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

Studiju kurss

Polinomu algebra

7.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

Lekcijas mērķis - apgūt atlikumu klašu un to gredzenu vispārinājumus - ideālus un faktorgredzenus patvaļīgos gredzenos.

Lekcijas kopsavilkums:

- gredzenos var definēt apakšstruktūras, kas vispārina $m\mathbb{Z}$un $m(X)R[X$ - *ideālus;*
- var vispārināt salīdzināmības jēdzienu;
- var vispārināt atlikumu gredzena jēdzienu - definēt *faktorgredzenu*.

1. Ideāli un faktorgredzeni

1.1. Ideāli

1.1.1. Motivācijas

Ir lietderīgi pētīt gredzena apakškopas, kas ir invariantas attiecībā uz reizināšanu ar gredzena elementiem.

1.1. piemērs. $m\mathbb{Z}$, $fR[X]$.

1.2. piemērs. Par gredzenu homomorfisma $f : R_1 \to R_2$ *kodolu* $Ker(f)$ sauc $f^{-1}(0_{R_2})$. Citiem vārdiem sakot,

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

$Ker(f)$ ir R_1 apakšgredzens, jo ja $f(x_1) = f(x_2) = 0$, tad

$$f(x_1 + x_2) = 0 + 0 = 0,$$

$$f(x_1x_2) = 0 \cdot 0 = 0.$$

Vēl viena kodola īpašība:

$$x \in Ker(f) \ \wedge a \in R_1 \implies ax \in Ker(f) :$$
$$f(x) = f(a)f(x) = f(a) \cdot 0 = 0.$$

Citiem vārdiem sakot $Ker(f)$ ir slēgta attiecībā uz reizināšanu ar gredzena elementiem.

1.1.2. Definīcijas un piemēri

Dots komutatīvs gredzens R un tā apakškopa J. Definēsim

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

Ja $A, B \subseteq R$, tad definēsim

$$AB = \{r \in R | r = \sum_{i=1}^{m} a_i b_i, \text{ kur } a_i \in A, b_i \in B\}.$$

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

1. I ir apakšgrupa attiecībā uz $+$,
2. $RI \subseteq I$ vai, citiem vārdiem sakot, $\forall\ r \in R$ izpildās $rI \subseteq I$ (I ir slēgta attiecībā uz reizināšanu ar R elementiem).

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

Ja k ir lauks, tad katrs ideāls ir vai nu $\{0\}$ vai k.

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

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

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

Katra gredzenu homomorfisma $f : R_1 \to R_2$ kodols ir ideāls.

1.4. piemērs. Ir dota polinomiāla vienādojumu sistēma

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

Visi polinomi formā

$$h = g_1 f_1 + \dots + g_m f_m$$

arī apmierina vienādojumu $h = 0$. 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 jebkuram ideālam J izpildās

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

1.5. piemērs. Maksimālie un pirmideāli gredzeniem $\mathbb{Z}$, $\mathbb{R}[X]$ un $Fun(\mathbb{R}, \mathbb{R})$.

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

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

Katram $r \in R$ izpildās

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

Bet $I \subseteq R$, tāpēc $R = I$. ■

1.1.3. Operācijas ar ideāliem

Ja ir doti vairāki ideāli $I_1, ..., I_n$, tad par to šķēlumu sauksim kopu

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

Ja ir dots galīgs skaits ideālu $I_1, ..., I_n$, tad par to summu sauksim kopu

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

Ja ir dots galīgs skaits ideālu $I_1, ..., I_n$, tad par to reizinājumu

sauksim kopu

$$I_1 ... I_n = \prod_{i=1}^{n} I_i = \{r \in R | r = \sum_{j=1}^{m} \prod_{i=1}^{n} x_{ij}, \text{ kur } x_{ij} \in I_i\}.$$

Ja ir dots ideāls I un $a \in R$, tad par I *paplašinājumu ar* a $\langle I, a \rangle$ sauc kopu $\{y \in R | y = x + ar\}$, kur $x \in I$, $r \in R$.

1.6. piemērs. $I_1 \cap I_2$, $I_1 + I_2$, $I_1 I_2$.

1.2. teorēma. Ideālu šķēlums, summa, reizinājums un paplašinājums ir ideāls.

PIERĀDĪJUMS

Šķēlums. Ja $x \in I_\alpha$ katram α, tad katram $r \in R$ izpildās $rx \in I_\alpha$, tātad

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

Summa. Ja $x = x_1 + x_2 + ... + x_n$, kur $x_i \in I_i$, tad katram $r \in R$ izpildās

$$rx = rx_1 + rx_2 + ... + rx_n \in \sum_{i=1}^{n} I_i.$$

Reizinājums. Ja $x = \sum_{j=1}^{m} x_{1j}x_{2j}...x_{nj}$, kur $x_i \in I_i$, tad katram $r \in R$ izpildās

$$rx = \sum_{j=1}^{m} (rx_{1j})x_{2j}...x_{nj} \in \prod_{i=1}^{n} I_i.$$

Paplašinājums. $y_i = x_1 + ar_i \implies$

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

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

■

1.1.4. Ideālu ģenerēšana

Patvaļīgam gredzenam R kopa aR ir ideāls katram $a \in R$, apzīmē ar $\langle a \rangle$. 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 ģenerētiem ideāliem*, elementus $a_1, ..., a_n$ sauc par ideāla *ģeneratoriem*.

1.1. piezīme. Par ideāla ģeneratoru kopu var domāt kā par lineāras telpas bāzes analogu.

1.7. 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 $X \notin \langle 2, X\rangle$.

1.3. teorēma.

1. $\mathbb{Z}$ ir GIG.
2. Katram laukam k polinomu gredzens $k[X]$ 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:

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

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

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

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

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

$r = f - qm \in I \implies r = 0 \implies f = qm \implies I \subseteq mR[X]$. Tā kā $mR[X] \subseteq I$, tad $mR[X] = I$. ■

1.4. teorēma. Ja k ir lauks un $\{f_1, ..., f_n\} \subset k[X]$, tad

1. $\langle f_1, ..., f_{n-1}, f_n \rangle = \langle f_1, ..., f_{n-1} \rangle + \langle f_n \rangle$.
2. $\langle f_1, ..., f_n \rangle = \langle LKD(f_1, ..., f_n) \rangle$.
3. $\sum_{i=1}^{m} \langle f_i \rangle = \langle LKD(f_1, ..., f_m) \rangle$.
4. $\bigcap_{i=1}^{m} \langle f_i \rangle = \langle MKD(f_1, ..., f_m) \rangle$.
5. $\prod_{i=1}^{m} \langle f_i \rangle = \langle \prod_{i=1}^{m} f_i \rangle$.

PIERĀDĪJUMS

1. $r \in \langle f_1, ..., f_{n-1}, f_n \rangle \iff$

$$r = \underbrace{g_1 f_1 + ... + g_{n-1} f_{n-1}}_{\in \langle f_1, ..., f_{n-1} \rangle} + \underbrace{g_n f_n}_{\in \langle f_n \rangle} \iff r \in \langle f_1, ..., f_{n-1} \rangle + \langle f_n \rangle.$$

2. Izmantosim matemātisko indukciju ar parametru n.

Indukcijas bāze

$n = 2$, apskatīsim $I = \langle f_1, f_2 \rangle$, apzīmēsim $d = LKD(f_1, f_2)$.

No vienas puses:

$$r \in \langle f_1, f_2 \rangle \iff r = g_1 f_1 + g_2 f_2 \implies$$
$$r = g_1 h_1 d + g_2 h_2 d = (g_1 h_1 + g_2 h_2) d \implies$$
$$r \in \langle d \rangle = \langle LKD(f_1, f_2) \rangle.$$

No otras puses:

$$r \in \langle LKD(f_1, f_2) \rangle \implies r = gd = g(u_1 f_1 + u_2 f_2) \implies$$
$$r = (gu_1) f_1 + (gu_2) f_2 \in \langle f_1, f_2 \rangle.$$

Indukcijas solis

Pieņemsim, ka apgalvojums ir pierādīts visiem $n < m$, pierādīsim, ka tad apgalvojums ir patiess, ja $n = m$.

1. $\Longrightarrow \langle f_1, ..., f_{m-1}, f_m\rangle = \underbrace{\langle f_1, ..., f_{m-1}\rangle}_{=\langle LKD(f_1,...,f_{m-1})\rangle} + \langle f_m\rangle =$

$$\langle LKD(LKD(f_1, ..., f_{m-1}), f_m)\rangle = \langle LKD(f_1, ..., f_n)\rangle.$$

3. seko no 1. un 2.

4. $g \in \bigcap_{i=1}^{m} \langle f_i\rangle \Longrightarrow g \in \langle f_i\rangle,\ \forall i \Longrightarrow f_i|g \Longrightarrow$

$$MKD(f_1, ..., f_m)|g \Longrightarrow g \in \langle MKD(f_1, ..., f_m)\rangle.$$

$$g \in \langle MKD(f_1, ..., f_m)\rangle \Longrightarrow MKD(f_1, ..., f_m)|g \Longrightarrow$$

$$f_i|g \Longrightarrow g \in \bigcap_{i=1}^{m} \langle f_i\rangle.$$

5. Patstāvīgi.

■

1.8. piemērs. $\langle X^2 - 1, X + 1\rangle = \langle X + 1\rangle$.
$\langle X^2 - 1\rangle \cap \langle X(X + 1)\rangle = \langle x(X^2 - 1)\rangle$.

1.2. Faktorgredzeni

1.2.1. Definīcijas

Ja $I \subseteq R$ ir ideāls, tad teiksim, ka divi elementi r_1 un r_2 ir salīdzināmi mod I, ja

$$r_1 - r_2 \in I.$$

Apzīmēsim to ar $r_1 \sim r_2$.

1.5. teorēma. Salīdzināmība mod I ir ekvivalences attiecība gredzenā R.

PIERĀDĪJUMS Līdzīgs veselo skaitļu un polinomu kongruences gadījumiem. ■

Ekvivalences klases apzīmēsim veidā $a + I$ (vai $[a]$). Ekvivalences klašu kopu apzīmēsim ar R/I.

Definēsim $r + S = \{r + s | s \in S\}$.

1.6. teorēma. $a \sim b \iff a + I = b + I.$

PIERĀDĪJUMS
$a \sim b \implies a - b \in I \implies a - b = x \in I.$

Redzam, ka

$$\forall y \in I : \; a + y = b + (x + y) \in b + I \implies a + I \subseteq b + I,$$

$$\forall z \in I : \; b + z = a + (-x + z) \in a + I \implies b + I \subseteq a + I.$$

Seko, ka $a + I = b + I$. ■

Ir definēta dabiskā projekcija

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

1.2.2. Operācijas

Operācijas ar ekvivalences klasēm:

- Saskaitīšana - $(a+I)+(b+I)=(a+b)+I$.
- Reizināšana - $(a+I)(b+I)=ab+I$.

1.7. 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.
3. π ir gredzenu homomorfisms, $Ker(\pi)=I$.

PIERĀDĪJUMS

1. Ja $a_1+I=a_2+I$ un $b_1+I=b_2+I$, tad $a_1=a_2+u$ un $a_1=a_2+v$, kur $u,v\in I$. Tad

$$(a_1+I)+(b_1+I)=(a_1+b_1)+I=$$
$$(a_2+b_2)+(u+v+I)=(a_2+b_2)+I,$$

$$(a_1 + I)(b_1 + I) = a_1b_1 + I = (a_2 + u)(b_2 + v) + I = \\ a_2b_2 + (ub_2 + va_2 + uv + I) = a_2b_2 + I.$$

2. Aksiomu pārbaude. $0 = 0 + I$, $1 = 1 + I$, $-(a + I) = -a + I$.

3. $a \in I \implies \pi(a) = I = 0 + I \implies I \subseteq Ker(\pi)$.

$\pi(b) = 0 + I \implies b \sim 0 \implies b \in I \implies Ker(\pi) \subseteq I$. Apkopojot redzam, ka $Ker(\pi) = I$. ■

Ekvivalences klašu gredzenu mod I apzīmē ar R/I.

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

1.8. teorēma. R ir komutatīvs unitārs gredzens, $I \subseteq R$ - ideāls.

1. R/I - integrāls gredzens $\iff$ I - pirmideāls.
2. R/I - lauks $\iff$ I - maksimāls ideāls.

PIERĀDĪJUMS

1. $\Leftarrow$

I - pirmideāls $\Longrightarrow$ $1+I \neq 0+I$ $\Longrightarrow$ faktorgredzenā R/I eksistē vieninieks $1+I$.

$$(a+I)(b+I) = 0+I \implies ab \in I \implies a \in I \vee b \in I \implies$$
$$a+I = 0 \vee b+I = 0.$$

$\Rightarrow$

$1+I \neq 0 \implies 1 \notin I \implies I \neq R$.

Dots, ka $(a+I)(b+I) = 0 \implies a+I = 0 \vee b+I$,

$(a+I)(b+I) = ab+I$, tātad ir dots, ka $ab \in I \implies a \in I \vee b \in I$.

2. $\Leftarrow$

I - maksimāls ideāls $\Longrightarrow$ $1+I \neq 0+I$ $\Longrightarrow$ faktorgredzenā R/I eksistē vienīnieks $1+I \neq 0+I$.

$a+I \neq 0 \implies a \notin I$. Apskatīsim ideālu $J = \langle I, a \rangle$, $I \subseteq J$. Tā kā I ir maksimāls ideāls, $a \in J$ un $a \notin I$, tad $J = R$. Seko, ka $1 \in J$ un $1 = x + ar$, kur $x \in I, r \in R$. Seko, ka

$$1 - ar = x \in I \implies 1 \sim ar \implies ar + I = 1 + I \implies r = a^{-1}.$$

$\Rightarrow$
$1+I \neq 0 \implies 1 \notin I \implies I \neq R$;

Dots, ka $\forall\ a \notin I$ eksistē $b = a^{-1}$:

$$(a+I)(b+I) = 1+I,$$

jāpierāda, ka I ir maksimāls ideāls: katram ideālam J izpildās nosacījums $I \subseteq J \implies J = I \vee J = R$.

Pieņemsim, ka eksistē ideāls J: $I \subset J \subset R$. Izvēlēsimies $b \in J, b \notin I$. Eksistē $c = b^{-1}$:

$$(b + I)(c + I) = 1 + I \implies bc + I = 1 + I.$$

Redzam, ka $bc \sim 1 \implies 1 = bc + x$, kur $x \in I$. Seko, ka $1 \in J \implies J = R$. ■

1.2. piezīme. No teorēmas seko, ka maksimāls ideāls ir pirmideāls.

2. 7.mājasdarbs

2.1. Obligātie uzdevumi

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

7.2 Atrast visus maksimālos ideālus gredzenos

(a) $\mathbb{Z}$,
(b) $\mathbb{Z}/12\mathbb{Z}$,
(c) $\mathbb{C}[X]$,
(d) $\mathbb{R}[X]$.

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

7.4 Noskaidrot, kādiem a faktorgredzens $\mathbb{F}_7[X]/\langle X^2 - a\rangle$ ir lauks.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

7.5 Dots, ka R ir integrāls gredzens ar vieninieku. Pierādīt, ka $R[X]$ ir GIG tad un tikai tad, ja R ir lauks.