5 paskaita. *Keitiniai.*

Tegu $V = \{v_1, v_2, ..., v_n\}$ - baigtinė, visiškai sutvarkyta aibė: $v_1 < v_2 < ... < v_n$ ir π - šios aibės kėlinys $(w_1, w_2, ..., w_n)$. Tuo pačiu žymeniu π žymėsime ir funkciją, kurią vadinsime **keitiniu**

$\pi : V \to V, \pi(v_1) = w_1, \pi(v_2) = w_2, ..., \pi(v_n) = w_n.$

Žinome, kad keitiniai yra abipus vienareikšmės funkcijos ir jų yra $n!$.

Pateiksime keitinių reiškimo būdus.

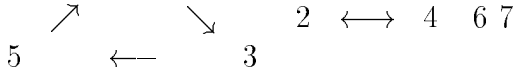
1. Keitinio, kaip funkcijos apibrėžtos baigtinėje aibėje, reiškimas lentele:

$$\begin{pmatrix} v_1 & v_2 & ... & v_n \\ w_1 & w_2 & ... & w_n \end{pmatrix}.$$

2. Reiškimas *grafu*. Grafas sudarytas iš viršūnių v_i ir orientuotų briaunų $\langle v_i, \pi(v_i)\rangle$, $1 \le i \le n$.

Pavyzdys. $V = \{1, 2, 3, 4, 5, 6, 7\}$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 1 & 6 & 7 \end{pmatrix}$$



3. Reiškimas nepriklausomais ciklais.

Tegu $v_i \in V$. Tada turime aibės V elementų seką

$v_i, \pi(v_i), \pi^2(v_i) = \pi(\pi(v_i)), ..., \pi^{k-1}(v_i), \pi^k(v_i) = v_i.$.

Gauname k ilgio ciklą $\left(v_i, \pi(v_i), \pi^2(v_i) = \pi(\pi(v_i)), ..., \pi^{k-1}(v_i)\right)$.

Jeigu $k = n$, tai visi aibės V elementai yra šiame cikle. Kitu atveju, egzistuoja $v_j \notin \left(v_i, \pi(v_i), \pi^2(v_i) = \pi(\pi(v_i)), ..., \pi^{k-1}(v_i)\right)$, kuriam konstruojame savo ciklą:

$\left(v_j, \pi(v_j), \pi^2(v_j) = \pi(\pi(v_j)), ..., \pi^{l-1}(v_j)\right)$.

Cikluose yra skirtingi elementai.

Jeigu $\pi^r(v_j) = \pi^s(v_i)$, tai $\pi^{r+1}(v_j) = \pi^{s+1}(v_i), \ldots, v_j = \pi^l(v_j) = \pi^{s+(l-r)}(v_i)$, tai elementas v_j priklausytų pirmąjam ciklui, o tai prieštarautų sąlygai.

Taigi, visi aibės V elementai suskyla į nepriklausomus ciklus keitinio π atžvilgiu.

Parodėme, kad bet kurį keitinį galima užrašyti kaip poromis nepriklausomų ciklų "sandauga". Šis skaidinys yra vienintėlis ciklų išsidėstymo tikslumu.

Paaiškinsime "sandaugos" sąvoką.

Apibrėžimas. *Tegu π , ρ - keitiniai aibėje V. Keitinių sandauga $\sigma = \pi \circ \rho$ vadinsime keitinį, apibrėžtą lygybe*

$$\sigma(v_i) = \rho(\pi(v_i)) \ , \ \forall v_i \in V.$$

Pastebėsime, kad taip apibrėžta sandauga yra funkcijų kompozicija. Ji nėra komutatyvi, t.y. ne visada $\pi \circ \rho = \rho \circ \pi$.

Pavyzdys. Kai $\pi = \begin{pmatrix} v_1 & v_2 & v_3 \\ v_3 & v_2 & v_1 \end{pmatrix}$, o $\rho = \begin{pmatrix} v_1 & v_2 & v_3 \\ v_3 & v_1 & v_2 \end{pmatrix}$, tai

$\pi \circ \rho = \begin{pmatrix} v_1 & v_2 & v_3 \\ v_2 & v_1 & v_3 \end{pmatrix} \neq \begin{pmatrix} v_1 & v_2 & v_3 \\ v_1 & v_3 & v_2 \end{pmatrix} = \rho \circ \pi$.

Tačiau, keitinio π kanoniniame skaidinyje esantys nepriklausomi ciklai komutuoja poromis.

Teiginys. *Tegu $S(V)$ - visų keitinių aibė aibėje V. Tada $(S(V), \circ)$ - **grupė**.*

Įrodymas. 1) Operacijos korektiškumas: jei $\pi, \rho \in S(V)$, tai $\pi \circ \rho \in S(V)$.

2) Asosiatyvumas: $(\pi \circ \rho) \circ \tau = \pi \circ (\rho \circ \tau)$.

$((\pi \circ \rho) \circ \tau)(v_i) = \tau((\pi \circ \rho)(v_i)) = \tau(\rho(\pi(v_i))) = (\rho \circ \tau)(\pi(v_i))$

$= (\pi \circ (\rho \circ \tau))(v_i)$.

3) Neutralaus elemento egzistavimas : $id(v_i) = v_i$, $\forall v_i \in V$, todėl

$id \circ \pi = \pi \circ id = \pi$, $\pi \in S(V)$.

4) Atvirkštinio elemento egzistavimas: jei $\pi(v_i) = w_i$, tai $\pi^{-1}(w_i) = v_i$.

Įrodyta.

Apibrėžimas. *Ciklas* (v_i, v_j) *vadinamas* ***transpozicija.***

Teiginys. *Kai* $|V| \geq 2$ *,tai bet kurį keitinį galima užrašyti transpozicijų sandauga.*

Įrodymas. Šį teiginį pakanka įrodyti k ilgio ciklui. Kai $k = 1, (v) = (u, v) \circ (u, v)$.

Kai $k = 2, (u, v) = (u, v)$, o

$k \geq 3, (v_1, v_2, ..., v_k) = (v_1, v_2) \circ (v_1, v_3) \circ \cdots \circ (v_1, v_k)$. Sandaugoje yra $k - 1$ transpozicija.

Įrodyta.

Pastebėsime, kad keitinio reiškimas transpozicijų sandauga yra nevienareikšmiškas.

Pavyzdžiui,

$$(v, u) = (v, u) \circ (v, u) \circ (v, u) .$$

Pastovus dydis šiame reiškime visdėlto yra: tai transpozicijų skaičiaus liekana dalijant jį iš 2.

Apibrėžimas. *Tegu* $\pi \in S(V)$. *Pora* (v_i, v_j), *kai* $v_i < v_j$, *bet* $\pi(v_i) > \pi(v_j)$ *vadinama keitinio* π ***inversija.***

π *vadinamas lyginiu keitiniu, jeigu* π *inversijų skaičius yra lyginis.*

π *vadinamas nelyginiu keitiniu, jeigu* π *inversijų skaičius yra nelyginis.*

Keitinio π inversijų skaičių žymėsime $|\pi|$, o ženklą $\text{sign}\pi = (-1)^{|\pi|}$.

Pastebėsime, kad id yra lyginis keitinys. Jei $\pi-$ lyginis, tai $\text{sign}\pi = 1$, jei $\pi-$ nelyginis, tai $\text{sign}\pi = -1$.

Teiginys. $|\pi \circ (a, b)| \equiv |\pi| + 1 \pmod 2$.

Įrodymas.

$$\pi = \begin{pmatrix} v_1 & ... & v_k & v_{k+1} & v_{k+2} & ... & v_{k+l+1} & v_{k+l+2} & v_{k+l+3} & ... & v_n \\ a_1 & ... & a_k & a & b_1 & ... & b_l & b & c_1 & ... & c_m \end{pmatrix},$$

$$\pi \circ (a,b) = \begin{pmatrix} v_1 & ... & v_k & v_{k+1} & v_{k+2} & ... & v_{k+l+1} & v_{k+l+2} & v_{k+l+3} & ... & v_n \\ a_1 & ... & a_k & b & b_1 & ... & b_l & a & c_1 & ... & c_m \end{pmatrix}.$$

Pažymėkime.

$p_a = |\{a_1, ..., a_k | a_i > a\}|$, $q_a = |\{a_1, ..., a_k | a_i > b\}|$

$p_b = |\{b_1, ..., b_l | b_i > a\}|$, $q_b = |\{b_1, ..., b_l | b_i > b\}|$

$p_c = |\{c_1, ..., c_m | c_i > a\}|$, $q_c = |\{c_1, ..., c_m | c_i > b\}|$.

Tegu r - keitinio

$$\begin{pmatrix} v_1 & ... & v_k & v_{k+2} & ... & v_{k+l+1} & v_{k+l+3} & ... & v_n \\ a_1 & ... & a_k & b_1 & ... & b_l & c_1 & ... & c_m \end{pmatrix}$$

inversijų skaičius.

Tada , kai $a < b$ turime

$|\pi| = p_a + (l - p_b) + (m - p_c) + q_a + q_b + (m - q_c) + r,$

$|\pi \circ (a,b)| = p_a + p_b + (m - p_c) + q_a + (l - q_b) + (m - q_c) + 1 + r.$

Todėl $|\pi| - |\pi \circ (a,b)| = 2(q_b - p_b) + 1 \equiv 1 \pmod 2$.

Atvejis $a > b$ nagrinėjamas analogiškai.

Įrodyta.

Turime, kad $\text{sign}(id) = 1$ ir $\text{sign}((a,b)) = -1$.

Transpozicijų skaičius keitinyje π yra pastovus dydis $\bmod 2$.

Jeigu turime du keitinio π reiškimus transpozicijų sandauga ;

$$\pi = \sigma_1 \cdots \sigma_k = \tau_1 \cdots \tau_l \ ,$$

tai

$$\text{sign}\pi = \text{sign}(\sigma_1 \cdots \sigma_k) = \text{sign}(\tau_1 \cdots \tau_l)$$

ir

$$\text{sign}\pi = (-1)^k = (-1)^l \Longrightarrow (-1)^{k-l} = 1 \Longrightarrow k - l \equiv 0 \pmod 2 \Longrightarrow k \equiv l \pmod 2.)$$

Išvados.

1. Keitinys yra lyginis tada ir tik tada, kai jis yra lyginio skaičiaus transpozicijų sandauga.

2. Keitinys yra nelyginis tada ir tik tada, kai jis yra nelyginio skaičiaus transpozicijų sandauga.

3. k-ciklas yra lyginis tada ir tik tada, kai k yra nelyginis ir atvirkščiai.

4. (lyginis) $\circ$ (lyginis) = (lyginis) .
(nelyginis) $\circ$ (nelyginis) = (lyginis) .
(nelyginis) $\circ$ (lyginis) = (nelyginis) .

5. sign$(\pi \circ \rho)$ =sign$(\pi)\cdot$sign(ρ) .

Lyginių keitinų aibę žymėsime A_n ir vadina **alternuojančia grupe**.

Teiginys. Lyginių ir nelyginių keitinių yra po lygiai $\dfrac{n!}{2}$.

Įrodymas. Nagrinėjama alternuojanti grupė A_n. Apibrėžiama aibė

$$U_{(a,b)} = \{\pi \in S_n | \pi = \sigma \circ (a,b)\,, \sigma \in A_n\} \subseteq S_n - A_n.$$

Tegu $|A_n| = m_1$, $|S_n - A_n| = m_2$. Tada aibės $U_{(a,b)}$ visi elementai skirtingi:
$\sigma_1 \circ (a,b) = \sigma_2 \circ (a,b) \Longleftrightarrow \sigma_1 \circ (a,b) \circ (a,b) = \sigma_2 \circ (a,b) \circ (a,b) \Longleftrightarrow \sigma_1 = \sigma_2$.
Taigi, $\left|U_{(a,b)}\right| = |A_n| = m_1 \leq m_2$.
Analogiškai, tegu turime aibę

$$W_{(a,b)} = \{\pi \in S_n | \pi = \rho \circ (a,b)\,, \rho \in S_n - A_n\} \subseteq A_n.$$

Kaip ir aibės $U_{(a,b)}$ taip ir aibės $W_{(a,b)}$ visi elementai skirtingi.
Tada $\left|W_{(a,b)}\right| = |S_n - A_n| = m_2 \leq m_1$.
Taigi, $m_1 = m_2 = \dfrac{n!}{2}$.
Įrodyta.