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

Studiju kurss

Algebriskās struktūras

7.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- atkārtot gredzenu teorijas pamatus.

Lekcijas kopsavilkums:

- var pētīt algebrisku struktūru - gredzenus, kas vispārina skaitļu kopu un operāciju īpašības.

Svarīgākie jēdzieni: gredzens, integrāls gredzens, lauks, matricu gredzeni, funkciju gredzeni, gredzenu homomorfismi un izomorfismi, homomorfisma attēls un kodols, apakšgredzens, ideāls, ideālu veidotājelementi.

Svarīgākie fakti un metodes: maksimālu un vienkāršu ideālu īpašības, gredzenu izomorfismu teorēma.

1. Gredzeni

1.1. Pamatdefinīcijas

1.1.1. Gredzena aksiomas

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 $a + 0 = 0 + a$,
  - 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.

Svarīgi speciālgadījumu 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 $b = 0$;

- integrālu gredzenu sauc par *lauku*, ja visi nenulles elementi ir invertējami.

Tālāk apskatām tikai unitārus gredzenus.

1.1.2. Elementi ar speciālām īpašībām

R - gredzens.

- Neitrālie elementi attiecība uz abām operācijām - 0, 1.
- Multiplikatīvi invertējamie elementi, veido grupu $\mathcal{U}(R)$.
- Nulles dalītāji (kreisie, labie, abpusējie) $\mathcal{ND}(R)$ - $a \in \mathcal{ND}(R) \iff \begin{cases} a \neq 0, \\ \exists\, b \neq 0 : \; ab = 0. \end{cases}$
- Nilpotentie elementi $\mathcal{N}(R)$: $a \in \mathcal{N}(R) \iff \exists\, n \in \mathbb{N}\colon\ a^n = 0.$
- Idempotentie elementi $\mathcal{ID}(R)$: $a \in \mathcal{ID}(R) \iff a^2 = a.$
- Nedalāmie elementi $\mathcal{I}(R)$: $a \in \mathcal{I}(R) \iff a$ nevar izteikt kā divu neinvertējamu nenulles elementu reizinājumu.

- Pirmelementi $\mathcal{P}(R)$: $a \in \mathcal{P}(R) \iff a \Big| xy \implies a|x$ vai $a|y$.

1.1.3. Grupoīdi gredzenos

R - gredzens.

Aditīvā grupa

$(R, +)$, komutatīva grupa.

R harakteristika $char(R)$ - elementa 1 aditīvā kārta - minimālais $n \in \mathbb{N}$: $n \cdot 1 = 0$. Ja kārta neeksistē, tad $char(R) = 0$.

R - integrāls gredzens $\implies$ $char(R)$ - pirmskaitlis.

1.1. piemērs. $char(\mathbb{Z}) = char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0$. $char(\mathbb{F}_p) = p$.

Multiplikatīvā grupa

$(\mathcal{U}(R), \cdot)$

Multiplikatīvais monoīds

$(R, \cdot)$.

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 $\mathbb{Z}[i]$ (integrāls gredzens, bet ne lauks).

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

X - kopa, R - komutatīvs gredzens. Apzīmēsim ar $\mathcal{F}un(X,R)$ 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 $\mathcal{F}un(X,R)$ ar šādām operācijām veido gredzenu (komutatīvi gredzeni ar nulles dalītājiem).

1.1. piezīme. 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*.

1.3. Gredzenu homomorfismi

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 homomorfismu*, 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 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.

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

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

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

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

1.2. piemērs. Gredzenu homomorfismu 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),
- tā ir slēgta atiecībā uz reizināšanu: $a, b \in S \implies ab \in S$,
- $1 \in S$.

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.

1.1. teorēma. Jebkura gredzenu homomorfisma attēls ir apakšgredzens.

1.5. Ideāli

1.5.1. Pamatfakti

Kopu $I \subseteq R$ sauksim par *kreiso (labo) ideālu*, ja

1. I ir apakšgrupa attiecībā uz $+$,
2. 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.

1.2. 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.

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

PIERĀDĪJUMS Pieņemsim, ka $u \in \mathcal{U}(R) \cap I$. 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 $R = I$. ■

1.3. piezīme. Seko, ka ideāls, kas satur vismaz vienu invertējamu elementu, sakrīt ar visu gredzenu.

1.4. 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 $R = \mathcal{F}un(\mathbb{R}, \mathbb{R})$, tad kopa $I_a = \{f \in R | f(a) = 0\}$ ir ideāls.

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

PIERĀDĪJUMS

1.5.2. Ideālu veidotājelementi

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

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

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

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

1.5. 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. 7.mājasdarbs

2.1. Obligātie uzdevumi

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