11. MINIMALAUS POLINOMO RADIMAS. POLINOMO SKAIDINIO KŪNAS

Norint rasti elemento $b \in F(a)$ iš 8.12 teiginio minimalų polinomą virš F, galima nagrinėti lygtį:

$$\beta_n b^n + \beta_{n-1} b^{n-1} + \ldots + \beta_1 b + \beta_0 = 0.$$

Elementas b yra tiesinė sistemos $1, a, a^2, \ldots, a^{n-1}$ kombinacija. Įrašę šią kombinaciją į nagrinėjamąją lygtį, sutraukę panašius narius ir, pagaliau, pasinaudoję tuo, kad sistema $1, a, a^2, \ldots, a^{n-1}$ tiesiškai nepriklausoma, gautus koeficientus prie šios sistemos narių prilyginę nuliui, gausime homogeninę tiesinę n lygčių su $n+1$ nežinomųjų $\beta_0, \beta_1, \ldots, \beta_n$ sistemą, turinčią nenulinį sprendinį.

8.14 pavyzdys. Tegu $K = GF(2)$, o $m(x) = x^3 + x^2 + 1$ – neredukuojamas polinomas virš $GF(2)$. Tada

$$GF(2)[x]\big/\left(x^3 + x^2 + 1\right) = \big\{\alpha_0 + \alpha_1 a + \alpha_2 a^2 \mid \alpha_0, \alpha_1, \alpha_2 \in GF(2), \\ a^3 + a^2 + 1 = 0\big\}.$$

Rasime algebrinio elemento $b = a + 1$ minimalųjį polinomą. Nagrinėjame lygtį

$$\beta_3 b^3 + \beta_2 b^2 + \beta_1 b + \beta_0 = 0, \quad , \beta_3, \beta_2, \beta_1, \beta_0 \in GF(2),$$
$$\beta_3 (a+1)^3 + \beta_2 (a+1)^2 + \beta_1 (a+1) + \beta_0 = 0.$$

Atsižvelgę į tai, kad $a^3 = a^2 + 1$, gausime

$$\begin{aligned} \beta_3 a + \beta_2 (a^2 + 1) + \beta_1 (a+1) + \beta_0 \cdot 1 &= 0, \\ \beta_2 a^2 + (\beta_3 + \beta_1) a + (\beta_2 + \beta_1 + \beta_0) \cdot 1 &= 0, \\ \beta_2 &= 0, \\ \beta_3 + \beta_1 &= 0, \\ \beta_2 + \beta_1 + \beta_0 &= 0. \end{aligned}$$

Išsprendę lygčių sistemą virš $GF(2)$, gausime $\beta_2 = 0$, $\beta_0 = \beta_1 = \beta_3$. Taigi minimalusis elemento $b = a+1$ polinomas virš $GF(2)$ yra x^3+x+1.

8.15 pavyzdys. Tegu $K = GF(3)$, o $m(x) = x^2+x+2$ neredukuojamas polinomas virš $GF(3)$. Tada

$$\begin{aligned} GF(3)[x]\big/_{(x^2+x+2)} &= \big\{[0],[1],[2],a,a+1,a+2,2a,2a+1,2a+2\big\} \\ &= GF(3)(a). \end{aligned}$$

Elemento a minimalusis polinomas virš $GF(3)$ yra x^2+x+2. Rasime elemento $b = 2a+2$ minimalųjį polinomą.

$$\begin{aligned} &\beta_2 b^2 + \beta_1 b + \beta_0 = 0, \quad \beta_2, \beta_1, \beta_0 \in GF(3), \\ &\beta_2(2a+2)^2 + \beta_1(2a+2) + \beta_0 = 0, \quad a^2 = 2a+1, \\ &\beta_2(a+2) + \beta_1(2a+2) + \beta_0 = 0, \\ &(\beta_2 + 2\beta_1)a + 2\beta_2 + 2\beta_1 + \beta_0 = 0, \\ &\qquad \beta_2 + 2\beta_1 = 0, \\ &2\beta_2 + 2\beta_1 + \beta_0 = 0, \end{aligned}$$

$$\beta_2 = \beta_1 = 2\beta_0 \quad \text{ir, kai} \quad \beta_0 = 2,\ \beta_1 = \beta_2 = 1.$$

Gavome, kad elemento $b = 2a+2$ minimalusis polinomas irgi $m(x) = x^2+x+2$ ir todėl

$$GF(3)[x]\big/_{(x^2+x+2)} = GF(3)(2a+2).$$

Be to, naujame kūne $GF(3)(2a+2)$ neredukuojamo virš $GF(3)$ polinomo $m(x) = x^2+x+2$ kanoninis skaidinys žiede $GF(3)(a)[x]$ yra

$$x^2+x+2 = (x-a)\big(x-(2a+2)\big) = (x+2a)(x+a+1).$$

8.16 teiginys. *Tegu $f(x) \in K[x]$ yra neredukuojamas virš kūno K polinomas, o a ir b – šio polinomo šaknys kuriame nors kūno K plėtinyje. Tada paprastieji plėtiniai $K(a)$ ir $K(b)$ yra izomorfiški:*

$$iz : K(a) \to K(b), \quad iz(a) = b, \quad iz(\alpha) = \alpha, \alpha \in K;$$

čia iz – kūnų izomorfizmas.

8.17 apibrėžimas. *Tegu $f(x) \in K[x]$, K – kūnas. Polinomo $f(x)$ skaidinio kūnu vadinamas kūno K plėtinys L, išsiskiriantis savybėmis:*

1) $f(x) = b(x-a_1)(x-a_2)\ldots(x-a_n)$ virš L,

2) L yra mažiausias kūno K plėtinys, kuriame visos polinomo $f(x)$ šaknys $a_1, a_2, \ldots, a_n$ yra kūno L elementai.

Taip apibrėžtas polinomo f skaidinio kūnas L žymimas $K(a_1, a_2, \ldots, a_n)$.

Tegu K – kūnas. Kiekvienam $f(x) \in K[x]$ egzistuoja šio polinomo skaidinio kūnas.

8.18 teiginys. *Du polinomo $f(x)$ skaidinio kūnai L_1 ir L_2 yra izomorfiški.*

Įrodymas. Tegu a ir b yra neredukuojamo polinomo $p(x) \in K[x]$ šaknys. Tada homomorfizmai

$$u : K[x] \to K(a)$$

ir

$$v : K[x] \to K(b)$$

indukuoja izomorfizmus

$$\bar{u} : K[x]/(p(x)) \to K(a)$$

ir

$$\bar{v} : K[x]/(p(x)) \to K(b).$$

Tada $iz = \bar{v} \cdot \bar{u}^{-1}$ yra ieškomasis izomorfizmas.

Pagrindinė 8.18 teiginio išvada yra ta, kad paprastasis algebrinis plėtinys $K(u)$ yra apibrėžtas vienareikšmiškai izomorfizmo tikslumu. Apie ˇšį plėtinį dar sako, kad jis gaunamas prijungiant prie kūno K neredukuojamo polinomo $p \in K[x]$ šaknį. Nereikia galvoti, kad ,prijungus vieną neredukuojamo polinomo šaknį, prijungsim ir likusias, t.y. paparastieji plėtiniai $K(u)$ ir $K(v)$ iš 8.1 teiginio ne visada sutampa. Pavyzdžiu galėtų būti neredukuojamas virš $\mathbf{Q}$ polinomas $x^4 - 2$. Aišku, kad plėtinyje $\mathbf{Q}\left(\sqrt[4]{2}\right)/\mathbf{Q}$, čia $\sqrt[4]{2}-$ aritmetinė ketvirto laipsnio šaknis iš 2, nėra kompleksinių polinomo x^4-2 šaknų $\pm i\sqrt[4]{2}$, t.y. $\mathbf{Q}\left(\sqrt[4]{2}\right) \neq \mathbf{Q}\left(\mathbf{i}\sqrt[4]{2}\right)$, nors šie kūnai ir yra izomorfiški.

8.19 teorema*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 teiginius 8.7 ir 8.12 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 8.7 išvadą polinomo f skaidymo kūnas yra vienintėlis izomorfizmo atžvilgiu.

Pavyzdys. Rasime polinomo x^4+4 skaidinio kūną virš $\mathbf{Q}$. Pastebėsime, kad šis polinomas nėra nereduokuojamas, nes

$$f(x) = \left(x^4 + 4\right) = \left(x^2 - 2x + 2\right)\left(x^2 + 2x + 2\right)$$

Sandaugoje esantys polinomai pagal Eizenšteino kriterijų(kai $p = 2$) nredukuojami. Turime: $x^2-2x+2 = (x-1-i)(x-1+i)$ ir $x^2+2x+2 = (x+1-i)(x+1+i)$ ir todėl polinomo $f(x)$ šaknys yra $\pm 1 \pm i$. Tada polinomo $f(x)$ skaidinio kūnas yra $\mathbf{Q}(\mathbf{i})$ ir $[\mathbf{Q}(\mathbf{i}) : \mathbf{Q}] = 2$.

Turime, kad $L_1 = K(a_1, a_2, \ldots, a_n)$, o $L_2 = K(b_1, b_2, \ldots, b_n)$; čia $b_i = a_{\sigma(i)}$, σ – aibės $\{1, 2, \ldots, n\}$ keitinys, t.y. ir $\{a_1, a_2, \ldots, a_n\}$, ir $\{b_1, b_2, \ldots, b_n\}$ yra ta pati polinomo $f(x)$ šaknų aibė, skiriasi, galbūt, tik tų šaknų užrašymo tvarka.