14. NEREDUKUOJAMŲ POLINOMŲ LAIPSNIS IR EILĖ

Neredukuojami polinomai baigtinių kūnų teorijoje vaidina panašų vaidmenį kaip ir pirminiai skaičiai skaičių teorijoje. Dauguma konstruktyvių uždavinių sprendimų remiasi neredukuojamų polinomų savybėmis. Su keliomis iš šių savybių jau esame susipažinę:

1. Neredukuojamas virš $GF(q)$ polinomas $f(x)$ yra savo šaknies α minimalusis polinomas, $I = \{g(x) \in GF(q)[x] \mid g(\alpha) = 0\} = \big(f(x)\big)$, t.y. α yra polinomo $g(x) \in GF(q)[x]$ šaknis tada ir tik tada, kai $g(x)$ dalijasi iš $f(x)$ (žr. 8.11 teiginį).

2. Bet kuriam natūraliajam skaičiui n virš bet kokio baigtinio kūno $GF(q)$ egzistuoja neredukuojamas n-ojo laipsnio polinomas.

Dabar nustatysime kitas neredukuojamų polinomų savybes.

11.1 teiginys. *Tegu $f(x) \in GF(q)[x]$ yra neredukuojamas n-ojo laipsnio polinomas, o α – viena iš polinomo $f(x)$ šaknų, esanti kūno $GF(q)$ plėtinyje. Tada polinomo $f(x)$ skaidinio kūnas K yra $\big(GF(q)\big)(\alpha) = GF(q^n)$.*

Įrodymas. Iš 8.17 apibrėžimo žinome, kad polinomo $f(x)$ skaidinio kūnas yra mažiausias kūno $GF(q)$ plėtinys, kuriame yra visos polinomo $f(x)$ šaknys. Todėl

$$GF(q) \subseteq \big(GF(q)\big)(\alpha) \subseteq K.$$

Kita vertus, $\big[\big(GF(q)\big)(\alpha) : GF(q)\big] = n$ ir $\big|\big(GF(q)\big)(\alpha)\big| = q^n$. Remiantis 9.3 teiginio 1) dalimi, visi kūno $\big(GF(q)\big)(\alpha)$ elementai yra polinomo $f_{q^n}(x) = x^{q^n} - x$ šaknys. Taigi $f_{q^n}(\alpha) = \alpha^{q^n} - \alpha = 0$ ir, remiantis 8.11 teiginiu, $f_{q^n(x)}$ dalijasi iš $f(x)$: visos polinomo $f(x)$ šaknys yra ir polinomo $f_{q^n}(x)$ šaknys. Todėl

$$K \subseteq \big(GF(q)\big)(\alpha)$$

ir

$$K = \big(GF(q)\big)(\alpha) = GF(q^n).$$

$\triangle$

11.2 teiginys. *Tegu $f(x) \in GF(q)[x]$ neredukuojamas n-ojo laipsnio polinomas. Tada polinomas $f_{q^m}(x) = x^{q^m} - x$ dalijasi iš $f(x)$ tada ir tik tada, kai m dalijasi iš n.*

Įrodymas. Jau žinome, kad polinomo $f(x)$ skaidinio kūnas yra $GF(q^n)$, o polinomo $f_{q^m}(x)$ skaidinio kūnas yra $GF(q^m)$. Be to, jei kūnas $GF(q^n)$ yra kūno $GF(q^m)$ pokūnis, $GF(q^n) \subset GF(q^m)$, tai m dalijasi iš n.

Tegu $f_{q^m}(x)$ dalijasi iš $f(x)$. Tada visos polinomo $f(x)$ šaknys yra ir polinomo $f_{q^m}(x)$ šaknys. Todėl $GF(q^n) \subset GF(q^m)$ ir m dalijasi iš n.

Priešingai, tegu m dalijasi iš n. Tada $GF(q^n) \subset GF(q^m)$ ir visos polinomo $f(x)$ šaknys priklauso kūnui $GF(q^m)$. Bet kūno $GF(q^m)$ elementai – tai polinomo $f_{q^m}(x)$ šaknys ir todėl polinomo $f(x)$ šaknis α yra polinomo $f_{q^m}(x)$ šaknis. Taigi $f_{q^m}(x)$ dalijasi iš $f(x)$.

$\triangle$

Neredukuojamų polinomų virš baigtinių kūnų šaknys reiškiamos paprastai.

11.3 teiginys. *Tegu $f(x) \in GF(q)[x]$ yra n-ojo laipsnio neredukuojamas polinomas ir α – kuri nors polinomo $f(x)$ šaknis polinomo skaidinio kūne $GF(q^n)$. Tada kūno $GF(q^n)$ elementai*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$$

yra visos skirtingos polinomo $f(x)$ šaknys ir n yra mažiausias natūralusis skaičius, kuriam teisinga lygybė $\alpha^{q^n} = \alpha$.

Įrodymas. Tegu $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_i \in GF(q)$, $0 \leqslant i \leqslant n$, o α – polinomo $f(x)$ šaknis polinomo skaidinio kūne $GF(q^n)$:

$$f(\alpha) = a_0 + a_1\,\alpha + \ldots + a_n \alpha^n = 0.$$

Kūno $GF(q^n)$ charakteristika yra pirminis skaičius p, o q yra p laipsnis. Todėl $a_i^q = a_i$ ir

$$\begin{aligned} f(\alpha^q) &= a_0 + a_1\alpha^q + \ldots + a_n\alpha^{qn} = a_0^q + a_1^q\alpha^q + \ldots + a_n^q\alpha^{qn} \\ &= a_0^q + (a_1\,\alpha)^q + \ldots + (a_n\alpha^n)^q = (a_0 + a_1\alpha + \ldots + a_n\alpha^n)^q \\ &= \big(f(\alpha)\big)^q = 0. \end{aligned}$$

Taigi, jeigu α yra polinomo $f(x)$ šaknis, tai ir α^q yra šio polinomo šaknis, taip pat šaknys yra ir elementai

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

Visi šioje sekoje esantys elementai yra skirtingi, nes, jeigu $\alpha^{q^i} = \alpha^{q^j}$, $0 \leqslant i < j \leqslant n-1$, tai

$$\begin{aligned} \left(\alpha^{q^i}\right)^{q^{n-j}} &= \left(\alpha^{q^j}\right)^{q^{n-j}}, \\ \alpha^{q^{n+i-j}} &= \alpha^{q^n} = \alpha, \\ \alpha^{q^{n+i-j}} - \alpha &= 0, \end{aligned}$$

t.y. α būtų polinomo $f_{q^{n+i-j}}(x) = x^{q^{n+i-j}} - x$ šaknis ir tada polinomas $f_{q^{n+i-j}}(x)$ dalytųsi iš $f(x)$, ir $n+i-j$ dalytųsi iš n. Bet tai prieštarauja nelygybėms $0 < n+i-j < n$.

$\triangle$

11.4 išvada. *Tegu $f(x) \in GF(q)[x]$ yra n-jo laipsnio neredukuojamas polinomas ir $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ – šio polinomo šaknys kūne $GF(q^n)$. Tada šių šaknų eilės kūno $GF(q^n)$ multiplikacinėje grupėje $GF(q^n)^*$ yra lygios:*

$$\operatorname{ord}_{GF(q^n)^*}(\alpha) = \operatorname{ord}_{GF(q^n)^*}(\alpha^q) = \ldots = \operatorname{ord}_{GF(q^n)^*}\left(\alpha^{q^{n-1}}\right).$$

Įrodymas. Grupė $GF(q^n)^*$ yra (q^n-1)-osios eilės ciklinė grupė, todėl elemento α eilė šioje grupėje yra q^n-1 daliklis:

$$q^n - 1 = m \cdot \operatorname{ord}_{GF(q^n)^*}(\alpha).$$

Tada

$$\operatorname{ord}_{GF(q^n)^*}\left(\alpha^{q^i}\right) = \frac{\operatorname{ord}_{GF(q^n)^*}(\alpha)}{\operatorname{DBD}\left(q^i, \operatorname{ord}_{GF(q^n)^*}(\alpha)\right)} = \frac{\operatorname{ord}_{GF(q^n)^*}(\alpha)}{\operatorname{DBD}\left(q^i, \frac{q^n-1}{m}\right)} =$$

$$= \operatorname{ord}_{GF(q^n)^*}(\alpha), \quad 0 \leqslant i \leqslant n-1,$$

nes $q = p^s$, $p = \operatorname{char} GF(q)$ ir $1 \leqslant \operatorname{DBD}\big(q^i, \frac{q^n-1}{m}\big) \leqslant \operatorname{DBD}\big(q^i, q^n-1\big) = 1$.

$\triangle$

11.5 apibrėžimas. *Neredukuojamo polinomo $f(x)$ eile vadinamas skaičius, lygus šio polinomo kurios nors šaknies eilei jo skaidinio kūno multiplikacinėje grupėje ir žymimas* $\operatorname{ord}\big(f(x)\big)$, *arba* $\operatorname{ord}\big(f\big)$.

Pateiksime pagrindines neredukuojamo polinomo eilės savybes, kurių įrodymai remiasi mums jau žinomais teiginiais.

11.6 teiginys. *Tegu $f(x)$ yra neredukuojamas polinomas virš $GF(q)$ ir* $\deg\big(f(x)\big) = n$. *Teisingi šie teiginiai:*

1. $\operatorname{ord} f(x)$ *yra $q^n - 1$ daliklis.*

2. Polinomas $f(x)$ yra polinomo $u_{\operatorname{ord}\left(f(x)\right)}(x) = x^{\operatorname{ord}(f)} - 1$ daliklis.

3. $\operatorname{ord}(f)$ *yra m daliklis tada ir tik tada, kai $f(x)$ yra $u_m(x) = x^m - 1$ daliklis.*

4. $\operatorname{ord}(f)$ *yra toks mažiausias teigiamas sveikas skaičius e, kad polinomas $f(x)$ yra $u_e(x) = x^e - 1$ daliklis.*

5. Tegu $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0$, $a_0 \neq 0$. Polinomo $f(x)$ eilė $\operatorname{ord}\big(f(x)\big)$ *yra lygi polinomo $f(x)$ lydinčiosios matricos*

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

eilei multiplikacinėje neišsigimusių matricų grupėje $GL\big(n, GF(q)\big)$.

Įrodymas. 1. Polinomo $f(x)$ skaidinio kūnas yra $GF(q^n)$ ir kiekviena polinomo $f(x)$ šaknis yra polinomo $u_{q^n-1}(x) = x^{q^n-1} - 1$ šaknis. Taigi visų polinomo $f(x)$ šaknų eilės yra $q^n - 1$ dalikliai.

2. Visų polinomo $f(x)$ šaknų eilės lygios $\operatorname{ord}(f)$, t.y. visos jos yra polinomo $u_{\operatorname{ord}(f)} = x^{\operatorname{ord}(f)} - 1$ šaknys. Todėl $f(x)$ yra $u_{\operatorname{ord}(f)}(x)$ daliklis.

3. Tegu $f(x)$ yra $u_m(x)$ daliklis. Tada visos polinomo $f(x)$ šaknys yra ir $u_m(x)$ šaknys ir šių šaknų eilės yra m dalikliai. Todėl $\operatorname{ord} f$ yra m daliklis. Atvirkščiai, tegu $m = m_1 \cdot \operatorname{ord}(f)$. Tada $u_{\operatorname{ord}(f)}(x) = x^{\operatorname{ord}(f)} - 1$ yra $x^{m_1 \cdot \operatorname{ord}(f)} - 1 = x^m - 1 = u_m(x)$ daliklis ir iš šio teiginio 2 dalies gauname, kad $f(x)$ yra $u_m(x)$ daliklis.

4. Šis teiginys yra 3 dalies tiesioginė išvada.

5. Polinomas $f(x)$ yra matricos A minimalusis polinomas, todėl $A^e = I$ tada ir tik tada, kai $f(x)$ yra polinomo $u_e(x) = x^e - 1$ daliklis. Tada norimas rezultatas išplaukia iš polinomo $f(x)$ eilės ir matricos $A \in GL\big(n, GF(q)\big)$ eilės apibrėžimų.

$\triangle$

Neredukuojamojo polinomo eilės skaičiavimo būdą panagrinėsime kiek vėliau, o dabar apsiribosime pavyzdžiu.

11.7 pavyzdys. Pateiksime mums jau žinomų neredukuojamų polinomų virš kūno $GF(2)$ eilių lentelę

$f(x)$	$\deg f(x) = n$	$2^n - 1$	$\operatorname{ord}(f)$
x	1	1	1
$x+1$	1	1	1
x^2+x+1	2	3	3
x^3+x+1	3	7	7
x^3+x^2+1	3	7	7
x^4+x+1	4	15	15
x^4+x^3+1	4	15	15
$x^4+x^3+x^2+x+1$	4	15	5

Iš šio pavyzdžio matome, kad neredukuojamo polinomo laipsnis nelemia šio polinomo eilės: polinomų $q(x) = x^4 + x + 1$ ir $p(x) = x^4 + x^3 + 1$ eilė yra lygi 15, o polinomo $r(x) = x^4 + x^3 + x^2 + x + 1$ eilė lygi 5.

11.8 teiginys. *Tegu polinomas* $f(x) \in GF(q)\,[x]$ *ir* $\deg f(x) = n \geqslant 1$. *Šios sąlygos yra ekvivalenčios:*

1. Polinomas $f(x)$ *yra primityviojo plėtinio* $GF(q^n)$ *virš* $GF(q)$ *elemento minimalusis polinomas.*

2. $f(x)$ *yra toks unitarusis polinomas, kad* $\operatorname{ord}\big(f(x)\big) = q^n - 1$.

Polinomas $f(x)$, tenkinantis teiginio sąlygas, vadinamas *primityviuoju polinomu*.

Taigi primityvusis n-ojo laipsnio polinomas virš $GF(q)$ yra toks neredukuojamas polinomas virš $GF(q)$, kad jo šaknis $\alpha \in GF(q^n)$ yra generuojantis kūno $GF(q^n)$ multiplikacinės grupės $GF(q^n)^*$ elementas.

Dabar pateiksime neredukuojamo polinomo $f(x) \in GF(q)$ eilės skaičiavimo metodą.

Tegu polinomo $f(x)$ laipsnis $\deg f(x) = n$.

A. Iš 11.5 apibrėžimo žinome, kad polinomo $f(x)$ eilė $e = \operatorname{ord}(f)$ yra toks mažiausias natūralusis skaičius, kad

$$x^e \equiv 1 \pmod{f(x)}.$$

B. Iš 11.6 teiginio 1 dalies žinome, kad e yra $q^n - 1$ daliklis. Todėl:

1. Randame skaičiaus $q^n - 1$ kanoninį skaidinį

$$q^n - 1 = \prod_{i=1}^{s} p_i^{\alpha_i}.$$

2. Iš B gauname:

$$p_i^{\alpha_i} \text{ yra } e \text{ daliklis} \iff e \text{ nėra } \frac{q^n-1}{p_i} \text{ daliklis} \iff$$

$$f(x) \text{ nėra } x^{\frac{q^n-1}{p_i}} - 1 \text{ daliklis} \iff$$

$$x^{\frac{q^n-1}{p_i}} \not\equiv 1 \pmod{f(x)}.$$

3. Aišku, jeigu $x^{\frac{q^n-1}{p_i}} \equiv 1 \pmod{f(x)}$, tai $p_i^{\alpha_i}$ nėra skaičiaus e daliklis ir todėl turėtume ieškoti tokio mažiausio skaičiaus r_i, $0 \leqslant r_i \leqslant \alpha_i$, kad

$$x^{\frac{q^n-1}{p_i^{r_i}}} \not\equiv 1 \pmod{f(x)}.$$

Tada $p_i^{\alpha_i-(r_i-1)} = p_i^{\alpha_i-r_i+1}$ – didžiausias pirminio skaičiaus p_i laipsnis – skaičiaus e daliklis. Tokiu būdu kiekvienam i, $1 \leqslant i \leqslant s$, suradę r_i, gausime

$$e = \prod_{i=1}^{s} p_i^{\alpha_i-r_i+1}.$$

11.9 pavyzdžiai. 1. Polinomas $f(x) = x^6 + x^5 + 1$ yra neredukuojamas polinomas virš $GF(2)$.

Kadangi $q = 2$, tai $q^6 - 1 = 63 = 3^2 \cdot 7$.

Patikrinsime, ar 3^2 yra ord (f) daliklis. Kadangi $\frac{63}{3} = 21$, tai

$$3^2 \text{ yra ord}\,(f) \text{ daliklis} \iff x^{21} \not\equiv 1 \pmod{x^6 + x^5 + 1}.$$

Pritaikę polinomų porai x^{21} ir $x^6 + x^5 + 1$ dalybos algoritmą, gausime

$$x^{21} \equiv x^5 + x^2 + x \pmod{x^6 + x^5 + 1} \not\equiv 1.$$

Taigi 3^2 yra ord (f) daliklis.

Patikrinsime, ar 7 yra ord (f) daliklis. Kadangi $\frac{63}{7} = 9$, tai

$$7 \text{ yra ord}(f) \text{ daliklis} \iff x^9 \not\equiv 1 \pmod{x^6 + x^5 + 1}.$$

Bet $x^9 \equiv x^5 + x^3 + x^2 + x + 1 \pmod{x^6 + x^5 + 1} \not\equiv 1$ ir todėl 7 yra ord (f) daliklis.

Taigi ord $(f) = 63$ ir, be to, matome, kad polinomas $f(x)$ yra primityvusis polinomas virš $GF(2)$.

2. Polinomas $g(x) = x^6 + x^5 + x^4 + x^2 + 1$ yra neredukuojamas polinomas virš $GF(2)$.

$$q = 2, \quad q^6 - 1 = 63 = 3^2 \cdot 7.$$

$$3^2 \text{ yra ord}\,(g) \text{ daliklis} \iff x^{21} \not\equiv 1 \pmod{x^6 + x^5 + x^4 + x^2 + 1}.$$

Bet $x^{21} \equiv 1 (\mathrm{mod}\ x^6 + x^5 + x^4 + x^2 + 1)$ ir todėl $9 = 3^2$ nėra ord (g) daliklis.

Patikrinsime, ar 3 yra ord (g) daliklis. Kadangi $\frac{63}{3^2} = 7$, tai

$$3 \text{ yra ord}\,(g) \text{ daliklis} \iff x^7 \not\equiv 1 \pmod{x^6 + x^5 + x^4 + x^2 + 1}.$$

Padalinę gausime $x^7 \equiv x^4 + x^3 + x^2 + x + 1 \pmod{x^6 + x^5 + x^4 + x^2 + 1} \not\equiv 1$, ir todėl 3 yra ord (g) daliklis.

Pagaliau,

$$7 \text{ yra ord}\,(g) \text{ daliklis} \iff x^9 \not\equiv 1 \pmod{x^6 + x^5 + x^4 + x^2 + 1}.$$

Padalinę gausime $x^9 \equiv x^3 + 1 \pmod{x^6 + x^5 + x^4 + x^2 + 1} \not\equiv 1$ ir todėl 7 yra ord (g) daliklis.

Taigi ord $(g) = 3 \cdot 7 = 21$.