5. kapitola. Polynomy jedné neurčité

In: Karel Hruša (author): Polynomy v moderní algebře. (Czech). Praha: Mladá fronta, 1970. pp. 63–83.

Persistent URL: http://dml.cz/dmlcz/403716

5. kapitola

POLYNOMY JEDNÉ NEURČITÉ

Vyjdeme z nějakého okruhu M s jednotkovým prvkem a vezmeme další prvek x, o němž budeme předpokládat, že nepatří do okruhu M. Budeme se snažit sestrojit pokud možno nejméně obsažný okruh $\mathsf{M}[x]$, který obsahuje všecky prvky okruhu M a mimo to ještě prvek x. Slovy „nejméně obsažný okruh" rozumíme takový okruh $\mathsf{M}[x]$, který má tu vlastnost, že každý jiný okruh, který splňuje vyslovené požadavky, ho obsahuje. Existence takového okruhu není předem nikterak zřejmá a je vlastně hlavním výsledkem následujících úvah.

Poněvadž $\mathsf{M}[x]$ má být okruh, musí to být komutativní grupa vzhledem k sčítání a kromě toho v něm musí být definováno násobení kterýchkoli dvou jeho prvků. Musí v něm tedy být obsaženy kromě prvku x i všechny součiny vzniklé opakovaným násobením prvku x, tj. součiny

$$x.x = x^2, \quad x.x.x = x^3, \quad x.x.x.x = x^4$$

atd. K tomu můžeme ještě připojit

$$x^1 = x, \quad x^0 = 1,$$

kde 1 je jednotkový prvek okruhu $\mathsf{M}[x]$. Poněvadž jde o násobení v okruhu $\mathsf{M}[x]$, které je komutativní a asociativní, jsou prvky x^r mocniny prvku x s přirozeným exponentem a platí pro ně vzorce uvedené ve větě 8 a v příkladu 24.

Dále musí být v okruhu $\mathsf{M}[x]$ obsaženy všecky součiny

prvků původního okruhu M a kterékoli mocniny x^i, tj. prvky

$$a_i x^i,$$

kde $a_i \in \mathsf{M}$ a $i \in \mathsf{N}_0$.

Konečně musí být v okruhu $\mathsf{M}[x]$ obsaženy i všecky součty prvků tvaru $a_i x^i$, tj. prvky

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_r x^r,$$

kde $a_0, a_1, a_2, a_3, \ldots, a_r$ jsou prvky okruhu M; přitom píšeme $a_0 x^0 = a_0 . 1 = a_0, a_1 x^1 = a_1 x$ podle definice mocniny s exponentem 0 a 1. Číslo r je prvek množiny N_0 všech přirozených čísel (včetně nuly); pro $r = 0$ má příslušný prvek okruhu $\mathsf{M}[x]$ tvar $a_0 x^0 = a_0$.

Tato úvaha nám ukázala, které prvky musí množina $\mathsf{M}[x]$ nutně obsahovat; dosud však nevíme, nemusí-li obsahovat ještě nějaké další prvky, chceme-li, aby byla okruhem. Nejprve však prostudujeme, které vlastnosti mají prvky, o nichž již víme, že patří do $\mathsf{M}[x]$.

Především je třeba si uvědomit, že jsme sice již od počátku této úvahy užívali v našich zápisech znaků sčítání a násobení, ale vůbec jsme nedefinovali, co máme rozumět sčítáním a násobením v okruhu $\mathsf{M}[x]$; naše dosavadní zápisy jsou prozatím jen prázdné formy bez konkrétního obsahu. To musíme napravit.

Při svých úvahách jsme vyšli z jakéhosi okruhu M, ve kterém ovšem je definováno sčítání i násobení; kromě toho z věty 8 víme, jak se násobí mocniny prvku x s přirozeným mocnitelem. Tyto naše znalosti nám umožní definovat sčítání a násobení mezi dosud známými prvky okruhu $\mathsf{M}[x]$.

Poněvadž jde o okruh, musí v něm být sčítání a násobení komutativní a asociativní a kromě toho musí být násobení distributivní vzhledem ke sčítání. Jsou-li tedy

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_r x^r = A,$$
$$b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \ldots + b_s x^s = B$$

dva prvky množiny $\mathsf{M}[x]$, musí pro jejich součet za předpokladu, že $s = r$, platit

$$(a_0 + a_1x + a_2x^2 + \ldots + a_rx^r) + (b_0 + b_1x + b_2x^2 + \\ + \ldots + b_rx^r) = (a_0 + b_0) + (a_1x + b_1x) + (a_2x^2 + \\ + b_2x^2) + \ldots + (a_rx^r + b_rx^r) = (a_0 + b_0) + (a_1 + \\ + b_1)\,x + (a_2 + b_2)\,x^2 + \ldots + (a_r + b_r)\,x^r.$$

Předpoklad $s = r$ není na závadu obecnosti; kdyby bylo například $s < r$, mohli bychom v druhém prvku doplnit další sčítance tvaru $0.x^i = 0$ pro $s < i \leqq r$.

Obdobně dostáváme pro součin

$$(a_0 + a_1x + a_2x^2 + \ldots + a_rx^r)\,(b_0 + b_1x + b_2x^2 + \ldots + b_sx^s) =$$

$$= a_0b_0 + a_1b_0x + a_2b_0x^2 + \ldots + a_rb_0x^r + \\ + a_0b_1x + a_1b_1x^2 + a_2b_1x^3 + \ldots + a_rb_1x^{r+1} + \\ + a_0b_2x^2 + a_1b_2x^3 + a_2b_2x^4 + \ldots + a^rb_2x^{r+2} + \\ + \ldots\ldots\ldots\ldots\ldots\ldots + \\ + a_0b_sx^s + a_1b_sx^{s+1} + a_2b_sx^{s+2} + \ldots + a_rb_sx^{r+s} =$$

$$= c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots\ldots + c_{r+s}x^{r+s},$$

kde

$$c_0 = a_0b_0,\ c_1 = a_1b_0 + a_0b_1,\ c_2 = a_2b_0 + a_1b_1 + a_0b_2,$$

$$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3,\ \ldots,\ c_{r+s} = a_rb_s.$$

Přitom je prvek c_i vyjádřen jako součet všech možných součinů a_jb_k, kde $j + k = i$.

Věta 9. Budiž dán okruh M s jednotkovým prvkem a prvek x, který do okruhu M nepatří. Budiž dále $\mathsf{M}[x]$ množina všech prvků

$$a_0 + a_1x + a_2x^2 + \ldots + a_rx^r,$$

kde $a_0, a_1, a_2, \ldots, a_r$ jsou prvky okruhu M. Je-li v množině M $[x]$ definováno sčítání vzorcem

$$(a_0 + a_1x + a_2x^2 + \ldots + a_rx^r) + (b_0 + b_1x + b_2x^2 + \\ + \ldots + b_rx^r) = (a_0 + b_0) + (a_1 + b_1)\,x + (a_2 + b_2)x^2 + \\ + \ldots + (a_r + b_r)x^r$$

a násobení vzorcem

$$(a_0 + a_1x + a_2x^2 + \ldots + a_rx^r)\,(b_0 + b_1x + b_2x^2 + \\ + \ldots + b_sx^s) = c_0 + c_1x + c_2x^2 + \ldots + c_{r+s}x^{r+s},$$

kde $c_0 = a_0b_0$, $c_1 = a_1b_0 + a_0b_1$, $c_2 = a_2b_0 + a_1b_1 + a_0b_2$, $\ldots$, $c_{r+s} = a_rb_s$, je množina M $[x]$ okruh.

Důkaz. Nejprve je třeba ověřit, že to, co se ve větě 9 nazývá sčítáním a násobením, je opravdu hodné těchto názvů, tj. že tyto výkony splňují požadavky vyslovené v definici 7.

Z vyslovené definice je především patrné, že ke každým dvěma prvkům množiny M $[x]$ existuje v této množině jejich součet i součin.

Komutativnost sčítání se ověří okamžitě: obrátíme-li pořadí sčítanců A, B, obrátí se i pořadí sčítanců ve výrazech $a_i + b_i$, ale to nemá vliv na výsledný součet, neboť v okruhu M je $b_i + a_i = a_i + b_i$. Je tedy $A + B = B + A$.

Obdobné tvrzení platí i pro součin: záměnou pořadí činitelů A, B se ve výrazu pro c_i zamění pouze pořadí sčítanců, z nichž je prvek c_i tvořen, neboť v okruhu M je $b_ka_j = a_jb_k$. Proto je $AB = BA$.

Ani ověření asociativnosti sčítání nepůsobí potíže. Přibereme-li k daným prvkům A, B ještě prvek

$$c_0 + c_1x + c_2x^2 + \ldots + c_ix^i = C,$$

pak součet $(A + B) + C$ má sčítance tvaru $[(a_i + b_i) + c_i]x^i$ a součet $A + (B + C)$ sčítance tvaru $[a_i + (b_i +$

$+ c_i)]x^i$, ale to je totéž vzhledem k tomu, že v okruhu M je $(a_i + b_i) + c_i = a_i + (b_i + c_i)$. Proto je $(A + B) + C = A + (B + C)$.

Poněkud složitější je ověření asociativnosti násobení. Poněvadž v součinu AB je mocnina x^i doprovázena součtem všech možných sčítanců tvaru $a_j b_k$, kde $j + k = i$, je v součinu $(AB)C$ mocnina x^h doprovázena součtem všech možných sčítanců $(a_j b_k)c_l$, kde $j + k = i$, $i + l = h$, neboli $j + k + l = h$. Podobně v součinu BC je mocnina x^m doprovázena součtem všech možných sčítanců $b_k c_l$, kde $k + l = m$; musí tedy být v součinu $A(BC)$ mocnina x^h doprovázena součtem všech možných sčítanců $a_j (b_k c_l)$, kde $k + l = m$, $j + m = h$, čili zase $j + k + l = h$. Avšak v okruhu M je $(a_j b_k)c_l = a_j (b_k c_l)$; proto také součet všech možných sčítanců tvaru $(a_j b_k)c_l$, kde $j + k + l = h$, je roven součtu všech možných sčítanců tvaru $a_j (b_k c_l)$, kde opět $j + k + l = h$, takže $(AB)C = A(BC)$.

Zbývá ještě ověřit distributivnost násobení vzhledem ke sčítání. V součinu $(A + B)C$ je mocnina x^i doprovázena součtem všech možných sčítanců tvaru $(a_j + b_j)c_k$, kde $j + k = i$, a v součtu $AC + BC$ je u x^i součet všech možných výrazů $a_j c_k + b_j c_k$, kde zase $j + k = i$. Ale v okruhu M je $(a_j + b_j)c_k = a_j c_k + b_j c_k$, a proto je $(A + B)C = AC + BC$.

Tím jsme ukázali, že jsou splněny všecky požadavky z definice 7 a že množina M $[x]$ s uvedenými operacemi je polookruh. Abychom ukázali, že to je okruh, musíme podle definice 8 ověřit, že tvoří aditivní grupu, tj. podle definice 6, že v polookruhu M $[x]$ existuje nulový prvek a že ke každému jeho prvku existuje opačný prvek.

Nulovým prvkem polookruhu M $[x]$ je prvek

$$0 = 0 + 0.x + 0.x^2 + \ldots + 0.x^r,$$

neboť podle definice sčítání je

$$A + 0 \quad (a_0 + 0) + (a_1 + 0)x + (a_2 + 0)x^2 + (a_r + 0)x^r = A.$$

Tento nulový prvek je ovšem totožný s nulovým prvkem okruhu M, neboť $M \subset M[x]$ a nulový prvek může být podle věty 1 nejvýš jeden.

Opačný prvek k prvku A vždy existuje a je jím prvek

$$-A = (-a_0) + (-a_1)x + (-a_2)x^2 + \ldots + (-a_r)x^r,$$

neboť

$$A + (-A) = [a_0 + (-a_0)] + [a_1 + (-a_1)]x + [a_2 + (-a_2)]x^2 + \ldots + [a_r + (-a_r)]x^r = 0 + 0.x + 0.x^2 + \ldots + 0.x^r = 0.$$

Tím jsme ověřili, že množina $M[x]$ s uvedenými operacemi je skutečně okruh. Zároveň je vidět, že tento okruh $M[x]$ je nejméně obsažný ze všech okruhů, které obsahují všecky prvky okruhu M a mimo to ještě prvek x. Každý takový okruh totiž musí podle toho, co jsme řekli na počátku tohoto článku, obsahovat všecky prvky

$$a_0 + a_1x + a_2x^2 + \ldots + a_rx^r,$$

a ty okruh $M[x]$ skutečně obsahuje. Má-li být co nejméně obsažný, nesmí už obsahovat žádné další. Je tedy okruh $M[x]$ skutečně ten, jehož nalezení jsme si položili za cíl na počátku tohoto článku.

K nalezeným výsledkům ještě připojíme několik dodatků.

Protože je $M[x]$ okruh, existuje v něm podle věty 3 rozdíl $A - B$ kterýchkoli dvou prvků A, B a je

$$A - B = A + (-B) = [a_0 + (-b_0)] + [a_1 + (-b_1)]x + [a_2 + (-b_2)]x^2 + \ldots + [a_r + (-b_r)]x^r = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \ldots + (a_r - b_r)x^r.$$

O okruhu M v celém tomto článku předpokládáme, že má jednotkový prvek. Proto i okruh M[x] má jednotkový prvek a je jím prvek

$$1 = 1 + 0.x + 0.x^2 + \ldots + 0.x^s.$$

Pro $B = 1$ totiž je $b_0 = 1$, $b_1 = b_2 = \ldots = b_s = 0$, takže v součinu $A.1$ se součet všech sčítanců $a_j b_k$, kde $j + k = i$, který je u mocniny x^i, redukuje na jediný prvek $a_i b_0 = a_i.1 = a_i$, kdežto všecky ostatní sčítance tohoto součtu jsou nulové. Je tedy

$$A.1 = a_0 + a_1 x + a_2 x^2 + \ldots + a_r x^r = A.$$

Tento jednotkový prvek je totožný s jednotkovým prvkem okruhu M, jehož existenci předpokládáme, vzhledem k tomu, že M $\subset$ M[x] a jednotkový prvek může být podle věty 1 nejvýš jeden.

Ještě si musíme všimnout toho, co vlastně znamená rovnost prvků okruhu M[x]. Je-li $a_i = b_i$ pro každé i, pak zřejmě pro příslušné prvky A, B okruhu M[x] je $A = B$, neboť jde o jeden a týž prvek. Je-li obráceně $A = B$, znamená to, že $A - B = 0$, tj.

$$(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \ldots + (a_r - b_r)x^r = 0.$$

Budeme předpokládat, že tuto rovnost lze splnit jen tak, že pro každé i je $a_i - b_i = 0$ a že tedy $a_i = b_i$. Tento předpoklad však z našich předcházejících úvah nijak neplyne; bylo by možné volit prvek x tak, aby existovalo takové přirozené číslo r a takové prvky $c_0, c_1, c_2, \ldots, c_r$ okruhu M, které by nebyly vesměs nulové, a přesto by bylo

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_r x^r = 0.$$

Pak by se ovšem mohlo stát, že by pro prvky A, B okruhu M[x] bylo $A = B$ přesto, že pro některé i by bylo $a_i \neq$

$\neq b_i$. Tuto možnost však ve svých dalších úvahách vyloučíme.

Abychom ukázali, že vyloučený případ může opravdu nastat, uvedeme příklad.

Příklad 25. Za okruh M zvolíme okruh C všech celých čísel a za prvek x vezmeme číslo $x = \sqrt{2} + \sqrt{3}$. Zřejmě $x \notin C$, takže pro okruh C a pro číslo x platí všecky dosavadní výsledky tohoto článku, pokud se týkají sčítání a násobení prvků okruhu $C[x]$. Poněvadž

$$x^2 = 5 + 2\sqrt{6}, \quad x^3 = 11\sqrt{2} + 9\sqrt{3}, \quad x^4 = 49 + 20\sqrt{6},$$

je například

$$A = 1 + 2x - 5x^2 + x^3 =$$

$$= 1 + 2(\sqrt{2} + \sqrt{3}) - 5(5 + 2\sqrt{6}) + (11\sqrt{2} + 9\sqrt{3}) =$$

$$= -24 + 13\sqrt{2} + 11\sqrt{3} - 10\sqrt{6},$$

$$B = 2x + 5x^2 + x^3 - x^4 =$$

$$= 2(\sqrt{2} + \sqrt{3}) + 5(5 + 2\sqrt{6}) + (11\sqrt{2} + 9\sqrt{3}) -$$

$$- (49 + 20\sqrt{6}) = -24 + 13\sqrt{2} + 11\sqrt{3} - 10\sqrt{6}.$$

Je tedy $A = B$ přesto, že $a_0 = 1$, $a_1 = 2$, $a_2 = -5$, $a_3 = 1$, $a_4 = 0$, $b_0 = 0$, $b_1 = 2$, $b_2 = 5$, $b_3 = 1$, $b_4 = -1$, takže $a_0 \neq b_0$, $a_2 \neq b_2$, $a_4 \neq b_4$. Utvoříme-li rozdíl $A - B$, shledáme, že

$$A - B = 1 - 10x^2 + x^4 = 0,$$

takže $A - B = 0$ a přitom $1 \neq 0$, $-10 \neq 0$, $1 \neq 0$. To je způsobeno tím, že jsme za x volili číslo $\sqrt{2} + \sqrt{3}$, které je kořenem rovnice

$$x^4 - 10x^2 + 1 = 0.$$

A nakonec ještě jednu poznámku. Mohlo by se snad zdát, že máme v okruhu $M[x]$ dvojí sčítání a dvojí násobení:

jednak to, které bylo zavedeno ve větě 9 mezi prvky okruhu $\mathsf{M}[x]$, jednak to, které je „uvnitř" jednotlivých prvků okruhu $\mathsf{M}[x]$, tj. sčítání typu $a_i x^i + a_j x^j$ a násobení prvku $a_i \in \mathsf{M}$ mocninou x^i. Ale není tomu tak, neboť můžeme položit

$$a_i x^i = a_i x^i + 0.x^j, \; a_j x^j = 0.x^i + a_j x^j.$$

Ostatní sčítance, které jsou nulové, nepíšeme. Pak je podle definice sčítání

$$(a_i x^i + 0.x^j) + (0.x^i + a_j x^j) =$$
$$= (a_i + 0)x^i + (0 + a_j)x^j = a_i x^i + a_j x^j,$$

takže znaménko + mezi jednotlivými sčítanci prvku z $\mathsf{M}[x]$ má týž význam jako znaménko + mezi prvky okruhu $\mathsf{M}[x]$. Podobně je tomu ve druhém případě. Prvek $a_i \in \mathsf{M}$ můžeme psát ve tvaru

$$a_i = a_0' + a_1' x + a_2' x^2 + \ldots + a_r' x^r,$$

v němž je $a_0' = a_i$ a pro všecky ostatní indexy j je $a_j' = 0$, a prvek x^i ve tvaru

$$x^i = b_0 + b_1 x + b_2 x^2 + \ldots + b_s x^s,$$

v němž je $b_i = 1$ a pro všecky ostatní indexy k je $b_k = 0$. Pak podle definice násobení je

$$a_i x^i = c_0 + c_1 x + c_2 x^2 + \ldots + c_{r+s} x^{r+s}.$$

Tu je $c_i = a_0' b_i = a_i . 1 = a_i$, neboť všecky ostatní sčítance součtu, kterým je vyjádřen prvek c_i, jsou nulové. Mimoto pro všecky ostatní indexy j je $c_j = 0$. Má tedy i (vynechané) znaménko násobení ve výrazu $a_i x^i$ týž význam jako znaménko násobení mezi prvky okruhu $\mathsf{M}[x]$.

Dosud jsme ještě vůbec nic neřekli o prvku x kromě toho, že nepatří do okruhu M a že splňuje rovnost

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_r x^r = 0$$

jen tehdy, je-li $c_0 = c_1 = c_2 = \ldots = c_r = 0$. Prvou z těchto podmínek však můžeme vynechat, neboť je obsažena ve druhé. Kdyby totiž bylo $x \in \mathsf{M}$, bylo by $x = a$, kde $a \in \mathsf{M}$, a odtud by plynulo

$$a - 1.x = 0, \text{ kde } -1 \neq 0.$$

To však odporuje druhé naší podmínce. Kromě toho by pro $x \in \mathsf{M}$ patřily do M i všecky mocniny x^i a s nimi i všecky prvky okruhu $\mathsf{M}[x]$, takže by bylo $\mathsf{M}[x] = \mathsf{M}$ a nedostali bychom nic nového.

Ani v dalších úvahách nebudeme charakter prvku x nijak blíže specifikovat; tím se tento prvek stane do jisté míry prázdným schématem a počítání s ním nabude jisté formálnosti.

Definice 15. Budiž dán okruh M s jednotkovým prvkem. Okruh $\mathsf{M}[x]$ všech prvků

$$a_0 + a_1x + a_2x^2 + \ldots + a_rx^r,$$

kde $a_0, a_1, a_2, \ldots, a_r$ jsou prvky okruhu M, se nazývá *okruh polynomů jedné neurčité x nad okruhem* M, je-li v něm definováno sčítání a násobení tak jako ve větě 9 a jestliže v něm z rovnosti

$$c_0 + c_1x + c_2x^2 + \ldots + c_rx^r = 0$$

vyplývá, že $c_0 = c_1 = c_2 = \ldots = c_r = 0$. Prvek x má název *neurčitá nad okruhem* M a prvky okruhu $\mathsf{M}[x]$ se jmenují *polynomy* (*mnohočleny*) *jedné neurčité x nad okruhem* M. Prvky a_ix^i se nazývají *členy* polynomu; prvek a_i se nazývá *koeficient* a číslo i *stupeň členu* a_ix^i. Prvky $a_0, a_1, a_2, \ldots, a_r$ se jmenují *koeficienty polynomu*

$$a_0 + a_1x + a_2x^2 + \ldots + a_rx^r.$$

Největší ze stupňů těch členů, které mají nenulové koefi-

cienty, se nazývá *stupeň polynomu*. Nulový prvek okruhu $M[x]$ se jmenuje *nulový polynom* a nepřisuzujeme mu žádný stupeň.

Podle toho, co jsme řekli již dříve, je součet, rozdíl i součin dvou polynomů z okruhu $M[x]$ zase polynom z okruhu $M[x]$. Je-li jeden z obou polynomů stupně r-tého a druhý stupně s-tého, pak jejich součet a rozdíl je stupně nejvýše rovného největšímu z obou čísel r, s a jejich součin je stupně nejvýše rovného součtu $r + s$. Může se totiž stát, že ve výsledku vyjde u jednoho nebo několika členů nejvyššího stupně nulový koeficient, a pak je stupeň výsledného polynomu nižší, než udává vzorec pro sčítání, odčítání nebo násobení polynomů. Při násobení to však může nastat jen tehdy, má-li okruh M dělitele nuly. Přitom považujeme nulový polynom za polynom stupně nižšího než kterýkoli nenulový polynom. Součet a rozdíl dvou polynomů, z nichž jeden je nulový, je ovšem téhož stupně jako druhý z obou polynomů; součin dvou polynomů, z nichž jeden je nulový, je zase polynom nulový.

Příklad 26. Za okruh M vezmeme okruh C_6 zbytkových tříd podle modulu 6 (viz příklad 16 na str. 41), jeho prvky však budeme označovat pouze znaky 0, 1, 2, 3, 4, 5, abychom si zjednodušili zápisy. V tomto okruhu se počítá podle tabulek uvedených na str. 45. Okruh $C_6[x]$ polynomů jedné neurčité x nad okruhem C_6 obsahuje polynomy neurčité x s koeficienty z okruhu C_6. V tomto okruhu například je

$$(1 + 2x + 3x^2 + 4x^3 + 5x^4) + (5 + 4x + 3x^2 + 2x^3 + x^4) =$$
$$= (1 + 5) + (2 + 4)x + (3 + 3)x^2 + (4 + 2)x^3 +$$
$$+ (5 + 1)x^4 = 0 + 0.x + 0.x^2 + 0.x^3 + 0.x^4 = 0,$$

neboť podle tabulky je $1 + 5 = 0$, $2 + 4 = 0$, $3 + 3 = 0$, $4 + 2 = 0$, $5 + 1 = 0$. V okruhu $C_6[x]$ je dále

$$(1 + 2x + 3x^2 + 4x^3 + 5x^4) - (5 + 4x + 3x^2 + 2x^3 + x^4) =$$
$$= (1 - 5) + (2 - 4)x + (3 - 3)x^2 + (4 - 2)x^3 +$$
$$+ (5 - 1)x^4 = 2 + 4x + 2x^3 + 4x^4,$$

neboť v okruhu C_6 je $1 - 5 = 2$, $2 - 4 = 4$, $3 - 3 = 0$, $4 - 2 = 2$, $5 - 1 = 4$. Obdobně počítáme

$$(3 + 2x + 4x^2)(1 + 3x + 3x^2) =$$
$$= 3.1 + 2.1x + 4.1x^2 +$$
$$+ 3.3x + 2.3x^2 + 4.3x^3 +$$
$$+ 3.3x^2 + 2.3x^3 + 4.3x^4 =$$
$$= 3 + 5x + x^2,$$

neboť podle tabulek je $3.1 = 3$, $2.1 + 3.3 = 2 + 3 = 5$, $4.1 + 2.3 + 3.3 = 4 + 0 + 3 = 1$, $4.3 + 2.3 = 0 + 0 = 0$, $4.3 = 0$.

Má-li okruh M dělitele nuly, má je ovšem i okruh $M[x]$ polynomů jedné neurčité x nad okruhem M. Jsou-li totiž a, b prvky okruhu M, pro něž platí $a \neq 0$, $b \neq 0$, ale $ab = 0$, platí to i v okruhu $M[x]$, neboť každý prvek z okruhu M je polynomem z okruhu $M[x]$ a prvky a, b jsou tedy děliteli nuly i v okruhu $M[x]$.

Pro praktické počítání má největší význam případ, kdy okruh M je oborem integrity. To nastane například vždy, je-li okruh M číselným okruhem.

Věta 10. Okruh polynomů jedné neurčité nad oborem integrity je také obor integrity.

Důkaz. Je-li okruh M oborem integrity, znamená to podle definice 11, že v něm neexistují dělitelé nuly, tj. že

v něm pro každé $a_r \neq 0$ a pro každé $b_s \neq 0$ je $a_r b_s \neq 0$. Každý nenulový polynom okruhu $\mathsf{M}[x]$ má aspoň jeden nenulový člen. Je-li nenulový polynom A r-tého stupně, má nenulový člen $a_r x^r$, kde $a_r \neq 0$. Je-li nenulový polynom B s-tého stupně, má nenulový člen $b_s x^s$, kde $b_s \neq 0$. Součin AB obou polynomů pak má také nenulový člen $c_{r+s} x^{r+s}$, neboť $c_{r+s} = a_r b_s \neq 0$, takže polynom AB je také nenulový.

Podle toho tedy součin dvou polynomů jedné neurčité nad oborem integrity, z nichž jeden je stupně r-této a druhý stupně s-tého, je stupně právě $(r + s)$-tého.

Je-li okruh M těleso, je to podle věty 7 také obor integrity, a proto podle právě dokázané věty 10 je oborem integrity i okruh polynomů jedné neurčité nad tělesem.

Vzniká otázka, je-li možné, aby okruh polynomů jedné neurčité byl tělesem.

Věta 11. Okruh polynomů $\mathsf{M}[x]$ jedné neurčité x nad okruhem M není nikdy těleso.

Důkaz. Má-li být okruh polynomů $\mathsf{M}[x]$ jedné neurčité x nad okruhem M těleso, musí být okruh M oborem integrity; kdyby totiž měl okruh M dělitele nuly, měl by je i okruh $\mathsf{M}[x]$ a nemohl by být podle věty 7 tělesem. Je-li však M obor integrity, neexistuje v oboru integrity $\mathsf{M}[x]$ převrácený prvek $A^{-1} = B$ k žádnému polynomu A, který je stupně $r \geqq 1$. Kdyby takový prvek B existoval, muselo by pro něj platit

$$AB = 1,$$

neboť prvek 1 je jednotkový prvek oboru integrity M i oboru integrity $\mathsf{M}[x]$. Polynom B nemůže být nulový; kdyby tomu tak bylo, bylo by $AB = 0$. Musí tedy být nenulový a pro jeho stupeň s platí $s \geqq 0$. Součin AB obou polynomů

pak je podle poznámky za větou 10 stupně $r + s \geq 1$, ale to není možné, neboť musí být roven jednotkovému prvku 1, což je polynom stupně nultého z $M[x]$.

Odtud podle věty 3 vyplývá, že v žádném okruhu polynomů jedné neurčité není možno bez omezení dělit, tj. že k libovolným polynomům $A \neq 0$, B tohoto okruhu nemusí v tomto okruhu existovat takový polynom X, aby bylo

$$AX = B.$$

Platí však věta poněkud obecnější:

Věta 12. V oboru integrity $T[x]$ polynomů jedné neurčité x nad tělesem T existuje ke každým dvěma polynomům $A \neq 0$, B právě jedna dvojice polynomů Q, R, pro niž platí

$$AQ + R = B,$$

přičemž polynom R je nižšího stupně než polynom A (nebo je nulový).

Důkaz této věty nebudeme provádět obecně, ale ukážeme ho na speciálním příkladu, z něhož však bude patrné, že by probíhal úplně stejně pro kterékoli polynomy $A \neq 0$, B z oboru integrity $T[x]$ polynomů jedné neurčité x nad kterýmkoli tělesem T.

Příklad 27. Za těleso T zvolíme těleso Q racionálních čísel a v oboru integrity $Q[x]$ polynomů s racionálními koeficienty zvolíme

$$A = 2 + 3x - 5x^2, \quad B = 3 - 4x - 6x^3 + 10x^4.$$

K nalezení polynomů Q, R použijeme způsobu, který se v literatuře běžně označuje názvem *metoda neurčitých koeficientů* nebo také *metoda porovnávání koeficientů*. Polynom A je v našem příkladu druhého stupně, polynom B čtvrtého

stupně; hledaný polynom Q tedy musí být druhého stupně a polynom R nejvýše prvního stupně, tj.

$$Q = q_0 + q_1x + q_2x^2,\ R = r_0 + r_1x,$$

kde q_0, q_1, q_2, r_0, r_1 jsou (dosud neznámé) prvky tělesa Q, přičemž

$$(2 + 3x - 5x^2)(q_0 + q_1x + q_2x^2) + (r_0 + r_1x) = \\ = 3 - 4x - 6x^3 + 10x^4.$$

Rozepíšeme-li napsané výkony podle definice násobení a sčítání, dostaneme podmínku

$$(2q_0 + r_0) + (3q_0 + 2q_1 + r_1)x + \\ + (-5q_0 + 3q_1 + 2q_2)x^2 + (-5q_1 + 3q_2)x^3 - \\ - 5q_2x^4 = 3 - 4x - 6x^3 + 10x^4.$$

Poněvadž má být polynom na levé straně roven polynomu na pravé straně, musí podle toho, co jsme řekli o rovnosti polynomů, být

$$\begin{aligned} 2q_0 \qquad\quad + r_0 \qquad &= 3, \\ 3q_0 + 2q_1 \qquad + r_1 &= -4, \\ -5q_0 + 3q_1 + 2q_2 \qquad &= 0, \\ -5q_1 + 3q_2 \qquad &= -6, \\ -5q_2 \qquad &= 10. \end{aligned}$$

Z těchto rovnic postupně vyjde (zdola nahoru)

$$q_2 = -\frac{10}{5} = -2, \quad q_1 = \frac{6 + 3q_2}{5} = 0,$$

$$q_0 = \frac{3q_1 + 2q_2}{5} = -\frac{4}{5},$$

$$r_1 = -4 - 3q_0 - 2q_1 = -\frac{8}{5}, \quad r_0 = 3 - 2q_0 = \frac{23}{5}.$$

Má-li daná úloha řešení, mohou jím být pouze polynomy

$$Q = \frac{4}{5} - 2x^2, \quad R = \frac{23}{5} - \frac{8}{5}x.$$

Zkouškou se snadno přesvědčíme, že nalezené polynomy úloze vyhovují. Jiné řešení úloha nemá.

Definice 16. Nechť polynomy $A \neq 0$, B, Q, R jedné neurčité splňují rovnost

$$AQ + R = B,$$

přičemž polynom R je nižšího stupně než polynom A (nebo je nulový). Pak se polynom Q nazývá *neúplný podíl* při dělení polynomu B polynomem A (v tomto pořadí) a polynom R *zbytek*. Postup, kterým se určují prvky Q, R na základě daných prvků A, B, se nazývá *dělení se zbytkem*.

Věta 12 tedy hovoří o tom, že v oboru integrity $T[x]$ polynomů jedné neurčité x nad tělesem T je vždy možno dělit se zbytkem libovolný polynom nenulovým polynomem. Požadavek, že jde o obor integrity polynomů nad tělesem, je přitom podstatný; kdybychom vzali místo tělesa T jen okruh nebo obor integrity, který není tělesem, mohlo by se stát, že by soustava rovnic, k níž jsme došli v příkladu 27, nemusela mít v tomto okruhu řešení. Pak by ovšem neexistoval ani neúplný podíl, ani zbytek.

Takový případ nastane například tehdy, jde-li o polynomy s celočíselnými koeficienty, tj. o polynomy nad oborem integrity C celých čísel. V oboru integrity $C[x]$ polynomů s celočíselnými koeficienty není možné dělení se zbytkem (s výjimkou některých speciálních případů).

Ve všech předcházejících úvahách o polynomech znamenalo písmeno x neurčitou, tj. jakýsi blíže nespecifikovaný

prvek, o němž víme, že nepatří do okruhu M, z něhož bereme koeficienty polynomů, a s nímž dovedeme počítat podle jistých dohodnutých pravidel. Je však možné do rovností obsahujících polynomy dosadit za neurčitou x libovolně zvolený prvek z libovolného okruhu M', který obsahuje všecky prvky okruhu M, jak říká následující věta.

Věta 13. (*Dosazovací pravidlo.*) Budiž dána rovnost mezi dvěma výrazy složenými z konečného počtu součtů nebo součinů polynomů jedné neurčité nad okruhem M. Tato rovnost zůstane zachována, nahradíme-li neurčitou kterýmkoli prvkem z libovolného okruhu $M' \supset M$.

Důkaz této věty jsme vlastně již provedli na str. 65, když jsme uvažovali o tom, jak máme definovat sčítání a násobení v okruhu $M[x]$. Vezmeme-li libovolný okruh $M' \supset M$, pak všechny koeficienty a_i, b_i polynomů A, B patří také do M'. Značí-li také písmeno x nějaký prvek okruhu M', pak oba výpočty uvedené na str. 65 jsou výpočty v okruhu M'. Tyto výpočty říkají, že vzorce definující součet a součin polynomů A, B jsou sestaveny tak, aby byly splněny pro každý prvek $x \in M'$. Totéž tvrzení pak zřejmě platí i pro všechny výrazy složené z konečného počtu součtů nebo součinů. Přitom ovšem nevylučujeme možnost dosazovat za x i prvky okruhu M vzhledem k tomu, že $M' \supset M$.

Příklad 28. V příkladu 27 na str. 76 jsme zjistili, že v oboru integrity $Q[x]$ polynomů jedné neurčité x s racionálními koeficienty platí

$$(2 + 3x - 5x^2)\left(-\frac{4}{5} - 2x^2\right) + \left(\frac{23}{5} - \frac{8}{5}x\right) =$$

$$= 3 - 4x - 6x^3 + 10x^4.$$

Tato rovnost nebude podle věty 13 porušena, dosadíme-li za x libovolné číslo z nějakého okruhu $\mathsf{M}' \supset \mathsf{Q}$. Zvolíme-li například $x = 1 - \sqrt{2}$, což je číslo z tělesa R reálných čísel, pro něž $\mathsf{R} \supset \mathsf{Q}$, dostaneme vzhledem k tomu, že

$$(1 - \sqrt{2})^2 = 3 - 2\sqrt{2},\ (1 - \sqrt{2})^3 = 7 - 5\sqrt{2},$$
$$(1 - \sqrt{2})^4 = 17 - 12\sqrt{2},$$

na levé straně číslo

$$(2 + 3 - 3\sqrt{2} - 15 + 10\sqrt{2})\left(-\frac{4}{5} - 6 + 4\sqrt{2}\right) +$$
$$+ \frac{23}{5} - \frac{8}{5} + \frac{8}{5}\sqrt{2} =$$
$$= (-10 + 7\sqrt{2})\left(-\frac{34}{5} + 4\sqrt{2}\right) + 3 + \frac{8}{5}\sqrt{2} =$$
$$= 68 - \frac{238}{5}\sqrt{2} - 40\sqrt{2} + 56 + 3 + \frac{8}{5}\sqrt{2} = 127 - 86\sqrt{2}$$

a na pravé straně číslo

$$3 - 4 + 4\sqrt{2} - 42 + 30\sqrt{2} + 170 - 120\sqrt{2} =$$
$$= 127 - 86\sqrt{2},$$

což potvrzuje správnost uvedené věty.

Dosazovací pravidlo dává i jinou možnost vypočítat neznámé koeficienty polynomů, než která byla uvedena v příkladu 27.

Příklad 29. Hledáme neznámé koeficienty q_0, q_1, q_2, r_0, r_1 tak, aby byla splněna rovnost

$$(2 + 3x - 5x^2)(q_0 + q_1x + q_2x^2) + (r_0 + r_1x) =$$
$$= 3 - 4x - 6x^3 + 10x^4,$$

kterou jsme měli již v příkladu 27. Dosadíme-li za x libovolné číslo nějakého okruhu $M' \supset Q$, dostaneme rovnici s pěti neznámými q_0, q_1, q_2, r_0, r_1. Provedeme-li to celkem pro 5 různých čísel x, dostaneme soustavu pěti rovnic, z nichž lze uvedené neznámé vypočítat. Za x budeme postupně dosazovat čísla: 1, $-\frac{2}{5}$, 0, -1 a 2. Dovede nás to k soustavě

$$\begin{aligned} r_0 + r_1 &= 3, \\ r_0 - \frac{2}{5} r_1 &= \frac{131}{25}, \\ 2q_0 + r_0 &= 3, \\ -6q_0 + 6q_1 - 6q_2 + r_0 - r_1 &= 23, \\ -12q_0 - 24q_1 - 48q_2 + r_0 + 2r_1 &= 107. \end{aligned}$$

První dvě hodnoty pro x jsme volili tak, aby pro ně bylo $2 + 3x - 5x^2 = 0$, aby tak vyšly co nejjednodušší rovnice; týž zřetel nás vedl při volbě hodnoty $x = 0$. Další hodnoty pak byly voleny celkem libovolně. Z prvých dvou rovnic vychází

$$r_0 = \frac{23}{5}, \quad r_1 = -\frac{8}{5},$$

z třetí dostáváme

$$q_0 = -\frac{4}{5},$$

a dosadíme-li tyto hodnoty do posledních dvou rovnic, vyjde

$$q_1 = 0, \quad q_2 = -2.$$

Tyto výsledky jsou v souhlasu s výsledky nalezenými v příkladu 27.

Cvičení. 49. Udejte, kolik je všech polynomů a) nultého, b) prvního, c) druhého, d) r-tého stupně v okruhu $C_2[x]$

polynomů jedné neurčité x nad tělesem C_2 zbytkových tříd podle modulu 2.

50. Opakujte předcházející úlohu pro okruh $C_3[x]$ polynomů jedné neurčité x nad tělesem C_3 zbytkových tříd podle modulu 3.

51. Ověřte, že v okruhu $C_2[x]$ polynomů jedné neurčité x nad tělesem C_2 zbytkových tříd podle modulu 2 platí: a) $(x+1)^2 = x^2 + 1$, b) $(x+1)^3 = x^3 + x^2 + x + 1$, c) $(x+1)^4 = x^4 + 1$. Přitom znak 1 značí zbytkovou třídu $\{1\}$.

52. Ověřte, že v okruhu $C_3[x]$ polynomů jedné neurčité x nad tělesem C_3 zbytkových tříd podle modulu 3 platí: a) $(x+1)^3 = x^3 + 1$, b) $(x+2)^3 = x^3 + 2$, c) $(x^2 + x + 1)(x^2 + 2x + 1) = x^4 + x^2 + 1$. Přitom znak 1 značí zbytkovou třídu $\{1\}$ a znak 2 zbytkovou třídu $\{2\}$.

53. Napište polynom a) $x^4 + x^3 + x^2 + x + 1$, b) $x^4 + 4x^3 + 6x^2 + 4x + 1$ jako polynom jedné neurčité $y = x + 1$. Nad jakým okruhem je to možné?

54. Najděte neúplný podíl a zbytek, dělíte-li v oboru integrity polynomů s racionálními koeficienty a) polynom $1 + x^2 + x^4$ polynomem $1 + x + x^2$, b) polynom $1 - 3x^2 - 2x^4$ polynomem $1 - 2x + 3x^2$, c) polynom $1 - 2x + 3x^2$ polynomem $1 - 3x^2 - 2x^4$.

55. V oboru integrity $C[x]$ polynomů jedné neurčité x s celočíselnými koeficienty lze dělit se zbytkem libovolný polynom $B \in C[x]$ každým polynomem $A \in C[x]$ r-tého stupně, v němž je koeficient $a_r = \pm 1$. Odůvodněte.

56. Rozložte v součin dvou polynomů prvního stupně následující polynomy: a) $x^2 - 15x + 54$, b) $x^2 - 15x - 54$, c) $12x^2 - 25x + 12$, d) $x^2 + x + 1$. Nad kterým číselným okruhem je tento rozklad možný?

57. Dá se dokázat, že nad tělesem R reálných čísel lze rozložit každý polynom jedné neurčité x s reálnými koefi-

cienty, který je stupně vyššího než druhého, v součin polynomů prvního nebo druhého stupně. Rozložte v tomto oboru na činitele pokud možno nejnižšího stupně tyto polynomy: a) $x^3 + 6x^2 + 11x + 6$, b) $x^3 - x^2 - x - 2$, c) $x^4 + x^2 + 1$, d) $x^4 + 1$.

58. Nad tělesem K komplexních čísel lze rozložit každý polynom jedné neurčité s komplexními koeficienty, který je stupně aspoň druhého, na součin polynomů prvního stupně. Rozložte podle toho nad $\mathsf{K}[x]$ všechny polynomy z předcházejícího cvičení.

59. Je-li $A = a_0 + a_1x + a_2x^2 + \ldots + a_rx^r$ polynom s komplexními koeficienty a je-li $\overline{A} = \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \ldots + \bar{a}_rx^r$, kde $\bar{a}_i$ je komplexně sdružené číslo k číslu a_i, pak $A + \overline{A}$, $A\overline{A}$ jsou polynomy jedné neurčité s reálnými koeficienty. Dokažte to. Polynomy A, $\overline{A}$ se nazývají *komplexně sdružené polynomy*.

60. Budiž A polynom s komplexními koeficienty a a komplexní číslo. Dosadíme-li do komplexně sdruženého polynomu $\overline{A}$ za neurčitou komplexně sdružené číslo $\bar{a}$ dostaneme číslo komplexně sdružené k číslu, které vznikne dosazením čísla a za neurčitou do polynomu A. Dokažte to.