NEREDUKUOJAMI POLINOMAI VIRŠ BAIGTINIŲ KŪNŲ

Neredukuojami polinomai baigtinių kūnų teorijoje vaidina panašų vaidmenį kaip ir pirminiai skaičiai skaičių teorijoje. Dauguma konstruktyvių uždavinių sprendimų remiasi neredukuojamų polinomų savybėmis. Štai keletas iš jų:

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 $f(x)$.

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.

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 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 $\big|\big(GF(q)\big)(\alpha)\big| = q^n$. Žinodami , kad 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, todėl $f_{q^n(x)}$ 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

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

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 $f(x)$.

Neredukuojamų polinomų virš baigtinių kūnų šaknys reiškiamos paprastai.

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

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

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 $0 < n+i-j < n$.

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:*

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

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

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

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

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