6. kapitola

POLYNOMY VÍCE NEURČITÝCH

V tvoření polynomů nad okruhem můžeme pokračovat takto: Zvolíme okruh $\mathsf{M}[x]$ polynomů jedné neurčité x nad okruhem M a nad okruhem $\mathsf{M}[x]$ můžeme sestrojit nový okruh polynomů další neurčité y, který budeme označovat $\mathsf{M}[x, y]$ a který ovšem vyhovuje větě 9. Prvky okruhu $\mathsf{M}[x, y]$ mají podle toho tvar

$$A = A_0 + A_1 y + A_2 y^2 + \ldots + A_s y^s,$$

kde A_j jsou polynomy jedné neurčité x nad okruhem M, tj.

$$A_j = a_{0j} + a_{1j} x + a_{2j} x^2 + \ldots + a_{rj} x^r,$$

kde $a_{ij} \in \mathsf{M}$. Prvkům a_{ij} jsme dali dva indexy i, j, z nichž první je roven exponentu příslušné mocniny neurčité x a druhý exponentu příslušné mocniny neurčité y. Předpokládáme, že ve všech polynomech A_j má neurčitá x týž exponent u nejvyšší mocniny; kdyby tomu tak nebylo, doplníme zbývající místa nulovými členy. Poněvadž je násobení v okruhu $\mathsf{M}[x, y]$ distributivní vzhledem k sčítání, můžeme libovolný prvek okruhu $\mathsf{M}[x, y]$ napsat v tvaru

$$\begin{aligned} A = a_{00} &+ a_{10}x + a_{20}x^2 + \ldots + a_{r0}x^r + \\ + a_{01}y &+ a_{11}xy + a_{21}x^2y + \ldots + a_{r1}x^ry + \\ + a_{02}y^2 &+ a_{12}xy^2 + a_{22}x^2y^2 + \ldots + a_{r2}x^ry^2 + \\ + &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + \\ + a_{0s}y^s &+ a_{1s}xy^s + a_{2s}x^2y^s + \ldots + a_{rs}x^ry^s. \end{aligned}$$

V uvedeném schématu však můžeme sčítat jednotlivé členy i po sloupcích, takže týž prvek $A \in \mathsf{M}[x, y]$ lze napsat i ve tvaru

$$A = A_0' + A_1'x + A_2'x^2 + \ldots + A_r'x^r,$$

kde

$$A_i' = a_{i0} + a_{i1}y + a_{i2}y^2 + \ldots + a_{is}y^s.$$

To však znamená, že okruh $\mathsf{M}[x, y]$ vznikne také jako okruh polynomů jedné neurčité x nad okruhem $\mathsf{M}[y]$, jinými slovy že pořadí obou neurčitých lze navzájem zaměnit, takže je

$$\mathsf{M}[x, y] = \mathsf{M}[y, x].$$

Pro okruh $\mathsf{M}[x, y]$ a pro jeho prvky zavedeme názvy zcela obdobné, jako jsme to učinili v definici 15 pro prvky okruhu $\mathsf{M}[x]$.

Definice 17. Budiž dán okruh M s jednotkovým prvkem. Okruh $\mathsf{M}[x, y]$ všech součtů konečného počtu sčítanců $a_{ij}x^iy^j$, kde $a_{ij} \in \mathsf{M}$, se nazývá *okruh polynomů dvou neurčitých x, y nad okruhem* M, je-li v něm definováno sčítání a násobení v souhlasu s větou 9 a jestliže v něm pro prvek $C \in \mathsf{M}[x, y]$ složený z konečného počtu sčítanců $c_{ij}x^iy^j$ z rovnosti $C = 0$ vyplývá, že $c_{ij} = 0$ pro každé i a pro každé j. Prvky x, y se nazývají *neurčité nad okruhem* M a prvky okruhu $\mathsf{M}[x, y]$ se jmenují *polynomy dvou neurčitých x, y nad okruhem* M. Prvky $a_{ij}x^iy^j$ se nazývají *členy* polynomu; prvek a_{ij} je *koeficient* a číslo $i + j$ *stupeň* členu $a_{ij}x^iy^j$. Prvky a_{ij} se jmenují *koeficienty polynomu*, jehož členy jsou $a_{ij}x^iy^j$. Největší ze stupňů těch členů polynomu, které mají nenulové koeficienty, se nazývá *stupeň polynomu.* Nulový prvek okruhu $\mathsf{M}[x, y]$ se jmenuje *nulový polynom* a nepřisuzujeme mu žádný stupeň.

Je třeba se zamyslet nad tím, jaký význam má sčítání a násobení polynomů dvou neurčitých x, y z okruhu

$\mathsf{M}[x, y]$, které má být podle definice 17 v souhlasu s větou 9.

Je-li v prvku $A \in \mathsf{M}[x, y]$ u mocniny y^j koeficient $A_j \in \mathsf{M}[x]$ a v prvku $B \in \mathsf{M}[x, y]$ u téže mocniny koeficient $B_j \in \mathsf{M}[x]$, je podle věty 9 v prvku $A + B \in \mathsf{M}[x, y]$ u mocniny y^j koeficient $A_j + B_j \in \mathsf{M}[x]$. Je-li v polynomu $A_j \in \mathsf{M}[x]$ u mocniny x^i koeficient $a_{ij} \in \mathsf{M}$ a v polynomu $B_j \in \mathsf{M}[x]$ u téže mocniny koeficient $b_{ij} \in \mathsf{M}$, je podle věty 9 v prvku $A_j + B_j \in \mathsf{M}[x]$ u mocniny x^i koeficient $a_{ij} + + b_{ij} \in \mathsf{M}$. Proto musí být také v prvku $A + B \in \mathsf{M}[x, y]$ u součinu $x^i y^j$ koeficient $a_{ij} + b_{ij} \in \mathsf{M}$, který je součtem koeficientů $a_{ij} \in \mathsf{M}$, $b_{ij} \in \mathsf{M}$ u součinu $x^i y^j$ v prvcích A, B okruhu $\mathsf{M}[x, y]$.

Podobně je v součinu prvků A, B okruhu $\mathsf{M}[x, y]$ podle věty 9 u mocniny y^j součet všech možných součinů $A_m B_n \in \mathsf{M}[x]$, kde $m + n = j$, a v součinu $A_m B_n \in \mathsf{M}[x]$ je podle téže věty u mocniny x^i součet všech možných součinů $a_{km} b_{ln} \in \mathsf{M}$, kde $k + l = i$. Proto musí být také v prvku $AB \in \mathsf{M}[x, y]$ u součinu $x^i y^j$ součet všech možných součinů $a_{km} b_{ln} \in \mathsf{M}$, kde $k + l = i$, $m + n = j$. Ale prvek $a_{km} \in \mathsf{M}$ je koeficient u součinu $x^k y^m$ v polynomu $A \in \mathsf{M}\,[x, y]$ a prvek $b_{ln} \in \mathsf{M}$ je koeficient u součinu $x^l y^n$ v polynomu $B \in \mathsf{M}\,[x, y]$, přičemž je $x^k y^m . x^l y^n = x^{k+l} y^{m+n} = x^i y^j$.

A také podle toho, co bylo řečeno na str. 71 a 72 před definicí 15, pro prvek $C \in \mathsf{M}[x, y]$ nastane rovnost $C = 0$ jen tehdy, je-li $C_j = c_{0j} + c_{1j}x + c_{2j}x^2 + \ldots + c_{rj}x^r = 0$ pro všecka j. Z téhož důvodu nastane pro prvky $C_j \in \mathsf{M}[x]$ rovnost $C_j = 0$ jen tehdy, je-li $c_{ij} = 0$ pro všecka i. Proto z rovnosti $C = 0$ pro polynom $C \in \mathsf{M}[x, y]$ vyplývá rovnost $c_{ij} = 0$ pro všecky koeficienty $c_{ij} \in \mathsf{M}$.

Z toho všeho plyne, že pro polynomy dvou neurčitých x, y nad okruhem M využíváme komutativnosti a asociativnosti sčítání a násobení a distributivnosti násobení vzhledem k sčítání tak, že při sčítání polyr omů sčítáme členy, které mají tytéž mocniny $x^i y^j$, a při násobení polynomů násobíme každý člen jednoho polynomu každým členem druhého. Rovnost dvou polynomů pak nastane právě tehdy, rovnají-li se sobě koeficienty u týchž mocnin $x^i y^j$.

Je-li okruh M oborem integrity, je také okruh $\mathsf{M}[x, y]$ polynomů dvou neurčitých oborem integrity, jak vyplývá dvojnásobným použitím věty 10. Ale obor integrity $\mathsf{M}[x, y]$ polynomů dvou neurčitých není nikdy tělesem, jak bezprostředně vyplývá z věty 11.

Dosazovací pravidlo lze aplikovat pro polynomy dvou neurčitých dvojím způsobem.

Věta 14. Budiž dána rovnost mezi dvěma výrazy složenými z konečného počtu součtů nebo součinů polynomů dvou neurčitých x, y nad okruhem M. Nahradíme-li neurčitou y kterýmkoli prvkem z libovolného okruhu $\mathsf{M}' \supset \mathsf{M}$, dostaneme rovnost mezi polynomy jedné neurčité x nad okruhem M'. Nahradíme-li obě neurčité x, y libovolně zvolenými prvky okruhu $\mathsf{M}' \supset \mathsf{M}$, dostaneme rovnost mezi prvky okruhu M'.

Důkaz. Věta vyplývá bezprostředně z definice sčítání a násobení polynomů dvou neurčitých nad okruhem M. Vezmeme-li libovolný okruh $\mathsf{M}' \supset \mathsf{M}$, pak všecky koeficienty a_{ij}, b_{ij} polynomů A, B z okruhu $\mathsf{M}[x, y]$ patří také do M'. Značí-li také y nějaký prvek okruhu M', jsou výpočty uvedené na str. 65 výpočty v okruhu $\mathsf{M}'[x]$. Tyto výpočty však říkají, že vzorce pro součet a součin polynomů A, B jsou sestaveny tak, aby byly splněny pro každý prvek $y \in \mathsf{M}'$, takže vzniká rovnost mezi polynomy jedné neurčité x okruhu $\mathsf{M}'[x]$. Totéž tvrzení pak platí i pro všecky výrazy složené z konečného počtu součtů a součinů. Druhá část věty je aplikace věty 13 na rovnost mezi polynomy jedné neurčité x z okruhu $\mathsf{M}'[x]$. Přitom ovšem nevylučuje me možnost $\mathsf{M}' = \mathsf{M}$.

Příklad 30. Máme rozhodnout, lze-li rozložit polynom druhého stupně

$$x^2 + 8xy + 4y^2 + 2x - 4y - 2$$

dvou neurčitých x, y nad oborem integrity C celých čísel na součin dvou polynomů prvního stupně. Je-li to možné, musí být

$$x^2 + 8xy + 4y^2 + 2x - 4y - 2 =$$
$$= (a_1x + a_2y + a_3)(b_1x + b_2y + b_3).$$

Koeficienty jsme označili a_1, a_2, a_3, b_1, b_2, b_3, abychom nemuseli psát dvojí indexy. Podle definice rovnosti dvou polynomů musí být

$$\begin{aligned} a_1b_1 &= 1, & a_1b_2 + a_2b_1 &= 8, \\ a_2b_2 &= 4, & a_1b_3 + a_3b_1 &= 2, \\ a_3b_3 &= -2, & a_2b_3 + a_3b_2 &= -4. \end{aligned}$$

Máme řešit tuto soustavu rovnic. Z rovnic v levém sloupci vyplývá jednak to, že existuje-li řešení, jsou všechny koeficienty a_i, b_i různé od nuly, jednak to, že

$$b_1 = \frac{1}{a_1}, \quad b_2 = \frac{4}{a_2}, \quad b_3 = -\frac{2}{a_3}.$$

Dosadíme-li odtud do rovnic v pravém sloupci, dostaneme

$$4 \cdot \frac{a_1}{a_2} + \frac{a_2}{a_1} = 8, \quad -2 \cdot \frac{a_1}{a_3} + \frac{a_3}{a_1} = 2,$$

$$-2 \cdot \frac{a_2}{a_3} + 4 \cdot \frac{a_3}{a_2} = -4$$

a po jednoduché úpravě obdržíme tři kvadratické rovnice

$$\left(\frac{a_2}{a_1}\right)^2 - 8 \cdot \frac{a_2}{a_1} + 4 = 0, \quad \left(\frac{a_3}{a_1}\right)^2 - 2 \cdot \frac{a_3}{a_1} - 2 = 0,$$

$$\left(\frac{a_2}{a_3}\right)^2 - 2 \cdot \frac{a_2}{a_3} - 2 = 0,$$

z nichž vyplývá

$$\frac{a_2}{a_1} = 4 \pm 2\sqrt{3} = (1 \pm \sqrt{3})^2, \quad \frac{a_3}{a_1} = 1 \pm \sqrt{3},$$

$$\frac{a_2}{a_3} = 1 \pm \sqrt{3}.$$

Z toho je vidět, že dané rovnice nelze splnit celými čísly a_1, a_2, a_3, takže daný polynom nelze rozložit v oboru integrity $C[x, y]$.

Rovnice však lze splnit v každém číselném tělese T, které obsahuje číslo $1 + \sqrt{3}$ (a v důsledku toho i číslo $1 - \sqrt{3} = \dfrac{-2}{1 + \sqrt{3}}$). Takovým tělesem je například těleso R reálných čísel. Pokusíme se tedy daný polynom rozložit v oboru integrity $R[x, y]$ polynomů dvou neurčitých x, y nad tělesem reálných čísel. Hodnoty vyplývající z prvních dvou rovnic dávají celkem čtyři myslitelné možnosti:

a) $\dfrac{a_2}{a_1} = (1 + \sqrt{3})^2, \quad \dfrac{a_3}{a_1} = 1 + \sqrt{3},$

$$\frac{a_2}{a_3} = \frac{a_2}{a_1} : \frac{a_3}{a_1} = 1 + \sqrt{3},$$

b) $\dfrac{a_2}{a_1} = (1 + \sqrt{3})^2, \quad \dfrac{a_3}{a_1} = 1 - \sqrt{3},$

$$\frac{a_2}{a_3} = \frac{(1 + \sqrt{3})^2}{1 - \sqrt{3}} = -5 - 3\sqrt{3},$$

c) $\frac{a_2}{a_1} = (1 - \sqrt{3})^2, \quad \frac{a_3}{a_1} = 1 + \sqrt{3},$

$$\frac{a_2}{a_3} = \frac{(1 - \sqrt{3})^2}{1 + \sqrt{3}} = -5 + 3\sqrt{3},$$

d) $\frac{a_2}{a_1} = (1 - \sqrt{3})^2, \quad \frac{a_3}{a_1} = 1 - \sqrt{3}, \quad \frac{a_2}{a_3} = 1 - \sqrt{3}.$

Poněvadž podle třetí rovnice má být

$$\frac{a_2}{a_3} = 1 \pm \sqrt{3},$$

může vyhovovat úloze jen případ a) nebo d). V případě a) je

$$a_1 : a_2 : a_3 = 1 : (4 + 2\sqrt{3}) : (1 + \sqrt{3})$$

a odtud vychází

$$b_1 : b_2 : b_3 = 1 : \frac{4}{4 + 2\sqrt{3}} : \frac{-2}{1 + \sqrt{3}} =$$

$$= 1 : (4 - 2\sqrt{3}) : (1 - \sqrt{3}),$$

takže jeden z hledaných rozkladů je

$$x^2 + 8xy + 4y^2 + 2x - 4y - 2 = [x + (4 +$$

$$+ 2\sqrt{3})y + (1 + \sqrt{3})]\,[x + (4 - 2\sqrt{3})y + (1 - \sqrt{3})].$$

O správnosti se můžeme přesvědčit roznásobením. Další rozklady dostaneme tak, že koeficienty u prvního polynomu znásobíme libovolným reálným číslem $k \neq 0$ a koeficienty druhého polynomu číslem $\frac{1}{k}$. Případ d) vede k témuž výsledku s činiteli navzájem zaměněnými.

Přibráním další neurčité z k okruhu $M[x, y]$ můžeme vytvořit okruh $M[x, y, z]$ polynomů tří neurčitých x, y, z nad okruhem M právě tak, jako jsme vytvořili okruh $M[x, y]$ z okruhu $M[x]$. Obdobně bychom mohli pokračovat dále a tvořit okruhy polynomů ještě většího počtu neurčitých. Polynomy tří neurčitých x, y, z nad okruhem M mají členy tvaru

$$a_{ijk}x^i y^j z^k,$$

kde $a_{ijk} \in M$ a i, j, k jsou přirozená čísla (včetně nuly). Počítáme s nimi opět na základě komutativnosti a asociativnosti sčítání a násobení a na základě distributivnosti násobení vzhledem ke sčítání obdobně jako s polynomy dvou neurčitých.

Cvičení. 61. Ověřte, že pro libovolná (komplexní) čísla a, b, x, y je $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 = (ax - by)^2 + (ay + bx)^2$.

62. Ověřte, že v okruhu $C_2[x, y]$ polynomů dvou neurčitých x, y nad tělesem C_2 zbytkových tříd podle modulu 2 platí: a) $(x + y + 1)^2 = x^2 + y^2 + 1$, b) $(x + y + 1)^4 = x^4 + y^4 + 1$. Přitom znak 1 značí zbytkovou třídu $\{1\}$.

63. Polynom a) $6x^2 - 5xy - 6y^2 + x + 5y - 1$, b) $x^2 + 2xy - y^2 - 6x + 2y + 1$, c) $x^2 + y^2 - 2x + 2y + 2$, d) $x^2 + y^2 + 1$ rozložte na součin dvou polynomů prvního stupně. Nad kterým číselným okruhem je to možné?

64. Jak je třeba volit číslo a, aby polynom $x^2 + 5xy + 6y^2 - x - 5y + a$ byl rozložitelný v součin dvou polynomů prvního stupně? Napište tento rozklad. Nad jakým okruhem je to možné?

65. Tutéž úlohu řešte pro polynom $x^2 - 2xy + 2y^2 + ax - 2y + 1$.

66. Ukažte, že a) polynom r-tého stupně jedné neurčité

má nejvýše $r + 1$ členů různých stupňů, b) polynom r-tého stupně dvou neurčitých má nejvýše $\frac{(r+1)(r+2)}{2}$ členů, z nichž každé dva mají aspoň u jedné neurčité různé exponenty, a že c) polynom r-tého stupně tří neurčitých má takových členů nejvýše $\frac{(r+1)(r+2)(r+3)}{6}$.

67. Ověřte, že pro libovolná (komplexní) čísla a, b, c, x, y, z platí: $(a^2 + b^2 + c^2)(x^2 + y^2 + z^2) = (ax + by + cz)^2 + (ay - bx)^2 + (az - cx)^2 + (bz - cy)^2$.

68. Z předcházejícího cvičení odvoďte, že pro libovolná (komplexní) čísla a, b, c je a) $(a^2 + b^2 + c^2)^2 = (a^2 + b^2 - c^2)^2 + (2ac)^2 + (2bc)^2$, b) $(a^2 + b^2 + c^2)^2 = (ab + bc + ca)^2 + (ac - b^2)^2 + (bc - a^2)^2 + (ab - c^2)^2$.

69. Ověřte, že pro libovolná (komplexní) čísla a, b, c, d, x, y, z, u je $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + u^2) = (ax + by + cz + du)^2 + (au + bz - cy - dx)^2 + (ay - bx + cu - dz)^2 + (az - bu - cx + dy)^2$.

70. Z předcházejícího cvičení odvoďte, že pro libovolná (komplexní) čísla a, b, c, d je a) $(a^2 + b^2 + c^2 + d^2)^2 = (a^2 + b^2 + 2cd)^2 + 2(a^2 + b^2)(c - d)^2 + (c^2 - d^2)^2$, b) $(a^2 + b^2 + c^2 + d^2)^2 = (2ab + 2cd)^2 + (a^2 - b^2 + c^2 - d^2)^2 + (2ad - 2bc)^2$, c) $(a^2 + b^2 + c^2 + d^2)^2 = (a^2 + bc + cd + bd)^2 + (b^2 + ac - cd - ad)^2 + (c^2 + ad - ab - bd)^2 + (d^2 + ab - bc - ac)^2$.

71. Dokažte, že pro libovolná reálná čísla x, y, z je $x^2 + y^2 + z^2 \geqq xy + xz + yz$. Kdy nastane rovnost?

72. Dokažte, že rovnost $x^3 + y^3 + z^3 - 3xyz = 0$ pro tři reálná čísla x, y, z nastane právě tehdy, když buď $x + y + z = 0$, nebo $x = y = z$.

73. Rozložte polynom $x^3 + y^3 + z^3 - 3xyz$ na součin tří polynomů prvního stupně (s komplexními koeficienty).

74. Rozložte polynom $x^4 + y^4 + z^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2$ v součin čtyř činitelů prvního stupně. Nad kterým číselným okruhem je to možné?

75. Je-li M okruh a x, y, z neurčité, odůvodněte, proč $\mathsf{M} \subset \mathsf{M}[x] \subset \mathsf{M}[x, y] \subset \mathsf{M}[x, y, z]$.