

# Polynomy v moderní algebře

---

## 2. kapitola. Neutrální a inverzní prvek. Grupa

In: Karel Hruša (author): Polynomy v moderní algebře. (Czech).  
Praha: Mladá fronta, 1970. pp. 15–28.

Persistent URL: <http://dml.cz/dmlcz/403713>

### Terms of use:

© Karel Hruša, 1970

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

## 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  $x \in M$  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  $x \in M$ , dosadíme 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  $n' \in M$  má tu vlastnost, že pro každé  $x \in M$  je  $x \circ n' = x$ , pak podle toho, co jsme právě dokázali, je  $n' = m$ . Obdobně z předpokladu existence dalšího prvku  $m' \in M$ , který má tu vlastnost, že pro každé  $x \in M$  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  $x \in M$  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

$$1 \cdot x = x \cdot 1 = x.$$

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  $a \in N_0$  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  $1 \cdot 1 = 1$  (neutrálním prvkem násobení je číslo 1). K žádnému jinému číslu  $a \in N_0$  neexistuje v této množině inverzní prvek násobení  $\bar{a}$ , neboť podmínku  $a \cdot \bar{a} = 1$  lze v této množině splnit jen pro  $a = \bar{a} = 1$ . Naproti tomu v množině  $C$  všech celých čísel existuje ke každému  $a \in C$  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  $a \cdot \bar{a} = 1$  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

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

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

**Příklad 8.** Budiž  $M$  množina všech přemístění roviny  $\rho$ , 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.

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

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

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

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

$$\begin{aligned} \mathfrak{I} * \mathfrak{I} &= \mathfrak{I}, & \mathfrak{R}_1 * \mathfrak{R}_2 &= \mathfrak{R}_2 * \mathfrak{R}_1 = \mathfrak{I}, \\ \mathfrak{E}_1 * \mathfrak{E}_1 &= \mathfrak{I}, & \mathfrak{E}_2 * \mathfrak{E}_2 &= \mathfrak{I}, & \mathfrak{E}_3 * \mathfrak{E}_3 &= \mathfrak{I} \end{aligned}$$

a to znamená, že

$$\bar{\mathfrak{I}} = \mathfrak{I}, \quad \bar{\mathfrak{R}}_1 = \mathfrak{R}_2, \quad \bar{\mathfrak{R}}_2 = \mathfrak{R}_1, \quad \bar{\mathfrak{E}}_1 = \mathfrak{E}_1, \quad \bar{\mathfrak{E}}_2 = \mathfrak{E}_2, \quad \bar{\mathfrak{E}}_3 = \mathfrak{E}_3.$$

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

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

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

$$\begin{aligned} (1 \Delta 1) \Delta 2 &= (2.2) \Delta 2 = 4 \Delta 2 = 6.9 = 54, \\ 1 \Delta (1 \Delta 2) &= 1 \Delta (3.3) = 1 \Delta 9 = 10.10 = 100. \end{aligned}$$

Její neutrálním prvkem je číslo 0, neboť pro každé  $x \in R$  je

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

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

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

Pro každé číslo  $x \in R$ , 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

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

a také

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

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  $\emptyset$  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  $\rho$ , jimiž se reprodukuje rovnostranný trojúhelník  $ABC$  v rovině  $\rho$  (viz příklad 8 na str. 19) je grupa vzhledem k operaci  $*$ ; 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

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


---

**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  $\rho$ , 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

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

dostaneme

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

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

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

$$\mathfrak{X}_1 \star \mathfrak{Z} = \mathfrak{G}_1, \quad \mathfrak{U} \star \mathfrak{X}_1 = \mathfrak{G}_1,$$

vyjde

$$\mathfrak{Z} = \overline{\mathfrak{X}_1} \star \mathfrak{G}_1 = \mathfrak{X}_2 \star \mathfrak{G}_1 = \mathfrak{G}_3,$$

$$\mathfrak{U} = \mathfrak{G}_1 \star \overline{\mathfrak{X}_1} = \mathfrak{G}_1 \star \mathfrak{X}_2 = \mathfrak{G}_2;$$

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  $[x, y] \in M \times M$  existuje prvek  $x \circ y \in M$ .

b) Operace  $\circ$  je asociativní.

c) Ke každému  $a \in M$  a ke každému  $b \in M$  existuje (aspoň jeden) prvek  $x \in M$  a (aspoň jeden) prvek  $y \in M$ , 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 všechny 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  $z \in M$  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  $u \in M, v \in M$ , 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  $x \in M$  je

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

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

c) existují takové prvky  $b \in M$ ,  $c \in M$ , 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  $n' \in M$ , že  $x \circ n' = x$  pro každé  $x \in M$ .

4'. Ke každému  $a \in M$  existuje prvek  $a' \in M$ , 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  $x \in M$  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

$$\begin{aligned} a' \circ a &= a' \circ (a \circ n') = a' \circ [a \circ (a' \circ a'')] = \\ &= a' \circ [(a \circ a') \circ a''] = a' \circ (n' \circ a'') = \\ &= (a' \circ n') \circ a'' = a' \circ a'' = n'. \end{aligned}$$

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  $\rho$  (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:

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

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

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

19. a) Dokažte, že množina  $M$  všech přemístění roviny  $g$ , 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  $e$ , jimiž se reprodukuje čtverec  $ABCD$ .

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