12. BAIGTINIAI KŪNAI

Ankstesniuose skyreliuose jau nagrinėjome baigtinių kūnų pavyzdžius: likinių klasių pirminio skaičiaus p moduliu kūną, $\mathbb{Z}/_{(p)} = GF(p)$ – svarbiausias iš jų. Dabar apibendrinsime mūsų žinias apie baigtinių kūnų struktūrą, aptarsime polinomų su koeficientais iš šių kūnų savybes. Ypač mus domins baigtinio kūno elementų minimaliųjų polinomų paieška, taip pat polinomų virš baigtinių kūnų faktorizacijos klausimai.

Pradžioje pastebėsime, kad bet kurio baigtinio kūno K charakteristika yra pirminis skaičius p, ir todėl į baigtinį kūną K galima žiūrėti kaip į pirminio kūno $GF(p)$ baigtinį plėtinį.

9.1 teiginys. *Tegu baigtinis kūnas K yra baigtinio kūno F plėtinys ir $[K : F] = d$. Tada $|K| = |F|^d$.*

Įrodymas. Tegu $\{a_1, \ldots, a_d\}$ yra vektorinės erdvės K virš F bazė. Tada

$$K = \{\alpha_1 a_1 + \ldots + \alpha_d a_d \mid \alpha_1, \ldots, \alpha_d \in F\} \quad \text{ir}$$

$$|K| = |F|^d.$$

$\triangle$

9.2 išvada. *Tegu K baigtinis kūnas, kurio $\mathrm{char}\, K = p$. Tada kūne K yra p^n elementų; čia $n = [K : GF(p)]$.*

Į baigtinio kūno elementus galima žiūrėti ir kaip į polinomo šaknis.

9.3 teiginys. *Tegu $\big|(K, +, \cdot)\big| = q$. Tada:*
1) visi kūno K elementai yra polinomo $f_q(x) = x^q - x$ šaknys;
2) kūnas K yra polinomo $f_q(x)$ skaidinio kūnas.

Įrodymas. 1) Aišku, kad $f(0) = 0^q - 0 = 0$. Be to, $(K^*, \cdot) = (K - \{0\}, \cdot)$ – yra multiplikacinė grupė, kurios eilė lygi $q - 1$, ir pagal 5.19 Lagranžo teoremą, kai $a \in K^*$, tai $a^{q-1} = 1$ ir $a^q = a$.

2) Polinomas $f_q(x)$ gali turėti daugiausiai q šaknų kūne K. Bet mes jas visas jau žinome – tai kūno K elementai:

$$f_q(x) = (x - a_1)(x - a_2) \dots (x - a_q);$$

čia $a_1, a_2, \dots, a_q$ – visi kūno K elementai.

Taigi K yra polinomo $f_q(x)$ skaidinio kūnas.

$\triangle$

9.4 teiginys. *1. Visiems pirminiams skaičiams p ir visiems natūraliesiems skaičiams n egzistuoja kūnas, turintis p^n elementų.*

2. Visi baigtiniai kūnai, turintys $q = p^n$ elementų, yra izomorfiški polinomo $f_q(x) = x^q - x$ skaidinio kūnui.

Įrodymas. Tegu K yra polinomo $f_q(x) = x^q - x \in GF(p)[x]$ skaidinio kūnas, o aibė $A \subseteq$ K – polinomo $f_q(x)$ šaknų aibė. Aibėje A yra q elementų, nes polinomas $f_q(x)$ neturi kartotinių šaknų: $f'_q(x) = qx^{q-1} - 1 = -1 \neq 0$ ir $\big(f_q(x), f'_q(x)\big) = 1$. Aibė A yra kūnas, nes:

a) $0, 1 \in A : 0^q = 0,\ 1^q = 1$;

b) kai $b \in A$, $b \neq 0$, tai ir $-b \in A$, nes $(-b)^q = -b$, ir $b^{-1} \in A$, nes $(b^{-1})^q = (b^q)^{-1} = b^{-1}$;

c) kai $a, b \in A$, $b \neq 0$, tai

$$a \pm b \in A : (a \pm b)^q = a^q \pm b^q = a \pm b;$$

$$a \cdot b^{-1} \in A : (a \cdot b^{-1})^q = a^q \cdot (b^q)^{-1} = a \cdot b^{-1}.$$

Polinomas $f_q(x)$ taip pat skaidosi tiesinių daugiklių sandauga virš kūno A, t. y. A – polinomo $f_q(x)$ skaidinio kūnas ir $A = K$. Taigi $|K| = q$.

$\triangle$

Visi baigtiniai kūnai, turintys $q = p^n$ (p – pirminis) elementų, izomorfiški vieni kitiems (visi jie izomorfiški polinomo $f_q(x) = x^q - x$ skaidinio kūnui) ir todėl galima kalbėti apie kūno iš q elementų vienatinumą. Visus šiuos kūnus žymėsime vienodai – $GF(q)$. Tiesa, lieka atviras kūno elementų reiškimo klausimas. Bet apie tai vėliau. Nagrinėjant kūno struktūrą svarbu išsiaiškinti, kokių kūnų plėtinys yra nagrinėjamas kūnas. Baigtiniams kūnams į šį klausimą galima atsakyti tiksliai.

9.5 teiginys. *Tegu K yra baigtinis kūnas, turintis $q = p^n$ (p – pirminis) elementų.*

1. Kai F yra kūno K pokūnis, tai $|F| = p^d$; čia d yra n daliklis.

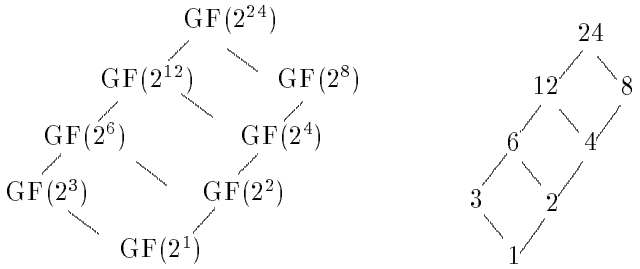
2. Kiekvienam skaičiaus n dalikliui d egzistuoja vienintelis kūno K pokūnis F, turintis p^d elementų.

Įrodymas. 1. Aišku, kad $K \supseteq F \supseteq GF(p)$ ir $|F| = p^d$; čia $d = \big[F : GF(p)\big]$. Bet $n = \big[K : GF(p)\big] = [K : F]\big[F : GF(p)\big] = [K : F] \cdot d$, todėl d yra n daliklis.

2. Tegu d yra n daliklis. Tada $p^d - 1$ yra $p^n - 1$ daliklis ir $x^{p^d-1} - 1$ yra $x^{p^n-1} - 1$ daliklis, t. y. $f_{p^n}(x)$ dalijasi iš $f_{p^d}(x)$ ir kiekviena polinomo $f_{p^d}(x)$ šaknis yra ir polinomo $f_{p^n}(x)$ šaknis. Kūnas K yra polinomo $f_{p^n}(x)$ skaidinio kūnas ir todėl jame bus polinomo $f_{p^d}(x)$ skaidymo kūnas F, kuriame p^d elementų. Bet kūno F elementai – tai polinomo $f_{p^d}(x)$ šaknys, o jų yra p^d, t.y. kiek elementų kūne F. Taigi dviejų skirtingų polinomo $f_{p^d}(x)$ skaidinio kūnų kūne K negali būti.

△

9.6 pavyzdys. Kūno $GF\big(2^{24}\big)$ pokūnių diagrama atitinka skaičiaus $n = 24$ daliklių diagramą:



Svarbi baigtinių kūnų savybė yra ir ta, kad baigtinio kūno $(K, +, \cdot)$ multiplikacinė grupė $K^* = \big(K - \{0\}, \cdot\big)$ yra ciklinė. Šią grupę generuojantys elementai vadinami primityviaisiais kūno K elementais (palyginkite su jau nagrinėtos grupės U_n generuojančiais elementais, kurie taip pat vadinami primityviaisiais).

Pastebėsime, kad multiplikacinė kūno $GF(p)$ grupė $GF(p)^*$ yra lygi U_p (žr. 6.7 pastabą). Tačiau net ir šiuo atveju nėra formulės primityviajam

elementui rasti. Tiesa, yra žinoma, jeigu pirminis skaičius $p = 4q + 1$, čia q – taip pat pirminis skaičius, tai 2 yra primityvusis elementas grupėje $U_p = GF(p)^*$, t. y. 2 – primityvusis kūno $GF(4q + 1)$, q – pirminis, elementas. Tokių kūnų pavyzdžiai yra $GF(5)$, $GF(13)$, $GF(17)$, $GF(29)$ ir t.t.

6.19 algoritmas, pagal kurį randamos primityviosios šaknys $\bmod p$, visiškai tinka ir kūno $GF(q)$ primityviesiems elementams ieškoti. Pačiame algoritme reikėtų tik pirminį skaičių p pakeisti skaičiumi q. Pabandykime įsitikinti tuo, kad pagal algoritmą galima rasti elementą $a \in GF(q)^*$, kurio eilė $\operatorname{ord}_{GF(q)^*}(a) = q - 1$.

1. Tegu $r = q-1 = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m}$ yra kanoninis skaičiaus r skaidinys.

2. Tegu $a_i \in GF(q)^*$ toks elementas, kad $a_i^{\frac{r}{p_i}} \neq 1$, $1 \leqslant i \leqslant m$. Toks elementas su visais i atsiras, nes polinomas $x^{\frac{r}{p_i}} - 1$ turi kūne ne daugiau kaip $\frac{r}{p_i} < r$ šaknų.

3. Elemento $b_i = a_i^{\frac{r}{p_i^{n_i}}}$ eilė lygi $p_i^{n_i}$, nes

$$b_i^{p_i^{n_i}} = \left(a^{\frac{r}{p_i^{n_i}}}\right)^{p_i^{n_i}} = a^r = 1, \quad \text{bet}$$

$$b_i^{p_i^{n_i-1}} = \left(a^{\frac{r}{p_i^{n_i}}}\right)^{p_i^{n_i-1}} = a^{\frac{r}{p_i}} \neq 1.$$

4. Elementas $a = b_1 b_2 \dots b_m$ yra primityvusis kūno $GF(q)$ elementas. Tai, kad $a^r = a^{q-1} = 1$, žinoma. Bet

$$a^{\frac{r}{p_i}} = b_1^{\frac{r}{p_i}} \dots b_{i-1}^{\frac{r}{p_i}} b_i^{\frac{r}{p_i}} b_{i+1}^{\frac{r}{p_i}} \dots b_m^{\frac{r}{p_i}} = b^{\frac{r}{p_i}} \neq 1,\ 1 \leqslant i \leqslant m.$$

Primityviųjų elementų kiekis baigtiniame kūne $GF(q)$ yra $\varphi(q-1)$; čia φ – Oilerio funkcija.

Įdomi primityviojo elemento egzistavimo baigtiniame kūne išvada yra tokia:

9.7 teiginys. *Tegu $GF(q)$ yra baigtinis kūnas. Su visais natūraliaisiais n egzistuoja neredukuojamas n-ojo laipsnio polinomas virš $GF(q)$.*

Įrodymas. Kūnas $GF(q^n)$ yra toks kūno $GF(q)$ plėtinys, kad $\big[GF(q^n) : GF(q)\big] = n$. Jeigu a yra primityvusis kūno $GF(q^n)$ elementas, tai $\big(GF(q)\big)(a) = GF(q^n)$ ir minimalusis elemento a polinomas $m(x)$ bus tas ieškomasis neredukuojamas n-ojo laipsnio polinomas virš $GF(q)$.

$\triangle$