XI skyrius. KŪNAI

1. Kūno sąvoka

1. 1. Šiame skyriuje nagrinėsime kūnus. Kūnas – tai aibė k, kurioje apibrėžti aibės k elementų du vidiniai kompozicijos dėsniai, žymimi $+$ ir $*$, ir vadinami aibės k elementų sudėtimi ir daugyba, tenkintys tam tikrą aksiomų sistemą. Kūno k elementų sudėtis ir daugyba savo savybėmis, kurias nusako aksiomų sistema, niekuo nesiskiria nuo racionalųijų ar realiųjų skaičių sudėties ir daugybos savybių. Kyla klausimas, ar ką nors laimime, kopijuodami skaičių sudėties ir daugybos savybes? Atsakymas: taip, labai daug laimime, nes kūnų be galo daug. Be galo daug net baigtinių kūnų. Todėl įvairius objektus, pavyzdžiui, kaip tiesinių lygčių sistemas, matricų algebras ir kitus, tikslinga nagrinėti su koeficientais kūne k, o neapsiriboti tik racionaliaisiais ar realiaisiais skaičiais. Tai vienas iš svarbiausių algebros mokslo bruožų – jos universalumas, grindžiamas aksiomatiniu metodu. Algebros objektai, nusokomi aksiomų sistemomis, kuriose slypi (užprogramuotos) esminės objektų savybės, tiriami pačiu bendriausiu savo didžiulėje įvairovėje atveju.

1. 2. Kūno apibrėžimas. Aibė k joje apibrėžtų jos elementų sudėties $+$ ir daugybos $*$ atžvilgiu yra vadinama kūnu, jei

1. Aibės k elementų sudėtis $+$ yra asociatyvi, t.y. $(\forall\alpha,\beta,\gamma \in k)((\alpha+\beta)+\gamma) = (\alpha+(\beta+\gamma))$.

2. Egzistuoja neutralus elementas $0 \in k$ aibės k elementų sudėties $+$ atžvilgiu, vadinamas nuliumi, t. y. $(\exists 0 \in k)(\forall\alpha \in k)(0+\alpha=\alpha)$.

3. Kiekvienam elementui $\alpha \in k$ egzistuoja simetrinis elementas aibės k elementų sudėties $+$ atžvilgiu, vadinamas priešingu elementu elementui α ir žymimas $-\alpha$, t.y. $(\forall\alpha \in k)(\exists\beta \in k)(\alpha+\beta=0)$.

4. Aibės k elementų sudėtis $+$ yra komutatyvi, t.y. $(\forall\alpha,\beta \in k)(\alpha+\beta=\beta+\alpha)$.

5. Aibės k elementų daugyba $*$ yra asociatyvi, t.y. $(\forall\alpha,\beta,\gamma \in k)((\alpha*\beta)*\gamma) = (\alpha*(\beta*\gamma))$.

6. Egzistuoja neutralus elementas $1 \in k$ aibės k elementų daugybos $*$ atžvilgiu, vadinamas vienetu, t.y. $(\exists 1 \in k)(\forall\alpha \in k)(1*\alpha=\alpha)$.

7. Kiekvienam elementui $\alpha \in k$ egzistuoja simetrinis elementas aibės k elementų daugybos $*$ atžvilgiu, vadinamas atvirkštiniu elementu elementui α ir žymimas α^{-1}, t.y. $(\forall\alpha \in k\setminus\{0\})(\exists\beta \in k\setminus\{0\})(\alpha*\beta=1)$.

8. Aibės k elementų daugyba $*$ komutatyvi, t.y. $(\forall\alpha,\beta \in k)(\alpha*\beta=\beta*\alpha)$.

9. Aibės k elementų sudėtį $+$ ir daugybą $*$ sieja distributyvumo dėsnis, t.y. $(\forall\alpha,\beta,\gamma \in k)((\alpha+\beta)*\gamma=\alpha*\gamma+\beta*\gamma)$.

1. 3. Kai aibės k elementų sudėtis $+$ tenkina 1 – 4 aksiomas, tai aibė k sudėties $+$ atžvilgiu yra vadinama Abelio grupė. Taigi 1 – 4 aksiomas galima pakeisti tokia formuluote:

I. $(k,+)$ – Abelio grupė. Neutralus elementas sudėties $+$ atžvilgiu žymimas 0 ir yra vadinamas kūno k nuliumi.

Kūno apibrėžimo 5 – 8 aksiomas galima pakeisti tokia formuluote:

II. $(k^*,*)$– Abelio grupė, čia $k^* =: k\setminus\{0\}$. Neutralus elementas daugybos $*$ atžvilgiu yra žymimas 1 ir yra vadinamas kūno k vienetu.

9-ąją kūno apibrėžimo aksiomą galima suformuluoti taip:

III. Sudėtis $+$ ir daugyba $*$ yra susieti distributyvumo dėsniu: bet kuriems $\alpha, \beta, \gamma \in k$,

$$(\alpha + \beta) * \gamma = \alpha * \gamma + \beta * \gamma.$$

1. Pastaba. Tais atvejais, kai norėsime atkreipti dėmesį į kūno k elementų sudėtį $+$ ir daugybą $*$, rašysime: $(k, +, *)$ yra kūnas

2. Pastaba. Daugybos ženklo $*$ tarp dauginamųjų sutarkime nerašyti, išskyrus atvejus, kai būtina pabrėžti daugybos kurias nors savybes.

Pratimai.

Remdamiesi kūno k apibrėžimo aksiomomis, įrodykite:

1. Kiekvienam $\alpha \in k$, $0\alpha = 0$.

2. Jei $\alpha\beta = 0$, $\alpha, \beta \in k$, tai $\alpha = 0$ ar $\beta = 0$.

3. Kiekvienam $\alpha \in k$, $(-1)\alpha = -\alpha$, čia -1 – priešingas elementas elementui 1.

1. 4. Pavyzdžiai.

1. Racionaliųjų skaičių aibė $\mathbb{Q}$ skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

2. Įsitikinsime, kad aibė $\mathbb{Q}(\sqrt{2}) =: \{a + b\sqrt{2} |\ a, b \in \mathbb{Q}\}$ skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

Akivaizdu, kad $(\mathbb{Q}(\sqrt{2}), +)$ – Abelio grupė.

Daugyba aibėje $\mathbb{Q}(\sqrt{2})^*$ apibrėžta.

Akivaizdžios aibės $\mathbb{Q}(\sqrt{2})^*$ elementų daugybos šios savybės: i) daugyba asociatyvi; ii) daugyba komutatyvi; iii) $1 \in \mathbb{Q}(\sqrt{2})^*$, nes $1 = 1 + 0\sqrt{2}$. Įsitikinsime, kad kiekvienam $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})^*$, t. y., kai bent vienas iš koeficientų a, b yra nelygus 0, atvirkštinis elementas $(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}}$ priklauso aibei $\mathbb{Q}(\sqrt{2})^*$. Padauginę trupmenos $\frac{1}{a+b\sqrt{2}}$ skaitiklį ir vardiklį iš $a - b\sqrt{2}$, gauname:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})^*.$$

Skaičių sudėtis ir daugyba yra susieti distributyvumo dėsniu: bet kuriems $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{2})$,

$$(\alpha + \beta) * \gamma = \alpha * \gamma + \beta * \gamma.$$

Įsitikinome, kad $\mathbb{Q}(\sqrt{2})$ iš tikrųjų skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

3. Apibrėžkime aibę $k = \mathbb{Q}(\sqrt{p}) =: \{a + b\sqrt{p} |\ a, b \in \mathbb{Q}\}$, čia p – pirminis skaičius. Taip pat, kaip ir antrajame pavyzdyje, galite įsitikinti, kad aibė $\mathbb{Q}(\sqrt{p})$ skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

4. Tarkime, kad $\mathbb{Q}(\sqrt[3]{p}) =: \{a + b\sqrt[3]{p} + c\sqrt[3]{p}^2 |\ a, b, c \in \mathbb{Q}\}$, čia p – pirminis skaičius. Akivaizdu, kad skaičių sudėtis $+$ ir daugyba $\cdot$ aibėje $\mathbb{Q}(\sqrt[3]{p})$ apibrėžti. Taip pat lengva įsitikinti,

kad sudėtis ir daugyba tenkina visas kūno apibrėžimo aksiomas, išskyrus 7-ąją, kaip ir 2-me ir 3-me pavyzdžiuose. Tuo tarpu įsitikinti, ar

$$\frac{1}{a + b\sqrt[3]{p} + c\sqrt[3]{p^2}} \in \mathbb{Q}(\sqrt[3]{p}),$$

čia $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \neq 0$, nėra taip paprasta, kaip 2-ne ar 3-me pavyzdžiuose. Jei

$$\frac{1}{a + b\sqrt[3]{p} + c\sqrt[3]{p^2}} \in \mathbb{Q}(\sqrt[3]{p}),$$

tai egzistuoja tokie $x, y, z \in \mathbb{Q}$, kad

$$\frac{1}{a + b\sqrt[3]{p} + c\sqrt[3]{p^2}} = x + y\sqrt[3]{p} + z\sqrt[3]{p^2}.$$

Šią lygybę perrašykime taip:

$$(a + b\sqrt[3]{p} + c\sqrt[3]{p^2})(x + y\sqrt[3]{p} + z\sqrt[3]{p^2}) = 1.$$

Šios lygybės kairėje pusėje esančius skaičius sudauginę, gauname:

$$ax + cpy + bpz + (bx + ay + cpz)\sqrt[3]{p} + (cx + by + az)\sqrt[3]{p^2} = 1 + 0\sqrt[3]{p} + 0\sqrt[3]{p^2}.$$

Šiame reiškinyje sulyginę koeficientus prie 1, $\sqrt[3]{p}$ ir $\sqrt[3]{p^2}$, gauname lygčių sistemą:

$$\begin{cases} ax & +cpy & +bpz & = 1 \\ bx & +ay & +cpz & = 0 \\ cx & +by & +az & = 0 \end{cases}$$

Šią lygčių sistemą išspręsime Kramerio metodu. Matricos, sudarytos iš koeficientų prie nežinomųjų, determinantas yra lygus:

$$\det\begin{pmatrix} a & cp & bp \\ b & a & cp \\ c & b & a \end{pmatrix} = a^3 + b^3p + c^3p^2 - 3abcp.$$

Tuomet

$$x = \frac{\det\begin{pmatrix} 1 & cp & bp \\ 0 & a & cp \\ 0 & b & a \end{pmatrix}}{a^3 + b^3p + c^3p^2 - 3abcp} = \frac{a^2 - bcp}{a^3 + b^3p + c^3p^2 - 3abcp},$$

$$y = \frac{\det\begin{pmatrix} a & 1 & bp \\ b & 0 & cp \\ c & 0 & a \end{pmatrix}}{a^3 + b^3p + c^3p^2 - 3abcp} = \frac{c^2p - ab}{a^3 + b^3p + c^3p^2 - 3abcp},$$

$$z=\frac{\det\begin{pmatrix} a & cp & 1\\ b & a & 0\\ c & b & 0\end{pmatrix}}{a^3+b^3p+c^3p^2-3abcp}=\frac{b^2-ac}{a^3+b^3p+c^3p^2-3abcp}.$$

Vadinasi, jei $a+b\sqrt[3]{p}+c\sqrt[3]{p}^2\neq 0,\ a,b,c\in\mathbb{Q}$, tai

$$(a+b\sqrt[3]{p}+c\sqrt[3]{p}^2)^{-1}=\frac{a^2-bcp}{a^3+b^3p+c^3p^2-3abcp}+$$

$$+\frac{c^2p-ab}{a^3+b^3p+c^3p^2-3abcp}\sqrt[3]{p}+\frac{b^2-ac}{a^3+b^3p+c^3p^2-3abcp}\sqrt[3]{p}^2\in\mathbb{Q}(\sqrt[3]{p}).$$

Įsitikinome, kad $\mathbb{Q}(\sqrt[3]{p})$ skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

Pratimas. Remdamiesi pagrindine aritmetikos teorema, įrodykite, kad lygtis $a^3+b^3p+c^3p^2-3abcp=0$ sveikaisiais skaičiais turi tik nulinį sprendinį. Kadangi ši lygtis yra homogeninė, tai ji ir racionaliaisiais skaičiais turi tik nulinį sprendinį.

5. Galima, pavyzdžiui, nagrinėti skaičių aibę

$$\mathbb{Q}(\sqrt[n]{p})=:\{\sum_{j=0}^{n-1}a_j\sqrt[n]{p}^j\mid a_j\in\mathbb{Q},\ 0\leq j\leq n-1\},$$

čia p – pirminis skaičius. Lengva įsitikinti, kad skaičių sudėtis ir daugyba apibrėžti aibėje $\mathbb{Q}(\sqrt[n]{p})$, t. y. bet kuriems $\alpha,\beta\in\mathbb{Q}(\sqrt[n]{p})$, $\alpha+\beta,\alpha\beta\in\mathbb{Q}(\sqrt[n]{p})$. Taip pat lengva įsitikinti, kad aibės $\mathbb{Q}(\sqrt[n]{p})$ skaičių sudėtis ir daugyba tenkina visas, išskyrus 7-ąją, kūno apibrėžimo aksiomas. Įrodyti tiesiogiai, t. y. taip, kaip darėme 4-me pavyzdyje, kad kiekvienam $\alpha=\sum_{j=0}^{n-1}a_j\sqrt[n]{p}^j\in\mathbb{Q}(\sqrt[n]{p})$, $\alpha\neq 0$, egzistuoja toks $\sum_{j=0}^{n-1}x_j\sqrt[n]{p}^j\in\mathbb{Q}(\sqrt[n]{p})$, kad

$$(\sum_{j=0}^{n-1}a_j\sqrt[n]{p}^j)(\sum_{j=0}^{n-1}x_j\sqrt[n]{p}^j)=1,$$

ne taip paprasta. Darant taip, kaip darėme 4-me pavyzdyje, prisieitų spręsti tiesinių lygčių sistemą, sudarytą iš n lygčių su n nežinomaisiais. Sprendžiant Kramerio metodu, reikėtų apskaičiuoti $n+1$ n-tos eilės determinantų. Tiesa, norint įrodyti, kad lygčių sistema yra suderinta, t. y. turi sprendinį, pakaktų įrodyti, kad matricos, sudarytos iš koeficientų prie nežinomųjų, determinantas yra nelygus nuliui. Šio determinanto išraiška gana sudėtinga: bendruoju atveju galime tvirtinti, kad šis determinantas yra koeficientų a_j, $0\leq j\leq n-1$, n-ojo laipsnio homogeninis polinomas $F(a_0,a_1,\ldots,a_{n-1})$. Taigi reikėtų įrodyti, kad lygtis $F(a_0,a_1,\ldots,a_{n-1})=0$ racionaliaisiais skaičiais turi tik nulinį sprendinį. Visas šias kliūtis galima apeiti šį uždavinį sprendžiant kitu būdu.

6. Įrodysime, kad kiekvienam pirminiam skaičiui p, likinių klasės $j+p\mathbb{Z}$, $0\leq j<p$, kurios gaunamos dalijant sveikuosius skaičius iš pirminio skaičiaus p, likinių klasių sudėties ir

daugybos atžvilgiu sudaro kūną. Šis kūnas yra žymimas $GF(p)$ ir yra vadinamas Galua kūnu (baigtiniai kūnai yra vadinami Galua kūnais, nes Galua pirmasis juos visus atrado ir ištyrė).

Kitaip tariant, $GF(p) = \mathbb{Z}/p\mathbb{Z} = \{p\mathbb{Z}, 1+p\mathbb{Z}, \dots, p-1+p\mathbb{Z}\}$. Primiminsime, kad $i+p\mathbb{Z} = j+p\mathbb{Z}$ tada ir tik tada, kai $p|i-j$, $(i+p\mathbb{Z})+(j+p\mathbb{Z}) = i+j+p\mathbb{Z}$, $(i+p\mathbb{Z})(j+p\mathbb{Z}) = ij+p\mathbb{Z}$. Akivaizdu, kad likinių klasių sudėtis ir daugyba tenkina visas, išskyrus galbūt 7-ąją, kūno apibrėžimo aksiomas. Įsitikinsime, kad likinių klasių daugyba tenkina ir 7-ąją aksiomą.

Imkime nenulinį aibės $GF(p)$ elementą $i + p\mathbb{Z}$, t. y. $p \not| i$. Kadangi p – pirminis skaičius ir p nedalija i, tai skaičių p ir i didžiausias bendrasis daliklis yra lygus 1. Vadinasi, egzistuoja tokie $j, l \in \mathbb{Z}$, kad $ij + pl = 1$. Tuomet $(i + p\mathbb{Z})(j + p\mathbb{Z}) = ij + p\mathbb{Z} = 1 - pl + p\mathbb{Z} = 1 + p\mathbb{Z}$. Kaip matome, elementui $i+p\mathbb{Z}$, $p \not| i$, egzistuoja atvirkštinis elementas $j+p\mathbb{Z}$. Taigi įrodėme, kad $GF(p)$ likinių sudėties ir daugybos atžvilgiu yra kūnas.

2. Pirminiai kūnai

2. 1. Šiame skyrelyje aprašysime mažiausius kūnus, t. y. tokius kūnus, kurie neturi pokūnių.

Apibrėžimas. Jei $(K, +, *)$ yra kūnas, tai aibės K poaibis k, kuris sudėties $+$ ir daugybos $*$ atžvilgiu yra taip pat kūnas, yra vadinamas kūno K pokūniu.

2. 2. Apibrėžimas. Kūnas k yra vadinamas pirminiu kūnu, jei k neturi jokių pokūnių, išskyrus patį kūną k.

Mums reikalinga dar viena svarbi sąvoka.

2. 3. Apibrėžimas. Kūnai $(K, +, *)$ ir $(L, +, *)$ yra vadinami izomorfiniais, jei egzistuoja tokia bijecija $f : K \to L$, kad bet kuriems $\alpha, \beta \in K$,

1. $f(\alpha + \beta) = f(\alpha) + f(\beta)$;
2. $f(\alpha * \beta) = f(\alpha) * f(\beta)$.

2. 4. Kūnų teorijos požiūriu izomorfiniai kūnai identiški. Svarbiausias kūnų teorijos uždavinys – aprašyti kūnus izomorfizmo tikslumu. Pirminius kūnus aprašysime izomorfizmo tikslumu.

Sakykime, k – pirminis kūnas. Sutarkime laikinai kūno k vienetą žymėti e, o ne 1, kad nepainiotume su natūraliųjų skaičių vienetu. Kūno k vienetą e sudėję su savimi n kartų, n – teigiamas sveikasis skaičius, gauname kūno k elementą $\underbrace{e + e + \ldots + e}_{n}$, kurį sutarkime žymėti ne. Matematinės indukcijos metodu galite įsitikinti, kad bet kuriems teigiamiems sveikiesiems skaičiams m, n,

1. $(m + n)e = me + ne$;
2. $(mn)e = m(ne)$.

Panašiai apibrėžkime $n(-e) = \underbrace{(-e) + (-e) + \ldots + (-e)}_{n}$, čia n – teigiamas sveikasis skaičius. Ir šiuo atveju teisingos lygybės: bet kuriems teigiamiems sveikiesiems skaičiams m, n,

1. $(m + n)(-e) = m(-e) + n(-e)$;
2. $(mn)(-e) = m(n(-e))$.

Akivaizdu, kad kiekvienam teigiamam sveikajam skaičiui n, $n(-e) = -(ne)$. Taigi galime apibrėžti ne, kai $n \in \mathbb{Z}$. Teigiamam sveikajam skaičiui n apibrėžėme ne. Jei n – neigiamas sveikasis skaičius, tai ne apibrėžkime taip: $ne = (-n)(-e) = -((-n)e)$. Kai $n = 0$, tai apibrėžkime $0e = 0$. Dabar galite įsitikinti, kad bet kuriems $m, n \in \mathbb{Z}$,

1. $(m+n)e = me + ne$;
2. $(mn)e = m(ne)$.

Apibrėžkime sveikųjų skaičių ir kūno k elementų daugybą: $n\alpha =: (ne)\alpha$, $n \in \mathbb{Z}$, $\alpha \in k$.

Akivaizdžiai teisingos lygybės: bet kuriems $m, n \in \mathbb{Z}$, $\alpha, \beta \in k$,

1. $(m+n)\alpha = m\alpha + n\alpha$;
2. $n(\alpha + \beta) = n\alpha + n\beta$;
3. $(mn)\alpha = m(n\alpha)$;
4. $n(\alpha\beta) = (n\alpha)\beta$.

2. 5. Tarkime, kad k – pirminis kūnas, e – šio kūno vienetas. Galimi du atvejai: i) kiekvienam natūraliajam $n \geq 1$, $ne \neq 0$; ii) Egzistuoja toks natūralusis skaičius $n_0 > 1$, kad $n_0 e = 0$. Aptarsime kiekvieną iš šių atvejų.

Tarkime, kad kiekvienam natūraliajam $n \geq 1$, $ne \neq 0$. Tuomet ir kiekvienam sveikajam skaičiui $n \neq 0$, $ne \neq 0$. Kūno k elementus ne, $n \in \mathbb{Z}$, galime sutapatinti su sveikaisiais skaičiais $n \in \mathbb{Z}$. Vadinasi, galime parašyti: $\mathbb{Z} \subset k$. Kadangi k – kūnas, o sveikųjų skaičių santykiai sudaro racionaliųjų skaičių kūną $\mathbb{Q}$, tai gauname, kad racionaliųjų skaičių kūnas $\mathbb{Q}$ yra kūno k pokūnis, t. y. galime parašyti $\mathbb{Q} \subset k$. Kadangi k – pirminis kūnas, tai $\mathbb{Q} = k$. Pirminis kūnas $\mathbb{Q}$ yra vadinamas nulinės charakteristikos kūnu.

Teiginys. Kiekvienas nulinės charakteristikos pirminis kūnas yra izomorfinis racionaliųjų skaičių kūnui $\mathbb{Q}$.

Dabar aptarsime antrąjį atvejį, kai egzistuoja toks natūralusis skaičius $n_0 > 1$, kad $n_0 e = 0$. Šiuo atveju egzistuoja toks mažiausias teigiamas sveikasis skaičius $p > 1$, kad $pe = 0$, o kiekvienam j, $1 \leq j < p$, $je \neq 0$. Įrodysime, kad p yra pirminis skaičius.

Tarkime, kad $p = p_1 p_2$, $p_1 < p$, $p_2 < p$. Tuomet $pe = (p_1 p_2)e = (p_1 e)(p_2 e) = 0$. Vadinasi, bent vienas iš kūno k elementų $p_1 e$ ar $p_2 e$ yra nulinis elementas. Vienu ar kitu atveju gauname prieštarą skaičiaus p parinkimui, nes $p > 1$ mažiausias teigiamas sveikasis skaičius toks, kad $pe = 0$. Taigi įrodėme, kad p – pirminis skaičius.

2. 6. Apibrėžimas. Sakykime, k – kūnas, e – šio kūno vienetas. Jei egzistuoja toks pirminis skaičius $p \in \mathbb{N}$, kad $pe = 0$, tai k yra vadinamas p charakteristikos kūnu, o pirminis skaičius p – kūno k charakteristika.

Teiginys. Kiekvienam pirminiam skaičiui $p \in \mathbb{N}$ egzistuoja p charakteristikos pirminis kūnas. Kiekvienas p charakteristikos pirminis kūnas yra izomorfinis likinių klasių moduliu p kūnui $GF(p)$.

Įrodymas. Pastebėsime, kad kiekvienam pirminiam skaičiui $p \in \mathbb{N}$, Galua kūnas $GF(p)$ yra pirminis, jo charakteristika yra lygi p. Iš tikrųjų, $p(1 + p\mathbb{Z}) = p + p\mathbb{Z} = p\mathbb{Z}$, t. y. kūno $GF(p)$ vienetas $1 + p\mathbb{Z}$, padaugintas iš pirminio skaičiaus p, yra lygus šio kūno nuliniam elementui $p\mathbb{Z}$. Taigi, kaip matome, kiekvienam pirminiam skaičiui $p \in \mathbb{N}$ egzistuoja p charakteristikos pirminis kūnas. Lieka įrodyti, kad kiekvienas p charakteristikos pirminis kūnas yra izomorfinis kūnui $GF(p)$.

Sakykime, k – p charakteristikos pirminis kūnas, e – šio kūno vienetas. Įrodysime, kad kūno k elementai 0, e, $2e$, ... , $(p-1)e$ sudaro kūno k pokūnį, izomorfinį Galua kūnui $GF(p)$. Kadangi k – pirminis kūnas, tai gausime, kad k yra izomorfinis kūnui $GF(p)$.

Pastebėsime, kad kūno k elementai 0, e, $2e$, ... , $(p-1)e$ yra tarp savęs skirtingi. Apibrėžkime atvaizdį

$$f : \mathbb{Z} \to k, \ f(j) = je, \ j \in \mathbb{Z}.$$

Šis atvaizdis turi savybes: bet kuriems $i, j \in \mathbb{Z}$,

1. $f(i+j) = f(i) + f(j)$. Iš tikrųjų: $f(i+j) = (i+j)e = ie + je = f(i) + f(j)$;
2. $f(ij) = f(i)f(j)$. Iš tikrųjų: $f(ij) = (ij)e = (ie)(je) = f(i)f(j)$.

Taigi $f : \mathbb{Z} \to k$ yra žiedų homomorfizmas. $f(j) = 0$ tada ir tik tada, kai $p|j$, t. y. $j \in p\mathbb{Z}$. Vadinasi, atvaizdis

$$\bar{f} : \mathbb{Z}/p\mathbb{Z} = GF(p) \to k, \ \bar{f}(j + p\mathbb{Z}) = f(j), \ j \in \mathbb{Z},$$

yra injektyvus homomorfizmas. Kaip matome, Galua kūnas $GF(p)$ yra izomorfinis savo vaizdui $\bar{f}(GF(p)) = \{0, e, 2e, \dots, (p-1)e\}$. $\triangle$

2. 7. Kaip matome, pirminiai kūnai yra šie: i) kiekvienas nulinės charakteristikos pirminis kūnas yra izomomorfinis racionaliųjų skaičių kūnui; ii) kiekvienam pirminiam skaičiui $p \in \mathbb{N}$ carakteristikos p pirminis kūnas yra izomorfinis kūnui $GF(p)$.

3. Kūnų plėtiniai

3. 1. Apibrėžimas. Kūnas K yra vadinamas kūno k plėtiniu, jei k yra kūno K pokūnis.

Teiginys. Kiekvienas kūnas yra vienintelio pirminio pokūnio plėtinys.

Įrodymas. Sakykime, K – kūnas. Šio kūno visų pokūnių sankirta $\bigcap\limits_{k \subset K} k = k_0$ yra pirminis kūnas, nes k_0 neturi pokūnių, išskyrus jį patį. $\triangle$

3. 2. Apibrėžimas. Jei kūno k pirminis pokūnis yra izomorfinis racionaliųjų skaičių kūnui, tai k yra vadinamas nulinės charakteristikos kūnu.

Pastebėsime, jei k nulinės charakteristikos kūnas, tai kiekvienam nenuliniam sveikajam skaičiui n ir kiekvienam $\alpha \in k$, $\alpha \neq 0$, $n\alpha \neq 0$.

3. 3. Apibrėžimas. Jei kūno k pirminis pokūnis yra izomorfinis kūnui $GF(p)$, $p \in \mathbb{N}$ – pirminis skaičius, tai k yra vadinamas p charakteristikos kūnu.

Pastebėsime, jei k yra p charakteristikos kūnas, tai kiekvienam $\alpha \in k$, $p\alpha = 0$. Iš tikrųjų: $p\alpha = p(e\alpha) = (pe)\alpha = 0\alpha = 0$.

Teiginys. Jei k – p charakteristikos kūnas, $p \in \mathbb{N}$ – pirminis skaičius, tai bet kuriems $\alpha, \beta \in k$,

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}, \ m \in \mathbb{N}.$$

Įrodymas. Įrodysime matematinės indukcijos metodu.

Kadangi α ir β yra perstatomi, remdamiesi Niutono binomo formule, galime parašyti lygybę:

$$(\alpha+\beta)^p = \sum_{j=1}^{p} \binom{p}{j} \alpha^j \beta^{p-j}.$$

Niutono binomo koeficientai

$$\binom{p}{j} = \frac{p!}{j!(p-j)!},\ 1 \le j \le p-1,$$

dalijasi iš pirminio skaičiaus p. Iš tikrųjų: kadangi Niutono binomo koeficiento skaitiklis dalijasi iš pirminio skaičiaus p, o vardiklis – nesidalija, remdamiesi pagrindine aritmetikos teorema, gauname $p|\binom{p}{j}$. Vadinasi, galime parašyti:

$$(\alpha+\beta)^p = \alpha^p + \beta^p.$$

Sakykime, kad kiekvienam $m \in \mathbb{N}$, $m < s$,

$$(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}.$$

Tuomet

$$(\alpha+\beta)^{p^s} = ((\alpha+\beta)^{p^{s-1}})^p = (\alpha^{p^{s-1}} + \beta^{p^{s-1}})^p =$$
$$= (\alpha^{p^{s-1}})^p + (\beta)^{p^{s-1}})^p = \alpha^{p^s} + \beta^{p^s}. \quad \triangle$$

4. Algebriniai ir transcendentiniai elementai

4. 1. Dabar nagrinėsime kūno k plėtinį K. Plėtinio K elementai pokūnio k atžvilgiu yra skirstomi į algebrinius ir transcendentinius.

Apibrėžimas. Sakykime, K yra kūno k plėtinys. Kūno K elementas θ yra vadinamas algebriniu virš k, jei egzistuoja toks polinomas $f(x) \in k[x]$, kad $f(\theta) = 0$. Priešingu atveju kūno K elementas θ yra vadinamas transcendentiniu virš k. Kitaip tariant, kūno K elementas θ yra transcendentinis virš k, jei kiekvienam nenuliniam polinomui $f(x) \in k[x]$, $f(\theta) \neq 0$.

Pavyzdžiai.

1. Sakykime, $k(x)$ – x kintamojo polinomų žiedo $k[x]$ virš kūno k santykių kūnas. Kūno $k(x)$ elementai, – tai polinomų santykiai $\frac{f(x)}{g(x)}$, $f(x), g(x) \in k[x]$, $g(x) \neq 0$. Polinomų santykiai $\frac{f_1(x)}{g_1(x)}$ ir $\frac{f_2(x)}{g_2(x)}$, $g_1(x) \neq 0$, $g_2(x) \neq 0$, yra lygūs kūno $k(x)$ elementai tada ir tik tada, kai $f_1(x)g_2(x) = g_1(x)f_2(x)$. Kūno $k(x)$ elementas x yra transcendentinis virš kūno k. Iš tikrųjų kiekvienas kūno $k(x)$ elementas, nepriklausantis k, yra transcendentinis virš k.

2. Panašiai, kaip ir pirmajame pavyzdyje, $k(x_1, x_2, \ldots, x_n)$ – n kintamųjų polinomų žiedo $k[x_1, x_2, \ldots, x_n]$ santykių kūnas, t. y. kintamųjų $x_1, x_2, \ldots, x_n$ racionaliųjų funkcijų kūnas. Kūno $k(x_1, x_2, \ldots, x_n)$ elementai $x_1, x_2, \ldots, x_n$ yra transcendentiniai virš kūno k. Šie elementai yra vadinami algebriškai nepriklausomais, nes neegzistuoja nenulinis polinomas $f(t_1, t_2, \ldots, t_n) \in k[t_1, t_2, \ldots, t_n]$ toks, kad būtų teisinga lygybė $f(x_1, x_2, \ldots, x_n) = 0$. Kaip

ir pirmajame pavyzdyje, kiekvienas racionaliųjų funkcijų kūno $k(x_1, x_2, \ldots, x_n)$ elementas, nepriklausantis k, yra transcendentinis virš k.

4. 2. Jei $\theta \in K$ yra algebrinis virš kūno K pokūnio k, tai egzistuoja toks mažiausio laipsnio polinomas $f(x) \in k[x]$, kad $f(\theta) = 0$. Polinomas $f(x)$ yra pirminis virš kūno k (neredukuojamas, neskaidomas polinomų žiede $k[x]$). Iš tikrųjų, jei būtų $f(x) = g(x)h(x)$, $\deg g(x) < \deg f(x)$, $\deg h(x) < \deg f(x)$, $g(x), h(x) \in k[x]$, tai gautume $g(\theta) = 0$ ar $h(\theta) = 0$, kas prieštarautų tam, kad polinomas $f(x) \in k[x]$ mažiausio laipsnio, kurio šaknimi yra θ. Be to, polinomą $f(x)$ galime normuoti, padauginę $f(x)$ iš atvirkštinio elemento koeficientui prie polinomo $f(x)$ aukščiausiojo x-o laipsnio. Mažiausio laipsnio normuoto polinomo $f(x) \in k[x]$, kurio šaknimi yra θ, koeficientas prie aukščiausiojo x laipsnio yra lygus 1.

Apibrėžimas. Jei elementas $\theta \in K$ yra algebrinis virš kūno K pokūnio k, tai mažiausio laipsnio normuotas polinomas $f(x) \in k[x]$, kurio šaknimi yra θ, t. y. $f(\theta) = 0$, yra vadinamas algebrinio elemento θ virš kūno k minimaliuoju polinomu.

Teiginys. Tarkime, kad $\theta \in K$ yra algebrinis virš pokūnio k, $f(x) = x^n + a_{n-1} + \ldots + a_1 x + a_0 \in k[x]$ – elemento θ normuotas minimalusis polinomas. Tuomet

$$k(\theta) =: \{b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1} |\, b_j \in k,\ 0 \le j \le n-1\}$$

yra mažiausias kūno K pokūnis, kuriam priklauso pokūnio k elementai ir elementas θ (kitaip tariant, $k(\theta)$ yra mažiausias pokūnio k plėtinys, kuriam priklauso elementas θ). $k(\theta)$ yra baigtinės dimensijos tiesinė erdvė virš kūno k, $\dim_k k(\theta) = \deg f(x) = n$.

Įrodymas. Akivaizdu, kad aibė $k(\theta)$ elementų sudėties atžvilgiu sudaro Abelio grupę. Taigi aibės $k(\theta)$ elementų sudėtis $+$ tenkina kūno apibrėžimo I-ąją aksiomų grupę.

Prieš įrodydami, kad aibės $k(\theta)$ elementų daugyba tenkina kūno apibrėžimo II-ąją aksiomų grupę, pirmiausia įsitikinsime, kad daugyba aibėje $k(\theta)$ apibrėžta. Tuo tikslu reikia įsitikinti, kad elemento θ visi teigiami sveikieji laipsniai priklauso aibei $k(\theta)$, t. y. elemento θ visi teigiami sveikieji laipsniai θ^j, $j \ge n$, yra tiesiškai išreiškiami elemento θ laipsniais θ^j, $0 \le j \le n-1$, su koeficientais iš kūno k. Jei bet kurie elemento θ visi teigiami sveikieji laipsniai θ^j, $j \ge 0$, priklauso aibei $k(\theta)$, tai ir bet kurių dviejų aibės $k(\theta)$ elementų sandauga priklauso aibei $k(\theta)$.

Kadangi $f(\theta) = 0$, tai

$$\theta^n = -a_{n-1}\theta^{n-1} - \ldots \_\ a_1\theta - a_0, \qquad (1).$$

Kaip matome, θ^n yra tiesiškai išreiškiamas elemento θ laipsniais θ_j, $0 \le j \le n-1$. Sakykime, kad $\theta^m \in k(\theta)$, $m \ge n$. Įrodysime, kad ir $\theta^{m+1} \in k(\theta)$.

Kadangi $\theta^m \in k(\theta)$, tai egzistuoja tokie $b_0, b_1, \ldots, b_{n-2}, b_{n-1} \in k$, kad

$$\theta^m = b_{n-1}\theta^{n-1} + b_{n-2}\theta^{n-2} + \ldots + b_1\theta + b_0, \qquad (2).$$

Padauginę (2) lygybę iš θ ir θ^n pakeitę (1) lygybės dešiniąja puse, gauname:

$$\theta^{m+1} = b_{n-1}(-a_{n-1}\theta^{n-1} - \ldots \_\ a_1\theta - a_0) + b_{n-2}\theta^{n-1} + \ldots + b_1\theta^2 + b_0\theta =$$

$$= (-b_{n-1}a_{n-1} + b_{n-2})\theta^{n-1} + \ldots + (-b_{n-1}a_1 + b_0)\theta - b_{n-1}a_0 \in k(\theta).$$

Dabar įrodysime, kad kiekvienam nenuliniam $\beta \in k(\theta)$, egzistuoja toks $\gamma \in k(\theta)$, kad $\beta\gamma = 1$.

Nagrinėkime atvaizdį

$$g_\beta : k(\theta) \to k(\theta),\ g_\beta(z) = \beta z,\ z \in k(\theta).$$

Akivaizdu, kad $k(\theta)$ – tiesinė erdvė virš kūno k, o apibrėžtasis atvaizdis yra tiesinis. Iš tikrųjų:

$$g_\beta(\lambda_1 z_1 + \lambda_2 z_2) = \beta(\lambda_1 z_1 + \lambda_2 z_2) = \lambda_1 \beta z_1 + \lambda_2 \beta z_2 =$$

$$= \lambda_1 g_\beta(z_1) + \lambda_2 g_\beta(z_2),\ \lambda_1, \lambda_2 \in k,\ z_1, z_2 \in k(\theta).$$

Tiesinio atvaizdžio g_β branduolys $\mathrm{Ker} g_\beta = \{0\}$. Kadangi tiesinės erdvės $k(\theta)$ dimensija virš kūno k yra baigtinė (ji yra lygi $n = \deg f(x)$), tai $g_\beta(k(\theta)) = k(\theta)$ (žinome, kad $\dim_k k(\theta) = \dim_k \mathrm{Ker} g_\beta + \dim_k g_\beta(k(\theta))$). Vadinasi, egzistuoja toks $\gamma \in k(\theta)$, kad $g_\beta(\gamma) = 1 \in k(\theta)$, t. y. $\beta\gamma = 1$.

Taigi aibės $k(\theta)$ elementų daugyba tenkina kūno apibrėžimo II-ąją aksiomų grupę. Akivaizdu, kad aibės $k(\theta)$ elementų sudėtis ir daugyba susieti distributyvumo dėsniu, nes šiuo dėsniu susieti kūno K elementų sudėtis ir daugyba. Taigi $k(\theta)$ yra kūno K pokūnis, kuriam priklauso pokūnio k elementai ir elementas θ. Iš kūno $k(\theta)$ konstrukcijos matome, kad šis kūno K pokūnis mažiausias, kuriam priklauso pokūnio k elementai ir elementas θ. $\triangle$

4. 3. Antras įrodymas. Apibrėžkime atvaizdį

$$F : k[x] \to K,\ F(g(x)) = g(\theta) \in K,\ g(x) \in k[x].$$

Akivaizdžios atvaizdžio F savybės:

1. $F(h(x) + g(x)) = F(h(x)) + F(g(x))$;
2. $F(h(x)g(x)) = F(h(x))F(g(x))$.

Vadinasi, F yra homomorfizmas. Šio homomorfizmo branduolys $\mathrm{Ker} F$ yra žiedo $k[x]$ idealas, sudarytas iš visų polinomų $g(x) \in k[x]$, tenkinančių sąlygą: $g(\theta) = 0$. Kadangi elemento θ minimalusis polinomas $f(x) \in k[x]$ yra pirminis virš k, tai kiekvienas polinomas $g(x)$, tenkinantis sąlygą $g(\theta) = 0$, dalijasi iš $f(x)$. Iš tikrųjų, remdamiesi dalybos su liekana formule polinomams, galime parašyti: $g(x) = f(x)h(x) + q(x)$, $\deg q(x) < \deg f(x)$. Į šią lygybę vietoje x įrašę θ, gauname $g(\theta) = f(\theta)h(\theta) + q(\theta)$, t. y. $q(\theta) = 0$. Kadangi $\deg q(x) < \deg f(x)$, tai $q(x) = 0$. Taigi $\mathrm{Ker} F = f(x)k[x]$. Homomorfizmo F vaizdas yra izomorfinis faktoržiedui $k[x]/f(x)k[x]$. Skyrelyje [?] yra įrodyta, kad šis faktoeržiedas yra kūnas. Lieka įrodyti, kad homomorfizmo F vaizdas yra $k(\theta)$.

Polinomo $g(x)$ vaizdas $F(g(x)) = g(\theta)$. Padaliję polinomą $g(x)$ iš elemento θ minimaliojo polinomo θ, gauname

$$g(x) = f(x)h(x) + q(x),\ \deg q(x) < \deg f(x).$$

Į šią lygybę vietoje x įrašę θ, gauname $g(\theta) = f(\theta)h(\theta) + q(\theta)$, t. y. $g(\theta) = q(\theta) \in k(\theta)$. Vadinasi, $\mathrm{Im} F \subset k(\theta)$. Įdėtis $k(\theta) \subset \mathrm{Im} F$ akivaizdi. Įrodėme, kad $k(\theta)$ yra izomorfinis kūnui $k[x]/f(x)k[x]$. $\triangle$

Apibrėžimas. Sakykime, $\theta \in K$ yra algebrinis elementas virš kūno K pokūnio k. Kūno $k(\theta)$ kaip tiesinės erdvės virš k dimensija $\dim_k k(\theta)$ yra vadinama kūno k plėtinio $k(\theta)$ laipsniu ir yra žymima $[k(\theta) : k]$.

4. 4. Įrodėme, kad kiekvienam kūno $k(\theta)$ nenuliniam elementui β egzistuoja atvirkštinis elementas $\beta^{-1} \in k(\theta)$. Kaip matome, šie įrodymai nėra konstruktyvūs. Iš įrodymų eigos nesimato, kaip nenuliniam elementui $\beta \in k(\theta)$ rasti elementą β^{-1}. Dabar nurodysime, kaip nenuliniam elementui $\beta \in k(\theta)$ konstruktyviai rasti β^{-1}. Šis nenuliniam elementui $\beta \in k(\theta)$ atvirkštinio elemento konstruktyvus egzistavimo įrodymas pagrįstas Euklido algoritmu polinomams.

Priminsime Euklido algoritmo esminius momentus.

Apibrėžimas. Polinomas $f(x)$ yra vadinamas nenulinių polinomų $f_1(x)$, $f_2(x)$ didžiausiu bendruoju dalikliu, jei

1. $f(x)|f_1(x)$, $f(x)|f_2(x)$ (t. y. polinomas $f(x)$ yra polinomų $f_1(x)$ ir $f_2(x)$ bendrasis daliklis);
2. Jei $h(x)|f_1(x)$, $h(x)|f_2(x)$, tai $h(x)|f(x)$.

Dviejų nenulinių polinomų didžiausią bendrąjį daliklį galima rasti Euklido algoritmu. Sakykime, nenuliniai polinomai $f_1(x), f_2(x) \in k[x]$. Remdamiesi dalybos su liekana formule, galime parašyti lygybes:

$$\begin{array}{lll}
f_1(x) & = f_2(x)h_2(x) + f_3(x), & \deg f_3(x) < \deg f_2(x), \\
f_2(x) & = f_3(x)h_3(x) + f_4(x), & \deg f_4(x) < \deg f_3(x), \\
f_3(x) & = f_4(x)h_4(x) + f_5(x), & \deg f_5(x) < \deg f_4(x), \\
\ldots & \ldots & \ldots \\
f_{m-3}(x) & = f_{m-2}(x)h_{m-2}(x) + f_{m-1}(x), & \deg f_{m-1}(x) < \deg f_{m-2}(x), \\
f_{m-2}(x) & = f_{m-1}(x)h_{m-1}(x) + f_m(x), & \deg f_m(x) < \deg f_{m-1}(x), \\
f_{m-1}(x) & = f_m(x)h_m(x) + 0, &
\end{array}$$

Paskutinė, nelygi nuliui, liekana $f_m(x)$ ir yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis.

Mūsų tikslams svarbi

4. 5. Išvada. Jei polinomų $f_1(x)$ ir $f_2(x)$, priklausančių žiedui $k[x]$, didžiausias bendrasis daliklis yra $d(x)$, tai egzistuoja tokie polinomai $g_1(x), g_2(x) \in k[x]$, kad

$$d(x) = f_1(x)g_1(x) + f_2(x)g_2(x).$$

Ši išvada svarbi tuo, kad polinomus $g_1(x), g_2(x) \in k[x]$ galima rasti efektyviai.

Įrodymas. Polinomams $f_1(x)$ ir $f_2(x)$ pritaikę Euklido algoritmą, gauname:

$$\begin{array}{lll}
f_1(x) & = f_2(x)h_2(x) + f_3(x), & \deg f_3(x) < \deg f_2(x), \\
f_2(x) & = f_3(x)h_3(x) + f_4(x), & \deg f_4(x) < \deg f_3(x), \\
f_3(x) & = f_4(x)h_4(x) + f_5(x), & \deg f_5(x) < \deg f_4(x), \\
\ldots & \ldots & \ldots \\
f_{m-3}(x) & = f_{m-2}(x)h_{m-2}(x) + f_{m-1}(x), & \deg f_{m-1}(x) < \deg f_{m-2}(x), \\
f_{m-2}(x) & = f_{m-1}(x)h_{m-1}(x) + f_m(x), & \deg f_m(x) < \deg f_{m-1}(x), \\
f_{m-1}(x) & = f_m(x)h_m(x) + 0, &
\end{array}$$

Kaip žinome, $f_m(x)$ yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis, t. y. $d(x) = \varepsilon f_m(x)$. Iš priešpaskutinės Euklido algoritmo lygybės gauname:

$$f_m(x) = f_{m-2}(x) - f_{m-1}(x)h_{m-1}(x).$$

Į šią lygybę įrašę polinomo f_{m-1} išraišką, gautą iš Euklido algoritmo aukščiau esančios lygybės, gauname:

$$f_m(x) = f_{m-2}(x) - (f_{m-3}(x) - f_{m-2}(x)h_{m-2}(x))h_{m-1}(x) =$$

$$= -f_{m-3}(x)h_{m-1}(x) + f_{m-2}(x)(1 + h_{m-2}(x)h_{m-1}(x)).$$

Į šią lygybę įrašę polinomo $f_{m-2}(x)$ išraišką polinomais f_{m-3} ir f_{m-4}, gauname polinomo $f_m(x)$ išraišką polinomais f_{m-3} ir f_{m-4}. Darydami tokius pertvarkymus ir toliau, galų gale gausime $f_m(x)$ išraišką polinomais $f_1(x)$ ir $f_2(x)$:

$$f_m(x) = f_1(x)\tilde{g}_1(x) + f_2(x)\tilde{g}_2(x).$$

Remdamiesi šia lygybe, gauname

$$d(x) = \varepsilon(f_1(x)\tilde{g}_1(x) + f_2(x)\tilde{g}_2(x)) = f_1(x)g_1(x) + f_2(x)g_2(x),$$

čia $g_1(x) = \varepsilon\tilde{g}_1(x)$, $g_2(x) = \varepsilon\tilde{g}_2(x)$

4. 6. Sakykime, K – kūnas, $\theta \in K$ yra algebrinis elementas virš kūno K pokūnio k, $f(x) = x^n + a_{n-1} + \ldots + a_1x + a_0 \in k[x]$ – elemento θ minimalusis polinomas. Dabar įrodysime, kad kiekvienam nenuliniam elementui $\beta = b_{n-1}\theta^{n-1} + \ldots + b_1\theta + b_0 \in k(\theta) \subset K$, egzistuoja atvirkštinis elementas $\beta^{-1} \in k(\theta)$. Šis įrodymas efektyvus ta prasme, kad remiantis šiuo įrodymu kiekvienu konkrečiu atveju nenuliniam elementui $\beta \in k(\theta)$ galima rasti atvirkštinį elementą β^{-1}.

Tegu $\beta = b_{n-1}\theta^{n-1} + \ldots + b_1\theta + b_0 \in k(\theta)$ – nenulinis elementas, t. y. bent vienas iš koeficientų $b_j \in k$, $0 \leq j \leq n-1$, nelygus 0. Sudarykime polinomą $g(x) = b_{n-1}x^{n-1} + \ldots + b_1x + b_0$. Kadangi algebrinio elemento $\theta \in K$ virš k minimalusis polinomas $f(x) = x^n + a_{n-1} + \ldots + a_1x + a_0 \in k[x]$ yra pirminis virš kūno k, tai polinomų $g(x)$ ir $f(x)$ didžiausias bendrasis daliklis yra lygus 1. Remiantis išvada, egzistuoja tokie polinomai $h(x), p(x) \in k[x]$, kad $g(x)h(x) + f(x)p(x) = 1$. Į šią lygybę vietoje x-o įrašę elementą θ, gauname: $g(\theta)h(\theta) + f(\theta)p(\theta) = 1$ arba $g(\theta)h(\theta) = 1$ (nes $f(\theta) = 0$).

Išnagrinėsime keletą pavyzdžių.

Pavyzdžiai.

1. Sakykime, $k = \mathbb{Q}$ racionaliųjų skaičių kūnas, $\theta \in \mathbb{R}$ yra polinomo $f(x) = x^3 - 5x + 5$ šaknis (nelyginio laipsnio polinomas $x^3 - 5x + 5$ turi relią šaknį ir yra pirminis virš racionaliųjų skaičių kūno $\mathbb{Q}$ remiantis Eizeinšteino kriterijumi). Kūnas $\mathbb{Q}(\theta)$ yra sudarytas iš skaičių $a_2\theta^2 + a_1\theta + a_0$, $a_2, a_1, a_0 \in \mathbb{Q}$.

Imkime, pavyzdžiui, $\beta = \theta^2 - 2\theta - 2$. Polinomų $x^2 - 2x - 2$ ir $f(x) = x^3 - 5x + 5$ didžiausias bendrasis daliklis yra lygus 1. Šį didžiausią bendrąjį daliklį rasime pritaikę polinomams $x^2 - 2x - 2$ ir $f(x) = x^3 - 5x + 5$ Euklido algoritmą.

$$\begin{array}{rcl} x^3 - 5x + 5 & = & (x^2 - 2x - 2)(x + 2) + x + 9 \\ x^2 - 2x - 2 & = & (x + 9)(x - 11) + 97 \end{array}.$$

Taigi

$$97 = x^2 - 2x - 2 - (x + 9)(x - 11) =$$

$$= x^2 - 2x - 2 - (x^3 - 5x + 5 - (x^2 - 2x - 2)(x + 2))(x - 11) =$$

$$= (x^2 - 2x - 2)(1 + (x + 2)(x - 11)) - (x^3 - 5x + 5)(x - 11) =$$

$$= (x^2 - 2x - 2)(x^2 - 9x - 21) - (x^3 - 5x + 5)(x - 11).$$

Į pastarąją lygybę vietoje x-o įrašę elementą θ, gauname:

$$(\theta^2 - 2\theta - 2)(\theta^2 - 9\theta - 21) = 97.$$

Vadinasi,

$$(\theta^2 - 2\theta - 2)^{-1} = \frac{1}{\theta^2 - 2\theta - 2} = \frac{\theta^2 - 9\theta - 21}{97}.$$

Patikrinimas. Sudauginkime $\theta^2 - 2\theta - 2$ ir $\theta^2 - 9\theta - 21$:

$$(\theta^2 - 2\theta - 2)(\theta^2 - 9\theta - 21) = \theta^4 - 11\theta^3 - 5\theta^2 + 60\theta + 42 \qquad (1).$$

Kadangi $\theta^3 = 5\theta - 5$, tai $\theta^4 = 5\theta^2 - 5\theta$. Įrašę šias θ^3 ir θ^4 reikšmes į (1) lygybę, gauname:

$$(\theta^2 - 2\theta - 2)(\theta^2 - 9\theta - 21) = 5\theta^2 - 5\theta - 55\theta + 55 - 5\theta^2 + 60\theta + 42 = 97.$$

2. Kaip ir pirmajame pavyzdyje $k = \mathbb{Q}$, $f(x) = x^3 - 5x + 5$, θ – polinomo $f(x)$ realioji šaknis. Imkime $\beta = \theta^2 + \theta + 1$. Kaip ir pirmajame pavyzdyje parašykime lygybes:

$$\begin{array}{rcl} x^3 - 5x + 5 & = & (x^2 + x + 1)(x - 1) + (-5x + 6) \\ x^2 + x + 1 & = & (-5x + 6)(-\frac{1}{5}x - \frac{11}{25}) + \frac{91}{25} \end{array}.$$

Vadinasi,

$$\frac{91}{25} = x^2 + x + 1 - (-5x + 6)(-\frac{1}{5}x - \frac{11}{25}) =$$

$$= x^2 + x + 1 - (x^3 - 5x + 5 - (x^2 + x + 1)(x - 1))(-\frac{1}{5}x - \frac{11}{25}) =$$

$$= (x^2 + x + 1)\frac{36 - 6x - 5x^2}{25} + (x^3 - 5x + 5)\frac{5x + 11}{25}.$$

Taigi

$$(\theta^2 + \theta + 1)^{-1} = \frac{1}{\theta^2 + \theta + 1} = \frac{36 - 6\theta - 5\theta^2}{91}.$$

Patikrinimas. Sudauginkime $36 - 6\theta - 5\theta^2$ ir $\theta^2 + \theta + 1$:

$$(\theta^2 + \theta + 1)(36 - 6\theta - 5\theta^2) = 36 + 30\theta + 25\theta^2 - 11\theta^3 - 5\theta^4 =$$

$$= 36 + 30\theta + 25\theta^2 - 55\theta + 55 - 25\theta^2 + 25\theta = 91.$$

Kaip matome, skaičiuodami klaidų nepadarėme.

4. 7. Kaip matėme, jei kūno K elementas θ yra algebrinis virš kūno K pokūnio k, tai $k(\theta)$ yra mažiausias kūno K pokūnis, kuriam priklauso pokūnio k elementai ir elementas θ. Įrodėme, kad $k(\theta)$ yra izomorfinis kūnui $k[x]/f(x)k[x]$, čia $f(x)$ elemento θ minimalusis polinomas. Duotam pirminiam virš k polinomui $f(x)$ konstruojant kūną $k[x]/f(x)k[x]$ nebūtina žinoti, ar polinomo $f(x)$ šaknis priklauso kuriam nors kūno k plėtiniui K, ar ne. Kūnas $k[x]/f(x)k[x]$ kaip tik ir yra mažiausias kūno k plėtinys, kuriam priklauso polinomo $f(x)$ šaknis. Kitaip tariant, duotajam pirminiam virš kūno k polinomui $f(x) \in k[x]$, galima sukonstruoti minimalų kūno k plėtinį, kuriam priklauso polinomo $f(x)$ šaknis. Be to, kaip įsitikinsime, visi minimalūs kūno k plėtiniai, kuriems priklauso kuri nors polinomo $f(x)$ šaknis, ir tik tokie kūno k plėtiniai yra tarp savęs izomorfiniai virš k.

Kūno k plėtinio $k[x]/f(x)k[x]$ sudarymas yra vadinamas pirminio virš k polinomo $f(x) \in k[x]$ šaknies prijungimo prie kūno k konstrukcija.

Apibrėžimas. Kūno k plėtiniai L_1 ir L_2 yra vadinami izomorfiniais virš k, jei egzistuoja tokia bijekcija $F : L_1 \to L_2$, kad bet kuriems $\alpha \in k$, $\beta, \gamma \in L_1$,

1. $F(\alpha) = \alpha$;
2. $F(\beta + \gamma) = F(\beta) + F(\gamma)$;
3. $F(\beta\gamma) = F(\beta)F(\gamma)$.

Teiginys. Sakykime, K – kūno k plėtinys, $\theta_1, \theta_2 \in K$. Tuomet atvaizdis

$$F : k(\theta_1) \to k(\theta_2),\ F(b_0 + b_1\theta_1 + \ldots + b_{n-1}\theta_1^{n-1}) = b_0 + b_1\theta_2 + \ldots + b_{n-1}\theta_2^{n-1},$$

$b_j \in k$, $0 \le j \le n-1$, yra kūnų $k(\theta_1)$ ir $k(\theta_2)$ izomorfizmas virš k tada ir tik tada, kai θ_1 ir θ_2 yra vieno ir to paties pirminio virš kūno k polinomo $f(x)$ šaknys.

Įrodymas. Sakykime, kad θ_1 ir θ_2 yra vieno ir to paties pirminio virš kūno k polinomo $f(x)$ šaknys. Teigiame, kad atvaizdis

$$F : k(\theta_1) \to k(\theta_2),\ F(b_0 + b_1\theta_1 + \ldots + b_{n-1}\theta_1^{n-1}) = b_0 + b_1\theta_2 + \ldots + b_{n-1}\theta_2^{n-1}$$

yra kūnų $k(\theta_1)$ ir $k(\theta_2)$ izomorfizmas virš k. Šis teiginys akivaizdus, prisiminus kaip kūnai $k(\theta_1)$ ir $k(\theta_2)$ yra sudaromi.

Sakykime, kad atvaizdis

$$F : k(\theta_1) \to k(\theta_2),\ F(b_0 + b_1\theta_1 + \ldots + b_{n-1}\theta_1^{n-1}) = b_0 + b_1\theta_2 + \ldots + b_{n-1}\theta_2^{n-1}$$

yra kūnų $k(\theta_1)$ ir $k(\theta_2)$ izomorfizmas virš k. Reikia įrodyti, kad elementai θ_1 ir θ_2 yra vieno ir to paties pirminio virš kūno k polinomo $f(x)$ šaknys. Kadangi $f(\theta_1) = 0$, tai ir $F(f(\theta_1)) = f(F(\theta_1)) = f(\theta_2) = 0$. $\triangle$

4. 8. Pirminio polinomo virš k šaknies prijungimo prie kūno k konstrukcija yra universali. Kad ir kokie būtų kūnas k, $f(x)$ pirminis polinomas virš k, egzistuoja kūno k mažiausias plėtinys L_1, kuriam priklauso polinomo $f(x)$ šaknis ir, be to, bet kurie du tokie plėtiniai yra izomorfiniai virš kūno k. Remdamiesi šia pirminio polinomo virš k šaknies prijungimo prie kūno k konstrukcija galime įrodyti, kad kiekvienam polinomui $g(x) \in k[x]$ egzistuoja toks minimalus kūno k plėtinys L, virš kurio polinomas $g(x)$ išsiskaido į pirmo laipsnio polinomus.

Sakykime, $g(x) \in k[x]$, $g(x) = g_1(x)g_2(x)\dots g_r(x)$ – polinomo $g(x)$ skaidinys pirminiais polinomais virš kūno k. Pasirinkime šio skaidinio pirminį virš kūno k polinomą, kurio laipsnis yra didesnis už 1. Tarkime, $g_{j_1}(x) \in k[x]$, $1 \le j_1 \le r$, – toks polinomas. Tuomet polinomo $g_{j_1}(x)$ šaknį θ prijungę prie kūno k, gauname kūno k plėtinį L_1. Kadangi $g_{j_1}(x) \in k[x] \subset L_1[x]$ ir egzistuoja polinomo $g_{j_1}(x)$ šaknis $\theta \in L_1$, tai bent $g_{j_1}(x)$ yra išskaidomas polinomas virš L_1. Vadinasi, gauname, kad polinomo $g(x)$ skaidinio $g_1(x)g_2(x)\dots g_r(x)$ be daugiklio $g_{j_1}(x)$ galbūt kai kurie ir kiti pirminiai daugikliai virš kūno k išsiskaido virš kūno k plėtinio L_1. Tęsdami šį šaknies prijungimo procesą, po baigtinio žingsnių skaičiaus gausime kūno k plėtinį L_s, kuriam priklauso visos polinomo $g(x)$ šaknys. Be to, bet kurie tokie plėtiniai yra izomorfiniai virš kūno k.

Apibrėžimas. Mažiausias kūno k plėtinys L, kuriam priklauso visos polinomo $f(x) \in k[x]$ šaknys, yra vadinamas polinomo $f(x)$ išskaidymo kūnu.

5. Baigtiniai kūnai

5. 1. Šiame skyrelyje aprašysime visus baigtinius kūnus.

Sakykime, $GF(q)$ – baigtinis kūnas, turintis q elementų, $GF(p)$ – kūno $GF(q)$ pirminis pokūnis, $n = [GF(q) : GF(p)] = \dim_{GF(p)} GF(q)$. Kadangi tiesinės erdvės $GF(q)$ virš kūno $GF(p)$ dimensija yra lygi n, tai tiesinė erdvė $GF(q)$ turi p^n elementų. Vadinasi, $q = p^n$. Kyla klausimas, ar kiekvienam teigiamam sveikajam skaičiui n egzistuoja kūnas $GF(p^n)$? Mūsų artimiausias tikslas į šį klausimą atsakyti: taip.

Teiginys. Baigtinio kūno $GF(p^n)$ elementai yra polinomo $x^{p^n} - x \in GF(p)[x]$ šaknys.

Įrodymas. Jei $GF(p^n)$ kūnas, tai šio kūno nenuliniai elementai sudaro Abelio grupę, kurios eilė yra lygi $p^n - 1$. Vadinasi, bet kurį šios grupės elementą $\alpha \in GF(p^n)^*$, pakėlę $p^n - 1$ laipsniu, gauname grupės vienetą: $\alpha^{p^n-1} = 1$. Kitaip tariant, nenuliniai kūno $GF(p^n)$ elementai yra polinomo $x^{p^n-1} - 1$ šaknys. Padauginę šį polinomą iš x-o, gauname, kad kiekvienas kūno $GF(p^n)$ elementas yra polinomo $x^{p^n} - x$ šaknis. $\triangle$

Pastebėsime, kad polinomas $x^{p^n} - x \in GF(p)[x]$ neturi kartotinių šaknų. Kaip žinome, polinomo šaknis yra kartotinė tada ir tik tada, kai ji yra šio polinomo ir jo išvestinės šaknis. Polinomo $x^{p^n} - x \in GF(p)[x]$ išvestinė yra lygi $p^n x^{p^n-1} - 1 = -1$ (p charakteristikos kūne $p\alpha = 0$), t. y. yra lygi -1 ir neturi šaknų.

Teorema. Kiekvienam teigiamam sveikajam skaičiui n ir kiekvienam pirminiam skaičiui p egzistuoja baigtinis kūnas $GF(p^n)$.

Įrodymas. Imkime polinomą $x^{p^n} - x \in GF(p)[x]$ ir nagrinėkime šio polinomo išskaidymo kūną L. Įrodysime, kad $L = GF(p^n)$.

Pirmiausia pastebėsime, kad $GF(p) \subset L$. Iš tikrųjų, nes kiekvienas kūno $GF(p)$ elementas yra polinomo $x^p - x$ šaknis, o $x^p - x | x^{p^n} - x$. Kadangi polinomas $x^{p^n} - x$ neturi kartotinių šaknų, lieka įrodyti, kad visos polinomo $x^{p^n} - x$ šaknys (o jų kūne L yra p^n) sudaro kūną.

Sakykime, kad α, β yra polinomo $x^{p^n} - x$ šaknys. Tuomet įsitikinsime, kad $\alpha + \beta$ ir $\alpha\beta$ taip pat yra polinomo $x^{p^n} - x$ šaknys.

Jei $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$, tai $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$.

Jei $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$, tai $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$.

Kadangi polinomo $x^{p^n} - x$ visų šaknų aibė yra stabili kūno L elementų sudėties ir daugybos atžvilgiu, tai ši aibė kūno L elementų sudėties ir daugybos atžvilgiu sudaro kūną. L – mažiausias kūno $GF(p)$ plėtinys, kuriam priklauso visos polinomo $x^{p^n} - x$ šaknys. Vadinasi, kūnas L yra sudarytas tik iš polinomo $x^{p^n} - x$ šaknų. Kadangi šis polinomas turi p^n šaknų, tai $|L| = p^n$. Taigi $L = GF(p^n)$. $\triangle$

6. Kūno algebriniai plėtiniai. Algebriškai uždari kūnai

6. 1. Nagrinėsime algebrinius plėtinius.

Teiginys. Sakykime, K – baigtinio laipsnio kūno k plėtinys. Tuomet kiekvienas kūno K elementas yra algebrinis virš k.

Įrodymas. Imkime kūno K elementą θ ir nagrinėkime šio elemento laipsnius 1, θ, θ^2, θ^3, $\ldots$, $\theta^m, \ldots$. Kadangi kūno K kaip tiesinės erdvės virš k dimensija $\dim_k K < \infty$, tai vektoriai $1, \theta, \theta^2, \theta^3, \ldots, \theta^m, \ldots$ yra tiesiškai priklausomi virš k. Vadinasi, egzistuoja toks $n \in \mathbb{N}$ ir tokie kūno k elementai α_j, $0 \leq j \leq n$, kurių bent vienas nelygus 0, kad

$$\alpha_n\theta^n + \alpha_{n-1}\theta^{n-1} + \ldots + \alpha_1\theta + \alpha_0 = 0.$$

Kaip matome, elementas θ yra nenulinio polinomo polinomo

$$\alpha_n x^n + \alpha_{n-1}x + \ldots + \alpha_1 x + \alpha_0 \in k[x]$$

šaknis. Taigi θ yra algebrinis elementas virš kūno k. $\triangle$

Teiginys. Jei K – kūno L baigtinio laipsnio plėtinys, o L – kūno k baigtinio laipsnio plėtinys, tai K yra kūno k baigtinio laipsnio plėtinys ir, be to, $[K : k] = [K : L][L : k]$.

Įrodymas. Sakykime, $\theta_1, \theta_2, \ldots, \theta_r$ – kūno K kaip tiesinės erdvės virš kūno L bazė, $\lambda_1, \lambda_2, \ldots, \lambda_s$ – kūno L kaip tiesinės erdvės virš kūno k bazė. Teigiame, kad $\theta_i\lambda_j$, $1 \leq i \leq r$, $1 \leq j \leq s$, – kūno K kaip tiesinės erdvės virš kūno k bazė.

Pirmiausia įrodysime, kad $\theta_i\lambda_j$, $1 \leq i \leq r$, $1 \leq j \leq s$, – tiesiškai nepriklausomi virš kūno k. Tuo tikslu nagrinėkime lygybę

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_{ij}\theta_i\lambda_j = 0, \ \alpha_{ij} \in k, \ 1 \leq i \leq r, \ 1 \leq j \leq s.$$

Įrodysime, kad bet kuriems $1 \leq i \leq r$, $1 \leq j \leq s$, $\alpha_{ij} = 0$. Tuo tikslu aukščiau parašytą lygybę perrašykime taip:

$$\sum_{i=1}^{r}\theta_i(\sum_{j=1}^{s}\alpha_{ij}\lambda_j) = 0, \ \alpha_{ij} \in k, \ 1 \leq i \leq r, \ 1 \leq j \leq s.$$

Kadangi θ_i, $1 \le i \le r$, – tiesiškai nepriklausomi virš L, tai kiekvienam i, $1 \le i \le r$,

$$\sum_{j=1}^{s} \alpha_{ij}\lambda_j = 0.$$

Kadangi λ_j, $1 \le j \le s$, – tiesiškai nepriklausomi virš k, tai bet kuriems i, j, $1 \le i \le r$, $1 \le j \le s$, $\alpha_{ij} = 0$. Kaip matome, elementai $\theta_i\lambda_j$, $1 \le i \le r$, $1 \le j \le s$, yra tiesiškai nepriklausomi virš kūno k.

Lieka įrodyti, kad kiekvienas kūno K elementas tiesiškai yra išreiškiamas elementais $\theta_i\lambda_j$, $1 \le i \le r$, $1 \le j \le s$, su koeficientais iš kūno k.

Sakykime, $\mu \in K$. Kadangi $\theta_1, \theta_2, \ldots, \theta_r$ – kūno K kaip tiesinės erdvės virš kūno L bazė, tai egzistuoja tokie $\nu_i \in L$, $1 \le i \le r$, kad

$$\mu = \nu_1\theta_1 + \nu_2\theta_2 + \ldots + \nu_r\theta_r. \tag{1}$$

Kadangi $\lambda_1, \lambda_2, \ldots, \lambda_s$ – kūno L kaip tiesinės erdvės virš kūno k bazė, tai kiekvienam i, $1 \le i \le r$, egzistuoja tokie $\alpha_{ij} \in k$, $1 \le j \le s$, kad

$$\nu_i = \alpha_{i1}\lambda_1 + \alpha_{i2}\lambda_2 + \ldots + \alpha_{is}\lambda_s. \tag{2}$$

Į (1) lygybę įrašę ν_i, $1 \le i \le r$, reikšmes iš (2) lygybės, gauname:

$$\mu = \sum_{i=1}^{r} \theta_i(\sum_{j=1}^{s} \alpha_{ij}\lambda_j) = \sum_{i=1}^{r}\sum_{j=1}^{s} \alpha_{ij}\theta_i\lambda_j.$$

Remdamiesi plėtinio laipsnio apibrėžimu, galime parašyti: $[L : k] = rs = [K : L][L : k]$. $\triangle$

6. 2. Išvada. Sakykime, K – kūno k plėtinys, θ_1, θ_2 – kūno K elementai algebriniai virš k. Tuomet elementai $\theta_1 + \theta_2$ ir $\theta_1\theta_2$ yra algebriniai virš kūno k.

Įrodymas. Nagrinėkime kūno k plėtinius $L =: k(\theta_1)$ ir $K =: L(\theta_2) = k(\theta_1, \theta_2)$. Akivaizdu, kad $\theta_1 + \theta_2, \theta_1\theta_2 \in K$. Įrodysime, kad K yra kūno k baigtinio laipsnio plėtinys. Tuomet remdamiesi anksčiau įrodytu teiginiu, gausime, kad elementai $\theta_1 + \theta_2$ ir $\theta_1\theta_2$ yra algebriniai virš kūno k.

Galime parašyti: $[K : k] = [K : L][L : k] < \infty$. Iš tikrųjų, $[k(\theta_1) : k] < \infty$, kadangi θ_1 yra algebrinis virš k ir $[L(\theta) : L] < \infty$, kadangi θ_2 yra algebrinis virš k ir tuo labiau virš kūno k plėtinio L. $\triangle$

6. 3. Akivaizdu, kad baigtinio skaičiaus algebrinių elementų virš kūno k suma ir sandauga yra algebriniai elementai virš k.

Apibrėžimas. Kūno k plėtinys K yra vadinamas kūno k algebriniu plėtiniu, jei kiekvienas kūno K elementas yra algebrinis virš k.

Kiekvienas kūno k baigtinio laipsnio plėtinys yra kūno k algebrinis plėtinys. Pateiksime kūno k begalinio laipsnio algebrinio plėtinio pavyzdį.

Pavyzdys. Pažymėkime raide P visų natūraliųjų pirminių skaičių aibę. Nagrinėkime racionaliųjų skaičių kūno $\mathbb{Q}$ mažiausią plėtinį K, kuriam priklauso visi skaičiai $\sqrt{p}$, $p \in$

P. Kiekvienas šio plėtinio K elementas vienareikšmiškai yra užrašomas baigtine suma taip: $a_0+a_1\sqrt{n_1}+\ldots+a_r\sqrt{n_r}$, čia $a_0, a_1, \ldots, a_r \in \mathbb{Q}$, o $n_1, \ldots, n_r$ tarp savęs skirtingi bekvadračiai natūralieji skaičiai. Įrodysime, kad racionaliųjų skaičių kūno $\mathbb{Q}$ begalinio laipsnio plėtinys K yra kūno $\mathbb{Q}$ algebrinis plėtinys.

Skaičiai $\sqrt{p} \in K$, $p \in P$ yra algebriniai virš $\mathbb{Q}$. Kaip žinome, algebrinių virš kurio nors kūno elementų suma ir sandauga yra algebriniai elementai virš to kūno. Vadinasi, kūno K elementai (šiuo atveju skaičiai) yra algebriniai virš $\mathbb{Q}$.

6. 4. Teiginys. Sakykime, kūnas K yra kūno k plėtinys. Tuomet visi kūno K elementai, algebriniai virš k, sudaro kūno K pokūnį L, kuris yra kūno k algebrinis plėtinys.

Įrodymas. Įrodymas akivaizdus.

Teiginys. Jei kūnas K yra kūno L algebrinis plėtinys, L yra kūno k algebrinis plėtinys, tai K yra kūno k algebrinis plėtinys.

Įrodymas. Sakykime, $\theta \in K$. Tuomet egzistuoja toks polinomas $f(x) \in L[x]$, $f(\theta) = 0$. Sakykime,

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,\ a_j \in L,\ 0 \leq j \leq n-1.$$

Nagrinėkime kūną $M = k(a_0, a_1, \ldots, a_{n-1})$. Kadangi elementai a_0, a_1, $\ldots$, a_{n-1} yra algebriniai virš kūno k, tai

$$\dim_k k(a_0, a_1, \ldots, a_{n-1}) < \infty.$$

Elementas θ yra algebrinis virš kūno $M = k(a_0, a_1, \ldots, a_{n-1})$. Taigi $\dim_M M(\theta) < \infty$. Vadinasi, ir $\dim_k M(\theta) < \infty$, t. y. θ yra alebrinis virš kūno k. $\triangle$

6. 5. Apibrėžimas. Kūnas k yra vadinamas algebriškai uždaras, jei kiekvienas polinomas $f(x) \in k[x]$, kurio laipsnis $\deg f(x) > 0$, turi bent vieną šaknį kūne k.

Algebriškai uždari kūnai nepaprastai svarbūs. Sprendžiant matematikos uždavinius, labai dažnai tenka nagrinėti polinomus, susijusius su tuo uždaviniu. Todėl svarbu žinoti, ar nagrinėjami polinomai turi šaknį duotajame kūne, ar ne.

Dabar suformuluosime teoremą, kurios neįrodysime. Šios teoremos įrodymas pagrįstas transfiničiosios indukcijos metodu (arba šiam metodui ekvivalenčia Corno lema).

Teorema. Kiekvienam kūnui k egzistuoja kūno k algebriškai uždaras algebrinis plėtinys $\bar{k}$.

6. 6. Pavyzdžiui, racionaliųjų skaičių kūno $\mathbb{Q}$ algebriškai uždaras algebrinis plėtinys $\bar{\mathbb{Q}}$ kaip aibė yra skaičios galios. Mes netrukus nagrinėsime algebriškai uždarą kompleksinių skaičių kūmą $\mathbb{C}$. Kompleksinių skaičių kūnas $\mathbb{C}$ kaip aibė yra realiųjų skaičių aibės $\mathbb{R}$ Dekarto kvadratas $\mathbb{R} \times \mathbb{R}$. Kadangi realiųjų skaičių aibė yra kontinuumo galios, tai ir kompleksinių skaičių aibė yra kontinuumo galios. Vadinasi, kompleksinių skaičių kūne $\mathbb{C}$ egzistuoja be galo daug transcendentinių virš $\mathbb{Q}$ elementų. Norėdami tiksliau suformuluoti teiginį apie transcendentinius skaičius virš $\mathbb{Q}$, apibrėšime vieną svarbią sąvoką.

Apibrėžimas. Sakykime, K – kūno k plėtinys. Kūno K elementai θ_1, θ_2, $\ldots$, θ_m yra vadinami algebriškai nepriklausomais, jei neegzistuoja tokio m kintamųjų polinomo

$$f(x_1, x_2, \ldots, x_m) \in k[x_1, x_2, \ldots, x_m],$$

kad $f(\theta_1, \theta_2, \ldots, \theta_m) = 0$.

Apibrėžimas. Kūno k plėtinio K elementų šeima $\{\theta_\alpha\}_{\alpha \in I}$, čia I – indeksų aibė, kuri gali būti tiek baigtinė, tiek ir begalinė, yra vadinama algebriškai nepriklausoma, jei kiekvienas šios šeimos baigtinis pošeimis yra algebriškai nepriklausomas.

Remdamiesi aibės galios sąvoka, galime suformuluoti teiginį apie realiuosius transcendentinius skaičius virš $\mathbb{Q}$.

Teorema. Realiųjų skaičių (o taip pat ir kompleksinių skaičių) kūne $\mathbb{R}$ egzistuoja kontinuumo galios algebriškai nepriklausomų skaičių šeima.

Taigi net algebriškai nepriklausomų realiųjų skaičių aibė yra kontinuumo galios. Nagrinėjant kai kuriuos konkrečius realius skaičius, atsakyti į klausimą, ar šie skaičiai algebriškai priklausomi, ar ne, būna gana sudėtinga. Pavyzdžiui, yra žinoma, kad skaičiai e ir π yra transcendentiniai virš $\mathbb{Q}$, bet nėra žinoma, ar šie skaičiai yra algebriškai priklausomi, ar ne. Tai, kad skaičius e yra transcendentinis virš $\mathbb{Q}$, įrodė prancūzų matematikas Ermitas dar praeitame šimtmetyje. Skaičiaus π transcendentiškumą virš $\mathbb{Q}$ 1882 metais įrodė vokiečių matematikas Lindemanas.

7. Kompleksinių skaičių kūnas

7. 1. Apibrėžkime aibę

$$\mathbb{C} = \{a + bi |\ a,\ b \in \mathbb{R},\ i^2 = -1\}.$$

Aibės $\mathbb{C}$ elementas $a + bi$, $a, b \in \mathbb{R}$, yra vadinamas kompleksiniu skaičiumi. a yra vadinama kompleksinio skaičiaus $a + bi$ realiąja dalimi ir žymima $\Re(a + bi)$, t. y. $a = \Re(a + bi)$, o b – šio kompleksinio skaičiaus menamąja dalimi ir žymima $\Im(a + bi)$, t. y. $b = \Im(a + bi)$. Du kompleksiniai skaičiai $a + bi$ ir $c + di$ yra lygūs pagal apibrėžimą tada ir tik tada, kai jų realiosios ir menamosios dalys yra lygios: $a = c, b = d$. Apibrėšime kompleksinių skaičių sudėtį ir daugybą ir įsitikinsime, kad kompleksiniai skaičiai apibrėžtų veiksmų atžvilgiu yra kūnas.

Aibės $\mathbb{C}$ elementų sudėtį apibrėžkime taip:

$$(a + bi) + (c + di) =: (a + b) + (c + d)i,\ \ a, b, c, d \in \mathbb{R}.$$

Akivaizdu, kad kompleksinių skaičių aibė sudėties atžvilgiu sudaro Abelio grupę.

Aibės $\mathbb{C}$ elementų daugybą apibrėžkime taip:

$$(a + bi)(c + di) =: (ac - bd) + (ad + bc)i,\ \ a, b, c, d \in \mathbb{R}.$$

1. Įsitikinkite, kad taip apibrėžta kompleksinių skaičių daugyba asociatyvi.
2. Akivaizdu, kad kompleksinis skaičius $1 = 1 + 0i$ daugybos atžvilgiu yra neutralus elementas, t. y. vienetas.
3. Kiekvienam nenuliniam kompleksinam skaičiui $a + bi$ egzistuoja atvirkštinis kompleksinis skaičius:

$$(a + bi)^{-1} = \frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \in \mathbb{C},$$

nes $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{R}$.

4. Kompleksinių skaičių daugyba komutatyvi: $(a+bi)(c+di) = (c+di)(a+bi)$. Įsitikinkite sudauginę šiuos kompleksinius skaičius.

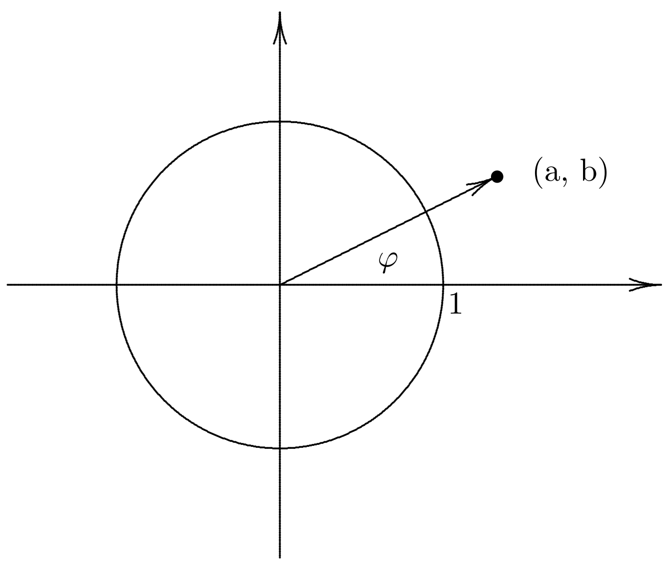
Dabar akivaizdu, kad kompleksinių skaičių aibė be nulinio elemento $\mathbb{C}^*$ daugybos atžvilgiu sudaro Abelio grupę. Kadangi kompleksinių skaičių sudėtis ir daugyba yra susieti distributyvumo dėsniu:

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma,\ \alpha, \beta, \gamma \in \mathbb{C},$$

(įsitikinkite atlikę veiksmus), tai kompleksinių skaičių aibė $\mathbb{C}$ kompleksinių skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

8. Kompleksinių skaičių geometrinė interpretacija

8. 1. Kompleksinius skaičius galima pavaizduoti plokštumos $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ taškais: kompleksinį skaičių $a + bi$ atitinka plokštumos $\mathbb{R}^2$ taškas, kurio koordinatės yra (a, b). Realiuosius skaičius $a = a + 0i$, $a \in \mathbb{R}$, atitinka plokštumos $\mathbb{R}^2$ tiesė $\{(a, 0)|\ a \in \mathbb{R}\}$, vadinama realiąja tiese ir žymima Re, o grynai menamuosius kompleksinius skaičius $0 + bi$, $b \in \mathbb{R}$, atitinka plokštumos $\mathbb{R}^2$ tiesė $\{(0, b)|\ b \in \mathbb{R}\}$, vadinama menamąja tiese ir žymima Im.



Plokštumos $\mathbb{R}^2$ taško (a, b), atitinakančio kompleksinį skaičių $a + bi$, atstumas iki koordinačių pradžios $(0, 0)$ $\sqrt{a^2 + b^2}$ yra vadinamas kompleksinio skaičiaus $a + bi$ moduliu ir yra žymimas $|a+bi|$. Įsitikinsime, kad funkcija $|\ | : \mathbb{C} \to \mathbb{R}_+$ (čia $\mathbb{R}_+$ – neneigiamų realiųjų skaičių aibė) yra multiplikatyvi:

$$|(a + bi)(c + di)| = |a + bi||c + di|,\ a, b, c, d \in \mathbb{R}.$$

Norint įrodyti pastarąją lygybę, patogu vietoje kompleksinio skaičiaus $a+bi$ modulio $|a+bi| = \sqrt{a^2+b^2}$ nagrinėti šio kompleksinio skaičiaus modulio kvadratą $|a+bi|^2 = a^2+b^2$. Taigi

$$|(a+bi)(c+di)|^2 = (ac-bd)^2 + (bc+ad)^2 = a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2 =$$

$$= (a^2+b^2)c^2 + (a^2+b^2)d^2 = (a^2+b^2)(c^2+d^2) = |a+bi|^2|c+di|^2.$$

8. 2. Apibrėžimas. Kompleksinis skaičius $a-bi$ yra vadinamas sujungtiniu kompleksiniam skaičiui $a+bi$ ir yra žymimas $\overline{a+bi}$.

Jei kompleksinį skaičių $a+bi$ atitinka plokštumos $\mathbb{R}^2$ taškas (a,b), tai sujungtinį kompleksinį skaičių $a-bi$ skaičiui $a+bi$ atitinka plokštumos $\mathbb{R}^2$ taškas $(a,-b)$, simetrinis taškui (a,b) realiosios tiesės $\{(a,0)|\ a \in \mathbb{R}\}$ atžvilgiu.

Pratimai.

1. Įrodykite, kad kopleksiniams skaičiams α, β teisinga lygybė: $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$.
2. Įrodykite, kad nenuliniam kopleksiniam skaičiui α teisinga lygybė: $\overline{\alpha^{-1}} = (\bar{\alpha})^{-1}$.

9. Kompleksinių skaičių trigonometrinė išraiška

9. 1. Kompleksinį skaičių $a+bi$ galima užrašyti trigonometrine išraiška. Sakykime, kampas tarp realiosios ašies ir vektoriaus, kurio pradžia yra taške $(0,0)$, o galas – taške (a,b) yra lygus φ. Šio vektoriaus ilgis yra lygus kompleksinio skaičiaus $a+bi$ moduliui $r = |a+bi| = \sqrt{a^2+b^2}$. Tuomet $a = r\cos\phi$, $b = r\sin\phi$. Taigi galime parašyti:

$$a+bi = r\cos\varphi + ir\sin\varphi = r(\cos + i\sin\varphi).$$

Ši kompleksinio skaičaius $a+bi$ išraiška yra vadinama trigonometrine.

Apibrėžimas. Kampas φ tarp realiosios ašies ir vektoriaus, kurio pradžia yra taške $(0,0)$, o galas – taške (a,b), yra vadinamas kompleksinio skaičiaus $a+bi$ argumentu ir yra žymimas $\arg(a+bi)$, t. y. $\varphi = \arg(a+bi)$. Apibrėžkime $\mathrm{Arg}(a+bi) =: \{\arg(a+bi) + 2\pi n|\ n \in \mathbb{Z}\}$.

Kompleksinius skaičius trigonometrinėje išraiškoje patogu dauginti. Sakykime, $a_1+b_1i = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $a_2+b_2i = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Tuomet

$$(a_1+b_1i)(a_2+b_2i) = r_1(\cos\varphi_1 + i\sin\varphi_1)r_2(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= r_1r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)).$$

Kaip matome,

$$\arg(\alpha\beta) = \begin{cases} \arg\alpha + \arg\beta, & \text{jei } \arg\alpha + \arg\beta < 2\pi \\ \arg\alpha + \arg\beta - 2\pi, & \text{jei } \arg\alpha + \arg\beta \geq 2\pi \end{cases},$$

$\alpha, \beta \in \mathbb{C}$.

9. 2. Remdamiesi kompleksinio skaičiaus daugiareikšmio argumento Argα apibrėžimu, galime parašyti:

$$\mathrm{Arg}(\alpha\beta) = \mathrm{Arg}\alpha + \mathrm{Arg}\beta,\ \alpha, \beta \in \mathbb{C},$$

čia

$$\mathrm{Arg}\alpha + \mathrm{Arg}\beta =: \{\varphi + \psi |\ \varphi \in \mathrm{Arg}\alpha,\ \psi \in \mathrm{Arg}\beta\}.$$

Kompleksinio skaičiaus trigonometrinę išraišką galima ir kitaip užrašyti. Į funkcijos $\exp(x) = e^x$ skleidinį eilute:

$$\exp(x) = \sum_{j=0}^{\infty} \frac{x^j}{j!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots$$

vietoje x-o įrašę $i\varphi$, $\varphi \in \mathbb{R}$, gauname:

$$\exp(i\varphi) = 1 + i\varphi - \frac{\varphi^2}{2!} - \frac{i\varphi^3}{3!} + \frac{\varphi^4}{4!} + \ldots =$$

$$= \sum_{j=0}^{\infty} \frac{(-1)^j \varphi^{2j}}{(2j)!} + i \sum_{j=1}^{\infty} \frac{(-1)^{j-1} \varphi^{2j-1}}{(2j-1)!} = \cos\varphi + i \sin\varphi.$$

Vadinasi, $a + bi = r(\cos\varphi + i\sin\varphi) = r\exp(i\varphi)$, čia $r = |a + bi|$, $\varphi = \arg(a + bi)$.

10. Kompleksinės plokštumos vienetinis apskritimas

10. 1. Visi kompleksiniai skaičiai α, kurių modulis $|\alpha|$ yra lygus 1, sudaro kompleksinėje plokštumoje $\mathbb{C}$ apskritimą S^1, kurio centras yra koordinačių pradžioje $(0, 0)$, o spindulys lygus 1. Įrodysime, kad apskritimas S^1 kompleksinių skaičių daugybos atžvilgiu yra Abelio grupė.

Akivaizdu, aibė S^1 yra stabili kompleksinių skaičių daugybos atžvilgiu. Iš tikrųjų, jei $\alpha, \beta \in S^1$, tai $\alpha\beta \in S^1$, nes $|\alpha\beta| = |\alpha||\beta| = 1$.

Akivaizdu, kad i) daugyba asociatyvi; ii) 1 – daugybos atžvilgiu vienetinis elementas; iii) jei $\alpha \in S^1$, tai $\alpha^{-1} \in S^1$; iv) daugyba komutatyvi. Taigi S^1 kompleksinių skaičų daugybos atžvilgiu yra Abelio grupė.

10. 2. Kompleksinė plokštuma be nulio $\mathbb{C}^*$ kompleksinių skaičių daugybos atžvilgiu yra grupė, $\mathbb{R}^*_+$ ir S^1 – šios grupės pogrupiai. Kiekvienas nenulinis kompleksinis skaičius α vienareikšmiškai yra užrašomas $\alpha = |\alpha| \exp(i\mathrm{arg}\alpha)$, $|\alpha| \in \mathbb{R}^*_+$, $\exp(i\mathrm{arg}\alpha) \in S^1$. Kitais žodžiais galima pasakyti taip: grupė $\mathbb{C}^*$ yra savo pogrupių $\mathbb{R}^*_+$ ir S^1 tiesioginė sandauga: $\mathbb{C}^* = \mathbb{R}^*_+ \times S^1$.

Apibūdinant Abelio grupę S^1 nuodugniau, reikalingos kai kurios matematinės analizės sąvokos. Tarsime, kad tos sąvokos, kurias paminėsime, yra žinomos.

Kompleksinę plokštumą $\mathbb{C}$, kaip metrinę erdvę atstumo funkcijos $d(\alpha, \beta) = |\alpha - \beta|$ atžvilgiu, galima sutapatinti su Euklido plokštuma $\mathbb{R}^2$. n-matės Euklido erdvės $\mathbb{R}^n$ poaibis yra kompaktinis tada ir tik tada, kai jis yra aprėžtas ir uždaras. Kadangi apskritimas S^1 kompleksinėje plokštumoje yra aprėžtas ir uždaras, tai S^1 yra kompaktinė aibė.

Daugybos operacija $S^1 \times S^1 \xrightarrow{\cdot} S^1$ yra tolydus atvaizdis. Galima pasakyti ir tiksliau: daugybos funkcija $x + yi = (a+ib)\cdot(c+id)$, $a, b, c, d \in \mathbb{R}$, $a^2+b^2 = 1$, $c^2+d^2 = 1$, yra glodi (o iš tikrųjų, analizinė) funkcija. Todėl grupė S^1 yra vadinama kompaktine realiąja Li grupe.

Teiginys. Nenulinių kompleksinių skaičių grupės $\mathbb{C}^*$ kiekvienas kompaktinis pogrupis G yra grupės S^1 pogrupis.

Įrodymas. Sakykime, G – grupės $\mathbb{C}^*$ kompaktinis pogrupis, bet $G \not\subset S^1$. Vadinasi, egzistuoja toks kompleksinis skaičius $\alpha \in G$, bet $\alpha \notin S^1$. Tuomet $|\alpha| \neq 1$. Kadangi G – grupė, tai kiekvienam $n \in \mathbb{Z}$, $\alpha^n \in G$. Aibė $\{\alpha^n \mid n \in \mathbb{Z}\}$ nėra kompaktinė. Iš tikrųjų. Apibrėžtumo dėlei tarkime, kad $|\alpha| > 1$. Tuomet

$$\lim_{n\to\infty} |\alpha|^n = \infty,$$

t. y. aibė G nėra aprėžta, vadinasi, nėra kompaktinė. Gavome prieštaravimą prielaidai. Taigi $G \subset S^1$. $\triangle$

10. 3. Kadangi kiekvienas grupės $\mathbb{C}^*$ baigtinis pogrupis G yra kompaktinis, tai remdamiesi įrodytu teiginiu, gauname $G \subset S^1$. Kitame skyrelyje aprašysime visus grupės S^1 baigtinius pogrupius (ir tuo pačiu visus grupės $\mathbb{C}^*$ kompaktinius pogrupius).

11. n-ojo laipsnio šaknys iš vieneto

11. 1. Pirmiausia šiame skyrelyje išnagrinėsime lygties $x^n - 1 = 0$ sprendinius kompleksiniais skaičiais. Sakykime, kompleksinis skaičius α yra šios lygties sprendinys, t. y. $\alpha^n = 1$. Remdamiesi kompleksinio skaičiaus modulio multiplikatyviąja savybe, galime parašyti: $|\alpha^n| = |\alpha|^n = 1$. Kadangi kompleksinio skaičiaus α modulis $|\alpha|$ yra neneigiamas realusis skaičius, tai gauname $|\alpha| = 1$. Vadinasi, lygties $x^n - 1 = 0$ sprendinį trigonometrine išraiška galime užrašyti taip: $\alpha = \cos\varphi + i\sin\varphi$. Įrašę šį skaičių į lygtį $x^n - 1 = 0$, gauname:

$$\alpha^n = \cos(n\varphi) + i\sin(n\varphi) = 1 = \cos(2\pi s) + i\sin(2\pi s),\ s \in \mathbb{Z}.$$

Taigi $n\varphi = 2\pi s$, $s \in \mathbb{Z}$. Iš šios lygybės gauname: $\varphi = \frac{2\pi s}{n}$, $s \in \mathbb{Z}$. Kintamajam s suteikę reikšmes $s = 0, 1, \ldots, n-1$, gauname n skirtingų φ reikšmių: $0, \frac{2pi}{n}, \frac{2pi2}{n}, \ldots, \frac{2pi(n-1)}{n}$, kurios priklauso intervalui $[0, 2\pi)$. Kitaip tariant, gavome n skirtingų komplesinių lygties $x^n - 1 = 0$ šaknų:

$$cos\frac{2\pi j}{n} + i\sin\frac{2\pi j}{n} = \exp(\frac{2\pi i j}{n}),\ 0 \leq j \leq n-1.$$

Bet, kaip žinome, n-ojo laipsnio lygtis kūne negali turėti daugiau šaknų nei n. Vadinasi, suradome visas lygties $x^n - 1 = 0$ šaknis.

Lygties $x^n - 1 = 0$ šaknys $\exp(\frac{2\pi j}{n})$, $0 \leq j \leq n-1$, kompleksinėje plokštumoje $\mathbb{C}$ išsidėsto vienetiname apskritime S^1 ir šį apskritimą dalija į n lygias dalis.

Teiginys. Lygties $x^n - 1 = 0$ šaknys $\exp(\frac{2\pi i j}{n})$, $0 \leq j \leq n-1$, sudaro ciklinę grupę (t. y. grupę, kurią generuoja vienas šios grupės elementas).

Įrodymas. Apibrėžkime atvaizdį

$$f : \mathbb{Z} \to \{\exp(\frac{2\pi i j}{n}) \mid 0 \leq j \leq n-1\} \subset S^1, f(j) = e^{\frac{2\pi i j}{n}},\ j \in \mathbb{Z}.$$

Šis atvaizdis yra siurjektyvus ir tenkina sąlygą: $f(j+l) = f(j) \cdot f(l)$, $j, l \in \mathbb{Z}$. Iš tikrųjų,

$$f(j+l) = \exp(\frac{2\pi i(j+l)}{n}) = \exp(\frac{2\pi ij}{n}) \cdot \exp(\frac{2\pi il}{n}) = f(j) \cdot f(l), ; j, l \in \mathbb{Z}.$$

Kitaip tariant, atvaizdis $f : \mathbb{Z} \to S^1$ yra homomorfizmas. Kadangi $\mathbb{Z}$ skaičių sudėties atžvilgiu yra begalinės eilės ciklinė grupė, tai šios grupės vaizdas $f(\mathbb{Z}) = \{\exp(\frac{2\pi ij}{n}) \mid 0 \leq j \leq n-1\}$ yra n-tos eilės grupės S^1 ciklinis pogrupis. Šio pogrupio sudaromoji yra $\exp(\frac{2\pi i}{n})$, t. y. šis elementas generuoja pogrupį $\{\exp(\frac{2\pi ij}{n}) \mid 0 \leq j \leq n-1\}$.

Homomorfizmo f branduolys $\mathrm{Ker} f = n\mathbb{Z} = \{nl \mid l \in \mathbb{Z}\}$. Remdamiesi pirmąja teorema apie homomorfizmą, matome, kad lygties $x^n - 1 = 0$ šaknų grupė $\{\exp(\frac{2\pi ij}{n}) \mid 0 \leq j \leq n-1\}$ yra izomorfinė grupei $\mathbb{Z}/n\mathbb{Z} = Z_n$. $\triangle$

11. 2. Galime susumuoti rezultatus apie grupės S^1 baigtinius pogrupius. Šios grupės baigtiniai pogrupiai – tai baigtinio laipsnio šaknų iš vieneto grupės ir šių grupių pogrupiai.

11. 3. Pagrindinė algebros teorema.

Pirmoji formuluotė. Kompleksinių skaičių kūnas $\mathbb{C}$ yra algebriškai uždaras.

Antroji formuluotė. Kiekvienas polinomas

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ a_j \in \mathbb{C},\ 0 \leq j \leq n,\ n \geq 1,$$

turi bent vieną šaknį $\alpha \in \mathbb{C}$.

Išvada. Kiekvinas n-ojo laipsnio polinomas

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ a_j \in \mathbb{C},\ 0 \leq j \leq n,\ n \geq 1,$$

yra išskaidomas pirmojo laipsnio polinomų sandauga:

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = a_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

čia α_1, α_2, …, $\alpha_n \in \mathbb{C}$ – polinomo $f(x)$ šaknys.