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

Studiju kurss

Algebriskās struktūras

8.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Gredzenu tiešā summa

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

1.1. Ārējā tiešā summa

Ir doti gredzeni R_1 un R_2. Par to *tiešo summu* sauc kopu $R_1 \times R_2$ ar šādām operācijām:

- saskaitīšana - ja $a, b \in R_1$, $a', b' \in R_2$, tad
$$(a, a') + (b, b') = (a + b, a' + b');$$
- reizināšana - ja $a, b \in R_1$, $a', b' \in R_2$, tad
$$(a, a') \cdot (b, b') = (ab, a'b').$$

Ārējo tiešo summu $(R_1 \times R_2, +, \cdot)$ apzīmē ar $R_1 \oplus R_2$.

Līdzīgi definē vairāk nekā divu gredzenu ārējo tiešo summu. Ja ir doti gredzeni $R_1, ..., R_n$, tad par to tiešo summu sauc kopu $R_1 \times R_2 \times ... \times R_n$ ar šādām operācijām:

- saskaitīšana - ja $a_i, b_i \in R_i$, tad

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n);$$

- reizināšana - ja $a_i, b_i \in R_i$, tad

$$(a_1, ..., a_n) \cdot (b_1, ..., b_n) = (a_1 b_1, ..., a_n b_n).$$

Šo konstrukciju var vispārināt arī uz begalīgas gredzenu kopas gadījumu.

1.1. teorēma.

1. $R_1 \oplus R_2$ ir gredzens.
2. Ja R_1, R_2 ir komutatīvi, tad $R_1 \oplus R_2$ arī ir komutatīvs.
3. Ja R_1, R_2 ir unitāri (ar multiplikatīvo neitrālo elementu), tad $R_1 \oplus R_2$ arī ir unitārs.

PIERADĪJUMS Aksiomu pārbaude. ■

1.2. Iekšējais tiešais reizinājums

Ievērosim, ka ideāls ir apakšgredzens.

1.2. teorēma. Dots gredzens R un tā ideāli I_1,...,I_n, kas apmierina šādus nosacījumus:

1. $\sum_{i=1}^{n} I_i = I_1 + ... + I_n = R$ (katrs $r \in R$ ir izsakāms formā
$$r = x_1 + ... + x_n,$$
kur $x_i \in I_i$)
2. $$\forall k, I_k \cap \sum_{i \neq k} I_i = \{0\}.$$

Tad $R \simeq I_1 \oplus ... \oplus I_n$.

PIERĀDĪJUMS

■

Ja $I_1, ..., I_n$ ir ideāli, kas apmierina iepriekšējās teorēmas nosacījumus, tad saka, ka R ir *iekšējā tiešā summa*

$$R = I_1 \oplus ... \oplus I_n.$$

1.1. piezīme. Ja $R = I_1 \oplus ... \oplus I_n$, tad jebkuriem $x_i \in I_i$, $x_j \in I_j$ izpildās $x_i x_j = 0$.

1.3. Ķīniešu atlikumu teorēma gredzenos

1.3. teorēma. I un J ir ideāli gredzenā R. Dots, ka $I + J = R$, $a, b \in R$ - patvaļīgi elementi. Tad

1. Sistēmai
$$\begin{cases} x = a(\text{mod } I) \\ x = b(\text{mod } J) \end{cases}$$
eksistē atrisinājums.

2. Jebkuri divi sistēmas atrisinājumi ir kongruenti mod $I \cap J$: ja x_1 un x_2 apmierina sistēmu, tad $x_1 \equiv x_2 (\text{mod } I \cap J)$.

PIERĀDĪJUMS

1. Tā kā $I + J = R$, tad eksistē $t \in I$, $t' \in J$ tādi, ka

$$a - b = t + t'.$$

Pārnesot dažus elementus uz pretējām pusēm, iegūsim

$$-t + a = t' + b.$$

Definēsim

$$X = -t + a = t' + b.$$

Redzam, ka

$$X - a = -t \in I,$$
$$X - b = t' \in J.$$

Tādējādi X apmierina sistēmu.

2. Ja sistēmai eksistē divi atrisinājumi X un Y, tad

$$X - Y \equiv 0 (\text{mod } I),$$

$$X - Y \equiv 0 (\text{mod } J).$$

Seko, ka

$$X - Y \equiv 0 (\text{mod } I \cap J).$$

■

1.4. teorēma. I un J ir ideāli gredzenā R. Dots, ka $I + J = R$. Tad

$$R/(I \cap J) \simeq R/I \times R/J.$$

PIERĀDĪJUMS Apzīmēsim $I \cap J$ ar K. Definēsim funkciju

$$\varphi : R/(I \cap J) \to R/I \times R/J,$$

$$\varphi(r + K) = (r + I, r + J).$$

Pierādīsim, ka φ ir korekti definēts bijektīvs gredzenu homomorfisms.

Korektums Ja $r + K = r' + K$, tad $r - r' \in K \subseteq I, J$. Seko, ka

$$\varphi(r + K) = (r + I, r + J) = (r' + I, r' + J) = \varphi(r' + K).$$

Sirjektivitāte Saskaņā ar ķīniešu atlikumu teorēmu gredzeniem katram pārim (a, b) eksistē klase x mod K tāda, ka

$$x \equiv a(\text{mod } I),$$

$$x \equiv b(\text{mod } J).$$

Seko, ka

$$\varphi(x + K) = (a + I, b + J).$$

Injektivitāte Ja $\varphi(r + K) = \varphi(r' + K)$, tad

$$(r + I, r + J) = (r' + I, r' + J).$$

No ķīniešu atlikumu teorēmas seko ka $r \equiv r'(\text{mod } K)$.

Homomorfisms

$$\varphi((r + K) + (r' + K)) = \varphi((r + r') + K) =$$
$$((r + r') + I, (r + r') + J) = ((r + I) + (r' + I), (r + J) + (r' + J)) =$$
$$(r + I, r + J) + (r' + I, r' + J) = \varphi(r + K) + \varphi(r' + K).$$

Reizināšana tiek pierādīta līdzīgi.
■

1.4. Pielietojumi veselo skaitļu teorijā

Šajā sadaļā ar $\mathbb{Z}_n$ apzīmēsim atlikumu klašu gredzenu mod n.

1.5. teorēma. $LKD(m_1, m_2) = 1 \implies \mathbb{Z}_{m_1 m_2} \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$.

PIERĀDĪJUMS Gredzenā $\mathbb{Z}$ eksistē ideāli

$$I_{m_1} = (m_1), I_{m_2} = (m_2).$$

Tā kā $LKD(m_1, m_2) = 1$, tad eksistē veseli skaitļi a_1, a_2 tādi, ka

$$1 = a_1 m_1 + a_2 m_2.$$

Seko, ka $\mathbb{Z} = I_{m_1} + I_{m_2}$.

Redzam, ka

$$I_{m_1} \cap I_{m_2} = (m_1 m_2).$$

Saskaņā ar vienu no iepriekšējām teorēmām

$$\underbrace{\mathbb{Z}/(m_1 m_2)}_{=\mathbb{Z}_{m_1 m_2}} \simeq \underbrace{\mathbb{Z}/(m_1) \oplus \mathbb{Z}/(m_2)}_{=\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}}.$$

■

1.6. teorēma.

$$LKD(m_1, m_2, ..., m_n) = 1 \implies$$
$$\mathbb{Z}_{m_1 m_2 ... m_n} \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_n}.$$

PIERĀDĪJUMS Matemātiskā indukcija ar parametru n. ■

1.2. piezīme. Speciālgadījumā iegūsim gredzenu izomorfismu

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus ... \oplus \mathbb{Z}_{p_l^{\alpha_l}},$$

ja $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_l^{\alpha_l}$.

1.7. teorēma.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_l^{\alpha_l} \implies U_n \simeq U_{p_1^{\alpha_1}} \times U_{p_2^{\alpha_2}} \times ... \times U_{p_l^{\alpha_l}}.$$

(grupu tiešā summa)

PIERĀDĪJUMS Atcerēsimies, ka bijekcija

$$\varphi : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus ... \oplus \mathbb{Z}_{p_l^{\alpha_l}}$$

ir dota ar nosacījumu

$$\varphi(x + n\mathbb{Z}) = (x + p_1^{\alpha_1}\mathbb{Z}, ..., x + p_l^{\alpha_l}\mathbb{Z})$$

Kopu bijekcija Ja klase $x + n\mathbb{Z}$ ir multiplikatīvi invertējama, tad eksistē klase $y + n\mathbb{Z}$ tāda, ka $xy \equiv 1 (\text{mod } n\mathbb{Z})$. Seko, ka

$$xy \equiv 1 (\text{mod } p_i^{\alpha_i}\mathbb{Z}).$$

Ja $x+n\mathbb{Z}$ ir invertējams, tad $\varphi(x+n\mathbb{Z}) = (x+p_1^{\alpha_1}\mathbb{Z}, ..., x+p_l^{\alpha_l}\mathbb{Z})$ arī ir invertējams, jo

$$(x+p_1^{\alpha_1}\mathbb{Z}, ..., x+p_l^{\alpha_l}\mathbb{Z}) \cdot (y+p_1^{\alpha_1}\mathbb{Z}, ..., y+p_l^{\alpha_l}\mathbb{Z}) = (1+p_1^{\alpha_1}\mathbb{Z}, ..., 1+p_l^{\alpha_l}\mathbb{Z})$$

Un otrādi - ja $(x+p_1^{\alpha_1}\mathbb{Z}, ..., x+p_l^{\alpha_l}\mathbb{Z})$ ir invertējams elements gredzenā $\mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus ... \oplus \mathbb{Z}_{p_l^{\alpha_l}}$, tad eksistē elementi $y_1, ..., y_l$ tādi, ka $xy_i \equiv 1 (\text{mod } p_i^{\alpha_i}\mathbb{Z})$. Seko, ka $y_i \equiv x^{-1} (\text{mod } p_i^{\alpha_i}\mathbb{Z})$.

Sistēmai

$$\begin{cases} y = x^{-1} (\text{mod } p_1^{\alpha_1}\mathbb{Z}) \\ y = x^{-1} (\text{mod } p_2^{\alpha_2}\mathbb{Z}) \\ ... \\ y = x^{-1} (\text{mod } p_l^{\alpha_l}\mathbb{Z}) \end{cases}$$

eksistē atrisinājums saskaņā ar ķīniešu atlikumu teorēmu gredzeniem. Seko, ka $x + n\mathbb{Z}$ ir invertējama klase.

Grupu homomorfisms

$$\varphi((x+n\mathbb{Z})(x'+n\mathbb{Z})) = \varphi(xx'+n\mathbb{Z}) =$$
$$(xx'+p_1^{\alpha_1}\mathbb{Z},...,xx'+p_l^{\alpha_l}\mathbb{Z}) =$$
$$(x+p_1^{\alpha_1}\mathbb{Z},...,x+p_l^{\alpha_l}\mathbb{Z})(x'+p_1^{\alpha_1}\mathbb{Z},...,x'+p_l^{\alpha_l}\mathbb{Z}) =$$
$$\varphi(x+n\mathbb{Z})\varphi(x'+n\mathbb{Z}).$$

■

1.1. piemērs. Pierādīsim, ka $U_{21} \simeq U_{28} \simeq U_{36} \simeq U_{42}$.
$U_{21} \simeq U_3 \times U_7 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.
$U_{28} \simeq U_4 \times U_7 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.
$U_{36} \simeq U_4 \times U_9 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.
$U_{42} \simeq U_2 \times U_3 \times U_7 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

$U_{13} \simeq \mathbb{Z}_{12} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3$

$U_{26} \simeq U_2 \times U_{13} \simeq \mathbb{Z}_{12} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3$

$U_{13} \not\simeq U_{21}$, jo U_{21} nesatur elementu ar kārtu 4.

2. Moduļi

2.1. Pamatdefinīcijas un piemēri

R ir komutatīvs unitārs gredzens. M ir komutatīva grupa ar aditīvu pierakstu.

Saka, ka M ir *kreisais R-modulis* , ja ir dota funkcija

$$R \times M \to M,$$

$$(r, m) \mapsto rm$$

(gredzena elementu *darbības funkcija*) ar šādām īpašībām:

1. $r(m + m') = rm + rm'$, $\forall r \in R$, $\forall m, m' \in M$ (darbības funkcija ir M-lineāra),
2. $(r + r')m = rm + r'm$, $\forall r, r' \in R$, $\forall m, \in M$ (darbības funkcija ir R-lineāra),
3. $1 \cdot m = m$, $\forall m \in M$ (darbības funkcija ir normēta vai unitāra).

Līdzīgi definē *labo R-moduli* - ar funkciju

$$R \times M \to M,$$

$$(r, m) \mapsto mr.$$

Tālāk uzskatīsim, ka visi moduļi ir kreisie.

Grupu M (bez gredzena darbības funkcijas) sauc par moduļa M *veidojošo telpu (underlying space)* .

2.1. piemērs. Gredzena R jebkurš ideāls I ir R-modulis, ja R darbība ir elementu reizināšana. Speciālgadījums - pats gredzens R arī ir R-modulis.

Jebkura komutatīva grupa A ir $\mathbb{Z}$-modulis, darbības funkcija ir

$$na = \underbrace{a + a + ... + a}_{n \text{ reizes}}.$$

Lineāra telpa L virs lauka k $(\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_p)$ ir k-modulis, darbības funkcija - reizināšana ar lauka elementu (piemēram, vektora reizināšana ar skalāru).

Ja lineārā telpā L virs lauka k ir dots lineārs operators $\mathcal{F} : L \to L$, tad komutatīvajā grupā $(L, +)$ tiek uzdota $k[X]$-moduļa darbība ar šādu nosacījumu: ja

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0,$$

tad

$$f(X) \cdot l = a_n \mathcal{F}^n l + a_{n-1} \mathcal{F}^{n-1} l + ... + a_1 \mathcal{F} l + a_0 l.$$

2.2. Apakšmoduļi

Ja $r \in R$ un $S \subseteq M$, tad apzīmēsim

$$rS = \{x \in M | x = rm, \text{ kur } m \in M\}.$$

Ja M ir R-modulis, tad apakšgrupu $S \leq M$ sauc par *apakšmoduli* (apzīmē $S \subseteq M$), ja

$$rS \subseteq S, \forall r \in R$$

vai, elementu terminos -

$$rs \in S, \forall r \in R, s \in S.$$

Moduli M sauc par vienkāršu, ja tam nav netriviālu apakšmoduļu (atšķirīgu no M un $\{0\}$).

2.2. piemērs. Komutatīvas grupas A kā $\mathbb{Z}$-moduļa jebkura apakšgrupa ir apakšmodulis.

Lineāras telpas L kā k-moduļa jebkura lineāra apakštelpa ir apakšmodulis.

Lineāras telpas L virs lauka k ar lineāru operatoru $\mathcal{F}$ kā $k[X]$-moduļa apakšmoduļi ir $\mathcal{F}$-invariantās apakštelpas.

Ja ir doti R-moduļa M vairāki apakšmoduļi $M_1, ..., M_n$, tad var apskatīt to šķēlumu $\bigcap_{i=1}^{n} M_i$.

2.1. teorēma. $\bigcap_{i=1}^{n} M_i$ ir R-modulis.

PIERĀDĪJUMS Patstāvīgi. ■

Ja ir doti R-moduļa M vairāki apakšmoduļi $M_1, ..., M_n$, tad par to summu $M_1 + ... + M_n = \sum_{i=1}^{n} M_i$ sauc kopu

$$\{x \in M | x = m_1 + ... + m_n, \text{ kur } m_i \in M_i\}.$$

2.2. teorēma. $\sum_{i=1}^{n} M_i$ ir R-modulis.

PIERĀDĪJUMS Patstāvīgi. ■

2.3. Moduļu homomorfismi

M, V ir divi R-moduļi. Funkciju

$$f : M \to V$$

sauc par *R-moduļu homomorfismu* , ja izpildās šādi nosacījumi:

1. $f(m + m') = f(m) + f(m')$ (f ir grupu homomorfisms);
2. $f(rm) = rf(m)$ (f komutē ar R darbību).

Par R-moduļu homomorfisma f attēlu $Im(f)$ sauc f kā funkcijas attēlu:

$$Im(f) = \{x \in V | x = f(m) \text{ kādam } m \in M\}.$$

Par R-moduļu homomorfisma f kodolu $Ker(f)$ sauc $f^{-1}(0_V)$:

$$Ker(f) = \{m \in M | f(m) = 0_V\}.$$

2.3. teorēma. Ja $f : M \to V$ ir moduļu homomorfisms, tad $Im(f) \subseteq V$ un $Ker(f) \subseteq V$.

PIERĀDĪJUMS Pārbaude. ■

2.4. Faktormoduļi

Ja ir dots R-modulis M un tā apakšmodulis $S \subseteq M$, tad var konstruēt faktorgrupu M/S, kurā var definēt R-moduļa struktūru ar šādu darbības funkciju:

$$r(m + S) = rm + S.$$

2.4. teorēma. M/S ir R-modulis.

PIERĀDĪJUMS

$$r((m+S)+(m'+S)) = r((m+m')+S) =$$
$$r(m+m')+S = rm+rm'+S = (rm+S)+(rm'+S) =$$
$$r(m+S)+r(m'+S).$$

$$(r+r')(m+S) = (r+r')m+S) =$$
$$rm+r'm+S = (rm+S)+(r'm+S) = r(m+S)+r'(m+S).$$

$$1(m+S) = 1\cdot m+S = m+S.$$

■

2.5. Moduļu veidotājelementi

R-moduļa M apakškopu Γ sauksim par tā veidotājsistēmu, ja

$$M = \{x \in M | x = r_1\gamma_1 + ... + r_n\gamma_n, \text{ kur } r_i \in R, \gamma_i \in \Gamma\}.$$

Ja M veidotājsistēma sastāv no viena elementa ($|\Gamma| = 1$), tad M sauc par *ciklisku moduli*.

2.3. piemērs. R kā R-modulis ir ciklisks.

Ja M veidotājsistēma Γ ir galīga kopa ($|\Gamma| < \infty$), tad M sauc par *galīgi ģenerētu (galīga tipa)* R-moduli.

2.4. piemērs. Jebkura galīga komutatīva grupa ir galīgi ģenerēts $\mathbb{Z}$-modulis.

2.6. Moduļu tiešā summa

2.6.1. Ārējā tiešā summa

Ja $M_1, ..., M_n$ ir R-moduļi, tad par to tiešo summu sauc grupu $M_1 \oplus ... \oplus M_n$, kurā R darbība ir uzdota šādā veidā:

$$r(m_1, ..., m_n) = (rm_1, ..., rm_n).$$

2.6.2. Iekšējā tiešā summa

Ja $M = M_1 + ... + M_n$ un katram j izpildās nosacījums

$$M_j \bigcap \sum_{1 \leq i \leq n, i \neq j} M_j = \{0\},$$

tad M sauc par apakšmoduļu $M_1, ..., M_n$ iekšējo tiešo summu.

2.7. k-algebras

Ja R ir komutatīvs unitārs gredzens, tad par R-algebru sauc kopu A ar šādām struktūrām:

1. A ir gredzens - $(A, +, \cdot)$;
2. A ir R-modulis ar operāciju $+$ definētu komutatīvās grupas struktūru, kas apmierina nosacījumu

$$r(aa') = (ra)a' = a(ra'),$$

visiem $r \in R, a, a' \in A$.

Zemāk apskatīsim tikai svarīgu speciālgadījumu - k-algebras, kur k ir lauks.

3. 8.mājasdarbs

8.1 Nosakiet grupas U_{2008} izomorfisma tipu (mēģiniet izteikt to formā $\mathbb{Z}_{p_1^{\alpha_1}} \oplus ... \oplus \mathbb{Z}_{p_m^{\alpha_m}}$, izmantojiet faktus par primitīvajām saknēm).

8.2 Kādos gadījumos lineāra telpa virs k ir vienkāršs k-modulis?

8.3 Kādos gadījumos lineāra telpa virs k ir izsakāma kā netriviālu apakšmoduļu tiešā summa?