11. IDEALAI, FAKTORŽIEDŽIAI, ALGEBRINIAI PLĖTINIAI

Komutatyviojo žiedo A adicinis pogrupis I vadinamas to žiedo idealu, kai $AI \subset I$.

Sakome, kad žiedo A elementas α lygsta to žiedo elementui β moduliu I, ir rašome $\alpha \equiv \beta \bmod I$, kai $\alpha - \beta \in I$. Tai yra ekvivalentumo ryšys. Juo remiantis faktoraibėje $A/_I$ galima apibrėžti žiedą, kuris vadinamas žiedo A faktoržiedžiu pagal idealą I.

Sakome, kad komutatyviojo žiedo A idealas I yra generuotas baigtinio skaičiaus elementų $\alpha_1, \alpha_2, \ldots, \alpha_m$ ir rašome $I = (\alpha_1, \alpha_2, \ldots, \alpha_m)$, kai:

1) bet kuris idealo elementas α yra tų elementų tiesinė kombinacija –

$$\alpha = \sum_{i=1}^{m} a_i \alpha_i \quad (a_i \in A,\ i = \overline{1, m}\,);$$

2) bet kuri tiesinė kombinacija

$$\sum_{i=1}^{m} a_i \alpha_i \quad (a_i \in A,\ i = \overline{1, m}\,)$$

priklauso idealui I.

Kai $m = 1$, idealas I vadinamas *vyriausiuoju*.

Idealas I vadinamas *pirminiu*, kai iš sąlygos $\alpha\beta \in I$ išplaukia – arba $\alpha \in I$, arba $\beta \in I$.

1 teorema. *Žiedo A idealas I yra pirminis tada ir tik tada, kai faktoržiedis $A/_I$ yra be nulio daliklių.*

Žiedo A idealas I yra vadinamas *maksimaliuoju*, kai jis nepriklauso jokiam kitam to žiedo idealui, išskyrus patį žiedą.

2 teorema. *Žiedo A idealas I yra maksimalus tada ir tik tada, kai faktoržiedis $A/_I$ yra kūnas.*

Žiedo A homomorfizmu žiede A' vadinamas atvaizdis $\varphi : A \to A'$, stabilus žiedo A veiksmų atžvilgiu.

3 teorema. 1. Jei φ yra žiedo A homomorfizmas žiede A', tai šio homomorfizmo branduolys $\operatorname{Ker}\varphi$ yra žiedo A idealas ir faktoržiedis $A/_{\operatorname{Ker}\varphi}$ izomorfiškas vaizdui $\varphi(A)$.

2. Jei I yra žiedo A idealas, tai egzistuoja žiedo A homomorfizmas φ faktoržiede $A/_I$, kurio branduolys $\operatorname{Ker}\varphi$ sutampa su idealu I.

Jei kūnas K yra kūno L pokūnis, tai kūnas L vadinamas K kūno plėtiniu.

Kūno K plėtinys L yra vektorinė erdvė virš kūno K.

Plėtinys L/K vadinamas baigtiniu, kai ši vektorinė erdvė yra baigtinės dimensijos. Plėtinio L/K laipsniu vadinama vektorinės erdvės dimensija $\dim_K L$ ir žymima $[L : K]$.

Plėtinio L elementas α vadinamas algebriniu virš kūno K, kai galima rasti nenulinį polinomą $f(t)$ su koeficientais iš kūno K, kurio šaknimi jis yra – $f(\alpha) = 0$. Priešingu atveju elementas α vadinamas transcendentiniu virš to kūno.

Plėtinys L/K vadinamas *algebriniu*, kai visi plėtinio elementai yra algebriniai virš kūno K.

4 teorema. *Kūno baigtinis plėtinys yra algebrinis.*

Algebriniai virš racionaliųjų skaičių kūno Q elementai vadinami *algebriniais skaičiais.*

Algebrinio virš kūno K elemento α minimaliuoju polinomu vadinamas žiedo $K[t]$ normuotasis žemiausio laipsnio polinomas, kurio šaknis yra α.

Tarkime, α yra algebrinis elementas virš kūno K, ir $\varphi_\alpha(t)$ – jo minimalusis m-ojo laipsnio polinomas. Aibė

$$K(\alpha) = \Big\{ \sum_{i=0}^{m-1} a_i \alpha^i \mid a_i \in K,\ i = \overline{0, m-1} \Big\}$$

yra kūno K m-ojo laipsnio plėtinys. Jis vadinamas elemento α generuotu plėtiniu.

PAVYZDŽIAI

1. Įrodysime, kad polinomų žiedo su sveikaisiais koeficientais $Z[t]$ vyriausiasis idealas (t) yra pirminis, bet ne maksimalus.

Sudarysime žiedo $Z[t]$ faktoržiedį pagal idealą (t). Du to žiedo polinomai

$$f(t) = a_n t^n + a_{n-1} t^n + \ldots + a_1 t + a_0$$

ir

$$g(t) = b_m t^n + b_{m-1} t^{m-1} + \ldots + b_1 t + b_0$$

priklauso vienam sluoksniui, kai $f(t) - g(t) \in (t)$, t.y. kai polinomų $f(t)$ ir $g(t)$ skirtumas dalosi iš polinomo t. Todėl šių polinomų laisvieji nariai a_0 ir b_0 turi būti lygūs. Priešingai – jei polinomų $f(t)$ ir $g(t)$ laisvieji nariai yra lygūs, tai jie priklauso vienam sluoksniui, nes jų skirtumas dalosi iš polinomo t. Polinomai su skirtingais laisvaisiais nariais priklauso skirtingiems sluoksniams, nes jų skirtumas nesidalo iš polinomo t. Vadinasi, tarp sluoksnių aibės ir polinomų laisvųjų narių aibės yra bijekcinis ryšys ir todėl faktoržiedis $Z[t]/_{(t)} = \{a + (t) \mid a \in Z\}$.

Apibrėžiame faktoržiedžio $Z[t]/_{(t)}$ atvaizdį φ į sveikųjų skaičių žiedą Z tokiu būdu:

$$\varphi(a + (t)) = a \quad \big(\forall a + (t) \in Z[t]/_{(t)}\big).$$

Nesunku įsitikinti, kad atvaizdis φ yra žiedų $Z[t]/_{(t)}$ ir Z izomorfizmas. Kadangi sveikųjų skaičių Z žiedas yra be nulio daliklių, tai idealas (t) yra pirminis. Bet žiedas Z nėra kūnas, todėl idealas (t) nėra maksimalus.

2. Rasime plėtinio $Q(\sqrt{5}, \sqrt{7})/Q$ laipsnį.

Kūną $Q(\sqrt{5}, \sqrt{7})$ gauname, prijungę prie racionaliųjų skaičių kūno Q algebrinį skaičių $\sqrt{5}$, o prie gautojo kūno – algebrinį skaičių $\sqrt{7}$. Turime plėtinių seką

$$Q \subset Q(\sqrt{5}) \subset Q(\sqrt{5}, \sqrt{7}).$$

Apskaičiuosime plėtinio $Q(\sqrt{5})/Q$ laipsnį. Algebrinio skaičiaus $\sqrt{5}$ minimalusis polinomas yra $\varphi_{\sqrt{5}}(t) = t^2 - 5$, nes polinomas $t^2 - 5$ yra normuotas ir neskaidus virš racionaliųjų skaičių kūno. Vadinasi,

$$[Q(\sqrt{5}) : Q] = \deg \varphi_{\sqrt{5}}(t) = 2.$$

Analogiškai skaičiuojame plėtinio $Q(\sqrt{5}, \sqrt{7})/Q(\sqrt{5})$ laipsnį. Algebrinio skaičiaus $\sqrt{7}$ minimalusis polinomas yra $\varphi_{\sqrt{7}}(t) = t^2 - 7$, nes jis yra normuotas ir neskaidus virš kūno $Q(\sqrt{5})$. Taigi

$$[Q(\sqrt{5}, \sqrt{7}) : Q(\sqrt{5})] = \deg \varphi_{\sqrt{7}}(t) = 2.$$

Iš baigtinių plėtinių sekos laipsnių formulės išplaukia lygybė

$$[Q(\sqrt{5}, \sqrt{7}) : Q] = [Q(\sqrt{5}, \sqrt{7}) : Q(\sqrt{5})][Q(\sqrt{5}) : Q] = 2 \cdot 2 = 4.$$

UŽDAVINIAI

11.1 Ar sudaro idealą:
1) aibė visų skaičiaus 12 kartotinių $12Z = \{12n \mid n \in Z\}$ sveikųjų skaičių žiede Z;
2) natūraliųjų skaičių aibė N sveikųjų skaičių žiede Z;
3) aibė sveikųjų skaičių $I = \{5x + 8y \mid x, y \in Z\}$ sveikųjų skaičių žiede Z;
4) aibė $I = \{ai \mid a \in Z\}$ sveikųjų Gauso skaičių žiede $Z[i] = \{a + bi \mid a, b \in Z\}$;
5) aibė $(1 + 2i) = \{(1 + 2i)\alpha \mid \alpha \in Z[i]\}$ sveikųjų Gauso skaičių žiede $Z[i]$;
6) aibė polinomų $(x) = \{xf(x, y) \mid f(x, y) \in Z[x, y]\}$ polinomų žiede $Z[x, y]$;
7) aibė polinomų $I = \{f(t) \mid f(0) = 0,\ f(t) \in Z[t]\}$ polinomų žiede $Z[t]$;
8) aibė polinomų $(x, y) = \{xf(x, y) + yg(x, y) \mid f(x, y), g(x, y) \in\in Q[x, y]\}$ polinomų žiede $Q[x, y]$?

11.2. Kurie iš aukščiau pateikto uždavinio idealų yra pirminiai, kurie – maksimalūs?

11.3. Sudarykite faktoržiedį:
1) žiedo Z pagal idealą $6Z$;
2) žiedo $3Z$ pagal idealą $18Z$;
3) žiedo $Z[i]$ pagal idealą (5);
4) žiedo $Z[i]$ pagal idealą $(i + 3i)$;
5) žiedo $Z[t]$ pagal idealą (t^2);
6) žiedo $Q[t]$ pagal idealą (t);
7) žiedo $K[x, y]$ pagal idealą (x);
8) žiedo $Z/_{8Z}$ pagal idealą $I = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.

11.4. Kurie iš šių atvaizdžių yra žiedų homomorfizmai:
1) $\varphi : Z \to Z$, $\varphi(n) = 2n \quad (\forall n \in Z)$;
2) $\varphi : Q[t] \to Q[t]$, $\varphi\big(f(t)\big) = tf(t) \quad (\forall f(t) \in Q[t])$;
3) $\varphi : R[t] \to R[t]$, $\varphi\big(f(t)\big) = f(e^t \cdot t) \quad (\forall f(t) \in R[t])$;
4) $\varphi : R[t] \to R$, $\varphi\big(f(t)\big) = f(0) \quad (\forall f(t) \in R[t])$?

11.5. Kokį idealą sveikųjų skaičių žiede Z generuoja skaičių pora 6 ir 8?

11.6. Įrodykite, kad komutatyviojo žiedo idealų sankirta yra to žiedo idealas.

11.7. Įrodykite, kad bet kuris sveikųjų skaičių žiedo idealas yra vyriausias.

11.8. Įrodykite, kad nenulinis pirminis sveikųjų skaičių žiedo idealas yra maksimalus.

11.9. Žiedo A idealų I_1 ir I_2 suma yra vadinama aibė

$$I_1 + I_2 = \{\alpha_1 + \alpha_2 \,|\, \alpha_1 \in I_1,\, \alpha_2 \in I_2\},$$

o sandauga – aibė

$$I_1 I_2 = \Big\{ \sum_{i=1}^{s} \alpha_i \beta_i \,|\, s \in N, \alpha_i \in I_1, \beta_i \in I_2 \Big\}.$$

Įrodykite, kad idealų suma ir sandauga yra to žiedo idealai.

11.10. Sakome, kad idealas I_1 dalijasi iš idealo I_2, kai $I_1 \subset I_2$. Įrodykite, kad idealų I_1 ir I_2 didžiausias bendrasis daliklis lygus tų idealų sumai $I_1 + I_2$.

11.11. Raskite šių algebrinių skaičių minimaliuosius polinomus:

1) $\sqrt[3]{2}$; 2) $\sqrt[3]{9} + \sqrt[3]{3} + 1$;

3) $\sqrt[3]{3} - 1$; 4) $\sqrt[3]{4} + \sqrt[3]{2}$.

11.12. Raskite šių plėtinių laipsnius:

1) $Q(\sqrt[4]{3})/Q$; 2) $Q(\eta)/Q$ kai $\eta^2 + \eta + 1 = 0$;

3) $Q(\sqrt{2}, \sqrt{3}, \sqrt{4})/Q$; 4) $Q(\sqrt[3]{2}, \eta)/Q$, kai $\eta^2 + \eta + 1 = 0$;

5) $Q(\sqrt{2}, i, \sqrt{-2})/Q$; 6) $Q(\sqrt{2}, \sqrt{3}, \sqrt{5})/Q$.

ATSAKYMAI

11.1. 1) Taip; 2) ne; 3) taip; 4) ne;
5) taip; 6) taip; 7) taip; 8) taip.

11.2. Pirminiai – 5), 6), 7), 8); maksimalūs – 5), 8).

11.3.

1) $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$; 2) $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}\}$;

3) $\big\{\overline{a + bi} \,|\, a, b = \overline{0,4}\,\big\}$; 4) $\big\{\bar{a} \,|\, a = \overline{0,9}\,\big\}$;

5) $\big\{\overline{at + b} \,|\, a, b \in Z\big\}$; 6) Q;

7) $K[y]$; 8) $\{\tilde{0}, \tilde{1}\}$.

11.4. 1) Ne; 2) ne; 3) taip; 4) taip.

11.5. (2).

11.11.

1) $t^3 - 2$; 2) $t^3 - 3t^2 - 6t - 4$;

3) $t^3 + 3t^2 + 3t - 2$; 4) $t^3 - 6t + 6$.

11.12. 1) 4; 2) 2; 3) 4; 4) 6; 5) 4; 6) 8.

Literatūra

1. Maknys M. *Algebros užduotys ir rekomendacijos*. – V.: VU, 1988. – 112 p.
2. Matuliauskas A. *Algebra*. – V.: Mokslas, 1985. – 382 p.
3. Bulota K., Survila P. *Algebra ir skaičių teorija*. – V.: Mokslas, 1976, – T. 1 – 480 p.; 1977. – T. 2 – 416 p.
4. Кострикин А. И. *Введение в алгебру*. – М.: Наука, 1977. – 496 с.
5. Проскуряков И. В. *Сборник задач по линейной алгебре*. – М.: Наука, 1974. – 384 с.
6. Фадеев Д. К., Соминский И. С. *Сборник задач по высшей алгебре*. – М.: Наука, 1977. – 298 с.