Polynomy v moderní algebře

1. kapitola. Operace v množině

In: Karel Hruša (author): Polynomy v moderní algebře. (Czech). Praha: Mladá fronta, 1970. pp. 5–14.

Persistent URL: http://dml.cz/dmlcz/403712

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 $x \in$ M, $y \in$ M, označovat symbolem M $\times$ M. Dvě uspořádané dvojice $[x, y] \in$ M $\times$ M, $[z, u] \in$ M $\times$ 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.

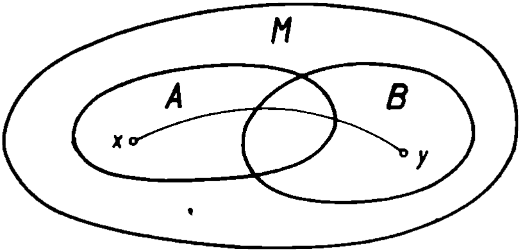
Také každý prvek množiny M může být obrazem některého prvku této množiny v zobrazení f, ale ani tady není řečeno, že množina všech obrazů musí množinu M vyčerpávat; může se stát, že v množině M existují prvky, které nejsou obrazy žádného prvku této množiny. A také není nikde řečeno, že každý prvek množiny 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 nějakých 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 množina 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 $[x, y] \in \in M \times M$, 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 $z = f(x, y) = x - y \in C$. 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 $N_0 \times N_0$, popř. $C \times C$, 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 $[X, Y] \in M \times M$ (tj. ke každé dvojici bodů roviny ϱ) přiřazen právě jeden bod $S \in M$ (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 $(M \times M) \cup M$ používat nějakou značku, např. $\circ$, $\star$ aj., kterou umístíme mezi obě složky dvojice $[x, y] \in M \times M$, 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 $x \circ y \in M$, $y \circ x \in M$, 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 $(x \circ y) \circ z \in M$, $x \circ (y \circ z) \in M$, 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 $(x \circ y) \star z \in M$, $(x \star z) \circ (y \star z) \in M$, 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 ⋆ 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 ○ násobení a za operaci ⋆ 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 $x \in \mathrm{C}$ a pro každé $y \in \mathrm{C}$ obě čísla $x - y, y - x$, ale pokud je $x \neq y$, je také $x - y \neq y - x$.

Příklad 5. Operace ● 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 ● 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:

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

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

(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.