Algebra ir geonetrija informatikams. Paskaitų konspektas. Rimantas Grigutis

9 paskaita. *Šaknys iš vieneto ir grupės.*

Kaip ir su kiekvienu nenuliniu kompleksiniu skaičiumi, taip ir su 1 turime lygiai n $n-$ojo laipsnio šaknų iš 1 :

$$1 = [1, 0] = \cos 0 + i \sin 0$$
$$\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n},$$

$k = 0, 1, 2, ..., n-1$.

Visos $n-$ ojo laipsnio šaknys iš vieneto yra apskritimo, kurio centas yra koordinačių pradžioje ir spindulys lygus 1, taškai. Vienas iš šių taškų sutampa su 1 (kai $k = 0$). Šaknies ε_1 argumentas yra $\frac{2\pi}{n} = 2\pi \cdot \frac{1}{n}$, t.y. n − oji apskritimo dalis. Kitų šaknų $\varepsilon_2, ..., \varepsilon_{n-1}$ argumentai yra $\frac{2\pi k}{n} = 2\pi \cdot \frac{2}{n}, ..., \frac{2\pi (n-1)}{n} = 2\pi \cdot \frac{n-1}{n}$. Visos $n-$ ojo laipsnio šaknys iš vieneto dalija vienetinį apskritimą į n lygių dalių. Visų $n-$ ojo laipsnio šaknų iš vieneto aibę žymėsime $U(n)$.

Apibrėžimas. $n-$ ojo laipsnio šaknis iš vieneto ε vadinama **primityviąja** $n-$ ojo laipsnio šaknimi iš vieneto, jei $\varepsilon^m \neq 1$ su $m < n$.

Aišku, kad skaičius $\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto. Kai $n > 2$, turime ir daugiau primityviųjų $n-$ ojo laipsnio šaknų iš vieneto. Teisinga tokia teorema:

Teorema. Skaičius $\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$ yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto tada ir tik tada, kai skaičių k ir n bendras didžiausias daliklis yra lygus 1 (tokius skaičius dar vadina tarpusavyje pirminiais skaičiais).

Įrodymas. $(\Rightarrow)$. Tegu k ir n yra tarpusavyje pirminiai skaičiai ir $\varepsilon_k^m = 1$. Tada

$$\frac{2\pi km}{n} = 2r\pi, \text{ čia } r \text{ - sveikas skaičius.}$$

Turime

$$km = nr,$$

ir todėl km dalijasi iš n. Bet k ir n yra tarpusavyje pirminiai skaičiai, todėl m dalijasi iš n. Tada turime, kad $m \geq n$ ir todėl skaičius $\varepsilon_k = \cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n}$ yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto.

$(\Leftarrow)$. Tegu ε_k yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto ir $d = \text{BDD}(k, n)$, $n = n_1 d, k = k_1 d$. Tada $\varepsilon_k = \cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n} = \cos\dfrac{2\pi k_1 d}{n_1 d} + i\sin\dfrac{2\pi k_1 d}{n_1 d} = \cos\dfrac{2\pi k_1}{n_1} + i\sin\dfrac{2\pi k_1}{n_1}$ ir $\varepsilon_{k_1}^{n_1} = 1$. Iš čia turime, kad $n = n_1$ ir $d = 1$, t.y. skaičiai n ir k yra tarpusavyje pirminiai.

Įrodyta.

Pavyzdys.

Primityvios n -ojo laipsnio šaknys iš 1

n	šaknų skaičius	Primityvios šaknys ε_k
3	2	$\varepsilon_1, \varepsilon_2$
4	2	$\varepsilon_1, \varepsilon_3$
5	4	$\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$
6	2	$\varepsilon_1, \varepsilon_5$
7	6	$\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6$
8	4	$\varepsilon_1, \varepsilon_3, \varepsilon_5, \varepsilon_7$
9	6	$\varepsilon_1, \varepsilon_2, \varepsilon_4, \varepsilon_5, \varepsilon_7, \varepsilon_8$
10	4	$\varepsilon_1, \varepsilon_3, \varepsilon_7, \varepsilon_9$
11	10	$\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7, \varepsilon_8, \varepsilon_9, \varepsilon_{10}$
12	4	$\varepsilon_1, \varepsilon_5, \varepsilon_7, \varepsilon_{11}$

.

Teiginys. Skaičius $\varepsilon_k = \cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n}$ yra primityvioji $n_1 = \dfrac{n}{d}-$ ojo laipsnio šaknis iš vieneto, čia $d = \text{BDD}(n, k)$.

Įrodymas. Skaičiai $n_1 = \dfrac{n}{d}$ ir $k_1 = \dfrac{k}{d}$ yra tarpusavyje pirminiai skaičiai ir todėl pagal ką tik įrodytą teoremą skaičius $\varepsilon_k = \cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n} = \cos\dfrac{2\pi k_1}{n_1} + i\sin\dfrac{2\pi k_1}{n_1} = \varepsilon_{k_1}$ yra primityvioji n_1- ojo laipsnio šaknis iš vieneto.

Įrodyta.

Teiginys(šaknų iš vieneto savybės).

1. Jeigu α ir $\beta \in U(n)$, tai ir $\alpha \cdot \beta \in U(n)$.

2. Jeigu $\alpha \in U(n)$, tai $\alpha^{-1} \in U(n)$.

3. Jeigu ε yra primityvioji n-ojo laipsnio šaknis iš 1, o $\alpha \in U(n)$, tai egzistuoja toks $k \in \mathbf{N}$, kad $\alpha = \varepsilon^k$.

4. Jeigu ε yra primityvioji n-ojo laipsnio šaknis iš 1, o β yra kuri nors n-ojo laipsnio šaknis iš α, tai skaičiai $\varepsilon^0\beta, \varepsilon^1\beta, \varepsilon^2\beta, ..., \varepsilon^{n-1}\beta$ yra visos skirtingos n-ojo laipsnio šaknys iš α.

Įrodymas. 1. Jei α ir $\beta \in U(n)$, tai $\alpha^n = \beta^n = 1$. Tada $(\alpha\beta)^n = \alpha^n\beta^n = 1$ ir $\alpha \cdot \beta \in U(n)$.

2. Jei $\alpha \in U(n)$, tai $\alpha^n = 1$. Tada $(\alpha^{-1})^n = \alpha^{-n} = (\alpha^n)^{-1} = 1$ ir $\alpha^{-1} \in U(n)$.

3. Tegu ε yra primityvioji n-ojo laipsnio šaknis iš 1. Tada skaičius $\varepsilon^k \in U(n)$, nes $\left(\varepsilon^k\right)^n = (\varepsilon^n)^k = 1$. Šaknų iš 1 sekoje $1 = \varepsilon^0, \varepsilon^1, \varepsilon^2, ..., \varepsilon^{n-1}$ nėra sutampančių, nes jei būtų $\varepsilon^k = \varepsilon^m$, čia $0 \leq k < m \leq n-1 < n$, tai $\varepsilon^{m-k} = 1$ ir $0 < m-k < n$, o tai prieštarautų tam, kad ε yra primityvioji n-ojo laipsnio šaknis iš 1. Gavome, kad sekoje $1 = \varepsilon^0, \varepsilon^1, \varepsilon^2, ..., \varepsilon^{n-1}$ yra visos skirtingos n-ojo laipsnio šaknys iš 1.

4. Tegu $\beta^n = \alpha$ ir ε yra primityvioji n-ojo laipsnio šaknis iš 1. Tada $\left(\varepsilon^k\beta\right)^n = \left(\varepsilon^k\right)^n \beta^n = 1 \cdot \alpha = \alpha$ ir $\varepsilon^k\beta$ yra n-ojo laipsnio šaknis iš α su visais $k \in \mathbf{Z}$. Skaičių $\beta = \varepsilon^0\beta, \varepsilon^1\beta, \varepsilon^2\beta, ..., \varepsilon^{n-1}\beta$ sekoje nėrs sutampančių,nes jei būtų $\varepsilon^k\beta = \varepsilon^m\beta$, čia $0 \leq k < m \leq n-1 < n$, tai $\varepsilon^{m-k} = 1$ ir $0 < m-k < n$, o tai prieštarautų tam, kad ε yra primityvioji n-ojo laipsnio šaknis iš 1. Gavome, kad sekoje $\beta = \varepsilon^0\beta, \varepsilon^1\beta, \varepsilon^2\beta, ..., \varepsilon^{n-1}\beta$ yra visos skirtingos n-ojo laipsnio šaknys iš α.

Įrodyta.

Apibrėžimas(grupės apibrėžimas). Tegu G yra aibė, kurioje apibrėžta operacija " $\cdot$ ", t.y. taisyklė, bet kuriai aibės G elementų porai (g_1, g_2) priskirianti aibės G elementą g_3. Aibė $(G, \cdot)$ vadinama grupe, jei teisingos šios savybės

G1. $g_1(g_2g_3) = (g_1g_2)g_3$ su visais $g_1, g_2, g_3 \in G$. Šią savybę vadiname veiksmo asociatyvumu.

G2. Egzistuoja toks $e \in G$, kad su visais $g \in G$ teisinga $eg = ge = g$. Elementą vadiname neutraliu grupės elementu.

G3. Su kiekvienu $g \in G$ egzistuoja toks $h \in G$, kad $gh = hg = e$. Elementą h vadiname atvirkštiniu elementui g ir žymesime g^{-1}.

Grupių pavyzdžiai.

1. Sveikųjų skaičių aibė $\mathbf{Z}$ sudėties $+$ atžvilgiu yra grupė.

2. Racionaliųjų skaičių aibė $\mathbf{Q}$ sudėties $+$ atžvilgiu yra grupė.

3. Realiųjų skaičių aibė $\mathbf{R}$ sudėties $+$ atžvilgiu yra grupė.

4. Kompleksinių skaičių aibė $\mathbf{C}$ sudėties $+$ atžvilgiu yra grupė.

5. Matricų aibės $M_{m\times n}(\mathbf{Z}), M_{m\times n}(\mathbf{Q}), M_{m\times n}(\mathbf{R}), M_{m\times n}(\mathbf{C})$ sudėties $+$ atžvilgiu yra grupė.

6. Dviejų sveikų skaičių aibė $\mathbf{Z}_2 = \{-1, 1\}$ sandaugos $\cdot$ atžvilgiu yra grupė.

7. Nenulinių racionaliųjų skaičių aibė $\mathbf{Q}$ sandaugos $\cdot$ atžvilgiu yra grupė.

8. Nenulinių realiųjų skaičių aibė $\mathbf{R}$ sandaugos $\cdot$ atžvilgiu yra grupė.

9. Nenulinių kompleksinių skaičių aibė $\mathbf{C}$ sandaugos $\cdot$ atžvilgiu yra grupė.

10. Neišsigimusių racionalių(realių, kompleksinių) matricų aibė $GL(n, K)$ sandaugos $\cdot$ atžvilgiu yra grupė.

11. Visų keitinių aibė S_n su joje apibrėžta kompozicijos operacija $\circ$ yra grupė.

12. n-ojo laipsnio kompleksinių šaknų iš 1 aibė $U(n)$ sandaugos $\cdot$ atžvilgiu yra grupė.

13. Aibė $\mathbf{Z}_n = \left\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\right\}$ operacijos "+", apibrėžtos formule

$$\bar{i} + \bar{j} = \left[\begin{array}{l} \overline{i+j}, \text{kai } i+j < n \\ \overline{i+j-n}, \text{ kai } i+j \geq n \end{array} \right. ,$$

yra grupė.

14.Tegu $\sigma = (1, 2, ..., n) \in S_n$. Keitinių aibė $\langle\sigma\rangle = \{id = \sigma^0, \sigma^1, \sigma^2, ..., \sigma^{n-1}\}$ su joje apibrėžta kompozicijos operacija $\circ$ yra grupė.

Iš apibrėžimo turime, kad grupės $(G, \cdot)$ neutralusis elementas apibrėžtas vienareikšmiškai: jei e' yra neutralusis grupės G elementas, tai $e' = e' \cdot e = e \cdot e' = e$.

Svarbiausia grupės savybė yra prastinimo taisyklė.

Teorema(prastinimo taisyklė). Tegu G yra grupė. Tada
• jei $ax = ay$, tai $x = y$.
• jei $xa = ya$, tai $x = y$.

Įrodymas. Tegu $ax = ay$. Padauginkime šią lygybę iš kairės iš a^{-1} ir pasinaudoję asociatyvumo savybe turėsime

$$x = a^{-1}ax = a^{-1}ay = y.$$

Tegu $xa = ya$. Padauginkime šią lygybę iš dešinės iš a^{-1} ir pasinaudoję asociatyvumo savybe turėsime

$$x = xaa^{-1} = yaa^{-1} = y.$$

Įrodyta.

Išvados. 1.Su kiekvienu grupės G elementu g egzistuoja vienintelis atvirkštinis g^{-1}.
2. Grupėje G lygtys $ax = b$ ir $xa = b$ išsprendžiamos vienareikšmiškai.

Įrodymas. 1. Tegu $gh = hg = e$. Tada

$$h = he = h\left(gg^{-1}\right) = (hg)\, g^{-1} = eg^{-1} = g^{-1}.$$

2. Jei $ax = b$, tai $x = a^{-1}b$ yra lygties sprendinys. Ir jei $ax_1 = b$, tai pagal prastinimo taisyklę lygybei $ax = ax_1$ turime $x = x_1$.
Jei $xa = b$, tai $x = ba^{-1}$ yra lygties sprendinys. Ir jei $x_1a = b$, tai pagal prastinimo taisyklę lygybei $xa = x_1a$ turime $x = x_1$.
Įrodyta.

Apibrėžimai. Grupė G vadinama **baigtine**, jei aibėje G yra baigtinis elementų skaičius. Aibės G elementų skaičių vadiname **grupės eile**. Sakoma, kad grupės G **elementai** a ir b **komutuoja**, jei $ab = ba$. Grupė G vadinama **komutatyvia grupe**, jei $ab = ba$ su visais $a, b \in G$.

Pavyzdžiai. 1. Grupės 1-5,6-10 yra begalinės eilės.

2. Grupės $\mathbf{Z}_2$ eilė yra 2, grupės S_n eilė yra $n!$, grupės $U(n)$ eilė yra n, grupės $\mathbf{Z}_n$ eilė yra n.

3. Grupės 1-4, 6-9,12-14 yra komutatyvios grupės.

4. Grupės 5,10,11 yra nekomutatyvios grupės.

Kai kurios grupės, net ir turėdamos skirtingos prigimties elementus ir skirtingai apibrežtas operacijas, turi vienodas savybes. Patikslinsime šį pastebėjimą.

Apibrėžimas. Tegu $(G, *)$ ir $(H, \circ)$ dvi grupės. Funkciją $f : G \to H$ vadinama grupių **izomorfizmu**, jeigu

1) f yra bijekcija,t.y.

• jei $f(g_1) = f(g_2)$, tai $g_1 = g_2$ su visais $g_1, g_2 \in G$, ir

• su visais $h \in H$ egzistuoja toks $g \in G$, kad $f(g) = h$.

2) Su visais $g_1, g_2 \in G$ teisinga $f(g_1 * g_2) = f(g_1) \circ f(g_2)$.

Jeigu egzistuoja grupių G ir H izomorfizmas, tai sakoma, kad grupės G ir H yra izomorfinėmis ir rašoma $G \approx H$.

Jau iš apibrėžimo matome, kad izomorfinėse grupėse vienos grupės elementų sandauga atitinka kitos grupės elementų sandaugą(dar sakoma, kad grupių izomorfizmas " išlaiko operaciją"). Šiuo požiūriu izomorfinės grupės yra vienodos. Dar daugiau, grupių izomorfizmo pagrindu galima kalbeti apie ekvivalentumo santykį:

1. $G \approx G$ (izomorfimu yra tapatusis atvaizdis $g \to g$).

2. Jei $G \approx H$, tai ir $H \approx G$ (jei f yra izomorfizmas, tai ir f^{-1} yra izomorfizmas).

3. Jei $G_1 \approx G_2$, o $G_2 \approx G_3$, tai $G_1 \approx G_3$ (izomorfizmų kompozicija yra izomorfizmas).

Pavyzdžiai. 1 . $(\mathbf{C},+) \approx \left(\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbf{R}) \right\}, + \right)$. Izomorfizmas: $a + ib \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

2. $(\mathbf{C}\setminus\{0\},\cdot) \approx \left(\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbf{R}), a^2+b^2 \neq 0 \right\}, \cdot \right)$. Izomorfizmas: $a+ib \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

3. $(\mathbf{R},+) \approx \left(\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbf{R}) \right\}, + \right)$. Izomorfizmas: $a \to \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

4. $(\mathbf{R}\setminus\{0\},\cdot) \approx \left(\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbf{R}), a \neq 0 \right\}, \cdot \right)$. Izomorfizmas: $a \to \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

5. $(\mathbf{Z}_n,+) \approx (U(n),\cdot)$. Izomorfizmas: $k \to \left[1, \frac{2\pi k}{n}\right]$.

6. $(\mathbf{Z}_n,+) \approx (\langle \sigma | \sigma = (1,2,...,n) \in S_n \rangle, \circ)$. Izomorfizmas: $k \to \sigma^k$.

7. $(\mathbf{R},+) \approx \left(\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbf{R} \right\}, \cdot \right)$. Izomorfizmas: $a \to \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$.