V skyrius. ŽIEDAI IR ŽIEDŲ HOMOMORFIZMAI

1. Žiedai

1. 1. Tarkime, kad netuščioje aibėje A apibrėžti jos elementų kompozicijos dėsniai $+$ ir $*$, vadinami aibės A elementų sudėtimi ir daugyba.

Apibrėžimas. Aibę A joje apibrėžtų jos elementų sudėties $+$ ir daugybos $*$ atžvilgiu vadinsime žiedu, jei

1. Sudėtis $+$ yra asociatyvi: bet kuriems $x, y, z \in A$,

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

2. Egzistuoja neutralus elementas 0 sudėties $+$ atžvilgiu: kiekvienam $x \in A$,

$$x + 0 = 0 + x = x;$$

3. Kiekvienam aibės A elementui x egzistuoja simetrinis elementas y sudėties $+$ atžvilgiu:

$$x + y = y + x = 0;$$

Elementui x simetrinį elementą sudėties $+$ atžvilgiu žymėsime $-x$ ir vadinsime priešingu elementu elementui x.

4. Sudėtis $+$ yra komutatyvi: bet kuriems $x, y \in A$,

$$x + y = y + x;$$

5. Daugyba $*$ yra asociatyvi: bet kuriems $x, y, z \in A$,

$$(x * y) * z = x * (y * z);$$

6. Sudėtis $+$ ir daugyba $*$ yra susieti distributyvumo dėsniais: bet kuriems $x, y, z \in A$,

$$(x + y) * z = x * z + y * z,$$

$$z * (x + y) = z * x + z * y.$$

1. 2. Žiedo $(A, +, *)$ elementas 0 yra vadinamas nuliumi. Remdamiesi $1 - 4$ aksiomomomis, matome, kad $(A, +)$ - Abelio grupė. Kaip matome, nereikalaujama, kad žiedo $(A, +, *)$ daugyba $*$ būtų komutatyvi.

Apibrėžimas. Jei žiedo $(A, +, *)$ daugyba $*$ yra komutatyvi (t.y. bet kuriems $x, y \in A$, $x * y = y * x$), tai $(A, +, *)$ yra vadinamas komutatyviuoju žiedu.

Kaip matome, nereikalaujama, kad žiede $(A, +, *)$ egzistuotų neutralus elementas daugybos $*$ atžvilgiu.

Apibrėžimas. Jei žiede $(A, +, *)$ egzistuoja neutralus elementas daugybos $*$ atžvilgiu, tai jį žymėsime 1 ir vadinsime žiedo vienetu, o $(A, +, *)$ – žiedu su vienetu.

1. 3. Mes nagrinėsime tiktai žiedus $(A, +, *)$ su vienetu. Jei žiedas neturi vieneto, tai yra žinoma, kaip galima prijungti vienetą ir gauti žiedą su vienetu.

Labai svarbi speciali žiedų klasė, – žiedų, kurių kiekvienam nenuliniam elementui egzistuoja nenulinis simetrinis elementas daugybos atžvilgiu.

Apibrėžimas. Nekomutatyvus žiedas $(A, +, *)$ su vienetu 1 yra vadinamas žiedu su dalyba arba nekomutatyviuoju kūnu, jei kiekvienam $x \in A$, $x \neq 0$, egzistuoja toks $y \in A$, $y \neq 0$, kad $x * y = y * x = 1$. Komutatyvus žiedas $(A, +, *)$ su dalyba yra vadinamas kūnu.

Elementui $x \in A, x \neq 0$, simetrinis elementas daugybos atžvilgiu $*$, jei jis tik egzistuoja, yra žymimas x^{-1} ir yra vadinamas atvirkštiniu elementu elementui x.

1. 4. Dabar apibrėšime požiedžio, idempotenčiojo, nilpotenčiojo elementų bei nulio daliklių sąvokas. Vėliau šias sąvokas pailiustruosime pavyzdžiais.

Apibrėžimas. Netuščias žiedo $(A, +, *)$ poaibis B, stabilus sudėties $+$ ir daugybos $*$ atžvilgiu yra vadinamas žiedo $(A, +, *)$ požiedžiu, jei $(B, +, *)$ yra žiedas.

Apibrėžimas. Žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas idempotentu arba idempotenčiuoju elementu, jei $a * a = a^2 = a$.

Apibrėžimas. Žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas kairiuoju žiedo nulio dalikliu, jei egzistuoja toks nenulinis elementas b, kad $a*b = 0$. Panašiai apibrėžiamas dešinysis žiedo nulio daliklis. Komutatyvaus žiedo atveju šios sąvokos sutampa ir toks elementas yra vadinamas žiedo nulio dalikliu.

Apibrėžimas. Žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas nilpotentu arba nilpotenčiuoju elementu, jei egzistuoja toks sveikasis skaičius $n > 0$, kad $a^n = 0$.

Apibrėžimas. Komutatyvus žiedas be nulio daliklių yra vadinamas sveikumo arba integralumo sritimi.

Pastabos. 1. Kūno požiedis bendruoju atveju nėra kūnas.

2. Žiedo nilpotentas yra tiek kairysis, tiek dešinysis žiedo nulio daliklis.

Pavyzdžiai.

1. Sveikųjų skaičių aibė $\mathbb{Z}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu yra komutatyvus žiedas su vienetu. Jį žymėsime $(\mathbb{Z}, +, \cdot)$.

2. Racionaliųjų skaičių aibė $\mathbb{Q}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu yra kūnas $(\mathbb{Q}, +, \cdot)$.

3. Realiųjų skaičių aibė $\mathbb{R}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu yra kūnas $(\mathbb{R}, +, \cdot)$.

4. Tarkime, kad $A=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$, čia $\bar{j}=j(\mathrm{mod} 4)$. Likinių moduliu 4 aibė A sudėties ir daugybos atžvilgiu yra žiedas. Akivaizdu, kad $\bar{2}^2=\bar{0}$. Taigi $\bar{2}$ yra nilpotentusis nagrinėjamo žiedo elementas.

5. Apibrėžkime aibę

$$\mathbb{H}=\{\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k \mid \alpha,\beta,\gamma,\delta\in\mathbb{R}\},$$

kurios elementai yra formalūs simboliai $\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k$. Elementai $\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k$ ir $\alpha'+\beta'\cdot i+\gamma'\cdot j+\delta'\cdot k$ yra lygūs pagal apibrėžimą tada ir tik tada, kai $\alpha=\alpha'$, $\beta=\beta'$, $\gamma=\gamma'$, $\delta=\delta'$. Be to, koeficientai prie simbolių i,j,k, gali būti parašyti ir dešinėje pusėje, t.y. $\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k$=$\alpha+i\cdot\beta+j\cdot\gamma+k\cdot\delta$. Apibrėšime aibės $\mathbb{H}$ elementų sudėtį ir daugybą.

Sudėtis + aibėje $\mathbb{H}$.

Pagal apibrėžimą

$$\begin{aligned}&(\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k)+(\alpha'+\beta'\cdot i+\gamma'\cdot j+\delta'\cdot k)=\\&=\alpha+\alpha'+(\beta+\beta')\cdot i+(\gamma+\gamma')\cdot j+(\delta+\delta')\cdot k.\end{aligned}$$

Akivaizdu, kad ($\mathbb{H}$, +)-Abelio grupė.

Daugyba $\cdot$ aibėje $\mathbb{H}$.

Norint apibrėžti aibės $\mathbb{H}$ elementų daugybą, pakanka apibrėžti elementų i, j, k, daugybos lentelę ir remtis žiedo apibrėžimo 6-ąja aksioma. Elementų i, j, k daugybos lentelę apibrėžkime taip:

$$i\cdot i=j\cdot j=k\cdot k=-1, i\cdot j=-j\cdot i=k, j\cdot k=-k\cdot j=i, k\cdot i=-i\cdot k=j.$$

Dabar, remdamiesi elementų i,j,k, daugybos lentele ir žiedo apibrėžimo 6-ąja aksioma, galime užrašyti aibės $\mathbb{H}$ dviejų elementų sandaugos išraišką:

$$\begin{gathered}(\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k)\cdot(\alpha'+\beta'\cdot i+\gamma'\cdot j+\delta'\cdot k)=\\=\alpha\alpha'-\beta\beta'-\gamma\gamma'-\delta\delta'+(\alpha\beta'+\beta\alpha'+\gamma\delta'-\delta\gamma')\cdot i+\\+\alpha\gamma'+\gamma\alpha'+\delta\beta'-\beta\delta')\cdot j+(\alpha\delta'+\delta\alpha'+\beta\gamma'-\gamma\beta')\cdot k.\end{gathered}$$

Pastebėsime, kad

$$(\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k)\cdot(\alpha-\beta\cdot i-\gamma\cdot j-\delta\cdot k)=\alpha^2+\beta^2+\gamma^2+\delta^2.$$

Remdamiesi pastarąja lygybe matome, kad kiekvienam nenuliniam elementui $\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k$ (t.y., kai bent vienas koeficientų α, β, γ, δ yra nelygus nuliui) egzistuoja atvirkštinis elementas

$$(\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k)^{-1}=(\alpha^2+\beta^2+\gamma^2+\delta^2)^{-1}\cdot(\alpha-\beta\cdot i-\gamma\cdot j-\delta\cdot k).$$

Kaip matome, $(\mathbb{H}, +, \cdot)$ yra nekomutatyvus žiedas su dalyba arba nekomutatyvus kūnas. Šis nekomutatyvus kūnas dar yra vadinamas kvaternionų kūnu. Pirmas kvaternionų kūną pradėjo tirti anglų matematikas Hamiltonas. Kvaternionų kūnas dažniausiai yra žymimas $\mathbb{H}(\mathbb{R})$ pabrėžiant, kad kvaternionai yra gaunami simbolius $1, i, j, k$, dauginant iš realiųjų skaičių ir po to sudedant. Galima nagrinėti kvaternionus $\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k$, kurių koeficientai $\alpha, \beta, \gamma, \delta$, yra racionalūs skaičiai. Taigi galime apibrėžti

$$\mathbb{H}(\mathbb{Q}) = \{\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k \mid \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}.$$

Nesunku įsitikinti, kad $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ taip pat yra nekomutatyvus kūnas, kuris yra vadinamas racionaliųjų kvaternionų kūnu.

6. Šiame pavyzdyje nagrinėsime racionaliųjų kvaternionų kūno $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ požiedį $(\mathbb{Q}(i), +, \cdot)$, čia

$$\mathbb{Q}(i) =: \{\alpha + \beta \cdot i \mid \alpha, \beta \in \mathbb{Q}\}.$$

Galite įsitikinti, kad racionaliųjų kvaternionų kūno $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ poaibis $\mathbb{Q}(i)$ yra stabilus sudėties $+$ ir daugybos $\cdot$ atžvilgiu ir tokiu būdu yra nekomutatyvaus kūno $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ požiedis. Įrodysime, kad $(\mathbb{Q}(i), +, \cdot)$ yra kūnas. Pirmiausia pastebėsime, kad aibės $\mathbb{Q}(i)$ elementų daugyba $\cdot$ yra komutatyvi, nes

$$(\alpha + \beta \cdot i) \cdot (\alpha' + \beta' \cdot i) = \alpha \cdot \alpha' - \beta \cdot \beta' + (\alpha \cdot \beta' + \beta \cdot \alpha') \cdot i = (\alpha' + \beta' \cdot i) \cdot (\alpha + \beta \cdot i).$$

Kiekvienam nenuliniam žiedo $(\mathbb{Q}(i), +, \cdot)$ elementui $\alpha + \beta \cdot i$, t.y. kai bent vienas koeficientų α, β nelygus 0, egzistuoja atvirkštinis elementas

$$(\alpha^2 + \beta^2)^{-1} \cdot (\alpha - \beta \cdot i).$$

Kaip matome, $(\mathbb{Q}(i), +, \cdot)$ yra kūnas. Šis kūnas yra vadinamas Gauso skaičių kūnu.

7. Panašiai kaip ir 6-jame pavyzdyje, nagrinėkime realiųjų kvaternionų kūno $(\mathbb{H}(\mathbb{R}), +, \cdot)$ požiedį $(\mathbb{C}, +, \cdot)$, čia $\mathbb{C} =: \{\alpha + \beta \cdot i \mid \alpha, \beta \in \mathbb{R}\}$. Kaip ir 6-jame pavyzdyje galima įsitikinti, kad $(\mathbb{C}, +, \cdot)$ yra kūnas. Šis kūnas yra vadinamas kompleksinių skaičių kūnu. Kompleksinių skaičių kūnas labai svarbus matematikoje. Vėliau šį kūną tirsime išsamiau.

1. 5. Dabar įrodysime teoremą apie baigtines sveikumo (integralumo) sritis, o po to aptarsime labai svarbų žiedo pavyzdį.

Priminsime, kad komutatyvaus žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas nulio dalikliu, jei egzistuoja toks nenulinis elementas $b \in A$, kad $a * b = 0$. Komutatyvus žiedas $(A, +, *)$ yra vadinamas sveikumo (integralumo) sritimi, jei žiedas A neturi nulio daliklių.

Teorema. Baigtinis komutatyvus žiedas $(A, +, *)$ be nulio daliklių yra kūnas.

Įrodymas. Kadangi $(A, +, *)$ yra žiedas, tai, norint įrodyti teoremą, reikia įrodyti, kad žiede $(A, +, *)$ yra vienetas ir kiekvienam nenuliniam žiedo $(A, +, *)$ elementui egzistuoja atvirkštinis elementas daugybos atžvilgiu. Pabrėžiame, kad teoremos formulavime nereikalavome žiedo vieneto egzistavimo.

Tarkime, kad $A = \{a_1, a_2, \ldots, a_n\}$, o $a_1 = 0$. Pirmiausia įrodysime, kad žiedo A nenulinius elementus $a_2, \ldots, a_n$, padauginę iš kurio nors fiksuoto nenulinio elemento $a_s, 2 \leq s \leq n$, gauname visus nenulinius žiedo A elementus $a_2, \ldots, a_n$, tik galbūt, surašytus kita tvarka nei $a_2, \ldots, a_n$. Iš tikrųjų taip yra. Visi elementai $a_2, a_3, \ldots, a_n$, yra tarpusavy skirtingi ir jų tarpe nėra nulinio. Jei būtų

$$a_i * a_s = a_j * a_s, \;\; i \neq j, \;\; 2 \leq s \leq n,$$

tai gautume

$$a_i * a_s - a_j * a_s = (a_i - a_j)a_s = 0,$$

kas įmanoma žiede be nulio daliklių tik tuo atveju, kai $a_i - a_j = 0$. Bet, jei $i \neq j$, tai ir $a_i \neq a_j$. Vadinasi, sudauginę elementus

$$a_2, \ldots, a_n, \quad \text{ar} \quad a_2 * a_s, \ldots, a_n * a_s, \quad 2 \leq s \leq n,$$

gauname vieną ir tą patį elementą. Taigi

$$a_2 * a_3 * \ldots * a_n = a_s^{n-1} * a_2 * a_3 * \ldots * a_n, \; 2 \leq s \leq n,$$

čia a_s^{n-1} reikia suprasti, kaip a_s sudaugintą su savimi $n-1$ kartą. Šią lygybę galime perrašyti ir taip:

$$a_2 * a_3 * \ldots * \hat{a}_r * \ldots * a_n(a_r - a_s^{n-1} * a_r) = 0.$$

čia stogelis virš elemento žymi, kad šio elemento sandaugoje nėra. Kadangi

$$a_2 * a_3 * \ldots * \hat{a}_r * \ldots * a_n \neq 0,$$

o žiedas A be nulio daliklių, tai bet kuriems r, s, $2 \leq r, s \leq n$, $a_r = a_s^{n-1} * a_r$. Vadinasi, a_s^{n-1}, $2 \leq s \leq n$, yra žiedo vienetas, t.y. kiekvienam s, $2 \leq s \leq n$, $a_s^{n-1} = 1$. Taigi įrodėme lygybes:

$$a_s^{n-1} = a_r^{n-1}, \;\; 2 \leq r, s \leq n.$$

Pastarąsias lygybes galima ir taip įrodyti: iš anksčiau įrodytų lygybių

$$a_2 * a_3 * \ldots * a_n = a_s^{n-1} * a_2 * a_3 * \ldots * a_n, \;\; 2 \leq s \leq n,$$

gauname: jei

$$a_s^{n-1} * a_2 * a_3 * \ldots * a_n = a_r^{n-1} * a_2 * a_3 * \ldots * a_n, \;\; 2 \leq r, s \leq n,$$

tai

$$(a_s^{n-1} - a_r^{n-1}) * a_2 * a_3 * \ldots * a_n = 0$$

arba $a_s^{n-1} = a_r^{n-1}$, $2 \leq r, s \leq n$.

Lieka įrodyti, kad kiekvienam nenuliniam žiedo A elementui a_s, $2 \leq s \leq n$, egzistuoja atvirkštinis elementas. Remdamiesi lygybe $a_s^{n-1} = 1$, $2 \leq s \leq n$, gauname, kad

$$a_s^{-1} = a_s^{n-2}, \quad 2 \leq s \leq n.$$

1. 6. Pastaba. Remdamiesi teoremos įrodymu, matome, kad kiekvienas baigtinio kūno, turinčio n elementų, nenulinis elementas, pakeltas $n-1$-uoju laipsniu, yra lygus šio kūno vienetui, kitaip tariant, kiekvienas šio kūno nenulinis elementas yra lygties $x^{n-1} = 1$ šaknis. Šis faktas gali būti įrodytas remiantis grupių teorija. Baigtinio kūno nenuliniai elementai sudaro Abelio grupę. Šios grupės eilė lygi $n - 1$. Kiekvienas Abelio grupės elementas, pakeltas laipsniu, lygiu grupės eilei, yra lygus grupės vienetui. Vėliau įrodysime, kad baigtinis kūnas gali turėti tik p^m, čia p-kuris nors pirminis skaičius, m-kuris nors natūralusis skaičius, elementų.

2. Matricų algebra

2. 1. Nagrinėsime svarbų žiedą, kuris yra vadinamas matricų algebra. Algebra yra vadinama tiesinė erdvė, kurioje apibrėžta žiedo struktūra, suderinta su tiesinės erdvės struktūra.

Apibrėžimas. Abelio grupė $(V, +)$ yra vadinama tiesine erdve virš kūno $(k, +, *)$, jei apibrėžtas atvaizdis (išorinis kompozicijos dėsnis)

$$\circ : k \times V \to V$$

tenkinantis sąlygas: bet kuriems $\alpha, \beta \in k$, $u, v \in V$,

1. $(\alpha * \beta) \circ u = \alpha \circ (\beta \circ u)$;
2. $1 \circ u = u$, $1-$ kūno k vienetinis elementas;
3. $(\alpha + \beta) \circ u = \alpha \circ u + \beta \circ u$;
4. $\alpha \circ (u + v) = \alpha \circ u + \alpha \circ v$.

Apibrėžimas. Tiesinė erdvė $(V, +)$ virš kūno $(k, +, *)$ yra vadinama algebra, jei tiesinėje erdvėje apibrėžtas kompozicijos dėsnis $\cdot$, tenkinantis sąlygas: bet kuriems α, β, $\gamma \in k$, $u, v, w \in V$,

$$(\alpha \circ u + \beta \circ v) \cdot (\gamma \circ w) = (\alpha * \gamma) \circ (u \cdot w) + (\beta * \gamma) \circ (v \cdot w),$$

$$(\gamma \circ w) \cdot (\alpha \circ u + \beta \circ v) = (\gamma * \alpha) \circ (w \cdot u) + (\gamma * \beta) \circ (w \cdot v).$$

Jei kompozicijos dėsnis $\cdot$ aibėje V asociatyvus, tai algebra $(V, +, \cdot)$ yra vadinama asociatyviąja. Vėliau nagrinėsime ir neasociatyvių algebrų pavyzdžius.

Pastaba. Norėdami pabrėžti algebros apibrėžime dalyvaujančių kompozicijos dėsnių įvairovę, jiems žymėti naudojomės įvairiais simboliais. Tik ženklą "+" naudojome tiek sudėčiai aibėje k, tiek ir aibėje V žymėti. Tokios žymėjimų įvairovės ateityje atsisakysime. Daugybai žymėti naudosimės $*$ arba $\cdot$ arba jokių ženklų nerašysime tarp komponuojamų elementų.

Apibrėžimas. Kūno k elementų šeima $(\alpha_{ij}), 1 \leq i \leq m, 1 \leq j \leq n$, sunumeruota dviem indeksais ir surašyta į lentelę

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}$$

yra vadinama $m \times n$ matrica, o α_{ij} – šios matricos ij-elementu arba ij-komponente (α_{ij} – matricos elementas, užrašytas matricos i-osios eilutės ir j-ojo stulpelio sankirtoje).

Sutarkime $m \times n$ matricą žymėti ir taip: $(\alpha_{ij})_{ij=1}^{m,n}$. Matricos $(\alpha_{ij})_{ij=1}^{m,n}$ ir $(\beta_{ij})_{ij=1}^{m,n}$ yra lygios tada ir tik tada, kai bet kuriems i, j, $1 \leq i \leq m$, $1 \leq j \leq n$,

$$\alpha_{ij} = \beta_{ij}.$$

Visų $m \times n$ matricų, kurių elementai priklauso kūnui k, aibę žymėsime $M_{m \times n}(k)$. Jei $m = n$, tai $n \times n$ matricos dar yra vadinamos n-os eilės kvadratinėmis matricomis. Visų $n \times n$ matricų su koeficientais kūne k aibę žymėsime $M_n(k)$.

Aibės $M_{m \times n}(k)$ elementų sudėtis $+$.

Jei

$$(\alpha_{ij})_{ij=1}^{m,n}, (\beta_{ij})_{ij=1}^{m,n} \in M_{m \times n}(k),$$

tai

$$(\alpha_{ij})_{ij=1}^{m,n} + (\beta_{ij})_{ij=1}^{m,n} =: (\alpha_{ij} + \beta_{ij})_{i,j=1}^{m,n}.$$

Nesunku įsitikinti, kad $(M_{m \times n}(k), +)$ – Abelio grupė. $m \times n$ nulinė matrica $(0)_{i,j=1}^{m,n}$, – šios grupės neutralus elementas.

Aibės $M_{m \times n}(k)$ elementų daugyba iš kūno k elementų (išorinis kompozicijos dėsnis su operatorių aibe k aibėje $M_{m \times n}(k)$).

Apibrėžkime atvaizdį:

$$k \times M_{m \times n}(k) \to M_{m \times n}(k), \quad (\lambda,\ (\alpha_{ij})_{i,j=1}^{m,n}) \mapsto \lambda \cdot (\alpha_{ij})_{i,j=1}^{m,n},$$

čia
$$\lambda \cdot (\alpha_{ij})_{i,j=1}^{m,n} =: (\lambda \cdot \alpha_{ij})_{i,j=1}^{m,n}, \ \ \lambda \in k, \ (\alpha_{ij})_{i,j=1}^{m,n} \in M_{m\times n}(k).$$

2. 2. Galite įsitikinti apibrėžto išorinio kompozicijos dėsnio šiomis savybėmis:

1. Bet kuriems $\lambda, \mu \in k, \ A \in M_{m\times n}(k)$
$$(\lambda \cdot \mu) \cdot A = \lambda \cdot (\mu \cdot A);$$

2. Kiekvienai matricai $A \in M_{m\times n}(k))$
$$1 \cdot A = A, \ \ 1 \in k;$$

3. Bet kuriems $\lambda, \mu \in k, \ A \in M_{m\times n}(k)$
$$(\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A;$$

4. Bet kuriems $\lambda, k, \ A, B \in M_{m\times n}(k)$
$$\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B.$$

Sutarkime, kad $(\alpha_{ij})_{i,j=1}^{m,n} \cdot \lambda = (\alpha_{ij} \cdot \lambda)_{i,j=1}^{m,n}$. Tuomet akivaizdu, kad $\lambda \cdot A = A \cdot \lambda$, $\lambda \in k, A \in M_{m\times n}(k)$.

2. 3. Apibrėžkime $m \times n$ matricą e_{ij}, kurios ij-elmentas lygus $1 \in k$, o visi kiti yra lygūs $0 \in k$. Tuomet kiekvieną $m \times n$ matricą $(\alpha_{ij})_{i,j=1}^{m,n}$ galima vienareikšmiškai užrašyti taip:
$$(\alpha_{ij})_{i,j=1}^{m,n} = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} \cdot e_{ij}.$$

Šis užrašas patogus atlikinėjant matricų sudėties ir daugybos veiksmus.

Prisiminę anksčiau pateiktą tiesinės erdvės apibrėžimą, pastebėsime, kad visų $m \times n$ matricų grupė $(M_{m\times n}(k), +)$ yra tiesinė erdvė virš kūno k, o e_{ij}, $1 \le i \le m$, $1 \le j \le n$, – šios tiesinės erdvės bazė (žiūrėkite tiesinės erdvės bazės apibrėžimą).

2. 4. Matricų daugyba.

Apibrėšime atvaizdį
$$M_{m\times n}(k) \times M_{n\times p}(k) \to M_{m\times p}(k),$$
kuris yra vadinamas matricų daugyba.

Tarkime, kad
$$A = (\alpha_{ij})_{i,j=1}^{m,n} \in M_{m\times n}(k), \ B = (\beta_{ij})_{i,j=1}^{n,p} \in M_{n\times p}(k).$$

Tuomet matricų

$$(\alpha_{ij})_{i,j=1}^{m,n} \quad \text{ir} \quad (\beta_{ij})_{i,j=1}^{n,p}$$

sandauga yra vadinama matrica

$$(\alpha_{ij})_{i,j=1}^{m,n} \cdot (\beta_{ij})_{i,j=1}^{n,p} =: (\gamma_{ij})_{i,j=1}^{m,p},$$

kurios ij-elementas γ_{ij} apibrėžiamas taip:

$$\gamma_{ij} = \sum_{s=1}^{n} \alpha_{is} \cdot \beta_{sj}, \quad 1 \leq i \leq m, \ 1 \leq j \leq p.$$

Paprastai tariant, matricos $(\gamma_{ij})_{i,j=1}^{m,p}$ ij-elementas yra gaunamas pirmosios matricos i eilutę paelemenčiui sudauginant su antrosios matricos j stulpeliu ir gautus rezultatus sudedant.

2. 5. Nesunku įsitikinti matricų daugybos šiomis savybėmis:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C), \ A \in M_{m\times n}(k), \ B \in M_{n\times p}(k), \ C \in M_{p\times r}(k);$
2. $(A + B) \cdot C = A \cdot C + B \cdot C, \ A, B \in M_{m\times n}(k), \ C \in M_{n\times p}(k);$
3. $C \cdot (A + B) = C \cdot A + C \cdot B, \ C \in M_{m\times n}(k), \ A, B \in M_{n\times p}(k);$
4. Kiekvienai matricai $A \in M_{m\times n}(k)$

$$\mathbf{1}_m \cdot A = A,$$

čia $\mathbf{1}_m =: (\delta_{ij})_{i,j=1}^{m}$, vadinama m eilės vienetine matrica, o

$$\delta_{ij} = \begin{cases} 1, & \text{jei } i = j, \\ 0, & \text{jei } i \neq j, \end{cases}$$

yra Kronekerio δ funkcija;

5. Kiekvienai matricai $A \in M_{m\times n}(k)$

$$A \cdot \mathbf{1}_n = A.$$

2. 6. Atidžiau panagrinėkime $M_n(k)$. Kaip žinome, $(M_n(k), +)$ – Abelio grupė. Matricų daugyba $\cdot$ apibrėžta aibėje $M_n(k)$.

$$\mathbf{1}_n =: \sum_{j=1}^{n} e_{jj}$$

– neutralus aibės $M_n(k)$ elementas daugybos atžvilgiu. Taigi $(M_n(k), +, \cdot)$ – žiedas (netgi algebra virš kūno k, nes $M_n(k)$ – tiesinė erdvė virš kūno k, o matricų daugyba yra suderinta su tiesinės erdvės struktūra).

Algebros $(M_n(k),+,\cdot)$ elementų e_{ij}, $1\le i,j\le n$, daugybos lentelė atrodo taip:

$$e_{ij}\cdot e_{pq}=\delta_{jp}e_{iq},\ \ 1\le i,j,p,q\le n,$$

čia δ_{jp} – Kronekerio simbolis (funkcija). Kaip matome, elementai e_{ij}, $1\le i,j\le n$, yra matricų algebros $M_n(k)$ tiek kairieji, tiek dešinieji nulio dalikliai, o e_{ii}, $1\le i\le n$, – šio algebros idempotentai.

Algebros $(M_n(k),+,\cdot)$ elementų daugyba vienareikšmiškai apibrėžiama žinant elementų e_{ij}, $1\le i,j\le n$, daugybos lentelę:

$$(\sum_{i,j=1}^{n}\alpha_{ij}\cdot e_{ij})\cdot(\sum_{r,s=1}^{n}\beta_{rs}\cdot e_{rs})=\sum_{i,r,s=1}^{n}\alpha_{ir}\cdot\beta_{rs}\cdot e_{is}.$$

Algebros $(M_n(k),+,\cdot)$, $n>1$, elementų daugyba nėra komutatyvi, nes, pavyzdžiui, $e_{11}\cdot e_{12}=e_{12}$, o $e_{12}\cdot e_{11}=0$. Kaip matome, elementai e_{ij}, $1\le i,j\le n$, yra matricų algebros $(M_n(k),+,\cdot)$ tiek kairieji, tiek dešinieji nulio dalikliai, o e_{ii}, $1\le i\le n$, – šio algebros idempotentai.

Pratimai.

1. Tarkime, $u=\sum_{j=1}^{n-1}e_{jj+1}\in M_n(k)$. Įrodykite, kad $u^s=\sum_{j=1}^{n-s}e_{jj+s}$. Atskiru atveju $u^{n-1}=e_{1n},u^n=0$.

2. Apibrėžkime atvaizdį:

$$\mathrm{Tr}:M_n(k)\to k,\ \mathrm{Tr}(\sum_{i,j=1}^{n}\alpha_{ij}e_{ij})=\sum_{j=1}^{n}\alpha_{jj}.$$

Įrodykite, kad
i) $\mathrm{Tr}(A\cdot B)=\mathrm{Tr}(B\cdot A)$;
ii) $\mathrm{Tr}(\lambda\cdot A+\mu\cdot B)=\lambda\cdot\mathrm{Tr}(A)+\mu\cdot\mathrm{Tr}(B)$;
iii) $\mathrm{Tr}(\mathbf{1}_n)=n\cdot 1$, čia $\lambda,\mu,1\in k,\ A,B\in M_n(k)$.

3. Tarkime, kad atvaizdis $f:M_n(\mathbb{Q})\to\mathbb{Q}$ turi savybes:
1. $f(\mathbf{1}_n)=n$;
2. $f(\lambda\cdot A+\mu\cdot B)=\lambda\cdot f(A)+\mu\cdot f(B),\lambda,\mu\in\mathbb{Q},\ A,B\in M_n(\mathbb{Q})$;
3. $f(A\cdot B)=f(B\cdot A)$.

Įrodykite, kad $f=\mathrm{Tr}$.

Nurodymas. Pasinaudokite lygybėmis:

$$e_{ii}=e_{ij}\cdot e_{ji},e_{ij}=e_{ii}\cdot e_{ij}=e_{ij}\cdot e_{jj},\ 1\le i,j\le n,$$

$$\mathbf{1}_n=\sum_{j=1}^{n}e_{jj},\ e_{ij}\cdot e_{pq}=0,j\neq p.$$

4. Įrodykite, kad lygtis $X \cdot Y - Y \cdot X = \mathbf{1}_n$ algebroje $(M_n(k), +, \cdot)$ neišprendžiama.

5. Tarkime, kad $A = \mathbb{Q}[x]$,

$$\frac{d}{dx} : \mathbb{Q}[x] \to \mathbb{Q}[x],\ \frac{d}{dx} f(x) =: f'(x),$$

yra diferencijavimo atvaizdis,

$$m : \mathbb{Q}[x] \to \mathbb{Q}[x],\ m(f(x)) =: x \cdot f(x),$$

yra dauginimo iš kitamojo x operatorius. Įrodykite:

$$\frac{d}{dx} \circ m - m \circ \frac{d}{dx} = id,$$

čia $id : \mathbb{Q}[x] \to \mathbb{Q}[x], id(f(x)) = f(x)$, – tapatusis atvaizdis.

6. Tarkime,kad žiedo $(A, +, *)$ elementai a ir b turi savybę: $b * a = q * a * b$, čia $q * a = a * q, q * b = b * q$. Įrodykite Niutono binomo formulės analogą:

$$(a + b)^n = \sum_{j=0}^{n} \begin{bmatrix} n \\ j \end{bmatrix}_q * a^{n-j} * b^j,$$

čia

$$\begin{bmatrix} n \\ j \end{bmatrix}_q = \frac{[n]_q!}{[j]_q! * [n-j]_q!},\ [m]_q! =: (q^m - 1) * (q^{m-1} - 1) * \cdots * (q - 1).$$

Įrodykite,kad

$$\lim_{q \to 1} \begin{bmatrix} n \\ j \end{bmatrix}_q = \binom{n}{j}.$$

7. Įrodykite, kad $\mathbb{H}(\mathbb{C})$ galima sutapatinti su matricų algebra $M_2(\mathbb{C})$, t.y. egzistuoja bijekcija $f : \mathbb{H}(\mathbb{C}) \to M_2(\mathbb{C})$, turinti savybes: bet kuriems $\alpha \in \mathbb{C}$, $a, b \in \mathbb{H}$,

1. $f(\alpha \cdot a) = \alpha \cdot f(a)$;
2. $f(a + b) = f(a) + f(b)$;
3. $f(a \cdot b) = f(a) \cdot f(b)$.

Kaip matome, algebra $\mathbb{H}(\mathbb{C})$ nėra kūnas.

3. Žiedo idealai

3. 1. Tarkime, kad $(A, +, *)$ žiedas su vienetu.

Apibrėžimas. Netuščias žiedo $(A, +, *)$ poaibis $\mathfrak{a}$ yra vadinamas kairiuoju (dešiniuoju) žiedo idealu, jei:

1. $x, y \in \mathfrak{a} \Rightarrow x \pm y \in \mathfrak{a}$;
2. $a \in A, x \in \mathfrak{a} \Rightarrow a * x \in \mathfrak{a}$ ($a \in A, x \in \mathfrak{a} \Rightarrow x * a \in \mathfrak{a}$).

Antrąją žiedo idealo apibrėžimo sąlygą galima užrašyti ir taip: $A * \mathfrak{a} \subset \mathfrak{a}$ ($\mathfrak{a} * A \subset \mathfrak{a}$, čia $A * \mathfrak{a} =: \{a * x \mid a \in A, x \in \mathfrak{a}\}$ ($\mathfrak{a} * A =: \{x * a \mid x \in \mathfrak{a}, a \in A\}$).

Apibrėžimas. Netuščias žiedo $(A, +, *)$ poaibis $\mathfrak{a}$ yra vadinamas abipusiu žiedo idealu, jei:

1. $x, y \in \mathfrak{a} \Rightarrow x \pm y \in \mathfrak{a}$;
2. $a \in A, x \in \mathfrak{a} \Rightarrow a * x, x * a \in A$.

Komutatyvaus žiedo atveju kairiojo, dešiniojo ir abipusio žiedo idealo sąvokos sutampa.

3. 2. Teiginys. Tarkime, $(A, +, *)$ – žiedas, $a \in A$. Tuomet $A * a = \{x * a \mid x \in A\}$ yra kairysis žiedo A idealas, $a * A = \{a * x \mid x \in A\}$ – dešinysis žiedo idealas, o poaibis $A * a * A = \{x * a * y \mid x, y \in A\}$ – abipusis žiedo A idealas.

Įrodymas. 1. Jei $x, y \in A * a$, tai egzistuoja tokie $u, v \in A$, kad $x = u * a, y = v * a$. Vadinasi, $x \pm y = u * a \pm v * a = (u \pm v) * a \in A * a$.

2. Jei $x \in A * a$, tai egzistuoja toks $u \in A$, kad $x = u * a$. Vadinasi, kiekvienam $b \in A, b * x = b * (u * a) = (b * u) * a \in A * a$.

Įrodėme, kad $A * a$ yra kairysis žiedo idealas. Panašiai įrodoma, kad $a * A$ – dešinysis, o $A * a * A$ – abipusis žiedo idealas. $\triangle$

Apibrėžimas. Idealas $A * a$ (arba $a * A$ ir $A * a * A$), generuotas vieno elemento a, yra vadinamas kairiuoju (arba dešiniuoju ir abipusiu) pagrindiniu žiedo A idealu.

Idealų sudėtis. Tarkime, kad $\mathfrak{a}$ ir $\mathfrak{b}$ – žiedo $(A, +, *)$ kairieji idealai. Apibrėšime idealų $\mathfrak{a}$ ir $\mathfrak{b}$ sumą

$$\mathfrak{a} + \mathfrak{b} =: \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\},$$

t. y. aibė $\mathfrak{a} + \mathfrak{b}$, sudaryta iš sumų $x + y$, čia $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Panašiai yra apibrėžiama dešiniųjų ir abipusių idealų suma.

3. 3. Teiginys. Žiedo $(A, +, *)$ kairiųjų (dešiniųjų, abipusių) idealų $\mathfrak{a}$ ir$\mathfrak{b}$ suma $\mathfrak{a} + \mathfrak{b}$ yra kairysis (dešinysis, abipusis) žiedo $(A, +, *)$ idealas.

Įrodymas. 1.Tarkime, kad $x, y \in \mathfrak{a} + \mathfrak{b}$. Vadinasi, egzistuoja tokie $u_1, u_2 \in \mathfrak{a}$ ir $v_1, v_2 \in \mathfrak{b}$, kad $x = u_1 + v_1$, $y = u_2 + v_2$. Taigi

$$x \pm y = (u_1 + v_1) \pm (u_2 + v_2) = (u_1 \pm u_2) + (v_1 \pm v_2) \in \mathfrak{a} + \mathfrak{b},$$

nes $u_1 \pm u_2 \in \mathfrak{a}$, $v_1 \pm v_2 \in \mathfrak{b}$.

2. Tarkime, kad $x \in \mathfrak{a} + \mathfrak{b}$, t. y. egzistuoja tokie $u \in \mathfrak{a}$, $v \in \mathfrak{b}$, kad $x = u + v$. Tuomet, jei $a \in A$, tai

$$a * x = a * (u + v) = a * u + a * v \in \mathfrak{a} + \mathfrak{b},$$

nes $a * u \in \mathfrak{a}, a * v \in \mathfrak{b}$.

Panašiai teiginys įrodomas dešiniesiems ir abipusiems idealams. $\triangle$

3. 4. Apibrėžimas. Idealas $A * a_1 + A * a_2 + \ldots A * a_s$, čia a_1, a_2, ..., $a_s \in A$, yra vadinamas kairiuoju žiedo $(A, +, *)$ idealu, generuotu elementų a_1, a_2, ..., a_s. Panašiai apibrėžiami dešinieji ir abipusieji idealai, generuoti elementų a_1, a_2, ..., a_s. Komutatyvaus žiedo atveju idealas $A * a_1 + A * a_2 + \ldots + A * a_s$ yra žymimas $(a_1, a_2, \ldots, a_s)$, o elementai a_1, a_2, ..., a_s – vadinami idealo sudaromosiomis.

Pastaba. Idealo žymėjimą $(a_1, a_2, \ldots, a_s)$ galima supainioti su Dekarto sandaugos A^s elementu. Bet tikėkimės, kad iš konteksto bus aišku, apie ką yra kalbama.

Pavyzdžiai.

1. Kūno $(k, +, *)$ idealai yra tik nulinis (0) ir k. Iš tikrųjų, jei $\mathfrak{a}$ – kūno nenulinis idealas, tai egzistuoja $\alpha \neq 0, \alpha \in \mathfrak{a}$. Tuomet $\alpha^{-1} \in k, \alpha \in \mathfrak{a} \Rightarrow \alpha^{-1} * \alpha = 1 \in \mathfrak{a} \Rightarrow k \subset \mathfrak{a}$. Vadinasi, $\mathfrak{a} = k$.

2. **Teiginys.** Sveikųjų skaičių žiedo $(\mathbb{Z}, +, \cdot)$ kiekvienas idealas yra pagrindinis.

Įrodymas. Idealas (0) yra pagrindinis. Tarkime, $\mathfrak{a} \neq (0)$. Kadangi $\mathfrak{a}$ idealas, tai $x \in \mathfrak{a} \Rightarrow (-1) \cdot x = -x \in \mathfrak{a}$. Vadinasi, idealui $\mathfrak{a}$ priklauso mažiausias nenulinis natūralusis skaičius n. Įrodysime, kad $\mathfrak{a} = (n) = n\mathbb{Z}$. Akivaizdu, kad $(n) \subset \mathfrak{a}$. Reikia tik įrodyti, kad $\mathfrak{a} \subset (n)$. Jei $x \in \mathfrak{a}$, tai remdamiesi dalybos su liekana formule (žr.[3. 1. 5.]), galime parašyti $x = n \cdot y + z, 0 \leq z < n$. Jei būtų $z \neq 0$, tai, kadangi $x, n \in \mathfrak{a}$, gautume $z = x - n \cdot y \in \mathfrak{a}$. O tai prieštarautų skaičiaus n parinkimui (priminsime: n – idealo $\mathfrak{a}$ mažiausias nenulinis natūralusis skaičius). Taigi $x = n \cdot y \in (n)$, t. y. $\mathfrak{a} \subset (n)$. $\triangle$

3. **Teiginys.** Matricų algebra $M_n(k)$, čia k – kūnas, neturi abipusių idealų, išskyrus (0) ir $M_n(k)$.

Įrodymas. Priminsime, kad

$$M_n(k) = \{\sum_{i,j=1}^{n} \alpha_{ij} e_{ij} \mid \alpha_{ij} \in k,\ 1 \leq i, j \leq n\}.$$

Pirmiausia įrodysime, jei $\mathfrak{a}$ yra abipusis idealas, kuriam priklauso kuris nors elementas $e_{i_0 j_0}$, tai $\mathfrak{a} = M_n(k)$. Iš tikrųjų, jei $e_{i_0 j_0} \in \mathfrak{a}$ ir $\mathfrak{a}$ – abipusis idealas, tai

$$e_{rs} = e_{r i_0} \cdot e_{i_0 j_0} \cdot e_{j_0 s} \in \mathfrak{a},\ 1 \leq r, s \leq n.$$

Vadinasi, ir $\sum\limits_{i,j=1}^{n} \alpha_{ij} e_{ij} \in \mathfrak{a}$ kad ir kokie būtų koeficientai $\alpha_{ij} \in k$, $1 \leq i, j \leq n$.

Dabar tarkime, kad $\mathfrak{a}$ – nenulinis abipusis algebros $M_n(k)$ idealas. Įrodysime, kad idealui $\mathfrak{a}$ priklauso bent vienas elementas $e_{i_0 j_0}$ ir remdamiesi anksčiau įrodytu faktu, užbaigsime teiginio įrodymą.

Kadangi $\mathfrak{a} \neq (0)$, tai idealui $\mathfrak{a}$ priklauso nenulinis elementas $a = \sum_{i,j=1}^{n} \alpha_{ij} \d{o} te_{ij}$. Tarkime, kad $\alpha_{i_0 j_0} \neq 0$. Elementas

$$e_{i_0 i_0} \cdot a \cdot e_{j_0 j_0} = \alpha_{i_0 j_0} e_{i_0 j_0} \in \mathfrak{a},$$

nes $a \in \mathfrak{a}$ ir $\mathfrak{a}$ – abipusis idealas. Kadangi $\alpha_{i_0 j_0} \neq 0$, tai

$$\alpha_{i_0 j_0}^{-1} \cdot (\alpha_{i_0 j_0} \cdot e_{i_0 j_0}) = e_{i_0 j_0} \in \mathfrak{a}\,. \ \triangle$$

3. 5. Algebra $M_n(k)$ turi kairiųjų ir dešiniųjų idealų, nesutampančių nei su (0), nei su $M_n(k)$. Pavyzdžiui, $e_{ij} \cdot M_n(k)$ – dešinysis idealas, kurio kiekvienas elementas turi pavidalą

$$\sum_{s=1}^{n} \alpha_{is} \cdot e_{is}.$$

Kaip matome, $e_{ij} \cdot M_n(k) \neq M_n(k)$. Be to, akivaizdu, kad $e_{ij} \cdot M_n(k) = e_{i1} \cdot M_n(k)$.

Pratimas. Įrodykite, kad komutatyvus žiedas $(A, +, *)$, kurio idealai yra tik (0) ir A, yra kūnas.

4. Žiedo faktoržiedas pagal idealą

4. 1. Tarkime, kad $(A, +, *)$ – žiedas, $\mathfrak{a}$ – šio žiedo abipusis idealas. Apibrėšime faktoržiedą $(A/\,\mathfrak{a}, +, *)$. Tuo tikslu apibrėžkime ekvivalentumo sąryšį aibėje A:

$$x \underset{\mathfrak{a}}{\sim} y \Longleftrightarrow x - y \in \mathfrak{a}\,.$$

Vietoje $x \underset{\mathfrak{a}}{\sim} y$ galima rašyti $x \equiv y (\operatorname{mod} \mathfrak{a})$. Aibės A faktoraibę pagal apibrėžtą ekvivalentumo sąryšį pažymėkime $A/\,\mathfrak{a}$. Faktoraibės $A/\,\mathfrak{a}$ elementai užrašomi $x + \mathfrak{a}$ (elementas $x + \mathfrak{a}$ dažnai yra žymimas $x (\operatorname{mod} \mathfrak{a})$). Remiantis ekvivalentumo sąryšio apibrėžimu,

$$x + \mathfrak{a} = y + \mathfrak{a} \Longleftrightarrow x - y \in \mathfrak{a}\,.$$

Aibės $A/\,\mathfrak{a}$ elementų sudėtis $+$.

Apibrėžkime elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}, x, y \in A$ sumą taip:

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) =: x + y + \mathfrak{a}\,.$$

Įsitikinsime, kad elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}$ suma $x + y + \mathfrak{a}$ nepriklauso nuo atstovų x ir y parinkimo. Tarkime, kad $x' + \mathfrak{a} = x + \mathfrak{a}, y' + \mathfrak{a} = y + \mathfrak{a}$. Tuomet $x' - x \in \mathfrak{a}, y' - y \in \mathfrak{a}$. Vadinasi, $x' + y' + \mathfrak{a} = x + y + \mathfrak{a}$, nes $(x' + y') - (x + y) = (x' - x) + (y' - y) \in \mathfrak{a}$ (priminsime: $x' - x \in \mathfrak{a}, y' - y \in \mathfrak{a} \Rightarrow (x' - x) + (y' - y) \in \mathfrak{a}$, nes $\mathfrak{a}$ yra idealas).

Nesunku įsitikinti, kad $(A/\,\mathfrak{a}, +)$ – Abelio grupė, $\mathfrak{a}$ – šios grupės neutralus elementas sudėties atžvilgiu.

Aibės $A/\,\mathfrak{a}$ elementų daugyba $*$.

Apibrėžkime elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}, x, y \in A$, sandaugą taip:

$$(x + \mathfrak{a}) * (y + \mathfrak{a}) =: x * y + \mathfrak{a}\,.$$

Įsitikinsime, kad elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}$ sandauga $x * y + \mathfrak{a}$ nepriklauso nuo atstovų x ir y parinkimo. Tarkime, kad $x' + \mathfrak{a} = x + \mathfrak{a}, y' + \mathfrak{a} = y + \mathfrak{a}$. Tuomet

$$(x' + \mathfrak{a}) * (y' + \mathfrak{a}) = x' * y' + \mathfrak{a}, \quad \text{o} \quad (x + \mathfrak{a}) * (y + \mathfrak{a}) = x * y + \mathfrak{a}\,.$$

Teigiame, kad $x' * y' + \mathfrak{a} = x * y + \mathfrak{a}$. Iš tikrųjų, nes

$$x' * y' - x * y = x' * y' - x' * y + x' * y - x * y = x' * (y' - y) + (x' - x) * y \in \mathfrak{a}$$

(priminsime: $\mathfrak{a}$ – abipusis idealas, $x' - x \in \mathfrak{a}, y' - y \in \mathfrak{a} \Rightarrow x' * (y' - y) \in \mathfrak{a}, (x' - x) * y \in \mathfrak{a} \Rightarrow x' * (y' - y) + (x' - x) * y \in \mathfrak{a}$).

Nesunku įsitikinti, kad aibės $A/\,\mathfrak{a}$ elementų daugyba yra asociatyvi. Įrodysime, kad aibės $A/\,\mathfrak{a}$ elementų sudėtis ir daugyba yra susieti distributyvumo dėsniais:

$$((x + \mathfrak{a}) + (y + \mathfrak{a})) * (z + \mathfrak{a}) = (x + \mathfrak{a}) * (z + \mathfrak{a}) + (y + \mathfrak{a}) * (z + \mathfrak{a}),$$

$$(z + \mathfrak{a}) * ((x + \mathfrak{a}) + (y + \mathfrak{a})) = (z + \mathfrak{a}) * (x + \mathfrak{a}) + (z + \mathfrak{a}) * (y + \mathfrak{a}).$$

Įrodysime tik pirmąją lygybę, nes antroji lygybė įrodoma panašiai.

$$((x + \mathfrak{a}) + (y + \mathfrak{a})) * (z + \mathfrak{a}) = (x + y + \mathfrak{a}) * (z + \mathfrak{a}) = (x + y) * z + \mathfrak{a} =$$

$$= x * z + y * z + \mathfrak{a} = (x * z + \mathfrak{a}) + (y * z + \mathfrak{a}) = (x + \mathfrak{a}) * (z + \mathfrak{a}) + (y + \mathfrak{a}) * (z + \mathfrak{a}).$$

Taigi aibė $A/\,\mathfrak{a}$ apibrėžtų jos elementų sudėties $+$ ir daugybos $*$ atžvilgiu yra žiedas. Jei žiedas $(A, +, *)$ turi vienetą 1, tai $1 + \mathfrak{a}$ yra žiedo $(A/\,\mathfrak{a}, +, *)$ vienetas.

4. 2. Apibrėžimas. Žiedas $(A/\,\mathfrak{a}, +, *)$ yra vadinamas žiedo $(A, +, *)$ faktoržiedu pagal abipusį idealą $\mathfrak{a}$.

5. Žiedų homomorfizmai

5. 1. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, 0_A ir 0_B yra žiedo A ir žiedo B nuliai.

Apibrėžimas. Atvaizdis $f : A \to B$ yra vadinamas homomorfizmu, jei bet kuriems $x, y \in A$:

1. $f(x + y) = f(x) + f(y)$;
2. $f(x * y) = f(x) * f(y)$.

Įrodysime keletą paprastų faktų.

5. 2. Teiginys. Jei $f : A \to B$ – homomorfizmas, tai:

1. $f(0_A) = 0_B$;
2. $f(-x) = -f(x), x \in A$.

Įrodymas. 1. Galime parašyti: $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$. Pirmoji iš šių lygybių gaunama remiantis tuo, kad $(0_A = 0_A + 0_A)$, o antroji – remiantis tuo, kad f – homomorfizmas. Prie lygybės $f(0_A) + f(0_A) = f(0_A)$ abiejų pusių pridėję elementui $f(0_A)$ priešingą elementą $-f(0_A)$, gauname:

$$(f(0_A) + f(0_A)) + (-f(0_A)) = f(0_A) + (-f(0_A)) = 0_B.$$

Bet kairėje lygybės pusėje esantis elementas yra lygus:

$$f(0_A) + ((f(0_A) + (-f(0_A)) = f(0_A) + 0_B = f(0_A).$$

Vadinasi, $f(0_A) = 0_B$.

2. Remdamiesi anksčiau įrodyta lygybe, gauname: $0_B = f(0_A) = f(x + (-x)) = f(x) + f(-x)$. Paskutinioji lygybė gaunama remiantis tuo, kad f – homomorfizmas. Vadinasi, $f(-x)$ yra elementui $f(x)$ priešingas elementas, t. y. $f(-x) = -f(x)$. $\triangle$

5. 3. Teiginys. Jei $f : A \to B$ – nenulinis homomorfizmas, 1_A – žiedo A vienetas, tai $f(1_A)$ yra žiedo B idempotentas (idempotentas – tai nenulinis elementas, tenkinantis lygtį: $x^2 = x$).

Įrodymas. Panašiai kaip ir įrodant [5. 2] teiginį, galime parašyti: $f(1_A) = f(1_A * 1_A) = f(1_A) * f(1_A)$. Žiede lygtį $x * x = x$ tenkina idempotentai. Kadangi $f(1_A) * f(1_A) = f(1_A)$, tai galime teigti tik, kad $f(1_A)$ yra žiedo B idempotentas. $\triangle$

Pastabos.

1. Štai paprastas pavyzdys, iliustruojantis, kad $f(1_A)$ gali ir nebūti žiedo B vienetu. Apibrėžkime žiedą

$$A = \mathbb{Q} * e_1 + \mathbb{Q} * e_2 =: \{\alpha * e_1 + \beta * e_2 \mid \alpha, \beta \in \mathbb{Q}\},$$

čia $\alpha * e_1 + \beta * e_2 = \gamma * e_1 + \delta * e_2$ tada ir tik tada, kai $\alpha = \gamma, \beta = \delta$. Apibrėžkime aibės A elementų sudėtį taip:

$$(\alpha_1 * e_1 + \alpha_2 * e_2) + (\beta_1 * e_1 + \beta_2 * e_2) =: (\alpha_1 + \beta_1) * e_1 + (\alpha_2 + \beta_2) * e_2.$$

Galite nesunkiai įsitikinti, kad $(A, +)$ yra Abelio grupė, o $0 =: 0 * e_1 + 0 * e_2$ – šios grupės nulis. Apibrėžkime elementų e_1, e_2 daugybos lentelę taip:

$$e_1^2 = e_1 * e_1 = e_1, e_2^2 = e_2 * e_2 = e_2, e_1 * e_2 = e_2 * e_1 = 0.$$

Remdamiesi 6-ąja žiedo apibrėžimo aksioma, daugybą galime išplėsti iki aibės A elementų daugybos. Taigi $(A, +, *)$ – žiedas. Apibrėžkime atvaizdį $f : A \to A$ taip:

$$f(\alpha_1 * e_1 + \alpha_2 * e_2) = \alpha_* e_1.$$

Žiedo $(A, +, *)$ vienetas daugybos atžvilgiu yra $e_1 + e_2$. Kaip matome, $f(e_1 + e_2) = e_1$, o e_1 yra žiedo A idempotentas.

2. Dažnai yra nagrinėjami žiedų homomorfizmai $f : A \to B$ siauresne prasme, kai reikalaujama, kad žiedo A vieneto 1_A vaizdas $f(1_A)$ būtų žiedo B vienetas.

5. 4. Teiginys. Jei $f : A \to B$ – siurjektyvus homomorfizmas, tai žiedo $(A, +, *)$ vieneto 1_A vaizdas $f(1_A)$ yra žiedo $(B, +, *)$ vienetas.

Įrodymas. Pažymėkime žiedo B elementą $f(1_A)$ raide e. Norint įrodyti, kad e yra žiedo B vienetas, reikia įrodyti, kad bet kuriam žiedo B elementui b, $e * b = b * e = b$. Kadangi $f : A \to B$ – siurjektyvus homomorfizmas, tai kiekvienam žiedo B elementui b egzistuoja toks žiedo A elementas a, kad $f(a) = b$. Lygybės $1_A * a = a * 1_A = a$ abi puses paveikę atvaizdžiu f, gauname: $f(1_A * a) = f(a * 1_A) = f(a)$. Šią lygybę pertvarkę, gauname: $f(1_A) * f(a) = f(a) * f(1_A) = f(a)$, t. y. $e * b = b * e = b$. △

Teiginys. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai. Jei $f : A \to B$ – homomorfizmas, tai $f(A)$ yra žiedo B požiedis.

Įrodymas. Jei $x, y \in f(A)$,tai egzistuoja tokie $a, b \in A$, kad $f(a) = x, f(b) = y$. Vadinasi, $x + y = f(a) + f(b) = f(a + b) \in f(A)$. Taigi žiedo B poaibis $f(A)$ yra stabilus sudėties atžvilgiu, $f(0_A) = 0_B \in f(A)$. Jei $x \in f(A)$, tai egzistuoja toks $a \in A$, kad $f(a) = x$. Tuomet $f(-a) = -f(a) = -x$. Vadinasi, $(f(A), +)$ yra Abelio grupė. Poaibis $f(A)$ taip pat yra stabilus ir daugybos atžvilgiu:

$$x * y = f(a) * f(b) = f(a * b) \in f(A),$$

čia $a, b \in A$ tokie, kad $f(a) = x, f(b) = y$. △

Apibrėžimas. Tarkime, kad $f : A \to B$ – homomorfizmas. Žiedo A poaibis $\mathrm{Ker}\, f =: \{x \in A \,|\, f(x) = 0_B\}$ (t. y. $\mathrm{Ker}\, f = f^{-1}(0_B)$) yra vadinamas homomorfizmo f branduoliu.

5. 5. Teorema. Homomorfizmo $f : A \to B$ branduolys Ker f yra žiedo A abipusis idealas. Žiedo A faktoržiedas $A/\mathrm{Ker}\ f$ yra izomorfinis žiedo A vaizdui $f(A)$.

Įrodymas. Pastebėsime , kad Ker $f \neq \emptyset$, nes $0_A \in$ Ker f (žr.[5. 2.]). Dabar patikrinsime abipusio idealo apibėžimo aksiomas.

1. Jei $x, y, \in$ Ker f, tai $f(x) = 0_B, f(y) = 0_B$. Vadinasi, $f(x \pm y) = f(x) \pm f(y) = 0_B + 0_B = 0_B$, t. y. $x \pm y \in$ Ker f.

2. Jei $x \in$ Ker $f, a \in A$, tai $f(x * a) = f(x) * f(a) = 0_B * f(a) = 0_B$. Panašiai, $f(a * x) = f(a) * f(x) = f(a) * 0_B = 0_B$. Taigi Ker f yra žiedo A abipusis idealas.

Kadangi Ker f yra žiedo A abipusis idealas, galima nagrinėti žiedo A faktoržiedą $A/\mathrm{Ker}\ f$ pagal idealą Ker f. Lieka įrodyti, kad $A/\mathrm{Ker}\ f$ yra izomorfinis žiedo A vaizdui $f(A)$.

Homomorfizmas $f : A \to B$ generuoja atvaizdį

$$\bar{f} : A/\mathrm{Ker}\ \to f(A),\ \bar{f}(x + \mathrm{Ker}\ f) =: f(x),\ x \in A.$$

Įrodysime, kad atvaizdis $\bar{f} : A/\mathrm{Ker}\ f \to f(A)$ yra korektiškai apibrėžtas, t. y. nepriklauso nuo ekvivalentumo klasės $x + \mathrm{Ker}\ f$ atstovo x parinkimo: jei $x + \mathrm{Ker}\ f = y + \mathrm{Ker}\ f$, tai ir $\bar{f}(x + \mathrm{Ker}\ f) = \bar{f}(y + \mathrm{Ker}\ f)$. Tarkime, kad $x + \mathrm{Ker}\ f = y + \mathrm{Ker}\ f$, t. y. $x - y \in \mathrm{Ker}\ f$. Tuomet $\bar{f}(x + \mathrm{Ker}\ f) = f(x)$, o $\bar{f}(y + \mathrm{Ker}\ f) = f(y)$. Kadangi $x - y \in \mathrm{Ker}\ f$, tai $f(x - y) = 0_B$. Vadinasi, $f(x) - f(y) = 0_B$, t. y. $f(x) = f(y)$.

Atvaizdis $\bar{f} : A/\mathrm{Ker}\ f \to f(A)$ yra siurjektyvus. Jei $b \in f(A)$, tai egzistuoja toks $a \in A$, kad $f(a) = b$ (remiamės atvaizdžio $f : A \to B$ siurjektyvumu). Tuomet $\bar{f}(a + \mathrm{Ker}\ f) = f(a) = b$. Įsitikinsime, kad šis atvaizdis yra ir injektyvus.

Jei $\bar{f}(a + \mathrm{Ker}\ f) = \bar{f}(a' + \mathrm{Ker}\ f)$, tai $f(a) = f(a')$ arba $f(a) - f(a') = 0_B$. Remdamiesi pastarąja lygybe, gauname: $f(a - a') = 0_B$,t. y. $a - a' \in \mathrm{Ker}\ f$, o tai ir reiškia, kad $a + \mathrm{Ker}\ f = a' + \mathrm{Ker}\ f$.

Atvaizdis $\bar{f} : A/\mathrm{Ker}\ f \to f(A)$ yra homomorfizmas, nes

$$\bar{f}((a + \mathrm{Ker}\ f) * (a' + \mathrm{Ker}\ f)) = \bar{f}(a * a' + \mathrm{Ker}\ f) =$$

$$= f(a * a') = f(a) * f(a') = \bar{f}(a + \mathrm{Ker}\ f) * \bar{f}(a' + \mathrm{Ker}\ f).$$

Kadangi $\bar{f}$ yra bijektyvus homomorfizmas, tai teorema pilnai įrodyta. $\triangle$

5. 6. Teiginys. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, $f : A \to B$ – siurjektyvus homomorfizmas. Tuomet žiedo A kairiojo (dešiniojo, abipusio) idealo $\mathfrak{a}$ vaizdas $f(\mathfrak{a})$ yra kairysis (dešinysis, abipusis) žiedo B idealas.

Įrodymas. Sakykime, $\mathfrak{a}$ – kairysis žiedo A idealas, $f(\mathfrak{a})$ – jo vaizdas. Jei $x, y \in f(\mathfrak{a})$, tai egzistuoja tokie $a, b \in \mathfrak{a}$, kad $f(a) = x$, $f(b) = y$. Tuomet $x \pm y = f(a) \pm f(b) = f(a \pm b) \in f(\mathfrak{a})$, nes $a \pm b \in \mathfrak{a}$. Jei $x \in f(\mathfrak{a})$, $y \in B$, tai egzistuoja tokie $a \in \mathfrak{a}$, $b \in A$, kad $f(a) = x$, $f(b) = y$. Tuomet $y * x = f(b) * f(a) = f(b * a) \in f(\mathfrak{a})$, nes $b * a \in \mathfrak{a}$.

Panašiai įrodoma, kad žiedo A dešiniojo (abipusio) idealo vaizdas yra žiedo B dešinysis (abipusis) idealas. $\triangle$

Teiginys. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, $f : A \to B$ – homomorfizmas. Tuomet žiedo B kairiojo (dešiniojo, abipusio) idealo $\mathfrak{b}$ pirmavaizdis $f^{-1}(\mathfrak{b})$ yra žiedo A kairysis (atitinkamai dešinysis, abipusis) idealas.

Įrodymas. Sakykime, kad $\mathfrak{b}$ – žiedo B kairysis idealas, $f^{-1}(\mathfrak{b})$ – jo pirmavaizdis. Jei $x, y \in f^{-1}(\mathfrak{b})$, t. y. $f(x), f(y) \in \mathfrak{b}$, tai $x \pm y \in f^{-1}(\mathfrak{b})$, nes $f(x \pm y) = f(x) \pm f(y) \in \mathfrak{b}$. Jei $x \in f^{-1}(\mathfrak{b})$, $y \in A$, tai $y * x \in f^{-1}(\mathfrak{b})$. Iš tikrųjų: $f(y * x) = f(y) * f(x) \in \mathfrak{b}$, nes $f(y) \in B$, $f(x) \in \mathfrak{b}$, o kadangi $\mathfrak{b}$ idealas, tai ir $f(y) * f(x) \in \mathfrak{b}$.

Panašiai įrodoma, kad žiedo B dešiniojo (abipusio) idealo pirmavaizdisas yra žiedo A dešinysis (abipusis) idealas. $\triangle$

Pratimas. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, $f : A \to B$ – siurjektyvus homomorfizmas, $\mathfrak{a}$ – žiedo A abipusis idealas. Įrodykite: $(f^{-1} \circ f)(\mathfrak{a}) = \mathfrak{a} + \mathrm{Ker}\ f$.

5. 7. Teiginys. Sakykime, kad $\mathfrak{a} \subset \mathfrak{b}$ yra žiedo A abipusieji idealai. Tuomet $\mathfrak{b} / \mathfrak{a}$ yra faktoržiedo $A/\mathfrak{a}$ abipusis idealas.

Įrodymas. Šį teiginį siūlome įrodyti skaitytojui.

Nagrinėsime žiedo idealus, nesutampančius su pačiu žiedu.

Teiginys. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, $f : A \to B$ – siurjektyvus homomorfizmas. Tuomet žiedo B abipusių idealų aibė I(B) yra ekvivalenti žiedo A abipusių idealų $\mathfrak{a}$, tenkinančių sąlygą $\mathfrak{a} \supset \mathrm{Ker}\ f$, aibei $I(A/\mathrm{Ker}\ f)$.

Įrodymas. Jei $\mathfrak{b}$ yra žiedo B abipusis idealas, tai $f^{-1}(\mathfrak{b})$ yra žiedo A abipusis idealas ir $\mathrm{Ker}\ f \subset f^{-1}(\mathfrak{b})$. Taigi galime apibrėžti atvaizdį $F : I(B) \to I(A/\mathrm{Ker}\ f)$, $F(\mathfrak{b}) = f^{-1}(\mathfrak{b})$, $\mathfrak{b} \in I(B)$. Įsitikinsime, kad F yra bijekcija.

Jei $\mathfrak{a}$ yra žiedo A abipusis idealas ir $\mathrm{Ker}\ f \subset \mathfrak{a}$, t. y. $\mathfrak{a} \in I(A/\mathrm{Ker}\ f)$, tai $\mathfrak{b} =: f(\mathfrak{a})$ yra žiedo B abipusis idealas. Be to, $F(\mathfrak{b}) = f^{-1}(f(\mathfrak{a})) = \mathfrak{a} + \mathrm{Ker}\ f = \mathfrak{a}$. Kaip matome, F yra siurjektyvus atvaizdis. Akivaizdu, kad F – injektyvus atvaizdis: jei $\mathfrak{b}_1 \neq \mathfrak{b}_2$, tai $f^{-1}(\mathfrak{b}_1) \neq f^{-1}(\mathfrak{b}_2)$, t. y. $F(\mathfrak{b}_1) \neq F(\mathfrak{b}_2)$. $\triangle$

5. 8. Sakykime, $(A, +, *)$ – žiedas, $I(A)$ yra šio žiedo visų abipusių idealų, nesutampančių su žiedu A, aibė. $I(A)$ įdėties $\subset$ atžvilgiu yra dalinai sutvarkyta aibė. Remdamiesi Corno lema (žr.[1. 5. 3]), įrodysime, kad aibėje $I(A)$ egzistuoja bent vienas maksimalus elementas.

Teiginys. Žiedo $(A, +, *)$ su vienetu visų abipusių idealų, nelygių žiedui A, aibėje $I(A)$ egzistuoja bent vienas maksimalus elementas įdėties $\subset$ atžvilgiu.

Įrodymas. Įsitikinsime, kad aibė $I(A)$ tenkina Corno lemos sąlygą. Sakykime, $\{\mathfrak{a}_\alpha\}_{\alpha \in P}$ yra žiedo A įdėties $\subset$ atžvilgiu tiesiškai sutvarkytų abipusių idealų šeima. Reikia įrodyti, kad žiedo A abipusių idealų šeima $\{\mathfrak{a}_\alpha\}_{\alpha\in P}$ aibėje $I(A)$ yra aprėžta iš viršaus. Tuo tikslu įrodysime, kad aibė $\cup_{\alpha\in P}\mathfrak{a}_\alpha$ yra žiedo A abipusis idealas, nelygus žiedui A.

Sakykime,

$$x, y \in \cup_{\alpha\in P}\mathfrak{a}_\alpha.$$

Tuomet egzistuoja toks $\alpha_0 \in P$, kad $x, y \in \mathfrak{a}_{\alpha_0}$. Kadangi $\mathfrak{a}_{\alpha_0}$ yra žiedo A abipusis idealas, tai

$$x \pm y \in \mathfrak{a}_{\alpha_0} \subset \cup_{\alpha\in P}\mathfrak{a}_\alpha.$$

Jei

$$x \in \cup_{\alpha\in P}\mathfrak{a}_\alpha, y \in A,$$

tai egzistuoja toks $\alpha_0 \in P$, kad $x \in \mathfrak{a}_{\alpha_0}$. Kadangi $\mathfrak{a}_{\alpha_0}$ yra žiedo A abipusis idealas, tai

$$x * y, y * x \in \mathfrak{a}_{\alpha_0} \subset \cup_{\alpha\in P}\mathfrak{a}_\alpha.$$

Kaip matome, $\cup_{\alpha\in P}\mathfrak{a}_\alpha$ yra žiedo A abipusis idealas ir kiekvienam $\alpha \in P$,

$$\mathfrak{a}_\alpha \in \cup_{\alpha\in P}\mathfrak{a}_\alpha.$$

Be to, šis idealas nesutampa su žiedu A. Priešingu atveju žiedo vienetas 1 priklausytų kuriam nors $\mathfrak{a}_\alpha$, $\alpha \in P$, o tai prieštarautų sąlygai, kad visi aibės $I(A)$ elementai yra žiedo A idealai, nesutampantys su A. Dabar, remdamiesi Corno lema, gauname, kad aibė $I(A)$ turi bent vieną maksimalų elementą $\mathfrak{m}$. $\triangle$

5. 9. Nuo šiol nagrinėsime tik komutatyvius žiedus $(A, +, *)$ su vienetu. Tegu $(A, +, *)$ toks žiedas, o $\mathfrak{m}$ – šio žiedo maksimalus idealas. Įrodysime komutatyvaus žiedo maksimalaus idealo svarbią savybę.

Teiginys. Jei komutatyvaus žiedo $(A, +, *)$ su vienetu elementų x ir y sandauga $x * y$ priklauso maksimaliam šio žiedo idealui $\mathfrak{m}$, tai bent vienas iš elementų x ar y priklauso $\mathfrak{m}$.

Įrodymas. Sakykime, kad žiedo A elementų x ir y sandauga $x * y$ priklauso maksimaliam idealui $\mathfrak{m}$. Jei elementas $x \in \mathfrak{m}$, tai teiginio įrodymas baigtas. Sakykime, kad $x \notin \mathfrak{m}$. Tuomet $A * x + \mathfrak{m}$ yra žiedo A idealas, nes $A * x$ ir $\mathfrak{m}$ yra idealai, o idealų suma, kaip žinome, yra idealas. Kadangi $x \in A * x + \mathfrak{m}$, bet $x \notin \mathfrak{m}$, tai $A * x + \mathfrak{m} = A$. Vadinasi, egzistuoja tokie $a \in A$, $m \in \mathfrak{m}$, kad $1 = a * x + m$. Padauginę šios lygybės abiejų pusių elementus iš y, gauname $y = a*x*y + m*y$. Remdamiesi sąlyga $x*y \in \mathfrak{m}$, gauname, kad ir $a * x * y \in \mathfrak{m}$. Kadangi $m \in \mathfrak{m}$, tai ir $m * y \in \mathfrak{m}$. Taigi ir elementas y priklauso idealui $\mathfrak{m}$, nes yra dviejų elementų $a * x * y$ ir $m * y$, priklausančių idealui $\mathfrak{m}$, suma. $\triangle$

5. 10. Teiginys. Komutatyvaus žiedo $(A, +, *)$ su vienetu 1 faktoržiedas $A/\mathfrak{m}$ pagal žiedo A idealą $\mathfrak{m}$ yra kūnas tada ir tik tada, kai $\mathfrak{m}$ yra maksimalus idealas.

Įrodymas. Kaip žinome, komutatyvaus žiedo $(A, +, *)$ su vienetu 1 faktoržiedas $A/\mathfrak{m}$ pagal žiedo A idealą $\mathfrak{m}$ yra žiedas. Sakykime, kad $\mathfrak{m}$ yra maksimalus idealas. Įrodysime, kad faktoržiedo $A/\mathfrak{m}$ kiekvienam nenuliniam elementui egzistuoja atvirkštinis elementas. Imkime $x + \mathfrak{m} \in A/\mathfrak{m}$, $x \notin \mathfrak{m}$. Idealas $A * x + \mathfrak{m}$ tenkina sąlygas:

(i) $\mathfrak{m} \subset A * x + \mathfrak{m}$;

(ii) $\mathfrak{m} \neq A * x + \mathfrak{m}$, $x \in A * x + \mathfrak{m}$, $x \notin \mathfrak{m}$.

Vadinasi, $A = A * x + \mathfrak{m}$. Taigi egzistuoja tokie $a \in A$, $m \in \mathfrak{m}$, kad $a * x + m = 1$. Teigiame, kad faktoržiedo $A/\mathfrak{m}$ elementas $a+\mathfrak{m}$ yra atvirkštinis elementui $x+\mathfrak{m}$. Iš tikrųjų:

$$(a + \mathfrak{m}) * (x + \mathfrak{m}) = a * x + \mathfrak{m} = 1 - m + \mathfrak{m} = 1 + \mathfrak{m}\,.$$

Sakykime, kad faktoržiedas $A/\mathfrak{m} = k$ yra kūnas. Atvaizdis $f : A \to k$ yra siurjektyvus homomorfizmas, kurio branduolys yra $\mathfrak{m}$. Pagal anksčiau įrodytą teiginį (žr,[5. 7.]), yra abipus vienareikšmė atitinkamybė tarp k idealų ir žiedo A idealų $\mathfrak{a}$, tenkinančių sąlygą: $\mathfrak{m} \subset \mathfrak{a}$. Kaip žinome, kūnas k neturi tarpinių idealų tarp $\{0\}$ ir paties kūno k. Vadinasi, nėra žiedo A tarpinių idealų tarp $\mathfrak{m}$ ir A. Taigi $\mathfrak{m}$ yra žiedo A maksimalus idealas. $\triangle$

6. Dalumas žieduose

6. 1. Nagrinėsime dalumo sąvoką žieduose.

Apibrėžimas. Sakykime, $(A, +, *)$ yra komutatyvus žiedas su vienetu 1, $a, b \in A$. Elementas b yra vadinamas elemento a dalikliu (dažnai ir taip yra sakoma: elementas b dalija elementą a) ir žymimas $b|a$, jei egzistuoja toks elementas $c \in A$, kad $a = b * c$.

Nagrinėjant kurio nors žiedo savybes, svarbu žinoti šio žiedo vieneto daliklius.

Teiginys. Komutatyvaus žiedo $(A, +, *)$ su vienetu 1 žiedo vieneto daliklių aibė A^* žiedo elementų daugybos $*$ atžvilgiu sudaro grupę.

Įrodymas. Aibė A^* netuščia, nes $1 \in A^*$ ($1|1$, nes $1 * 1 = 1$). Sakykime, kad $a, b \in A^*$, t. y. egzistuoja tokie $c, d \in A$, kad $a * c = 1$, $b * d = 1$. Tuomet $(a * b) * (c * d) = (a * c) * (b * d) = 1 * 1 = 1$, t. y., jei a ir b yra vieneto 1 dalikliai, tai elementas $a * b$ taip pat yra vieneto daliklis. Vadinasi, žiedo A poaibis A^* yra stabilus žiedo elementų daugybos $*$ atžvilgiu. Daugyba $*$ yra asociatyvi, $1 \in A^*$. Jei $a \in A^*$, tai egzistuoja toks $b \in A$, kad $a * b = 1$. Bet šią lygybę galima ir taip užrašyti: $b * a = 1$. Taigi $b \in A^*$ ir yra atvirkštinis elementas elementui a. Grupė $(A^*, *)$ yra komutatyvi, nes žiedas A yra komutatyvus. $\triangle$

Apibrėžimas. Komutatyvaus žiedo $(A, +, *)$ su vienetu 1 elementai a ir b yra vadinami asocijuotais (ekvivalenčiais), jei egzistuoja toks žiedo vieneto daliklis u (t. y. $u \in A^*$), kad $a = b * u$. Jei a ir b yra asocijuoti, tai rašysime $a \approx b$.

Kitaip tariant, elementai a ir b yra asocijuoti (ekvivalentūs), jei $a|b$ ir $b|a$.

Teiginys. Binarusis sąryšis $\approx$ aibėje A yra ekvivalentumo sąryšis.

Įrodymas. 1. Kiekvienam $a \in A$, $a \sim a$, nes $a = a * 1$, $1 \in A^*$.

2. Jei $a \approx b$, tai $b \approx a$. Iš tikrųjų, jei $a \approx b$, tai egzistuoja toks $u \in A^*$, kad $a = b * u$. Bet $u^{-1} \in A^*$. Vadinasi, $b = a * u^{-1}$, t. y. $b \approx a$.

3. Jei $a \approx b$ ir $b \approx c$, tai ir $a \approx c$. Iš tikrųjų, jei $a \approx b$ ir $b \approx c$, tai egzistuoja tokie $u, v \in A^*$, kad $a = b * u$, $b = c * v$. Iš šių lygybių gauname: $a = b * u = c * (v * u)$, t. y. $a \approx c$, nes kadangi $u, v \in A^*$, tai ir $u * v \in A^*$. $\triangle$

6. 2. Apibrėžimas. Komutatyvaus žiedo $(A, +, *)$ su vienetu 1 elementas π, kuris nėra lygus jokiam vieneto dalikliui, yra vadinamas pirminiu, jei elemento π dalikliai yra tik žiedo A vieneto 1 dalikliai ir elementai, ekvivalentūs elementui π.

Pavyzdžiai.

1. Sveikųjų skaičių žiedo $(\mathbb{Z}, +, \cdot)$ vieneto dalikliai yra $\{1, -1\}$. Ekvivalentūs pirminiai skaičiai skiriasi ženklu. Kalbant apie pirminius skaičius, iš dviejų, tarpusavy ekvivalenčių pirminių skaičių, visuonet galime pasirinkti teigiamąjį.

2. Skaičių aibė $\mathbb{Z}[\sqrt{2}] =: \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ skaičių sudėties $+$ ir daugybos $*$ atžvilgiu sudaro komutatyvų žiedą su vienetu $1 = 1 + 0\sqrt{2}$. Šis žiedas turi be galo daug vieneto daliklių. Pavyzdžiui, $\varepsilon = 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ yra žiedo vieneto dakiklis. Iš tikrųjų: $-1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, o $(-1 + \sqrt{2})(1 + \sqrt{2}) = -(-1)^2 + (\sqrt{2})^2 = 1$. Elementai ε^n, $n \in \mathbb{Z}$ yra vieneto dalikliai. Visų žiedo $\mathbb{Z}[\sqrt{2}]$ vieneto daliklių grupė yra $\{\pm\varepsilon^n | n \in \mathbb{Z}\}$.

Pavyzdžiui, žiedo $\mathbb{Z}[\sqrt{2}]$ elementai $\sqrt{2}$, 3, 5, $3+\sqrt{2}$, $3-\sqrt{2}$, 11, 13, $5+2\sqrt{2}$, $5-2\sqrt{2}$, 19, $5 + \sqrt{2}$, $5 - \sqrt{2}$ ir t. t., yra pirminiai, tarpusavy neekvivalentūs. Be įrodymo paaiškinsime, kaip galite rasti žiedo $\mathbb{Z}[\sqrt{2}]$ tarpusavy neekvivalenčius pirminius elementus. Teigiami sveikieji pirminiai skaičiai p, tenkinantys sąlygą $p \equiv \pm 1 (\mathrm{mod} 8)$, yra pirminiai ir žiede $\mathbb{Z}[\sqrt{2}]$. Teigiami sveikieji pirminiai skaičiai p, tenkinantys sąlygą $p \equiv 3, 5 (\mathrm{mod} 8)$, yra išskaidomi dviejų neekvivalenčių pirminių elementų $a + b\sqrt{2}$ ir $a - b\sqrt{2}$, priklausančių žiedui $\mathbb{Z}[\sqrt{2}]$, sandauga: $p = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Elementai $a + b\sqrt{2}$ ir $a - b\sqrt{2}$ yra apibrėžti daugiklių $\pm\varepsilon^n$, $n \in \mathbb{Z}$, tikslumu. Pareikalaukime, kad pirminio skaičiaus p, $p \equiv 3, 5 (\mathrm{mod} 8)$, pirminių daugiklių $a + b\sqrt{2}$ ir $a - b\sqrt{2}$ sveikosios dalys a būtų teigiamos ir mažiausios. Taip apibrėžtus žiedo $\mathbb{Z}[\sqrt{2}]$ pirminius elementus $a + b\sqrt{2}$, $a - b\sqrt{2}$ ir pirminius skaičius p, $p \equiv \pm 1 (\mathrm{mod} 8)$ vadinsime žiedo $\mathbb{Z}[\sqrt{2}]$ normuotais pirminiais elementais.

Dabar suformuluosime svarbią teoremą apie žiedo $\mathbb{Z}[\sqrt{2}]$ nenulinių elementų išskaidymą pirminių elementų sandauga. Šios teoremos neįrodysime.

Teorema. Žiedo $\mathbb{Z}[\sqrt{2}]$ kiekvienas nenulinis elementas yra vienareikšmiškai išskaidomas vieneto daliklio ir normuotų pirminių elementų sandauga, jei nekreipiame dėmesio į dauginamųjų tvarką.

3. Panašiai kaip ir 2-me pavyzdyje, nagrinėkime žiedą $\mathbb{Z}[\sqrt{-5}] =: \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu. Šio žiedo vieneto daliklių grupė yra $\{1, -1\}$. Tai įrodysime.

Sakykime, $a+b\sqrt{-5}|1$. Tuomet egzistuoja toks $c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, kad $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$, t. y. $ac - 5bd = 1$, $ad + bc = 0$. remdamiesi šiomis lygybėmis, matome, kad ir $(a - b\sqrt{-5})(c - d\sqrt{-5}) = 1$. Vadinasi,

$$(a + b\sqrt{-5})(c + d\sqrt{-5})(a - b\sqrt{-5})(c - d\sqrt{-5}) = 1$$

arba

$$(a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2) = 1.$$

Ši lygybė galima tik tuo atveju, jei $a^2 + 5b^2 = 1$, $a, b \in \mathbb{Z}$. Lygtis $a^2 + 5b^2 = 1$ sveikaisiais skaičiais turi tik šiuos sprendinius: $a = 1, b = 0$ ir $a = -1, b = 0$. Pagaliau įrodėme, kad žiedo $\mathbb{Z}[\sqrt{-5}]$ vieneto dalikliai yra tik $\{1, -1\}$.

Žiedo $\mathbb{Z}[\sqrt{-5}]$ elementai 3, 7, $4+\sqrt{-5}$ ir $4-\sqrt{-5}$ yra pirminiai. Pavyzdžiui, įrodysime, kad 3 yra pirminis elementas. Sakykime, kad $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 3$. Panašiai kaip ir anksčiau, galime įrodyti, kad $(a - b\sqrt{-5})(c - d\sqrt{-5}) = 3$. Vadinasi,

$$(a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2) = 9.$$

Kadangi $a^2 + 5b^2|9$, tai skaičius $a^2 + 5b^2$ gali būti lygus 1, 3 arba 9. Jei $a^2 + 5b^2 = 1$, tai $a = \pm 1, b = 0$. Šiuo atveju $c + d\sqrt{-5} = \pm 3$. Lygtis $a^2 + 5b^2 = 3$ sprendinių sveikaisiais skaičiais neturi. Jei $a^2 + 5b^2 = 9$, tai $a = \pm 3, b = 0$. Pagaliau išnagrinėjome visus atvejus ir įsitikinome, kad 3 yra pirminis elementas. Panašiai įrodoma, kad 7 yra žiedo $\mathbb{Z}[\sqrt{-5}]$ pirminis elementas.

Dabar įrodysime, kad $4 + \sqrt{-5}$ yra taip pat žiedo $\mathbb{Z}[\sqrt{-5}]$ pirminis elementas. Sakykime, kad

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 4 + \sqrt{-5}.$$

Tuomet $ac - 5bd = 4$, $ad + bc = 1$. Remdamiesi šiomis lygybėmis, galite įsitikinti, kad

$$(a - b\sqrt{-5})(c - d\sqrt{-5}) = 4 - \sqrt{-5}.$$

Vadinasi,

$$(a + b\sqrt{-5})(c + d\sqrt{-5})(a - b\sqrt{-5})(c - d\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}) = 21.$$

Sudauginę šios lygybės kairėje pusėje reiškinius, gauname: $(a^2 + 5b^2)(c^2 + 5d^2) = 21$. Vadinasi, $a^2 + 5b^2$ gali būti lygus 1, 3, 7, 21. Bet lygtys $a^2 + 5b^2 = 3$, $a^2 + 5b^2 = 7$ sprendinių sveikaisiais skaičiais neturi. Jei $a^2 + 5b^2 = 1$, tai $a = \pm 1, b = 0$. Šiuo atveju $c + d\sqrt{-5} = \pm(4 + \sqrt{-5})$. Jei $a^2 + 5b^2 = 21$, tai tuomet $c^2 + 5d^2 = 1$. Šiuo atveju $a + b\sqrt{-5} = \pm(4 + \sqrt{-5})$. Panašiai įrodoma, kad žiedo $\mathbb{Z}[\sqrt{-5}]$ elementas $4 - \sqrt{-5}$ yra taip pat pirminis.

Bet štai siurprizas:

$$3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = 21.$$

Žiedo $\mathbb{Z}[\sqrt{-5}]$ elementas 21 yra išskaidomas pirminiais elementais dviem visiškai skirtingais būdais! Žiede $\mathbb{Z}[\sqrt{-5}]$ nėra vienareikšmio išskaidymo nenulinių elementų pirminiais elementais.

7. Polinomų žiedai

7. 1. Šiame skyrelyje nagrinėsime polinomų žiedą.

Apibrėžimas. Tarkime, $(A, +, *)$ – komutatyvus žiedas su vienetu 1. Begalinę formalią sumą $\sum\limits_{j \geq 0} a_j x^j = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m + \ldots$, $a_j \in A$, $j \geq 0$, vadinsime kintamojo x polinomu su koeficientais žiede A, jei egzistuoja toks neneigiamas sveikasis skaičius n, kad kiekvienam $j > n$, $a_j = 0$.

Apibrėžimas. Kintamojo x polinomus $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m + \ldots$ ir $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m + \ldots$ su koeficientais žiede A vadinsime lygiais ir žymėsime $f(x) = g(x)$ tada ir tik tada, kai kiekvienam $j \geq 0$, $a_j = b_j$. Visų kintamojo x polinomų su koeficientais žiede A aibę žymėsime $A[x]$.

Pastabos.

1. Polinomą $0 + 0x + 0x^2 + \ldots + 0x^m + \ldots$ vadinsime nuliniu ir sutapatinsime su žiedo A nuliumi 0.

2. Polinomą $1 + 0x + 0x^2 + \ldots + 0x^m + \ldots$ sutapatinsime su žiedo A vienetu 1.

3. Jei polinomo $f(x) = \sum\limits_{j \geq 0} a_j x^j$, $f(x) \in A[x]$, visi koeficientai $a_j = 0$, kai $j > n$, tai vietoje begalinės sumos $\sum\limits_{j \geq 0} a_j x^j$ rašysime baigtinę sumą $\sum\limits_{j=0}^{n} a_j x^j$.

Apibrėžimas. Sakysime, kad nenulinis polinomas $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in A[x]$ yra laipsnio n, jei $a_n \neq 0$. Polinomo $f(x)$ laipsnį žymėsime $\deg f(x)$.

Aibės $A[x]$ elementų sudėtis.

Sakykime, kad $f(x) == \sum\limits_{j \geq 0} a_j x^j$, $g(x) = \sum\limits_{j \geq 0} b_j x^j \in A[x]$. Tuomet $f(x) + g(x) =: \sum\limits_{j \geq 0} (a_j + b_j) x^j$.

Akivaizdu, kad $(A[x], +)$ yra Abelio grupė.

Aibės $A[x]$ elementų daugyba.

Sakykime, kad $f(x) == \sum\limits_{j\geq 0} a_j x^j$, $g(x) = \sum\limits_{j\geq 0} b_j x^j \in A[x]$. Tuomet

$$f(x) \cdot g(x) =: \sum_{j\geq 0} (\sum_{\substack{r+s=j \\ r,s\geq 0}} a_r * b_s) x^j.$$

Akivaizdu, kad dviejų polinomų sandauga yra polinomas.

Pratimas. Įrodykite, kad polinomų daugyba yra asociatyvi.

Teiginys. Aibė $A[x]$ polinomų sudėties ir daugybos atžvilgiu yra komutatyvus žiedas su vienetu 1.

Įrodymas. Kaip minėjome, $(A[x], +)$ yra Abelio grupė. Polinomų daugyba yra asociatyvi, 1 – daugybos atžvilgiu vienetas. Polinomų daugyba komutatyvi, nes žiedo A elementų daugyba komutatyvi. Lieka įsitikinti, kad polinomų sudėtis ir daugyba yra susieti distributyvumo dėsniu

$$(f(x) + g(x)) \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x), \quad f(x), g(x), h(x) \in A[x].$$

Sakykime, kad $f(x) = \sum\limits_{j\geq 0} a_j x^j$, $g(x) = \sum\limits_{j\geq 0} b_j x^j$, $h(x) = \sum\limits_{j\geq 0} c_j x^j$. Tuomet

$$(f(x) + g(x)) \cdot h(x) = \sum_{j\geq 0} (\sum_{\substack{r+s=j \\ r,s\geq 0}} (a_r + b_r) * c_s) x^j = \sum_{j\geq 0} (\sum_{\substack{r+s=j \\ r,s\geq 0}} (a_r * c_s + b_r * c_s)) x^j =$$

$$= \sum_{j\geq 0} (\sum_{\substack{r+s=j \\ r,s\geq 0}} a_r * c_s) x^j + \sum_{j\geq 0} (\sum_{\substack{r+s=j \\ r,s\geq 0}} b_r * c_s) x^j = f(x) \cdot h(x) + g(x) \cdot h(x).$$

Apibrėžimas. $(A[x], +, \cdot)$ yra vadinamas kintamojo x polinomų žiedu su koeficientais žiede A.

7. 2. Teiginys. Jei žiedas $(A, +, *)$ neturi nulio daliklių, tai ir polinomų žiedas $A[x]$ neturi nulio daliklių.

Įrodymas. Sakykime, $f(x) = \sum\limits_{j\geq 0}^{n} a_j x^j$, $g(x) = \sum\limits_{j\geq 0}^{m} b_j x^j \in A[x]$ atitinkamai n-ojo ir m-ojo laipsnių polinomai (t.y. $a_n \neq 0$ ir $b_m \neq 0$). Tuomet

$$f(x) \cdot g(x) = (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) \cdot (b_m x^m + b_{m-1} + \ldots + b_1 x + b_0) =$$

$$= a_n * b_m x^{n+m} + (a_n * b_{m-1} + a_{n-1} * b_m) x^{n+m-1} + \ldots + a_0 * b_0.$$

Kadangi $a_n \neq 0, b_m \neq 0$, tai $a_n * b_m \neq 0$ (nes žiedas A neturi nulio daliklių). Vadinasi, jei $f(x) \neq 0, g(x) \neq 0$, tai ir $f(x) \cdot g(x) \neq 0$. $\triangle$

7. 3. Išvada. Jei $f(x) \neq 0, g(x) \neq 0$, tai deg $(f(x) \cdot g(x)) =$ deg $f(x) +$ deg $g(x)$.

7. 4. Polinomų dalumo sąvoka yra dalumo sąvokos žiede atskiras atvejis.

Apibrėžimas. Tarkime, kad $f(x), g(x) \in A[x]$. Sakysime polinomas $g(x)$ dalija polinomą $f(x)$ (arba polinomas $g(x)$ yra polinomo $f(x)$ daliklis) ir žymėsime $g(x)|f(x)$, jei egzistuoja toks polinomas $h(x) \in A[x]$, kad $f(x) = g(x) \cdot h(x)$.

Teiginys. Jei komutatyvus žiedas $(A, +, *)$ su vienetu 1 neturi nulio daliklių, tai kintamojo x polinomų žiedo $A[x]$ vieneto daliklių grupė $(A[x])^*$ sutampa su žiedo A vieneto daliklių grupe A^*

Įrodymas. Sakykime, $f(x) \in A[x]$ ir $f(x)|1$, t. y. egzistuoja toks $g(x) \in A[x]$, kad $f(x) \cdot g(x) = 1$. Remdamiesi šia lygybe, matome, kad deg $f(x) +$ deg $g(x) =$ deg $1 = 0$. Kadangi deg $f(x) \geq 0$, deg $g(x) \geq 0$, tai deg $f(x) = 0$, t. y. $f(x) = a \in A$. Remdamiesi sąlyga $a|1$, gauname, kad $f(x) = a \in A^*$. Įrodėme: $(A[x])^* \subset A^*$. Įdėtis $A^* \subset (A[x])^*$ – akivaizdi. Taigi $(A[x])^* = A^*$. $\triangle$

7. 5. Dabar išnagrinėsime kintamojo x polinomų su koeficientais kūne k žiedą $k[x]$. Šio žiedo struktūra pakankamai paprasta.

Dalybos su liekana formulė.

Sakykime, kad $f(x), g(x) \in k[x]$. Tuomet egzistuoja tokie vienintelia polinomai $h(x)$ ir $r(x)$, priklausantys žiedui $k[x]$, kad

$$f(x) = g(x) \cdot h(x) + r(x)$$

ir deg $r(x) <$ deg $g(x)$.

Įrodymas. Sakykime, kad $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $g(x) = b_m x^m + b_{m-1} + \ldots + b_1 x + b_0$, $a_n \neq 0$, $b_m \neq 0$. Jei $n < m$, tai imkime $h(x) = 0$, $r(x) = f(x)$. Tuomet dalybos su liekana formulę galime užrašyti taip: $f(x) = g(x) \cdot 0 + f(x)$, deg $f(x) <$ deg $g(x)$.

Jei $n \geq m$, tai polinomą $g(x)$ padauginę iš $\frac{a_n}{b_m} x^{n-m}$ ir atėmę iš polinomo $f(x)$, gauname: $f(x) - g(x) \cdot \frac{a_n}{b_m} x^{n-m} = (a_{n-1} - \frac{a_n}{b_m} * b_{m-1})x^{n-1} + \ldots =: f_1(x)$. Šią lygybę perrašykime taip: $f(x) = g(x) \cdot \frac{a_n}{b_m} x^{n-m} + f_1(x)$. Polinomo $f_1(x)$ laipsnis nėra didesnis nei $n - 1$. Jei deg $f_1(x) < m$, tai šiuo atveju polinomo $f(x)$ dalyba iš polinomo $g(x)$ baigta ir dalybos su liekana formulė atrodo taip: $f(x) = g(x) \cdot (c_1 x^{n-m}) + f_1(x)$, čia $c_1 = \frac{a_n}{b_m}$. Jei deg $f_1(x) \geq m$, tai, panašiai kaip ir anksčiau, polinomą $f_1(x)$ dalijame iš polinomo $g(x)$ ir gauname lygybę: $f_1(x) = g(x) \cdot (c_2 x^{\deg f_1 - m}) + f_2(x)$, čia deg $f_2(x) <$ deg $f_1(x) \leq n - 1$. Atlikę šiuos veiksmus, gauname: $f(x) = g(x) \cdot (c_1 x^{n-m} + c_2 x^{\deg f_1 - m}) + f_2(x)$. Jei deg $f_2(x) < m$, tai polinomo $f(x)$ dalyba iš polinomo $g(x)$ baigta. Jei deg $f_2(x) \geq m$, tai, kaip ir anksčiau, polinomą $f_2(x)$ dalijame iš polinomo $g(x)$. Šį procesą tęsiame tol, kol gauname, kad liekanos laipsnis yra mažesnis už polinomo $g(x)$ laipsnį m. Taigi po baigtinio žingsnių skaičiaus gausime: $f(x) = g(x) \cdot h(x) + r(x)$, deg $r(x) <$ deg $g(x)$.

Lieka įrodyti, kad polinomai $h(x)$ ir $r(x)$ vienareikšmiškai apibrėžiami. Sakykime, kad $f(x) = g(x)\cdot h'(x)+r'(x)$, deg $r'(x) <$ deg $g(x)$. Tuomet iš lygybės $f(x) = g(x)\cdot h(x)+r(x)$ atėmę lygybę $f(x) = g(x)\cdot h'(x)+r'(x)$, gauname: $g(x)\cdot(h(x)-h'(x))+(r(x)-r'(x)) = 0$. Jei būtų $h(x) - h'(x) \neq 0$, tai polinomo $g(x) \cdot (h(x) - h'(x))$ laipsnis būtų deg $g(x)$ + deg $(h(x) - h'(x)) \geq m$, o polinomo $r(x) - r'(x)$ laipsnis būtų griežtai mažesnis už m. Vadinasi, polinomas $g(x) \cdot (h(x) - h'(x)) + (r(x) - r'(x))$ negalėtų būti lygus 0. Taigi $h(x) = h'(x)$, $r(x) = r'(x)$.

7. 6. Apibrėžimas. Polinomas $f(x)$ yra vadinamas nenulinių polinomų $g_1(x)$, $g_2(x)$, ... , $g_s(x)$, didžiausiu bendruoju dalikliu, jei

1. $f(x)|g_1(x)$, $f(x)|g_2(x)$, ... , $f(x)|g_s(x)$ (t. y. polinomas $f(x)$ yra polinomų $g_1(x)$, $g_2(x)$, ... , $g_s(x)$ bendras daliklis);
2. Jei $h(x)|g_1(x)$, $h(x)|g_2(x)$, ... , $h(x)|g_s(x)$, tai $h(x)|f(x)$.

Teiginys. Polinomų $g_1(x)$, $g_2(x)$, ... , $g_s(x)$ didžiausias bendrasis daliklis vienareikšmiškai yra apibrėžiamas daugiklio $\varepsilon \in k^*$ tikslumu.

Įrodymas. Jei $f_1(x)$ ir $f_2(x)$ yra polinomų $g_1(x)$, $g_2(x)$, ... , $g_s(x)$ didžiausi bendriausieji dalikliai, tai remdamiesi polinomų $g_1(x)$, $g_2(x)$, ... , $g_s(x)$ didžiausio bendrojo daliklio apibrėžimu, gauname, kad $f_1(x)|f_2(x)$ ir $f_2(x)|f_1(x)$. Vadinasi, egzistuoja tokie $g_1(x) \in k[x]$ ir $g_2(x) \in k[x]$, kad $f_2(x) = f_1(x)\cdot h_1(x)$ ir $f_1(x) = f_2(x)\cdot h_2(x)$. Remdamiesi šiomis lygybėmis, gauname:

$$f_2(x) = f_1(x) \cdot h_1(x) = f_2(x) \cdot h_2(x) \cdot h_1(x)$$

arba $f_2(x)\cdot(1 - h_2(x)\cdot h_1(x)) = 0$. Kadangi žiedas $k[x]$ neturi nulio dakiklių ir $f_2(x) \neq 0$, tai $h_1(x) \cdot h_2(x) = 1$, t. y. $h_1(x), h_2(x) \in k^*$. Pažymėję $h_2(x) = \varepsilon \in k^*$, gauname $f_1(x) = \varepsilon \cdot f_2(x)$. $\triangle$

7. 7. 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:

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

Paskutinė, nelygi nuliui, liekana $f_m(x)$ ir yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis. Tai įrodysime. Polinomas $f_m(x)$ dalija polinomą f_{m-1}. Remdamiesi priepaskutine lygybe, matome, kad $f_m(x)$ dalija polinomą f_{m-2}. Kildami parašytomis lygybėmis aukštyn, gauname, kad $f_m(x)$ dalija polinomus $f_{m-3}(x), \ldots, f_2(x)$ ir $f_1(x)$. Jei polinomas $h(x)$ dalija polinomus $f_1(x)$ ir $f_2(x)$, tai, remdamiesi pirmąja lygybe, matome, kad $f_1(x)$ dalija $f_3(x)$. Leisdamiesi lygybėmis žemyn, gausime, kad $f_1(x)$ dalija ir $f_m(x)$. Taigi $f_m(x)$ yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis.

7. 8. 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

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

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

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

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: $f_m(x) = f_{m-2}(x) - f_{m-1}(x) \cdot h_{m-1}(x)$. Į šią lygybę įrašę polinomo f_{m-1} išraišką, gautą iš Euklido algoritmo aukščiau esančios lygybės, gauname: $f_m(x) = f_{m-2}(x) - (f_{m-3}(x) - f_{m-2}(x) \cdot h_{m-2}(x)) \cdot h_{m-1}(x) = -f_{m-3}(x) \cdot h_{m-1}(x) + f_{m-2}(x) \cdot (1 + h_{m-2}(x) \cdot h_{m-1}(x))$. Į šią lygybę įrašę polinomo $f_{m-2}(x)$ išraišką polinomais f_{m-3} ir f_{m-4}, gausime 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 $f_2(x)$:

$$f_m(x) = f_1(x) \cdot g_1'(x) + f_2(x) \cdot g_2'(x).$$

Remdamiesi šia lygybe, gauname $d(x) = \varepsilon \cdot (f_1(x) \cdot g_1'(x) + f_2(x) \cdot g_2'(x)) = f_1(x) \cdot g_1(x) + f_2(x) \cdot g_2(x)$, čia $g_1(x) = \varepsilon \cdot g_1'(x)$, $g_2(x) = \varepsilon \cdot g_2'(x)$. $\triangle$

7. 9. Pirminis polinomas.

Apibrėžimas. Polinomas $p(x) \in k[x]$ yra vadinmas pirminiu virš kūno k, jei polinomas $p(x)$ neišskaidomas dviejų polinomų $f(x), g(x) \in k[x]$, kurių laipsniai mažesni už polinomo $p(x)$ laipsnį, sandauga $f(x) \cdot g(x)$. Kitaip tariant, polinomas $p(x)$ yra pirminis virš kūno k, jei lygybė $p(x) = f(x) \cdot g(x)$, $f(x), g(x) \in k[x]$, yra galima tik tuo atveju, kai $p(x) = \varepsilon \cdot f(x)$, $g(x) = \varepsilon^{-1}$ arba $p(x) = \varepsilon \cdot g(x)$, $f(x) = \varepsilon^{-1}$, $\varepsilon \in k^*$.

Jei kūnas k yra kūno K pokūnis, tai polinomų žiedas $k[x]$ yra žiedo $K[x]$ požiedis. Polinomas $p(x) \in k[x]$ pirminis virš kūno k gali nebūti pirminiu virš kūno K, t. y. gali būti išskaidomas dviejų polinomų $f(x), g(x) \in K[x]$, $\deg f(x) < \deg p(x)$, $\deg g(x) < \deg p(x)$, sandauga $f(x) \cdot g(x)$.

Pavyzdžiui, polinomas $x^2 - 2 \in \mathbb{Q}[x]$ yra pirminis virš kūno $\mathbb{Q}$, nes $\sqrt{2} \notin \mathbb{Q}$ ir todėl šis polinomas nėra išskaidomas dviejų pirmojo laipsnio polinomų su racionaliais koeficientais sandauga. Bet šis polinomas nėra pirminis virš kūno $\mathbb{Q}(\sqrt{2})$, nes $x^2-2 = (x-\sqrt{2})\cdot(x+\sqrt{2})$.

Apibrėžimas. Polinomą $f(x) \in k[x]$ vadinsime normuotu, jei jo koeficientas prie aukščiausiojo x laipsnio yra lygus 1, t. y. jei $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$.

Nagrinėkime žiedą $k[x]$. Kaip ir bendruoju žiedų teorijos atveju, polinomus $f(x)$ ir $g(x)$ vadinsime ekvivalenčiais, jei $f(x) = \varepsilon \cdot g(x)$, $\varepsilon \in k^*$. Tarpusavy ekvivalenčių polinomų aibėje $\{\varepsilon \cdot f(x) | \varepsilon \in k^*\}$ egzistuoja vienitelis normuotas polinomas. Jei $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$, tai, polinomą $f(x)$ padauginę iš a_n^{-1}, gausime normuotą polinomą $a_n^{-1} \cdot f(x) = x^n + a_n^{-1}a_{n-1}x^{n-1} + \ldots + a_n^{-1}a_1 x + a_n^{-1}a_0$, priklausantį polinomo $f(x)$ ekvivalentumo klasei. Kalbėdami apie polinomų didžiausią bendrąjį daliklį apibrėžtumo dėlei galime turėti omenyje polinomų normuotą didžiausią bendrąjį daliklį.

Įrodysime pirminių polinomų $p(x) \in k[x]$ labai svarbią savybę.

7. 10. Teorema. Jei žiedo $k[x]$ pirminis polinomas $p(x)$ dalija polinomų $f(x), g(x) \in k[x]$ sandaugą $f(x) \cdot g(x)$, tai $p(x)$ dalija bent vieną iš polinomų: $f(x)$ ar $g(x)$.

Įrodymas. Jei $p(x) | f(x)$, tai teoremos teiginys įrodytas. Jei $p(x) \not| f(x)$, tai polinomų $p(x)$ ir $f(x)$ didžiausias bendrasis daliklis yra lygus 1. Vadinasi, egzistuoja tokie polinomai $u(x), v(x) \in k[x]$, kad $p(x) \cdot u(x) + f(x) \cdot v(x) = 1$. Padauginę šią lygybę iš $g(x)$, gauname: $p(x) \cdot u(x) \cdot g(x) + f(x) \cdot g(x) \cdot v(x) = g(x)$. Polinomas $p(x)$ dalija polinomą, esantį kairėje šios lygybės pusėje, vadinasi, $p(x)$ dalija ir $g(x)$. $\triangle$

7. 11. Teorema. Kiekvienas nenulinis polinomas $f(x) \in k[x]$ vienareikšmiškai išskaidomas vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga, jei nekreipiame dėmesio į dauginamųjų tvarką.

Įrodymas. Visų pirmiausia įrodysime, kad kiekvieną nenulinį polinomą $f(x) \in k[x]$ galima išskaidyti vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga.

Nulinio laipsnio nenulinis polinomas yra vieneto daliklis. Šiuo atveju teiginys yra teisingas. Pirmojo laipsnio polinomą $a_1 x + a_0$, $a_1 \neq 0$, galime užrašyti taip: $a_1 x + a_0 = a_1(x + a_1^{-1}a_0)$. Tai ir yra polinomo $a_1 x + a_0$ skaidinys vieneto daliklio a_1 ir normuoto pirminio polinomo $x + a_1^{-1}a_0$ sandauga. Sakykime, teiginys yra įrodytas kiekvienam nenuliniam polinomui $f(x) \in k[x]$, kurio laipsnis yra mažesnis nei n. Įrodysime, kad kiekvienas ir n-ojo laipsnio polinomas yra išskaidomas vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga. Imkime n-ojo laipsnio polinomą $f(x) \in k[x]$. Jei $f(x)$ yra pirminis virš kūno k, tai, iškėlę prieš skliaustus polinomo $f(x)$ koeficientą prie aukščiausiojo x laipsnio, gausime ieškomą polinomo $f(x)$ skaidinį. Jei $f(x)$ nėra pirminis virš kūno k, tai egzistuoja tokie $g(x), h(x) \in k[x]$, $\deg g(x) < \deg f(x)$, $\deg h(x) < \deg f(x)$, kad

$f(x) = g(x) \cdot h(x)$. Polinomai $g(x), h(x)$ pagal prielaidą yra išskaidomi vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga. Taigi tokia sandauga yra išskaidomas ir polinomas $f(x)$.

Dabar įrodysime skaidinio vienatį. Sakykime, kad

$$f(x) = \varepsilon \cdot p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x) = \eta \cdot q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x),$$

$\varepsilon, \eta \in k^*$, $p_1(x)$, $p_2(x)$, …, $p_r(x)$, $q_1(x)$, $q_2(x)$, …, $q_s(x)$ – normuoti pirminiai polinomai virš k. Reikia įrodyti, kad $r = s$, $\varepsilon = \eta$ ir egzistuoja toks skaičių 1, 2, …, r keitinys j_1, j_2, …, j_r, kad $p_1(x) = q_{j_1}(x)$, $p_2(x) = q_{j_2}(x)$, …, $p_r(x) = q_{j_r}(x)$.

Visiškai akivaizdu, kad $\varepsilon = \eta = a_n$ – polinomo $f(x)$ koeficientas prie aukščiausiojo x laipsnio. Polinomas $p_1(x)$ yra pirminis virš k ir

$$p_1(x) | q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x).$$

Jei $p_1(x) \not| q_1(x)$, tai, remdamiesi įrodyta pirminių polinomų savybe, gauname:

$$p_1(x) | q_2(x) \cdot \ldots \cdot q_s(x).$$

Taip tęsdami toliau, po baigtinio žingsnių skaičiaus, gausime, kad $p_1(x) | q_{j_1}(x)$. Kadangi $p_1(x)$ ir $q_{j_1}(x)$ yra normuoti pirminiai polinomai virš k ir $p_1(x) | q_{j_1}(x)$, tai $p_1(x) = q_{j_1}(x)$. Polinomų žiedas $k[x]$ neturi nulio daliklių, vadinasi,

$$\varepsilon \cdot p_1(x) \cdot (p_2(x) \cdot \ldots \cdot p_r(x) - q_1(x) \cdot q_2(x) \cdot \ldots \cdot \hat{q}_{j_1}(x) \cdot \ldots \cdot q_s(x)) = 0$$

tik tuo atveju, kai

$$p_2(x) \cdot \ldots \cdot p_r(x) - q_1(x) \cdot q_2(x) \cdot \ldots \cdot \hat{q}_{j_1}(x) \cdot \ldots \cdot q_s(x) = 0,$$

t. y., kai

$$p_2(x) \cdot \ldots \cdot p_r(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot \hat{q}_{j_1}(x) \cdot \ldots \cdot q_s(x)$$

(stogelis virš polinomo rodo, kad to polinomo sandaugoje nėra). Teoremos įrodymą galima užbaigti matematinės indukcijos metodu, tarus, kad kiekvieno polinomo, kurio laipsnis yra mažesnis nei polinomo $f(x)$ laipsnis, skaidinio pirminiais polinomais vienatis įrodyta. $\triangle$

8. Polinomų žiedo $k[x]$ idealų struktūra

8. 1. Polinomų žiedo $k[x]$ idealų struktūra paprasta.

Teiginys. Polinomų žiedas $k[x]$ yra pagrindinių idealų žiedas. Kitais žodžiais tariant, jei $\mathfrak{a}$ yra žiedo $k[x]$ idealas, tai egzistuoja toks polinomas $f(x) \in k[x]$, kad $\mathfrak{a} = f(x) \cdot k[x]$. Kaip paprastai, $f(x) \cdot k[x]$ sudaro visi polinomai, polinomo $f(x)$ kartotiniai, t. y. $f(x) \cdot k[x] = \{f(x)g(x) |\ g(x) \in k[x]\}$.

Įrodymas. Jei $\mathfrak{a} = \{0\}$, tai $\mathfrak{a} = \{0\} = 0 \cdot k[x]$. Jei $\mathfrak{a} \neq \{0\}$, tai egzistuoja mažiausio laipsnio polinomas $f(x)$, priklausantis idealui $\mathfrak{a}$. Remdamiesi idealo apibrėžimu, gauname, kad $f(x) \cdot k[x] \subset \mathfrak{a}$. Įrodysime, kad kiekvienas idealo $\mathfrak{a}$ polinomas priklauso $f(x) \cdot k[x]$, t. y. $f(x)$ dalija kiekvieną polinomą $g(x)$, priklausantį idealui $\mathfrak{a}$. Sakykime, $g(x) \in \mathfrak{a}$. Polinomams $f(x)$ ir $g(x)$ pritaikę dalybos su liekana formulę, galime parašyti: $g(x) = f(x) \cdot h(x) + r(x)$, $\deg r(x) < \deg f(x)$. Polinomas $r(x)$ priklauso idealui $\mathfrak{a}$, nes $g(x) \in \mathfrak{a}$, $f(x) \in \mathfrak{a}$, vadinasi, ir $r(x) = g(x) - f(x) \cdot h(x) \in \mathfrak{a}$. Kadangi $\deg r(x) < \deg f(x)$, tai $r(x) = 0$, nes priešingu atveju gautume prieštaravimą polinomo $f(x)$ išrinkimui, kaip mažiausio laipsnio, priklausančio idealui $\mathfrak{a}$. Iš lygybės $r(x) = 0$ gauname $g(x) = f(x) \cdot h(x)$, t. y. $g(x) \in f(x) \cdot k[x]$. Taigi $\mathfrak{a} = f(x) \cdot k[x]$. $\triangle$

Akivaizdu, kad $f(x) \cdot k[x] \subset g(x) \cdot k[x]$ tada ir tik tada, kai $g(x)|f(x)$. Vadinasi, $f(x) \cdot k[x] = g(x) \cdot k[x]$ tada ir tik tada, kai $f(x)|g(x)$ ir $g(x)|f(x)$, t. y. , kai polinomai $f(x)$ ir $g(x)$ yra ekvivalentūs.

Teiginys. Polinomų žiedo $k[x]$ idealas $f(x) \cdot k[x]$ yra maksimalus tada ir tik tada, kai $f(x)$ yra pirminis virš kūno k polinomas.

Įrodymas. Sakykime, kad idealas $f(x) \cdot k[x]$ nėra maksimalus. Tuomet egzistuoja toks idealas $g(x) \cdot k[x]$, kad $f(x) \cdot k[x] \subset g(x) \cdot k[x] \subset k[x]$, bet $f(x) \cdot k[x] \neq g(x) \cdot k[x]$, $g(x) \cdot k[x] \neq k[x]$. Iš sąlygos $f(x) \cdot k[x] \subset g(x) \cdot k[x]$ gauname, kad $g(x)|f(x)$. Iš sąlygų $f(x) \cdot k[x] \neq g(x) \cdot k[x]$, $g(x) \cdot k[x] \neq k[x]$ gauname, kad $\deg g(x) > 0$ ir $\deg g(x) < \deg f(x)$. Taigi šiuo atveju $f(x)$ nėra pirminis virš kūno k.

Tarkime, kad $f(x)$ yra pirminis polinomas virš kūno k. Jei būtų $f(x) \cdot k[x] \subset g(x) \cdot k[x]$, tai gutume $g(x)|f(x)$. Kadangi $f(x)$ yra pirminis polinomas virš kūno k, tai arba $g(x) \in k^*$ arba $f(x)$ ir $g(x)$ yra ekvivalentūs. Pirmuoju atveju idealas $g(x) \cdot k[x] = k[x]$, o antruoju – $f(x) \cdot k[x] = g(x) \cdot k[x]$. Kaip matome, jei $f(x)$ yra pirminis polinomas virš kūno k, tai idealas $f(x) \cdot k[x]$ yra maksimalus. $\triangle$

Anksčiau įrodėme, kad žiedo faktoržiedas pagal maksimalų idealą yra kūnas. Sakykime, $f(x)$ – žiedo $k[x]$ pirminis polinomas virš kūno k. Kaip žinome, $f(x) \cdot k[x]$ yra žiedo $k[x]$ maksimalus idealas. Trumpumo dėlei šį idealą pažymėkime raide $\mathfrak{f}$.

8. 2. Dabar tirsime polinomų žiedo $k[x]$ faktoržiedą $k[x]/\mathfrak{f}$ pagal maksimalų idealą $\mathfrak{f} = f(x) \cdot k[x]$.

Teorema. Tarkime, kad $f(x) \in k[x]$ pirminis polinomas virš kūno k. Polinomų žiedo $k[x]$ faktoržiedas $k[x]/\mathfrak{f}$ pagal maksimalų idealą $\mathfrak{f} = f(x) \cdot k[x]$ yra kūno k plėtinys, kuriame polinomas $f(x)$ turi šaknį.

Įrodymas. Polinomų žiedo $k[x]$ faktoržiedas $k[x]/\mathfrak{f}$ pagal maksimalų idealą $\mathfrak{f} = f(x) \cdot k[x]$ yra kūnas. Nagrinėkime faktoržiedo $k[x]/\mathfrak{f}$ elementus $\alpha + \mathfrak{f}$, $\alpha \in k$. Įsitikinsime, kad atvaizdis $F : k \to k[x]/\mathfrak{f}$, $\alpha \to \alpha + \mathfrak{f}$, $\alpha \in k$, yra injektyvus homomorfizmas. Sakykime, kad $F(\alpha) = F(\beta)$, $\alpha, \beta \in k$. Kadangi $F(\alpha) = \alpha + \mathfrak{f}$, $F(\beta) = \beta + \mathfrak{f}$, tai iš lygybės $F(\alpha) = F(\beta)$

gauname, kad $\alpha+\mathfrak{f}=\beta+\mathfrak{f}$, t. y. $\alpha-\beta\in\mathfrak{f}$. Sąlyga $\alpha-\beta\in\mathfrak{f}$ ekvivalenti sąlygai $f(x)|\alpha-\beta$. Bet $f(x)|\alpha-\beta$ tik tuo atveju, jei $\alpha-\beta=0$, nes deg $f(x)>0$, o deg $(\alpha-\beta)\leq 0$. Įrodėme, kad F – injektyvus atvaizdis.

Dabar įsitikinsime, kad F yra homomorfizmas. Bet kuriems $\alpha,\beta\in k$, gauname $F(\alpha+\beta)=\alpha+\beta+\mathfrak{f}=(\alpha+\mathfrak{f})+(\beta+\mathfrak{f})=F(\alpha)+F(\beta)$. Panašiai, bet kuriems $\alpha,\beta\in k$, gauname $F(\alpha\cdot\beta)=\alpha\cdot\beta+\mathfrak{f}=(\alpha+\mathfrak{f})\cdot(\beta+\mathfrak{f})=F(\alpha)\cdot F(\beta)$.

Kadangi $F:k\to k[x]/\mathfrak{f}$ injektyvus homomorfizmas, tai galime sutapatinti kūną k su jo vaizdu $F(k)\in k[x]/\mathfrak{f}$. Pažymėję kūną $k[x]/\mathfrak{f}$ raide K, kūną k galime nagrinėti kaip kūno K pokūnį. Taigi $f(x)\in k[x]\subset K[x]$. Pažymėkime raide θ kūno $K=k[x]/\mathfrak{f}$ (priminsime, kad $\mathfrak{f}=f(x)\cdot k[x]$) elementą $x+\mathfrak{f}$. Sakykime, kad $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+A_1x+a_0$, $a_j\in k\subset K$, $0\leq j\leq n$. Tuomet $f(\theta)=a_n\theta^n+a_{n-1}\theta^{n-1}+\ldots+A_1\theta+a_0=f(x)+\mathfrak{f}=\mathfrak{f}$. Bet $\mathfrak{f}$ yra kūno nulinis elementas. Taigi $f(\theta)=0$, t. y. θ yra polinomo $f(x)$ šaknis. $\triangle$

Pavyzdžiai.

1. Nagrinėkime $\mathbb{Q}[x]$ ir polinomą x^2-2. Šis polinomas yra pirminis virš $\mathbb{Q}$. Faktoržiedo $\mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x])$ elementai vienareikšmiškai gali būti užrašomi taip : $a+bx+(x^2-2)\cdot\mathbb{Q}[x]$. Sudauginkime šio faktoržiedo du elementus :

$$(a+bx+(x^2-2)\cdot\mathbb{Q}[x])\cdot(c+dx+(x^2-2)\cdot\mathbb{Q}[x])=ac+(ad+bc)x+bdx^2+(x^2-2)\cdot\mathbb{Q}[x]=$$

$$ac+(ad+bc)x+bd(x^2-2+2)+(x^2-2)\cdot\mathbb{Q}[x]=ac+2bd+(ad+bc)x+(x^2-2)\cdot\mathbb{Q}[x].$$

Kita vertus, aibė $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}|a,b\in\mathbb{Q}\}$ skaičių sudėties ir daugybos atžvilgiu yra kūnas. Tuo įsitikinsime. Akivaizdu, kad ši aibė yra stabili sudėties ir daugybos. Vadinasi, $(\mathbb{Q}(\sqrt{2}),+,\cdot)$ yra komutatyvus žiedas. Jei $a+b\sqrt{2}\neq 0$, tai

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{(a-b\sqrt{2})\cdot(a+b\sqrt{2})}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{-b\sqrt{2}}{a^2-2b^2}.$$

Įsitikinome, kad $(\mathbb{Q}(\sqrt{2}),+,\cdot)$ yra kūnas. Dabar įrodysime, kad $\mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x])$ yra izomorfinis kūnui $(\mathbb{Q}(\sqrt{2}),+,\cdot)$. Atvaizdis $F:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x])$, $F(a+b\sqrt{2})=a+bx+(x^2-2)\cdot\mathbb{Q}[x]$, $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, yra izomorfizmas. Akivaizdu, kad F yra bijekcija. Iš anksčiau sudaugintų kūno $\mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x])$ elementų matome, kad F išsaugo sudėties ir daugybos veiksmus.

2. Nagrinėkime $\mathbb{Q}[x]$ ir polinomą x^3-2. Polinomas x^3-2 yra pirminis virš racionaliųjų skaičių kūno $\mathbb{Q}$. Iš tikrųjų. Jei šis polinomas nebūtų pirminis virš $\mathbb{Q}$, tai jį būtų galima išskaidyti arba į trijų pirmos eilės polinomų arba į pirmos ir antros eilės polinomų su racionaliaisiais koeficientais sandaugą. Vienu ar kitu atveju šis polinomas turėtų racionalią šaknį. Bet kubinė šaknis iš dviejų nėra racionalus skaičius, o kitos šio polinomo šaknys yra kompleksinės.

Faktoržiedo $\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$ elementai vienareikšmiškai gali būti užrašomi taip: $a+bx+cx^2+(x^3-2)\cdot\mathbb{Q}[x]$. Prieš sudaugindami kūno $\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$ du elementus, sutarkime idealą $(x^3-2)\cdot\mathbb{Q}[x]$ žymėti $\mathfrak{m}$, o $\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$ – K. Sudauginkime šio kūno du elementus: $(a+bx+cx^2+\mathfrak{m})\cdot(a'+b'x+c'x^2+\mathfrak{m}) = aa'+(ab'+ba')x+(ac'+bb'+ca')x^2+(bc'+cb')x^3+cc'x^4+\mathfrak{m} = aa'+(ab'+ba')x+(ac'+bb'+ca')x^2+(bc'+cb')(x^3-2+2)+cc'(x^4-2x+2x)+\mathfrak{m} = aa'+2(bc'+cb')+(ab'+ba'+2cc')x+(ac'+bb'+ca')x^2+\mathfrak{m}$, nes $x^3-2, x^4-2x=(x^3-2)\cdot x\in\mathfrak{m}$.

Kaip ir pirmajame pavyzdyje, galite įsitikinti, kad kūnas K yra izomorfinis kūnui $\mathbb{Q}(\sqrt[3]{2})$. Atvaizdis $F:\mathbb{Q}(\sqrt[3]{2})\to K=\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$, $F(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a+bx+cx^2+\mathfrak{m}$, $a+b\sqrt[3]{2}+c\sqrt[3]{4}\in\mathbb{Q}(\sqrt[3]{2})$, yra šių kūnų izomorfizmas.

Pratimas. Pasinaudoję Euklido algoritmu, raskite elementui $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ atvirkštinį elementą.