas:

- rakstiski mājasdarbi,
- viens rakstisks kontroldarbs,
- rakstisks eksāmens.

Kontroldarba un eksāmena darba izpildes laikā atļauts izmantot

personīgos lekciju konspektus, docētāju sagatavotus metodiskos materiālus un vispārīga rakstura mācību grāmatas. Visi uzdevumi ir jāpilda pilnīgi patstāvīgi.

Galīgā vērtējuma veidošanās:

- mājasdarbi - 30%,
- kontroldarbs - 30%,
- eksāmena darbs - 30%,
- paaugstinātas grūtības uzdevumi - 10%.

Literatūra:

- Mācību grāmatas - DU pieejamās grāmatas algebrā (latviešu, angļu, krievu valodā)
- Papildliteratūra -
  Šteiners K Augstākā matemātika IV, lekciju konspekts inženierzinātņu un dabaszinātņu studentiem. - R.:Apgāds Zvaigzne ABC, 1999. - 167.lpp.
- Internet resursi - www.wikipedia.org.

2. Gredzeni - atkārtojums no skaitļu teorijas kursa

2.1. 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:

- 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: visiem $a, b \in R$ izpildās $ab = ba$.

Gredzenu sauc par *gredzenu ar vieninieku (unitāru gredzenu)*, ja eksistē neitrālais elements 1 attiecībā uz reizināšanas operāciju: katram $a \in R$ izpildās

$$a \cdot 1 = 1 \cdot a = a.$$

Pēc noklusēšanas šajā kursā uzskatīsim, ka visi gredzeni ir unitāri.

Gedzena elementu sauksim par *(multiplikatīvi) invertējamu*, ja tam eksistē labais un kreisais inversais elements attiecībā uz reizināšanu: $a \in R$ ir invertējams, ja eksistē $z = a^{-1} \in R$ tāds, ka $az = za = 1$. R invertējamo elementu kopu apzīmēsim ar $U(R)$.

2.1. teorēma.

1. Kopa $U(R)$ ir grupa attiecībā uz reizināšanas operāciju.
2. $a \notin U(R) \wedge b \in R \implies au, ua \notin U(R)$.

PIERĀDĪJUMS

1. Jāpārbauda grupas aksiomas.

2. Dots, ka $a \notin U(R)$, $b \in R$. Pieņemsim, ka $au \in U(R)$. Seko, ka eksistē x tāds, ka $au \cdot x = 1$. Seko, ka $a(ux) = 1 \implies a$ ir invertējams - pretruna.

■

Gredzenu sauc par *integrālu gredzenu*, ja tas ir komutatīvs un tajā nav *nulles dalītāju*: $ab = 0 \implies a = 0 \vee b = 0$.

Integrālu gredzenu R sauc par *lauku*, ja visi nenulles elementi ir invertējami: $u \neq 0 \implies u \in U(R)$.

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

- "Pats galvenais" gredzens - $\mathbb{Z}$ (integrāls gredzens, bet ne lauks);
- kanoniskie skaitļu gredzeni - $\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ (lauki);
- atlikumu klašu gredzeni mod m - $\mathbb{Z}_m$ (komutatīvi gredzeni ar nulles dalītājiem, ja m nav pirmskaitlis).
- atlikumu klašu gredzeni mod p, kur p ir pirmskaitlis - $\mathbb{F}_p$,$GF(p)$ (lauki).

2.2. 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).

2.3. piemērs. *Funkciju gredzeni.* Fiksēsim kopu X un gredzenu R. Apzīmēsim ar $Fun(X, R)$ visu funkciju $X \to R$ kopu. 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).

Viens no svarīgākajiem modernās matemātikas sasniegumiem (1940.-1960.gadi) - jebkurš komutatīvs gredzens var tikt interpretēts kā nepārtrauktu funkciju gredzens virs kādas kopas (gredzena *spektra*).

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: ja $a \in S$ un $b \in S$, tad $ab \in S$.

2.2. Gredzenu homomorfizmi

Ja ir doti divi gredzeni $(R_1, +_{R_1}, *_{R_1})$ un $(R_2, +_{R_2}, *_{R_2})$, tad funkciju

$$f : R_1 \to R_2$$

sauc par *gredzenu homomorfizmu*, ja tā saglabā gredzena operācijas (komutē ar gredzena operācijām):

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

Gredzenu homomorfizmu sauc par *gredzenu izomorfizmu*, 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.

2.4. piemērs. Gredzenu homomorfizmu piemēri -

- jebkura gredzena vienības attēlojums,
- nulles attēlojums starp jebkuriem diviem gredzeniem,
- mazāka skaitļu gredzena iekļaušana lielākā,
- redukcija mod m.

3. Polinomu teorijas pamatfakti

3.1. Motivācijas

3.1.1. Gredzenu paplašinājumi

Sākot no šīs vietas uzskatīsim, ka visi gredzeni ir komutatīvi.

Pieņemsim, ka R ir komutatīvs gredzens, $S \subseteq R$ ir tā apakšgredzens. Katram $t \in R$ 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 apakšgredzenu $S[t]$ uzskatot t par ārēju elementu, kas neapmierina nekādas sakarības.

3.1.2. 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.

3.2. Viena argumenta polinomi

3.2.1. Pamatdefinīcijas

Pieņemsim, ka ir dots komutatīvs gredzens R, apzīmēsim ar 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

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, ..., f_n + g_n, 0, ...),$$
$$f \cdot g = (h_0, h_1, h_2, ...),$$

kur

$$h_k = \sum_{i=0}^{k} f_i g_{k-i}.$$

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

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

PIERĀDĪJUMS (Daļēji patstāvīgajam darbam) Ir jāpārbauda visas komutatīvā gredzena aksiomas:

- Komutatīvas grupas struktūra attiecībā uz +:
  - asociativitāte izpildās katram indeksam, tātad arī visai virknei,
  - neitrālais elements ir nulles virkne $(0, ...)$,
  - elementa $f = (a_0, a_1, ...)$ aditīvi inversais elements

$$-f = (-a_0, -a_1, ...),$$

– komutativitāte izpildās katram indeksam, tātad arī visai virknei,

- operācijas $\cdot$ asociativitāte: pierādām, ka asociativitāte izpildās katram indeksam, ja

$$f = (a_0, a_1, ..., a_n, 0, ...),$$
$$g = (b_0, b_1, ..., b_n, 0, ...),$$
$$h = (c_0, c_1, ..., c_n, 0, ...),$$

tad

$$((f \cdot g) \cdot h)_k = \sum_{i=0}^{k} (\sum_{j=0}^{i} a_j b_{i-j}) c_{k-i} =$$

$$= \sum_{j=0}^{k} a_j (\sum_{i=j}^{k} b_{i-j} c_{k-i}) = \sum_{i=0}^{k} a_i (\sum_{j=i}^{k} b_{j-i} c_{k-j}),$$

no otras puses,

$$(f \cdot (g \cdot h))_k = \sum_{i=0}^{k} (\sum_{j=0}^{k-i} a_i b_j) c_{k-i-j} = \sum_{i=0}^{k} a_i (\sum_{j'=i}^{k} b_{j'-i} c_{k-j'}),$$

kur $j' = i + j$,

- distributivitāte: pierādām, ka distributivitāte izpildās katram indeksam,
- operācijas $\cdot$ komutativitāte: pierādām, ka komutativitāte izpildās katram indeksam,
- multiplikatīvā neitrālā elementa (vieninieka) eksistence: apzīmējam $(1, 0, ...)$ ar 1, pārbaudām, ka katram $f \in R^*$ izpildās $f \cdot 1 = 1 \cdot f = f$.

■

Ja $f = (f_0, 0, ...)$, $g = (g_0, 0, ...)$, tad

$$f + g = (f_0 + g_0, 0, ...),$$

$$fg = (f_0 g_0, 0, ...).$$

Tādējādi elementi formā $(a, 0, ...)$ veido apakšgredzenu, kas ir izomorfs sākotnējam gredzenam R, tāpēc šo apakšgredzenu var identificēt ar R un ievērot, ka $R \leq R^*$.

3.2. piemērs. $(a, 0, ...,)(f_0, f_1, ...) = (af_0, af_1, ...)$.

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

$$X^2 = (0, 0, 1, 0, ...),$$

$$X^3 = (0, 0, 0, 1, 0, ...),$$

$$...$$

Redzam, ka $(\underbrace{0, ..., 0}_{k \text{ nulles}}, a, 0, ...) = aX^k$ un

$$(a_0, a_1, ..., a_n, 0, ...) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n.$$

Kopu R^* ar divām definētajām binārajām operācijām sauc par *viena argumenta polinomu gredzenu virs* R, apzīmē kā $R[X]$. Parasti polinomus mēs rakstīsim formā

$$a_0 + a_1X + a_2X^2 + ... + a_nX^n.$$

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 sauksim par *locekļiem (termiem)*.

Polinomus formā X^m sauksim 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* $\deg(f)$.

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

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

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

Divi polinomi ir vienādi tad un tikai tad, ja tiem ir vienādi koeficienti pie visām argumenta pakāpēm.

3.1. piezīme. Definēsim

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

.

3.2. teorēma. Ja R ir integrāls gredzens un $f, g \in R[X]$, tad ir spēkā šādi apgalvojumi:

1. $\deg(f+g) \leq \max(\deg(f), \deg(g))$;
2. $\deg(fg) = \deg(f) + \deg(g)$;
3. $R[X]$ ir integrāls gredzens;
4. $f \in U(R[X]) \iff \deg(f) = 0 \wedge f \in U(R)$.

PIERĀDĪJUMS

1. Divu polinomu summas vecākā koeficienta indekss nevar būt lielāks nekā lielākā no polinomu pakāpēm (var būt mazāks, ja koeficienti pie dažiem monomiem saīsinās).

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

Pieņemsim, ka neviens no polinomiem nav 0. Polinomu reizinājuma vecākais koeficients ir polinomu vecāko koeficientu reizinājums. Ja

$$f = f_n X^n + ...,$$
$$g = g_m X^m + ...,$$

tad

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

Ja R ir integrāls gredzens, tad $f_n g_m \neq 0$ un

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

3. $fg = 0 \implies \deg(f) + \deg(g) = -\infty$. Tas ir iespējams tikai tad, ja $\deg(f) = -\infty$ vai $\deg(g) = -\infty$, tātad $f = 0$ vai $g = 0$.

4. $fg = 1 \implies \deg(f) + \deg(g) = 0 \implies \deg(f) = \deg(g) = 0$ un $f, g \in U(R)$.

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

3.2.2. Substitūcijas

Ja ir dots polinoms $f(X) = a_n X^n + ... + a_0 \in R[X]$, tad katram $t \in R$ elements $f(t)$ tiek saukts par *substitūciju* vai *substitūcijas rezultātu* (X vietā tiek ievietots konkrēts elements t).

Tādējādi katram $t \in R$ ir definēta funkcija

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

Var redzēt, ka katram t funkcija Φ_t ir gredzenu homomorfizms:

$$\Phi_t(f+g) = (f+g)(t) = f(t) + g(t) = \Phi_t(f) + \Phi_t(g)$$
$$\Phi_t(fg) = (fg)(t) = f(t)g(t) = \Phi_t(f)\Phi_t(g).$$

3.2.3. 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 $f = hg$.

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

Dalāmības īpašības - līdzīgas veselo skaitļu dalāmības īpašībām.

3.2.4. Dalīšana ar atlikumu

R ir integrāls komutatīvs gredzens, $f, g \in R[X]$, $\deg(f) \geq \deg(g)$ un g vecākais koeficients ir invertējams. Definēsim

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

(f *redukcija ar* g)

3.5. piemērs.

3.3. teorēma. $\deg\Big(\mathcal{R}(f,g)\Big) < \deg(f)$.

PIERĀDĪJUMS Pieņemsim, ka $\mathcal{H}(f) = a_n X^n$, $\mathcal{H}(g) = b_m X^m$, kur $n \geq m$.

Ievērosim, ka $\frac{\mathcal{H}(f)}{\mathcal{H}(g)}$ ir polinoms $\frac{a_n}{b_m} X^{n-m}$.

Redzam, ka

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

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

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

3.6. piemērs. $f = X^5 + X^2 + 1$, $g = X^2 + X + 1$ virs $\mathbb{Z}$. Veiksim vairākas redukcijas pēctecīgi:

1.

$$f \to f_1 = \mathcal{R}(f,g) = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} \cdot g = f - X^3 \cdot g = -X^4 - X^3 + X^2 + 1;$$

2.

$$f_1 \to f_2 = \mathcal{R}^2(f,g) = \mathcal{R}(f_1,g) = f_1 - (-X^2) \cdot g = 2X^2 + 1;$$

$$f_2 \to f_3 = \mathcal{R}^3(f,g) = \mathcal{R}(f_2,g) = f_2 - 2 \cdot g = -2X - 1;$$

Redzam, ka $\mathcal{R}^4(f,g)$ nav definēts, jo $\deg\left(\mathcal{R}^3(f,g)\right) < \deg(g)$.

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

$$\begin{aligned} f = X^3 g + f_1 &= X^3 g + (-X^2) g + f_2 = \\ &= X^3 g + (-X^2) g + 2g + (-2X - 1) = \\ &= (X^3 - X^2 + 2) g + (-2X - 1). \end{aligned}$$

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

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

3.4. teorēma. (*viena argumenta polinomu dalīšana ar atlikumu*) Ja R ir integrāls komutatīvs gredzens, $f, g \in R[X]$ un g vecākais koeficients ir invertējams, tad eksistē viens un tikai viens polinomu pāris $q, r \in R[X]$ tāds, ka

1. $f = qg + r$,
2. $\deg(r) < \deg(g)$.

PIERĀDĪJUMS Pieņemsim, ka

$$f = a_n X^n + \ldots + a_0,$$
$$g = b_m X^m + \ldots + b_0,$$

kur $a_n, b_m \neq 0$ un b_m^{-1} eksistē.

q un r eksistence.

1.apakšgadījums. Ja $m > n$, tad definēsim

$$q = 0, r = f.$$

2.apakšgadījums. Ja $m \leq n$, tad izmantosim matemātisko indukciju ar indukcijas parametru $\deg(f)$.

Indukcijas bāze. Ja $n = 0$, tad definēsim

$$q = \frac{a_n}{b_m}, r = 0.$$

Indukcijas solis. Pieņemsim, ka (q, r) eksistences apgalvojums ir spēkā, ja $\deg(f) < n$ un pierādīsim, ka tad tas ir spēkā, ja $\deg(f) = n$.

Atradīsim $\mathcal{R}(f, g) = f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)} g$. Apzīmēsim $\frac{\mathcal{H}(f)}{\mathcal{H}(g)}$ ar q_0.

Redzam, ka

$$f = q_0 g + \mathcal{R}(f, g),$$

kur $\deg(\mathcal{R}(f,g)) < n = \deg(f)$.

Saskaņā ar indukcijas pieņēmumu eksistē polinomi q_1, r_1 tādi, ka

$$\mathcal{R}(f,g) = q_1 g + r_1, \text{ kur } \deg(r_1) < \deg(g) = m.$$

Tagad redzam, ka

$$f = q_0 g + \mathcal{R}(f,g) = q_0 g + (q_1 g + r_1) = (q_0 + q_1)g + r_1.$$

Varam definēt $q = q_0 + q_1$ un $r = r_1$.

q un r vienīgums.

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

$$f = qg + r = q'g + r'.$$

Tas nozīmē, ka $(q - q')g = r' - r$.

Zināms, ka $\deg(r' - r) < \deg(g)$.

No otras puses, $\deg\Big((q-q')g\Big) = \deg(q-q') + \deg(g)$. Tā kā

$$\deg\Big((q-q')g\Big) = \deg(q-q') + \deg(g) < \deg(g),$$

tad $\deg(q-q') = -\infty \implies \begin{cases} q = q', \\ r = r'. \end{cases}$ ■

3.3. Viena argumenta pakāpju rindas (patstāvīgā lasīšana)

Polinomi tika definēti kā ierobežotas gredzena elementu virknes - tikai galīgs skaits elementu virknē ir atšķirīgi no nulles.

Ja atļausim neierobežotas elementu virknes, tad iegūsim *viena argumenta pakāpju rindu gredzenus*.

Pieņemsim, ka ir dots komutatīvs gredzens R, apzīmēsim ar $R^\sharp$ tā elementu bezgalīgu virkņu kopu. Atšķirībā no R^* kopas $R^\sharp$ elementiem $(a_0, a_1, ..., a_n, ...)$ var būt bezgalīgi daudz nenulles elementu.

Kopā $R^\sharp$ definēsim divas bināras operācijas tāpat kā kopā R^*.

Jāatzīmē, ka šīs operācijas ir korekti definētas, jo katra koeficienta aprēķināšanai ir jāveic galīgs skaits gredzena operāciju.

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

Tāpat kā polinomu gadījumā apzīmēsim ar X elementu $(0, 1, 0, ...)$. Redzam, ka jebkurš

$$(a_0, a_1, ...) \in R^\sharp$$

viennozīmīgi izsakās formā

$$(a_0, a_1, ...) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n + ... = \sum_{i=0}^{\infty} a_i X^i.$$

Kopu $R^\sharp$ ar divām definētajām binārajām operācijām sauc par *viena argumenta (formālo) pakāpju rindu gredzenu virs* R, apzīmē kā $R[[X]]$, elementus sauc par (formālām) pakāpju rindām.

Polinomu var uzskatīt par pakāpju rindu, tāpēc ir definēta funkcija

$$R[X] \to R[[X]],$$

$$f(X) \mapsto f(X)$$

(dabiskā iekļaušana).

Pakāpju rindu gredzenos elementa pakāpei deg nav jēgas. Tās vietā definē elementa *kārtu*: par pakāpju rindas f kārtu $\omega(f)$ sauc minimālo indeksu, kuram atbilstošais koeficients nav nulle (jaunākā koeficienta indeksu).

3.6. teorēma. Ja R ir integrāls gredzens un $f, g \in R[[X]]$, tad ir spēkā šādi apgalvojumi

1. $\omega(f+g) \geq \min(\omega(f), \omega(g))$.
2. $\omega(fg) = \omega(f) + \omega(g)$.
3. $R[[X]]$ ir integrāls gredzens.
4. dabiskā iekļaušana $R[X] \to R[[X]]$ ir gredzenu homomorfizms.

PIERĀDĪJUMS 1. Divu pakāpju rindu summas jaunākā koeficienta indekss nevar būt mazāks kā mazākā no pakāpju rindu kārtām (var būt lielāks, ja koeficienti pie dažiem monomiem saīsinās).

2. Pakāpju rindu reizinājuma jaunākais koeficients ir pakāpju rindu jaunāko koeficientu reizinājums. Ja

$$f = a_n X^n + ...,$$
$$g = b_m X^m + ...,$$

tad

$$fg = (a_n X^n + ...)(b_m X^m + ...) = (a_n b_m) X^{n+m} + ...$$

Ja gredzens ir integrāls, tad $a_n b_m \neq 0$ un

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

3. Ja $fg = 0$, tad $\deg(f) + \deg(g) = -\infty$. Tas ir iespējams tikai tad, ja $f = 0$ vai $g = 0$.

4. Dabiskās iekļaušanas sašaurinājums uz $R[X] \subset R[[X]]$ ir vienības funkcija, tātad tas ir gredzenu homomorfizms. ■

4. 1.mājasdarbs

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

1.3 Atrodiet piemērus funkciju gredzeniem $Fun(X, R)$, 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 $n \geq 2$.