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

Praeitame skyriuje mes matėme, kad baigtinio matavimo Galua plėtinys yra separabilusis ir normalusis plėtinys (Išvada 5.6). Dabar įrodysime, kad teisingas ir atvirkščias teiginys.

Visų pirma mes įsitikinsime tuo, kad ne visi neredukuojami polinomai yra separabilieji. Pradėsime apibrėžimu.

Apibrėžimas 6.1 Tegu K yra kūnas. Mažiausias kūno K pokūnis vadinamas **pirminiu K pokūniu.** Jeigu pirminio K pokūnio elementų skaičius yra pirminis skaičius p, tai sakome, kad **kūno K charakteristika** yra lygi p , o jeigu pirminiame K pokūnyje yra begalinis elementų skaičius, tai sakome, kad kūno K **charakteristika yra lygi nuliui**.

Pastebėsime, kad kūno K pirminis pokūnis yra izomorfinis arba baigtiniam kūnui $\mathrm{GF}(p)$, jeigu kūno K charakteristika yra lygi pirminiam skaičiui p, arba racionaliųjų skaičių kūnui $\mathbf{Q}$, jeigu kūno K charakteristika yra lygi 0. Jeigu kūno K charakteristika yra p, tai $0 = pa = \underbrace{a + \cdots + a}_{p \text{ kartų}}$ su visais $a \in K$. Kita kūno K, kurio charakteristika yra p, aritmetikos įtatybė pasireiškia lygybėje $(a+b)^p = a^p + b^p$ su visais $a, b \in K$, nes visi binominiai koeficientai išskyrus pirmąjį ir paskutinįjį dalijasi iš p.(Dėl tos pačios priežasties yra teisinga ir lygybė $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ su visais $a, b \in K$ ir $n \in \mathbf{N}$). Iš čia turime, kad virš kūno K, kurio charakteristika

yra p, polinomas $x^p + 1 = (x+1)^p$ nėra neruduokajamas.

Apibrėžimas 6.2 *Tegu* $f \in K[x]$, $f(x) = \sum_{i=1}^{n} a_i x^i$. *Polinomo* $f(x)$ **išvestine** $f'(x)$ *vadiname polinomą*

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1},$$

čia $ia_i = \underbrace{a_i + \cdots + a_i}_{i \text{ kartų}}$.

Šis išvestinės apibrėžimas realiems polinomas sutampa su įprastu išvestinės apibrėžimu, naudojančiu ribos savoką. Bet baigtiniuose kūnuose ribos savokos nėra, todėl ir prireikė formalaus išvestinės apibrėžimo. Tai leidžia suformuluoti polinomo separabilumo sąlygą.

Teiginys 6.3 *Tegu* $f(x)$ *yra neredukuojamas polinomas virš kūno* K. *Tada šios 4 sąlygos yra ekvivalenčios:*

(1) *polinomas* f *turi nors vieną kartotinę šaknį (skaidinio kūne);*

(2) $\mathrm{BDD}(f, f') \neq 1$;

(3) *kūno* K *charakteristika* $p \neq 0$ *ir* $f(x) = g(x^p)$, *čia* $g(x) \in K[x]$;

(4) *visos polinomo šaknys yra kartotinės.*

Įrodymas. Tegu F yra polinomo f skaidinio kūnas.

$(1) \Rightarrow (2)$. Tegu r yra polinomo $f(x)$ kartotinė šaknis: $f(x) = (x-r)^2 g(x)$, čia $g(x) \in F[x]$. Tada viena išvestinės $f'(x) = 2(x-r)g(x) + (x-r)^2 g'(x) = (x-r)(2g(x) + (x-r)g'(x))$ šaknimi yra $r : f'(r) = 0$ ir todėl $\mathrm{BDD}(f, f') \neq 1$.

$(2) \Rightarrow (3)$. Kadangi f yra neredukuojamas polinomas, o $\deg(f') < \deg(f)$ ir $\mathrm{BDD}(f, f') \neq 1$, tai $f'(x) \equiv 0$. Bet tai neįmanoma virš nulinės charakteristikos kūno, todėl $\mathrm{char}\, K = p > 0$ ir todėl $f(x) = \sum_{i=0}^{n} a_{ip} x^{ip} = g(x^p)$, čia $g \in K[x]$.

$(3) \Rightarrow (4)$. Tegu $f(x) = g(x^p)$ ir tegu $g(x) = (x-a_1)^{m_1} \cdots (x-a_s)^{m_s}$ kūne F. Tada

$$f(x) = g(x^p) = (x^p - a_1)^{m_1} \cdots (x^p - a_s)^{m_s} = (x-a_1)^{pm_1} \cdots (x-a_s)^{pm_s},$$

čia $a_i^p = a_i$, $\mathrm{char}\, F = p$. Gavome, kad kiekvienos polinomo f šaknies kartotinumas ne mažesnis už p.

$(4) \Rightarrow (1)$. Akivaizdu (aš tikiuosi).
Įrodyta.

Išvada 6.4 *Neredukuojamas polinomas virš kūno, kurio charakteristika yra lygi* 0, *yra separabilus.*

Paskutinioji išvada mums sako, kad *polinomo virš nulinės charakteristikos kūno skaidinio kūnas yra Galua plėtinys.* Tai teisinga ir polinomams virš baigtinių kūnų(žr.:C. Paskaita apie neredukuojamus polinomus virš baigtinių kūnų). Tačiau tai nėra teisinga begaliniams kūnams, kurių charakteristika yra lygi p.

Pavyzdys. Tegu kūno K charakteristika yra lygi p (pavyzdžiui, GF(p)) ir tegu u yra transcendentinis elementas virš K. Tada racionaliųjų funkcijų kūno $K(u)$ charakteristika yra lygi p ir polinomas $x^p - u$ yra neredukuojamas žiede $(K(u))[x]$, bet $x^p - u = (x-r)^p$ virš polinomo $x^p - u$ skaidinio kūno, čia $r-$ polinomo šaknis. Gavome, kad neredukuojamas polinomas gali turėti kartotines šaknis, tiesa, tik virš begalinių baigtinės charakteristikos kūnų.

Grįžkime prie Išvados 5.6 atvirkščio teiginio įrodymo. Iš pradžių pastebėsime, kad kiekvienas kūnų izomorfizmas $\sigma : K \to L$ generuoja žiedų izomorfizmą $\sigma_x : K[x] \to L[x]$, čia $\sigma_x\left(\sum\limits_{i=0}^{n} a_i x^i\right) = \sum\limits_{i=0}^{n} \sigma(a_i) x^i$ (skaitytojui paliekame įrodyti, kad tai yra žiedų izomorfizmas).

Teorema 6.6 *Tegu $\sigma : K \to L$ yra kūnų izomorfizmas ir tegu $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in K[x]$ yra separabilus $n-$ojo laipsnio polinomas($n > 0$). Jeigu F yra polinomo f skaidinio kūnas virš K, o E yra polinomo $\sigma_x(f) = \sum\limits_{i=0}^{n} \sigma(a_i) x^i$ skaidinio kūnas virš L, tai egzistuoja lygiai $[F:K]$ izomorfizmą σ generuojančių izomorfizmų $\bar{\sigma} : F \to E$* (izomorfizmas σ generuoja izomorfizmą $\bar{\sigma}$, jeigu $\bar{\sigma}(a) = \sigma(a)$ su visais $a \in K$).

Įrodymas. Įrodysime indukcija pagal $m = [F:K]$. Jeigu $m = 1$, tai $F = K$ ir todėl polinomo f skaidinio kūnu yra K, o polinomo $\sigma_x(f)$ skaidinio kūnu yra L, taigi, $E = L$. Turime, kad tada $\bar{\sigma} = \sigma$. Tegu dabar teorema yra teisinga su visais kūnais K ir visais polinomais $h(x) \in K[x]$, kurių skaidinio kūno laipsnis virš K yra mažesnis už m. Tegu $[F:K] = m > 1$ ir g yra polinomo f nereduojamas

daugiklis, kurio laipsnis yra $d > 1$. . Polinomas $\sigma_x(g)$ yra nereduokuojamas virš L , nes σ_x yra izomorfizmas. Mes galime apibrėžti žiedų homomorfizmų kompoziciją

$$K[x] \xrightarrow{\sigma_x} L[x] \xrightarrow{\pi} L[x] / \langle \sigma_x(g) \rangle$$

kurios branduolys $\ker \pi\sigma_x = \langle g \rangle$. Tegu $u \in F$ yra polinomo g šaknis, o $v \in E$ kuri nors polinomo $\sigma_x(g)$ šaknis. Parašykime homomorfizų teoremą žiedams diagrama

$$\begin{array}{ccc} K[x] & \xrightarrow{\pi\sigma_x} & L[x] / \langle \sigma_x(g) \rangle \\ & {\scriptstyle \pi'} \searrow \quad \nearrow {\scriptstyle \overline{\pi\sigma_x}} & \\ & K[x] / \langle g \rangle & \end{array}$$

čia $\overline{\pi\sigma_x}$– kūnų izomorfizmas. tada pagal Teoremą 1.5 turime

$$K(u) \approx K[x] / \langle g \rangle \approx L[x] / \langle \sigma_x(g) \rangle \approx L(v).$$

Tegu $v_1, ..., v_d$ yra visos polinomo $\sigma_x(g)$ šaknys. Tada pagal Teoremą 1.6 egzistuoja lygiai d tokių kūnų izomorfizmų $\tau_j : K(u) \to L(v_j)$, kad σ generuoja τ_j ir $\tau_j(u) = v_j$. Iš Teoremos 1.5 turime, kad $[K(u) : K] = d > 1$. Tada pagal Teoremą 1.8 gauname, kad $[F : K(u)] = \frac{[F:K]}{[K(u):K]} = \frac{m}{d} < m$. Turime, kad kūnas F yra polinomo f skaidinio kūnas virš $K(u)$ ir su visais $1 \leq j \leq d$ kūnas E yra polinomo $\sigma_x(f)$ skaidinio kūnas virš $L(v_j)$. Pagal indukcijos prielaidą turime, kad su visais $1 \leq j \leq d$ egzistuoja lygiai $\frac{m}{d} = [F : K(u)]$ izomorfizmų $\omega : F \to E$, kuriuos generuoja τ_j. Iš čia turime, kad egzistuoja lygiai $d \cdot \frac{m}{d} = m = [F : K]$ izomorfizmų, kuriuos generuoja σ.

Įrodyta.

Dabar įrodysime norimą teoremą.

Teorema 6.7 *Tegu F/K yra kūno plėtinys. Tada teiginiai yra ekvivalentūs:*
(1) *F/K yra baigtinis Galua plėtinys.*
(2) *F/K yra baigtinis, normalusis, separabilusis plėtinys.*
(3) *F yra separabilaus polinomo skaidinio kūnas virš K.*

Įrodymas. (1) $\Rightarrow$ (2) : tai Išvada 5.6.
(2) $\Rightarrow$ (3) : Tegu $\{v_1, ..., v_n\}$ yra kūno F bazė virš K (plėtinys F/K yra baigtinis). Tegu $f_i \in K[x]$ yra minimalusis v_i polinomas virš K , čia $1 \leq i \leq n$.

Plėtinys F/K yra separabilusis, todėl visi f_i yra separabilūs virš K. Plėtinys F/K yra normalusis, todėl F yra separabilaus polinomo $f = f_1 \cdots f_n$ skaidinio kūnas, nes visos polinomų f_i šaknys, o taip pat ir polinomo f šaknys, yra kūne F.

(3) $\Rightarrow$ (1) : Tegu F yra separabilaus polinomo $f \in K[x]$ skaidinio kūnu. Tegu $G = \mathrm{Gal}(F/K)$. Tada $G = \mathrm{Gal}(F/K'')$, nes F yra taip pat ir polinomo f, kaip polinomo virš K'', skaidinio kūnas. Tada pagal Teoremą 6.6 turime

$$[F : K] = |\mathrm{Gal}(F/K)| = |\mathrm{Gal}(F/K'')| = [F : K''].$$

Gavome, kad $K = K''$ ir todėl F/K yra baigtinis Galua plėtinys.
Įrodyta.

Taigi, nuo šiol į baigtinį Galua plėtinį galima žiūrėti kaip į separabilaus polinomo skaidinio kūną.