Algebros paskaitos

Rimantas Grigutis

5 paskaita.
Dalumas su liekana.
BDD. Tarpusavyje pirminiai polinomai.
Neredukuojami polinomai.

Nors polinomų žiedas $\mathbf{K}[x]$ ir yra kūno $\mathbf{K}$ plėtinys: $\mathbf{K}[x] \supset \mathbf{K}$, bet savo savybėmis yra panašus į sveikųjų skaičių žiedą $\mathbf{Z}$. Kaip ir sveikųjų skaičių žiede, taip ir polinomų virš kūno žiede yra teisinga dalumo su liekana teorema.

5.1 **Teorema(dalumas su liekana).** *Tegu* $f(x)$, $g(x) \in \mathbf{K}[x]$ ir $g(x) \neq 0$. *Egzistuoja vienintėliai polinomai* $q(x)$ *ir* $r(x)$ *su kuriais teisinga lygybė*

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

čia $\deg r(x) < \deg g(x)$.

Įrodymas. Tegu $f(x) = a_n x^n + \cdots + a_0$ ir $g(x) = b_m x^m + \cdots + b_0$. Polinomų $q(x)$ ir $r(x)$ egzistavimą ir vienatinumą įrodysime matematine indukcija pagal polinomo $f(x)$ laipsnį n.

Egzistavimas.

Indukcijos bazė. Jei $n = 0$, tai $f(x) = a_0 \in K$ ir tada galimi du atvejai:

(i) jei $\deg g(x) = 0$, t.y. $g(x) = b_0 \neq 0$, tai

$$f(x) = g(x) \cdot \tfrac{a_0}{b_0} + 0 \text{ ir } \deg 0 = -\infty < 0 = \deg g(x)\,.$$

(ii) jei $\deg g(x) > 0$, ta$i$

$$f(x) = g(x) \cdot 0 + f(x) \text{ ir } 0 = \deg f(x) < \deg g(x)\,.$$

Indukcijos prielaida. Tegu teiginys yra teisingas visiems polinomams, kurių laipsnis $< n$.

Indukcijos teiginį įrodysime n - ojo laipsnio polinomui $f(x)$. Galimi du atvejai:

(i) jei $n < m$, tai

$$f(x) = g(x) \cdot 0 + f(x) \text{ ir } n = \deg f(x) < \deg g(x) = m.$$

(ii) jei $n \geq m$, tai polinomo

$$f_1(x) = f(x) - \tfrac{a_n}{b_m} x^{n-m} g(x)$$

laipsnis yra mažesnis už n ir pagal indukcijos prielaidą egzistuoja tokie polinomai $q_1(x)$ ir $r(x)$ iš $\mathbf{K}[x]$, kad

$$f_1(x) = g(x) \cdot q(x) + r(x) \text{ ir } \deg r(x) < \deg g(x).$$

Tada

$$f(x) = g(x) \cdot \left(\tfrac{a_n}{b_m} x^{n-m} + q_1(x) \right) g(x) + r(x) \text{ ir } \deg r(x) < \deg g(x).$$

Vienatinumas.
Tegu

$$f(x) = g(x) \cdot p(x) + s(x) \text{ ir } \deg s(x) < \deg g(x).$$

Tada

$$\begin{gathered} 0 = g(x) \cdot (q(x) - p(x)) + (r(x) - s(x)) \\ g(x) \cdot (q(x) - p(x)) = (s(x) - r(x)) \end{gathered}$$

ir pagal *4.3 Teiginį* turime

$$\deg g(x) + \deg(q(x) - p(x)) = \deg(s(x) - r(x)) < \deg g(x).$$

Bet $g(x) \neq 0$ ir todėl tai įmanoma tik tuo atveju, kai

$$q(x) - p(x) = s(x) - r(x) = 0.$$

Įrodyta.

5.2 **Pavyzdys**. Padalinsime polinomą $f(x) = 3x^4 - 5x^3 + 2x + 4$ iš polinomo $g(x) = x^2 - 2x + 5$ su liekana.

$$\begin{gathered} f_1(x) = (3x^4 - 5x^3 + 2x + 4) - \tfrac{3}{1} x^{4-2} (x^2 - 2x + 5) = x^3 - 15x^2 + 2x + 4 \\ f_2(x) = (x^3 - 15x^2 + 2x + 4) - \tfrac{1}{1} x^{3-2} (x^2 - 2x + 5) = -13x^2 - 3x + 4 \\ f_3(x) = (-13x^2 - 3x + 4) - \tfrac{-13}{1} (x^2 - 2x + 5) = -29x + 69 \end{gathered}$$

Tada

$$f(x) = f_1(x) + 3x^2 g(x)$$
$$f_1(x) = f_2(x) + xg(x)$$
$$f_2(x) = f_3(x) + 13g(x)$$
$$f_3(x) = -29x + 69$$

ir

$$f(x) = f_1(x) + 3x^2 g(x)$$
$$f(x) = f_2(x) + xg(x) + 3x^2 g(x) = f_2(x) + g(x)(3x^2 + x)$$
$$f(x) = f_3(x) + 13g(x) + g(x)(3x^2 + x) = f_3(x) + g(x)(3x^2 + x - 13)$$
$$f(x) = g(x)(3x^2 + x - 13) + (-29x + 69).$$

5.3 **Apibrėžimas.** *Tegu $f(x)$ ir $g(x)$ yra nenuliniai polinomai virš kūno* $\mathbf{K}$. *Polinomas $d(x) \in \mathbf{K}[x]$, kurio vyriausias koeficientas yra lygus* 1, *vadinamas polinomų $f(x)$ ir $g(x)$ bendruoju didžiausiu dalikliu, jeigu*

1. $f(x) \vdots d(x), g(x) \vdots d(x)$.

2. Jeigu $f(x) \vdots d_1(x), g(x) \vdots d_1(x)$ su $d_1(x) \in \mathbf{K}[x]$, *tai* $d(x) \vdots d_1(x)$.
Bendro didžiausio daliklio žymuo: $d(x) = \mathrm{BDD}(f(x), g(x))$.

5.4 **Teorema.** *Su visais* $f(x), g(x) \in \mathbf{K}[x]$, $f(x), g(x) \neq 0$ *egzistuoja tokie polinomai* $u(x), v(x) \in \mathbf{K}[x]$, *kad*

$$\mathrm{BDD}(f(x), g(x)) = f(x) \cdot u(x) + g(x) \cdot v(x).$$

Įrodymas pakeitus, žodžius *sveikas skaičius* į *polinomas*, o *mažiausias teigiamas skaičius* į *mažiausio laipsnio polinomas*, yra toks pats kaip *1.7 Teoremos* įrodymas.

Kaip ir sveikųjų skaičių atveju, dviejų polinomų BDD radimui naudojamas Euklido algoritmas.

5.5 **Euklido algoritmas BDD skaičiavimui.** Turime du polinomus $f(x), g(x) \in \mathbf{K}[x]$, $f(x), g(x) \neq 0$.Rašysime dalybos su liekana teoremą

Tegu $f_0 = f(x)$ ir $f_1 = g(x)$. Tada

$$\begin{array}{cc} f_0 = f_1 q_1 + f_2 & \deg f_2 < \deg f_1 \\ f_1 = f_2 q_2 + f_3 & \deg f_3 < \deg f_2 \\ \ldots & \ldots \\ f_{k-2} = f_{k-1} q_{k-1} + f_k & \deg f_k < \deg f_{k-1} \\ f_{k-1} = f_k q_k. & \end{array}$$

Sveikieji skaičiai sudaro mažėjančią seką

$$\deg f_1 > \deg f_2 > \deg f_3 > \cdots > \deg f_{k-1} > \deg f_k \geq 0.$$

Tada $\mathrm{BDD}(f(x), g(x)) = f_k(x)$.

5.6 **Išplėstinis Euklido algoritmas BDD tiesinei išraiškai rasti.**

$$\begin{array}{c} f_0 = f(x) \cdot 1 + g(x) \cdot 0 \\ f_1 = f(x) \cdot 0 + g(x) \cdot 1 \\ f_2 = f(x) \cdot u_2(x) + g(x) \cdot v_2(x) \\ f_3 = f(x) \cdot u_3(x) + g(x) \cdot v_3(x) \\ \cdots \\ f_k = f(x) \cdot u_k(x) + g(x) \cdot v_k(x) \\ u_j(x) = u_{j-2}(x) - q_{j-1}(x) \cdot u_{j-1}(x) \\ v_j(x) = v_{j-2}(x) - q_{j-1}(x \cdot) v_{j-1}(x) \end{array}$$

Tada $\mathrm{BDD}(f(x), g(x)) = f_k(x) = f(x) \cdot u_k(x) + g(x) \cdot v_k(x)$.

5.7 **Apibrėžimas.** *Du polinomai* $f(x), g(x) \in \mathbf{K}[x]$ *vadinami tarpusavyje pirminiais, jeigu* $\mathrm{BDD}(f(x), g(x)) = 1$.

5.8 **Teorema.** *Jei polinomai* $f(x), g(x) \in \mathbf{K}[x]$ *yra tarpusavyje pirminiai, tai egzistuoja tokie* $u(x), v(x) \in \mathbf{K}[x]$, *kad* $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$.

Įrodymas. Tegu $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$ ir $\mathrm{BDD}(f(x), g(x)) = d(x)$. Tada

$$1 = \underbrace{\underbrace{f(x) \cdot u(x)}_{\text{dalijasi iš } d(x)} + \underbrace{g(x) \cdot v(x)}_{\text{dalijasi iš } d(x)}}_{\text{dalijasi iš } d(x)},$$

t,y. 1 dalijasi iš $d(x)$ ir todėl $d(x) = 1$.
Įrodyta.

5.9 **Teiginys(tarpusavyje pirminių polinomų savybė).** *Tegu* $f_1(x), ..., f_m(x)$ *ir* $g_1(x), ..., g_n(x)$ *yra dvi tokios polinomų sekos, kad*

$$\mathrm{BDD}(f_i(x), g_j(x)) = 1$$

su visais $1 \le i \le m, 1 \le j \le n$.
Tada

$$\mathrm{BDD}(f_1(x) \cdots f_m(x), g_1(x) \cdots g_n(x)) = 1.$$

Be įrodymo.

Dabar pateiksime teiginį, kurio analogo sveikųjų skaičių žiede nėra. Priminsime, kad mes žinome tokius kūnus $\mathbf{K}$: trys begaliniai skaičių kūnai - racionalųjų skaičių $\mathbf{Q}$, realiųjų skaičių $\mathbf{R}$ ir kompleksinių skaičių $\mathbf{C}$, ir baigtiniai kūnai $\mathbf{Z}_p$, turintys p elementų. Turime, kad $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ ir tada sakome, kad $\mathbf{R}$ yra $\mathbf{Q}$ plėtinys, $\mathbf{C}$ yra ir $\mathbf{Q}$, ir $\mathbf{R}$ plėtinys. Žemiau kalbėdami apie kūnų plėtinius turėsime galvoje būtent šiuos pavyzdžius(nors teiginiai yra teisingi ir bendru atveju).

5.10 **Teiginys.** *Jei $f(x)$ ir $g(x)$ yra tarpusavyje pirminiai polinomai virš kūno $\mathbf{K}$, tai jie neturi bendrų šaknų jokiame kūno $\mathbf{K}$ plėtinyje $\mathbf{L}$, $\mathbf{L} \supseteq \mathbf{K}$.*

Įrodymas. Jei $f(x)$ ir $g(x)$ yra tarpusavyje pirminiai polinomai virš kūno $\mathbf{K}$, tai pagal *5.8 Teoremą* egzistuoja tokie polinomai $u(x)$ ir $v(x)$, kad

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

Jeigu kūno $\mathbf{K}$ plėtinyje $\mathbf{L}$ būtų bendra polinomų $f(x)$ ir $g(x)$ šaknis x_0, $f(x_0) = g(x_0) = 0$, tai iš

$$1 = f(x_0) \cdot u(x_0) + g(x_0) \cdot v(x_0) = 0$$

gautume prieštarą, nes bet kuriame kūne $1 \neq 0$.
Įrodyta.

Pirminių sveikųjų skaičių vaidmenį polinomų žiede vaidina neredukuojami polinomai.

5.11 **Apibrėžimas.** *Teigiamo laipsnio polinomas $p(x) \in \mathbf{K}[x]$, kurio vyriausias koeficientas lygus 1, vadinamas neredukuojamu polinomu virš kūno $\mathbf{K}$, jeigu jis dalijasi tik iš nenulinių kūno elementų $a \in \mathbf{K}$ ir savo paties nenulinių kartotinių $ap(x)$.*

Polinomo sąvybė būti neredukuojamu priklauso nuo kūno **K**, virš kurio polinomas yra nagrinėjamas. Pavyzdžiui, polinomas $f(x) = x^2 - 2$ yra neredukuojamas virš racionaliųjų skaičių kūno **Q,** bet yra redukuojamas virš realiųjų skaičių kūno **R**, nes $f(x) = x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

5.12 **Teiginys**. *Bet kuris teigiamo laipsnio polinomas iš* $\mathbf{K}[x]$ *dalijasi iš kurio nors neredukuojamo polinomo virš* $\mathbf{K}$.

5.13 **Teiginys(neredukuojamų polinomų savybė).** *Tegu* $f_1(x), ..., f_m(x)$ *yra tokia polinomų iš* $\mathbf{K}[x]$ *seka, kad polinomas* $f_1(x) \cdots f_m(x)$ *dalijasi iš neredukuojamo polinomo* $p(x) \in \mathbf{K}[x]$. *Tada egzistuoja toks* $j, 1 \leq j \leq m$, *kad* $f_j(x)$ *dalijasi iš* $p(x)$.

Be įrodymo.

Pateiksime teiginį, kurio analogo sveikųjų skaičių žiede nėra.

5.14 **Teiginys.** *Jeigu neredukuojamas polinomas* $p(x) \in \mathbf{K}[x]$ *ir polinomas* $f(x) \in \mathbf{K}[x]$ *turi bendrą šaknį kuriame nors kūno* K *plėtinyje* $\mathbf{L} \supset \mathbf{K}$, *tai* $f(x) \vdots p(x)$.

Įrodymas. Tegu $d(x)$ =BDD$(f(x), p(x)) \in \mathbf{K}[x]$ ir neredukuojamas virš **K** polinomas $p(x)$ dalijasi iš $d(x)$.Tada arba $p(x) = d(x)$ ir $f(x) \vdots p(x)$, arba $d(x)$ =BDD$(f(x), p(x)) = 1$ ir pagal *5.8 Teoremą* egzistuoja tokie polinomai $u(x)$ ir $v(x)$, kad

$$f(x) \cdot u(x) + p(x) \cdot v(x) = 1.$$

Tegu dabar polinomai $p(x)$ ir $f(x)$ kūno **K** plėtinyje **L** turi bendrą šaknį $\alpha \in \mathbf{L}$:t.y. $f(\alpha) = p(\alpha) = 0$. Tada

$$1 = f(\alpha) \cdot u(\alpha) + p(\alpha) \cdot v(\alpha) = 0$$

gautume prieštarą, nes bet kuriame kūne $1 \neq 0$.

Įrodyta.

5.15 **Teorema(apie kanoninį polinomo skaidinį).** *Su kiekvienu teigiamo laipsnio polinomu* $f(x) = a_n x^n + \cdots + a_0 \in \mathbf{K}[x]$ *egzistuoja tokie neredukuojami virš kūno* K *polinomai* $p_1(x), p_2(x), ..., p_s(x)$ *(tarp jų gali būti sutampančių), kad*

$$f(x) = a_n \cdot p_1(x) \cdot p_2(x) \cdot \dots \cdot p_s(x),$$

Šiame skaidinyje sutraukę panašius daugiklius turėsime kanoninį polinomo f skaidinį:

$$f(x) = a_n \cdot p_{i_1}^{k_1}(x) \cdot p_{i_2}^{k_2}(x) \cdots p_{i_t}^{k_t}(x),$$

$p_i(x) \neq p_j(x)$.
Be įrodymo.

5.16 **Teorema**. *Yra be galo daug neredukuojamų polinomų virš bet kurio kūno.*

Įrodymas. Įrodysime prieštaros būdu. Sakykime, egzistuoja baigtinis neredukuojamų polinomų skaičius: $p_1(x), p_2(x), ..., p_m(x)$. Pagal *5.12 Teiginį* polinomas $f(x) = p_1(x) p_2(x) \cdots p_m(x) + 1$ dalijasi iš neredukuojamo polinomo. Tada turėtų egzistuoti toks $i, 1 \leq i \leq m$, kad $f(x) \vdots p_i(x)$ ir

$$1 = \underbrace{\underbrace{f(x)}_{\text{dalijasi iš } p_i(x)} - \underbrace{p_1(x) p_2(x) \cdots p_m(x)}_{\text{dalijasi iš } p_i(x)}}_{\text{dalijasi iš } p_i(x)},$$

t.y. $1 \vdots p_i(x)$ ir pagal 4.6.7 teiginį $\deg 1 \geq \deg p_i(x)$. Bet tai prieštarautų neredukuojamo polinomo apibrėžimui, nes $\deg p_i(x) > 0$, o $\deg 1 = 0$.
Įrodyta.

Apie neredukuojamus polinomus virš baigtinio kūno $\mathbf{Z}_p$ ir racionaliųjų skaičių kūno $\mathbf{Q}$

5.16 teorema yra akivaizdi polinomų žiedams virš begalinių kūnų $\mathbf{K}$, tokių kaip $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, nes dvinariai $x - a$ yra neredukuojami polinomai su visais $a \in \mathbf{K}$.Tačiau polinomų žiedams virš baigtinių kūnų $\mathbf{Z}_p$ teorema nėra akivaizdi. Yra žinomi n- ojo laipsnio neredukuojamų polinomų virš baigtinio kūno $\mathbf{Z}_p$ skaičiaus $N_p(n)$ įverčiai :

$$\frac{1}{n}\left(p^n - \frac{p^n - p}{p-1}\right) \leq N_p(n) \leq \frac{1}{n}(p^n - p).$$

Pastebėkime, kad

$$N_p(n) \geq \frac{1}{n}\left(p^n - \frac{p^n - p}{p-1}\right) = \frac{1}{n}\left(p^n - p^{n-1} - \cdots - p\right) > 0.$$

Iš įverčio $N_p(n) > 0$ matome, kad su visais pirminiais skaičiais p egzistuoja bet kokio natūralaus laipsnio n neredukuojamas polinomas virš $\mathbf{Z}_p$. Tokia pati situacija ir polinomų žiede virš racionaliųjų skaičių $\mathbf{Q}[x]$: egzistuoja bet kokio natūralaus laipsnio n neredukuojamas polinomas virš $\mathbf{Q}$ (žr. 5 pratybas).

Apie neredukuojamus polinomus virš kompleksinių skaičių kūno C.

Fundamentalioji algebros teorema teigia:

5.17 **Fundamentalioji algebros teorema**. *Bet kokia algebrinė lygtis* $a_n x^n + \cdots + a_1 x + a_0 = 0$, $n \geq 1$ *su kompleksiniais koeficientais* $a_i \in \mathbf{C}$ $(0 \leq i \leq n)$ *turi mažiausiai vieną kompleksinį sprendinį.*

Be įrodymo.

Iš šios teoremos matome, kad $n-$ ojo laipsnio polinomas virš kopleksinių skaičių kūno $\mathbf{C}$ turi lygiai n šaknų. Akivaizdu, kad tada neredukuojami polinomai virš $\mathbf{C}$ yra tik pirmojo laipsnio polinomai $x - a, a \in \mathbf{C}$.

Apie neredukuojamus polinomus virš kompleksinių skaičių kūno R.

5.18 **Apibrėžimas.** *Tegu polinomas*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{C}[x].$$

Tada polinomas $\bar{f}(x)$ *yra apibrėžiamas lygybe*

$$\bar{f}(x) = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0,$$

čia $\bar{a}_i$ *yra skaičiaus* a_i *jungtinis.*

5.19 **Lema.** (1) *Tegu polinomas* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{C}[x]$ *ir* $z \in \mathbf{C}$. *Tada*

$$\overline{f(z)} = \bar{f}(\bar{z}).$$

(2) *Tegu polinomas* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{R}[x]$ ir $z \in \mathbf{C}$. *Tada*

$$\overline{f(z)} = f(\bar{z}).$$

Visus neredukuojamus polinomus virš realiųjų skaičių kūno **R** aprašo ši teorema.

5.20 **Teorema.** *Jei* $f(x)$ yra *neredukuojamas polinomas virš realiųjų skaičių kūno* **R** *, tai* $f(x)$*yra arba pirmojo laipsnio polinomas* $x-a, a \in \mathbf{R}$, *arba toks kvadratinis trinaris* x^2+px+q, *kad* $p^2-4q<0$.

Įrodymas. Aišku, kad polinomai $p(x) = x-a, a \in \mathbf{R}$, ir $p(x) = x^2+px+q$, $p^2-4q<0$ yra neredukuojami virš **R.** Į polinomą $f(x)$ galima žiūrėti ir kaip į polinomą virš **C**. Pagal *5.17 Fundamentaliąją algebros teoremą* polinomas $f(x)$ turi kompleksinę šaknį $z_0 = a+ib: \ f(z_0) = 0$. Galimi du atvejai.

1) Jei $z_0 \in \mathbf{R}$, tai $z_0 = a$ ir $f(x) \vdots (x-a)$ ir kadangi $f(x)-$ neredukuojamas, tai $f(x) = x-a$.

2) Jei $z_0 \notin \mathbf{R}$, tai $z_0 = a+ib, b \neq 0$, ir $\bar{z}_0 \neq z_0$. Pagal *5.19 Lemą* turime

$$f(z_0) = 0 \Rightarrow \overline{f(z_0)} = f(\bar{z}_0) = 0,$$

t.y polinomas $f(x)$ turi mažiausiai dvi šaknis z_0 ir $\bar{z}_0$. Tada $f(x)$ dalijasi iš $(x-z_0)(x-\bar{z}_0)$. Bet

$$(x-z_0)(x-\bar{z}_0) = x^2 - x(z_0+\bar{z}_0) + z_0 \cdot \bar{z}_0 = x^2 - 2ax + (a^2+b^2) \in \mathbf{R}[x]$$

ir

$$p^2 - 4q = 4a^2 - 4a^2 - 4b^2 = -4b^2 < 0,$$

taigi $(x-z_0)(x-\bar{z}_0)$ yra neredukuojamas polinomas virš **R**. Tada

$$f(x) = (x-z_0)(x-\bar{z}_0) = x^2 - 2ax + (a^2+b^2).$$

Įrodyta.