3. Operace

In: Herbert Kästner (author); Peter Göthner (author); Karel Horák (translator): Algebra, každý začátek je lehký. (Czech). Praha: Mladá fronta, 1986. pp. 89–125.

Persistent URL: http://dml.cz/dmlcz/404147

3. OPERACE

$2 \circ 4 = 3$ a $7 \circ 17 = 12$?

3.1 POJEM OPERACE

Operace jako zobrazení — mnoho příkladů, některé už důvěrně známé, ale snad i nějaké méně známé

Tisková chyba? Početní chyba? Jistě uvažujete o správnosti rovností uvedených v nadpise, pokud máte na mysli základní početní operace v číselném oboru. K tomuto problému se ještě vrátíme.

Vedle sčítání, násobení, odčítání a dělení racionálních čísel jsme už poznali i další operace, např. tvoření průniku, sjednocení a rozdílu množin a skládání přiřazení. Na některé známé příklady se podíváme blíže:

Sčítání přirozených čísel	Odčítání zlomků
$(6; 7) \mapsto 13$	$(9; 7) \mapsto 2$
$(0; 8) \mapsto 8$	$(17; 0) \mapsto 17$
$(2; 9) \mapsto 11$	$(0{,}5; 9) \mapsto ?$

Průnik množin	Sjednocení množin
$(\{1; 2\}, \{3\}) \mapsto \emptyset$	$(\{a, b\}, \{c\}) \mapsto \{a, b, c\}$
$(\{7; 8\}, \{8; 9\}) \mapsto \{8\}$	$(\{a\}, \emptyset) \mapsto \{a\}$
$(\{7, 4, 0\}, \emptyset) \mapsto \emptyset$	$(\{a, b\}, \{a, b\}) \mapsto \{a, b\}$

Naše příklady ukazují, že „operační předpis" uspořádané dvojici prvků množiny M jednoznačně přiřazuje opět prvek z M. Operaci tedy můžeme chápat jako speciální zobrazení, přičemž vzory jsou uspořádané dvojice prvků množiny M a obrazy jsou prvky z M. Sčítání celých nezáporných čísel je zobrazení $N_0 \times N_0$ do N_0. Odčítání nezáporných racionálních čísel je zobrazení

z $\mathsf{Q}^+ \times \mathsf{Q}^+$ na Q^+, protože ne každé dvojici nezáporných racionálních čísel je přiřazen nějaký obraz. Průnik a sjednocení jsou zobrazení $\mathscr{P}(M) \times \mathscr{P}(M)$ na $\mathscr{P}(M)$.

Sestrojme ještě následující příklad: každé uspořádané dvojici celých nezáporných čísel (a, b) přiřaďme jako obraz číslo $(a + b)^2$. Také toto zobrazení můžeme chápat jako operaci. Protože ale jako obrazy nedostaneme všechna celá nezáporná čísla, nýbrž jen druhé mocniny, máme před sebou zobrazení $\mathsf{N}_0 \times \mathsf{N}_0$ do N_0.

Příklady nám naznačují, jak by asi měl být pojem operace v množině M definován:

Definice 3.1. Nechť M je neprázdná množina. Každé zobrazení φ z $M \times M$ do M se nazývá *binární operace v množině* M. Přiřazuje-li φ dvojici (a, b) jako obraz prvek c, píšeme místo $\varphi(a, b) = c$ také $a \circ b = c$. Množina M se nazývá *nosič operace*.

Protože operace jsou speciální zobrazení, mohli bychom mluvit o definičním oboru a oboru hodnot operace. Tak je např. definičním oborem dělení v množině R reálných čísel množina $\mathsf{R} \times (\mathsf{R} \setminus \{0\})$. Je-li definiční obor operace φ: $M \times M \to M$ roven $M \times M$, nazýváme φ *neomezeně definovanou operací*; platí-li $\mathscr{D}(\varphi) \subset M \times M$ a $\mathscr{D}(\varphi) \neq M \times M$, nazývá se φ *parciální operace*.

Pojem binární operace v množině M zavedený v D(3.1) se dá zobecnit dvěma směry. Přiřadíme-li prostřednictvím zobrazení φ každé uspořádané n-tici $(a_1, \ldots, a_n)$ prvků a_i množiny M prvek z M, mluvíme o n-ární operaci v množině M. V ještě obecnějším smyslu můžeme mluvit také o n-ární operaci, máme-li zobrazení z $M_1 \times \times M_2 \times \ldots \times M_n$ do M. Např. skalární součin dvou vektorů a „násobení" vektoru reálným číslem jsou takové binární operace, v nichž vystupují navzájem rozdílné množiny.

Také tvoření aritmetického průměru dvou racionálních čísel můžeme chápat jako neomezeně definovanou binární operaci:

$$(a, b) \mapsto c = \frac{a + b}{2}.$$

Tak se také dají vyložit rovnosti uvedené v nadpisu. Interpretujeme-li značku „$\circ$" jako symbol pro tvoření aritmetického průměru racionálních čísel, jsou uvedené rovnosti pravdivé výroky.

Při počítání s přirozenými čísly bychom teď chtěli používat sčítání jen na podmnožině S sudých čísel. Používáme přitom vlastně „novou" operaci „$+$", kterou můžeme chápat jako zobrazení z $S \times S$ do S. Jinak ovšem každý školák ví, že 2 a 4 je 6 bez ohledu na to, zda se na to díváme jako na sčítání celých čísel anebo jako na sčítání sudých čísel. Toto „nové" sčítání nazýváme zúžením sčítání celých čísel na množinu sudých čísel. Obecně se operace $\circ_A$ definovaná v množině A nazývá *zúžení operace* $\circ_B$ *definované v množině* B, právě když $A \subset B$ a pro libovolná $a, b \in A$ platí: $a \circ_A b = a \circ_B b$. Není však řečeno, že operace $\circ_A$, která je zúžením operace $\circ_B$ na množinu $A \subset B$, je v této množině A neomezeně definovaná operace. Zúžíme-li např. sčítání $+$ v N_0 na podmnožinu L lichých čísel, není $+_L$ neomezeně definovaná operace v L, neboť např. $3 \in L$, $5 \in L$, $3 + 5 = 8$, ale $8 \notin L$. Prvek 8 přiřazený dvojici $(3; 5)$ tedy už v množině L neleží. Naproti tomu zúžením operace sčítání v N_0 na množinu S sudých čísel se nedostaneme ven z množiny S, protože součet dvou libovolných sudých čísel je vždy zas sudý. Říkáme také, že S je *uzavřená vzhledem ke sčítání*.

Abychom získali představu o rozmanitosti operací, podívejme se ještě na některé důležité příklady:

Příklady. (1) V odstavci 1.7, příklad (2) jsme zavedli

zbytkové třídy celých čísel modulo m. Budeme je teď označovat $(0)_m$, $(1)_m$, ..., $(m-1)_m$. Protože zbytkové třídy jsou po dvou disjunktní neprázdné množiny, může každý prvek jednoznačně reprezentovat třídu, do které patří. Dohodněme se, že pro označení třídy budeme používat nejmenší nezáporné číslo v ní obsažené.
V množině zbytkových tříd celých čísel modulo 4 zaveďme „sčítání zbytkových tříd" a „násobení zbytkových tříd":

(1) $$(a)_4 + (b)_4 = (a + b)_4;$$
(2) $$(a)_4 . (b)_4 = (ab)_4.$$

Např. je

$$(3)_4 + (2)_4 = (5)_4 = (1)_4; \quad (2)_4 . (3)_4 = (6)_4 = (2)_4.$$

Uvědomte si, že symboly + a . mají různý význam. V rovnostech (1) a (2) bychom jako modul mohli také zvolit místo čtyřky libovolné celé kladné číslo. Definice operací v množině zbytkových tříd modulo m by pak byla dána vztahy (1′) $(a)_m + (b)_m = (a + b)_m$; (2′) $(a)_m . (b)_m = (ab)_m$. Sčítání a násobení zbytkových tříd jsme objasnili prostřednictvím „reprezentantů". Musíme ještě ukázat, že definice (1′) a (2′) mají smysl, a to tak, že dokážeme, že tyto operace „souhlasí" s tvořením zbytkových tříd. Vezměme místo a a b dva jiné reprezentanty $a' \in (a)_m$ a $b' \in (b)_m$, takže musí platit $a' + b' \in (a + b)_m$ a $a' . b' \in (ab)_m$. Dokážeme první z uvedených vztahů:
$a, a' \in (a)_m$ znamená, že $a = a' + rm$, a $b, b' \in (b)_m$ znamená, že $b = b' + sm$. Sečtením obou rovností dostaneme $a + b = a' + b' + (r + s)\, m$, tj. oba součty $a + b$ i $a' + b'$ leží ve stejné zbytkové třídě. Všech 16 možností aditivního (resp. multiplikativního) spojení zbytkových tříd modulo 4 lze zapsat pomocí tabulky (tabulky operace):

+	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(0)_4$	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(1)_4$	$(1)_4$	$(2)_4$	$(3)_4$	$(0)_4$
$(2)_4$	$(2)_4$	$(3)_4$	$(0)_4$	$(1)_4$
$(3)_4$	$(3)_4$	$(0)_4$	$(1)_4$	$(2)_4$

·	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(0)_4$	$(0)_4$	$(0)_4$	$(0)_4$	$(0)_4$
$(1)_4$	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(2)_4$	$(0)_4$	$(2)_4$	$(0)_4$	$(2)_4$
$(3)_4$	$(0)_4$	$(3)_4$	$(2)_4$	$(1)_4$

Přitom v levém krajním sloupci tabulky stojí levý sčítanec (resp. levý činitel) a v horním řádku pravý sčítanec (resp. pravý činitel).

(2) Ve skladovací hale opravárenského podniku používají k záznamu stavu různých náhradních dílů k určitému datu t_0 „číselný obdélník". Skládá se z n řádků a m sloupců, obsahuje tedy nm čísel. Každé z nich poskytuje informaci o tom, kolik náhradních dílů daného druhu je ve skladu k dispozici. Takový číselný obdélník se nazývá $n \times m$ *matice*; nm čísel a_{ik} nazýváme *prvky matice*. Znázorňujeme-li je pomocí proměnné, je použití dvojitého indexu účelné.

$$\begin{array}{l} \qquad\qquad\qquad\qquad \downarrow k\text{-tý sloupec} \\ i\text{-tý řádek} \rightarrow \begin{pmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1m} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \dots & a_{ik} & \dots & a_{im} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nm} \end{pmatrix} n \times m \text{ matice} \end{array}$$

První index i prvku a_{ik} matice A nazýváme *řádkovým indexem*. Udává, ve kterém řádku prvek stojí. Druhý index k, *sloupcový index*, vyjařuje, že a_{ik} patří do k-tého sloupce. Tak např. prvek a_{35} (čti: a-tři-pět) stojí v 3. řádku a 5. sloupci matice. Dvojice (n, m) přirozených čísel popisuje typ matice. Tak matice typu (4; 7) má právě 4 řádky a 7 sloupců. Matice budeme označovat velkými písmeny $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, ... Dvě matice $\mathbf{A} = (a_{ik})$ a $\mathbf{B} = (b_{ik})$ stejného typu (n, m) se rovnají, právě když se rovnají po

složkách, tj. právě když platí: $a_{ik} = b_{ik}$ pro $i \in \{1, 2, \ldots, n\}$ a $k \in \{1, 2, \ldots, m\}$. Takto definovaná rovnost matic je relace ekvivalence. Přírůstek a úbytek náhradních dílů, ke kterému dojde v určitém časovém období, může být právě popsán $n \times m$ maticí. Kladná čísla charakterizují přírůstek, záporná čísla úbytek a číslo nula značí, že nedošlo k žádným změnám. „Nový" stav v čase t_1 dostaneme zřejmě tak, že pro každý náhradní díl k původnímu počtu přičteme to číslo, které udává přírůstek, resp. úbytek tohoto dílu. To neznamená nic jiného, než že obě matice musíme sečíst následujícím způsobem:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} & \ldots & b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n1} & b_{n2} & \ldots & b_{nm} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \ldots & a_{1m} + b_{1m} \\ a_{21} + b_{21} & a_{22} + b_{22} & \ldots & a_{2m} + b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \ldots & a_{nm} + b_{nm} \end{pmatrix}, \qquad (3)$$

resp. ve zkrácené formě $(a_{ik}) + (b_{ik}) = (a_{ik} + b_{ik})$.
Zřejmě je součet dvou $n \times m$ matic, jejichž prvky jsou celá čísla, zase $n \times m$ matice celých čísel. Musíme si uvědomit, že (3) definuje součet matic jen pro matice stejného typu. Tak např. je

$$\begin{pmatrix} 2 & 1 & 7 \\ 5 & 3 & 0 \end{pmatrix} + \begin{pmatrix} 9 & -1 & 8 \\ -4 & 0 & 11 \end{pmatrix} = \begin{pmatrix} 11 & 0 & 15 \\ 1 & 3 & 11 \end{pmatrix}.$$

Naproti tomu matice

$$\begin{pmatrix} 2 & 1 \\ 3 & 0 \\ 4 & 7 \end{pmatrix} \text{ a } \begin{pmatrix} 2 & 1 & 9 & -3 \\ 5 & 1 & 8 & -4 \end{pmatrix}$$

se podle (3) sečíst nedají.

Problematika stavu zásob zprvu vyžadovala uvažovat jako prvky matice celá čísla. Upustíme-li od této věcné souvislosti, pak můžeme jako prvky matice připustit i racionální nebo reálná čísla. Matice, jejichž prvky jsou reálná čísla a mají tvar $1 \times m$, resp. $n \times 1$, nazýváme *řádkovým*, resp. *sloupcovým vektorem*. (3) tak kromě jiného definuje i součet takovýchto vektorů.

Nyní jsme blízko otázce, zda lze matice také „násobit". Otázku musíme nejdříve upřesnit: Můžeme definovat — vedle sčítání matic — maticovou operaci tak, aby byla účelná, tj. aby jednak mělo smysl použít ji při řešení problémů, jednak aby se „snášela" s už uvedeným sčítáním matic? Vyjděme opět z konkrétní problémové situace: V podniku se vyrábějí tři meziprodukty M_1, M_2 a M_3; pro každý z nich je potřeba určité množství surovin S_1 a S_2. Matice A poskytuje přehled o jejich spotřebě. Matice **B** charakterizuje, v jakém rozsahu se oba meziprodukty podílejí na výrobě obou konečných produktů K_1 a K_2.

$$\begin{array}{c} \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} M_1 & M_2 & M_3 \end{array} \\ \begin{pmatrix} 12 & 4 & 3 \\ 2 & 8 & 7 \end{pmatrix} \end{array} = \mathbf{A}, \qquad \begin{array}{c} \\ M_1 \\ M_2 \\ M_3 \end{array} \begin{array}{c} \begin{array}{cc} K_1 & K_2 \end{array} \\ \begin{pmatrix} 1 & 5 \\ 4 & 2 \\ 7 & 11 \end{pmatrix} \end{array} = \mathbf{B}.$$

Chceme-li nyní vědět, kolik jednotek suroviny S_1 je potřeba k výrobě konečného produktu K_1, pak zřejmě musíme sečíst součiny 12.1, 4.4 a 3.7. Odpovídajícím způsobem můžeme pro každý z obou konečných produktů určit spotřebu surovin vzhledem ke každé z nich zvlášť a výsledky zapsat do 2×2 matice. Data určená maticemi **A** a **B** k tomu plně dostačují. Záleží tedy jen na tom, abychom vhodně popsali operaci mezi maticemi **A** a **B**. Podle našeho příkladu dostáváme:

$$\begin{pmatrix} 12 & 4 & 3 \\ 2 & 8 & 7 \end{pmatrix} \cdot \begin{pmatrix} 1 & 5 \\ 4 & 2 \\ 7 & 11 \end{pmatrix} =$$

$$= \begin{pmatrix} 12.1 + 4.4 + 3.7 & 12.5 + 4.2 + 3.11 \\ 2.1 + 8.4 + 7.7 & 2.5 + 8.2 + 7.11 \end{pmatrix} =$$

$$= \begin{pmatrix} 49 & 101 \\ 83 & 103 \end{pmatrix} = \mathbf{C}\,.$$

Ze součinové matice **C** můžeme vyčíst spotřebu surovin. Uveďme si ještě jednou, že každý prvek **C** je součtem součinů některých prvků **A** a **B**. Abychom dostali prvek c_{ij} v i-tém řádku a j-tém sloupci matice **C**, musíme i-tý řádek **A** „vynásobit" j-tým sloupcem **B** (v tomto pořadí). Jak se tvoří každý z těchto součinů „řádek krát sloupec", si dobře zapamatujete z následujícího schématu:

$$(a_{i1}\ a_{i2} \ldots a_{im}) \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{mj} \end{pmatrix} = \left(\ldots \sum_{k=1}^{m} a_{ik} b_{kj} \ldots \right) = \begin{pmatrix} \vdots \\ \ldots\ c_{ij}\ \ldots \\ \vdots \end{pmatrix}$$

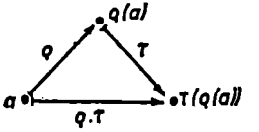
Tyto definice násobení matic můžeme zapsat také stručněji:

$$(a_{ik}) \cdot (b_{kj}) = \left(\sum_{k=1}^{m} a_{ik} b_{kj} \right) = (c_{ij}). \qquad (4)$$

Chceme-li $n \times m$ matici **A** násobit $r \times s$ maticí **B** podle (4), musí mít první činitel **A** právě tolik sloupců, kolik má druhý činitel **B** řádků, tj. musí být $m = r$. Matice **A**, **B** s touto vlastností nazveme *sdružené* (v tomto pořadí).

Vyjdeme-li opět z toho, že prvky matic jsou reálná čísla, je násobení ve (4) zavedeno pomocí sčítání a násobení reálných čísel. Ke vztahům mezi sčítáním a násobením matic dojdeme v odstavci 3.2.

(3) V odstavci 1.6 bylo objasněno skládání přiřazení. Je-li M libovolná neprázdná množina a T množina všech prostých zobrazení M na sebe, pak je skládáním prvků z T, tzv. transformací množiny M, dána neomezeně definovaná binární operace v T: Výsledkem složení dvou prvků ϱ a τ z T je takové zobrazení, které dostaneme, jestliže na každý prvek $a \in M$ provedeme nejprve ϱ a pak na obraz $\varrho(a)$ zobrazení τ.



Objasníme tento obecný postup na příkladech: Nechť M je konečná množina $\{1, 2, 3\}$. Pak se T skládá ze šesti zobrazení $\pi_1 = \begin{pmatrix}123\\123\end{pmatrix}$, $\pi_2 = \begin{pmatrix}123\\132\end{pmatrix}$, $\pi_3 = \begin{pmatrix}123\\213\end{pmatrix}$, $\pi_4 = \begin{pmatrix}123\\231\end{pmatrix}$, $\pi_5 = \begin{pmatrix}123\\312\end{pmatrix}$ a $\pi_6 = \begin{pmatrix}123\\312\end{pmatrix}$. Tato čísla v závorkách nejsou matice, jak jsme s nimi pracovali v příkladu 2, ale znázorňují tabulky hodnot. Složíme-li např. π_3 s π_5, dostaneme $\begin{pmatrix}123\\213\end{pmatrix} \cdot \begin{pmatrix}123\\312\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix} = \pi_2$. Jako cvičení složte další zobrazení, např. π_2 a π_4, případně π_4 a π_2!

Obsahuje-li M právě n prvků $1, 2, \ldots, n$, skládá se T z $1.2 \ldots n = n!$ zobrazení množiny M na sebe. Každé možné pořadí $(i_1, \ldots, i_n)$ n různých prvků z M ve schématu $\begin{pmatrix}1 & 2 & \ldots & n\\ i_1 & i_2 & \ldots & i_n\end{pmatrix}$ popisuje totiž právě jeden prvek T. Každé prosté zobrazení konečné množiny M na sebe se nazývá *permutace.*

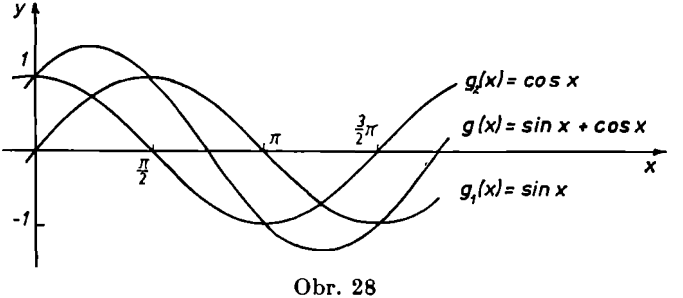
Nechť E je množina všech bodů roviny. Z množiny

všech prostých zobrazení E na sebe vyberme množinu všech shodností S. To jsou posunutí, otočení, osové souměrnosti nebo taková zobrazení, která dostaneme složením uvedených speciálních zobrazení. Zřejmě složením shodných zobrazení vznikne opět shodnost, to jste používali už ve škole. Skládáním shodností je na E dána neomezeně definovaná operace. Převádí-li shodnost ϱ obrazec Φ, tedy neprázdnou podmnožinu množiny E, na obrazec Φ', nazývají se Φ a Φ' *kongruentní (shodné)*.

(4) Budeme se zabývat množinou F všech funkcí reálné proměnné definovaných na intervalu $\langle a, b\rangle$ reálných čísel. V F zavedeme jako sčítání funkcí následující operaci označovanou $\oplus$:

$(f \oplus g)(x) = f(x) + g(x)$ pro libovolné $f, g \in F$ a pro všechna $x \in \langle a, b\rangle$. (5)

Sčítání funkcí je tedy zavedeno prostřednictvím sčítání funkčních hodnot — to jsou reálná čísla. Tato operace se užívá vždy, kdykoli jsou funkce aditivně spojeny. Tak můžeme např. $f(x) = mx + n$ chápat jako součet funkcí $f_1(x) = mx$ a $f_2(x) = n$, funkci $g(x) = \sin x + \cos x$ jako součet funkcí $g_1(x) = \sin x$ a $g_2(x) = \cos x$ (srov. obr. 28).



Obr. 28

Omezíme-li se na funkce, jejichž definiční obor je množina všech celých kladných čísel, tedy na posloupnosti reálných čísel, definuje (5) zároveň i sčítání číselných posloupností a často pak píšeme:

$$(a_n) \oplus (b_n) = (a_n + b_n) \text{ pro libovolné posloupnosti } (a_n), (b_n). \tag{5'}$$

Součet dvou posloupností (a_n) a (b_n) se tedy skládá z členů $a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, \ldots$ Zajímavé je, že součet dvou konvergentních posloupností je vždy zas konvergentní posloupnost.

(5) Nakonec ještě spojíme dohromady několik dvojic operací. Už v odstavci 1.4 byly nápadné analogie mezi vlastnostmi operací $\bigcap$ a $\bigcup$. Ukazuje se, že shody takového druhu se mohou vyskytnout i u jiných dvojic.

Nechť $T = \{1, 2, 3, 4, 6, 12\}$ je množina všech celých kladných čísel, jež jsou děliteli čísla 12. Utvoření největšího společného dělitele (resp. nejmenšího společného násobku) dvou libovolných prvků z T dává vždy jednoznačně určený prvek z T, tj. v T jsou neomezeně definovány obě operace $a \wedge b = D(a, b)$ a $a \vee b = n(a, b)$. Už z porovnání tabulek obou operací lze učinit zajímavá odhalení.

V R byly tvořením maxima, resp. minima dvou reálných čísel zavedeny dvě operace $(a, b) \mapsto \max(a, b)$ a $(a, b) \mapsto \min(a, b)$. Každé uspořádané dvojici $(a, b) \in \mathsf{R} \times \mathsf{R}$ je operací „max", resp. „min" jako výsledek přiřazeno to z čísel a nebo b, které není menší, resp. není větší než to druhé. Jak jsme viděli, není snadné pro každou „novou" operaci nalézt nový spojovací znak. Často jsme sahali pro známé symboly (např. „.."), i když se nejednalo o operaci v číselném oboru. Tak budeme postupovat i napříště a nové spojovací znaky budeme používat jen tam, kde by mohlo dojít k záměně.

JE 17,2 % Z 93,6 ROVNO 93,6 % Z 17,2?

3.2 VLASTNOSTI OPERACÍ

Čtenář se seznámí s vlastnostmi operací; zjistí, za jakých podmínek je operace komutativní, asociativní, popřípadě invertibilní

Uvidíme, že otázku položenou v nadpisu je snadné zodpovědět. Počítáme-li totiž a procent z b, přičemž a a b jsou libovolné zlomky, pak je uspořádané dvojici (a, b) jednoznačně přiřazeno zlomek $\frac{ab}{100}$. Budeme počítání procent chápat jako operaci neomezeně definovanou na $\mathbb{Q}^*$, budeme pro ni užívat znaku % a psát $a \,\%\, b = \frac{ab}{100}$. Shora položenou otázku můžeme nyní převést na otázku obecnější, zda pro libovolné $a, b \in \mathbb{Q}^*$ platí $a \,\%\, b = b \,\%\, a$. Je-li výsledek nezávislý na pořadí „operandů", nazývá se operace komutativní.

Definice 3.2. Neomezeně definovaná operace $\circ$ na množině M se nazývá *komutativní*, právě když pro všechna $a, b \in M$ platí $a \circ b = b \circ a$.

Víme, že sčítání celých čísel a násobení zlomků patří mezi komutativní operace. Díky poslední skutečnosti se dá ukázat, že operace % je na $\mathbb{Q}^*$ komutativní: platí $a \,\%\, b = \frac{ab}{100} = \frac{ba}{100} = b \,\%\, a$ pro všechna $a, b \in \mathbb{Q}^*$. Tím je také zodpovězena otázka z nadpisu: Platí-li totiž $a \,\%\, b = b \,\%\, a$ pro všechny zlomky a a b, platí také $17{,}2 \,\%\, 93{,}6 = 93{,}6 \,\%\, 17{,}2$. Naproti tomu z rovnosti $2^4 = 4^2$ neplyne, že umocňování přirozených čísel

je komutativní operace; je přece možné hned uvést protipříklady.

Vyjmenujme teď několik dalších příkladů komutativních operací: Sčítání a násobení zbytkových tříd (srov. příklad 1 v odstavci 3.1) jsou operace s touto vlastností. Pro libovolné zbytkové třídy $(a)_m$, $(b)_m$ totiž platí:

$$(a)_m + (b)_m = (a + b)_m = (b + a)_m = (b)_m + (a)_m$$

a

$$(a)_m \cdot (b)_m = (ab)_m = (ba)_m = (b)_m \cdot (a)_m .$$

Protože sčítání a násobení zbytkových tříd bylo definováno pomocí sčítání a násobení celých čísel, je pochopitelné, že podáváme důkaz vlastností těchto operací se zbytkovými třídami odkazem na odpovídající vlastnosti operací na **Z**. Objasněme tento princip ještě na dalších příkladech:

Sčítání reálných funkcí definovaných na intervalu I je komutativní operace. Byla definována pomocí sčítání reálných čísel; platí proto $f \oplus g = g \oplus f$ pro libovolné funkce f a g z F díky rovnosti $(f \oplus g)(x) = f(x) + g(x) = g(x) + f(x) = (g \oplus f)(x)$ pro všechna $x \in I$. Snadno se můžeme přesvědčit, že komutativní je i sčítání posloupností reálných čísel (opět chápané jako speciální funkce s definičním oborem $\mathbf{N}_0$).

Podobně je komutativní sčítání matic stejného typu, zavedené v příkladu 2 odstavce 3.1, neboť platí:

$$(a_{ik}) + (b_{ik}) = (a_{ik} + b_{ik}) = (b_{ik} + a_{ik}) = \\ = (b_{ik}) + (a_{ik}) .$$

Násobení sdružených matic bylo sice definováno pomocí sčítání i násobení reálných čísel — obě operace jsou komutativní; domněnka, že na základě toho je také násobení matic komutativní, se však ukazuje jako nesprávná. Je-li třeba matice **A** typu (2; 3) a matice **B** typu

(3; 4), součin **AB** sice existuje, ovšem matice **B** a **A** se v tomto pořadí násobit nedají, poněvadž nejsou sdružené. I když se omezíme na čtvercové matice typu (n, n), je možno uvést protipříklady jako

$$\begin{pmatrix} 2 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix},$$

ale

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -2 & 0 \end{pmatrix}.$$

Skládání transformací v množině M (srov. příklad 2 v odstavci 3.1) je obecně nekomutativní operace, jak ukazuje už složení dvou následujících permutací:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Můžeme ale dokázat komutativitu skládání pro speciální množiny transformací, např. pro množinu všech posunutí v rovině, nebo i pro množinu všech otočení kolem pevného bodu roviny.

Nakonec si ještě uvědomme, že všechny operace uvedené v příkladu 5 odstavce 3.1 jsou komutativní, neboť jistě platí $a \wedge b = b \wedge a$ pro všechna celá kladná čísla a, b a $\max(x, y) = \max(y, x)$ pro všechna reálná čísla x, y.

Že jsou obě operace $\cap$ a $\cup$ komutativní, bylo předvedeno už v odstavci 1.4. Máme-li zjistit průnik tří množin A, B a C, můžeme utvořit nejprve $A \cap B$ a pak průnik této množiny s množinou C. Ale můžeme také počítat průnik A s předem zjištěným průnikem $B \cap C$. Bylo by jistě zlé, kdyby oba postupy vedly k různým výsledkům. Tvrzení $(A \cap B) \cap C = A \cap (B \cap C)$ z věty V(1.2) nás však uklidňuje.

Je-li nějaká operace „nezávislá na uzávorkování jednotlivých prvků", jako např. i sjednocení množin nebo součet a násobení reálných čísel, nazývá se *asociativní*.

Definice 3.3. Operace $\circ$ v množině M se nazývá *asociativní*, právě když pro všechna $a, b, c \in M$ platí

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

Zatímco u asociativní operace můžeme jednotlivé operandy libovolně spojovat a provádět na nich postupně danou operaci, u neasociativních operací musíme vždy dbát úmluvy, že pokud nejsou použity závorky, postupujeme při provádění operace jako při psaní zleva doprava. To znamená, že $9 - 5 - 3$ je totéž jako $(9 - 5) - 3$, což musíme odlišovat od $9 - (5 - 3)$.

Důkaz, že sčítání a násobení zbytkových tříd je asociativní, je poměrně jednoduchý. Také sčítání funkcí zavedené v příkladu 4 odstavce 3.1 má tuto vlastnost, neboť platí:

$$\begin{aligned}((f \oplus g) \oplus h)(x) &= (f \oplus g)(x) + h(x) = \\ &= (f(x) + g(x)) + h(x) = \\ &= f(x) + (g(x) + h(x)) = \\ &= f(x) + (g \oplus h)(x) = (f \oplus (g \oplus h))(x)\end{aligned}$$

pro libovolné funkce f, g a h a pro všechna $x \in I$.

Skládání permutací, otáčení nebo souměrností je asociativní, neboť dokonce skládání libovolných přiřazení má tuto vlastnost (srov. odstavec 1.6).

Prozkoumejme ještě některé operace uvedené v příkladu 5 odstavce 3.1. Asociativita $\cap$ a $\cup$ byla už ukázána v odstavci 1.4. Platí ale také

(1) $\max(a, \max(b, c)) = \max(\max(a, b), c)$ a
(2) $\min(a, \min(b, c)) = \min(\min(a, b), c)$.

V (1), resp. (2) je totiž v každém z obou výrazů určeno

to z čísel a, b, c, které není menší (resp. není větší) než každé z obou zbylých čísel.

Při důkazu asociativity „nejmenšího společného dělitele" je potřeba jednoznačně vyjádřit každé přirozené číslo jako součin mocnin prvočísel. Přirozené číslo n přitom píšeme jako součin mocnin všech prvočísel, přičemž je exponent roven nule, právě když příslušné prvočíslo není dělitelem čísla n. Kupříkladu je

$$14 = 2^1.3^0.5^0.7^1.11^0 \ldots,$$
$$20 = 2^2.3^0.5^1.7^0.11^0 \ldots,$$

přičemž ... naznačuje, že všechna další prvočísla vystupují v rozkladu s exponentem nula. Vystupuje-li v rozkladu na prvočinitele čísla a (resp. b) prvočíslo p s exponentem α_p (resp. β_p), obsahuje, jak známo, nejmenší společný dělitel $D(a, b)$ toto prvočíslo s exponentem $\min(\alpha_p, \beta_p)$. Platí tedy pro $a = \prod_{i \in N_0} p_i^{\alpha_i}$, $b = \prod_{i \in N_0} p_i^{\beta_i}$ a $c = \prod_{i \in N_0} p_i^{\gamma_i}$ také $D(D(a, b), c) = \prod_{i \in N_0} p_i^{\min(\min(\alpha_i, \beta_i), \gamma_i)} =$

$$= \prod_{i \in N_0} p_i^{\min(\alpha_i, \min(\beta_i, \gamma_i))} = D(a, D(b, c)),$$

přičemž jsme využili prve dokázanou asociativitu operace tvoření minima. Analogicky ukážeme, že také operace nejmenší společný násobek je asociativní, přičemž se využije (1).

Sčítání a násobení reálných čísel je jak komutativní, tak i asociativní; odčítání a dělení nemají žádnou z těchto vlastností. Přesto je domněnka, že komutativita a asociativita jsou navzájem související vlastnosti operace, nesprávná. Existují komutativní operace, jež nejsou asociativní, např. tvoření aritmetického průměru dvou reálných čísel, a asociativní operace, jež nejsou komutativní, např. skládání permutací.

Nepostačitelnost číselného oboru při počítání bývá často podnětem k jeho rozšíření. Zjistíme, že jisté rovnice v daném oboru nemají řešení. Tak např. v N_0 nejsou řešitelné ani všechny rovnice tvaru $a + x = b$, ani všechny rovnice tvaru $ay = b$ pro daná $a, b \in \mathsf{N}_0$. Říkáme tomu, že sčítání a násobení není v N_0 *invertibilní*, tj. dva sčítanci (činitelé) sice určují jednoznačně svůj součet (součin), obráceně se ale vždy nedá ze součtu a jednoho sčítance (součinu a jednoho činitele) určit druhý sčítanec (činitel).

Definice 3.4. Neomezeně definovaná operace $\circ$ na množině M se nazývá *invertibilní*, právě když pro libovolná a, $b \in M$ existují x a y z M taková, že platí $a \circ x = b$ a $y \circ a = b$.

Násobení v množině racionálních čísel různých od nuly je invertibilní operace. Naproti tomu násobení libovolných reálných čísel tuto vlastnost nemá, protože např. rovnice $0.x = 17$ nemá v R řešení. Vlastnost invertibility operace $\circ$ je totožná s požadavkem existence řešení rovnic uvedených v D(3.4), tj. operace $\circ$ je v M invertibilní, právě když každá rovnice $a \circ x = b$ a $y \circ a = b$ má v M alespoň jedno řešení.

Skládání transformací množiny M je invertibilní operace. Na důkaz ukažme pro dané transformace ϱ a τ řešení rovnice $\varrho.x = \tau$. Protože $\varrho(\varrho^{-1}.\tau) = (\varrho.\varrho^{-1}).\tau = \tau$, splňuje tuto podmínku $x = \varrho^{-1}.\tau$. Přitom je ϱ^{-1} inverzní zobrazení k ϱ a spolu s ϱ a τ jsou také ϱ^{-1} a $\varrho^{-1}.\tau$ prvky množiny T všech transformací M. Odpovídajícím způsobem se ukáže, že i každá rovnice $y.\varrho = \tau$ pro $\varrho, \tau \in T$ má v T řešení.

Proto je i skládání všech permutací konečné množiny M invertibilní.

Sčítání matic a sčítání funkcí jsou invertibilní operace.

Není obtížné tato tvrzení dokázat. Použije se pouze toho, že sčítání reálných čísel má tuto vlastnost.

Také sčítání zbytkových tříd je invertibilní operace, neboť každá rovnice $(a)_m + (x)_m = (b)_m$ má řešení $(x)_m = (b - a)_m$, protože pro daná celá čísla a a b má rovnice $a + x = b$ v $\mathbf{Z}$ vždy řešení, totiž $x = b - a$. Že násobení zbytkových tříd vzhledem k libovolnému modulu m invertibilní být nemusí, ukazuje následující protipříklad: Rovnice $(2)_4 . (x)_4 = (3)_4$ nemá v množině všech zbytkových tříd modulo 4 řešení, neboť jinak by muselo existovat celé číslo x takové, že $2x - 3 = 4c$ pro $c \in \mathbf{Z}$. Na levé straně této rovnice stojí ale liché číslo, zatímco na pravé straně vždy sudé číslo.

Také následující operace nejsou invertibilní. Důkaz dostaneme v každém jednotlivém případě nalezením rovnice, která v oboru příslušné operace nemá řešení. Překontrolujte to!

— Násobení čtvercových matic

$$\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & u \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}.$$

— Tvoření průniku množin $\{a, b, c\} \cap X = \{a, d\}$.

— Tvoření sjednocení množin $\{a, b\} \cup X = \{a\}$.

— Největší společný dělitel dvou čísel v množině všech dělitelů čísla 12 $D(4, x) = 6$.

— Nejmenší společný násobek dvou čísel v množině všech dělitelů čísla 12 $n(4, x) = 2$.

— Tvoření maxima, resp. minima dvou reálných čísel $\max(4, x) = 1$, $\min(x, 3) = 100$.

Existují invertibilní operace, jež nejsou komutativní, např. skládání transformací, a také invertibilní operace, jež nejsou asociativní, např. tvoření aritmetického

průměru dvou racionálních čísel. Vlastnost invertibility není tedy svázána ani s komutativitou, ani s asociativitou.

Z rovnosti $a + c = b + c$ můžeme usuzovat na $a = b$, tj. sčítanec c na obou stranách rovnosti smíme vyškrtnout. Také rovnost $ac = bc$, kde a, b, c jsou celá čísla, se dá zkrátit na $a = b$, pokud c je číslo různé od nuly.

Definice 3.5. Říkáme, že neomezeně definovaná operace $\circ$ na množině M má vlastnost *krácení*, právě když pro libovolná $a, b, c \in M$ současně platí (1) a (2):

(1) Z $a \circ c = b \circ c$ plyne $a = b$.
(2) Z $c \circ a = c \circ b$ plyne $a = b$.

Stejně jako komutativita a asociativita, je i možnost krácení vlastnost dané operace; proto nemůžeme přechod od $a \circ c = b \circ c$ k $a = b$ motivovat „dělením" obou stran rovnosti číslem c, tj. užitím další operace.

Pravidla vyjádřená v (1) a (2) definice D(3.5) se nazývají — ne příliš účelně — pravidla krácení, i když zřejmě s krácením zlomků nijak nesouvisejí.

Je jasné, že pro komutativní operace z podmínky (1) plyne podmínka (2), a obráceně, také podmínka (2) dává podmínku (1). Jak už zdůraznil předchozí příklad, z $a.0 = b.0$ neplyne $a = b$. Může tedy nastat případ, že operace nemá vlastnost krácení, přesto však jisté prvky jejího nosiče můžeme vždy „zkrátit". Říkáme pak, že takový prvek je *regulární*. Číslo nula je sice vůči sčítání racionálních čísel regulární, ne však vzhledem k násobení.

Zatímco invertibilita operace $\circ$ v množině M je totožná s podmínkou existence řešení lineárních rovnic, vlastnost krácení zaručuje jednoznačnost jejich řešení. Můžeme tedy vyslovit následující větu:

Věta 3.1. *Je-li operace* $\circ$ *definovaná v množině* M *invertibilní a má-li přitom vlastnost krácení, pak pro libovolná* $a, b \in M$ *má každá z rovnic* $a \circ x = b$ *a* $y \circ a = b$ *právě jedno řešení.*

Důkaz. Existence řešení je zaručena vlastností invertibility operace $\circ$; zbývá ukázat jednoznačnost. Předpokládejme, že $a \circ x = b$ má dvě různá řešení x_1 a x_2, takže z $a \circ x_1 = b$ a $a \circ x_2 = b$ díky rovnosti pravých stran plyne i rovnost levých stran: $a \circ x_1 = a \circ x_2$, a na základě vlastnosti krácení je $x_1 = x_2$ ve sporu s předpokladem. Analogicky se dokáže, že také každá rovnice $y \circ a = b$ má právě jedno řešení.

Skládání transformací množiny M, ale i sčítání zbytkových tříd, sčítání matic a funkcí jsou operace s vlastností krácení. Abychom to dokázali pro poslední tři jmenované operace, musíme využít skutečnosti, že sčítání celých čísel (resp. reálných čísel) má vlastnost krácení. Ukážeme to na příkladu sčítání funkcí definovaných na intervalu I: Podle předpokladu platí $f \oplus g = h \oplus g$, tedy pro všechna $x \in I$ $(f \oplus g)(x) = (h \oplus g)(x)$. Odtud plyne $f(x) + g(x) = h(x) + g(x)$, což je rovnost reálných čísel, tudíž $f(x) = h(x)$ pro všechna $x \in I$, tedy $f = h$.

Naproti tomu následující operace nemají vlastnost krácení, což dokážeme udáním protipříkladu:

— Násobení čtvercových matic:

$$\text{Je} \quad \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix},$$

$$\text{avšak} \quad \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix}.$$

— Tvoření průniku množin:

Je $\{a, c\} \cap \{a, b\} = \{a, d\} \cap \{a, b\}$,

avšak $\{a, c\} \neq \{a, d\}$.

— Násobení zbytkových tříd:

Je $(0)_4 . (2)_4 = (0)_4 . (3)_4$,

avšak $(2)_4 \neq (3)_4$.

— Nejmenší společný násobek v množině všech dělitelů čísla 12:

Je $n(3; 4) = n(6; 4)$,

avšak $3 \neq 6$.

— Tvoření maxima reálných čísel:

Je $\max(2; 17) = \max(1; 17)$,

avšak $2 \neq 1$.

Nyní už také jistě nebude obtížné najít příklady, jež ukazují. že největší společný dělitel dvou přirozených čísel, sjednocení množin stejně jako tvoření minima dvou reálných čísel nejsou operace s vlastností krácení.

Jestliže jsme až dosud uvažovali vlastnosti, jež se týkaly jen jedné operace, budou nás teď zajímat pravidla, kterým podléhá „souhra" dvou operací v množině M.

Definice 3.6. Na množině M nechť jsou neomezeně definovány dvě operace označené jako „násobení" $\circ$ a jako „sčítání" $\#$. Násobení se nazývá *distributivní vzhle-*

dem ke sčítání, právě když pro všechna $a, b, c \in M$ platí

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

a

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

Násobení v R je distributivní vzhledem ke sčítání, neboť platí $a(b + c) = ab + ac$ a $(b + c)\, a = ba + ca$, tj. smíme „odstranit závorky" a čísla „roznásobit". Naproti tomu sčítání není distributivní vzhledem k násobení. Formulace v D(3.6) také ukazuje, že vztah „je distributivní k" není symetrický.

V obou rovnostech v definici D(3.6) jsou na pravé straně užity závorky; to znamená, že nejdříve počítáme „součiny" a pak „součet součinů". To, že je při počítání s čísly můžeme vypustit, spočívá v úmluvě, že „násobení má přednost před sčítáním". Budeme tuto úmluvu přenášet i na jiné operace, pokud nebude hrozit nedorozumění.

Násobení zbytkových tříd se chová distributivně ke sčítání. Pro libovolné zbytkové třídy $(a)_m$, $(b)_m$, $(c)_m$ platí

$$(a)_m \cdot ((b)_m + (c)_m) = (a)_m \cdot (b + c)_m = (a(b + c))_m =$$
$$= (ab + ac)_m = (ab)_m + (ac)_m =$$
$$= (a)_m \cdot (b)_m + (a)_m \cdot (c)_m.$$

Rozmyslete si, které vlastnosti sčítání a násobení celých čísel se využily při tomto malém důkazu!

V příkladu 2 odstavce 3.1 bylo zavedeno sčítání a násobení matic na základě dvou různých problémů z oblasti ekonomie, k jejichž formulaci se obě operace hodily. Překvapuje proto, že obě tyto operace definované zdánlivě nezávisle jsou spolu svázány vlastností distributivnosti. Objasněme tuto skutečnost nejprve na speciálních příkladech 2×2 matic!

Pro libovolné matice **A**, **B** a **C** takové, že **B** a **C** jsou stejného typu a **A** a **B** jsou sdružené, platí

$$(a_{ik}).((b_{kj}) + (c_{kj})) = (a_{ik})\,(b_{kj} + c_{kj}) =$$
$$= (\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj})) = (\sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj}) =$$
$$= (\sum_{k=1}^{n} a_{ik}b_{kj}) + (\sum_{k=1}^{n} a_{ik}c_{kj}) = (a_{ik}).(b_{kj}) + (a_{ik}).(c_{kj}).$$

Tím je dokázán jeden z obou požadavků D(3.6). Že násobení a sčítání splňuje i druhou rovnost, je možno ukázat analogicky.

Ve větě V(1.2) odstavce 1.4 bylo zdůrazněno, že operace $\cap$ a $\cup$ jsou dokonce navzájem distributivní. Je zajímavé, že takováto symetrie vzhledem k vlastnosti distributivnosti je i u obou dalších dvojic operací zavedených v příkladu 5 odstavce 3.1. Platí jak

$$D(a, n(b, c)) = n(D(a, b), D(a, c)),$$

tak i

$$n(a, D(b, c)) = D(n(a, b), n(a, c)),$$

$$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c)),$$
$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c)).$$

Důkazy přenecháváme čtenáři.

TĚŽKÁ ÚLOHA „MUŽE V ČERNÉM"

3.3 PRVKY SE SPECIÁLNÍMI VLASTNOSTMI
O neutrálních, pohlcujících a navzájem inverzních prvcích

Nemá vůbec lehkou úlohu, „muž v černém", jak se také často při kopané říká rozhodčímu — „neutrálu". Zatímco každý hráč může nasadit všechny své schopno-

sti a volní vlastnosti, aby svému mužstvu co nejvíce dopomohl k vítězství, musí se rozhodčí chovat neutrálně. Každé své rozhodnutí činí sám na základě pravidel, jeho možné sympatie či antipatie k jednomu mužstvu nesmějí ovlivnit vývoj utkání.

Sčítáme-li celá čísla, hraje roli „neutrála" nula. Pro libovolné celé číslo c platí $0 + c = c + 0 = c$, tj. číslo nula při sčítání ostatní čísla neovlivňuje. Proto také nazýváme nulu *neutrálním prvkem vzhledem ke sčítání celých čísel.*

Takové neutrální prvky najdeme i v jiných soustavách. Tak 1 se chová neutrálně při násobení racionálních čísel — jak známo, platí $1.a = a.1 = a$ pro všechna $a \in \mathbf{Q}$. 1 není ovšem neutrální vůči sčítání, stejně jako není nula neutrální vůči násobení. Muž, který je určen jako rozhodčí na zápasy kopané, se přece také může zúčastnit zápasu v házené jako hráč a rozhodně tam nemusí být neutrální.

Definice 3.7. Prvek n množiny M se nazývá *neutrální prvek vzhledem k neomezeně definované operaci* $\circ$ *na* M, právě když pro všechna $a \in M$ platí

$$a \circ n = n \circ a = a.$$

Platí-li $a \circ n = a$ (resp. $n \circ a = a$) pro všechna $a \in M$, nazývá se n *pravý neutrální* (resp. *levý neutrální*) *prvek operace* $\circ$.

Zřejmě je každý neutrální prvek zároveň pravý neutrální, tak i levý neutrální.

Pokusíme se vypátrat ještě další neutrální prvky: $(0)_m$, resp. $(1)_m$ jsou neutrální prvky v množině zbytkových tříd modulu m vzhledem ke sčítání, resp. vzhledem k násobení zbytkových tříd. Důkaz (jednoduchý) se vám jistě podaří. Využije se přitom skutečnost, že 0 (resp. 1)

je neutrální prvek vzhledem ke sčítání (resp. násobení) celých čísel.
Při sčítání matic stejného typu hraje roli neutrálního prvku, jak snadno nahlédneme, matice, jejíž prvky jsou vesměs nuly. Násobíme-li $n \times n$ matici $\mathbf{A}$ zleva $n \times n$ maticí

$$\mathbf{E} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

dostaneme $\mathbf{E}.\mathbf{A} = \mathbf{A}$, neboť při násobení i-tého řádku matice $\mathbf{A}$ k-tým sloupcem matice $\mathbf{E}$ dostaneme součet součinů, jež jsou vesměs rovny nule s výjimkou součinu $a_{ik}.1$. Také když násobíme matici $\mathbf{A}$ zprava maticí $\mathbf{E}$, dostaneme opět $\mathbf{A}$: platí jak $\mathbf{E}.\mathbf{A} = \mathbf{A}$, tak i $\mathbf{A}.\mathbf{E} = \mathbf{A}$, ačkoli jak známo, násobení matic není komutativní. Vyjasněte si působení matice $\mathbf{E}$ při násobení prozkoumáním příkladů, které si sami vyberete!
Tak jako v množině zbytkových tříd jsou i v množině $n \times n$ matic definovány dvě operace „sčítání" a „násobení". Vůči každé z obou operací existuje neutrální prvek. Pro lepší rozlišení se neutrální prvek vzhledem k aditivně popsané operaci také nazývá *nulový prvek* a vzhledem k multiplikativně popsané operaci *jednotkový prvek*; díky analogii s čísly 0 a 1 opravdu sugestivní označení pro neutrální prvky.
Identické zobrazení ι je prvek množiny T všech transformací množiny M. Je-li nyní φ libovolný prvek z T, platí jak $(\iota.\varphi)(a) = \varphi(\iota(a)) = \varphi(a)$, tak i $(\varphi.\iota)(a) = \iota(\varphi(a)) = \varphi(a)$ pro všechna $a \in M$, tj. $\iota.\varphi = \varphi.\iota = \varphi$. Je tedy ι neutrální prvek vzhledem ke skládání transformací množiny M.
V množině všech permutací tří prvků 1, 2, 3 může být

neutrální prvek znázorněn jako $\pi_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix}$, v množině všech posunutí roviny je to posunutí $\overrightarrow{PP}$ s nulovou „velikostí posunutí" a v množině všech otočení roviny kolem daného bodu je to otočení o nulový úhel. Vzhledem ke sčítání funkcí definovaných na intervalu I má vlastnost neutrálního prvku funkce n, kde $n(x) = 0$ pro všechna $x \in I$. Je-li totiž f libovolný prvek z množiny F těchto funkcí, tak pro všechna $x \in I$ platí: $(n \oplus f)(x) = n(x) + f(x) = 0 + f(x) = f(x)$, a tudíž $n \oplus f = f$, a protože víme, že operace $\oplus$ je komutativní, je také $f \oplus n = f$ pro všechna $f \in F$. Je tudíž také jasné, jak musí vypadat posloupnost, jež má hrát roli neutrálního prvku vzhledem ke sčítání posloupností reálných čísel. V potenční množině $\mathscr{P}(M)$ množiny M je množina M sama neutrálním prvkem vzhledem k operaci $\bigcap$ a prázdná množina $\emptyset$ je neutrální prvek vůči operaci $\bigcup$. Platí totiž $A \cap M = M \cap A = A$ a $A \cup \emptyset = \emptyset \cup A = A$ pro libovolnou množinu A z $\mathscr{P}(M)$ (srov. V(1.2)). Vám přenecháváme nalezení neutrálního prvku vzhledem k operacím $\wedge$ a $\vee$ zavedeným v množině všech dělitelů přirozeného čísla t a prozkoumání toho, zda existují neutrální prvky vůči operacím „tvoření maxima dvou reálných čísel", resp. „tvoření minima dvou reálných čísel" definovaných na R.

Není zajímavé hledat neutrální prvek vůči operaci $^0/_0$.

Uvažujme ještě, zda kromě 0 neexistuje ještě další neutrální prvek vzhledem ke sčítání celých čísel. To zřejmě nemůže nastat, neboť za předpokladu, že by existovalo $n \in \mathsf{Z}$, $n \neq 0$, rovněž s vlastností neutrálního prvku, plyne z rovnosti $n + a = a$ pro každé $a \in \mathsf{Z}$ ihned $n = a - a = 0$, což je ve sporu s předpokladem.

Můžeme to však dokázat ještě jinak: Předpokládejme, že n je spolu s nulou neutrální prvek vůči sčítání. Pak platí kromě $0 + n = n$ (1) také $0 + n = 0$ (2). Jednou

používáme toho, že 0 je neutrální prvek, podruhé, že n jako neutrální prvek při sčítání neovlivňuje žádný prvek, tedy ani nulu. Protože levé strany rovností (1) a (2) se rovnají, rovnají se i pravé strany. Je tedy $n = 0$, tj. vzhledem ke sčítání v Z existuje právě jeden neutrální prvek. Srovnáním obou myšlenkových postupů zjistíme, že jsme v prvém důkazu zahrnutím odčítání celých čísel užili více pomocných prostředků než v druhém důkazu. Protože jsme ve druhé úvaze vůbec nepoužili vlastností sčítání celých čísel, můžeme tento postup použít i na libovolnou operaci $\circ$. Tím je dokázáno, že operace v množině M nemůže mít více než jeden neutrální prvek.

Obě shora uvedené úvahy dovolují ještě další důsledek: Má-li operace $\circ$ jak pravý neutrální prvek n_P, tak i levý neutrální prvek n_L, musejí se díky rovnostem $n_L \circ n_P = n_L$ (působení pravého neutrálního prvku) a $n_L \circ n_P = n_P$ (působení levého neutrálního prvku) oba prvky shodovat. Pro operaci $\circ$ mohou tedy nastat jen následující případy:

— má pravý a nemá levý neutrální prvek,
— má levý a nemá pravý neutrální prvek,
— nemá ani levý, ani pravý neutrální prvek,
— má právě jeden neutrální prvek.

V množině F všech funkcí tedy kromě funkce $n(x) = 0$ pro všechna $x \in I$ neexistuje žádný další neutrální prvek vzhledem ke sčítání a identické zobrazení je jediný neutrální prvek vzhledem ke skládání transformací. Ve zkoumaných příkladech nenastal případ, že by operace měla jen pravý, ale nikoli levý neutrální prvek. Odčítání nezáporných celých čísel je takovou operací, neboť platí sice $a - 0 = a$ pro všechna $a \in \mathsf{N}_0$, neexistuje však prvek $n \in \mathsf{N}_0$ s vlastností $n - a = a$ pro libovolné $a \in \mathsf{N}_0$.

Neutrální prvek tedy neovlivňuje při provádění ope-

race ostatní prvky. Mohou se ale vyskytnout i speciální prvky, jež se vůči operaci chovají právě obráceně: Pozorujeme-li chování nuly při násobení reálných čísel, zjistíme, že tento prvek „pohlcuje" všechna ostatní čísla: Pro každé reálné číslo x platí $0.x = x.0 = 0$.

Definice 3.8. Prvek a množiny M se nazývá *agresívní prvek vzhledem k operaci* $\circ$ *definované na* M, právě když pro všechna $x \in M$ platí

$$a \circ x = x \circ a = a.$$

Prázdná množina $\emptyset$ v $\mathscr{P}(M)$ vystupuje jako agresívní prvek, uvažujeme-li ji vzhledem k operaci $\cap$, a množina M má tuto vlastnost vzhledem ke sjednocení (srov. V(1.2)). V množině $M = \{1, 2, 3, 4, 6, 12\}$ je číslo 1 agresívní prvek vůči tvoření největšího společného dělitele. Takový prvek můžeme v M najít i pro operaci nejmenšího společného násobku.

Má-li množina M vzhledem k asociativní operaci $\circ$ zavedené na M neutrální prvek n, pak je operace $\circ$ invertibilní, právě když jsou pro každý $a \in M$ řešitelné speciální rovnice $a \circ x = n$ a $y \circ a = n$. Je-li totiž $\circ$ invertibilní, jsou řešitelné všechny rovnice tvaru $a \circ x = b$ a $y \circ a = b$, tím spíše tedy i uvedené rovnice. A naopak, jsou-li tyto speciální rovnice řešitelné, jejich řešení označme např. $x = \bar{a}_P$, $y = \bar{a}_L$; pak můžeme hned dostat i řešení obecných rovnic: $a \circ x = b$ má řešení $x = \bar{a}_P \circ b$ a $y \circ a = b$ má řešení $y = b \circ \bar{a}_L$. Provedeme zkoušku: $a \circ x = a \circ (\bar{a}_P \circ b) = (a \circ \bar{a}_P) \circ b = n \circ b = b, y \circ a = (b \circ \bar{a}_L) \circ a = b \circ (\bar{a}_L \circ a) = b \circ n = b$.

Má tedy smysl ptát se na řešení — závisející zřejmě jen na a — rovnic $a \circ x = n$, resp. $y \circ a = n$. Kupříkladu ke každému celému číslu c přísluší v $(\mathbb{Z}, +)$ jako řešení rovnic $c + x = 0$ a $y + c = 0$ celé číslo $-c$ a v $(\mathbb{R} \setminus \{0\}, .)$ je racionálnímu číslu $r \neq 0$ rovnicí $r.x = x.r =$

$= 1$ přiřazeno racionální číslo $x = \frac{1}{r}$. Číslu 0 však tímto způsobem nemůžeme přiřadit žádné racionální číslo, protože rovnice $0.x = x.0 = 1$ nemá řešení.

Definice 3.9. Nechť $\circ$ je operace definovaná v množině M a nechť n je neutrální prvek vzhledem k $\circ$.
Prvek $\bar{a} \in M$ se nazývá *inverzním prvkem k a vzhledem* k $\circ$, právě když platí

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

Platí-li $a \circ \bar{a} = n$ (resp. $\bar{a} \circ a = n$), nazývá se $\bar{a}$ *pravý inverzní* (resp. *levý inverzní*) *prvek k a vzhledem k* $\circ$.

Zřejmě je $\bar{a}$ inverzní prvek k a, právě když je jak pravý, tak i levý inverzní prvek k a. U komutativních operací pojmy „pravý inverzní" a „levý inverzní" splývají.

Úvodní příklady vedou k domněnce, že k prvku a existuje nejvýše jeden inverzní prvek. Správnost této domněnky dokážeme pro asociativní operace v odstavci 4.2.

Díky symetrii rovností (*) vystupují prvky a a $\bar{a}$ zcela rovnoprávně, tj. je-li $\bar{a}$ inverzní prvek k a, je také a inverzní prvek k $\bar{a}$.

Prvek $\bar{a}$ inverzní k a často označujeme jako a^{-1} (resp. $-a$ při aditivním způsobu psaní); záměny s mocninou a^{-1} se nemusíme obávat, jak se později ukáže.

Chceme-li pátrat po dalších dvojicích navzájem inverzních prvků, musíme se omezit na zkoumání takových operací, jež mají neutrální prvek. V množině zbytkových tříd modulo 4 najdeme vzhledem ke sčítání ke každému prvku právě jeden takový, že jejich součet dá zbytkovou třídu $(0)_4 : (0)_4 + (0)_4 = (0)_4$, $(1)_4 + (3)_4 = (3)_4 + (1)_4 = (0)_4$ a $(2)_4 + (2)_4 = (0)_4$.

Naproti tomu neexistuje zbytková třída modulo 4, jež by byla řešením rovnice $(2)_4.(x)_4 = (1)_4$, tj. zbytková

třída $(2)_4$ nemá vzhledem k násobení zbytkových tříd inverzní prvek. Každá $n \times m$ matice (a_{ik}) má vůči sčítání matic inverzní prvek, totiž matici $(-a_{ik})$, neboť zřejmě platí

$$(a_{ik}) + (-a_{ik}) = (a_{ik} + (-a_{ik})) = (0).$$

V množině všech $n \times n$ matic existují jak prvky, jež vzhledem k násobení matic mají inverzní prvek, tj. inverzní matici, tak i takové prvky, pro něž žádnou inverzní matici nenajdeme. Podívejme se na dva příklady: K matici $\mathbf{A} = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$ je inverzní matice $\mathbf{A}^{-1} = \begin{pmatrix} 1/3 & -1/3 \\ 1/3 & 2/3 \end{pmatrix}$; platí $\mathbf{A}.\mathbf{A}^{-1} = \mathbf{A}^{-1}.\mathbf{A} = \mathbf{E}$. Přesvědčte se o tom! K matici $\mathbf{B} = \begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix}$ naproti tomu neexistuje inverzní matice. To se dá snadno ověřit, zkusíme-li vyřešit maticovou rovnici

$$\begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

jež vede na soustavu čtyř lineárních rovnic o čtyřech neznámých a, b, c, d. Má-li matice $\mathbf{A}$ inverzní matici, nazývá se *regulární*, jinak se $\mathbf{A}$ nazývá *singulární matice*. Mezi singulární matice patří mimo jiné ty, jež obsahují řádky nebo sloupce se samými nulami, a takové, u nichž je řádek, resp. sloupec, násobkem jiného řádku, resp. sloupce, což byl případ shora uvedeného příkladu.

Vůči skládání transformací existuje ke každému prvku prvek inverzní. Můžeme ukázat, že inverzní prvek k posunutí je posunutí, inverzní prvek k otočení okolo bodu P_0 je otočení okolo P_0, inverzní prvek ke shodnosti je shodnost.

Zatímco vzhledem ke sčítání funkcí ke každé funkci

existuje inverzní prvek, např. je $f(x) = -3x + \sin x$ a $g(x) = 3x - \sin x$ taková dvojice, pro operace uvedené v příkladu 5 odstavce 3.1 najdeme prvky, jež tuto vlastnost nemají. Tak v množině všech dělitelů čísla 12 neexistuje vzhledem k největšímu společnému děliteli inverzní prvek ke 4. Rovnice $\{a, b, c\} \cup X = \emptyset$ nemá v $\mathcal{P}(M)$ řešení, neexistuje tam tedy množina, jež by byla vůči $\cup$ inverzní k množině $\{a, b, c\}$. Nebude pro vás obtížné zkonstruovat další takové příklady.

RESPEKT SE VYPLÁCÍ

3.4 RELACE KONGRUENCE

Čtenář se dozví, za jakých podmínek relace ekvivalence respektuje operace a jak můžeme přirozeným způsobem definovat operaci mezi třídami rozkladu

Každé celé kladné číslo n patří buď do množiny P prvočísel, nebo do množiny P' složených čísel. $\mathbb{N}_0 \setminus \{0\}$ se tak rozpadá na dvě třídy P a P'. Ověřme na příkladech, jak je tento rozklad $\mathfrak{Z}$ množiny $\mathbb{N}_0 \setminus \{0\}$ respektován sčítáním přirozených čísel:

$$2 + 3 = 5, \quad 12 + 1 = 13, \quad 7 + 6 = 13,$$
$$3 + 5 = 8, \quad 4 + 6 = 10, \quad 11 + 9 = 20.$$

Zjišťujeme, že součet dvou prvočísel může být prvek jak P, tak i P'; také součet dvou složených čísel může být jak prvek P, tak i P'. Přičteme-li konečně prvočíslo ke složenému číslu, může zas součet ležet v kterékoli z obou tříd. Náš rozklad sčítání celých kladných čísel vůbec nerespektuje. Zdalipak respektuje alespoň násobení?

Zvolme jiný rozklad množiny $\mathbb{Z}$ celých čísel — rozdělme ji na třídu K_z záporných čísel, třídu K_k kladných čísel a třídu K_0, jež obsahuje jen nulu. Prověřme teď

chování tohoto rozkladu vůči sčítání. Součet dvou záporných čísel je sice vždy záporný, součet dvou kladných čísel vždy kladný a součet dvou prvků z K_0 vždy prvek z K_0, ale jakmile se při sčítání setkají prvky různých tříd, mohou se vyskytnout „nedisciplinovanosti“:

$$-3 + 2 = -1 \in K_z, \quad -3 + 4 = 1 \in K_k,$$
$$-3 + 3 = 0 \in K_0.$$

Zatímco náš rozklad nedostatečně respektuje sčítání, násobení se podřizuje, neboť pro libovolné $a, b \in \mathbf{Z}^+$, platí:

$$(+a).(-b) \in K_z, \quad 0.(+a) \in K_0, \quad 0.0 \in K_0,$$
$$(-a).(+b) \in K_z, \quad (+a).0 \in K_0,$$
$$(-a).(-b) \in K_k, \quad 0.(-a) \in K_0,$$
$$(+a).(+b) \in K_k, \quad (-a).0 \in K_0.$$

Příslušnost součinu dvou celých čísel do jedné třídy závisí tedy jen na příslušnosti jednotlivých činitelů do té které třídy, a ne na speciální volbě činitelů uvnitř dané třídy.

Vraťme se nakonec ještě jednou k rozkladu množiny $\mathbf{Z}$ všech celých čísel na zbytkové třídy podle relace ekvivalence „kongruentní (mod m)“. V příkladu 1 odstavce 3.1 bylo už ukázáno, že sčítání celých čísel je tvořením zbytkových tříd, resp. příslušnou relací ekvivalence respektováno: Pro $a', a'' \in (a)_m$ a $b', b'' \in (b)_m$ leží ve stejné zbytkové třídě také $a' + b'$ a $a'' + b''$, totiž v $(a + b)_m$. Za stejných předpokladů dostaneme pro $a' \equiv a''$ (mod m) a $b' \equiv b''$ (mod m), tj. $a' = a'' + gm$ a $b' = b'' + hm$, vynásobením obou posledních rovností

$$a'b' = a''b'' + m(a''h + b''g + mgh), \text{ tj.}$$
$$a'b' \equiv a''b'' \text{ (mod } m).$$

Leží-li tedy jak a' a a'', tak i b' a b'' ve stejných zbytkových třídách, platí totéž i pro $a'b'$ a $a''b''$. Relace

ekvivalence „kongruentní (mod m)“ v Z má tedy tu vlastnost, že respektuje sčítání a násobení celých čísel; takovou relaci nazýváme relace *kongruence*.

Definice 3.10. Relace ekvivalence R v množině M se nazývá *relace kongruence v struktuře* $(M, \circ)$, právě když relace R respektuje operaci $\circ$, tj. když pro všechna $a, b, a', b' \in M$ platí:

$$\text{Z } aRa' \text{ a } bRb' \text{ plyne } (a \circ b)R(a' \circ b').$$

Respekt se vyplácí! Tato snášenlivost relace „kongruentní (mod m)“ vůči sčítání, resp. násobení celých čísel dovoluje definovat v množině zbytkových tříd přirozeným způsobem novou operaci. V příkladu 1 odstavce 3.1 jsme to už předvedli: zbytkové třídy tvoří nosič nové operace. Dvě zbytkové třídy sčítáme, resp. násobíme tak, že v každé z obou tříd zvolíme libovolné celé číslo (reprezentanta) a ta sečteme, resp. vynásobíme. Každé celé číslo, které takto dostaneme, určuje jednoznačně a nezávisle na reprezentantu zbytkovou třídu, která je podle definice součtem, resp. součinem daných zbytkových tříd. Tímto způsobem jsou definovány operace v podílové množině $\mathbf{Z}/R$, která je vytvořena relací ekvivalence „kongruentní (mod m)“; množina $\mathbf{Z}/R$ tak získává strukturu: ze $(\mathbf{Z}, +, .)$ a R dostáváme $(\mathbf{Z}/R, +, .)$.

Shora uvažovaný rozklad množiny Z na třídy K_z, K_0, K_k je odvozen z relace ekvivalence, jež se ukázala jako snášenlivá vůči násobení celých čísel. Můžeme proto podle stejného principu v množině $\{K_z, K_0, K_k\}$ zavést násobení $\circ$ pomocí reprezentantů (viz tabulku).

$\circ$	K_z	K_0	K_k
K_z	K_k	K_0	K_z
K_0	K_0	K_0	K_0
K_k	K_z	K_0	K_k

Znovu abstrahujeme: Je-li relace ekvivalence R v M zároveň relací kongruence v $(M, \circ)$, můžeme mezi třídami ekvivalence podílové množiny M/R definovat operaci $\odot$ prostřednictvím reprezentantů:

$$K_x \odot K_y = K_z \Leftrightarrow x \circ y = z.$$

Přirozeně můžeme místo x, y zvolit i jiné reprezentanty x', y' z tříd ekvivalence K_x, K_y; to, že R je relace kongruence, naručuje, že součin $x' \circ y' = z'$ určitě zas patří do třídy K_z.

$(M/R, \odot)$ nazýváme *podílovou strukturou*, *faktorovou strukturou*, a nebo také *strukturou zbytkových tříd* $(M, \circ)$ vzhledem k R.

Už v příkladu 1 odstavce 3.1 jsme zjistili, že se mnohé vlastnosti operace $\circ$ v M přenášejí na operaci $\odot$ v M/R. Vysvětlení pro to najdeme v následujících odstavcích.

3.5 CVIČENÍ

1. Zjistěte, zda zúžení sčítání číselných posloupností na podmnožiny M_i $(i = 1, 2, 3)$ je neomezeně definovaná operace.
   a) M_1: množina všech aritmetických posloupností;
   b) M_2: množina všech geometrických posloupností;
   c) M_3: množina všech rostoucích posloupností.

2. Přesvědčte se, zda operace $\circ_1$ a $\circ_2$ definované následujícími tabulkami jsou komutativní či invertibilní a zda mají neutrální prvek.

$\circ_1$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\circ_2$	a	b	c	d
a	d	b	c	a
b	b	b	b	b
c	c	b	d	c
d	a	b	c	d

3. Dokažte:
$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c))$
a
$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$.

4. Nechť $\circ_3$ je operace v $\mathbf{N}_0 \setminus \{0\}$, která číslům $a \neq 0$, $b \neq 0$ přiřazuje číslo, jež dostaneme zapsáním číslic obou čísel a a b za sebe (příklad: $a = 14$, $b = 156$, $a \circ_3 b = 14\,156$). Ukažte, že $\circ_3$ je asociativní, ale není komutativní. Zjistěte, zda $\circ_3$ je invertibilní a zda má vlastnosti krácení. Obsahuje množina $\mathbf{N}_0 \setminus \{0\}$ vůči $\circ_3$ levý (pravý) neutrální prvek?

5. V množině E všech bodů roviny je definována následující operace: jestliže $P \neq Q$, je $P \triangle Q$ třetí vrchol T rovnostranného trojúhelníka PQT značeného v matematicky kladném smyslu; v případě $P = Q$ položme $P \triangle Q = P$. Zjistěte, zda $\triangle$ je komutativní, asociativní či invertibilní. Má $\triangle$ vlastnost krácení?

6. Následující „tvoření průměrů" dvou čísel můžeme chápat jako operace:
aritmetický průměr racionálních čísel
$$a \circ_4 b = \frac{a + b}{2};$$
geometrický průměr nezáporných reálných čísel
$$a \circ_5 b = \sqrt{ab};$$
harmonický průměr kladných reálných čísel
$$a \circ_6 b = \frac{2ab}{a + b}.$$
Zjistěte, zda jsou tyto operace komutativní, asociativní či invertibilní a zda je mezi nimi operace s vlastností krácení. Dokažte, že žádná z uvedených operací nemá neutrální prvek a že každý prvek je vůči těmto operacím idempotentní, tj. že platí $a \circ_4 a = a \circ_5 a = a \circ_6 a = a$ pro všechna vhodná a.

7. Dokažte asociativitu operací $\wedge$ a $\vee$ využitím vztahu: $a = b \Leftrightarrow a \mid b$ a $b \mid a$.

8. Které z následujících operací mají levý, které pravý a které oboustranný neutrální prvek?
$a \uparrow b = a^b$ v $\mathbf{N}_0$, $a \square b = |a - b|$ v $\mathbf{Q}^*$,
$a \circ b = a + b - 7$ v $\mathbf{Z}$.

9. Má-li operace vlastnost krácení, nemusí ještě být invertibilní. Doložte to na příkladu operace $a \uparrow b = a^b$ v $\mathbf{N} \setminus \{1\}$.

10. Jsou dány následující objekty s operacemi (množina a operace):

a) $(\mathbf{Z}, \circ)$, $a \circ b = a - b$,
b) $(\mathbf{N}_0, \circ)$, $a \circ b = a^b$,
c) $(\mathbf{Z}, \circ)$, $a \circ b = 2a + b$,
d) $(\mathbf{Z}, \circ)$, $a \circ b = a + b - ab$,
e) $(\mathbf{N}_0, \circ)$, $a \circ b = a$,
f) $(\mathbf{N}_0, \circ)$, $a \circ b = 0$.

Zjistěte, které operace jsou komutativní a které asociativní. Dokažte: operace v b), d), e) a f) nejsou invertibilní a v c) je jednoznačně řešitelná každá rovnice $a \circ x = c$, ale už ne každá rovnice $y \circ b = c$ je řešitelná. Pro které operace existuje neutrální prvek?

11. Je dán obdélník se středem M a osami souměrnosti g_p a g_q. Nechť m je středová souměrnost se středem M a p, resp. q osová souměrnost s osami g_p, resp. g_q, n nechť je identické zobrazení. Sestavte tabulku skládání těchto zobrazení obdélníka na sebe.
Spočítejte $p.p.q.n.m.n.q.m.p$ na základě úvah a prostřednictvím tabulky. Řešte soustavu rovnic

$$x.y = p,$$
$$y.x^2.q = m.y^2.$$

Jaká zajímavá pravidla jste objevili při počítání s těmito speciálními zobrazeními?

12. Řešte maticovou rovnici $\mathbf{AX} + \mathbf{BX} = \mathbf{C} + \mathbf{D}$, kde $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1 & -2 \\ -1 & 0 \end{pmatrix}$, $\mathbf{C} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{D} = \begin{pmatrix} 1 & -3 \\ 0 & 2 \end{pmatrix}$. Jaké vlastnosti maticových operací se využijí při řešení? Které z matic jsou regulární?