

*DAUGAVPILS UNIVERSITĀTE*  
*Dabaszinātņu un matemātikas fakultāte*  
*Matemātikas katedra*

*Studiju kurss*

# SKAITĻU TEORIJA

## 6.lekcija

*Docētājs: Dr. P. Daugulis*

*2012./2013.studiju gads*

# Saturs

<b>1. Atlikumu sakaitīšanas īpašības</b>	<b>4</b>
1.1. Grupas . . . . .	4
1.1.1. Pamatdefinīcijas . . . . .	4
1.1.2. Aditīvais pieraksts . . . . .	5
1.1.3. Apakšgrupas . . . . .	5
1.1.4. Cikliskās apakšgrupas . . . . .	6
1.2. $\mathbb{Z}$ un atlikumu aditīvo grupu īpašības . . . . .	7
1.2.1. Pamatfakti . . . . .	7
1.2.2. Aditīvo grupu cikliskās apakšgrupas . . . . .	8
1.2.3. Atlikumu aditīvās grupas apakšgrupu klasifikācija . . . . .	12
<b>2. 5.mājasdarbs</b>	<b>14</b>
2.1. Obligātie uzdevumi . . . . .	14
2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi	15

Lekcijas mērķis:

- apgūt svarīgas algebriskas struktūras - grupu pamatjēdzienus,
- apgūt atlikumu aditīvo grupu īpašības.

### Lekcijas kopsavilkums:

- var definēt divas svarīgu algebrisku struktūru: grupas, apskatīt to vienkāršākās īpašības,
- atlikumu aditīvajā grupā var pilnībā saprast apakšgrupu tipus.

**Svarīgākie jēdzieni:** grupa, aditīvais pieraksts, apakšgrupa, cikliska apakšgrupa, aditīvās grupas cikliska apakšgrupa, cikliskas apakšgrupas ģenerators.

**Svarīgākie fakti un metodes:** atlikumu aditīvās grupas eksistence, aditīvo grupu ciklisko apakšgrupu īpašības, atlikumu aditīvās grupas apakšgrupu klasifikācija.

# 1. Atlikumu sakaitīšanas īpašības

## 1.1. Grupas

### 1.1.1. Pamatdefinīcijas

Par *grupu* sauc kopu  $G$ , kurā ir uzdota viena bināra (divu argumentu) operācija

$$G \times G \rightarrow G,$$

$$(x, y) \mapsto xy$$

kas apmierina šādas īpašības:

- operācija ir asociatīva:  $(xy)z = x(yz)$ ,  $\forall x, y, z$ ,
- $\exists$  neitrālais (vienības) elements  $e$ :  $xe = ex = x$ ,  $\forall x \in G$ ,
- $\forall x \in G \exists y = x^{-1} \in G$  ( $x$  inversais elements):  $xy = yx = e$ .

Grupās operāciju apzīmē ar kādu atdalošo simbolu  $(\cdot, *, +)$ .

Ja operācija ir komutatīva, tad grupu sauc par *komutatīvu* (*Ābela grupu*). Mēs šajā kursā sākot ar šo vietu strādāsim ar komutatīvajām grupām.

### 1.1.2. Aditīvais pieraksts

Komutatīvām grupām bieži lieto *aditīvo pierakstu* -

- par atdalošo simbolu izmanto  $+$  vai līdzīgu simbolu,
- neitrālo elementu apzīmē ar  $0$ ,
- inverso elementu  $-x$ .

**1.1. piemērs.**  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  ar saskaitīšanas operāciju ir komutatīvas grupas.  $(m\mathbb{Z}, +)$  ir komutatīva grupa. Vektoru kopa ar vektoru saskaitīšanas operāciju ir grupa.

### 1.1.3. Apakšgrupas

Grupas apakškopu  $H$  sauksim par  $G$  *apakšgrupu* ( $H \leq G$ ), ja

1.  $\begin{cases} h \in H \\ h' \in H \end{cases} \implies h + h' \in H;$
2.  $h \in H \implies -h \in H;$
3.  $e \in H.$

#### 1.1.4. Cikliskās apakšgrupas

Fiksēsim  $a \in G$ . Kopu  $\{0, \pm a, \pm 2a, \pm 3a, \dots\}$  sauc par *ciklisku apakšgrupu ar ģeneratoru  $a$* , apzīmē ar  $\langle a \rangle$ .

Par  $a$  kārtu sauc mazāko  $n \in \mathbb{N}$  tādu, ka  $n \cdot a = 0$ , ja tāds eksistē. Ja tāds  $n$  neeksistē,  $a$  kārtā ir  $\infty$ .

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

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

$$-2a = (n - 2)a, \dots$$

## 1.2. $\mathbb{Z}$ un atlikumu aditīvo grupu īpašības

### 1.2.1. Pamatfakti

#### 1.1. teorēma.

1.  $(\mathbb{Z}, +)$  ir komutatīva grupa.
2.  $\forall m \in \mathbb{Z}$ :  $(\mathbb{Z}/m, +)$  ir komutatīva grupa (*atlikumu aditīvā grupa*).

#### PIERĀDĪJUMS

1. Skaitļu un atlikumu klašu saskaitīšana ir asociatīva un komutatīva.

$0 \in \mathbb{Z}$  un  $[0] \in \mathbb{Z}/m$  ir neitrālie elementi.

$\forall x \in \mathbb{Z} : x + (-x) = 0 \equiv 0 \pmod{m} \implies -[x] = [-x] \implies$  klases  $[x]$  inversais elements ir klase  $[-x]$ . ■

**1.2. piezīme.** Atlikumu aditīvajām grupām vienmēr izmanto aditīvo pierakstu. Tālāk parasti identificēsim  $x$  un  $[x]$ .

### 1.2.2. Aditīvo grupu cikliskās apakšgrupas

**1.2. teorēma.** (ciklisko apakšgrupu īpašības)  $A \in \{\mathbb{Z}, \mathbb{Z}/m\}$ ,  $m \in \mathbb{Z}$ .

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

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



**1.3. 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.  $LKD(a, m) = d$ . No iepriekšējās teorēmas seko, ka  $\langle a \rangle \leq \langle d \rangle$ .

Saskaņā ar lineārās kombinācijas īpašību

$$d = ua + vm \implies d \equiv ua \pmod{m} \implies$$

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

2. Apzīmēsim  $LKD(a, m)$  ar  $d$ ,  $LKD(a', m)$  ar  $d'$ . Saskaņā ar iepriekšējo apgalvojumu

$$(d = d') \implies \langle a \rangle = \langle d \rangle = \langle d' \rangle = \langle a' \rangle.$$

$$\langle a \rangle = \langle a' \rangle \implies \langle d \rangle = \langle d' \rangle \iff \begin{cases} \langle d \rangle \leq \langle d' \rangle \\ \langle d' \rangle \leq \langle d \rangle \end{cases} \implies \begin{cases} \exists n' \in \mathbb{Z} : d \equiv n'd' \pmod{m} \\ \exists n \in \mathbb{Z} : d' \equiv nd \pmod{m} \end{cases} \implies \begin{cases} d = n'd' + mq' \\ d' = nd + mq \end{cases} \implies$$

$$\begin{cases} d \equiv 0 \pmod{d'} \\ d' \equiv 0 \pmod{d} \end{cases} \implies \begin{cases} d' \mid d \\ d \mid d' \end{cases} \implies d = d'.$$

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

$$LKD(d, m) = d \implies \frac{m}{LKD(d, m)} \cdot d = m \equiv 0 \pmod{m} \implies |\langle a \rangle| = |\langle d \rangle| \leq n.$$

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

$$\exists u, v \in \{1, \dots, n\} : \begin{cases} u > v \\ ua \equiv va \pmod{m} \end{cases} \implies \underbrace{(u - v)}_{=w} d \equiv 0 \pmod{m}.$$

$$\begin{cases} 0 < w < n \\ wd \equiv 0 \pmod{m} \end{cases} \implies \begin{cases} 0 < wd < m \\ wd = mq \end{cases} \implies \text{- pretruna. } \blacksquare$$

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

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

### 1.2.3. Atlikumu aditīvās grupas apakšgrupu klasifikācija

1.4. teorēma.  $A \in \{\mathbb{Z}, \mathbb{Z}/m\}$ ,  $m \in \mathbb{Z}$ .

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

#### PIERĀDĪJUMS

$A = \mathbb{Z}$  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:  $\langle g \rangle \subsetneq H \implies \exists x \in H : ng \neq x, \forall n \in \mathbb{Z}$ .

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.

$$A = \mathbb{Z}/m$$

Izmantosim kanonisko PAK  $\{0, 1, \dots, m-1\}$ .

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:  $\exists x \in H : nb \not\equiv x \pmod{m}, \forall n \in \mathbb{Z}$ .

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.

$d = b \implies b \mid x \implies \exists n \in \mathbb{Z} : x = nb \implies x \equiv nb \pmod{m}$  -  
pretruna. ■

## 2. 5.mājasdarbs

### 2.1. Obligātie uzdevumi

5.1 Atrast visas apakšgrupas, to ģeneratorus un elementu skaitu.

(a)  $\mathbb{Z}/28$ ;

(b)  $\mathbb{Z}/72$ .

5.2 Atrisināt vienādojumus

(a)  $2x \equiv 1 \pmod{21}$ ;

(b)  $15x \equiv 18 \pmod{24}$ ;

(c)  $27x \equiv 28 \pmod{36}$ .

(Norādījums: izmantojiet zināmos faktus par  $\mathbb{Z}/m$  apakšgrupām)

5.3 Atrast  $\sum_{n=1}^{m-1} n = 1 + 2 + \dots + (m-1) \pmod{m}$ .

## 2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.4 Doti  $m, a \in \mathbb{Z}/m$ . Ar ko ir vienāda  $a$  kārta? (Par komutatīvas grupas  $G$  elementa  $g$  kārtu sauc mazāko  $n \in \mathbb{N} \cup \{0\} : n \cdot a = 0$ ).