KEITINIAI. SIMETRINĖ GRUPĖ $\mathbf{S}_n$.

Paskaitos konspektas

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

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

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 $\langle v_i, \pi(v_i) \rangle$, $1 \leq i \leq n$.

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

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

$$\begin{array}{ccccccccc} & & 1 & & & & & & \\ & \nearrow & & \searrow & & 2 & \longleftrightarrow & 4 & 6\ 7 \\ 5 & & \longleftarrow & & 3 & & & & \end{array}$$

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. Mes jau buvome susidūrę su ekvivalentumo sąryšį atitinkančiu aibės skaidiniu (sveikieji skaičiai kuriuo nors moduliu).

Keitinį π atitinka baigtinės aibės V skaidinys S_π.

$v_i \equiv v_j \,(\operatorname{mod} \pi) \Longleftrightarrow v_j = \pi^s\,(v_i)\ ,\ s \in N\ .$

Tai ekvivalentumo sąryšis :

1) $v_i \equiv v_i\,(\operatorname{mod}\pi)\,.$

2) $v_i \equiv v_j\,(\operatorname{mod}\pi) \Longleftrightarrow v_j \equiv v_i\,(\operatorname{mod}\pi)$

$v_j = \pi^s\,(v_i) \Longrightarrow \pi^{k-s}\,(v_j) = v_i.$

3) $v_i \equiv v_j\,(\operatorname{mod}\pi)\,, v_j \equiv v_k\,(\operatorname{mod}\pi) \Longrightarrow v_i \equiv v_k\,(\operatorname{mod}\pi)$

$v_j = \pi^s\,(v_i)\,, v_k = \pi^t\,(v_j) = \pi^t\,(\pi^s\,(v_i)) = \pi^{t+s}\,(v_i)\,.$

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.

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.

Indukcija pagal k . 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 nevienareikš- miškas. Pavyzdžiui,

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

Pastovus dydis šiame reiškime visdėlto yra: tai transpozicijų skaičius mod 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 $sgn\pi=(-1)^{|\pi|}$.

Pastebėsime, kad id yra lyginis keitinys. Jei $\pi-$ lyginis, tai $sgn\pi=1$, jei $\pi-$ nelyginis, tai $sgn\pi=-1$.

Pavyzdys.[..........] .

Teiginys. $|\pi\circ(a,b)|\equiv|\pi|+1\,(\mathrm{mod}\,2)$.

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 $|\pi|-|\pi\circ(a,b)|=2\,(q_b-p_b)+1\equiv 1\,(\mathrm{mod}\,2)$.

Atvejis $a>b$ nagrinėjamas analogiškai.

Įrodyta.

Turime, kad $sgn\,(id) = 1$ ir $sgn\,((a,b)) = -1$.

Transpozicijų skaičius keitinyje π yra pastovus dydis $\bmod 2$. Jeigu turime du keitinio π reiškimus transpozicijų snadauga ;

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

tai $sgn\pi = sgn\,(\sigma_1 \cdots \sigma_k) = sgn\,(\tau_1 \cdots \tau_l)$ ir $sgn\pi = (-1)^k = (-1)^l \Longrightarrow (-1)^{k-l} = 1 \Longrightarrow k - l \equiv 0 \,(\bmod 2) \Longrightarrow k \equiv l\,(\bmod 2.)$

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

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

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

4. $(\text{lyginis}) \circ (\text{lyginis}) = (\text{lyginis})$.

$(\text{nelyginis}) \circ (\text{nelyginis}) = (\text{lyginis})$.

$(\text{nelyginis}) \circ (\text{lyginis}) = (\text{nelyginis})$.

5. $sgn\,(\pi \circ \rho) = sgn\,(\pi) \cdot sgn\,(\rho)$.

Lyginių keitinų aibę žymėsime A_n .

Teiginys. *A_n yra grupė.*

Įrodymas. Akivaizdu. Šią grupę 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.

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 $L_a \in S_n$.

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

Pavyzdys2. 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

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

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

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

$$L_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (123456)$$

$$L_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (135)(246)$$

$$L_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (14)(25)(36)$$

$$L_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (153)(264)$$

$$L_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (165432)$$

$$L_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = id.$$