KŪNŲ TEORIJA

2000 metų rudens paskaitos

1. Kūnų plėtiniai

2. Galua grupės

Šiame skyriuje mes apibrėšime Galua grupes. Prancūzų matematikas E. Galua (Évariste Galois, 1812-1832) domėjosi grupių teorijos taikymu kūnų plėtiniams, apibrėžiamų polinomų pagalba, nagrinėti. Tame tarpe jis norėjo rasti tikslias polinomų išsprendžiamumo radikalais sąlygas. Problema formuluojama taip: ar galima rasti bet kurio laipsnio polinomo šaknų išraiškas, naudojant tik keturis aritmetinius veiksmus ir bet kurio natūralaus laipsnio traukimo šaknies veiksmus iš polinomo koeficientų. Iš pradžių norvegų matematikas N.H. Abelis (N.H. Abel, 1802-1829) pateikė penktojo laipsnio polinomo su racionaliais koeficientais neišsprendžiamo radikalais pavyzdį, o šiek tiek vėliau E.Galua nurodė tikslią šio rezultato priežastį, kiekvienam polinomui priskirdamas baigtinę grupę. Galua teorija skelbia: polinomas išsprendžiamas radikalais tada ir tik tada, kada jo grupė, kuri ir vadinama Galua grupe, yra išsprendžiama. Šiame kurse mes pabandysime tai įrodyti.

Tegu E ir F yra kūno K plėtiniai. Tokį nenulinį kūnų homomorfizmą $\sigma : E \to F$, kad $\sigma(a) = a$, su visais $a \in K$ vadina $\mathbf{K-homomorfizmu}$. $K-$ izomorfizmas $\sigma : F \to F$ vadinamas kūno F $\mathbf{K-automorfizmu}$. Visų $K-$ automorfizmų aibę pažymėkime $\mathrm{Gal}(F/K)$. (Pastebėkime, kad visų kūno F automorfizmų aibę žymi $\mathrm{Aut}(F)$, kuri, kaip nesunku parodyti, yra grupė.)

Lema 2.1 *Aibė $Gal(F/K)$ yra grupė kompozicijos atžvilgiu. Šią grupę mes vadinsime kūno F Galua grupe virš K.*

Įrodymas. Mes parodysime, kad $\mathrm{Gal}(F/K)$ yra visų kūno F bijekcijų grupės $A(F)$ pogrupis. Turime $\mathrm{id}_F \in \mathrm{Gal}(F/K)$, taigi $\mathrm{Gal}(F/K)$ nėra tuščia. Tegu dabar $\phi, \theta \in \mathrm{Gal}(F/K)$. Tada $\phi\theta^{-1}$ yra kūno F automorfizmas, nes dviejų žiedo izomorfizmų kompozicija yra žiedo izomorfizmas. Beto, $\phi\theta^{-1}(a) = \phi(\theta^{-1}(a)) = \phi(a) = a$ su visais $a \in K$. Taigi, $\phi\theta^{-1} \in \mathrm{Gal}(F/K)$ ir pagal pagrindinę pogrupio savybę [5.7 teiginys,3] turime, kad $\mathrm{Gal}(F/K)$ yra grupė.

Įrodyta.

Dabar pateiksime teoremą, kuri taikoma kai kurioms paprastoms Galua grupėms skaičiuoti.

Teorema 2.2 *Tegu F/K yra kūno plėtinys ir elemento $u \in F$ minimalusis polinomas yra $p \in K[x]$. Tada su visias $\sigma \in Gal(F/K)$ elementas $\sigma(u)$ taip pat yra polinomo p šaknis. Kitaip sakant, kiekvienas $\sigma \in Gal(F/K)$ yra polinomo šaknų, esančių kūne F, keitinys(perstata).*

Įrodyti paliekame skaitytojui.

Pavyzdys. Nagrinėkime kompleksinių skaičių kūną $\mathbf{C}$. Žinome, kad $\mathbf{C} = \mathbf{R}(i)$ ir polinomo x^2+1 šaknys yra i ir $-i$. Todėl, pagal Teoremą 2.2, grupėje $\mathrm{Gal}(F/K)$ yra tik du elementai. Nesunku patikrinti, kad funkcija $a + ib \to a - ib$ yra kūno $\mathbf{C}$ $\mathbf{R}$- automorfizmas, todėl $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) \approx \mathbf{Z}_2$, nes yra tik viena grupė, turinti du elementus.

Pavyzdys. Nagrinėkime $\mathbf{Q}\left(\sqrt{5}\right)$ kaip kūno $\mathbf{Q}$ plėtinį. Skaičiai $\sqrt{5}$ ir $-\sqrt{5}$ yra neredukuojamo polinomo $x^2 - 5 \in \mathbf{Q}[x]$ šaknys. Pagal Teoremą 2.2 grupėje $\mathrm{Gal}\left(\mathbf{Q}\left(\sqrt{5}\right)/\mathbf{Q}\right)$ *yra* tik 2 elementai. Nesunku patikrinti, kad funkcija $\sigma : \mathbf{Q}\left(\sqrt{5}\right) \to \mathbf{Q}\left(\sqrt{5}\right)$, $\sigma\left(a + \sqrt{5}b\right) = a - \sqrt{5}b$ yra netrivialusis kūno $\mathbf{Q}\left(\sqrt{5}\right)$ $\mathbf{Q}$- automorfizmas, todėl $\mathrm{Gal}(\mathbf{Q}\left(\sqrt{5}\right)/\mathbf{Q}) \approx \mathbf{Z}_2$, nes yra tik viena grupė, turinti du elementus.

Pavyzdys. Nagrinėkime $\mathbf{Q}\left(\sqrt[3]{5}\right)$. Skaičius $\sqrt[3]{5}$ yra vienintėlis realusis polinomo x^3-5 šaknis ir $\mathbf{Q} \subset \mathbf{Q}\left(\sqrt[3]{5}\right) \subset \mathbf{R}$. Pagal Teoremą 2.2 grupėje $\mathrm{Gal}\left(\mathbf{Q}\left(\sqrt[3]{5}\right)/\mathbf{Q}\right)$ yra tik vienas elementas.

Matome, kad kiekvienam kūno plėtiniui galima priskirti grupę. Norėtųsi žinoti, ką gali mums pasakyti Galua grupė apie patį plėtinį.

Mes matėme, kad kiekvienam kūno plėtiniui F/K galima priskirti grupę $\mathrm{Gal}(F/K)$. Nagrinėdami tarpinį kūną $K \subset E \subset F$, ką galima pasakyti apie ryšį tarp grupių $\mathrm{Gal}(F/E)$ ir $\mathrm{Gal}(F/K)$?

Teorema 2.3 *Tegu F/K yra kūno plėtinys. Tada*

1. Su kiekvienu tarpiniu kūnu E grupė $E' =$ $\mathrm{Gal}(F/E)$ *yra grupės* $\mathrm{Gal}(F/K)$

pogrupis.

2. Su kiekvienu grupės $\mathrm{Gal}(F/K)$ *pogrupiu* H *aibė*
$H' = \{v \in F | \sigma(v) = v$ su visais $\sigma \in H\}$ *yra tarpinis plėtinio* F/K *kūnas.*

Įrodymas. (1) Tegu E yra tarpinis kūnas. Tada
$\mathrm{Gal}(F/E) = \{\sigma \in \mathrm{Aut}(F) | \sigma(b) = b$ su visais $b \in E\} \subseteq$
$\{\sigma \in \mathrm{Aut}(F) | \sigma(a) = a$ su visais $a \in K\} = \mathrm{Gal}(F/K)$.
Taigi, $\mathrm{Gal}(F/E)$ yra $A(F)$ pogrupis, esantis grupėje $\mathrm{Gal}(F/K)$ ir $E' = \mathrm{Gal}(F/E)$ yra $\mathrm{Gal}(F/K)$ pogrupis, $E' = \mathrm{Gal}(F/E) < \mathrm{Gal}(F/K)$.
(2) Tegu $H < \mathrm{Gal}(F/K)$. Kadangi $K \subseteq H'$, tai H' yra netuščia, turinti 0 ir1. Tada su visais $u, v \in H'$ turime $\sigma(u - v) = \sigma(u) - \sigma(v) = u - v$ ir $\sigma(uv) = \sigma(u)\sigma(v) = uv$ su visais $\sigma \in H$. Taigi, $u - v$ ir uv priklauso H' ir todėl H' yra F požiedis. Beto, su visais $0 \neq u \in H'$ turime $\sigma(u^{-1}) = \sigma(u)^{-1} = u^{-1}$, taigi $u^{-1} \in H'$. Gavome, kad H' yra kūno F pokūnis, turintis K.
Įrodyta.

Jeigu H yra grupės $\mathrm{Gal}(F/K)$ pogrupis, tai H' vadinsime grupe H **apibrėžtu kūnu** kūne F. Taigi mes jau žinome, kaip kiekvienam tarpiniam kūnui E priskirti grupės $\mathrm{Gal}(F/K)$ pogrupį E' ir kaip kiekvienam grupės $\mathrm{Gal}(F/K)$ pogrupiui H priskirti tarpinį kūną H', esantį tarp F ir K. Norėtųsi žinoti, ar šie priskirimai apibrėžia abipus vienareikšmę atitiktį tarp plėtinio F/K tarpinių kūnų ir grupės $\mathrm{Gal}(F/K)$ pogrupių. Plėtinio $\mathbf{Q}\left(\sqrt[3]{5}\right)/\mathbf{Q}$ pavyzdys rodo, kad ne visada. Tada norėtųsi žinoti tas sąlygas kada taip yra.

Dabar pateiksime kūno plėtinio F/K ir šios atitikties pagrindinius teiginius, kurių įrodymą palieku skaitytojams.

Teiginiai:

1. $F' = \langle \mathrm{id}_F \rangle$.

2. $K' = \mathrm{Gal}(F/K)$.

3. $\langle \mathrm{id}_F \rangle = F$.

4. Jeigu L ir E yra tokie tarpiniai kūnai, kad $L \subseteq M$, tai $M' < L'$.

5. Jeigu H ir J yra tokie grupės $\mathrm{Gal}(F/K)$ pogrupiai, kad $H < J$, tai J' yra H' pokūnis.

6. Su kiekvienu tarpiniu kūnu L ir kiekvienu pogrupiu $H <\mathrm{Gal}(F/K)$ turime $L \subseteq (L')' = L''$ ir $H < (H')' = H''$.

7. Su kiekvienu tarpiniu kūnu L ir kiekvienu pogrupiu $H <\mathrm{Gal}(F/K)$ turime $L' = (L'')' = L'''$ ir $H' = (H'')' = H'''$.

Šiuos teiginius galime apibendrinti tokia diagrama:

$$
\begin{array}{lcc@{\qquad\qquad}cc}
F & \to & \langle \mathrm{id}_F \rangle & \mathrm{Gal}\,(F/K) & K \\
\cup & & \wedge & \vee & \cap \\
M & \to & M' & J & \to \; J' \\
\cup & & \wedge & \vee & \cap \\
L & \to & L' & H & \to \; H' \\
\cup & & \wedge & \vee & \cap \\
K & \to & \mathrm{Gal}\,(F/K) & \langle \mathrm{id}_F \rangle & \to \; F
\end{array}
$$

Pastebėsime, kad iš Teiginio 6 turime, kad su visais tarpiniais kūnais L teisinga $L \subseteq L''$ ir su kiekvienu pogrupiu $H <\mathrm{Gal}(F/K)$ teisinga $H < H''$. Tarpinį kūną L vadinsime **uždaru**, jeigu $L = L''$. Panašiai, pogrupį $H <\mathrm{Gal}(F/K)$ vadinsime **uždaru,** jeigu $H = H''$.

Teorema 2.4 *Tegu F/K yra kūno plėtinys. Egzistuoja abipus vienareikšmė atitiktis tarp uždarų tarpinių kūnų ir uždarų grupės $Gal(F/K)$ pogrupių: $E \to E' <Gal(F/K)$ su kiekvienu uždaru tarpiniu kūnu E.*

Įrodymas. Parodysime, kad ši atiktis yra injekcija. Tegu E ir L yra tokie du tarpiniai kūnai, kad $E' = L'$. Bet E ir L yra uždari, todėl $E = E'' = L'' = L$. Dabar parodysime, kad atitiktis yra siurjekcija. Su kievienu uždaru pogrupiu $H <\mathrm{Gal}(F/K)$ turime $H = H'' = (H')'$ ir todėl kūną H' atitinka pogrupis H.
Įrodyta.

Svarbu pastebėti, kad $\mathrm{Gal}(F/K)'$ nebūtinai sutampa su K ir gali būti didesnis už K. Kitaip sakant, kūnas K gali būti ir ne uždaras.

Apibrėžimas 2.5 Tegu F/K yra kūno plėtinys. Kūnas F vadinamas **Galua kūnu** virš K, jeigu $\mathrm{Gal}(F/K)' = K$. Šiuo atveju kūno plėtinys F/K yra vadinamas **Galua plėtiniu.**