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

9. Radikalinis plėtinys ir polinomo išsprendžiamumas radikalais

Šiame skyriuje mes įrodysime, kad polinomas virš nulinės charakteristikos kūno yra išsprendžiamas tada ir tik tada, kada jo Galua grupė yra išsprendžiama.

Apibrėžimas 9.1 *Kūno plėtinys F/K vadinamas **radikaliniu** K **plėtiniu**, jeigu egzistuoja tokie elementai $r_1, ..., r_m$, kad*

1. $F = K(r_1, ..., r_m)$ ir

2. Egzistuoja tokie teigiami sveiki skaičiai $n_1, ..., n_m$, kad $r_1^{n_1} \in K$ ir $r_i^{n_i} \in K(r_1, ..., r_{i-1})$.

*Polinomas $f(x) \in K[x]$ vadinamas **išsprendžiamu radikalais**, jeigu egzistuoja toks radikalinis plėtinys F/K, kad visos $f(x)$ šaknys yra kūne F.*

Taigi, polinomas $f(x) \in K[x]$ yra išsprendžiamas radikalais, jeigu egzistuoja tokia kūnų grandinė

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = F,$$

kad

(1) $K_i = K_{i-1}(r_i)$, čia $r_i^{n_i} \in F_{i-1}$, $n_i \in \mathbf{N}$ ir

(2) F yra polinomo $f(x)$ skaidinio kūnas.

Norint sukonstruoti radikalinį plėtinį, reikia nagrinėti dvinario $x^n - a \in K[x]$, čia $n \in \mathbf{N}, a \in K$, skaidinio kūną. Pradėsime atskiru atveju, dvinario $x^n - 1$ tyrimu. Šio dvinario šaknis vadina n -ojo laipsnio šaknimis iš 1. n -ojo laipsnio šaknis vadinama **primityviąja** n -ojo laipsnio šaknimi iš 1, jeigu jos eilė polinomo $x^n - 1$ skaidinio kūno multiplikacinėje grupėje yra lygi n.

Teiginys 9.2 *Tegu K yra kūnas, kurio charakteristika yra lygi 0, o F yra polinomo $x^n - 1$ skaidinio kūnas. Tada*

(1) Kūne F egzistuoja primityvioji n -ojo laipsnio šaknis iš 1.

(2) Jeigu ζ yra primityvioji n -ojo laipsnio šaknis iš 1, tai $F = K(\zeta)$.

(3) Gal(F/K) yra komutatyvi grupė.

(4) Jeigu $E \supseteq F$, tai su visais $a \in E$ polinomo $x^n - a \in E[x]$ Galua grupė yra ciklinė ir jos eilė yra n daliklis.

Įrodymas. (1) Polinomas $x^n - 1$ yra separabilus, nes $(x^n - 1)' = nx^{n-1}$ ir $\mathrm{BDD}(x^n - 1, nx^{n-1}) = 1$, ir todėl kūne F yra n skirtingų n -ojo laipsnio šaknų iš 1. Visos n -ojo laipsnio šaknys iš 1 sudaro $F^\times$ baigtinį pogrupį C ir šis pogrupis yra ciklinis. Kievienas generuojantis šią grupę elementas ir yra primityvioji n -ojo laipsnio šaknis iš 1.

(2) Visos n -ojo laipsnio šaknys iš 1 yra ζ laipsniai, todėl $F = K(C) = K(\zeta)$.

(3) Parodysime, kad funkcija $\Psi : \mathrm{Gal}(F/K) \to \mathbf{Z}_n^\times$, $\Psi(\sigma) = j \bmod n$, jeigu $\sigma(\zeta) = \zeta^j$, yra injektyvus homomorfizmas , t.y. Gal(F/K) yra komutatyvios grupės pogrupis ir todėl irgi yra komutatyvi grupė. Jeigu ζ yra primityvioji n -ojo laipsnio šaknis iš 1, tai likusios primityviosios n -ojo laipsnio šaknys iš 1 yra ζ^j, kai $\mathrm{BDD}(j, n) = 1$. Elementas $\sigma(\zeta)$ su visais $\sigma \in \mathrm{Aut}(F) \supset \mathrm{Gal}(F/K)$ yra primityvioji n -ojo laipsnio šaknis iš 1, tai jis yra lygus ζ^j su tokiu j, kad $\mathrm{BDD}(j, n) = 1$. Taigi, funkcija $\Psi(\sigma) = j \bmod n$ yra injekcija, nes $F = K(\zeta)$. Ši funkcija yra homomorfizmas, nepriklausantis nuo primityvaus elemento pasirinkimo(patikrinti paliekame skaitytojui).

(4) Tegu r yra polinomo $x^n - a$ šaknis šio polinomo skaidinio kūne virš E. Tegu $\zeta \in E$ yra primityvioji n -ojo laipsnio šaknis iš 1. Tada nesunku patikrinti, kad aibė $\{r, r\zeta, ..., r\zeta^{n-1}\} \subseteq E$ yra visų skirtingų polinomo šaknų aibė. Gavome, kad polinomo $x^n - a$ skaidinio kūnas yra $E(r)$ ir visi $\sigma \in \mathrm{Gal}(E(r)/E)$ yra visiškai apibrėžti savo reikšme $\sigma(r)$. Tegu $\sigma_1 \in \mathrm{Gal}(E(r)/E)$ apibrėžtas formule $\sigma_1(r) =$

$r\zeta$. Tada Gal$(E(r)/E) = \langle\sigma_1\rangle$ ir $\sigma_1^n = 1$.

Įrodyta.

Teiginys 9.3 *Tegu K yra nulinės charakteristikos kūnas ir E/K yra radikalinis plėtinys. Tada egzistuoja toks tarpinis kūnas $E \supseteq F \supseteq K$, kad F/K yra normalusis radikalinis plėtinys.*

Įrodymas. Tegu E/K yra radikalinis plėtinys $r_1, ..., r_m \in E$ ir $n_1, ..., n_m \in \mathbf{N}$ yra tokie elementai, kad (1) $E = K(r_1, ..., r_n)$ ir (2) $r_i^{n_i} \in K(r_1, ..., r_{i-1})$ su $1 \leq i \leq m$. Tegu f_i yra elemento r_i minimalusis polinomas virš K ($1 \leq i \leq m$) ir $f = f_1 \cdots f_m$. Polinomas f yra separabilus ir pagal Teoremą 6.7 polinomo f skaidinio kūnas F yra normalusis plėtinys. Iš Fundamentaliosios Teoremos II dalies įrodymo žinome, kad kiekviena polinomo f šaknis yra reiškiama $\sigma(r_i)$, čia $1 \leq i \leq m$ ir $\sigma \in$Gal(F/K). Iš čia su visais $\sigma \in$Gal(F/K) ir visais $1 \leq i \leq m$ turime, kad $\sigma(r_i) \in K(\sigma(r_1), ..., \sigma(r_{i-1}))$. Taigi, jeigu Gal$(F/K) = \{\sigma_1, ..., \sigma_k\}$, tai $F = K(\{\sigma_j(r_i) | 1 \leq i \leq m, 1 \leq j \leq k\})$ yra normalusis radikalinis plėtinys.

Įrodyta.

Dabar mes jau pasiruošę pagrindinio skyriaus teiginio įrodymui.

Teorema 9.4 *Tegu K yra nulinės charakteristikos kūnas. Teigiamo laipsnio polinomas $f \in K[x]$ yra išsprendžiamas radikalais tada ir tik tada, kada yra išsprendžiama polinomo f Galua grupė.*

Įrodymas. Mes įrodysime tik tokį teiginį: *jeigu teigiamo laipsnio polinomas $f \in K[x]$ yra išsprendžiamas radikalais tai yra išsprendžiama ir polinomo f Galua grupė.*

Tegu E/K yra radikalinis kūno plėtinys ir polinomo f skaidinio kūnas F yra tarpinis kūnas: $E \supseteq F \supseteq K$. Iš Teiginio 9.3 galime tarti, kad E yra normalusis radikalinis plėtinys. Tegu $r_1, ..., r_m \in E$ ir $n_1, ..., n_m \in \mathbf{N}$ yra tokie elementai, kad (1) $E = K(r_1, ..., r_n)$ ir (2) $r_i^{n_i} \in K(r_1, ..., r_{i-1})$ su $1 \leq i \leq m$. Tegu $n =$ MBK$(n_1, ..., n_m)$ ir ζ yra primityvioji n - ojo laipsnio šaknis iš 1 virš K. Tada $\zeta^{\frac{n}{n_i}} \in K(\zeta)$ yra primityvioji n_i - ojo laipsnio šaknis iš 1. Turime, kad plėtinys $E(\zeta)/K(\zeta)$ yra normalusis radikalinis plėtinys ir $E(\zeta)/K$ yra Galua plėtinys (Teorema 6.7). Iš Fundamentaliosios teoremos II dalies, žinodami, kad F/K yra Galua plėtinys (Teorema 6.7), turime, kad Gal(F/K) yra grupės Gal$(E(\zeta)/K)$ faktorgrupė. Taigi, gavę tai, kad Gal$(E(\zeta)/K)$ yra išsprendžiama, pagal Teoremą

8.9 turėtume, kad ir grupė Gal(F/K) yra išsprendžiama ir tuo pačiu įrodytume mūsų teiginį.

Tegu su visais $1 \leq i \leq m$, $F_i = K(r_1, ..., r_i)$. Mes parodysime kaip sukonstruoti grupei $G =$Gal$(E(\zeta)/K)$ normaliąją pogrupių grandinę. Kūnas $F_0 = K(\zeta)$ yra seprabilaus polinomo $x^n - 1 \in K[x]$ skaidinio kūnas, todėl pagal Fundamentaliosios teoremos II dalį $N_0 =$Gal$(E(\zeta)/K(\zeta))$ normalusis grupės G pogrupis ir $G/N_0 \approx$Gal$(K(\zeta)/K)$ yra komutatyvi grupė pagal Teiginį 9.2 (3). Su visais $1 \leq i \leq m$ kūne F_{i-1} yra visos n_i - ojo laipsnio šaknys iš 1 ir F_i yra polinomo $x^{n_i} - r_i^{n_i}$ skaidinio kūnas ir todėl plėtinys F_i/F_{i-1} yra Galua plėtinys. Pagal Fundamentaliosios teoremos II dalį $N_i =$Gal$(E(\zeta)/F_i)$ yra normalusis grupės $N_{i-1} =$Gal$(E(\zeta)/F_{i-1})$ pogrupis ir $N_{i-1}/N_i \approx$Gal(F_i/F_{i-1}). Pagal Teoremą 9.2 (4) grupė Gal(F_i/F_{i-1}) yra ciklinė ir todėl komutatyvi. Visą konstrukciją pavaizduosime lentele:

$$
\begin{array}{ccccc}
K = & K \subset & K(r_1) \subset \cdots & \subset K(r_1, ..., r_m) = & E \\
\| & & & & \cap \\
K \subset & K(\zeta) \subset & K(\zeta, r_1) \subset \cdots & \subset K(\zeta, r_1, ..., r_m) = & E(\zeta) \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\
K' & (K(\zeta))' & (K(\zeta, r_1))' \cdots & (K(\zeta, r_1, ..., r_m))' & (E(\zeta))' \\
 & \overset{\|}{F_0} & \overset{\|}{F_1} & \overset{\|}{F_m} & \\
\| & \| & \| & \| & \| \\
G \rhd & N_0 \rhd & N_1 \rhd \cdots & \rhd N_m = & \left\langle \mathrm{id}_{E(\zeta)} \right\rangle
\end{array}
$$

Gavome, kad

$$G \rhd N_0 \rhd N_1 \rhd \cdots \rhd N_m = \left\langle \mathrm{id}_{E(\zeta)} \right\rangle$$

yra normalioji grupės G pogrupių grandinė. Taigi, $G =$Gal$(E(\zeta)/K)$ ir, tuo pačiu, grupė Gal(F/K) yra išsprendžiamos.

Įrodyta.