4. CIKLINĖS GRUPĖS

5.10 apibrėžimas. *Tegu* $(A, \cdot)$ *yra grupė, o* $a \in A$ *ir* $\mathrm{ord}_A a = n < \infty$. *Tada* $\big(\{a^1, a^2, \ldots, a^{n-1}, a^n = e\}, \cdot\big)$ *yra* A *pogrupis. Jis vadinamas baigtiniu cikliniu generuojamu elemento* a *pogrupiu ir žymimas* $\langle a \rangle$.

Jeigu $\mathrm{ord}_A a = \infty$, *tai* $\big(\{\ldots, a^{-2}, a^{-1}, e_A, a, a^2, \ldots, \}, *\big)$ *yra begalinis* A *pogrupis, vadinamas begaliniu cikliniu pogrupiu* $\langle a \rangle$. *Elementas* a *abiem atvejais vadinamas generuojančiuoju grupės* A *elementu.*

Ciklinių grupių pavyzdžiai:

a) sveikųjų skaičių grupė $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ – begalinė ciklinė grupė;

b) grupė $(Z_n, +) = \langle {}_nK_1, + \rangle$ – baigtinė ciklinė grupė.

Pastebėsime, kad elemento $a \in A$ eilė yra lygi ciklinio pogrupio $\langle a \rangle$ eilei: $|\langle a \rangle| = \mathrm{ord}\ a$, todėl, norint rasti grupės elemento eilę, tenka nagrinėti atitinkamą ciklinį pogrupį. Tam reikia mokėti pakankamai efektyviai skaičiuoti grupės $(A, \cdot)$ elemento a laipsnį a^n (ypač, kai n didelis). Paprasčiausias būdas tai padaryti – atlikti $n - 1$ grupės veiksmą.

5.12 pastaba. Reiktų mokėti skaičiuoti grupės elemento atvirkštinį elementą, t.y. rasti elemento eilę. Panagrinėsime šį klausimą.

5.13 apibrėžimas. *Jeigu* $(A, \cdot)$ *yra grupė, o* B, C – *netušti* A *poaibiai, tai* $B \cdot C = \{a \in A \mid a = b \cdot c,\ b \in B, c \in C\}$.

Dabar apibendrinsime sveikųjų skaičių grupėje $\mathbb{Z}$ apibrėžtą sąryšį $\equiv \pmod n$ bet kuriai grupei.

5.14 teiginys. *Tegu* $(B, \cdot)$ *yra grupės* $(A, \cdot)$ *pogrupis. Sąryšis*

$$\sim = \big\{(a_1, a_2) \mid a_1 \cdot B = a_2 \cdot B\big\}, \quad a_1 \sim a_2$$

yra ekvivalentumo sąryšis.

Įrodyti paliekame skaitytojui.

Šį ekvivalentumo sąryšį atitinkančio skaidinio $_\sim\pi$ aibės vadinamos *grupės A kairiaisiais sluoksniais pogrupio B atžvilgiu.*

Jeigu A yra baigtinė grupė, tai skaidinys $_\sim\pi$ yra

$$A = B \cup (a_1 \cdot B) \cup (a_2 \cdot B) \cup \ldots \cup (a_m \cdot B), \quad a_1, a_2, \ldots, a_m \in A.$$

Panašiai apibrėžiami ir *grupės A dešinieji sluoksniai pogrupio B atžvilgiu* ir skaidinys $\pi_\sim$.

Akivaizdu, jeigu A yra komutatyvioji grupė, tai kairysis sluoksnis $a \cdot B$ sutampa su dešiniuoju sluoksniu $B \cdot a$: $a \cdot B = B \cdot a$.

5.15 pavyzdys. $A = S_3$, $B = \{id, (12)\}$.

Kairieji sluoksniai	Dešinieji sluoksniai
B	B
$\{(13), (132)\}$	$\{(13), (123)\}$
$\{(23), (123)\}$	$\{(23), (132)\}$

$$_\sim\pi \neq \pi_\sim.$$

5.16 pavyzdys. $A = Z_8$, $B = \{\overline{0}, \overline{4}\}$. Skirtingi kairieji (dešinieji) grupės Z_8 sluoksniai B atžvilgiu yra

$$\begin{aligned}
\overline{0} + \mathrm{B} &= \{\overline{0}, \overline{4}\} = \mathrm{B}_0,\\
\overline{1} + \mathrm{B} &= \{\overline{1}, \overline{5}\} = \mathrm{B}_1,\\
\overline{2} + \mathrm{B} &= \{\overline{2}, \overline{6}\} = \mathrm{B}_2,\\
\overline{3} + \mathrm{B} &= \{\overline{3}, \overline{7}\} = \mathrm{B}_3,
\end{aligned}$$

$$A = B_0 \cup B_1 \cup B_2 \cup B_3.$$

5.17 pastaba. Jeigu grupė $(A, *)$ yra baigtinė, tai visi kairieji (dešinieji) sluoksniai kurio nors pogrupio B atžvilgiu yra tos pačios galios, nes dėl prastinimo taisyklės grupėje

$$\begin{aligned}
a * b_1 = a * b_2 &\iff b_1 = b_2,\\
c_1 * a = c_2 * a &\iff c_1 = c_2.
\end{aligned}$$

5.18 apibrėžimas. *Grupės A pogrupio B indeksu vadinamas skaidinio $\pi_\sim$ (arba $_\sim\pi$) aibių skaičius ir žymimas $|A : B|$.*

5.19 Lagranžo[1] teorema. *Jeigu A yra baigtinė grupė, o B – A pogrupis, tai*

$$|A| = |B| \cdot |A : B|.$$

Dėl 5.17 pastabos teoremos įrodymas akivaizdus.

5.20 pastaba. *Jeigu $a \in A$, tai $\mathrm{ord}_A a = |\langle a \rangle|$ dalo grupės eilę $|A|$.*

Tačiau ne kiekvienam $|A|$ dalikliui d galima rasti tokį $a \in A$, kad $\mathrm{ord}_A a = d$.

5.21 pavyzdys. Tegu $A = S_3$ yra 3-osios eilės keitinių grupė. Kadangi $|S_3| = 3! = 6$, tai šioje grupėje nerasime nei 4-osios, nei 5-osios eilės elementų. Kita vertus, grupėje nėra taip pat ir 6-osios eilės elementų, nes

$$\begin{aligned}
&\mathrm{ord}\,(id) = 1,\\
&\mathrm{ord}\,(12) = \mathrm{ord}\,(13) = \mathrm{ord}\,(23) = 2,\\
&\mathrm{ord}\,(123) = \mathrm{ord}\,(132) = 3.
\end{aligned}$$

Kartu gavome, kad S_3 nėra ciklinė grupė.

Naudodamiesi paskutine pastaba pateiksime baigtinės grupės elemento eilės radimo algoritmą.

5.22 algoritmas. *Žinoma: eilės n grupė $(A, \cdot)$; elementas $a \in A$; 1 – neutralusis grupės A elementas.*

Rezultatas: elemento a eilė $N = \mathrm{ord}_{\mathrm{A}}\mathrm{a}$.

1. Randame skaičiaus n kanoninį skaidinį $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$; priskiriame $N := n$; $i := 0$.
2. $i := i + 1$. Jeigu $i > k$, tai N išvedame; skaičiavimų pabaiga.
3. $N := N\big/p_i^{m_i}$, $G := a^N$.
4. Jeigu $G = 1$, tai vykdome 2. Kol $G \neq 1$ priskiriame $G := G^{m_i}$; $N := N \cdot p_i$. Vykdome 2.

$\triangle$

Baigtinių ciklinių grupių pogrupių ir elementų eiles apibrėžia kitas teiginys.

5.43 teiginys. *Tegu $\langle a \rangle = \{a, a^2, \dots, a^n = e\}$ yra ciklinė grupė, o φ – Oilerio funkcija.*

[1] J. L. Lagrange, 1736–1813, – prancūzų matematikas ir mechanikas.

1. Visi grupės $\langle a\rangle$ pogrupiai yra cikliniai.

2. $\mathrm{ord}\,(\mathrm{a}^{\mathrm{k}}) = \frac{\mathrm{n}}{\mathrm{DBD}\,(\mathrm{k,n})}$.

3. Jeigu natūralusis skaičius k yra n daliklis, tai

a) grupėje $\langle a\rangle$ egzistuoja pogrupis, kurio eilė yra lygi k;

b) grupėje $\langle a\rangle$ egzistuoja pogrupis, kurio indeksas grupėje $\langle a\rangle$ yra lygus k.

4. a) Jeigu natūralusis skaičius k yra n daliklis, tai grupėje $\langle a\rangle$ yra $\varphi(k)$ k-osios eilės elementų;

b) grupėje $\langle a\rangle$ yra $\varphi(n)$ generuojančių šią grupę elementų: tai aibė $\{a^r \mid 1 \leqslant r \leqslant n,\ \mathrm{DBD}(r,n)=1\}$.

Įrodymas. 1. Tegu B yra ciklinės grupės $\langle a\rangle$ pogrupis ir k – toks mažiausias natūralusis skaičius, kad $a^k \in B$. Parodysime, kad $\langle a^k\rangle = B$. Jeigu $a^d \in B$ ir $d = qk + r$, $0 \leqslant r < k$, tai $a^d = (a^k)^q \cdot a^r$. Taigi $a^r = a^d \cdot (a^k)^{-q} \in B$ ir todėl $r = 0$, nes mažiausias laipsnio rodiklis, kuriuo pakėlus a gausime grupės B elementą, yra k, o $r < k$. Tada $d = kq$, $a^d \in \langle a^k\rangle$ ir todėl $B = \langle a^k\rangle$ – ciklinė grupė.

2. Elemento $a^k \in \langle a\rangle$ eilė yra toks mažiausias natūralusis skaičius $s = \mathrm{ord}\,a^k$, kad $(a^k)^s = a^{k\cdot s} = e$. Tada n yra $k\cdot s$ daliklis, $n \mid k\cdot s$ ir $\frac{n}{\mathrm{DBD}\,(k,n)}$ yra $\frac{k\cdot s}{\mathrm{DBD}\,(k,n)}$ daliklis. Bet žinome, kad

$$\mathrm{DBD}\left(\frac{k}{\mathrm{DBD}\,(k,n)}, \frac{n}{\mathrm{DBD}\,(k,n)}\right) = 1,$$

ir todėl $\frac{n}{\mathrm{DBD}\,(k,n)} \mid s$.

Mažiausias toks s, tenkinantis šią sąlygą, ir yra $\frac{n}{\mathrm{DBD}\,(k,n)}$.

3. Tegu $n = k\cdot l$.

a) Tada $\left|\langle a^l\rangle\right| = \frac{n}{\mathrm{DBD}\,(n,l)} = \frac{n}{l} = k$.

b) Grupės $\langle a^k\rangle$ indeksas grupėje $\langle a\rangle$ yra

$$\Big(\langle a\rangle : \langle a^k\rangle\Big) = \frac{n}{|\langle a^k\rangle|} = \frac{n}{\frac{n}{\mathrm{DBD}\,(n,k)}} = \frac{n}{\frac{n}{k}} = k.$$

4. Elemento a^l eilė yra lygi k tik tada, kai $k = \frac{n}{\mathrm{DBD}\,(n,l)}$.

Pažymėkime $\mathrm{DBD}\,(n,l) = d$, tada $n = k\cdot d$.

Elemento a^r, $1 \leqslant r \leqslant n$, eilė yra lygi k tada ir tik tada, kai $\mathrm{DBD}\,(n,r) = \mathrm{DBD}\,(n,l) = d$. Taigi skaičius r turi:

pirma, dalytis iš d, $r = d\cdot s$, $1 \leqslant s \leqslant k$;

antra, $\mathrm{DBD}\left(\frac{n}{d}, \frac{r}{d}\right) = (k,s) = 1$.

Gavome, kad elemento a^r eilė yra lygi k tada ir tik tada, kai $r = d \cdot s$, $1 \leqslant s \leqslant k$, DBD $(s,k) = 1$. Tokių natūraliųjų r, $1 \leqslant r \leqslant n$, tenkinančių šią sąlygą, ir yra $\varphi(k)$.

$\triangle$

5.44 išvada. *Jeigu grupės A eilė yra pirminis skaičius p, tai visi grupės A elementai $a \neq e_A$ yra generuojantys šią grupę, o pati grupė A – ciklinė.*

Įrodyti paliekame skaitytojui (žr. 5.43 teiginio 4b) dalį).

5.45 pavyzdžiai. 1. Visi grupės $(\mathbb{Z}_n, +)$ pogrupiai yra cikliniai ir lygūs

$$\{0, (\overline{m})d, (\overline{m})2d, \ldots, (\overline{m})(\frac{n}{d} - 1)\};$$

čia d yra n daliklis, o $\overline{m}$ – bet kuris generuojantis grupę $\mathbb{Z}_n$ elementas, t.y. DBD $(m,n) = 1$.

2. Visi grupės $(\mathbb{Z}, +)$ pogrupiai yra cikliniai ir lygūs

$$\{\ldots, -2r, -r, 0, r, 2r, \ldots\};$$

čia r – bet kuris natūralusis skaičius.