10 paskaita. *Simetrijų grupės. Ciklinės grupės. Cayley teorema.*

Apibrėžimas. Geometrinės figūros F atvaizdis į ją pačią, nekeičiantis atstumų tarp figūros taškų, vadinamas **figūros F simetrija**.

Tegu g_1 ir g_2 yra figūros F simetrijos, t.y. funkcijos $g_1, g_2 : F \to F$, nekeičiančios atstumų tarp figūros taškų:
distance$(A, B) =$ distance$(g_1(A), g_1(B)) =$ distance$(g_2(A), g_2(B))$,
čia $A, B \in F$.
Simetrijų g_1 ir g_2 kompozicija $g_1 \circ g_2 : (g_1 \circ g_2)(A) = g_1(g_2(A))$ yra simetrija. Simetrijų g_1 ir g_2 kompoziciją $g_1 \circ g_2$ vadinsime **simetrijų g_1 ir g_2 sandauga** ir žymėsime $g_2 \cdot g_1$ arba tiesiog $g_2 g_1$, t.y. $g_2 g_1 = g_1 \circ g_2$.

Trikampio posūkių grupė.
Tegu turime lygiakraštį trikampį ACB (viršūnės rašomos pagal laikrodžio rodyklę)ir $O-$ šio trikampio centras. Trikampio ACB posūkį 120° kampu prieš laikrodžio rodyklę centro O atžvilgiu pažymėkime raide a. Aišku, kad a yra trikampio ACB simetrija. a galima užrašyti ir taip:

$$a = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix},$$

čia viršutinėje eilutėje išvardintos trikampio viršūnės, o apatinėje nurodyta kur kokia viršūnė pereina atlikus posūkį a.
Panašiai apibrėžiamas trikampio ACB posūkis 240° kampu prieš laikrodžio rodyklę centro O atžvilgiu: pažymėkime raide b. Tada

$$b = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}.$$

Tegu $e-$ trikampio ACB posūkis 0° kampu prieš laikrodžio rodyklę centro O atžvilgiu:

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}.$$

Teorema. Lygiakraščio trikampio(arba tiesiog trikampio) posūkiai e, a, b simetrijų sandaugos atžvilgiu yra grupė $D = (\{e, a, b\}, \cdot)$.

Įrodyti paliekame skaitytojui.

Pateiksime trikampio posūkių grupės veiksmų lentelę:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

,

čia veiksmų lentelėje esanti sandauga $g_1 \cdot g_2$ reiškia, kad g_1 imamas iš lentelės eilutės, o g_2 - iš lentelės stulpelio.

Trikampio simetrijų grupė.

Be minėtų posūkių e, a, b yra dar trys lygiakraščio trikampio ACB simetrijos pusiaukraštinių AL, BM, CN atžvilgiu:

$$c = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, d = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, f = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.$$

Teorema. Lygiakraščio trikampio(arba tiesiog trikampio) simetrijos e, a, b, c, d, f simetrijų sandaugos atžvilgiu yra grupė $S = (\{e, a, b, c, d, f\}, \cdot)$.

Įrodyti paliekame skaitytojui.

Pateiksime trikampio posūkių grupės veiksmų lentelę:

$\cdot$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

.

Panašiai galima apibrėžti *stačiakampio posūkių, stačiakampio simetrijų, kvadrato posūkių, kvadrato simetrijų, rombo simetrijų, tasyklingojo n-kampio posūkių grupes.*

Bet kokios algebrinės struktūros tyrimas prasideda nuo postruktūrių nagrinėjimo. Nenusižengsime ir mes šiai tradicijai ir pradėsime apibrėžimu.

Apibrėžimas. Tegu G yra grupė. Poaibis $H \subseteq G$ vadinamas grupės G pogrupiu(arba tiesiog pogrupiu), jei

1) su visais $h \in H$ teisinga $h^{-1} \in H$

2) su visais $h_1, h_2 \in H$ teisinga $h_1 h_2 \in H$.

Iš apibrėžimo turime, kad grupės G pogrupis H yra pats grupė. Mes rašysime $H \leq G$ arba $H < G$. Kiekviena grupė G turi du trivialius pogrupius: $\{e\} \leq G$ ir $G \leq G$. Galėtume pateikti ir daugiau pogrupių pavyzdžių. Tačiau apsiribokime tomis grupėmis, kurias paminėjome šiame skyriuje:

- $D < S$.
- $\{e, c\} < S$,- 2 eilės pogrupis.
- $\{e, d\} < S$,- 2 eilės pogrupis.
- $\{e, f\} < S$, ,- 2 eilės pogrupis.

Pastebėkime, kad tai ir yra visi netrivialūs trikampio simetrijų grupės pogrupiai. Beto jie visi pasižymi tuo, kad jie yra vieno kurio nors elemento laipsniai, pvz.: $D = \{e, a, a^2\}$, nes $a^2 = b$, o $e = a^0$. Apibendrinsime šį pastebėjimą.

Teiginys. Tegu $g \in G$. Tada

$$\langle g \rangle = \left\{ g^k | k = 0, \pm 1, \pm 2, ... \right\}$$

yra grupės G pogrupis, generuojamas elementu g. Šią grupę vadina **cikline grupe** generuojama g.

Įrodymas paliekamas skaitytojui.

Mes jau žinome nemažai ciklinių grupių pavyzdžių. Paminėsime svarbiausius:

- sveikųjų skaičių grupė $(\mathbf{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ yra begalinė ciklinė grupė
- grupė $(\mathbf{Z}_n, +) = \langle \bar{1} \rangle$ yra baigtinė ciklinė grupė.

Ciklinės grupės įgalina apibrėžti grupės elemento eilę: grupės G elemento $g \in G$ eile vadina ciklinės grupės, generuotos elementu g, $\langle g \rangle \leq G$, eilę ir žymi $\mathrm{ord}(g) = |\langle g \rangle|$.

Pastebėsime, kad mūsų paminėti ciklinių grupių pavyzdžiai yra svarbiausi, nes visos ciklinės grupės yra izomorfiškos arba sveikųjų skaičių grupei $\mathbf{Z}$, arba vienai iš grupių $\mathbf{Z}_n, n \in \mathbf{N}$, priklausomai nuo to, ar kalbama apie begalinę, ar apie baigtinę ciklinę grupę.

Teorema apie ciklines grupes. 1. Baigtinė ciklinė grupė $\langle g \rangle_n$, kurioje yra n elementų, yra izomorfinė grupei $\mathbf{Z}_n$:

$$\langle g \rangle_n = (\{g, g^2, ..., g^{n-1}, g^n = e\}, +) \approx (\mathbf{Z}_n, +).$$

2. Begalinė ciklinė grupė $\langle g \rangle$ yra izomorfinė grupei $\mathbf{Z}$.

Įrodymas. 1. Funkcija $\varphi_n : \mathbf{Z}_n \to \langle g \rangle_n$, apibrėžta formule $\varphi_n\left(\bar{k}\right) = g^k$ yra izomorfizmas:

a) φ_n yra abipus vienareikšmė funkcija, nes, jei $\varphi_n\left(\bar{k}\right) = \varphi_n\left(\bar{l}\right)$, tai $g^k = g^l$, $0 \leq k \leq l \leq n-1$, ir $g^{l-k} = e$ ir todėl $l = k$ ir $\bar{l} = \bar{k}$.

b) Turime

$$\varphi_n\left(\bar{k} + \bar{l}\right) = \left[\begin{array}{c} \varphi_n\left(\overline{k+l}\right), \text{ kai } k+l < n \\ \varphi_n\left(\overline{k+l-n}\right), \text{ kai } k+l \geq n \end{array} \right.$$
$$= \left[\begin{array}{c} g^{k+l} \\ g^{k+l-n} = g^{k+l-n} g^n = g^{k+l} \end{array} \right.$$
$$= g^k g^l = \varphi_n\left(\bar{k}\right) \varphi_n\left(\bar{l}\right).$$

2. Funkcija $\varphi_0 : \mathbf{Z} \to \langle g \rangle$, apibrėžta formule $\varphi_0(k) = g^k$ yra izomorfizmas:

a) φ_0 yra abipus vienareikšmė funkcija, nes, jei $\varphi_0(k) = \varphi_0(l)$, tada ir tik tada, jei $g^k = g^l$, ir $g^{l-k} = e$ ir todėl $l - k = 0$ ir $k = l$.

b) Turime

$$\varphi_0(k+l) = g^{k+l} = g^k \, g^l = \varphi_0(k) \, \varphi_0(l).$$

Įrodyta.

Dabar parodysime, kad į bet kurią baigtinę grupę galima žiūrėti kaip į keitinių grupės S_n pogrupį.

Teorema(A.Cayley). *Tegu* $(G,\cdot)$ *yra baigtinė grupė, turinti* n *elementų. Tada egzistuoja funkcija*

$$f : G \to S(G) = S_n,$$

tenkinanti savybes

$$f(g_1) = f(g_2) \Longleftrightarrow g_1 = g_2, \text{ (injektyvumas)}$$
$$f(g \cdot h) = f(g) \circ f(h). \text{ (homomorfizmas)}$$

Įrodymas.$\forall a \in G$ konstruojame keitinį $L_a : G \to G$, $L_a(g) = g \cdot a$. Taigi

$$L_a = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 a & g_2 a & \cdots & g_n a \end{pmatrix}$$

ir $L_a \in S_n$.

Turime aibių lygybę

$$\{g_1, g_2, ..., g_n\} = \{g_1 \cdot a, g_2 \cdot a, ..., g_n \cdot a\} = G.$$

Turime

1) $L_a \in S_n$,

2) $L_a^{-1} = L_{a^{-1}}$,

3) $L_{a\cdot b}(g) = g \cdot (a \cdot b) = (g \cdot a) \cdot b = L_b(L_a(g)) = (L_a \circ L_b)(g)$, taigi, $L_{a\cdot b} = L_a \circ L_b$.

Gavome, kad keitiniai $L_{g_1}, L_{g_2}, ..., L_{g_n}$ sudaro grupę $H \subset S(G) = S_n$.

Funkcija $f : G \to H \subset S_n$ apibrėžta formule $f(g) = L_g$.

Įrodyta.

Pavyzdys1. Rombo simetrijų grupės įdėjimas į simetrinę grupę.

Tegu $G = \{e, a, b, c\}$ - rombo simetrijų grupė. Čia e ir a posūkiai atitinkamai $0°$ ir $180°$ kampu, o b ir c simetrijos įstrižainių atžvilgiu. Tada veiksmų lentelė šioje grupėje

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

ir $L_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = id$, $L_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} = (ea)(bc)$, $L_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (eb)(ac)$, $L_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = (ec)(ab)$.

Pavyzdys 2. Ciklinės grupės (pvz. n-ojo laipsnio šaknų iš 1 multiplikacinės grupės) įdėjimas į simetrinę grupę.

Tegu ε - primityvioji n-ojo laipsnio šaknis iš vieneto. Tada visos n-ojo laipsnio šaknis iš vieneto yra primityviosios šaknies ε laipsniai : $\varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}, \varepsilon^n = 1$ ir

$$L_\varepsilon = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \dots & \varepsilon^{n-1} & \varepsilon^n \\ \varepsilon^2 & \varepsilon^3 & \varepsilon^4 & \dots & \varepsilon^n & \varepsilon \end{pmatrix}$$
$$L_{\varepsilon^2} = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \dots & \varepsilon^{n-1} & \varepsilon^n \\ \varepsilon^3 & \varepsilon^4 & \varepsilon^5 & \dots & \varepsilon^{n+1} & \varepsilon^{n+2} \end{pmatrix}$$

ir t.t. Pavyzdžiui, kai $n = 6$ turime reiškimą keitiniais:

$$L_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (123456)$$
$$L_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (135)(246)$$
$$L_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (14)(25)(36)$$
$$L_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (153)(264)$$
$$L_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (165432)$$
$$L_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = id.$$