16. VIENETO ŠAKNYS IR PRIMITYVIEJI KŪNO ELEMENTAI

Šiame skyrelyje mus domins polinomo $x^n - 1$ faktorizacija virš baigtinio kūno $GF(q)$. Taip pat pateiksime vieneto šaknų, nagrinėtų kompleksinių skaičių teorijoje, apibendrinimą baigtiniuose kūnuose.

12.1 apibrėžimas. *Tegu polinomo $x^n - 1 \in GF(q)[x]$ skaidinio kūnas yra $GF(q^s)$. Šis kūnas vadinamas n-ciklotominiu kūnu virš kūno $GF(q)$. Polinomo $x^n - 1$ šaknys šiame n-ciklotominiame kūne $GF(q^s)$ yra vadinamos n-ojo laipsnio vieneto šaknimis virš kūno $GF(q)$. Šių vieneto šaknų aibę žymėsime E_n.*

Prisiminkime, kad panašiai buvo apibrėžtos ir kompleksinės n-ojo laipsnio vieneto šaknys. Nagrinėdami polinomą $x^n - 1$ virš racionaliųjų skaičių kūno $\mathbb{Q}$, vieneto šaknimis vadinome polinomo $x^n - 1$ šaknis, esančias šio polinomo skaidinio kūne virš $\mathbb{Q}$. Šis skaidinio kūnas yra tam tikras kompleksinių skaičių kūno $\mathbb{C}$ pokūnis. Vaizdi yra šių vieneto šaknų geometrinė interpretacija: tai taisyklingojo n-kampio, įbrėžto į vienetinį apskritimą, kurio centras yra kompleksinės plokštumos koordinačių pradžioje, viršūnės.

Baigtinio kūno atveju vieneto šaknų aibės E_n struktūrą nusako toks teiginys:

12.2 teiginys. *Tegu $n \in \mathbb{N}$ ir kūno $GF(q)$ charakteristika yra lygi p. Tada:*

1. Jeigu DBD $(n, p) = 1$, *tai vieneto šaknų aibė E_n yra n-osios eilės ciklinis multiplikacinės kūno $GF(q^s)$ grupės $GF(q^s)^*$ pogrupis.*

2. Jeigu DBD $(n, p) > 1$ *(t.y.* DBD $(n, p) = p$*) ir $n = mp^r$ (čia $m, r \in \mathbb{N}$ ir* DBD $(m, p) = 1$*), tai vieneto šaknų aibė $E_n = E_m$. Kiekvienos iš šių šaknų kartotinumas yra lygus p^r.*

Įrodymas. 1. Jeigu DBD $(n, p) = 1$, tai polinomas $x^n - 1$ neturi kartotinių šaknų jokiame kūno $GF(q)$ plėtinyje, nes šis polinomas ir jo

išvestinė $(x^n-1)' = nx^{n-1}$ yra tarpusavyje pirminiai polinomai. Taigi aibėje E_n yra n polinomo x^n-1 šaknų: $|E_n| = n$. Jeigu $\alpha, \beta \in E_n$, tai

$$\left(\alpha\,\beta^{-1}\right)^n = \alpha^n\left(\beta^{-1}\right)^n = \alpha^n\left(\beta^n\right)^{-1} = 1$$

ir $\alpha\,\beta^{-1} \in E_n$.

Taigi E_n yra ciklinės grupės $GF(q^s)^*$ pogrupis ir todėl E_n pati yra ciklinė grupė.

2. Jeigu $n = mp^r$ (čia DBD $(m,p) = 1$), tai

$$x^n - 1 = x^{mp^r} - 1 = \left(x^m - 1\right)^{p^r}.$$

Įrodymui baigti belieka pasinaudoti 1.

$\triangle$

Toliau baigtinio kūno $GF(q)$ charakteristika $\operatorname{char} GF(q)$ bus pirminis skaičius p, tarpusavyje pirminis skaičiui n.

12.3 apibrėžimas. *n-ojo laipsnio vieneto šaknis virš kūno $GF(q)$, generuojanti ciklinę grupę E_n, vadinama primityviąja n-ojo laipsnio vieneto šaknimi virš kūno $GF(q)$.*

Vieneto šaknų grupė E_n yra ciklinė, todėl, remiantis 5.43 teorema, egzistuoja $\varphi(n)$ skirtingų primityviųjų n-ojo laipsnio vieneto šaknų virš kūno $GF(q)$. Jeigu ω yra viena iš primityviųjų n-ojo laipsnio vieneto šaknų virš $GF(q)$, tai visos kitos primityviosios n-ojo laipsnio vieneto šaknys virš $GF(q)$ yra ω^s; čia $1 \leqslant s \leqslant n$, DBD $(s,n) = 1$. Pastebėsime, kad $\varphi(n) > 0$, ir todėl visiems teigiamiems sveikiems skaičiams n, tarpusavyje pirminiams skaičiui q, egzistuoja primityvioji n-ojo laipsnio vieneto šaknis virš kūno $GF(q)$.

12.4 teiginys. *Tegu $GF(q^s)$ yra polinomo $u_n(x) = x^n - 1 \in GF(q)$ skaidinio kūnas. Tada s yra toks mažiausias teigiamas sveikas skaičius, kad n yra $q^s - 1$ daliklis, t.y. $q^s \equiv 1 \pmod n$. Šiuo atveju sakoma, kad skaičius s yra skaičiaus q eilė* $\bmod n$ *ir rašoma $s = \operatorname{ord}_n(q)$.*

Įrodymas. Tegu ω yra primityvioji n-ojo laipsnio vieneto šaknis virš $GF(q)$. Tada

$$\omega \in GF(q^k) \iff \omega^{q^k} = \omega \iff \omega^{q^k-1} = 1 \iff q^k \equiv 1 \pmod n,$$

o s yra toks mažiausias k, kuriam $\omega \in GF(q^k)$ ir todėl s – toks mažiausias teigiamas sveikas skaičius, kad $q^s \equiv 1 \,(\mathrm{mod}\, n)$.

$\triangle$

Reikėtų skirti primityviuosius polinomo $u_n(x) = x^n - 1$ skaidinio kūno $GF(q^s)$ elementus, kaip ciklinę grupę $GF(q^s)^*$ generuojančius, ir primityviąsias n-ojo laipsnio vieneto šaknis virš kūno $GF(q)$, kaip ciklinę grupę E_n generuojančius elementus.

12.5 teiginys. *1. Tegu a yra primityvusis polinomo $u_n(x) = x^n - 1$ skaidinio kūno $GF(q^s)$ elementas. Tada primityviųjų kūno $GF(q^s)$ elementų aibė $\mathcal{A}$ yra*

$$\mathcal{A} = \left\{a^k \mid DBD\left(k, q^s - 1\right) = 1\right\}, \quad |\mathcal{A}| = \varphi\left(q^s - 1\right),$$

o n-ojo laipsnio primityviųjų vieneto šaknų virš $GF(q)$ aibė $\mathcal{B}$ yra

$$\mathcal{B} = \left\{a^k \mid k = \frac{q^s - 1}{n} \cdot m,\ m < n,\ \mathrm{DBD}\,(m, n) = 1\right\}, \quad |\mathcal{B}| = \varphi\,(n).$$

2. Aibės $\mathcal{A}$ ir $\mathcal{B}$ sutampa tada ir tik tada, kai $n = q^s - 1$.
Visais kitais atvejais $\mathcal{A} \cap \mathcal{B} = \emptyset$.

Įrodysime teiginio 1 dalį, o 2 dalį paliksime įrodyti skaitytojui.

Įrodymas. 1. Primityviojo kūno $GF(q^s)$ elemento a eilė yra lygi $q^s - 1$, todėl n yra $q^s - 1$ daliklis: $q^s - 1 = nr$. Tada

$$\mathrm{ord}\,(a^k) = \frac{q^s - 1}{\mathrm{DBD}\,(k, q^s - 1)} = \frac{nr}{\mathrm{DBD}\,(k, nr)}.$$

Elementas a^k yra primityvioji n-ojo laipsnio vieneto šaknis tada ir tik tada, kai

$$\frac{nr}{\mathrm{DBD}\,(k, nr)} = n \iff \mathrm{DBD}\,(k, nr) = r \iff k = rm,\ \mathrm{DBD}\,(m, n) = 1.$$

Tai įrodo pirmąją teiginio dalį.

$\triangle$

Žinodami primityvųjį kūno $GF(q^s)$ elementą, remdamiesi ką tik įrodytu teiginiu galime faktorizuoti polinomą $u_n(x) = x^n - 1$ virš kūno $GF(q)$.

Tegu a yra primityvusis kūno $GF(q^s)$ elementas ir $s = \mathrm{ord}_n(q)$. Iš 12.5 teiginio žinome, kad

$$\omega = a^{\frac{q^s-1}{n}}$$

yra primityvioji n-ojo laipsnio vieneto šaknis ir todėl visos polinomo $u_n(x)$ šaknys yra ω laipsniai

$$1, \omega, \omega^2, \ldots, \omega^{n-1}.$$

Suradę šių elementų minimaliuosius polinomus ir sudauginę skirtingus neredukuojamus virš $GF(q)$ polinomus, gausime polinomo $u_n(x) = x^n - 1$ kanoninį skaidinį virš $GF(q)$.

Visiems i, $0 \leqslant i \leqslant n-1$, elemento ω^i jungtiniai elementai yra

$$\omega^i, \omega^{iq}, \omega^{iq^2}, \ldots, \omega^{iq^{m-1}};$$

čia m yra toks mažiausias sveikas teigiamas skaičius, kad $\omega^{iq^m} = \omega^i$, t.y. $iq^m \equiv i \,(\mathrm{mod}\, n)$. Paskutinė sąlyga apibrėžia elemento ω^i jungtinių elementų skaičių m.

Šių elemento ω^i jungtinių elementų minimalus polinomas yra

$$m_i(x) = (x - \omega^i)(x - \omega^{iq})(x - \omega^{iq^2}) \ldots (x - \omega^{iq^{m-1}});$$

čia m yra mažiausias sveikas teigiamas skaičius, kuriam $iq^m \equiv i \,(\mathrm{mod}\, n)$.

12.6 apibrėžimas. *Elemento ω^i jungtinių elementų skirtingų laipsnio rodiklių aibė*

$$C_i = \{i, iq, iq^2, \ldots, iq^{m-1}\};$$

čia m yra mažiausias sveikas teigiamas skaičius, kuriam $iq^m \equiv i \,(mod\, n)$, vadinama i-aja skaičiaus q ciklotomine aibe moduliu n.

Skaičiaus q ciklotominės aibės $\mathrm{mod}\, n$ nepriklauso nuo konkretaus primityvaus kūno $GF(q^s)$ elemento parinkimo. Be to, žinodami šios aibės elementus, galime iš anksto pasakyti, kiek neredukuojamų polinomų bus polinomo $u_n(x)$ kanoniniame skaidinyje ir kokie šių polinomų laipsniai.

12.7 pavyzdys. Faktorizuosime polinomą $u_{15}(x) = x^{15} - 1$ virš kūno $GF(2)$.

Žinome, kad $n = 15$, $q = 2$. Todėl $s = \mathrm{ord}_{15}(2) = 4$ ir kūnas $GF(2^4) = GF(16)$ yra polinomo $u_{15}(x)$ skaidinio kūnas. Iš 11.14 pavyzdžio matėme,

kad polinomas $x^4 + x^3 + 1$ yra primityvusis polinomas, todėl jo šaknis a yra primityvusis kūno $GF(16)$ elementas. Bet

$$\omega = a^{\frac{(q^s-1)}{n}} = a^{\frac{16-1}{15}} = a$$

taip pat yra ir primityvioji n-ojo laipsnio vieneto šaknis. Rasime skirtingas skaičiaus 2 ciklotomines aibes moduliu 15 (žr. 11.14 pavyzdį):

$$\begin{aligned}
&C_0 = \{0\},\\
&C_1 = \{1,2,4,8\},\\
&C_3 = \{3,6,9,12\}, \quad 3\cdot 2^3 = 24 \equiv 9 \,(\mathrm{mod}\,15),\\
&C_5 = \{5,10\},\\
&C_7 = \{7,11,13,14\},\ 7\cdot 2^2 = 28 \equiv 13 \,(\mathrm{mod}\,15),\\
&\qquad 7\cdot 2^3 = 56 \equiv 11 \,(\mathrm{mod}\,15).
\end{aligned}$$

Taigi polinomo $u_{15}(x)$ kanoniniame skaidinyje yra vienas pirmojo laipsnio polinomas, vienas antrojo laipsnio polinomas ir trys ketvirtojo laipsnio polinomai:

$$\begin{aligned}
m_0(x) &= x + 1,\\
m_1(x) &= x^4 + x^3 + 1,\\
m_3(x) &= x^4 + x^3 + x^2 + x + 1,\\
m_5(x) &= x^2 + x + 1,\\
m_7(x) &= x^4 + x + 1.
\end{aligned}$$

Polinomo $u_{15}(x)$ kanoninis skaidinys yra

$$x^{15} - 1 = (x+1)\,(x^4+x^3+1)\,(x^4+x^3+x^2+x+1)\,(x^2+x+1)\,(x^4+x+1).$$

Ieškodami polinomo $u_n(x) = x^n - 1 \in GF(q)[x]$ kanoninio skaidinio, naudojomės šio polinomo skaidinio kūnu $GF(q^s)$.