

O GRUPÁCH A OKRUHOCH I

ANTON LEGÉŇ, Bratislava

V tomto článku sa budeme zaoberať najjednoduchšími vlastnosťami grúp a okruhov. Obsah článku je v podstate určený sylabami zo základov teórie grúp — jednou z tém pre voliteľný seminár v 4. ročníku gymnázií. Pred čítaním článku odporúčame prečítať článok o teórii čísel.

Kvôli zjednodušeniu (skráteniu) formulácií budeme používať nasledujúce označenie:

- N — množina všetkých prirodzených čísel,
- Z — množina všetkých celých čísel,
- Q — množina všetkých racionálnych čísel,
- R — množina reálnych čísel,
- C — množina všetkých komplexných čísel,
- $Q^+(R^+)$ — množina všetkých kladných racionálnych (reálnych) čísel,
- $Z^-(Q^-, R^-)$ — množina všetkých záporných celých (racionálnych, reálnych) čísel,
- $Z_0(Q_0, R_0, C_0)$ — množina všetkých nenulových celých (racionálnych, reálnych, komplexných) čísel,
- \circ — operácia skladania zobrazení.

Úvod

Značná časť školskej matematiky je venovaná štúdiu vlastností čísel a počtových výkonom alebo operáciám s nimi, ako sú sčítanie, odčítanie, násobenie, odmocňovanie a pod. V tomto článku uvedieme všeobecnú definíciu operácie. Skôr než to urobíme, postupne si všimneme niektoré ich vlastnosti.

Najskôr uvažujme o sčítaní, pričom sa obmedzíme iba na celé čísla. Ak máme nejaké dve celé čísla, môžeme im priradiť jediné celé číslo — ich súčet, pričom výsledok nezávisí od poradia sčítancov. Tejto vlastnosti hovoríme komutatívnosť sčítania. Okrem toho pre sčítanie platí aj asociatívny zákon: Pre každé tri celé čísla x, y, z platí $x + (y + z) = (x + y) + z$. Osobitnú úlohu má pri sčítaní číslo 0 (nula). Ak číslo 0 pripočítame ku ktorémukoľvek celému číslu, dostaneme opäť to isté číslo. Okrem toho, ku každému celému číslu b existuje celé číslo x (obyčajne ho označujeme znakom $-b$), o ktorom platí $b + x = x + (-b) = 0$. Táto vlastnosť sčítania nám dovoľuje riešiť rovnice tvaru $a + x = b$.

Uvažujme o násobení, pričom sa obmedzíme na kladné racionálne čísla. V tomto prípade každé dve kladné racionálne čísla určujú jediné kladné racionálne číslo, a to ich súčin. Tak ako sčítanie, aj násobenie je komutatívne a asociatívne. Úlohu čísla 0 pri sčítaní preberá pri násobení číslo 1. Vieme, že $b \cdot 1 = 1 \cdot b = b$ pre každé kladné racionálne číslo (ale nielen pre ne). Analogicky, ku každému kladnému racionálnemu číslu b existuje kladné racionálne číslo x (obyčajne ho označujeme znakom $1/b$), o ktorom platí: $b \cdot x = x \cdot b = 1$. (Je zrejmé, že ak by sme uvažovali o násobení nezáporných racionálnych čísel, tak posledné tvrdenie neplatí.)

Ak uvažujeme o odčítaní, pričom budeme odčítať iba prirodzené čísla, zistíme, že situácia je podstatne odlišná. Tak napríklad nie každé dve prirodzené čísla majú rozdiel, ktorý by bol prirodzeným číslom, teda odčítanie nie je v množine N vo všeobecnosti možné. Ak by sme vyšetrovaný čiselný obor rozšírili na množinu Z , tak túto závadu odstráníme, ale zistíme, že odčítanie nie je ani komutatívne, ani asociatívne. Okrem toho nenájdeme žiadne celé číslo, ktoré by pri odčítaní hralo podobnú úlohu ako číslo 1 pri násobení, alebo číslo 0 pri sčítovaní.

Na uvedených príkladoch sme videli, že operácie sčítania, odčítania a násobenia majú isté vlastnosti, ktorých splnenie však závisí od toho, na akých množinách ich uvažujeme. Prvou spoločnou vlastnosťou je to, že v každom prípade dve čísla určujú jediné tretie číslo, ktoré je opäť z uvažovanej množiny. Ďalšou vlastnosťou je splnenie niektorých rovností a existencia prvkov, ktoré majú vzhľadom na uvažovanú operáciu isté výsadné postavenie. Na nasledujúcom príklade ukážeme, že tieto vlastnosti nie sú podmienené tým, že sme uvažovali čiselné množiny s obvyklými počtovými výkonmi.

Nech R^+ je množina všetkých kladných reálnych čísel a nech $x \Delta y = \sqrt{xy}$. Aj v tomto prípade ľubovoľné dve kladné reálne čísla x, y určujú jediné kladné reálne číslo \sqrt{xy} — ich geometrický priemer. Geometrický priemer čísel x a y nezávisí od ich poradia, t. j. $\sqrt{xy} = \sqrt{yx}$. Tejto vlastnosti hovoríme komutatívnosť.

Nech Q je množina všetkých racionálnych čísel a $x \square y = \frac{1}{2}(x + y)$ je aritmetický priemer čísel x a y . V tomto prípade tiež ľubovoľné dve racionálne čísla x, y určujú jediné racionálne číslo, pričom $x \square y = y \square x$ pre každé $x, y \in Q$.

Nech α je rovina s pravouhlou súradnicovou sústavou Ox, Oy . Priradme každej dvojici X, Y ($X = (x_1, y_1), Y = (x_2, y_2)$) bodov z α bod $S = \left(\frac{1}{2}(x_1 + x_2), \frac{1}{2}(y_1 + y_2) \right)$. (Ak $X \neq Y$, tak S je stredom úsečky XY ; ak $X = Y$, tak $S = X = Y$.) Aj v tomto prípade každá dvojica X, Y bodov z α určuje jediný bod, ktorý opäť patrí do α . Ak označíme znakom

$X * Y$ bod S , ktorý priraďujeme dvojici X, Y , tak zrejme platí $X * Y = Y * X$.

Nech α je rovina spolu s pevnou sústavou kartézskych súradníc Oxy a nech $A = (a, b)$ je nejaký bod z α . Potom posunutie určené vektorom \mathbf{OA} je zobrazenie $f_{ab}: (x, y) \mapsto (x + a, y + b)$. Označme znakom F množinu všetkých posunutí roviny α . Ak f_{ab} a f_{cd} sú nejaké dve posunutia (t. j. prvky z F), tak zobrazenie, ktoré vznikne ich zložením, je opäť posunutie: $(x, y) \xrightarrow{f_{ab}} (x + a, y + b) \xrightarrow{f_{cd}} (x + a + c, y + b + d)$, ktoré budeme označovať znakom $f_{cd} \circ f_{ab}$. Je zrejmé, že toto posunutie je jednoznačne určené a nezávisí od poradia skladania jednotlivých posunutí. Ak posunutie f_{ab} zložíme s posunutím f_{00} (t. j. s posunutím určeným nulovým vektorom), dostaneme opäť posunutie f_{ab} . Z toho vyplýva, že posunutie f_{00} hrá pri skladaní posunutí takú istú úlohu ako číslo 0 pri sčítaní alebo číslo 1 pri násobení. Nech f_{ab}, f_{cd} a f_{gh} sú nejaké tri posunutia. Potom $(x, y) \xrightarrow{f_{gh}} \mapsto (x + g, y + h) \xrightarrow{f_{ab} \circ f_{cd}} (x + a + c + g, y + b + b + d)$. Z toho vyplýva, že $(f_{ab} \circ f_{cd}) \circ f_{gh}$ je posunutie určené vektorom \mathbf{OP} , kde $P = (a + c + g, b + d + h)$. Podobne $(x, y) \xrightarrow{f_{cd} \circ f_{gh}} (x + c + g, y + d + h) \xrightarrow{f_{ab}} (x + a + c + g, y + b + d + g)$. Teda $f_{ab} \circ (f_{cd} \circ f_{gh})$ je posunutie určené tým istým vektorom \mathbf{OP} . Z toho vyplýva, že $(f_{ab} \circ f_{cd}) \circ f_{gh} = f_{ab} \circ (f_{cd} \circ f_{gh})$. Teda skladanie translácií je asociatívne. Z toho, čo sme doteraz dokázali, vyplýva, že skladanie posunutí roviny α má tie isté vlastnosti ako sčítanie celých čísel, násobenie kladných racionálnych čísel.

Podobné tvrdenie platí aj o množine všetkých rovinných alebo priestorových vektoroch so sčítaním vektorov.

V každom z uvedených príkladov sme ľubovoľnej usporiadanej dvojici prvkov z uvažovanej množiny (Z, Q^+, F) priradili jediný prvak z tejto množiny; určili sme teda zobrazenie kartézskeho súčinu $Z \times Z (Q^+ \times Q^+, F \times F)$ do $Z (Q^+, F)$. Takéto zobrazenia budeme nazývať binárnymi operáciami. Uvedené operácie majú isté vlastnosti, ktoré — ako sme to videli — sú v istom zmysle toho istého druhu. Špecifikovaním týchto vlastností (čo neskôr urobíme) dostaneme rôzne typy algebraických štruktúr s jednou (neskôr s dvoma) binárnymi operáciami.

2. Binárne operácie

V predchádzajúcim odseku sme si ukázali niekoľko príkladov binárnych operácií. Skôr ako uvedieme presnú definíciu binárnej operácie, zopakujeme niektoré známe pojmy.

Usporiadaná dvojica prvkov u a v je množina $(u, v) = \{\{u\}, \{u, v\}\}$. Prvky u a v nazývame zložkami usporiadanej dvojice (u, v) ; u prvou zložkou

a v druhou zložkou. Teda usporiadaná dvojica je množina, ktorej prvkami sú množiny, a to množina $\{u\}$ pozostávajúca z prvku u a množina $\{u, v\}$ pozostávajúca z prvkov u a v . Ak (u, v) a (x, y) sú dve usporiadane dvojice, tak $(u, v) = (x, y)$ práve vtedy, keď $u = x$ a $v = y$.

Ak A a B sú nejaké množiny, tak pod ich kartézskym súčinom rozumieme množinu $A \times B$ všetkých usporiadaných dyoje (a, b) , ktorých prvá zložka patrí do A a druhá zložka patrí do B . Ak $A = B$, tak namiesto $A \times A$ budeme písat A^2 .

Zobrazením $f : A \rightarrow B$ množiny A do množiny B rozumieme takú podmnožinu $f \subseteq A \times B$, o ktorej platí: Ku každému $a \in A$ existuje práve jedno $b \in B$, že $(a, b) \in f$. Prvok b nazývame obrazom prvku a v zobrazení f a obvykle ho označujeme $f(a)$ alebo $a \xrightarrow{f} b$ (ak nemôže dôjsť k nedorozumeniu, tak iba $a \mapsto b$).

Nech $f : A \rightarrow B$ je zobrazenie, $X \subseteq A$ a $Y \subseteq B$. Množinu $\{f(x); x \in X\}$ (t. j. množinu všetkých obrazov prvkov z X) nazývame obrazom množiny X v zobrazení f a označujeme ju $f(X)$. Množinu $\{x \in A; f(x) \in Y\}$ (t. j. množinu všetkých tých prvkov z A , ktorých obrazy patria do Y) nazývame vzorom množiny Y v zobrazení f a označujeme ju $f^*(Y)$. Ak $Y = \{b\}$, tak namiesto $f^*(\{b\})$ budeme písat iba $f^*(b)$ a každý prvok z tejto množiny budeme nazývať vzorom prvku b .

Definícia 1. Binárnu operáciu na množine A ($A \neq \emptyset$) rozumieme každé zobrazenie f množiny A^2 do množiny A . Prvok $f(x, y)$, kde $(x, y) \in A^2$ budeme nazývať kompozíciou prvkov x a y a množinu A nosičom operácie f .

Pretože zápis $f(x, y)$ pre kompozíciu prvkov x a y je komplikovaný, budeme operácie označovať znakmi \circ , \square , $,$, $+$ a kompozíciu prvkov x a y budeme označovať: $x \circ y$ (čítaj: x krúžok y); $x \square y$ (čítaj: x štvorček y); $x \cdot y$ alebo iba xy (čítaj: x krát y); $x + y$ (čítaj: x plus y) podľa toho, akým symbolom budeme označovať uvažovanú operáciu. V tom prípade, keď operáciu budeme označovať znakom $.$ ($+$), budeme ju nazývať násobenie (sčítanie), a to aj vtedy, keď nosič tejto operácie nebude číselná množina a operácia $.$ ($+$) nebude násobením (sčítaním) čísel.

Všimnime si dve veľmi dôležité vlastnosti operácie na množine A , ktoré sú zahrnuté v jej definícii. Prvou z nich je jednoznačnosť operácie. To znamená, že kompozícia ľubovoľných dvoch prvkov z A je určená jednoznačne. Táto vlastnosť je dôsledkom toho, že operácia je zobrazením. Druhou vlastnosťou je uzavretosť operácie, čo znamená, že kompozícia ľubovoľných prvkov z A patrí opäť do A .

Teraz uvedieme niekoľko príkladov operácií.

Priklad 1. Sčítanie je operácia na množine \mathbb{N} všetkých prirodených čísel, pretože každej usporiadanej dvojici $(x, y) \in \mathbb{N}^2$ priraduje prirodzené číslo $x + y$, ktoré — ako vieme — je jediné. Obdobne aj násobenie je

operáciou na množine N . Naproti tomu odčítanie a delenie nie sú operáciami na množine N , pretože rozdiel a podiel lubovoľných prirodzených čísel nemusí byť prirodzené číslo. Ak by sme však uvažovali množinu Z všetkých celých čísel, tak odčítanie je už na Z operáciou.

Priklad 2. Nech $A = \{a, b, c\}$ a nech $\square: A^2 \rightarrow A$ je zobrazenie definované takto: $(a, a) \mapsto a, (a, b) \mapsto b, (a, c) \mapsto c, (b, a) \mapsto b, (b, b) \mapsto a, (b, c) \mapsto a, (c, a) \mapsto c, (c, b) \mapsto a, (c, c) \mapsto b$. Túto operáciu môžeme znázorniť aj nasledujúcou tabuľkou:

\square	a	b	c
a	a	b	c
b	b	a	a
c	c	a	b

Tabuľku sme zostavili tak, aby kompozícia $x \square y$ ležala na priesčníku riadku určeného prvkom x so stĺpcom, ktorý je určený prvkom y . Tabuľky, ktorými znázorňujeme operácie na konečných množinách, nazývame multiplikačnými tabuľkami alebo Cayleyho tabuľkami. Neskôr uvidíme, že zápis operácií (na množinách, ktoré nemajú príliš veľa prvkov) pomocou multiplikačných tabuliek má okrem prehľadnosti niekoľko výhod, na ktoré upozorníme.

Priklad 3. Nech A je množina všetkých vektorov v rovine, t. j. množina všetkých usporiadaných dvojíc (a, b) reálnych čísel. Obvyklý súčet vektorov (a, b) a (c, d) definovaný vzťahom $(a, b) + (c, d) = (a + c, b + d)$ je binárna operácia na množine A . Analogicky, súčet lubovoľných dvoch trojrozmerných vektorov (t. j. usporiadaných trojíc reálnych čísel) je binárna operácia na množine všetkých takýchto vektorov.

Priklad 4. Nech \mathcal{A} je množina všetkých zhodných zobrazení roviny α , ktorými sa reprodukuje daný štvorec $ABCD$ ležiaci v rovine α . Množina \mathcal{A} pozostáva z ôsmich prvkov, ktoré označíme takto:

$$\begin{aligned} i &= \begin{pmatrix} A & B & C & D \end{pmatrix}, & a &= \begin{pmatrix} A & B & C & D \\ B & D & A & C \end{pmatrix}, & b &= \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}, \\ c &= \begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}, & d &= \begin{pmatrix} A & B & C & D \\ D & B & C & A \end{pmatrix}, & e &= \begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}, \\ f &= \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}, & g &= \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \end{aligned}$$

(i je identické zobrazenie, a je otočenie o 90° , b otočenie o 180° , c otočenie o 270° , d súmernosť podľa osi CB , e súmernosť podľa osi AD , f a g súmernosti podľa symetrál jednotlivých strán uvažovaného štvorca.) Potom skladanie

zobrazení je operácia na množine \mathcal{A} . Multiplikačnou tabuľkou tejto operácie je nasledujúca tabuľka:

\circ	i	a	b	c	d	e	f	g
i	i	a	b	c	d	e	f	g
a	a	b	c	i	g	f	d	e
b	b	c	i	a	e	d	g	f
c	c	i	a	b	f	g	e	d
d	d	f	e	g	i	b	a	c
e	e	g	d	f	b	i	c	a
f	f	e	g	d	c	a	i	b
g	g	d	f	e	a	c	b	i

Definícia 2. Hovoríme, že operácia \square na množine A je komutatívna, keď pre každé $a, b \in A$ platí: $a \square b = b \square a$.

Komutatívne operácie budeme obyčajne označovať znakom $+$.

Sčítanie a násobenie prirodzených čísel sú komutatívne operácie. Operácie z príkladov 2 a 3 sú komutatívne. Naproti tomu odčítanie celých čísel nie je komutatívna operácia, pretože $4 - 2 = 2$ a $2 - 4 = -2$. Tak isto aj operácia popísaná v príklade 4 nie je komutatívou operáciou, pretože $a \circ g = e \neq d = g \circ a$.

Ak máme zistiť, či operácia popísaná multiplikačnou tabuľkou je komutatívna, stačí zistiť, či je symetrická podľa hlavnej uhlopriečky, t. j. podľa uhlopriečky idúcej z ľavého horného rohu do pravého dolného rohu tabuľky. Pomocou tohto kritéria ľahko zistíme, že tabuľka z príkladu 2 určuje komutatívnu operáciu, zatiaľ čo tabuľka z príkladu 4 určuje nekomutatívnu operáciu.

Predpokladajme, že na množine A je definovaná nejaká binárna operácia \square a nech $x, y, z \in A$. Pretože $x' = x \square y$ a $y' = y \square z$ sú prvky z A , má zmysel hovoriť o kompozícii $x' \square z = (x \square y) \square z$, resp. $x \square y' = x \square (y \square z)$ prvkov x' a z , resp. prvkov x a y' . Tieto kompozície nemusia byť vždy totožné. Napríklad, ak za operáciu \square vezmeme aritmetický priemer a za čísla x, y, z vezmeme čísla 1, 2, 3, tak $x \square y = \frac{1}{2}(1+2) = 3/2$ a $y' = y \square z = \frac{1}{2}(2+3) = 5/2$. Potom $(x \square y) \square z = 9/4$ a $x \square (y \square z) = 7/4$. V uvedenom prípade výrazy $x \square (y \square z)$ a $(x \square y) \square z$ označujú rôzne prvky z R ; teda „aritmetický priemer“ troch čísel závisí od spôsobu, akým ho vypočítame. (Lepšie povedané nemá zmysel hovoriť o aritmetickom priemere troch (a viacerých) prvkov, pretože nie je jednoznačne určený.) Tento výsledok sice nesúhlasí s našou skúsenosťou so sčítovaním (násobením)

čísel, ale je celkom prirodzený. Niet totiž dôvodu očakávať, že všeobecné binárne operácie budú mať také isté vlastnosti, aké majú obvyklé operácie s číslami. To, že výsledok sčítania (násobenia) troch alebo viacerých čísel nezávisí od spôsobu uzátvorkovania, je dôsledkom toho, že sčítanie (násobenie) je asociatívna operácia v zmysle nasledujúcej definície:

Definícia 3. Hovoríme, že operácia \square na množine A je asociatívna, ak pre ľubovoľné tri prvky $x, y, z \in A$ platí: $(x \square y) \square z = x \square (y \square z)$, t. j. ak spĺňa tzv. asociatívny zákon.

Operácie sčítania a násobenia z príkladu 1 sú asociatívnymi operáciami. Odčítanie na množine Z celých čísel nie je asociatívna operácia, pretože: $3 - (4 - (-2)) = -3$ a $(3 - 4) - (-2) = 1$. Operácia z príkladu 2 je tiež neasociatívna, pretože $c \circ (c \circ b) = c \circ a = c$ a $(c \circ c) \circ b = b \circ b = a$. Tento príklad ukazuje, že pri preverovaní asociatívneho zákona treba vyskúšať všetky možné (usporiadane) trojice prvkov z A . Operácia popísaná v príklade 4 je asociatívna. Nebudeme to však dokazovať, pretože toto naše tvrdenie je dôsledkom všeobecného tvrdenia, ktoré si vyslovíme v nasledujúcom príklade.

Príklad 5. Nech $F(A)$ je množina všetkých zobrazení množiny A do A ($A \neq \emptyset$) a $f, g \in F(A)$. Označme znakom $f \circ g$ zobrazenie A do A definované takto: Pre každé $x \in A$ $(f \circ g)(x) = f(g(x))$ ($f \circ g$ je zobrazenie zložené zo zobrazení f a g). Ukážeme, že operácia \circ skladania zobrazení je asociatívna. Aby sme to dokázali, stačí ukázať, že pre ľubovoľné tri zobrazenia $f, g, h \in F(A)$ platí $(f \circ g) \circ h = f \circ (g \circ h)$. Táto rovnosť však platí práve vtedy, keď pre každé $x \in A$ platí $[(f \circ g) \circ h](x) = [f \circ (g \circ h)](x)$. Vypočítajme výraz na ľavej strane tejto rovnosti: $[(f \circ g) \circ h]x = (f \circ g)(h(x)) = f(g(h(x)))$. Úpravou pravej strany dostávame: $[f \circ (g \circ h)](x) = f[(g \circ h)(x)] = f(g(h(x)))$. Pretože výsledky sú totožné, uvedená rovnosť je pravdivá. Z toho však vyplýva, že operácia skladania zobrazení je asociatívnou operáciou. K tomuto príkladu — v špeciálnom znení — sa ešte podrobne vrátíme.

Pretože v príklade 4 skladáme zhodné zobrazenia roviny, ktoré reprodukujú daný štvorec $ABCD$, uvedená multiplikačná tabuľka určuje asociatívnu operáciu.

Doteraz uvedené príklady operácií ukazujú, že komutatívny a asociatívny zákon sú navzájom nezávislé, t. j. že existujú neasociatívne komutatívne operácie a nekomutatívne asociatívne operácie. Je samozrejmé, že existujú operácie, ktoré spĺňajú oba zákony (sčítanie a násobenie prirodzených čísel), práve tak ako existujú operácie nesplňajúce ani jeden z uvedených zákonov.

Definícia 4. Usporiadanú dvojicu (G, \square) , kde G je neprázdna množina a \square je operácia na G , nazývame grupoid. Množinu G nazývame nosičom grupoidu (G, \square) a \square nazývame operáciou grupoidu (G, \square) .

$(N, +)$, (N, \cdot) , $(Z, -)$, $(\{a, b, c\}, \square)$ kde \square je operácia popísaná tabuľkou z príkladu 2, $(\mathcal{A}, \circ) = (\{i, a, b, c, d, e, f, g\}, \circ)$, kde \circ je operácia z príkladu 4, $(F(A), \circ)$, kde \circ je operácia skladania zobrazení, sú grupoidy.

Grupoid, ktorého operácia je komutatívna, nazývame komutatívnym grupoidom. Takýmto grupodom sú grupoidy $(N, +)$, (N, \cdot) , $(\{a, b, c\}, \square)$.

Definícia 5. Grupoid, ktorého operácia je asociatívna nazývame pologrupou.

Z vyššie uvedených príkladov sú pologrupami nasledujúce grupoidy: $(N, +)$, (N, \cdot) , (\mathcal{A}, \circ) a $(F(A), \circ)$.

Cvičenia

1. Dokážte, že usporiadane dvojice (u, v) a (x, y) sú totožné práve vtedy, keď $x = u$ a $y = v$.

2. Nech R^+ je množina všetkých kladných reálnych čísel. Zistite, či aritmetický priemer $\frac{1}{2}(x + y)$ a geometrický priemer \sqrt{xy} sú asociatívne operácie na R^+ .

3. Nech R je množina všetkých reálnych čísel. Označme znakom $\max\{x, y\}$ väčšie z čísel x a y a $\min\{x, y\}$ menšie z čísel x a y . Sú \max a \min operácie na R a spĺňajú komutatívny alebo asociatívny zákonn?

4. Nech $d(x, y)$ je najväčší spoločný deliteľ a $n(x, y)$ je najmenší spoločný násobok prirodzených čísel x a y . Dokážte, že d a n sú operácie na množine N všetkých prirodzených čísel a zistite, či sú asociatívne a komutatívne.

5. Zistite, či je množina všetkých zhodných zobrazení reprodukujúcich daný trojuholník ABC s operáciou skladania zobrazení pologrupou. Ak je, zostavte jej multiplikačnú tabuľku.

6. To isté, čo v predchádzajúcim cvičení urobte pre daný obdĺžnik $ABCD$.

7. Nech 2^A je množina všetkých podmnožín množiny A . Zistite, či operácie: zjednotenie $(X, Y) \mapsto X \cup Y$ a prienik $(X, Y) \mapsto X \cap Y$ ($X, Y \in 2^A$) sú asociatívne a komutatívne na 2^A .

8. Na množine $A = \{a, b, c, d\}$ definujte takú binárnu operáciu, ktorá bude mať iba jednu neasociatívnu trojicu.

9. Na množine $A = \{a, b, c, d\}$ definujte takú binárnu operáciu ktorá bude mať iba dve nekomutatívne dvojice.

10. Je možné na trojprvkovej množine definovať takú binárnu operáciu, ktorá by mala práve jednu neasociatívnu trojicu?

3. Neutrálne a inverzné prvky

Ak je na množine A definovaná operácia, tak niektoré prvky z A môžu mať vzhľadom na túto operáciu niektoré špeciálne vlastnosti. Ak napríklad uvažujeme pologrupu (N, \cdot) prirodzených čísel s operáciou násobenia, tak takýmto prvkom je číslo 1: $a \cdot 1 = 1 \cdot a = a$ pre každé $a \in N$. Podobne sa správa prvak a z príkladu 2: $a \square x = x \square a = x$ pre každé $x \in A$. Prvky,

ktoré majú túto vlastnosť (vzhľadom na nejakú operáciu) nazývame neutrálnymi prvkami tejto operácie.

Definícia 6. Nech \square je operácia na množine A . Prvok $e \in A$ nazývame ľavým (pravým) neutrálnym prvkom operácie \square , ak pre každé $x \in A$ platí: $e \square x = x$ ($x \square e = x$).

Priklad 6. Nech $A = \{a, b, c, d\}$ a \square je operácia na A popísaná nasledujúcou tabuľkou:

\square	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	b	c	b	d
d	c	d	c	c

Potom prvky a a b sú ľavými neutrálnymi prvkami operácie \square , ale nie sú pravými neutrálnymi prvkami operácie \square . Podobným spôsobom by sme mohli nájsť príklad operácie, ktorá má viac než jeden pravý neutrálny prvok, ale nemá ani jeden ľavý neutrálny prvok.

Priklad 7. Nech $A = \{a, b, c\}$ a \square je operácia na A popísaná nasledujúcou multiplikačnou tabuľkou:

\square	a	b	c
a	a	c	c
b	b	b	c
c	c	c	c

Potom prvak a je pravým neutrálnym prvkom operácie \square , ale nie je ľavým neutrálnym prvkom tejto operácie. Dá sa nájsť príklad operácie, ktorá má ľavý neutrálny prvok, ale nemá ani jeden pravý neutrálny prvok.

Veta 1. Nech \square je operácia na množine A a $e \in A$ je jej ľavým neutrálnym prvkom a f je jej pravým neutrálnym prvkom. Potom $e = f$.

Dôkaz. Pretože e je ľavým neutrálnym prvkom, $e \square f = f$. Keďže f je pravým neutrálnym prvkom, $e \square f = e$. Z uvedených rovností vyplýva rovnosť $e = f$.

Z predchádzajúcej vety vyplýva, že nosič binárnej operácie môže obsahovať najviac jeden prvak, ktorý by bol aj ľavým aj pravým neutrálnym prvkom tejto operácie.

Definícia 7. Prvok z nosiča operácie \square , ktorý je jej ľavým aj pravým neutrálnym prvkom, nazývame neutrálnym prvkom operácie \square . Ak operá-

ciou bude súčin (súčet), tak neutrálny prvok budeme nazývať jednotkovým (nulovým) prvkom alebo len jednotkou (nulou).

Ak operácia grupoidu (pologrupy) (G, \square) má neutrálny prvok e , tak ho (ju) nazývame grupoidom (pologrupou) s neutrálnym prvkom (alebo monoidom). Prvok e nazývame neutrálnym prvkom grupoidu (pologrupy, monoidu) (G, \square) .

Pologrupa $(F(A), \circ)$ ($F(A)$) je množina všetkých zobrazení množiny A a \circ je operácia skladania zobrazení) je pologrupa s neutrálnym prvkom (je ním identické zobrazenie množiny A). Podobne, množina všetkých zhodných zobrazení reprodukujúcich daný štvorec s operáciou skladania zobrazení je pologrupa s neutrálnym prvkom (je ním prvak i).

Príklad 8. Čitateľ sa už stretol s tzv. binomickou rovnicou $x^n = 1$ (n je prirodzené číslo). Vieme, že všetky (komplexné) korene tejto rovnice sú určené vzťahom $x_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$, kde $k = 0, 1, \dots, n-1$ (alebo ľubovoľným n po sebe nasledujúcim celým číslam). Uvažujme teraz o množine K_n všetkých koreňov uvedenej rovnice. Súčin $x_k x_j$ ľubovoľných dvoch koreňov x_k a x_j koreňov rovnice $x^n = 1$ je opäť jej koreňom. Aby sme to dokázali, musíme ukázať, že $(x_k x_j)^n = 1$. To je však pravda, lebo $(x_k x_j)^n = x_k^n x_j^n = 1 \cdot 1 = 1$. Z toho vyplýva, že násobenie komplexných čísel je operácia na K_n . Pretože násobenie komplexných čísel je asociatívne a číslo 1 je koreňom našej rovnice, (K_n, \cdot) je monoid.

Ak sa chceme presvedčiť, či operácia zadaná multiplikačnou tabuľkou má ľavý (pravý) neutrálny prvak, stačí zistiť, či niekterý z prvkov určuje riadok (stĺpec) totožný s horným (ľavým) riadkom (stĺpcem).

Definícia 8. Nech (G, \square) je grupoid s neutrálnym prvkom e . Hovoríme, že prvak $a' \in G$ ($a'' \in G$) je ľavým (pravým) inverzným prvkom vzhľadom na operáciu \square k prvku $a \in G$, keď $a' \square a = e$ ($a \square a'' = e$).

Veta 2. Ak x' je ľavým a x'' je pravým inverzným prvkom k prvku x z monoidu (G, \cdot) , tak $x' = x''$.

Dôkaz. Pretože x' je ľavým a x'' je pravým inverzným prvkom k prvku x , platí $x' \cdot x = e = x \cdot x''$. Keďže $x' = x' \cdot e = x' \cdot (x \cdot x'') = (x' \cdot x) \cdot x'' = e \cdot x'' = x''$, dôkaz vety je skončený.

Z vety vyplýva, že ak nejaký prvak monoidu (asociatívnosť operácie sme v dôkaze využívali!) má ľavý aj pravý inverzný prvak, tak tieto prvky sú totožné. Táto veta nám dovoľuje vyslovie nasledujúcu definíciu.

Definícia 9. Hovoríme, že prvak monoidu má inverzný prvak, ak má aj ľavý aj pravý inverzný prvak. Prvok ku ktorému existuje inverzný prvak, budeme nazývať invertibilným prvkom.

Z predchádzajúcej vety vyplýva tiež i to, že ak k nejakému prvku monoidu existuje inverzný prvok, tak existuje jediný. Inverzný prvok k prvku x vzhladom na násobenie (sčítanie) budeme označovať znakom x^{-1} ($-x$ a nazývať opačným prvkom k prvku x).

Ak chceme priamo z multiplikačnej tabuľky zistieť, či k nejakému prvku x existuje ľavý inverzný prvok, stačí preveriť, či v stĺpci určenom prvkom x leží neutrálny prvok. Ľavým inverzným prvkom je potom prvok, ktorý určuje riadok, ktorého priesecníkom s naším stĺpcom je nájdený neutrálny prvok. Pravý inverzný prvok sa hľadá podobne, len riadky a stĺpce si vymenia úlohy.

Neutrálny prvok operácie je inverzným prvkom sám k sebe. Prvok b z príkladu 2 je tiež svojím inverzným prvkom; naproti tomu k prvku c neexistuje ani ľavý ani pravý inverzný prvok. Priamo z tabuľky v príklade 4 sa dá zistiť, že každý prvok má inverzný prvok.

Ak y je koreňom rovnice $x^n = 1$ (t. j. keď platí $y^n = 1$), tak aj $1/y$ je jej koreňom, lebo $\left(\frac{1}{y}\right)^n = \frac{1}{y^n} = \frac{1}{1} = 1$. Z toho vyplýva, že ku každému $y \in K_n$ existuje v K_n inverzný prvok vzhladom na násobenie komplexných čísel, ktoré, ako sme ukázali, je operáciou na K_n . (Inverzným prvkom k $y \in K_n$ je číslo $1/y$.)

Pre grupoidy veta 2 vo všeobecnosti neplatí. Grupoid z príkladu 2 nie je pologrupa (neasociatívnu trojicou je trojica (c, c, b)). Prvok b má dva rôzne inverzné prvky, a to b a c , čo sa dá ľahko zistiť z tabuľky. Nasledujúci príklad ukazuje, že existujú pologrupy, v ktorých existujú prvky majúce viac než jeden ľavý inverzný prvok. (Je zrejmé, že takéto prvky nemôžu mať pravé inverzné prvky.)

Priklad 9. V tomto príklade ukážeme, že zobrazenie $f : N \rightarrow N$ definované predpisom $f : n \mapsto n + 1$ a patriace do pologrupy $F(N)$ má v tejto pologrupe nekonečne mnoho ľavých inverzných prvkov, a teda ani jeden pravý. Ľavými inverznými prvkami k prvku f budú zobrazenia f_k , $k = 1, 2, \dots$, ktoré sú definované takto:

$$\begin{aligned} f_k(n) &= n - 1, \text{ ak } n > 1 \\ f_k(1) &= k. \end{aligned}$$

Teraz ukážeme, že $f_k \circ f$ je pre každé k identické zobrazenie množiny N . Skutočne: $(f_k \circ f)(n) = f_k(f(n)) = f_k(n + 1) = (n + 1) - 1 = n$ pre každé $n \in N$. Z toho však vyplýva, že $f_k \circ f$ je identické zobrazenie množiny N . Je zrejmé, že zobrazenia f_1, f_2, f_3, \dots sú navzájom rôzne, je ich nekonečne mnoho a všetky sú ľavými inverznými prvkami k f v pologrupe $F(N)$.

Veta 3. Kompozícia ľubovoľných dvoch invertibilných prvkov monoidu je opäť invertibilný prvok.

Dôkaz. Nech x' je inverzným prvkom k prvku x a y' je inverzným prvkom k prvku y . Potom $y' \cdot x'$ je inverzným prvkom k prvku $x \cdot y$. Skutočne: $(x \cdot y) \cdot (y' \cdot x') = x \cdot (y \cdot y') \cdot x' = x \cdot e \cdot x' = x \cdot x' = e$. Podobne by sa dokázalo, že prvak $y' \cdot x'$ je aj ľavým inverzným prvkom k prvku $x \cdot y$. Z toho vyplýva, že $x \cdot y$ je invertibilný prvak.

Poznámka. Vetu 3 možno zovšeobecniť na libovoľný konečný počet činiteľov.

Z vety vyplýva, že inverzný prvak ku kompozícii dvoch invertibilných prvkov sa rovná kompozícii v opačnom poradí k nim inverzných prvkov.

Cvičenia

11. Zistite, či operácie z cvičení 2, 3, 4, 5, 6, 7 majú neutrálne prvky.

12. Zistite, ktoré prvky majú ľavé (pravé) inverzné prvky vzhľadom na operácie z cvičení 2, 3, 4, 5, 6, 7.

13. Nájdite neutrálny prvak operácie $\square : R \times R \rightarrow R$ (R je množina všetkých reálnych čísel) definovanej vzťahom $x \square y = xy + x + y$.

14. Zistite, ku ktorým reálnym číslam existujú inverzné prvky vzhľadom na operáciu definovanú v predchádzajúcim cvičením.

15. Nech 2^A je množina všetkých podmnožín množiny A s operáciou rozdielu množín ($X \square Y = X \setminus Y$ pre každé $X, Y \in 2^A$). Dokážte, že prázdna množina je pravým neutrálnym prvkom tejto operácie, ale nie je jej ľavým neutrálnym prvkom. Ďalej dokážte, že pravým inverzným prvkom k množine $X \in 2^A$ je každá množina $Y \in 2^A$ s vlastnosťou $Y \supseteq X$.

16. Nech 2^A je množina všetkých podmnožín množiny A s operáciou symetrická differencia ($X \dot{-} Y = (X \setminus Y) \cup (Y \setminus X)$ pre každé $X, Y \in 2^A$). Nájdite neutrálny prvak tejto operácie a dokážte, že každá množina $X \in 2^A$ má inverzný prvak vzhľadom na túto operáciu. Zostavte multiplikačnú tabuľku tejto operácie pre množinu $A = \{a, b, c\}$.

17. Nech $A = \{0, 1, 2, 3\}$. Definujme na A operáciu \square takto: $x \square y$ sa rovná zvyšku, ktorý dostaneme po delení čísla $x^3 + 2xy$ číslom 4. Zostavte multiplikačnú tabuľku tejto operácie a zistite, či má neutrálny prvak.

18. Nájdite príklad takej binárnej operácie, ktorá bude mať práve toľko ľavých neutrálnych prvkov, kolko prvkov má jej nosič.

19. Nájdite príklad monoidu, ktorý bude obsahovať prvak majúci práve dva ľavé inverzné prvky.

20. Ukážte na príklade, že podmienku asociatívnosti z vety 2 nemožno vynechať.

4. Grupy

Definícia 10. Monoid (G, \cdot, e) nazývame grupou, ak ku každému jeho prvku existuje inverzný prvak (vzhľadom na jeho operáciu).

Teda množina G s binárnou operáciou na G je grupou práve vtedy, keď platí:

1. Pre každé $x, y, z \in G$ je $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (asociatívny zákon).

2. Existuje prvok $e \in G$ s vlastnosťou $e \cdot x = x \cdot e = x$ pre každé $x \in G$ (existencia neutrálneho prvku).

3. Ku každému $x \in G$ existuje také $x' \in G$, že $x \cdot x' = x' \cdot x = e$.

Pretože ďalej operáciu grupy budeme označovať a nazývať násobenie, neutrálny prvok budeme nazývať jednotkovým prvkom alebo iba jednotkou a inverzný prvok k prvku x budeme označovať x^{-1} . Ak grupová operácia bude komutatívna, tak ju budeme označovať + a neutrálny prvok budeme nazývať nulovým prvkom alebo iba nulou a označovať 0; inverzný prvok k prvku x budeme nazývať opačným prvkom k prvku x a označovať $-x$. V prípade, že nebude môcť prísť k nedorozumeniu, tak grupu $(G, .)$ budeme označovať iba znakom G a budeme hovoriť o grupe G .

Priklad 10. Nech R^+ označuje množinu všetkých kladných reálnych čísel. Pretože súčin kladných reálnych čísel je opäť kladné reálne číslo, násobenie je operácia na R^+ . Keďže násobenie je komutatívna a asociatívna operácia a prevrátená hodnota kladného reálneho čísla je kladné reálne číslo (inverzný prvok vzhľadom na operáciu násobenia), $(R^+, .)$ je komutatívna grupa (jednotkovým prvkom je číslo 1).

Priklad 11. Nech Q_0 je množina všetkých nenulových racionálnych čísel. Pretože súčin lubovoľných nenulových racionálnych čísel je nenulové racionálne číslo, násobenie je operácia na Q_0 . Pretože aj ostatné podmienky z definície grupy sú splnené (preverte ich podrobne!), $(Q_0, .)$ je grupa (dokonca komutatívna).

Lahko sa dá nahliadnuť, že operácia na množine všetkých zhodných zobrazení reprodukujúcich daný štvorec spĺňa podmienky uvedené v definícii grupy. Teda tieto zobrazenia tvoria vzhľadom na operáciu skladania zobrazení grupu, ktorú budeme označovať \mathcal{A} .

Monoid $(K_n, .)$ všetkých koreňov rovnice $x^n = 1$ je grupa. V podstate sme to dokázali za definíciou 8, kde sme ukázali, že ku každému koreňu existuje inverzný prvok vzhľadom na násobenie, ktorý je tiež koreňom uvažovanej rovnice. Túto grupu budeme nazývať grupou všetkých n -tých odmocín z jednotky.

Priklad 12. Nech K je množina všetkých komplexných jednotiek, t. j. množina všetkých komplexných čísel, ktorých absolútна hodnota sa rovná 1. Pretože súčin $(\cos \varphi + i \sin \varphi)(\cos \psi + i \sin \psi) = \cos(\varphi + \psi) + i \sin(\varphi + \psi)$ komplexných jednotiek je opäť komplexná jednotka, násobenie je operácia na K . Pretože násobenie je asociatívna a komutatívna operácia a číslo 1 je komplexnou jednotkou, $(K, .)$ je monoid. Inverzný prvok (vzhľadom na násobenie) ku komplexnej jednotke $(\cos \varphi + i \sin \varphi)$ je číslo $= \cos \varphi - i \sin \varphi$ — teda opäť komplexná jednotka a teda, $(K, .)$ je grupa, ktorú budeme nazývať grupou komplexných jednotiek.

Priklad 13. Nech Z je množina všetkých celých čísel. Ak delíme nejaké celé číslo x číslom 5, dostaneme tzv. neúplný podiel q a zvyšok r (q a r sú

celé čísla, jednoznačne určené), pričom platí:

$$x = 5q + r, \quad 0 \leq r < 5.$$

Všetkých možných zvyškov je 5: 0, 1, 2, 3, 4. Množiny všetkých celých čísel, ktoré po delení číslom 5 budú dávať ten istý zvyšok r budeme nazývať zvyškovou triedou modulo 5. Všetkých zvyškových tried je práve toľko, kolko je zvyškov po delení číslom 5. Keďže každé celé číslo patrí práve do jednej triedy, máme množinu Z rozloženú na päť tried. Triedu, do ktorej patrí číslo x , budeme označovať \bar{x} a množinu všetkých zvyškových tried modulo 5 budeme označovať Z_5 . Celé číslo y bude patriť do triedy \bar{x} práve vtedy, keď po delení číslom 5 dá ten istý zvyšok ako číslo x , t. j. práve vtedy, keď bude platiť: $x = 5q + r$ a $y = 5q_1 + r$. Táto podmienka je však ekvivalentná s podmienkou $x - 5q = y - 5q_1$. Úpravou tejto rovnosti zistíme, že x a y patria do tej istej triedy práve vtedy, keď $x - y = 5(q - q_1) = 5q'$, t. j. práve vtedy, keď rozdiel $x - y$ bude deliteľný piatimi.

Predpokladajme teraz, že $\bar{x}_1 = \bar{x}_2$ a $\bar{y}_1 = \bar{y}_2$, t. j. že $x_1 - x_2 = 5q_1$ a $y_1 - y_2 = 5q_2$. Sčítaním týchto dvoch rovností a úpravou výsledku dostaneme vzťah $(x_1 + y_1) - (x_2 + y_2) = 5(q_1 + q_2) = 5q$. Z toho však vyplýva, že čísla $x_1 + y_1$ a $x_2 + y_2$ patria do tej istej zvyškovej triedy, t. j. že $x_1 + y_1 = x_2 + y_2$. Podobne odčítaním zistíme, že $x_1 - y_1 = x_2 - y_2$. Uvažujme teraz o rozdieli $x_1y_1 - x_2y_2$. Platí: $x_1y_1 - x_2y_2 = (x_1 - x_2)y_1 + x_2(y_1 - y_2) = 5q_1y_1 + x_25q_2 = 5(q_1y_1 + x_2q_2) = 5q'$. Z toho však vyplýva, že čísla x_1y_1 a x_2y_2 patria do tej istej zvyškovej triedy modulo 5.

Z posledných vzťahov vyplýva: Ak si zvolíme nejaké dve triedy \bar{x} a \bar{y} a z nich vyberieme po jednom číslе, tak trieda, do ktorej patrí súčet a súčin vybraných čísel, nezávisí od toho ako sme tieto čísla vybrali, ale závisí iba od voľby tried \bar{x} a \bar{y} . Tento fakt nám dovoľuje na Z_5 definovať operácie nasledujúcim spôsobom:

1. sčítanie \oplus : $\bar{x} \oplus \bar{y} = \overline{x + y}$ pre ľubovoľné $\bar{x}, \bar{y} \in Z_5$;

2. násobenie \odot : $\bar{x} \odot \bar{y} = \overline{xy}$ pre ľubovoľné $\bar{x}, \bar{y} \in Z_5$.

Z definície operácie \oplus vyplýva, že súčet zvyškových tried \bar{x} a \bar{y} je trieda, do ktorej patrí číslo $x + y$. Podobne, súčin dvoch tried \bar{x} a \bar{y} je trieda, do ktorej patrí číslo xy . Aby sme si tieto operácie mohli lepšie predstaviť, zostavíme si ich multiplikačné tabuľky:

\oplus	0	1	2	3	4		0	1	2	3	4
0	0	1	2	3	4		0	0	0	0	0
1	1	2	3	4	0		1	2	3	4	
2	2	3	4	0	1		2	4	1	3	
3	3	4	0	1	2		3	1	4	2	
4	4	0	1	2	3		4	3	2	1	

Z tabuľiek sa možno presvedčiť, že obe operácie sú komutatívne, že majú neutrálne prvky (0 resp. 1). Z definície operácií \oplus a \odot vyplýva, že sú asociatívne. Skutočne: $\bar{x} \oplus (\bar{y} \oplus \bar{z}) = \bar{x} \oplus (\bar{y} + \bar{z}) = \bar{x} + (\bar{y} + \bar{z}) = = (\bar{x} + \bar{y}) + \bar{z} = (\bar{x} + \bar{y}) \oplus \bar{z} = (\bar{x} \oplus \bar{y}) \oplus \bar{z}$ a $(\bar{x} \odot \bar{y}) \odot \bar{z} = \bar{x} \bar{y} \odot \bar{z} = = (\bar{x} \bar{y}) \bar{z} = \bar{x} (\bar{y} \bar{z}) = \bar{x} \odot \bar{y} \bar{z} = \bar{x} \odot (\bar{y} \odot \bar{z})$. (V oboch prípadoch sme využívali iba definíciu príslušnej operácie a asociatívnosť sčítania, resp. násobenia celých čísel.) Z prvej tabuľky vidno, že ku každému prvku zo Z_5 existuje opačný prvok (vzhľadom na operáciu \oplus). Z druhej tabuľky vidime, že 0 nemá inverzný prvok, ale všetky ostatné ho už majú. Z toho, čo sme si tu povedali vyplýva, že (Z_5, \oplus) je grupa, ktorú nazývame aditívou grupou zvyškových tried modulo 5 a (Z_5, \odot) je monoid. Pomocou druhej tabuľky sa dá zistiť, že nenulové prvky zo Z_5 tvoria vzhľadom na operáciu \odot (zúženú na túto množinu) grupu (jej multiplikačná tabuľka je vyčiarkaná). K tomuto príkladu sa — vo všeobecnejšej forme — ešte vrátim.

V nasledujúcej vete urobíme „revíziu“ definície grupy. V definícii sme žiadali aby operácia grupy mala jednotkový prvok a aby ku každému prvku existoval inverzný prvok. Dokážeme, že tieto podmienky možno zoslabiť, a to tak, že budeme žiadať iba jednostranný jednotkový prvok (napríklad ľavý) a iba jednostranný inverzný prvok (ľavý).

Veta 4. Pologrupa (G, \cdot) je grupa práve vtedy, keď má ľavú jednotku a ku každému $a \in G$ existuje ľavý inverzný prvok.

Dôkaz. Je zrejmé, že každá grupa splňa obe podmienky vety. Obrátene, nech (G, \cdot) je pologrupa, ktorá splňa obe podmienky vety. Dokážeme, že (G, \cdot) je grupa. Najskôr dokážeme, že ľavý inverzný prvok a' k prvku $a \in G$ je aj jeho pravým inverzným prvkom, t. j. dokážeme, že $aa' = e$, kde e je ľavá jednotka z G . Keďže každý prvok z G má ľavý inverzný prvok, má ho aj a' — označme ho a'' . Počítajme: $aa' = e(aa') = (a''a')(aa') = a''(a'a) a' = a''(ea') = a''a' = e$. Tým sme dokázali, že $aa' = e$, teda a' je aj pravým inverzným prvkom k prvku a . Teraz dokážeme, že e je aj pravou jednotkou pologrupy (G, \cdot) . Nech $a \in G$ je ľubovoľný prvok. Potom $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$. Tým je dôkaz vety skončený.

Pri ďalšej vete, ktorú uvedieme, budeme predpokladať, že čitateľ je oboznámený s podmienkami existencie koreňa všeobecnej lineárnej rovnice $ax = b$. (Existencia koreňa závisí od čísel a a b). Teraz dokážeme, že každá rovnica $ax = b$ má v grupe koreň. Pretože násobenie grupy je vo všeobecnosti nekomutatívne, má zmysel hovoriť aj o rovnici $ya = b$.

Veta 5. Nech (G, \cdot) je grupa. Potom rovnice $ax = b$ a $ya = b$ majú pre každé a a b z G práve jeden koreň (v G).

Dôkaz. Predpokladajme, že rovnica $ax = b$ má v G koreň z . Potom vyňásobením zľava rovnosti $az = b$ prvkom a^{-1} dostaneme $z = a^{-1}b$. Z toho

vyplýva, že ak uvedená rovnica má v G koreň, tak ním musí byť prvok $a^{-1}b$. O tom, že tento prvok je skutočne koreňom uvažovanej rovnice, sa presvedčíme dosadením. Koreň rovnice $ya = b$ nájdeme analogicky. (Je ním prvok ba^{-1} .)

Z predchádzajúcej vety vyplýva, že existencia koreňa rovníc $ax = b$ a $ya = b$ je nutnou podmienkou na to, aby pologrupa bola grupou. V nasledujúcej vete dokážeme, že aj postačujúcou.

Veta 6. Nech (G, \cdot) je pologrupa, a nech pre každé $a, b \in G$ majú rovnice $ax = b$ a $ya = b$ v G aspoň jeden koreň. Potom (G, \cdot) je grupa.

Dôkaz. Aby sme dokázali, že (G, \cdot) je grupa, treba dokázať, že G má ľavú jednotku a že ku každému prvku z G existuje ľavý inverzný prvok. Potom na základe vety 4 bude (G, \cdot) grupou. Zvoľme $c \in G$ pevne. Potom rovnica $yc = c$ má v G koreň — označme ho e . (Platí $ec = c$.) Dokážeme, že koreň e poslednej rovnice je ľavou jednotkou pologrupy (G, \cdot) , t. j. dokážeme, že $ed = d$ pre každé $d \in G$. Keďže každá rovnica tvaru $ax = b$ má koreň v G , má ho aj rovnica $cx = d$. Z toho vyplýva, že prvok d môžeme vyjadriť v tvare $d = ch$. Počítajme: $ed = e(ch) = (ec)h = ch = d$. (dosadili sme namiesto d prvok ch , potom sme využili asociatívny zákon, ďalej rovnosť $ec = c$). Z posledného vzťahu vyplýva, že e je ľavá jednotka pologrupy (G, \cdot) . To, že každý prvok má ľavý inverzný prvok, vyplýva z toho, že rovnica $xa = e$ má v G koreň; tento koreň je zrejmé hľadaným ľavým inverzným prvkom k prvku a . Tým je dôkaz vety skončený.

Teraz zavedieme ďalší pojem, a to mocninu prvku grupy. Analýzou definície mocniny zistíme, že po formálnej stránke je taká istá, ako definícia mocniny reálneho čísla. Prirodzená mocnina a^n prvku z grupy G je definovaná takto:

$$\begin{aligned} a^n &= a, \text{ ak } n = 1; \\ a^n &= aa^{n-1} \text{ pre } n > 1. \end{aligned}$$

Ak $n = 0$, tak $a^0 = e$; ak n je celé záporné číslo, tak $a^n = (a^{-1})^{-n}$. Z uvedenej definície vyplýva, že n -tú mocninu pre prirodzené n sme mohli definovať už v pologrupe, ale nie v grupoide, lebo v nej využívame asociatívnosť násobenia.

Ak operáciu grupy označujeme znakom $+$, tak n -tú mocninu prvku a grupy nazývame n -tý násobok a označujeme ho na . Definíciu celočíselného násobku prvku a grupy s operáciou $+$ možno pre prirodzené n formulovať takto:

$$1a = a \text{ a } na = a + (n - 1)a, \text{ ak } n > 1.$$

Pre $n = 0$ položme $0a = 0$, kde znak 0 na pravej strane uvedenej rovnosti je nulový prvok (neutrálny prvok) grupy. Ak n je celé záporné číslo, tak $na = (-n)(-a)$, kde $-a$ je opačný prvok k prvku a .

Pre počítanie s takto definovanou mocninou platia analogické pravidlá ako pre mocniny reálnych čísel. Indukciou sa dá dokázať, že pre prirodzené čísla m a n platí $a^n a^m = a^{n+m}$ a $(a^n)^m = a^{nm}$. Pravidlo $(ab)^n = a^n b^n$ platí práve vtedy, keď $ab = ba$. Uvedené pravidlá platia dokonca pre každé celé čísla m a n . Dokážeme jedno z nich, napríklad, $a^n a^m = a^{n+m}$. Ostatné prenecháme čitateľovi ako cvičenie.

Dôkaz urobíme najskôr pre $m, n \in N$, a to indukciou vzhľadom na m . Ak $m = 1$, tak $a^n a^1 = a^n a = a^{n+1}$ podľa definície mocniny. Predpokladajme, že nás vzťah platí pre všetky $k \leq m$; dokážeme, že platí aj pre $k = m + 1$. Skutočne: $a^n a^{m+1} = a^n a^m a = a^{n+m} a = a^{n+m+1}$ (najskôr sme využili definíciu mocniny, potom indukčný predpoklad a opäť definíciu mocniny). Predpokladajme teraz, že aj m aj n sú záporné. Potom $a^n a^m = (a^{-1})^{-n} (a^{-1})^{-m} = (a^{-1})^{-n-m} = a^{n+m}$. Ak $m = -h$, kde $0 \leq h \leq n$, položme $k = n - h \geq 0$. Potom $a^n a^m = a^k a^{-h} = a^k a^{h(a^{-1})^{-1}} = a^k$, čo sme mali dokázať. Ak $m = -h$, kde $h > n$, položme $k = -n + h > 0$. Potom $a^n a^m = a^n a^{-h} = a^n a^{-n-k} = a^n (a^{-1})^{n+k} = a^n (a^{-1})^n (a^{-1})^k = = a^n (a^n)^{-1} a^{-k} = a^{-k}$, čo bolo treba dokázať. Ak by bolo m kladné a n záporné, postupovali by sme analogicky alebo by sme využili to, čo sme už dokázali. Tým je dôkaz pravidla skončený.

Dalšou analógiou s reálnymi číslami je tzv. pravidlo o krátení. Vieme, že v rovnosti medzi číslami môžeme krátiť ľubovoľným nenulovým číslom. Keďže operácia grupy je vo všeobecnosti nekomutatívna, máme dve pravidlá o krátení — ľavé a pravé:

Z každej rovnosti $ax = ay$ ($xa = ya$) medzi prvkami grupy vyplýva rovnosť $x = y$.

Skutočne, ak rovnosť $ax = ay$ vynásobíme zľava inverzným prvkom k prvému a , dostaneme požadovanú rovnosť. Pravé pravidlo o krátení sa dokáže analogicky.

Je prirodzené položiť si otázku (po skúsenostach s rovnicami), či platnosť oboch pravidiel o krátení nie je aj postačujúcou podmienkou na to, aby pologrupa bola grupou. Nasledujúci príklad ukazuje, že tomu tak nie je. V monoide $(N, .)$, ktorý nie je grupou (napr. k číslu 2 neexistuje v N inverzny prvok vzhľadom na násobenie), platí pravidlo o krátení.

Cvičenia

21. Zistite, ktorá z naledujúcich algebraických štruktúr je grupou, a ktorá je iba monoidom, prípadne iba pologrupou: $(N, .)$, $(N, +)$, $(Z, +)$, $(Z^-, +)$, $(Z, .)$, $(Q^+, +)$, $(Q^+, .)$, $(Q_0, +)$, $(Q_0, .)$, $(R, .)$, $(R, +)$, $(R_0, +)$, $R_0, .)$, $(C, .)$, $(C_0, .)$, $(C, .)$.

22. Na množine $A = \{a, b, c, d\}$ definujte operáciu \square pomocou multiplikačnej tabuľky tak, aby (A, \square)

- a) bol grupoid a nebola pologrupa;
- b) bola pologrupa a neboli monoid;

- c) bol monoid a nebola grupa;
d) bola grupa.

23. Nech 2^A je množina všetkých podmnožín množiny A . Dokážte, že 2^A je grupa vzhľadom na operáciu symetrická diferencia.

24. Zostavte multiplikačnú tabuľku operácie symetrická diferencia pre množinu $A = \{a, b, c\}$.

25. Nech $\bar{K} = \bigcup_{n=1}^{\infty} K_n$, kde K_n je množina všetkých odmocní z 1. Dokážte, že \bar{K} s operáciou násobenia je komutatívna grupa.

26. Nech $M = \{1, 2, 3\}$. Permutáciou množiny M rozumieme ktorúkoľvek z nasledujúcich bijekcií na množine M :

$$\begin{aligned}\pi_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \pi_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \pi_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \pi_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \pi_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \pi_6 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.\end{aligned}$$

Dokážte, že množina $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$ s operáciou skladania zobrazení, je grupa. Je komutatívna? Zostavte multiplikačnú tabuľku operácie tejto grupy.

27. Riešte rovnice $\pi_3x = \pi_4$ a $y\pi_3 = \pi_4$. (π_3, π_4 majú ten istý význam ako v predchádzajúcom cvičení).

28. Nech $A = \{a, b, c\}$. Pomocou multiplikačnej tabuľky z cvičenia 24 vyriešte rovnicu $\{a, b\} \cdot x = \{b, c\}$.

29. Dokážte, že pre každé celé čísla m a n každý prvok a grupy platí $a^n a^m = a^{n+m}$.

30. Nech prvky a, b z grupy G komutujú, t. j. nech $ab = ba$. Dokážte, že pre každé celé číslo n platí: $(ab)^n = a^n b^n$. (Návod: Najskôr dokážte — indukciou — že vztah platí pre všetky prirodzené čísla.)

31. Dokážte, že každá konečná pologrupa, v ktorej platia obe pravidlá o krátení, je grupa.

32. Nájdite príklad pologrupy s ľavou jednotkou, v ktorej bude mať každý prvok pravý inverznyj prvok a ktorá nebude grupou.

33. Nech $x_1, x_2, \dots, x_n (n \geq 2)$ sú lubovoľné prvky z grupy G . Dokážte, že platí: $(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} \dots x_2^{-1} x_1^{-1}$.

5. Grupy zvyškových tried

V tomto odseku sa vrátime k príkladu 13. Nech Z je množina všetkých celých čísel a $n > 1$. Ak celé číslo m delíme číslom n , tak dostaneme tzv. neúplný podiel q a zvyšok r (q a r sú celé čísla), pričom platí

$$m = nq + r, \quad 0 \leq r < n.$$

Týmito dvoma podmienkami sú čísla q a r jednoznačne určené. Všetkých možných zvyškov je n ; sú nimi čísla $0, 1, 2, \dots, n - 1$. Množinu všetkých celých čísel, ktoré po delení číslom n dajú ten istý zvyšok r , budeme nazývať zvyškovou triedou modulo n . Zvyškových tried modulo n je práve toľko, kolko je zvyškov po delení číslom — teda n . Keďže každé celé číslo patri

práve do jednej triedy modulo n (zvyšok je určený jednoznačne), máme množinu Z rozloženú na n navzájom disjunktných množín. Triedu určenú číslom m (t. j. triedu, do ktorej patrí číslo m) budeme označovať \bar{m} a množinu všetkých zvyškových tried modulo n znakom Z_n . Nech m a p sú nejaké celé čísla. Triedy \bar{m} a \bar{p} budú totožné práve vtedy, keď ich zvyšky po delení číslom n budú rovnaké, t. j. práve vtedy, keď bude platí $m = qn + r$ a $p = q_1n + r$. Táto podmienka je však ekvivalentná s podmienkou $m - nq = p - nq_1$. Úpravou tejto rovnosti zistíme, že $\bar{m} = \bar{p}$ práve vtedy, keď $m - p = n(q - q_1) = n \cdot q'$, t. j. práve vtedy, keď rozdiel $m - p$ je deliteľný číslom n .

Predpokladajme, že $\bar{m}_1 = \bar{m}_2$ a $\bar{p}_1 = \bar{p}_2$, t. j. že $m_1 - m_2 = nq_1$ a $p_1 - p_2 = nq_2$. Sčítaním týchto dvoch rovností a úpravou dostaneme $m_1 + p_1 - (m_2 + p_2) = n(q_1 + q_2) = nq$. Z tohto však vyplýva, že čísla $\underline{m_1 + p_1}$ a $\underline{m_2 + p_2}$ patria do tej istej triedy modulo n , t. j. že $\underline{m_1 + p_1} = \underline{m_2 + p_2}$. Uvažujme teraz o rozdieli $m_1p_1 - m_2p_2$. Pretože $m_1p_1 - m_2p_2 = (m_1 - m_2)p_1 + m_2(p_1 - p_2) = nq_1p_1 + m_2nq_2 = n(q_1p_1 + m_2q_2) = nq$, čísla m_1p_1 a m_2p_2 určujú tú istú triedu modulo n .

Z posledných dvoch výsledkov vyplýva: Ak zvolíme nejaké dve triedy \bar{x} a \bar{y} (modulo n) a z nich vyberieme po jednom číslе, ktoré nazývame reprezentantmi týchto tried, tak triedy, do ktorých patria súčet a súčin reprezentantov, nezávisí od ich voľby, ale závisí iba od voľby tried \bar{x} a \bar{y} . Táto skutočnosť nám dovoľuje definovať na Z_n dve operácie:

$$\text{sčítanie } \oplus: \bar{x} + \bar{y} = \underline{\bar{x} + \bar{y}},$$

$$\text{násobenie } \odot: \bar{x} \cdot \bar{y} = \underline{\bar{x} \cdot \bar{y}},$$

pre ľubovoľné $\bar{x}, \bar{y} \in Z_n$.

Z definície operácie \oplus vyplýva, že súčet zvyškových tried \bar{x} a \bar{y} je trieda, do ktorej patrí číslo $\bar{x} + \bar{y}$. Podobne súčin tried \bar{x} a \bar{y} je trieda, do ktorej patrí číslo $\bar{x} \cdot \bar{y}$.

Pretože sčítanie a násobenie celých čísel sú komutatívne operácie, tak aj operácie \oplus a \odot na Z_n sú komutatívne. Obe operácie majú neutrálne prvky. Neutrálnym prvkom operácie \oplus je $\bar{0}$ a neutrálnym prvkom operácie \odot je $\bar{1}$. Keďže $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$ a $(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \bar{x}(\bar{y} \cdot \bar{z})$ (pre všetky $x, y, z \in Z$), čísla $\bar{x} + \bar{y} + \bar{z}$ a $\bar{x} \cdot \bar{y} \cdot \bar{z}$ určujú tie isté triedy. To isté platí aj o číslach $(\bar{x} \cdot \bar{y}) \cdot \bar{z}$ a $\bar{x}(\bar{y} \cdot \bar{z})$. Z toho však vyplýva, že operácie \oplus a \odot sú asociatívne. Tým sme dokázali, že (Z_n, \oplus) a (Z_n, \odot) sú komutatívne monoidy. Monoid (Z_n, \oplus) je však komutatívnu grupou, pretože $\bar{x} + \underline{-x} = \underline{\bar{x}} + \underline{-x} = \bar{0}$. (Ku každej triede $\bar{x} \in Z_n$ existuje opačná trieda, a to $\underline{-x}$.)

Predpokladajme, že \underline{n} je prvočíslo a $\bar{m} \neq \bar{0}$, $\bar{p} \neq \bar{0}$ sú nejaké triedy zo Z_n . Potom aj trieda $\bar{m}\bar{p} = \bar{m} \odot \bar{p} \neq \bar{0}$. Skutočne. Ak by sa $\bar{m}\bar{p} = \bar{0}$, tak $n \mid mp$. Pretože n je prvočíslo, $n \mid m$ alebo $n \mid p$, teda $\bar{m} = \bar{0}$ alebo $\bar{p} = \bar{0}$. To je však spor s výberom tried \bar{m} a \bar{p} . Z toho však vyplýva, že operáciu \odot

možno zúžiť na $(Z_n^+ = \{1, 2, \dots, \overline{n-1}\})$. (Ak n nie je prvočíslo, tak to nemožno urobiť — prečo?) Teda (Z_n^+, \odot) je komutatívny monoid. Dokážeme, že je grupou. Aby sme to dokázali, treba ukázať, že ku každému prvku $\bar{m} \in Z_n^+$ existuje inverzný prvok (vzhľadom na operáciu \odot). Ak $\bar{m} \in Z_n^+$, tak najväčší spoločný deliteľ (m, n) čísel m a n sa rovná 1 (číslo n má iba dva delitele — a to 1 a n), t. j. $1 = mp + nq$. Z poslednej rovnosti vyplýva, že čísla 1 a $mp + nq$ patria do tej istej triedy, a to do triedy $\bar{1}$. Ale trieda $mp + nq$ je totožná s triedou $\bar{1} = \bar{m} \odot \bar{p}$ (využili sme definíciu operácie \oplus a \odot). Z tejto rovnosti vyplýva, že \bar{p} je inverzným prvkom k prvku \bar{m} . Tým je dokázané, že (Z_n^+, \odot) je komutatívna grúpa.

Poznámka. Dôkaz posledného tvrdenia nie je celkom korektný. Nekorektnosť dôkazu spočíva v tom, že sme v ňom využívali aj definíciu operácie \oplus .

Je zrejmé, že trieda určená prvkom x podľa modulu n je iná ako množina určená tým istým číslom x podľa modulu m ($m \neq n$ sú prirodzené čísla). Nech napríklad $n = 3$ a $m = 5$. Potom triedy modulo 3 sú množiny: $\bar{0} = \{0, 3, -3, 6, -6, \dots\} = \{3k; k \in \mathbb{Z}\}$; $\bar{1} = \{1, -2, 4, -5, \dots\} = \{3k + 1; k \in \mathbb{Z}\}$; $\bar{2} = \{2, -1, 5, -4, 8, -7, \dots\} = \{3k + 2; k \in \mathbb{Z}\}$. Naproti tomu triedami modulo 5 sú množiny: $\bar{0} = \{0, 5, -5, 10, -10, \dots\} = \{5k; k \in \mathbb{Z}\}$, $\bar{1} = \{1, -4, 6, -9, 11, -14, \dots\} = \{5k + 1; k \in \mathbb{Z}\}$, $\bar{2} = \{2, -3, 7, -8, 12, -13, \dots\} = \{5k + 2; k \in \mathbb{Z}\}$, $\bar{3} = \{3, -2, 8, -7, 13, -12, \dots\} = \{5k + 3; k \in \mathbb{Z}\}$, $\bar{4} = \{4, -1, 9, -6, 14, -11, \dots\} = \{5k + 4; k \in \mathbb{Z}\}$.