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

Studiju kurss

Polinomu algebra

1.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Gredzeni - atkārtojums no skaitļu teorijas kursa

1.1. Pamatdefinīcijas

Par *gredzenu (ring)* sauc kopu R, kurā ir uzdotas divas binārās operācijas

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

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 $a + 0 = 0 + a$,
  - katram a 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: $a(b+c) = ab + ac, (a+b)c = ac + bc$.

Var domāt, ka ir dotas divas operāciju tabulas, kurās rindas un kolonnas tiek indeksētas ar kopas elementiem, un rūtiņās tiek ierakstīti operāciju rezultāti.

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

Gredzenu sauc par komutatīvu, 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.

Gredzena 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 $U(R)$. Kopa $U(R)$ ir grupa attiecībā uz reizināšanas operāciju.

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

Integrālu gredzenu sauc par *lauku*, ja visi nenulles elementi ir invertējami: ja $u \neq 0$, tad u ir invertējams.

1.1. piemērs. Skaitļu gredzeni.

"Pats galvenais" gredzens - $\mathbb{Z}$ (integrāls gredzens, bet ne lauks).

Kanoniskie skaitļu gredzeni - $\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ (lauki).

Gausa skaitļu gredzens $\mathbb{Z}[i]$, Eizenšteina skaitļu gredzens $\mathbb{Z}[\zeta]$ (integrāli gredzeni, bet ne 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 mod p - U_p ($\mathbb{F}_p$,$GF(p)$) (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. 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).

1.4. piemērs. Kopas X pakāpju kopa $\mathcal{P}(X)$ ar operācijām Δ (simetriskā starpība) un $\cap$ (šķēlums) (komutatīvi gredzeni ar nulles

dalītājiem).

1.2. 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):

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

Par gredzenu homomorfizmu var domāt kā par funkciju, kas saglabā gredzenu operāciju tabulas.

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.

Par gredzenu homorfizma $f : R_1 \to R_2$ *attēlu* sauc kopu

$$Im(f) = \{b \in R_2 | \exists a : b = f(a)\}.$$

Par gredzenu homorfizma $f : R_1 \to R_2$ *kodolu* sauc kopu

$$Ker(f) = \{a \in R_1 | f(a) = 0_{R_2}\}.$$

1.5. piemērs. Gredzenu homomorfizmu piemēri -

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

Ja $m_1 \neq m_2$, tad $\mathbb{Z}_{m_1} \not\cong \mathbb{Z}_{m_2}$.

1.3. Apakšgredzeni

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 $ab \in S$.

1.6. piemērs. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

1.1. teorēma. Jebkura gredzenu homomorfizma attēls ir apakšgredzens.

2. Polinomu teorijas pamatfakti

2.1. Motivācijas

2.1.1. Gredzenu paplašinājumi

Pieņemsim, ka R ir komutatīvs gredzens, $S \subseteq R$ ir tā apakšgredzens. Katram $t \in R$ definēsim apakšgredzena S *paplašinājumu ar* t - kopu

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

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 kopu $S[t]$ 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.

Neliela problēma šajā pieejā ir tur, ka galīgiem laukiem dažādi polinomi var uzdot vienādas funkcijas.

2.2. Viena argumenta polinomi

2.2.1. Pamatdefinīcijas

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

Pieņemsim, ka ir dots komutatīvs gredzens R, apzīmēsim ar R^* tā elementu bezgalīgu virkņu kopu, kurās ir tikai galīgs skaits nenulles elementu.

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

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

$$f = (a_0, a_1, ..., a_n, 0, ...),$$
$$g = (b_0, b_1, ..., b_n, 0, ...),$$

tad

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ..., a_n + b_n, 0, ...),$$
$$f \cdot g = (c_0, c_1, c_2, ...),$$

kur

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

2.1. 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, 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

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

- operācijas $\cdot$ komutativitāte: pierādām, ka komutativitāte izpildās katram indeksam, ja $f = (a_0, a_1, ..., a_n)$ un $g = (b_0, b_1, ..., b_n)$,

tad

$$(f \cdot g)_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} b_i a_{k-i} = (g \cdot f)_k,$$

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

■

Elementi formā $(a, 0, ...)$ veido apakšgredzenu, kas ir izomorfs sākotnējam gredzenam R, tāpēc šo apakšgredzenu var identificēt ar R.

2.1. piezīme. (Patstāvīgais darbs) Funkcija $\iota : R \to R^*$, kas ir definēta ar atbilstību

$$\iota(a) = (a, 0, ...)$$

(*dabiskā iekļaušana*), ir gredzenu homomorfizms, jo

$$\iota(a + b) = (a + b, 0, ...) = \iota(a) + \iota(b)$$
$$\iota(a \cdot b) = (a \cdot b, 0, ...) = \iota(a) \cdot \iota(b)$$

Funkcija $\pi : R^* \to R$, kas ir definēta ar atbilstību

$$\pi((a_0, a_1, ...)) = a_0$$

(*dabiskā projekcija*), arī ir gredzenu homomorfizms, jo

$$\pi(a + b) = \pi((a_0 + b_0, ...)) = a_0 + b_0 = \pi(a) + \pi(b)$$
$$\pi(a \cdot b) = \pi((a_0 \cdot b_0, ...)) = a_0 \cdot b_0 = \pi(a) \cdot \pi(b).$$

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

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

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 var lietot jebkuru citu simbolu: $R[X] \simeq R[Y]$ visiem simboliem X,Y.

Gredzena elementus a_i sauc par polinoma *koeficientiem*.

Polinomu sauc par *nulles polinomu*, ja visi koeficienti ir nulles (gredzenā R).

Polinoma koeficientu a_0 sauc par *brīvo locekli*.

Nenulles koeficientu ar maksimālo indeksu sauc par polinoma *vecāko koeficientu*. Vecākā koeficienta indeksu sauc par *polinoma pakāpi*, apzīmē kā $deg(a)$. Nulles polinomam $0 = (0, 0, ...)$ pakāpi definē vienādu ar $-\infty$ vai nedefinē vispār. Ja $deg(a) = 1(2, 3)$, tad a ir *lineārs (kvadrātisks, kubisks)* polinoms.

Par *monomu* sauc polinomu formā aX^m.

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

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

2.2. 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. $f \in R[X]$ ir invertējams tad un tikai tad, ja $deg(f) = 0$ un $a \in U(R)$.

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.

Polinomu reizinājums vecākais koeficients ir polinomu vecāko koeficientu reizinājums. Ja

$$f = a_n X^n + ..., \tag{1}$$

$$g = b_m X^m + ..., \tag{2}$$

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

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

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

4. Ja $fg = 1$, tad $deg(f) + deg(g) = 0$. Tātad $deg(f) = deg(g) = 0$ un $f, g \in U(R)$. Ja $f \in U(R)$, tad $f \in U(R[X])$.

■

2.2.2. Substitūcijas un universālā īpašība

Ja ir dots polinoms $f(X) = a_0 + a_1X + a_nX^n \in R[X]$, 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:

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

2.3. teorēma. (*Polinomu gredzena universālā īpašība*) Ir spēkā šādi apgalvojumi

1. Ja komutatīvs gredzens R satur apakšgredzenu S, tad katram $t \in R$ eksistē viens un tikai viens gredzenu homomorfizms
$$\Psi_t : S[t] \to R$$
tāds, ka katram $s \in S$ izpildās $\Psi_t(s) = s$ un $\Psi_t(X) = t$.
2. Ja R un S ir patvaļīgi komutatīvi gredzeni, $t \in R$, $\psi : S \to R$ - gredzenu homomorfizms, tad eksistē viens un tikai viens gredzenu homomorfizms $\Psi_t : S[X] \to R$ tāds, ka $\psi = \Psi_t \circ \iota$, kur ι ir dabiskā iekļaušana.

PIERĀDĪJUMS

1. Eksistence. Definēsim $\Psi_t = \Phi_t$, tas ir gredzenu homomorfizms, kurš apmierina prasības.

Vienīgums. Pieņemsim, ka gredzenu homomorfizms Ψ'_t apmierina

prasības $\Psi'_t(s) = s$ un $\Psi'_t(X) = t$. Tad katram $f \in R[X]$

$$\Psi'_t(f) = \Psi'_t(\sum_{i=0}^{deg(f)} a_i X^i) = \sum_{i=0}^{deg(f)} \Psi'_t(a_i X^i) =$$

$$= \sum_{i=0}^{deg(f)} a_i \Psi'_t(X^i) = \sum_{i=0}^{deg(f)} a_i \Psi'_t(X)^i = \sum_{i=0}^{deg(f)} a_i t^i = f(t) = \Phi_t(X).$$

Redzam, ka $\Psi'_t = \Phi_t$.

2. Tiek pierādīts līdzīgi kā 1. Patstāvīgais darbs. ■

Ja ir doti divi gredzeni $S \leq R$, tad elementu $r \in R$ sauc par *algebrisku elementu virs* S, ja eksistē $f \in S[X]$, kuram

$$\Phi_r(f) = 0.$$

Citiem vārdiem sakot, r apmierina polinomiālu vienādojumu ar koeficientiem gredzenā S:

$$f(r) =_R 0.$$

Ja r neapmierina nekādu polinomiālu vienādojumu ar koeficientiem gredzenā S, tad to sauc par *transcendentu virs* S.

2.1. piemērs. Skaitlis $\sqrt{2}$ ir algebrisks virs $\mathbb{Z}$ un $\mathbb{Q}$, jo tas apmierina vienādojumu $X^2 - 2 = 0$.

Skaitlis π ir transcendents virs $\mathbb{Q}$, jo tas neapmierina nekādu algebrisku vienādojumu.

2.2.3. Dalīšana ar atlikumu

2.3. piezīme. Atkārtot polinomu dalīšanas algoritmu.

2.2. piemērs. Izdalīsim $f = X^5 + X^2 + 1$ ar $g = X^2 + X + 1$ virs $\mathbb{Z}$:

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

Apskatīsim dalīšanas procedūru pa soļiem:

1. Pirmajā solī atņemsim no f tādu g daudzkārtni, lai pēc atņemšanas iegūtā polinoma pakāpe būt mazāka nekā $deg(f)$:
$$f \to f_1 = f - X^3 \cdot g = -X^4 - X^3 + X^2 + 1;$$
2. Otrajā solī atņemsim no f_1 tādu g daudzkārtni, lai pēc atņemšanas iegūtā polinoma pakāpe būt mazāka nekā $deg(f_1)$:
$$f_1 \to f_2 = f_1 - (-X^2) \cdot g = 2X^2 + 1;$$
3. Trešajā solī atņemsim no f_2 tādu g daudzkārtni, lai pēc atņemšanas iegūtā polinoma pakāpe būt mazāka nekā $deg(f_2)$:
$$f_2 \to f_3 = f_2 - 2 \cdot g = -2X - 1;$$

Rezultātā iegūsim, ka

$$f = X^3 g + f_1 = X^3 g + (-X^2)g + f_2 =$$
$$= X^3 g + (-X^2)g + 2g + (-2X - 1) =$$
$$= (X^3 - X^2 + 2)g + (-2X - 1).$$

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

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

2.4. 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

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

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 pēc $deg(f)$.

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

$$q = a_n b_n^{-1}, r = 0.$$

Indukcijas solis. Pieņemsim, ka pirmais apgalvojums ir spēkā, ja $deg(f) < n$ un pierādīsim, ka tad tas ir spēkā, ja $deg(f) = n$. Redzam, ka

$$f = (a_n b_m^{-1} X^{n-m})g + f_1,$$

kur $deg(f_1) < n = deg(f)$. Saskaņā ar indukcijas pieņēmumu eksistē polinomu q_1 un r_1 tādi, ka

$$f_1 = q_1 g + r_1,$$

kur $deg(r_1) < deg(g) = m$. Tagad redzam, ka

$$f = (a_n b_m^{-1} X^{n-m})g + f_1 = (a_n b_m^{-1} X^{n-m} + q_1)g + r.$$

Varam definēt $q = a_n b_m^{-1} X^{n-m} + q_1$.

q un r vienīgums.

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

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

Tas nozīmē, ka

$$(q - q')g = r' - r.$$

Bet $deg(r' - r) < deg(g)$. No otras puses

$$deg((q - q')g) = deg(q - q') + deg(g).$$

Tā kā

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

tad $deg(q - q') = -\infty$, tātad arī $deg(r' - r) = -\infty$, $q = q'$ un $r = r'$.
■

Ja $f = qg$, tad teiksim, ka f dalās ar g, apzīmē kā $g|f$.

2.3. piemērs. $x - 1|x^2 - 1$.

2.3. Viena argumenta pakāpju rindas

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

Ja atļaut 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 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.

Var pārbaudīt, ka kopa $R^\sharp$ ar šīm operācijām veido komutatīvu gredzenu ar nulli $(0, ...)$ un vieninieku $(1, 0, ...)$.

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 rindas speciālgadījumu, tāpēc ir definēta funkcija $R[X] \to R[[X]]$ (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).

2.5. 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.

■

2.4. Vairāku argumentu polinomi un pakāpju rindas

2.4.1. Motivācijas

Pieņemsim, ka R ir komutatīvs gredzens, $S \subseteq R$ ir tā apakšgredzens. Katrai R elementu virknei $t_1, ..., t_n \in R$ definēsim apakšgredzena S *paplašinājumu ar elementiem* $t_1, ..., t_n$ - kopu

$$S[t_1, ..., t_n] = \{a \in R | b = \sum_{i_1, ...i_n} a_{i_1 ... i_n} t_1^{i_1} ... t_n^{i_n}\}.$$

Citiem vārdiem sakot $S[t_1, ..., t_n]$ ir mazākais apakšgredzens, kas satur S,$t_1, ..., t_n$. Līdzīgi kā viena argumenta polinomu gadījumā var atrast divu elementu summu un reizinājumu.

Lietderīgi ir pētīt kopu $S[t_1, ..., t_n]$ uzskatot $t_1, ..., t_n$ par ārējiem elementiem, kas neapmierina nekādas sakarības.

Ja funkcija $f : R^n \to R$ ir uzdota ar polinomiālu likumu

$$f(t_1, ..., t_n) = \sum_{i_1, ...i_n} f_{i_1 ... i_n} t_1^{i_1} ... t_n^{i_n},$$

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

2.4.2. Definīcijas

Ir dots komutatīvs gredzens R.

Iterēsim polinomu gredzena konstrukciju:

1. Konstruēsim viena argumenta polinomu gredzenu $R[X]$.
2. Konstruēsim viena argumenta polinomu gredzenu virs $R[X]$ - $R[X][Y]$:

$$R \rightsquigarrow R[X] \rightsquigarrow R[X][Y] \rightsquigarrow (R[X][Y])[Z] \rightsquigarrow ...$$

$R[X][Y]$ elementi ir izsakāmi formā

$$\sum_{j=0}^{k} b_j Y^k = \sum_{j=0}^{k} (\sum_{i=0}^{n} a_{ij} X^i) Y^k = \sum_{i=0,j=0}^{n,k} a_{ij} X^i Y^k$$

$R[X][Y]$ ar definētajām summas un reizināšanas operācijām sauc par *divu argumentu polinomu gredzenu virs* R un apzīmē ar $R[X, Y]$.

Iterējot šo konstrukciju n reizes, iegūst *n-argumentu polinomu gredzenu virs* R -

$$R[X_1, ..., X_n] = R[X_1, ..., X_{n-1}][X_n].$$

Par *n-argumentu monomu* sauc polinomu formā $aX_1^{m_1}...X_n^{m_n}$. Par monoma pakāpi sauc tā argumentu pakāpju summu $m_1 + ... + m_n$.

Divi n-argumentu polinomi ir vienādi tad un tikai tad, ja tiem ir vienādi visi monomu koeficienti.

Par n-argumentu polinoma pakāpi sauc maksimālo monoma pakāpi.

n-argumentu polinomu sauc par *homogēnu m-tās pakāpes polinomu*, ja katra monoma pakāpe ir vienāda ar m.

2.6. teorēma. Ja R ir integrāls gredzens un $f, g \in R[X_1, ..., X_n]$, tad ir spēkā šādi apgalvojumi

1. $deg(f + g) \leq max(deg(f), deg(g))$.
2. $deg(fg) = deg(f) + deg(g)$.
3. $R[X_1, ..., X_n]$ ir integrāls gredzens.
4. $f \in R[X_1, ..., X_n]$ ir invertējams tad un tikai tad, ja $deg(f) = 0$ un $a \in U(R)$.

Vairāku argumentu pakāpju rindas definē līdzīgi viena argumenta gadījumam.

3. 1.mājasdarbs

1. Pierādīt, ka komutatīvs gredzens ar vieninieku ir integrāls gredzens tad un tikai tad, ja izpildās *multiplikatīvās saīsināšanas likums*:
$$\text{ja } xy = xz \text{ un } x \neq 0, \text{ tad } y = z.$$
2. Gredzenam $(\mathcal{P}(X), \Delta, \cap)$ atrodiet aditīvo neitrālo elementu, aditīvā inversā elementa atrašanas operāciju, multiplikatīvo neitrālo elementu, multiplikatīvi invertējamos elementus.
3. Atrodiet piemērus funkciju gredzeniem $Fun(X, R)$, kuros eksistē nulles dalītāji.
4. Cik ir dažādu kubisko polinomu virs $\mathbb{F}_p$?
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 $n \geq 2$.