KŪNŲ TEORIJA

2000 metų rudens paskaitos

1. Kūnų plėtiniai

2. Galua grupės

3. Polinomų Galua grupės

Kaip ir Galua domėjosi polinomų šaknų radimu, taip ir mes paklausime, kokiuose kūnuose polinomas įgyja šaknis. Antrame skyriuje mes nagrinėjome kūno plėtinius, gautus prijungiant neredukuojamo polinomo šaknį(visi šie plėtiniai yra paprastieji). Dabar mes apibendrinsim šaknies prijungimo veiksmą ir kalbėsime apie apie polinomo šaknų prijungimą, t.y. kalbėsime apie algebrinius plėtinius gaunamus paprastųjų plėtinių pagrindu.

Apibrėžimas *3.1 Tegu K yra kūnas ir polinomo $f(x) \in K[x]$ laipsnis yra n. Kūno plėtinys F/K vadinamas polinomo f skaidymo kūnu virš K, jeidu egzistuoja tokie elementai $r_1, ..., r_n \in F$, kad $f(x) = a(x - r_1)\cdots(x - r_n)$ su $a \in K$ ir $F = K(r_1, ..., r_n)$.*

Teorema 3.2 *Tegu polinomo $f \in K[x]$ laipsnis yra $n > 0$. Tada egzistuoja polinomo f skaidymo kūnas F virš K ir $[F : K] \leq n!$.*

Įrodymas. Indukcija pagal n. Jeigu $n = 1$, tai pats kūnas K yra polinomo f skaidymo kūnas virš K. Tegu teorema yra teisinga su visais kūnais $L \supset K$ ir su bet kokiu polinomu $g \in L[x]$, kurio laipsnis yra mažesnis už n. Tegu dabar $p \in K[x]$ yra polinomo f neredukuojamas daliklis ir r_1 yra polinomo p šaknis. Tada f kaip polinomas iš $K(r_1)[x]$ turi šaknį kūne $K(r_1)$ ir $f = (x - r_1)g$ su $g \in K(r_1)[x]$ ir $\deg g = n-1$. Tada pagal indukcijos prielaidą egzistuoja toks polinomo g skaidymo kūnas $F/K(r_1)$ virš $K(r_1)$, kad $[F : K(r_1)] \leq (n-1)!$. Tada nesunku patikrinti(ir tai paliekame padaryti skaitytojams), kad F yra polinomo f skaidymo kūnas. Beto, pagal Teoremas 1.8 ir 1.5 turime, kad $[F : K] = [F : K(r_1)][K(r_1) : K] \leq (n-1)!n = n!$.

Įrodyta.

Pastebėsime, kad $K(r_1,...,r_n) = K(r_1)(r_2)\cdots(r_n)$ ir todėl pagal Teoremą 1.6 polinomo f skaidymo kūnas yra vienintėlis izomorfizmo atžvilgiu.

Apibrėžimas 3.3 Tegu polinomo $f \in K[x]$ laipsnis yra $n > 0$, o $F-$ polinomo f skaidymo kūnas. Grupė $\mathrm{Gal}(F/K)$ vadinama **polinomo f Galua grupe** virš K.

Pavyzdys. Žinome, kad kompleksinių skaičių kūnas $\mathbf{C}$ yra polinomo x^2+1 skaidymo kūnas virš $\mathbf{R}$, todėl polinomo x^2+1 Galua grupė virš $\mathbf{R}$ yra izomorfinė dviejų elementų grupei $\mathbf{Z}_2$. Aišku, kad ir polinomo x^2+5 Galua grupė virš $\mathbf{Q}$ yra izomorfinė $\mathbf{Z}_2$.

Pavyzdys. Nagrinėkime dabar polinomą $f = x^3+5x^2+x+5$ virš baigtinio kūno $GF_{(3)}$. Tada $f = x^3-1 = (x-1)(x^2+1)$ virš $GF_{(3)}$. Iš polinomo f skaidinio matome, kad polinomo f skaidymo kūnas virš $GF_{(3)}$ sutampa su neredukuojamo virš $GF_{(3)}$ polinomo $p = x^2+1$ skaidymo kūnu. Tegu u yra polinomo p šaknis, esanti kūno $GF_{(3)}$ plėtinyje. Tada $GF_{(3)}(u)$ yra polinomo p skaidymo kūnas, nes $p = (x-u)(x-u') \in GF_{(3)}(u)[x]$, čia $u' \in GF_{(3)}(u)$. (Tai teisinga, nes polinomas yra įverčio homomorfizmo $\phi_u : GF_{(3)}(u)[x] \to GF_{(3)}(u)$ branduolyje ir todėl dalijasi iš branduolį $\ker\phi_u$ generuojančio polinomo $x-u$). Taigi, $\left[GF_{(3)}(u) : GF_{(3)}\right] = 2$ ir todėl grupėje $\mathrm{Gal}\Big(GF_{(3)}(u)/GF_{(3)}\Big)$ yra tik du elementai ir todėl $\mathrm{Gal}\Big(GF_{(3)}(u)/GF_{(3)}\Big) \approx \mathbf{Z}_2$.

Prieš pateikiant sudėtingesnį pavyzdį, įrodysime lemą.

Lema 3.4 *Tegu F/K yra baigtinio matavimo plėtinys ir $L \subseteq E$ yra tarpiniai kūnai. Tada $[L' : E'] \leq [E : L]$ ir, atskiru atveju, $|\mathrm{Gal}(F/K)| \leq [F : K]$.*

Įrodymas. Indukcija pagal $n = [E : L]$. Teiginys akivaizdus, kai $n = 1$. Tegu dabar $n > 1$ ir su visais $j < n$ lemos teiginys yra teisingas. Parinkime $u \in E$ taip, kad $u \notin L$. Kadangi $[E : L] < \infty$, tai u yra algebrinis virš L (Teorema 1.7) ir u minimaliojo polinomo $p \in L[x]$ laipsnis yra $k > 1$. Pagal Teoremas 1.5 ir 1.8 turime $[L(u) : L] = k$ ir $[E : L(u)] = \frac{n}{k}$.

Jeigu $k < n$, tai $1 < \frac{n}{k} < n$ ir pagal indukciją $[L' : E'] = \left[L' : L(u)'\right]\left[L(u)' : E'\right] \leq k \cdot \frac{n}{k} = n = [E : L]$. Gavome ko siekėme.

Tegu dabar $k = n$, taigi, $E = L(u)$. Lemos teiginiui įrodyti mums pakanka sukonstruoti injektyvią funkciją tarp grupės L' pogrupio E' kairiųjų sluoksnių aibės S ir elemento u minimalaus polinomo $p \in L[x]$ skirtingų šaknų aibės T. (Aibėje T yra ne daugiau kaip n elementų, nes $\deg(p) = n$.)

Tegu $\tau E'$ yra kairysis sluoksnis pogrupio $E' \leq L'$ atžvilgiu. Apibrėžkime funkciją $\psi : S \to T$ formule $\psi(\tau E') = \tau(u)$. Ši funkcija apibrėžta korektiškai, nes iš $\tau E' = \sigma E'$ turime $\sigma = \tau\rho$, čia $\rho \in E'$. Todėl $\sigma(u) = \tau\rho(u) = \tau(u)$, nes iš to, kad $u \in E$ teisinga $\rho(u) = u$. Parodysime, kad ψ yra injekcija. Tegu $\tau(u) = \sigma(u)$. Pagal Teoremą 1.5 su kiekvienu $w \in E$ turime, kad $w = \sum_{i=0}^{n-1} a_i u^i$, čia $a_0, ..., a_{n-1} \in L$. Tada $\sigma^{-1}\tau(w) = \sum_{i=0}^{n-1} a_i \sigma^{-1}\tau(u)^i = \sum_{i=0}^{n-1} a_i u^i = w$, taigi $\sigma^{-1}\tau \in E'$. Gavome, kad ψ yra injentyvi funkcija ir todėl $[L' : E'] = |S| \leq |T| \leq n = [E : L]$.

Jeigu, pagaliau, $L = K$ ir $E = F$, tai turime $|\mathrm{Gal}(F/K)| \leq [F : K]$.

Įrodyta.

Dabar išnagrinėsime tokį pavyzdį.

Pavyzdys. Pateiksime polinomo $f = x^3 - 5 \in \mathbf{Q}[x]$ skaidymo kūną ir Galua grupę. Kūne $\mathbf{Q}\left(\sqrt[3]{5}\right)$ yra polinomo f šaknis, bet šis kūnas nėra polinomo f skaidymo kūnas, nes jame tik viena polinomo f šaknis. Polinomų žiede $\mathbf{Q}\left(\sqrt[3]{5}\right)[x]$ turime $f = \left(x - \sqrt[3]{5}\right)\left(x^2 + \sqrt[3]{5}x + \sqrt[3]{25}\right)$ ir kvadratinis trinaris $x^2 + \sqrt[3]{5}x + \sqrt[3]{25}$ yra needukuojamas virš $\mathbf{Q}\left(\sqrt[3]{5}\right)$. Tegu $\zeta = \left(-1 + i\sqrt{3}\right)\frac{\sqrt[3]{5}}{2}$. Skaičius ζ yra polinomo f šaknis virš $\mathbf{Q}$, taigi, ζ yra polinomo $x^2 + \sqrt[3]{5}x + \sqrt[3]{25}$ šaknis virš $\mathbf{Q}\left(\sqrt[3]{5}\right)$. Dabar aišku, kad $F = \mathbf{Q}\left(\sqrt[3]{5}, \zeta\right)$ yra polinomo $x^3 - 5$ skaidymo kūnas virš $\mathbf{Q}$. Toliau, pagal Teoremas 1.8 ir 1.5, turime $[F : \mathbf{Q}] = \left[\mathbf{Q}\left(\sqrt[3]{5}, \zeta\right) : \mathbf{Q}\left(\sqrt[3]{5}\right)\right]\left[\mathbf{Q}\left(\sqrt[3]{5}\right) : \mathbf{Q}\right] = 2 \cdot 3 = 3!$

Dabar rasime polinomo f Galua grupę. Pagal Teoremą 2.2 šios Galua grupės elementai yra polinomo f šaknų $\sqrt[3]{5}, \zeta, \bar{\zeta}$, čia $\bar{\zeta}$ - kompleksinio skaičiaus ζ jungtinis, keitiniai. Tegu grupės $\mathrm{Gal}(F/K)$ elementas τ kompleksiniam skaičiui priskiria jo jungtinį, o elementas σ cikliškai perstato polinomo šaknis: $\sigma\left(\sqrt[3]{5}\right) = \zeta, \sigma(\zeta) = \bar{\zeta}, \sigma\left(\bar{\zeta}\right) = \sqrt[3]{5}$ ir su visais $q \in \mathbf{Q}$ turime $\sigma(q) = q$. Nesunku patikrinti(tai paliekame atlikti skaitytojui), kad σ yra automorfizmas. Automorfizmo σ eilė yra 3, o automorfizmo τ eilė yra 2. Toliau, $\sigma\tau(\zeta) = \sqrt[3]{5}$, bet $\tau\sigma(\zeta) = \zeta$. Gavome, kad grupė $\mathrm{Gal}(F/\mathbf{Q})$ yra nekomutatyvi ir pagaliau pagal Lemą 3.4 turime, kad $|\mathrm{Gal}(F/\mathbf{Q})| \leq 6$. Vienintėlė nekomutatyvi grupė, kurios eilė neviršija 6 yra keitinių grupė S_3. Taigi, $\mathrm{Gal}(F/\mathbf{Q}) \approx S_3$. Iš tikrųjų, grupėje yra 6 elementai: $\mathrm{id}_{\mathrm{Gal}(F/K)}, \tau,\ \sigma,\ \tau\cdot\sigma, \sigma\cdot\tau$ ir $\sigma\cdot\sigma$. Izomorfizmą apibrėžime priskirimu ψ : $\psi\left(\mathrm{id}_{\mathrm{Gal}(F/K)}\right) = \mathrm{id}_{S_3} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\psi(\tau) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$, $\psi(\sigma) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$, $\psi(\tau\cdot\sigma) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$, $\psi(\sigma\cdot\tau) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$, $\psi(\sigma\cdot\sigma) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$.

Norint įsitikinti, kad tai izomorfizmas, pakanka palyginti veiksmų lenteles šiose grupėse:

grupėje $\mathrm{Gal}(F/\mathbf{Q})$:

$\cdot$	id	τ	σ	$\tau\sigma$	$\sigma\tau$	σ^2
id	id	τ	σ	$\tau\sigma$	$\sigma\tau$	σ^2
τ	τ	id	$\tau\sigma$	σ	σ^2	$\sigma\tau$
σ	σ	$\sigma\tau$	σ^2	τ	$\tau\sigma$	id
$\tau\sigma$	$\tau\sigma$	σ^2	$\sigma\tau$	id	σ	τ
$\sigma\tau$	$\sigma\tau$	σ	τ	σ^2	id	$\tau\sigma$
σ^2	σ^2	$\tau\sigma$	id	$\sigma\tau$	τ	σ

ir grupėje S_3 :

$\circ$	id	(12)	(123)	(23)	(13)	(132)
id	id	(12)	(123)	(23)	(13)	(132)
(12)	(12)	id	(23)	(123)	(132)	(13)
(123)	(123)	(13)	(132)	(12)	(23)	id
(23)	(23)	(132)	(13)	id	(123)	(12)
(13)	(13)	(123)	(12)	(132)	id	(23)
(132)	(132)	(23)	id	(13)	(12)	(123)

.