10. KŪNŲ PLĖTINIAI

Polinomų žiedo $K[x]$ faktorizacija neredukuojamo polinomo $f(x)$ moduliu teikia mums naujų kūnų pavyzdžių (žr.7.29 pavyzdį). Be to, pradinis kūnas K sutapatinamas su naujojo kūno $K[x]/_{(f(x))}$ pokūniu. Šiuo atveju sakoma, kad kūnas $K[x]/_{(f(x))}$ yra kūno K plėtinys.

8.1 apibrėžimas. *Jeigu $F \subseteq$ K ir F, K yra kūnai tų pačių operacijų atžvilgiu, tai kūnas F vadinamas kūno K pokūniu, o kūnas K vadinamas kūno F plėtiniu.*

8.2 teiginys. *Tegu F_i yra kūno K pokūniai; čia $i \in I$. Tada $\bigcap\limits_{i \in I} F_i$ irgi yra kūno pokūnis.*

Įrodyti paliekame skaitytojui.

8.3 apibrėžimas. *Visų kūno K pokūnių sankirta vadinama pirminiu kūnu kūne K. Jį žymėsime $P(K)$.*

Pastebėsime, kad pirminis kūnas $P(K)$ yra mažiausias kūno K pokūnis, kurio plėtinys yra kūnas K.

Išsiaiškinsime, kokie būna pirminiai kūnai.

Tegu $P(K)$ – pirminis kūnas kūne K. Kūno K elementas 1 priklauso visiems kūno K pokūniams, todėl $1 \in P(K)$ ir $\{k \cdot 1 \mid k \in \mathbb{N}\} \subset P(K)$.

Galimi du atvejai:

1. Elemento 1 eilė $\mathrm{ord}_{(K,+)} 1 = \infty$.

Kūno $P(K)$ elementais yra $0 = 0 \cdot 1$, $(-k) \cdot 1 = k \cdot (-1)$, $k \in \mathbb{N}$, ir todėl aibė $\{k \cdot 1 \mid k \in \mathbb{Z}\} \subset P(K)$. Visi aibėje $\{k \cdot 1 \mid k \in \mathbb{Z}\}$ esantys elementai yra skirtingi, nes vieneto eilė grupėje $(K, +)$ – begalinė. Ši grupė yra izomorfiška sveikųjų skaičių grupei: izomorfizmas $f : \mathbb{Z} \to \{k \cdot 1 \mid k \in \mathbb{Z}\}$ apibrėžtas lygybe $f(k) = k \cdot 1$.

Pirminiame kūne $P(K)$ taip pat yra elementai

$$(n \cdot 1) \cdot (m \cdot 1)^{-1} = \frac{n \cdot 1}{m \cdot 1}, \quad m \neq 0.$$

Taigi kūne $P(K)$ yra aibė $\left\{\frac{n\cdot 1}{m\cdot 1} \mid n \in \mathbb{Z}, m \in \mathbb{N}, (n \cdot m) = 1\right\}$, kuri kūne K apibrėžtų operacijų atžvilgiu yra kūnas. Šis kūnas yra izomorfiškas racionaliųjų skaičių kūnui $\mathbb{Q}$ ir todėl yra pirminis kūnas kūne K . Šiuo atveju $P(K)$ yra izomorfiškas (algebriškai tapatus) $\mathbb{Q}$.

2. Elemento 1 eilė $\mathrm{ord}_{(K,+)} 1 = p < \infty$.

Pastebėsime, kad $\mathrm{ord}_{(K,+)}(a) = p$, kai $a \in K - \{0\}$. Tegu $\mathrm{ord}_K a = r$.

$$p \cdot a = \underbrace{a + a + \ldots + a}_{p} = a \underbrace{(1 + 1 + \ldots + 1)}_{p} = a \cdot 0 = 0,$$

taigi $r \leqslant p$. Priešingai,

$$r \cdot a = \underbrace{a + a + \ldots + a}_{r} = 0 \Rightarrow r \cdot a \cdot a^{-1}$$
$$= \underbrace{aa^{-1} + aa^{-1} + \ldots + aa^{-1}}_{r} = r \cdot 1 = 0,$$

taigi $p \leqslant r$ ir $p = r = \mathrm{ord}_K(a)$.

Skaičius p yra pirminis. Tegu, priešingai, $p = s \cdot t$, $1 < s, t < p$.

$$0 = p \cdot 1 = s \cdot (t \cdot 1) = \underbrace{(t \cdot 1) + (t \cdot 1) + \ldots + (t \cdot 1)}_{s},$$

taigi $\mathrm{ord}_K(t \cdot 1) \leqslant s < p$ – prieštara.

Aibė $\{1 \cdot 1, 2 \cdot 1, \ldots, (p-1) \cdot 1, p \cdot 1 = 0\}$ kūne K esančių operacijų atžvilgiu yra kūnas, izomorfiškas baigtiniam kūnui $GF(p)$. Bet $P(K)$ – mažiausias kūno K pokūnis, todėl pats $P(K)$ yra izomorfiškas kūnui $GF(p)$.

8.4 apibrėžimas. *Tegu $(K, +, \cdot)$ yra kūnas. Jei $\mathrm{ord}_{(K,+)} 1 = p < \infty$, skaičius p yra vadinamas kūno K charakteristika, žymima $\mathrm{char}\, K = p$, o kai $\mathrm{ord}_{(K,+)} 1 = \infty$, skaičius 0 yra vadinamas kūno K charakteristika, žymima $\mathrm{char}\, K = 0$.*

8.5 išvados. *1. Baigtinio kūno charakteristika yra pirminis skaičius.*

2. Tegu kūno K charakteristika $\mathrm{char}\, K = p$ – pirminis skaičius. Tada

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}, \qquad (a-b)^{p^n} = a^{p^n} - b^{p^n}, \quad \text{su visais } a, b \in K, n \in \mathbb{N}.$$

Įrodymas. 1. Akivaizdu.

2. Pasinaudokime Niutono binomo formule

$$(a+b)^{p^n} = a^{p^n} + C^1_{p^n} a^{p^n-1} b + \ldots + C^{p^n-1}_{p^n} a \cdot b^{p^n-1} + b^{p^n},$$

$$C^k_{p^n} = \frac{p^n(p^n-1)\ldots(p^n-k+1)}{1\cdot 2\cdot \ldots \cdot k} \in \mathbb{Z}, \qquad 0 \leqslant k \leqslant p^n.$$

Skaičius p yra pirminis, todėl, kai $1 \leqslant k \leqslant p^n - 1$, p iš eilės einančių dauginamųjų sandugoje $1\cdot 2\cdot \ldots \cdot k$ nesidalija iš p^n . Samprotaujant pagal indukciją , turėsime

$$\begin{aligned} C^k_{p^n} &= \frac{p^n(p^n-1)\ldots(p^n-k+1)}{1\cdot 2\cdot \ldots \cdot k} \\ &= p\Big(\underbrace{\frac{p^{n-1}(p^n-1)\ldots(p^n-k+1)}{1\cdot 2\cdot \ldots \cdot k}}_{\in \mathbb{Z}}\Big) \equiv 0 \pmod p. \end{aligned}$$

Taigi $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Antroji formulė įrodoma remiantis pirmąja:

$$a^{p^n} = \big((a-b)+b\big)^{p^n} = (a-b)^{p^n} + b^{p^n} \Rightarrow (a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

$\triangle$

Kūno F plėtinys K turi savybes:

1) $(K,+)$ yra komutatyvioji grupė;

2) visiems $\alpha \in F$ ir visiems $a \in K$ sandauga $\alpha \cdot a \in K$;

3) visiems $\alpha, \beta \in F$ ir visiems $a, b \in K$:

$$\begin{aligned} &(\alpha+\beta)\cdot a = \alpha\cdot a + \beta\cdot a, \\ &\alpha(a+b) = \alpha\cdot a + \alpha\cdot b, \\ &(\alpha\cdot\beta)\cdot a = \alpha(\beta\cdot a), \\ &1\cdot a = a. \end{aligned}$$

Kūnas K yra vektorinė erdvė virš kūno F. Jeigu šios vektorinės erdvės dimensija yra baigtinis skaičius, tai sakoma, kad K yra baigtinis F plėtinys ir šio plėtinio laipsnis $[K:F] = \dim_F K$.

8.6 pavyzdys. Tegu K yra baigtinis kūnas, kurio $\operatorname{char} K = p$. Tada K yra $GF(p)$ baigtinis plėtinys ir kartu vektorinė erdvė virš $GF(p)$. Tegu

$[K : GF(p)] = n$. Tada $K \approx \big(GF(p)\big)^n$. Taip pat matome, kad baigtinio kūno K elementų skaičius yra lygus p^n.

8.7 išvada. *Tegu L yra baigtinis kūno K plėtinys, o K – baigtinis kūno F plėtinys. Tada L yra baigtinis F plėtinys ir*

$$[L : F] = [L : K] \cdot [K : F].$$

8.8 apibrėžimas. *Tegu K yra kūno F plėtinys, o $a \in K$. Mažiausias kūno F plėtinys, kuriam priklauso elementas a, vadinamas paprastuoju kūno F plėtiniu ir žymimas $F(a)$. Elementas a vadinamas generuojančiu šį plėtinį elementu.*

Jeigu elementas $a \in K$ tenkina lygtį $\alpha_n a^n + \alpha_{n-1} a^{n-1} + \ldots + \alpha_1 a + \alpha_0 = 0$, $\alpha_n, \alpha_{n-1}, \ldots, \alpha_1, \alpha_0 \in F$, tai jis a vadinamas algebriniu kūno K elementu.

Kūno F plėtinys K vadinamas algebriniu plėtiniu, jeigu visi kūno K elementai yra algebriniai virš F elementai.

8.9 pavyzdys. 1. $\mathbb{C}$ yra paprastasis algebrinis $\mathbb{R}$ plėtinys: $\mathbb{C} = \mathbb{R}(i)$. Tegu $a + ib \in \mathbb{C}$, tada polinomo $f(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$ viena iš šaknų ir yra $a + ib$: $f(a + ib) = 0$.

2. Tegu $F = GF(2)$ ir $f(x) = x^2 + x + 1$ yra neredukuojamas polinomas virš $GF(2)$. Žinome, kad $GF(2)[x]\big/\big(x^2 + x + 1\big)$ yra kūno $GF(2)$ plėtinys:

$$GF(2)[x]\big/\big(x^2 + x + 1\big) = \big\{[0], [1], [x], [x+1]\big\} = GF(2)(\alpha);$$

čia $\alpha = [x]$. Taigi kalbame apie paprastąjį plėtinį. Negana to,

$$\begin{array}{lll} f_1(x) = x, & f_1\big([0]\big) & = [0], \\ f_2(x) = x + 1, & f_2\big([1]\big) & = [0], \\ f_3(x) = x^2 + x + 1, & f_3\big([x]\big) & = [0], \\ & f_3\big([x+1]\big) & = [0], \end{array}$$

todėl $GF(2)(\alpha)$ – paprastasis algebrinis $GF(2)$ plėtinys.

8.10 apibrėžimas. *Tegu K yra kūno F plėtinys, o $a \in K$ – algebrinis elementas virš F. Aibė $I = \big\{g(x) \in F[x] \mid g(a) = 0\big\}$ yra žiedo $F[x]$ idealas. Polinomų žiedas $F[x]$ yra vyriausiųjų idealų sritis, todėl egzistuoja*

toks vienintelis unitarusis polinomas $m(x) \in F[x]$, *kad* $I = \big(m(x)\big)$. *Šis polinomas* $m(x)$ *vadinamas minimaliuoju elemento* $a \in K$ *polinomu virš kūno* F. *Polinomo* $m(x)$ *laipsnis* $\deg m(x)$ *vadinamas elemento* a *laipsniu virš kūno* F.

8.11 teiginys. *Tegu* K *yra kūno* F *plėtinys, o* $m(x)$ – *minimalusis elemento* $a \in K$ *polinomas virš* F. *Tada:*

1. Polinomas $m(x)$ *yra vienintelis unitarusis neredukuojamas polinomas virš* F, *kurio šaknis yra* a: $m(a) = 0$.

2. Polinomas $m(x)$ *yra vienintelis unitarusis mažiausiojo laipsnio polinomas virš* F, *kurio šaknis yra* a: $m(a) = 0$.

3. Polinomas $m(x)$ *yra vienintelis unitarusis polinomas virš* F, *tenkinantis sąlygą: jeigu* $f(x) \in F[x]$ *ir* $f(a) = 0$, *tai* $f(x)$ *dalijasi iš* $m(x)$.

Įrodyti paliekame skaitytojui, pastebėdami, kad visi teiginiai yra minimaliojo, kartu ir generuojančio ideala $I = \big\{g(x) \in F[x] \mid g(a) = 0\big\}$, polinomo apibrėžimo išvados.

Minimaliųjų algebrinių elementų polinomų paieška yra svarbus, bet ne visada lengvas uždavinys. Vėliau nurodysime tų polinomų radimo būdus, o dabar pasitenkinsime bendrais samprotavimais ir pateiksime pavyzdi.

8.12 teiginys. *Tegu* K *yra kūno* F *plėtinys,* $a \in K$ – *algebrinis* n*-ojo laipsnio elementas virš* F, *kurio minimalusis polinomas yra* $m(x)$. *Tada:*

1. Paprastasis plėtinys $F(a)$ – *izomorfiškas kūnui* $F[x]\big/\big(m(x)\big)$.

2. $[F(a) : F] = n$, *o* $1, a, \ldots, a^{n-1}$ *yra vektorinės erdvės* $F(a)$ *bazė virš* F.

3. Kiekvienas kūno $F(a)$ *elementas* $b \in F(a)$ *yra algebrinis virš* F, *o jo laipsnis yra* n *daliklis.*

Įrodymas. 1. Funkcija $u : F[x] \to F(a)$, apibrėžta lygybe $u\big(f(x)\big) = f(a)$, yra žiedų homomorfizmas. Tada $\operatorname{Ker} u = \big\{g(x) \in F[x] \mid g(a) = 0\big\} = \big(m(x)\big)$ ir $F[x]\big/\big(m(x)\big)$ yra izomorfiškas $u\big(F[x]\big)$. Bet $u\big(F[x]\big) = F(a)$, nes: viena vertus, $a = u(x) \in u(F[x])$, $F \subseteq u(F[x])$ ir todėl $F(a) \subseteq u(F[x])$; kita vertus, $u\big(F[x]\big) = \big\{f(a) \mid f(x) \in F[x]\big\} \subseteq F(a)$.

2. a) Sistema $1, a, \ldots, a^{n-1}$ yra generuojanti vektorinę erdvę $F(a)$ sistema.

Tegu $b \in F(a)$, t.y. $b = f(a)$; čia $f(x) \in F[x]$. Pritaikę polinomų porai $f(x)$ ir $m(x)$ dalumo algoritmą, gausime

$$f(x) = q(x)\, m(x) + r(x), \qquad r(x) = \alpha_s x^s + \ldots + \alpha_0, \quad s < n$$

ir

$$b = f(a) = q(a)m(a) + r(a) = r(a) = \alpha_s a^s + \ldots + \alpha_0 \cdot 1.$$

b) Sistema $1, a, \ldots, a^{n-1}$ yra tiesiškai nepriklausoma vektorinėje erdvėje $F(a)$.

Tegu $\alpha_0 \cdot 1 + \alpha_1 \cdot a + \ldots + \alpha_{n-1}a^{n-1} = 0$, t.y. $f(a) = 0$; čia

$$f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} \in F[x].$$

Bet nenulinio polinomo, kurio viena iš šaknų yra a, minimalus laipsnis yra $n = \deg\, m(x)$ ir todėl $f(x) \equiv 0$, t.y.

$$\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 0.$$

3. Tegu $b \in F(a)$. Vektorinės erdvės $F(a)$ dimensija $\dim_F F(a) = [F(a) : F] = n$, todėl $n + 1$ elemento sistema $1, b, b^2, \ldots, b^n$ yra tiesiškai priklausoma, t.y. atsiras tokie ne visi nuliniai elementai $\beta_0, \beta_1, \beta_2, \ldots, \beta_n \in F$, kad

$$\beta_0 \cdot 1 + \beta_1 \cdot b + \ldots + \beta_n b^n = 0,$$

t.y.

$$f(b) = 0, \quad \text{kur} \quad f(x) = \beta_0 + \beta_1 x + \ldots + \beta_n x^n \in F[x].$$

Taigi b yra algebrinis elementas ir $F(b)$ – baigtinis kūno F plėtinys. Be to, $F(b) \subseteq F(a)$. Remiantis 8.7 išvada,

$$n = [F(a) : F] = [F(a) : F(b)] \cdot [F(b) : F].$$

Gavome, kad b laipsnis, kuris lygus $[F(b) : F]$, yra n daliklis.