VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
MATEMATIKOS INSTITUTAS
TIKIMYBIŲ TEORIJOS IR SKAIČIŲ TEORIJOS KATEDRA

Kastytis Bandžiulis

LAIPSNIAI BAIGTINIUOSE KŪNUOSE

Bakalauro baigiamasis darbas

Leidžiu ginti .....

Darbo vadovas prof. Paulius Drungilas

Vilnius 2022

Turinys

Įvadas **2**

1 Kūnai, baigtiniai kūnai **5**

1.1 Kūnas 5

1.2 Kaip konstruoti $\mathbb{F}_q$ pavyzdį. 6

1.3 Kūno plėtiniai ir skaidinio kūnas 8

2 Oilerio kriterijus ir jo apibendrinimas **10**

2.1 Oilerio kriterijus 10

2.2 Apibendrintas Oilerio kriterijus 11

3 Oilerio kriterijus r-tojo laipsnio šakniai **12**

Summary 14

Literatūra **15**

Įvadas

Kūnas yra aibė, kurioje apibrėžtos jos elementų sumos ir daugybos operacijos, tenkinančios tam tikras sąlygas (žr. 1.1 skyrelį). Racionaliųjų skaičių aibė $\mathbb{Q}$, realiųjų skaičių aibė $\mathbb{R}$ ir kompleksinių skaičių aibė $\mathbb{C}$ yra paprasčiausi kūnų pavyzdžiai. Šiame darbe nagrinėjami baigtiniai kūnai – kūnai, turintys baigtinį skaičių elementų. Kiekvieno tokio kūno elementų skaičius lygus p^n, kur $n \in \mathbb{N}$, o p yra pirminis skaičius. Taigi joks kūnas negali turėti lygiai 6 elementus, nes 6 nėra pirminio skaičiaus laipsnis. Kita vertus, kiekvienam pirminio laipsniui $q = p^n$ egzistuoja vienintelis (kūnų izomorfizmo tikslumu) kūnas, žymimas $\mathbb{F}_q$, turintis lygiai p^n elementų (žr. [5, p. 236]).

Laipsniai baigtiniuose kūnuose ir bendra baigtinių kūnų teorija yra svarbi skaičių teorijoje ir algebroje, taikoma kriptografijoje, kodavime ir signalų analizėje. Polinominių lygčių sprendinių egzistavimas yra vienas iš svarbiausių klausimų šiose srityse, ir Oilerio kriterijus leidžia patikrinti ar baigtinio kūno elementas yra kokio nors kito elemento kvadratas (žr. 2 teoremą). Straipsnis [1] išplečia kriterijų platesnei kategorijai baigtinių kūnų ir laipsniams, didesniems už 2.

Pirmame skyriuje apibrėžta kūno sąvoką ir iliustruota pavyzdžiais. Taip pat paaiškinta, kaip konstruojami baigtiniai kūnai $\mathbb{F}_q$ bet kokiam pirminio skaičiaus laipsniui q, apibrėžtos kūnų plėtinio ir polinomo skaidinio kūno sąvokos. Antrame skyriuje įrodytas klasikinis Oilerio kriterijus, leidžiantis nustatyti, kada kūno $\mathbb{F}_p$, p – pirminis skaičius, elementas yra kokio nors kito elemento laipsnis. Taip pat įrodytas šio kriterijaus apibendrinimas bet kokiam baigtiniam nelyginės eilės kūnui $\mathbb{F}_q$. Trečiame skuriuje šis kriterijus dar labiau apibendrinamas.

Galima rasti netiesioginius ryšius su Winterhof'o [8] straipsniu, kur skaičius elementų, tenkinantys tam tikrą multiplikatyvių charakterių savybę, sutampa su šaknų generuojančia ciklinę grupės eilę $\frac{q-1}{r}$, kur q yra pirminio skaičiaus laipsnis ir r yra

šaknies laipsnis. Algoritminės savybės šaknų ieškojime nagrinėjamos straipsnyje [4], trumpai aptariamos ir baigtinių kūnų naudojimas kriptografijoje.

Verta paminėti, kad [1] straipsnyje rastas vienas neteisingas teiginys (žr. pastraipą prieš 4 teoremos formuluotę). Paaiškinimą galima rasti pastraipoje po 3 teoremos įrodymo.

1 skyrius

Kūnai, baigtiniai kūnai

1.1 Kūnas

1 apibrėžimas (Kūnas)**.** Nagrinėkime aibę A ir joje apibrėžtas binarines operacijas $+$ ir $\cdot$ (vadinsime sudėtimi ir daugybą). Trejetas $(A, +, \cdot)$ vadinamas **kūnu** (žr. [2, p. 166]), jei su visais $x, y, z \in A$ tenkinamos šios sąlygos:

- aibė A yra uždarą abejų operacijų atžvilgiu:

$$x + y \in A \text{ ir } x \cdot y \in A;$$

- sudėtis ir daugybą yra asociatyvios operacijos:

$$x + (y + z) = (x + y) + z \text{ ir } x \cdot (y \cdot z) = (x \cdot y) \cdot z;$$

- sudėtis ir daugyba yra komutatyvios operacijos:

$$x + y = y + x \text{ ir } x \cdot y = y \cdot x;$$

- egzistuoja neutralūs elementai operacijų $+$ ir $\cdot$ atžvilgiu, t. y. egzistuoja tokie elementai $0, 1 \in A$, kad

$$0 + x = x + 0 = x \text{ ir } 1 \cdot x = x \cdot 1 = x;$$

- sudėtį ir daugybą sieja distributyvumo dėsnis:

$$x \cdot (y + z) = x \cdot y + x \cdot z;$$

- kiekvienas elementas turį atvirkštinį elementą sudėties atžvilgiu, t. y. kiekvienam $x \in A$ egzistuoja toks $-x \in A$, kad $x + (-x) = 0$;
- kiekvienas nenulinis elementas turi atvirkštinį elementą daugybos atžvilgiu, t. y. kiekvienam $x \in A \setminus \{0\}$ egzistuoja toks $x^{-1} \in A$, kad $x \cdot x^{-1} = 1$.

Nesunku įsitikinti, kad racionaliųjų skaičių aibė $\mathbb{Q}$ skaičių sumos ir daugybos atžvilgiu yra kūnas. Panašiai, realiųjų skaičių aibė $\mathbb{R}$ ir kompleksinių skaičių aibė $\mathbb{C}$ skaičių sumos ir daugybos atžvilgiu taip pat yra kūnai. Kita vertus, sveikųjų skaičių aibė $\mathbb{Z}$ sudėties ir daugybos atžvilgiu nėra kūnas, nes, pavyzdžiui, skaičius 2 neturi atvirkštinio skaičiaus daugybos atžvilgiu, t. y. lygtis $2x = 1$ neturi sprendinių aibėje $\mathbb{Z}$.

Šiame darbe nagrinėsime baigtinius kūnus – kūnus, kurių elementų skaičius yra baigtinis. Kiekvieno tokio kūno elementų skaičius lygus p^n, kur $n \in \mathbb{N}$, o p yra pirminis skaičius. Taigi joks kūnas negali turėti lygiai 6 elementus, nes 6 nėra pirminio skaičiaus laipsnis. Kita vertus, kiekvienam pirminio laipsniui $q = p^n$ egzistuoja vienintelis (kūnų izomorfizmo tikslumu) kūnas, žymimas $\mathbb{F}_q$, turintis lygiai p^n elementų (žr. [5, p. 236]).

1.2 Kaip konstruoti $\mathbb{F}_q$ pavyzdį.

Paaiškinsime, kaip galima konstruoti baigtinius kūnus. Tegul p – pirminis skaičius. Nagrinėkime kintamojo t polinomų žiedą $\mathbb{F}_p[t]$. Kiekvienam $n \in \mathbb{N}$ egzistuoja n-tojo laipsnio neredukuojamas polinomas $p(t) \in \mathbb{F}_p[t]$ (žr. [3, p. 84]). Kadangi $\mathbb{F}_p$ yra kūnas, tai $\mathbb{F}_p[t]$ yra pagrindinių idealų žiedas (žr. [2, p. 248]). Kadangi $p(t)$ yra neredukuojamas žiede $\mathbb{F}_p[t]$, tai šio žiedo idealas $(p(t)) = \{p(t)a(t) : a(t) \in \mathbb{F}_p[t]\}$ yra maksimalus (žr. [2, p. 249]). Todėl faktoržiedas $\mathbb{F}_p[t]/(p(t))$ yra kūnas (žr. [2, p. 188]). Šio kūno elementai turi pavidalą

$$a(t) + (p(t)) = \{a(t) + p(t)b(t) : b(t) \in \mathbb{F}_p[t]\}, \quad \text{kur} \quad a(t) \in \mathbb{F}_p[t],$$

ir žymimi $\overline{a(t)}$. Taigi elementas $\overline{a(t)}$ yra žiedo $\mathbb{F}_p[t]$ poaibis, sudarytas iš visų šio žiedo polinomų, kurių dalybos iš $p(t)$ liekana sutampa su polinomo $a(t)$ dalybos iš $p(t)$ liekana. Kūno $\mathbb{F}_p[t]/(p(t))$ elementų suma ir daugyba apibrėžtos tokiomis

lygybėmis:

$$\overline{a(t)} + \overline{b(t)} := \overline{a(t) + b(t)},$$
$$\overline{a(t)} \cdot \overline{b(t)} := \overline{a(t)b(t)},$$

kur $a(t), b(t) \in \mathbb{F}_p[t]$. Be to, kiekvieną elementą $\overline{a(t)}$ galima vienintelių būdu išreikšti pavidalu

$$r_0 + r_1 t + \cdots + r_{n-1}t^{n-1} + (p(t)), \tag{1.1}$$

kur $r_0 + r_1 t + \cdots + r_{n-1}t^{n-1}$ yra polinomo $a(t)$ dalybos iš polinomo $p(t)$ liekana. Taigi (1.1) lygybėje skirtingi koeficientų rinkiniai $(r_0, r_1, \ldots, r_{n-1})$ atitinka skirtingus kūno $\mathbb{F}_p[t]/(p(t))$ elementus. Todėl šis kūnas turi lygiai p^n elementų.

1 pavyzdys. Sukonstruosime kūną $\mathbb{F}_9$. Kadangi $p = 3$ ir $9 = 3^2$, tai reikia rasti antrojo laipsnio neredukuojamą polinomą $p(t) \in \mathbb{F}_3$. Nagrinėkime pavidalo $at^2 + b$, $a \neq 0$, polinomus žiede $\mathbb{F}_3[t]$. 1.1 lentelėje pateiktos visų tokių polinomų reikšmės, kai $t \in \mathbb{F}_3$. Žinome, kad antrojo laipsnio polinomas yra neredukuojamas virš kokio nors kūno tada ir tik tada, kai jis neturi šaknų šiame kūne. Lentelėje matyti, kad polinomas $p(t) = t^2 + 1$ neturi šaknų kūne $\mathbb{F}_3$, todėl yra neredukuojamas.

$at^2 + b$	$t = 0$	$t = 1$	$t = 2$
t^2	0	1	1
$t^2 + 1$	1	1	2
$t^2 + 2$	2	0	0
$2t^2$	0	2	2
$2t^2 + 1$	1	0	0
$2t^2 + 2$	2	2	1

1.1 lentelė: Pavidalo $at^2 + b$ polinomų reikšmės.

Taigi kūnas

$$\mathbb{F}_3[t]/(t^2 + 1) = \{a + bt + (t^2 + 1) : a, b \in \mathbb{F}_3\}$$

turi lygiai 9 elementus. Svarbu atsiminti, kad šiame kūne $\overline{t^2 + 1} = \overline{0}$, todėl $\overline{t^2} = \overline{-1} = \overline{2}$. Štai keletas aritmetinių veiksmų pavyzdžių šiame kūne:

$$\overline{t + 1} + \overline{2t + 1} = \overline{3t + 2} = \overline{2},$$
$$\overline{t + 1} \cdot \overline{t + 1} = \overline{t^2 + 2t + 1} = \overline{2 + 2t + 1} = \overline{2t}$$

1.3 Kūno plėtiniai ir skaidinio kūnas

Nagrinėjant kūno savybes, ypač kalbant apie tam tikro laipsnio šaknų egzistavimą, prireiks kelių papildomų įrankių, kurie padės nagrinėti atitinkamas polinomų šaknis.

2 apibrėžimas ([5, p. 223])**.** Tegul E ir F – kūnai. Jei $F \subset E$, tai kūnas E vadinamas kūno F **plėtiniu** ir žymima $E : F$.

Nesunku suvokti, kad kūnas E yra tiesinė erdvė virš kūno F. Ši interpretacija leidžia taikyti tiesinės algebros metodus ir labai praverčia nagrinėjant kūnų plėtinius (žr. [7]). Tiesinės erdvės E virš F dimensija žymima $[E : F]$ ir vadinama plėtinio $E : F$ **laipsniu**. Jei $[E : F] < \infty$, tai plėtinys $E : F$ vadinamas **baigtiniu**. Priešingu atveju plėtinys vadinamas **begaliniu**. Verta pastebėti, kad jei plėtinys $E : F$ yra baigtinis, tai nebūtinai kūnas E yra baigtinis. Pavyzdžiui, kompleksinių skaičių kūnas $\mathbb{C}$ yra begalinis, nors plėtinys $\mathbb{C} : \mathbb{R}$ yra baigtinis (jo laipsnis lygus 2). Kita vertus, plėtinys $\mathbb{R} : \mathbb{Q}$ yra begalinis (jei jis būtų baigtinis, tai aibė $\mathbb{R}$ būtų skaičioji).

3 apibrėžimas ([7, p.71])**.** Tegul $E : F$ – kūnų plėtinys. Elementas $\alpha \in E$ vadinamas **algebriniu virš** F, jei jis yra kokio nenulinio polinomo iš $F[x]$ šaknis, t. y. jei egzistuoja toks nenulinis polinomas $p(x) \in F[x]$, kad $p(\alpha) = 0$.

Pavyzdžiui, skaičius $\sqrt{2}$ yra algebrinis virš $\mathbb{Q}$, nes jis yra polinomo $x^2 - 2$ šaknis. Kita vertus, gerai žinoma, kad skaičius π nėra algebrinis virš $\mathbb{Q}$ (bet yra algebrinis virš $\mathbb{R}$, nes yra polinomo $x - \pi$ šaknis).

4 apibrėžimas ([7, p.129])**.** Tegul F – kūnas. Plėtinys $E : F$ vadinamas polinomo $p(x) \in F[x]$ **skaidinio kūnu**, jei tenkinamos šios dvi sąlygos:

1) polinomas $p(x)$ žiede $E[x]$ užrašomas pirmojo laipsnio polinomų sandauga;

2) jei E' ir L yra tokie kūnai, kad $F \subset E' \subset M$, $E \subset M$ ir plėtinys $E' : F$ taip pat tenkina 1) sąlygą, tai $E' = E$.

Apibrėžimo antroji sąlyga reiškia, kad skaidinio kūnas yra pats mažiausias kūnas E, tenkinantis apibrėžimo pirmąją sąlygą. Akivaizdu, kad skaidinio kūnas gaunamas sukirtus visus kūno M pokūnius, tenkinančius apibrėžimo pirmąją sąlygą.

2 pavyzdys. Virš kūno $\mathbb{Q}$ polinomas $f(x) = x^2 + 1$ nesiskaidys į pirmo laipsnio polinomus, tačiau mes galime prijungti kompleksinį vienetą i prie kūno $\mathbb{Q}$, i yra

algebrinis virš $\mathbb{Q}$ ir plėtinys $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ bus šio polinomo skaidinio kūnas.

3 pavyzdys. Mes galime traktuoti $\mathbb{F}_q$ kaip plėtinį virš $\mathbb{F}_p$, imkime pavyzdį $\mathbb{F}_9 : \mathbb{F}_3$, kur

$$\mathbb{F}_3[t]/(t^2 + 1) \cong \mathbb{F}_9$$

Virš kūno $\mathbb{F}_3$ polinomas $f(x) = x^9 - x$ turi dvi šaknis, 0 ir 1, tačiau tiesiškai neišsiskaido, bet virš $\mathbb{F}_9$ išsiskaido:

$$x^9 - x = \prod_{a \in \mathbb{F}_9} (x - a).$$

Taigi kūnas $\mathbb{F}_9$ yra polinomo $x^9 - x \in \mathbb{F}_3[x]$ skaidinio kūnas. Panašiai yra ir bendruoju atveju – kūnas $\mathbb{F}_{p^n}$ yra polinomo $x^{p^n} - x \in \mathbb{F}_p[x]$ skaidinio kūnas, kur $n \in \mathbb{N}$, o p yra pirminis skaičius.

2 skyrius

Oilerio kriterijus ir jo apibendrinimas

Mums svarbu išnagrinėti, kada ir kokie kūno elementai turės šaknį kūne $\mathbb{F}_q$, Oilerio kriterijus mums sako, kada elementas turės kvadratinę šaknį. Patį kriterijų galimą apibendrinti iki bet kokio p laipsnio ir bet kokio laipsnio šaknies.

2.1 Oilerio kriterijus

1 teorema (Oilerio kriterijus, [1, 3, 6])**.** *Tegul $p > 2$ – pirminis skaičius, $\mathbb{F}_p^*$ - kūno $\mathbb{F}_p$ multiplikatyvioji grupė, sudaryta iš šio kūno nenulinių elementų, ir $a \in \mathbb{F}_p^*$. Lygtis $a = x^2$ turi sprendinį kūne $\mathbb{F}_p$ tada ir tik tada, kai*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Įrodymas. Yra žinoma, kad bet kurio baigtinio kūno $\mathbb{F}_q$ multiplikatyvioji grupė $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ yra ciklinė (žr. [3, p. 80]). Todėl egzistuoja toks $g \in \mathbb{F}_p^*$, kad

$$\mathbb{F}_p^* = \{g^i : i = 0, 1, \ldots, p-1\}.$$

Vadinasi, egzistuoja toks $k \in \{0, 1, \ldots, p-1\}$, kad $a = g^k$. Tada

$$a^{(p-1)/2} = g^{k(p-1)/2}.$$

Kadangi g yra $p-1$ eilės elementas, tai $g^{k(p-1)/2} = 1$ tada ir tik tada, kai skaičius $k(p-1)/2$ dalijasi iš $p-1$. Taip yra tada ir tik tada, kai skaičius k yra lyginis. Belieka pastebėti, kad elementas $a = g^k$ yra kvadratas tada ir tik tada, kai skaičius k yra lyginis. □

2.2 Apibendrintas Oilerio kriterijus

Oilerio kriterijų galima apibendrinti bet kuriam baigtiniam kūnui $\mathbb{F}_{p^n}$, $p > 2$.

2 teorema (Apibendrintas Oilerio kriterijus, [1]). *Tegul $q = p^n$, kur $p > 2$ – pirminis skaičius, $n \in \mathbb{N}$, $\mathbb{F}_q^*$ - kūno $\mathbb{F}_q$ multiplikatyvioji grupė, sudaryta iš šio kūno nenulinių elementų, ir $a \in \mathbb{F}_q^*$. Lygtis $a = x^2$ turi sprendinį kūne $\mathbb{F}_q$ tada ir tik tada, kai*

$$a^{(q-1)/2} \equiv 1 \pmod{q}.$$

Įrodymas (pagal [1]). Kūnas $\mathbb{F}_q$ yra vienareikšmiškai apibrėžtas (izomorfizmo tikslumu) kaip polinomo $f(x) = x^q - x$ skaidinio kūnas [5, p. 236], kurį sudaro visos $f(x)$ šaknys.

Lygtis $a = x^2$ turi šaknį kūne $\mathbb{F}_q$ tada ir tik tada, kai polinomas $x^2 - a$ išsiskaido į tiesinius daugiklius žiede $\mathbb{F}_q[x]$. Taip yra tada ir tik tada, kai polinomas $x^2 - a$ yra polinomo $f(x) = x^q - x$ daliklis. Perrašykime šį polinomą:

$$f(x) = x^q - x = x \cdot x^{q-1} - x = x(x^{q-1} - 1) = x((x^2)^{\frac{q-1}{2}} - 1) =$$
$$= x((x^2 - a + a)^{\frac{q-1}{2}} - 1) = x\left((x^2 - a + a)^{\frac{q-1}{2}} - a^{\frac{q-1}{2}} + a^{\frac{q-1}{2}} - 1\right).$$

Remiantis tapatybe $X^n - Y^n = (X - Y)(X^{n-1} + X^{n-2}Y + \cdots + Y^{n-1})$, gauname, kad polinomas $(x^2 - a + a)^{\frac{q-1}{2}} - a^{\frac{q-1}{2}}$ dalijasi iš polinomo $x^2 - a$, todėl egzistuoja toks polinomas $h(x) \in \mathbb{F}_q[x]$, kad $(x^2 - a + a)^{\frac{q-1}{2}} - a^{\frac{q-1}{2}} = (x^2 - a)h(x)$. Taigi

$$f(x) = x\left((x^2 - a)h(x) + a^{\frac{q-1}{2}} - 1\right) = (x^2 - a)xh(x) + \left(a^{\frac{q-1}{2}} - 1\right)x.$$

Gavome, kad polinomo $f(x)$ dalybos iš $x^2 - a$ liekana lygi $\left(a^{\frac{q-1}{2}} - 1\right)x$. Taigi polinomas $f(x)$ dalijasi iš $x^2 - a$ tada ir tik tada, kai $a^{\frac{q-1}{2}} - 1 = 0$. Todėl ir lygtis $a = x^2$ turi šaknį kūne $\mathbb{F}_q$ tada ir tik tada, kai $a^{\frac{q-1}{2}} = 1$. □

4 pavyzdys. Nagrinėkime baigtinį kūną $\mathbb{F}_9$. Kadangi

$$\overline{2}^{(9-1)/2} = \overline{2}^4 = \overline{1}$$

$$\overline{t}^4 = (\overline{t}^2)^2 = \overline{2}^2 = \overline{1},\ \overline{2t}^4 = \overline{2}^4 \cdot \overline{t}^4 = \overline{1} \cdot \overline{1} = \overline{1}$$

tai, remiantis apibendrintu Oilerio kriterijumi, lygtis $x^2 = a$ turi sprendinį kūne $\mathbb{F}_9$ su kiekvienu $a \in \{\overline{1}, \overline{2}, \overline{t}, \overline{2t}\}$.

Antra teorema išplėtė kūną, virš kurio galėtume įvertinti kvadratinių šaknų egzistavimą, bet galima dar ir nagrinėti bet kokio r-tojo laipsnio šaknų egzistavimą. Mes turime pakankamai įrankiu ir technikos įrodyti Oilerio kriterijų bet kokiai r-tojo laipsnio šakniai.

3 skyrius

Oilerio kriterijus r-tojo laipsnio šakniai

3 teorema (Oilerio kriterijus r-tojo laipsnio šakniai, [1]). *Tegul $q = p^n$, kur $p > 2$ – pirminis skaičius, $n \in \mathbb{N}$, $\mathbb{F}_q^*$ - kūno $\mathbb{F}_q$ multiplikatyvioji grupė, sudaryta iš šio kūno nenulinių elementų. Tarkime, kad natūralusis skaičius r yra skaičiaus $q-1$ daliklis ir $a \in \mathbb{F}_q^*$. Tada*

1. *Lygtis $a = x^r$ turi sprendinį kūne $\mathbb{F}_q$ tada ir tik tada, kai $a^{(q-1)/r} = 1$.*
2. *Yra lygiai $\frac{q-1}{r}$ r-tųjų laipsnių grupėje $\mathbb{F}_q^*$, t. y. šioje grupėje yra lygiai $\frac{q-1}{r}$ elementų, kurie užrašomi pavidalu x^r su kokiu nors $x \in \mathbb{F}_q^*$.*

Įrodymas. 1. Vėl pasinaudosime faktu, kad kūnas $\mathbb{F}_q$ yra polinomo $f(x) = x^q - x$ skaidinio kūnas, sudarytas iš visų šio polinomo šaknų.

Tegul $a \in \mathbb{F}_q^*$. Raskime polinomo $f(x) = x^q - x$ dalybos iš polinomo $g(x) = x^r - a$ liekaną. Polinomą $f(x)$ galima perrašyti:

$$f(x) = x^q - x = x \cdot x^{q-1} - x = x(x^{q-1} - 1) = x((x^r)^{\frac{q-1}{r}} - 1) =$$
$$= x((x^r - a + a)^{\frac{q-1}{r}} - 1) = x\left((x^r - a + a)^{\frac{q-1}{r}} - a^{\frac{q-1}{r}} + a^{\frac{q-1}{r}} - 1\right).$$

Panašiai, kaip ir 2 teoremos įrodyme, matome, kad polinomas $(x^r - a + a)^{\frac{q-1}{r}} - a^{\frac{q-1}{r}}$ dalijasi iš polinomo $x^r - a$, todėl egzistuoja toks polinomas $h(x) \in \mathbb{F}_q[x]$, kad

$$(x^r - a + a)^{\frac{q-1}{r}} - a^{\frac{q-1}{r}} = (x^r - a)h(x).$$

Taigi

$$f(x) = x\left((x^r - a)h(x) + a^{\frac{q-1}{r}} - 1\right) = (x^r - a)xh(x) + \left(a^{\frac{q-1}{r}} - 1\right)x.$$

Gavome, kad polinomo $f(x)$ dalybos iš $x^r - a$ liekana lygi $\left(a^{\frac{q-1}{r}} - 1\right) x$. Taigi polinomas $f(x)$ dalijasi iš $x^r - a$ tada ir tik tada, kai $a^{\frac{q-1}{r}} - 1 = 0$. Belieka pastebėti, kad lygtis $a = x^2$ turi šaknį kūne $\mathbb{F}_q$ tada ir tik tada, kai polinomas $f(x)$ dalijasi iš polinomo $x^r - a$.

2. Atvaizdis $\psi : \mathbb{F}_q^* \to \mathbb{F}_q^*$, apibrėžtas lygybe $\psi(x) = x^r$, $x \in \mathbb{F}_q^*$, yra grupių homomorfizmas. Jo vaizdas $\psi(\mathbb{F}_q^*)$ bus sudarytas iš visų grupės $\mathbb{F}_q^*$ elementų, kurie yra r-tieji laipsniai. Tuomet vaizdas $\psi(\mathbb{F}_q^*)$ yra izomorfinis faktorgrupei $\mathbb{F}_q^*/\ker\psi$ (žr. [2, p. 115]). Čia $\ker\psi = \{x \in \mathbb{F}_q^* : \psi(x) = x^r = 1\}$ yra homomorfizmo ψ branduolys. Kadangi polinomas $x^r - 1$ turi lygiai r šaknų kūne $\mathbb{F}_q$, tai branduolys $\ker\psi$ turi lygiai r elementų. Iš čia išplaukia, kad faktorgrupė $\mathbb{F}_q^*/\ker\psi$ turi lygiai $\frac{q-1}{r}$ elementų. Vadinasi, grupėje $\mathbb{F}_q^*$ yra lygiai $\frac{q-1}{r}$ r-tųjų laipsnių. □

Straipsnyje [1] yra vienas neteisingas teiginys (žr. pastraipą prieš 4 teoremos formuluotę). Teigiama, kad jei natūralusis skaičius r nėra skaičiaus $q - 1$ daliklis, tai atvaizdis $\psi : \mathbb{F}_q^* \to \mathbb{F}_q^*$, apibrėžtas lygybe $\psi(x) = x^r$, $x \in \mathbb{F}_q^*$, yra izomorfizmas. Imkime $q = 9$ ir $r = 6$. Tuomet $\psi(1) = 1^6 = 1$ ir $\psi(2) = 2^6 = (2^3)^2 = (-1)^2 = 1$. Vadinasi, $\psi(x)$ nėra injekcija, todėl nebus ir izomorfizmas.

5 pavyzdys. $\mathbb{F}_9$ turės šaknis laipsniams $r = 2, 4, 8$, kiekvienas laipsnis atitinkamai turės $4, 2, 1$ šaknis. Įdomu pastebėti, kadangi $r = 8$ sutampa su multiplikatyviosios grupės eile, tai vienintelis elementas kuris turės šaknį bus $\overline{1}$, nes visi elementai atsivaizduos į jį.

Powers in finite fields

Summary

This work deals with the powers of elements of finite fields. The proof of the classical criterion of Euler for squares in finite fields of prime order is presented. Moreover, the proof of two generalizations of this criterion for general finite fields of odd order is presented. The work is based mainly on [1].

Literatūra

[1] A. Aabrandt, V. L. Hansen, *A note on powers in finite fields,* International Journal of Mathematical Education in Science and Technology, 47(6), 987–991, 2016.

[2] P. Drungilas, H. Markšaitis, *Algebra. I dalis,* Vilniaus universiteto leidykla, 2013.

[3] K. Ireland, M. I. Rosen, *A Classical Introduction to Modern Number Theory,* Graduate Texts in Mathematics, Springer, 1990.

[4] J. Gathen, M. Nöcker, *Computing special powers in finite fields,* Mathematics of Computation, 73(247), 1499–1523, 2003.

[5] S. Lang, *Algebra,* Springer, 2002.

[6] A. Novikas, *Skaičių teorija, paskaitų konspektas,* 2021.

[7] I. N. Stewart, *Galois Theory,* CRC Press, 2015.

[8] A. Winterhof, *On the distribution of powers in finite fields,* Finite Fields and Their Applications, 4(1), 43–54, 1998.