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

Studiju kurss

Veselo skaitļu teorija

7.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt atlikumu aditīvo grupu īpašības.

Lekcijas kopsavilkums:

- atlikumu aditīvajā grupā var pilnībā saprast apakšgrupu tipus,
- atlikumu aditīvajā grupā ir spēkā vektoru bāzes vispārinājums - sadalījums apakšgrupu tiešajā summā.

Svarīgākie jēdzieni: aditīvās grupas cikliska apakšgrupa, cikliskas apakšgrupas ģenerators, p-primāra apakšgrupa.

Svarīgākie fakti un metodes: veselo skaitļu un atlikumu aditīvo grupu ciklisko apakšgrupu īpašības, atlikumu aditīvās grupas apakšgrupu klasifikācija, p-primāro apakšgrupu īpašības, atlikumu aditīvās grupas sadalījums tiešajā summā.

1. Atlikumu aditīvās grupas īpašības

Agrāk tika norādīts, ka

- atlikumu klašu mod m kopa $\mathbb{Z}_m$ ir grupa attiecībā uz atlikumu saskaitīšanu;
- $|\mathbb{Z}_m| = |m| \implies \mathbb{Z}_m$ ir galīga grupa;
- $\mathbb{Z}_m$ ir komutatīva grupa;
- tiek izmantots aditīvais pieraksts.

Iegūsim divus svarīgus rezultātus:

- jebkura $\mathbb{Z}_m$ apakšgrupa ir cikliska ("viendimensionāla", ja izmanto vektoru analoģiju - kaut kas līdzīgs plaknes vektoru telpai);
- $\mathbb{Z}_m$ var sadalīt apakšgrupu tiešajā summā (vektoru bāzes eksistences analogs).

1.1. Aditīvo grupu cikliskās apakšgrupas

$a \in A$, kur $A = \mathbb{Z}$ vai $\mathbb{Z}_m$. Apzīmēsim ar $\langle a \rangle$ kopu

$$\{n \cdot a\}_{n \in \mathbb{Z}} = \{0, \pm a, \pm 2a, \pm 3a, ...\} \subseteq A$$

a sauc par *ģeneratoru*.

1.1. piezīme. Ja $A = \mathbb{Z}_m$, tad $\langle a \rangle = \{a, 2a, ..., \underbrace{na}_{=0}\}$.

$-a = (n-1)a$,$-2a = (n-2)a$,...

1.1. teorēma. (ciklisko apakšgrupu īpašības) $A \in \{\mathbb{Z}, \mathbb{Z}_m\}$, $m \in \mathbb{Z}$.

1. $\forall\ a \in A\ \langle a \rangle \leq A$.
2. $\langle 1 \rangle = A$ (A ir *cikliska grupa* ar ģeneratoru 1).
3. $a|b \implies \langle b \rangle \leq \langle a \rangle$.

PIERĀDĪJUMS

1. Slēgtums: $(na) + (n'a) = (n + n')a \in \langle a \rangle$.

Neitrālais elements: $0 \cdot a = 0 \implies 0 \in \langle a \rangle$.

Inversie elementi: $na + (-n)a \equiv 0 \implies -(na) \in \langle a \rangle$.

2. $\langle 1 \rangle \subseteq A$.
$\forall\, n \in \mathbb{Z} :\ n = n \cdot 1 \implies A \subseteq \langle 1 \rangle \implies \langle 1 \rangle = A$.

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

1.2. teorēma. (ciklisko apakšgrupu īpašības atlikumu aditīvajās grupās) $m \in \mathbb{Z}$, $m \geq 2$.

1. $\langle a \rangle = \langle LKD(a, m) \rangle$.
2. $\langle a \rangle = \langle a' \rangle \iff LKD(a, m) = LKD(a', m)$.
3. $|\langle a \rangle| = \frac{m}{LKD(a,m)}$.

PIERĀDĪJUMS

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

Saskaņā ar lineārās kombinācijas īpašību
$d = ua + vm \implies d \equiv ua(\mathrm{mod}\ m) \implies$
$\forall\ n \in \mathbb{Z}: \quad nd \equiv n(ua) \equiv (nu)a(\mathrm{mod}\ m) \implies \langle d\rangle \leq \langle a\rangle \implies \langle d\rangle = \langle a\rangle.$

2. Apzīmēsim $LKD(a,m)$ ar d, $LKD(a',m)$ ar d' Saskaņā ar iepriekšējo apgalvojumu
$\Big(d = d'\Big) \implies \langle a\rangle = \langle d\rangle = \langle d'\rangle = \langle a'\rangle.$

$$\langle a\rangle = \langle a'\rangle \implies \langle d\rangle = \langle d'\rangle \iff \begin{cases} \langle d\rangle \leq \langle d'\rangle \\ \langle d'\rangle \leq \langle d\rangle \end{cases} \implies$$

$$\begin{cases} \exists\ n' \in \mathbb{Z}: \ d \equiv n'd'(\mathrm{mod}\ m) \\ \exists\ n \in \mathbb{Z}: \ d' \equiv nd(\mathrm{mod}\ m) \end{cases} \implies \begin{cases} d = n'd' + mq' \\ d' = nd + mq \end{cases} \implies$$

$$\begin{cases} d \equiv 0(\mathrm{mod}\ d') \\ d' \equiv 0(\mathrm{mod\ d}) \end{cases} \implies \begin{cases} d'|d \\ d|d' \end{cases} \implies d = d'.$$

3. Apzīmēsim $LKD(a,m)$ ar d, $\frac{m}{d}$ ar n. $\langle a\rangle = \langle d\rangle$.

$$LKD(d,m)=d \Longrightarrow \frac{m}{LKD(d,m)}\cdot d = m \equiv 0(\text{mod } m)$$

Apskatīsim $S=\{d,2d,...,(n-1)d,\underbrace{nd}_{=0}\}$. Pierādīsim, ka $|S|=n$.

$$\exists\, u,v\in\{1,...,n\}: \begin{cases} u>v \\ ua\equiv va(\text{mod } m) \end{cases} \Longrightarrow$$

$$\underbrace{(u-v)}_{=w} d \equiv 0(\text{mod } m).$$

$$\begin{cases} 0<w<n \\ wd\equiv 0(\text{mod } m) \end{cases} \Longrightarrow \begin{cases} 0<wd<m \\ wd=mq \end{cases} \Longrightarrow \text{- pretruna. } \blacksquare$$

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

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

1.2. Atlikumu aditīvās grupas apakšgrupu klasifikācija

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

$\forall\, H \leq A,\ H \neq \{0\}:\ \Big(\exists\, g \in A:\ \langle g \rangle = H\Big)$.

PIERĀDĪJUMS

$\underline{A = \mathbb{Z}}$ Dota $H \leq \mathbb{Z}$. Apskatīsim minimālo $g \in H$, $g > 0$.

Saskaņā ar iepriekšējo teorēmu $\langle g \rangle \leq H$. Pierādīsim, ka $\langle g \rangle = H$.

Pieņemsim pretējo: $\langle g \rangle \lneq H \implies \exists\, x \in H:\ ng \neq x, \forall\, n \in \mathbb{Z}$.

Izdalīsim x ar g:

$$x = qg + r,\ \text{kur } 0 \leq r \leq g - 1.$$

$$\begin{cases} x \in H \\ g \in H \end{cases} \implies x - qg = r \in H.$$

$r = 0 \implies x = qg$ - pretruna ar to, ka $x \notin \langle g \rangle$.

$r > 0 \implies$ pretruna, jo g ir minimālais pozitīvais H elements.

$\underline{A = \mathbb{Z}_m}$
Izmantosim kanonisko PAK $\{0, 1, ..., m-1\}$.
Dota $H \leq \mathbb{Z}_m$. Apskatīsim minimālo $b \in H$.
Saskaņā ar 1. $\langle b \rangle \leq H$.
Pierādīsim, ka $\langle b \rangle = H$.

Pieņemsim pretējo: $\exists\, x \in H : \; nb \not\equiv x (\text{mod } m), \forall\, n \in \mathbb{Z}$.
Saskaņā ar lineārās kombinācijas īpašību $\exists\, u, v \in H$:

$$\underbrace{LKD(b,x)}_{=d} = \underbrace{ub}_{\in H} + \underbrace{vx}_{\in H} \implies d \in H.$$

$d < b \implies$ pretruna, jo tad b nav minimālais elements.

$d = b \implies b|x \implies \exists\, n \in \mathbb{Z} : x = nb \implies x \equiv nb (\text{mod } m)$ - pretruna. ■

1.3. Atlikumu aditīvā grupa kā tiešā summa

Vai var izteikt $\mathbb{Z}_m$ kā savu apakšgrupu tiešo summu?

Var domāt par analoģiju ar vektoriem: $\forall$ vektors viennozīmīgi izsakās kā bāzes vektoru lineāra kombinācija. Analogs būtu vērtīgs rezultāts.

1.3.1. p-primārās apakšgrupas

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

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

1.2. piemērs. $\mathbb{Z}_{12}$. $T_2 = \{0, 3, 6, 9\}$, $T_3 = \{0, 4, 8\}$, $T_5 = \{0\}$.

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

1. $\forall\ p \in \mathbb{P} :\ T_p \leq \mathbb{Z}_m$.
2. $p \notin \{p_1, ..., p_l\} \implies T_p = \{0\}$.

3. $\forall\ p_j \in \{p_1, ..., p_l\} \implies T_{p_j} = \langle \frac{m}{p_j^{\alpha_j}} \rangle$.

4. $\forall\ p_j \in \{p_1, ..., p_l\} \implies |T_{p_j}| = p_j^{\alpha_j}$.

5. $p \neq p' \implies T_p \cap T_{p'} = \{0\}$.

PIERĀDĪJUMS

1. Neitrālais elements: $p \cdot 0 = 0 \implies 0 \in T_p,\ \forall\ p \in \mathbb{P}$.

Inversais elements: $a \in T_p \iff p^\alpha a \equiv 0 (\text{mod } m) \implies$
$p^\alpha (-a) \equiv 0 (\text{mod } m) \implies -a \in T_p$.

Slēgtums

$$\begin{cases} a \in T_p \\ a' \in T_p \end{cases} \implies \begin{cases} p^\alpha a \equiv 0 (\text{mod } m) \\ p^{\alpha'} a' \equiv 0 (\text{mod } m) \end{cases} \implies$$

$$p^{\alpha+\alpha'}(a + a') \equiv p^{\alpha+\alpha'} a + p^{\alpha+\alpha'} a'$$
$$\equiv p^{\alpha'}(p^\alpha a) + p^\alpha (p^{\alpha'} a') \equiv 0 (\text{mod } m).$$

2. $p \notin \{p_1, ..., p_l\} \Longrightarrow LKD(p, m) = 1 \Longrightarrow LKD(p^\alpha, m) = 1$

$\Longrightarrow p^\alpha \in \mathcal{U}_m \Longrightarrow p^\alpha a \equiv 0 (\text{mod } m) \Longleftrightarrow$

$(p^\alpha)^{-1} p^\alpha a \equiv (p^\alpha)^{-1} 0 (\text{mod } m) \Longleftrightarrow a \equiv 0 (\text{mod } m).$

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

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

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

4. Seko no iepriekšējas teorēmas.

5. $a \in T_p \cap T_{p'} \Longrightarrow \exists\, n, n' \in \mathbb{Z} : \; nt_p \equiv n' t_{p'} \equiv a (\text{mod } m) \Longrightarrow$

$$nt_p - n't_{p'} = mq \Longrightarrow n\frac{m}{p^\alpha} - n'\frac{m}{p^{\alpha'}} = mq \Longrightarrow$$

$$np^{\alpha'} - n'p^\alpha = p^\alpha p'^{\alpha'} q \Longrightarrow \begin{cases} np^{\alpha'} \equiv 0(\text{mod } p^\alpha) \\ n'p^\alpha \equiv 0(\text{mod } p'^{\alpha'}) \end{cases} \Longrightarrow$$

$n \equiv 0(\text{mod } p^\alpha) \Longrightarrow p^\alpha | n \Longrightarrow nt_p \equiv 0(\text{mod } m) \Longrightarrow$
$a \equiv 0(\text{mod } m)$. ■

1.3.2. Struktūras teorēma

1.3. piemērs. $\mathbb{Z}_{12}$. $T_2 = \{0, 3, 6, 9\}$, $T_3 = \{0, 4, 8\}$, $T_5 = \{0\}$.

$1 \equiv 9 + 4$, $2 \equiv 6 + 8$, $5 \equiv 9 + 8$, $7 \equiv 3 + 4$, $10 \equiv 6 + 4$, $11 \equiv 3 + 8$ - viennozīmīgi.

$\mathbb{Z}_{30}$. $T_2 = \{0, 15\}$, $T_3 = \{0, 10, 20\}$, $T_5 = \{0, 6, 12, 18, 24\}$.

$1 \equiv 10 + 5 + 6$, $2 \equiv 0 + 20 + 12$, $3 \equiv 15 + 0 + 18$, $4 \equiv 0 + 10 + 24$, $7 \equiv 15 + 10 + 12$, ... - viennozīmīgi.

1.5. teorēma. (*speciālgadījums - divi pirmskaitļi*) $m = p_1^{\alpha_1} p_2^{\alpha_2}$. $\forall\, a \in \mathbb{Z}_m$ ir viennozīmīgi izsakāms formā

$$a \equiv a_1 + a_2 (\mathrm{mod}\ m),\ \text{kur}\ a_i \in T_{p_i}.$$

PIERĀDĪJUMS

Eksistence

Izmantosim apzīmējumus $\begin{cases} t_{p_1} = \frac{m}{p_1^{\alpha_1}} = p_2^{\alpha_2} \\ t_{p_2} = \frac{m}{p_2^{\alpha_2}} = p_1^{\alpha_1}. \end{cases}$

$$LKD(t_{p_1}, t_{p_2}) = 1 \Longrightarrow \exists\, u, v \in \mathbb{Z}:\ 1 = u t_{p_1} + v t_{p_2} \Longrightarrow$$

$$a \equiv a \cdot 1 \equiv a(u t_{p_1} + v t_{p_2}) \equiv \underbrace{a u t_{p_1}}_{=a_1} + \underbrace{a v t_{p_2}}_{=a_2}.$$

$$\begin{cases} p_1^{\alpha_1} a_1 \equiv 0 (\mathrm{mod}\ m) \\ p_2^{\alpha_2} a_2 \equiv 0 (\mathrm{mod}\ m) \end{cases} \Longrightarrow \begin{cases} a_1 \in T_{p_1} \\ a_2 \in T_{p_2}. \end{cases}$$

Viennozīmīgums

$$a \equiv a_1 + a_2 \equiv a_1' + a_2' \Longrightarrow 0 \equiv \underbrace{(a_1 - a_1')}_{\in T_{p_1}} + \underbrace{(a_2 - a_2')}_{\in T_{p_2}} \Longrightarrow$$

$$\begin{cases} a_1 - a_1' \equiv -(a_2 - a_2') \\ T_{p_1} \cap T_{p_2} = \{0\} \end{cases} \Longrightarrow \begin{cases} a_1 - a_1' \equiv 0 \\ a_2 - a_2' \equiv 0. \end{cases} \blacksquare$$

1.6. teorēma.

$m = p_1^{\alpha_1} ... p_l^{\alpha_l}$. $\forall\ a \in \mathbb{Z}_m$ ir viennozīmīgi izsakāms formā

$$a \equiv a_1 + ... + a_l (\text{mod } m), \text{ kur } a_i \in T_{p_i}.$$

PIERĀDĪJUMS

Eksistence

Izmantosim apzīmējumu $t_{p_i} = \frac{m}{p_i^{\alpha_i}}$.

$LKD(t_{p_1}, ..., t_{p_l}) = 1 \Longrightarrow \exists\ u_1, ..., u_l \in \mathbb{Z} :\ 1 = \sum_{i=1}^{l} u_1 t_{p_i} \Longrightarrow$

$$a \equiv a \cdot 1 \equiv a\Big(\sum_{i=1}^{l} u_1 t_{p_i}\Big) \equiv \sum_{i=1}^{l} a u_i t_{p_i} \equiv \sum_{i=1}^{l} a_i.$$

$p_i^{\alpha_i} a_i \equiv 0 (\text{mod } m) \Longrightarrow a_i \in T_{p_i}$.

Viennozīmīgums Līdzīgs 2 pirmskaitļu gadījumam, var izmantot matemātisko indukciju. $\blacksquare$

1.3. piezīme. Grupu teorijas terminos iegūtais rezultāts nozīmē, ka $\mathbb{Z}_m = T_{p_1} \oplus ... \oplus T_{p_l}$ vai $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{\alpha 1}} \oplus ... \oplus \mathbb{Z}_{p_l^{\alpha l}}$.

2. 7.mājasdarbs

2.1. Obligātie uzdevumi

7.1 Atrast visas cikliskās apakšgrupas, to ģeneratorus un elementu skaitu.

(a) $\mathbb{Z}_{28}$;
(b) $\mathbb{Z}_{72}$.

7.2 Atrast p-primārās apakšgrupas un to ģeneratorus, izteikt dotos atlikumus summas veidā.

(a) $\mathbb{Z}_{36}$, $4, 7, 26$;
(b) $\mathbb{Z}_{80}$, $70, 71, 72$.

7.3 Atrisināt vienādojumus

(a) $2x \equiv 1 (\mathrm{mod}\ 21)$;
(b) $15x \equiv 18 (\mathrm{mod}\ 24)$;
(c) $27x \equiv 28 (\mathrm{mod}\ 36)$.

(*Norādījums: izmantojiet p-primārās apakšgrupas un sadalījumu tiešajā summā*)

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

7.4 $p \in \mathbb{P}$. Vai eksistē tādas apakšgrupas $A \leq \mathbb{Z}_{p^\alpha}$, $A \neq \{0\}$ un $B \leq \mathbb{Z}_{p^\alpha}$, $B \neq \{0\}$, ka $\mathbb{Z}_{p^\alpha} = A \oplus B$? (Ja atbilde ir negatīva, tas nozīmē, ka sadalījums p-primāro apakšgrupu tiešajā summā nevar tikt uzlabots).