Polynomy v moderní algebře

ŠKOLA MLADÝCH MATEMATIKŮ

POLYNOMY V MODERNÍ ALGEBŘE

26

Vydal ÚV Matematické olympiády v nakladatelství Mladá fronta

ŠKOLA MLADÝCH MATEMATIKŮ

polynomy v moderní algebře

KAREL HRUŠA

PRAHA
VYDAL ÚV MATEMATICKÉ OLYMPIÁDY
V NAKLADATELSTVÍ MLADÁ FRONTA

Recenzovali dr. Jiří Jarník a dr. Miroslav Šisler

PŘEDMLUVA

Výklady o polynomech (mnohočlenech) tvoří podstatnou část školní algebry: s polynomy pracují žáci vlastně od okamžiku, kdy začnou zapisovat čísla pomocí písmen. Mnohočlen se tu zpravidla chápe jako funkce jedné nebo i více proměnných, i když se to někdy výslovně nezdůrazňuje. Bylo tedy možné postavit se na toto stanovisko a učinit předmětem úvah některé další vlastnosti funkcí zvaných mnohočleny, které navazují na látku probíranou ve škole.

Ale takto zaměřený obsah knížky by neodpovídal tomu, co tvoří podstatu současné algebry (označované též názvem moderní algebra), která se zabývá studiem množin, ne nutně číselných, v nichž jsou definovány určité operace. Chtěl-li jsem tedy sestavit knížku, která by ukázala čtenáři částečný obraz toho, čím se dnes algebra zabývá, nezbývalo mi nic jiného než učinit osou výkladu množiny s operacemi (zvané též algebraické struktury). Pak bylo ovšem nutné opustit i funkční definici polynomů, jak ji známe ze školy, a definovat množinu polynomů algebraicky jako množinu s jistými operacemi. Tím se otvírá čtenáři nový pohled na některá fakta, s nimiž se setkal již dříve v jiných souvislostech. Věřím, že se tím rozšíří jeho obzor. Zejména pak prosím čtenáře, aby bedlivě sledoval logickou stavbu celého výkladu, která chce být bez mezer.

Východiskem každé matematické teorie je určitý počet definic. Pro snazší orientaci jsou všechny důležité definice

v této knížce výrazně uvedeny a pojmy v nich zavedené jsou vytištěny *kurzívou*. Z definic odvozujeme věty, za jejichž zněním pak následuje důkaz vyslovené věty. K ilustraci definic a vět je připojena řada příkladů v textu a ke kontrole pochopení probrané látky jsou na konci každého článku uvedena cvičení. Úkolem většiny z nich je dát čtenáři možnost, aby si ověřil, do jaké míry porozuměl vysloveným definicím a větám, a jen menší část z nich procvičuje počtářskou pohotovost a zběhlost. Na konci knížky jsou připojeny výsledky těchto cvičení, popř. více či méně podrobné návody k jejich řešení. Snad ani není třeba připomínat, že se má čtenář nejprve pokusit o řešení sám, a teprve nebude-li si vědět rady, uchýlit se k návodu.

Nakonec je třeba uvést ještě jednu poznámku týkající se terminologie. V knížce se užívá názvu přirozená čísla pro čísla 0, 1, 2, 3, 4, ... V některých učebnicích i v jiných matematických knihách se však číslo 0 za přirozené číslo nepovažuje. Patří-li číslo 0 mezi přirozená čísla či nikoli, to se nedá dokázat, to je věcí úmluvy. Lze najít dostatek důvodů pro jedno i pro druhé a také proti jednomu i proti druhému. Sám považuji za nejpádnější důvod pro to, aby se číslo 0 od ostatních přirozených čísel neodtrhovalo, fakt, že se děti seznamují s číslem 0 spolu s ostatními přirozenými čísly hned od počátku školní docházky. Aby však nevznikl u čtenáře zmatek, je vždy zřetelně uvedeno, jde-li o množinu všech přirozených čísel i s nulou (označení N_0), či bez nuly (označení N).

Karel Hruša

1. kapitola

OPERACE V MNOŽINĚ

Ve škole se hodně zabýváme početními výkony čili operacemi, mezi něž patří například sčítání, odčítání, násobení, dělení aj. V tomto článku budeme definovat pojem operace poněkud obecněji, a proto si nejprve všimneme některých společných vlastností, které mají operace, s nimiž jsme se ve škole setkali. Při sčítání, odčítání, násobení i dělení jsou vždy dána dvě čísla a určitým postupem, jemuž jsme se ve škole učili, k nim hledáme třetí číslo, které je oběma danými čísly jednoznačně určeno. Ke každé dvojici daných čísel tedy hledáme jedno jediné třetí číslo. Přitom (aspoň v některých případech) záleží na pořadí obou čísel v dané dvojici (např. $x - y$ znamená zpravidla něco jiného než $y - x$). Jde tu tedy o uspořádané dvojice, tj. o dvojice, u nichž je podstatné, která jejich složka je první a která je druhá.

Je-li dána množina M, budeme množinu všech uspořádaných dvojic $[x, y]$, kde $x \in \mathsf{M}$, $y \in \mathsf{M}$, označovat symbolem $\mathsf{M} \times \mathsf{M}$. Dvě uspořádané dvojice $[x, y] \in \mathsf{M} \times \mathsf{M}$, $[z, u] \in \mathsf{M} \times \mathsf{M}$ považujeme za sobě rovné, shodují-li se ve svých prvcích i v jejich uspořádání, tj.

$[x, y] = [z, u]$ právě tehdy, když $x = z$ a zároveň $y = u$. Naproti tomu

$[x, y] \neq [z, u]$ právě tehdy, když $x \neq z$ nebo $y \neq u$ (nebo obojí).

Abychom pracovali s jasnými pojmy, uvedeme nejprve definici zobrazení v množině.

Definice 1. Budiž dána množina M. Množinu $f \subset M \times M$ nazýváme *zobrazení v množině* M, má-li tuto vlastnost:

Jestliže v dvojicích $[x_1, y_1]$, $[x_2, y_2]$ z množiny f je $x_1 = x_2$, pak také $y_1 = y_2$.

Jsou-li x, y prvky téže dvojice $[x, y] \in f$, pak prvku x říkáme *vzor* prvku y a prvku y říkáme *obraz* prvku x v zobrazení f a píšeme $y = f(x)$.

Často tu mluvíme také o přiřazení a říkáme, že obraz $y \in M$ je přiřazen vzoru $x \in M$.

Z definice 1 vyplývá, že každý prvek množiny M může být vzorem některého prvku této množiny v zobrazení f. Nikde však není řečeno, že množina všech vzorů musí množinu M vyčerpávat; může se stát, že v množině M existují prvky, které nejsou vzory žádného prvku množiny M. Jestliže však nějaký prvek množiny M je vzorem některého prvku této množiny v zobrazení f, je vzorem právě jednoho prvku množiny M.

Také každý prvek množiny M může být obrazem některého prvku této množiny v zobrazení f, ale ani tady není řečeno, že množina všech obrazů musí množinu M vyčerpávat; může se stát, že v množině M existují prvky, které nejsou obrazy žádného prvku této množiny. A také není nikde řečeno, že každý prvek množiny M, který je obrazem některého jejího prvku, musí být obrazem jen jednoho prvku této množiny; může se stát, že jeden a týž prvek množiny M je obrazem většího počtu prvků této množiny v zobrazení f.

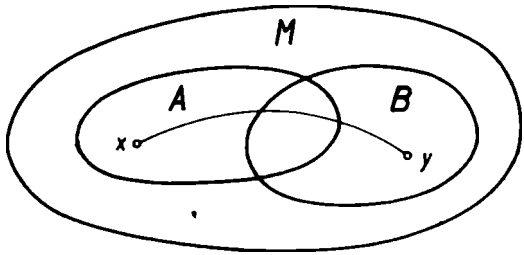
Podmínku uvedenou v definici 1 můžeme vyslovit i v tvaru:

Jestliže v dvojicích $[x_1, y_1]$, $[x_2, y_2]$ z množiny f je $y_1 \neq y_2$, pak také $x_1 \neq x_2$.

Jsou-li tedy dva různé prvky množiny M obrazy něja-

kých prvků této množiny v zobrazení f, jsou to obrazy dvou různých prvků.

Situace je schematicky znázorněna na obr. 1, kde množina všech vzorů je označena písmenem A a množina všech obrazů písmenem B.



Obr. 1.

S pojmem zobrazení v množině M jsme se setkali již mnohokrát ve škole; tu byla množinou M zpravidla nějaká číselná množina (tj. množina, jejíž prvky jsou čísla) a místo názvu zobrazení jsme užívali názvu funkce. Množina A se pak nazývala obor funkce a množina B obor funkčních hodnot. Naše definice však je poněkud obecnější, protože M může znamenat zcela libovolnou neprázdnou, nikoli jen číselnou množinu. Další rozdíl mezi naší definicí a definicí běžně užívanou ve škole je zavedení množiny M, která má tu vlastnost, že obsahuje jak množinu A (obor funkce), tak i množinu B (obor funkčních hodnot), takže $A \cup B \subset M$. Pro naše účely je totiž vhodné připustit i tu možnost, že ne každý prvek množiny M je vzorem některého prvku této množiny v zobrazení f.

Po této průpravě budeme definovat operaci v množině M jako jisté zobrazení v množině $(M \times M) \cup M$. Tato mno-

žina obsahuje jednak uspořádané dvojice z množiny $M \times M$, jednak jednotlivé prvky z množiny M.

Definice 2. Budiž dána množina M. Zobrazení f v množině $(M \times M) \cup M$, v němž množinou vzorů je část množiny $M \times M$ a množinou obrazů část množiny M, nazýváme *operace v množině* M.

Je-li v operaci f prvek $z \in M$ obrazem prvku $[x, y] \in M \times M$, píšeme $z = f(x, y)$.

Operace f je tedy zobrazení, v němž je vzorem uspořádaná dvojice $[x, y] \in M \times M$ a obrazem prvek $z \in M$; množina f je tvořena uspořádanými dvojicemi, jejichž složení je toto:

$$[[x, y], z] \in f.$$

Proto bychom měli podle definice 1 spíše psát $z = f([x, y])$; tento zápis by však byl zbytečně složitý.

Příklad 1. Sčítání je operace v množině N_0 všech přirozených čísel (včetně nuly), neboť ke každé dvojici $[x, y] \in N_0 \times N_0$ přísluší jako obraz číslo $x + y \in N_0$ a toto číslo je, jak víme ze školy, jediné. Množinou vzorců je tu celá množina $N_0 \times N_0$, množinou obrazů je množina N_0. Značí-li tedy písmeno f sčítání, je $f(x, y) = x + y$. Obdobné tvrzení platí i pro násobení v množině N_0, které je dáno vzorcem $f(x, y) = xy$. Také odčítání je operace v množině N_0, kterou můžeme vyjádřit vzorcem $f(x, y) = x - y$. Tu má každá uspořádaná dvojice $[x, y] \in N_0 \times N_0$, kde $x \geq y$, za obraz číslo $x - y \in N_0$. Množinou vzorů je množina všech takových dvojic $[x, y] \in N_0 \times N_0$, v nichž je $x \geq y$. Vezmeme-li však v úvahu odčítání jako operaci v množině C všech celých čísel, pak množinou vzorů je celá množina $C \times C$, neboť ke každé dvojici $[x, y] \in C \times C$ existuje

obraz $z = f(x, y) = x - y \in \mathsf{C}$. Také dělení (beze zbytku) je operace v množině N_0 i v množině C, pro kterou platí $f(x, y) = x : y$; množinou vzorů je množina všech takových dvojic $[x, y]$ z množiny $\mathsf{N}_0 \times \mathsf{N}_0$, popř. $\mathsf{C} \times \mathsf{C}$, v nichž je $x = ky$, kde k je prvek množiny N_0, popř. C, a $y \neq 0$.

Příklad 2. Operace však nemusí být definovány pouze v číselných množinách. Budiž například M množina všech bodů roviny ϱ a přiřaďme ke každé dvojici X, Y různých bodů této roviny střed S úsečky XY; pro $X = Y$ položme $S = X = Y$. Také tu je ke každé dvojici $[X, Y] \in \mathsf{M} \times \mathsf{M}$ (tj. ke každé dvojici bodů roviny ϱ) přiřazen právě jeden bod $S \in \mathsf{M}$ (tj. právě jeden bod roviny ϱ), takže jde skutečně o operaci f v množině M všech bodů roviny ϱ, přičemž je $f(X, Y) = S$. Pro tuto operaci neexistuje žádný mezinárodně zavedený symbol; nic nám však nebrání, abychom si pro naši potřebu takový symbol zavedli; můžeme psát např. $f(X, Y) = X \bullet Y$. Také můžeme pro tuto operaci zavést i zvláštní název, budeme jí říkat třeba *operace střed.*

Abychom přiblížili naše zápisy co nejvíce zápisům operací známých ze školy, budeme raději místo písmene značícího zobrazení v množině $(\mathsf{M} \times \mathsf{M}) \cup \mathsf{M}$ používat nějakou značku, např. $\circ$, $\star$ aj., kterou umístíme mezi obě složky dvojice $[x, y] \in \mathsf{M} \times \mathsf{M}$, jež je vzorem v uvedeném zobrazení, podobně jako to činíme ve škole se značkami $+$, $-$ aj. Budeme tedy psát např. $f(x, y) = x \circ y$ apod. A také operaci f budeme v tomto případě označovat názvem operace $\circ$.

Definice 3. a) Nechť $\circ$ značí operaci v množině M.

Jestliže pro každé dva prvky x, y množiny M, pro něž existují prvky $x \circ y \in \mathsf{M}$, $y \circ x \in \mathsf{M}$, platí

$$x \circ y = y \circ x,$$

nazývá se operace $\circ$ *komutativní.*

Jestliže pro každé tři prvky x, y, z množiny M, pro něž existují prvky $(x \circ y) \circ z \in \mathsf{M}$, $x \circ (y \circ z) \in \mathsf{M}$, platí

$$(x \circ y) \circ z = x \circ (y \circ z),$$

nazývá se operace $\circ$ *asociativní.*

b) Nechť $\circ$, $\star$ značí operace v množině M (které nemusí být navzájem různé).

Jestliže pro každé tři prvky x, y, z množiny M, pro něž existují prvky $(x \circ y) \star z \in \mathsf{M}$, $(x \star z) \circ (y \star z) \in \mathsf{M}$, platí

$$(x \circ y) \star z = (x \star z) \circ (y \star z),$$

nazývá se operace $\star$ *distributivní vzhledem k operaci* $\circ$.

Přitom závorky jako obvykle značí, kterou operaci máme provádět napřed.

Příklad 3. Sčítání v množině N_0 všech přirozených čísel (včetně nuly) je operace komutativní, neboť pro každá dvě čísla x, y množiny N_0 existují obě čísla $x + y, y + x$ a víme, že pro každá dvě přirozená čísla x, y je

$$x + y = y + x.$$

Je to také operace asociativní, neboť pro každá tři čísla x, y, z množiny N_0 existují čísla $(x + y) + z$, $x + (y + z)$, přičemž platí

$$(x + y) + z = x + (y + z).$$

Také násobení v množině N_0 je operace komutativní i asociativní, neboť jestliže v definici 3a) za operaci $\circ$ vezmeme násobení, dostaneme

$$xy = yx, \quad (xy)z = x(yz),$$

ale to je správné pro každá dvě, popř. pro každá tři přirozená čísla. Násobení přirozených čísel je distributivní vzhledem ke sčítání: vezmeme-li v definici 3b) za operaci

sčítání a za operaci $\star$ násobení, dostaneme

$$(x + y)z = xz + yz,$$

a to je správné pro každá tři přirozená čísla x, y, z. Naproti tomu sčítání přirozených čísel není distributivní vzhledem k násobení. Jestliže totiž v definici 3b) vezmeme za operaci $\circ$ násobení a za operaci $\star$ sčítání, vyjde rovnost

$$xy + z = (x + z)(y + z),$$

ale ta není splněna pro každá tři přirozená čísla x, y, z, jak se snadno přesvědčíme (třeba na příkladě $x = y = z = 1$).

Příklad 4. Odčítání v množině N_0 všech přirozených čísel (včetně nuly) je operace komutativní. V této množině existují obě čísla $x - y, y - x$ pouze tehdy, je-li $x = y$; pak je

$$x - y = y - x = 0.$$

Naproti tomu odčítání v množině C všech celých čísel není operace komutativní, neboť v této množině existují pro každé $x \in \mathsf{C}$ a pro každé $y \in \mathsf{C}$ obě čísla $x - y, y - x$, ale pokud je $x \neq y$, je také $x - y \neq y - x$.

Příklad 5. Operace $\bullet$ v množině M všech bodů roviny ϱ, popsaná v příkladu 2 na str. 9 (operace střed), je komutativní, neboť pro každé dva body X, Y roviny ϱ je $X \bullet Y = Y \bullet X$. Jsou-li $[x_1, x_2]$, $[y_1, y_2]$ souřadnice bodů X, Y, pak

$$X \bullet Y = [\tfrac{1}{2}(x_1 + y_1), \tfrac{1}{2}(x_2 + y_2)],$$
$$Y \bullet X = [\tfrac{1}{2}(y_1 + x_1), \tfrac{1}{2}(y_2 + x_2)],$$

ale to je jeden a týž bod. Operace $\bullet$ však není asociativní. Je-li $X = [x_1, x_2]$, $Y = [y_1, y_2]$, $Z = [z_1, z_2]$, pak

$$(X \bullet Y) \bullet Z = [\tfrac{1}{2}(\tfrac{1}{2}(x_1 + y_1) + z_1), \tfrac{1}{2}(\tfrac{1}{2}(x_2 + y_2) + z_2)] = [\tfrac{1}{4}(x_1 + y_1 + 2z_1), \tfrac{1}{4}(x_2 + y_2 + 2z_2)],$$

$$X \bullet (Y \bullet Z) = [\tfrac{1}{2}(x_1 + \tfrac{1}{2}(y_1 + z_1)), \tfrac{1}{2}(x_2 + \tfrac{1}{2}(y_2 + z_2))] = [\tfrac{1}{4}(2x_1 + y_1 + z_1), \tfrac{1}{4}(2x_2 + y_2 + z_2)];$$

tyto dva body však mohou být různé. Operace $\bullet$ však je také distributivní vzhledem k sobě samé, tj. pro každé tři body X, Y, Z množiny M platí

$$(X \bullet Y) \bullet Z = (X \bullet Z) \bullet (Y \bullet Z).$$

Označíme-li opět $X = [x_1, x_2]$, $Y = [y_1, y_2]$, $Z = [z_1, z_2]$, je podle předcházejícího

$$(X \bullet Y) \bullet Z = [\tfrac{1}{4}(x_1 + y_1 + 2z_1), \tfrac{1}{4}(x_2 + y_2 + 2z_2)]$$

a kromě toho

$$(X \bullet Z) \bullet (Y \bullet Z) = [\tfrac{1}{2}(\tfrac{1}{2}(x_1 + z_1) + \tfrac{1}{2}(y_1 + z_1)), \tfrac{1}{2}(\tfrac{1}{2}(x_2 + z_2) + \tfrac{1}{2}(y_2 + z_2))] = [\tfrac{1}{4}(x_1 + y_1 + 2z_1), \tfrac{1}{4}(x_2 + y_2 + 2z_2)].$$

Oba výsledky dávají jeden a týž bod.

Cvičení. 1. Budiž R^+ množina všech kladných (reálných) čísel. Zjistěte, jsou-li komutativní a asociativní tyto operace v množině R^+: a) $f(x, y) = \frac{1}{2}(x + y)$ (aritmetický průměr), b) $f(x, y) = \sqrt{xy}$ (geometrický průměr), c) $f(x, y) = \dfrac{2xy}{x + y}$ (harmonický průměr).

2. Budiž R^+ množina všech kladných (reálných) čísel. Zjistěte, jsou-li komutativní a asociativní tyto operace v množině R^+:

a) $f(x, y) = \dfrac{xy}{x + y}$, b) $f(x, y) = \sqrt{x^2 + y^2}$, c) $f(x, y) = \dfrac{xy}{\sqrt{x^2 + y^2}}$.

3. Budiž Q^+ množina všech kladných racionálních čísel. Ukažte, že v této množině je umocňování distributivní vzhledem k násobení (dělení).

4. M je množina všech přemístění roviny ϱ, jimiž se reprodukuje rovnostranný trojúhelník ABC ležící v rovině ϱ. Tato množina se skládá z šesti prvků, které označíme takto:

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} = \mathfrak{I}, \qquad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} = \mathfrak{R}_1, \qquad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} = \mathfrak{R}_2,$$

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = \mathfrak{S}_1, \qquad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = \mathfrak{S}_2, \qquad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = \mathfrak{S}_3.$$

(Při tomto označení jsou pod sebou napsány vrcholy trojúhelníka, které si odpovídají v uvedeném přemístění; $\mathfrak{I}$ je identické přemístění, $\mathfrak{R}_1$, $\mathfrak{R}_2$ jsou rotace kolem středu trojúhelníka, $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_2$ jsou osové souměrnosti.) V množině M definujeme operaci $\star$ takto: $\mathfrak{X} \star \mathfrak{Y}$ je přemístění, které vznikne tak, že provedeme nejprve přemístění $\mathfrak{X}$ a po něm přemístění $\mathfrak{Y}$, např. $\mathfrak{R}_1 \star \mathfrak{S}_2 = \mathfrak{S}_3$. Vyšetřete, je-li operace $\star$ komutativní a asociativní.

5. Cvičení 4 opakujte pro přemístění roviny ϱ, jimiž se reprodukuje a) čtverec $ABCD$, b) obdélník $ABCD$.

6. a) V rovině ϱ jsou dány dvě různoběžky p, q. V množině M všech bodů roviny ϱ je dána operace $\circ$ takto: obrazem uspořádané dvojice $[X, Y] \in M \times M$ je ten bod $X \circ Y = Z$ roviny ϱ, pro který platí $XZ \parallel p$, $YZ \parallel q$. Vyšetřte, je-li tato operace komutativní a asociativní. b) Ukažte, že operace $\bullet$ z příkladu 2 na str. 9 je distributivní vzhledem k operaci $\circ$ ze cvič. a).

7. V rovině ϱ je dán bod O. V množině M všech bodů roviny ϱ je dána operace $\circ$ takto: Jsou-li X, Y dva různé body roviny ϱ a neprochází-li přímka XY bodem O, je $Z = X \circ Y$ čtvrtý vrchol rovnoběžníka $XOYZ$; leží-li body X, Y na polopřímce p s počátkem O, je $Z = X \circ Y$

ten bod polopřímky p, pro který platí $OZ = OX + OY$; jsou-li OX, OY opačné polopřímky a je-li $OX \geqq OY$, je $Z = X \circ Y$ ten bod polopřímky OX, pro který platí $OZ = OX - OY$; jsou-li OX, OY opačné polopřímky a je-li $OX \leqq OY$, je $Z = X \circ Y$ ten bod polopřímky OY, pro který platí $OZ = OY - OX$; je-li $X = Y = O$, je $Z = X \circ Y = O$. Ukažte, že je operace $\circ$ v množině M komutativní a asociativní.

8. Budiž M množina, jejímiž prvky jsou reálná čísla (všechna nebo jen některá). Dokažte, že

$$\max(x, y) = \begin{cases} x, \text{ je-li } x \geqq y \\ y, \text{ je-li } x < y \end{cases}, \quad \min(x, y) = \begin{cases} y, \text{ je-li } x \geqq y \\ x, \text{ je-li } x < y \end{cases}$$

jsou operace v množině M, které jsou obě komutativní, obě asociativní a každá z nich je distributivní vzhledem k druhé.

9. Budiž dána množina Z a označme M systém všech jejích podmnožin. Je-li $A \in M$, $B \in M$ (tj. je-li $A \subset Z$, $B \subset Z$), označme $A \cup B = S$, $A \cap B = P$. Ukažte, že $\cup$ a $\cap$ jsou operace v množině M, které jsou obě komutativní, obě asociativní a každá z nich je distributivní vzhledem k druhé.

10. Je-li $D(x, y)$ největší společný dělitel a $n(x, y)$ nejmenší společný násobek přirozených čísel x, y, ukažte, že D, n jsou operace v množině N všech přirozených čísel (bez nuly), které jsou obě komutativní, obě asociativní a každá z nich je distributivní vzhledem k druhé.

2. kapitola

NEUTRÁLNÍ A INVERZNÍ PRVEK. GRUPA

Je-li v množině definována nějaká operace, může se stát, že existují v této množině prvky, které mají vzhledem k této operaci určité speciální vlastnosti.

Věta 1. Budiž M množina, v níž je definována operace $\circ$. Existují-li v množině M prvky m, n, které mají tu vlastnost, že pro každé $x \in \mathsf{M}$ je

$$m \circ x = x, \quad x \circ n = x,$$

pak $m = n$, a takový prvek existuje v množině M jen jeden.

Důkaz. Poněvadž obě napsané rovnosti jsou splněny pro každé $x \in \mathsf{M}$, dosaďme do první z nich $x = n$ a do druhé $x = m$. Dostaneme

$$m \circ n = n, \quad m \circ n = m$$

a odtud vyplývá, že $n = m$. Jestliže nějaký další prvek $n' \in \mathsf{M}$ má tu vlastnost, že pro každé $x \in \mathsf{M}$ je $x \circ n' = x$, pak podle toho, co jsme právě dokázali, je $n' = m$. Obdobně z předpokladu existence dalšího prvku $m' \in \mathsf{M}$, který má tu vlastnost, že pro každé $x \in \mathsf{M}$ je $m' \circ x = x$, plyne $m' = n$. Je tedy $m = n = m' = n'$; nejde tu o čtyři různé prvky, ale o jediný.

Všimněme si toho, že ve větě 1 nepředpokládáme žádnou speciální vlastnost operace $\circ$ kromě toho, že pro každé $x \in \mathsf{M}$ existují oba prvky $m \circ x$ i $x \circ n$; zejména tedy nepředpokládáme, že operace $\circ$ je komutativní.

Definice 4. Je-li v množině M definována operace $\circ$, pak prvek $n \in M$, který má tu vlastnost, že pro každé $x \in M$ je

$$n \circ x = x \circ n = x,$$

nazýváme *neutrální prvek operace* $\circ$.

Věta 1 říká, že v každé množině M, v níž je definována operace $\circ$, existuje nejvýše jeden (tj. jeden nebo žádný) neutrální prvek této operace.

Příklad 6. V množině N_0 všech přirozených čísel (včetně nuly) existuje neutrální prvek sčítání a je jím číslo 0, neboť pro každé $x \in N_0$ je

$$0 + x = x + 0 = x.$$

V téže množině existuje také neutrální prvek násobení, jímž je číslo 1, neboť pro každé $x \in N_0$ je

$$1 . x = x . 1 = x.$$

Táž tvrzení platí i pro množinu C všech celých čísel, pro množinu Q všech racionálních čísel, pro množinu R všech reálných čísel i pro množinu K všech komplexních čísel. Naproti tomu v žádné číselné množině M neexistuje neutrální prvek odčítání, neboť sice pro každé $x \in M$ je $x - 0 = x$, ale neexistuje žádné $n \in M$, aby pro každé $x \in M$ bylo $n - x = x$. Na příkladu odčítání je vidět, že z existence „neutrálního prvku zprava" ($x - 0 = x$) nikterak nevyplývá existence „neutrálního prvku zleva".

Věta 2. Budiž M množina, v níž je definována operace $\circ$, která je asociativní. Existují-li k prvku $a \in M$ v množině M prvky b, c, které mají tu vlastnost, že

$$a \circ b = n, \quad c \circ a = n,$$

kde n je neutrální prvek operace $\circ$, pak $b = c$ a takový prvek existuje v množině M jen jeden.

Důkaz. Poněvadž $a \circ b = n$, $c \circ a = n$, je podle vlastnosti neutrálního prvku

$$b = n \circ b = (c \circ a) \circ b, \quad c = c \circ n = c \circ (a \circ b),$$

přičemž oba prvky $(c \circ a) \circ b$, $c \circ (a \circ b)$ v množině M existují, neboť existují prvky $n \circ b$ i $c \circ n$. Vzhledem k tomu, že operace je asociativní, je

$$(c \circ a) \circ b = c \circ (a \circ b)$$

a odtud vyplývá, že $b = c$. Jestliže nějaký další prvek $b' \in M$ má tu vlastnost, že $a \circ b' = n$, pak podle toho, co už bylo dokázáno, je $b' = c$. Obdobně z předpokladu existence dalšího prvku $c' \in M$, pro který platí $c' \circ a = n$, vyplývá, že $c' = b$. Je tedy $b = c = b' = c'$; nejde tu o čtyři různé prvky, ale o jediný.

Tentokrát je v důkazu věty 2 podstatný předpoklad, že operace $\circ$ je asociativní; bez tohoto předpokladu věta neplatí.

Definice 5. Je-li v množině M definována operace $\circ$, pak prvky a, $\bar{a}$, které mají tu vlastnost, že

$$a \circ \bar{a} = \bar{a} \circ a = n,$$

kde n je neutrální prvek operace $\circ$, nazýváme *navzájem inverzní prvky operace* $\circ$. O prvku $\bar{a}$ říkáme, že je *inverzní k prvku* a a o prvku a říkáme, že je *inverzní k prvku* $\bar{a}$ v operaci $\circ$.

Věta 2 říká, že v každé množině M, v níž je definována asociativní operace $\circ$, existuje ke každému prvku $a \in M$ nejvýše jeden inverzní prvek $\bar{a} \in M$ této operace.

Inverzní prvek k prvku a budeme zásadně označovat $\bar{a}$; podle toho také označíme inverzní prvek k prvku $\bar{a}$ symbolem $\bar{\bar{a}}$.

Z věty 2 vyplývá, že v asociativní operaci $\circ$ je inverzním prvkem k inverznímu prvku $\bar{a}$ původní prvek a, tj. že

$$\bar{\bar{a}} = a.$$

Je-li totiž $\bar{a}$ inverzním prvkem k prvku a, pak

$$a \circ \bar{a} = \bar{a} \circ a = n.$$

Je-li dále $\bar{\bar{a}}$ inverzním prvkem k prvku $\bar{a}$, pak

$$\bar{a} \circ \bar{\bar{a}} = \bar{\bar{a}} \circ \bar{a} = n.$$

Oba poslední vzorce však říkají, že a i $\bar{\bar{a}}$ jsou inverzní prvky k prvku $\bar{a}$, ale takový prvek je podle věty 2 nejvýše jeden. Musí tedy být $\bar{\bar{a}} = a$.

Příklad 7. V množině N_0 všech přirozených čísel (včetně nuly) existuje inverzní prvek sčítání pouze k číslu 0 a je jím zase číslo 0, neboť $0 + 0 = 0$ (neutrálním prvkem sčítání je tu číslo 0). K žádnému jinému číslu $a \in \mathsf{N}_0$ neexistuje v této množině inverzní prvek sčítání $\bar{a}$, neboť podmínku $a + \bar{a} = 0$ lze v této množině splnit jen pro $a = \bar{a} = 0$. V téže množině existuje inverzní prvek násobení pouze k číslu 1 a je jím zase číslo 1, neboť $1 . 1 = 1$ (neutrálním prvkem násobení je číslo 1). K žádnému jinému číslu $a \in \mathsf{N}_0$ neexistuje v této množině inverzní prvek násobení $\bar{a}$, neboť podmínku $a . \bar{a} = 1$ lze v této množině splnit jen pro $a = \bar{a} = 1$. Naproti tomu v množině C všech celých čísel existuje ke každému $a \in \mathsf{C}$ inverzní prvek sčítání $\bar{a}$ a je jím opačné číslo $-a$, neboť

$$a + (-a) = (-a) + a = 0.$$

V množině C existuje inverzní prvek násobení pouze k číslům 1 a -1, neboť rovnost $a . \bar{a} = 1$ lze v této množině splnit jen tehdy, je-li $a = \bar{a} = 1$ nebo $a = \bar{a} = -1$. Rovněž

v množině Q všech racionálních čísel, v množině R všech reálných čísel i v množině K všech komplexních čísel existuje ke každému prvku a inverzní prvek sčítání $\bar{a}$, pro který platí $\bar{a} = -a$. Ve všech těchto množinách také existuje ke každému prvku $a \neq 0$ inverzní prvek násobení $\bar{a}$, jímž je převrácené číslo $\frac{1}{a}$, neboť pro každé $a \neq 0$ je

$$a.\frac{1}{a} = \frac{1}{a}.a = 1.$$

V žádné číselné množině však neexistuje inverzní prvek násobení k číslu 0, neboť v žádné číselné množině neexistuje takové číslo x, aby $0.x = 1$.

Příklad 8. Budiž M množina všech přemístění roviny ϱ, jimiž se reprodukuje rovnostranný trojúhelník ABC ležící v této rovině. V této množině, která má šest prvků: $\mathfrak{I}$, $\mathfrak{R}_1$, $\mathfrak{R}_2$, $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, definujeme operaci $\star$ jako postupné skládání těchto přemístění — viz cvič. 4 na str. 13. Operaci $\star$ vyjadřuje následující tabulka.

$\mathfrak{X} \star \mathfrak{Y} = \mathfrak{Z}$	$\mathfrak{X}$ \ $\mathfrak{Y}$	$\mathfrak{I}$	$\mathfrak{R}_1$	$\mathfrak{R}_2$	$\mathfrak{S}_1$	$\mathfrak{S}_2$	$\mathfrak{S}_3$
	$\mathfrak{I}$	$\mathfrak{I}$	$\mathfrak{R}_1$	$\mathfrak{R}_2$	$\mathfrak{S}_1$	$\mathfrak{S}_2$	$\mathfrak{S}_3$
	$\mathfrak{R}_1$	$\mathfrak{R}_1$	$\mathfrak{R}_2$	$\mathfrak{I}$	$\mathfrak{S}_2$	$\mathfrak{S}_3$	$\mathfrak{S}_1$
	$\mathfrak{R}_2$	$\mathfrak{R}_2$	$\mathfrak{I}$	$\mathfrak{R}_1$	$\mathfrak{S}_3$	$\mathfrak{S}_1$	$\mathfrak{S}_2$
	$\mathfrak{S}_1$	$\mathfrak{S}_1$	$\mathfrak{S}_3$	$\mathfrak{S}_2$	$\mathfrak{I}$	$\mathfrak{R}_2$	$\mathfrak{R}_1$
	$\mathfrak{S}_2$	$\mathfrak{S}_2$	$\mathfrak{S}_1$	$\mathfrak{S}_3$	$\mathfrak{R}_1$	$\mathfrak{I}$	$\mathfrak{R}_2$
	$\mathfrak{S}_3$	$\mathfrak{S}_3$	$\mathfrak{S}_2$	$\mathfrak{S}_1$	$\mathfrak{R}_2$	$\mathfrak{R}_1$	$\mathfrak{I}$

Z ní je vidět, že neutrálním prvkem této operace je prvek $\mathfrak{I}$, neboť pro každé $\mathfrak{X} \in \mathsf{M}$ je

$$\mathfrak{X} \star \mathfrak{I} = \mathfrak{I} \star \mathfrak{X} = \mathfrak{X},$$

a že ke každému prvku $\mathfrak{X} \in \mathsf{M}$ existuje v této operaci inverzní prvek $\overline{\mathfrak{X}} \in \mathsf{M}$. Z tabulky totiž vyčteme

$$\mathfrak{I} \star \mathfrak{I} = \mathfrak{I}, \quad \mathfrak{R}_1 \star \mathfrak{R}_2 = \mathfrak{R}_2 \star \mathfrak{R}_1 = \mathfrak{I},$$

$$\mathfrak{S}_1 \star \mathfrak{S}_1 = \mathfrak{I}, \quad \mathfrak{S}_2 \star \mathfrak{S}_2 = \mathfrak{I}, \quad \mathfrak{S}_3 \star \mathfrak{S}_3 = \mathfrak{I}$$

a to znamená, že

$$\overline{\mathfrak{I}} = \mathfrak{I}, \ \overline{\mathfrak{R}_1} = \mathfrak{R}_2, \ \overline{\mathfrak{R}_2} = \mathfrak{R}_1, \ \overline{\mathfrak{S}_1} = \mathfrak{S}_1, \ \overline{\mathfrak{S}_2} = \mathfrak{S}_2, \ \overline{\mathfrak{S}_3} = \mathfrak{S}_3.$$

Příklad 9. Všimněme si ještě operace $\triangle$ v množině R všech reálných čísel, která je dána vzorcem

$$x \triangle y = (x + y)(1 + xy).$$

Množinou vzorů je tu množina všech číselných dvojic $[x, y] \in \mathsf{R} \times \mathsf{R}$. Tato operace není asociativní, neboť např.

$$(1 \triangle 1) \triangle 2 = (2.2) \triangle 2 = 4 \triangle 2 = 6.9 = 54,$$

$$1 \triangle (1 \triangle 2) = 1 \triangle (3.3) = 1 \triangle 9 = 10.10 = 100.$$

Jejím neutrálním prvkem je číslo 0, neboť pro každé $x \in \mathsf{R}$ je

$$x \triangle 0 = 0 \triangle x = (x + 0)(1 + x.0) = x.1 = x.$$

Poněvadž operace $\triangle$ není asociativní, nemůžeme očekávat, že by pro ni platila věta 2 a že by ke každému číslu $x \in \mathsf{R}$ existovalo nejvýše jedno takové číslo $\bar{x} \in \mathsf{R}$, že

$$x \triangle \bar{x} = \bar{x} \triangle x = 0.$$

Pro každé číslo $x \in \mathsf{R}$, které je různé od čísel 0, 1, -1, existují v množině R taková čísla dvě a obě jsou navzájem různá: jsou to čísla $-x$ a $-\frac{1}{x}$, pro něž je

$$x \triangle (-x) = (x - x)(1 - x.x) = 0$$

a také

$$x \triangle \left(-\frac{1}{x}\right) = \left(x - \frac{1}{x}\right)\left(1 - x \,.\, \frac{1}{x}\right) = 0.$$

Pro $x = 1$ a pro $x = -1$ je ovšem $-x = -\frac{1}{x}$ a pro $x = 0$ číslo $-\frac{1}{x}$ neexistuje.

Definice 6. Množina M, v níž je definována operace $\circ$, se jmenuje *grupa vzhledem k operaci* $\circ$, má-li tyto vlastnosti:

1. Ke každému prvku $[x, y] \in M \times M$ existuje prvek $x \circ y \in M$.
2. Operace $\circ$ je asociativní.
3. V množině M existuje neutrální prvek n operace $\circ$.
4. Ke každému prvku $x \in M$ existuje inverzní prvek $\bar{x} \in M$ vzhledem k operaci $\circ$.

Operace $\circ$ se v tomto případě nazývá *grupová operace.*

V definici grupy nepředpokládáme, že je grupová operace komutativní (ale nevylučujeme to). Je-li grupová operace $\circ$ komutativní, nazývá se množina M *komutativní grupa vzhledem k operaci* $\circ$.

Z definice 6 vyplývá, že prázdná množina $\varnothing$ není grupou vzhledem k žádné operaci, neboť v každé grupě musí podle bodu 3 existovat aspoň jeden prvek, totiž neutrální prvek n grupové operace $\circ$.

Příklad 10. Množina N_0 všech přirozených čísel (včetně nuly) není grupa vzhledem ke sčítání ani vzhledem k násobení, neboť tu není splněn požadavek 4 z definice 6. Množina C všech celých čísel je komutativní grupa vzhledem ke sčítání, není to však grupa vzhledem k násobení, neboť násobení v množině C opět nesplňuje požadavek 4 z defi-

nice 6. Množina Q všech racionálních čísel, množina R všech reálných čísel i množina K všech komplexních čísel jsou komutativní grupy vzhledem ke sčítání; žádná z nich však není grupou vzhledem k násobení, neboť k číslu 0 neexistuje v žádné z těchto množin inverzní prvek násobení. Naproti tomu množina Q^+ všech kladných racionálních čísel, množina R^+ všech kladných reálných čísel, množina Q' všech nenulových racionálních čísel i množina R' všech nenulových reálných čísel jsou komutativní grupy vzhledem k násobení, ale žádná z nich není grupou vzhledem ke sčítání, neboť nesplňují požadavek 3 a v důsledku toho ani požadavek 4 z definice 6. Množina M všech přemístění roviny ϱ, jimiž se reprodukuje rovnostranný trojúhelník ABC v rovině ϱ (viz příklad 8 na str. 19) je grupa vzhledem k operaci $\star$; není to však komutativní grupa.

Věta 3. Je-li množina M grupa vzhledem k operaci $\circ$ a jsou-li a, b libovolné prvky množiny M, existuje právě jeden prvek $x \in M$ a právě jeden prvek $y \in M$, pro něž platí

$$a \circ x = b, \quad y \circ a = b.$$

Důkaz. a) Předpokládejme, že hledaný prvek x existuje; aplikujeme-li na rovnost $a \circ x = b$ operaci $\circ$ s inverzním prvkem $\bar{a}$ „zleva", dostaneme

$$\bar{a} \circ (a \circ x) = \bar{a} \circ b.$$

Levou stranu lze na základě asociativnosti upravit takto:

$$\bar{a} \circ (a \circ x) = (\bar{a} \circ a) \circ x = n \circ x = x,$$

takže

$$x = \bar{a} \circ b.$$

Splňuje-li tedy nějaký prvek x danou rovnost, může to být jen právě nalezený prvek x, který je jediný, neboť k prvku a

existuje jediný inverzní prvek $\bar{a}$ vzhledem k operaci $\circ$ a výsledek operace $\circ$ je rovněž jediný. Je třeba ještě vyzkoušet, zda tento prvek danou rovnost skutečně splňuje. To však je zřejmé, neboť

$$a \circ (\bar{a} \circ b) = (a \circ \bar{a}) \circ b = n \circ b = b.$$

b) Obdobně dokážeme, že druhou rovnost splňuje jediný prvek

$$y = b \circ \bar{a};$$

při důkazu však musíme aplikovat operaci $\circ$ s inverzním prvkem $\bar{a}$ „zprava".

Jde-li o grupu, která je komutativní, je ovšem $x = y$; není-li grupa komutativní, může se stát, že $x \neq y$.

Příklad 11. Hledáme-li v grupě M všech přemístění roviny ϱ, jimiž se reprodukuje rovnostranný trojúhelník ABC, vzhledem k operaci $\star$ (viz příklad 8 na str. 19) takové prvky $\mathfrak{X}$, $\mathfrak{Y}$, pro něž je

$$\mathfrak{R}_1 \star \mathfrak{X} = \mathfrak{R}_2, \quad \mathfrak{Y} \star \mathfrak{R}_1 = \mathfrak{R}_2,$$

dostaneme

$$\mathfrak{X} = \overline{\mathfrak{R}_1} \star \mathfrak{R}_2 = \mathfrak{R}_2 \star \mathfrak{R}_2 = \mathfrak{R}_1,$$

$$\mathfrak{Y} = \mathfrak{R}_2 \star \overline{\mathfrak{R}_1} = \mathfrak{R}_2 \star \mathfrak{R}_2 = \mathfrak{R}_1;$$

tu je $\mathfrak{X} = \mathfrak{Y}$. Hledáme-li však v téže grupě prvky $\mathfrak{Z}$, $\mathfrak{U}$ tak, aby

$$\mathfrak{R}_1 \star \mathfrak{Z} = \mathfrak{S}_1, \quad \mathfrak{U} \star \mathfrak{R}_1 = \mathfrak{S}_1,$$

vyjde

$$\mathfrak{Z} = \overline{\mathfrak{R}_1} \star \mathfrak{S}_1 = \mathfrak{R}_2 \star \mathfrak{S}_1 = \mathfrak{S}_3,$$

$$\mathfrak{U} = \mathfrak{S}_1 \star \overline{\mathfrak{R}_1} = \mathfrak{S}_1 \star \mathfrak{R}_2 = \mathfrak{S}_2;$$

v tomto případě je $\mathfrak{Z} \neq \mathfrak{U}$. Nalezené výsledky můžeme ovšem ověřit i přímo v tabulce operace $\star$ v příkladu 8.

V definici 6 jsme mohli místo požadavků 3 a 4 požadovat existenci takových prvků x, y, aby bylo $a \circ x = b$,

$y \circ a = b$ pro každé dva prvky a, b množiny M. To vyplývá z následující věty.

Věta 4. Nechť je v množině M definována operace $\circ$, která má tyto vlastnosti:

a) Ke každému prvku $[x, y] \in \mathsf{M} \times \mathsf{M}$ existuje prvek $x \circ y \in \mathsf{M}$.

b) Operace $\circ$ je asociativní.

c) Ke každému $a \in \mathsf{M}$ a ke každému $b \in \mathsf{M}$ existuje (aspoň jeden) prvek $x \in \mathsf{M}$ a (aspoň jeden) prvek $y \in \mathsf{M}$, který splňuje rovnost $a \circ x = b$, popř. $y \circ a = b$.

Pak je množina M grupa vzhledem k operaci $\circ$.

Důkaz. Musíme ukázat, že operace $\circ$ má všecky vlastnosti z definice 6. Požadavky 1 a 2 z definice 6 jsou totožné s požadavky a) a b) naší věty. Splnění požadavku 3 dokážeme takto: Vezměme některý prvek $z \in \mathsf{M}$ a označme n a m ty prvky množiny M, pro něž je

$$z \circ n = z, \quad m \circ z = z.$$

Takové prvky podle vlastnosti c) existují. Je-li x zcela libovolný prvek množiny M, existují podle téže vlastnosti takové prvky $u \in \mathsf{M}$, $v \in \mathsf{M}$, že

$$u \circ z = x, \quad z \circ v = x.$$

Pak je

$$x \circ n = (u \circ z) \circ n = u \circ (z \circ n) = u \circ z = x,$$

$$m \circ x = m \circ (z \circ v) = (m \circ z) \circ v = z \circ v = x.$$

Proto podle věty 1 je $m = n$, takže pro každé $x \in \mathsf{M}$ je

$$x \circ n = n \circ x = x$$

a prvek n je tedy neutrálním prvkem operace $\circ$. Zbývá dokázat splnění požadavku 4. Je-li $a \in \mathsf{M}$, pak podle bodu

c) existují takové prvky $b \in \mathsf{M}$, $c \in \mathsf{M}$, že

$$a \circ b = n, \quad c \circ a = n,$$

kde n je neutrální prvek operace $\circ$. Odtud podle věty 2 plyne, že $b = c$ a že tedy tento prvek je inverzním prvkem $\bar{a}$ k prvku a v operaci $\circ$.

Poznámka. V definici grupy nebylo třeba požadovat existenci neutrálního prvku a existenci inverzního prvku. Místo požadavků 3 a 4 z definice 6 stačí tyto poněkud slabší požadavky:

3′. Existuje takový prvek $n' \in \mathsf{M}$, že $x \circ n' = x$ pro každé $x \in \mathsf{M}$.

4′. Ke každému $a \in \mathsf{M}$ existuje prvek $a' \in \mathsf{M}$, pro nějž je $a \circ a' = n'$.

Tyto požadavky se liší od požadavků 3 a 4 tím, že požadují „neutrálnost" a „inverznost" prvků n' a a' jen „z jedné strany". Dokážeme, že také $n' \circ x = x$ pro každé $x \in \mathsf{M}$ a že $a' \circ a = n'$; tím bude dokázáno, že n' je neutrální prvek operace $\circ$ a že a' je inverzní prvek k prvku a v operaci $\circ$.

Nejprve dokážeme, že $a' \circ a = n'$. Označme a'' ten prvek množiny M, pro který platí $a' \circ a'' = n'$. Takový prvek podle bodu 4′ existuje. Pak platí

$$a' \circ a = a' \circ (a \circ n') = a' \circ [a \circ (a' \circ a'')] =$$
$$= a' \circ [(a \circ a') \circ a''] = a' \circ (n' \circ a'') =$$
$$= (a' \circ n') \circ a'' = a' \circ a'' = n'.$$

Přitom jsme nejprve použili toho, že $a = a \circ n'$, pak toho, že $n' = a' \circ a''$, dále asociativnosti operace $\circ$, potom toho, že $a \circ a' = n'$, načež opět asociativnosti operace $\circ$, pak toho, že $a' \circ n' = a'$, a konečně znovu toho, že $a' \circ a'' = n'$. Tím je dokázáno, že a' je inverzní prvek k prvku a v operaci $\circ$.

Na základě toho už snadno vyjde, že také $n' \circ x = x$. Označíme-li x' ten prvek množiny M, pro který platí $x \circ x' = n'$, pak podle toho, co jsme právě dokázali, je také $x' \circ x = n'$. Proto

$$n' \circ x = (x \circ x') \circ x = x \circ (x' \circ x) = x \circ n' = x.$$

Přitom jsme nejprve použili toho, že $n' = x \circ x'$, pak asociativnosti operace $\circ$, dále toho, že $x' \circ x = n'$, a konečně toho, že $x \circ n' = x$. Je tedy skutečně n' neutrální prvek operace $\circ$.

Cvičení. 11. V množině C všech celých čísel jsou dány operace $\circ$, $*$ vzorci $x \circ y = x + y + 1$, $x * y = x + y - xy$. Vyšetřte, mají-li tyto operace neutrální prvky a ke kterým prvkům množiny C existují inverzní prvky těchto operací. Jak se změní výsledek, vezmete-li místo množiny C množinu R všech reálných čísel?

12. Vyšetřte, má-li operace střed v množině M všech bodů roviny ϱ (viz příklad 2 na str. 9) neutrální prvek.

13. V množině M reálných čísel (některých nebo všech) jsou dány operace max, min tak jako ve cvič. 8 na str. 14. Vyšetřte, za jakých podmínek existují neutrální prvky těchto operací a zda k některým prvkům množiny M existují inverzní prvky vzhledem k těmto operacím.

14. Budiž dána množina Z a označme M systém všech jejích podmnožin. V množině M jsou dány operace $\cup$ a $\cap$ (sjednocení a průnik). Vyšetřte, mají-li tyto operace neutrální prvek a ke kterým prvkům množiny M existují v těchto operacích inverzní prvky.

15. V množině N všech přirozených čísel (bez nuly) jsou dány operace D a n (největší společný dělitel a nejmenší společný násobek). Vyšetřte, mají-li tyto operace neutrální prvek a ke kterým prvkům množiny N existují v těchto operacích inverzní prvky.

16. Dokažte, že inverzním prvkem asociativní operace $\circ$ k prvku $a \circ b$ je prvek $\bar{b} \circ \bar{a}$, kde $\bar{a}$, $\bar{b}$ jsou inverzní prvky k prvkům a, b vzhledem k operaci $\circ$.

17. V množině $M = \{a, b, c\}$ je dána operace $\star$ touto tabulkou:

$x \star y$	x \ y	a	b	c
	a	a	b	c
	b	b	c	a
	c	c	a	b

Vyšetřte, je-li množina M grupou vzhledem k této operaci, najděte neutrální prvek této operace a ke každému prvku množiny M udejte inverzní prvek vzhledem k této operaci (pokud existuje).

18. Tutéž úlohu řešte pro množinu $M = \{a, b, c, d\}$, v níž je definována operace $\star$ tabulkou

$x \star y$	x \ y	a	b	c	d
	a	a	a	a	a
	b	a	b	c	d
	c	a	c	d	b
	d	a	d	b	c

19. a) Dokažte, že množina M všech přemístění roviny ϱ, jimiž se reprodukuje obdélník $ABCD$, je grupa vzhledem

k postupnému skládání $\star$ těchto přemístění. Najděte neutrální prvek operace $\star$ a ke každému prvku množiny M udejte inverzní prvek vzhledem k operaci $\star$. b) Úlohu opakujte pro množinu M všech přemístění roviny ϱ, jimiž se reprodukuje čtverec $ABCD$.

20. Je dána množina $\mathsf{M} = \{a, b\}$. V množině M udejte operaci $\circ$ tak, aby M byla grupou vzhledem k této operaci. Úlohu opakujte pro množinu $\mathsf{M} = \{a, b, c\}$ a pro množinu $\mathsf{M} = \{a, b, c, d\}$.

3. kapitola

MNOŽINY SE DVĚMA OPERACEMI

Největší důležitost pro nás budou mít množiny, v nichž jsou definovány dvě operace. Jednu z těchto operací budeme nazývat sčítání a druhou násobení.

Definice 7. Nechť jsou v množině M definovány operace $\oplus$ a $\odot$, které mají tyto vlastnosti:

1. Pro každé $[x, y] \in M \times M$ existuje $x \oplus y \in M$ i $x \odot y \in M$.
2. Obě operace jsou komutativní a asociativní.
3. Operace $\odot$ je distributivní vzhledem k operaci $\oplus$.

Pak se operace $\oplus$ nazývá *sčítání* a operace $\odot$ se nazývá *násobení* v množině M.

Neutrální prvek sčítání se nazývá *nulový prvek* a neutrální prvek násobení se nazývá *jednotkový prvek*. Inverzní prvek sčítání se jmenuje *opačný prvek* a inverzní prvek násobení se jmenuje *převrácený prvek*.

Množina M, v níž je definováno sčítání a násobení, se nazývá *polookruh*.

Pro takto definované operace jsme zavedli symboly $\oplus$ a $\odot$, aby nám to připomínalo běžně užívané symboly $+$ a $.$ pro sčítání a násobení čísel. Uvedené operace však nemusí mít se sčítáním a násobením čísel nic společného.

Polookruh může být grupou vzhledem k sčítání $\oplus$, může být také grupou vzhledem k násobení $\odot$, ale nemusí tomu

tak být, protože nemusí obsahovat ani nulový prvek, ani jednotkový prvek a také ke každému prvku polookruhu nemusí existovat ani opačný prvek, ani převrácený prvek. O existenci těchto prvků se v definici 7 nic nepředpokládá.

Požadavky uvedené v definici 7 můžeme rozepsat takto: Pro každé $x \in \mathsf{M}$, pro každé $y \in \mathsf{M}$ a pro každé $z \in \mathsf{M}$ je

$$x \oplus y = y \oplus x, \qquad x \odot y = y \odot x,$$
$$(x \oplus y) \oplus z = x \oplus (y \oplus z), \qquad (x \odot y) \odot z = x \odot (y \odot z),$$
$$(x \oplus y) \odot z = (x \odot z) \oplus (y \odot z).$$

Pro úplnost můžeme poznamenat, že se v některých knihách komutativnost a asociativnost násobení nepředpokládá a pak se polookruh, v němž je násobení komutativní, označuje názvem komutativní polookruh a polookruh, v němž je násobení asociativní, názvem asociativní polookruh. My se však budeme zabývat pouze polookruhy, které jsou komutativní a asociativní, a nebudeme si proto zbytečně komplikovat názvosloví.

Příklad 12. Množina N_0 všech přirozených čísel (včetně nuly) s obyčejným sčítáním a násobením, jak je známe ze školy, je polookruh, neboť ke každé dvojici $[x, y] \in \mathsf{N}_0 \times \mathsf{N}_0$ jsou definována čísla $x + y \in \mathsf{N}_0$, $xy \in \mathsf{N}_0$ a pro libovolná čísla x, y, z množiny N_0 je

$$x + y = y + x, \qquad xy = yx,$$
$$(x + y) + z = x + (y + z), \qquad (xy)z = x(yz),$$
$$(x + y)z = xz + yz.$$

Nulovým prvkem je tu číslo 0 a jednotkovým prvkem je číslo 1, neboť pro každé $x \in \mathsf{N}_0$ je

$$x + 0 = 0 + x = x, \quad x.1 = 1.x = x.$$

Opačný prvek existuje pouze k číslu 0 a je jím zase číslo 0; převrácený prvek existuje pouze k číslu 1 a je jím zase

číslo 1. Také množina N všech přirozených čísel (bez nuly) je polookruh. Ten však nemá nulový prvek; jednotkovým prvkem je opět číslo 1. Rovněž množina S všech sudých přirozených čísel (bez nuly) je polookruh; v něm však neexistuje ani nulový, ani jednotkový prvek. Také množina C všech celých čísel, množina Q všech racionálních čísel, množina R všech reálných čísel a množina K všech komplexních čísel jsou polookruhy. Ve všech těchto polookruzích je nulovým prvkem číslo 0 a jednotkovým prvkem číslo 1.

Ukážeme si ještě dva příklady polookruhů, v nichž jsou operace $\oplus$ a $\odot$ definovány jinak než obvykle.

Příklad 13. Budiž L množina všech lichých kladných čísel. V množině L budeme definovat operace $\oplus$ a $\odot$ takto:

$$x \oplus y = x + y + 1, \quad x \odot y = \tfrac{1}{2}(x + 1)(y + 1) - 1.$$

Máme ukázat, že množina L s takto definovaným sčítáním a násobením je polookruh.

Ke každé dvojici $[x, y] \in \mathsf{L} \times \mathsf{L}$ přísluší čísla $x \oplus y$, $x \odot y$, která patří také do L. To je zřejmé, neboť součet $x + y$ dvou lichých čísel je sudé číslo a $x \oplus y = x + y + 1$ je tedy liché číslo; čísla $x + 1$, $y + 1$ jsou obě sudá, jejich součin je násobek čtyř a polovina tohoto součinu je násobek dvou, takže číslo $x \odot y = \frac{1}{2}(x + 1)(y + 1) - 1$ je liché. Jsou-li dále čísla x, y kladná, jsou i čísla $x \oplus y$, $x \odot y$ kladná a patří tedy do L.

Operace $\oplus$ a $\odot$ mají i další vlastnosti uvedené v definici 7.

a) Komutativnost: Platí

$$x \oplus y = x + y + 1, \quad y \oplus x = y + x + 1.$$

Odtud však je vidět, že pro každá dvě čísla x, y množiny L je $x \oplus y = y \oplus x$. Podobně

$$x \circ y = \tfrac{1}{2}(x+1)(y+1) - 1,$$
$$y \circ x = \tfrac{1}{2}(y+1)(x+1) - 1,$$

takže pro každá dvě čísla x, y množiny L je $x \circ y = y \circ x$.

b) Asociativnost: Platí

$$(x \oplus y) \oplus z = (x + y + 1) + z + 1,$$
$$x \oplus (y \oplus z) = x + (y + z + 1) + 1,$$

takže pro každá tři čísla x, y, z množiny L je $(x \oplus y) \oplus z = x \oplus (y \oplus z)$. Podobně

$$(x \circ y) \circ z = \tfrac{1}{2}\left(\tfrac{1}{2}(x+1)(y+1) - 1 + 1\right)(z+1) - 1,$$
$$x \circ (y \circ z) = \tfrac{1}{2}(x+1)\left(\tfrac{1}{2}(y+1)(z+1) - 1 + 1\right) - 1$$

a odtud po velmi snadné úpravě vyplývá, že pro každ tři čísla x, y, z množiny L je $(x \circ y) \circ z = x \circ (y \circ z)$.

c) Distributivnost operace $\circ$ vzhledem k operaci $\oplus$: Platí

$$(x \oplus y) \circ z = \tfrac{1}{2}(x + y + 1 + 1)(z+1) - 1,$$
$$(x \circ z) \oplus (y \circ z) = \tfrac{1}{2}(x+1)(z+1) - 1 + \tfrac{1}{2}(y+1)(z+1) - 1 + 1.$$

Lehko ověříme, že obě tato čísla jsou si rovna, takže pro každá tři čísla x, y, z množiny L je $(x \oplus y) \circ z = (x \circ z) \oplus (y \circ z)$.

Je tedy vskutku operace $\oplus$ sčítání a operace $\circ$ násobení v množině L. Podle naší definice je tedy např. $3 \oplus 5 = 9$, $5 \oplus 5 = 11$, $3 \circ 5 = 11$, $5 \circ 5 = 17$ atd.

Nulový prvek v polookruhu L neexistuje, neboť neexistuje takové $n \in \mathsf{L}$, aby pro všecka $x \in \mathsf{L}$ bylo $x \oplus n = x$, čili

$$x + n + 1 = x.$$

Jednotkovým prvkem polookruhu L je číslo 1, neboť podmínku $x \circ n = x$, neboli

$$\tfrac{1}{2}(x+1)(n+1) - 1 = x,$$

můžeme upravit na tvar

$$(x + 1)(n - 1) = 0,$$

což platí pro $n = 1$ a pro každé $x \in \mathsf{L}$.

Možná, že by čtenáře zajímalo, jaký rozumný smysl můžeme dát operacím $\oplus$ a $\odot$ v množině L. Poněvadž je číslo 1 jednotkový prvek polookruhu L, hraje číslo 1 v polookruhu L tutéž úlohu jako číslo 1 v polookruhu N všech přirozených čísel (bez nuly). Poněvadž dále $1 \oplus 1 = 1 + 1 + 1 = 3$, má číslo 3 v polookruhu L tutéž úlohu jako číslo $1 + 1 = 2$ v polookruhu N. Z toho, že $3 \oplus 1 = 3 + 1 + 1 = 5$, soudíme, že číslu $5 \in \mathsf{L}$ odpovídá číslo $2 + 1 = 3 \in \mathsf{N}$ atd. Matematickou indukcí se dá dokázat, že každé číslo $x = 2u - 1 \in \mathsf{L}$ odpovídá číslu $u \in \mathsf{N}$. Obdobně číslo $y = 2v - 1 \in \mathsf{L}$ odpovídá číslu $v \in \mathsf{N}$. Pak také číslo

$$x \oplus y = x + y + 1 = 2u - 1 + 2v - 1 + 1 = 2(u + v) - 1 \in \mathsf{L}$$

odpovídá číslu $u + v \in \mathsf{N}$ a číslo

$$x \odot y = \tfrac{1}{2}(x + 1)(y + 1) - 1 = \tfrac{1}{2}(2u - 1 + 1)(2v - 1 + 1) - 1 = 2uv - 1 \in \mathsf{L}$$

odpovídá číslu $uv \in \mathsf{N}$. Množina L tedy vznikne z množiny N pouhým přejmenováním prvků: místo $u \in \mathsf{N}$ píšeme $2u - 1 \in \mathsf{L}$. Obě množiny se liší pouze označením svých prvků. Kdyby se byl historický vývoj matematiky odehrál tak, že by se k zapisování přirozených čísel užívalo pouze znaků, jimiž dnes zapisujeme prvky množiny L, museli bychom počítat podle pravidel platných v polookruhu L. Pak by výpočty $3 \oplus 5 = 9$, $5 \oplus 5 = 11$, $3 \odot 5 = 11$, $5 \odot 5 = 17$ znamenaly totéž jako naše obvyklé výpočty $2 + 3 = 5$, $3 + 3 = 6$, $2.3 = 6$, $3.3 = 9$ atd. Nahlédneme to například z tabulky

N	1	2	3	4	5	6	7	8	9	10	...
L	1	3	5	7	9	11	13	15	17	19	...

v níž jsou pod sebou uvedeny ty prvky množin N a L, které si navzájem odpovídají. Podle ní můžeme každý výpočet v množině N „přeložit" do množiny L tak, že prvky množiny N nahradíme odpovídajícími prvky množiny L a operace $+$ a $\cdot$ v množině N operacemi $\oplus$ a $\odot$ v množině L. Má tedy výpočet $2 + 3 = 5$ v množině N týž význam jako výpočet $3 \oplus 5 = 9$ v množině L apod.

Úmluva. V dalším textu budeme zapisovat sčítání v polookruhu M znakem $+$ a násobení znakem $\cdot$ (popř. budeme znak násobení vůbec vynechávat). Nulový prvek budeme označovat znakem 0 a jednotkový prvek znakem 1. Opačný prvek k prvku a budeme označovat $-a$ a převrácený prvek k prvku a budeme označovat a^{-1}.

Tohoto označení budeme užívat i tehdy, nebude-li mít sčítání a násobení v polookruhu M nic společného se sčítáním a násobením čísel. Kdyby však mohlo nastat nedorozumění, vrátíme se k dosavadním znakům $\oplus$ a $\odot$.

Příklad 14. Budiž M množina skládající se z prvků 0, 1, tj. $M = \{0, 1\}$. V množině M budeme definovat sčítání a násobení takto:

$$0 + 0 = 0,\ 0 + 1 = 1 + 0 = 1 + 1 = 1,$$
$$0.0 = 0.1 = 1.0 = 0,\ 1.1 = 1.$$

Abychom mohli tvrdit, že množina M s takto definovaným sčítáním a násobením je polookruh, musíme ověřit, že jsou splněny všecky požadavky z definice 7.

Oba výkony jsou definovány pro všecky dvojice $[x,$

$y] \in \mathsf{M} \times \mathsf{M}$, jak je patrné z jejich zavedení. Také komutativnost sčítání i násobení odtud bezprostředně vyplývá. Asociativnost těchto operací ověříme tak, že vyšetříme postupně všecky případy, které mohou nastat:

$$(0 + 0) + 0 = 0 + 0 = 0, \quad 0 + (0 + 0) = 0 + 0 = 0,$$
$$(0 + 0) + 1 = 0 + 1 = 1, \quad 0 + (0 + 1) = 0 + 1 = 1,$$
$$(0 + 1) + 0 = 1 + 0 = 1, \quad 0 + (1 + 0) = 0 + 1 = 1,$$
$$(1 + 0) + 0 = 1 + 0 = 1, \quad 1 + (0 + 0) = 1 + 0 = 1,$$
$$(0 + 1) + 1 = 1 + 1 = 1, \quad 0 + (1 + 1) = 0 + 1 = 1,$$
$$(1 + 0) + 1 = 1 + 1 = 1, \quad 1 + (0 + 1) = 1 + 1 = 1,$$
$$(1 + 1) + 0 = 1 + 0 = 1, \quad 1 + (1 + 0) = 1 + 1 = 1,$$
$$(1 + 1) + 1 = 1 + 1 = 1, \quad 1 + (1 + 1) = 1 + 1 = 1.$$

Obdobně bychom ověřili i asociativnost násobení. Ještě je třeba ukázat, že násobení je distributivní vzhledem ke sčítání:

$$(0 + 0).0 = 0.0 = 0, \qquad 0.0 + 0.0 = 0 + 0 = 0,$$
$$(0 + 0).1 = 0.1 = 0, \qquad 0.1 + 0.1 = 0 + 0 = 0,$$
$$(0 + 1).0 = 1.0 = 0, \qquad 0.0 + 1.0 = 0 + 0 = 0,$$
$$(1 + 0).0 = 1.0 = 0, \qquad 1.0 + 0.0 = 0 + 0 = 0,$$
$$(0 + 1).1 = 1.1 = 1, \qquad 0.1 + 1.1 = 0 + 1 = 1,$$
$$(1 + 0).1 = 1.1 = 1, \qquad 1.1 + 0.1 = 1 + 0 = 1,$$
$$(1 + 1).0 = 1.0 = 0, \qquad 1.0 + 1.0 = 0 + 0 = 0,$$
$$(1 + 1).1 = 1.1 = 1, \qquad 1.1 + 1.1 = 1 + 1 = 1.$$

Uvedený postup jsme mohli poněkud zkrátit, neboť tu jde o komutativní operace a není třeba znovu provádět výpočty, které vzniknou pouhou záměnou prvků; úspora takto vzniklá však je jen nepatrná. To tedy znamená, že množina M je opravdu polookruh, v němž je operace $+$ sčítání a operace $.$ násobení. (Bylo by možné také ukázat, že v polookruhu M je sčítání distributivní vzhledem k násobení, ale to nás v tomto okamžiku nezajímá.)

Prvek 0 je nulovým prvkem polookruhu M, neboť

$$0 + 0 = 0, \quad 1 + 0 = 0 + 1 = 1,$$

a prvek 1 je jeho jednotkovým prvkem, protože

$$0.1 = 1.0 = 0, \quad 1.1 = 1.$$

Opačný prvek existuje pouze k prvku 0 a tímto opačným prvkem je zase prvek 0, neboť $0 + 0 = 0$, takže $-0 = 0$. Převrácený prvek existuje pouze k prvku 1 a tímto převráceným prvkem je zase prvek 1, neboť $1.1 = 1$, takže $1^{-1} = 1$. K prvku 1 neexistuje opačný prvek a k prvku 0 neexistuje převrácený prvek, protože neexistuje žádné $x \in M$ tak, aby $1 + x = 0$, popř. $0.x = 1$.

Čtenář se asi ptá, jaký smysl má toto podivné počítání. Označme Z nějakou množinu výroků (pravdivých i nepravdivých), která má tu vlastnost, že ke každým dvěma výrokům **A**, **B** z množiny Z patří do Z i jejich alternativa **A nebo B** a konjunkce **A a zároveň B**. Množinu Z můžeme rozložit do dvou tříd: do jedné, kterou označíme symbolem 0, zařadíme všecky nepravdivé výroky z množiny Z a do druhé, kterou označíme symbolem 1, zařadíme všecky pravdivé výroky z množiny Z. Označme dále $M = \{0, 1\}$. Patří-li výrok **A** do třídy $x \in M$ a výrok **B** do třídy $y \in M$, patří výrok **A nebo B** do třídy $x + y \in M$ a výrok **A a zároveň B** do třídy $xy \in M$. Uvedené definice sčítání a násobení v množině M nejsou nic jiného než pravidla známá z logiky:

Jsou-li dva výroky nepravdivé, je i jejich alternativa nepravdivá,
je-li aspoň jeden ze dvou výroků pravdivý, je jejich alternativa pravdivá;
je-li aspoň jeden ze dvou výroků nepravdivý, je jejich konjunkce nepravdivá,
jsou-li dva výroky pravdivé, je jejich konjunkce pravdivá.

Zavedené počítání nám dovoluje zcela mechanicky rozhodnout o pravdivosti či nepravdivosti každého výroku zce-

la libovolně složeného z alternativy a konjunkce výroků.

Ukažme si to na této úloze: Jednoho cestovatele zajali divoši a uvěznili ho v místnosti se dvěma východy pod dozorem dvou strážců. Náčelník kmene řekl zajatci: „Jeden východ vede na svobodu a druhý na smrt. Tvoji strážci vědí, kam který východ vede, a můžeš se jich na to zeptat. Smíš však položit jen jedinou otázku a jen jedinému z nich a nesmíš se ptát, co by řekl ten druhý. Ale upozorňuji tě, že jeden ze strážců mluví vždycky pravdu a druhý stále lže.“ Cestovatel chvíli přemýšlel, pak vyslovil otázku a na základě odpovědi, kterou dostal, spolehlivě rozhodl, který východ vede na svobodu. Jak zněla ta otázka?

Vžijme se do situace ubohého cestovatele. Zajímá ho pravdivost dvou výroků:

A: Tento východ vede na svobodu.
B: Ty mluvíš pravdu.

Z těchto výroků musí sestavit takový složený výrok **X**, aby kladná odpověď na otázku: „Je pravda, že **X**?“ znamenala, že výrok **A** je pravdivý, a aby záporná odpověď znamenala, že výrok **A** je nepravdivý, a to bez ohledu na pravdivost či nepravdivost výroku **B**. Sestaví-li všecky možnosti, které mohou nastat, do přehledné tabulky, dostane:

A	B	X*	X
1	1	1	1
1	0	1	0
0	1	0	0
0	0	0	1

Ve sloupcích označených **A**, **B** jsou zapsány pravdivostní třídy, do nichž patří výroky **A**, **B**, ve sloupci označeném **X*** je uvedena odpověď, kterou cestovatel dostane (znak 1 značí „ano", znak 0 značí „ne") a ve sloupci nadepsaném **X** je uvedena skutečná pravdivostní třída, do níž patří výrok **X**. Kromě výroků **A**, **B** zavedeme ještě dva další výroky, které jsou jejich negacemi:

A′: Tento východ vede na smrt.
B′: Ty lžeš.

Potom úloze vyhovuje tento výrok **X**:

(**A a zároveň B**) **nebo** (**A**′ **a zároveň B**′).

Označíme-li pravdivostní třídy výroků **A**, **B**, **A**′, **B**′, **X** po řadě písmeny a, b, a', b', x, pak

$$x = ab + a'b';$$

přitom pro $a = 1$ je $a' = 0$, pro $a = 0$ je $a' = 1$, pro $b = 1$ je $b' = 0$ a pro $b = 0$ je $b' = 1$. Lehko se přesvědčíme, že takto vypočtená třída x splňuje podmínky vyjádřené výše uvedenou tabulkou. Otázka, kterou cestovatel položí, zní tedy takto: „Je pravda, že tento východ vede na svobodu a ty přitom mluvíš pravdu nebo že vede na smrt a ty přitom lžeš?"*)

Podle věty 1 existuje v každém polookruhu M nejvýše jeden nulový prvek 0 a podle věty 2 existuje ke každému prvku $a \in \mathsf{M}$ nejvýše jeden opačný prvek $-a \in \mathsf{M}$. Mezi všemi polookruhy jsou nejdůležitější takové, v nichž existu-

*) Podmínku, že se nesmí ptát žádného ze strážců na to, co by řekl druhý strážce, položil náčelník cestovateli proto, aby mu zabránil položit otázku: „Co by mi odpověděl tvůj kamarád, kdybych se ho zeptal, vede-li tento východ na svobodu?" Odpověď na tuto otázku totiž vyjadřuje negaci skutečného stavu bez ohledu na to, kterému strážci byla položena, neboť jeden z nich — lhostejno který — mluví pravdu a druhý lže.

je právě jeden nulový prvek a v nichž ke každému prvku existuje právě jeden opačný prvek, tj. polookruhy, které jsou vzhledem ke sčítání (komutativními) grupami.

Definice 8. Polookruh M, který je (komutativní) grupou vzhledem k sčítání, se nazývá *okruh*. Tato grupa se jmenuje *aditivní grupa okruhu* M.

Podle věty 3 existuje ke každým dvěma prvkům a, b okruhu M právě jeden prvek $x \in M$, pro který platí

$$a + x = b$$

a v důsledku komutativnosti sčítání také $x + a = b$. Tento prvek můžeme podle téže věty vyjádřit v tvaru

$$x = b + (-a),$$

kde $-a$ je opačný prvek k prvku a.

Definice 9. Prvek x, pro který platí

$$a + x = b,$$

označujeme názvem *rozdíl* prvků b, a (v tomto pořádku) a píšeme $x = b - a$.

Operace, která k prvkům b, a množiny M přiřazuje nejvýše jeden rozdíl $b - a \in M$, nazývá se *odčítání*.

Z věty 3 tedy vyplývá, že ke každým dvěma prvkům b, a okruhu M existuje jediný rozdíl $b - a \in M$ a že

$$b - a = b + (-a),$$

takže rozdíl prvků b, a můžeme nahradit součtem prvku b a opačného prvku $-a$. Je-li $b = 0$, plyne odtud

$$0 - a = 0 + (-a) = -a;$$

můžeme tedy opačný prvek $-a$ považovat za rozdíl $0 - a$. Je-li $b = a$, pak

$$a - a = a + (-a) = 0;$$

rozdílem dvou sobě rovných prvků tedy je nulový prvek 0.

Na základě věty 4 můžeme říci toto: Existuje-li ke každým dvěma prvkům b, a polookruhu M i rozdíl $b - a \in \mathsf{M}$, pak polookruh M je okruh, tj. je to grupa vzhledem k sčítání.

Jestliže polookruh není okruh, může se stát, že k některým jeho prvkům b, a rozdíl $b - a$ neexistuje, popř. není určen jednoznačně.

Příklad 15. Množina C všech celých čísel je okruh, neboť ke každým dvěma jeho prvkům b, a existuje rozdíl $b - a \in \mathsf{C}$. Tento rozdíl je jediný a platí

$$b - a = b + (-a).$$

Obdobné tvrzení můžeme vyslovit i o množině Q všech racionálních čísel, o množině R všech reálných čísel i o množině K všech komplexních čísel. Naproti tomu množina N_0 všech přirozených čísel (včetně nuly) není okruh a v něm existuje rozdíl $b - a$ pouze tehdy, je-li $b \geqq a$, ale v případě $b < a$ rozdíl $b - a$ neexistuje. Ani množina $\mathsf{M} = \{0, 1\}$ z příkladu 14 není okruh; je sice $0 - 0 = 0$, $1 - 0 = 1$, ale rozdíl $0 - 1$ neexistuje, protože neexistuje žádné $x \in \mathsf{M}$, pro které by bylo $1 + x = 0$, a rozdíl $1 - 1$ není v množině M určen jednoznačně, protože podmínku $1 + x = 1$ splňuje $x = 0$ i $x = 1$.

Věta 5. Pro každý prvek x okruhu M platí

$$0.x = 0;$$

přitom 0 je nulový prvek okruhu M.

Důkaz. Zvolme některý prvek $a \in M$. Podle definice nulového prvku je

$$a + 0 = a.$$

Odtud na základě distributivnosti násobení vzhledem k sčítání vyplývá, že pro každé $x \in M$ je

$$ax = (a + 0)x = ax + 0.x,$$

takže

$$0.x = ax - ax = 0.$$

To tedy znamená, že součin dvou prvků okruhu M, z nichž aspoň jeden je nulový, je roven tomuto nulovému prvku. Nesmíme se však nechat svést k ukvapenému závěru, že také obráceně z rovnosti

$$xy = 0$$

vyplývá, že musí být buď $x = 0$, nebo $y = 0$. Existují okruhy, v nichž $xy = 0$ přesto, že $x \neq 0$ i $y \neq 0$. Dříve však, než uvedeme příklad takového okruhu, vyslovíme definici:

Definice 10. Prvky $x \neq 0, y \neq 0$, pro něž je

$$xy = 0,$$

nazývají se *dělitelé nuly*.

Příklad 16. Budiž C množina všech celých čísel a $m > 1$ přirozené číslo, které budeme nazývat *modul*. Dělíme-li libovolné číslo $x \in C$ modulem m, dostaneme neúplný podíl q a zbytek r, přičemž

$$x = mq + r, \quad 0 \leqq r < m,$$

kde q, r jsou čísla z množiny C. Uvedenými podmínkami jsou čísla q, r stanovena jednoznačně. Všech možných zbytků je celkem m; jsou to čísla

$$0, 1, 2, 3, \ldots, m - 1.$$

Všecka celá čísla, která při dělení modulem m dávají týž zbytek r, tvoří množinu, kterou budeme nazývat *zbytková třída podle modulu m*. Všech zbytkových tříd podle modulu m je právě tolik, kolik je různých zbytků, tj. m, a každé celé číslo patří právě do jedné z nich. Zbytkovou třídu, do níž patří číslo x, budeme označovat $\{x\}$; tento symbol znamená množinu všech celých čísel, která při dělení modulem m dávají týž zbytek jako číslo x. Dává-li číslo x při dělení modulem m zbytek r, pak čísla x_1, x_2 patří do třídy $\{x\}$ právě tehdy, existují-li taková celá čísla q_1, q_2, že

$$x_1 = mq_1 + r, \; x_2 = mq_2 + r,$$

a to nastane právě tehdy, když

$$x_1 - x_2 = m(q_1 - q_2) = mq,$$

kde q je celé číslo, čili když je jejich rozdíl násobkem modulu m.

Vezmeme-li nyní dvě zbytkové třídy $\{x\}$, $\{y\}$ a zvolíme-li libovolná čísla $x_1 \in \{x\}$, $x_2 \in \{x\}$, $y_1 \in \{y\}$, $y_2 \in \{y\}$, pak podle toho, co už víme, jsou rozdíly $x_1 - x_2$, $y_1 - y_2$ násobky modulu m, tj.

$$x_1 - x_2 = mq, \; y_1 - y_2 = mq',$$

kde q, q' jsou vhodná celá čísla. Odtud vychází

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = \\ = mq + mq' = m(q + q'),$$

takže čísla $x_1 + y_1$, $x_2 + y_2$ patří také do téže zbytkové třídy podle modulu m. Podobně dostaneme

$$(x_1 - y_1) - (x_2 - y_2) = (x_1 - x_2) - (y_1 - y_2) = \\ = mq - mq' = m(q - q'),$$

a proto i čísla $x_1 - y_1$, $x_2 - y_2$ patří do téže zbytkové třídy podle modulu m. A konečně

$$x_1y_1 - x_2y_2 = (x_1 - x_2)y_1 + x_2(y_1 - y_2) =$$
$$= mqy_1 + x_2mq' = m(qy_1 + q'x_2),$$

a to znamená, že čísla x_1y_1, x_2y_2 patří rovněž do téže zbytkové třídy podle modulu m.

Odtud plyne: Zvolíme-li zbytkové třídy $\{x\}$, $\{y\}$ a vybereme-li zcela libovolně v každé z těchto tříd po jednom čísle, pak zbytkové třídy, do nichž patří součet, rozdíl a součin těchto vybraných čísel, závisí jen na volbě zbytkových tříd $\{x\}$, $\{y\}$ a nezávisí na tom, která čísla z tříd $\{x\}$, $\{y\}$ jsme zvolili k výpočtu. Součty $x_1 + y_1$, $x_2 + y_2$ patří ovšem do téže třídy jako součet $x + y$, tj. do třídy $\{x + y\}$, a podobná tvrzení platí i o rozdílu a součinu.

To nám umožní definovat v množině C_m všech zbytkových tříd podle modulu m operace takto:

$\{x\} + \{y\} = \{x + y\}$, $\{x\} - \{y\} = \{x - y\}$, $\{x\}\{y\} = \{xy\}$.

Můžeme říci, že součtem zbytkových tříd $\{x\}$, $\{y\}$ podle modulu m rozumíme tu zbytkovou třídu podle modulu m, do níž patří součet $x + y$, a podobně můžeme interpretovat i další napsané definice operací. Sčítání a násobení tříd má vlastnosti požadované v definici 7, jak se dá snadno ověřit. To tedy znamená, že množina C_m s uvedeným sčítáním a násobením je polookruh. Poněvadž dále ke každým dvěma zbytkovým třídám podle modulu m existuje i jejich rozdíl, je množina C_m s uvedenými operacemi dokonce okruh; říkáme mu *okruh zbytkových tříd podle modulu m.*

Nulovým prvkem je třída $\{0\}$, neboť pro každou třídu $\{x\}$ je

$$\{x\} + \{0\} = \{x + 0\} = \{x\}.$$

Všimněme si nyní dělitelů nuly, tj. ptejme se, za jakých podmínek může v okruhu C_m být

$$\{x\}\{y\} = \{0\}.$$

To lze přepsat v tvaru

$$\{xy\} = \{0\},$$

který říká, že číslo xy musí patřit do třídy $\{0\}$, tj. musí dávat při dělení modulem m zbytek 0 a musí tedy být násobkem modulu m, takže

$$xy = mq,$$

kde q je vhodné celé číslo. Mohou nastat dva případy:

a) Je-li m prvočíslo, pak aspoň jedno z čísel x, y musí být násobkem čísla m,*) a to znamená, že buď $\{x\} = \{0\}$, nebo $\{y\} = \{0\}$.V okruhu zbytkových tříd podle prvočíselného modulu tedy neexistují dělitelé nuly.

b) Je-li však m složené číslo, tj. je-li $m = m_1 m_2$, kde $1 < m_1 < m$, $1 < m_2 < m$, může se stát, že číslo x je násobkem čísla m_1 a číslo y násobkem čísla m_2 a žádné z nich není násobkem modulu m. Pak $\{x\} \neq \{0\}$, $\{y\} \neq \{0\}$, a přitom $\{x\}\{y\} = \{0\}$, takže obě třídy jsou děliteli nuly.

Okruh C_2 zbytkových tříd podle modulu 2 obsahuje dvě třídy $\{0\}$, $\{1\}$. Třídu $\{0\}$ tvoří všecka sudá čísla a třídu $\{1\}$ všecka lichá čísla. Sčítání a násobení v okruhu C_2 je definováno takto:

$$\{0\} + \{0\} = \{0\},\ \{0\} + \{1\} = \{1\} + \{0\} = \{1\},$$

$$\{1\} + \{1\} = \{0\},$$

$$\{0\}\{0\} = \{0\}\{1\} = \{1\}\{0\} = \{0\},\ \{1\}\{1\} = \{1\}.$$

Tyto rovnosti ovšem neznamenají nic jiného než známá pravidla: Součet dvou sudých čísel je sudé číslo, součet dvou čísel, z nichž jedno je sudé a druhé liché, je liché číslo atd. Poněvadž je číslo 2 prvočíslo, neexistují v okruhu C_2 dělitelé nuly. Prvek $\{0\}$ je nulovým prvkem a prvek $\{1\}$ jednotkovým prvkem okruhu C_2, takže $-\{0\} = \{0\}$, $-\{1\} = \{1\}$, $\{1\}^{-1} = \{1\}$, ale převrácený prvek k prvku $\{0\}$ neexistuje.

*) Používáme tu známé věty: je-li součin xy dvou celých čísel násobkem prvočísla m, pak aspoň jedno z čísel x, y je násobkem prvočísla m, tj. buď $x = mq_1$, nebo $y = mq_2$, kde q_1, q_2 jsou celá čísla.

Ukážeme ještě příklad okruhu C_6 zbytkových tříd podle modulu 6. Tento okruh má šest prvků, jejichž sčítání a násobení je dáno následujícími tabulkami.

$\{x\} + \{y\}$

$\{x\}$ \ $\{y\}$	{0}	{1}	{2}	{3}	{4}	{5}
{0}	{0}	{1}	{2}	{3}	{4}	{5}
{1}	{1}	{2}	{3}	{4}	{5}	{0}
{2}	{2}	{3}	{4}	{5}	{0}	{1}
{3}	{3}	{4}	{5}	{0}	{1}	{2}
{4}	{4}	{5}	{0}	{1}	{2}	{3}
{5}	{5}	{0}	{1}	{2}	{3}	{4}

$\{x\}\{y\}$

$\{x\}$ \ $\{y\}$	{0}	{1}	{2}	{3}	{4}	{5}
{0}	{0}	{0}	{0}	{0}	{0}	{0}
{1}	{0}	{1}	{2}	{3}	{4}	{5}
{2}	{0}	{2}	{4}	{0}	{2}	{4}
{3}	{0}	{3}	{0}	{3}	{0}	{3}
{4}	{0}	{4}	{2}	{0}	{4}	{2}
{5}	{0}	{5}	{4}	{3}	{2}	{1}

Odtud je vidět, že v okruhu C_6 zbytkových tříd podle modulu 6 je $\{2\}\{3\} = \{0\}$, $\{3\}\{4\} = \{0\}$, takže třídy $\{2\}$, $\{3\}$, $\{4\}$ jsou dělitelé nuly v tomto okruhu. Také v okruhu C_6 je prvek $\{0\}$ nulovým prvkem a prvek $\{1\}$ jednotkovým prvkem; proto $-\{0\} = \{0\}$, $-\{1\} = \{5\}$, $-\{2\} = \{4\}$, $-\{3\} = \{3\}$, $-\{4\} = \{2\}$, $-\{5\} = \{1\}$, $\{1\}^{-1} = \{1\}$, $\{5\}^{-1} = \{5\}$ a převrácené prvky k prvkům $\{0\}$, $\{2\}$, $\{3\}$, $\{4\}$ neexistují. Z toho je vidět, že v okruhu může podmínku $a = -a$ splňovat i jiný prvek než nulový a podmínku $a = a^{-1}$ i jiný prvek než jednotkový.

Příklad 17. Máme zjistit, pro která celá čísla n je číslo $3n^2 + 2n + 7$ násobkem pěti. Úlohu můžeme formulovat tak, že se ptáme, je-li možné, aby číslo $3n^2 + 2n + 7$ patřilo do zbytkové třídy $\{0\}$ podle modulu 5, čili aby $\{3n^2 + 2n + 7\} = \{0\}$. Podle pravidel o počítání v okruhu C_5 zbytkových tříd podle modulu 5 je

$$\{3n^2 + 2n + 7\} = \{3\}\{n\}^2 + \{2\}\{n\} + \{2\}.$$

Dosadíme-li sem za $\{n\}$ postupně všecky zbytkové třídy podle modulu 5, dostaneme

$$\{3\}\{0\}^2 + \{2\}\{0\} + \{2\} = \{0\} + \{0\} + \{2\} = \{2\},$$
$$\{3\}\{1\}^2 + \{2\}\{1\} + \{2\} = \{3\} + \{2\} + \{2\} = \{2\},$$
$$\{3\}\{2\}^2 + \{2\}\{2\} + \{2\} = \{2\} + \{4\} + \{2\} = \{3\},$$
$$\{3\}\{3\}^2 + \{2\}\{3\} + \{2\} = \{2\} + \{1\} + \{2\} = \{0\},$$
$$\{3\}\{4\}^2 + \{2\}\{4\} + \{2\} = \{3\} + \{3\} + \{2\} = \{3\}.$$

Odtud je vidět, že úlohu řeší všecka celá čísla $n \in \{3\}$, tj. všecka čísla $n = 5k + 3$, kde k je celé číslo.

Příklad 18. Značí-li písmeno n libovolné celé číslo, máme dokázat, že z čísel $n^3 - 1$, n^3, $n^3 + 1$ je právě jedno násobkem sedmi. Budeme vyšetřovat, do které zbytkové třídy podle modulu 7 patří čísla $n^3 - 1$, n^3, $n^3 + 1$. Poněvadž

$$\{n^3 - 1\} = \{n\}^3 - \{1\}, \{n^3\} = \{n\}^3, \{n^3 + 1\} = \{n\}^3 + \{1\},$$

stačí za $\{n\}$ brát postupně všecky zbytkové třídy podle modulu 7:

$$\{0\}^3 = \{0\}, \{0\}^3 - \{1\} = \{6\}, \{0\}^3 + \{1\} = \{1\},$$
$$\{1\}^3 = \{1\}, \{1\}^3 - \{1\} = \{0\}, \{1\}^3 + \{1\} = \{2\},$$
$$\{2\}^3 = \{1\}, \{2\}^3 - \{1\} = \{0\}, \{2\}^3 + \{1\} = \{2\},$$
$$\{3\}^3 = \{6\}, \{3\}^3 - \{1\} = \{5\}, \{3\}^3 + \{1\} = \{0\},$$
$$\{4\}^3 = \{1\}, \{4\}^3 - \{1\} = \{0\}, \{4\}^3 + \{1\} = \{2\},$$
$$\{5\}^3 = \{6\}, \{5\}^3 - \{1\} = \{5\}, \{5\}^3 + \{1\} = \{0\},$$
$$\{6\}^3 = \{6\}, \{6\}^3 - \{1\} = \{5\}, \{6\}^3 + \{1\} = \{0\}.$$

Patří-li tedy číslo n do zbytkové třídy $\{0\}$, je číslo n^3 násobkem sedmi; patří-li číslo n do některé ze zbytkových tříd $\{1\}$, $\{2\}$, $\{4\}$, je číslo $n^3 - 1$ násobkem sedmi; patří-li číslo n do některé ze zbytkových tříd $\{3\}$, $\{5\}$, $\{6\}$, je číslo $n^3 + 1$ násobkem sedmi.

Definice 11. Okruh, v němž neexistují dělitelé nuly, se nazývá *obor integrity*.

Příklad 19. Množina C všech celých čísel, množina Q všech racionálních čísel, množina R všech reálných čísel i množina K všech komplexních čísel jsou obory integrity, neboť jsou to okruhy, v nichž je podmínka $xy = 0$ splněna jen tehdy, když buď $x = 0$, nebo $y = 0$. Množina S všech sudých čísel (kladných, záporných i nuly) je rovněž obor integrity. Také každý okruh C_p zbytkových tříd podle prvočíselného modulu p je obor integrity. Oborem integrity není například množina N_0 všech přirozených čísel (včetně nuly), neboť to není okruh, nebo okruh C_m zbytkových tříd podle složeného modulu m, neboť v něm existují dělitelé nuly.

V oboru integrity platí tato věta:

Věta 6. Jsou-li x, y prvky oboru integrity a je-li $a \neq 0$, pak z rovnosti

$$ax = ay$$

vyplývá rovnost

$$x = y.$$

Důkaz. Rovnost $ax = ay$ můžeme přepsat v tvaru $ax - ay = 0$ a tu zase podle cvič. 22e) na str. 52 v tvaru $a(x - y) = 0$. Poněvadž jde o obor integrity, v němž neexistují dělitelé nuly, a poněvadž podle předpokladu je $a \neq 0$, musí být $x - y = 0$, čili $x = y$.

Věta 6 neplatí v okruhu, který není oborem integrity, neboť tam se může stát, že prvek a je dělitelem nuly, a pak může být $a(x - y) = 0$, i když $x - y \neq 0$.

Větu 6 často formulujeme v tvaru: V oboru integrity lze rovnost „krátit" nenulovým prvkem tohoto oboru integrity.

Vraťme se však zase k polookruhům. Podle věty 1 existuje v každém polookruhu M nejvýše jeden jednotkový prvek 1 a podle věty 2 existuje ke každému $a \in M$ nejvýše jeden převrácený prvek $a^{-1} \in M$. Zvláštní pozornost si zasluhují polookruhy, v nichž existuje právě jeden jednotkový prvek a v nichž ke každému nenulovému prvku existuje právě jeden převrácený prvek, tj. polookruhy, jejichž nenulové prvky tvoří vzhledem k násobení (komutativní) grupu. Přitom ovšem do pojmu polookruhu zahrnujeme i okruhy.

Definice 12. Tvoří-li všecky nenulové prvky polookruhu M (komutativní) grupu M′ vzhledem k násobení, nazývá se tato grupa *multiplikativní grupa polookruhu* M. Okruh, jehož nenulové prvky tvoří multiplikativní grupu, nazývá se *těleso*.

Multiplikativní grupu polookruhu M budeme označovat M'.

Podle věty 3 existuje ke každým dvěma prvkům a, b multiplikativní grupy M' polookruhu M právě jeden prvek $x \in M'$, pro který platí

$$ax = b$$

a v důsledku komutativnosti násobení také

$$xa = b.$$

Tento prvek můžeme podle téže věty vyjádřit v tvaru

$$x = ba^{-1},$$

kde a^{-1} je převrácený prvek k prvku a.

Definice 13. Prvek x, pro který platí

$$ax = b,$$

označujeme názvem *podíl* prvků b, a (v tomto pořádku) a píšeme

$$x = \frac{b}{a} \text{ nebo také } x = b : a.$$

Operace, která k prvkům b, a polookruhu M přiřazuje nejvýše jeden podíl $\frac{b}{a} \in M$, nazývá se *dělení*.

Z věty 3 tedy vyplývá, že ke každým dvěma prvkům b, a multiplikativní grupy M' polookruhu M existuje jediný podíl $\frac{b}{a} \in M'$ a že

$$\frac{b}{a} = ba^{-1},$$

takže podíl prvků b, a můžeme nahradit součinem prvku b a převráceného prvku a^{-1}. Je-li $b = 1$, plyne odtud

$$\frac{1}{a} = 1.a^{-1} = a^{-1};$$

můžeme tedy převrácený prvek a^{-1} považovat za podíl $\frac{1}{a}$. Je-li $b = a$, pak

$$\frac{a}{a} = a.a^{-1} = 1;$$

podílem dvou sobě rovných prvků tedy je jednotkový prvek 1.

Je-li M obor integrity a je-li $b = 0$, pak pro každé $a \neq 0$ je $\frac{0}{a} = 0$, neboť podmínku $ax = 0$ v oboru integrity splňuje jediný prvek $x = 0$. Avšak i v mnohých polookruzích, které nejsou obory integrity, je $\frac{0}{a} = 0$ pro každé $a \neq 0$. Naproti tomu pro $a = 0$ podíl $\frac{b}{0}$ nedefinujeme v žádném polookruhu pro žádné b.

Je-li M těleso, pak z předcházejících úvah vyplývá, že v něm existuje podíl $\frac{b}{a}$ kterýchkoli dvou prvků b, $a \neq 0$. Je-li $a = 0$, podíl $\frac{b}{a}$ neexistuje.

Na základě věty 4 můžeme říci toto: Existuje-li ke každým dvěma prvkům b, $a \neq 0$, polookruhu M podíl $\frac{b}{a}$, pak nenulové prvky polookruhu M tvoří multiplikativní grupu, a je-li M okruh, je to těleso. Každé těleso tedy obsahuje dvě grupy: jednak aditivní grupu, kterou tvoří

všecky jeho prvky bez výjimky, jednak multiplikativní grupu, kterou tvoří všecky jeho nenulové prvky. Každé těleso T obsahuje nulový prvek 0 a jednotkový prvek 1, přičemž $0 \neq 1$; kdyby bylo $0 = 1$, pak by pro každé $x \in T$ bylo $x = x.1 = x.0 = 0$ a multiplikativní grupa by neexistovala, neboť těleso T by v tomto případě obsahovalo jediný prvek 0 a po jeho vynechání bychom dostali prázdnou množinu, která však nemůže být grupou.

Příklad 20. Množina Q všech racionálních čísel, množina R všech reálných čísel i množina K všech komplexních čísel s obvykle definovaným sčítáním a násobením jsou tělesa, neboť jsou to aditivní grupy a všechny jejich nenulové prvky tvoří multiplikativní grupu. Množiny Q' všech nenulových racionálních čísel, R' všech nenulových reálných čísel a K' všech nenulových komplexních čísel nejsou tělesa; jsou to sice multiplikativní grupy, ale nejsou to aditivní grupy, neboť v nich chybí nulový prvek 0. Totéž platí i o množině Q^+ všech kladných racionálních čísel a o množině R^+ všech kladných (reálných) čísel. Množina C všech celých čísel rovněž není těleso; je to sice aditivní grupa, ale po vynechání nulového prvku z ní nevznikne multiplikativní grupa. Množina C_7 všech zbytkových tříd pole modulu 7 je těleso, neboť je to aditivní grupa a vynecháním nulového prvku $\{0\}$ vznikne multiplikativní grupa (viz cvič. 27 na str. 53). Totéž platí pro každou množinu C_p všech zbytkových tříd podle prvočíselného modulu p. Naproti tomu množina C_8 všech zbytkových tříd podle modulu 8 není těleso, neboť po vynechání nulového prvku $\{0\}$ nevznikne multiplikativní grupa (viz cvič. 28 na str. 53). Totéž platí o každé množině C_m zbytkových tříd podle složeného modulu m.

Věta 7. V tělese neexistují dělitelé nuly.

Důkaz. Nechť pro prvky x, y tělesa T je

$$xy = 0,$$

kde 0 je nulový prvek. Je-li $y = 0$, nejsou prvky x, y dělitelé nuly. Je-li $y \neq 0$, existuje k němu převrácený prvek y^{-1}. Pak

$$x = x.1 = x(yy^{-1}) = (xy)y^{-1} = 0.y^{-1} = 0,$$

takže x, y nejsou dělitelé nuly ani v tomto případě.

To však znamená, že každé těleso je také oborem integrity a že tedy okruh, který není oborem integrity, nemůže být tělesem.

Cvičení. 21. Za předpokladu, že existují napsané symboly, dokažte následující rovnosti pro prvky x, y libovolného polookruhu:

$$\text{a) } -(x+y) = (-x) + (-y),$$

$$\text{b) } -(x-y) = (-x) + y,$$

$$\text{c) } x(-y) = (-x)y = -(xy), \quad \text{d) } (-x)(-y) = xy.$$

22. Za předpokladu, že jsou jednoznačně definovány napsané symboly, dokažte následující rovnosti pro prvky x, y, z libovolného polookruhu:

$$\text{a) } (x+y) - z = x + (y-z),$$

$$\text{b) } x - (y+z) = (x-y) - z,$$

$$\text{c) } x - (y-z) = (x-y) + z,$$

$$\text{d) } (x+z) - (y+z) = x - y, \quad \text{e) } x(y-z) = xy - xz.$$

23. Za předpokladu, že existují napsané symboly, dokažte následující rovnosti pro prvky x, y libovolného polookruhu:

$$\text{a) } (xy)^{-1} = x^{-1}y^{-1}, \quad \text{b) } (x:y)^{-1} = x^{-1}y, \quad \text{c) } (-x):y = x:(-y) = -(x:y), \quad \text{d) } (-x):(-y) = x:y.$$

24. Za předpokladu, že jsou jednoznačně definovány napsané symboly, dokažte následující rovnosti pro prvky x, y, z libovolného polookruhu:

a) $(xy) : z = x.(y : z)$, b) $x : (yz) = (x : y) : z$,

c) $x : (y : z) = (x : y).z$, d) $(xz) : (yz) = x : y$.

25. Za předpokladu, že jsou jednoznačně definovány napsané symboly, dokažte následující rovnosti pro prvky x, y, u, v libovolného polookruhu:

a) $\frac{x}{u} = \frac{y}{v}$, právě když $vx = uy$, b) $\frac{x}{u} + \frac{y}{v} = \frac{vx + uy}{uv}$,

c) $\frac{x}{u} - \frac{y}{v} = \frac{vx - uy}{uv}$, d) $\frac{x}{u}.\frac{y}{v} = \frac{xy}{uv}$, e) $\frac{x}{u} : \frac{y}{v} = \frac{x}{u}.\frac{v}{y} = \frac{vx}{uy}$.

26. Ověřte, že operace definované vzorci $\{x\} + \{y\} = \{x + y\}$, $\{x\} - \{y\} = \{x - y\}$, $\{x\}\{y\} = \{xy\}$ v množině C_m všech zbytkových tříd podle modulu m (viz str. 43) jsou opravdu sčítání, odčítání a násobení.

27. V tělese C_7 zbytkových tříd podle modulu 7 najděte a) nulový prvek, b) jednotkový prvek, c) ke každému prvku opačný prvek, d) ke každému nenulovému prvku převrácený prvek a ověřte tak, že C_7 je těleso.

28. Pokuste se o totéž v okruhu C_8 zbytkových tříd podle modulu 8 a ukažte, že C_8 není těleso.

29. Dokažte, že číslo $n^2 + n + 2$ není pro žádné celé číslo n násobkem patnácti.

30. Nechť množina M je komutativní grupa vzhledem k operaci $\oplus$ (sčítání). Definujeme-li v množině M další operaci $\odot$ vzorcem $x \odot y = 0$ pro každé $x \in M$ a pro každé $y \in M$, je operace $\odot$ násobení. Dokažte.

31. V intervalu $N = \langle 0, 10 \rangle$ jsou dány operace max (sčítání) a min (násobení) — viz cvič. 8 na str. 14. Najděte nulový a jednotkový prvek tohoto polookruhu. Je tento polookruh okruhem?

32. V množině M všech podmnožin množiny Z jsou dány operace $\cup$ (sčítání) a $\cap$ (násobení) — viz cvič. 9 na str. 14. Najděte nulový a jednotkový prvek tohoto polookruhu. Je polookruh M okruhem?

33. V množině N všech přirozených čísel (bez nuly) jsou dány operace: největší společný dělitel (sčítání) a nejmenší společný násobek (násobení) — viz cvič. 10 na str. 14. Vyšetřte existenci nulového a jednotkového prvku tohoto polookruhu.

34. V množině C všech celých čísel jsou dány operace $\oplus$ (sčítání) a $\odot$ (násobení) vzorci: $x \oplus y = x + y + 1$, $x \odot y = xy + x + y$. Ukažte, že množina C s takto definovanými operacemi je obor intengrity. Najděte jeho nulový a jednotkový prvek.

35. Opakujte cvič. 34 pro množinu Q všech racionálních čísel a pro operace $\oplus$ a $\odot$ dané vzorci: $x \oplus y = x + y - 1$, $x \odot y = x + y - xy$. Je množina Q s operacemi $\oplus$ a $\odot$ těleso? Který je jeho nulový a jednotkový prvek?

36. Jak je třeba definovat sčítání a násobení v množině M, která má právě dva různé prvky, aby vznikl obor integrity s jednotkovým prvkem? Je tento obor integrity těleso?

37. Jak je třeba definovat sčítání a násobení v množině M, která má právě tři různé prvky, aby vznikl obor integrity s jednotkovým prvkem? Je tento obor integrity těleso?

38. Řešte obdobnou úlohu pro množinu M, která má právě čtyři navzájem různé prvky.

39. Ukažte, že jednoprvková množina $M = \{0\}$, v níž je definováno sčítání $0 + 0 = 0$ a násobení $0.0 = 0$, je obor integrity. Proč to není těleso?

40. Jsou-li a, b racionální čísla, pak množina M všech čísel tvaru $a + b\sqrt{2}$, v níž je definováno sčítání a násobení obvyklým způsobem, je těleso. Dokažte.

4. kapitola

VNĚJŠÍ OPERACE

Dosud jsme se zabývali operacemi v množině M, tj. operacemi, jichž se zúčastnily pouze prvky množiny M. Označíme-li takovou operaci např. symbolem $\circ$, jde tu o tři prvky množiny M: $x \in M$, $y \in M$, $x \circ y \in M$. Tyto operace budeme nazývat *vnitřní*. Jsou však možné i operace *vnější*, tj. operace, jichž se zúčastní jednak prvky množiny M, jednak prvky jiné množiny N, která nemusí mít s množinou M vůbec nic společného. Jde tu vlastně o operaci v množině $M \cup N$. Uvedeme příklad jedné takové operace.

Definice 14. Budiž M množina, v níž je definována operace $\circ$, která má neutrální prvek n. Budiž dále N_0 množina všech přirozených čísel (včetně nuly). V množině $M \cup N_0$ definujeme operaci $\square$ takto:

Je-li $x \in M$, $r \in N_0$, pak $x \square r \in M$ a platí

1. $x \square 0 = n$,
2. $x \square (r + 1) = (x \square r) \circ x$

za předpokladu, že prvek $(x \square r) \circ x \in M$ existuje pro každé $r \in N_0$.

Přitom nevylučujeme, že $N_0 \subset M$.

Operace $\square$ je v definici 14 definována indukcí: V bodu 1 je vysloveno, co máme rozumět symbolem $x \square 0$, a bod 2 udává rekurentním vzorcem, jak se vypočítá prvek $x \square \square (r + 1)$ na základě (už známého) prvku $x \square r$.

Rozepíšeme-li podle definice 14 prvky $x \square r$ pro několik malých čísel, r, dostaneme:

$$x \square 0 = n,$$
$$x \square 1 = (x \square 0) \circ x = n \circ x = x,$$
$$x \square 2 = (x \square 1) \circ x = x \circ x,$$
$$x \square 3 = (x \square 2) \circ x = (x \circ x) \circ x,$$
$$x \square 4 = (x \square 3) \circ x = [(x \circ x) \circ x] \circ x$$

atd. Je-li operace $\circ$ asociativní, můžeme v konečných výsledcích závorky vynechat, neboť na jejich umístění nezáleží. Pak je

$$x \square 0 = n, \quad x \square 1 = x, \quad x \square 2 = x \circ x,$$
$$x \square 3 = x \circ x \circ x, \quad x \square 4 = x \circ x \circ x \circ x$$

atd., takže se prvek $x \square r$ pro $r \geqq 2$ jeví jako výsledek operace $\circ$ aplikované postupně na r prvků vesměs rovných prvku x.

Příklad 21. Vnější operaci $\square$, která byla zavedena v definici 14, dobře známe ze školy i z praxe. Je-li M číselný polookruh a vezmeme-li za operaci $\circ$ násobení v tomto polookruhu, dají se podmínky 1 a 2 z definice 14 přepsat v tvaru

$$1.\ x \square 0 = 1,$$
$$2.\ x \square (r + 1) = (x \square r).x,$$

neboť neutrálním prvkem násobení je číslo 1. Je však zřejmé, že číslo $x \square r \in M$ není nic jiného než *mocnina* $x^r \in M$, jejímž exponentem je přirozené číslo $r \in N_0$, neboť mocniny s přirozeným exponentem se definují rekurentně takto:

$$1.\ x^0 = 1,$$
$$2.\ x^{r+1} = x^r.x,$$

ale to je totéž jako předcházející vzorce. Poněvadž je náso-

bení asociativní operace, můžeme několik mocnin s nejmenšími přirozenými exponenty rozepsat takto:

$$x^0 = 1, \quad x^1 = x, \quad x^2 = x.x, \quad x^3 = x.x.x, \quad x^4 = x.x.x.x$$

atd., jak je dobře známo ze školy. Uvedené vzorce platí pro každé (komplexní) číslo x.

Příklad 22. Jiný neméně dobře známý příklad vnější operace $\square$ je tvoření tzv. *přirozených násobků*, které vzniknou tak, že v číselném polookruhu M vezmeme za operaci $\circ$ sčítání a za prvek n neutrální prvek sčítání, tj. číslo 0. Dostaneme vzorce

$$1.\ x \square 0 = 0,$$
$$2.\ x \square (r + 1) = (x \square r) + x.$$

Je-li $\mathsf{N}_0 \subset \mathsf{M}$, můžeme položit $x \square r = xr$ a máme dobře známé vzorce

$$1.\ x.0 = 0,$$
$$2.\ x(r + 1) = xr + x,$$

z nichž vyplývá, že

$$x.0 = 0, \quad x.1 = x, \quad x.2 = x + x,$$
$$x.3 = x + x + x, \quad x.4 = x + x + x + x$$

atd. Také tyto vzorce platí pro každé (komplexní) číslo x.

Příklad 23. Jako další příklad vezmeme množinu M všech přemístění roviny ϱ, jimiž se reprodukuje rovnostranný trojúhelník ABC, s operací $\star$, jíž je postupné skládání těchto přemístění (viz příklad 8 na str. 19). Poněvadž je operace $\star$ asociativní a má neutrální prvek $\mathfrak{I}$, dostaneme pro každé $\mathfrak{X} \in \mathsf{M}$ postupně

$$\mathfrak{X} \square 0 = \mathfrak{I}, \mathfrak{X} \square 1 = \mathfrak{X}, \mathfrak{X} \square 2 = \mathfrak{X} \star \mathfrak{X}, \mathfrak{X} \square 3 = \mathfrak{X} \star \mathfrak{X} \star \mathfrak{X}$$

atd. Speciálně je

$$\mathfrak{I} \square 0 = \mathfrak{I}, \mathfrak{I} \square 1 = \mathfrak{I}, \mathfrak{I} \square 2 = \mathfrak{I} \star \mathfrak{I} = \mathfrak{I};$$

matematickou indukcí se dá dokázat, že pro každé $r \in \mathsf{N}_0$ je $\mathfrak{I} \square r = \mathfrak{I}$. Dále je

$$\mathfrak{S}_1 \square 0 = \mathfrak{I}, \mathfrak{S}_1 \square 1 = \mathfrak{S}_1, \mathfrak{S}_1 \square 2 = \mathfrak{S}_1 * \mathfrak{S}_1 = \mathfrak{I}$$

a odtud opět matematickou indukcí plyne, že pro každé sudé $r \in \mathsf{N}_0$ je $\mathfrak{S}_1 \square r = \mathfrak{I}$ a pro každé liché $r \in \mathsf{N}_0$ je $\mathfrak{S}_1 \square r = \mathfrak{S}_1$. Obdobná tvrzení platí i pro $\mathfrak{S}_2$ a $\mathfrak{S}_3$. Konečně

$$\mathfrak{R}_1 \square 0 = \mathfrak{I}, \ \mathfrak{R}_1 \square 1 = \mathfrak{R}_1, \ \mathfrak{R}_1 \square 2 = \mathfrak{R}_1 * \mathfrak{R}_1 = \mathfrak{R}_2,$$
$$\mathfrak{R}_1 \square 3 = \mathfrak{R}_2 \square \mathfrak{R}_1 = \mathfrak{I}$$

a pro každé $r = 3k$, kde $k \in \mathsf{N}_0$, je $\mathfrak{R}_1 \square r = \mathfrak{I}$, pro každé $r = 3k + 1$ je $\mathfrak{R}_1 \square r = \mathfrak{R}_1$ a pro každé $r = 3k + 2$ je $\mathfrak{R}_1 \square r = \mathfrak{R}_2$. Obdobně pro každé $r = 3k$ je $\mathfrak{R}_2 \square r = \mathfrak{I}$, pro každé $r = 3k + 1$ je $\mathfrak{R}_2 \square r = \mathfrak{R}_2$ a pro každé $r = 3k + 2$ je $\mathfrak{R}_2 \square r = \mathfrak{R}_1$.

Věta 8. Je-li operace $\circ$ v množině M asociativní, splňuje operace $\square$, která k ní přísluší podle definice 14, tyto vzorce:

a) $(x \square r) \circ (x \square s) = x \square (r + s)$,

b) $(x \square r) \square s = x \square (rs)$

pro každé $r \in \mathsf{N}_0$ a pro každé $s \in \mathsf{N}_0$; je-li nadto operace $\circ$ také komutativní, pak

c) $(x \square r) \circ (y \square r) = (x \circ y) \square r$

pro každé $r \in \mathsf{N}_0$.

Důkaz. Všechny tři vzorce dokážeme matematickou indukcí.

a) Zvolme libovolné přirozené číslo $r \in \mathsf{N}_0$.

I. Podle bodu 1 z definice 14 a podle vlastnosti neutrálního prvku n je

$$(x \square r) \circ (x \square 0) = (x \square r) \circ n = x \square r = x \square (r + 0).$$

II. Jestliže pro nějaké $s \in \mathsf{N}_0$ platí

$$(x \square r) \circ (x \square s) = x \square (r + s),$$

pak

$$(x \square r) \circ [x \square (s + 1)] = (x \square r) \circ [(x \square s) \circ x] =$$
$$= [(x \square r) \circ (x \square s)] \circ x = [x \square (r + s)] \circ x =$$
$$= x \square (r + s + 1).$$

Nejprve jsme použili bodu 2 z definice 14, potom asociovanosti operace $\circ$, dále předpokladu uvedeného na počátku bodu II a nakonec opět bodu 2 z definice 14.

Z bodů I a II vyplývá na základě principu matematické indukce, že vzorec a) platí pro každé libovolně zvolené $r \in \mathsf{N}_0$ a pro každé $s \in \mathsf{N}_0$.

b) Zvolme opět libovolné přirozené číslo $r \in \mathsf{N}_0$.

I. Podle bodu 1 z definice 14 je

$$(x \square r) \square 0 = n = x \square 0 = x \square (r.0).$$

II. Jestliže pro nějaké $s \in \mathsf{N}_0$ platí

$$(x \square r) \square s = x \square (rs),$$

pak

$$(x \square r) \square (s + 1) = [(x \square r) \square s] \circ (x \square r) =$$
$$= [x \square (rs)] \circ (x \square r) = x \square (rs + r) = x \square [r (s + 1)].$$

Nejprve jsme použili bodu 2 z definice 14, dále předpokladu uvedeného na počátku bodu II, potom vzorce a) a nakonec toho, že $rs + r = r (s + 1)$.

Z bodů I a II vyplývá na základě principu matematické indukce, že vzorec b) platí pro každé libovolně zvolené $r \in \mathsf{N}_0$ a pro každé $s \in \mathsf{N}_0$.

c) I. Podle bodu 1 z definice 14 a podle vlastností neutrálního prvku n je

$$(x \square 0) \circ (y \square 0) = n \circ n = n = (x \circ y) \square 0.$$

II. Jestliže pro nějaké $r \in \mathsf{N}_0$ platí

$$(x \square r) \circ (y \square r) = (x \circ y) \square r,$$

pak

$$[x \square (r+1)] \circ [y \square (r+1)] = [(x \square r) \circ x] \circ [(y \square r) \circ y] =$$
$$= \{[(x \square r) \circ x] \circ (y \square r)\} \circ y = \{(x \square r) \circ [x \circ (y \square r)]\} \circ$$
$$\circ y = \{(x \square r) \circ [(y \square r) \circ x]\} \circ y = \{[(x \square r) \circ (y \square r)] \circ$$
$$\circ x\} \circ y = [(x \square r) \circ (y \square r)] \circ (x \circ y) = [(x \circ y) \square r] \circ$$
$$\circ (x \circ y) = (x \circ y) \square (r+1).$$

Přitom jsme použili nejprve bodu 2 z definice 14, potom asociativnosti operace $\circ$, pak ještě jednou asociativnosti operace $\circ$, dále komutativnosti operace $\circ$, načež opět asociativnosti operace $\circ$ a potom ještě jednou asociativnosti operace $\circ$, dále předpokladu uvedeného na počátku bodu II a nakonec opět bodu 2 z definice 14.

Z bodů I a II vyplývá na základě principu matematické indukce, že vzorec c) platí pro každé $r \in \mathsf{N}_0$.

Příklad 24. Pro mocniny s přirozeným mocnitelem (viz příklad 21 na str. 56) dává věta 8 známé vzorce

$$\text{a)}\ x^r.x^s = x^{r+s},$$
$$\text{b)}\ (x^r)^s = x^{rs},$$
$$\text{c)}\ x^r.y^r = (xy)^r,$$

které platí vzhledem k tomu, že násobení je operace asociativní a komutativní. Z obdobného důvodu platí pro přirozené násobky (viz příklad 22 na str. 57) vzorce

$$\text{a)}\ xr + xs = x(r+s),$$
$$\text{b)}\ (xr)s = x(rs),$$
$$\text{c)}\ xr + yr = (x+y)r.$$

Naproti tomu pro operaci $\square$ vznikající opakovaným použitím operace $\star$ v množině M všech přemístění roviny ϱ,

která reprodukují rovnostranný trojúhelník ABC (viz příklad 23 na str. 57), platí jen vzorce

$$\text{a)}\quad (\mathfrak{X} \square r) \star (\mathfrak{X} \square s) = \mathfrak{X} \square (r + s),$$
$$\text{b)}\quad (\mathfrak{X} \square r) \square s = \mathfrak{X} \square (rs),$$

neboť operace $\star$ je asociativní. Tato operace však není komutativní, a proto neplatí vzorec c), jak je vidno například z toho, že

$$(\mathfrak{R}_1 \square 2) \star (\mathfrak{S}_1 \square 2) = \mathfrak{R}_2 \star \mathfrak{I} = \mathfrak{R}_2,$$

ale

$$(\mathfrak{R}_1 \star \mathfrak{S}_1) \square 2 = \mathfrak{S}_2 \square 2 = \mathfrak{I}.$$

Poznámka. V definici 14 jsme předpokládali, že operace $\circ$ má neutrální prvek n. Kdyby tomu tak nebylo, nebylo by možné použít definice 14 k definování prvku $x \square 0$. Mohli bychom to obejít například tak, že bychom položili $x \square 0 = y$, kde y je nějaký vhodný prvek množiny M. Pro takto definovanou operaci $\square$ ovšem neplatí věta 8, neboť při jejím důkazu bylo podstatné, že $x \square 0 = n$.

Druhá možnost, jak lze neexistenci neutrálního prvku operace $\circ$ obejít, je ta, že v definici 14 nahradíme bod 1 podmínkou $x \square 1 = x$. Pak však máme definovány prvky $x \square r$ jen pro taková $r \in \mathsf{N}_0$, pro něž platí $r \geqq 1$. V tomto případě věta 8 platí; v důkazu jejích vzorců je však třeba změnit bod I takto:

$$\text{a)}\quad (x \square r) \circ (x \square 1) = (x \square r) \circ x = x \square (r + 1),$$
$$\text{b)}\quad (x \square r) \square 1 = x \square r = x \square (r.1),$$
$$\text{c)}\quad (x \square 1) \circ (y \square 1) = x \circ y = (x \circ y) \square 1.$$

Cvičení. Ve cvič. 41—48 znamená symbol $\square$ vnější operaci podle definice 14, popř. podle předcházející poznámky.

41. Operace $\circ$ v množině R_0^+ všech nezáporných (reálných) čísel, která je dána vzorcem $x \circ y = \sqrt{x^2 + y^2}$ (viz cvič. 2 b) na str. 12), má neutrální prvek 0. Ukažte, že

pro každé $r \in \mathsf{N}_0$ je $x \square r = x \sqrt[r]{\ }$ a ověřte, že pro takto definovanou operaci $\square$ platí všechny vzorce z věty 8.

42. Operace $\circ$ v množině Q^+ všech kladných racionálních čísel, která je dána vzorcem $x \circ y = \frac{xy}{x+y}$ (viz cvič. 2a) na str. 12), nemá neutrální prvek. Ukažte, že tato operace vede k vnější operaci $x \square r = \frac{x}{r}$ a vyšetřete, splňuje-li tato vnější operace vzorce z věty 8.

43. Prostudujte vnější operaci $\square$ v číselném tělese T, která vznikne tak, že v definici 14 vezmete za operaci $\circ$ dělení a položíte $x \square 0 = 1$.

44. Řešte obdobnou úlohu s tím rozdílem, že za operaci $\circ$ vezmete odčítání a položíte $x \square 0 = 0$.

45. V tělese C_5 zbytkových tříd podle modulu 5 vyšetřete všechny přirozené násobky a všechny mocniny s přirozeným exponentem všech prvků tělesa C_5.

46. Tutéž úlohu řešte v okruhu C_6 zbytkových tříd podle modulu 6.

47. Ukažte, že v okruhu C_m zbytkových tříd podle modulu m je $\{m-1\}^{2k} = \{1\}$ a $\{m-1\}^{2k+1} = \{m-1\}$ pro všechna $k \in \mathsf{N}_0$.

48. Vyšetřte všecky prvky $\mathfrak{X} \square r$ v množině M všech přemístění roviny ϱ, jimiž se reprodukuje a) obdélník $ABCD$ b) čtverec $ABCD$ s operací $\star$ (viz cvič. 19 na str. 27).

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.

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

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

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 $M[x, y]$ polynomů dvou neurčitých oborem integrity, jak vyplývá dvojnásobným použitím věty 10. Ale obor integrity $M[x, y]$ 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 $M' \supset M$, dostaneme rovnost mezi polynomy jedné neurčité x nad okruhem M'. Nahradíme-li obě neurčité x, y libovolně zvolenými prvky okruhu $M' \supset M$, 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 $M' \supset M$, pak všecky koeficienty a_{ij}, b_{ij} polynomů A, B z okruhu $M[x, y]$ patří také do M'. Značí-li také y nějaký prvek okruhu M', jsou výpočty uvedené na str. 65 výpočty v okruhu $M'[x]$. Tyto výpočty však říkají, že vzorce pro součet a součin polynomů A, B jsou sestaveny tak, aby byly splněny pro každý prvek $y \in M'$, takže vzniká rovnost mezi polynomy jedné neurčité x okruhu $M'[x]$. 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

$$a_1b_1 = 1, \qquad a_1b_2 + a_2b_1 = 8,$$
$$a_2b_2 = 4, \qquad a_1b_3 + a_3b_1 = 2,$$
$$a_3b_3 = -2, \qquad a_2b_3 + a_3b_2 = -4.$$

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

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

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

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

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

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

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

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 $\mathsf{M}[x, y]$ můžeme vytvořit okruh $\mathsf{M}[x, y, z]$ polynomů tří neurčitých x, y, z nad okruhem M právě tak, jako jsme vytvořili okruh $\mathsf{M}[x, y]$ z okruhu $\mathsf{M}[x]$. 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 $a_{ijk} \in \mathsf{M}$ 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 $\mathsf{C}_2[x, y]$ 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 $\mathsf{M} \subset \mathsf{M}[x] \subset \mathsf{M}[x, y] \subset \mathsf{M}[x, y, z]$.

VÝSLEDKY CVIČENÍ A NÁVODY K JEJICH ŘEŠENÍ

1. Operace v množině

1. Všechny jsou komutativní, ale žádná není asociativní. — 2. Všechny jsou komutativní i asociativní. — 3. Plyne ze vzorců $(xy)^z = x^z y^z$, $(x : y)^z = x^z : y^z$. — 4. Operace $\star$ není komutativní, je však asociativní. Při komutativnosti stačí najít jediný případ, kdy $\mathfrak{X} \star \mathfrak{Y} \neq \mathfrak{Y} \star \mathfrak{X}$; při asociativnosti můžeme označit například $\mathfrak{X} = \begin{pmatrix} A & B & C \\ K & L & M \end{pmatrix}$, $\mathfrak{Y} = \begin{pmatrix} K & L & M \\ N & O & P \end{pmatrix}$, $\mathfrak{Z} = \begin{pmatrix} N & O & P \\ Q & R & S \end{pmatrix}$, kde KLM, NOP, QRS jsou permutace vrcholů A, B, C. — 5. a) M má 8 prvků; operace není komutativní, je však asociativní. b) M má 4 prvky; operace je komutativní i asociativní. — 6. a) Operace $\bigcirc$ není komutativní, ale je asociativní (ověřte konstrukčně i početně tak, že přímky p, q vezmete za osy souřadnic). b) Ověřte konstrukčně i početně. — 7. Je-li $O = [0, 0]$, $X = [x_1, y_1]$, $Y = [x_2, y_2]$, je $X \bigcirc Y = [x_1 + x_2, y_1 + y_2]$. — 8. Při komutativnosti je třeba odlišit případy $x \geqq y$, $y \geqq x$, při asociativnosti případy $x \geqq y \geqq z$, $x \geqq z \geqq y$, $y \geqq x \geqq z$, $y \geqq z \geqq x$, $z \geqq x \geqq y$, $z \geqq y \geqq x$. — 9. Použije se definice sjednocení a průniku (znázorněte Vennovými diagramy). — 10. Na základě rozkladu v prvočinitele a s využitím výsledku cvič. 8.

2. Neutrální a inverzní prvek. Grupa

11. Operace $\bigcirc$ má neutrální prvek $n = -1$ a inverzní prvek $\bar{x} = -x - 2$; operace $\star$ má neutrální prvek $n = 0$ a inverzní prvek

$\bar{x} = \frac{x}{x-1}$. V množině C existuje inverzní prvek operace $\star$ pouze k číslům 0 a 2, v množině R ke každému $x \neq 1$. — 12. Nemá neutrální prvek. — 13. Operace max má neutrální prvek $n \in M$, jestliže pro každé $x \in M$ je $x \geqq n$; inverzní prvek existuje pouze k číslu n a je $\bar{n} = n$. Obdobně pro operaci min. — 14. Neutrální prvek operace $\cup$ je $\varnothing$ a pak $\bar{\varnothing} = \varnothing$, neutrální prvek operace $\cap$ je Z a pak $\bar{Z} = Z$; k jiným prvkům inverzní prvky neexistují. — 15. Operace D nemá neutrální prvek; operace n má neutrální prvek 1 a je $\bar{1} = 1$, inverzní prvky k ostatním prvkům neexistují. — 17. M je grupa, $n = a$, $\bar{a} = a$, $\bar{b} = c$, $\bar{c} = b$. — 18. M není grupa, $n = b$, $\bar{a}$ neexistuje, $\bar{b} = b$, $\bar{c} = d$, $\bar{d} = c$. — 19. Neutrální prvek je identické přemístění $\mathfrak{I}$ a mimoto a) každý prvek je sám k sobě inverzní, b) každý prvek je sám k sobě inverzní s výjimkou rotací $\mathfrak{R} = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$, $\mathfrak{R}' = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}$, pro něž je $\overline{\mathfrak{R}} = \mathfrak{R}'$, $\overline{\mathfrak{R}'} = \mathfrak{R}$. — 20. Je-li a neutrální prvek, je operace $\bigcirc$ dána tabulkou

	a	b
a	a	b
b	b	a

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Pro $M = \{a, b, c, d\}$ dostaneme další případy, zaměníme-li mezi sebou prvky b, c, popř. b, d.

3. Množiny se dvěma operacemi

21. a) Z podmínek $x + (-x) = 0$, $y + (-y) = 0$ plyne $(x + y) + [(-x) + (-y)] = 0$; b) z podmínek $x + (-x) = 0$, $(-y) + y = 0$ plyne $(x - y) + [(-x) + y] = 0$; c) z podmínky $x + (-x) = 0$ plyne $xy + (-x)y = 0$ a z podmínky $y + (-y) = 0$ plyne $xy + x(-y) = 0$; d) plyne z c). — 22. a) Je-li $y - z = u$, je $y = u + z$ a pak po úpravě $x + y = (x + u) + z$; b) je-li $x - (y + z) = u$, je po úpravě $x = y + (z + u)$; c) je-li $x - y = u$ a $y - z = v$, je $x = u + y$, $y = z + v$ a odtud $x = (u + z) + v$; d) je-li $x - y = u$, je $x = u + y$ a pak $x + z = u + (y + z)$; e) je-li $y - z = u$, je $y = u + z$ a pak $xy = xu + xz$. — 23. a), b) Obdobně jako 21 a), b); c), d) plyne z 21 c). — 24. Obdobně jako 22 a), b), c), d). — 25. a) Je-li $\frac{x}{u} = z$, $\frac{y}{v} = z$, je $x = uz$, $y = vz$ a $vx = vuz$, $uy = uvz$; b), c) je-li $\frac{x}{u} = z$, $\frac{y}{v} = t$, je $x = uz$, $y = vt$ a pak $vx = vuz$, $uy = uvt$, $vx \pm uy = vuz \pm uvt$; za týchž podmínek je d) $xy = uz.vt$, e) $x \,.\, vt = y \,.\, uz$. — 26. Podle definice 7 a 9. — 27. a) $\{0\}$; b) $\{1\}$; c) — $\{0\} = \{0\}$, $-\{1\} = \{6\}$, $-\{2\} = \{5\}$, $-\{3\} = \{4\}$; d) $\{0\}^{-1}$ neexistuje, $\{1\}^{-1} = \{1\}$, $\{2\}^{-1} = \{4\}$, $\{3\}^{-1} = \{5\}$, $\{6\}^{-1} = \{6\}$. — 28. a) $\{0\}$; b) $\{1\}$; c) — $\{0\} = \{0\}$, $-\{1\} = \{7\}$, $-\{2\} = \{6\}$, $-\{3\} = \{5\}$, $-\{4\} = \{4\}$; d) $\{1\}^{-1} = \{1\}$, $\{3\}^{-1} = \{3\}$, $\{5\}^{-1} = \{5\}$, $\{7\}^{-1} = \{7\}$, $\{0\}^{-1}$, $\{2\}^{-1}$, $\{4\}^{-1}$, $\{6\}^{-1}$ neexistují. — 29. Stačí ukázat, že $\{n^3 + n + 2\} = \{n\}^2 + \{n\} + \{2\} \neq \{0\}$ pro všecky zbytkové třídy podle modulu 3 i pro všecky zbytkové třídy podle modulu 5. — 30. Podle definice 7. — 31. Nulovým prvkem je číslo 0, jednotkovým prvkem číslo 10; polookruh M není okruhem, viz cvič. 13. — 32. Nulovým prvkem je $\varnothing$, jednotkovým prvkem je Z; M není okruh, viz cvič. 14. — 33. Nulový prvek neexistuje, jednotkovým prvkem je číslo 1.

viz cvič. 15. — **34.** Podle definice 7, 8, 11; nulovým prvkem je číslo -1, jednotkovým prvkem číslo 0. — **35.** Podle definice 7, 8, 11, 12; nulovým prvkem je číslo 1, jednotkovým prvkem číslo 0. — **36.** Je-li a nulový prvek a b jednotkový prvek, pak

$x + y$:

	a	b
a	a	b
b	b	a

xy:

	a	b
a	a	a
b	a	b

— **37.** Je-li a nulový prvek a b jednotkový prvek, pak

$x + y$:

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

xy:

	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

Tabulku sčítání lze vyplnit jediným způsobem (viz cvič. 20), totéž platí pro první dva řádky a pro první dva sloupce tabulky pro násobení; nemůže být $c.c = a$, neboť M nemá dělitele nuly; nemůže být $c.c = c$, neboť pak by bylo $b = c$. — **38.** Obdobně musí být

$x + y$:

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

xy:

	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

První dva řádky a první dva sloupce tabulky pro násobení jsou zřejmé. Nemůže být $cd = a$, neboť neexistují dělitelé nuly; nemůže být $cd = c$, neboť $d \neq b$; nemůže být $cd = d$, neboť $c \neq b$; musí tedy být $cd = b$. Obdobně odvodíme, že $cc = d$, $dd = c$. První řádek a první sloupec tabulky pro sčítání je zřejmý. Nemůže být $b + c = a$, neboť pak by $bc + cc = ac$, čili $c + d = a$ a nevznikla by aditivní grupa. Není možné, aby $b + c = b$, neboť $c \neq a$; není možné, aby $b + c = c$, neboť $b \neq a$; musí tedy být $b + c = d$. Odtud $bc + cc = cd$. čili $c + d = b$ a obdobně $d + b = c$. — 39. Jsou splněny podmínky z definic 7, 8, 11. — 40. $(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$, $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}$,

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2} \cdot \sqrt{2}.$$

4. Vnější operace

41. $x \square 0 = 0 = x\sqrt{0}$, $x \square (r + 1) = (x \square r) \bigcirc x = \sqrt{x^2 r + x^2} = x\sqrt{r + 1}$. — 42. $x \square 1 = x$, $x \square (r + 1) = (x \square r) \bigcirc x = \frac{x^2}{r} : \left(\frac{x}{r} + x\right) = \frac{x}{r + 1}$. — 43. $x \square r = \frac{1}{x^r}$, $x \square (r + 1) = (x \square r) \bigcirc x = \frac{1}{x^r} : x = \frac{1}{x^{r+1}}$. — 44. $x \square r = -rx$, $x \square (r + 1) = (x \square r) \bigcirc x = -rx - x = -(r + 1)x$. — 45. $n\{0\} = \{0\}$ pro každé $n \in \mathsf{N}_0$; $0\{1\} = \{0\}$, $1\{1\} = \{1\}$, $2\{1\} = \{2\}$, $3\{1\} = \{3\}$, $4\{1\} = \{4\}$; $0\{2\} = \{0\}$, $1\{2\} = \{2\}$, $2\{2\} = \{4\}$, $3\{2\} = \{1\}$, $4\{2\} = \{3\}$ atd.; pro každé $n \in \mathsf{N}_0$ a pro každé $\{x\} \in \mathsf{C}_5$ je $(n + 5)\{x\} = n\{x\}$; $\{0\}^0 = \{1\}$, $\{0\}^n = \{0\}$ pro každé $n \geqq 1$; $\{1\}^n = \{1\}$ pro každé $n \in \mathsf{N}_0$; $\{2\}^0 = \{1\}$, $\{2\}^1 = \{2\}$, $\{2\}^2 = \{4\}$, $\{2\}^3 = \{3\}$, $\{2\}^{n+4} = \{2\}^n$ pro každé $n \in \mathsf{N}_0$; $\{3\}^0 = \{1\}$, $\{3\}^1 = \{3\}$, $\{3\}^2 = \{4\}$, $\{3\}^3 = \{2\}$, $\{3\}^{n+4} = \{3\}^n$ pro každé $n \in \mathsf{N}_0$; $\{4\}^0 = \{1\}$, $\{4\}^1 = \{4\}$, $\{4\}^{n+2} = \{4\}^n$ pro každé $n \in \mathsf{N}_0$. — 46. $n\{0\} = \{0\}$ pro každé $n \in \mathsf{N}_0$; $0\{1\} = \{0\}$, $1\{1\} = \{1\}$, $2\{1\} = \{2\}$, $3\{1\} =$

$= \{3\}$, $4\{1\} = \{4\}$, $5\{1\} = \{5\}$, $(n+6)\{1\} = n\{1\}$ pro každé $n \in \mathsf{N}_0$; $0\{2\} = \{0\}$, $1\{2\} = \{2\}$, $2\{2\} = \{4\}$, $(n+3)\{2\} = n\{2\}$ pro každé $n \in \mathsf{N}_0$; $0\{3\} = \{0\}$, $1\{3\} = \{3\}$, $(n+2)\{3\} = n\{3\}$ pro každé $n \in \mathsf{N}_0$; $0\{4\} = \{0\}$, $1\{4\} = \{4\}$, $2\{4\} = \{2\}$, $(n+3)\{4\} = n\{4\}$ pro každé $n \in \mathsf{N}_0$; $0\{5\} = \{0\}$, $1\{5\} = \{5\}$, $2\{5\} = \{4\}$, $3\{5\} = \{3\}$, $4\{5\} = \{2\}$, $5\{5\} = \{1\}$, $(n+6)\{5\} = n\{5\}$ pro každé $n \in \mathsf{N}_0$; $\{0\}^0 = \{1\}$, $\{0\}^n = \{0\}$ pro každé $n \geqq 1$; $\{1\}^n = \{1\}$ pro každé $n \in \mathsf{N}_0$; $\{2\}^0 = \{1\}$, $\{2\}^1 = \{2\}$, $\{2\}^2 = \{4\}$, $\{2\}^{n+2} = \{2\}^n$ pro každé $n \geqq 1$; $\{3\}^0 = \{1\}$, $\{3\}^n = \{3\}$ pro každé $n \geqq 1$; $\{4\}^0 = \{1\}$, $\{4\}^n = \{4\}$ pro každé $n \geqq 1$; $\{5\}^0 = \{1\}$, $\{5\}^1 = \{5\}$, $\{5\}^{n+2} = \{5\}^n$ pro každé $n \in \mathsf{N}_0$. — **47.** $\{m-1\}^3 = \{m^2 - 2m + 1\} = \{1\}$, $\{m-1\}^{2k} = (\{m-1\}^2)^k = \{1\}^k = \{1\}$, $\{m-1\}^{2k+1} = \{m-1\}^{2k}\{m-1\} = \{1\}\{m-1\} = \{m-1\}$. — **48.** a) $\mathfrak{X} \square 0 = \mathfrak{Z}$, $\mathfrak{X} \square 1 = \mathfrak{X}$, $\mathfrak{X} \square (n+2) = \mathfrak{X} \square n$ pro každé $n \in \mathsf{N}_0$. b) Pro každé $\mathfrak{X} \neq \mathfrak{R}$, $\mathfrak{X} \neq \mathfrak{R}'$ je $\mathfrak{X} \square 0 = \mathfrak{Z}$, $\mathfrak{X} \square 1 = \mathfrak{X}$, $\mathfrak{X} \square (n+2) = \mathfrak{X} \square n$; $\mathfrak{R} \square 0 = \mathfrak{Z}$, $\mathfrak{R} \square 1 = \mathfrak{R}$, $\mathfrak{R} \square 2 = \mathfrak{R}''$, $\mathfrak{R} \square 3 = \mathfrak{R}'$, $\mathfrak{R} \square (n+4) = \mathfrak{R} \square n$ pro každé $n \in \mathsf{N}_0$ a obdobně pro $\mathfrak{R}'$; přitom $\mathfrak{R}'' = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$.

5. Polynomy jedné neurčité

49. a) 1; b) 2; c) 4; d) 2^r, neboť koeficient $a_r = \{1\}$, kdežto každé a_i pro $i < r$ může nabýt kterékoli z hodnot $\{0\}$, $\{1\}$. — **50.** 2.3^r, neboť koeficient a_r může nabýt pouze hodnot $\{1\}$, $\{2\}$, kdežto každé a_i pro $i < r$ kterékoli z hodnot $\{0\}$, $\{1\}$, $\{2\}$. — **53.** a) $y^4 - 3y^3 + 4y^2 - 2y + 1$; b) y^4. — **54.** a) $1 - x + x^2$, 0; b) $-\frac{29}{27} - \frac{4}{9}x - \frac{2}{3}x^2, \frac{56}{27} - \frac{46}{27}x$; c) $0, 1 - 2x + 3x^2$. — **55.** Je-li $A = a_0 + a_1x + a_2x^2 + \ldots + a_rx^r$, kde $a_r = \pm 1$, $B = b_0 + b_1x + b_2x^2 + \ldots + b_sx^s$, kde $b_s \neq 0$, a je-li $s \geqq r$, pak neúplný podíl $Q = q_0 + q_1x + q_2x^2 + \ldots + q_{s-r}x^{s-r}$ a zbytek $R = z_0 + z_1x + z_2x^2 + \ldots + z_{r-1}x^{r-1}$. Pro neznámé koeficienty q_i dostaneme $s - r + 1$ rovnic tvaru $a_rq_{s-r} = b_s$, $a_rq_{s-r-1} + a_{r-1}q_{s-r} = b_{s-1}$, $a_rq_{s-r-2} + a_{r-1}q_{s-r-1} + a_{r-2}q_{s-r} = b_{s-2}$, ..., z nichž je mož-

no postupně vypočítat $q_{s-r}, q_{s-r-1}, q_{s-r-2}, \ldots$, neboť $a_r = \pm 1$. Pro koeficienty z_i dostaneme r rovnic tvaru $c_i + z_i = b_i$, kde $0 \leqq i < r$, přičemž výraz c_i je utvořen z koeficientů a_j a (již vypočtených) q_k. — **56.** a) $(x - 6)(x - 9)$; b) $(x + 3)(x - 18)$; c) $(4x - 3)(3x - 4)$; d) $\left(x + \frac{1 + i\sqrt{3}}{2}\right)\left(x + \frac{1 - i\sqrt{3}}{2}\right)$; jednoho činitele můžeme přitom ještě násobit libovolným (komplexním) číslem $k \neq 0$ a druhého číslem $\frac{1}{k}$. — **57.** a) $(x + 1)(x + 2)(x + 3)$, b) $(x - 2)(x^2 + x + 1)$; c) $(x^2 + x + 1)(x^2 - x + 1)$; d) $(x^2 + x\sqrt{2} + 1)(x^2 - x\sqrt{2} + 1)$. — **58.** a) $(x + 1)(x + 2)(x + 3)$; b) $(x - 2)\left(x + \frac{1 + i\sqrt{3}}{2}\right)\left(x + \frac{1 - i\sqrt{3}}{2}\right)$; c) $\left(x + \frac{1 + i\sqrt{3}}{2}\right)\left(x + \frac{1 - i\sqrt{3}}{2}\right)\left(x - \frac{1 + i\sqrt{3}}{2}\right)\left(x - \frac{1 - i\sqrt{3}}{2}\right)$; d) $\left(x + \frac{1 + i}{\sqrt{2}}\right)\left(x + \frac{1 - i}{\sqrt{2}}\right)\left(x - \frac{1 + i}{\sqrt{2}}\right)\left(x - \frac{1 - i}{\sqrt{2}}\right)$. — **59.** Polynom $A + \bar{A}$ má koeficienty $a_i + \bar{a}_i$, kde $0 \leqq i \leqq r$, polynom $A\bar{A}$ má koeficienty $a_0\bar{a}_0, a_1\bar{a}_0 + a_0\bar{a}_1, a_2\bar{a}_0 + a_1\bar{a}_1 + a_0\bar{a}_2, \ldots$, což jsou reálná čísla. — **60.**

$\overline{a_0 + a_1 a + a_2 a^2 + \ldots + a_r a^r} = \bar{a}_0 + \bar{a}_1\bar{a} + \bar{a}_2\bar{a}^2 + \ldots + \bar{a}_r\bar{a}^r$.

6. Polynomy více neurčitých

63. a) $(2x - 3y + 1)(3x + 2y - 1)$; b) $[(1 + \sqrt{2})x - y + (1 - \sqrt{2})][(-1 + \sqrt{2})x + y - (1 + \sqrt{2})]$; c) $(x + iy - 1 + i)(x - iy - 1 - i)$; jednoho činitele můžeme přitom násobit libovolným komplexním číslem $k \neq 0$ a druhého číslem $\frac{1}{k}$; d) nelze rozložit. —

64. $a = -6$, $(x + 2y - 3)(x + 3y + 2)$. — **65.** $a = 2$, $[x - (1 - i)y + 1][x - (1 + i)y + 1]$; $a = 0$, $[x - (1 + i)y + i][x - (1 - i)y - i]$. — **66.** b) Polynom dvou neurčitých má nejvýše $k + 1$ členů k-tého stupně s různými exponenty; polynom r-tého stupně má

tedy nejvýše $1 + 2 + 3 + \ldots + (r + 1) = \frac{(r + 1)(r + 2)}{2}$ členů s různými exponenty. c) Podle b) dostaneme $\frac{1.2}{2} + \frac{2.3}{2} + \frac{3.4}{2} + \ldots + \frac{(r + 1)(r + 2)}{2} = \frac{(r + 1)(r + 2)(r + 3)}{6}$; jednotlivé členy upravíme podle vzorce $\frac{(k+1)(k+2)}{2} = \frac{(k+1)(k+2)(k+3-k)}{6} =$ $= -\frac{k(k+1)(k+2)}{6} + \frac{(k+1)(k+2)(k+3)}{6}$. — **68.** Položíme a) $x = a, y = b, z = -c$; b) $x = b, y = c, z = a$. — **70.** Položíme a) $x = a, y = b, z = d, u = c$; b) $x = b, y = a, z = d, u = c$; c) $x = a, y = c, z = d, u = b$. — **71.** Vychází se z nerovnosti $(x - y)^2 + (x - z)^2 + (y - z)^2 \geqq 0$. — **72.** $x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 - xy + y^2 - xz - yz + z^2)$ a dále podle cvič. 71. — **73.** $(x + y + z)(x + \varepsilon y + \varepsilon^2 z)(x + \varepsilon^2 y + \varepsilon z)$, kde $\varepsilon = \frac{-1 + i\sqrt{3}}{2}$. — **74.** $(x + y + z)(x + y - z)(x - y + z)(x - y - z)$.

OBSAH

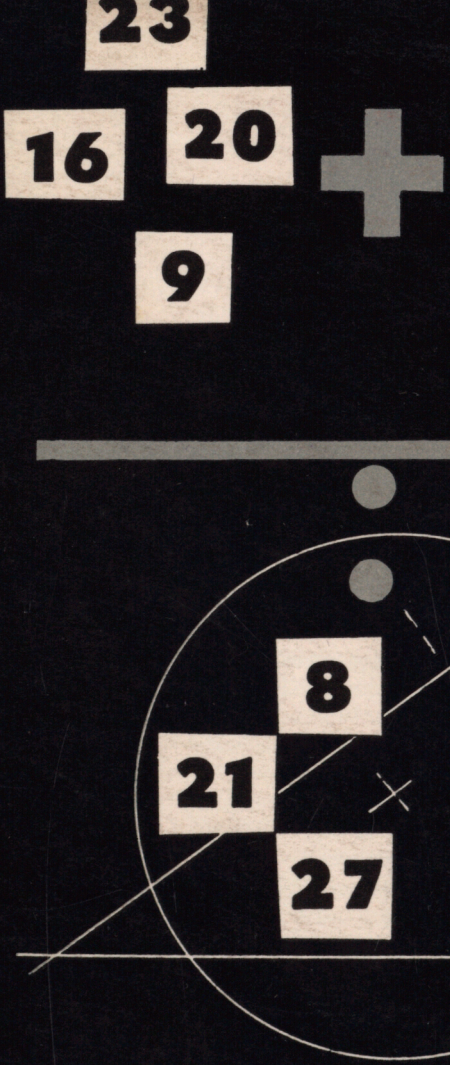
ŠKOLA MLADÝCH MATEMATIKŮ

polynomy v moderní algebře

KAREL HRUŠA

Pro účastníky matematické olympiády
vydává ÚV Matematické olympiády
v nakladatelství Mladá fronta
Řídí akademik Josef Novák
Obálku navrhl Jaroslav Příbramský
Odpovědný redaktor Milan Daneš
Publikace číslo 2906
Edice Škola mladých matematiků, svazek 26
Vytiskl Mír, novinářské závody, n. p.,
závod 6, Praha 2, Legerova 22
4,48 AA, 4,62 VA. 104 stran
Náklad 5500 výtisků. 1. vydání
Praha 1970. 508/21/8.5

23-028-70 03-2 Cena brož. výt. Kčs 8,—



23-028-70
03/2
Cena brož.
Kčs 8,—