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

Studiju kurss

Algebriskās struktūras

7.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

3. 7.mājasdarbs 25

Lekcijas mērķis:

•

Lekcijas kopsavilkums:

•

Svarīgākie jēdzieni:

Svarīgākie fakti un metodes:

1. Gredzeni

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:

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

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

$+$ operācijai izmanto aditīvo pierakstu, $\cdot$ operācijai - multiplikatīvo pierakstu.

Citas definīcijas un fakti, kas zināmi no iepriekšējiem kursiem:

- 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;
- gredzena elementu sauksim par (multiplikatīvi) invertējamu, ja tam eksistē labais un kreisais inversais elements attiecībā uz reizināšanu; R invertējamo elementu kopu apzīmēs ar $\mathcal{U}(R)$, $(\mathcal{U}(R), \cdot)$;
- gredzenu sauc par *integrālu gredzenu*, ja tas ir komutatīvs un tajā nav nulles dalītāju: ja $ab = 0$, tad $a = 0$ vai $b = 0$;
- R ir integrāls gredzens $\iff$ $ab = ac \wedge a \neq 0$ $\iff$ $b = c$ (izpildās multiplikatīvās saīsināšanas īpašība);

- $a \in R$ sauc par *nilpotentu*, ja $a^k = 0$ kādam $k \in \mathbb{N}$;
- $a \in R$ sauc par *idempotentu*, ja $a^2 = a$;
- integrālu gredzenu sauc par *lauku*, ja visi nenulles elementi ir invertējami.

1.1. teorēma. *R ir galīgs integrāls gredzens $\Longrightarrow$ R ir lauks.*

PIERĀDĪJUMS Jāpierāda, ka $\forall a \in R, a \neq 0$, $\exists b \in R$ tāds, ka

$$ab = 1.$$

Pieņemsim, ka $a_1, ..., a_n$ ir visi dažādie R nenulles elementi. Starp tiem ir arī 1.

Pierādīsim, ka patvaļīgam elementam a_k $\exists$ a_k^{-1}. Apskatīsim elementus

$$a_k a_1, a_k a_2, ..., a_k a_n.$$

Tie visi ir dažādi nenulles elementi, jo pretējā gadījumā būtu

$$a_k a_i = a_k a_j \Longrightarrow a_i = a_j.$$

Tādējādi eksistē m tāds, ka

$$a_k a_m = 1.\blacksquare$$

1.2. Klasiskie gredzeni

1.2.1. 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 - $\mathbb{F}_p$ - lauki).

1.2.2. Matricu gredzeni

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).

1.2.3. 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).

Piemēram, $\mathbb{Z}$ spektrs ir pirmskaitļu kopa (vienkāršotā interpretācijā) un katru veselu skaitli n var identificēt ar funkciju, kas katram pirmskaitlim p piekārto $ord_p(n)$. Viena no svarīgākajām neatrisinātajām problēmām mūsdienu matemātikā ir minētās atbilstības vispārināšana uz nekomutatīvo gredzenu gadījumu - *nekomutatīvās ģeometrijas problēma*.

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

1.3. 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:

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

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

Visi gredzeni un gredzenu homomorfismi veido *gredzenu kategoriju* **Ring**.

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

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

1.2. piemērs. Gredzenu homomorfizmu piemēri -

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

1.4. 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 $ab \in S$.

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

Nepārtrauktas un diferencējamas viena reāla argumenta funkciju kopas ir apakšgredzeni visu funkciju gredzenos.

1.2. teorēma. Jebkura gredzenu homomorfizma attēls ir apakšgredzens.

2. Ideāli un faktorgredzeni

2.1. Ideāli

2.1.1. Pamatfakti

Dots gredzens R un tā apakškopa J. Definēsim

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

un

$$Ja = \{r \in R | r = xa, \text{ kur } x \in J\}.$$

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 *kreiso (labo) ideālu*, ja

1. I ir apakšgrupa attiecībā uz $+$,

2. $RI \subseteq I$ ($IR \subseteq R$) vai, citiem vārdiem sakot, katram $r \in R$ izpildās $rI \subseteq I$ ($Ir \subseteq I$) (I ir slēgta attiecībā uz reizināšanu ar R elementiem).

Kopu I sauksim par *ideālu* vai *abpusēju ideālu*, ja tas ir gan kreisais, gan labais ideāls.

2.1. piezīme. Kreisie un labi ideāli var būt atšķirīgi tikai nekomutatīvos gredzenos, piemēram, matricu gredzenos.

Ja gredzens ir komutatīvs, tad lai kopa būtu ideāls, pietiek, lai tā būtu kreisais vai labais ideāls.

2.1. teorēma. R - gredzens, I - ideāls. $I \cap \mathcal{U}(R) \neq \emptyset \implies I = R$.

PIERĀDĪJUMS Pieņemsim, ka $u \in U(R) \cap I$. I ir ideāls $\Longrightarrow$

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

Katram $r \in R$ izpildās

$$r \cdot 1 = r \in RI,$$

tātad $R \subseteq I$. Bet $I \subseteq R$, tāpēc $R = I$. ■

2.1. 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 homomorfizma $f : R_1 \to R_2$ kodols ir ideāls.

2.1.2. Operācijas ar ideāliem

Ja ir doti vairāki ideāli I_α, tad var apskatīt $\bigcap_\alpha I_\alpha$.

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

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

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

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

2.2. teorēma. Ideālu šķēlums, summa un reizinājums 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

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

2.1.3. Ideālu veidotājelementi

Patvaļīgam gredzenam R kopa aR ir ideāls katram $a \in R$, apzīmē ar (a). Tādus ideālus sauc par *galvenajiem ideāliem* .

Ja gredzenā R katrs ideāls ir galvenais, tad R sauc par *galveno ideālu gredzenu (GIG)*.

Patvaļīgam gredzenam R un fiksētiem elementiem $\{a_1, a_2, ..., a_n\}$ kopa

$$\{r \in R | r = a_1x_1 + a_2x_2 + ... + a_nx_n, \text{ kur } x_i \in R\}$$

ir ideāls katrai kopai $\{a_1, ..., a_n\} \subseteq R$, apzīmē ar $(a_1, a_2, ..., a_n)$. Tādus ideālus sauc par *galīgi ģenerētiem ideāliem*, elementus $a_1, ..., a_n$ sauc par ideāla *ģeneratoriem*.

2.2. piemērs. Ideāls $(2, X) \in \mathbb{Z}[X]$ nav galvenais, to nevar izteikt formā (a). Tā kā $2 \in (2, X)$, tad $a = \pm 2$, bet tad $X \notin (2, X)$.

2.2. piezīme. $\mathbb{Z}$ ir GIG.

Katram laukam k polinomu gredzens $k[X]$ ir GIG.

2.2. Faktorgredzeni

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

$$r_1 - r_2 \in I.$$

Apzīmēsim to ar $r_1 \equiv r_2 (\text{mod } I)$ vai $r_1 \sim r_2$.

Kongruence mod I ir ekvivalences attiecība gredzenā R.

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

2.3. piezīme. $a \equiv b (\text{mod } I) \iff a + I = b + I$.

Ir definēta dabiskā projekcija

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

Operācijas ar ekvivalences klasēm:

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

2.3. 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 homomorfizms, $Ker(\pi) = I$.

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

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

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

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

3. Ja $a \in I$, tad $\pi(a) = I = 0 + I$, tāpēc $I \subseteq Ker(\pi)$. Ja $\pi(b) = 0 + I$, tad $b \sim 0$, tātad $b \in I$. Seko, ka $Ker(\pi) \subseteq I$ un $Ker(\pi) = I$.

■

Ekvivalences klašu gredzenu mod I apzīmē ar R/I.

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

Ideālu $I \subseteq R$ sauc par *maksimālu* , ja neeksistē neviens ideāls $J \neq R$ tāds, ka $I \subset J$.

Ideālu $I \subseteq R$, kur R ir komutatīvs gredzens, sauc par *vienkāršu (prime)*, ja $ab \in I \implies a \in I \vee b \in I$.

2.4. teorēma. Dots komutatīvs gredzens R.

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

PIERĀDĪJUMS
■

2.3. Gredzenu izomorfismu teorēmas

2.5. teorēma. I ir ideāls gredzenā R. Dabiskā projekcija

$$\pi : R \to R/I$$

ir sirjektīvs gredzenu homomorfisms un $Ker(\pi) = I$.

PIERĀDĪJUMS
Sirjektivitāte Katrai klasei $a + I$ izpildās

$$a + I = \pi(a).$$

Homomorfisms $\pi(a+b) = a+b+I = (a+I)+(b+I) = \pi(a)+\pi(b)$.
$\pi(ab) = ab + I = ab + aI + bI + I^2 = (a + I)(b + I)$.

Kodols $\pi(a) = a + I = 0 + I \iff a \in I$.
■

2.6. teorēma. (*Pirmā gredzenu izomorfismu teorēma*) Dots gredzenu homomorfisms $f : R \to S$, $Ker(f) = K$. Tad

$$R/K \simeq Im(f).$$

PIERĀDĪJUMS Definēsim funkciju

$$\varphi : R/K \to Im(f),$$

$$\varphi(a + K) = f(a)$$

un pierādīsim, ka φ ir korekti definēts gredzenu izomorfisms.

Korektums

$$a + K = a' + K \implies a - a' \in K \implies f(a - a') = 0_R \implies$$
$$f(a) = f(a') \implies \varphi(a + K) = \varphi(a' + K).$$

Sirjektivitāte $\forall s \in Im(f)\ \exists r \in R : s = f(r) \implies s = \varphi(r + K)$.

Injektivitāte

$$\varphi(a+K)=\varphi(a'+K) \implies f(a)=f(a') \implies$$
$$f(a)-f(a')=0_R=f(a-a') \implies$$
$$a-a'\in K \implies a+K=a'+K.$$

Homomorfisms

$$\varphi((a+K)+(b+K))=\varphi(a+b+K)=f(a+b)=$$
$$f(a)+f(b)=\varphi(a+K)+\varphi(b+K).$$

$$\varphi((a+K)(b+K))=\varphi(ab+K)=f(ab)=$$
$$f(a)f(b)=\varphi(a+K)\varphi(b+K).$$

■

3. 7.mājasdarbs

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

(a) racionālie skaitļi, kuriem saucējs (pēc kopīgo reizinātāju saīsināšanas) nedalās ar doto pirmskaitli p, operācijas - skaitļu saskaitīšana un reizināšana;

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

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

(d) fiksētas kopas X visu apakškopu kopa, operācijas - simetriskā starpība un apvienojums;

(e) simetriskas 2×2 matricas ar reāliem elementiem, operācijas - matricu saskaitīšana un reizināšana;

(f) viena reāla argumenta funkcijas ar nosacījumu $f(x) = 0$, ja $x \in D \subseteq \mathbb{R}$, D - fiksēta kopa, operācijas - funkciju saskaitīšana un reizināšana;

(g) viena reāla argumenta funkcijas, operācijas - funkciju saskaitīšana un kompozīcija.

7.2 R - gredzens ar vieninieku. Pierādīt, ka ja xy un yx ir invertējami, tad x un y arī ir invertējami.

7.3 Atrodiet visus invertējamos elementus, nulles dalītājus, nilpotentos un idempotentos elementus gredzenā $\mathcal{M}_2(\mathbb{R})$.

7.4 Atrast visus maksimālos ideālus gredzenā $\mathbb{Z}$.