## Predslov

Algebra patrí medzi najstaršie matematické disciplíny. V minulosti bola chápaná ako náuka o počítaní s písmenami vo význame čísel (tzv. všeobecnými číslami) na rozdiel od aritmetiky, ktorá sa chápala ako náuka o počítaní s konkrétnymi číslami (tzv. zvláštnymi číslami). Takéto chápanie sa i dnes často odráža pri vyučovaní elementárnej (stredoškolskej) algebry.

Pod súčasnou algebrou chápeme najmä náuku o algebraických štruktúrach, náuku o polynómoch a algebraických rovniciach a lineárnu algebru. Pritom sa polynómy, algebraické rovnice i lineárna algebra niekedy chápu ako súčasť široko ponímanej náuky o algebraických štruktúrach.

Cieľom týchto skrípt je vyložiť prístupným spôsobom pre študentov učiteľského štúdia (kombinácií s matematikou) základné poznatky o najznámejších algebraických štruktúrach – grupách, okruhoch, oboroch integrity, telesách a poliach. V II. a III. dieli skrípt plánujeme výklad základných poznatkov o polynómoch a algebraických rovniciach resp. základy lineárnej algebry.

I. diel sme rozčlenili na 15 kapitol. Úvodná kapitola, v ktorej sa zaoberáme zvyškovými triedami celých čísel, je akýsi jednotiaci prvok pre celý náš výklad a v ďalších kapitolách sa k zvyškovým triedam celých čísel často vraciame. Nasleduje osem kapitol venovaných základným poznatkom o grupách. V deviatej kapitole uvádzame klasifikáciu všetkých konečných grúp do rádu 15. Nasleduje päť kapitol o okruhoch, oboroch integrity, telesách a poliach a záverečná pätnásta kapitola je venovaná ekvivalentným a dôsledkovým úpravám pri riešení algebraických rovníc nad obormi integrity.

Usilovali sme sa dodržať prehľadnú štruktúru skrípt. Položky ako definície, lemy, vety, dôsledky a príklady sú číslované spôsobom $x.y$, kde $x$ je číslo kapitoly a $y$ je poradové číslo položky v kapitole $x$. Takto napríklad pri odvolaní sa na definíciu 12.8 (teleso, pole) je možné rýchlo vyhľadať požadovanú definíciu ako položku č. 8 v kapitole 12. Definície pojmov, ktoré nie sú v tomto texte uvedené, možno nájsť v [6].

Číselné obory prirodzených, celých, racionálnych, reálnych a komplexných čísel označujeme v tomto texte symbolmi $N, Z, Q, R$, resp. $C$. Ak máme na mysli len podmnožinu kladných resp. záporných čísel daného číselného oboru, pridávame hore symbol $+$ resp. $-$. Napríklad $N^+$ označuje množinu všetkých kladných prirodzených čísel, $Z^-$ označuje množinu všetkých záporných celých čísel, a pod. Ďalej symbolom $\mathrm{D}(k,l)$ označujeme najväčší spoločný deliteľ a symbolom $\mathrm{n}(k,l)$ najmenší spoločný násobok prirodzených čísel $k, l$. Symbol $\mathcal{P}(X)$ používame na označenie potenčnej množiny (množiny všetkých podmnožín) množiny $X$ a symbolom $\mathrm{id}_X$ označujeme identické zobrazenie na množine $X$. Skladanie zobrazení robíme tak ako v [6] a nie ako napr. v [5].

Ďakujeme recenzentom **RNDr. P. Hrnčiarovi, CSc.** a **Doc. RNDr. D. Palumbínymu, CSc.** za starostlivé prečítanie rukopisu tohto textu a ich cenné podnety. Uvítame i podnety z radov čitateľov, ktoré možno posielať napr. e-mailom na adresu **haviar@bb.sanet.sk** alebo **klenovca@pdf.umb.sk**.

V Banskej Bystrici, 20 apríla 1998

autori

## 1. Zvyškové triedy celých čísel

Vieme, že goniometrická funkcia sínus je periodická a to s periódou $360^0$. Znamená to, že napr. uhly $30^0, 30^0 + 360^0, \ldots, 30^0 + k \cdot 360^0, \ldots$, $k \in N$ sa v istom zmysle „rovnajú“, presnejšie tomu hovoríme, že sú kongruentné podľa modulu 360. Podobne je to pri určovaní hodín (s periódou 12 hodín alebo 24 hodín) prípadne dní (napríklad s periódou 7 dní). Kongruenciami celých čísel sa budeme teraz podrobnejšie zaoberať.

1.1 Definícia. Nech $a, b, m \in Z$, $m > 1$. Budeme hovoriť, že číslo $a$ je kongruentné s číslom $b$ podľa modulu $m$ (alebo modulo $m$), ak $m \mid a - b$.

Ak $a$ je kongruentné s $b$ podľa modulu $m$, tak píšeme $a \equiv b \pmod m$ alebo skrátene $a \equiv_m b$.

Ak $m \nmid a - b$, tak hovoríme, že $a$ nie je kongruentné s $b$ podľa modulu $m$ a píšeme $a \not\equiv b \pmod m$.

1.2 Veta. *Nech $m \in Z$, $m > 1$. Potom pre každé $a$, $b$, $c \in Z$ platí*

*a)* $a \equiv a \pmod m$,

*b)* *ak* $a \equiv b \pmod m$, *tak* $b \equiv a \pmod m$,

*c)* *ak* $a \equiv b \pmod m$ *a* $b \equiv c \pmod m$, *tak* $a \equiv c \pmod m$.

Dôkaz. Dôkazy týchto tvrdení vyplývajú z vlastností deliteľnosti. Na ukážku uvedieme dôkaz časti c).

Nech $a \equiv b \pmod m$ a $b \equiv c \pmod m$. Potom $m \mid a - b$ a $m \mid b - c$, z čoho vyplýva, že $m \mid (a - b) + (b - c)$, t.j. $m \mid a - c$ čo znamená, že $a \equiv c \pmod m$. □

Vlastnosti a), b), c) z predchádzajúcej vety vlastne hovoria, že binárna relácia $\equiv$ (podľa modulu $m$) je na množine $Z$ reláciou ekvivalencie. Vytvára teda rozklad množiny $Z$. Nasledujúca veta ukazuje, ktoré celé čísla patria do jednej triedy tohto rozkladu.

1.3 Veta. *Dve celé čísla $a$, $b$ sú kongruentné podľa modulu $m$ vtedy a len vtedy, keď pri delení číslom $m$ majú rovnaký zvyšok.*

Dôkaz. Nech $a \equiv b \pmod m$. Potom $m \mid a - b$, teda existuje $k \in Z$ také, že $a - b = m \cdot k$, t.j. $a = b + m \cdot k$. Nech pri delení čísla $b$ číslom $m$ je zvyšok $r$, t.j.

$$b = m \cdot q + r, \qquad 0 \le r < m.$$

Potom

$$a = b + m \cdot k = m \cdot q + r + m \cdot k = m \cdot (q + k) + r, \quad 0 \le r < m.$$

To znamená, že aj pri delení čísla $a$ číslom $m$ je ten istý zvyšok $r$.

Obrátene, nech pri delení čísel $a$, $b$ číslom $m$ je zvyšok $r$, t.j.

$$a = m \cdot q_1 + r, \quad b = m \cdot q_2 + r, \quad 0 \le r < m.$$

Potom $a - b = m \cdot (q_1 - q_2)$, teda $m \mid a - b$, čo znamená, že $a \equiv b \pmod m$. □

Nech $m \in Z$, $m > 1$. Označme $a_m = \{x \in Z;\, x \equiv a \pmod m\}$. Množinu $a_m$ (niekedy, najmä pri riešení úloh, ju budeme označovať $\overline{a}$) budeme volať *zvyšková trieda (podľa modulu $m$)* a číslo $a$ budeme volať *reprezentant* (zvyškovej triedy $a_m$).

Z vety 1.3 vyplýva, že do zvyškovej triedy $a_m$ budú patriť všetky celé čísla, ktoré pri delení číslom $m$ majú taký istý zvyšok ako číslo $a$, t.j.

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad a_m = b_m.$$

Kongruencia podľa modulu $m$ teda vytvára rozklad množiny celých čísel na $m$ zvyškových tried $0_m, 1_m, \ldots, (m-1)_m$. Systém zvyškových tried, ktorý vytvorí kongruencia podľa modulu $m$ budeme označovať $Z/\equiv_m$ alebo $\overline{Z}_m$.

1.4 Príklad. Ak $m = 4$, tak možné zvyšky sú 0, 1, 2, 3 a
$\{\ldots, -8, -4, 0, 4, 8, \ldots\} = \cdots = \overline{-8} = \overline{-4} = \overline{0} = \overline{4} = \overline{8} = \ldots,$
$\{\ldots, -7, -3, 1, 5, 9, \ldots\} = \cdots = \overline{-7} = \overline{-3} = \overline{1} = \overline{5} = \overline{9} = \ldots,$
$\{\ldots, -6, -2, 2, 6, 10, \ldots\} = \cdots = \overline{-2} = \overline{2} = \overline{6} = \overline{10} = \ldots,$
$\{\ldots, -5, -1, 3, 7, 11, \ldots\} = \cdots = \overline{-5} = \overline{-1} = \overline{3} = \overline{7} = \overline{11} = \ldots.$
Príslušný rozklad množiny celých čísel je teda systém $\overline{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Nasledujúce tvrdenie a jeho dôsledok ukazujú, že niektoré vlastnosti rovnosti celých čísel a kongruencie celých čísel sú rovnaké.

1.5 Veta. *Nech $a, b, c, d, m \in Z$, $m > 1$. Ak $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, tak*

$$a + c \equiv b + d \pmod{m}, \tag{1}$$

$$a \cdot c \equiv b \cdot d \pmod{m}. \tag{2}$$

Dôkaz. Nech $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$. Potom $m \mid a - b$ a $m \mid c - d$, z čoho vyplýva

$$m \mid (a-b) + (c-d), \quad \text{teda} \quad a + c \equiv b + d \pmod{m}$$

a tiež

$$m \mid (a-b) \cdot d + (c-d) \cdot a, \quad \text{teda} \quad a \cdot c \equiv b \cdot d \pmod{m}.$$

□

1.6 Dôsledok. *Nech $a \equiv b \pmod{m}$, $c \in Z$, $n \in N$. Potom*

$$a + c \equiv b + c \pmod{m}, \tag{3}$$

$$a \cdot c \equiv b \cdot c \pmod{m}, \tag{4}$$

$$a^n \equiv b^n \pmod{m}. \tag{5}$$

Dôkaz. Pre každé celé číslo $c$ je $c \equiv c \pmod{m}$ (lebo relácia $\equiv$ je na množine $Z$ reflexívna). Vzťah (3) potom vyplýva z (1) a vzťah (4) vyplýva z (2).

Vzťah (5) dokážeme matematickou indukciou.

a) Pre $n = 0$ daný vzťah zrejme platí (lebo $a^0 = 1$, $b^0 = 1$ a $1 \equiv 1 \pmod{m}$).

b) Ukážeme ďalej, že ak vzťah (5) platí pre $k$ ($k \in N$), tak platí aj pre $k+1$. Ak $a^k \equiv b^k \pmod{m}$ (čo je indukčný predpoklad), tak z (2) vyplýva, že $a^k \cdot a \equiv b^k \cdot b \pmod{m}$, t.j. $a^{k+1} \equiv b^{k+1} \pmod{m}$.

Vzťah (5) teda platí pre každé $n \in N$. □

Pravidlá pre počítanie s kongruenciami môžeme využiť napríklad aj pri určovaní zvyškov pri delení „veľkých“ čísel a pri niektorých tvrdeniach ich môžeme použiť namiesto dôkazu matematickou indukciou.

Pri riešení úloh budeme kongruencie často zapisovať do reťazca (podobne ako rovnosti) a príslušný modul zapíšeme až na koniec.

1.7 Príklad. Určte zvyšok pri delení čísla $255 \cdot 302 + 11^{17}$ číslom 4.

Riešenie. Pretože $255 \equiv 3 \pmod 4$ a $302 \equiv 2 \pmod 4$, tak (podľa (2)) $255 \cdot 302 \equiv 3 \cdot 2 \pmod 4$, z čoho na základe tranzitívnosti (lebo $3 \cdot 2 = 6 \equiv 2 \pmod 4$) dostávame $255 \cdot 302 \equiv 2 \pmod 4$.

Ďalej, $11^{17} \equiv 3^{17} \pmod 4$ (podľa (5)) a $3^{17} = 3^{2\cdot 8+1} = 3 \cdot 9^8 \equiv 3 \pmod 4$ (lebo $9^8 \equiv 1^8 \pmod 4$), teda $11^{17} \equiv 3 \pmod 4$.

Nakoniec (podľa (1)), $255 \cdot 302 + 11^{17} \equiv 2 + 3 \pmod 4$ a pretože $2 + 3 \equiv 1 \pmod 4$, tak $255 \cdot 302 + 11^{17} \equiv 1 \pmod 4$ čo znamená, že zvyšok čísla $255 \cdot 302 + 11^{17}$ pri delení číslom 4 je 1.

Ako sme už spomenuli, celé riešenie môžeme zapísať stručne pomocou reťazca kongruencií takto:

$$255 \cdot 302 + 11^{17} \equiv 3 \cdot 2 + 3^{17} \equiv 6 + 3^{2\cdot 8+1} \equiv 2 + 3 \cdot 9^8 \equiv 2 + 3 \cdot 1^8 \equiv 1 \pmod 4.$$

1.8 Príklad. Dokážte, že pre každé $n \in N^+$ platí: číslo 13 delí $3^{n+1} + 4^{2n-1}$.

Riešenie. Stačí ukázať, že $3^{n+1} + 4^{2n-1} \equiv 0 \pmod{13}$. Postupnými úpravami s využitím vlastností kongruencie dostávame:
$3^{n+1} + 4^{2n-1} \equiv 3^{n-1+2} + 4^{2(n-1)+1} \equiv 9 \cdot 3^{n-1} + 4 \cdot 16^{n-1} \equiv 9 \cdot 3^{n-1} + 4 \cdot 3^{n-1} \equiv 13 \cdot 3^{n-1} \equiv 0 \cdot 3^{n-1} \equiv 0 \pmod{13}$.

1.9 Príklad. Dokážte, že pre každé $n \in N^+$ platí: číslo 13 nedelí $3^n - 2$.

Riešenie. Pretože $3^3 \equiv 1 \pmod{13}$, je vhodné osobitne vyšetriť prípady keď $n$ je deliteľné číslom 3 (t.j. $n = 3k$), keď pri delení čísla $n$ tromi je zvyšok 1 (t.j. $n = 3k + 1$) a keď pri delení čísla $n$ tromi je zvyšok 2 (t.j. $n = 3k + 2$):

1. Ak $n = 3k$, tak $3^n - 2 \equiv 3^{3k} - 2 \equiv 1^k - 2 \equiv -1 \equiv 12 \pmod{13}$.
2. Ak $n = 3k + 1$, tak $3^n - 2 \equiv 3^{3k+1} - 2 \equiv 3 \cdot 1^k - 2 \equiv 1 \pmod{13}$.
3. Ak $n = 3k + 2$, tak $3^n - 2 \equiv 3^{3k+2} - 2 \equiv 9 \cdot 1^k - 2 \equiv 7 \pmod{13}$.

Pri delení $3^n - 2$ číslom 13 sú teda možné len zvyšky 12, 1, 7, čo znamená, že $13 \nmid 3^n - 2$.

Urobte dôkazy tvrdení z príkladov 1.8 a 1.9 matematickou indukciou a porovnajte obtiažnosť riešení. Pokúste sa vytvoriť analogické úlohy k predchádzajúcim príkladom.

Všimnime si ďalej, že zákon krátenia nenulovým číslom pre násobenie pri kongruenciách (na rozdiel od rovnosti) neplatí. Napríklad $2 \cdot 8 \equiv 2 \cdot 1 \pmod{14}$, ale $8 \not\equiv 1 \pmod{14}$. Ak však číslo, ktorým krátime a modul sú nesúdeliteľné čísla, tak krátenie je možné.

1.10 Veta. *Nech $a, b, c, m \in Z$, $m > 1$. Ak $a \cdot c \equiv b \cdot c \pmod m$ a $\mathrm{D}(m, c) = 1$, tak $a \equiv b \pmod m$.*

Dôkaz. Nech $a \cdot c \equiv b \cdot c \pmod m$ a $\mathrm{D}(m, c) = 1$. Potom $m \mid a \cdot c - b \cdot c$, t.j $m \mid (a - b) \cdot c$, z čoho vyplýva, že $m \mid a - b$, teda $a \equiv b \pmod m$. □

Na systéme zvyškových tried $\overline{Z}_m$ môžeme definovať (vzhľadom na vetu 1.5) operáciu sčítania $\oplus$ a operáciu násobenia $\odot$ takto:

$$a_m \oplus b_m = (a + b)_m, \qquad a_m \odot b_m = (a \cdot b)_m .$$

Súčet (súčin) dvoch tried teda nájdeme tak, že vyberieme (ľubovoľných) reprezentantov príslušných tried a nájdeme zvyškovú triedu do ktorej patrí súčet (súčin)

týchto reprezentantov. Z vety 1.5 vyplýva, že operácie $\oplus$, $\odot$ sú korektne definované, t.j., že dostávame ten istý výsledok bez ohľadu na výber reprezentantov.

Vlastnosti operácií sčítania a násobenia na množine zvyškových tried $\overline{Z}_m$ sú uvedené v nasledujúcej vete.

1.11 VETA. *Nech $\oplus$ a $\odot$ sú operácie sčítania a násobenia na systéme zvyškových tried $\overline{Z}_m$. Potom*

*a) obidve operácie sú komutatívne a asociatívne,*

*b) v $\overline{Z}_m$ existuje nulový prvok (t.j. neutrálny prvok operácie $\oplus$) a jednotkový prvok (t.j. neutrálny prvok operácie $\odot$),*

*c) ku každému prvku zo $\overline{Z}_m$ existuje opačný prvok (t.j. inverzný prvok vzhľadom na operáciu $\oplus$),*

*d) operácia $\odot$ je distributívna vzhľadom na operáciu $\oplus$.*

DÔKAZ. Uvedieme dôkaz asociatívnosti operácie $\oplus$. Nech $a_m, b_m, c_m \in \overline{Z}_m$. Potom

$$a_m \oplus (b_m \oplus c_m) = a_m \oplus (b+c)_m = (a+(b+c))_m =$$
$$=((a+b)+c)_m = (a+b)_m \oplus c_m = (a_m \oplus b_m) \oplus c_m,$$

čo znamená, že operácia $\oplus$ (na $\overline{Z}_m$) je asociatívna. □

Aj dôkazy ostatných vlastností operácií $\oplus$, $\odot$ sú jednoduché, využívajú sa pri nich vlastnosti operácií sčítania a násobenia celých čísel a čitateľ si ich môže urobiť ako cvičenie (cvičenie 6).

## Cvičenia

**1.** Nech $a = 352 \cdot 71 + 55^2 \cdot 86 + 15 \cdot 39$. Určte

a) paritu čísla $a$;

b) poslednú číslicu čísla $a$;

c) zvyšok po delení čísla $a$ číslom 7.

**2.** Dokážte, že:

a) číslo $2^{70} + 3^{70}$ je deliteľné číslom 13;

b) číslo $23^{25} + 25^{23}$ je deliteľné číslom 48.

**3.** Dokážte, že pre každé $n \in N$ je číslo $6^{n+1} + 13 \cdot 5^{2n}$ násobkom čísla 19.

**4.** Dokážte, že pre každé $n \in N$ platí: číslo 7 nedelí $3^n + 5^{3n+4}$.

**5.** Dokážte, že pre každé $n \in N^+$ platí: číslo 31 delí $5^{n+1} + 6^{2n-1}$.

**6.** Podrobne dokážte vetu 1.11.

**7.** Určte nulový prvok, jednotkový prvok a zistite ku ktorým prvkom existujú inverzné prvky vzhľadom na operácie $\oplus$, $\odot$ v

a) $\overline{Z}_6$, b) $\overline{Z}_5$, c) $\overline{Z}_{14}$, d) $\overline{Z}_{17}$.

## 2. Základné poznatky o grupoidoch

Predmetom algebry bolo pôvodne skúmanie problémov súvisiacich s riešením (algebraických) rovníc. Vieme, že *rovnica* (napríklad s jednou neznámou $x$) je istý typ výrokovej formy $\mathcal{V}(x)$, ktorá má tvar $L(x) = P(x)$, kde $L(x)$, $P(x)$ sú výrazy (termy) s premennou $x$, pričom najviac jeden je konštantou. Pod *riešením* rovnice $\mathcal{V}(x)$ rozumieme určenie všetkých jej koreňov (t.j. určenie jej oboru pravdivosti $\mathcal{P}$) buď vymenovaním prvkov alebo pomocou množinových operácií s intervalmi, resp. konečnými množinami. Ak je definičný obor rovnice (výrokovej formy $\mathcal{V}(x)$) konečná množina $A$, je možné vyriešiť ju tak, že pre každý prvok $a \in A$ sa overí, či je $\mathcal{V}(a)$ pravdivý výrok. Obor pravdivosti $\mathcal{P}$ potom určíme vymenovaním prvkov. Tento spôsob riešenia nazveme *dosadzovacia metóda*.

2.1 Príklad. V $\overline{Z}_{10}$ riešte rovnicu: a) $\overline{4} \oplus x = \overline{2}$, b) $\overline{4} \odot x = \overline{2}$.

Riešenie. a) Dosadzovacou metódou zistíme, že koreňom danej rovnice je prvok (trieda) $\overline{8}$. K tomuto výsledku môžeme dospieť aj takým spôsobom, že k obidvom stranám rovnice pripočítame prvok $\overline{6}$ a postupne dostávame:

$$\overline{6} \oplus (\overline{4} \oplus x) = \overline{6} \oplus \overline{2}, \quad (\overline{6} \oplus \overline{4}) \oplus x = \overline{8}, \quad \overline{0} \oplus x = \overline{8}, \quad x = \overline{8}.$$

b) Dosadzovacou metódou zistíme, že koreňmi sú prvky $\overline{3}$ a $\overline{8}$. V tomto prípade analogický postup (úpravy) ako v časti a) nemôžeme použiť (prečo ?).

To, či daná rovnica má riešenie, koľko má riešení a či existuje nejaký postup (napr. ekvivalentné úpravy), pomocou ktorého dané korene nájdeme, závisí ako od množiny, v ktorej rovnicu riešime tak aj od vlastností operácií, ktoré sa v zápise rovnice nachádzajú.

Aj to je jeden z dôvodov, prečo sa skúmajú (študujú) množiny spolu s operáciami.

Ak množina $A$ je neprázdna a $*_1, \ldots, *_n$ sú (binárne) operácie na $A$, tak usporiadanú $(n+1)$-ticu $(A, *_1, \ldots, *_n)$ nazývame *(binárnou) algebrou* (alebo *algebraickou štruktúrou*). Množinu $A$ nazývame *nosičom* danej algebry. O operáciách $*_1, \ldots, *_n$ hovoríme, že sú operáciami danej algebry.

V tejto časti sa budeme zaoberať algebrami s jednou operáciou.

2.2 Definícia. Algebru $(A, *)$ s jednou binárnou operáciou nazývame grupoid.

Ak operácia $*$ je komutatívna (asociatívna), tak hovoríme, že grupoid $(A, *)$ je komutatívny (asociatívny). Neutrálny prvok operácie $*$ (ak existuje) voláme neutrálny prvok grupoidu $(A, *)$. Ak $(A, *)$ je grupoid, tak niekedy hovoríme, že $A$ (spolu) s operáciou $*$ je grupoid. Často namiesto $(A, *)$ píšeme len $A$ a hovoríme o grupoide $A$.

2.3 Príklad. Algebry $(N, +)$, $(\mathcal{P}(A), \cap)$, $(Z^-, +)$, $(Z, -)$, $(\overline{Z}_n, \oplus)$, $(\overline{Z}_n, \odot)$ sú grupoidy.

Z daných grupoidov môžeme zostrojiť nový grupoid pomocou tzv. priameho súčinu.

Ak $(G, \circ)$ a $(H, \triangle)$ sú grupoidy, tak na karteziánskom súčine $G \times H$ môžeme definovať operáciu $*$ takto:

$$(a, b) * (c, d) = (a \circ c, b \triangle d). \tag{1}$$

2.4 Definícia. Nech $(G, \circ)$ a $(H, \triangle)$ sú grupoidy. Grupoid $(G \times H, *)$, ktorého operácia $*$ je daná rovnosťou (1), nazývame priamy súčin grupoidu $(G, \circ)$ a grupoidu $(H, \triangle)$ (v uvedenom poradí).

Vlastnosti priameho súčinu grupoidov závisia v podstatnej miere od vlastností grupoidov, z ktorých je skonštruovaný.

2.5 Veta. *Nech $(G, \circ)$ a $(H, \triangle)$ sú grupoidy a $(G \times H, *)$ ich priamy súčin. Potom*

*a) ak operácie $\circ$, $\triangle$ sú komutatívne (asociatívne), tak aj operácia $*$ je komutatívna (asociatívna),*

*b) ak $e_1$ je neutrálny prvok grupoidu $G$ a $e_2$ neutrálny prvok grupoidu $H$, tak $(e_1, e_2)$ je neutrálny prvok grupoidu $G \times H$,*

*c) ak k prvku $a \in G$ existuje inverzný prvok $b \in G$ (vzhľadom na operáciu $\circ$) a ak k prvku $c \in H$ existuje inverzný prvok $d \in H$ (vzhľadom na operáciu $\triangle$), tak prvok $(b, d) \in G \times H$ je inverzný k prvku $(a, c) \in G \times H$ (vzhľadom na operáciu $*$).*

Dôkaz tohto tvrdenia je jednoduchý, podrobne si ho zapíšte (cvičenie 1).

2.6 Príklad. Dané sú grupoidy $(\mathcal{P}(\{1\}), \cap)$ a $(\overline{Z}_2, \oplus)$. Ich priamym súčinom je grupoid, ktorého nosičom je množina $\{(\emptyset, \overline{0}), (\emptyset, \overline{1}), (\{1\}, \overline{0}), (\{1\}, \overline{1})\}$ a operácia $*$ je daná rovnosťou: $(X, x) * (Y, y) = (X \cap Y, x \oplus y)$. Operácia $*$ je komutatívna a asociatívna, jej neutrálnym prvkom je $(\{1\}, \overline{0})$. Napíšte operačnú tabuľku operácie $*$.

Definíciu a vlastnosti priameho súčinu grupoidov je možné zovšeobecniť pre ľubovoľný počet gropoidov. Nájdite napríklad priamy súčin grupoidov $(\overline{Z}_2, \oplus)$, $(\mathcal{P}(\{1\}), \cup)$, $(\overline{Z}_3, \odot)$.

Ak $(G, *)$ je grupoid a $A$, $B$ neprázdne podmnožiny množiny $G$, tak množinu $\{x * y \mid x \in A \ \& \ y \in B\}$ budeme označovať $A * B$. V prípade, že jedna z množín je jednoprvková, napr. $A = \{a\}$, tak namiesto $\{a\} * B$ píšeme $a * B$. Všimnime si, že napr. množina $3 \cdot N = \{3 \cdot x \mid x \in N\}$ (t.j. množina všetkých prirodzených násobkov čísla 3) je spolu s operáciou obvyklého sčítania grupoidom (lebo ak $a$, $b \in 3 \cdot N$, t.j. $a = 3k$, $b = 3l$, $k, l \in N$, tak aj $a + b = 3(k + l) \in 3 \cdot N$). Pretože $3 \cdot N \subseteq N$, je grupoid $(3 \cdot N, +)$ v istom zmysle „časťou“ grupoidu $(N, +)$.

2.7 Definícia. Nech $(A, *)$ je grupoid. Ak neprázdna podmnožina $B$ množiny $A$ spolu so zúžením operácie $*$ na množinu $B$ je grupoidom, t.j. ak platí

$$\forall\, a, b \in B;\ a * b \in B$$

tak hovoríme, že $(B, *)$ (alebo stručne $B$) je podgrupoid grupoidu $(A, *)$.

V predchádzajúcej definícii sme operáciu na $A$ aj jej zúženie na $B$ označili rovnako, tak ako sa to obvykle v matematike robí.

Ak nejaká vlastnosť platí pre všetky prvky nejakej množiny, tak zrejme platí aj pre všetky prvky jej ľubovoľnej podmnožiny. Z toho a z definícií komutatívnosti, asociatívnosti a neutrálneho prvku bezprostredne vyplýva nasledujúce tvrdenie.

2.8 Veta. *Ak je grupoid komutatívny (asociatívny), tak je komutatívny (asociatívny) aj každý jeho podgrupoid. Ak grupoid má neutrálny prvok, tak tento je neutrálnym prvkom každého jeho podgrupoidu, ktorý ho obsahuje.*

2.9 Lema. *Nech $(A, *)$ je grupoid a nech $\{(B_j, *) \mid j \in J\}$ je systém jeho podgrupoidov. Ak $B = \bigcap_{j \in J} B_j \neq \emptyset$, tak aj $(B, *)$ je podgrupoid grupoidu $(A, *)$.*

Dôkaz. Nech $a, b \in B = \bigcap_{j \in J} B_j$. Potom pre každé $j \in J$ je $a, b \in B_j$ a teda aj $a * b \in B_j$, čo znamená, že $a * b \in B$. □

Neprázdny prienik ľubovoľného systému podgrupoidov je teda opäť podgrupoid.

Ak $(A, *)$ je grupoid a neprázdna podmnožina $M \subseteq A$ netvorí jeho podgrupoid, t.j existujú prvky $a$, $b \in M$, že $a * b \notin M$, bude nás zaujímať najmenší podgrupoid grupoidu $A$ obsahujúci množinu $M$.

2.10 Veta. *Nech $(A, *)$ je grupoid a nech $M$ je neprázdna podmnožina množiny $A$. Potom existuje práve jeden podgrupoid $[M]$ grupoidu $(A, *)$, o ktorom platí*

a) $M \subseteq [M]$,
b) *ak $H$ je ľubovoľný podgrupoid grupoidu $A$, ktorý obsahuje množinu $M$, tak $[M] \subseteq H$.*

*Existuje teda práve jeden najmenší podgrupoid grupoidu $A$ obsahujúci množinu $M$ (vzhľadom na usporiadanie množiny $\mathcal{P}(A)$ inklúziou).*

Dôkaz. Nech $\{(B_j, *) \mid j \in J\}$ je systém všetkých podgrupoidov grupoidu $(A, *)$, ktoré obsahujú množinu $M$. Z lemy 2.9 vyplýva, že $B = \bigcap_{j \in J} B_j$ je podgrupoid grupoidu $A$, pričom $M \subseteq B$ (lebo $M \subseteq B_j$ pre každé $j \in J$). Ukážeme, že $B = [M]$. Vieme už, že podmienka a) je splnená. Overíme aj splnenie podmienky b). Nech $H$ je ľubovoľný podgrupoid grupoidu $A$ obsahujúci množinu $M$. Potom existuje $i \in J$, že $H = B_i$ (lebo do systému $\{(B_j, *) \mid j \in J\}$ patria všetky podgrupoidy grupoidu $A$ obsahujúce množinu $M$) a teda $B = \bigcap_{j \in J} B_j \subseteq B_i = H$. Treba ešte ukázať, že podgrupoid $[M]$ je určený jednoznačne. Predpokladajme, že aj $[M]'$ je podgrupoid grupoidu $A$ spĺňajúci a) aj b). Potom $[M] \subseteq [M]'$ (lebo $[M]$ spĺňa podmienku b)) aj $[M]' \subseteq [M]$ (lebo aj $[M]'$ spĺňa podmienku b)), teda $[M] = [M]'$. □

2.11 Definícia. Nech $(A, *)$ je grupoid a nech $M$ je neprázdna podmnožina množiny $A$. Najmenší podgrupoid $[M]$ grupoidu $(A, *)$ obsahujúci množinu $M$ budeme nazývať podgrupoid generovaný množinou $M$.

V prípade, že množina $M$ je konečná, napr. $M = \{a_1, a_2, \ldots, a_n\}$, namiesto označenia $[\{a_1, a_2, \ldots, a_n\}]$ používame označenie $[a_1, a_2, \ldots, a_n]$.

2.12 Príklad. Dokážte, že nosič podgrupoidu grupoidu $(N, +)$, ktorý je generovaný prvkom 3 je množina $3 \cdot N^+$, t.j., že $[3] = 3 \cdot N^+$.

Riešenie. a) Množina $3 \cdot N^+$ tvorí podgrupoid grupoidu $(N, +)$ a zrejme obsahuje množinu $\{3\}$ (lebo $3 = 3 \cdot 1$). Podgrupoid $[3]$ je ale zo všetkých podgrupoidov, ktoré obsahujú množinu $\{3\}$ najmenší a tak $[3] \subseteq 3 \cdot N^+$.

b) Pretože $3 \in [3]$, tak aj $3 + 3 = 2 \cdot 3 \in [3]$, aj $6 + 3 = 3 \cdot 3 \in [3]$, atď., čiže každý prvok množiny $3 \cdot N^+$ je aj prvkom množiny $[3]$, čo znamená, že $3 \cdot N^+ \subseteq [3]$ (podrobný dôkaz sa urobí matematickou indukciou; zapíšte ho).

Z a) a b) vyplýva, že $[3] = 3 \cdot N^+$.

Dôležitou algebraickou úpravou (ktorá sa využíva napr. pri riešení rovníc) je tzv. krátenie. Pre ľubovoľné reálne čísla $a$, $b$, $c$ platí: ak $a+b=a+c$, tak $b=c$. V $Z_{15}$ ale napríklad $\overline{3}\odot\overline{2}=\overline{3}\odot\overline{7}$, ale $\overline{2}\neq\overline{7}$. Podobne, pre množiny $A=\{1,2\}$, $B=\{1,3\}$, $C=\{1,4\}$ platí, že $A\cap B=A\cap C$, ale $B\neq C$.

2.13 Definícia. Nech $(A,*)$ je grupoid. Ak pre ľubovoľné prvky $a,b,c\in A$ platí

$$a*b=a*c \implies b=c, \tag{2}$$

$$b*a=c*a \implies b=c, \tag{3}$$

hovoríme, že v grupoide $(A,*)$ platia zákony o krátení.

Ak platí (2) hovoríme, že platí ľavý zákon o krátení, ak platí (3) hovoríme, že platí pravý zákon o krátení.

Ak je operácia grupoidu daná operačnou tabuľkou a ak platí ľavý zákon o krátení, tak sa zrejme v žiadnom riadku poľa tabuľky výskyt žiadneho prvku nezopakuje a ak platí pravý zákon o krátení tak platí analogické tvrdenie pre stĺpce.

Operácia grupoidu $A$ musí spĺňať len požiadavku, aby bola definovaná pre každú dvojicu prvkov z $A$. Ak má operácia grupoidu aj niektoré ďalšie vlastnosti (napr. asociatívnosť, existencia neutrálneho prvku, atď.) dostávame špeciálnejšie štruktúry, s ktorými sa v algebre často pracuje.

2.14 Definícia. Grupoid, ktorého operácia je asociatívna, nazývame pologrupa. Ak má naviac pologrupa neutrálny prvok, nazývame ju monoid. ∎

2.15 Príklad. Nech $M$ je neprázdna množina a nech $M^M$ je systém všetkých zobrazení $M\to M$. Ak $f,g\in M^M$, tak aj $f\circ g\in M^M$, t.j. $(M^M,\circ)$ je grupoid. Skladanie zobrazení je asociatívna operácia, preto grupoid $(M^M,\circ)$ je pologrupou. Naviac, pre ľubovoľné zobrazenie $f\in M^M$ a pre identické zobrazenie $\mathrm{id}_M$ platí $f\circ\mathrm{id}_M=\mathrm{id}_M\circ f=f$, t.j. identické zobrazenie $\mathrm{id}_M\in M^M$ je neutrálny prvok pologrupy $(M^M,\circ)$. Pologrupa $(M^M,\circ)$ je teda monoidom.

2.16 Definícia. Monoid, v ktorom ku každému prvku existuje inverzný prvok sa nazýva grupa.

Grupoid $(G,*)$ je teda grupou, ak

1. $\forall\, a,b,c\in G;\ (a*b)*c=a*(b*c)$,
2. $\exists e\in G\,\forall a\in G;\ a*e=e*a=a$,
3. $\forall a\in G\,\exists a'\in G;\ a*a'=a'*a=e$.

Ak operácia $*$ grupy $(G,*)$ je komutatívna hovoríme, že grupa $G$ je *komutatívna* alebo *Abelova*.

Poznámka. Pretože binárna operácia môže mať najviac jeden neutrálny prvok (pozri napr. vetu 12.1 v [6]) je neutrálny prvok grupy určený jednoznačne a pretože operácia grupy je asociatívna, existuje ku každému prvku grupy jediný inverzný prvok (pozri vetu 12.2 v [6]).

2.17 Príklad. Grupami sú napríklad nasledujúce štruktúry: $(R,+)$, $(Q,+)$, $(Z,+)$, $(\overline{Z}_n,\oplus)$, $(R^+,\cdot)$, $(Q^+,\cdot)$, $(R\setminus\{0\},\cdot)$, $(Q\setminus\{0\},\cdot)$, $(\{1,-1,i,-i\},\cdot)$, $(\{-1,1\},\cdot)$.

Grupy sa v súvislosti s riešením algebraických rovníc skúmali už v 19. storočí. V ďalších kapitolách sa budeme skúmaniu grúp venovať podrobnejšie a systematickejšie, teraz uvedieme len niekoľko najzákladnejších pojmov a poznatkov.

Bijektívne zobrazenie množiny $A$ na množinu $A$ nazývame *transformáciou* množiny $A$. Množinu všetkých transformácií množiny $A$ označujeme $T(A)$. Transformáciu konečnej množiny nazývame *permutácia*. Transformáciu (permutáciu) $\{(1, a_1), (2, a_2), \ldots, (n, a_n)\}$ konečnej množiny $\boldsymbol{n} = \{1, 2, \ldots, n\}$ zapisujeme takto: $\begin{pmatrix} 1 & 2 & \ldots n \\ a_1 & a_2 & \ldots a_n \end{pmatrix}$.

2.18 Príklad. Súčin (zloženie) dvoch transformácií množiny $A$ je opäť transformácia množiny $A$, operácia skladania zobrazení (a teda aj transformácií) je asociatívna, identické zobrazenie $\mathrm{id}_A$ je transformácia množiny $A$ a inverzné zobrazenie k transformácii množiny $A$ je opäť transformácia množiny $A$. Z toho vyplýva, že $(T(A), \circ)$ je grupa; voláme ju grupa všetkých transformácií množiny $A$.

Grupa permutácií množiny $\boldsymbol{n} = \{1, 2, \ldots, n\}$ sa nazýva *symetrická grupa stupňa* $n$ a označuje sa $S_n$. Počet jej prvkov je $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$, lebo pre výber obrazu prvku 1 je $n$ možností, pre výber obrazu prvku 2 je potom už len $(n-1)$ možností, atď. Napíšte operačnú tabuľku grupy $S_3$ (cvičenie 7).

2.19 Príklad. Symetrický rozdiel množín $\triangle$ je operáciou na systéme $\mathcal{P}(A)$ všetkých podmnožín množiny $A$. Táto operácia je asociatívna a komutatívna (pozri napr. vetu 6.6 v [6]). Prázdna množina je neutrálnym prvkom a ku každej množine $X \in \mathcal{P}(A)$ je inverzným prvkom tá istá množina $X$ ($X \triangle X = \emptyset$). To znamená, že $(\mathcal{P}(A), \triangle)$ je komutatívna grupa. Napíšte operačnú tabuľku grupy $(\mathcal{P}(\{1, 2\}), \triangle)$.

Poznámka. Vo všeobecných úvahách označujeme často operáciu grupy *multiplikatívne* „$\cdot$“ a od toho sa odvíja aj názov a označenie inverzného prvku k prvku $a$ – *prevrátený* prvok „$a^{-1}$“ (neutrálny prvok označujeme zvyčajne písmenom $e$).

Pri komutatívnych grupách sa operácia niekedy označuje *aditívne* „$+$“, neutrálny prvok sa nazýva *nulovým* prvkom (označenie „0“) a inverzný prvok k $a$ sa nazýva *opačným* prvkom (označenie „$-a$“).

2.20 Veta. *V každej grupe $(G, \cdot)$ platia zákony o krátení.*

Dôkaz. Nech $a, b, c \in G$ a nech $a \cdot b = a \cdot c$. K prvku $a$ existuje inverzný prvok $a^{-1}$. Z rovnosti $a \cdot b = a \cdot c$ potom (po vynásobení rovnosti prvkom $a^{-1}$ zľava) postupne dostávame: $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$, $(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$, $e \cdot b = e \cdot c$, $b = c$. Analogicky sa ukáže platnosť pravého zákona o krátení. □

2.21 Veta. *Nech $(G, \cdot)$ je grupa. Potom pre ľubovoľné prvky $a, b \in G$ platí:*

*a)* $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$,

*b)* $(a^{-1})^{-1} = a$.

Dôkaz. a) Ukážeme, že prvok $b^{-1} \cdot a^{-1}$ je inverzným prvkom k prvku $a \cdot b$. Pretože $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$ (a analogicky sa ukáže, že $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$), tak prvok $b^{-1} \cdot a^{-1}$ je inverzným prvkom k prvku $a \cdot b$. Keďže inverzný prvok je v grupe určený jednoznačne, tak $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

b) Pretože $a \cdot a^{-1} = a^{-1} \cdot a = e$, tak prvok $a$ je inverzný k prvku $a^{-1}$ a teda $(a^{-1})^{-1} = a$. □

2.22 Definícia. Ak je podgrupoid grupy $G$ grupou, nazývame ho podgrupou grupy $G$.

*Triviálnymi podgrupami* grupy $G$ nazývame jej podgrupy $G$ a $\{e\}$, kde $e$ je neutrálny prvok grupy $G$.

2.23 Príklad. Grupa $(\overline{Z}_6, \oplus)$ má, okrem triviálnych podgrúp, len nasledovné podgrupy: $\{\overline{0}, \overline{3}\}$, $\{\overline{0}, \overline{2}, \overline{4}\}$ (Presvedčte sa o tom podrobne pomocou operačnej tabuľky).

Nasledujúca veta je *kritériom* (obsahuje nutnú a postačujúcu podmienku), kedy je podmnožina grupy jej podgrupou.

2.24 Veta. *Nech $H$ je neprázdna podmnožina grupy $G$. $H$ je podgrupou grupy $G$ práve vtedy, keď platí:*

$$\forall\, a, b \in H;\ a \cdot b^{-1} \in H. \tag{4}$$

Dôkaz. Ak $H$ je podgrupou grupy $G$, tak podmienka (4) zrejme platí. Obrátene, nech platí podmienka (4). Pretože množina $H$ je neprázdna, patrí do nej aspoň jeden prvok $a$. Potom ale do $H$ patrí aj prvok $a \cdot a^{-1} = e$. Pre každý prvok $b \in H$ patrí do $H$ aj prvok (vieme už, že $e \in H$) $e \cdot b^{-1} = b^{-1}$. Teraz už stačí ukázať (vzhľadom na vetu 2.8), že $H$ je podgrupoid grupy $G$. Ak $a, b \in H$, tak aj $a, b^{-1} \in H$ a teda $a \cdot (b^{-1})^{-1} = a \cdot b \in H$. □

2.25 Príklad. Ukážte, že množina $5 \cdot Z = \{5 \cdot x \mid x \in Z\}$ je podgrupou grupy $(Z, +)$.

Riešenie. Ak $a, b \in 5 \cdot Z$, tak $a = 5x$, $b = 5y$, $x, y \in Z$. Potom $a + (-b) = 5x + (-5y) = 5(x - y) \in 5 \cdot Z$, lebo $x - y \in Z$.

2.26 Veta. *Nech $(G, \cdot)$ je grupa a nech $\{H_j \mid j \in J\}$ je systém jej podgrúp. Ak $H = \bigcap_{j \in J} H_j$, tak $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$.*

Dôkaz. Pretože pre každé $j \in J$ je $e \in H_j$, tak $\bigcap_{j \in J} H_j \neq \emptyset$. Nech $a, b \in \bigcap_{j \in J} H_j$. Potom pre každé $j \in J$ je $a, b \in H_j$, teda (lebo $H_j$ je grupa) $a \cdot b^{-1} \in H_j$ z čoho vyplýva, že $a \cdot b^{-1} \in \bigcap_{j \in J} H_j$. To znamená, že $\bigcap_{j \in J} H_j$ je nosič podgrupy. □

Analogicky, ako je pre grupoidy zavedený pojem podgrupoidu generovaného množinou, je možné zaviesť aj pojem podgrupy generovanej danou množinou. Používame aj analogické názvy a označenia.

2.27 Príklad. Dokážte, že nosič podgrupy grupy $(Z, +)$, ktorá je generovaná množinou $\{10, 15\}$ je množina $5Z = \{5n \mid n \in Z\}$ (t.j., že $[10, 15] = 5Z$).

Riešenie. a) Množina $5Z$ je podgrupa grupy $(Z, +)$ (pozri príklad 2.25). Zrejme $\{10, 15\} \subseteq 5Z$ a pretože podgrupa $[10, 15]$ je zo všetkých podgrúp, ktoré obsahujú prvky 10, 15 najmenšia (vzhľadom na inklúziu), tak $[10, 15] \subseteq 5Z$.

b) Zrejme $0, 5, -5 \in [10, 15]$ lebo $[10, 15]$ je grupa a $0 = 10 + (-10)$, $5 = 15 + (-10)$, $-5 = -15 + 10$. Nech $x \in 5Z$. Potom $x = 5n$, $n \in Z$.

1. Ak $n = 0$, tak $x = 0 \in [10, 15]$.

2. Ak $n > 0$, tak $x = 5 + 5 + \cdots + 5$ ($n$-krát) a pretože $5 \in [10, 15]$, tak aj $x \in [10, 15]$.

3. Ak $n < 0$, tak $x = 5n = (-5) \cdot (-n) = (-5) + (-5) + \cdots + (-5)$ ($-n$-krát, $-n \in Z^+$) a pretože $-5 \in [10, 15]$, tak aj $x \in [10, 15]$.

Teda aj $5Z \subseteq [10, 15]$, čo spolu s časťou a) znamená, že $[10, 15] = 5Z$.

Vieme už, že pri riešení rovníc s použitím istých úprav musíme byť opatrní. Ani „vynásobenie“ obidvoch strán rovnice tým istým prvkom nemusí byť ekvivalentnou úpravou. Napríklad v $\overline{Z}_8$ má rovnica $\overline{5} \odot x = \overline{3}$ jediný koreň $\overline{7}$, ale po vynásobení obidvoch strán prvkom $\overline{2}$ dostávame rovnicu $\overline{2} \odot x = \overline{6}$, ktorej koreňom je okrem prvku $\overline{7}$ aj prvok $\overline{3}$. V tomto prípade (pretože v monoide $(\overline{Z}_8, \odot)$ neplatí zákon o krátení) horeuvedené rovnice nie sú ekvivalentné (t.j nemajú rovnakú množinu riešení).

2.28 Veta. *V grupe $(G, \cdot)$ má každá rovnica $a \cdot x = b$, $y \cdot a = b$, kde $a, b \in G$ a $x, y$ sú neznáme, jediné riešenie (t.j. pre každé dva prvky $a, b \in G$ existuje jediný prvok $x_0 \in G$ a jediný prvok $y_0 \in G$, že $a \cdot x_0 = b$, $y_0 \cdot a = b$).*

Dôkaz. Zrejme prvok $a^{-1} \cdot b$ je riešením rovnice $a \cdot x = b$. Predpokladajme, že $x_1$ aj $x_2$ sú riešenia rovnice $a \cdot x = b$. Potom $a \cdot x_1 = b$ aj $a \cdot x_2 = b$, z čoho dostávame $a \cdot x_1 = a \cdot x_2$ a po krátení $x_1 = x_2$. Existencia jediného riešenia rovnice $y \cdot a = b$ sa ukáže analogicky. □

Ak grupa $(G, \cdot)$ je komutatívna, tak samozrejme obidve rovnice z predchádzajúcej vety majú to isté riešenie (sú ekvivalentné).

2.29 Príklad. V $S_6$ riešte rovnice

(a) $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 2 & 3 \end{pmatrix} \circ X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 2 & 4 \end{pmatrix},$$

(b) $$Y \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 2 & 4 \end{pmatrix}.$$

Riešenie. Inverznou permutáciou k permutácii $\left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 5&1&4&6&2&3 \end{smallmatrix}\right)$ je permutácia $\left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 2&5&6&3&1&4 \end{smallmatrix}\right)$. Z dôkazu predchádzajúcej vety potom vyplýva, že riešením rovnice (a) je permutácia

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix}$$

a riešením rovnice (b) je permutácia

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}.$$

V obidvoch prípadoch urobte skúšku.

## Cvičenia

**1.** Podrobne dokážte vetu 2.5.

**2.** Dané sú grupoidy $(Z_3, +)$, $(\mathcal{P}(\{a\}), \cap)$, . Nájdite grupoid, ktorý je ich priamym súčinom a určte jeho vlastnosti.

**3.** Na množine $N$ je daná operácia $\oplus$ takto:

$$a_n \dots a_1 a_0 \oplus b_m \dots b_1 b_0 = a_n + \dots + a_1 + a_0 + b_m + \dots + b_1 + b_0$$

(t.j. súčtom dvoch čísel je obvyklý súčet ich ciferných súčtov). Zistite, či v grupoide $(N, \oplus)$ platia zákony o krátení a určte nosič podgrupoidu generovaného množinou a) $\{9\}$, b) $\{3\}$, c) $\{1, 2, \dots, 10\}$.

**4.** Na množine $Q$ je daná operácia $*$ takto:

$$a * b = ab - \frac{3}{2}a - \frac{3}{2}b + \frac{15}{4}.$$

Zistite, či grupoid $(Q, *)$ je grupou.

**5.** Nech $A = \{1, 2\}$. Napíšte operačnú tabuľku operácie grupoidu $(A^A, \circ)$ a určte jeho vlastnosti.

**6.** Nech $K_3$ je množina všetkých tretích (komplexných) odmocnín z čísla 1, t.j. $K_3 = \left\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right\}$. Ukážte, že $(K_3, \cdot)$ je grupa.

**7.** Napíšte operačnú tabuľku symetrickej grupy stupňa 3.

**8.** Na množine $Z \times (Z \setminus \{0\})$ je daná operácia $\oplus$ takto: $(a, b) \oplus (c, d) = (ad + bc, bd)$. Zistite, či $(Z \times (Z \setminus \{0\}, \oplus)$ je grupa.

**9.** Na množine $R \setminus \{0, 1\}$ definujeme funkcie takto:
$f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{x}{x-1}$, $f_5(x) = \frac{x-1}{x}$, $f_6(x) = \frac{1}{1-x}$.
a) Napíšte tabuľku pre operáciu $\circ$ na množine $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.
b) Ukážte, že $(G, \circ)$ je grupa.

**10.** Na množine $M_{2,2}(C)$ všetkých matíc typu $2 \times 2$ nad $C$ (t.j. na množine $M_{2,2}(C) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in C\right\}$) je dané sčítanie takto: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} u & v \\ w & t \end{pmatrix} = \begin{pmatrix} a+u & b+v \\ c+w & d+t \end{pmatrix}$. Ukážte, že $(M_{2,2}(C), \oplus)$ je grupa; voláme ju aditívna grupa (komplexných) štvorcových matíc typu $2 \times 2$.

**11.** Nech $(M_{2,2}(C), +)$ je aditívna grupa matíc typu $2 \times 2$. Zistite, či nasledujúce podmnožiny množiny $M_{2,2}(C)$ sú nosiče podgrúp grupy $(M_{2,2}(C), +)$.

a) $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in R\right\}$, b) $\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R\right\}$,

c) $\left\{\begin{pmatrix} a & b \\ 1 & c \end{pmatrix} \mid a, b, c \in R\right\}$, d) $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0\right\}$.

**12.** Na množine $M_{2,2}(C)$ všetkých matíc typu $2 \times 2$ nad $C$ je dané násobenie takto: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} u & v \\ w & t \end{pmatrix} = \begin{pmatrix} au+bw & av+bt \\ cu+dw & cv+dt \end{pmatrix}$. Nech

$$M^* = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in C,\ ad - bc \neq 0\right\}$$

Ukážte, že $(M^*, \cdot)$ je grupa; voláme ju multiplikatívna grupa (komplexných) regulárnych matíc typu $2 \times 2$.

**13.** Nech $(M^*, \cdot)$ je multiplikatívna grupa regulárnych matíc typu $2 \times 2$. Zistite, či nasledujúce množiny sú nosiče podgrúp grupy $(M^*, \cdot)$.

a) $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b \in R, a \neq 0 \vee b \neq 0\right\}$, b) $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1\right\}$,
c) $\left\{\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \mid a,b,c \in R, b \neq 0 \wedge c \neq 0\right\}$,

**14.** Na systéme všetkých reálnych funkcií $R^R$ definujeme sčítanie takto: $f \oplus g = h$ ak $f(x) + g(x) = h(x)$ pre každé číslo $x \in R$.

a) Ukážte, že $(R^R, \oplus)$ je Abelova grupa

b) Zistite, či $H$ je jej podgrupa v nasledujúcich prípadoch

$H = \{f \in R^R \mid f(1) = 0\}$,
$H = \{f \in R^R \mid f \text{ je rastúca}\}$,
$H = \{f \in R^R \mid f \text{ je párna}\}$.

**15.** Určte podgrupu grupy $(\overline{Z}_{12}, \oplus)$, generovanú množinou
a) $\{\overline{9}\}$ b) $\{\overline{6}\}$, c) $\{\overline{6}, \overline{9}\}$ d) $\{\overline{2}, \overline{9}\}$ e) $\{\overline{11}\}$, f) $\{\overline{4}, \overline{6}, \overline{8}\}$.

**16.** Určte podgrupu grupy $(Z, +)$, generovanú množinou
a) $\{8, 10, 12\}$, b) $\{7, 8\}$, c) $\{-1\}$, d) $N$, e) $\{30, 33, 42, 45\}$, f) $\{0\}$.

**17.** Určte podgrupu grupy $(Q \setminus \{0\}, \cdot)$ generovanú množinou
a) $\{2\}$, b) $N$.

**18.** Určte podgrupu grupy $(S_3, \circ)$, generovanú množinou
a) $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$, b) $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$.

**19.** Určte podgrupu multiplikatívnej grupy regulárnych matíc typu $2 \times 2$, generovanú množinou
a) $\left\{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$, b) $\left\{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right\}$.

**20.** V $\overline{Z}_{72}$ riešte rovnicu
a) $\overline{52} \oplus x = \overline{43}$, b) $\overline{18} \odot x = \overline{54}$, c) $\overline{35} \odot x = \overline{16}$.

**21.** Rovnicu $\overline{6} \cdot x \oplus \overline{5} = \overline{3}$ riešte a) v $\overline{Z}_{10}$, b) v $\overline{Z}_{41}$.

**22.** V $\mathcal{P}(\{1, 2, 3, 4, 5, 6, 7, 8\})$ riešte rovnicu
a) $\{1, 3, 4, 7, 8\} \cap X = \{3, 7, 8\}$, b) $\{2, 5, 6, 7\} \triangle X = \{1, 3, 5, 7, 8\}$
c) $\{1, 2, 3, 4\} \cup X = \{1, 2, 3, 4, 8\}$.

**23.** V množine $M$ všetkých štvorcových matíc typu $2 \times 2$ nad $C$ riešte rovnicu
a) $\begin{pmatrix} 2 & 1 \\ -3 & 1 \end{pmatrix} \cdot X = \begin{pmatrix} 4 & 3 \\ -1 & -7 \end{pmatrix}$, b) $X \cdot \begin{pmatrix} 2 & 1 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ -1 & -7 \end{pmatrix}$,
c) $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot X = \begin{pmatrix} 3 & 2 \\ 6 & 4 \end{pmatrix}$

**24.** V $S_5$ riešte rovnice

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \circ X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$, b) $Y \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$.

## 3. Izomorfizmus grupoidov

Pri riešení konštrukčných úloh v geometrii je po diskusii častá odpoveď, že daná úloha má jediné riešenie. Znamená to, že všetky geometrické útvary zostrojené pomocou nájdenej a popísanej konštrukcie sú zhodné.

Ak vieme, že napríklad dva trojuholníky sú zhodné (t.j. existuje zhodné zobrazenie, v ktorom sa jeden trojuholník zobrazí na druhý) a poznáme vlastnosti niektorého z nich, poznáme už aj vlastnosti toho druhého (sú také isté).

Podobnú úlohu má pri skúmaní algebraických štruktúr izomorfizmus. V algebre zvyčajne nebudeme rozlišovať algebraické štruktúry, ktoré sa líšia len označením operácií a označením prvkov. Napríklad, nech $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ a nech $\circ$ je operácia na $A$, $*$ operácia na $B$, ktoré sú dané nasledovnými tabuľkami.

| $\circ$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

Tab. 1

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $d$ | $a$ | $c$ |
| $c$ | $c$ | $a$ | $d$ | $b$ |
| $d$ | $d$ | $c$ | $b$ | $a$ |

Tab. 2

Vidíme, že ak v tabuľke 1 nahradíme symbol $\circ$ symbolom $*$ a prvky 1, 2, 3, 4 postupne prvkami $a$, $b$, $c$, $d$, dostaneme z nej tabuľku 2. Teda grupoid (grupa) $(B, *)$ je „kópiou“ grupoidu $(A, \circ)$. Podstata tohto úzkeho vzťahu medzi uvedenými grupoidmi je v tom, že existuje bijekcia $f = \{(1, a), (2, b), (3, c), (4, d)\}$ , o ktorej platí

$$\forall\, x, y \in A;\ f(x \circ y) = f(x) * f(y).$$

3.1 Definícia. Nech $(G, \circ)$ a $(H, *)$ sú grupoidy. Ak existuje bijekcia $f : G \to H$, o ktorej platí

$$\forall x, y \in G;\ f(x \circ y) = f(x) * f(y)$$

hovoríme, že $f$ je izomorfné zobrazenie (izomorfizmus) grupoidu $(G, \circ)$ na grupoid $(H, *)$.

3.2 Príklad. a) Logaritmická funkcia $\log : R^+ \to R$ je bijekcia a pretože

$$\forall\, x, y \in R^+;\ \log(x \cdot y) = \log x + \log y,$$

tak funkcia log je izomorfizmom grupoidu (grupy) $(R^+, \cdot)$ na grupoid (grupu) $(R, +)$.

b) Inverzná funkcia k logaritmickej funkcii $\log : R^+ \to R$ je exponenciálna funkcia $g : R \to R^+$, $g(x) = 10^x$. Pretože inverzná funkcia k bijekcii je tiež bijekcia a pretože

$$\forall\, x, y \in R;\ g(x + y) = 10^{x+y} = 10^x \cdot 10^y = g(x) \cdot g(y),$$

tak zobrazenie $g$ je izomorfizmom grupy $(R, +)$ na grupu $(R^+, \cdot)$.

3.3 Veta. *Ak $f$ je izomorfné zobrazenie grupoidu $(G, \circ)$ na grupoid $(H, *)$, tak inverzné zobrazenie $f^{-1}$ je izomorfným zobrazením grupoidu $(H, *)$ na grupoid $(G, \circ)$.*

Dôkaz. Ak $f$ je bijekcia $G$ na $H$, tak $f^{-1}$ je bijekcia $H$ na $G$. Nech $x, y \in H$. Potom (lebo $f$ je bijekcia) existujú prvky $a, b \in G$, že $f(a) = x$, $f(b) = y$, teda $f^{-1}(x) = a$, $f^{-1}(y) = b$. Na základe toho (a s využitím, že $f$ je izomorfizmus) dostávame

$$f^{-1}(x * y) = f^{-1}(f(a) * f(b)) = f^{-1}(f(a \circ b)) = \mathrm{id}_G(a \circ b) = a \circ b = f^{-1}(x) \circ f^{-1}(y)$$

čo znamená, že $f^{-1}$ je izomorfizmom grupoidu $(H, *)$ na grupoid $(G, \circ)$. □

3.4 Definícia. Ak existuje izomorfné zobrazenie grupoidu $(G, \circ)$ na grupoid $(H, *)$ hovoríme, že grupoidy $(G, \circ)$ a $(H, *)$ sú izomorfné.

Pretože zložením bijektívnych zobrazení vznikne bijektívne zobrazenie, ľahko sa môžeme presvedčiť o platnosti nasledovného tvrdenia (jeho dôkaz si podrobne zapíšte).

3.5 Veta. *Nech $f$ je izomorfizmus grupoidu $(G, \cdot)$ na grupoid $(K, \triangle)$ a nech $g$ je izomorfizmus grupoidu $(K, \triangle)$ na grupoid $(H, *)$. Potom zložené zobrazenie $g \circ f$ je izomorfizmus grupoidu $(G, \cdot)$ na grupoid $(H, *)$.*

3.6 Príklad. Zúžená funkcia $f$ k funkcii log (príklad 3.2) na interval $(1, \infty)$ je bijekciou na množinu $R^+$ (načrtnite jej graf). Teda funkcia $f : (1, \infty) \to R^+$ je izomorfizmus grupoidu (pologrupy) $((1, \infty), \cdot)$ na grupoid (pologrupu) $(R^+, +)$.

Funkcia $g : R^+ \to R^-$, $g(x) = -x$ je zrejme bijekcia a pretože pre každé $a, b \in R^+$

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

je funkcia $g$ izomorfizmom grupoidu (pologrupy) $(R^+, +)$ na grupoid (pologrupu) $(R^-, +)$.

Podľa vety 3.5 je potom zložené zobrazenie

$$g \circ f : (1, \infty) \to R^-,\ (g \circ f)(x) = g(f(x)) = g(\log x) = -\log x$$

izomorfným zobrazením grupoidu (pologrupy) $((1, \infty), \cdot)$ na grupoid (pologrupu) $(R^-, +)$.

Nech $\mathcal{A}$ je ľubovoľný neprázdny systém grupoidov. Na $\mathcal{A}$ definujeme reláciu $\cong$ podmienkou

$$(G, \circ) \cong (H, *) \quad \text{práve vtedy, keď} \quad (G, \circ) \text{ a } (H, *) \quad \text{sú izomorfné.}$$

Relácia $\cong$ je na $\mathcal{A}$ reflexívna (izomorfizmom $(G, \circ)$ na $(G, \circ)$ je $\mathrm{id}_G$). Z vety 3.3 vyplýva, že relácia $\cong$ je symetrická a podľa vety 3.5 je aj tranzitívna. Teda relácia $\cong$ je na $\mathcal{A}$ ekvivalenciou, t.j. určuje rozklad systému $\mathcal{A}$. Dva grupoidy patria teda do tej istej triedy rozkladu práve vtedy, keď sú izomorfné. Ako sme už v úvode spomenuli, izomorfné grupoidy, ktoré sa líšia nanajvýš označením prvkov a operácií nepokladáme obyčajne za rôzne. Môžeme teda povedať, že algebra sa nezaoberá skúmaním jednotlivých grupoidov, ale skúmaním tried daných reláciou $\cong$, resp., že algebra sa zaoberá skúmaním takých vlastností grupoidov, ktoré sa pri izomorfizme prenášajú (sú vzhľadom na izomorfizmus *invariantné*). Takými vlastnosťami je napr. asociatívnosť, existencia neutrálneho prvku, atď.

3.7 Veta. *Nech $f$ je izomorfizmus grupoidu $(G, \circ)$ na grupoid $(H, *)$. Potom platí:*

*a) ak je operácia $\circ$ asociatívna (komutatívna), tak aj operácia $*$ je asociatívana (komutatívna),*

*b) ak $e$ je neutrálny prvok grupoidu $(G, \circ)$, tak $f(e)$ je neutrálny prvok grupoidu $(H, *)$,*

*c) ak $a, a' \in G$ sú navzájom inverzné prvky v grupoide $(G, \circ)$, tak $f(a), f(a')$ sú navzájom inverzné prvky v grupoide $(H, *)$.*

Dôkaz. a) Nech $a, b, c \in H$. Pretože $f$ je bijekcia, tak existujú v $G$ prvky $x, y, z$, že $f(x) = a$, $f(y) = b$, $f(z) = c$. Potom (pretože $f$ je izomorfizmus a operácia $\circ$ je asociatívna) dostávame

$$a * (b * c) = f(x) * (f(y) * f(z)) = f(x) * (f(y \circ z) = f(x \circ (y \circ z)) =$$
$$= f((x \circ y) \circ z) = f(x \circ y) * f(z) = (f(x) * f(y)) * f(z) = (a * b) * c$$

čo znamená, že operácia $*$ je asociatívna. Invariantnosť komutatívnosti sa ukáže analogicky.

b) Nech $a \in H$. Potom existuje $x \in G$, že $f(x) = a$ a

$$a * f(e) = f(x) * f(e) = f(x \circ e) = f(x) = a.$$

Analogicky sa ukáže, že aj $f(e) * a = a$ a teda $f(e)$ je neutrálny prvok grupoidu $(H, *)$.

c) Ak $a, a' \in G$ sú inverzné prvky, tak

$$f(a) * f(a') = f(a \circ a') = f(e) \quad \text{a analogicky aj} \quad f(a') * f(a) = f(e)$$

čo znamená, že prvky $f(a), f(a') \in H$ sú inverzné. □

Bezprostredne z predchádzajúcej vety vyplýva nasledovný dôsledok.

3.8 Dôsledok. *Nech grupoid $(G, \circ)$ je izomorfný s grupoidom $(H, *)$. Potom $(G, \circ)$ je pologrupa (monoid, grupa) vtedy a len vtedy, keď $(H, *)$ je pologrupa (monoid, grupa).*

3.9 Príklad. Na množine $R$ je daná operácia $*$ takto: $a * b = \frac{ab-a-b+3}{2}$. Zistite, či zobrazenie $f : R \to R$, $f(x) = 2x + 1$ je izomorfizmus grupoidu $(R, \cdot)$ na grupoid $(R, *)$ a určte vlastnosti grupoidu $(R, *)$.

Riešenie. Zobrazenie (funkcia) $f$ je zrejme bijekcia (podrobne sa presvedčte). Pretože pre každé $a, b \in R$ je

$$f(a \cdot b) = 2ab + 1,$$
$$f(a) * f(b) = (2a + 1) * (2b + 1) = \frac{(2a + 1)(2b + 1) - (2a + 1) - (2b + 1) + 3}{2} =$$
$$= 2ab + 1,$$

teda $f(a \cdot b) = f(a) * f(b)$, tak $f$ je izomorfizmus.

Grupoid $(R, \cdot)$ je monoid s neutrálnym prvkom 1, preto aj $(R, *)$ je monoid s neutrálnym prvkom $f(1) = 2 \cdot 1 + 1 = 3$.

Obtiažnejšou môže byť úloha ukázať, že dané grupoidy sú izomorfné (t.j. nájsť príslušný izomorfizmus) resp. ukázať, že dané grupoidy nie sú izomorfné (t.j., že neexistuje izomorfizmus jedného grupoidu na druhý).

3.10 Príklad. Zistite, či sú izomorfné
a) grupoidy (pologrupy) $(2N^+, +)$ a $(3N^+, +)$,
b) grupoidy (pologrupy) $(2N^+, \cdot)$ a $(3N^+, \cdot)$,
c) grupoidy (grupy) $(Q, +)$ a $(Q^+, \cdot)$.

Riešenie. a) Ak $x \in 2N^+$, tak $x = 2a$, $a \in N^+$. Zobrazenie

$$f : 2N^+ \to 3N^+, \ f(2a) = 3a$$

je zrejme bijekcia (podrobne sa presvedčte) a pre každé $x, y \in 2N^+$ je

$$f(x+y) = f(2a+2b) = f(2(a+b)) = 3(a+b) = 3a+3b = f(2a)+f(2b) = f(x)+f(y),$$

teda $f$ je izomorfizmus grupoidu $(2N^+, +)$ na grupoid $(3N^+, +)$.

b) Zobrazenie $f$ z časti a) nie je izomorfizmom grupoidu $(2N^+, \cdot)$ na grupoid $(3N^+, \cdot)$ lebo napríklad pre prvky $4 = 2 \cdot 2$, $6 = 2 \cdot 3 \in 2N^+$ je

$$f((2 \cdot 2) \cdot (2 \cdot 3)) = f(2 \cdot 12) = 3 \cdot 12 = 36,$$

ale

$$f(2 \cdot 2) \cdot f(2 \cdot 3) = (3 \cdot 2) \cdot (3 \cdot 3) = 54,$$

teda $f((2 \cdot 2) \cdot (2 \cdot 3)) \neq f(2 \cdot 2) \cdot f(2 \cdot 3)$. Vidíme, že ak existuje izomorfizmus grupoidu $(2N^+, \cdot)$ na grupoid $(3N^+, \cdot)$, tak by asi mal „vymieňat'“ všetky dvojky a trojky medzi rozkladom vzoru a obrazu. Ak $x \in 2N^+$, tak sa zrejme dá zapísať v tvare $x = 2^\alpha \cdot 3^\beta \cdot a$, $\alpha \geq 1, \beta \geq 0, 2 \nmid a, 3 \nmid a$. Ukážeme, ze zobrazenie

$$g : 2N^+ \to 3N^+, \ g(x) = g(2^\alpha \cdot 3^\beta \cdot a) = 3^\alpha \cdot 2^\beta \cdot a$$

je izomorfizmus grupoidu $(2N^+, \cdot)$ na grupoid $(3N^+, \cdot)$.

Nech $x, y \in 2N^+$. Potom $x = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot a$, $y = 2^{\alpha_2} \cdot 3^{\beta_2} \cdot b$, $\alpha_1 \geq 1, \beta_1 \geq 0, 2 \nmid a, 3 \nmid a$, $\alpha_2 \geq 1, \beta_2 \geq 0, 2 \nmid b, 3 \nmid b$. Ak $g(x) = g(y)$, t.j. $3^{\alpha_1} \cdot 2^{\beta_1} \cdot a = 3^{\alpha_2} \cdot 2^{\beta_2} \cdot b$, tak z vety o jednoznačnom rozklade prirodzeného čísla na súčin prvočísel vyplýva, že $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$, $a = b$, t.j. $x = y$. Zobrazenie $g$ je teda injekcia. Ak $y \in 3N^+$, tak sa dá zapísať v tvare $y = 3^\alpha \cdot 2^\beta \cdot c$, $\alpha \geq 1, \beta \geq 0, 3 \nmid c, 2 \nmid c$. Potom $g(2^\alpha \cdot 3^\beta \cdot c) = y$, pričom $2^\alpha \cdot 3^\beta \cdot c \in 2N^+$. Zobrazenie $g$ je teda aj surjekcia. Nakoniec, ak $x, y \in 2N^+$, $x = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot a$, $y = 2^{\alpha_2} \cdot 3^{\beta_2} \cdot b$, $\alpha_1 \geq 1, \beta_1 \geq 0, 2 \nmid a, 3 \nmid a$, $\alpha_2 \geq 1, \beta_2 \geq 0, 2 \nmid b, 3 \nmid b$, tak (pretože $\alpha_1 + \alpha_2 \geq 1$, $\beta_1 + \beta_2 \geq 0$, $2 \nmid a \cdot b$, $3 \nmid a \cdot b$) dostávame

$$\begin{aligned} g(x \cdot y) &= g(2^{\alpha_1} \cdot 3^{\beta_1} \cdot a \cdot 2^{\alpha_2} \cdot 3^{\beta_2} \cdot b) = g(2^{\alpha_1+\alpha_2} \cdot 3^{\beta_1+\beta_2} \cdot a \cdot b) = \\ &= 3^{\alpha_1+\alpha_2} \cdot 2^{\beta_1+\beta_2} \cdot a \cdot b = (3^{\alpha_1} \cdot 2^{\beta_1} \cdot a) \cdot (3^{\alpha_2} \cdot 2^{\beta_2} \cdot b) = g(x) \cdot g(y). \end{aligned}$$

Zobrazenie $g$ je teda izomorfizmus grupoidu $(2N^+, \cdot)$ na grupoid $(3N^+, \cdot)$.

c) Ukážeme (sporom), že neexistuje izomorfné zobrazenie grupy $(Q, +)$ na grupu $(Q^+, \cdot)$. Predpokladajme, že zobrazenie $f : Q \to Q^+$ je izomorfizmus. Pretože $f$ je bijekcia, existuje $a \in Q$, že $f(a) = 2$. Určme obraz prvku $\frac{a}{2}$ (t.j. $f\left(\frac{a}{2}\right) \in Q^+$). Pretože $f$ je izomorfizmus, postupne dostávame

$$f(a) = 2, \quad f\left(\frac{a}{2} + \frac{a}{2}\right) = 2, \quad f\left(\frac{a}{2}\right) \cdot f\left(\frac{a}{2}\right) = 2, \quad \left(f\left(\frac{a}{2}\right)\right)^2 = 2,$$

čo je spor, lebo neexistuje racionálne číslo, ktorého druhá mocnina je 2.

Ak na trojprvkovej množine $A = \{1, 2, 3\}$ chceme definovať (napr. pomocou operačnej tabuľky) operáciu $\circ$ tak, aby štruktúra $(A, \circ)$ bola grupou, tak po zvolení jednotkového prvku je už doplnenie poľa tabuľky jednoznačné (presvedčte sa o tom). Znamená to, že všetky trojprvkové grupy sú navzájom izomorfné (t.j. patria do jednej triedy rozkladu, ktorý je daný reláciou $\cong$). V takomto prípade hovoríme, že existuje jediná (až na izomorfizmus) trojprvková grupa. Zaradením (*klasifikáciou*) niektorých ďalších konečných grúp do tried ekvivalencie podľa relácie $\cong$ sa budeme zaoberať neskôr.

Na množine $Z_n = \{0, 1, \ldots, n-1\}$ môžeme definovať operáciu $\oplus$ takto: $a \oplus b$ je zvyšok pri delení čísla $a + b$ číslom $n$, teda

$$a \oplus b = r, \quad \text{kde} \quad a + b = nq + r, \quad 0 \leq r < n$$

čo môžeme zapísať aj takto

$$a \oplus b = a + b - nq, \quad 0 \leq a \oplus b < n.$$

Nech $n \in Z$, $n > 1$. Vieme už, že $(\overline{Z}_n, \oplus)$ (kde $\overline{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ je systém zvyškových tried podľa modulu $n$) je grupa. Zobrazenie $f : Z_n \to \overline{Z}_n$, $f(x) = \overline{x}$ je bijekcia (podrobne sa presvedčte) a pre každé $a, b \in Z_n$ je

$$f(a \oplus b) = \overline{a \oplus b} = \overline{a + b - nq} = \overline{a} \oplus \overline{b} \oplus \overline{(-nq)} = \overline{a} \oplus \overline{b} = f(a) \oplus f(b)$$

čo znamená, že $(Z_n, \oplus) \cong (\overline{Z}_n, \oplus)$. Tieto štruktúry teda nerozlišujeme a obidve voláme *(aditívna) grupa zvyškových tried podľa modulu n.*

Analogicky môžeme na množine $Z_n$ definovať operáciu $\odot$: $a \odot b$ je zvyšok pri delení čísla $a \cdot b$ číslom $n$. Podrobne ukážte, že $(Z_n, \odot) \cong (\overline{Z}_n, \odot)$ (cvičenie 6). Aj v tomto prípade teda príslušné grupoidy (monoidy) nerozlišujeme a hovoríme o monoide zvyškových tried s operáciou násobenia.

## Cvičenia

**1.** Nájdite izomorfné zobrazenie grupoidu $(\{0, 1\}, \cdot)$ na grupoid $(\{\emptyset, \{1\}\}, \cap)$.

**2.** Na množine $A = \{a, b, c, d, e, f\}$ definujte Cayleyho tabuľkou operáciu $*$ tak, aby zobrazenie $\varphi = \{(0, c), (1, d), (2, a), (3, b), (4, f), (5, e)\}$ bolo izomorfným zobrazením grupoidu $(Z_6, +)$ na grupoid $(A, *)$.

**3.** Ukážte, že grupoid $(P(M), \cap)$ je izomorfný s grupoidom $(P(M), \cup)$ (úlohu najprv riešte pre $M = \{1, 2\}$).

**4.** Daný je grupoid $(Q, *)$, kde operácia $*$ je definovaná takto:

$$a * b = \frac{ab - 3a - 3b + 15}{2}.$$

a) Overte, že zobrazenie $f = \{(x, y) \in Q^2 \mid y = \frac{x-3}{2}\}$ je izomorfizmus grupoidu $(Q, *)$ na grupoid $(Q, \cdot)$.

b) Nájdite izomorfizmus grupoidu $(Q, \cdot)$ na grupoid $(Q, *)$ (priamo overte - urobte skúšku, že nájdené zobrazenie je naozaj požadovaný izomorfizmus).

c) Na základe toho, že grupoidy $(Q, \cdot)$, $(Q, *)$ sú izomorfné určte vlastnosti operácie grupoidu $(Q, *)$.

**5.** Na množine $A = \{1, 2, 3\}$ je daná operácia $\circ$ a na množine $B = \{a, b, c\}$ operácia $*$ nasledovnými tabuľkami:

| $\circ$ | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 1 |
| 3 | 3 | 1 | 2 |

| $*$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $b$ | $a$ |

Zistite, či grupoid $(A, \circ)$ je izomorfný s grupoidom $(B, *)$.

**6.** Na množine $Z_n = \{0, 1, \ldots, \ldots, n-1\}$ je daná operácia $\odot$ takto: $a \odot b$ je zvyšok pri delení čísla $a \cdot b$ číslom $n$, teda

$$a \odot b = r, \quad \text{kde} \quad a \cdot b = nq + r, \quad 0 \leq r < n.$$

Ukážte, že grupoidy $(Z_n, \odot)$, $(\overline{Z}_n, \odot)$ sú izomorfné.

**7.** Ukážte, že grupoidy $((0, 1), \cdot)$ a $((1, \infty), \cdot)$ sú izomorfné.

**8.** Nech $A = \{5^n \mid n \in N\}$. Ukážte, že grupoidy $(A, \cdot)$ a $(N, +)$ sú izomorfné.

**9.** Nájdite izomorfizmus grupoidu $(\{0, -1, 1\}, \cdot)$ na grupoid $(\{f_0, f_1, f_2\}, \circ)$, pričom $f_0 = \emptyset$, $f_1 = \{(0, 1), (1, 0)\}$, $f_2 = \{(0, 0), (1, 1)\}$.

**10.** Nájdite všetky izomorfizmy grupy $(Z_4, +)$ na grupu $(\{1, -1, i, -i\}, \cdot)$.

**11.** Na množine $Z$ definujeme operácie $\circ$ a $*$ takto

$$x \circ y = x + y + 1, \qquad x * y = x + y - 1.$$

Nájdite izomorfné zobrazenie grupoidu $(Z, \circ)$ na $(Z, *)$.

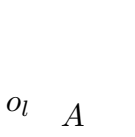
**12.** Ukážte, že grupoidy $(Q, +)$, $(Z, \cdot)$ nie sú izomorfné.

## 4. Grupy. Príklady grúp

Ako sme už spomenuli v druhej kapitole, grupy sa začali skúmať už v 19. storočí. Francúz E. Galois a Nór H. Abel ukázali pomocou grúp, že korene algebraickej rovnice piateho stupňa s komplexnými koeficientami sa už nedajú vyjadriť pomocou jej koeficientov a operácií sčítania, násobenia a odmocňovania (tak, ako sa dajú vyjadriť korene ľubovoľnej algebraickej rovnice druhého, tretieho a štvrtého stupňa s komplexnými koeficientami). To bol súčasne aj silný podnet k skúmaniu grúp a iných algebraických štruktúr. Ďalším impulzom je snaha popísať napríklad symetrie geometrických útvarov.

Nech $U$ je množina bodov nejakého geometrického útvaru. Symbolom $d(X, Y)$ označujeme vzdialenosť bodov $X, Y$. Permutácia $f : U \to U$ sa nazýva *symetria* útvaru $U$, ak zachováva vzdialenosti, t.j. ak pre ľubovoľné body $A, B \in U$ platí $d(A, B) = d(f(A), f(B))$. Identické zobrazenie $\mathrm{id}_U$ je zrejme symetria. Ak $f$, $g$ sú symetrie útvaru $U$, tak aj $f \circ g$ je symetria útvaru $U$ a inverzné zobrazenie $f^{-1}$ je tiež symetria útvaru $U$ (pozri napr. vetu 12.5 v [6]). V nasledujúcom príklade popíšeme grupu symetrií štvorca.

4.1 Príklad. Daný je štvorec $ABCD$. V symetrickom zobrazení môže byť každý vrchol štvorca zobrazený do ľubovoľného jeho vrchola. Ak pevne zvolíme obraz niektorého vrchola, tak dva susedné vrcholy je možné zobraziť dvomi spôsobmi. Keď je daná poloha jedného vrchola a s ním susedných dvoch vrcholov, tak je už jednoznačne určený každý bod štvorca a teda určená je aj symetria. Štvorec má teda osem symetrií. Sú to zhodné zobrazenia $i$, $r_1$, $r_2$, $r_3$, $l$, $p$, $v$, $h$, kde $i$ je identické zobrazenie, $r_1$, $r_2$, $r_3$ sú rotácie o $90^0$, $180^0$, $270^0$ (proti smeru pohybu hodinových ručičiek) a $l$, $p$, $v$, $h$ sú osové súmernosti s osami $o_l$, $o_p$, $o_v$, $o_h$, tak ako je to znázornené na obrázku 1. Príslušná operácia skladania zobrazení je popísaná v tabuľke 1.




Obr. 1

| $\circ$ | $i$ | $r_1$ | $r_2$ | $r_3$ | $l$ | $p$ | $v$ | $h$ |
|---|---|---|---|---|---|---|---|---|
| $i$ | $i$ | $r_1$ | $r_2$ | $r_3$ | $l$ | $p$ | $v$ | $h$ |
| $r_1$ | $r_1$ | $r_2$ | $r_3$ | $i$ | $v$ | $h$ | $p$ | $l$ |
| $r_2$ | $r_2$ | $r_3$ | $i$ | $r_1$ | $p$ | $l$ | $h$ | $v$ |
| $r_3$ | $r_3$ | $i$ | $r_1$ | $r_2$ | $h$ | $v$ | $l$ | $p$ |
| $l$ | $l$ | $h$ | $p$ | $v$ | $i$ | $r_2$ | $r_3$ | $r_1$ |
| $p$ | $p$ | $v$ | $l$ | $h$ | $r_2$ | $i$ | $r_1$ | $r_3$ |
| $v$ | $v$ | $l$ | $h$ | $p$ | $r_1$ | $r_3$ | $i$ | $r_2$ |
| $h$ | $h$ | $p$ | $v$ | $l$ | $r_3$ | $r_1$ | $r_2$ | $i$ |

Tab. 1

Dôležitým príkladom grupy je grupa symetrií pravidelného $n$-uholníka (jej špeciálnym prípadom je už spomenutá grupa symetrí štvorca).

4.2 Príklad. Analogickou úvahou ako pri symetriách štvorca zistíme, že počet všetkých symetrií pravidelného $n$-uholníka je $2n$. Z celkového počtu $2n$ symetrií je

$n$ rotácií o $k \cdot \frac{360^0}{n}$, $k \in \{0, 1, \ldots, n-1\}$ a $n$ osových súmerností. Grupu symetrií pravidelného $n$-uholníka nazývame *dihedrálna* grupa stupňa $n$ a označujeme ju $D_n$. Samotné rotácie tvoria zrejme tiež grupu (podgrupu grupy $D_n$). Nazývame ju grupa *rotácií* pravidelného $n$-uholníka a označujeme ju $C_n$. Grupa $C_n$ je izomorfná s grupou $(Z_n, \oplus)$.

Jednou z dvoch štvorprvkových grúp (až na izomorfizmus) je, ako neskôr uvidíme, grupa symetrií obdĺžnika. Popíšeme ju v nasledujúcom príklade.

4.3 Príklad. Symetriami (ľubovoľného) obdĺžnika sú identické zobrazenie $i$, otočenie $r$ o $180^0$ a osové súmernosti $h$ a $v$ podľa horizontálnej a vertikálnej osi prechádzajúcej stredom obdĺžnika (obrázok 2). Operácia skladania na množine $\{i, r, h, v\}$ je popísaná v tabuľke 2.

$o_v$

$o_h$

| $\circ$ | $i$ | $r$ | $h$ | $v$ |
|---|---|---|---|---|
| $i$ | $i$ | $r$ | $h$ | $v$ |
| $r$ | $r$ | $i$ | $v$ | $h$ |
| $h$ | $h$ | $v$ | $i$ | $r$ |
| $v$ | $v$ | $h$ | $r$ | $i$ |

Obr. 2 Tab. 2

Vidíme, že grupa $(\{i, r, h, v\}, \circ)$ je komutatívna, neutrálny prvok je $i$ a každý prvok je sám k sebe inverzným.

4.4 Príklad. Známymi a často využívanými číselnými grupami sú (ako sme už uviedli aj v príklade 2.16) napr. štruktúry: $(C, +)$, $(R, +)$, $(Q, +)$, $(Z, +)$, $(C \setminus \{0\}, \cdot)$, $(R^+, \cdot)$, $(Q^+, \cdot)$, $(R \setminus \{0\}, \cdot)$, $(Q \setminus \{0\}, \cdot)$. Všetky uvedené grupy sú nekonečné a komutatívne. Grupy $(\{1, -1, i, -i\}, \cdot)$, $(\{-1, 1\}, \cdot)$, $(Z_n, \oplus), n \in N, n > 1$ sú konečné komutatívne grupy.

4.5 Príklad. Vieme už, že $(\overline{Z}_n, \oplus)$ je grupa. Ukážeme, že $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ je grupa vtedy a len vtedy, keď $p$ je prvočíslo.

a) Najprv dokážeme (sporom), že $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ je grupoid. Predpokladajme, že $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ nie je grupoid, teda, že existujú prvky $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$ také, že $\overline{a} \odot \overline{b} = \overline{0}$ (t.j $\overline{a} \odot \overline{b} \notin \overline{Z}_p \setminus \{\overline{0}\}$). Potom $\overline{a \cdot b} = \overline{0}$, teda $a \cdot b \equiv 0 \pmod{p}$, t.j. $p \mid a \cdot b$. Pretože $p$ je prvočíslo, tak $p \mid a$ alebo $p \mid b$, čo znamená, že $a \equiv 0 \pmod{p}$ alebo $b \equiv 0 \pmod{p}$, t.j. $\overline{a} = \overline{0}$ alebo $\overline{b} = \overline{0}$, čo je spor.

Z vety 1.11 vyplýva, že operácia $\odot$ je asociatívna a komutatívna na $\overline{Z}_p$ (a teda aj na $\overline{Z}_p \setminus \{\overline{0}\}$) s neutrálnym prvkom $\overline{1}$. Grupoid $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ je teda monoidom.

Nech $p$ je prvočíslo a nech $\overline{a} \in \overline{Z}_p \setminus \{\overline{0}\}$. Vynásobme všetky prvky množiny $\overline{Z}_p \setminus \{\overline{0}\}$ prvkom $\overline{a}$. Dostaneme prvky $\overline{a} \odot \overline{1}$, $\overline{a} \odot \overline{2}$, $\ldots$, $\overline{a} \odot \overline{(p-1)}$. Z vety 1.10 vyplýva, že každé dva z týchto prvkov sú navzájom rôzne a teda $\{\overline{a} \odot \overline{1}, \overline{a} \odot \overline{2}, \ldots, \overline{a} \odot \overline{(p-1)}\} = \overline{Z}_p \setminus \{\overline{0}\}$. Je preto medzi nimi aj prvok $\overline{1}$. Nech je to napr. $\overline{a} \odot \overline{b}$. Potom $\overline{a}^{-1} = \overline{b}$. Z uvedeného vyplýva, že ku každému prvku množiny $\overline{Z}_p \setminus \{\overline{0}\}$ existuje inverzný prvok, teda monoid $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ je grupou (komutatívnou).

b) Ak $p$ je zložené číslo, tak $p = a \cdot b$, $1 < a < p, 1 < b < p$ a $\overline{a} \odot \overline{b} = \overline{p} = \overline{0}$ čo znamená, že $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ nie je dokonca ani grupoid.

4.6 Príklad. Z vety 2.5 vyplýva, že priamym súčinom grúp je grupa.

Poznámka. Operáciu priameho súčinu aditívnych grúp $(Z_n, \oplus)$, $(Z_m, \oplus)$ budeme označovať tiež $\oplus$ a podobne budeme postupovať aj v iných analogických prípadoch.

4.7 Príklad. Izomorfizmus grupy $(G, \cdot)$ na seba (t.j. na grupu $(G, \cdot)$) sa nazýva *automorfizmus*. Identické zobrazenie $\mathrm{id}_G$ je zrejme automorfizmus. Zložením automorfizmov vznikne automorfizmus a inverzné zobrazenie k automorfizmu je automorfizmus (pozri vety 3.3 a 3.5). Množina všetkých automorfizmov (s operáciou skladania zobrazení) je teda grupou. Označujeme ju $\mathrm{Aut}(G)$. Presvedčte sa, že

$$\mathrm{Aut}(Z_4) = \{\mathrm{id}_{Z_4}, \{(0,0),(1,3),(2,2),(3,1)\}\}$$

a že $\mathrm{Aut}(Z_4) \cong Z_2$.

Riešenie binomických rovníc poznáme už zo strednej školy. Binomická rovnica $x^n = 1$ má v obore komplexných čísel $n$ koreňov, ktoré možno vyjadriť v goniometrickom tvare:

$$x_k = \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n},\ k \in \{0, \ldots, n-1\}.$$

4.8 Príklad. Množinu všetkých riešení binomickej rovnice $x^n = 1$ označíme $K_n$. Ukážeme, že množina $K_n$, s operáciou násobenia komplexných čísel, je grupou. Nazýva sa aj grupa $n$-tých (komplexných) odmocnín jednotky.

Operácia násobenia komplexných čísel je asociatívna (aj komutatívna). Neutrálnym prvkom je číslo $x_0 = \cos 0 + i \cdot \sin 0 = 1 \in K_n$. Neutrálny prvok je samozrejme inverzný sám k sebe. Inverzným prvkom k prvku $x_m$, $m \in \{1, 2, \ldots n-1\}$ je prvok $x_{n-m}$, lebo podľa Moivreovej vety je

$$\begin{aligned} x_m \cdot x_{n-m} &= \cos\left(\frac{2m\pi}{n} + \frac{2(n-m)\pi}{n}\right) + i \cdot \sin\left(\frac{2m\pi}{n} + \frac{2(n-m)\pi}{n}\right) = \\ &= \cos 2\pi + i \cdot \sin 2\pi = \cos 0 + i \cdot \sin 0 = 1 \in K_n \end{aligned}$$

a $x_{n-m} \in K_n$ lebo pre $m \in \{1, \ldots, n-1\}$ je $n - m \in \{1, \ldots, n-1\}$.

Grupa $(K_n, \cdot)$ je samozrejme podgrupou grupy $(C \setminus \{0\}, \cdot)$ a na dôkaz, že je grupou (podgrupou) sme mohli použiť aj vetu 2.24.

*Grupou transformácií* množiny $A$ budeme volať takú neprázdnu množinu $H$ bijekcií množiny $A$ na $A$ (spolu s operáciou skladania zobrazení, ktorá obsahuje $\mathrm{id}_A$, s každou dvojicou bijekcií $f$, $g$ aj $f \circ g$ a s každou bijekciou $f$ aj k nej inverznú bijekciu $f^{-1}$. Najväčšou (vzhľadom na usporiadanie inklúziou) grupou transformácií danej množiny $A$ je teda grupa všetkých bijekcií $A$ na $A$, t.j. grupa $T(A)$ všetkých transformácií množiny $A$ (pozri príklad 2.18).

Grupami transformácií sú teda napr. grupy symetrií geometrických útvarov. Podobne, grupa $\mathrm{Aut}(G)$ všetkých automorfizmov grupy $G$ je grupou transformácií množiny $G$.

4.9 Veta (Cayleyho). *Každá grupa je izomorfná s nejakou grupou transformácií.*

Dôkaz. Nech $(G, \cdot)$ je grupa. Pre každé $a \in G$ definujme zobrazenie $f_a : G \to G$, $f_a(x) = a \cdot x$ (tzv. ľavá translácia na $G$ daná prvkom $a$). Nech $T$ je množina všetkých zobrazení tvaru $f_a$, t.j. $T = \{f_a;\ a \in G\}$.

Ak $f_a$, $f_b \in T$, tak

$$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b \cdot x) = a \cdot (b \cdot x) = (a \cdot b) \cdot x = f_{a \cdot b}(x)$$

čo znamená, že aj $f_a \circ f_b \in T$.

Pretože pre každé $x \in G$ je $f_e(x) = e \cdot x = x$, tak $f_e = \mathrm{id}_G \in T$.

Ďalej, pre ľubovoľný prvok $x \in G$ a pre ľubovoľnú transláciu $f_a \in T$ platí

$$(f_a \circ f_{a^{-1}})(x) = f_1(x) \text{ a podobne } (f_{a^{-1}} \circ f_a)(x) = f_e(x) = x.$$

Preto každý prvok $f_a \in T$ je bijekcia a $(T, \circ)$ je grupa transformácií na $G$.

Teraz ukážeme, že grupy $(G, \cdot)$ a $(T, \circ)$ sú izomorfné. Nech $\varphi$ je zobrazenie $G \to T$ dané predpisom $\varphi(c) = f_c$. Ak $c \neq d$, tak $f_c \neq f_d$ (pretože $f_c(e) = c$, ale $f_d(e) = d$). Teda $\varphi$ je prosté zobrazenie. Je zrejmé, že $\varphi$ je aj surjekcia. Nakoniec, pre každé $x, y \in G$ platí

$$\varphi(x \cdot y) = f_{x \cdot y} = \varphi(x) \circ \varphi(y).$$

Zobrazenie $\varphi : G \to T$ je teda izomorfizmus grupy $(G, \cdot)$ na grupu $(T, \circ)$. □

Z uvedenej vety vyplýva, že ľubovoľnú grupu je možné nahradiť vhodnou (izomorfnou) grupou transformácií.

4.10 Príklad. Nájdite grupu transformácií izomorfnú s grupou $(\{1, -1, i, -i\}, \cdot)$.

Riešenie. Určíme ľavé translácie na množine $\{1, -1, i, -i\}$ dané prvkami 1, $-1$, $i$, $-i$:
$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$, $f_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}$, $f_i = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}$, $f_{-i} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$. Označme $T = \{f_1, f_{-1}, f_i, f_{-i}\}$. podľa Cayleyho vety je grupa $(\{1, -1, i, -i\}, \cdot)$ izomorfná s grupou $(T, \circ)$. Izomorfizmom je zobrazenie $\varphi = \{(1, f_1), (-1, f_{-1}), (i, f_i), (-i, f_{-i})\}$. Zostrojte operačné tabuľky pre obidve grupy.

## Cvičenia

**1.** Popíšte grupu symetrií a) kosoštvorca, b) rovnostranného trojuholníka (dihedrálnu grupu $D_3$), c) rovnostranného päťuholníka (dihedrálnu grupu $D_5$).

**2.** Určte počet symetrií a) kocky, b) pravidelného štvorstena, c) pravidelného osemstena.

**3.** Popíšte tie symetrie kocky, ktoré zobrazujú jeden (pevne zvolený) vrchol do seba.

**4.** Načrtnite geometrický útvar v rovine, ktorého grupa symetrií je izomorfná s grupou a) $(Z_5, \oplus)$, b) $(S_3, \cdot)$.

**5.** Napíšte operačnú tabuľku grupy $(\mathcal{P}(\{1, 2, 3\}), \triangle)$.

**6.** Nájdite podgrupu grupy permutácií štvorprvkovej množiny, ktorá je izomorfná s grupou symetrií štvorca.

**7.** Dokážte, že

a) $\mathrm{Aut}\,(Z_5, \oplus) \simeq (Z_4, \oplus)$, b) $\mathrm{Aut}\,(Z_6, \oplus) \simeq (Z_2, \oplus)$, c) $\mathrm{Aut}\,(Z_3, \oplus) \simeq (Z_2, \oplus)$.

**8.** Ukážte, že grupa $S_3$ je izomorfná s grupou svojich automorfizmov $\mathrm{Aut}(S_3)$.

**9.** Ukážte, že grupa automorfizmov grupy symetrií obdĺžnika je izomorfná s grupou $S_3$.

**10.** Nech $(G, \cdot)$ je grupa, $c \in G$. Ukážte, že zobrazenie $f_c : x \mapsto cxc^{-1}$ je automorfizmus grupy $(G, \cdot)$. Automorfizmy $f_c$, $c \in G$, dané uvedeným spôsobom, nazývame *vnútorné automorfizmy* grupy $G$.

**11.** Určte vymenovaním všetky vnútorné automorfizmy grupy $(S_3, \cdot)$.

**12.** Zistite, či nasledujúce dvojice grúp sú izomorfné:
a) $(Z_2 \times Z_2, +)$, $(Z_6, +)$,
b) $(Z_6, +)$, $(Z_7 \setminus \{0\}, \cdot)$,
c) $(Z_2 \times Z_2, +)$, $(Z_4, +)$,
d) $(Z_2 \times Z_2, +)$, $(\mathcal{P}(\{1, 2\}), \triangle)$,
e) $(E \times E, +)$, $(C, +)$,
f) $(E \setminus \{0\}, \cdot)$, $(E^+, \cdot)$,
g) $(E \setminus \{0\}, \cdot)$, $(C \setminus \{0\}, \cdot)$.

**13.** Určte grupu transformácií izomorfnú s grupou
a) $(\mathcal{P}(\{1, 2\}), \triangle)$, b) $(Z_7 \setminus \{0\}, \cdot)$.

## 5. Cyklické grupy. Rád prvku v grupe

Vieme už, že binomická rovnica $x^n = 1$ má v obore komplexných čísel $n$ koreňov, ktoré možno vyjadriť v goniometrickom tvare ako

$$x_k = \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n},\ k = 0, \ldots, n-1.$$

V kapitole 4 (príklad 4.8) sme ukázali, že množina $\{x_0, \ldots, x_{n-1}\}$ týchto koreňov s operáciou násobenia tvorí grupu. Všimnime si zaujímavú štruktúru tejto grupy. Podľa Moivrovej vety

$$\cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n} = (\cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n})^k,$$

a teda $x_k = x_1^k \in [x_1]$ pre každé $k = 0, \ldots, n-1$, odkiaľ vyplýva $K_n = [x_1]$. Pripomeňme si, že vo všeobecnosti pre grupu $G$ a $a \in G$ symbol $[a]$ označuje najmenšiu podgrupu grupy $G$ obsahujúcu prvok $a$.

5.1 Definícia. *Grupa $(G, \cdot)$ sa nazýva cyklická, ak existuje taký prvok $a \in G$, že $G = [a]$. Prvok $a$ nazývame potom generátorom grupy $G$.*

Rovnakú štruktúru ako cyklická grupa $(K_n, \cdot)$ má aj grupa $(C_n, \circ)$ všetkých rotácií pravidelného $n$-uholníka. Je ľahké vidieť, že rotácia $r_1$ o uhol $\frac{2\pi}{n}$ je generátorom tejto grupy a že $r_k = r_1 \circ \cdots \circ r_1$ ($k$-krát) je rotácia o uhol $\frac{2k\pi}{n}$ pre každé $k = 0, \ldots, n-1$ ($r_0$ je identické zobrazenie). Evidentne teda zobrazenie $f : K_n \to C_n,\ f(x_k) = r_k$, ktoré koreňu $\cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n}$ rovnice $x^n = 1$ priradí rotáciu pravidelného $n$-uholníka o uhol $\frac{2k\pi}{n}$ funguje ako izomorfizmus grupy $(K_n, \cdot)$ na grupu $(C_n, \circ)$. Neskôr uvidíme, že každé dve konečné cyklické grupy majúce rovnaký počet prvkov sú izomorfné. Teraz sa oboznámime s dôležitým pojmom *mocniny prvku*, ktorý možno zaviesť v ľubovoľnej grupe.

5.2 Definícia. *V grupe $(G, \cdot)$ definujeme pre každé $n \in Z$ a pre každý prvok $a \in G$ grupovú mocninu $a^n$ nasledovne:*

$$a^n = \begin{cases} (a \cdot a \cdot \ldots \cdot a)_{k\text{-krát}}, & \text{ak } n \in Z^+, \\ e, & \text{ak } n = 0, \\ (a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1})_{k\text{-krát}}, & \text{ak } n = -k \in Z^-. \end{cases}$$

Pravidlá pre počítanie s mocninami, ktoré sú nám dobre známe v grupe $(R, \cdot)$, zovšeobecňuje pre grupové mocniny v ľubovoľnej grupe nasledujúca veta.

5.3 Veta. *Nech $(G, \cdot)$ je grupa, $a, b \in G$ a nech $m, n \in Z$. Potom*
*a) $a^{n+m} = a^n \cdot a^m$,*
*b) $(a^n)^m = a^{n \cdot m}$,*
*c) ak $a \cdot b = b \cdot a$, tak $(a \cdot b)^n = a^n \cdot b^n$.*

Dôkaz. Pretože grupová mocnina $a^n$ je definovaná v závislosti od „znamienka“ exponenta $n$, je potrebné pri preverovaní uvedených pravidiel a), b), c) rozlišovať „znamienka“ jednotlivých exponentov.

1. prípad: $n, m \in Z^+$. Potom

a)

$$a^{n+m} = (a \cdot a \cdot \ldots \cdot a)_{(n+m)\text{-krát}} =$$
$$= (a \cdot a \cdot \ldots \cdot a)_{n\text{-krát}} \cdot (a \cdot a \cdot \ldots \cdot a)_{m\text{-krát}} = a^n \cdot a^m.$$

b)

$$(a^n)^m = [(a \cdot a \cdot \ldots \cdot a)_{n\text{-krát}} \cdot \ldots \cdot (a \cdot a \cdot \ldots \cdot a)_{n\text{-krát}}]_{m\text{-krát}} =$$
$$= (a \cdot a \cdot \ldots \cdot a)_{(n\cdot m)\text{-krát}} = a^{n\cdot m}.$$

2. prípad: $n = 0,\ m \in Z^+$. Potom

a)

$$a^{n+m} = a^m = e \cdot a^m = a^0 \cdot a^m = a^n \cdot a^m,$$

b)

$$(a^n)^m = e^m = e = a^0 = a^{0\cdot m} = a^{n\cdot m}.$$

3. prípad: $n = -k \in Z^-, m \in Z^+,\ k < m$. Potom

a)

$$a^{n+m} = a^{-k+m} = (a \cdot a \cdot \ldots \cdot a)_{(-k+m)\text{-krát}} =$$
$$= (a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1})_{k\text{-krát}} \cdot (a \cdot a \cdot \ldots \cdot a)_{m\text{-krát}} =$$
$$= a^{-k} \cdot a^m = a^n \cdot a^m,$$

b)

$$(a^n)^m = (a^{-k})^m = [(a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1})_{k\text{-krát}} \cdot \ldots \cdot (a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1})_{k\text{-krát}}]_{m\text{-krát}} =$$
$$= (a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1})_{(k\cdot m)\text{-krát}} = a^{-k\cdot m} = a^{n\cdot m}.$$

Ďalšie prípady v a),b) prenecháme na čitateľa.

c)

1. prípad: $n \in Z^+$.

$$(a \cdot b)^n = [(a \cdot b) \cdot \ldots \cdot (a \cdot b)]_{n\text{-krát}} =$$
$$= (a \cdot a \cdot \ldots \cdot a)_{n\text{-krát}} \cdot (b \cdot b \cdot \ldots \cdot b)_{n\text{-krát}} = a^n \cdot b^n,$$

pričom sme využili predpoklad, že $a \cdot b = b \cdot a$.

2. prípad: $n = 0$.

$$(a \cdot b)^n = e = e \cdot e = a^0 \cdot b^0 = a^n \cdot b^n.$$

3. prípad: $n = -k \in Z^-$.

$$(a \cdot b)^n = [(a \cdot b)^{-1} \cdot \ldots \cdot (a \cdot b)^{-1}]_{k\text{-krát}} =$$
$$= [(b^{-1} \cdot a^{-1}) \cdot \ldots \cdot (b^{-1} \cdot a^{-1})]_{k\text{-krát}} =$$
$$= (a^{-1})_{k\text{-krát}} \cdot (b^{-1})_{k\text{-krát}} = a^{-k} \cdot b^{-k} = a^n \cdot b^n,$$

pričom sme využili rovnosť $b^{-1} \cdot a^{-1} = a^{-1} \cdot b^{-1}$ vyplývajúcu z rovnosti $a \cdot b = b \cdot a$. □

Poznámka. Ak je grupa označovaná aditívne, tak namiesto označenia $a^n$ často používame označenie $n \times a$. Potom rovnosti a), b), c) z vety 5.3 majú tvar $(n+m) \times a = (n \times a) + (m \times a),\ m \times (n \times a) = (m \cdot n) \times a,\ n \times (a \cdot b) = (n \times a) \cdot (n \times b)$.

Z nasledujúcej vety je zrejmé, prečo sú mocniny prvkov dôležité pri štúdiu cyklických grúp.

5.4 Veta. *Grupa $G$ je cyklická vtedy a len vtedy, keď pozostáva z mocnín niektorého svojho prvku (generátora).*

Dôkaz. V ľubovoľnej grupe $(G,\cdot)$ s neutrálnym prvkom $e$ musí pre každú jej podgrupu platiť, že ak obsahuje prvok $a$, tak obsahuje aj neutrálny prvok $e=a^0$, inverzný prvok $a^{-1}$ a pre každé kladné celé číslo $k$ aj všetky mocniny $a^k$, $(a^{-1})^k$, t.j. obsahuje aj množinu $\{a^n \mid n\in Z\}$ všetkých mocnín prvku $a$. Teda $[a]\supseteq\{a^n \mid n\in Z\}$. Ľahko sa overí (použitím vety 2.24), že množina $\{a^n \mid n\in Z\}$ je podgrupa grupy $G$ obsahujúca prvok $a$. Keďže $[a]$ je definovaná ako najmenšia podgrupa grupy $G$ obsahujúca prvok $a$, dostávame, že $[a]\subseteq\{a^n \mid n\in Z\}$. Tým sme dokázali, že $[a]=\{a^n \mid n\in Z\}$, odkiaľ tvrdenie vety bezprostredne vyplýva. □

Ukázali sme, že cyklická grupa $G=[a]$ s generátorom $a$ pozostáva zo všetkých mocnín $a^n$, $n\in Z$. Cyklické grupy $K_n=[x_1]$, $C_n=[r_1]$ spomínané v úvode tejto kapitoly boli konečné. V takom prípade sa niektoré mocniny generátora musia rovnať. Skutočne, ľahko je vidieť, že v grupe $K_n$ pre ľubovoľné $k\in\{0,\dots,n-1\}$ platí

$$(x_1)^k=\cos\frac{2k\pi}{n}+i\cdot\sin\frac{2k\pi}{n}=\cos\frac{2(k+n)\pi}{n}+i\cdot\sin\frac{2(k+n)\pi}{n}=$$
$$=(x_1)^{k+n}=(x_1)^{k+2n}=(x_1)^{k+3n}=\cdots=(x_1)^{k-n}=(x_1)^{k-2n}=\dots.$$

Všeobecne, ak v grupe $(G,\cdot)$ platí $a^n=a^m$ pre $n>m$, tak $a^{n-m}=e$ a v konečnej grupe zrejme vždy musí existovať najmenšie kladné celé číslo $k$ s vlastnosťou $a^k=e$.

5.5 Definícia. *Nech $(G,\cdot)$ je ľubovoľná grupa a nech $a$ je prvkom $G$. Ak existuje najmenšie kladné celé číslo $k$ s vlastnosťou $a^k=e$, hovoríme, že rád prvku $a$ je $k$ a píšeme $r(a)=k$. Ak také číslo $k$ neexistuje, hovoríme, že rád prvku $a$ je nekonečno a píšeme $r(a)=\infty$ (niekedy sa namiesto toho hovorí, že rád prvku $a$ je nula a píše $r(a)=0$). Rádom grupy $G$ nazývame kardinálne číslo jej nosiča, $|G|$ (pozri poznámku 5.6), t.j. v konečnom prípade pod rádom grupy rozumieme počet jej prvkov.*

**5.6 Poznámka.** Pripomíname, že kardinálne číslo konečnej množiny vyjadruje počet jej prvkov. Aby sa tento pojem dal zovšeobecniť pre ľubovoľné (aj nekonečné) množiny, definuje sa na systéme $\mathcal{S}$ všetkých množín (podotýkame, že systém $\mathcal{S}$ je „tak veľký“, že nie je množinou, pozri [6]) relácia ekvivalencie $\sim$ tak, že pre množiny $A,B$ platí $A\sim B$ vtedy, keď existuje bijektívne zobrazenie $g:A\to B$. Vo všeobecnosti je potom *kardinálne číslo* množiny $A$ definované ako tá trieda ekvivalencie $\sim$ systému $\mathcal{S}$ do ktorej patrí $A$. Pre kardinálne číslo množiny $A$ sa tiež používa pojem *kardinalita* alebo *mohutnosť* množiny $A$ a zaužívané označenie preň je $|A|$. Teda $|A|$ je trieda všetkých množín ktoré možno bijektívne zobraziť na $A$ (táto spoločná vlastnosť intuitívne vyjadruje, že množiny s rovnakou kardinalitou sú „rovnako veľké“). Kardinálne čísla konečných množín sú prirodzené čísla $0,1,2,3,\dots$, kardinálne čísla nekonečných množín sa označujú hebrejskými znakmi $\aleph_0,\aleph_1,\aleph_2,\dots$. Pritom $\aleph_0$ je kardinálne číslo množiny $N$ prirodzených čísel a teda v zmysle definície aj všetkých nekonečných množín, ktoré sa dajú bijektívne zobraziť na $N$ (t.j. sú „rovnako veľké“ ako $N$), napr. $2N,Z,Q,\dots$. Čiže $|N|=|2N|=|Z|=|Q|=\aleph_0$.

Kardinálne čísla sú lineárne usporiadané reláciou $\leq$, pričom $|A|\leq|B|$ platí práve vtedy, keď existuje prosté zobrazenie $f:A\to B$. Súčet $|A|+|B|$ kardinálnych čísel

$|A|$ a $|B|$ je definovaný ako kardinálne číslo $|A \cup B|$ množiny $A \cup B$, pričom sa predpokladá, že množiny $A, B$ sú disjunktné. Súčin $|A| \cdot |B|$ kardinálnych čísel $|A|$ a $|B|$ je definovaný ako kardinálne číslo $|A \times B|$ karteziánskeho súčinu $A \times B$. Operácie sčítania a násobenia kardinálnych čísel sú komutatívne a asociatívne a sčítanie je distributívne vzhľadom na násobenie. Sčítanie a násobenie kardinálnych čísel konečných množín je zhodné so sčítaním a násobením prirodzených čísel.

O ráde konečnej cyklickej grupy môžeme vysloviť nasledovné tvrdenie.

5.7 Veta. *Rád konečnej cyklickej grupy sa rovná rádu ľubovoľného jej generátora.*

Dôkaz. Nech $G$ je konečná cyklická grupa a nech $a$ je jej ľubovoľný generátor. Teda $G = [a] = \{a^n \mid n \in Z\}$ na základe vety 5.4. Ak $r(a) = \infty$, tak pre ľubovoľné $i, j \in Z,\ i < j$ máme $a^i \neq a^j$, pretože rovnosť $a^i = a^j$ by viedla k sporu $a^{j-i} = e$. Pretože ale $G$ je konečná, nemôže pozostávať z nekonečne mnoho navzájom rôznych mocnín, preto $r(a) \neq \infty$, a teda $r(a) = k$ pre nejaké kladné celé číslo $k$. Ukážeme, že $G = \{e, a, a^2, \ldots, a^{k-1}\}$. Nech $n \in Z$. K číslam $n, k$ existuje jediná dojica celých čísel $q, r$, že $n = kq+r,\ 0 \leq r < k$. Potom $a^n = a^{kq+r} = (a^k)^q \cdot a^r = e^q \cdot a^r = a^r \in G$, teda $G = \{a^n \mid n \in Z\} = \{e, a, a^2, \ldots, a^{k-1}\}$. Pre $i, j \in \{1, \ldots, k\},\ i < j$ sú pritom prvky $a^i, a^j$ už rôzne, pretože rovnosť $a^i = a^j$ by opäť viedla k $a^{j-i} = e$, pričom $0 < j - i < k$, čo by bolo v spore s tým, že $r(a) = k$. Teda $|G| = k = r(a)$. □

Pojem rádu prvku resp. rádu grupy ilustrujeme v nasledujúcich známych príkladoch.

**5.8 Príklad.** a) Už v úvode tejto kapitoly sme ukázali, že grupa $(K_n, \cdot)$ komplexných $n$-tých odmocnín z jednej je cyklická s generátorom $x_1 = \cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}$. Platí $r(x_1) = n = |K_n|$ a $K_n = \{x_1, x_1^2, \ldots, x_1^{n-1}, 1\}$.

b) Grupa $(C_n, \circ)$ rotácií pravidelného $n$-uholníka s generátorom $r_1$ (rotácia o uhol $\frac{2\pi}{n}$), ktorá je s $(K_n, \cdot)$ izomorfná, má generátor $r_1$, pričom opäť $r(r_1) = n = |C_n|$ a $C_n = \{r_1, r_1^2, \ldots, r_1^{n-1}, \mathrm{id}\}$.

**5.9 Príklad.** a) V grupe $(Z_n, \oplus)$ platí $2 = 1 \oplus 1 = 2 \times 1,\ 3 = 1 \oplus 1 \oplus 1 = 3 \times 1, \ldots, n = n \times 1 = 0$, teda je cyklická s generátorom 1, pričom $r(1) = n = |Z_n|$.

b) Aj nekonečná grupa $(Z, +)$ je zrejme cyklická s generátorom 1, avšak rád prvku 1 v grupe $(Z, +)$ je $\infty$.

Nasledujúca veta potvrdzuje, ze cyklické grupy v príkladoch 5.8a),b) a 5.9a) sú izomorfné a že $(Z_n, \oplus)$ je (až na izomorfizmus) jediná $n$-prvková cyklická grupa. Možno pritom ukázať, že ak $n$ je prvočíslo, tak každý prvok grupy $(Z_n, \oplus)$ rôzny od 0 má rád $n$, a teda je jej generátorom (cvičenie 2). Podobne, $(Z, +)$ je (až na izomorfizmus) jediná cyklická grupa s generátorom rádu $\infty$. Pre rád takejto grupy používame označenie $\aleph_0$.

5.10 Veta. *Nech $(G, \cdot)$ je cyklická grupa s generátorom $a$.*
*a) Ak generátor $a$ má konečný rád $n$, tak grupa $(G, \cdot)$ je izomorfná s grupou $(Z_n, \oplus)$.*
*b) Ak generátor $a$ má rád $\infty$, tak grupa $(G, \cdot)$ je izomorfná s grupou $(Z, +)$.*

Dôkaz. a) Nech $G = [a]$ a $r(a) = n$. Potom (pozri dôkaz vety 5.7) $G = \{a, a^2, \ldots, a^{n-1}, e\}$. Z uvedeného vyplýva, že zobrazenie $f : Z_n \to G$ definované predpisom $f(i) = a^i,\ i = 0, 1, \ldots, n-1$, je bijektívne. Teraz overíme, že zobrazenie $f$ zachováva grupové operácie, t.j. že

$$f(i \oplus j) = f(i) \cdot f(j).$$

Pretože $i \oplus j = i + j - nq$, pričom $0 \leq i \oplus j < n$ (pozri kap. 3), tak

$$f(i \oplus j) = a^{i \oplus j} = a^{i+j-nq} = a^i \cdot a^j \cdot (a^n)^{-q} = a^i \cdot a^j \cdot e = a^i \cdot a^j = f(i) \cdot f(j).$$

Teda $f$ je izomorfizmus grupy $(Z_n, \oplus)$ na grupu $(G, \cdot)$.

b) Ak $G = [a] = \{a^i \mid a \in Z\}$ pričom $r(a) = \infty$, tak všetky mocniny $a^i,\ i \in Z$, sú navzájom rôzne (pozri opäť dôkaz vety 5.7). Preto zobrazenie $g : Z \to G$ definované predpisom $g(i) = a^i,\ i \in Z$ je bijektívne. Pre každé $i, j \in Z$ naviac evidentne platí

$$g(i + j) = a^{i+j} = a^i \cdot a^j = g(i) \cdot g(j),$$

teda $g$ je izomorfizmus grupy $(Z, +)$ na grupu $(G, \cdot)$. □

Posledné tvrdenie tejto kapitoly hovorí o tom aká je štruktúra všetkých podgrúp danej cyklickej grupy.

VETA 5.11. *Každá podgrupa cyklickej grupy je cyklická.*

DÔKAZ. Nech $G = [a]$ je cyklická grupa, t.j. $G = \{a^n \mid n \in Z\}$ a nech $H$ je jej podgrupa. Ak $H = \{e\}$, tak $H$ je cyklická. Ak $H$ je netriviálna, tak musí existovať najmenšie nenulové prirodzené číslo $k$ s vlastnosťou $a^k \in H$. Je zrejmé, že potom $[a^k] \subseteq H$. Ukážeme obrátenú inklúziu. Nech $a^m \in H$. Číslo $m$ možno vyjadriť v tvare $m = k \cdot q + r$, kde $0 \leq r < k$. Potom $a^r = a^{m-kq} = a^m \cdot a^{-kq} = a^m \cdot [(a^k)^q]^{-1} \in H$, pretože $a^m, (a^k)^q \in H$. Avšak $a^r \in H$ implikuje $r = 0$, lebo $k$ je najmenšie prirodzené číslo také, že $a^k \in H$. Čiže $a^m = (a^k)^q \in [a^k]$. Tým sme ukázali, že $H \subseteq [a^k]$. Teda $H = [a^k]$ a veta je dokázaná. □

## Cvičenia

**1.** Nech $k$ je rád prvku $a$ v grupe $(G, \cdot)$. Dokážte, že $a^n = e$ vtedy a len vtedy, keď číslo $n$ je násobkom čísla $k$.

**2.** Ukážte, že ak $n$ je prvočíslo, tak každý prvok grupy $(Z_n, \oplus)$ rôzny od 0 je jej generátorom.

**3.** Nájdite všetky generátory cyklických grúp $(Z_8, \oplus)$ a $(Z_{12}, \oplus)$.

**4.** Nájdite všetky podgrupy grúp $(Z_8, \oplus)$ a $(Z_{12}, \oplus)$ a ich generátory.

**5.** Určte všetky izomorfizmy medzi cyklickými grupami $(Z_n, \oplus)$, $(K_n, \cdot)$ a $(C_n, \circ)$ pre $n = 8$ a $n = 12$.

**6.** Zistite, či nasledujúca grupa je cyklická. Ak áno, nájdite všetky jej generátory a určte ich rád:

a) $(Z_2 \times Z_3, \oplus)$
b) $(Z_3 \times Z_4, \oplus)$
c) $(Z_2 \times Z_4, \oplus)$
d) $(Z_4 \times Z_4, \oplus)$
e) $(Z_2 \times Z_3 \times Z_4, \oplus)$
f) $(Z_2 \times Z_3 \times Z_5, \oplus)$
g) $(Z_7 \setminus \{0\}, \cdot)$
h) $(\{2^n \mid n \in Z\}, \cdot)$
i) $(\{1, -1, i, -i\}, \cdot)$

**7.** Ukážte, že v grupe majú prvok a jeho inverzný prvok vždy ten istý rád.

**8.** Ukážte, že v grupe $(G, \cdot)$ majú prvok $a \cdot b$ a prvok $b \cdot a$ ten istý rád pre ľubovoľné $a, b \in G$.

**9.** Ukážte, ze prvok $a^k$ je generátorom $n$-prvkovej cyklickej grupy $[a]$ práve vtedy, keď čísla $k, n$ sú nesúdeliteľné.

**10.** Nájdite podgrupu $(R \times R, +)$, ktorá
a) je cyklická
b) nie je cyklická (aspoň tri).

**11.** Nájdite všetky cyklické podgrupy
a) grupy symetrií štvorca $D_4$;
b) dihedrálnej grupy (symetrií pravidelného $n$-uholníka) $D_n$ ;
c) grupy symetrií kocky;
d) symetrickej grupy $S_3$
a určte všetky ich generátory.

## 6. Grupy transformácií

V tejto časti sa budeme podrobnejšie zaoberať grupami transformácií množiny $\boldsymbol{n} = \{1, 2, \ldots, n\}$. Najskôr ukážeme, že ak sú množiny $A$, $B$ ekvivalentné, tak príslušné grupy všetkých transformácií $T(A)$, $T(B)$ sú izomorfné.

Operáciu skladania zobrazení budeme často označovať multiplikatívne a teda používať aj príslušnú terminológiu, ako napr. súčin zobrazení a pod. Ak nemôže prísť k nedorozumeniu, tak sa niekedy pri výpočtoch vynecháva aj symbol operácie.

6.1 Lema. *Ak existuje bijekcia množiny $A$ na množinu $B$, tak grupy transformácií $T(A)$ a $T(B)$ sú izomorfné.*

Dôkaz. Nech zobrazenie $f : A \to B$ je bijekcia. Definujme zobrazenie $\varphi : T(A) \to T(B)$, $\varphi(g) = fgf^{-1}$ (obrázok 1), kde $g \in T(A)$ je ľubovoľná transformácia množiny $A$.

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle \varphi(g)} \\ A & \xleftarrow[\ f^{-1}\ ]{} & B \end{array}$$

Obr. 1

Ak $\varphi(g_1) = \varphi(g_2)$, tak $fg_1f^{-1} = fg_2f^{-1}$, z čoho (po krátení) dostávame $g_1 = g_2$ čo znamená, že zobrazenie $\varphi$ je injekcia. Ak $h \in T(B)$, tak $f^{-1}hf \in T(A)$ a $\varphi(f^{-1}hf) = ff^{-1}hff^{-1} = h$, teda $\varphi$ je aj surjekcia. Zobrazenie $\varphi$ je teda bijekcia $T(A)$ na $T(B)$.

Pre ľubovoľné transformácie $g_1, g_2 \in T(A)$ je

$$\varphi(g_1g_2) = fg_1g_2f^{-1} = fg_1f^{-1}fg_2f^{-1} = \varphi(g_1)\varphi(g_2),$$

teda $\varphi$ je izomorfné zobrazenie grupy $T(A)$ na grupu $T(B)$. □

Z predchádzajúvej lemy vyplýva, že pri skúmaní grúp transformácií konečných množín sa môžeme obmedziť na symetrické grupy $S_n$ a na ich podgrupy (t.j. na grupy transformácií množiny $\boldsymbol{n}$.

6.2 Definícia. Ak o permutácii $f \in S_n$ platí

$$f(a_1) = a_2,\ f(a_2) = a_3,\ \ldots,\ f(a_{m-1}) = a_m,\ f(a_m) = a_1,$$

pričom čísla $a_1, \ldots, a_m \in \boldsymbol{n}$ $(m \leq n)$ sú navzájom rôzne a ak pre každé číslo $a \in \boldsymbol{n} \setminus \{a_1, \ldots a_m\}$ platí $f(a) = a$ hovoríme, že $f$ je cyklická permutácia (stručne cyklus). Píšeme $f = (a_1\, a_2\, \ldots\, a_m)$ a číslo $m$ nazývame dĺžkou cyklu $(a_1\, a_2\, \ldots\, a_m)$.

6.3 Príklad. Permutácia $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ je cyklus dĺžky 3. Môžeme ho zapísať v tvare (2 5 3) alebo (5 3 2) alebo (3 2 5).

Ak permutácia $f \in S_n$ je identita, tak obyčajne píšeme $f = \mathrm{id}_{\boldsymbol{n}}$ (alebo $f = \mathrm{id}$).

6.4 Definícia. O cykloch $(a_1 \ldots a_r)$, $(b_1 \ldots b_s) \in S_n$ hovoríme, že sú disjunktné, ak sú disjunktné množiny $\{a_1, \ldots, a_r\}$, $\{b_1, \ldots, b_s\}$.

6.5 Lema. *Rád cyklu v grupe $S_n$ sa rovná jeho dĺžke.*

Dôkaz. Nech $f = (a_1\, a_2\, \ldots\, a_m) \neq \mathrm{id}_{\boldsymbol{n}}$. Potom

$$f^2(a_m) = a_2, \quad f^3(a_m) = a_3, \quad \ldots, \quad f^{m-1}(a_m) = a_{m-1}$$

(podrobne sa presvedčte), čo znamená, že permutácie $f$, $f^2$, $\ldots$, $f^{m-1}$ nie sú identické zobrazenia. Zrejme ale $f^m = \mathrm{id}_{\boldsymbol{n}}$, teda rád cyklu $f = (a_1\, a_2\, \ldots\, a_m)$ v grupe $S_n$ je $m$. □

6.6 Lema. *Ak $f = (a_1 \ldots a_r)$, $g = (b_1 \ldots b_s)$ sú disjunktné cykly, tak $f \cdot g = g \cdot f$.*

Dôkaz. Ak $c \in \{a_1, \ldots a_r\}$, tak $f(g(c)) = f(c)$ (lebo $g(c) = c$) a tiež $g(f(c)) = f(c)$ (lebo $f(c) \in \{a_1, \ldots, a_r\}$).

Ak $c \in \{b_1, \ldots, b_s\}$, tak analogicky dostávame, že $f(g(c)) = g(c) = g(f(c))$.

Ak $c \in \boldsymbol{n} \setminus (\{a_1, \ldots, a_r\} \cup \{b_1, \ldots, b_s\})$, tak zrejme $f(g(c)) = c = g(f(c))$. □

6.7 Dôsledok. *Nech $f = (a_1 \ldots a_r)$, $g = (b_1 \ldots b_s)$ sú disjunktné cykly v $S_n$. Potom rád permutácie $f \cdot g$ je najmenší spoločný násobok dĺžok cyklov $f$, $g$.*

Dôkaz. Pretože v grupe $S_n$ sú cykly $f$, $g$ sú disjunktné, tak $f \cdot g = g \cdot f$ a teda podľa vety 5.3 je $(f \cdot g)^m = f^m \cdot g^m$ (pre každé celé číslo $m$). Preto $(f \cdot g)^m = \mathrm{id}_{\boldsymbol{n}}$ práve vtedy, keď $f^m = \mathrm{id}_{\boldsymbol{n}}$ a $g^m = \mathrm{id}_{\boldsymbol{n}}$, t.j. práve vtedy, keď $m$ je spoločný násobok dĺžok cyklov $f$, $g$. Rád permutácie $f \cdot g$ je teda najmenší spoločný násobok dĺžok cyklov $f$, $g$. □

Poznámka. Predchádzajúci dôsledok je možné prirodzeným spôsobom zovšeobecniť pre ľubovoľný konečný počet navzájom disjunktných cyklov.

6.8 Veta. *Každú permutáciu $f \in S_n$ rôznu od identickej permutácie je možné napísať v tvare súčinu disjunktných cyklov.*

Dôkaz. Nech $x, y \in \boldsymbol{n}$ a nech $f \in S_n$. Budeme písať $x \sim y$, ak existuje $m \in Z$, že $f^m(x) = y$. Zrejme pre každé $x \in \boldsymbol{n}$ je $x \sim x$ (lebo $f^0(x) = x$). Ak $x \sim y$ (t.j. existuje $m \in Z$, že $f^m(x) = y$), tak $y \sim x$ (lebo $f^{-m}(y) = x$). Nakoniec, ak $x \sim y$ a $y \sim z$, t.j. ak existujú $m, n \in Z$, že $f^m(x) = y$ a $f^n(y) = z$, tak $z = f^n(y) = f^n(f^m(x)) = f^{n+m}(x)$, teda $x \sim z$. Z uvedeného vyplýva, že relácia $\sim$ je na množine $\boldsymbol{n}$ reláciou ekvivalencie a vytvára teda rozklad $\boldsymbol{n}/_\sim$ množiny $\boldsymbol{n}$. Ak $x \in \boldsymbol{n}$, tak prvky $x, f(x), f^2(x), \ldots$ nemôžu byť všetky rôzne (lebo $\boldsymbol{n}$ je konečná množina). Existuje teda také $m \in N^+$, že $f^m(x) = x$ (lebo ak napr. $f^i(x) = f^j(x)$, $j > i$, tak $f^{j-i}(x) = x$, $j - i \in N^+$). Nech $p \in N^+$ je najmenšie také, že $f^p(x) = x$. Prvky $x, f(x), f^2(x), \ldots, f^{p-1}(x)$ sú navzájom rôzne ( v opačnom prípade by existovalo číslo $k \in N^+$, $k < p$, že $f^k(x) = x$ a to by bol spor). Pre každé $i, j \in \{1, 2, \ldots, p-1\}$ je $f^i(x) \sim f^j(x)$ a množina $\{x, f(x), \ldots, f^{p-1}(x)\}$ tvorí jednu triedu rozkladu danú reláciou $\sim$.

Cyklus $(x\, f(x) \ldots f^{p-1}(x))$ označme $g_j$. Potom pre $a \in \{x, f(x), \ldots, f^{p-1}\}$ je $g_j(a) = f(a)$ a pre $a \notin \{x, f(x), \ldots, f^{p-1}\}$ je $g_j(a) = a$.

Množina $\boldsymbol{n}$ je konečná a teda aj jej rozklad $\boldsymbol{n}/_\sim$ tvorí konečný počet tried $T_1, T_2, \ldots, T_r$. Každá trieda $T_i$ určuje cyklus $g_i$, pre ktorý platí

$$g_i(a) = \begin{cases} f(a), & \text{pre } a \in T_i, \\ a, & \text{pre } a \notin T_i. \end{cases}$$

Pretože triedy rozkladu $\boldsymbol{n}/_\sim$ sú navzájom disjunktné, tak aj cykly $g_1, g_2, \ldots, g_r$ sú navzájom disjunktné.

Treba ešte ukázať, že $f = g_1 \cdot g_2 \cdot \ldots \cdot g_r$. Nech $a \in \boldsymbol{n}$. Potom existuje $j \in \{1, 2, \ldots, r\}$, že $a \in T_j$. Z toho vyplýva, že aj $f(a) \in T_j$ a platí $f(a) = g_j(a)$. Preto

$$(g_1 \cdot \ldots \cdot g_{j-1} \cdot g_j \cdot g_{j+1} \cdot \ldots \cdot g_r)(a) = g_j(a) = f(a),$$

čo znamená, že $f = g_1 \cdot g_2 \cdot \ldots \cdot g_r$. □

Dôkaz predchádzajúcej vety dáva aj návod, ako hľadať rozklad permutácie na disjunktné cykly. Nech $f \in S_9$, $f = \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 5&1&7&9&2&6&3&4&8 \end{smallmatrix}\right)$. Pretože $f(1) = 5$, $f^2(1) = 2$ a $f^3(1) = 1$, tak jeden z hľadaných cyklov je cyklus $(1\,5\,2)$. Zvolíme ďalší „nezaradený“ prvok, napr. 3. V tomto prípade $f(3) = 7$ a $f^2(3) = 3$, preto ďalším cyklom je cyklus $(3\,7)$. Analogicky nájdeme cyklus $(4\,9\,8)$. Teda

$$f = (1\,5\,2) \cdot (3\,7) \cdot (4\,9\,8).$$

Cyklus dĺžky 1, t.j. cyklus (6) sme v zápise rozkladu vynechali, lebo reprezentuje identické zobrazenie.

6.9 Príklad. Dané sú permutácie $f, g \in S_7$,

$$f = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 3&1&7&5&2&4&6 \end{pmatrix}, \qquad g = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 4&1&5&7&6&3&2 \end{pmatrix}.$$

Nájdite permutáciu $h \in S_7$, pre ktorú $f^{80} \cdot h = g^{130}$.

Riešenie. Pri riešení danej rovnice využijeme, že $S_7$ je grupa (operáciou je skladanie zobrazení, neutrálnym prvkom je $\mathrm{id}_{\boldsymbol{7}}$ a inverzným prvkom k permutácii $t$ je inverzné zobrazenie $t^{-1}$) a môžeme teda používať známe pravidlá pre počítanie s mocninami.

Permutácia $f$ je cyklus dĺžky 7, teda

$$f^{80} = f^{7\cdot 11+3} = (f^7)^{11} \cdot f^3 = \mathrm{id}_{\boldsymbol{7}}^{11} \cdot f^3 = f^3 = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 6&7&4&1&3&2&5 \end{pmatrix}.$$

Permutáciu $g$ napíšeme ako súčin disjunktných cyklov: $g = (1\,4\,7\,2) \cdot (3\,5\,6)$. Rád permutácie $g$ je $\mathrm{n}(4, 3) = 12$. Potom

$$g^{130} = (g^{12})^{10} \cdot g^{10} = \mathrm{id}_{\boldsymbol{7}}^{10} \cdot g^{10} = g^{10}.$$

Ďalej, pretože $g^{12} = \mathrm{id}_{\boldsymbol{7}}$, tak $g^{10} = g^{-2} = (g^{-1})^2$, teda

$$g^{130} = g^{10} = (g^{-1})^2 = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 7&4&5&2&6&3&1 \end{pmatrix}.$$

Rovnicu $f^{80} \cdot h = g^{130}$ môžeme teda zapísať v tvare

$$\begin{pmatrix} 1&2&3&4&5&6&7 \\ 6&7&4&1&3&2&5 \end{pmatrix} \cdot h = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 7&4&5&2&6&3&1 \end{pmatrix}.$$

Jej riešením je (pozri vetu 2.27) permutácia: $\begin{pmatrix} 1&2&3&4&5&6&7 \\ 2&3&7&6&1&5&4 \end{pmatrix}$.

6.10 Definícia. Cyklickú permutáciu dĺžky 2 voláme transpozícia.

6.11 Veta. *Každú permutáciu množiny $\boldsymbol{n}$ je možné rozložiť na súčin transpozícií.*

Dôkaz. Podľa vety 6.8 môžeme ľubovoľnú permutáciu $f \in S_n$ rozložiť na súčin (disjunktných) cyklov. Každý cyklus $(a_1\, a_2\, \ldots\, a_k)$ môžeme rozložiť na súčin transpozícií napríklad takto:

$$(a_1\, a_2\, \ldots a_k) = (a_1\, a_k) \cdot (a_1\, a_{k-1}) \cdot \ldots \cdot (a_1\, a_3) \cdot (a_1\, a_2).$$

Po dosadení do rozkladu permutácie na cykly dostávame rozklad permutácie na súčin transpozícií. □

Nech $f$ je permutácia množiny $\boldsymbol{n}$ a $a, b \in \boldsymbol{n}$. Usporiadanú dvojicu $(f(a), f(b))$ budeme volať *inverzia* permutácie $f$ (alebo v permutácii $f$), ak $a < b$ a $f(a) > f(b)$. Napríklad inverzie permutácie $f = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 3&4&1&5&2 \end{smallmatrix}\right)$ sú usporiadané dvojice $(3,1)$, $(3,2)$, $(4,1)$, $(4,2)$, $(5,2)$. Jej rozklad na transpozície je $f = (1\,3) \cdot (2\,5) \cdot (2\,4)$, ale aj napríklad $f = (1\,3) \cdot (1\,2) \cdot (1\,5) \cdot (1\,2) \cdot (2\,4)$. Nasledujúca lema ukazuje súvis medzi počtom inverzií danej permutácie a počtom transpozícií (v jej rozklade na transpozície).

6.12 Lema. *Permutácia $f$ množiny $\boldsymbol{n}$ je súčinom párneho počtu transpozícií práve vtedy, keď obsahuje párny počet inverzií.*

Dôkaz. Všimnime si, že ak permutácia $f$ je identické zobrazenie, tak počet jej inverzií je 0. Stačí teda ukázať, že pri vynásobení permutácie $f$ (zľava) transpozíciou $t = (a\, b)$ sa zmení počet inverzií o nepárne číslo. V permutácii $f$ označme $a = f(i)$ a $b = f(j)$, t.j. $f = \begin{pmatrix} \ldots & i & \ldots & j & \ldots \\ \ldots & a & \ldots & b & \ldots \end{pmatrix}$. Potom

$$(a\, b) \cdot \begin{pmatrix} \ldots & i & \ldots & j & \ldots \\ \ldots & a & \ldots & b & \ldots \end{pmatrix} = \begin{pmatrix} \ldots & i & \ldots & j & \ldots \\ \ldots & b & \ldots & a & \ldots \end{pmatrix}.$$

Vynásobením permutácie $f$ transpozíciou $t = (a\, b)$ dostaneme teda permutáciu, ktorá sa od permutácie $f$ líši len tým, že v jej zápise sú (v druhom riadku) vymenené medzi sebou čísla $a$, $b$ (t.j. obrazy prvkov $i$, $j$). Určme pre každé $k \in \boldsymbol{n}$, ako táto zmena ovplyvní počet inverzií medzi usporiadanými dvojicami utvorený mi z prvkov $f(k)$, $f(i)$, $f(j)$.

a) Pre $k \in \boldsymbol{n}$, $i < k < j$ v permutácii $t \cdot f$ buď dve inverzie pribudnú, buď dve ubudnú, buď ostane počet nezmenený (jedna pribudne a jedna ubudne).

b) Pre $k \in \boldsymbol{n}$, $k < i$ alebo $k > j$ ostáva počet inverzií v $t \cdot f$ zrejme nezmenený.

Ďalej si všimnime, že ak $(a, b)$ je v $f$ inverzia, tak $(b, a)$ nie je v $t \cdot f$ inverzia a naopak.

Z toho vyplýva, že celková zmena inverzií je nepárna. Ak teda

$$f = t_n \cdot t_{n-1} \cdot \ldots \cdot t_2 \cdot t_1,$$

kde $t_1$, $t_2$, …, $t_n$ sú transpozície a celkový počet inverzií permutácie $f$ je $r$, tak $r \equiv n \pmod 2$ (t.j. čísla $r$, $n$ majú rovnakú paritu). □

6.13 Definícia. Permutácia sa nazýva párna, ak je súčinom párneho počtu transpozícií a nazýva sa nepárna, ak je súčinom nepárneho počtu transpozícií.

6.14 Veta. *Množina všetkých párnych permutácií množiny* $\boldsymbol{n}$ *tvorí podgrupu grupy* $S_n$.

Dôkaz. Identické zobrazenie $\mathrm{id}_{\boldsymbol{n}}$ je párna permutácia a preto množina párnych permutácií je neprázdna. Ak $f$, $g$ sú párne permutácie, tak existujú transpozície $f_1, f_2, \ldots, f_{2r}, g_1, g_2, \ldots, g_{2s}$ také, že

$$f = f_1 \cdot f_2 \cdot \ldots \cdot f_{2r}, \quad g = g_1 \cdot g_2 \cdot \ldots \cdot g_{2s}.$$

Potom

$$f \cdot g^{-1} = f_1 \cdot f_2 \cdot \ldots \cdot f_{2r} \cdot g_{2s}^{-1} \cdot \ldots \cdot g_2^{-1} \cdot g_1^{-1}$$

je zrejme tiež párna permutácia, čo (podľa vety 2.24) znamená, že množina všetkých párnych permutácií je podgrupou grupy všetkých permutácií. □

Grupu všetkých párnych permutácií na množine $\boldsymbol{n}$, voláme *alternujúca grupa n-tého stupňa* a označujeme ju $A_n$.

6.15 Dôsledok. *Rád alternujúcej grupy n-tého stupňa je* $|A_n| = \frac{n!}{2}$.

Dôkaz. Ukážeme, že z celkového počtu $n!$ $(n > 1)$ permutácií v $S_n$ je $\frac{n!}{2}$ párnych. Označme $B$ množinu všetkých nepárnych permutácií. Ukážeme, že zobrazenie $\varphi : A_n \to B$, $\varphi(f) = (1\,2) \cdot f$ je bijekcia.

Pretože v grupe platí zákon o krátení, tak z rovnosti $(1\,2) \cdot f_1 = (1\,2) \cdot f_2$ vyplýva $f_1 = f_2$ a teda $\varphi$ je injekcia.

Nech $g \in B$. Potom (v grupe $S_n$) má rovnica $(1\,2) \cdot f = g$ (s neznámou $f$) riešenie a naviac, $f$ musí byť párna permutácia. Teda pre $g \in B$ existuje $f \in A_n$, že $\varphi(f) = g$, čo znamená, že zobrazenie $\varphi$ je aj surjekcia. □

## Cvičenia

**1.** Dané sú permutácie $f = \begin{pmatrix} 1&2&3&4&5&6 \\ 3&1&2&6&4&5 \end{pmatrix}$, $g = \begin{pmatrix} 1&2&3&4&5&6 \\ 6&1&5&3&4&2 \end{pmatrix}$, $h = \begin{pmatrix} 1&2&3&4&5&6 \\ 1&3&4&5&2&6 \end{pmatrix}$, $k = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 6&4&5&7&3&1&2 \end{pmatrix}$, $l = \begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 6&1&3&9&7&10&8&5&4&2 \end{pmatrix}$, $m = (1\,4)(1\,2\,3)(4\,5)(1\,4)$, $n = (1\,2\,3\,4\,5)(6\,7)(1\,3\,5\,7)(1\,6\,3)$.

a) Zapíšte každú z daných permutácií ako súčin disjunktných cyklov.

b) Zapíšte každú z daných permutácií ako súčin transpozícií.

c) Určte, ktorá z daných permutácií je párna.

d) Určte rád daných permutácií.

**2.** Nech $a = \begin{pmatrix} 1&2&3&4&5 \\ 5&3&4&2&1 \end{pmatrix}$, $b = \begin{pmatrix} 1&2&3&4&5 \\ 4&1&3&5&2 \end{pmatrix}$, $c = \begin{pmatrix} 1&2&3&4&5 \\ 1&3&2&5&4 \end{pmatrix}$.

a) Určte rády prvkov $a, b, c$.

b) Určte prvky $a^{195}$, $b^{-84}$, $(ab^2)^{-3}$.

c) Určte prvky $x, y$, pre ktoré platí $bxa = c$, $ayb = c$.

**3.** Určte dvojprvkovú a trojprvkovú grupu transformácií na množine $\{1, 2, 3\}$.

**4.** Zistite, či nasledujúce množiny sú podgrupy grupy $(S_4, \cdot)$.

a) $\{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$,

b) $\{(1), (1\,3), (2\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3\,4), (1\,4\,3\,2)\}$.

**5.** Napíšte tabuľku pre operáciu alternujúcej grupy $A_4$.

**6.** Ukážte, že grupa $(S_3, \cdot)$ je generovaná množinou $\{(1\,2),\ (1\,2\,3)\}$.

**7.** Určte vymenovaním podgrupu

a) grupy $S_3$ generovanú množinou $\{(1\,2),\ (2\,3)\}$,

b) grupy $S_4$ generovanú množinou $\{(1\,3),\ (1\,4)\}$.

**8.** V $S_9$ riešte rovnicu

a) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&1&6&8&9&2&4&7&5 \end{pmatrix} \cdot f = \begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&4&9&6&8&5&1&2&7 \end{pmatrix}^{223}$,

b) $f \cdot \begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&4&9&6&8&5&1&2&7 \end{pmatrix} = \begin{pmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&1&6&8&9&2&4&7&5 \end{pmatrix}^{-146}$.

**9.** V $S_{10}$ riešte rovnicu

a) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 7&9&8&5&6&3&10&4&2&1 \end{pmatrix} \cdot f = \begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 9&1&7&5&10&8&2&4&3&6 \end{pmatrix}^{154}$,

b) $\begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 9&1&7&5&10&8&2&4&3&6 \end{pmatrix} \cdot f = \begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 7&9&8&5&6&3&10&4&2&1 \end{pmatrix}^{88}$.

**10.** Dokážte, že rád ľubovoľného prvku grupy $S_{10}$ je najviac 30.

## 7. Rozklad podľa podgrupy. Lagrangeova veta

V kapitole 1 sme zaviedli pojem kongruencie podľa modulu $m$ na množine $Z$ celých čísel. Túto kongruenciu môžeme chápať aj v nasledovnom zmysle. Zvoľme pre grupu $(Z,+)$ všeobecné označenie $(G,\cdot)$ a označme jej podgrupu $mZ = \{m\cdot k \mid k \in Z\}$ symbolom $H$. Vidíme, že $a \equiv b \pmod m$ práve vtedy, keď $a\cdot b^{-1} \in H$. To nás privádza k zovšeobecnenému pojmu *kongruencie podľa podgrupy* $H$ pre ľubovoľnú grupu $G$ a jej podgrupu $H$.

7.1 Definícia. *Nech $(G,\cdot)$ je grupa a $H$ jej podgrupa. O prvkoch $a,b \in G$ budeme hovoriť, že $a$ je sprava kongruentné s $b$ podľa podgrupy $H$ a písať $a \equiv_p b(H)$, ak $a\cdot b^{-1} \in H$. Podobne, budeme hovoriť, že $a$ je zľava kongruentné s $b$ podľa $H$ a písať $a \equiv_l b\ (H)$, ak $a^{-1}\cdot b \in H$. Relácie $\equiv_p (H)$ a $\equiv_l (H)$ nazveme pravá a ľavá kongruencia podľa podgrupy $H$.*

7.2 Veta. *Nech $H$ je podgrupa grupy $G$.*

*a) Pravá (resp. ľavá) kongruencia podľa podgrupy $H$ je relácia ekvivalencie na $G$.*

*b) Trieda ekvivalencie pravej (resp. ľavej) kongruencie podľa podgrupy $H$ obsahujúca prvok $a$ je $\{h\cdot a \mid h\in H\} = Ha$ (resp. $\{a\cdot h \mid h\in H\} = aH$).*

*c) $|Ha| = |H| = |aH|$ pre všetky $a \in G$.*

Dôkaz. Urobíme ho pre pravé kongruencie podľa podgrupy $H$ (pre ľavé je dôkaz analogický) a budeme pritom skrátene písať $a \equiv b$ namiesto $a \equiv_p b(H)$.

a) Nech $a,b,c \in G$. Potom $a \equiv a$, pretože $a\cdot a^{-1} = e \in H$; teda $\equiv$ je reflexívna relácia na $G$. Symetrickosť relácie $\equiv$ ukazuje nasledujúci reťazec implikácií:

$$a \equiv b \Rightarrow a\cdot b^{-1} \in H \Rightarrow (a\cdot b^{-1})^{-1} \in H \Rightarrow b\cdot a^{-1} \in H \Rightarrow b \equiv a.$$

Nech teraz $a \equiv b$ a $b \equiv c$, t.j. $a\cdot b^{-1} \in H$ a $b\cdot c^{-1} \in H$. Potom $a\cdot c^{-1} = (a\cdot b^{-1})\cdot(b\cdot c^{-1}) \in H$, t.j. $a \equiv c$. Teda $\equiv$ je aj tranzitívna, čiže je relácia ekvivalencie na $G$.

b) Trieda ekvivalencie obsahujúca prvok $a \in G$ je

$$\{x\in G \mid x\equiv a\} = \{x\in G \mid x\cdot a^{-1}\in H\} = \{x\in G \mid x\cdot a^{-1} = h\in H\} = \\ = \{x\in G \mid \exists h\in H;\ x = h\cdot a\} = \{h\cdot a \mid h\in H\} = Ha.$$

c) Ukážeme, že zobrazenie $f : Ha \to H$ dané predpisom $f(h\cdot a) = h$ je bijekcia. Každý prvok $h \in H$ má v zobrazení $f$ vzor $h\cdot a \in Ha$, teda $f$ je evidentne surjektívne zobrazenie. Nech teraz $f(h_1\cdot a) = f(h_2\cdot a)$, t.j. $h_1 = h_2$. Potom triviálne $h_1\cdot a = h_2\cdot a$, teda $f$ je injektívne. Veta je dokázaná. □

7.3 Definícia. *Nech $H$ je podgrupa grupy $G$. Triedy ekvivalencie pravej (resp. ľavej) kongruencie podľa podgrupy $H$ na $G$ budeme nazývať pravé (resp. ľavé) triedy grupy $G$ podľa podgrupy $H$.*

7.4 Dôsledok. *Nech $H$ je podgrupa grupy $G$.*

*a) Množina $G$ je zjednotením pravých (resp. ľavých) tried grupy $G$ podľa $H$.*

*b) Dve pravé (resp. ľavé) triedy grupy $G$ podľa $H$ sú alebo disjunktné alebo totožné.*

*c) Pre všetky $a,b \in G$ platí $Ha = Hb \Leftrightarrow a\cdot b^{-1} \in H$ a $aH = bH \Leftrightarrow a^{-1}\cdot b \in H$.*

*d) Ak $\mathcal{P}$ (resp. $\mathcal{L}$) je množina všetkých (po dvoch disjunktných) pravých (resp. ľavých) tried grupy $G$ podľa $H$, tak $|\mathcal{P}| = |\mathcal{L}|$.*

Dôkaz. a),b) sú priamymi dôsledkami 7.2 a). Rovnosť $Ha = Hb$ implikuje existenciu $h_1, h_2 \in H$ tak, že $h_1 \cdot a = h_2 \cdot b$. Potom $a \cdot b^{-1} = h_1^{-1} \cdot h_2 \in H$. Obrátene, ak $a \cdot b^{-1} = h_0 \in H$, tak $a = h_0 \cdot b$, a teda $Ha = Hb$ (overenie tejto rovnosti prenechávame na čitateľa ako cvičenie 1). Tým je ukázané c). Definujme teraz zobrazenie $f : \mathcal{P} \to \mathcal{L}$ predpisom $f(Ha) = a^{-1}H$. Zobrazenie $f$ je zrejme surjektívne. Ukážeme injektívnosť $f$. Nech $f(Ha) = f(Hb)$, t.j. $a^{-1}H = b^{-1}H$. Potom, podľa c), je $(a^{-1})^{-1} \cdot b^{-1} = a \cdot b^{-1} \in H$ a odtiaľ (opäť podľa c)) $Ha = Hb$. Teda $f$ je bijekcia a $|\mathcal{P}| = |\mathcal{L}|$. $\square$

Z tvrdenia 7.4 c) vzhľadom na definíciu 7.1 vyplýva, že

$$\forall a, b \in G;\ Ha = Hb \Leftrightarrow a \equiv_p b(H).$$

Tvrdenie 7.4 d) nám umožňuje uviesť nasledujúcu definíciu (pozri aj poznámku 5.6).

7.5 Definícia. *Kardinálne číslo $|\mathcal{P}| = |\mathcal{L}|$ množiny pravých (ľavých) tried grupy $G$ podľa podgrupy $H$ nazývame indexom podgrupy $H$ v grupe $G$ a označujeme $[G : H]$.*

Ak $G$ je komutatívna grupa, tak pravá a ľavá kongruencia podľa podgrupy $H$ sú totožné relácie, pretože platí

$$a \equiv_p b(H) \Leftrightarrow a \cdot b^{-1} \in H \Leftrightarrow (a \cdot b^{-1})^{-1} \in H \Leftrightarrow$$
$$\Leftrightarrow b \cdot a^{-1} \in H \Leftrightarrow a^{-1} \cdot b \in H \Leftrightarrow a \equiv_l b(H).$$

Každá pravá trieda komutatívnej grupy $G$ podľa podgrupy $H$ je teda súčasne aj ľavá trieda a $\mathcal{P} = \mathcal{L}$. Ak sú pravá a ľavá kongruencia podľa podgrupy $H$ totožné, hovoríme len o kongruencii podľa podgrupy $H$ a píšeme $a \equiv b(H)$. V takom prípade budeme hovoriť len o triedach grupy $G$ podľa podgrupy $H$ a zvyčajne budeme pre ne používať označenie pravých tried $Ha$. Množinu tried grupy $G$ podľa podgrupy $H$ budeme označovať $G/H$.

**7.6 Príklad.** Už v úvode tejto kapitoly sme naznačili, že kongruencia $\equiv$ modulo $m$ definovaná na grupe $(Z, +)$ v kapitole 1 je vlastne kongruencia podľa podgrupy $mZ$, kde $mZ = \{m \cdot k \mid k \in Z\}$ je podgrupa grupy $Z$. Systém zvyškových tried $\overline{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ (v inom označení $Z/\equiv_m$), ktorý vytvorila v kapitole 1 kongruencia modulo $m$ je totožný so systémom $Z/mZ$ tried grupy $Z$ podľa podgrupy $mZ$. Skutočne, podgrupa $mZ = mZ + 0$ je totožná so zvyškovou triedou $\overline{0}$ a triedy $mZ + 1,\ mZ + 2, \ldots,\ mZ + (m-1)$ grupy $Z$ podľa podgrupy $mZ$, ktoré sa z podgrupy $mZ$ získajú "posunutím pomocou operácie $+$", sú totožné postupne so zvyškovými triedami $\overline{1},\ \overline{2}, \ldots,\ \overline{m-1}$. Teda $\overline{Z}_m = Z/mZ$.

Nasledujúci príklad ukazuje, že pravá a ľavá kongruencia grupy $G$ podľa podgrupy $H$ (a teda aj pravý a ľavý rozklad $G$ podľa podgrupy $H$) môžu byť totožné aj v nekomutatívnej grupe $G$, avšak vo všeobecnosti to v nekomutatívnej grupe neplatí.

**7.7 Príklad.** Nech $(G,\cdot)=(S_3,\circ)$ a nech $H_1$ je cyklická podgrupa $G$ generovaná prvkom (123). Teda $H_1=\{(123),(132),\mathrm{id}\}$. Pravé triedy grupy $G$ podľa $H_1$ sú

$$H_1(123)=\{(132),\mathrm{id},(123)\}=H_1(132)=H_1\mathrm{id}=H_1,$$
$$H_1(12)=\{(13),(23),(12)\}=H_1(23)=H_1(13)$$

a ľavé triedy grupy $G$ podľa podgrupy $H_1$ sú

$$(123)H_1=\{(132),\mathrm{id},(123)\}=(132)H_1=\mathrm{id}H_1=H_1,$$
$$(12)H_1=\{(23),(13),(12)\}=(23)H_1=(13)H_1$$

(cvičenie 2). Čiže $\mathcal{P}=\{H_1,\{(13),(23),(12)\}\}=\mathcal{L}$, napriek tomu, že grupa $G$ je nekomutatívna – napr. $(12)\circ(23)=(123)\neq(132)=(23)\circ(12)$. V tomto prípade je totožnosť pravého a ľavého rozkladu zrejme dôsledkom faktu, že $[G:H_1]=2$. Preto aj pravá a ľavá kongruencia podľa $H_1$ sú totožné relácie. Vidíme, že $(123)\equiv(132) \pmod{H_1}$, $(132)\equiv\mathrm{id} \pmod{H_1}$, $(12)\equiv(23) \pmod{H_1}$ a $(23)\equiv(13) \pmod{H_1}$. Všimnime si ešte, že $|G|=[G:H_1]\cdot|H_1|=2\cdot 3$.

Nech teraz $H_2$ je cyklická podgrupa generovaná prvkom (12). Teda $H_2=\{(12),\mathrm{id}\}$. Pravé triedy grupy $G$ podľa $H_2$ sú

$$H_2(12)=\{\mathrm{id},(12)\}=H_2,$$
$$H_2(23)=\{(123),(23)\}=H_2(123),$$
$$H_2(13)=\{(132),(13)\}=H_2(132),$$

čiže $\mathcal{P}=\{H_2,\{(123),(23)\},\{(132),(13)\}\}$. Ľavé triedy grupy $G$ podľa $H_2$ sú

$$(12)H_2=\{\mathrm{id},(12)\}=H_2,$$
$$(23)H_2=\{(132),(23)\}=(132)H_2,$$
$$(13)H_2=\{(123),(13)\}=(123)H_2,$$

čiže $\mathcal{L}=\{H_2,\{(132),(23)\},\{(123),(13)\}\}$ (cvičenie 2). Zistili sme, že rozklad $\mathcal{P}$ grupy $G$ na pravé triedy podľa $H_2$ je rôzny od rozkladu $\mathcal{L}$ grupy $G$ na ľavé triedy podľa $H_2$. Teda aj pravá kongruencia $\equiv_p \pmod{H_2}$ je rôzna od ľavej kongruencie $\equiv_l \pmod{H_2}$. Vidíme napríklad, že $(23)\equiv_p(123) \pmod{H_2}$ a $(13)\equiv_p(132) \pmod{H_2}$, ale $(23)\not\equiv_l(123) \pmod{H_2}$ a $(13)\not\equiv_l(132) \pmod{H_2}$. Index $H_2$ v $G$ je $[G:H_2]=3$ a opäť vidíme, že $|G|=[G:H_2]\cdot|H_2|=3\cdot 2$.

7.8 Veta (**Langrangeova**). *Nech $G$ je grupa a $H$ je ľubovoľná jej podgrupa. Potom*

$$|G|=[G:H]\cdot|H|.$$

*V prípade konečnej grupy je teda jej rád násobkom rádu ľubovoľnej jej podgrupy.*

Dôkaz. Uvažujme o množine $\mathcal{P}=\{Ha\mid a\in G\}$ pravých tried grupy $G$ podľa podgrupy $H$. Utvorme karteziánsky súčin množín $\mathcal{P}$ a $H$. Prvkami $\mathcal{P}\times H$ sú všetky usporiadané dvojice tvaru $(Hx,h)$, kde $Hx$ je trieda zo systému $\mathcal{P}$ a $h$ je prvok podgrupy $H$. Pretože množina $G$ je zjednotením disjunktných pravých tried z uvažovanej množiny $\mathcal{P}$ (podľa 7.4a) ), každému prvku $a\in G$ možno priradiť práve jednu triedu $Hx$ zo systému $\mathcal{P}$, do ktorej patrí. Ak ale $a\in Hx$, znamená

to, že $a = h \cdot x$ pre nejaké $h \in H$. Pritom $h$ je jednoznačne určené prvkom $a$ a reprezentantom $x$ (pozri vetu 2.27). Preto môžeme korektne definovať zobrazenie $f : G \to \mathcal{P} \times H$, ktoré každému $a \in G$ priradí dvojicu $(Hx, h) \in \mathcal{P} \times H$, pričom platí $a = h \cdot x \in Hx$. Ukážeme, že zobrazenie $f$ je bijektívne.

Ak $a, b \in G,\ a \neq b$, tak alebo $a, b$ patria do tej istej triedy $Hx$ alebo existujú dve rôzne triedy $Hx \neq Hy$, že $a \in Hx,\ b \in Hy$. V prvom prípade $a = h_1 \cdot x,\ b = h_2 \cdot x$, pričom musí byť $h_1 \neq h_2$ (opak vedie k sporu $a = b$); teda $f(a) = (Hx, h_1) \neq (Hx, h_2) = f(b)$. V druhom prípade evidentne $f(a) \neq f(b)$, lebo $Hx \neq Hy$. Tým sme ukázali, že zobrazenie $f$ je injektívne.

Zvoľme ľubovoľnú dvojicu $(Hx, h) \in \mathcal{P} \times H$. Hľadáme k nej vzor $a \in G$ v zobrazení $f$. Položme $a = h \cdot x \in Hx$. Potom evidentne $f(a) = f(h \cdot x) = (Hx, h)$. Teda $f$ je aj surjektívne.

Pretože sme našli bijektívne zobrazenie množiny $G$ na množinu $\mathcal{P} \times H$, platí pre ich kardinálne čísla rovnosť $|G| = |\mathcal{P} \times H|$, odkiaľ (podľa definície súčinu kardinálnych čísel – pozri poznámku 5.6) dostávame $|G| = |\mathcal{P}| \cdot |H|$. Pretože $|\mathcal{P}| = [G : H]$ podľa definície 7.5, dostávame požadované tvrdenie $|G| = [G : H] \cdot |H|$.

Ak $G$ je konečná, kardinálne čísla $|G|,\ [G : H],\ |H|$ zapisujeme ako prirodzené čísla a môžeme teda povedať, že $|G|$ je násobkom čísla $|H|$ tak ako je to obvyklé v súvislosti s deliteľnosťou prirodzených čísel. □

Obrátené tvrdenie k Lagrangeovej vete však neplatí. Napríklad alternujúca grupa $A_4$ (cvičenie 5 predchádzajúcej kapitoly) má rád 12, ale nemá podgrupu rádu 6 (presvedčte sa).

Lagrangeova veta má viacero zaujímavých dôsledkov.

7.9 Dôsledok. *V konečnej grupe je rád každého prvku deliteľom rádu grupy.*

Dôkaz. Nech $|G| = n$ a nech $a \in G$. Uvažujme o cyklickej podgrupe $[a]$ grupy $G$. Podľa Lagrangeovej vety $|G| = [G : [a]] \cdot |[a]|$. Pretože podľa vety 5.7 je $|[a]| = r(a)$, dostávame ihneď požadované tvrdenie $n = [G : [a]] \cdot r(a)$. □

7.10 Dôsledok. *Každá grupa prvočíselného rádu je cyklická a každý jej prvok s výnimkou neutrálneho prvku je jej generátorom.*

Dôkaz. Nech $|G| = p$, kde $p$ je prvočíslo. Podľa dôsledku 7.9 pre rád ľubovoľného prvku $a \in G$ platí $r(a) \mid p$, t.j. $r(a) \in \{1, p\}$. Pretože $r(a) = 1$ len pre $a = e$, každý prvok $a \in G \setminus \{e\}$ má rád $p$. Potom ale $[a] = \{a, a^2, \ldots, a^{p-1}, e\} = G$, lebo $[a] \subseteq G$ a $|[a]| = p = |G|$. Teda $G$ je cyklická a každý prvok $a \in G \setminus \{e\}$ je jej generátorom. □

7.11 Dôsledok (**Malá Fermatova veta**). *Ak $p$ je prvočíslo a $a$ je celé číslo, tak*

$$a^p \equiv a \pmod{p}.$$

Dôkaz. Multiplikatívna grupa $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ nenulových zvyškových tried modulo $p$ (pozri 4.5) má $p-1$ prvkov $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. Nech $a$ je ľubovoľné celé číslo. Ak $a \equiv 0 \pmod{p}$, tak tvrdenie triviálne platí. Nech teda $a \not\equiv 0 \pmod{p}$, t.j. zvyšková trieda $\overline{a} \in \overline{Z}_p \setminus \{\overline{0}\}$. Podľa dôsledku 7.9 pre rád prvku $\overline{a}$ v grupe $(\overline{Z}_p \setminus \{\overline{0}\}, \odot)$ platí $r(\overline{a}) \mid p-1$, t.j. existuje prirodzené číslo $m$, že $r(\overline{a}) \cdot m = p-1$. Pretože $(\overline{a})^{r(\overline{a})} = \overline{1}$, dostávame $(\overline{a})^{p-1} = (\overline{a})^{r(\overline{a}) \cdot m} = [(\overline{a})^{r(\overline{a})}]^m = (\overline{1})^m = \overline{1}$. Teda $a^{p-1} \equiv 1 \pmod{p}$, odkiaľ po vynásobení číslom $a$ dostaneme požadovaný vzťah $a^p \equiv a \pmod{p}$. □

7.12 Dôsledok. *Každá štvorprvková grupa je izomorfná alebo s cyklickou grupou* $(Z_4, \oplus)$ *alebo s grupou symetrií obdĺžnika.*

Dôkaz. Nech $(G, \cdot)$ má 4 prvky $a, b, c, e$. Podľa dôsledku 7.9 platí, že $r(a), r(b), r(c) \in \{2, 4\}$. Ak niektorý z prvkov $a, b, c$ má rád 4, tak cyklická podgrupa ním generovaná má rád 4 a teda sa rovná $G$. V tomto prípade $(G, \cdot) \cong (Z_4, \oplus)$. Ostáva prípad, že $r(a) = r(b) = r(c) = 2$. Súčin $a \cdot b$ sa zrejme nemôže rovnať prvku $a$ resp. $b$ resp. $e$, lebo by sme dostali rovnosti $a \cdot b = a = a \cdot e$ resp. $a \cdot b = b = e \cdot b$ resp. $a \cdot b = e = a \cdot a$, ktoré po krátení vedú na sporné rovnosti $b = e$ resp. $a = e$ resp. $b = a$. Preto nutne $a \cdot b = c$. Úplne analogicky sa ukáže, že platí $b \cdot a = c$, $b \cdot c = a = c \cdot b$, $a \cdot c = b = c \cdot a$. Teda v tomto prípade má grupa $(G, \cdot)$ tabuľku

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

čiže je izomorfná s grupou symetrií obdĺžnika (pozri tabuľku 2 v kapitole 4). □

Výhodu použitia Malej Fermatovej vety ukážeme na riešení nasledujúcej úlohy.

7.13 Príklad. Ukážte, že ak $a, b \in Z$ nie sú násobkom čísla 7, tak $a^6 + b^6 + 5$ je násobkom čísla 7.

Riešenie. Ak $7 \nmid a$, $7 \nmid b$, tak $\mathrm{D}(a, 7) = \mathrm{D}(b, 7) = 1$ a pre prvočíslo 7 dostávame z dôsledku 7.11 (po krátení), že $a^6 \equiv 1 \pmod 7$ a $b^6 \equiv 1 \pmod 7$, z čoho $a^6 + b^6 \equiv 2 \pmod 7$. Odtiaľ $a^6 + b^6 + 5 \equiv 0 \pmod 7$, teda $7 \mid a^6 + b^6 + 5$.

Ak $x \in Z$ a $7 \nmid x$, tak existujú celé čísla $k$, $r$, že $x = 7k + r$, $r \in \{1, 2, 3, 4, 5, 6\}$. Pri riešení predchádzajúcej úlohy sme teda mohli využiť zápis čísel $a$, $b$ v uvedenom tvare. Tento postup však vedie k zdĺhavým a jednotvárnym výpočtom (presvedčte sa).

## Cvičenia

**1.** Ukážte, že ak $H$ je podgrupa grupy $G$ a $a \cdot b^{-1} \in H$, tak $Ha = Hb$.

**2.** Overte správnosť rozkladov v príklade 7.7.

**3.** Nech $H$ je podgrupa grupy $G$. Dokážte, že $Ha = Hb$ implikuje $H(a \cdot c) = H(b \cdot c)$ pre ľubovoľné $a, b, c \in G$.

**4.** Nech $H$ je podgrupa grupy $G$. Označme pre $a \in G$, $HaH = \{h_1 \cdot a \cdot h_2 \mid h_1, h_2 \in H\}$. Ukážte, že pre $a, b \in G$ buď platí $HaH = HbH$ alebo $HaH \cap HbH = \varnothing$.

**5.** Nájdite všetky triedy grupy $G$ podľa podgrupy $H$:
a) $G = (R \setminus \{0\}, \cdot)$, $H = \{-1, 1\}$;
b) $G = (R \setminus \{0\}, \cdot)$, $H = R^+$;
c) $G = (C \setminus \{0\}, \cdot)$, $H = R^+$;
d) $G = (Q, +)$, $H = Z$;
e) $G = (C, +)$, $H = R$;

f) $G = (Z \times Z, +)$, $H = 3Z \times 2Z$;
g) $G = (R \times R, +)$, $H = \{(3x, 2x) \mid x \in R\}$;
h) $G = (Z_{12}, \oplus)$, $H = \{\overline{0}, \overline{4}, \overline{8}\}$;
i) $G = (D_3, \circ)$, $H = \{i, v\}$;
j) $G = (D_4, \circ)$, $H = \{i, r_1, r_2, r_3\}$;
k) $G = (C_8, \circ)$, $H = \{i, r_4\}$;
l) $G = (K_4, \cdot)$, $H = \{-1, 1\}$.

**6.** Daná je grupa $(G, \circ)$ všetkých transformácií $f_{a,b} : R \to R$ určených predpisom $f_{a,b}(x) = a \cdot x + b$, kde $a \in R \setminus \{0\}, b \in R$. Určte pravé a ľavé triedy grupy $G$ podľa podgrupy $H$, ak
a) $H = \{f_{a,b} \mid a = 1\}$,
b) $H = \{f_{a,b} \mid b = 0\}$.
Porovnajte $\mathcal{P}$ a $\mathcal{L}$ v oboch prípadoch!

**7.** Nech $H$ je podgrupa konečnej grupy $G$ a $K$ je podgrupa $H$. Dokážte, že

$$[G : K] = [G : H] \cdot [H : K].$$

**8.** Pomocou dôsledku 7.9 ukážte, že každá grupa rádu $p^n$, kde $p$ je prvočíslo, má podgrupu rádu $p$.

**9.** Nech $G$ je cyklická grupa rádu $n$. Ukážte, že pre každý deliteľ $d$ čísla $n$ existuje práve jedna podgrupa rádu $d$ grupy $G$.

**10.** Ukážte, že každá grupa rádu 6 je buď cyklická alebo izomorfná s grupou $D_3$.

## 8. Normálne podgrupy, kongruencie na grupách a faktorové grupy

Pomocou binárnej relácie kongruencie modulo $m$ sme v kapitole 1 uskutočnili faktorizáciu (rozklad) množiny celých čísel $Z$ na zvyškové triedy. Ukázali sme pritom, že relácia $\equiv \pmod m$, podľa ktorej sme faktorizáciu uskutočnili je kompatibilná (zlučiteľná) s operáciami sčítania a násobenia (veta 1.5). V dôsledku toho sme mohli definovať sčítanie a násobenie aj na množine zvyškových tried $\overline{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ a získať tak tzv. faktorové algebry $(\overline{Z}_m, \oplus)$ a $(\overline{Z}_m, \odot)$. V kapitole 6 sme ukázali, že množinu zvyškových tried možno dostať aj ako množinu $Z/mZ$ všetkých tried grupy $(Z, +)$ podľa pogrupy $mZ = \{m \cdot k \mid k \in Z\}$. Zovšeobecnením týchto poznatkov, a síce faktorizáciou ľubovoľných grúp podľa tzv. normálnych podgrúp a ekvivalentne podľa tzv. kongruencií, sa budeme zaoberať v tejto kapitole.

Ak v uvedenom príklade $m = 2$, dostaneme množinu $Z/2Z = \{P, N\}$, kde $P = 2Z$ je trieda párnych celých čísel a $N = 2Z + 1$ je trieda nepárnych celých čísel. Táto tvorí (spolu s operáciou sčítania) tzv. faktorovú grupu $(Z/2Z, +)$ izomorfnú s grupou $(Z_2, \oplus)$, kde operácia sčítania tried vlastne vyjadruje ako „sa sčitujú parity“:

$$P + P = P,\ P + N = N,\ N + P = N,\ N + N = P.$$

Podobne, faktorizáciou multiplikatívnej grupy $(R \setminus \{0\}, \cdot)$ nenulových reálnych čísel podľa podgrupy $R^+$ kladných reálnych čísel dostaneme faktorovú grupu $\{R^+, R^-\}$ s operáciou násobenia

$$R^+ \cdot R^+ = R^+,\ R^+ \cdot R^- = R^-,\ R^- \cdot R^+ = R^-,\ R^- \cdot R^- = R^+,$$

teda faktorizácia nám tentoraz dáva pohľad na to, ako sa „násobia znamienka“:

$$+ \cdot + = +,\ \ + \cdot - = -,\ \ - \cdot + = -,\ \ - \cdot - = +.$$

Faktorizácia nám zjednodušuje pohľad na veci aj v bežnom živote. Stotožňovanie dní v roku do siedmich tried, pondelok až nedeľa, umožňuje, že činnosť škôl, úradov, kostolov, obchodov, atď. nemusí byť plánovaná na každý deň roku osobitne, ale je organizovaná spravidla v súlade s jednoduchou „faktorovou štruktúrou“ pondelok až nedeľa. Podobne napr. pôdorysné zobrazenie predmetu stotožňuje všetky body predmetu majúce rovnaký priemet vo vertikálnom smere a získame tak prehľadnú faktorovú štruktúru obrazu predmetu pri pohľade zhora – pôdorys. Obraz predmetu môžeme faktorizovať aj v iných smeroch – pri pohľade zboku, spredu atď.

Teraz sa vráťme k faktorizácii grúp, najprv podľa (špeciálnych) podgrúp. Súčinom tried $Ha$, $Hb$ grupy $(G, \cdot)$ podľa pogrupy $H$ reprezentovaných prvkami $a, b$ by prirodzene mala byť trieda $H(a \cdot b)$ obsahujúca prvok $a \cdot b$, t.j.

$$(Ha) \cdot (Hb) = H(a \cdot b). \tag{1}$$

Odteraz budeme, tak ako je tomu v algebre zvykom, symbol násobenia $\cdot$ často vynechávať a napr. namiesto $a \cdot b$ písať len $ab$, a pod. Všimnime si, že násobenie tried uvedené v (1) bude korektne definovať operáciu vtedy, keď výsledok násobenia nebude závisieť od prvkov použitých na reprezentovanie tried, čiže ak bude platiť

$$Ha = Hc \wedge Hb = Hd \Rightarrow H(ab) = H(cd). \tag{2}$$

Pre aké podgrupy $H$ bude toto platiť? Najprv si všimnime, že podľa 7.4 c) rovnosť $Ha = Hc$ implikuje $ac^{-1} \in H$, odkiaľ dostávame $(ad)(cd)^{-1} = add^{-1}c^{-1} = ac^{-1} \in H$. Opäť 7.4 c) implikuje $H(ad) = H(cd)$. Ak by sa nám podarilo ukázať, že $Hb = Hd$ implikuje $H(ab) = H(ad)$, mali by sme $H(ab) = H(ad) = H(cd)$, t.j. implikácia (2) by platila. Rovnosť $Hb = Hd$ podľa 7.4 c) implikuje $bd^{-1} = h \in H$ a aby sme dostali $H(ab) = H(ad)$, podľa 7.4 c) potrebujeme, aby $(ab)(ad)^{-1} = abd^{-1}a^{-1} = aha^{-1} \in H$. Ako ale zaručiť, aby $aha^{-1} \in H$? V prípade, že grupa $G$ je komutatívna, platí $ah = ha$, t.j. skutočne $aha^{-1} = h \in H$. V prípade, že $G$ nie je komutatívna, budeme kvôli platnosti (2) požadovať, aby podgrupa $H$ s každým prvkom $h$ obsahovala aj tzv. *konjugovaný* prvok $aha^{-1}$.

8.1 Definícia. *Podgrupa $H$ grupy $G$ sa nazýva normálna (alebo invariantná) v $G$, ak s každým prvkom $h$ obsahuje aj všetky konjugované prvky $aha^{-1}$ $(a \in G)$, t.j.*

$$h \in H \Rightarrow \forall a \in G;\ aha^{-1} \in H. \tag{3}$$

8.2 Lema. *Pogrupa $H$ grupy $G$ je normálna v $G$ práve vtedy, keď*

$$\forall a \in G;\ aH = Ha \tag{4}$$

*t.j. ak sa pravé a ľavé triedy grupy $G$ podľa $H$ rovnajú.*

Dôkaz. Nech podgrupa $H$ grupy $G$ je normálna, t.j. pre každé $a \in G$ a $h \in H$ platí $aha^{-1} = h' \in H$. Potom $ah = h'a$, teda $aH \subseteq Ha$. Analogicky (po zámene prvkov $a, a^{-1}$) platí $a^{-1}ha = h' \in H$ t.j. pre každé $a \in G$ a $h \in H$ existuje $h' \in H$, že $ha = ah'$, čiže $Ha \subseteq aH$. Teda $aH = Ha$ pre každé $a \in G$.

Obrátene, ak platí (4) a $h \in H, a \in G$, tak $ah \in aH = Ha$ t.j existuje $h' \in H$, že $ah = h'a$, odkiaľ $aha^{-1} = h' \in H$. Teda platí (3) a lema je dokázaná. □

Ako sme už vyššie uviedli, v komutatívnej grupe $G$ je každá podgrupa $H$ normálna a v nekomutatívnej grupe $G$ normálnosť pogrupy $H$ zaručuje, že platí (2), a teda prirodzené násobenie tried z $G/H$ je korektná operácia. Nasledujúca veta hovorí, že táto operácia definuje na $G/H$ grupu.

8.3 Veta. *Nech $(G, \cdot)$ je grupa a $H$ je jej normálna podgrupa. Množina $G/H$ všetkých tried grupy $G$ podľa $H$ tvorí grupu vzhľadom na operáciu definovanú v (1). Ak grupa $G$ je komutatívna, tak aj grupa $(G/H, \cdot)$ je komutatívna. Ak $G$ je cyklická, tak aj $G/H$ je cyklická.*

Dôkaz. $(G/H, \cdot)$ je grupoid, pretože $H$ je normálna podgrupa. Overenie asociatívnosti násobenia v $G/H$ a v prípade komutatívnosti $G$ aj komutatívnosti $G/H$ prenechávame na čitateľa (cvičenie 1). Trieda $H = He$ je neutrálnym prvkom v $G/H$, pretože pre ľubovoľnú triedu $Ha \in G/H$ máme

$$(Ha)(He) = Hae = Ha = Hea = (He)(Ha).$$

Inverzným prvkom k triede $Ha$ je trieda $Ha^{-1}$, pretože

$$(Ha)(Ha^{-1}) = Haa^{-1} = He = Ha^{-1}a = (Ha^{-1})(Ha).$$

Teda $(G/H, \cdot)$ je grupa. Ak $G$ je cyklická s generátorom $a$, tak aj $G/H$ je cyklická s generátorom $Ha$, pretože $(Ha)^m = Ha^m$ pre všetky celé čísla $m$. □

8.4 Definícia. *Grupu $(G/H, \cdot)$ opísanú vo vete 8.3 nazývame faktorovou grupou grupy $(G, \cdot)$ podľa jej normálnej podgrupy $H$.*

Faktorovú grupu $Z/mZ$ možno získať z grupy $(Z, +)$ aj zlučovaním jej prvkov podľa „novej rovnosti“, kompatibilnej s operáciou $+$. Touto „novou rovnosťou“, vedúcou k rovnakému rozkladu množiny $Z$, je kongruencia modulo $m$, pričom vzťah medzi podgrupou $mZ$ a kongruenciou $\equiv \pmod m$ je

$$a \equiv b \pmod m \Leftrightarrow a - b \in mZ. \tag{5}$$

Teraz ukážeme, že aj vo všeobecnosti možno každú faktorovú grupu $(G/H, \cdot)$ grupy $G$ podľa jej normálnej podgrupy $H$ získať pomocou relácie ekvivalencie kompatibilnej s operáciou grupy $(G, \cdot)$.

8.5 Definícia. *Binárnu reláciu ekvivalencie $\equiv$ na grupe $(G, \cdot)$ kompatibilnú s grupovou operáciou $\cdot$, t.j. takú, že pre ľubovoľné $a, b, c, d \in G$*

$$a \equiv b \wedge c \equiv d \Rightarrow a \cdot b \equiv c \cdot d,$$

*nazývame kongruenciou grupy $(G, \cdot)$.*

Súvis medzi kongruenciami grupy a normálnymi podgrupami je zovšeobecnením vzťahu (5) na grupe $(Z, +)$.

8.6 Veta. *a) Nech $\equiv$ je kongruencia grupy $(G, \cdot)$. Potom $H(\equiv) = \{a \in G \mid a \equiv e\}$ je normálna podgrupa grupy $G$ a pre ľubovoľné $a, b \in G$ platí*

$$a \equiv b \Leftrightarrow ab^{-1} \in H(\equiv). \tag{6}$$

*b) Nech $H$ je normálna podgrupa grupy $(G, \cdot)$. Potom binárna relácia $\equiv_H$ na $G$ určená vzťahom*

$$a \equiv_H b \Leftrightarrow ab^{-1} \in H \tag{7}$$

*je kongruencia grupy $G$ a platí $\{a \in G \mid a \equiv_H e\} = H$.*

*c) Kongruencia $\equiv_{H(\equiv)}$ je totožná s kongruenciou $\equiv$ a normálna podgrupa $H(\equiv_H)$ je totožná s normálnou podgrupou $H$.*

**8.7 Poznámka.** Všimnime si, že binárna relácia $\equiv_H$ priradená k normálnej podgrupe $H$ podľa vzťahu (7) je vlastne relácia pravej kongruencie modulo $H$, $\equiv_p \pmod H$, zavedená v kapitole 7. Je ľahké ukázať, že aj relácia ľavej kongruencie modulo $H$, $\equiv_l \pmod H$, je totožná s reláciou $\equiv_H$. Skutočne, s využitím 7.4 c) a 8.2 ihneď dostávame

$$a \equiv_l b \pmod H \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH \Leftrightarrow Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow a \equiv_H b.$$

Dôkaz vety 8.6. a) Nech $\equiv$ je kongruencia grupy $(G, \cdot)$ a nech $H = \{a \in G \mid a \equiv e\}$. Pre ľubovoľné $a, b \in H$ platí $a \equiv e,\ b \equiv e$, odkiaľ zo symetrickosti a reflexívnosti relácie $\equiv$ a jej kompatibilnosti s operáciou $\cdot$ dostaneme postupne $e \equiv b,\ b^{-1}e \equiv b^{-1}b,\ b^{-1} \equiv e,\ ab^{-1} \equiv ae,\ ab^{-1} \equiv a$. Pretože $a \equiv e$, z tranzitívnosti relácie $\equiv$ máme $ab^{-1} \equiv e$, t.j. $ab^{-1} \in H$. Teda $H$ je podgrupa grupy $G$. Nech teraz $h \in H$ a $a \in G$. Potom $h \equiv e$, odkiaľ dostaneme postupne $ah \equiv ae,\ aha^{-1} \equiv$

$aea^{-1},\ aha^{-1} \equiv e$, t.j. $aha^{-1} \in H$. Teda $H$ je normálna podgrupa $G$. Je zrejmé, že pre ľubovoľné $a, b \in G$ platí

$$a \equiv b \Leftrightarrow ab^{-1} \equiv e \Leftrightarrow ab^{-1} \in H,$$

čím je vzťah (6) dokázaný.

b) Nech $H$ je normálna podgrupa grupy $G$ a $\equiv$ je binárna relácia na $G$ daná vzťahom (7), t.j. $\equiv$ je pravá kongruencia modulo $H$, $\equiv_p \pmod{H}$, z definície 7.1. Vo vete 7.2 sme ukázali, že táto relácia je relácia ekvivalencie na $G$. Pretože $a \equiv b \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$ podľa 7.4 c), je kompatibilita relácie $\equiv$ s operáciou grupy $(G, \cdot)$ ekvivalentná so vzťahom (2), ktorého platnosť v prípade normálnej podgrupy $H$ sme vlastne overili už pred definíciou 8.1. Teda $\equiv$ je kongruencia grupy $G$. Napokon, $\{a \in G \mid a \equiv e\} = \{a \in G \mid ae^{-1} = a \in H\} = H$.

c) Zo (6) a (7) máme

$$a \equiv_{H(\equiv)} b \Leftrightarrow ab^{-1} \in H(\equiv) \Leftrightarrow a \equiv b$$

a analogicky

$$H(\equiv_H) = \{a \in G \mid a \equiv_H e\} = \{a \in G \mid ae^{-1} \in H\} = \{a \in G \mid a \in H\} = H. \quad \square$$

Faktorová grupa $G/H$ grupy $G$ podľa normálnej podgrupy $H$ je podľa definície 8.4 množinou pravých tried grupy $G$ podľa $H$, ktoré sú podľa 8.2 totožné s ľavými triedami grupy $G$ podľa $H$. Tieto triedy boli v kapitole 7 zavedené ako triedy ekvivalencie množiny $G$ podľa pravej resp. ľavej kongruencie modulo $H$. Ako sme ukázali v poznámke 8.7, obe tieto relácie ekvivalencie sú v prípade normálnej podgrupy $H$ totožné s kongruenciou $\equiv_H$ určenou vzťahom (7). Vidíme teda, že prvky faktorovej grupy $G/H$ podľa normálnej podgrupy $H$ sú triedy ekvivalencie určené kongruenciou $\equiv_H$ a že teda faktorizácia podľa normálnej podgrupy $H$ je vlastne to isté ako faktorizácia podľa kongruencie $\equiv_H$. Preto sa pre faktorovú grupu popri označenii $G/H$ používa aj označenie $G/\equiv_H$.

Kongruenciu $\equiv_H$ priradenú k normálnej podgrupe $H$ grupy $G$ spôsobom opísaným vo vete 8.6 budeme nazývať (v súlade s kapitolou 7) *kongruenciou modulo* $H$. Normálna podgrupa $H(\equiv)$ grupy $(G, \cdot)$ priradená ku kongruencií $\equiv$ sa v literatúre zvykne nazývať *jadrom* kongruencie $\equiv$. Z časti c) vety 8.6 vyplýva, že kongruencie grupy sú totožné práve vtedy, keď ich jadrá sú totožné normálne podgrupy a obrátene, normálne podgrupy grupy sú totožné práve vtedy, keď kongruencie podľa týchto podgrúp sú totožné.

**8.8 Príklad.** Vráťme sa ku grupe $(Z, +)$. Z doteraz uvedeného vyplýva, že jadrom kongruencie $\equiv \pmod{m}$ tejto grupy je normálna podgrupa $mZ = \{m \cdot k \mid k \in Z\}$ a že kongruencia modulo $mZ$ je kongruencia $\equiv \pmod{m}$. Všimnime si, že pre $m = 0$ dostaneme najmenšiu kongruenciu $\equiv \pmod{0} = \{(a, a) \mid a \in Z\}$ grupy $(Z, +)$, ktorá je vlastne rovnosťou na $Z$. Ak stotožňujeme prvky grupy $Z$ podľa tejto kongruencie, získame najväčšiu faktorovú grupu $\{\{a\} \mid a \in Z\}$ izomorfnú so $Z$. Pre $m = 1$ máme naopak najväčšiu kongruenciu $\equiv \pmod{1} = Z \times Z$ grupy $(Z, +)$, ktorá stotožňuje všetky celé čísla do jednej triedy a získaná faktorová grupa $\{Z\}$ je najmenšia. Pre $m \geq 2$ dáva faktorizácia podľa kongruencie $\equiv \pmod{m}$ netriviálne faktorové grupy $(\overline{Z}_m, \oplus)$.

Všimnime si, že podľa Lagrangeovej vety má grupa $(Z_p, \oplus)$ prvočísleného rádu $p$ iba podgrupy rádov 1 a $p$. Má teda iba dve normálne podgrupy, $\{e\}$ a $Z_p$, ktorým odpovedajú najmenšia kongruencia $\{(a,a) \mid a \in Z_p\}$ a najväčšia kongruencia $Z_p \times Z_p$. Grupy $G$ majúce iba triviálne kongruencie $\{(a,a) \mid a \in G\}$ a $G \times G$ (alebo ekvivalentne iba triviálne normálne podgrupy $\{e\}$ a $G$) nazývame *jednoduchými* grupami. Príkladom jednoduchých grúp sú teda grupy zvyškových tried modulo prvočíslo $p$.

Predchádzajúce úvahy ilustrujeme ešte v dvoch príkladoch.

**8.9 Príklad.** V príklade 7.7 sme uvažovali o dvoch cyklických podgrupách nekomutatívnej grupy $(S_3, \circ)$: $H_1 = [(123)] = \{(123), (132), \mathrm{id}\}$, $H_2 = [(12)] = \{(12), \mathrm{id}\}$. Videli sme, že pravé triedy $H_1$, $H_1(12)$ rozkladu $S_3$ podľa $H_1$ sú súčasne aj ľavými triedami rozkladu, teda podľa 8.2 je $H_1$ normálna. (V cvičení 2 ukážte, že $H_1$ obsahuje s každým prvkom $h \in H_1$ všetky konjugované prvky $aha^{-1}$ pre $a \in S_3$.) Kongruencia $\equiv_{H_1}$ modulo $H_1$ stotožňuje prvky v triede $H_1$ a prvky v triede $H_1(12)$ a žiadne iné. Násobenie tried vo faktorovej grupe $S_3/H_1$ funguje takto:

$$H_1 \circ H_1(12) = H_1(12) = H_1(12) \circ H_1,$$
$$H_1(12) \circ H_1(12) = H_1 = H_1 \circ H_1.$$

Teda faktorová grupa $(S_3/H_1, \circ)$ je izomorfná s grupou $(Z_2, \oplus)$.

Na druhej strane sme videli, že $H_2(23) = \{(123), (23)\} \neq \{(132), (23)\} = (23)H_2$. Všimnime si, že $H_2$ s prvkom $(12)$ neobsahuje konjugovaný prvok $(23)(12)(23)^{-1} = (13)$. Podgrupa $H_2$ nie je normálna a vzťahom (1) nemožno teda definovať násobenie tried korektne. Skutočne, vidíme, že $H_2(23) = H_2(123)$ a $H_2(13) = H_2(132)$, ale

$$H_2((23)(13)) = H_2(123) = \{(13), (123)\},$$
$$H_2((123)(132)) = H_2 = \{(12), \mathrm{id}\}.$$

Ďalej, pretože $H_2$ nie je normálna podgrupa, relácie pravej a ľavej kongruencie modulo $H_2$ nie sú totožné. Skutočne, $(123) \equiv_p (23) \pmod{H_2}$, $(123) \not\equiv_l (23) \pmod{H_2}$. Podobne, $(132) \equiv_l (23) \pmod{H_2}$, ale $(132) \not\equiv_p (23) \pmod{H_2}$. □

**8.10 Príklad.** Zoberme nekomutatívnu grupu $(D_4, \circ)$ symetrií štvorca (príklad 4.1) a jej podgrupy $C_4 = \{r_1, r_2, r_3, i\}$, $K = \{v, i\}$. Zaujíma nás, či tieto podgrupy sú normálne a ak áno, ako vyzerajú príslušné faktorové grupy.

Index podgrupy $C_4$ v grupe $D_4$ je $[D_4 : C_4] = \frac{|D_4|}{|C_4|} = 2$. Keďže jedna pravá (i ľavá) trieda grupy $D_4$ podľa $C_4$ je samotná podgrupa $C_4$, ostávajúca pravá (i ľavá) trieda $D_4$ podľa $C_4$ musí byť $\{p, h, l, v\} = C_4 v$. Teda každá pravá trieda grupy $D_4$ podľa $C_4$ je súčasne i ľavá trieda, preto v súlade s 8.2 je $C_4$ normálna podgrupa $D_4$. Kongruencia $\equiv_{C_4}$ modulo $C_4$ stotožňuje navzájom prvky v triede $C_4$ a prvky v triede $C_4 v$ a žiadne iné. Je jasné, že faktorová grupa $(D_4/\equiv_{C_4}, \circ) = (\{C_4, C_4 v\}, \circ)$ je izomorfná s grupou $(Z_2, \oplus)$.

Pravé triedy grupy $D_4$ podľa podgrupy $K$ sú

$$K,\ Kp = \{r_3, p\},\ Kh = \{r_2, h\},\ Kl = \{r_1, l\},$$

zatiaľčo ľavé triedy $D_4$ podľa $K$ sú

$$K,\ pK = \{r_1, p\},\ hK = \{r_2, h\},\ lK = \{r_3, l\}.$$

Vidíme, že $Kp \neq pK$ a $Kl \neq lK$, preto podgrupa $K$ nie je invariantná. Skutočne, s prvkom $v$ podgrupa $K$ neobsahuje konjugovaný prvok $pvp^{-1} = h = lvl^{-1}$. To, že násobenie pravých tried nemožno korektne definovať vzťahom (1) vidno z toho, že napr. $Kp = Kr_3$ a $Kr_1 = Kl$, ale

$$K(pr_1) = Kv = K = \{v, i\},$$
$$K(r_3 l) = Kh = \{r_2, h\}.$$

Analogicky sa možno presvedčiť, že ani násobenie ľavých tried nemožno definovať vzťahom (1) (cvičenie 3).

To, že relácie pravej a ľavej kongruencie modulo $K$ nie sú totožné vidno opäť priamo z pravých a ľavých tried rozkladu. Tak napríklad $p \equiv_p r_3 \pmod K$ a $p \not\equiv_p r_1 \pmod K$, zatiaľčo $p \not\equiv_l r_3 \pmod K$ a $p \equiv_l r_1 \pmod K$.

## Cvičenia

**1.** Ukážte, že násobenie tried v $G/H$ dané vzťahom (1) je asociatívne a za predpokladu komutatívnosti grupy $G$ je aj komutatívne.

**2.** Presvedčte sa, že podgrupa $H_1$ grupy $(S_3, \circ)$ v príklade 8.9 obsahuje s každým prvkom aj všetky k nemu konjugované prvky.

**3.** V príklade 8.10 ukážte, že násobenie ľavých tried nemožno korektne definovať vzťahom (1).

**4.** Ukážte, že na každej grupe $(G, \cdot)$ je relácia „byť konjugovaným prvkom“, t.j. relácia

$$R = \{(x, y) \in G \times G \mid x = aya^{-1} \text{ pre nejaké } a \in G\}$$

reláciou ekvivalencie.

**5.** Nájdite všetky normálne podgrupy a kongruencie danej grupy:
a) $(K_4, \cdot)$
b) $(Z_6, \oplus)$
c) $(Z_{12}, \oplus)$
d) $(Z, +)$
e) $(D_3, \circ)$
f) $(D_4, \circ)$
g) $(C_5, \circ)$
h) $(S_3, \circ)$.

**6.** Zistite, či $H$ je normálna podgrupa grupy $G$ a v kladnom prípade opíšte kongruenciu $\equiv_H$ modulo $H$ a faktorovú grupu $G/H$.
a) $G = (D_4, \circ),\ H = \{i, r^2\}$
b) $G = (S_3, \circ),\ H = [(13)]$
c) $G = (S_4, \circ),\ H = [(123)]$
d) $G = (S_4, \circ),\ H = [(1234)]$
e) $G = (Z_2 \times Z_4, \oplus),\ H = [(12)]$
f) $G = (Z_6 \times Z_8, \oplus),\ H = [(22)]$
g) $G = (Z_2 \times Z_4 \times Z_6, \oplus),\ H = [(1, 1, 3)]$
h) $G = (Z, +),\ H = 5Z$
i) $G = Z \times Z \times Z,\ H = \{(x, 0, y) \mid x, y \in Z\}$
j) $G = (R \times R, +),\ H = \{(x, y) \mid 2x + y = 0\}$

k) $G = (C, +),\ H = R \setminus \{0\}$
l) $G = (C \setminus \{0\}, \cdot),\ H = R \setminus \{0\}$
m) $G = (K_{12}, \cdot),\ H = \{c \in C \mid c^4 = 1\}$.

**7.** Zistite, či priamky $p : -4x + 2y - 1 = 0,\ q : 2x - y - 1 = 0$ a $r : y = 2x$ ako podmnožiny $R \times R$ určujú triedy rozkladu faktorovej grupy $(R \times R/2R \times R, +)$. Ak áno, nájdite ich vzájomné súčty..

**8.** Zistite, či nasledujúce grupy sú izomorfné. V kladnom prípade určte príslušný izomorfizmus.
a) $(D_4/[r^2], \circ)$ a $(D_2, \circ)$
b) $(S_4/[(123)], \circ)$ a $(K_4, \cdot)$
c) $(Z/5Z, +)$ a $(C_5, \circ)$
d) $(Z_2 \times Z_4/[(12)], \oplus)$ a $(D_2, \circ)$
e) $(Z_6 \times Z_8/[(2, 2)], \oplus)$ a $(Z_2 \times Z_2, \oplus)$
f) $(R \setminus \{0\}/\{-1, 1\}, \cdot)$ a $(R^+, \cdot)$
g) $(R \times R/[(2, 1)], +)$ a $(R, +)$
h) $(C/R, +)$ a $(R, +)$
i) $(C \setminus \{0\}/R \setminus \{0\}, \cdot)$ a $(R \setminus \{0\}, \cdot)$
j) $K_{12}/\{c \in C \mid c^2 = 1\}, \cdot)$ a $(D_3, \circ)$.

**9.** Nech $H, K$ sú normálne podgrupy grupy $(G, \cdot)$. Dokážte, že aj $H \cap K$ a $HK = \{h \cdot k \mid h \in H, k \in K\}$ sú normálne podgrupy grupy $G$.

**10.** Ukážte, že ak $K \subseteq H$ sú normálne podgrupy grupy $(G, \cdot)$, tak $K$ je normálna podgrupa grupy $H$ a faktorová grupa $H/K$ je normálna podgrupa grupy $G/K$.

## 9. Klasifikácia konečných grúp do rádu 15

V kapitole 3 sme ukázali, že relácia $\cong$ (byť izomorfný) je reflexívna, symetrická a tranzitívna na systéme všetkých grupoidov, a teda aj grúp. (Tento systém je tak veľký, že už nie je množinou, preto termín „množina“ preň nepoužívame.) Relácia $\cong$ určuje rozklad systému všetkých grúp, pričom dve grupy patria do tej istej triedy rozkladu práve vtedy, keď sú izomorfné. Ako sme už uviedli, izomorfné grupy nepovažujeme z algebraického hľadiska za rôzne a v algebre vlastne skúmame triedy grúp dané reláciou $\cong$. Určenie tried rozkladu systému konečných grúp podľa relácie $\cong$ (nájdenie reprezentantov všetkých tried) nazývame *klasifikáciou* konečných grúp. V tejto kapitole uvedieme klasifikáciu konečných grúp až do rádu 15.

Vieme už, že ak rád grupy $G$ je prvočíslo $p$, tak rád každého prvku $a \in G$, $a \neq e$ ($e$ je neutrálny prvok), je $r(a) = p$, t.j. $G$ je cyklická grupa a každý prvok s výnimkou neutrálneho je jej generátorom. Je zrejmé, že cyklická grupa $(G, \cdot)$ rádu $p$ je izomorfná s grupou $(Z_p, +)$ pri izomorfizme

$$\varphi : G = \{e, a, a^2, \ldots, a^{p-1}\} \to \{0, 1, 2, \ldots, p-1\},$$
$$\varphi(e) = 0,\ \varphi(a) = 1,\ \varphi(a^2) = 2,\ \ldots,\ \varphi(a^{p-1}) = p-1.$$

Dostali sme nasledovné tvrdenie.

9.1 Veta. *Pre $p \in \{2, 3, 5, 7, 11, 13\}$ je každá grupa rádu $p$ izomorfná s grupou $(Z_p, +)$.*

Hovoríme, že $(Z_p, +)$ je jediná (až na izomorfizmus) grupa rádu $p$.

Bez dôkazu uvedieme ďalšie tvrdenie (dôkaz možno nájsť v [4] alebo [12]).

9.2 Veta. *Ak $p$ je nepárne prvočíslo, tak každá grupa rádu $2p$ je izomorfná buď s cyklickou grupou $Z_{2p}$ alebo s dihedrálnou grupou $D_p$ (grupou symetrií pravidelného $p$-uholníka).*

Na základe týchto dvoch tvrdení vieme už pre väčšinu rádov $n$, $n \leq 15$, napísať zoznam všetkých (až na izomorfizmus) grúp rádu $n$. Do zoznamu ďalej dopíšeme pre $n \in \{8, 9, 12, 15\}$ tie navzájom neizomorfné grupy rádu $n$, ktoré už poznáme: pre $n = 8$ sú to $Z_2 \times Z_2 \times Z_2$, $Z_2 \times Z_4$, $Z_8$ a $D_4$, pre $n = 9$ sú to $Z_3 \times Z_3$ a $Z_9$, pre $n = 12$ sú to $Z_2 \times Z_6$, $Z_{12}$, $D_6$ a $A_4$ a pre $n = 15$ je to grupa $Z_{15}$ (pozri 4.2, 4.4, 4.6 a cvičenie 5 v kapitole 6).

Dá sa ukázať [4], že iné (až na izomorfizmus) grupy rádov 9 a 15 už neexistujú, a že úplnú klasifikáciu konečných grúp do rádu 15 dopĺňajú už len jedna ďalšia grupa rádu 8 (označíme ju $Q_8$) a jedna ďalšia grupa rádu 12 (označíme ju $T$).

| **rád** | **zoznam grúp** | **referencie** |
|---|---|---|
| 1 | $\{e\}$ | |
| 2 | $Z_2$ | 9.1 |
| 3 | $Z_3$ | 9.1 |
| 4 | $Z_2 \times Z_2$, $Z_4$ | 7.12 |
| 5 | $Z_5$ | 9.1 |
| 6 | $Z_6$, $D_3$ | 9.2 |
| 7 | $Z_7$ | 9.1 |
| 8 | $Z_2 \times Z_2 \times Z_2$, $Z_2 \times Z_4$, $Z_8$, $D_4$, $Q_8$ | 9.3, [4] |
| 9 | $Z_3 \times Z_3$, $Z_9$ | [4] |
| 10 | $Z_{10}$, $D_5$ | 9.2 |
| 11 | $Z_{11}$ | 9.1 |
| 12 | $Z_2 \times Z_6$, $Z_{12}$, $D_6$, $A_4$, $T$ | 9.4, [4] |
| 13 | $Z_{13}$ | 9.1 |
| 14 | $Z_{14}$, $D_7$ | 9.2 |
| 15 | $Z_{15}$ | [4] |

Grupu $Q_8$ rádu 8 a grupu $T$ rádu 12 (ktoré sme už v tabuľke uviedli) v nasledujúcich dvoch príkladoch podrobnejšie popíšeme.

9.3 Príklad. Grupa $Q_8$, nazývaná aj grupa kvaterniónov, je definovaná ako podgrupa multiplikatívnej grupy $M^*$ regulárnych (komplexných) matíc typu $2 \times 2$ (pozri cvičenie 2.12) generovaná maticami

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{a} \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad \text{kde } i^2 = -1,$$

teda $Q_8 = [A, B]$. Najprv určíme rády prvkov $A$, $B$. Neutrálny prvok, t.j. maticu $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ označíme $I$.

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
$$A^4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \quad \text{t.j. } r(A) = 4.$$
$$B^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$
$$B^4 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \quad \text{t.j. } r(B) = 4.$$

Ukážeme ďalej, že každý prvok grupy $[A,B]$ je možné zapísať v tvare $A^iB^j$, $i,j \in \{0,1,2,3\}$, t.j. že $[A,B] = \{A^iB^j;\ i,j \in \{0,1,2,3\}\}$. Najskôr sa presvedčíme, že $H = \{A^iB^j;\ i,j \in \{0,1,2,3\}\}$ je podgrupa grupy $M^*$.

Pretože napr. $A = A^1B^0 \in H$, tak $H \neq \emptyset$.

Nech $X, Y \in H$. Potom $X = A^iB^j$, $Y = A^rB^s$ a $XY^{-1} = A^iB^jB^{-s}A^{-r} = A^iB^kA^l$, $i,k,l \in \{0,1,2,3\}$. Vieme už, že $A^2 = B^2$ a priamym výpočtom sa môžeme presvedčiť, že $BA = A^3B = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$. Pre exponenty $k,l$ rozlíšime nasledovné prípady:

1. Ak $k = 0$ alebo $l = 0$, tak zrejme $XY^{-1} \in H$.

2. Ak $k = 2$ alebo $l = 2$, tak s využitím rovnosti $A^2 = B^2$ opäť dostávame, že $XY^{-1} \in H$.

V prípade, že $k,l \in \{1,3\}$ ostáva vyšetriť ešte nasledovné štyri prípady:

3. Ak $k = 1$, $l = 1$, tak $XY^{-1} = A^iBA = A^iA^3B = A^mB$, $m \in \{0,1,2,3\}$.

4. Ak $k = 1$, $l = 3$, tak $XY^{-1} = A^iBA^3 = A^iBAA^2 = A^iA^3BB^2 = A^mB^3$, $m \in \{0,1,2,3\}$.

5. Ak $k = 3$, $l = 1$, tak $XY^{-1} = A^iB^3A = A^iB^2BA = A^iA^2A^3B = A^nB$, $n \in \{0,1,2,3\}$.

6. Ak $k = 3$, $l = 3$, tak $XY^{-1} = A^iB^3A^3 = A^iB^2BAA^2 = A^iA^2A^3BB^2 = A^nB^3$, $n \in \{0,1,2,3\}$.

Vidíme, že vo všetkých prípadoch je $XY^{-1} \in H$, teda (podľa vety 2.6) $H$ je podgrupou grupy $M^*$. Pretože $H$ obsahuje $A$, $B$ a $[A,B]$ je najmenšia podgrupa grupy $M^*$ obsahujúca $A$, $B$, máme inklúziu $[A,B] \subseteq H$. Opačná inklúzia je zrejmá. Teda $Q_8 = [A,B] = H$.

Presvedčíme sa, že rád grupy $[A,B]$ je 8. Ak vypočítame ešte $AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ vidíme, že matice $A$, $A^2$, $A^3$, $I$, $B$, $B^3$, $AB$, $A^3B$ sú rôzne. V ostatných ôsmich prípadoch (pre $i,j \in \{0,1,2,3\}$ je možné napísať celkove 16 súčinov tvaru $A^iB^j$) dostávame: $B^2 = A^2$, $AB^2 = AA^2 = A^3$, $AB^3 = AA^2B = A^3B$, $A^2B = B^2B = B^3$, $A^2B^2 = A^2A^2 = I$, $A^2B^3 = B^2B^3 = B$, $A^3B^2 = A^3A^2 = A$, $A^3B^3 = AA^2B^2B = AIB = AB$. Grupa

$$Q_8 = [A,B] = \{A, A^2, A^3, I, B, B^3, AB, A^3B\}$$

má teda 8 prvkov.

Poznámka. 1. Keďže $B^3 = A^2 \cdot B$, tak množinu $Q_8$ možno popísať aj takto:

$$Q_8 = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\},$$

čo sa často robí.

2. Ak súčin $AB$ označíme $C$, môžeme overiť, že platí

$$A^2 = B^2 = C^2 = ABC = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

a dostávame Hamiltonovu formulu pre bázu telesa kvaterniónov. Často sa tiež používa označenie $A = i$, $B = j$, $C = k$.

9.4 Príklad. Grupa $T$ je neabelovská podgrupa grupy $S_3 \times S_4$ rádu 12, generovaná prvkami $a$, $b$ takými, že $r(a) = 6$, $a^3 = b^2$, $ba = a^{-1}b$.

Máme teda rovnosti $a^6 = e$ ($e$ je neutrálny prvok), $a^3 = b^2$, $ba = a^{-1}b = a^5b$. Môžeme sa presvedčiť (analogicky ako v predchádzajúcom príklade), že každý prvok grupy $[a, b]$ je tvaru

$$a^i b^j, \quad i \in \{0, 1, 2, 3, 4, 5\},\ j \in \{0, 1\}.$$

Grupa

$$[a, b] = \{e, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\} \tag{1}$$

má teda 12 prvkov (podrobne sa presvedčte, že uvedené prvky sú rôzne). Toto je tzv. *abstraktná* reprezentácia grupy $T$. Uvedieme aj *konkrétnu* reprezentáciu.

Vieme, že

$$(S_3, \circ) = (\{\mathrm{id}, (12), (13), (23), (123), (132)\}, \circ), \quad (Z_4, +) = (\{0, 1, 2, 3\}, +).$$

Grupa $S_3 \times Z_4$ (t.j. priamy súčin grúp $S_3$ a $Z_4$) má teda 24 prvkov. Nájdeme v nej generátory $a$, $b$. Položme $a = ((123), 2)$, $b = ((12), 1)$. Pretože $r((123)) = 3$, $r(2) = 2$, tak $r(a) = 6$. Presvedčte sa, že aj $a^3 = b^2$ a $ba = a^{-1}b$. Po dosadení za $a$, $b$ do (1) dostávame konkrétnu reprezentáciu grupy $T$

$$\begin{aligned}[a, b] =\{&(\mathrm{id}, 0), ((123), 2), ((132), 0), (\mathrm{id}, 2), ((123), 0), ((132), 2),\\ &((12), 1), ((13), 3), ((23), 1), ((12), 3), ((13), 1), ((23), 3)\}.\end{aligned}$$

Klasifikácia všetkých konečných grúp je jeden z najťažších *otvorených* (t.j. doposiaľ nevyriešených) problémov súčasnej matematiky a nie je vôbec jasné či sa ho v najbližších desiatkach rokov podarí vyriešiť. Zatiaľ nepoznáme ani vzorec, ktorý by pre ľubovoľné prirodzené číslo $n$ určoval, koľko je (až na izomorfizmus) konečných grúp rádu $n$.

Nedávno sa však podarilo dokončiť úplnú klasifikáciu konečných jednoduchých grúp. (Pojem jednoduchej grupy sme zaviedli na konci predchádzajúcej kapitoly.) Prvé pokusy matematikov v tomto smere začali už okolo roku 1890, ale až v roku 1954 po vytýčení novej stratégie R. Brauerom na Svetovom kongrese matematikov v Amsterdame začala, ako sa tomu hovorí dnes, „tridsaťročná vojna“ s konečnými jednoduchými grupami. V poslednej fáze začatej v r. 1982, D. Gorenstein, R. Lyons a R. Solomon zavŕšili klasifikačný proces, na ktorom sa však počas desiatok rokov podieľala celá plejáda svetových matematikov (viac si o tom možno prečítať napríklad v [4]). Popri nedávnom dokončení dôkazu slávnej Veľkej Fermatovej vety A. Wilesom (1995), ktorým bol vyriešený vyše 350 rokov otvorený matematický problém, je klasifikácia konečných jednoduchých grúp jeden z najviac cenených výsledkov dosiahnutých v matematike v 20. storočí.

## 10. Okruhy a podokruhy. Izomorfizmus okruhov

Grupy, ktorými sme sa zaoberali v predchádzajúcich kapitolách, sú algebraické štruktúry s jednou binárnou operáciou. Rovnako často sa však v algebre skúmajú štruktúry s dvoma binárnymi operáciami. Aj v bežnej školskej praxi pribudne k operácii sčítania prirodzených čísel už v druhom ročníku operácia násobenia. Vo väčšine elementárnych školských úloh sa používa popri sčitovaní aj násobenie. Prv než pristúpime k abstraktnému štúdiu algebier s dvoma binárnymi operáciami, uvedieme si typický príklad.

**10.1 Príklad.** Algebraická štruktúra $(Z, +, \cdot)$, kde $Z$ je množina celých čísel, sa dá zrejme opísať nasledovnými vlastnosťami:

1. algebra $(Z, +)$ je komutatívna grupa, kde nula funguje ako neutrálny prvok a opačné číslo k danému číslu ako inverzný prvok;
2. násobenie celých čísel je asociatívne, teda algebra $(Z, \cdot)$ je pologrupa;
3. sčítanie a násobenie sú zviazané distributívnymi zákonmi:

$$\forall a, b, c \in Z;\ a \cdot (b + c) = a \cdot b + a \cdot c$$
$$\forall a, b, c \in Z;\ (b + c) \cdot a = b \cdot a + c \cdot a.$$

Naviac vieme povedať, že násobenie je komutatívne a jednotka funguje ako neutrálny prvok pri násobení. Teda $(Z, \cdot)$ je dokonca komutatívny monoid. ∎

Algebru $(Z, +, \cdot)$ z predchádzajúceho príkladu budeme nazývať okruhom celých čísel v zmysle nasledujúcej definície.

10.2 Definícia. *Algebraickú štruktúru $(A, +, \cdot)$, kde $A$ je neprázdna množina a $+, \cdot$ sú binárne operácie na $A$, nazývame okruhom, ak*

1. *$(A, +)$ je komutatívna grupa.*
2. *$(A, \cdot)$ je pologrupa.*
3. *Operácia $\cdot$ je distributívna vzhľadom na operáciu $+$, t.j. platí*

$$\forall a, b, c \in A;\ a \cdot (b + c) = a \cdot b + a \cdot c \quad \textit{(distributívnosť zľava)}$$

$$\forall a, b, c \in A;\ (b + c) \cdot a = b \cdot a + c \cdot a \quad \textit{(distributívnosť sprava)}$$

*Ak aj operácia $\cdot$ je komutatívna, hovoríme o komutatívnom okruhu $(A, +, \cdot)$.*

Operácie $+$ resp. $\cdot$ nazývame sčítaním resp. násobením okruhu. Neutrálny prvok grupy $(A, +)$ nazývame *nulou okruhu* a označujeme $0_A$ a inverzný prvok k prvku $a$ nazývame *opačný prvok* a označujeme $-a$. Ak pologrupa $(A, \cdot)$ má tiež neutrálny prvok, nazývame ho *jednotkou okruhu* a označujeme $1_A$. Podobne ako pri grupách, namiesto o okruhu $(A, +, \cdot)$ hovoríme často len o okruhu $A$.

Matematickou indukciou vzhľadom na počet sčítancov možno ľahko dokázať platnosť nasledujúceho zovšeobecneného distributívneho zákona v okruhu (cvičenie 1).

10.3 Lema. *V okruhu $A$ platí pre ľubovoľné prvky $a, b_1, \ldots, b_n$*

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n,$$

$$(b_1 + b_2 + \cdots + b_n) \cdot a = b_1 \cdot a + b_2 \cdot a + \cdots + b_n \cdot a.$$

Ďalšie vlastnosti okruhov sú uvedené v nasledovnom tvrdení:

10.4 Lema. *Nech $(A,+,\cdot)$ je okruh a $a,b\in A$. Potom*
*a)* $a\cdot 0_A = 0_A\cdot a = 0_A$
*b)* $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$
*c)* $(-a)\cdot(-b) = a\cdot b$
*d) ak $A$ má jednotku, tak* $a\cdot(-1_A) = (-1_A)\cdot a = -a$.

Dôkaz. a) Platí $a\cdot 0_A = a\cdot(0_A+0_A) = a\cdot 0_A + a\cdot 0_A$, odkiaľ pripočítaním $-a\cdot 0_A$ máme $0_A = a\cdot 0_A$. Analogicky sa ukáže $0_A\cdot a = 0_A$.

b) Platí $a\cdot b+a\cdot(-b) = a\cdot(b+(-b)) = a\cdot 0_A = 0_A$, odkiaľ vyplýva $a\cdot(-b) = -(a\cdot b)$. Analogicky sa ukáže $(-a)\cdot b = -(a\cdot b)$.

c) Tvrdenie bezprostredne vyplýva z b).

d) Podľa b) platí $a\cdot(-1_A) = -(a\cdot 1_A) = -a$. Analogicky $(-1_A)\cdot a = -(1_A\cdot a) = -a$. □

Ak o prvkoch $a$, $b$, $x$ okruhu $(A,+,\cdot)$ platí $b+x=a$ hovoríme, že $x$ je *rozdiel* prvkov $a$, $b$ (v uvedenom poradí) a píšeme $x=a-b$. Pretože $(A,+)$ je grupa, má rovnica $b+x=a$ (s neznámou $x$) jediné riešenie (veta 2.28) $x=a+(-b)$. V okruhu je teda pre každé dva prvky $a$, $b$ jednoznačne určený ich rozdiel $a-b=a+(-b)$ (rozdiel prvkov $a$, $b$ je súčet prvku $a$ a prvku opačného k prvku $b$).

Pod rádom prvku $a$ v okruhu $(A,+,\cdot)$ sa vždy myslí jeho rád v aditívnej grupe $(A,+)$, t.j. najmenšie kladné celé číslo $k$ také, že $k\times a = 0_A$, ak také $k$ existuje a $\infty$, ak také $k$ neexistuje. Najmenší spoločný násobok rádov prvkov okruhu (ak existuje) sa nazýva *charakteristikou okruhu* v zmysle nasledujúcej definície.

10.5 Definícia. *Charakteristikou okruhu $A$ nazývame najmenšie kladné celé číslo $k$ také, že $k\times a = 0_A$ pre všetky $a\in A$. Ak také číslo $k$ neexistuje, charakteristika okruhu $A$ je nekonečno. Píšeme* $\operatorname{char} A = k$ *resp.* $\operatorname{char} A = \infty$.

10.6 Veta. *Ak okruh $A$ má jednotku, jeho charakteristika sa rovná rádu jednotky, t.j.* $\operatorname{char} A = r(1_A)$.

Dôkaz. Predpokladajme, že okruh $A$ má jednotku a že $r(1_A)=k$. Teda $k\times 1_A = (1_A+1_A+\cdots+1_A)_{k\text{-krát}} = 0_A$. Pretože pre ľubovoľné $a\in A$ platí $a = 1_A\cdot a$, môžeme písať s použitím lemy 10.3

$$k\times a = (a+\cdots+a)_{k\text{-krát}} = (1_A\cdot a+\cdots+1_A\cdot a)_{k\text{-krát}} = \\ = (1_A+\cdots+1_A)_{k\text{-krát}}\cdot a = (k\times 1_A)\cdot a = 0_A\cdot a = 0_A.$$

V tomto prípade je teda zrejmé, že $\operatorname{char} A = r(1_A) = k$. Ak $r(1_A)=\infty$, neexistuje kladné celé číslo $k$ tak, aby $k\times 1_A = 0_A$, a teda $\operatorname{char} A = \infty$. □

**10.7 Príklad.** Jedným z najznámejších okruhov je okruh $(\overline{Z}_m,\oplus,\odot)$ zvyškových tried modulo $m$, ktorým sme sa zaoberali už v 1. kapitole. Všimnime si, že tvrdenia vo vete 1.5 vlastne hovoria, že $(\overline{Z}_m,\oplus,\odot)$ je komutatíny okruh. Podľa 10.6 je jeho charakteristika $\operatorname{char}\overline{Z}_m = r(\overline{1}) = m$. V kapitole 12 sa budeme zaoberať ďalšími vlastnosťami tohto okruhu.

**10.8 Príklad.** K okruhu $(Z,+,\cdot)$ v príklade 10.1 priradíme okruh $(M_{2,2}(Z),+,\cdot)$ celočíselných matíc typu $2\times 2$ so sčítaním a násobením danými vzťahmi

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix} + \begin{pmatrix} a' & b'\\ c' & d'\end{pmatrix} = \begin{pmatrix} a+a' & b+b'\\ c+c' & d+d'\end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Ľahko je vidieť, že komutatívnosť a asociatívnosť sčítania matíc vyplývajú priamo z komutatívnosti a asociatívnosti sčítania celých čísel. Podobne, z vlastností grupy $(Z, +)$ je zrejmé, že nulou okruhu je matica $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ a opačným prvkom k matici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ je matica $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. Preverenie asociatívnosti násobenia matíc a distributívnosti násobenia vzhľadom na sčítanie prenechávame na čitateľa (cvičenie 2). Okruh $(M_{2,2}(Z), +, \cdot)$ nazývame tiež okruhom štvorcových matíc stupňa 2 nad $Z$. Je zrejmé, že analogické okruhy matíc možno vytvoriť aj nad ďalšími číselnými okruhmi $(Q, +, \cdot)$, $(R, +, \cdot)$ a $(C, +, \cdot)$. (V lineárnej algebre sa neskôr budeme zaoberať aj maticami všeobecného typu $m \times n$.) Vo všetkých týchto okruhoch matíc nad niektorým číselným okruhom je jednotkou matica $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (cvičenie 3) a podľa 10.6 je ich charakteristika $r\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \infty$. Zaujímavé je, že násobenie matíc nie je komutatívna operácia, pretože napr.

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

ale

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

Tiež si všimnime, že súčin dvoch nenulových prvkov okruhu môže byť nulou okruhu.

**10.9 Príklad.** K okruhu reálnych čísel $(R, +, \cdot)$ s obvyklým sčítaním a násobením možno priradiť okruh $(R^R, \oplus, \odot)$ všetkých funkcií $f : R \to R$ so sčítaním a násobením definovanými „bodovo“:

$$\forall x \in R;\ (f \oplus g)(x) = f(x) + g(x)$$
$$\forall x \in R;\ (f \odot g)(x) = f(x) \cdot g(x).$$

Podobne ako v predchádzajúcom príklade je zrejmé, že vlastnosti operácií $+$ a $\cdot$ na $R$ sa priamo prenesú na operácie $\oplus$ a $\odot$ na $R^R$. Na čitateľa prenechávame preveriť, že je tomu tak v prípade komutatívnosti a asociatívnosti násobenia (cvičenie 4). Distributívnosť operácie $\odot$ vzhľadom na operáciu $\oplus$ tiež priamo vyplýva z distributívnosti $\cdot$ vzhľadom na $+$ na $R$, pretože pre ľubovoľné $f, g, h \in R^R$ a $x \in R$ platí

$$[f \odot (g \oplus h)](x) = f(x) \cdot (g \oplus h)(x) = f(x) \cdot (g(x) + h(x)) =$$
$$f(x) \cdot g(x) + f(x) \cdot h(x) = (f \odot g)(x) + (f \odot h)(x) = [(f \odot g) \oplus (f \odot h)](x).$$

Teda $[f \odot (g \oplus h)] = [(f \odot g) \oplus (f \odot h)]$ a analogicky platí distributívnosť sprava. Nulovým prvkom $0_{R^R}$ je evidentne funkcia identicky rovná nule a opačným prvkom k funkcií $f$ je funkcia $\ominus f$ daná predpisom $(\ominus f)(x) = -f(x)$. Okruh $(R^R, +, \cdot)$ má ako jednotkový prvok funkciu identicky rovnú jednej. Opäť je zrejmé z vety 10.6, že $\operatorname{char} R^R = \infty$. K funkciám $f$ takým, že $\forall x \in R;\ f(x) \neq 0$ existuje aj inverzný prvok

$\frac{1}{f}(x) = \frac{1}{f(x)}$, pretože $(f \odot \frac{1}{f})(x) = f(x) \cdot \frac{1}{f(x)} = 1$. Okruh $(R^R, \oplus, \odot)$ nazývame okruhom funkcií definovaných bodovo nad $R$. Opäť si všimnime, že súčin dvoch nenulových prvkov môže byť nula okruhu - napr. súčin funkcií $f, g$ takých, že pre $x \geq 0$ je $f(x) = -\pi$ a $g(x) = 0$ a pre $x < 0$ je $f(x) = 0$ a $g(x) = \sqrt{2}$ je nulová funkcia, t.j. nula okruhu $R^R$.

Analogicky ako pri grupách, aj u okruhov možno hovoriť o podalgebrách (podokruhoch) daného okruhu.

10.10 Definícia. *Okruh $(B, \oplus, \odot)$ sa nazýva podokruhom okruhu $(A, +, \cdot)$, ak jeho operácie $\oplus$ a $\odot$ sú zúžením operácií $+$ resp. $\cdot$ na množinu $B$, t.j.*

$$\forall a, b \in B;\ a \oplus b = a + b \wedge a \odot b = a \cdot b.$$

*Okruh $A$ sa potom nazýva nadokruhom okruhu $B$.*

Aby teda daná neprázdna podmnožina $B$ okruhu $(A, +, \cdot)$ určovala (alebo hovoríme: indukovala) podokruh okruhu $A$, musí byť v prvom rade uzavretá vzhľadom na sčítanie a násobenie okruhu $A$. Nasledujúci príklad ukazuje, že to nestačí.

**10.11 Príklad.** V okruhu $(R, +, \cdot)$ reálnych čísel uvažujme o podmnožine $S = \{a + b\sqrt{3} \mid a, b \in N^+\}$. Je ľahké presvedčiť sa, že množina $S$ je uzavretá vzhľadom na sčítanie a násobenie reálnych čísel. Skutočne, pre ľubovoľné $a, b, c, d \in N^+$ platí

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3} \in S,$$
$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} \in S.$$

Napriek tomu je jasné, že nejde o podokruh okruhu $(R, +, \cdot)$, pretože algebra $(S, +, \cdot)$ nie je vôbec okruhom. Hoci $(S, \cdot)$ je pologrupa a násobenie je distributívne vzhľadom na sčítanie v algebre $(S, +, \cdot)$, $(S, +)$ je len komutatívna pologrupa, keďže $0 = 0 + 0\sqrt{3} \notin S$.

Kritérium, či daná podmnožina okruhu je vzhľadom na zúžené operácie podokruhom je obsiahnuté v nasledujúcej vete.

10.12 Veta. *Nech $(A, +, \cdot)$ je okruh a $B$ je neprázdna podmnožina $A$. Podmnožina $B$ indukuje podokruh okruhu $A$ práve vtedy, keď*

$$\forall a, b \in B;\ a + (-b) \in B \wedge a \cdot b \in B. \tag{1}$$

Dôkaz. Ak $(B, +, \cdot)$ je podokruh okruhu $(A, +, \cdot)$ tak (1) evidentne platí. Obrátene, nech pre neprázdnu podmnožinu $B$ množiny $A$ platí podmienka (1). Je zrejmé, že so „zdedenými“ operáciami sčítania a násobenia okruhu $A$ „zdedila“ podmnožina $B$ aj asociatívnosť oboch operácií, komutatívnosť sčítania a distributívnosť násobenia vzhľadom na sčítanie. Ostatné axiómy okruhu pre $(B, +, \cdot)$ možno tiež ľahko odvodiť z (1) (cvičenie 5; pozri aj vetu 2.24). Teda $(B, +, \cdot)$ je podokruhom okruhu $(A, +, \cdot)$. □

Najmenším (v zmysle množinovej inklúzie) podokruhom ľubovoľného okruhu je zrejme okruh $(\{0_A\}, +, \cdot)$ – hovoríme mu *triviálny okruh*. Zaujímať nás však budú

netriviálne podokruhy daných okruhov. Jeden zaujímavý podokruh okruhu $C$ je uvedený v nasledujúcom príklade.

**10.13 Príklad.** a) Nech $(C, +, \cdot)$ je okruh komplexných čísel. Označme symbolom $Z[i]$ podmnožinu tých komplexných čísel, ktoré majú tvar $a+bi$, kde $a, b \in Z$. Ukážeme, že $(Z[i], +, \cdot)$ je podokruh okruhu $(C, +, \cdot)$ – niekedy sa mu hovorí okruh Gaussových celých čísel. Stačí preveriť podmienku (1) z vety 10.12. Je zrejmé, že pre všetky $c, d \in Z$ je $-(c + di) = (-c) + (-d)i$. Teda

$$\forall a, b, c, d \in Z;\ (a + bi) + (-c) + (-d)i = (a - c) + (b - d)i \in Z[i].$$

Taktiež platí

$$\forall a, b, c, d \in Z;\ (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \in Z[i].$$

Teda $(Z[i], +, \cdot)$ je podokruh okruhu $(C, +, \cdot)$.

b) Ukážeme, že množina $A = \{a + b \cdot \sqrt[3]{2} \mid a, b \in Z\}$ netvorí podokruh okruhu $(R, +, \cdot)$.

Predpokladajme, že $A$ je podokruhom okruhu $(R, +, \cdot)$. Potom (pretože $0 + 1 \cdot \sqrt[3]{2} = \sqrt[3]{2} \in A$) platí $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4} \in A$, teda existujú celé čísla $x, y$ také, že

$$\sqrt[3]{4} = x + y \cdot \sqrt[3]{2}. \tag{2}$$

Z (2) dostávame (po vynásobení oboch strán rovnosti číslom $\sqrt[3]{2}$)

$$2 = x \cdot \sqrt[3]{2} + y \cdot \sqrt[3]{4}. \tag{3}$$

Z (2) a (3) máme po úprave

$$2 - xy = (x + y^2) \cdot \sqrt[3]{2}.$$

Ak $x + y^2 \neq 0$, tak $\sqrt[3]{2} = \frac{2-xy}{x+y^2}$ a to je spor s tým, že $\sqrt[3]{2}$ nie je racionálne číslo. Ak $x + y^2 = 0$, tak aj $2 - xy = 0$ a z týchto dvoch rovníc dostávame po úprave $y^3 = -2$, čo je spor s tým, že $y$ je celé číslo.

Platí teda $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4} \notin A$, čo znamená, že $A$ nie je uzavretá vzhľadom na násobenie, a teda nemôže byť podokruhom.

10.14 Veta. *Každý podokruh okruhu $(Z, +, \cdot)$ má tvar $nZ = \{n \cdot k \mid k \in Z\}$ pre nejaké nezáporné celé číslo $n$.*

Dôkaz. Ak $B$ je podokruhom okruhu $Z$, tak $B$ musí byť prvom rade podgrupou aditívnej grupy $(Z, +)$. Pretože grupa $(Z, +)$ je cyklická (s generátorom 1 resp. $-1$), každá jej podrupa $B$ podľa vety 5.11 je tiež cyklická, čiže generovaná nejakým prvkom $n \in Z$, z čoho vyplýva, že $B$ pozostáva zo všetkých násobkov generátora $n$. Ak teda $B$ je podokruhom okruhu $Z$, tak $B = nZ = \{n \cdot k \mid k \in Z\}$ pre nejaké nezáporné celé číslo $n$. Ľahko sa overí, že každá podmnožina $B = nZ$ skutočne indukuje podokruh okruhu $(Z, +, \cdot)$. Pre $n = 0$ máme triviálny podokruh $0Z = \{0\}$, pre $n = 1$ máme *nevlastný* podokruh $1Z = Z$ a pre $n \geq 2$ máme *vlastné* netriviálne podokruhy $nZ$. □

Podobne ako u grúp, aj u okruhov budeme o najmenšom podokruhu daného okruhu $A$ obsahujúcom vybranú množinu prvkov $M \subseteq A$ hovoriť, že je to podokruh generovaný množinou $M$ a označovať ho $\langle M \rangle$. Ak $M = \{a_1, \ldots, a_n\}$, tak podokruh generovaný množinou $M$ označíme $\langle a_1, \ldots, a_n \rangle$ a hovoríme, že je generovaný prvkami $a_1, \ldots, a_n$.

10.15 Veta. *Nech $(A,+,\cdot)$ je okruh a $\varnothing \neq M \subseteq A$. Podokruh $\langle M\rangle$ generovaný množinou $M$ je prienikom všetkých podokruhov obsahujúcich množinu $M$.*

Dôkaz. Nech $\{B_i \mid i \in I\}$, kde $I$ je neprázdna indexová množina, je množina všetkých podokruhov okruhu $A$ obsahujúcich množinu $M$. Našou úlohou je ukázať, že $\cap_{i\in I} B_i = \langle M\rangle$. Prenechávame na čitateľa overiť, že $\cap_{i\in I} B_i$, je opäť podokruhom okruhu $A$ (cvičenie 6). Pretože každý prvok $m \in M$ patrí do každého podokruhu $B_i$, patrí aj do $\cap_{i\in I} B_i$, čiže podookruh $\cap_{i\in I} B_i$ okruhu $A$ obsahuje množinu $M$. Keďže $\langle M\rangle$ je definovaný ako najmenší podokruh okruhu $A$ obsahujúci $M$, máme inklúziu $\langle M\rangle \subseteq \cap_{i\in I} B_i$. Na druhej strane, keďže samotný podokruh $\langle M\rangle$ je jedným z prvkov množiny $\{B_i \mid i \in I\}$ (lebo je podokruhom $A$ a obsahuje $M$), musí byť $\cap_{i\in I} B_i \subseteq \langle M\rangle$ . Teda $\langle M\rangle = \cap B_i$ a dôkaz je skončený. □

Tak ako izomorfizmus grúp bol definovaný ako bijekcia grúp zachovávajúca grupové operácie, izomorfizmus okruhov bude definovaný ako bijekcia okruhov zachovávajúca operácie okruhu.

10.16 Definícia. *Nech $(A,+,\cdot)$, $(B,\oplus,\odot)$ sú okruhy. Bijektívne zobrazenie $f : A \to B$, ktoré zachováva sčítanie a násobenie okruhov, t.j.*

$$\forall x, y \in A;\ f(x+y) = f(x) \oplus f(y) \ \wedge\ f(x\cdot y) = f(x) \odot f(y)$$

*sa nazýva izomorfizmus okruhu $(A,+,\cdot)$ na okruh $(B,\oplus,\odot)$, Hovoríme, že okruh $A$ je izomorfný s okruhom $B$ a píšeme $A \cong B$.*

Podobne ako izomorfné grupy, ani izomorfné okruhy nepovažujeme z algebraického hľadiska za rôzne. Preto napr. bežne stotožňujeme okruh $(Z,+,\cdot)$ celých čísel s podokruhom $\{\frac{p}{1} \mid p \in Z\}$ okruhu racionálnych čísel $(Q,+,\cdot)$, hoci, ako ukážeme v kapitole 13, okruh $(Q,+,\cdot)$ neobsahuje priamo celé čísla. Podokruh $\{\frac{p}{1} \mid p \in Z\}$ okruhu $Q$ je však izomorfnou kópiou okruhu $Z$ pri izomorfizme $f : Z \to Q$, $f(p) = \frac{p}{1}$.

Prenechávame na čitateľa overiť (cvičenie 7) niekoľko nasledujúcich tvrdení o izomorfizme okruhov, ktoré sú analogickými tvrdeniami k vetám o izomorfizme grúp uvedeným v kapitole 3.

10.17 Veta. *1. Ak $f$ je izomorfizmus okruhu $(A,+,\cdot)$ na okruh $(B,\oplus,\odot)$, tak inverzné zobrazenie $f^{-1}$ je izomorfizmus okruhu $(B,\oplus,\odot)$ na okruh $(A,+,\cdot)$.*

*2. Ak $f : A \to B$ a $g : B \to C$ sú izomorfizmy okruhov, tak aj zložené zobrazenie $g \circ f : A \to C$ je izomorfizmus okruhov.*

*3. Nech $f$ je izomorfizmus okruhu $(A,+,\cdot)$ na okruh $(B,\oplus,\odot)$. Potom platí:*

*a) ak $A$ je komutatívny okruh, tak aj $B$ je komutatívny okruh;*

*b) ak okruh $A$ má jednotkový prvok $1_A$, tak okruh $B$ má jednotkový prok $1_B = f(1_A)$;*

*c) ak $a, a' \in A$ sú navzájom inverzné prvky v okruhu $A$, tak $f(a), f(a')$ sú navzájom inverzné prvky v okruhu $B$.*

## Cvičenia

**1.** Dokážte matematickou indukciou lemu 10.3.

**2.** Overte, že násobenie celočíselných matíc typu $2 \times 2$ je asociatívne a že je distributívne vzhľadom na sčítanie.

**3.** Presvedčte sa o tom, že matica $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ je jednotkovým prvkom okruhu $(M_{2,2}(Z), +, \cdot)$.

**4.** Ukážte, že komutatívnosť a asociatívnosť operáciii $\oplus$ a $\odot$ na $R^R$ definovaných v príklade 10.9 bezprostredne vyplýva z komutatívnosti a asociatívnosti operácií $+$ a $\cdot$ okruhu $(R, +, \cdot)$.

**5.** Podrobne overte jednotlivé kroky dôkazu vety 10.12.

**6.** Dokážte, že ak $\{B_i \mid i \in I\}$ je množina podokruhov okruhu $A$, tak aj $\bigcap(B_i \mid i \in I)$ je podokruhom okruhu $A$.

**7.** Dokážte tvrdenia vo vete 10.17.

**8.** Zistite, či nasledujúce algebry sú okruhmi ( $+$ a $\cdot$ všade znamenajú obvyklé sčítanie a násobenie). Ak áno, určte ich charakteristiku a prípadné ďalšie vlastnosti (jednotka okruhu, komutatívnosť okruhu).

a) $(N, +, \cdot)$

b) $(2Z, +, \cdot)$, kde $2Z$ sú párne celé čísla

c) $(A, +, \cdot)$, kde $A = \{a + b\sqrt{2} \mid a, b \in Z\}$

d) $(B, +, \cdot)$, kde $B = \{a + b\sqrt{2} \mid a, b \in N\}$

e) $(C, +, \cdot)$, kde $C = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} \mid a, b, c \in Q\}$

f) $(K_n, +, \cdot)$, kde $K_n = \{c \in C \mid c^n = 1\}$ je množina $n$-tých komplexných odmocnín z jednej

g) $(K, +, \cdot)$, kde $K = \cup_{n=1}^{\infty} K_n$ je množina všetkých komplexných odmocnín z jednej

h) $\left(\left\{\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in Z\right\}, +, \cdot\right)$ (matice $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ nazývame trojuholníkové)

i) $(N^N, \oplus, \odot)$, kde $N^N$ je množina všetkých funkcií $f : N \to N$ a $\oplus$ a $\odot$ sú operácie definované v príklade 10.9

j) $(R^N, \oplus, \odot)$

k) $(N^R, \oplus, \odot)$

l) $(Q[i], +, \cdot)$, kde $Q[i] = \{a + bi \mid a, b \in Q\}$.

**9.** Nech $\mathcal{P}(X)$ je potenčná množina neprázdnej množiny $X$, t.j množina všetkých podmnožín množiny $X$. Zistite, či $(\mathcal{P}(X), +, \cdot)$ je okruh v nasledujúcich prípadoch, keď pre ľubovoľné $A, B \subseteq X$ je vždy $A \cdot B = A \cap B$ a

a) $A + B = A \cup B$

b) $A + B = A - B$

c) $A + B = A \triangle B = (A \cup B) - (A \cap B)$.

**10.** Zistite, či nasledujúce množiny tvoria podokruhy okruhu $(Z, +, \cdot)$:

a) $Z^- = \{k \in Z \mid k < 0\}$

b) $\{-1, 0, 1\}$

c) $\{3^n \mid n \in Z\}$.

**11.** Nájdite všetky podokruhy okruhov $(Z_8, \oplus, \odot)$ a $(Z_{12}, \oplus, \odot)$.

**12.** Vráťte sa k cvičeniu 8 a u každej algebry o ktorej zistíte, že je okruhom nájdite nejaký jej nadokruh.

**13.** Ukážte, že každý podokruh okruhu $(Z, +, \cdot)$ obsahujúci 1 je totožný so $Z$.

**14.** Nájdite aspoň po tri podokruhy okruhov $Z, Q, R, C, Z[i], Q[\sqrt{2}], M_{2,2}(Z)$.

**15.** Nájdite podokruhy okruhu $(C, +, \cdot)$, ktoré sú generované daným prvkom resp. množinou:

a) $\frac{1}{2}$, b) $i$, c) $\{\frac{3}{4}, i\}$, d) $\{12, 15\}$, e) $\{12, 15, i\}$, f) $Z \cup \{i, \sqrt{2}\}$.

**16.** V nasledujúcich okruhoch určte podokruhy generované uvedeným prvkom (množinou). Nájdite charakteristiky týchto podokruhov.

a) $\langle 3 \rangle$ v $Z_6,\ Z_{24},\ Z_{25}$

b) $\langle 8, 12 \rangle$ v $Z_{18},\ Z_{19},\ Z_{20},\ Z_{30}$

c) $\langle (8, 12) \rangle$ v $Z_{11} \times Z_{13},\ Z_{12} \times Z_{13},\ Z_{16} \times Z_{18},\ Z_{18} \times Z_{16}$.

d) $\langle \{1\}, \{2\} \rangle$, $\langle \{1, 3\}, \{4\} \rangle$, $\langle \{1, 2\}, \{2, 3\} \rangle$, $\langle \{1, 3\}, \{2, 4\} \rangle$ v $\mathcal{P}(\{1, 2, 3, 4\}, \triangle, \cap)$.

**17.** Ukážte, že relácia „byť izomorfný“ na systéme všetkých okruhov je reflexívna, symetrická a tranzitívna.

**18.** Ukážte, že izomorfné okruhy majú rovnakú charakteristiku.

**19.** Ku každému z okruhov v cvičení 8 nájdite aspoň jeden rôzny izomorfný okruh.

**20.** Nájdite izomorfizmus okruhov

a) $(K_4, +, \cdot)$ a $(Z_4, \oplus, \odot)$

b) $(2Z, +, \cdot)$ a $(Z, +, \cdot)$

c) $(Z_3 \times Z_4, \oplus, \odot)$ a $(Z_{12}, \oplus, \odot)$

d) $(Z[\sqrt{2}], +, \cdot)$ a $(Z[-\sqrt{3}], +, \cdot)$

e) $(Z[i], +, \cdot)$ a $(Z \times Z, +, \cdot)$

f) $\left( \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in Z \right\}, +, \cdot \right)$ a $(Z \times Z \times Z, +, \cdot)$

g) $((2Z)^N, \oplus, \odot)$ a $(Z^N, \oplus, \odot)$.

## 11. Adjunkcia, algebraické a transcendentné prvky

Vieme už, že podokruh okruhu $A'$ generovaný neprázdnou množinou $M$ je prienikom všetkých podokruhov, ktoré množinu $M$ obsahujú, t.j. je to najmenší (vzhľadom na usporiadanie inklúziou) podokruh okruhu $A'$ obsahujúci množinu $M$. V súvislosti so skúmaním polynómov nás bude zaujímať hlavne podokruh okruhu $A'$ generovaný množinou $A \cup \{t\}$, pričom $A$ je podokruh okruhu $A'$ a $t \in A' \setminus A$. Naviac, o všetkých okruhoch v tejto kapitole budeme predpokladať, že sú to komutatívne okruhy s jednotkou.

11.1 Príklad. Dokážte, že množina $A = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in Z\right\}$ je nosičom podokruhu okruhu reálnych čísel $R$, ktorý je generovaný množinou $Z \cup \left\{\sqrt[3]{2}\right\}$.

Riešenie. Množina $A$ je nosičom podokruhu okruhu $R$ (podrobne sa presvedčte).

a) Ak $x \in Z$, tak $x \in A$ (lebo $x = x + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4}$). Pretože $\sqrt[3]{2} = 0 + 1 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4}$, tak aj $\sqrt[3]{2} \in A$. Z toho vyplýva, že podokruh $A$ obsahuje množinu $Z \cup \left\{\sqrt[3]{2}\right\}$ a preto $\left\langle Z \cup \left\{\sqrt[3]{2}\right\}\right\rangle \subseteq A$.

b) Nech $x$ je ľubovoľný prvok množiny $A$. Potom existujú $a, b, c \in Z$, že $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Pretože $a, b, c, \sqrt[3]{2}, \sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ sú prvky okruhu $\left\langle Z \cup \left\{\sqrt[3]{2}\right\}\right\rangle$, tak aj $a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \left\langle Z \cup \left\{\sqrt[3]{2}\right\}\right\rangle$, teda $A \subseteq \left\langle Z \cup \left\{\sqrt[3]{2}\right\}\right\rangle$.

Z a) a b) vyplýva, že $A = \left\langle Z \cup \left\{\sqrt[3]{2}\right\}\right\rangle$.

Podobným postupom ako v uvedenom príklade môžeme dokázať nasledovné tvrdenie.

11.2 Veta. *Nech $(A', +, \cdot)$ je komutatívny okruh s jednotkou a nech $(A, +, \cdot)$ je jeho podokruh, ktorý obsahuje jednotku. Ak $t \in A' \setminus A$, tak*

$$\langle A \cup \{t\}\rangle = \{a_0 + a_1 t + \cdots + a_n t^n \mid a_0, a_1, \ldots, a_n \in A,\ n \in N\}.$$

Dôkaz. Označme $\{a_0 + a_1 t + \cdots + a_n t^n \mid a_0, a_1, \ldots, a_n \in A,\ n \in N\} = B$. Množina $B$ je uzavretá vzhľadom na odčítanie a násobenie (podrobne sa presvedčte), teda $(B, +, \cdot)$ je podokruh okruhu $(A', +, \cdot)$.

Pretože $A \cup \{t\} \subseteq B$ (opäť sa podrobne presvedčte) a podokruh $\langle A \cup \{t\}\rangle$ je najmenším z podokruhov, ktoré obsahujú množinu $A \cup \{t\}$, tak $\langle A \cup \{t\}\rangle \subseteq B$.

Ak $x \in A$, tak existujú $a_0, a_1, \ldots, a_n \in A$, $n \in N$, že $x = a_0 + a_1 t + \cdots + a_n t^n$. Pretože $a_0, a_1, \ldots, a_n, t \in \langle A \cup \{t\}\rangle$, tak aj $x \in \langle A \cup \{t\}\rangle$ čo znamená, že aj $B \subseteq \langle A \cup \{t\}\rangle$.

Preto $\langle A \cup \{t\}\rangle = B$. □

Okruh $\langle A \cup \{t\}\rangle$ (aj jeho nosič) budeme označovať $A[t]$ a budeme hovoriť, že vznikol *adjunkciou* prvku $t$ k okruhu $A$. Prvky okruhu $A[t]$ budeme často označovať $a(t)$, $b(t)$, $f(t)$ a pod.

Prvky $1 + 2i^2 + 3i^4$, $3 + i^2$, kde $i \in C$ je imaginárna jednotka sú (podľa vety 11.2) prvkami okruhu $Z[i]$. Platí $1 + 2i^2 + 3i^4 = 3 + i^2$ z čoho po úprave dostávame $-2 + i^2 + 3i^4 = 0$. Všimnime si, že v okruhu $Z[i]$ je možné jeden prvok vyjadriť viacerými spôsobmi a že rovnosť tvaru $a_0 + a_1 i + \ldots a_n i^n = 0$ môže platiť aj v prípade, keď prvky $a_0, a_1, \ldots, a_n$ nie sú všetky nulové. V uvedenom prípade je $a_0 = -2$, $a_1 = 0$, $a_2 = 1$, $a_3 = 0$, $a_4 = 3$.

Vieme už, že každý prvok $a(t)$ okruhu $A[t]$ môžeme zapísať v tvare

$$a(t) = a_0 + a_1 t + \cdots + a_n t^n, \tag{1}$$

kde $a_0, a_1, \ldots, a_n \in A$, $n \in N$.

Ak pre ľubovoľný prvok $a(t) \in A[t]$ tvaru (1) platí $a(t) = 0_A$ vtedy a len vtedy, keď $a_0 = a_1 = \cdots = a_n = 0_A$ hovoríme, že prvok $t$ je *transcendentným* prvkom nad okruhom $A$. Ak existuje taký prvok $a(t) \in A[t]$ tvaru (1), pre ktorý platí $a(t) = 0_A$ a aspoň jeden z prvkov $a_0, a_1, \ldots, a_n$ je nenulový hovoríme, že $t$ je *algebraickým* prvkom nad okruhom $A$. Algebraické prvky nad okruhmi $Z$, $Q$, $R$ nazývame aj algebraickými číslami.

11.3 Príklad. Ukážte, že číslo $\sqrt{3} - \sqrt{2}$ je algebraickým číslom nad okruhom $Z$.

Riešenie. Označme $t = \sqrt{3} - \sqrt{2}$. Potom $t^2 = 5 - 2\sqrt{6}$. Z toho dostávame $t^2 - 5 = -2\sqrt{6}$. Ďalej, opäť po umocnení a po úprave máme $t^4 - 10t^2 + 1 = 0$, teda $(\sqrt{3} - \sqrt{2})^4 - 10(\sqrt{3} - \sqrt{2})^2 + 1 = 0$ čo znamená, že $\sqrt{3} - \sqrt{2}$ je algebraickým číslom nad okruhom $Z$.

O číslach $\pi$ (Ludolfovo číslo), $e$ (základ prirodzených logaritmov) je možné ukázať, že sú transcendentnými nad okruhom $Z$ (resp. $Q$).

Ak uvažujeme dva algebraické prvky $t_1$, $t_2$ nad okruhom $A$, tak okruhy $A[t_1]$, $A[t_2]$ nemusia byť (ako ukazuje nasledujúci príklad) izomorfné.

11.4 Príklad. Dokážte, že okruhy $Z[\sqrt{2}]$, $Z[i]$ nie sú izomorfné.

Dôkaz. Nosiče okruhov $Z[\sqrt{2}]$, $Z[i]$ sú množiny $\{a + b\sqrt{2} \mid a, b \in Z\}$, $\{a + bi \mid a, b \in Z\}$ (podrobne sa presvedčte). Pri dôkaze, že dané okruhy nie sú izomorfné budeme postupovať sporom. Predpokladajme, že existuje izomorfné zobrazenie $f : Z[\sqrt{2}] \to Z[i]$. Vieme, že $f(1) = 1$. Preto napríklad $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$. Nech $f(2) = a + bi$. Pre číslo 2 potom platí:

$$2 = f(2) = f(\sqrt{2} \cdot \sqrt{2}) = f(\sqrt{2}) \cdot f(\sqrt{2}) = (a + bi) \cdot (a + bi) = a^2 - b^2 + 2abi.$$

Pretože 2 je celé číslo, tak $a = 0$ alebo $b = 0$.

Ak $a = 0$, tak $2 = -b^2$, čo je spor (lebo 2 je kladné číslo).

Ak $b = 0$, tak $2 = a^2$, čo je opäť spor (lebo neexistuje celé číslo, ktorého druhá mocnina je 2).

Nemôže teda existovať izomorfné zobrazenie okruhu $Z[\sqrt{2}]$ na okruh $Z[i]$.

Ak $x$, $y$ sú transcendentné prvky nad okruhom $A$, tak možno ukázať, že okruhy $A[x]$ a $A[y]$ sú izomorfné. Izomorfizmom je zobrazenie

$$f : A[x] \to A[y], \quad f(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1y + \cdots + a_ny^n.$$

Dá sa ukázať, že k ľubovoľnému okruhu $A$ (komutatívnemu s jednotkou) existuje nadokruh $A'$ a prvok $t \in A' \setminus A$, ktoré je transcedentným prvkom nad okruhom $A$.

Z uvedených poznatkov vyplýva, že vždy môžeme predpokladať existenciu transcendentného prvku nad ľubovoľným okruhom (a že na jeho označení nezáleží).

Ak $x$ je transcendentný prvok nad okruhom $A$, tak prvky okruhu $A[x]$ voláme *polynómy (jednej neurčitej)* nad okruhom $A$ a okruh $A[x]$ teda voláme okruh polynómov (jednej neurčitej) nad okruhom $A$. Ak $f(x) \in A[x]$, pričom $f(x) = a_0 + a_1x + \ldots a_nx^n$, $a_n \neq 0_A$, tak prvky $a_0, a_1, \ldots, a_n$ nazývame koeficienty polynómu $f(x)$. Koeficient $a_n$ voláme vedúcim koeficientom a číslo $n$ stupňom polynómu $f(x)$. Ak stupeň polynómu je $n$, tak píšeme $\operatorname{st} f(x) = n$. Stupeň nulového polynómu definujeme ako $-\infty$. Každý nenulový prvok okruhu $A$ je polynómom nultého stupňa.

11.5 VETA. *Nech* $f(x) = a_0 + a_1x + \cdots + a_rx^r$, $g(x) = b_0 + b_1x + \cdots + b_sx^s$ *sú polynómy nad okruhom* $A$, *pričom* $\operatorname{st} f(x) = r$, $\operatorname{st} g(x) = s$. *Potom*

(R) $f(x) = g(x)$ *práve vtedy, keď* $r = s$ *a* $a_i = b_i$ *pre každé* $i \in \{0, 1, \ldots, r\}$.

DÔKAZ. Nech $f(x) = a_0 + a_1x + \cdots + a_rx^r$, $a_r \neq 0_A$, $g(x) = b_0 + b_1x + \cdots + b_sx^s$, $a_s \neq 0_A$ a nech $f(x) = g(x)$. Predpokladajme, že $r \geq s$. Prvok $g(x)$ okruhu $A[x]$ môžeme zapísať v tvare $g(x) = c_0 + c_1x + \cdots + c_rx^r$, kde $c_i = b_i$ pre $i \in \{0, \ldots, s\}$ a $c_j = 0_A$ inak. Z rovnosti $f(x) = g(x)$ po úprave dostávame

$$f(x) - g(x) = (a_0 - c_0) + (a_1 - c_1)x + \cdots + (a_r - c_r)x^r = 0_A.$$

Pretože $x$ je transcedentný prvok, tak $a_i - c_i = 0_A$ (t.j. $a_i = c_i$) pre každé $i \in \{0, \ldots, r\}$. Preto $\operatorname{st} f(x) = \operatorname{st} g(x)$ (lebo $b_r = c_r = a_r \neq 0_A$) a $a_i = b_i$ pre každé $i \in \{o, \ldots, r\}$.

Obrátene, ak $\operatorname{st} f(x) = \operatorname{st} g(x)$ a pre každé $i \in \{0, \ldots, \operatorname{st} f(x)\}$ je $a_i = b_i$, tak zrejme $f(x) = g(x)$.

Z vlastností operácií okruhu vyplýva, že súčtom polynómov

$$f(x) = a_0 + a_1x + \cdots + a_rx^r, \quad f(x) = b_0 + b_1x + \cdots + b_sx^s, \quad r \geq s$$

je polynóm

(S) $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_rx^r$

a ich súčinom je polynóm

(N) $$f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{r+s}x^{r+s},$$

kde $c_k = \sum_{i=0}^{k} a_ib_{k-i}$, pre $k \in \{0, 1, \ldots, r + s\}$.

Zovšeobecnením predchádzajúcich úvah je možné analogicky zaviesť okruh polynómov viac neurčitých. Podobným postupom, ako vo vete 11.2 je možné dokázať nasledujúce tvrdenie.

11.6 VETA. *Nech* $(A', +, \cdot)$ *je komutatívny okruh s jednotkou a nech* $(A, +, \cdot)$ *je jeho podokruh, ktorý obsahuje jednotku. Ak* $t_1, \ldots, t_n \in A' \setminus A$, *tak nosičom podokruhu* $\langle A \cup \{t_1, \ldots, t_n\}\rangle$ *je množina*

$$\{a_0t_1^{k_{01}} \ldots t_n^{k_{0n}} + \cdots + a_rt_1^{k_{r1}} \ldots t_n^{k_{rn}} \mid a_0, \ldots, a_r \in A, k_{01}, \ldots, k_{rn} \in N\}.$$

Okruh $\langle A \cup \{t_1, \ldots, t_n\}\rangle$ budeme označovať $A[t_1, \ldots, t_n]$ a budeme hovoriť, že vznikol adjunkciou prvkov $t_1, \ldots, t_n$ k okruhu $A$. Prvok (súčet)

(2) $$a_0t_1^{k_{01}} \ldots t_n^{k_{0n}} + \cdots + a_rt_1^{k_{r1}} \ldots t_n^{k_{rn}}$$

môže obsahovať aj viac členov s tou istou $n$-ticou exponentov. Ak sú všetky usporiadané $n$-tice exponentov v súčte (2) navzájom rôzne, tak hovoríme, že súčet (2) je zapísaný v *kanonickom* tvare. Ak pre každý kanonický tvar súčtu (2) platí

$$a_0t_1^{k_{01}} \ldots t_n^{k_{0n}} + \cdots + a_rt_1^{k_{r1}} \ldots t_n^{k_{rn}} = 0_A$$

práve vtedy, keď $a_0 = \cdots = a_r = 0_A$ hovoríme, že prvky $t_1, \ldots, t_n$ sú nad okruhom $A$ *algebraicky nezávislé*. Ak existuje taký kanonický tvar súčtu (2), ktorý sa rovná nulovému prvku a aspoň jeden z prvkov $a_0, \ldots, a_r$ je nenulový hovoríme, že prvky $t_1, \ldots, t_n$ sú nad okruhom $A$ *algebraicky závislé*.

Nech prvky $x_1, x_2, \ldots, x_n$ sú algebraicky nezávislé nad okruhom $A$. Podokruh generovaný množinou $A \cup \{x_1, x_2, \ldots, x_n\}$ nazývame *okruh polynómov neurčitých* $x_1, x_2, \ldots, x_n$ *nad okruhom* $A$. Prvky okruhu $A[x_1, x_2, \ldots, x_n]$ nazývame *polynómy neurčitých* $x_1, x_2, \ldots, x_n$ *nad okruhom* $A$ a prvky $x_1, x_2, \ldots, x_n$ nazývame *neurčité*.

Podrobnejšie sa s polynómami oboznámite neskôr.

## Cvičenia

**1.** Dokážte, že
a) $Q\left[\sqrt{8}\right] = Q\left[\sqrt{2}\right]$, b) $Z\left[\sqrt{8}\right] \neq Z\left[\sqrt{2}\right]$, c) $Q\left[1+\sqrt{3}\right] = Q\left[1-\sqrt{3}\right]$.

**2.** Dokážte, že
a) $Q\left[i+\sqrt{2}\right] = Q\left[i, \sqrt{2}\right]$, b) $Q\left[\sqrt{2}+\sqrt{3}\right] = Q\left[\sqrt{2}, \sqrt{3}\right]$.

**3.** Dokážte, že
a) $Q\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} \mid a, b \in Q\right\}$,
b) $Q\left[\sqrt{2}+\sqrt{3}\right] = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in Q\right\}$,
c) $Q\left[\sqrt[3]{-3}\right] = \left\{a + b\sqrt[3]{-3} + c\sqrt[3]{9} \mid a, b, c \in Q\right\}$,
d) $Q\left[i+\sqrt{2}\right] = \left\{a + b\sqrt{2} + ci + di\sqrt{2} \mid a, b, c, d \in Q\right\}$.

**4.** Dokážte, že platí:
a) $Q \subset Q\left[i\right] \subset Q\left[i+\sqrt{2}\right]$, b) $Q \subset Q\left[\sqrt{6}\right] \subset Q\left[\sqrt{2}, \sqrt{3}\right]$.

**5.** Dokážte, že neplatí ani $Q\left[\sqrt{2}\right] \subseteq Q\left[\sqrt{6}\right]$ ani $Q\left[\sqrt{6}\right] \subseteq Q\left[\sqrt{2}\right]$.

**6.** Dokážte, že číslo a) $\sqrt{5}+1$, b) $2-3i$, c) $\sqrt{3}-\sqrt{2}$, d) $\sqrt{2+\sqrt{2}}$, e) $\sqrt{3}+\frac{1}{\sqrt{3}}$, f) $\sqrt{5}+\sqrt[4]{5}$, g) $\sqrt[3]{3}+\sqrt[3]{9}$ je algebraické nad $Q$.

**7.** Určte nosič okruhu $Q\left[\sqrt[4]{2}\right]$.

**8.** Nech $t$ je transcendentný prvok nad okruhom $A$. Dokážte, že aj $t+1$ je transcendentný nad $A$.

**9.** Nech $t$ je transcendentný prvok nad okruhom $A$. Dokážte, že aj $t \cdot x$, kde $x \in A$, $x \neq 0_A$ je transcendentný nad $A$.

**10.** Dokážte, že okruhy $Q[\sqrt{2}]$, $Q[\sqrt{3}]$ nie sú izomorfné.

## 12. Obory integrity, telesá, polia

V príkladoch 10.8 a 10.9 sme upozornili na to, že súčin dvoch nenulových prvkov okruhu môže byť rovný nule. Také prvky okruhov nazývame *deliteľmi nuly* v zmysle nasledujúcej definície.

12.1 Definícia. *Nenulový prvok $a$ okruhu $(A, +, \cdot)$ nazývame pravým (ľavým) deliteľom nuly, ak existuje aspoň jeden nenulový prvok $b \in A$ tak, že $b \cdot a = 0_A$ ($a \cdot b = 0_A$). Každý pravý alebo ľavý deliteľ nuly nazývame deliteľom nuly.*

V príklade 10.8 sme ukázali, že

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_{M_{2,2}(Z)}.$$

Teda matica $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ je ľavým deliteľom nuly a matica $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ pravým deliteľom nuly v okruhu $M_{2,2}(Z)$. Čitateľ iste ľahko nájde ďalšie delitele nuly v okruhu $M_{2,2}(Z)$ (cvičenie 1). V príklade 10.9 sme ako delitele nuly v okruhu $R^R$ uviedli isté funkcie $f, g$. Opäť doporučujeme čitateľovi nájsť ďalšie príklady deliteľov nuly okruhu $R^R$ (cvičenie 2).

12.2 Definícia. *Oborom integrity nazývame netriviálny komutatívny okruh $(A, +, \cdot)$ s jednotkou ktorý nemá delitele nuly, t.j. spĺňa*

$$\forall a, b \in A;\ a \neq 0_A \ \wedge\ b \neq 0_A \Rightarrow a \cdot b \neq 0_A.$$

Dôkaz nasledujúcej lemy prenechávame na čitateľa (cvičenie 3).

12.3 Lema. *Každý podokruh oboru integrity je opäť oborom integrity.*

Pretože okruh $(C, +, \cdot)$ komplexných čísel je zrejme oborom integrity, sú aj číselné okruhy $R, Q, Z$, ktoré sú jeho podokruhmi, obormi integrity.

Predchádzajúce tvrdenie však nemožno modifikovať v tom zmysle, že ak $B$ je podokruh okruhu $A$ a $B$ je obor integrity, tak aj $A$ je obor integrity. Ako kontrapríklad stačí položiť $A = (R^R, \oplus, \odot)$ a zobrať podmnožinu $B$ tých funkcií $f : R \to R$, pre ktoré platí: ak $f(x) = 0$ pre nejaké $x \in R$ tak $f(x) = 0$ pre všetky $x \in R$. Čiže $B$ pozostáva z funkcií, ktorých graf nepretína os $x$ a z nulovej funkcie. Je zrejmé, že $(B, \oplus, \odot)$ je oborom integrity, podokruhom $A$, ale $A$ nie je oborom integrity ako sme ukázali v 10.9.

**12.4 Príklad.** Ukážeme, že okruh $(\overline{Z}_n, \oplus, \odot)$ zvyškových tried modulo $n$ je oborom integrity práve vtedy, keď $n$ je prvočíslo.

Najprv ukážeme, že ak $n$ je prvočíslo, tak $(\overline{Z}_n, \oplus, \odot)$ je obor integrity. Stačí ukázať, že pre ľubovoľné dva prvky $\overline{k}, \overline{m} \in \overline{Z}_n$, $\overline{k} \odot \overline{m} = \overline{0}$ implikuje $\overline{k} = \overline{0}$ alebo $\overline{m} = \overline{0}$. Nech teda $\overline{k} \odot \overline{m} = \overline{0}$, t.j. $\overline{km} = \overline{0}$. Potom $k \cdot m \equiv 0 \pmod{n}$, t.j. $n \mid k \cdot m$. Pretože $n$ je prvočíslo, nutne to implikuje $n \mid k$ alebo $n \mid m$. Teda $\overline{k} = \overline{0}$ alebo $\overline{m} = \overline{0}$, čo bolo treba ukázať.

Obrátene, nech $n$ nie je prvočíslo. Teda $n = k \cdot m$ pre nejaké $1 < k < n$, $1 < m < n$. Potom ale $\overline{k} \in \overline{Z}_n \setminus \{\overline{0}\}$, $\overline{m} \in \overline{Z}_n \setminus \{\overline{0}\}$, pričom $\overline{k} \cdot \overline{m} = \overline{k \cdot m} = \overline{n} = \overline{0}$. Teda $\overline{Z}_n$ nie je oborom integrity.

Keďže obory integrity nemajú delitele nuly, môžeme pri riešení rovníc nad obormi integrity používať pravidlá o krátení sprava i zľava ako to ukazuje nasledujúca veta.

12.5 VETA. *Komutatívny okruh s jednotkou $(A, +, \cdot)$ je oborom integrity práve vtedy, keď v ňom platia nasledujúce zákony o krátení nenulovým prvkom:*

$$\forall x, y \in A, \forall a \in A \setminus \{0_A\};\ ax = ay \Rightarrow x = y \quad \textit{(krátenie zľava)}$$
$$\forall x, y \in A, \forall a \in A \setminus \{0_A\};\ xa = ya \Rightarrow x = y \quad \textit{(krátenie sprava).}$$

**12.6 Poznámka.** Na základe komutatívnosti krátenie zľava implikuje krátenie sprava a obrátene. Stačí teda používať iba jeden z týchto zákonov.

DÔKAZ VETY 12.5. Nech $A$ je obor integrity a platí $ax = ay$, kde $a \neq 0_A$. Potom $ax - ay = 0_A$ t.j. $a \cdot (x - y) = 0_A$. Pretože $A$ nemá delitele nuly a prvok $a \neq 0_A$, musí byť $x - y = 0_A$ t.j. $x = y$.

Obrátene, nech v komutatívnom okruhu $(A, +, \cdot)$ s jednotkou platia zákony o krátení nenulovým prvkom. Predpokladajme, že prvok $a \neq 0_A$ by bol ľavým deliteľom nuly. Potom existuje $b \neq 0_A$ tak, že $a \cdot b = 0_A = a \cdot 0_A$. Po krátení zľava dostaneme $b = 0_A$, spor. Z komutatívnosti vyplýva, že $A$ nemá ani pravé delitele nuly. Teda $A$ je oborom integrity. □

Predchádzajúca veta znamená, že pri riešení rovníc nad číselnými obormi integrity $Z, Q, R, C$ môžeme bez obáv používať pravidlá o krátení nenulovým prvkom, tak ako sme na to zvyknutí aj zo školskej praxe. Ak naša rovnica obsahuje ale operácie + a · z okruhu, ktorý nie je oborom integrity, pri riešení treba postupovať opatrnejšie, tak ako to ukazuje aj nasledujúci príklad.

**12.7 Príklad.** Máme riešiť nad $Z_8$ rovnicu

$$x^2 + 4x + 3 = 0$$

(namiesto symbolov $\oplus$ a $\odot$ pre operácie okruhu $Z_8$ budeme, pre jednoduchosť používať len symboly + a ·). Po úprave máme

$$(x + 1) \cdot (x + 3) = 0.$$

Nad číselnými okruhmi $Z, Q, R, C$ sme zyknutí z toho vyvodiť, že $x+1 = 0 \vee x+3 = 0$. (Dôvodom toho je práve to, že $Z, Q, R, C$ sú obory integrity!) Avšak teraz sme nad $Z_8$, ktorý nie je oborom integrity a má delitele nuly $2, 4, 6$. Preto prípady

$$x + 1 = 0 \vee x + 3 = 0 \Leftrightarrow x = 7 \vee x = 5$$

sú iba jednou z možností. Ďalšími sú

$$x + 1 = 2 \wedge x + 3 = 4 \Leftrightarrow x = 1 \wedge x = 1$$
$$x + 1 = 4 \wedge x + 3 = 2 \Leftrightarrow x = 3 \wedge x = 7$$
$$x + 1 = 4 \wedge x + 3 = 4 \Leftrightarrow x = 3 \wedge x = 1$$
$$x + 1 = 4 \wedge x + 3 = 6 \Leftrightarrow x = 3 \wedge x = 3$$
$$x + 1 = 6 \wedge x + 3 = 4 \Leftrightarrow x = 5 \wedge x = 1.$$

Riešeniami danej rovnice teda sú $x = 7,\ x = 5,\ x = 1$ a $x = 3$.

12.8 Definícia. *Okruh $(A, +, \cdot)$ s jednotkou $1_A \neq 0_A$ v ktorom každý nenulový prvok má vzhľadom na násobenie inverzný prvok, nazývame telesom. Komutatívne teleso, t.j. také kde násobenie je komutatívna operácia, nazývame pole.*

12.9 Poznámka. Ak $(A, +, \cdot)$ je okruh a pre prvky $a$, $b$, $x$, kde $b \neq 0_A$, platí $b \cdot x = a$ hovoríme, že $x$ je *podiel* prvkov $a\,b$ (v uvedenom poradí) a píšeme $x = \frac{a}{b}$ alebo $x = a : b$. Ak $(A, +, \cdot)$ je pole, tak každá rovnica $b \cdot x = a$, $b \neq 0_A$ (s neznámou $x$) má jediné riešenie $x = a \cdot b^{-1}$ (lebo $(A - \{0_A\}, \cdot)$ je grupa). V poli je teda pre každé dva prvky $a$, $b$, $b \neq 0$ jednoznačne určený ich podiel $\frac{a}{b} = a \cdot b^{-1}$ (podiel prvkov $a$, $b$ je súčin prvku $a$ a prvku inverzného k prvku $b$).

Možno ukázať (cvičenie 14), že pre podiely v poli $(A, +, \cdot)$ platí pre každé $a, b, c, d \in A$, $b \neq 0$, $d \neq 0$:

$$\frac{a}{b} = \frac{c}{d} \quad \text{práve vtedy, keď} \quad a \cdot d = b \cdot c, \tag{1}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}, \tag{2}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}, \tag{3}$$

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \tag{4}$$

$$\text{ak} \quad a \neq 0, \quad \text{tak} \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}. \tag{5}$$

**12.10 Príklad.** Z definície 12.8 vyplýva, že okruh $(\overline{Z}_n, \oplus, \odot)$ zvyškových tried modulo $n$ je pole práve vtedy, keď $(\overline{Z}_n \setminus \{\overline{0}\}, \odot)$ je grupa. V príklade 4.5 bolo ukázané, že $(\overline{Z}_n \setminus \{\overline{0}\}, \odot)$ je grupa práve vtedy, keď $n$ je prvočíslo. Dostávame teda, že okruh $(\overline{Z}_n, \oplus, \odot)$ zvyškových tried modulo $n$ je pole práve vtedy, keď $n$ je prvočíslo.

12.11 Veta. *Každé pole je oborom integrity.*

Dôkaz. Nech $(A, +, \cdot)$ je pole a nech $a, b \in A \setminus \{0_A\}$. Potrebujeme ukázať, že aj $a \cdot b \neq 0_A$. Predpokladajme, že by platilo $a \cdot b = 0_A$. Pretože $A$ je pole, k nenulovému prvku $a$ existuje inverzný prvok $a^{-1}$. Dostávame teda $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_A = 0_A$, t.j. $(a^{-1}a)b = 0_A$, čiže $b = 0_A$, spor. Dôkaz je skončený. □

Predchádzajúcu vetu nemožno zrejme obrátiť. Nie každý obor integrity je pole, ako ukazuje príklad oboru integrity $(Z, +, \cdot)$, kde jedine čísla 1 a $-1$ majú inverzný prvok. V konečnom prípade však platí aj obrátené tvrdenie k vete 12.11.

12.12 Veta. *Každý konečný obor integrity je pole.*

Dôkaz. Nech $(A, +, \cdot)$ je konečný obor integrity s prvkami $0_A, a_1, \ldots, a_n$. Už z definície 12.2 vyplýva, že $A$ má jednotku. Aby sme ukázali, že každý nenulový prvok $a_i$ má inverzný prvok, utvorme súčiny $a_i a_1, a_i a_2, \ldots, a_i a_n$. Tieto súčiny sú nenulové a navzájom rôzne, t.j. $\{a_i a_1, \ldots, a_i a_n\} = \{a_1, \ldots, a_n\}$. Ak by totiž napr. $a_i a_1 = a_i a_2$, tak po krátení máme $a_1 = a_2$, spor. Keďže teda súčiny $a_i a_1, \ldots, a_i a_n$ zahŕňajú všetky nenulové prvky z $A$, niektorý z nich, napr. $a_i a_j$, musí byť rovný jednotke, t.j. $a_i a_j = 1_A$. Z komutatívnosti máme, že aj $a_j a_i = 1_A$, čiže $a_j = a_i^{-1}$. Tým je dôkaz vety hotový. □

Z konečných polí teda už poznáme $Z_2, Z_3, Z_5, Z_7, Z_{11}, Z_{13}$, atď. Nekonečným poľom je okruh $(C, +, \cdot)$ všetkých komplexných čísel, i jeho podokruhy (podpolia) $(R, +, \cdot)$ a $(Q, +, \cdot)$. Pritom vieme, že jednotkou vo všetkých týchto okruhoch je číslo 1, k racionálnemu číslu $\frac{p}{q} \in Q \setminus \{0\}$ je inverzným prvkom číslo $\frac{q}{p}$, k reálnemu číslu $r \in R \setminus \{0\}$ je inverzným prvkom číslo $\frac{1}{r}$ a ku komplexnému číslu $a+bi \in C \setminus \{0\}$ je inverzným prvkom číslo $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, pretože platí

$$(a+bi) \cdot \left( \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \right) = \frac{a^2+abi}{a^2+b^2} - \frac{abi-b^2}{a^2+b^2} = \frac{a^2+b^2}{a^2+b^2} = 1.$$

Príkladom nekonečného nečíselného poľa je obor integrity $(B, \oplus, \odot)$ uvedený za lemou 12.3.

Existuje nekonečné teleso, ktoré nie je pole? Také teleso skonštruoval v r. 1843 anglický matematik W.R. Hamilton a jeho konštrukciu si ukážeme v nasledovnom príklade. Prvkami tohto nekomutatívneho telesa sú isté matice typu $2 \times 2$ nad poľom komplexných čísel, ktoré sa nazývajú *kvaternióny* - hovoríme o *telese kvaterniónov.*

**12.13 Príklad.** Nech $H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in C \right\}$. Pripomeňme, že pre komplexné číslo $\alpha = a+bi$ symbol $\overline{\alpha}$ znamená komplexne združené číslo $a-bi$. Teda pre $\beta = c+di$ platí $-\overline{\beta} = -c+di$. Ukážeme, že množina matíc uvedeného špeciálneho tvaru nad poľom $C$ s obvyklým sčítaním a násobením matíc tvorí nekomutatívne teleso.

To, že sčítanie a násobenie matíc sú operácie na $H$ ukazujú nasledovné výpočty:

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} + \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha+\gamma & \beta+\delta \\ -\overline{(\beta+\delta)} & \overline{\alpha+\gamma} \end{pmatrix} \in H,$$
$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \cdot \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\overline{\delta} & \alpha\delta + \beta\overline{\gamma} \\ -\overline{\beta}\gamma - \overline{\alpha\delta} & -\overline{\beta}\delta + \overline{\alpha\gamma} \end{pmatrix} \in H,$$

pretože $\overline{\alpha\gamma - \beta\overline{\delta}} = \overline{\alpha\gamma} - \overline{\beta}\delta$ a $-\overline{(\alpha\delta + \beta\overline{\gamma})} = -\overline{\alpha\delta} - \overline{\beta}\gamma$.

Prenechávame na čitateľa preveriť, že sčítanie a násobenie kvaterniónov sú asociatívne, sčítanie je komutatívne a násobenie kvaterniónov je distributívne vzhľadom na sčítanie (cvičenie 4). Je vidieť, že nulová matica $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ i jednotková matica $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ sú kvaternióny a opačná matica k $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$ je $\begin{pmatrix} -\alpha & -\beta \\ \overline{\beta} & -\overline{\alpha} \end{pmatrix} \in H$. Ostáva ukázať, že každý nenulový kvaternión má v $H$ inverzný prvok a že násobenie kvaterniónov nie je komutatívne. Nech $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ je nenulová matica z $H$, t.j. aspoň jedno z čísel $a, b, c, d$ je rôzne od 0. Potom aj číslo $s = a^2+b^2+c^2+d^2 \neq 0$. Priamym výpočtom sa možno presvedčiť, že inverzným prvkom k uvedenej matici je matica $\begin{pmatrix} \frac{a-bi}{s} & -\frac{c+di}{s} \\ \frac{c-di}{s} & \frac{a+bi}{s} \end{pmatrix}$ (cvičenie 5). Teda $(H, +, \cdot)$ je teleso. Pretože platí napríklad

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

teleso kvaterniónov nie je komutatívne.

Pod podtelesom (podpoľom) daného telesa (poľa) $(A,+,\cdot)$ rozumieme teleso (pole) $(B,\oplus,\odot)$ také, že $B \subseteq A$ a operácie $\oplus$ a $\odot$ sú zúžením operácií $+$ a $\cdot$ na podmnožinu $B$, t.j. platí

$$\forall a,b \in B;\ a \oplus b = a + b \in B \wedge a \odot b = a \cdot b \in B.$$

Inak povedané, je to teleso (pole), ktoré je podokruhom okruhu $A$.

**12.14 Príklad.** V príklade 10.13 sme ukázali, že okruh $Z[i] = \{a+bi \mid a,b \in Z\}$ Gaussových celých čísel je podokruhom poľa $(C,+,\cdot)$ všetkých komplexných čísel. Avšak komutatívny okruh $Z[i]$ nie je telesom. Hoci obsahuje jednotkový prvok $1 = 1+0i$, jediné invertovateľné (t.j. majúce inverzný prvok) prvky v $Z[i]$ sú zrejme $1,-1,i,-i$. Vidíme, že napr. $(1+i)\cdot(\frac{1}{2}-\frac{1}{2}i) = 1$, t.j. $(1+i)^{-1} = \frac{1}{2}-\frac{1}{2}i \notin Z[i]$. Preto podokruh $Z[i]$ poľa $C$ nie je jeho podpoľom. □

V poslednej časti tejto kapitoly sa budeme zaoberať charakteristikou v oboroch integrity a poliach a dôsledkami z nej vyplývajúcimi.

Z vety 10.6 vieme, že v okruhu $(A,+,\cdot)$ s jednotkou je charakteristika okruhu rovná rádu jednotky (v aditívnej grupe $(A,+)$ ), t.j. $\mathrm{char}A = r(1_A)$. Ľahko sa ukáže, že v obore integrity $A$ je rád každého nenulového prvku rovný $\mathrm{char}A$. Skutočne, ak $a \in A \setminus \{0_A\}$, tak pre ľubovoľné kladné celé číslo $k$ možno tak ako v dôkaze 10.6 rozpísať $k \times a = (k \times 1_A)\cdot a$. Keďže $A$ je oborom integrity a platí $a \neq 0_A$, dostávame

$$k \times a = 0_A \Leftrightarrow k \times 1_A = 0_A.$$

Odtiaľ je zrejmé, že $r(a) = r(1_A) = \mathrm{char}A$.

Už vieme, že obor integrity $(Z,+,\cdot)$ má charakteristiku $\infty$ a obor integrity $(Z_p,\oplus,\odot)$, kde $p$ je prvočíslo, má charakteristiku $p$. Teraz ukážeme, že takéto charakteristiky sú jediné možné u oborov integrity.

12.15 Veta. *Charakteristika oboru integrity je buď $\infty$ alebo prvočíslo.*

Dôkaz. Stačí zrejme ukázať, že charakteristika oboru integrity nie je zložené číslo. Nech $\mathrm{char}A = r(1_A) = k$ a predpokladajme, že $k = m\cdot n$, kde $1 < m,n < k$. Potom máme

$$0_A = k \times 1_A = (m\cdot n)\times 1_A = (m\times 1_A)\cdot(n\times 1_A).$$

Pretože $A$ je oborom integrity, dostávame $m\times 1_A = 0_A$ alebo $n\times 1_A = 0_A$, čo je v spore s predpokladom $r(1_A) = k$. □

Vo vete 10.15 sme ukázali, že podokruh $\langle M\rangle$ okruhu $(A,+,\cdot)$ generovaný množinou $M$ je prienikom všetkých podokruhov okruhu $A$ obsahujúcich množinu $M$. Podobne možno ukázať, že prienik všetkých podpolí poľa $(F,+,\cdot)$ obsahujúcich vybranú množinu prvkov $M$ je najmenším podpoľom poľa $(F,+,\cdot)$ obsahujúcim $M$, teda podpoľom generovaným množinou $M$ (označujeme ho tiež symbolom $\langle M\rangle$).

12.16 Veta. *Nech $(A,+,\cdot)$ je obor integrity. Ak $\mathrm{char}A = \infty$, tak $\langle 1_A\rangle \cong Z$. Ak $\mathrm{char}\,A = p$, tak $\langle 1_A\rangle \cong Z_p$.*

Dôkaz. V prvom prípade je zobrazenie $f : Z \to \langle 1_A\rangle$ dané predpisom $f(n) = n\times 1_A$ izomorfizmus okruhu $(Z,+,\cdot)$ na podokruh okruhu $A$ generovaný jednotkou. V druhom prípade je podokruh $\langle 1_A\rangle$ izomorfný s okruhom $(Z_p,\oplus,\odot)$ pri zobrazení $g : Z_p \to \langle 1_A\rangle$ danom predpisom $f(n) = n\times 1_A$, pričom $0 \le n < p$. Prenechávame na čitateľa preveriť, že uvedené zobrazenia sú izomorfizmy (cvičenie 6). □

Pretože pole je oborom integrity, je aj charakteristika poľa buď $\infty$ alebo nejaké prvočíslo $p$. O podpoliach generovaných jednotkou hovorí nasledujúca veta.

12.17 Veta. *Nech $(F,+,\cdot)$ je pole. Ak* $\operatorname{char} F = \infty$, *tak* $\langle 1_F\rangle \cong Q$. *Ak* $\operatorname{char} F = p$, *tak* $\langle 1_F\rangle \cong Z_p$.

Dôkaz. V druhom prípade je izomorfizmus rovnaký ako v 12.16. Ak $\operatorname{char} F = \infty$, treba si uvedomiť ako vyzerá podpole $\langle 1_F\rangle$ generované jednotkovým prvkom $1_F$. Je zrejmé, že pre každé prirodzené číslo $q$ obsahuje aditívnu mocninu $q \times 1_F$ (majme na mysli, že $r(1_F) = \infty$!) i opačný prvok k nej $-(q \times 1_F)$ označovaný $(-q)\times 1_F$. Tiež obsahuje prvok $1_F + (-1_F) = 0_F$. Teda pre každé celé číslo $r$ platí, že $r \times 1_F \in \langle 1_F\rangle$. Zároveň podpole $\langle 1_F\rangle$ musí obsahovať všetky inverzné prvky $(r \times 1_F)^{-1}$. Pozostáva teda zo súčinov $(q \times 1_F)\cdot(r \times 1_F)^{-1}$, kde $q, r \in Z,\ r \neq 0$. Preto zobrazenie $h : Q \to \langle 1_F\rangle$ definované predpisom $h(\frac{q}{r}) = (q\times 1_F)\cdot(r\times 1_F)^{-1}$ je surjektívne. Korektnosť definície zobrazenia $h$ (t.j. to, že rovnosť racionálnych čísel $\frac{q}{r} = \frac{q'}{r'}$ implikuje rovnosť ich obrazov $h(\frac{q}{r}) = h(\frac{q'}{r'})$ ) a jeho injektívnosť vyplývajú z nasledovného výpočtu:

$$\frac{q}{r} = \frac{q'}{r'} \Leftrightarrow r'q = q'r \Leftrightarrow (r'q)\times 1_F = (q'r)\times 1_F \Leftrightarrow (r'\times 1_F)\cdot(q\times 1_F) =$$
$$= (q'\times 1_F)\cdot(r\times 1_F) \Leftrightarrow h\left(\frac{q}{r}\right) = ((q\times 1_F)\times(r\times 1_F)^{-1} =$$
$$= (r'\times 1_F)^{-1}\cdot(q'\times 1_F) = (q'\times 1_F)\cdot(r'\times 1_F)^{-1} = h\left(\frac{q'}{r'}\right).$$

Teda $h$ je bijekcia poľa $Q$ na podpole $\langle 1_F\rangle$. Ostáva ukázať, že $h$ zachováva operácie sčítania a násobenia. Platí

$$h\left(\frac{q}{r}+\frac{q'}{r'}\right) = h\left(\frac{qr'+q'r}{rr'}\right) = ((qr'+q'r)\times 1_F)\cdot((rr')\times 1_F)^{-1} =$$
$$= ((qr')\times 1_F + (q'r)\times 1_F)\cdot((r\times 1_F)\cdot(r'\times 1_F))^{-1} =$$
$$= ((q\times 1_F)\cdot(r'\times 1_F) + (q'\times 1_F)\cdot(r\times 1_F))\cdot(r\times 1_F)^{-1}\cdot(r'\times 1_F)^{-1} =$$
$$= (q\times 1_F)\cdot(r\times 1_F)^{-1} + (q'\times 1_F)\cdot(r'\times 1_F)^{-1} = h\left(\frac{q}{r}\right) + h\left(\frac{q'}{r'}\right),$$

$$h\left(\frac{q}{r}\cdot\frac{q'}{r'}\right) = h\left(\frac{qq'}{rr'}\right) = ((qq')\times 1_F)\cdot((rr')\times 1_F)^{-1} =$$
$$= (q\times 1_F)\cdot(q'\times 1_F)\cdot(r\times 1_F)^{-1}\cdot(r'\times 1_F)^{-1} = h\left(\frac{q}{r}\right)\cdot h\left(\frac{q'}{r'}\right).$$

Teda $h$ je izomorfizmus. □

12.18 Dôsledok. *Každé konečné pole má prvočíselnú charakteristiku.*

Dôkaz. Pretože pole charakteristiky $\infty$ obsahuje podľa 12.17 nekonečné podpole izomorfné s $Q$, charakteristika konečného poľa musí byť prvočíslo. □

Z predchádzajúceho dôsledku a vety vyplýva, že aj každý konečný obor integrity má prvočíselnú charakteristiku. Nie každý obor integrity s prvočíselnou charakteristikou musí byť ale konečný. Napríklad obor integrity $Z_5[x]$ polynómov jednej neurčitej nad poľom $Z_5$ má zrejme charakteristiku 5, ale je nekonečný.

## Cvičenia

**1.** Nájdite aspoň 5 deliteľov nuly v okruhu $M_{2,2}(Z)$.

**2.** Nájdite aspoň 5 deliteľov nuly v okruhu $R^R$.

**3.** Dokážte lemu 12.3.

**4.** Presvedčte sa podrobnými výpočtami, že sčítanie a násobenie kvaterniónov sú asociatívne, sčítanie je komutatívne a násobenie kvaterniónov je distributívne vzhľadom na sčítanie.

**5.** Preverte výpočtom správnosť vzorca inverzného kvaterniónu v príklade 12.13.

**6.** O zobrazeniach $f, g$ v dôkaze vety 12.16 ukážte, že sú izomorfizmy okruhov.

**7.** Nájdite všetky delitele nuly v okruhoch $Z_8, Z_{10}, Z_{12}$ a $Z_{24}$.

**8.** Zistite, či nasledujúci okruh s obvyklými operáciami je oborom integrity, telesom, poľom. Ak nie je oborom integrity, určte jeho delitele nuly. Ak nie je poľom, určte nenulové prvky, ktoré nemajú inverzný prvok. (V úlohách f)–j) symbol $Y^X$ označuje okruh všetkých zobrazení množiny $X$ do okruhu $Y$ s operáciami definovanými „bodovo“.)

a) $Z_3 \times Z_3$
b) $Z \times Z$
c) $A \times B$, kde $A, B$ sú netriviálne okruhy
d) $Q[\sqrt{6}]$
e) $Q[\pi]$
f) $R^N$
g) $R^{[0,1]}$
h) $Z_{12}^{\{0,1\}}$
i) $A^B$, kde $A$ je okruh a $B \neq \varnothing$
j) $\mathcal{P}(X)$, kde $A + B = (A \cup B) - (A \cap B),\ A \cdot B = A \cap B$.

**9.** Zistite, či platí výrok:
a) Každý podokruh poľa je pole.
b) Každý nadokruh poľa je pole.
Ak áno, dokážte ho, ak nie, uveďte kontrapríklad.

**10.** Ukážte, že pole $C$ je izomorfné s okruhom matíc tvaru $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in R$.

**11.** Ukážte, že zvyšková trieda $\overline{k} \in \overline{Z}_n$ nie je deliteľom nuly v $\overline{Z}_n$ práve vtedy, keď $k$ a $n$ sú nesúdeliteľné.

**12.** Ukážte, že $(A, +, \cdot)$ je pole, ak

a) $A = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in Q \right\}$,

b) $A = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in E \right\}$.

**13.** a) Ukážte, že pole $(A, +, \cdot)$ z cvičenia 12 a) je izomorfné s poľom $Q[\sqrt{2}]$.
b) Ukážte, že pole $(A, +, \cdot)$ z cvičenia 12 b) je izomorfné s poľom $(R, +, \cdot)$.

**14.** Dokážte (1) – (5) z poznámky 12.9.

## 13. Podielové pole oboru integrity

Tak ako sa z oboru integrity $(Z, +, \cdot)$ celých čísel známou konštrukciou tvorenia zlomkov a ich stotožňovania podľa určitého pravidla vytvorí pole racionálnych čísel $(Q, +, \cdot)$, možno z ľubovoľného oboru integrity $(A, +, \cdot)$ analogickou konštrukciou zlomkov a ich vhodným stotožňovaním vytvoriť pole, ktoré bude pôvodný obor integrity (presnejšie jeho izomorfnú kópiu) obsahovať ako podokruh. Ide o tzv. konštrukciu *podielového poľa oboru integrity*, ktoré budeme označovať $(Q(A), +, \cdot)$. Zatiaľ, čo v obore integrity $(A, +, \cdot)$ sme mohli prvky sčitovať, odčitovať, násobiť a pritom používať pravidlá o krátení súčinu, v podielovom poli budeme môcť prvky $Q(A)$ (a teda aj prvky $A$) už aj deliť. Pritom podielové pole $(Q(A), +, \cdot)$ bude v istom zmysle najmenšie pole obsahujúce daný obor integrity $(A, +, \cdot)$.

13.1 Definícia. *Nech $(A, +, \cdot)$ je obor integrity. Zlomkom nad $A$ nazývame každú usporiadanú dvojicu $[a, b]$, kde $a \in A$, $b \in A \setminus \{0_A\}$. Množinu všetkých zlomkov nad $A$ budeme označovať symbolom* $\mathrm{Zlom}(A)$. *Dva zlomky $[a, b]$, $[a', b']$ nazývame ekvivalentnými a píšeme $[a, b] \equiv [a', b']$, ak $ab' = a'b$.*

13.2 Lema. *Relácia $\equiv$ je reláciou ekvivalencie na množine* $\mathrm{Zlom}(A)$.

Dôkaz. Pre ľubovoľný zlomok $[a, b]$ nad $A$ platí $ab = ab$, teda $[a, b] \equiv [a, b]$ a relácia $\equiv$ je reflexívna. Symetrickosť $\equiv$ je tiež evidentná. Aby sme ukázali tranzitívnosť, predpokladajme, že $[a, b] \equiv [a_1, b_1]$ a $[a_1, b_1] \equiv [a_2, b_2]$. Potom $ab_1 = a_1 b$ a $a_1 b_2 = a_2 b_1$. Po vynásobení prvej rovnosti prvkom $b_2$ a druhej rovnosti prvkom $b$ dostaneme $ab_1 b_2 = a_1 b b_2$ a $a_1 b_2 b = a_2 b_1 b$. Pretože (na základe komutatívnosti násobenia) $a_1 b b_2 = a_1 b_2 b$, platí aj $ab_1 b_2 = a_2 b_1 b$, čiže (opäť na základe komutatívnosti násobenia) $ab_2 b_1 = a_2 b b_1$. Pretože $A$ je obor integrity, môžeme poslednú rovnosť krátiť sprava nenulovým prvkom $b_1$. Dostaneme $ab_2 = a_2 b$, z čoho vyplýva $[a, b] \equiv [a_2, b_2]$. □

Sčítanie a násobenie zlomkov nad ľubovoľným oborom integrity definujeme nasledovne:

$$[a, b] \boxplus [c, d] = [ad + bc, bd], \tag{1}$$

$$[a, b] \boxdot [c, d] = [ac, bd]. \tag{2}$$

13.3 Lema. *Sčítanie a násobenie zlomkov nad oborom integrity $A$ definované vzťahmi (1) a (2) sú binárne operácie na množine* $\mathrm{Zlom}(A)$.

Dôkaz. Tvrdenie vlastne hovorí, že množina $\mathrm{Zlom}(A)$ je uzavretá vzhľadom na sčítanie a násobenie definované vyššie. Evidentne

$$[ad + bc, bd] \in \mathrm{Zlom}(A) \wedge [ac, bd] \in \mathrm{Zlom}(A) \Leftrightarrow bd \neq 0_A.$$

Pretože ale $[a, b], [c, d] \in \mathrm{Zlom}(A)$ znamenajú, že $b \neq 0_A \wedge d \neq 0_A$ a $A$ je obor integrity, požadovaný vzťah $bd \neq 0_A$ platí. □

Nech $(A, +, \cdot)$ je ľubovoľný obor integrity. Označme symbolom $Q(A)$ množinu všetkých tried rozkladu množiny $\mathrm{Zlom}(A)$ podľa ekvivalencie $\equiv$. Prvkami množiny $Q(A) = \mathrm{Zlom}(A)/\equiv$ sú teda triedy zlomkov v tvare $\overline{[a, b]} = \{[x, y] \in \mathrm{Zlom}(A); [x, y] \equiv [a, b]\}$. Častejšie označenie týchto tried je $\frac{a}{b}$ prípadne $a/b$.

**13.4 Poznámka.** Symbol $\frac{a}{b}$ neoznačuje teda zlomok $[a, b]$ nad oborom integrity $A$, ale triedu všetkých zlomkov $[x, y]$ nad $A$ pre ktoré platí $[x, y] \equiv [a, b]$, t.j. $xb =$

*ya*. Pre $A = Z$ tiež racionálne číslo $\frac{a}{b}$ nechápeme ako jediný zlomok s čitateľom $a$ a menovateľom $b$, ale ako triedu všetkých zlomkov s ním ekvivalentných.

Teraz ukážeme, že aj na množine $\mathrm{Zlom}(A)/\equiv$ možno korektne definovať sčítanie a násobenie prirodzeným spôsobom, t.j. nasledovne:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{ad+bc}{bd}, \tag{3}$$

$$\frac{a}{b} \odot \frac{c}{d} = \frac{ac}{bd}. \tag{4}$$

13.5 Veta. *Nech* $(A, +, \cdot)$ *je obor integrity. Relácia* $\equiv$ *je na množine* $\mathrm{Zlom}(A)$ *kompatibilná s operáciami* $+$ *a* $\cdot$*, t.j. platí*

$$[a,b] \equiv [a',b'] \wedge [c,d] \equiv [c',d'] \;\Rightarrow\; [a,b] \boxplus [c,d] \equiv [a',b'] \boxplus [c',d'], \tag{5}$$

$$[a,b] \equiv [a',b'] \wedge [c,d] \equiv [c',d'] \;\Rightarrow\; [a,b] \boxdot [c,d] \equiv [a',b'] \boxdot [c',d']. \tag{6}$$

*Teda* $\oplus$ *a* $\odot$ *definované v (3), (4) sú binárne operácie na množine* $Q(A)$*.*

**13.6 Poznámka.** Vzťahy (5) a (6) vlastne ukazujú, že sčítanie v (3) a násobenie v (4) nezávisia od výberu zlomkov z daných tried – výsledok sčítania a násobenia bude aj pri rôznych výberoch reprezentantov vždy tá istá trieda. V nasledujúcej kapitole ukážeme, že taká relácia ekvivalencie na okruhu je tzv. kongruencia okruhu, ktorá umožňuje vytvoriť faktorový okruh – podobne ako tomu bolo u grúp v kapitole 8.

Dôkaz vety 13.5. Nech $[a,b] \equiv [a',b']$ a $[c,d] \equiv [c',d']$, teda $ab' = a'b$ a $cd' = c'd$. Po vynásobení prvej rovnosti prvkom $dd'$ a druhej rovnosti prvkom $bb'$ dostaneme $ab'dd' = a'bdd'$ a $cd'bb' = c'dbb'$. Odtiaľ po sčítaní a úprave ( s použitím komutatívnosti násobenia) máme $(ad+bc)b'd' = (a'd'+b'c')bd$, čiže $[ad+bc, bd] \equiv [a'd'+b'c', b'd']$, t.j. $[a,b] \boxplus [c,d] \equiv [a',b'] \boxplus [c',d']$, čiže platí (5). Podobne vzájomným vynásobením rovností $ab' = a'b$ a $cd' = c'd$ dostaneme po úprave $acb'd' = a'c'bd$, čiže $[ac, bd] \equiv [a'c', b'd']$, t.j. $[a,b] \boxdot [c,d] \equiv [a',b'] \boxdot [c',d']$, a teda aj (6) platí. Dôkaz je skončený. $\square$

13.7 Veta. *Nech* $(A, +, \cdot)$ *je obor integrity. Potom algebra* $(Q(A), \oplus, \odot)$*, kde* $Q(A) = \mathrm{Zlom}(A)/\equiv$ *a operácie* $\oplus$ *a* $\odot$ *sú definované vzťahmi (3),(4), je pole obsahujúce podokruh izomorfný s* $A$*.*

Dôkaz. Prenechávame na čitateľa overiť priamo výpočtom, že operácie sčítania a násobenia zlomkov v (1),(2) sú komutatívne a asociatívne (cvičenie 1). Ľahko sa tiež ukáže, že nulovým prvkom v $Q(A)$ je trieda $\frac{0}{1}$, jednotkovým prvkom trieda $\frac{1}{1}$ a opačným prvkom k $\frac{a}{b}$ je $\frac{-a}{b}$ (cvičenie 2). Ak teraz $\frac{a}{b}$ je nenulový prvok $Q(A)$, t.j. $\frac{a}{b} \neq \frac{0}{1}$, tak $a \cdot 1 \neq b \cdot 0$, čiže $a \neq 0$, a teda $[b,a] \in \mathrm{Zlom}(A)$ a evidentne trieda $\overline{[b,a]} = \frac{b}{a}$ je inverzný prvok k $\frac{a}{b}$. Ostáva ukázať distributívnosť operácie $\odot$ vzhľadom na operáciu $\oplus$. Zrejme

$$\frac{a}{b} \cdot \left(\frac{c}{d} \oplus \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{acf+ade}{bdf},$$

$$\left(\frac{a}{b} \odot \frac{c}{d}\right) \oplus \left(\frac{a}{b} \odot \frac{e}{f}\right) = \frac{ac}{bd} \oplus \frac{ae}{bf} = \frac{acbf+bdae}{bdbf}.$$

Rovnosť výsledných tried vpravo platí vtedy, keď ich reprezentanti sú v relácií $\equiv$. Avšak $[acf + ade, bdf] \equiv [acbf + bdae, bdbf]$, pretože $(acf + ade) \cdot bdbf = (acbf + bdae) \cdot bdf$. Teda $(Q(A), \oplus, \odot)$ je pole.

Tvrdíme, že množina $A' = \{\frac{a}{1} \mid a \in A\}$ tvorí podokruh poľa $Q(A)$, a že tento je izomorfný s pôvodným okruhom $A$ pri izomorfizme $f : A \to A'$, $f(a) = \frac{a}{1}$. Overenie týchto tvrdení prenechávame na čitateľa (cvičenie 3). □

13.8 Definícia. *Pole $(Q(A), \oplus, \odot)$ definované vyššie nazývame podielové pole oboru integrity $A$. Ak $A = Z$, podielové pole $(Q(Z), \oplus, \odot)$ nazývame poľom racionálnych čísel a označujeme ho jednoducho $(Q, +, \cdot)$.*

**13.9 Príklad.** Ukážeme, že podielové pole oboru integrity $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ je izomorfné s podpoľom $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b, \in Q\}$ poľa $R$ reálnych čísel.

Nosičom podielového poľa $Q(Z[\sqrt{2}])$ oboru integrity $Z[\sqrt{2}]$ je podľa vety 13.7 množina

$$Q(Z[\sqrt{2}]) = \mathrm{Zlom}(Z[\sqrt{2}])/_{\equiv} = \left\{ \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \mid a, b, c, d \in Z,\ c + d\sqrt{2} \neq 0 \right\},$$

kde $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ označuje triedu zlomkov nad $Z[\sqrt{2}]$ ekvivalentných (v relácii $\equiv$) so zlomkom $[a + b\sqrt{2}, c + d\sqrt{2}]$. Operácie na $Q(Z[\sqrt{2}])$ sú dané vzťahmi (3),(4).

Nech $Q' = \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \mid a, b, c, d \in Z,\ c + d\sqrt{2} \neq 0 \right\}$ je podmnožina reálnych čísel. Ľahko sa možno presvedčiť, že $Q'$ je podpole $R$ a že zobrazenie $f : Q(Z[\sqrt{2}]) \to Q'$ dané predpisom $f\left(\frac{a+b\sqrt{2}}{c+d\sqrt{2}}\right) = \frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ je izomorfizmus polí. Ukážeme, že množiny reálnych čísel $Q'$ a $Q(\sqrt{2})$ sú totožné, odkiaľ vyplýva, že $f$ je aj hľadaný izomorfizmus podielového poľa $Q(Z[\sqrt{2}])$ na podpole $Q(\sqrt{2})$ poľa $R$.

Nech $r' \in Q'$ je reálne číslo. Potom

$$r' = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{cb - ad}{c^2 - 2d^2}\sqrt{2} \in Q(\sqrt{2}),$$

lebo $r'$ má tvar $a' + b'\sqrt{2}$ pre $a', b' \in Q$. Teda $Q' \subseteq Q(\sqrt{2})$. Obrátene, nech $r \in Q(\sqrt{2})$. Potom

$$r = a + b\sqrt{2} = \frac{p}{q} + \frac{p'}{q'}\sqrt{2} = \frac{pq' + qp'\sqrt{2}}{qq'} = \frac{pq' + qp'\sqrt{2}}{qq' + 0\sqrt{2}} \in Q',$$

lebo $r$ má tvar $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$. Teda aj $Q(\sqrt{2}) \subseteq Q'$ a množiny $Q(\sqrt{2})$, $Q'$ reálnych čísel sú skutočne totožné.

Na záver pomocou konštrukcie podielového poľa zostrojíme príklad nekonečného poľa konečnej charakteristiky.

**13.10 Príklad.** V kapitole 11 sme uviedli ako adjunkciou transcendentného prvku $x$ nad daným okruhom $A$ možno vytvoriť okruh $A[x]$ polynómov jednej neurčitej nad $A$. Zvoľme teraz za $A$ okruh $(Z_p, \oplus, \odot)$, kde $p$ je prvočíslo. $Z_p[x]$ je (nekonečná) množina všetkých polynómov $f(x) = a_0 + a_1x + \cdots + a_nx^n$, kde $n \in N$ a koeficienty $a_0, a_1, \ldots, a_n \in Z_p$. Sčítanie a násobenie v okruhu $(Z_p[x], +, \cdot)$

sú definované tak ako bolo uvedené v kapitole 11. Súčinom dvoch nenulových polynómov s vedúcimi členmi $a_n x^n, a_m x^m$, kde $a_n \in Z_p \setminus \{0\}$, $a_m \in Z_p \setminus \{0\}$ je polynóm s vedúcim členom $a_n a_m x^{n+m}$. Pretože $Z_p$ je obor integrity, platí aj $a_n \cdot a_m \neq 0$, preto súčinom nenulových polynómov je opäť nenulový polynóm, a teda $(Z_p[x], +, \cdot)$ je obor integrity. Jeho charakteristika je podľa vety 10.6 rovná rádu jednotky (ktorou je polynóm 1), t.j. $\mathrm{char}(Z_p[x]) = r(1) = p$, pretože $p \times 1 = 0$ v $Z_p$. Podielové pole $Q(Z_p[x])$, často označované $Z_p(x)$, obsahuje podľa vety 13.7 podokruh izomorfný so $Z_p[x]$. Preto pole $Z_p(x)$ je nekonečné a jeho charakteristika je $\mathrm{char}(Z_p(x)) = r(1) = p$.

## Cvičenia

**1.** Overte, že operácie sčítania a násobenia zlomkov definované vzťahmi (1) a (2) sú komutatívne a asociatívne.

**2.** Overte, že nulovým prvkom v podielovom poli $Q(A)$ je trieda $\frac{0}{1}$, jednotkovým prvkom trieda $\frac{1}{1}$ a opačným prvkom k triede $\frac{a}{b}$ je trieda $\frac{-a}{b}$.

**3.** Overte, že množina tried $A' = \{\frac{a}{1} \mid a \in A\}$ je podokruhom podielového poľa $Q(A)$ a že zobrazenie $f : A \to A'$, $f(a) = \frac{a}{1}$ je izomorfizmus okruhov.

**4.** Ukážte, že podielové pole oboru integrity $Z[i] = \{a + bi \mid a, b \in Z\}$ je izomorfné s poľom $Q(i) = \{a + bi \mid a, b, \in Q\}$.

**5.** Ukážte, že najmenší obor integrity obsahujúci $Z$ a číslo $\frac{1}{3}$ je $Z[\frac{1}{3}] = \{\frac{k}{3^n} \mid k \in Z, n \in N\}$ a ukážte, že jeho podielové pole je izomorfné s poľom $Q$.

**6.** Zostrojte podielové pole $Z_3(x)$ oboru integrity $Z_3[x]$.

**7.** Ukážte, že podielové pole oboru integrity $Z[x]$ je izomorfné s podielovým poľom oboru integrity $Q[x]$.

**8.** Ukážte, že ak $(A, +, \cdot)$ je pole, tak $Q(A) \cong A$.

**9.** Ukážte, že ak obor integrity $A$ je podokruhom oboru integrity $B$, tak jeho podielové pole $Q(A)$ je podpoľom podielového poľa $Q(B)$.

## 14. Ideály, kongruencie na okruhoch a faktorové okruhy

V 1. kapitole sme z okruhu celých čísel $(Z,+,\cdot)$ stotožňovaním prvkov podľa relácie ekvivalencie $\equiv \pmod m$, zlučiteľnej (kompatibilnej) s operáciami sčítania a násobenia vytvorili okruh zvyškových tried modulo $m$, $\overline{Z}_m = \{\overline{0},\overline{1},\ldots,\overline{m-1}\}$. V tejto kapitole túto konštrukciu zovšeobecníme a ukážeme ako z ľubovoľného okruhu $(A,+,\cdot)$ možno pomocou relácie ekvivalencie na $A$ zlučiteľnej so sčítaním a násobením okruhu, tzv. kongruencie okruhu, utvoriť analogickým spôsobom tzv. faktorový okruh.

V kapitole 8 sme sa zaoberali faktorizáciou grúp. Ukázali sme, že stotožnenie prvkov grupy $(G,\cdot)$ podľa normálnej podgrupy $H$ je ekvivalentné so stotožňovaním prvkov grupy $(G,\cdot)$ podľa kongruencie $\equiv_H$ a že faktorová grupa $G/H$ tried grupy $G$ podľa $H$ je to isté ako faktorová grupa $G/\equiv_H$ tried kongruencie $\equiv_H$. V tejto kapitole využijeme tieto poznatky z faktorizácie grúp a ukážeme, že aj okruhy možno faktorizovať vo všeobecnosti podľa kongruencií práve tak ako podľa špeciálnych podokruhov, ktoré nazveme *ideálmi* okruhu.

Nech $I$ je podokruh okruhu $(A,+,\cdot)$. Pretože $(A,+)$ je komutatívna grupa, je podgrupa $(I,+)$ normálna a možno teda utvoriť faktorovú grupu $(A/I,+)$. Jej prvkami sú triedy v tvare $I+a$, ktorých sčitovanie podľa prirodzeného predpisu

$$(I+a)+(I+b)=I+(a+b) \tag{1}$$

je korektné vďaka normálnosti podgrupy $I$. Je možné zaviesť aj násobenie tried tak aby štruktúra $(A/I,+,\cdot)$ bola okruhom? Pozrime sa na to, kedy prirodzené násobenie tried podľa predpisu

$$(I+a)\cdot(I+b)=I+(a\cdot b) \tag{2}$$

bude korektne definované t.j. nezávislé na výbere reprezentantov násobených tried. Čiže ak máme dvojakú reprezentáciu tried, $I+a=I+c$ a $I+b=I+d$, za akých podmienok kladených na $I$ dostaneme rovnaký výsledok $I+(a\cdot b)=I+(c\cdot d)$? Ľahko sa dá ukázať, že popri podmienke

$$a,b\in I \Rightarrow a-b\in I \tag{3}$$

ktorá hovorí, že $I$ je (normálnou) podgrupou (komutatívnej) grupy $(A,+)$, je postačujúcou podmienkou

$$a\in I, x\in A \Rightarrow ax\in I \wedge xa\in I. \tag{4}$$

Skutočne, rovnosti $I+a=I+c,\ I+b=I+d$ implikujú $a-c\in I,\ b-d\in I$, odkiaľ za podmienky (4) dostaneme $(a-c)b\in I,\ c(b-d)\in I$, t.j. $I+(ab)=I+(cb)=I+(cd)$.

14.1 Definícia. *Neprázdnu podmnožinu $I$ okruhu $(A,+,\cdot)$ nazývame ideálom okruhu $A$, ak spĺňa podmienky (3),(4) uvedené vyššie.*

Ľahko je vidieť, že z podmienok (3),(4) vyplýva, že ideál $I$ okruhu $(A,+,\cdot)$ spĺňa podmienky a)-c) z vety 10.12, a teda je podokruhom okruhu $A$ (cvičenie 1).

14.2 Veta. *Nech $(A,+,\cdot)$ je okruh a $I$ je jeho ideál. Množina $A/I$ všetkých tried aditívnej grupy $(A,+)$ podľa normálnej podgrupy $(I,+)$ s operáciami sčítania a násobenia tried definovanými podľa vzťahov (1),(2) tvorí okruh. Ak okruh $A$ je komutatívny, tak aj okruh $A/I$ je komutatívny. Ak $A$ má jednotku $1_A \notin I$, tak $A/I$ má jednotku $I+1$.*

Dôkaz. Už sme vyššie ukázali, že podmienky (3),(4) kladené na $I$ zaručujú, že sčítanie a násobenie definované na množine tried $A/I$ podľa (1), (2) sú korektne definované operácie (t.j. nezávislé na výbere reprezentantov tried). Pretože naša konštrukcia začala vytorením faktorovej grupy $(A/I,+)$ grupy $(A,+)$ podľa podgrupy $(I,+)$, axiómy okruhu týkajúce sa sčitovania sú splnené, ak ukážeme, že grupa $(A/I,+)$ je komutatívna. To však bezprostredne vyplýva na základe vety 8.3 z toho, že $(A,+)$ je komutatívna. Distributívnosť násobenia vzhľadom na sčítanie možno preveriť priamym výpočtom:

$$\begin{aligned}(I+a)[(I+b)+(I+c)] &= (I+a)[I+(b+c)] = \\ &= I+a(b+c) = I+(ab+ac) = (I+ab)+(I+ac).\end{aligned}$$

Taktiež priamym výpočtom možno preveriť asociatívnosť násobenia tried a komutatívnosť násobenia tried v prípade, že okruh $(A,+,\cdot)$ je sám komutatívny. Prenechávame to na čitateľa (cvičenie 2). Ak okruh $A$ má jednotku $1 \notin I$, tak pre ľubovoľnú triedu $I+a$ platí

$$(I+a)(I+1) = I+(a1) = I+a = I+(1a) = (I+1)(I+a),$$

teda $I+1$ je jednotka okruhu $A/I$. □

14.3 Definícia. *Okruh $(A/I,+,\cdot)$ opísaný v predchádzajúcej vete nazývame faktorový okruh okruhu $A$ podľa ideálu $I$.*

Ak okruh $A$ má jednotku a $1 \in I$, tak z podmienky (4) vyplýva, že pre každé $x \in A$ platí $x = 1 \cdot x \in I$, teda $I = A$. V tom prípade faktorový okruh $A/I$ je nezaujímavý – pozostáva z jedinej triedy, ktorou je $I = A$. Ideál $I = A$ nazývame *nevlastný* ideál, ostatné ideály sú *vlastné*. Každý okruh $A$ má *triviálny* ideál $\{0_A\}$, pričom faktorový okruh $A/\{0_A\}$ pozostáva z jednoprvkových tried $\{0_A\}+a = \{a\}$ $(a \in A)$ a teda je izomorfný s pôvodným okruhom $A$ pri izomorfizme $f : A \to A/\{0_A\},\ f(a) = \{0_A\}+a$.

14.4 Lema. *Teleso nemá netriviálne vlastné ideály.*

Dôkaz. Ak $(T,+,\cdot)$ je teleso, $I$ je jeho netriviálny ideál a $b \in I \setminus \{0_T\}$, tak vzhľadom na (4) dostaneme $1 = bb^{-1} \in I$ a to, ako sme vyššie ukázali, implikuje $I = T$. Teda $I$ je nevlastný ideál. □

**14.5 Príklad.** Presvedčme sa, že $mZ = \{m \cdot k \mid k \in Z\}$ je ideálom okruhu $(Z,+,\cdot)$. Je zrejmé, že $\varnothing \neq mZ \subseteq Z$. Podmienka (3) vyplýva triviálne z výpočtu $m \cdot k - m \cdot l = m \cdot (k-l) \in mZ$ a podmienka (4) zas z výpočtov $(x \in Z)$

$$(m \cdot k) \cdot x = m \cdot (k \cdot x) \in mZ,\ x \cdot (m \cdot k) = m \cdot (x \cdot k) \in mZ.$$

Teda $mZ$ je ideálom okruhu $Z$ a faktorový okruh $Z/mZ$ je vlastne okruhom zvyškových tried $\overline{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, ak si uvedomíme, že $mZ+0 = \overline{0},\ mZ+1 = \overline{1}, \ldots, mZ+(m-1) = \overline{m-1}$. □

Pre $m = 0$ je $mZ = \{0\}$ a už sme naznačili, že faktorizáciou podľa nulového ideálu dostaneme faktorový okruh $Z/0Z \cong Z$, ktorý je teda oborom integrity. Pre $m = 1$ je $mZ = Z$ a tiež sme už naznačili, že faktorový okruh $Z/1Z$ pozostáva z jedinej triedy $Z$. Jednoprvkový okruh nepovažujeme za obor integrity. Vieme, že pre $m \geq 2$ je faktorový okruh $Z/mZ$ (okruh zvyškových tried modulo $m$) oborom integrity (poľom) práve vtedy, keď $m$ je prvočíslo. Otázkou je, či môžeme vo všeobecnosti na základe vlastností ideálu $I$ okruhu $A$ usúdiť, že faktorový okruh $A/I$ bude oborom integrity resp. poľom. Túto otázku zodpovieme v nasledujúcej časti.

14.6 Definícia. *Ideál $I$ okruhu $A$ nazývame prvoideálom, ak spĺňa podmienku*

$$\forall a, b \in A;\ a \cdot b \in I \Rightarrow a \in I \vee b \in I.$$

14.7 Veta. *Nech $(A, +, \cdot)$ je komutatívny okruh s jednotkou. Faktorový okruh $A/I$ je oborom integrity práve vtedy, keď $I$ je vlastný prvoideál.*

Dôkaz. Nech $A/I$ je oborom integrity. Potom $I$ je vlastný, pretože $A/A$ s jedinou triedou $A$ nie je oborom integrity. Nech $a \cdot b \in I$. Potom v $A/I$ máme $0_{A/I} = I = I + ab = (I + a)(I + b)$. Keďže $A/I$ je oborom integrity, dostávame $I = I + a$ alebo $I = I + b$, čiže $a \in I$ alebo $b \in I$. Teda $I$ je vlastný prvoideál.

Obrátene, nech $I$ je vlastný prvoideál. Potom $A/I$ je aspoň 2-prvkový faktorový okruh. Predpokladajme, že v $A/I$ platí $(I + a)(I + b) = 0_{A/I}$, t.j. $I + ab = I$. Potom $ab \in I$, a keďže $I$ je prvoideál, dostávame $a \in I$ alebo $b \in I$. Teda $I + a = I$ alebo $I + b = I$, čiže $A/I$ je oborom integrity. □

14.8 Definícia. *Ideál $I$ okruhu $A$ nazývame maximálnym ideálom, ak $I \neq A$ a pre ľubovoľný ideál $J$ okruhu $A$*

$$I \subseteq J \subseteq A \Rightarrow J = I \ \vee \ J = A.$$

Teda maximálny ideál je maximálnym prvkom v čiastočne usporiadanej množine všetkých ideálov okruhu usporiadaných množinovou inklúziou.

14.9 Veta. *Nech $(A, +, \cdot)$ je komutatívny okruh s jednotkou. Faktorový okruh $A/I$ je poľom práve vtedy, keď $I$ je maximálny ideál.*

Dôkaz. Nech $A/I$ je poľom. Potom $I \neq A$, v opačnom prípade by $A/I$ nebol ani oborom integrity. Predpokladajme, že $J$ je ideál okruhu $A$ taký, že $I \subsetneq J \subseteq A$. Potom existuje prvok $a \in J \setminus I$, teda $I + a$ je nenulová trieda v poli $A/I$. Nech $I + b$ je trieda k nej inverzná, t.j. $(I + a)(I + b) = I + 1$, odkiaľ máme $1 - ab \in I \subseteq J$. Keďže $a \in J$, platí aj $ab \in J$. Potom aj súčet $(1 - ab) + ab \in J$, t.j. $1 \in J$, čiže $J = A$. Ukázali sme, že $I$ je maximálny ideál.

Obrátene, nech $I$ je maximálny ideál. Potom $1 \notin I$, v opačnom prípade by $I = A$. Z vety 14.2 vyplýva, že $A/I$ je komutatívny okruh s jednotkou $I+1$. Ostáva ukázať, že každý nenulový prvok v $A/I$ má inverzný prvok. Nech $I + a \neq I$, t.j. $a \notin I$. Množina $J = \{y + ax \mid y \in I, x \in A\}$ je zrejme ideálom pre ktorý platí $I \subseteq J \subseteq A$. Dá sa ukázať, že $J$ je najmenším ideálom obsahujúcim $I$ a prvok $a \notin I$ (cvičenie 3). Pretože $0 + a \cdot 1 = a \in J$, máme $I \neq J$. Keďže $I$ je maximálny ideál, znamená to, že $J = A$. Teda $1 \in J$, čiže $1 = y + a \cdot x$ pre nejaké $y \in I, x \in A$. Preto $1 - ax = y \in I$, odkiaľ máme $I + 1 = I + ax = (I + a)(I + x)$. Teda $I + x$ je hľadaným inverzným prvkom k prvku $I + a$ v okruhu $A/I$. Dôkaz je skončený. □

14.10 Dôsledok. *Každý maximálny ideál komutatívneho okruhu $A$ s jednotkou je prvoideálom.*

Dôkaz. Tvrdenie možno okamžite odvodiť aj z toho, že každé pole je oborom integrity (veta 12.10) a z predchádzajúcich viet 14.7. a 14.9. □

14.11 Dôsledok. *Jedinými prvoideálmi okruhu $Z$ sú $\{0\}, Z$ a $nZ$, kde $n$ je prvočíslo. Jedinými maximálnymi ideálmi okruhu $Z$ sú $nZ$, kde $n$ je prvočíslo.*

Dôkaz. Vo vete 10.14 sme ukázali, že $nZ = \{n \cdot k \mid k \in Z\}$ pre nezáporné celé čísla $n$ sú jedinými podokruhmi okruhu $Z$. Pre $n \geq 2$ je faktorový okruh $Z/nZ = \overline{Z}_n$ oborom integrity práve vtedy, keď $n$ je prvočíslo (veta 12.4) a vtedy je dokonca poľom (dôsledok 12.11). Z viet 14.7 a 14.9 vyplýva, že z podokruhov $nZ$ pre $n \geq 2$ sú prvoideály a maximálne ideály práve tie, kde $n$ je prvočíslo. Naviac je zrejmé, že podokruhy $0Z = \{0\}$, $1Z = Z$ sú prvoideály, ale nie maximálne ideály. □

V poslednej časti tejto kapitoly ukážeme, že ideály okruhov súvisia s kongruenciami okruhov analogicky ako normálne podgrupy grúp súvisia s kongruenciami grúp.

14.12 Definícia. *Kongruenciou okruhu $(A, +, \cdot)$ nazývame každú reláciu ekvivalencie $\equiv$ na $A$, ktorá je zlučiteľná so sčítaním a násobením okruhu $A$, t.j. platí*

$$\forall a, b, a', b' \in A;\ a \equiv a' \wedge b \equiv b' \ \Rightarrow\ a + b \equiv a' + b' \wedge a \cdot b \equiv a' \cdot b'.$$

14.13 Veta. *a) Nech $\equiv$ je kongruencia okruhu $A$. Potom $I(\equiv) = \{a \in A;\ a \equiv 0_A\}$ je ideál okruhu $A$ a pre ľubovoľné $a, b \in A$ platí*

$$a \equiv b \Leftrightarrow a - b \in I(\equiv). \tag{6}$$

*b) Nech $I$ je ideál okruhu $A$. Potom binárna relácia $\equiv_I$ na $A$ definovaná vzťahom*

$$a \equiv_I b \Leftrightarrow a - b \in I \tag{7}$$

*je kongruencia okruhu $A$ a platí $\{a \in A \mid a \equiv_I 0_A\} = I$.*

*c) Kongruencia $\equiv_{I(\equiv)}$ je totožná s kongruenciou $\equiv$ a ideál $I(\equiv_I)$ je totožný s ideálom $I$.*

Dôkaz. a) Nech $a, b \in I(\equiv)$. Potom $a \equiv 0_A$, $b \equiv 0_A$, odkiaľ $a - b \equiv 0_A$, čiže $a - b \in I(\equiv)$. Pre $a \in I(\equiv)$ a ľubovoľné $x \in A$ máme $a \equiv 0_A$, $x \equiv x$, odkiaľ vyplýva $a \cdot x \equiv 0_A \cdot x \equiv 0_A$, $x \cdot a \equiv x \cdot 0_A = 0_A$, čiže $a \cdot x, x \cdot a \in I(\equiv)$. Ukázali sme, že $I(\equiv)$ je ideálom okruhu $A$. Je zrejmé, že pre ľubovoľné $a, b \in A$ platí

$$a - b \in I(\equiv) \Leftrightarrow a - b \equiv 0_A \Leftrightarrow a \equiv b.$$

b) Prenechávame na čitateľa overiť, že relácia $\equiv_I$ je reflexívna, symetrická a tranzitívna na $A$. Ak $a \equiv_I b$ a $c \equiv_I d$, čiže $a - b \in I$ a $c - d \in I$, tak aj $(a - b) + (c - d) = (a + c) - (b + d) \in I$, pretože $I$ je podokruh $A$. Zo (7) potom dostaneme požadované $a + c \equiv_I b + d$. Na druhej strane $a - b \in I$ implikuje $(a - b)c = ac - bc \in I$ t.j. $ac \equiv_I bc$ podľa (7). Podobne $c - d \in I$ implikuje $b(c - d) = bc - bd \in I$ t.j. $bc \equiv_I bd$ podľa (7). Z tranzitívnosti relácie $\equiv_I$ potom

máme $ac \equiv_I bd$. Teda relácia $\equiv_I$ je kompatibilná so sčítaním a násobením okruhu $A$, je teda kongruencia na $A$. Opäť s použitím (7) dostaneme $\{a \in A \mid a \equiv_I 0_A\} = \{a \in A \mid a - 0_A \in I\} = \{a \in A \mid a \in I\} = I$.

c) S použitím (6) a (7) máme

$$a \equiv_{I(\equiv)} b \Leftrightarrow a - b \in I(\equiv) \Leftrightarrow a \equiv b$$

a analogicky

$$a \in I(\equiv_I) \Leftrightarrow a \equiv_I 0_A \Leftrightarrow a \in I. \quad \square$$

Podobne ako u grúp, ideál $I(\equiv)$ priradený ku kongruencii $\equiv$ na okruhu $A$ podľa vzťahu (6) nazývame *jadrom* okruhovej kongruencie $\equiv$. Kongruenciu $\equiv_I$ priradenú k ideálu $I$ podľa vzťahu (7) budeme volať *kongruenciou modulo* $I$.

Časť c) predchádzajúcej vety teda hovorí, že (podobne ako u grúp) konštrukcie v bodoch a),b) sú navzájom inverzné. Vyplýva z toho, že kongruencie na okruhu sú totožné práve vtedy, keď ich jadrá sú totožné ideály a obrátene, ideály na okruhu sú totožné práve vtedy, keď kongruencie modulo tieto ideály sú totožné.

**14.14 Príklad.** Jadrom kongruencie $\equiv \pmod m$ na okruhu $(Z, +, \cdot)$, ktorou sme sa zaoberali už v kapitole 1, je ideál $mZ$. Obrátene, kongruencia modulo $mZ$ je práve kongruencia $\equiv \pmod m$. Pre $m = 0$ máme najmenšiu kongruenciu $\equiv \pmod 0 = \{(a, a) \mid a \in Z\}$ ktorá je rovnosťou na $Z$. Stotožňovaním prvkov okruhu $Z$ podľa tejto najmenšej kongruencie získame najväčší faktorový okruh $\{\{a\} \mid a \in Z\}$ izomorfný so $Z$. Pre $m = 1$ máme najväčšiu kongruenciu $\equiv \pmod 1 = Z \times Z$, stotožňujúcu prvky okruhu do jednej triedy a získame tak najmenší faktorový okruh $\{Z\}$ izomorfný s $\{0\}$. Pre $m = p$ (prvočíslo) získame stotožňovaním celých čísel podľa kongruencie $\equiv \pmod p$ pole $\overline{Z}_p = \{\overline{0}, \ldots, \overline{p-1}\}$.

## Cvičenia

**1.** Ukážte, že každý ideál okruhu $A$ je podokruhom $A$.

**2.** Výpočtom sa presvedčte o asociatívnosti násobenia tried danom vzťahom (2) v množine $A/I$ a ukážte, že je komutatívne, ak $A$ je komutatívny okruh.

**3.** Nech $A$ je okruh, $I$ je jeho ideál a nech $a \in A \setminus I$. Ukážte, že $J = \{y + ax \mid y \in I, x \in A\}$ je najmenším ideálom v $A$ obsahujúcim $I$ a prvok $a$.

**4.** Nech $A = \{1, 2, 3, 4\}$. Potom $(\mathcal{P}(A), \triangle, \cap)$ je okruh (cvičenie 10.9).

a) Ukážte, že podokruh $\langle\{1\}, \{2, 3\}\rangle$ nie je jeho ideálom.

b) Ukážte, že podokruh $\langle\{1\}, \{1, 2\}\rangle$ je jeho ideálom a napíšte operačnú tabuľku príslušného faktorového okruhu.

**5.** Ukážte, že tvrdenie v cvičení 1 nemožno obrátiť. Nájdite aspoň 5 príkladov okruhov a ich podokruhov, ktoré nie sú ideálmi.

**6.** Zistite, ktoré z nasledujúcich množín $M_i$ sú ideálmi okruhu $A_i$. Ktoré ideály $M_i$ sú prvoideálmi a ktoré maximálnymi ideálmi?

a) $M_1 = Z,\ A_1 = Z[\sqrt{2}]$

b) $M_2 = Z,\ A_2 = Q$

c) $M_3 = \{ax + by \mid x, y \in Z\}\ (a, b \in Z),\ A_3 = Z$

d) $M_4 = \{(a, 2a) \mid a \in R\},\ A_4 = R \times R$

e) $M_5 = \{(a, 0) \mid a \in R\},\ A_5 = R \times R$

f) $M_6 = \{(2a, 3a) \mid a \in Z\},\ A_6 = Z \times Z$
g) $M_7 = \{(2a, 3b) \mid a, b \in Z\},\ A_7 = Z \times Z$
h) $M_8 = \{(a, 7b) \mid a, b \in Z\},\ A_8 = Z \times Z$

**7.** V prípade, že v cvičení 5 je $M_i$ ideálom okruhu $A_i$, určte faktorový okruh $A_i/M_i$. Ak $M_i$ nie je vlastným prvoideálom, nájdite v okruhu $A_i/M_i$ nejakých deliteľov nuly. Ak $M_i$ nie je maximálnym ideálom, nájdite v okruhu $A_i/M_i$ nejaké nenulové neinvertovateľné prvky (t.j. nemajúce inverzný prvok).

**8.** Zistite, ktoré z nasledujúcich relácií $R_i$ sú kongruenciami okruhu $A_i$. Ak $R_i$ je kongruenciou, nájdite jej jadro $I(R_i)$ a určte faktorový okruh $A_i/I(R_i)$.
a) $aR_1b \Leftrightarrow a^2 = b^2,\ A_1 = Z$
b) $aR_2b \Leftrightarrow 8 \mid a - b, A_2 = Z$
c) $(a, b)R_3(c, d) \Leftrightarrow a = c,\ A_3 = R \times R$
d) $(a, b)R_4(c, d) \Leftrightarrow a - c = b - d,\ A_4 = R \times R$
e) $(a, b)R_5(c, d) \Leftrightarrow a - c,\ b - d \in 2Z,\ A_5 = Z \times Z$
f) $(a, b)R_6(c, d) \Leftrightarrow a - c \in 5Z,\ b - d \in 3Z,\ A_6 = Z \times Z$
g) $(a, b)R_7(c, d) \Leftrightarrow a = d,\ A_7 = Z_2 \times Z_2$
h) $f(x)R_8g(x) \Leftrightarrow f(0) - g(0) \in 2Z,\ A_8 = Z[x]$
i) $f(x)R_9g(x) \Leftrightarrow f(-1) = g(-1),\ A_9 = Q[x]$
j) $f(x)R_{10}g(x) \Leftrightarrow f(x) - g(x) \in [x^2],\ A_{10} = Z_3[x]$

**9.** Ukážte, že
a) $Z/7Z \cong Z_7$
b) $Z \times Z/3Z \times 8Z \cong Z_3 \times Z_8$
c) $Q[x]/[x^2 - 2] \cong Q[\sqrt{2}]$
d) $R[x]/[x^2 + x + 1] \cong C$.

## 15. Ekvivalentné a dôsledkové úpravy pri riešení algebraických rovníc nad obormi integrity.

V kapitole 11 sme zaviedli pojem okruhu polynómov $A[x]$ jednej neurčitej $x$ nad okruhom $A$. V tejto kapitole budeme predpokladať, že $A$ je oborom integrity, pričom najčastejšie budeme mať na mysli číselný obor integrity $Z$ a číselné polia $Q, R, C$ a $Z_p$ ($p$-prvočíslo). Nulovým prvkom v nich je číslo 0, preto označenie $0_A$ tentoraz nebudeme používať. V týchto oboroch integrity sa v školskej praxi najčastejšie riešia *algebraické rovnice*

$$(f(x) =)\ a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0, \tag{1}$$

resp. úlohy, ktoré vedú na takéto rovnice. Teraz sa budeme zaoberať predovšetkým tzv. ekvivalentnými a neekvivalentnými úpravami pri riešení algebraických rovníc nad obormi integrity, pričom svoj výklad sa budeme snažiť ilustrovať príkladmi z bežnej školskej praxe. Poznamenávame, že samotnými postupmi (algoritmami) pri riešení tých typov algebraických rovníc (kvadratické, 3. a 4. stupňa, binomické, reciproké), ktoré je možné vo všeobecnosti uspokojivo vyriešiť, sa budeme zaoberať v učebnom texte o polynómoch.

Pod algebraickou rovnicou nad oborom integrity $A$ najčastejšie máme na mysli rovnicu v tvare (1), kde koeficienty polynómu $f(x)$ sú prvkami oboru integrity $A$. V praxi však často taká rovnica má tvar

$$(L(x) =)\ b_0 + b_1x + \cdots + b_nx^n = c_0 + c_1x + \cdots + c_mx^m\ (= P(x)), \tag{2}$$

kde $L(x)$ a $P(x)$ sú polynómy neurčitej $x$ nad daným oborom integrity $A$ nazývané ľavá a pravá strana rovnice (2). Pod *koreňom* alebo *riešením rovnice* (1) resp. (2) *v obore integrity* $A' \supseteq A$ máme na mysli taký prvok $d \in A'$, pre ktorý $f(d) = a_0 + a_1d + a_2d^2 + \cdots + a_nd^n = 0$ resp. $L(d) = P(d)$. Riešiť rovnicu znamená nájsť všetky jej korene (riešenia).

15.1 Definícia. *Majme dve algebraické rovnice*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n = 0 \tag{3}$$

$$g(x) = b_0 + b_1x + \cdots + b_mx^m = 0 \tag{4}$$

*nad oborom integrity $A$. Rovnice (3) a (4) sa nazývajú ekvivalentnými rovnicami v obore integrity $A' \supseteq A$, ak každý koreň rovnice (3) je aj koreňom rovnice (4) a obrátene, každý koreň rovnice (4) je aj koreňom rovnice (3).*

Predchádzajúcu definíciu ilustrujeme v 15.2, kde u všetkých rovníc je $A = Z$, zatiaľčo oborom integrity $A'$ sú striedavo $Z, Q, R$ a $C$.

**15.2 Príklad.** Rovnice $4x^2-5x+1 = 0$ a $2x^2-x-1 = 0$ sú ekvivalentné v obore integrity $Z$, ale nie v $Q$. Prvá má totiž v $Q$ korene $1, \frac{1}{4}$, druhá má v $Q$ korene $1, -\frac{1}{2}$. Teda celočíselný koreň majú rovnaký – číslo 1. Podobne rovnice $x^2 - 4x + 4 = 0$ a $x^3 - 2x^2 - 3x + 6 = 0$ sú ekvivalentné v $Z$ a $Q$, v ktorých majú obe jediný koreň 2, ale nie v $R$, lebo druhá rovnica má v $R$ ešte korene $\sqrt{3}$ a $-\sqrt{3}$. Napokon, rovnice $x^2 - 1$ a $x^4 - 1$ sú ekvivalentné v $Z, Q$ aj v $R$, ale nie v $C$. Prvá má dva celočíselné korene 1 a $-1$ a druhá má okrem $1, -1$ ešte dva komplexne združené korene $i$ a $-i$.

V predchádzajúcom príklade sme videli, že ekvivalentnosť rovníc závisí podstatne od oboru integrity $A'$, v ktorom hľadáme korene rovníc.

Úpravy, použitím ktorých danú rovnicu vždy prevedieme na rovnicu s ňou ekvivalentnú nazývame *ekvivalentnými*. Medzi ekvivalentné úpravy patrí predovšetkým pravidlo o pričítaní rovnakého polynómu k obom stranám rovnice ako o tom hovorí nasledujúca veta.

15.3 Veta. *Nech $A$ je obor integrity a $L(x), P(x)$ sú polynómy jednej neurčitej nad $A$. Algebraická rovnica (2) je ekvivalentná v ľubovoľnom obore integrity $A' \supseteq A$ s algebraickou rovnicou*

$$L(x) + F(x) = P(x) + F(x) \tag{5}$$

*kde $F(x)$ je ľubovoľný polynóm jednej neurčitej nad $A$.*

Dôkaz. Ak $d \in A'$ je koreňom rovnice (2), t.j. platí rovnosť $L(d) = P(d)$ v $A'$, tak je zrejmé, že v $A'$ platí aj rovnosť $L(d) + F(d) = P(d) + F(d)$, čiže $d$ je aj koreňom rovnice (5). Obrátene, ak $d \in A'$ je koreňom (5), tak v $A'$ platí rovnosť $L(d) + F(d) = P(d) + F(d)$, odkiaľ po pričítaní opačného prvku $-F(d)$ k prvku $F(d)$ dostaneme rovnosť $L(d) = P(d)$, čiže $d$ je aj koreňom (2). Ukázali sme, že rovnice (2) a (5) sú v $A'$ ekvivalentné. □

Dôkazy nasledujúcich dvoch viet sú podobné a prenechávame ich na čitateľa.

15.4 Veta. *Nech $A$ je obor integrity a $L(x), P(x)$ sú polynómy jednej neurčitej nad $A$. Algebraická rovnica (2) je ekvivalentná v ľubovoľnom obore integrity $A' \supseteq A$ s algebraickou rovnicou*

$$c \cdot L(x) = c \cdot P(x) \tag{6}$$

*kde $c$ je ľubovoľný nenulový prvok z oboru integrity $A$.*

15.5 Veta. *Nech $A$ je obor integrity a $L(x), P(x)$ sú polynómy jednej neurčitej nad $A$. Množina všetkých riešení algebraickej rovnice (2) v ľubovoľnom obore integrity $A' \supseteq A$ je podmnožinou množiny všetkých riešení algebraickej rovnice*

$$L(x) \cdot F(x) = P(x) \cdot F(x), \tag{7}$$

*kde $F(x)$ je ľubovoľný polynóm jednej neurčitej nad $A$.*

Teda každý koreň rovnice (2) v $A'$ je aj koreňom rovnice (7) v $A'$. Obrátene to však vo všeobecnosti neplatí – rovnica (7) môže mať v $A'$ viac koreňov než rovnica (2). V 15.2 sme uviedli rovnicu $x^2 - 1 = 0$, ktorá má v $C$ korene 1 a $-1$. Po jej vynásobení polynómom $F(x) = x^2 + 1$ dostaneme rovnicu

$$(x^2 - 1) \cdot (x^2 + 1) = 0 \cdot (x^2 + 1).$$

Táto je vlastne rovnicou $x^4 - 1 = 0$, ktorá (ako sme v 15.2 uviedli) má v $C$ štyri korene $1, -1, i, -i$. Preto úprava vo vete 15.5 nie je ekvivalentná.

Úprave rovnice pri ktorej vo všeobecnosti nedostaneme rovnicu ekvivalentnú s pôvodnou rovnicou hovoríme *dôsledková* (alebo *neekvivalentná*) úprava. Takou je teda aj vynásobenie oboch strán rovnice rovnakým polynómom. Pri dôsledkovej

úprave nemusíme (hoci na druhej strane môžeme) dostať rovnicu ekvivalentnú s pôvodnou rovnicou.

**15.6 Príklad.** Rovnica nad $R$

$$2x^2 + 2x + 1 = 5x^2 - 2x - 3 \tag{8}$$

sa ekvivalentnou úpravou prevedie na rovnicu

$$3(x + \frac{2}{3})(x - 2) = 0.$$

Dôsledkovou úpravou možno (8) previesť na rovnicu

$$(2x^2 + 2x + 1) \cdot (x^2 - 2) = (5x^2 - 2x - 3) \cdot (x^2 - 2), \tag{9}$$

ekvivalentnú s rovnicou

$$3(x + \frac{2}{3})(x - 2)(x + \sqrt{2})(x - \sqrt{2}) = 0.$$

Vidíme, že množina riešení rovnice (8), $\{-\frac{2}{3}, 2\}$, je vlastnou podmnožinou množiny riešení rovnice (9), $\{-\frac{2}{3}, 2, -\sqrt{2}, \sqrt{2}\}$, teda rovnice (8) a (9) nie sú ekvivalentné. Naproti tomu inou dôsledkovou úpravou dostaneme z (8) rovnicu

$$(2x^2 + 2x + 1) \cdot (x^2 + 3) = (5x^2 - 2x - 3) \cdot (x^2 + 3), \tag{10}$$

ekvivalentnú s rovnicou

$$3(x + \frac{2}{3})(x - 2)(x^2 + 3) = 0,$$

ktorá je v $R$ ekvivalentná s rovnicou (8), pretože polynóm $x^2 + 3$ nemožno nad $R$ ďalej rozložiť. Avšak (10) nie je ekvivalentná s (8) v $C$, pretože v $C$ možno $x^2 + 3$ rozložiť na súčin $(x + \sqrt{3}i)(x - \sqrt{3}i)$, teda (10) má v $C$ okrem koreňov $-\frac{2}{3}$ a 2 aj korene $-\sqrt{3}i$ a $\sqrt{3}i$.

Ďalšou dôsledkovou úpravou algebraickej rovnice s číselnými koeficientami je umocnenie oboch strán rovnice.

15.7 Veta. *Nech $A \subseteq A'$ sú podobory integrity poľa $C$ komplexných čísel. Množina všetkých riešení v $A'$ algebraickej rovnice nad $A$*

$$L(x) = P(x) \tag{2}$$

*je podmnožinou množiny všetkých riešení algebraickej rovnice*

$$L(x)^2 = P(x)^2. \tag{11}$$

Dôkaz. Je opäť jednoduchý. Ak $c \in A'$ je koreňom rovnice (2), tak v $A' \subseteq C$ platí rovnosť komplexných čísel $L(c) = P(c)$, čiže platí aj rovnosť $L(c)^2 = P(c)^2$. Preto $c$ je aj koreňom rovnice (11). □

To, že rovnica (11) môže mať vo všeobecnosti viac koreňov ako rovnica (2) možno ilustrovať mnohými príkladmi. Tak napríklad rovnica $x^2 = 1$ má v $C$ dva korene 1 a $-1$, ale po umocnení sa prevedie na rovnicu $x^4 = 1$, ktorá má v $C$ štyri korene: popri $1, -1$ aj $i, -i$.

Pri riešení rovníc nad číselnými obormi integrity v školskej praxi sa často používajú dôsledkové úpravy. Ako sme vyššie ukázali, takýmito úpravami síce dostaneme všetky korene pôvodnej rovnice, ale výsledná rovnica často má viac koreňov než pôvodná. Preto sa treba skúškou presvedčiť, ktoré z koreňov výslednej rovnice sú aj koreňmi pôvodnej rovnice. Ak používame iba ekvivalentné úpravy, máme zaručené, že korene výslednej rovnice sú aj koreňmi pôvodnej rovnice a skúška nie je nevyhnutnou súčasťou riešenia. Dôsledkové úpravy by sme síce vždy mohli pridaním dodatočných podmienok nahradiť ekvivalentnými, ale spravidla sa tým postup riešenia komplikuje a „spomaľuje“, a preto sa dáva prednosť „rýchlejším“ dôsledkovým úpravám aj „za cenu skúšky“, ktorú treba následne urobiť.

Na záver si ukážeme, ako možno istý typ úloh v školskej praxi riešiť prevedením na rovnice nad obormi integrity zvyškových tried $\overline{Z}_n$.

**15.8 Príklad.** Máme úlohu zistiť, koľkými spôsobmi možno 25 detí v „škole v prírode“ umiestniť v $2-$ a $3-$posteľových izbách.

Potrebujeme teda zistiť, koľkými spôsobmi možno číslo 25 napísať v tvare $2x + 3y$, kde $x, y$ sú nezáporné celé čísla. Máme teda vlastne riešiť tzv. diofantickú rovnicu

$$2x + 3y = 25. \tag{12}$$

Pre každú dvojicu $(x, y)$ ktorá je riešením musí platiť aj rovnosť $2x + 3y \equiv 25 \pmod 2$ t.j. $\overline{2} \odot \overline{x} \oplus \overline{3} \odot \overline{y} = \overline{25}$ v obore integrity $\overline{Z}_2$. (Poznamenávame, že modul 2 bol zvolený preto, lebo najmenší koeficient v rovnici (12) je 2.) Pretože $\overline{2} = \overline{0}$, $\overline{3} = \overline{1}$ a $\overline{25} = \overline{1}$ v $\overline{Z}_2$, dostávame $\overline{y} = \overline{1}$, odkiaľ vyplýva, že $y = 2k+1$ pre $k \in Z$. Po dosadení do (12) dostaneme $2x+3(2k+1) = 25$, odkiaľ $2x = 22-6k$, $x = 11-3k$. Riešením rovnice (12) v $Z$ sú teda všetky dvojice $(11 - 3k, 2k + 1)$, kde $k \in Z$. Pretože nás zaujímajú iba nezáporné riešenia, hľadáme $k \in Z$ pre ktoré $11-3k \geq 0 \wedge 2k+1 \geq 0$. Ľahko je vidieť, že riešením sú $k = 0, 1, 2, 3$. Úloha má teda 4 riešenia:

1. pre $k = 0$ je riešením $(x, y) = (11, 1)$, čiže 11 dvojposteľových a 1 trojposteľová izba;
2. pre $k = 1$ je riešením $(x, y) = (8, 3)$, čiže 8 dvojposteľových a 3 trojposteľové izby;
3. pre $k = 2$ je riešením $(x, y) = (5, 5)$, čiže 5 dvojposteľových a 5 trojposteľových izieb;
4. pre $k = 3$ je riešením $(x, y) = (2, 7)$, čiže 2 dvojposteľové a 7 trojposteľových izieb.

**15.9 Príklad.** Zaujíma nás koľkými spôsobmi možno 19 litrov vína rozdeliť do $3-$, $4-$ a $5-$litrových demižónov.

Opäť to vedie na diofantickú rovnicu

$$3x + 4y + 5z = 19. \tag{13}$$

Pretože 3 je najmenší koeficient, prevedieme ju na rovnicu

$$\overline{3} \odot \overline{x} \oplus \overline{4} \odot y \oplus \overline{5} \odot \overline{z} = \overline{19}$$

nad $\overline{Z}_3$. Keďže $\overline{3} = \overline{0},\ \overline{4} = \overline{1},\ \overline{5} = \overline{2}$ a $\overline{19} = \overline{1}$ v $\overline{Z}_3$, dostávame $\overline{y} \oplus \overline{2} \odot \overline{z} = \overline{1}$. Teda $y + 2z = 3k + 1,\ k \in Z$. Zvolíme $z$ za parameter a dostaneme $y = 3k + 1 - 2z$. Po dosadení do (13) máme $3x+4(3k+1-2z)+5z = 19$, odkiaľ $3x = 15-12k+3z,\ x = 5 - 4k + z$. Riešením rovnice (13) sú teda trojice $(5 - 4k + z, 1 + 3k - 2z, z)$, kde $k, z \in Z$. Pretože nás zaujímajú iba nezáporné riešenia, hľadáme $k, z \in Z$ pre ktoré $5-4k+z \geq 0 \wedge 1+3k-2z \geq 0 \wedge z \geq 0$, čiže $4k-5 \leq z \leq \frac{1+3k}{2} \wedge z \geq 0$. Pre $k$ musí teda platiť $4k - 5 \leq \frac{1+3k}{2}$, odkiaľ $8k - 10 \leq 1 + 3k,\ 5k \leq 11$, čiže $k = 0, 1, 2$. Pre $k = 0$ vyhovuje $z = 0$, pre $k = 1$ vyhovujú $z = 0, 1, 2$ a pre $k = 2$ vyhovuje $z = 3$. Úloha má teda 5 riešení:

1. pre $k = 0, z = 0$ je riešením $(x, y, z) = (5, 1, 0)$, čiže 5 trojlitrových a 1 štvorlitrový demižón;

2. pre $k = 1, z = 0$ je riešením $(x, y, z) = (1, 4, 0)$, čiže 1 trojlitrový a 4 štvorlitrové demižóny;

3. pre $k = 1, z = 1$ je riešením $(x, y, z) = (2, 2, 1)$, čiže 2 trojlitrové, 2 štvorlitrové a 1 päťlitrový demižón;

4. pre $k = 1, z = 2$ je riešením $(x, y, z) = (3, 0, 2)$, čiže 3 trojlitrové a 2 päťlitrové demižóny;

5. pre $k = 2, z = 3$ je riešením $(x, y, z) = (0, 1, 3)$, čiže 1 štvorlitrový a 3 päťlitrové demižóny.

## Použitá literatúra


[1] G. Birkhoff, S. Mac Lane, *Prehľad modernej algebry*, Alfa, Bratislava, 1979.

[2] A. Haviar, P. Hrnčiar, P. Klenovčan, *Algebra I.*, Pedagogická fakulta, Banská Bystrica, 1991, skriptá.

[3] A. Haviar, A. Legéň, *Algebraické štruktúry*, SPN, Bratislava, 1977, skriptá.

[4] T.W. Hungerford, *Algebra, Graduate Texts in Mathematics 73*, Springer-Verlag, 1981.

[5] T. Katriňák a kol., *Algebra a teoretická aritmetika (1)*, Alfa, Bratislava, 1985.

[6] P. Klenovčan, A. Haviar, M. Haviar, *Úvod do štúdia matematiky*, Pedagogická fakulta UMB, Banská Bystrica, 1996, skriptá.

[7] A. Legéň, *Grupy, okruhy a zväzy*, Alfa, Bratislava, 1980.

[8] M. P. Lelčuk a kol., *Praktičeskije zaňatija po algebre i teorii čisel*, Vyšejšaja škola, Minsk, 1986.

[9] S. Mac Lane, G. Birkhoff, *Algebra*, Alfa, Bratislava, 1973.

[10] R. Solomon, *On Finite Simple Groups and Their Classification*, Notices of the American Mathematical Society **42, n. 2** (1995), 231-239.

[11] P. Svätokrížny, *Algebra (pre poslucháčov III. ročníka DŠ na PI)*, SPN, Praha, 1964.

[12] J. Weil, *Rozpracované řešení úloh z vyšší algebry*, Academia, Praha, 1987.

[13] Š. Znám, *Teória čísel*, Alfa, Bratislava, 1977.


### Ďalšia odporúčaná literatúra


[14] J. Bečvář, *Úvod do algebry*, SPN, Praha, 1984.

[15] L. Bican a kol., *Sbírka úloh z algebry pro učitelské studium*, SPN, Praha, 1984.

[16] A. Bicanová, T. Kepka, E. Nováková, *Sbírka úloh, příkladů a cvičení z algebry*, SPN, Praha, 1984.

[17] G. Birkhoff, T. C. Bartee, *Aplikovaná algebra*, Alfa, Bratislava, 1981.

[18] A. K. Fadejev, J. S. Sominskij, *Zbierka úloh z vyššej algebry*, Alfa, Bratislava, 1968.

[19] T. Katriňák, A. Legéň, *Algebra*, UK, Bratislava, 1974, skriptá.

[20] M. Kolibiar a kol., *Vybrané partie z matematiky I.*, UK, Bratislava, 1979, skriptá.

[21] A. I. Kostrikin, *Sbornik zadač po algebre*, Nauka, Moskva, 1987.

[22] A. G. Kuroš, *Kapitoly z obecné algebry*, Academia, Praha, 1977.

[23] L. C. Larson, *Metódy riešenia matematických problémov*, Alfa, Bratislava, 1990.

[24] L. Procházdka a kol., *Algebra*, Academia, Praha, 1990.

[25] B. L. Van der Waerden, *Algebra*, Nauka, Moskva, 1976.

**Obsah**


Predslov 1

1. Zvyškové triedy celých čísel 2
2. Základné poznatky o grupoidoch 7
3. Izomorfizmus grupoidov 17
4. Grupy. Príklady grúp 23
5. Cyklické grupy. Rád prvku v grupe 28
6. Grupy transformácií 34
7. Rozklad podľa podgrupy. Lagrangeova veta 40
8. Normálne podgrupy, kongruencie na grupách a faktorové grupy 46
9. Klasifikácia konečných grúp do rádu 15 53
10. Okruhy a podokruhy. Izomorfizmus okruhov. 57
11. Adjunkcia, algebraické a transcendentné prvky 65
12. Obory integrity, telesá, polia 69
13. Podielové pole oboru integrity 77
14. Ideály, kongruencie na okruhoch a faktorové okruhy 81
15. Ekvivalentné a dôsledkové úpravy pri riešení rovníc nad obormi integrity 87

Použitá literatúra. Ďalšia odporúčaná literatúra 92