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

Studiju kurss

Algebriskās struktūras

6.lekcija

Docētājs: Dr. P. Daugulis

2010./2011.studiju gads

Saturs

Lekcijas mērķis:

- apgūt komutatīvo grupu klasifikāciju.

Lekcijas kopsavilkums:

- komutatīvu galīgu grupu struktūra ir līdzīga vektoru grupu struktūrai: eksistē cikliskas "koordinātu" apakšgrupas, jebkurš elements izsakās kā šo apakšgrupu elementu lineāra kombinācija.

Svarīgākie jēdzieni: p-primārā apakšgrupa, komutatīva p-grupa.

Svarīgākie fakti un metodes: p-primāro apakšgrupu īpašības, galīgas komutatīvas grupas izteikšana p-primāru apakšgrupu tiešās summas veidā, maksimālās kārtas elementa cikliskās apakšgrupas atšķelšana komutatīvā p-grupā, rezultējošais sadalījums tiešajā summā, vispārējās galīgo komutatīvo grupu teorijas specializācija atlikumu aditīvo un multiplikatīvo grupu gadījumos.

1. Galīgās komutatīvās grupas

Šīs sadaļas mērķis ir aprakstīt galīgo komutatīvo grupu klasifikāciju - pierādīt, ka katra galīga komutatīva grupa ir izomorfa ciklisku grupu tiešajam reizinājumam.

1.1. piezīme. Lietojot analoģiju ar vektoru grupu, var teikt, ka galīgās komutatīvās grupas ir līdzīgas vektoru grupai, kuriem katrā komponentē notiek atlikumu klašu saskaitīšana.

Šajā sadaļā visas grupas ir komutatīvas.

Izmantosim aditīvo pierakstu. Piemēram,

- $A + B = \{g | g = a + b, \text{ kur} a \in A, b \in B\}$.
- komutatīvu grupu tiešais reizinājums

$$A_1 \times ... \times A_n = \prod_{i=1}^{n} A_i$$

tiek saukts par *tiešo summu* un apzīmēts ar

$$A_1 \oplus ... \oplus A_n = \bigoplus_{i=1}^{n} A_i;$$

- apakšgrupa, kuru ģenerē $g \in A$ ar kārtu k ir

$$\langle g \rangle = \{x \in A | x = n \cdot g,\ n \in \mathbb{Z}\} = \{g, 2g, 3g, ..., (k-1)g, \underbrace{kg}_{=0}\},$$

$$|\langle g \rangle| = k,$$

Pārtulkosim zināmos faktus par cikliskajām grupām un tiešo reizinājumu aditīvajā valodā:

- $a \in A$ kārta ir k ($k \in \mathbb{N}$ ir mazākais skaitlis: $ka = 0$) $\Longrightarrow$

$$ma = 0 \iff k|m;$$

- $a \in A$ kārta ir k un $l|k \implies la$ kārta ir $\frac{k}{l}$;

- A_1,..., $A_n \leq A$ un $\forall g \in A$ ir viennozīmīgi izsakāms formā

$$g = g_1 + ... + g_n = \sum_{i=1}^{n} g_i, \text{ kur } g_i \in A_i \implies$$

$$A = A_1 \oplus ... \oplus A_n;$$

- $A_1, A_2 \leq A$, $A = A_1 + A_2$ un $A_1 \cap A_2 = \{0\} \implies$

$$A = A_1 \oplus A_2.$$

1.2. piezīme. Var rasties grūtības, strādājot ar komutatīvām grupām multiplikatīvajā pierakstā, piemēram, ar atlikumu multiplikatīvajām grupām.

1.1. Komutatīvās grupas sadalījums primāro grupu tiešajā summā

A ir komutatīva grupa, $p \in \mathbb{P}$. Definēsim

$$A(p) = \{g \in A | \exists\ k \in \mathbb{N} : p^k g = 0\}.$$

$A(p)$ sauc par *A p-primāro apakšgrupu.*

1.3. piezīme. $0 \in A(p)$, $\forall p$, jo 0 kārta ir vienāda ar $1 = p^0$. $\mathbb{Z}_{12}$.

Ja $A = A(p)$, tad A sauc par *komutatīvu p-grupu.*

1.1. teorēma. $\forall\ p \in \mathbb{P}$: $A(p) \leq A$.

PIERĀDĪJUMS
Neitrālais elements
$0 \in A(p)$ $\forall p$, jo 0 kārta ir $1 = p^0$.

Inversais elements
$p^n a = 0 \iff p^n(-a) = -(p^n a) = 0.$

Reizinājums

$$\begin{cases} p^n a = 0 \\ p^m b = 0. \end{cases}$$

Apzīmēsim $\max(n, m)$ ar w. $\Longrightarrow$

$$p^w(a+b) = p^w a + p^w b = p^{w-n}(p^n a) + p^{w-m}(p^m b) = 0 + 0 = 0.\blacksquare$$

1.2. teorēma. *A ir galīga komutatīva grupa, $g \in A$, $|\langle g \rangle| = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$. Tad g var izteikt formā*

$$g = \sum_{i=1}^{n} g_i, \text{ kur } g_i \in A(p_i).$$

PIERĀDĪJUMS Matemātiskā indukcija ar parametru n.

Indukcijas bāze
$n = 1 \implies |\langle g \rangle| = p^\alpha \implies p^\alpha g = 0 \implies g \in A(p).$

Indukcijas solis Pieņemsim, ka apgalvojums ir pierādīts visos gadījumos, kad $|\langle g \rangle|$ dala ne vairāk kā $n-1$ pirmskaitlis un pierādīsim, ka tad apgalvojums ir patiess, ja $|\langle g \rangle|$ dala n pirmskaitļi.

Pieņemsim, ka

$$|\langle g\rangle| = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n} = \underbrace{(p_1^{\alpha_1} ... p_{n-1}^{\alpha_{n-1}})}_{u} \underbrace{(p_n^{\alpha_n})}_{v}.$$

Citiem vārdiem sakot $k = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$ ir g kārta: mazākais naturālais skaitlis, kuram $kg = 0$.

$$LKD(u, v) = 1 \implies \exists\, a, b \in \mathbb{Z}\colon\ au + bv = 1.$$

"Sašķelsim" g:

$$g = 1 \cdot g = (au + bv)g = aug + bvg = a(ug) + b(vg) = b\widetilde{g} + ag_n.$$

$$p_n^{\alpha_n} g_n = \underbrace{p_n^{\alpha_n} u}_{=k} g = kg = 0 \implies g_n \in A(p_n).$$

Līdzīgā veidā: $(p_1^{\alpha_1} ... p_{n-1}^{\alpha_{n-1}})\widetilde{g} = (p_1^{\alpha_1} ... p_{n-1}^{\alpha_{n-1}})vg = kg = 0.$

$\widetilde{g}$ kārtu dala ne vairāk kā $n-1$ pirmskaitļi $p_1, ..., p_{n-1} \implies$ saskaņā

ar indukcijas pieņēmumu

$$\widetilde{g} = \sum_{i=1}^{n-1} g_i, \text{ kur } g_i \in A(p_i).$$

Apvienojot visu, iegūstam, ka

$$g = b\Big(\sum_{i=1}^{n-1} g_i\Big) + ag_n = \Big(\sum_{i=1}^{n-1} bg_i\Big) + ag_n, \text{ kur } \begin{cases} bg_i \in A(p_i), \\ ag_n \in A(p_n). \end{cases} \blacksquare$$

1.3. teorēma. *A ir galīga komutatīva grupa, $|A| = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$, tad*

$$A = A(p_1) \oplus A(p_2) \oplus ... \oplus A(p_n).$$

PIERĀDĪJUMS

Viennozīmīgums

Pierādīsim, ka $\forall\ g \in A$ ir viennozīmīgi izsakāms formā

$$g = \sum_{i=1}^{n} g_i, \text{ kur } g_i \in A(p_i).$$

$|\langle g\rangle| \mid |A| \implies$ saskaņā ar iepriekšējo teorēmu g var izteikt formā

$$g = \sum_{i=1}^{n} g_i, \text{ kur } g_i \in A(p_i).$$

Pieņemsim, ka g var izteikt divos veidos:

$$g = \sum_{i=1}^{n} g_i = \sum_{i=1}^{n} h_i, \text{ kur } g_i, h_i \in A(p_i).$$

A ir komutatīva grupa $\implies g_n - h_n = \sum_{i=1}^{n-1}(h_i - g_i)$.
$\forall i\ h_i - g_i \in A(p_i) \implies h_i - g_i$ kārta ir $p_i^{\beta_i}$.

Apzīmēsim $p_1^{\beta_1} ... p_{n-1}^{\beta_{n-1}}$ ar K.
$K\left(\sum_{i=1}^{n-1} h_i - g_i\right) = 0 \implies K \underbrace{(g_n - h_n)}_{\in A_{p_n}} = 0$

$\implies$ $g_n - h_n$ kārta dala K, bet tā ir vienāda ar p_n pakāpi.
$LKD(K, p_n) = 1 \implies g_n - h_n$ kārta ir $1 \implies g_n = h_n$.

Līdzīgā veidā pierāda, ka $\forall i\ g_i = h_i$. ■

1.1. piemērs. $\mathbb{Z}_{12} = A(2) \oplus A(3)$.
$\mathbb{Z}_{15} = A(3) \oplus A(5)$.

1.2. Maksimālas kārtas elementa apakšgrupas atšķelšana

Dots, ka A ir galīga komutatīva p-grupa. $g \in A$ sauc par *maksimālas kārtas elementu*, ja tā kārta ir maksimāla.

1.2. piemērs. $1 \in \mathbb{Z}_m$. Primitīvās saknes grupā $\mathcal{U}_m$.

1.4. teorēma. *A ir galīga komutatīva p-grupa, g ir maksimālas kārtas elements. Tad eksistē $H \leq A$:*

$$A = \langle g \rangle \oplus H.$$

PIERĀDĪJUMS (patstāvīgā lasīšana)
Apskatīsim visas A apakšgrupas N, kurām izpildās nosacījums

$$N \cap \langle g \rangle = \{0\}.$$

Vismaz viena tāda apakšgrupa eksistē - $\{0\}$. Apzīmēsim visu šādu apakšgrupu kopu ar $\mathcal{N}$.

$|A| < \infty \implies \exists$ maksimāla attiecībā uz iekļaušanu apakšgrupa H: $H \lneq H' \implies H' \notin \mathcal{N}$.

Mērķis: pierādīt, ka

$$A = \langle g \rangle + H,$$

tad no grupu tiešā reizinājuma/summas īpašībām sekos, ka

$$A = \langle g \rangle \oplus H.$$

Pieņemsim pretējo - $\langle g \rangle + H \subsetneq A \implies \exists\, x \notin \langle g \rangle + H$, $x \neq 0$.

Pieņemsim, ka $k \in \mathbb{N}$ ir mazākais skaitlis, kuram

$$p^k x \in \langle g \rangle + H.$$

Tāds k eksistē, jo x kārta ir p pakāpe - $p^j x = 0 \in \langle g \rangle + H$.

$y = p^{k-1}x \notin \langle g \rangle + H,$
$py = p^k x = tg + h,$ kur $h \in H.$

g ir maksimālas kārtas p^n elements $\Longrightarrow$ $p^n a = 0\ \forall a \in G$: $\Longrightarrow$

$$p^n y = 0 = p^{n-1}(py) = p^{n-1}tg + p^{n-1}h \Longrightarrow$$

$$p^{n-1}tg = -p^{n-1}h \in \langle g \rangle \cap H = \{0\} \Longrightarrow$$

$p|t \Longrightarrow t = mp \Longrightarrow py = tg + h = pmg + h \Longrightarrow$

$$h = py - pmg = p\underbrace{(y - mg)}_{=z}.$$

Redzam, ka $z \notin H$, jo pretējā gadījumā $z = y - mg = h' \in H$ un $y = mg + h' \in \langle g \rangle + H.$

Kopa $S = H + \mathbb{Z}z$ ir G apakšgrupa, kas satur H.

$$\begin{cases} z \in S \\ z \notin H \end{cases} \Longrightarrow H \lneqq S.$$

$$\Big(H \text{ ir maksimālā apakšgrupa: } \langle g\rangle \cap H = \{0\}\Big) \Longrightarrow \langle g\rangle \cap S \neq \{0\}.$$

Pieņemsim, ka $w \in \langle g\rangle \cap S$, $w \neq 0 \Longrightarrow w = sg = h_1 + rz$.

$p \nmid r$, jo pretējā gadījumā

$$w = \underbrace{sg}_{\in\langle g\rangle} = h_1 + l\underbrace{pz}_{=h} = \underbrace{h_1 + lh}_{\in H} \in \langle g\rangle \cap H = \{0\}.$$

$$\Longrightarrow LKD(p,r) = 1 \Longrightarrow \exists\, u, v \in \mathbb{Z}\colon\ 1 = up + vr.$$

Redzam, ka

$$\begin{aligned} y = 1 \cdot y = (up + vr)y = u(py) + v(ry) = \\ u(tg + h) + v(r(z + mg)) = utg + uh + v(rz + rmg) = \\ utg + uh + v(sg - h_1 + rmg) = \\ (ut + vs + vrm)g + (uh - vh_i) \in \langle g\rangle + H. \end{aligned}$$

Tā ir pretruna, jo saskaņā ar pieņēmumu $y \notin \langle g\rangle + H$. ■

1.5. teorēma. *A ir galīga komutatīva grupa. Tad*

$$A = A_1 \oplus ... \oplus A_n, \text{ kur}$$

1. $\forall\, i:\ A_i$ ir cikliska grupa,
2. $\forall\, |A_i| = p_i^{\alpha_i}$.

PIERĀDĪJUMS Saskaņā ar iepriekš pierādītu teorēmu

$$A = A(p_1) \oplus A(p_2) \oplus ... \oplus A(p_n), \text{ kur } |A(p_j)| = p_j^{\beta_j}.$$

Pierādīsim, ka $\forall\, p\ A(p)$ ir ciklisku grupu tiešā summa. Izmantosim matemātisko indukciju ar parametru $|A(p)|$.

Indukcijas bāze $|A(p)| = p \implies A(p)$ nesatur netriviālas apakšgrupas saskaņā ar Lagranža teorēmu $\implies \forall\, g \neq e:\ \langle g \rangle = A(p) \implies A(p)$ ir cikliska grupa.

Indukcijas solis Apskatīsim maksimālas kārtas elementu $g \in A(p)$. Saskaņā ar iepriekšējo teorēmu

$$A(p) = \langle g \rangle \oplus H,$$

kur H ir mazāka grupa, uz kuru attiecas indukcijas pieņēmums - tā ir ciklisku grupu tiešā summa. ■

1.4. piezīme. Pierādītās teorēmas var apkopot šādā veidā: A ir galīga komutatīva grupa $\Longrightarrow$ $A \simeq \mathbb{Z}_{p_1^{\alpha_1}} \oplus ... \mathbb{Z}_{p_l^{\alpha_l}}$.

1.3. Atlikumu klašu grupas

1.3.1. Aditīvās grupas

Šajā sadaļā apzīmēsim $\mathbb{Z}/m\mathbb{Z}$ ar $\mathbb{Z}_m$.

$p \in \mathbb{P}$. Definēsim *p-primāro apakšgrupu*

$$T_p = \{a \in \mathbb{Z}_m | \exists\ \alpha \in \mathbb{N} \cup \{0\} : p^\alpha a \equiv 0 (\text{mod } m)\}.$$

1.6. teorēma. $A = \mathbb{Z}_m$, $m \in \mathbb{Z}$.

1. $a|b \Longrightarrow \langle b \rangle \leq \langle a \rangle$.

2. $\langle a \rangle = \langle LKD(a,m) \rangle$.

PIERĀDĪJUMS

1. $a|b \implies b = aq \implies \forall\, n \in \mathbb{Z}:\ nb = (nq)a \implies nb \in \langle a \rangle$.

2. Apzīmēsim $LKD(a,m)$ ar d. No iepriekšējās teorēmas seko, ka $\langle a \rangle \leq \langle d \rangle$.

Saskaņā ar lineārās kombinācijas īpašību

$d = ua + vm \implies d \equiv ua (\mathrm{mod}\ m) \implies$

$\forall\, n \in \mathbb{Z}:\ nd \equiv n(ua) \equiv (nu)a (\mathrm{mod}\ m) \implies \langle d \rangle \leq \langle a \rangle \implies \langle d \rangle = \langle a \rangle$. ■

1.5. piezīme. Seko, ka ir savstarpēji viennozīmīga atbilstība starp m dalītājiem un $\mathbb{Z}_m$ apakšgrupām.

1.3. piemērs. $\mathbb{Z}_{20}$. Apakšgrupas: $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle = \langle 6 \rangle$, $\langle 4 \rangle = \langle 8 \rangle$, $\langle 5 \rangle$, $\langle 10 \rangle$.

1.7. teorēma. $LKD(n,m)=1 \implies \mathbb{Z}_{nm} \simeq \mathbb{Z}_n \oplus \mathbb{Z}_m$.

PIERĀDĪJUMS Pārbaudīsim, ka $(1,1)$ ir grupas $\mathbb{Z}_n \oplus \mathbb{Z}_m$ veidotājelements.

$k(1,1)=(k,k)=(0,0) \implies n|k$ un $m|k$.
$LKD(n,m)=1 \implies nm|t$.

Seko, ka $|\langle(1,1)\rangle| \geq nm \implies \langle(1,1)\rangle \supseteq \mathbb{Z}_n \oplus \mathbb{Z}_m$. ■

1.8. teorēma. $m=p_1^{\alpha_1}...p_l^{\alpha_l}$.

1. $\forall\ p_j \in \{p_1,...,p_l\} \implies T_{p_j}=\langle \frac{m}{p_j^{\alpha_j}} \rangle$.
2. $\mathbb{Z}_m = T_{p_1} \oplus ... \oplus T_{p_l}$.

PIERĀDĪJUMS

1. Simbolu ekonomijas dēļ apzīmēsim $\begin{cases} p=p_j \\ \alpha=\alpha_j \\ t_p=\frac{m}{p^\alpha} \end{cases}$

$$p^\alpha t_p = m \implies p^\alpha t_p \equiv 0 (\mathrm{mod}\ m) \implies t_p \in T_p \implies \boxed{\langle t_p \rangle \leq T_p}.$$

$$a \in T_p \implies p^\beta a \equiv 0 (\mathrm{mod}\ m) \implies p^\beta a = mq \implies$$
$$p^\beta a = p^\alpha t_p q \implies t_p | p^\beta a \implies t_p | a \implies a \in \langle t_p \rangle \implies$$
$$T_p \leq \langle t_p \rangle \implies \boxed{T_p = \langle t_p \rangle}.$$

4. Seko no iepriekšējas teorēmas. ■

1.3.2. Multiplikatīvās grupas

Skaitļu teorijas kursā tika pierādīts, ka

- multiplikatīvi invertējamo atlikumu klašu mod m kopa $\mathcal{U}_m$ ir galīga komutatīva grupa attiecībā uz atlikumu reizināšanu;
- $|\mathcal{U}_m| = \varphi(m)$;
- tiek izmantots multiplikatīvais pieraksts (kaut arī grupa ir komutatīva).

Atlikuma $a \in \mathcal{U}_m$ cikliskā apakšgrupa

$$\langle a \rangle = \{a^n\}_{n \in \mathbb{Z}} = \{1, a, a^2, ..., a^{-1}, a^{-2}, ...\}.$$

1.4. piemērs. $m = 13$. $\langle 2 \rangle = \mathcal{U}_{13}$.

$a \in \mathcal{U}_m$ multiplikatīvā kārta ($P_m(a)$ vai $P(a)$): mazākais $k \in \mathbb{N}$:

$$a^k \equiv 1 \text{ (mod m)}.$$

Pierādītās $\mathcal{U}_m$ īpašības:

- φ ir multiplikatīva funkcija;
- $a \in \mathcal{U}_m \implies a^m \equiv 1 (\text{mod } m)$ (Eilera teorēma);
- $a \in \mathcal{U}_m \implies a^{L(m)} \equiv 1 (\text{mod } m)$ (pastiprinātā Eilera teorēma).

2. 6.mājasdarbs

2.1. Obligātie uzdevumi

6.1 Noteikt, cik ir katras kārtas elementu grupā

(a) $\mathbb{Z}_2 \oplus \mathbb{Z}_4$;
(b) $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$.

6.2 A ir galīga komutatīva p-grupa. Pierādīt, ka

(a) kopa $pA = \{g \in A | g = px, x \in A\}$ ir apakšgrupa;
(b) $pA \lneqq A$.

6.3 Noteikt, vai grupas ir izomorfas:

(a) $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ un $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$;
(b) $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ un $\mathbb{Z}_9 \oplus \mathbb{Z}_{24}$;

6.4 Izsakiet tiešās summas/reizinājuma veidā šādas grupas:

(a) $(\mathbb{Z}_{28}, +)$;
(b) $(\mathcal{U}_{28}, \cdot)$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

6.5 G ir galīga p-grupa: $\forall\ g \in G\ \exists n \in \mathbb{N} : g^{p^n} = e$. Pierādīt, ka $Z(G) \neq \{e\}$.