6. ŽIEDAI IR IDEALAI

Iš sveikųjų skaičių pavyzdžio matome, kad aibėje gali būti apibrėžta ne viena operacija. Mus domins algebrinės struktūros su dviem operacijomis.

6.1 apibrėžimas. *Tegu R yra netuščia aibė, kurioje apibrėžtos dvi operacijos: $+$ (sudėtis) ir $\cdot$ (daugyba). Jei algebrinėje struktūroje $(R, +, \cdot)$ patenkintos sąlygos:*

$R1$: $(R, +)$ – komutatyvioji grupė ($G1$–$G5$ sąlygos),

$R2$: $(R, \cdot)$ – pusgrupė ($G1$–$G2$ sąlygos),

$R3$ (sandaugos distributyvumas sudėties atžvilgiu)

$$(a + b) \cdot c = a \cdot c + b \cdot c \qquad c \cdot (a + b) = c \cdot a + c \cdot b,$$

tai struktūra $(R, +, \cdot)$ vadinama žiedu.

6.2 apibrėžimas. *Tegu $(R, +, \cdot)$ yra žiedas.*

1. Jeigu $(R, \cdot)$ yra monoidas ($G1-G3$ sąlygos) ir neutralusis šio monoido elementas $1 \neq 0$, tai R vadinamas žiedu su vienetu.

2. Jeigu $(R, \cdot)$ yra komutatyvioji pusgrupė ($G1, G2, G5$ sąlygos), tai R vadinama komutatyviuoju žiedu.

3. Jeigu komutatyviajame žiede su vienetu R iš lygybės $a \cdot b = 0$, $a, b \in R$, gauname arba $a = 0$, arba $b = 0$, tai žiedas R vadinamas integralumo sritimi.

4. Jeigu $(R - \{0\}, \cdot)$ yra grupė, tai R vadinamas lauku.

5. Jeigu $(R - \{0\}, \cdot)$ yra komutatyvioji grupė, tai R vadinamas kūnu.

6. Jeigu netuščias žiedo (kūno) R poaibis S yra žiedas (kūnas) tų pačių kaip ir R operacijų atžvilgiu, tai S vadinamas požiedžiu (pokūniu).

6.3 pavyzdžiai. 1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ yra kūnai.

2. $(\mathbb{Z}, +, \cdot)$ – integralumo sritis.

3. $(\mathbb{Z}_p, +, \cdot)$, p – pirminis skaičius, – integralumo sritis: jeigu $\overline{m} \cdot \overline{n} = \overline{0}$, tai $m \cdot n \equiv 0 (mod\ p)$ ir $p \mid m \cdot n$. Tada arba $p \mid m$, arba $p \mid n$, t.y. arba $\overline{m} = \overline{0}$, arba $\overline{n} = \overline{0}$.

4. $(\mathbb{Z}_{m\cdot n}, +, \cdot)$, $m, n > 1$ – natūralieji skaičiai, – komutatyvusis žiedas su vienetu, bet ne integralumo sritis: $\overline{m} \neq \overline{0}$ ir $\overline{n} \neq 0$, bet $\overline{m} \cdot \overline{n} = \overline{0}$.

Tokie nenuliniai žiedo R elementai a, b, kuriems galioja lygybė $a \cdot b = 0$, vadinami *nulio dalikliais.*

5. $(2\mathbb{Z}, +, \cdot)$ – komutatyvusis žiedas be vieneto.

6. $\big(M_2(\mathbb{R}), +, \cdot\big)$ – nekomutatyvusis žiedas su vienetu $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ir nulio dalikliais, pavyzdžiui:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

6.4 pastabos. 1. Jeigu žiede R yra 1, tai $1 \neq 0$ ir $|R| \geqslant 2$.

2. Žiede $(R, +, \cdot)$ galioja:

$$\begin{aligned} &1 \cdot a = a \cdot 1 = a \ \ , a \in R, \\ &0 \cdot a = a \cdot 0 = 0 \ \ , a \in R, \\ &(-a) \cdot b = a \cdot (-b) = -(ab) \ \ , a, b \in R. \end{aligned}$$

3. Kiekvienas kūnas K yra integralumo sritis: jeigu $a \cdot b = 0$ ir $a \neq 0$, tai

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b,$$

t.y. $b = 0$.

4. Kiekviena baigtinė integralumo sritis K yra kūnas: jeigu $a_1, a_2, \ldots, a_n$ visi skirtingi K elementai, o $a \in K$, $a \neq 0$, tai $a(a_i - a_j) \neq 0$, $i \neq j$, nes $a \neq 0$, $a_i - a_j \neq 0$ ir K – integralumo sritis. Taigi aibėje $\{aa_1, aa_2, \ldots, aa_n\} = \{a_1, a_2, \ldots, a_n\}$ egzistuoja toks i, $1 \leqslant i \leqslant n$, kad $1 = aa_i$ ir $a_i = a^{-1}$. Taip kiekvienam nenuliniam baigtinės integralumo srities elementui galime rasti atvirkštinį.

Ši pastaba rodo, kad baigtinė integralumo sritis $(\mathbb{Z}_p, +, \cdot)$, turinti p (p – pirminis skaičius) elementų, yra kūnas. Šis kūnas žymimas $GF(p)$ ir vadinamas Galua[1] kūnu, turinčiu p elementų.

5. Vederborno[2] teorema (be įrodymo). Baigtinis laukas yra kūnas.

Pagrindinis žiedo ir kūno skirtumas yra tas, kad žiede ne kiekvienas nenulinis elementas turi atvirkštinį.

---

[1] E. Galois, 1811–1832, – prancūzų matematikas.

[2] J. H. M. Wedderburn, 1882–1948, – amerikiečių matematikas.

6.5 pavyzdžiai. 1) Sveikųjų skaičių žiede $(\mathbb{Z}, +, \cdot)$ tik du elementai 1 ir -1 turi atvirkštinius (sandaugos atžvilgiu).

2) Kvadratinių matricų žiede $(M_2(\mathbb{R}), +, \cdot)$ tik neišsigimusios matricos turi atvirkštines.

Svarbu yra ir tai, kad žiedo R elementas a, turintis atvirkštinį, tikrai nėra nulio daliklis: $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow b = 0$.

6.6 teiginys. *Visi žiedo su vienetu $(R, +, \cdot)$ elementai, turintys atvirkštinius, sudaro grupę $U(R)$ operacijos „$\cdot$" atžvilgiu.*

Įrodymas. Pakanka įrodyti G1 savybę : jeigu $a, b \in U(R)$, tai $a \cdot b \in U(R)$, nes $(a \cdot b) \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot (b^{-1}a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = 1 \in U(R)$.

△

7.1 apibrėžimas. *Žiedo $(R, +, \cdot)$ poaibis $I \subseteq$ R vadinamas idealu, jeigu patenkintos šios sąlygos:*

a) $a, b \in I \Rightarrow a - b \in I$;

b) $r \in R$, $a \in I \Rightarrow ar \in I$ ir $ra \in I$.

7.2 pastabos. 1. Žiedo R idealas I yra žiedo R požiedis, bet ne kiekvienas žiedo R požiedis S yra žiedo R idealas. Štai pavyzdžiai:

a) $\mathbb{Z}$ yra $\mathbb{Q}$ požiedis, bet ne idealas, nes

$$1 \in \mathbb{Z}, \quad \frac{1}{2} \in \mathbb{Q} \quad \text{bet} \quad 1 \cdot \frac{1}{2} \notin \mathbb{Z}.$$

b) Diagonaliųjų matricų požiedis $D_n(\mathbb{R})$ nėra idealas n-osios eilės kvadratinių matricų žiede $M_n(\mathbb{R})$.

2. Kiekviename žiede $(R, +, \cdot)$ yra bent du idealai: $S = \{0\}$ ir $S = R$. Jie vadinami trivialiaisiais.

3. Tegu duotas žiedo R su vienetu idealas I , o a yra idealo I elementas, turintis atvirkštinį. Tada $I = R$.

Tegu $a \in I$ toks, kad $a^{-1} \in R$. Tada $e = a \cdot a^{-1} \in I$ ir bet kokiam $r \in R$ $r \cdot e = r \in I$, t.y. $R = I$.

Iš šios pastabos matome, kad kūnas $(K, +, \cdot)$ gali turėti tik trivialiuosius idealus: $I = \{0\}$ ir $I = R$.

4. Žiedo R idealų sankirta $\bigcap\limits_{\alpha \in A} I_\alpha$ yra idealas:

a) jeigu $a, b \in \bigcap\limits_{\alpha \in A} I_\alpha$, tai su visais $\alpha \in A$, teisinga $a, b \in I_\alpha$ ir todėl su visais $\alpha \in A$, $a - b \in I_\alpha$, t.y. $a - b \in \bigcap\limits_{\alpha \in A} I_\alpha$;

b) jeigu $r \in R$ ir $a \in \bigcap\limits_{\alpha \in A} I_\alpha$, t.y. su visais $\alpha \in A$ $a \in I_\alpha$ ir todėl su visais $\alpha \in A$, $r \cdot a \in I_\alpha$, $ar \in I_\alpha$, t.y. $ar \in \bigcap\limits_{\alpha \in A} I_\alpha$, $ra \in \bigcap\limits_{\alpha \in A} I_\alpha$.

7.3 apibrėžimas. *1. Tegu $(R, +, \cdot)$ komutatyvusis žiedas su vienetu, o $S \subseteq$ R – netuščias poaibis. Idealų, kurių poaibis yra S, sankirta vadinama idealu, generuotu S, ir žymima (S).*

Idealas (a), $a \in R$, vadinamas pagrindiniu idealu (generuotu a) –

$$(a) = \{ra \mid r \in R\}.$$

2. Integralumo sritis R, kurios kiekvienas idealas J yra pagrindinis ir kuriai egzistuoja toks $a \in R$, kad $J = (a)$, vadinama pagrindinių idealų sritimi.

7.4 pavyzdys. Tegu $n \in \mathbb{N}$. Tada $(n) = \{n \cdot m \mid m \in \mathbb{Z}\} = n \cdot \mathbb{Z}$ yra pagrindinis idealas žiede $\mathbb{Z}$. Iš 5.43 teiginio žinome, kad bet kuris sveikųjų skaičių žiedo adicinis pogrupis yra ciklinis, t.y. generuojamas vienu elementu, todėl bet kuris žiedo $\mathbb{Z}$ idealas yra pagrindinis ir $\mathbb{Z}$ – pagrindinių idealų sritis.

Kitas mums svarbus pagrindinių idealų žiedo pavyzdys – polinomų virš kūno K žiedas $K[x]$.

7.5 apibrėžimas. *1. Tegu $(K, +, \cdot)$ yra kūnas. Polinomų su koeficientais iš K aibė*

$$K[x] = \left\{ f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \mid a_n, a_{n-1}, \ldots, a_0 \in K \right\}$$

įprastų sudėties ir sandaugos operacijų polinomams atžvilgiu sudaro žiedą, vadinamą polinomų virš K žiedu.

2. Tegu $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in K[x]$, $a_n \neq 0$. Skaičius n vadinamas polinomo $f(x)$ laipsniu, žymima $\deg f(x) = n$, o koeficientas a_n vadinamas vyriausiuoju koeficientu, žymima $l(f)$. Jeigu polinomo vyriausias koeficientas $l(f) = a_n = 0$, t.y. $f(x) = 0$, tai susitarsime laikyti $\deg f(x) = -\infty$. Polinomas $f(x)$, kurio $l(f) = a_n = 1$, vadinamas unitariuoju.

7.6 teiginys (dalybos algoritmas). *Tegu* $f(x) \in K[x]$ *ir* $g(x) \in K[x]$, $\deg g(x) > 0$. *Tada egzistuoja vieninteliai polinomai* $q(x)$ *ir* $r(x)$ *iš* $K[x]$, *tenkinantys sąlygas:*

1) $f(x) = q(x)\, g(x) + r(x)$;

2) $\deg r(x) < \deg\ g(x)$.

7.9 apibrėžimas. *Tegu* $f(x), g(x) \in K$, K *yra kūnas. Sakoma, kad polinomas* $f(x)$ *dalijasi iš polinomo* $g(x)$ ($g(x)$ *yra* $f(x)$ *daliklis), jeigu egzistuoja toks polinomas* $h(x) \in K[x]$, *kad*

$$f(x) = g(x)h(x).$$

7.10 teiginys. *1. Tegu* $f(x) \in K[x]$. *Kūno* K *elementas* a *yra polinomo* $f(x)$ *šaknis tada ir tik tada, kada* $f(x)$ *dalijasi iš* $x - a$.

2. Polinomas $0 \neq f(x) \in K[x]$ *turi ne daugiau kaip* $n = \deg\ f(x)$ *šaknų kūne* K.

7.11 teiginys. *Polinomų žiedas* $K[x]$ *virš kūno* K *yra pagrindinių idealų sritis, t.y. bet kuriam žiedo* $K[x]$ *idealui* I *egzistuoja vienintelis unitarusis polinomas* $g(x) \in K[x]$, *kad*

$$I = (g(x)).$$

Įrodymas. Žinoma, kad polinomų žiedas $K[x]$ virš kūno yra integralumo sritis.

Tegu I yra nenulinis idealas $K[x]$ ir $f(x)$ – mažiausiojo laipsnio polinomas, priklausantis I. Polinomas $g(x) = l(f)^{-1} f(x)$ taip pat priklauso idealui I. Belieka įsitikinti, kad $I = \big(g(x)\big)$.

1. Polinomas $g(x)$ yra unitarusis polinomas.

2. Jeigu $h(x)$ bet koks polinomas iš I, tai polinomų porai $h(x)$, $g(x)$ pritaikę dalybos algoritmą, gausime

$$\begin{aligned} &h(x) = q(x)g(x) + r(x), \\ &q(x),\ r(x) \in K[x], \\ &\deg\ r(x) < \deg\ g(x). \end{aligned}$$

Bet $r(x) = h(x) - q(x)g(x) \in I$, todėl

$$r(x) = 0 \quad \text{ir} \quad h(x) = q(x)g(x).$$

3. Jeigu $g_1(x)$ yra toks unitarusis polinomas, kad

$$I = \big(g(x)\big) = \big(g_1(x)\big), \quad \text{tai}$$

$$g(x) = c_1 g_1(x), \quad g_1(x) = c\, g(x), \quad c_1, c \in K[x] \quad \text{ir}$$

$$g_1(x) = c\, c_1 g_1(x), \quad \text{ir} \quad cc_1 = 1, \quad \text{t.y.} \quad c_1, c \in K.$$

Taigi

$$g_1(x) = g(x).$$

$\triangle$

7.12 teiginys. *Tegu $f_1(x), f_2(x), \ldots, f_m(x)$ yra polinomai virš kūno K. Tada egzistuoja toks vienintelis unitarusis polinomas $d(x) \in K[x]$, kad:*

1) f_i dalijasi iš d visiems i, $1 \leqslant i \leqslant m$;

2) jeigu f_i dalijasi iš g visiems i, $1 \leqslant i \leqslant m$; $g \in K[x]$, tai ir d dalijasi iš g.

Polinomas d vadinamas *didžiausiuoju bendruoju polinomų $f_1, f_2, \ldots, f_m$ dalikliu* ir žymimas $d = \text{DBD}\,(f_1, f_2, \ldots, .f_m)$. Be to,

$$d = a_1 f_1 + a_2 f_2 + \ldots + a_m f_m, \quad a_1, a_2, \ldots, a_m \in K[x]\,.$$

Įrodymas. Aibė $I = \big\{b_1 f_1 + b_2 f_2 + \ldots + b_m f_m \mid b_1, b_2, \ldots, b_m \in K[x]\big\}$ yra žiedo $K[x]$ idealas:

1) jeigu $b_{i1} f_1 + b_{i2} f_2 + \ldots + b_{im} f_m \in I$, $i = 1, 2$, tai

$$\begin{aligned}&\big(b_{11} f_1 + b_{12} f_2 + \ldots + b_{1m} f_m\big) - \big(b_{21} f_1 + b_{22} f_2 + \ldots + b_{2m} f_m\big)\\ &= \big(b_{11} - b_{21}\big) f_1 + \big(b_{12} - b_{22}\big) f_2 + \ldots + \big(b_{1m} - b_{2m}\big) f_m \in I;\end{aligned}$$

2) jeigu $b_1 f_1 + b_2 f_2 + \ldots + b_m f_m \in I$, $r \in K[x]$, tai

$$r\big(b_1 f_1 + b_2 f_2 + \ldots + b_m f_m\big) = \big(rb_1\big) f_1 + \big(rb_2\big) f_2 + \ldots + \big(rb_m\big) f_m \in I.$$

Kadangi $K[x]$ yra pagrindinių idealų sritis, todėl egzistuoja vienintelis unitarusis polinomas $d \in K[x]$, generuojantis idealą $I = (d)$, t.y. polinomas d išsiskiria teiginyje esančiomis savybėmis.

$\triangle$

7.16 apibrėžimas. *1. Jeigu* $\text{DBD}\,(f_1, f_2, \ldots, f_m) = 1$, *tai sakoma, kad polinomai $f_1, f_2, \ldots, f_m$ yra tarpusavyje pirminiai.*

2. Jeigu $(f_i, f_j) = 1$, $i \neq j$, *tai sakoma, kad polinomai* $f_1, f_2, \ldots, f_m$ *yra poromis tarpusavyje pirminiai.*

Grįžkime prie abstrakčių žiedų.

7.17 apibrėžimas. *Tegu* $(R, +, \cdot)$ *ir* $(S, \oplus, \odot)$ *yra žiedai. Funkcija* $f : R \to S$ *vadinama žiedų homomorfizmu, jeigu visiems* $a, b \in R$

$$f(a + b) = f(a) \oplus f(b),$$
$$f(a \cdot b) = f(a) \odot f(b).$$

Dar sakoma, kad žiedų homomorfizmas yra funkcija, stabili žiedinių operacijų atžvilgiu.

Bijektyvus žiedų homomorfizmas $f : R \to S$ vadinamas *žiedų izomorfizmu, o patys žiedai – izomorfiškais.*

7.18 pavyzdys. Funkcija $f : \mathbb{Z} \to \mathbb{Z}_m$, $f(n) = K_n = \overline{\mathrm{n}}$ yra žiedų homomorfizmas, bet ne izomorfizmas, nes, pavyzdžiui,

$$f(0) = f(m) = \overline{0}.$$

7.19 apibrėžimas. *Tegu* $f : R \to S$ *yra žiedų homomorfizmas. Aibė*

$$\mathrm{Ker}\, f = \{a \in R \mid f(a) = 0 \in S\}$$

vadinama homomorfizmo f *branduoliu.*

Pagrindinės homomorfizmo branduolio savybės yra:

1. Homomorfizmo branduolys yra idealas. Tegu $f : (R, +, \cdot) \to (S, \oplus, \odot)$ yra žiedų homomorfizmas, tada:

1) $(\mathrm{Ker}\, f, +) \subseteq (\mathrm{R}, +)$ – normalusis pogrupis,

2) visiems $r \in R$, $r \cdot \mathrm{Ker}\, f \subseteq \mathrm{Ker\, f}$, $\mathrm{Ker}\, f \cdot r \subseteq \mathrm{Ker\, f}$, nes, kai $a \in \mathrm{Ker\, f}$,

$$f(r \cdot a) = f(r) \odot f(a) = f(r) \odot 0 = 0,$$
$$f(a \cdot r) = f(a) \odot f(r) = 0 \odot f(r) = 0.$$

2. Tegu $(R, +, \cdot)$ yra žiedas, o I – žiedo R idealas. Aibės

$$a + I = \{a + i \mid i \in I\}$$

sudaro žiedo R skaidinį, nes

$$a + I = b + I \iff a - b \in I.$$

Naudojantis gautu skaidiniu, konstruojama faktoraibė $R/_I$, kurioje apibrėžiamos dvi operacijos:

$$(a+I) \oplus (b+I) = (a+b)+I,$$
$$(a+I) \odot (b+I) = (a \cdot b)+I.$$

Jau žinome, kad $(R/_I, \oplus)$ yra komutatyvioji grupė. Operacija $\odot$ apibrėžta korektiškai.

Tegu

$$a+I = c+I, \qquad b+I = d+I, \quad \text{t.y.}$$
$$a-c \in I, \qquad b-d \in I.$$

$$ab-cd = ab-cb+cb-cd = \underset{\in I}{(a-c)}b + c\underset{\in I}{(b-d)} \in I, \quad \text{t.y.}$$

$$(a+I) \odot (b+I) = ab+I = cd+I = (c+I) \odot (d+I)$$

Taigi $(R/_I, \oplus, \odot)$ *yra žiedas, vadinamas žiedo* R *faktoržiedžiu moduliu* I. *Tada funkcija* $f : R \to R/_I$, $f(a) = a+I$, *yra žiedų homomorfizmas, kurio branduolys* $\operatorname{Ker} f = I$.

7.20 pavyzdys. Faktoržiedis $\mathbb{Z}/_{(n)}$ yra izomorfiškas žiedui $\mathbb{Z}_n$:

$$\left(\mathbb{Z}/_{(n)}, +, \cdot\right) \approx (\mathbb{Z}_n, +, \cdot).$$