KŪNŲ TEORIJA
2000 metų rudens paskaitos

1. Kūnų plėtiniai

2. Galua grupės

3. Polinomų Galua grupės

4. Mažos eilės grupių klasifikacija

5. Fundamentalioji teorema

6. Separabilusis ir normalusis plėtinys

7. Klasikiniai brėžimo skriestuvu ir liniuote uždaviniai

8. Išspendžiamos grupės

Visos grupės, kurias mes nagrinėsime yra baigtinės. Kitoje paskaitoje mes matysime, kad polinomas yra išsprendžiamas tada ir tik tada, kada jo Galua grupė yra išsprendžiama. Tai ir yra pagrindinė šių grupių nagrinėjimo priežastis. Pradėsime apibrėžimu.

Apibrėžimas 8.1 *Grupė G vadinama **išsprendžiama**, jeigu egzistuoja šios grupės tokia pogrupių grandinė* $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n$, kai
(1) N_i *yra normalusis* N_{i-1} *pogrupis su visais* $i = 1, 2, ..., n$,
(2) N_{i-1}/N_i *yra ciklinės grupės su visais* $i = 1, 2, ..., n$,
(3) $N_n = \langle 1 \rangle$.

Šioje paskaitoje mes apsiribosime išsprendžiamų ir neišsprendžiamų grupių pavyzdžiais ir be įrodymų suformuluosime teiginius, aprašančius pakankamai dideles šių grupių klases.

Pavyzdys 8.2 *Keitinių grupės S_2* ir S_3 *yra išsprendžiamos.*

Keitinių grupė S_2 yra pati išsprendžiama, nes pati yra ciklinė.

Keitinių grupė S_3 turi tokią pogrupių grandinę $S_3 \rhd A_3 \rhd \langle \mathrm{id} \rangle$, čia A_3- lyginių keitinių grupė, turinti 3 elementus. A_3 yra normalusis S_3 pogrupis ir $S_3/A_3 \approx \mathbf{Z}_3$. Taigi, S_3 yra išsprendžiama grupė.

Pavyzdys 8.3 *Keitinių grupė S_4 yra išsprendžiama.*

Keitinių grupė S_4 turi tokią pogrupių grandinę $S_4 \rhd A_4 \rhd V \rhd \langle (13)(24) \rangle \rhd \langle \mathrm{id} \rangle$, čia A_4- lyginių keitinių grupė, turinti 12 elementų; $V-$ Kleino ketvirtinė grupė(Klein Viergruppe) : visi 2 -os eilės grupės A_4 elementai ir id : $V = \{\mathrm{id}, (12)(23), (13)(24), (14)(23)\} \approx \mathbf{Z}_2 \times \mathbf{Z}_2$. Tai, kad A_4 yra normalusis S_4 pogrupis, V yra normalusis A_4 pogrupis, $\langle (13)(24) \rangle$ yra normalusis V pogrupis paliekame įrodyti skaitytojui. Iš Lagranžo teoremos turime, kad $|S_4/A_4| = 2$, $|A/V| = 3$, $|V/\langle (13)(24) \rangle| = 2$, $|\langle (13)(24) \rangle / \langle \mathrm{id} \rangle| = 2$, todėl $S_4/A_4 \approx \mathbf{Z}_2$, $A/V \approx \mathbf{Z}_3$, $V/\langle (13)(24) \rangle \approx \mathbf{Z}_2$ ir $\langle (13)(24) \rangle / \langle \mathrm{id} \rangle \approx \mathbf{Z}_2$, t.y. visos faktorgrupės yra ciklinės. Gavome, kad S_4 yra išsprendžiama.

Teorema 8.4 (Galua,1832) *Keitinių grupė S_n , $n \geq 5$ yra neišsprendžiama.*

Teoremos įrodymas remiasi lemomis.

Lema 8.5 *Lyginių keitinių grupė A_n yra generuojama ilgio* 3 *ciklais.*

Įrodymas. Bet kuris lyginis keitinys σ yra lyginio skaičiaus transpozicijų sandauga: $\sigma = t_1 t_2 \cdots t_{2m-1} t_{2m}$. Dviejų transpozicijų sandaugą visada galima užrašyti ilgio 3 ciklų sandauga:

$$(ij)(kl) = \left\{ \begin{array}{cc} (ij)(jl) = (ijl) & \text{kai } j = k \\ (ij)(jk)(jk)(kl) = (ijk)(jkl) & \text{kai } i,j,k,l \text{ yra skirtingi} \\ \mathrm{id} & \text{kai } (ij) = (kl) \end{array} \right\}.$$

Įrodyta.

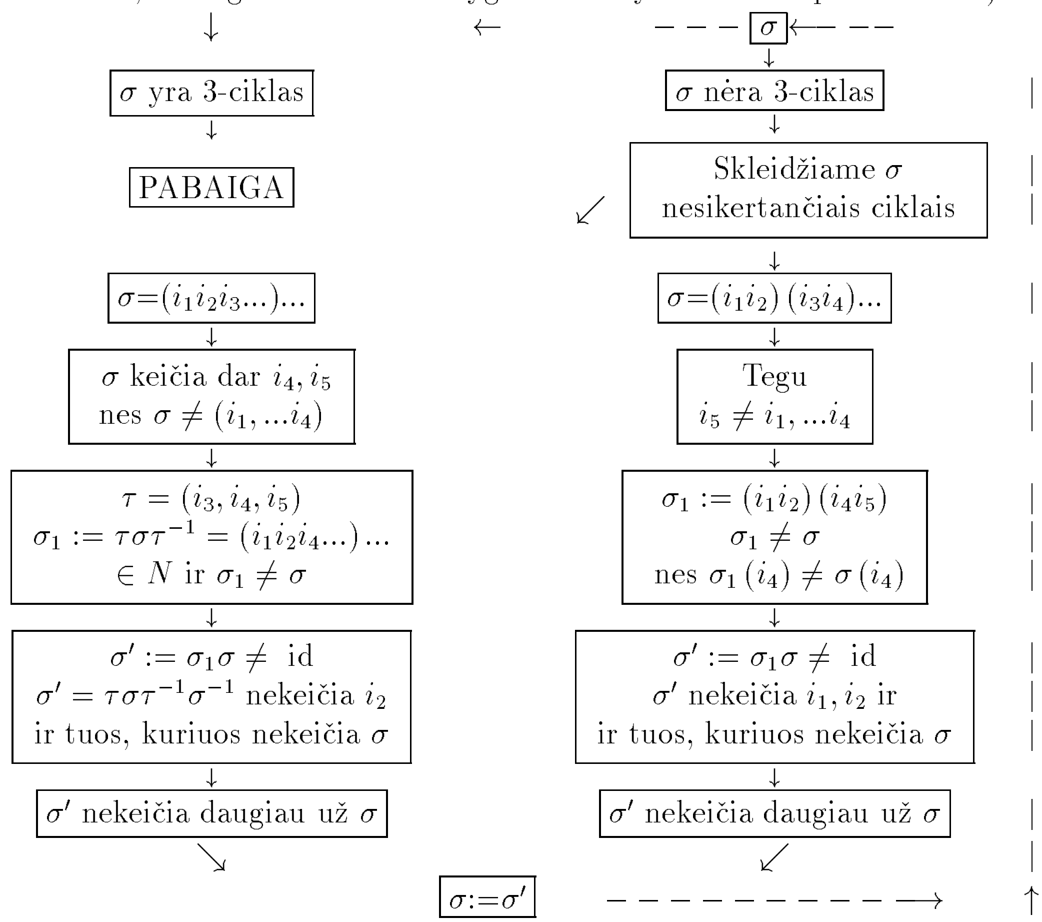
Lema 8.6 *Normalusis A_n $(n \geq 5)$ pogrupis N, turintis ilgio* 3 *ciklą, sutampa su A_n*

Įrodymas. Tegu c yra ilgio 3 ciklas pogrupyje N, o d yra bet kuris ilgio 3 ciklas grupėje A_n. Žinoma, kad egzistuoja toks $\sigma \in S_n$, kad $d = \sigma c \sigma^{-1}$. Jeigu $\sigma \in A_n$, tai $d \in N$, nes N yra normalusis pogrupis. Jeigu $\sigma \notin A_n$ ir $n \geq 5$, tai egzistuoja tokia transpozicija $t \in S_n$, kad $t\sigma \in A_n$. Tada $d = tdt^{-1} = t\sigma c \sigma^{-1} t \in N$ ($t = t^{-1}$).

Įrodyta.

Lema 8.7 *Kiekvienas* $A_n \, (n \geq 5)$ *normalusis pogrupis* N, $N \neq \langle \mathrm{id} \rangle$, *turi ilgio 3 ciklą.*

Įrodymas. Tegu $\sigma \in N$ ir $\sigma \neq \mathrm{id}$. Jeigu σ nėra ilgio 3 ciklas, tai mes parodysime kaip rasti tokį $\sigma' \in N, \sigma \neq \mathrm{id}$, kuris nekeistų daugiau elementų iš $\{1, ..., n\}$ negu σ (pastebėkime, kad ilgio 2 ciklas nėra lyginis keitinys ir todėl nepriklauso N).



Įrodyta.

Iš šių trijų lemų mes turime, kad grupėje $A_n (n \geq 5)$ nėra netrivialių normaliųjų pogrupių. Tokias grupes vadina **paprastomis grupėmis**. Taigi, $A_n (n \geq 5)$ yra paprastoji grupė.

Lema 8.8 Keitinių grupėje S_n , $n \geq 5$, yra tik tris normalieji pogrupiai $1, A_n$ ir S_n.

Įrodymas. Tegu N yra normalusis S_n pogrupis. Tada $N \cap A_n$ yra normalusis A_n pogrupis. Grupė A_n yra paprastoji, todėl arba $N \cap A_n = A_n$, arba $N \cap A_n = \langle \mathrm{id} \rangle$. Pirmuoju atveju, $N \supseteq A_n$, o A_n indeksas grupėje yra 2, todėl N yra arba A_n, arba S_n. Antruoju atveju, funkcija $\varphi : N \to S_n / A_n$, $\varphi(x) = xA_n$ yra injektyvi ir todėl grupėje N yra arba 1, arba 2 elementai. Jeigu grupėje N yra 1 elementas, tai $N = \langle \mathrm{id} \rangle$. Grupėje negali būti lygiai 2 elementų, nes jeigu $c \in N$, tai ir $\sigma c \sigma^{-1} \in N$ su visiais $\sigma \in S_n$.

Įrodyta.

Teoremos 8.4 įrodymas. Turime tik tokią keitinių grupės S_n normaliąją grandinę: $S_n \triangleright A_n \triangleright \langle \mathrm{id} \rangle$. Bet grupė A_n yra nekomutatyvi: pvz.: $(123)(124) = (14)(23)$, bet $(124)(123) = (13)(24)$. Taigi, A_n yra neciklinė ir S_n nėra išsprendžiama.

Įrodyta.

Dabar pateiksime teoremas be įrodymų, aprašančias išsprendžiamų grupių klases.

Teorema 8.9 *Visi išsprendžiamos grupės pogrupiai ir visos faktorgrupės yra išsprendžiamos grupės.*

Teiginys 8.10 *Baigtinė p -grupė G, t.y. grupė, turinti p^s elementų, yra išsprendžiama.*

Teiginys 8.11 *Visos grupės, kurių eilė < 60, yra išsprendžiamos.*

Teorema 8.12(Feit-Thomson,1963) *Nelyginės eilės grupė yra išsprendžiama.*