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

Studiju kurss

Algebriskās struktūras

8.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt svarīgākos komutatīvo gredzenu tipus.

Lekcijas kopsavilkums:

- var definēt vairāks gredzenu īpašības, ar kuru palīdzību var klasificēt gredzenus.

Svarīgākie jēdzieni: kongruences klase mod I, faktorgredzens R/I, integrāls gredzens, integrāla gredzena daļu lauks, galīgās faktorizācijas gredzens, stabilizējoša augošu ideālu virkne, Nēteres gredzens, viennozīmīgās faktorizācijas gredzens, galveno ideālu gredzens, Eiklīda norma, Eiklīda gredzens, stabilizējoša dilstoša ideālu virkne, Artina gredzens.

Svarīgākie fakti un metodes: IG īpašības, daļu lauka īpašības, GFG īpašības, NG īpašības, VFG īpašības, GIG īpašības, Eiklīda algoritms un citas EG īpašības, komutatīvo gredzenu iekļaušanas hierarhija.

1. Faktorgredzeni

1.1. Klases mod I

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.

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

Ir definēta dabiskā projekcija

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

1.2. Operācijas ar klasēm un faktorgredzens

Operācijas ar ekvivalences klasēm:

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

1.1. 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. 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.

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

2. Komutatīvo gredzeni tipi

2.1. Integrālie gredzeni

2.1.1. Pamatfakti

R - komutatīvs gredzens (KG) ir integrāls gredzens (IG), ja tajā nav nulles dalītāju.

2.1. piemērs. Visi skaitļu gredzeni un to apakšgredzeni.

2.1. teorēma. R - IG.

1. $\left\{ \begin{array}{l} ab = ac \\ a \neq 0 \end{array} \right. \Longrightarrow b = c$ (multiplikatīvās saīsināšanas īpašība)
2. $R[X]$ - IG.

PIERĀDĪJUMS Tika dots polinomu algebras kursā. ■

2.2. teorēma. R - galīgs IG $\Longrightarrow$ R - 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 $a_k a_m = 1$.■

2.1.2. Integrāla gredzena daļu lauks

R - IG. Apskatīsim kopu $R \times \underbrace{R^*}_{=R\setminus\{0\}}$.

Kopā $R \times R^*$ definēsim šādu attiecību:

$$(a_1, b_1) \asymp (a_2, b_2) \iff a_1 b_2 = a_2 b_1.$$

2.3. teorēma. Attiecība $\asymp$ ir ekvivalence.

PIERĀDĪJUMS

Refleksivitāte

$ab = ab \implies (a, b) \asymp (a, b)$.

Simetrija

$$(a_1, b_1) \asymp (a_2, b_2) \implies a_1 b_2 = a_2 b_1 \implies (a_2, b_2) \asymp (a_1, b_1).$$

Tranzitivitāte

Ja $(a_1, b_1) \asymp (a_2, b_2)$ un $(a_2, b_2) \asymp (a_3, b_3)$, tad

$$a_1 b_2 = a_2 b_1,$$
$$a_2 b_3 = a_3 b_2.$$

Reizinot pirmo vienādību ar b_3, iegūsim

$$a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_2 b_1.$$

Saīsinot abas puses ar $b_2 \implies a_1 b_3 = a_3 b_1 \implies (a_1, b_1) \asymp (a_3, b_3)$.
■

Attiecība $\asymp$ ir ekvivalence $\implies$ tā definē kopas $R \times R^*$ sadalījumu atbilstošajās ekvivalences klasēs. Iegūto faktorkopu (ekvivalences klašu kopu) apzīmēsim ar $Q(R)$. Pāra (a, b) pārstāvēto klasi apzīmēsim ar $[a, b]$.

Kopā $Q(R)$ definēsim divas operācijas:

- saskaitīšanu: $[a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2]$,

- reizināšanu: $[a_1, b_1] \cdot [a_2, b_2] = [a_1 a_2, b_1 b_2]$.

2.4. teorēma. R - IG.

1. $(Q(R), +, \cdot)$ ir lauks.
2. Funkcija $\iota : R \to Q(R)$, $\iota(a) = [a, 1]$, ir injektīvs gredzenu homomorfisms.

PIERĀDĪJUMS 1. Jāpārbauda, ka operācijas nav atkarīgas no pārstāvju izvēles. Jāpārbauda visas lauka aksiomas.

Var pārbaudīt, ka $0 = [0, 1]$, $1 = [1, 1]$, $[a, b]^{-1} = [b, a]$.

2. $\iota(a_1) = \iota(a_2) \implies a_1 = a_2 \implies \iota$ ir injektīva. Īpašības

$$\iota(a_1 + a_2) = \iota(a_1) + \iota(a_2),$$
$$\iota(a_1 a_2) = \iota(a_1)\iota(a_2)$$

seko no operāciju definīcijām. ■

2.1. piezīme. Iepriekšējās teorēmas otrais punkts nozīmē to, ka R var interpretēt kā $Q(R)$ apakšgredzenu. Šī iemesla dēļ $Q(R)$ sauc par *R daļu lauku*.

2.2. piemērs. $\mathbb{Q} = Q(\mathbb{Z})$.

k ir lauks $\Longrightarrow$ $Q(k) \simeq k$. Gredzenu izomorfismu $\varphi : k \to Q(k)$ var izvēlēties formā

$$\varphi(a) = (a, 1).$$

2.2. Galīgās faktorizācijas (atomārie) gredzeni

IG R sauc par *galīgas faktorizācijas gredzenu (GFG, atomisku gredzenu)*, ja $\forall\ r \in R \backslash \mathcal{U}(R)$, $r \neq 0$, ir izsakāms galīga nedalāmu elementu reizinājuma veidā:

$$\exists\ \{x_1, ..., x_n\} \subseteq \mathcal{I}(R) :\ r = x_1 ... x_n.$$

2.5. teorēma.

1. $\mathbb{Z}$ ir GFG.
2. R - GFG $\Longrightarrow$ $R[X]$ ir GFG.

PIERĀDĪJUMS
1. Seko no aritmētikas pamatteorēmas.
2. Izmantosim matemātisko indukciju pēc polinoma pakāpes.

■

2.3. Nēteres gredzeni

2.3.1. Definīcija

R - IG. Ideālu virkni $I_1, I_2, ...$ sauc par augošu, ja

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$$

Augošu ideālu virkni sauc par *stabilizējošu*, ja $\exists\ M \in \mathbb{N}$ tāds, ka visiem $n \geq M$: $I_n = I_M$.

IG R sauc par *Nēteres gredzenu (NG)*, ja katra augoša ideālu virkne ir stabilizējoša.

2.3. piemērs. $\mathbb{Z}$.

2.3.2. Īpašības

2.6. teorēma.

1. R - NG $\Longrightarrow$ R - GFG.
2. R - NG $\Longleftrightarrow$ katrs ideāls I ir galīgi ģenerēts.
3. R - NG $\Longrightarrow$ $R[X_1, ..., X_n]$ - NG.
4. R - NG, nav lauks $\Longrightarrow$ R satur vismaz vienu nedalāmu elementu.

PIERĀDĪJUMS

2.4. Viennozīmīgās faktorizācijas gredzeni

2.4.1. Definīcija

IG R ir *viennozīmīgas faktorizācijas gredzens (VFG, faktoriāls gredzens)*, ja $\forall\ a \in R\backslash\{0\}$ ir izsakāms formā

$$a = \underbrace{u}_{\in \mathcal{U}(R)} \underbrace{p_1 p_2 ... p_k}_{p_i \in \mathcal{I}(R)}, \text{ kur}$$

šāds sadalījums ir noteikts viennozīmīgi ar precizitāti līdz elementu kārtībai un aizvietošanai ar asociētiem elementiem, citiem vārdiem sakot:

$$a = u p_1 p_2 ... p_k = u' p'_1 p'_2 ... p'_m \implies$$

1. $k = m$
2. pēc p'_i pārkārtošanas $\forall\ i\ \exists\ u_i \in \mathcal{U}(R)$ tāds, ka $p_i = u_i p'_i$.

2.4. piemērs. VFG - jebkurš lauks, $\mathbb{Z}$.

2.4.2. Īpašības

2.7. teorēma.

1. R - VFG $\Longrightarrow$ $R[X_1, ..., X_n]$ - VFG.

2.5. piemērs. Nav VFG - bieži faktorgredzeni,
$\mathbb{Z}[-\sqrt{5}] \simeq \mathbb{Z}[X] \Big/ \langle X^2 + 5 \rangle$.

2.5. Galveno ideālu gredzeni

2.5.1. Definīcija

IG R ir *galveno ideālu gredzens (GIG)*, ja katrs R ideāls ir galvenais - var tikt ģenerēts ar vienu elementu.

Par GIG R elementu $\{a_1, ..., a_n\}$ LKD sauc elementu a:

$$\langle a \rangle = \langle a_1, ..., a_n \rangle.$$

2.6. piemērs. $\mathbb{Z}$ - GIG

2.6. Eiklīda gredzeni

2.6.1. Definīcija

IG R sauksim par *Eiklīda gredzenu (EG)*, ja var definēt *Eiklīda normas funkciju*

$$\mathbf{N} : R\backslash\{0\} \to \mathbb{N} \cup \{0\},$$

kas apmierina šādu nosacījumu: visiem $a, b \in R$, $b \neq 0$, eksistē $q, r \in R$ tādi, ka

- $a = qb + r$,
- $\mathbf{N}(r) < \mathbf{N}(b)$ vai $r = 0$,
- $\mathbf{N}(ab) \geq \mathbf{N}(a)$ visiem $a, b \neq 0$.

2.7. piemērs. Ja $R = \mathbb{Z}$, tad var paņemt $\mathbf{N}(a) = |a|$ vai $\mathbf{N}(a) = |a|^2$ - teorēma par veselo skaitļu dalīšanu ar atlikumu.

Ja $R = k[X]$, k - lauks, tad var paņemt $\mathbf{N}(a) = \deg(a)$ - teorēma par polinomu dalīšanu ar atlikumu.

$\mathbb{Z}[X]$ nav Eiklīda gredzens - nav viegli pierādīt.

Ja R ir lauks, tad var paņemt $\mathbf{N}(a) = 1$.

2.6.2. Eiklīda algoritms Eiklīda gredzenos

R - EG. Tad gredzenā R var definēt Eiklīda algoritmu analoģiski gredzenam $\mathbb{Z}$ ar analoģiskām īpašībām.

Eiklīda algoritma saistība ar LKD

2.8. teorēma.

1. Pēdējais nenulles atlikums Eiklīda algoritma realizācijā ar sākuma datiem (a, b) ir vienāds ar $LKD(a, b)$.
2. Eksistē elementu pāris pāris (x, y) tāds, ka

$$LKD(a, b) = xa + yb$$

($LKD(a, b)$ ir a un b *R-lineāra kombinācija.*)

PIERĀDĪJUMS Līdzīgi $\mathbb{Z}$ gadījumam.

2.6.3. Faktorizācija Eiklīda gredzenos

2.9. teorēma. R - EG $\Longrightarrow$ R - GFG.

PIERĀDĪJUMS

1.solis

Pierādīsim palīgapgalvojumu (lemmu): ja $a = bc$, kur b, c ir nedalāmi, tad $\mathbf{N}(a) > \mathbf{N}(b)$.

No normas definīcijas seko, ka $\mathbf{N}(a) \geq \mathbf{N}(b)$. Pieņemsim, ka $\mathbf{N}(a) = \mathbf{N}(b)$. Izdalīsim b ar a:

$$b = qa + r, \text{ kur } r = 0 \vee \mathbf{N}(a) > \mathbf{N}(r).$$

$r = 0 \Longrightarrow b = qa$, bet $a = bc = a(qc)$, $1 = qc$ un c ir invertējams - pretruna. Tātad $\mathbf{N}(a) > \mathbf{N}(r)$.

Redzam, ka

$$\mathbf{N}(a) = \mathbf{N}(b) \leq \mathbf{N}(b(1-qc)) = \mathbf{N}(b-bqc) = \mathbf{N}(b-qa) = \mathbf{N}(r) < \mathbf{N}(a).$$

Esam ieguvuši pretrunu, tāpēc $\mathbf{N}(a) > \mathbf{N}(b)$.

2.solis

Ja a ir izsakāms formā $a = b_1...b_k$, kur katram i elements ir b_i ir neinvertējams, tad

$$\mathbf{N}(a) = \mathbf{N}(b_1...b_k) > \mathbf{N}(b_1...b_{k-1}) > ... > \mathbf{N}(b_1)$$

Esam ieguvuši dilstošu nenegatīvu skaitļu virkni, kuras garums nepārsniedz $\mathbf{N}(a)$.

Elementam a apskatīsim sadalījumu ar garāko iespējamo dilstošo virkni. Tas ir sadalījums ar nedalāmiem elementiem, jo pretējā gadījumā virkni varētu padarīt garāku. ■

2.10. teorēma. R - EG $\Longrightarrow$ R - VFG.

PIERĀDĪJUMS

■

2.7. Artina gredzeni

2.7.1. Definīcija

R - KG. Ideālu virkni $I_1, I_2, ...$ sauc par dilstošu, ja

$$I_1 \supseteq I_2 \supseteq ... \supseteq I_n \supseteq ...$$

Dilstošu ideālu virkni sauc par *stabilizējošu*, ja $\exists\, M \in \mathbb{N}$ tāds, ka visiem $n \geq M$: $I_n = I_M$.

KG R sauc par *Artina gredzenu (AG)*, ja katra dilstoša ideālu virkne ir stabilizējoša.

2.8. piemērs. Jebkurš lauks vai lokāls gredzens (ar vienu īstu ideālu).

2.8. Komutatīvo gredzenu iekļaušanas hierarhija

2.11. teorēma.

1. Komutatīvie gredzeni $\supset$ integrālie gredzeni $\supset$ $\supset$ viennozīmīgās faktorizācijas gredzeni $\supset$ galveno ideālu gredzeni $\supset$ Eiklīda gredzeni $\supset$ lauki.
2. Integrālie gredzeni $\supset$ galīgās faktorizācijas gredzeni $\supset$ Nēteres gredzeni $\supset$ viennozīmīgās faktorizācijas gerdzeni.

PIERĀDĪJUMS ■

3. 8.mājasdarbs

3.1. Obligātie uzdevumi

8.1 R - IG, bet ne lauks. Pierādīt, ka $R[X]$ nav GIG.

8.2 R - IG. Pierādīt, ka $R[X_1, X_2, ...]$ (bezgalīgi daudz argumentu) nav NG.

8.3 Pierādīt, ka $\mathbb{Z}[\sqrt{-5}]$ nav VFG.

8.4 (a) Atrast visus ideālus gredzenā $\mathbb{Z}$.
(b) Pierādīt, ka $\mathbb{Z}$ nav AG.
(c) Pierādīt, ka $\mathbb{Z}$ ir NG.