9. IDEALAI IR KŪNAI

Išsiaiškinsime, koks turėtų būti komutatyviojo žiedo R su vienetu idealas I, kad faktoržiedis $R/_I$ būtų integralumo sritis arba kūnas.

7.21 apibrėžimas. *Tegu R yra komutatyvusis žiedas su vienetu.*

1. Elementas $a \in R$ dalijasi iš $b \in R$, jeigu egzistuoja toks $c \in R$, kad $a = b \cdot c$.

Elementas b vadinamas a dalikliu (rašoma $b \mid a$).

Vieneto dalikliai žiede yra elementai, turintys atvirkštinius.

2. Elementai a ir b vadinami asocijuotais elementais, jeigu egzistuoja toks vieneto daliklis ε, kad $a = \varepsilon b$.

3. Elementas c vadinamas pirminiu žiedo R elementu jeigu, pirma, jis nėra vieneto daliklis, antra, visi elemento c dalikliai yra arba vieneto dalikliai, arba asocijuoti su c elementai (iš lygybės $c = df$ gauname, kad d ir f arba vieneto dalikliai, arba asocijuoti su c; šie dalikliai vadinami trivialiais).

7.22 išvados. 1. $a \mid a$.

2. $a \mid b, b \mid c \Rightarrow a \mid c$.

3. $a \mid b, b \mid a \iff a$ asocijuotas su b.

4. Saryšis $\{(a, b) \mid a$ asocijuotas su $b\}$ yra ekvivalentumo saryšis žiede R .

5. Vieneto dalikliai žiede $(R, +, \cdot)$ sudaro multiplikacinę grupę.

Šiuos teiginius įrodyti paliekame skaitytojui.

7.23 apibrėžimas. *1. Žiedo R idealas $P \neq R$ vadinamas pirminiu, jeigu iš $a \cdot b \in P$, $a, b \in R$ išplaukia arba $a \in P$, arba $b \in P$.*

2. Žiedo R idealas $M \neq R$ vadinamas maksimaliuoju, jeigu su visais idealais I, tenkinančiais sąlygą $M \subseteq$ I, galioja arba $I = M$, arba $I = R$.

7.24 teiginys. *Tegu R yra komutatyvusis žiedas su vienetu.*

1. Idealas M maksimalus tada ir tik tada, kai faktoržiedis $R/_M$ yra kūnas.

2. Idealas P pirminis tada ir tik tada, kai faktoržiedis $R/_P$ yra integralumo sritis.

3. Tegu R yra pagrindinių idealų sritis. Faktoržiedis $R/_{(a)}$ yra kūnas tada ir tik tada, kai a – pirminis žiedo R elementas.

Įrodymas. 1. Tegu M yra maksimalus idealas ir todėl $M \neq R$; $a + M \neq 0 + M$ – nenulinis faktoržiedžio $R/_M$ elementas, $a \notin M$. Rasime šiam elementui atvirkštinį.

Aibė $I = \{a \cdot r + m \mid r \in R, m \in M\}$ yra žiedo R idealas (patikrinkite!).

Kadangi $M \subset I$, $I \neq M$, todėl $I = R$. Taigi žiedo R vienetinį elementą galima išreikšti

$$1 = a \cdot r + m, \quad r \in R, \ m \in M.$$

Tada $(a + M) \cdot (r + M) = ar + M = (1 - m) + M = 1 + M$ ir $r + M$ yra elemento $a + M$ atvirkštinis.

Tegu $R/_M$ yra kūnas ir I toks žiedo idealas, kad $M \subset I$, $I \neq M$. Jei $a \in I$, $a \notin M$, tai $a + M$ – nenulinis kūno $R/_M$ elementas, todėl jis turi atvirkštinį $r + M : (a + M)(r + M) = 1 + M$, $ar + M = 1 + M$. Kadangi $1 = \underset{\in I}{ar} + \underset{\in I}{m} \in I$, todėl $I = R$. Taigi M yra maksimalus idealas.

2. Jeigu P yra pirminis idealas, tai $R/_P$ – komutatyvusis žiedas su vienetu: $1 \notin P$ ir $1 + P \neq 0 + P$.

$$(a + P)(b + P) = 0 + P \iff ab + P = 0 + P \iff ab \in P \iff \text{arba}$$

$$a \in P, \text{ arba } b \in P \iff \text{arba } a + P = 0 + P, \text{ arba } b + P = 0 + P.$$

Taigi R neturi nulio daliklių ir todėl yra integralumo sritis.

3. Tegu $a \in R$. 1) Jeigu a yra elementas, turintis atvirkštinį, tai $(a) = (1) = R$. Tada $R/_{(a)} = \{R\}$ – aibė iš vieno elemento – negali būti kūnu.

2) Jeigu a yra elementas, neturintis atvirkštinio, bet ir ne pirminis, tai a turi netrivialų daliklį b $(a = b \cdot c, c \in R)$, išsiskiriantį savybėmis:

(i) $b \neq 0$ (jeigu $b = 0$, tai $a = b = 0$ ir a būtų asocijuotas su b);

(ii) $b \notin (a)$ (jeigu $b \in (a) \Rightarrow b = a \cdot r = b \cdot c \cdot r, r \in R \Rightarrow b(1 - cr) = 0, b \neq 0 \Rightarrow 1 = cr (R - \text{integralumo sritis}) \Rightarrow c - \text{elementas, turintis atvirkštinį} \Rightarrow a - \text{asocijuotas su } b \Rightarrow$ prieštara).

Taigi $(a) \subset (b) \subset R$, $(b) \neq (a)$, $(b) \neq R$, todėl (a) nėra maksimalus idealas ir $R/_{(a)}$ nėra kūnas.

3) a yra pirminis ir todėl $(a) \neq (1) = R$.

Tegu I yra toks žiedo R idealas, kad $I \supset (a)$. Bet R – pagrindinių idealų sritis, todėl $I = (b)$, $b \in R$ ir $(b) \supset (a)$, t.y. $a \in (b)$ ir $a = b \cdot r$, $r \in R$. a yra pirminis elementas, todėl b yra trivialus a daliklis: jeigu b – elementas, turintis atvirkštinį, tai $(b) = (1) = R$; jeigu b yra asocijuotas su elementu a, tai $(b) = (a)$. Taigi (a) yra maksimalus žiedo R idealas ir todėl $R/_{(a)}$ – kūnas.

$\triangle$

7.25 pavyzdys. Sveikųjų skaičių žiedas $\mathbb{Z}$ yra pagrindinių idealų sritis. Vieneto dalikliai žiede $\mathbb{Z}$ – tai ± 1, o pirminiai skaičiai – tai pirminiai žiedo $\mathbb{Z}$ elementai. Todėl faktoržiedis $\mathbb{Z}/_{(n)}$ yra kūnas tada ir tik tada, kai $n = p$ – pirminis skaičius; $\mathbb{Z}/_{(p)} = GF(p)$.

7.26 pavyzdys. Tegu K yra kūnas ir $K[x]$ – polinomų žiedas virš kūno K. Vieneto dalikliai polinomų žiede $K[x]$ – tai visi nenuliniai kūno K elementai. Kitų vieneto daliklių nėra, nes iš $f_1 \cdot f_2 = 1$, $f_1, f_2 \in K[x]$, gautume $\deg f_1 + \deg f_2 = 0$ ir $\deg f_1 = \deg f_2 = 0$.

Polinomai f ir g yra asocijuoti tik tada, kai $f = c \cdot g$ su kuriuo nors kūno K elementu c.

Pirminiai žiedo $K[x]$ elementai vadinami neredukuojamais polinomais. Neredukuojami polinomai polinomų žiedo dalumo teorijoje vaidina tą patį vaidmenį kaip ir pirminiai skaičiai sveikųjų skaičių dalumo teorijoje.

Kiekvienas teigiamo laipsnio polinomas $f(x) \in K[x]$ virš kūno K gali būti vienareikšmiškai išreikštas sandauga

$$f = a\, p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n};$$

čia: $a \in K$, $p_1, p_2, \dots, p_n$ – skirtingi unitarieji neredukuojami polinomai; $\alpha_1, \alpha_2, \dots, \alpha_n$ – natūralieji laipsnio rodikliai. Neredukuojamų polinomų pavyzdžiai:

1) $x^2 + 2$ neredukuojamas virš $\mathbb{R}$, bet redukuojamas virš $\mathbb{C}$: $x^2 + 2 = \left(x + i\sqrt{2}\right)\left(x - i\sqrt{2}\right)$;

2) $x^2 - 2$ neredukuojamas virš $\mathbb{Q}$, bet redukuojamas virš $\mathbb{R}$: $x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$.

Neredukuojamų polinomų paieška – vienas iš pagrindinių klausimų, susijusių su polinomų žiedu $K[x]$. Žinome, kad polinomų žiedas $K[x]$ yra pagrindinių idealų sritis. Todėl 7.24 teiginio 3 dalis polinomams skamba taip:

Tegu $f(x) \in K[x]$. Faktoržiedis $K[x]/_{(f(x))}$ yra kūnas tada ir tik tada, kai f – neredukuojamas virš kūno K polinomas.

Ištirsime faktoržiedžio $K[x]/_{(f(x))}$ struktūrą.

Tegu $f(x)$ polinomas virš kūno K, $0 \leqslant n = \deg\ f(x)$. Faktoržiedis

$$K[x]/_{(f(x))} = \{g(x) + (f(x)) \mid g(x) \in K[x]\}.$$

Tegu $\deg\ g(x) \geqslant n$. Pritaikę dalumo algoritmą polinomų porai $g(x)$ ir $f(x)$, gausime $g(x) = q(x)\, f(x) + r(x)$, $\deg\ r(x) < \deg\ f(x) = n$.

$$g(x) + \big(f(x)\big) = \underset{\in \big(f(x)\big)}{q(x)f(x)} + r(x) + \big(f(x)\big) = r(x) + \big(f(x)\big)$$

ir

$$K[x]/_{(f(x))} = \big\{r(x) + \big(f(x)\big) \mid r(x) \in K[x],\ \deg\ r(x) < n\big\}.$$

Aibę $r(x) + \big(f(x)\big)$ žymėsime $\big[r(x)\big]_{f(x)}$, arba tiesiog $\big[r(x)\big]$.

Jeigu $\deg\ f(x) = 0$, tai polinomas f yra vieneto daliklis $\big(f(x) = a \in K\big)$ ir todėl

$$K[x]/_{(f(x))} = K[x]/_{K[x]} = \{\, K[x]\,\} = \{[0]\}.$$

Tegu $\deg\ f(x) \geqslant 1$. Į kūną K galima žiūrėti kaip į žiedo $K[x]/_{(f(x))}$ pokūnį: $K \subset K[x]/_{(f(x))}$, kuriame, jei $a, b \in K$, tai

$$[a]_{f(x)} = [b]_{f(x)} \iff a - b \quad \text{dalijasi iš} \quad f(x) \iff a - b = 0 \iff a = b.$$

Taigi funkcija $f : K \to K[x]/_{(f(x))}$, $f(a) = [a]$, yra injekcija.

Tegu $[x]_{f(x)} = \alpha$. Bet kurį elementą iš $K[x]/_{(f(x))}$ galima užrašyti

$$\begin{aligned}
&\big[a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0\big] \\
&= \big[a_{n-1}\big]\big[x^{n-1}\big] + \big[a_{n-2}\big]\big[x^{n-2}\big] + \ldots + \big[a_1\big][x] + \big[a_0\big] \\
&= a_{n-1}[x]^{n-1} + a_{n-2}[x]^{n-2} + \ldots + a_1[x] + a_0 \\
&= a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_1\alpha + a_0\,.
\end{aligned}$$

Taigi faktoržiedžio $K[x]/_{(f(x))}$ elementai yra K-tiesinės elementų $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ kombinacijos ir todėl šiuos elementus patogu įsivaizduoti kaip

polinomų iš $K[x]$ reikšmes $\alpha = [x]_{f(x)}$ (kai $f(\alpha) = 0$, nes $f(\alpha) = \big[f(x)\big]_{f(x)} = [0]_{f(x)}$).

7.27 pavyzdys. 1. Tegu K yra kūnas, o $f(x) = ax + b$, $a, b \in K$, $a \neq 0$. Elementas $x = -ba^{-1}$ yra polinomo f šaknis, todėl

$$K[x]\big/_{(ax+b)} = \big\{c + a_1x + \ldots + a_nx^n \mid ax + b = 0\big\}$$
$$= \big\{c + a_1(-ba^{-1}) + \ldots + a_n(-ba^{-1})^n \mid c, a_1, \ldots, a_n \in K,\ n \in N\big\} \approx K.$$

2. Tegu $K = \mathbb{Z}$ yra sveikųjų skaičių žiedas, o $f(x) = 10x - 1$. Faktoržiedis

$$\begin{aligned}\mathbb{Z}[x]\big/_{(10x-1)} &= \big\{a_0 + a_1x + \ldots + a_nx^n \mid 10x - 1 = 0\big\}\\ &= \big\{a_0 + a_1x + \ldots + a_nx^n \mid 10x = 1\big\}\\ &= \big\{a_0 + a_1x + \ldots + a_nx^n \mid 0 \leqslant a_i < 10,\\ &\quad 1 \leqslant i \leqslant n, a_0 \in \mathbb{Z}, n \in \mathbb{N}, x =,, \frac{1}{10}\text{“}\big\}\\ &\approx \Big\{a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} \mid 0 \leqslant a_i < 10,\\ &\quad a_0 \in \mathbb{Z}, n \in \mathbb{N}\Big\}\end{aligned}$$

– baigtinių dešimtainių trupmenų žiedas. Pastebėsime, kad šiuo atveju $\mathbb{Z}[x]\big/_{(10x-1)}$ nėra izomorfiškas $\mathbb{Z}$.

7.28 pavyzdys. Polinomas $f(x) = x^2 + 1$ yra neredukuojamas polinomas virš $\mathbb{R}$. Žinome, kad

$$\mathbb{R}[x]\big/_{(x^2+1)} = \big\{a + b[x]_{(x^2+1)} \mid a, b \in \mathbb{R}\big\}.$$

Pažymėkime $[x]_{(x^2+1)} = i$. Tada

$$\begin{aligned}i^2 = [x]^2_{(x^2+1)} &= [x^2]_{(x^2+1)} = \big[x^2 + 1 - 1\big]_{(x^2+1)}\\ &= \big[x^2 + 1\big]_{(x^2+1)} - [1]_{(x^2+1)} = -1.\end{aligned}$$

Veiksmai šiame kūne turi šias savybes:

1) $(a + ib) + (c + id) = (a + c) + i(b + d)$.

2) $(a + ib) \cdot (c + id) = ac + i(ad + bc) + i^2bd = (ac - bd) + i(ad + bc)$.

3) Jeigu $a+ib \neq 0$, tai

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

Kūnas $\mathbb{R}[x]/(x^2+1)$ izomorfiškas kompleksinių skaičių kūnui: izomorfizmas

$$iz : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}, \quad iz\big(a+b[x]_{(x^2+1)}\big) = a+ib, \quad a,b \in \mathbb{R}.$$

Pastebėsime, jei kūnas K yra baigtinis, o m – jo elementų skaičius, tai elementų skaičius faktoržiedyje $K[x]/(f(x))$ yra lygus m^n; čia $n = \deg\, f$.

7.29 pavyzdžiai. 1. Tegu $K = GF(2)$, o $f(x) = x+1$. Elementų skaičius faktoržiedyje $GF(2)[x]/(x+1)$ yra $2^1 = 2$: $GF(2)[x]/(x+1) = \{[0],[1]\} \approx GF(2)$.

2. Tegu $K = GF(3)$, o $f(x) = x^2+1$.

Elementų skaičius faktoržiede $GF(3)[x]/(x^2+1)$ yra $3^2 = 9$ ir

$GF(3)[x]/(x^2+1) = \{[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2]\} = \{[ab] \mid [ab] = [ax+b], a,b = 0,1,2\}$.

Veiksmų lentelės komutatyviame faktoržiedyje $GF(3)[x]/(x^2+1)$ yra

$+$	[00]	[01]	[02]	[10]	[11]	[12]	[20]	[21]	[22]
[00]	[00]	[01]	[02]	[10]	[11]	[12]	[20]	[21]	[22]
[01]	[01]	[02]	[00]	[11]	[12]	[10]	[21]	[22]	[20]
[02]	[02]	[00]	[01]	[12]	[10]	[11]	[22]	[20]	[21]
[10]	[10]	[11]	[12]	[20]	[21]	[22]	[00]	[01]	[02]
[11]	[11]	[12]	[10]	[21]	[22]	[20]	[01]	[02]	[00]
[12]	[12]	[10]	[11]	[22]	[20]	[21]	[02]	[00]	[01]
[20]	[20]	[21]	[22]	[00]	[01]	[02]	[10]	[11]	[12]
[21]	[21]	[22]	[20]	[01]	[02]	[00]	[11]	[12]	[10]
[22]	[22]	[20]	[21]	[02]	[00]	[01]	[12]	[10]	[11]

$\cdot$	[00]	[01]	[02]	[10]	[11]	[12]	[20]	[21]	[22]
[00]	[00]	[00]	[00]	[00]	[00]	[00]	[00]	[00]	[00]
[01]	[00]	[01]	[02]	[10]	[11]	[12]	[20]	[21]	[22]
[02]	[00]	[02]	[01]	[20]	[22]	[21]	[10]	[12]	[11]
[10]	[00]	[10]	[20]	[02]	[12]	[22]	[01]	[11]	[21]
[11]	[00]	[11]	[22]	[12]	[20]	[01]	[21]	[02]	[10]
[12]	[00]	[12]	[21]	[22]	[01]	[10]	[11]	[20]	[02]
[20]	[00]	[20]	[10]	[01]	[21]	[11]	[02]	[22]	[12]
[21]	[00]	[21]	[12]	[11]	[02]	[20]	[22]	[10]	[01]
[22]	[00]	[22]	[11]	[21]	[10]	[02]	[12]	[01]	[20]

Iš daugybos lentelės matome, kad faktoržiedyje $GF(3)[x]/(x^2+1)$ nėra nulio daliklių, todėl baigtinė integralumo sritis $GF(3)[x]/(x^2+1)$ yra kūnas ir polinomas $f(x) = x^2 + 1$ neredukuojamas virš $GF(3)$.

3. Tegu $K = GF(2)$, o $f(x) = x^2 + 1$.

Elementų skaičius faktoržiedyje $GF(2)[x]/(x^2+1)$ yra $2^2 = 4$ ir

$GF(2)[x]/(x^2+1) = \{[0], [1], [x], [x+1]\}$.

Veiksmų lentelės šiame žiede yra

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[1]$	$[x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x+1]$	$[0]$

Matome, kad faktoržiedis $GF(2)[x]/(x^2+1)$ nėra kūnas, nes jame yra nulio daliklis $[x+1][x+1]=[0]$. Taigi polinomas x^2+1 nėra neredukuojamas. Iš tikrųjų $x^2+1=(x+1)^2$ virš $GF(2)$.

Daugybos lentelė faktoržiedyje $K[x]/(f(x))$, čia K – baigtinis kūnas, leidžia spręsti, redukuojamas ar neredukuojamas polinomas $f(x)$. Tiesa, šis būdas nėra patogiausias.

7.30 apibrėžimas. *Tegu K yra kūnas, o $f(x)\in K[x]$. Kūno elementas $a\in K$ vadinamas polinomo $f(x)$ šaknimi, jeigu $f(a)=0$.*

Polinomo $f(x)$ šaknies a kartotinumu vadinsime tokį natūralųjį skaičių k, kad $f(x)$ dalijasi iš $(x-a)^k$, bet nesidalija iš $(x-a)^{k+1}$.

Pagrindinės polinomo šaknų savybės:

1. $a\in K$ yra polinomo $f(x)\in K[x]$ šaknis tada ir tik tada, kai $f(x)$ dalijasi iš $x-a$.

2. Tegu $a_1,a_2,\ldots,a_m\in K$ – skirtingos polinomo $f(x)\in K[x]$ šaknys, kurių kartotinumai atitinkamai lygūs $k_1,k_2,\ldots,k_m$. Tada $f(x)$ dalijasi iš $(x-a_1)^{k_1}(x-a_2)^{k_2}\ldots(x-a_m)^{k_m}$ ir todėl $k_1+k_2+\ldots+k_m\leqslant \deg f(x)$.

3. Polinomo $f(x)\in K[x]$ šaknis a yra kartotinė tada ir tik tada, kai a yra taip pat polinomo $f(x)$ išvestinės $f'(x)$ šaknis.

7.31 teiginys. *Tegu K yra kūnas, o $f(x)\in K[x]$.*

1. Pirmojo laipsnio polinomai neredukuojami virš K ir turi po vieną paprastąją šaknį.

2. Tegu deg $f(x) = 2$ *arba* 3; $f(x)$ *neredukuojamas virš* K *tada ir tik tada, kai* $f(x)$ *neturi šaknų kūne* K.

3. Tegu deg $f(x) \geqslant 4$. *Ne visada polinomas* $f(x)$, *neturintis šaknų virš* K, *yra neredukuojamas.*

Įrodymas. 1 yra apibrėžimų išvada.

2. Neredukuojamas polinomas $f(x)$ neturi šaknų kūne K (žr. 7.30 1 savybę).

Jeigu $f(x)$ neturi šaknų, o $f(x)$ redukuojamas virš K, tai $f(x) = g(x)h(x)$; čia $\min\big(\deg\, g(x), \deg\, h(x)\big) = 1$. Tegu deg $g(x) = 1$. Tada $g(x) = ax + b$, $a, b \in K$, $a \neq 0$ ir $g(x)$ šaknis yra elementas $-ba^{-1}$. Šis elementas yra ir $f(x)$ šaknis. Prieštara įrodo teiginį.

3. Tegu $K = GF(2)$, polinomas $f(x) = (x^2 + x + 1)(x^2 + x + 1)$ neturi šaknų kūne $GF(2)$, bet yra redukuojamas.

$\triangle$

7.32 pavyzdys. Pasinaudoję 7.31 teiginio 1 ir 2 dalimis, nesunkiai sudarysime pirmojo, antrojo ir trečiojo laipsnio neredukuojamų polinomų virš kūnų iš 2 ir 3 elementų lenteles:

$$f(x) = ax^3 + bx^2 + cx + d$$

$GF(2)$

a	b	c	d
0	0	1	0
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	1

a	b	c	d
0	0	1	0
0	0	1	1
0	0	1	2
0	1	0	1
0	1	1	2
0	1	2	2

$GF(3)$

a	b	c	d
1	0	2	1
1	0	2	2
1	1	0	2
1	1	1	2
1	1	2	1
1	2	0	1
1	2	1	1
1	2	2	1