Algebros paskaitos

Rimantas Grigutis

4 paskaita.

Polinomų žiedas. Polinomo laipsnis. Polinomų dalumo sąvybės. Hornerio schema. Polinomo reiškimas dvinario laipsniais. Polinomų šaknys ir jų skaičius

Polinomų žiedas.

4.1 **Apibrėžimas.** *Polinomu virš kūno* $\mathbf{K}$ *vadiname begalinę kūno* $\mathbf{K}$ *elementų seką* $(a_0, a_1, a_2, ...)$, *kurios beveik visi (t.y. visi, išskyrus baigtinį skaičių) elementai yra lygūs* 0. *Sakysime, kad du polinomai* $(a_0, a_1, a_2, ...)$ *ir* $(b_0, b_1, b_2, ...)$ *yra lygūs, jeigu* $a_i = b_i$ *su visais* $i = 0, 1, 2, ...$.

Polinomų aibėje apibėžiami šie veiksmai:

1. Polinomų sudėtis:

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...) .$$

2. Polinomų daugyba:

$$(a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) = (c_0, c_1, c_2, ...) ,$$

čia

$$c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0 = \sum_{s=0}^{i} a_s b_{i-s} = \sum_{s+t=i} a_s b_t .$$

Šių operacijų atžvilgiu *polinomų aibė sudaro komutatyvų žiedą su vienetu.* Vienetas šiame žiede yra polinomas $(1, 0, 0, ...)$.

Atsižvelgę į tai, kad

$$(a, 0, 0, ...) + (b, 0, 0, ...) = (a + b, 0, 0, ...)$$

ir

$$(a, 0, 0, ...) \cdot (b, 0, 0, ...) = (ab, 0, 0, ...),$$

ir bendru atveju,

$$(a, 0, 0, ...) \cdot (b_0, b_1, b_2, ...) = (ab_0, ab_1, ab_2, ...),$$

mes polinomą $(a, 0, 0, ...)$ galime sutapatinti su elementu a.
Pažymėkime dabar polinomą $(0, 1, 0, 0, ...)$ raide x. Tada

$$x^2 = (0, 0, 1, 0, ...), x^3 = (0, 0, 0, 1, 0, ...) \text{ ir t.t.}$$

Dabar polinomą galima reikšti ir taip:

$$\begin{gathered}(a_0, a_1, a_2, ...) = (a_0, 0, 0, ...) + (0, a_1, 0, ...) + (0, 0, a_2, 0, ...) = \\ a_0 (1, 0, 0, ...) + a_1 (0, 1, 0, ...) + a_2 (0, 0, 1, 0, ..) + \cdots = \\ a_0 + a_1 x + a_2 x + \cdots + a_n x^n.\end{gathered}$$

Žymėjimas. *Visų polinomų virš kūno* $\mathbf{K}$ *aibę žymėsime* $\mathbf{K}[x]$.

Polinomo laipsnis.

4.2 **Apibrėžimas** *Polinomo* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, $a_n \neq 0$, *elementas* a_n *vadinamas vyriausiuoju polinomo* $f(x)$ *koeficientu, o skaičius* n *- polinomo* $f(x)$ *laipsniu, žymuo:* $n = \deg f$. *Susitarta, kad* $\deg 0 = -\infty$.

4.3 **Teiginys.** *Dviejų polinomų sandaugos laipsnis yra lygus tų polinomų laipsnių sumai*:

$$\deg (f \cdot g) = \deg f + \deg g.$$

Įrodymas paliekamas skaitytojams.

4.4 **Pastaba.** Yra susitarta, kad $(-\infty) + (-\infty) = -\infty$; $(-\infty) + n = -\infty$; $n + (-\infty) = -\infty$.

Polinomų dalumo savybės. Hornerio schema

4.5 **Apibrėžimas.** *Jeigu polinomų porai* $f(x)$ *ir* $g(x), g(x) \neq 0$, *egzistuoja toks polinomas* $h(x)$, *kad* $f(x) = g(x) \cdot h(x)$, *tai sakysime, kad polinomas* f *dalijasi be liekanos(arba tiesiog dalijasi) iš polinomo* g. *Rašysime* $f \vdots g$. *Polinomas* g *vadinamas polinomo* f *dalikliu.*

4.6 **Teiginys (Pagrindinės polinomų dalumo savybės)**

1. Jei $f, g, h \in \mathbf{K}[x]$ *ir* $f \vdots h$ *ir* $g \vdots h$ *, tai* $(f \pm g) \vdots h$.

2. Jei $f, g, h \in \mathbf{K}[x]$ *ir* $f \vdots h$ *, tai* $(f \cdot g) \vdots h$.

3. Jei $f \in \mathbf{K}[x]$ *ir* $f \neq 0$, *tai* $0 \vdots f$.

4. Jei $f \in \mathbf{K}[x]$ *ir* $a \in \mathbf{K}, a \neq 0$,*tai* $f \vdots a$.

5. Jei $f \in \mathbf{K}[x]$ *ir* $1 \vdots f$, *tai* $\deg f = 0$ *ir* $f = a \in \mathbf{K}$.

6. Jei $f, g \in \mathbf{K}[x]$ *ir* $f \vdots g$ *ir* $g \vdots f$ *, tai* $f = a \cdot g$, *čia* $a \in \mathbf{K}$.

7. Jei $f, g \in \mathbf{K}[x]$ *, f(x)*$\neq 0$, *ir* $f \vdots g$ *, tai* $\deg f \geq \deg g$.

Nagrinėsime polinomo $f(x) \in \mathbf{K}[x]$ dalumą iš dvinario $x - c, c \in \mathbf{K}$.

4.7 **Teorema.** *Tegu*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{K}[x] \text{ ir } c \in \mathbf{K}.$$

Tada egzistuoja toks polinomas $h(x) \in \mathbf{K}[x]$ *ir toks* $r \in \mathbf{K}$, *kad*

$$f(x) = (x - c) h(x) + r.$$

Įrodymas. Iš *4.3 Teiginio* turime, kad polinomo $h(x)$ laipsnis turėtų būti lygus $n - 1$, o pats polinomas $h(x)$ turėtų būti lygus $b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$. Tada

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ &= (x - c)\left(b_{n-1} x^{n-1} + \cdots + b_1 x + b_0\right) + r. \end{aligned}$$

Palyginę kairės ir dešinės pusių koeficientus prie vienodų laipsnių, turėsime :

$$\begin{array}{cc} a_n = b_{n-1} & b_{n-1} = a_n \\ a_{n-1} = b_{n-2} - c b_{n-1} & b_{n-2} = a_{n-1} + c b_{n-1} \\ a_{n-2} = b_{n-3} - c b_{n-2} & b_{n-3} = a_{n-2} + c b_{n-2} \\ \cdots & \cdots \\ a_1 = b_0 - c b_1 & b_0 = a_1 + c b_1 \\ a_0 = r - c b_0 & r = a_0 + c b_0 \end{array}.$$

Įrodyta.

4.8 **Pastaba.** Dažniausiai polinomo $h(x)$ koeficientai skaičiuojami **Hornerio schema:**

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c	$\mathbf{b}_{n-1} = a_n$	$\mathbf{b}_{n-2} = a_{n-1} + cb_{n-1}$	$\cdots$	$\mathbf{b}_0 = a_1 + cb_1$	$\mathbf{r} = a_0 + cb_0$

Matome, kad $f(c) = (c - c)\, h(c) + r = r$, t.y. elementas r yra polinomo f reikšmė elemente c.

4.9 **Pavyzdys.** Tegu polinomas $f(x) = 2x^5 - 4x^3 + 3x^2 + x - 5$, o $c = 2$. Tada polinomo f Hornerio schema yra:

	2	0	-4	3	1	-5
$c = 2$	2	4	4	11	23	41

$$2x^5 - 4x^3 + 3x^2 + x - 5 = (x - 2)\left(2x^4 + 4x^3 + 4x^2 + 11x + 23\right) + 41$$

ir $f(2) = 41$.

Polinomo reiškimas dvinario laipsniais.

4.10 **Teorema.** Tegu

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbf{K}[x].$$

Tada egzistuoja tokie $r_0, r_1, ..., r_n \in \mathbf{K}$, kad

$$f(x) = r_n (x - c)^n + r_{n-1} (x - c)^{n-1} + \cdots + r_1 (x - c) + r_0.$$

Įrodymas. Naudodamiesi *4.7 Teorema* turėsime

$$\begin{gathered} f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \\ = (x - c)\left(b_{1,n-1} x^{n-1} + \cdots + b_{1,1} x + b_{1,0}\right) + r_0 \\ = (x - c)\left((x - c)\left(b_{2,n-2} x^{n-2} + \cdots + b_{2,1} x + b_{2,0}\right) + r_1\right) + r_0 \\ = (x - c)^2 \left(b_{2,n-2} x^{n-2} + \cdots + b_{2,1} x + b_{2,0}\right) + (x - c)\, r_1 + r_0 \\ = (x - c)^2 \left((x - c)\left(b_{3,n-3} x^{n-3} + \cdots + b_{3,1} x + b_{3,0}\right) + r_2\right) + (x - c)\, r_1 + r_0 \\ \cdots \\ = r_n (x - c)^n + r_{n-1} (x - c)^{n-1} + \cdots + r_1 (x - c) + r_0 \end{gathered}$$

Elementus r_i galima rasti Hornerio schema:

	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0	
	$b_{1,n-1}$	$b_{1,n-2}$	$\cdots$	$b_{1,1}$	$b_{1,0}$	r_0	
c	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	
$\cdots$	$b_{n-1,1}$	$b_{n-1,0}$	r_{n-2}				
c	$b_{n,0}$	r_{n-1}					
c	r_n						

.

Įrodyta.

4.11 **Pavyzdys.** Parašykime polinomą $f(x) = 2x^5 - 4x^3 + 3x^2 + x - 5$ dvinario $x - 2$ laipsniais:

	2	0	-4	3	1	-5
2	2	4	4	11	23	41
2	2	8	20	51	125	
2	2	12	44	139		
2	2	16	76			
2	2	20				
2	2					

Tada

$$f(x) = 2x^5 - 4x^3 + 3x^2 + x - 5$$
$$= 2(x-2)^5 + 20(x-2)^4 + 76(x-2)^3 + 139(x-2)^2 + 125(x-2) + 41.$$

Polinomų šaknys ir jų skaičius

4.12 **Teorema(Bezout).** *Polinomas $f(x) \in \mathbf{K}[x]$ dalijasi iš $x - c$ tada ir tik tada, kada c yra polinomo $f(x)$ šaknis, t.y. $f(c) = 0$.*

Įrodymas paliekamas skaitytojui.

4.13 **Teorema(polinomo šaknų skaičius)**. *Tegu $f(x) \in \mathbf{K}[x]$.* Jei $\deg f = n$, *tai polinomo $f(x)$ šaknų skaičius neviršija n.*

Įrodymas. Matematinė indukcija pagal n.

Indukcijos bazė: $n = 0$. Teiginys yra teisingas visiems nulinio laipsnio polinomams, nes šie polinomai neturi šaknų.

Indukcijos prielaida: teiginys yra teisingas visiems polinomams, kurių laipsnis mažesnis už n.

Indukcijos teiginys skiriamas $n-$ ojo laipsnio polinomui $f(x)$.

Nagrinėkime kelis atvejus.

1. Jeigu polinomas $f(x)$ neturi šaknų kūne $\mathbf{K}$, tai polinomui f teiginys yra teisingas.

2. Jeigu c_1 yra polinomo $f(x)$ šaknis, tai pagal *4.12 Bezout teoremą*

$$f(x) = (x - c_1)\, h(x)$$

ir

$$\deg h(x) = n - 1.$$

Jeigu c_2- kita polinomo $f(x)$ šaknis $(c_1 \neq c_2)$, tada

$$f(c_2) = (c_2 - c_1)\, h(c_2) = 0$$

ir

$$h(c_2) = 0.$$

Taigi, kiekviena polinomo $f(x)$ šaknis, skirtinga šakniai c_1 yra ir polinomo h šaknis(atvirkščias teiginys akivaizdus). Pritaikius polinomui $h(x)$ indukcijos prielaidą, turėsime, kad $h(x)$ turi ne daugiau kaip $n - 1$ šaknį. Tada polinomas $f(x)$ turės ne daugiau kaip n šaknų.

Įrodyta.

4.14 **Pastaba.** Teorema yra teisinga ir polinomams virš komutatyvių žiedų su vienetu, kuriuose nėra **nulio daliklių**(tokiuose žieduose iš $a \cdot b = 0$, turime, kad arba $a = 0$, arba $b = 0$). Tokie žiedai yra vadinami *integralumo sritimis*. Integralumo sritimi yra visi kūnai. Integralumo srities bet ne kūno pavyzdžiu galėtų būti sveikųjų skaičių žiedas $\mathbf{Z}$. Iš kitos pusės, jeigu K nėra integtalumo sritis(pavyzdžiui, tokiais žiedais yra visi $\mathbf{Z}_m$, kai $m-$ sudėtinis) tai teoremos teiginys nėra teisingas: pavyzdžiui, polinomas polinomas $f(x) = x^2$ virš $\mathbf{Z}_9$ turi tris šaknis: $\bar{0}, \bar{3}, \bar{6}$. Tikrai $0^2 = 0 \pmod 9,\ 3^2 = 0 \pmod 9,\ 6^2 = 0 \pmod 9$.

4.15 **Teorema(apie polinominį ir funkcionalinį tapatumą)**. *Tegu* $\mathbf{K}$ *yra begalinis kūnas(pvz.* $\mathbf{Q}$**,** $\mathbf{R}$ *arba* $\mathbf{C}$*) ir polinomai* $f_1(x), f_2(x) \in \mathbf{K}[x]$. *Jeigu* $f_1(c) = f_2(c)$ *su visais* $c \in \mathbf{K}$, *tai* $f_1(x) = f_2(x)$.

Įrodymas. Nagrinėkime polinomą $F(x) = f_1(x) - f_2(x)$. Šio polinomo laipsnis $\deg F(x) = n \leq \max\{\deg f; \deg g\}$. Tegu dabar $c_1, c_2, ..., c_{n+1}$ yra skirtingi begalinio kūno $\mathbf{K}$ elementai ir pagal teoremos sąlygą turime, kad $f_1(c_i) = f_2(c_i)$ su visais $i = 1, 2, ..., n+1$. Tada n-ojo laipsnio polinomas $F(x)$ turi $n+1$ šaknį ir pagal *4.13 Teoremą* $F(x) = 0$ ir $f_1(x) = f_2(x)$.

Įrodyta.

4.16 **Pastaba.** Virš *baigtinių* kūnų $\mathbf{K}$ (pavyzdžiui, virš $\mathbf{Z}_p$, $p-$ pirminis skaičius) teoremos teiginys nėra teisingas. Pavyzdžiui, skirtingų polinomų $f_1(x) = x^7 + \bar{4}x + \bar{1}$ ir $f_2(x) = \bar{5}x + \bar{1}$ virš kūno $\mathbf{Z}_7$ reikšmės visuose kūno $\mathbf{Z}_7$ elementuose sutampa:

$$
\begin{array}{cc}
f_1(\bar{0}) = f_2(\bar{0}) = \bar{1}; & f_1(\bar{1}) = f_2(\bar{1}) = \bar{6}; \\
f_1(\bar{2}) = f_2(\bar{2}) = \bar{4}; & f_1(\bar{3}) = f_2(\bar{3}) = \bar{2}; \\
f_1(\bar{4}) = f_2(\bar{4}) = \bar{0}; & f_1(\bar{5}) = f_2(\bar{5}) = \bar{5}; \\
\multicolumn{2}{c}{f_1(\bar{6}) = f_2(\bar{6}) = \bar{3}.}
\end{array}
$$