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

Sekdami pitagoriečiais (V a. pr.Kr.), senieji graikai "skaičiais" vadino tik sveikuosius skaičius ir racionaliuosius skaičius. Tačiau domėdamiesi aristokratijos simboliu - geometrinio vidurkio dydžiu $a : b = b : c$ susidūrė su iracionalumu: kam yra lygus dviejų šventųjų skaičių 1 ir 2 geometrinis vidurkis ?(Pats skaičius buvo pitagoriečių filosofinio misticizmo pagrindas: prisiminkime kad ir jų posakį " viskas yra skaičius"). Geometrinį vidurkį formuluodami geometriškai: "kam yra lygi kvadrato įstrižainė?" - teko pripažinti, kad šis santykis nėra "skaičius". Tai griovė buvusią aritmetikos ir geometrijos harmoniją. Tik Eudokso ($408 - 355$ m.pr.Kr.) santykių teorija "įveikė" šią graikų matematikos "krizę": algebriniai dydžiai buvo reiškiami geometriškai, pavyzdžiui $\sqrt{2}$ buvo reiškiama kvadrato, kurio plotas yra lygus 2, kraštine, o visos algebrinės operacijos buvo apibrėžiamos geometriškai. Tai buvo savotiškas iracionaliųjų skaičių pripažinimas. Ir tai teikė vilties, kad šių "brėžiamų" skaičių jiems pakaks savo reikmėms. Net žymiesiems savo brėžimo skriestuvu ir liniuote uždaviniams: kubo dvigubinimo, kampo trisekcijos, skritulio kvadratūros,- išspręsti. Dabar mes pamatysime, kodėl šios jų viltys nepasiteisino.

Tegu turime liniuotę, kurios ilgis bus 1, ir skriestuvą, kuriuo galime brėžti bet kurio spindulio apskritimus. Skaičių (tiksliau būtų atkarpą, kurios ilgis yra šis

skaičus) vadinsime **brėžiamu**, jeigu jis yra 1 arba jį galima nubrėžti atlikus tik šiuos veiksmus:

• sujungti du brėžiamus taškus atkarpa;

• brėžti apskritimą, kurio centras yra brėžiamame taške ir spindulys yra brėžiamas skaičius.

Apibrėžimas 7.1 *Tegu K yra realiųjų skaičių $\mathbf{R}$ pokūnis. Dekarto sandaugą $K \times K \subset \mathbf{R} \times \mathbf{R}$ vadinsime $K-$ plokštuma. Tiese $K-$ plokštumoje vadinsime tiesę, einančią per du $K-$ plokštumos taškus. Ši tiesė yra reiškiama lygtimi*

$$ax + by + c = 0, \text{ čia } a, b, c \in K.$$

Apskritimu $K-$ plokštumoje vadinsime apskritimą, kurio centras yra $K-$ taške, o spindulys yra iš K. Šis apskritimas yra reiškiamas lygtimi

$$(x - a)^2 + (y - b)^2 = r^2 \text{ , čia } a, b, r \in K.$$

Lema 7.2 *Tegu $L_1 \neq L_2$ yra dvi $K-$ tiesės ir $C_1 \neq C_2$ du $K-$ apskritimai. Tada*

(1) $L_1 \cap L_2 = \emptyset$ arba turi vieną bendrą $K-$ tašką;

(2) $L_1 \cap C_1 = \emptyset$ arba turi vieną, arba turi du $K(\sqrt{s})-$ taškus, čia $s \in K$;

(3) $C_1 \cap C_2 = \emptyset$ arba turi vieną, arba turi du $K(\sqrt{s})-$ taškus, čia $s \in K$.

Įrodymas. Sankirtų taškai gaunami sprendžiant arba tiesinių lygčių sistemą su koeficientais iš K, arba vienos tiesinės ir vienos kvadratinės lygties, arba dviejų kvadratinių lygčių sistemas su koeficientais iš K. Šios sistemos suvedamos blogiausiu atveju į vieno nežinomojo kvadratinės lygties su koeficientais iš K sprendimą. Detales paliekame skaitytojui.

Įrodyta.

Lema 7.3 (1) *Jeigu a ir b yra brėžiami skaičiai, tai ir $a \pm b$, ab ir $\frac{a}{b}$,($b \neq 0$) yra brėžiami.*

(2) *Jeigu $a > 0$ yra brėžiamas, tai ir $\sqrt{a}$ yra brėžiamas.*

Įrodymas. (1) Iš mokyklos laikų mokame brėžti tiesę, einančią per duotą tašką ir lygiagrečią arba statmeną duotai tiesei. Žinome taip pat kaip brėžti $a \pm b$. Norint brėžti $a \cdot b$, viename smailaus kampo su viršūne O spindulyje reikia atidėti taškus A ir B taip, kad $OA = 1$ ir $OB = a$ (tegu $a > 1$), o kitame spindulyje – tašką

C taip, kad $OC = b$. Nubrėžę tiesę, einančią per tašką B ir lygiagrečią atkarpai AC gausime susikirtimo tašką D taško C spindulyje. Iš trikampių OAC ir OBD panašumo gauname $\frac{OA}{OC} = \frac{OB}{OD} \Rightarrow \frac{1}{b} = \frac{a}{OD} \Rightarrow OD = a \cdot b$.

Norint nubrėžti skaičių $\frac{1}{a}$, $a > 1$, reikia smailiojo kampo viename spindulyje atidėti vienetinę atkarpą OA ir atkarpą $OB = a$, o kitame spindulyje atkarpą $OC = 1$. Nubrėžę tiesę, einančią per tašką B ir lygiagrečią atkarpai AC gausime susikirtimo tašką D taško C spindulyje. Tada gauname $\frac{OA}{OC} = \frac{OB}{OD} \Rightarrow \frac{1}{1} = \frac{a}{OD} \Rightarrow OD = \frac{1}{a}$. Dabar mokėsime brėžti ir skaičių $a \cdot \frac{1}{b} = \frac{a}{b}$.

(2) Brėžiame $a + 1$ skersmens apskritimą. Jo skersmenyje AB taip atidedame tašką C, kad $AC = a$ ir $CB = 1$. Iš taško C iškeliame stamenį, kuris kerta apskritimą taške D. Tada $\frac{AC}{CD} = \frac{CD}{CB} \Rightarrow CD^2 = AC \cdot CB \Rightarrow CD = \sqrt{a}$.

Įrodyta.

Teorema 7.4 (Pagrindinė brėžimo teorema). (1) *Brėžiamų skaičių aibė yra kūnas.*

(2) *Skaičius a yra brėžiamas tada ir tik tada, kada jis yra plėtinyje*

$$\mathbf{Q}\left(\sqrt{a_1}, ..., \sqrt{a_r}\right), a_i \in \mathbf{Q}\left(\sqrt{a_1}, ..., \sqrt{a_{i-1}}\right) \text{ ir } a_1 \in \mathbf{Q}.$$

Įrodymas. (1) Tai tiesioginė Lemos 7.3 (1) išvada.

(2) Iš (1) matome, kad brėžiamų skaičių kūnas yra $\mathbf{Q}$ plėtinys(pagaliau $\mathbf{Q}$ yra mažiausias kūnas turintis sveikąjį 1). Iš Lemos 7.3 (2) turime, kad visi skaičiai iš $\mathbf{Q}\left(\sqrt{a_1}, ..., \sqrt{a_r}\right)$ yra brėžiami. Iš kitos pusės pagal Lemą 7.2 kiekvienas brėžiamas skaičius yra kūne $\mathbf{Q}\left(\sqrt{a_1}, ..., \sqrt{a_r}\right)$.

Įrodyta.

Išvada 7.5 (Pagrindinė brėžimo sąlyga) *Jeigu a yra brėžiamas skaičius, tai a yra algebrinis virš $\mathbf{Q}$ ir plėtinio $\mathbf{Q}(a)/\mathbf{Q}$ laipsnis $[\mathbf{Q}(a) : \mathbf{Q}]$ yra lygus 2^m.*

Įrodymas. Jeigu a yra brėžiamas skaičius, tai iš Teoremos 1.8 kūnų grandinei $\mathbf{Q} \subset \mathbf{Q}(a) \subset \mathbf{Q}\left(\sqrt{a_1}, ..., \sqrt{a_r}\right)$mes žinome, kad $[\mathbf{Q}(a) : \mathbf{Q}]$ yra

$\left[\mathbf{Q}\left(\sqrt{a_1}, ..., \sqrt{a_r}\right) : \mathbf{Q}\right] = 2^r$ daliklis.

Įrodyta.

Dabar galime kalbėti apie klasikinių brėžimo skriestuvu ir liniuote uždavinių išsprendžiamumą.

Teiginys 7.6 *Negalima skriestuvu ir liniuote nubrėžti kubą, kurio tūris dvigubai didesnis už duotijo kubo tūrį.*

Įrodymas. Iš tikrųjų mums pakanka parodyti, kad negalima nubrėžti kubo, kurio tūris yra lygus 2. Tam reikia mokėti nubrėžti kubinės lygties $x^3 - 2 = 0$ šaknį. Pagal Eizenšteino (F. G. M. Eisenstein, 1823-1852) kriterijų (kai $p = 2$) polinomas $f(x) = x^3 - 2$ yra neredukuojamas virš $\mathbf{Q}$. Todėl, kaip žinome, $\left[\mathbf{Q}\left(\sqrt[3]{2}\right) : \mathbf{Q}\right] = 3$ ir pagal Pagrindinę brėžimo sąlygą turime, kad skaičius $\sqrt[3]{2}$ nėra brėžiamas.

Įrodyta.

Teiginys 7.7 *Negalima skrietuvu ir liniuote bet kurį kampą padalyti į tris lygias dalis.*

Įrodymas. Aišku, kad kampo brėžimas yra ekvivalentus šio kampo trigonometrinių funkcijų reikšmių brėžimui. Taigi, norėdami padalyti kampą α į tris dalis, turėtume mokėti nubrėžti lygties $\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}$ sprendinį. Pavyzdžiui, jeigu $\alpha = 60°$, tai mes turėtume mokėti nubrėžti lygties $8x^3 - 6x - 1 = 0$ sprendinį. Bet polinomas $g(x) = 8x^3 - 6x - 1$ neturi racionaliųjų šaknų(o jomis galėtų būti tik skaičiai $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$, bet patikrinus taip nėra), todėl jis yra neredukuojamas virš $\mathbf{Q}$. Taigi, $[\mathbf{Q}(\cos 20°) : \mathbf{Q}] = 3$ ir pagal Pagrindinę brėžimo sąlygą turime, kad skaičius $\cos 20°$, o tuo tarpu ir $\frac{\alpha}{3} = 20°$ nėra brėžiamas.

Įrodyta.

Teiginys 7.8 *Negalima skrietuvu ir liniuote nubrėžti kvadratą, kurio plotas būtų lygus skritulio plotui.*

Įrodymas. Norėdami nubrėžti kvadratą, kurio plotas yra lygus sritulio, kurio spindulys yra r, plotui, turėtume mokėti nubrėžti lygties $x^2 - \pi = 0$ sprendinį. Bet skaičius π yra transcendentinis (pirmasis tai įrodė F.Lindemanas(1852-1939) 1882 metais), todėl polinomas $h(x) = x^2 - \pi$ yra neredukuojamas virš $\mathbf{Q}$ ir pagal Pagrindinę brėžimo sąlygą turime, kad skaičius $\sqrt{\pi}$ nėra brėžiamas.

Įrodyta.

Aptarkime dar vieną klasikinį brėžimo skriestuvu ir liniuote uždavinį: *ar galima įbrėžti į apskritimą taisyklingąjį $n-$kampį?* Aišku, jeigu apskritimo spindulį laikysime lygiu 1, o centru pasirinksime koordinačių pradžią, tai reikia mokėti

brėžti lygrties $x^n - 1$ sprendinius. Pažiūrėkime, kada tai galima padaryti. Visų pirma pastebėsime, kad polinomas $x^n - 1$ yra redukuojamas:

$$(*) \qquad x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right).$$

Lema 7.9 *Jeigu p yra pirminis skaičius, tai polinomas $x^{p-1}+x^{p-2}+\cdots+x+1$ yra neredukuojamas virš $\mathbf{Q}$ ir plėtinio $\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right)/\mathbf{Q}$ laipsnis $\left[\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right):\mathbf{Q}\right] = p-1$.*

Įrodymas. Kai $n = p$, lygybėje $(*)$ atlikime kintamųjų keitinį $t = x - 1$:

$$(t+1)^p - 1 = t \cdot \left((t+1)^{p-1} + (t+1)^{p-2} + \cdots + t + 1 + 1\right).$$

Tada

$$f(t+1) = \frac{(t+1)^p - 1}{t} = t^{p-1} + \mathrm{C}_p^{p-1} \cdot t^{p-2} + \cdots + \mathrm{C}_p^3 \cdot t^2 + \mathrm{C}_p^2 \cdot t^2 + p \cdot t.$$

Žinome, kad C_p^i dalijasi iš p su visais $1 \le i \le p-1$. Tada pagal Eizenšteino kriterijų polinomas $f(t+1)$, o tuo pačiu ir polinomas $x^{p-1}+x^{p-2}+\cdots+x+1$, yra neredukuojamas virš $\mathbf{Q}$. Iš Išvados 6.4 turime, kad neredukuojami polinomai virš $\mathbf{Q}$ yra separabilūs, todėl $\left[\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right):\mathbf{Q}\right] = \deg\left(x^{p-1} + x^{p-2} + \cdots + x + 1\right) = p-1$. Priminsime, kad $\mathrm{e}^{\frac{2\pi i}{p}}$ yra polinomo $x^p - 1 = 0$ šaknis.

Įrodyta.

Lema 7.10 *Tegu $p-$ nelyginis pirminis skaičius. Tada $\left[\mathbf{Q}\left(\cos\frac{2\pi}{p}\right) \supset \mathbf{Q}\right] = \frac{p-1}{2}$.*

Įrodymas. Tegu $p-$ nelyginis pirminis skaičius. Žinodami lygybę $\mathrm{e}^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, matome, kad norint įbrėžti į apskritimą taisyklingąjį $p-$kampį, reikia mokėti brėžti $\cos\frac{2\pi}{p}$. Turime $\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right) \supset \mathbf{Q}\left(\cos\frac{2\pi}{p}\right) \supset \mathbf{Q}$. Skaičius $\mathrm{e}^{\frac{2\pi i}{p}}$ yra lygties $x^2 - 2\cos\frac{2\pi}{p}\cdot x + 1 = 0$ sprendinys, beto šis skaičius yra kompleksinis(neprikl auso $\mathbf{R}$). Todėl plėtinio $\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right)/\mathbf{Q}\left(\cos\frac{2\pi}{p}\right)$ laipsnis $\left[\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right):\mathbf{Q}\left(\cos\frac{2\pi}{p}\right)\right] = 2$. Pagal Teoremą 1.8 kūnų grandinei $\mathbf{Q}\left(\mathrm{e}^{\frac{2\pi i}{p}}\right) \supset \mathbf{Q}\left(\cos\frac{2\pi}{p}\right) \supset \mathbf{Q}$ turime

$\left[\mathbf{Q}\left(\cos\frac{2\pi}{p}\right) \supset \mathbf{Q}\right] = \frac{p-1}{2}$.

Įrodyta.

Teiginys 7.11 *Tegu p yra pirminis skaičius. Jeigu į apskritimą galima įbrėžti taisyklingąjį $p-$kampį, tai $p = 2^{2^r} + 1$, t.y. pirminis p yra pirminis Ferma(P.Fermat,1601-1665) skaičius.*

Įrodymas. Jeigu mes galime įbrėžti į apskritimą taisyklingąjį $p-$kampį, tai pagal Pagrindinę brėžimo sąlygą ir Lemą 7.10 turime $\frac{p-1}{2} = 2^m$, čia $m-$ natūralusis skaičius, ir $p = 2^{m+1} + 1$. Bet skaičius $2^n + 1$ yra pirminis, jeigu n yra 2 laipsnis, nes priešingai skaičius n turėtų nelyginį daliklį d, t.y. $n = d \cdot s$, ir tada skaičius $2^n + 1$ nebūtų pirminis:

$$2^n + 1 = (2^s)^d + 1 = (2^s + 1)\left(2^{s(d-1)} - 2^{s(d-2)} + \cdots + 1\right).$$

Taigi $p = 2^{2^r} + 1$ su natūraliuoju r.
Įrodyta.

Ferma manė, kad skaičiai $2^{2^n} + 1$ yra pirminiai su visais natūraliaisiais n ir paskelbė, kad patikrino, kai $n \leq 5$. Iš čia visi pirminiai skaičiai, turintys pavidalą $2^{2^n} + 1$, vadinami Ferma pirminiais skaičiais. Kai $n = 0, 1, 2, 3, 4$ skaičiai $p = 3, 5, 17, 257, 65537$ tikrai yra pirminiai. Bet 1732 m. L.Oileris (L.Euler,1707-1783) nustatė, kad skaičius $2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$ yra sudėtinis. Iki šiol nėra žinoma daugiau pirminių Ferma skaičių.

Pastebėsime, kad Teiginys 7.11 nusako tik būtinas taisyklingojo $p-$ kampio brėžimo sąlygas. Brėžti taisyklingąjį trikampį galima, nes $\cos\left(\frac{2\pi}{3}\right) = \cos 120^\circ = -\frac{1}{2}$. Galima brėžti ir taisyklingąjį $5-$kampį, nes $\cos\left(\frac{2\pi}{5}\right) = \cos 72^\circ = \frac{\sqrt{5}-1}{4}$. 1801 metais 18-metis K.F.Gausas(K.F.Gauss, 1777-1855) parodė, kad $\cos\left(\frac{2\pi}{17}\right) =$

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17} - 2\sqrt{34 + 2\sqrt{17}}}}$$

ir tuo pačiu, kad galima brėžti taisyklingąjį $17-$ kampį. Gausas įrodė dar daugiau: *į apskritimą galima įbrėžti taisyklingąjį $n-$kampį tada ir tik tada, kada skaičiaus n kanoninis skaidinys yra $n = 2^k \cdot p \cdots q$, čia $k = 0, 1, 2, ...,$ o $p, ..., q$ yra pirminiai Ferma skaičiai.*

Norint mums pakartoti Gauso rezultatą, reiktų įrodyti teiginį atvirkščią Teiginiui 7.11.

Teiginys 7.12 *Jeigu $p = 2^k + 1$ yra pirminis skaičius, tai į apskritimą galima įbrėžti taisyklingąjį $p-$kampį.*

Įrodymas. Mes jau žinome, kad užtenka parodyti, kad galima nubrėžti skaičių $\cos\left(\frac{2\pi}{p}\right)$. Skaičius $\cos\left(\frac{2\pi}{p}\right) \in \mathbf{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset \mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right)$, ir pagal Teoremą 6.7 kūnas $\mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right)$ yra Galua kūnas virš $\mathbf{Q}$, nes jis yra neredukuojamo virš $\mathbf{Q}$ polinomo $x^{p-1} + x^{p-2} + \cdots + x + 1$ skaidinio kūnas. Tegu $\sigma \in \mathrm{Gal}\left(\mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right)/\mathbf{Q}\right)$. Tada $\sigma\left(e^{\frac{2\pi i}{p}}\right) = e^{\frac{2\pi i}{p}m}$, su apibrėžtu m, $1 \leq m \leq p-1$. Iš čia funkcija $\sigma \to m$ apibrėžia grupių izomorfizmą $\mathrm{Gal}\left(\mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right)/\mathbf{Q}\right) \to (\mathbf{Z}/p\mathbf{Z})^{\times}$. Taigi Galua plėtinio $\mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right)/\mathbf{Q}$ Galua grupė G yra izomorfiška baigtinio kūno $\mathrm{GF}(p)$ multiplikacinei grupei $(\mathbf{Z}/p\mathbf{Z})^{\times}$, kurios eilė yra lygi $p - 1 = 2^k$. Gavome, kad G yra $p-$ grupė.

Iš Silovo Teoremos 4.4 (1), kai $p = 2$, žinome, kad egzistuoja tokia grupės G pogrupių grandinė

$$(1) = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_{k-1} \subset G_k = G,$$

kad faktorgrupės G_{i+1}/G_i su visais $0 \leq i \leq k-1$ eilė lygi 2. Šią pogrupių grandinę atitinka kūno $\mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right)$ pokūnių grandinė

$$(1)' = G_0' = \mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right) \supset G_1' \supset G_2' \supset \cdots \supset G_{k-1}' \supset G_k' = G' = \mathbf{Q},$$

ir $[G_i : G_{i+1}] = 2$ su visais $0 \leq i \leq k-1$. Jeigu $u_i \in G_i$ ir $u_i \notin G_{i+1}$ ir polinomas $x^2 + b_i x + c_i$, čia $b_i, c_i \in G_{i+1}$, yra minimalusis u_i polinomas, tai $u_i = \dfrac{-b_i \pm \sqrt{b_i^2 - 4c_i}}{2}$, $0 \leq i \leq k-1$. Tegu dabar $a_{i+1} = b_i^2 - 4c_i \in G_{i+1}$. Tada $G_i = G_{i+1}\left(\sqrt{a_{i+1}}\right)$ ir $\mathbf{Q}\left(e^{\frac{2\pi i}{p}}\right) = \mathbf{Q}\left(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_k}\right)$ ir $a_i \in \mathbf{Q}\left(\sqrt{a_{i+1}}, ..., \sqrt{a_k}\right)$ ir $a_k \in \mathbf{Q}$. Įrodymui baigti belieka pasinaudoti Padrindine brėžimo teorema(Teorema 7.4).

Įrodyta.