UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Pedagogická fakulta

ÚVOD DO ŠTÚDIA MATEMATIKY

P. Klenovčan, A. Haviar, M. Haviar

1996

Obsah

Úvod

Tento učebný text je určený pre študentov prvých ročníkov učiteľského štúdia v kombináciách s matematikou. Jeho zámerom je pomôcť posluchárom preklenúť počiatočné ťažkosti súvisiace s prechodom od stredoškolskej matematiky, zameranej na aplikácie matematických poznatkov vhodných pre široké spektrum pracovníkov, k špecializovanej príprave budúcich učiteľov matematiky. Od budúceho učiteľa matematiky sa vyžaduje dôkladné osvojenie si celej škály základných matematických poznatkov a metód práce. Hlavná zmena sa prejavuje v tom, že nestačí poznať „recepty" (návody) na riešenie úloh, ale treba poznať aj možnosti a spôsoby tvorby nových receptov a dokázať odôvodniť správnosť používaných postupov. Znamená to zvládnuť špecifický spôsob matematického myslenia a osvojiť si istú „matematickú kultúru" pri ústnom a písomnom prejave.

Pri písaní textu sme mali na zreteli nielen matematické, ale aj didaktické hľadiská, preto sme pri objasňovaní pojmov a rôznych súvislostí (najmä pri príkladoch a cvičeniach) vychádzali často z poznatkov, ktoré si čitateľ osvojil už v rámci stredoškolskej matematiky. Takisto vo formuláciách sme sa snažili o presnosť a precíznosť, ale nie na úkor zrozumiteľnosti.

Usporiadanie učiva je vždy problémom, ktorý nemožno celkom uspokojivo vyriešiť, lebo každá z rozumných alternatív má prednosti aj nedostatky. Vnútorná štruktúra kapitol je prispôsobená ich obsahu a rozsahu. Vety, definície a príklady sú číslované, čo pomáha pri odvolaní sa na ne v ďalšom texte. Ak sa odvolávame napr. na vetu 2 znamená to, že ide o vetu 2 v príslušnej (tej istej) kapitole. Ak sa odvolávame na vetu 3.2 tak ide o vetu 2 z kapitoly 3. Symbolom □ označujeme koniec príkladu a koniec dôkazu.

Za cenné pripomienky, ktoré nám pomohli pri konečnej úprave textu, ďakujeme obom recenzentom.

Banská Bystrica, november 1996

Autori

1. Rozširovanie číselných oborov

Jedným z najčastejšie používaných pojmov, s ktorými ste sa doteraz pri štúdiu matematiky stretávali je pojem čísla. Postupne ste sa oboznamovali s prirodzenými, celými, racionálnymi a reálnymi číslami. Na strednej škole niektorí z vás preberali aj učivo o komplexných číslach. Poznáte základné vlastnosti sčítania, násobenia, odčítania, delenia, umocňovania, odmocňovania a usporiadania. Nie všetky vlastnosti sú však spoločné pre všetkých päť spomenutých číselných oborov (o číselnom obore hovoríme zvyčajne vtedy, keď na danej číselnej množine uvažujeme aj nejaké operácie, t.j. počtové výkony). Postupne ste sa dozvedali o potrebe rozšíriť obor prirodzených čísel na obor celých, obor celých na obor racionálnych a obor racionálnych na obor reálnych čísel. Preberali ste základné vlastnosti operácií a usporiadania a s ich pomocou ste riešili rôzne úlohy.

V tejto časti si stručne niektoré vlastnosti dôležité pre ďalšie štúdium zopakujeme. Neskôr sa budeme vlastnosťami číselných oborov zaoberať podrobnejšie, najmä v predmetoch matematická analýza a teoretická aritmetika tak, aby čitateľ získal ďalšie poznatky a nadhľad potrebný pre budúceho učiteľa matematiky.

Potrebu rozširovania číselných oborov budeme demonštrovať na jednoduchých typoch rovníc, ktoré v rozšírenom obore majú korene, hoci v pôvodnom žiadny koreň nemajú. Tentoraz nás budú zaujímať len tzv. algebraické rovnice o jednej neznámej, t.j. rovnice typu

$$\text{(R)} \qquad a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_n \neq 0.$$

Čísla $a_n, a_{n-1}, \ldots, a_1, a_0$ voláme koeficienty, neznámou je x. Medzi takéto rovnice patria vám už známe lineárne, kvadratické, binomické a reciproké rovnice.

Prirodzené čísla. Prirodzené čísla sú ideálne (t.j. nehmotné) objekty, ktoré utvorili ľudia pri skúmaní vzťahov medzi súbormi reálnych objektov. Ich vytvorenie bolo teda dôsledkom prirodzených potrieb pri riešení úloh bežného života, keď sa abstrahovalo od veľkosti, farby a ďalších vlastností, ale podstatné bolo len to, či predmety dvoch súborov možno zoradiť do dvojíc, alebo či jeden súbor má menej predmetov ako druhý. V tejto súvislosti boli zavedené vzťahy „menej“ a „viac“ a oveľa neskôr aj ich symbolické vyjadrenie $<$ a $>$.

Vzťah (binárna relácia) $<$ má tri základné vlastnosti:

$$\text{(1)} \qquad \text{ak } m < n, \text{ tak neplatí } n < m \qquad \text{(asymetričnosť)},$$

$$\text{(2)} \qquad \text{ak } m < n \text{ a } n < k, \text{ tak } m < k \qquad \text{(tranzitívnosť)},$$

pre každé dve prirodzené čísla m, n platí práve jeden zo vzťahov

$$\text{(3)} \qquad m < n, \quad m = n, \quad n < m \qquad \text{(trichotomičnosť)}.$$

Ukázalo sa užitočným aj používanie vzťahu $\leq$, ktorý s predchádzajúcim bezprostredne súvisí. Platí

$$a \leq b \text{ práve vtedy, keď } a < b \text{ alebo } a = b.$$

Vzťah $\leq$ má teda vlastnosť: pre každé prirodzené číslo a je $a \leq a$, ktorú nazývame reflexívnosť.

V praktickej činnosti človek utvára zo súborov objektov nové súbory. Keď si začal všímať súvislosti medzi počtami prvkov pôvodných súborov a počtami prvkov z nich utvorených súborov, zaviedol počítanie s prirodzenými číslami.

Základnými operáciami (počtovými výkonmi) na množine prirodzených čísel sú sčítanie a násobenie. Počet prvkov konečnej množiny A označíme symbolom $|A|$. Ak $|A| = n$ hovoríme, že množina A má n prvkov alebo, že počet prvkov množiny A je n. Súvis medzi počtami prvkov množín a operáciami je daný vzťahmi:

ak $m = |A|$, $n = |B|$ a ak $A \cap B = \emptyset$, tak $m + n = |A \cup B|$,
ak $m = |A|$, $n = |B|$, tak $m \cdot n = |A \times B|$,

kde $A \times B$ je karteziánsky súčin množín A, B, t.j. $A \times B$ je množina všetkých usporiadaných dvojíc, ktorých prvá zložka je z množiny A a druhá z množiny B (podrobnejšie sa budeme karteziánskym súčinom zaoberať v kapitole 3).

Poznámka. Pri násobení často znak operácie „.“ vynechávame.

Uvedené operácie majú nasledovné základné vlastnosti. Pre ľubovoľné prirodzené čísla m, n, k platí

$$m + n = n + m, \qquad m \cdot n = n \cdot m, \tag{4}$$

$$(m + n) + k = m + (n + k), \qquad (m \cdot n) \cdot k = m \cdot (n \cdot k), \tag{5}$$

$$m \cdot (n + k) = m \cdot n + m \cdot k. \tag{6}$$

V (4) je uvedená tzv. komutatívnosť operácií, v (5) asociatívnosť operácií a (6) je distributívnosť násobenia vzhľadom na sčítanie.

Operácie sčítania a násobenia sú kompatibilné s reláciou usporiadania v nasledujúcom zmysle: pre ľubovoľné prirodzené čísla m, n, k platí

$$\text{ak} \quad m < n, \quad \text{tak} \quad m + k < n + k, \tag{7}$$

$$\text{ak} \quad m < n, k \neq 0, \quad \text{tak} \quad m \cdot k < n \cdot k. \tag{8}$$

Vlastnosť (7) sa volá monotónnosť sčítania vzhľadom k nerovnosti a vlastnosť (8) sa volá monotónnosť násobenia vzhľadom k nerovnosti.

S usporiadaním prirodzených čísel súvisí aj nasledujúca, často využívaná vlastnosť, ktorá sa nazýva vlastnosťou *dobrého usporiadania*:

Každá neprázdna množina prirodzených čísel obsahuje najmenší prvok.

Číslo 0 (ktorým označujeme počet prvkov prázdnej množiny) sa niekedy nezaraďuje medzi prirodzené čísla. My však nulu budeme považovať za prirodzené číslo.

Množinu všetkých nenulových (kladných) prirodzených čísel budeme označovať N^+ a množinu všetkých prirodzených čísel budeme označovať N.

Dôležitou vlastnosťou oboru prirodzených čísel je tzv. princíp matematickej indukcie.

Predpokladajme, že M je taká podmnožina množiny N, o ktorej platí:

(i) 0 je prvkom množiny M,
(ii) ak n je prvkom M, tak aj $n + 1$ je prvkom M.

Potom $M = N$.

Na predchádzajúcej vlastnosti je založená metóda dôkazu matematickou indukciou.

Matematická indukcia. Nech a je prirodzené číslo a nech $P(n)$ je tvrdenie o čísle n (výroková forma s jedinou premennou n). Ak dokážeme

a) $P(a)$ je pravdivé,
b) pre každé prirodzené číslo $k \geq a$ z pravdivosti $P(k)$ vyplýva pravdivosť $P(k+1)$,

tak $P(n)$ je pravdivé pre všetky prirodzené čísla $n \geq a$.

PRÍKLAD 1. Dokážte, že pre všetky prirodzené čísla $n \geq 1$ platí

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2.$$

RIEŠENIE. a) Zrejme pre $n = 1$ uvedená rovnosť platí (ľavá aj pravá strana sa rovná 1).

b) Ukážeme ďalej, že ak uvedená rovnosť platí pre k, tak platí aj pre $k+1$, t.j., že z rovnosti

$$1^3 + 2^3 + \cdots + k^3 = \frac{1}{4}k^2(k+1)^2$$

vyplýva rovnosť

$$1^3 + 2^3 + \cdots + k^3 + (k+1)^3 = \frac{1}{4}(k+1)^2(k+2)^2.$$

Napíšeme ľavú stranu poslednej rovnosti a s využitím indukčného predpokladu (t.j. prvej rovnosti) postupne upravujeme:

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{1}{4}k^2(k+1)^2 + (k+1)^3 = (k+1)^2(\frac{1}{4}k^2 + k + 1) = \\ &= (k+1)^2\frac{k^2+4k+4}{4} = \frac{1}{4}(k+1)^2(k+2)^2. \end{aligned}$$

Teda uvedená rovnosť platí pre každé prirodzené číslo $n \geq 1$. □

Uvedieme ešte tzv. druhý princíp matematickej indukcie, ktorý je s hore uvedenou metódou ekvivalentný, niektoré problémy sa však riešia pomocou tejto druhej metódy.

Druhý princíp matematickej indukcie. Nech a je prirodzené číslo a nech $P(n)$ je tvrdenie o n pre každé prirodzené číslo $n \geq a$. Ak

a) $P(a)$ je pravdivé,
b) pre každé prirodzené číslo $k \geq a$ z pravdivosti $P(a), P(a+1), \ldots, P(k)$ vyplýva pravdivosť $P(k+1)$,

tak $P(n)$ platí pre každé prirodzené číslo $n \geq a$.

Už v ďalšej kapitole o deliteľnosti budeme využívať obidva spôsoby dôkazu matematickou indukciou, ktoré sme tu spomenuli.

Matematická indukcia je metóda, ktorou sa môžeme pokúsiť riešiť každý problém typu: „Dokážte, že $P(n)$ platí pre všetky prirodzené čísla $n \geq a$“. Takéto tvrdenia sa nazývajú všeobecné tvrdenia.

Iný typ tvrdenia je tzv. existenčné tvrdenie, ktoré možno vyjadriť v tvare: „Existuje také x (patriace do nejakej množiny S), že platí $P(x)$“. Tento typ tvrdenia je možné často dokázať pomocou Dirichletovho princípu.

Dirichletov princíp. Nech k, n sú nenulové prirodzené čísla. Ak je $k \cdot n + 1$ objektov rozdelených do n skupín, tak jedna zo skupín obsahuje aspoň $k+1$ objektov.

Použitie tohto princípu ukážeme na nasledujúcom jednoduchom príklade.

PRÍKLAD 2. Vo vnútri štvorca $ABCD$ so stranou dĺžky 1 je daných päť bodov P_1, P_2, P_3, P_4, P_5. Dokážte, že aspoň jedna z úsečiek P_iP_j má veľkosť menšiu ako $\frac{\sqrt{2}}{2}$.

RIEŠENIE. Rozdeľme daný štvorec úsečkami, ktorých krajné body sú stredy protiľahlých strán, na štyri zhodné štvorce. Veľkosť uhlopriečky každého z nich je $\frac{\sqrt{2}}{2}$. Podľa Dirichletovho princípu (pre $k = 1$, $n = 4$) jeden z týchto štvorcov obsahuje aspoň dva body a ich vzdialenosť je zrejme menšia ako $\frac{\sqrt{2}}{2}$. □

Dôsledkami uvedených vlastností a ďalšími vlastnosťami prirodzených čísel sa budeme zaoberať ešte viackrát neskôr.

Celé čísla. Už jednoduchá algebraická rovnica (teda rovnica typu (R)), napr. $x + 2 = 0$, ktorej koeficienty sú prirodzené čísla nemá v obore prirodzených čísel riešenie. Súvisí to s tým, že k nenulovým prirodzeným číslam neexistujú opačné čísla.

Keď chcel človek vyjadriť hodnoty menšie ako nula (nadmorská výška pod úrovňou morskej hladiny a pod.) začal používať aj opačné čísla k prirodzeným číslam. Opačné číslo k číslu x označujeme $-x$. Číslo opačné k prirodzenému číslu, ktoré už nevyjadruje počet prvkov nejakej množiny (nie je to už prirodzené číslo), nazývame záporné číslo. Opačné číslo $-x$ je číslom x jednoznačne určené a to vzťahom

$$x + (-x) = 0. \tag{9}$$

Treba si však uvedomiť, že znak $-$ pred symbolom premennej neznamená, že ide o záporné číslo. Ak napr. $x = -3$, tak $-x = 3$.

Množinu všetkých prirodzených čísel a všetkých k nim opačných čísel budeme označovať Z a nazývať množina všetkých celých čísel. Každé prirodzené číslo je teda aj celým (celým nezáporným) číslom.

Racionálne čísla. Opäť môžeme nájsť jednoduchú algebraickú rovnicu s celočíselnými koeficientami, napr. $3 \cdot x - 2 = 0$, ktorá nemá celočíselné riešenie. To je dôvod (matematický) pre zavedenie racionálnych čísel, ktoré zapisujeme pomocou zlomkov. Ak a, b sú celé čísla, pričom $b \neq 0$, tak $\frac{a}{b}$ je zápis (jeden zo zápisov) racionálneho čísla. Ku každému nenulovému racionálnemu číslu $\frac{a}{b}$ existuje tzv. prevrátené číslo $\frac{b}{a}$, ktoré je jednoznačne určené číslom $\frac{a}{b}$ a to vzťahom

$$\frac{a}{b} \cdot \frac{b}{a} = 1. \tag{10}$$

Množinu všetkých racionálnych čísel budeme označovať písmenom Q. Každé celé číslo je aj racionálnym číslom. V obore racionálnych čísel má každá rovnica $a \cdot x = b$ (kde a, b sú racionálne čísla, $a \neq 0$) riešenie.

Reálne čísla. Jednoduchá rovnica s racionálnymi koeficientami, napr. $x^2 - 2 = 0$ nemá v obore racionálnych čísel riešenie. Môžeme to tiež interpretovať ako nasledujúci poznatok geometrickej povahy, známy už starogréckym matematikom: ak

zostrojíme rovnoramenný pravouhlý trojuholník, ktorého každé rameno má dĺžku 1, tak dĺžku prepony (vieme, že je to $\sqrt{2}$) nemožno vyjadriť žiadnym racionálnym číslom.

Každé racionálne číslo možno znázorniť (zobraziť) na číselnej osi. Z toho čo sme uviedli ale vyplýva, že nie každý bod číselnej osi je obrazom niektorého racionálneho čísla. Znamená to, že na číselnej osi existujú akési „medzery“. Ak pridáme k racionálnym číslam, ktorých tzv. dekadické zápisy sú buď ukončené alebo periodické neukončené aj čísla s neukončenými neperiodickými zápismi (tzv. iracionálne čísla) dostaneme množinu všetkých reálnych čísel. Budeme ju označovať písmenom E.

Základné vlastnosti usporiadania a operácií ostávajú v platnosti aj pre celé, racionálne a reálne čísla, avšak vlastnosť (8) má tvar

(8a) $$\text{ak} \quad m < n \quad \text{a} \quad k > 0, \quad \text{tak} \quad m \cdot k < n \cdot k,$$

(8b) $$\text{ak} \quad m < n \quad \text{a} \quad k < 0, \quad \text{tak} \quad m \cdot k > n \cdot k.$$

Príklad 3. Dokážte, že pre ľubovoľné dve nezáporné reálne čísla a, b platí $\frac{a+b}{2} \geq \sqrt{a \cdot b}$.

Riešenie. Predpokladajme, že uvedené tvrdenie neplatí, teda že platí: existujú také nezáporné reálne čísla a, b, že $\frac{a+b}{2} < \sqrt{a \cdot b}$. Po umocnení postupnými („dovolenými“) úpravami dostávame

$$\begin{aligned} \frac{a^2 + 2ab + b^2}{4} &< ab, \\ a^2 + 2ab + b^2 &< 4ab, \\ a^2 - 2ab + b^2 &< 0, \\ (a - b)^2 &< 0. \end{aligned}$$

Teda ak predpokladáme, že platí negácia pôvodného tvrdenia, dostaneme nepravdivé tvrdenie. To znamená, že pre ľubovoľné nezáporné reálne čísla a, b platí pôvodné tvrdenie, t.j., že $\frac{a+b}{2} \geq \sqrt{a \cdot b}$. □

V predchádzajúcom príklade bol použitý tzv. dôkaz sporom. Týmto aj ďalšími typmi dôkazov sa budeme podrobnejšie zaoberať v šiestej kapitole. Po preštudovaní tejto kapitoly odporúčame vrátiť sa k predchádzajúcemu príkladu (a samozrejme aj k ďalším dôkazom, ktoré sa dovtedy v texte vyskytnú).

Ku každému reálnemu číslu x môžeme priradiť nezáporné reálne číslo, ktoré sa volá absolútna hodnota tohoto čísla. Absolútnu hodnotu reálneho čísla x označujeme $|x|$ a definujeme takto:

(11) $$|x| = \quad x, \qquad \text{ak } x \geq 0,$$

(12) $$|x| = -x, \qquad \text{ak } x < 0.$$

V nasledujúcom tvrdení sú zhrnuté niektoré základné vlastnosti absolútnej hodnoty.

VETA 1. *Pre každé reálne číslo a platí*
a) $|a| = |-a|$,
b) $a \leq |a|, \qquad -a \leq |a|$.

Platnosť tvrdení uvedených vo vete môžeme overiť rozlíšením prípadov $a \geq 0$ a $a < 0$.

VETA 2. *Pre ľubovoľné reálne čísla a, b platí*
a) $|a+b| \leq |a| + |b|$,
b) $|a \cdot b| = |a| \cdot |b|$.

DÔKAZ. a) Nech $a + b \geq 0$. Pretože (podľa vety 1.b)) $a \leq |a|$, $b \leq |b|$, sčítaním týchto nerovností dostávame $a + b \leq |a| + |b|$, t.j. $|a + b| \leq |a| + |b|$. Podobne v prípade $a + b < 0$ (opäť podľa vety 1.b)) $-a \leq |a|$, $-b \leq |b|$, z čoho $-a - b = -(a + b) = |a + b| \leq |a| + |b|$.

Časť b) je zrejme pravdivá, ak aspoň jedno z čísel a, b je nulové a dôkaz možno ukončiť rozlíšením nasledovných štyroch prípadov: 1. $a > 0$, $b > 0$, 2. $a > 0$, $b < 0$, 3. $a < 0$, $b > 0$, 4. $a < 0$, $b < 0$. □

Komplexné čísla. Ukazuje sa, že ani rozšírenie číselnej množiny na množinu reálnych čísel nie je postačujúce. Opäť existuje jednoduchá rovnica s reálnymi koeficientami, napr. $x^2 + 1 = 0$, ktorá nemá v obore reálnych čísel riešenie. Množina reálnych čísel bola rozšírená na množinu komplexných čísel, ktorú budeme označovať C.

Každé komplexné číslo možno zapísať v tvare $a + b \cdot i$, kde i je tzv. imaginárna jednotka, o ktorej platí

$$i^2 = -1, \tag{13}$$

(t.j. i je vlastne jedno z riešení rovnice $x^2 + 1 = 0$ v obore komplexných čísel).

Používanie komplexných čísel má veľký význam v aplikáciách matematiky a to najmä vo fyzike a v technických oboroch.

Pretože učivo o komplexných číslach sa v niektorých triedach stredných škôl nepreberá, budeme sa komplexným číslam venovať trochu podrobnejšie.

Dve komplexné čísla $a + bi$, $c + di$ sa rovnajú, keď $a = c$, $b = d$.

Pre súčet a súčin komplexných čísel $a + bi$, $c + di$ platí

$$\begin{aligned}(a + bi) + (c + di) &= a + c + (b + d)i,\\ (a + bi) \cdot (c + di) &= ac - bd + (ad + bc)i.\end{aligned}$$

Pri počítaní s komplexnými číslami sa teda postupuje podobne ako pri sčitovaní a násobení algebraických výrazov, pričom ešte používame, že $i^2 = -1$.

PRÍKLAD 4. Nájdite reálne čísla x, y pre ktoré platí

$$(2 - i)x + (5 + 6i)y = 1 - 3i.$$

RIEŠENIE. Ak upravíme ľavú stranu na tvar $a + bi$, dostaneme

$$(2x + 5y) + (-x + 6y)i = 1 - 3i,$$

z čoho dostávame sústavu rovníc

$$2x + 5y = 1, \qquad -x + 6y = -3,$$

ktorej riešením je $x = \frac{21}{17}$, $y = \frac{-5}{17}$. □

PRÍKLAD 5. Nájdite všetky komplexné čísla $x+yi$, pre ktoré $(x+yi)^2 = -3-4i$ (t.j. $x+yi = \sqrt{-3-4i}$).

RIEŠENIE. Po úprave dostávame

$$(x^2 - y^2) + 2xyi = -3 - 4i.$$

Táto rovnica je ekvivalentná systému rovníc

$$x^2 - y^2 = -3, \qquad 2xy = -4.$$

Po umocnení obidvoch rovníc a sčítaní dostaneme $(x^2+y^2)^2 = 25$, z čoho $x^2+y^2 = 5$ ($x^2+y^2 = -5$ nevyhovuje lebo x, y sú reálne čísla). Z tejto rovnice a z prvej rovnice nášho systému rovníc dostávame $x^2 = 1$, $y^2 = 4$ a teda $x = \pm 1$, $y = \pm 2$. Z druhej rovnice sústavy vyplýva, že ak $x = 1$, tak $y = -2$ a ak $x = -1$, tak $y = 2$. Daná úloha má teda dve riešenia: $1 - 2i$ a $-1 + 2i$. □

Ak v rovine zvolíme pravouhlý súradnicový systém, tak obrazom každého komplexného čísla je práve jeden bod roviny. Obrazom čísla $a+bi$ je bod $[a, b]$. Niekedy však za obraz čísla $a + bi$ pokladáme vektor, ktorý je daný orientovanou úsečkou so začiatočným bodom $[0, 0]$ a koncovým bodom $[a, b]$.

Komplexné čísla $a + bi$, $a - bi$ sa volajú komplexne združené čísla. Súčin komplexne združených čísel $(a + bi) \cdot (a - bi)$ je nezáporné reálne číslo $a^2 + b^2$. Číslo $\sqrt{a^2 + b^2}$ určuje vzdialenosť obrazu komplexného čísla $a + bi$ od začiatku súradnicového systému a nazýva sa jeho absolútnou hodnotou. Označuje sa $|a+bi|$.

PRÍKLAD 6. Určte $\left|\frac{3+i}{3-4i}\right|$.

RIEŠENIE. $\frac{3+i}{3-4i} = \frac{(3+i)\cdot(3+4i)}{(3-4i)\cdot(3+4i)} = \frac{5+15i}{25} = \frac{1}{5} + \frac{3}{5}i$, z čoho vyplýva, že $\left|\frac{3+i}{3-4i}\right| = \sqrt{\frac{1}{25} + \frac{9}{25}} = \frac{\sqrt{10}}{5}$. □

VETA 3. *Pre ľubovoľné komplexné čísla $u = a + bi$, $v = c + di$ platí*

$$|u + v| \le |u| + |v| \qquad a \qquad |u \cdot v| = |u| \cdot |v|.$$

DÔKAZ. Nerovnosť $|u + v| \le |u| + |v|$ je postupne ekvivalentná s nerovnosťami (pozor na umocňovanie, to nie je vždy ekvivalentná úprava):

$$\begin{aligned}
|(a + bi) + (c + di)| &\le |a + bi| + |c + di|,\\
|a + c + (b + d)i| &\le |a + bi| + |c + di|,\\
\sqrt{(a + c)^2 + (b + d)^2} &\le \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2},\\
(a + c)^2 + (b + d)^2 &\le a^2 + b^2 + 2\sqrt{(a^2 + b^2) \cdot (c^2 + d^2)} + c^2 + d^2,\\
ac + bd &\le \sqrt{(a^2 + b^2) \cdot (c^2 + d^2)}.
\end{aligned}$$

Ak $ac + bd < 0$, tak nerovnosť $ac + bd \le \sqrt{(a^2 + b^2) \cdot (c^2 + d^2)}$ je pravdivá a teda pravdivá je aj pôvodná nerovnosť. Ak $ac + bd \ge 0$, tak v ekvivalentných úpravách pokračujeme ďalej a dostávame

$$\begin{aligned}
(ac + bd)^2 &\le (a^2 + b^2) \cdot (c^2 + d^2),\\
0 &\le (ad)^2 - 2abcd + (bc)^2,\\
0 &\le (ad - bc)^2.
\end{aligned}$$

Pretože nerovnosť $0 \leq (ad - bc)^2$ je pravdivá pre ľubovoľné reálne čísla a, b, c, d, je pravdivá aj pôvodná nerovnosť.

Dôkaz rovnosti $|u \cdot v| = |u| \cdot |v|$ je jednoduchší, pokúste sa ho zapísať samostatne. □

Nech $a+bi$ je komplexné číslo rôzne od nuly. Veľkosť orientovaného uhla, ktorého vrcholom je začiatok súradnicového systému, začiatočným ramenom je kladná časť osi x a koncové rameno prechádza obrazom čísla $a + bi$ nazývame argument alebo amplitúda čísla $a + bi$. Ak amplitúdu komplexného čísla $u = a + bi$ označíme φ, tak

$$\cos\varphi = \frac{a}{|u|}, \qquad \sin\varphi = \frac{b}{|u|}.$$

Z toho dostaneme

$$a + bi = |u| \cdot (\cos\varphi + i\sin\varphi),$$

a to je tzv. goniometrický (trigonometrický) tvar komplexného čísla, ktorý je výhodný najmä pri násobení a delení komplexných čísel. Ak

$$u = |u| \cdot (\cos\varphi + i\sin\varphi), \quad v = |v| \cdot (\cos\psi + i\sin\psi),$$

tak

$$\begin{aligned} u \cdot v &= |u| \cdot |v| \cdot (\cos(\varphi + \psi) + i\sin(\varphi + \psi)), \\ \frac{u}{v} &= \frac{|u|}{|v|} \cdot (\cos(\varphi - \psi) + i\sin(\varphi - \psi)). \end{aligned}$$

Vzťah pre súčin dostávame priamo pomocou súčtových vzorcov a pomocou neho dostávame vzťah pre podiel, ak si uvedomíme, že pre prevrátenú hodnotu čísla v platí

$$\frac{1}{v} = \frac{1}{|v|} \cdot (\cos(-\psi) + i\sin(-\psi))$$

(lebo prevrátená hodnota je určená rovnosťou $v \cdot \frac{1}{v} = 1$).

Komplexné číslo, ktorého absolútna hodnota je 1 (t.j. číslo, ktorého obraz leží na jednotkovej kružnici) sa nazýva komplexná jednotka. Matematickou indukciou možno ukázať, že pre mocniny komplexnej jednotky platí

$$(\cos\varphi + i\sin\varphi)^n = \cos n \cdot \varphi + i\sin n \cdot \varphi.$$

Uvedený vzťah nazývame Moivrova veta a používame ho najmä pri umocňovaní komplexných čísel.

Vzniká prirodzená otázka, či aj teraz sa dá nájsť rovnica typu (R), ktorá by nemala v obore komplexných čísel riešenie. V roku 1799 Gauss dokázal, že každá algebraická rovnica, ktorej koeficienty sú komplexné čísla, má v obore komplexných čísel riešenie. To znamené, že kvôli riešeniu rovníc typu (R) už nie je potrebné obor komplexných čísel ďalej rozširovať. Týmito otázkami sa ale budete podrobnejšie zaoberať neskôr v predmete algebra.

Cvičenia.

1. Dokážte, že pre ľubovoľné prirodzené čísla a, b, c, d platí: ak $a < c$, $b < d$, tak $a + b < c + d$ aj $a \cdot b < c \cdot d$.

2. Dokážte, že pre ľubovoľné prirodzené čísla a, b, c platí:

a) ak $a + c < b + c$, tak $a < b$,

b) ak $a \cdot c < b \cdot c$ a $0 < c$, tak $a < b$.

3. Dokážte, že pre všetky kladné prirodzené čísla n platí:

a) $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$,

b) $1^4 + 2^4 + \cdots + n^4 = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1)$,

c) $1 - 3 + 5 - 7 + \cdots + (-1)^{n-1}(2n-1) = (-1)^{n-1}n$,

d) $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = \frac{1}{4}n(n+1)(n+2)(n+3)$.

4. Dokážte, že ak n je prirodzené číslo, tak:

a) $2^n > 2n + 1$ pre $n \geq 3$,

b) $2^n > n^2$ pre $n \geq 5$.

5. Dokážte, že pre každé prirodzené číslo $n \geq 1$ platí:

a) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$,

b) $\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \geq \frac{1}{2}$.

6. Nech S je štvorec so stranou dĺžky 2 cm. Dokážte, že z ľubovoľných deviatich bodov ležiacich v S možno vybrať také tri, ktoré sú vrcholmi trojuholníka s obsahom menším ako $\frac{1}{2}\,\mathrm{cm}^2$.

7. Dokážte, že v každej skupine šiestich ľudí sú buď aspoň traja ľudia, ktorí sa navzájom poznajú, alebo aspoň traja, ktorí sú si navzájom neznámi.

8. Z aritmetickej postupnosti $1, 4, 7, \ldots, 100$ vyberme 20 navzájom rôznych prirodzených čísel. Dokážte, že medzi nimi sú dve rôzne čísla, ktorých súčet je 104.

8. Rozdiel $\sqrt{|40\sqrt{2} - 57|} - \sqrt{40\sqrt{2} + 57}$ je celé číslo. Nájdite ho.

9. Porovnajte čísla:

a) $\frac{9}{\sqrt{11}-\sqrt{2}}$, $\frac{6}{3\sqrt{3}}$, b) $\log_3 108$, $\log_5 375$.

10. Dokážte, že pre ľubovoľné reálne čísla a, b platí:

a) $a^2 + b^2 + 1 \geq ab + a + b$,

b) $(a^2 + b^2)^3 - (a^3 + b^3)^2 \geq 0$,

c) $(a^2 - b^2)(a^4 - b^4) \leq (a^3 - b^3)^2$.

11. Dokážte, že pre reálne čísla a, b, c platí:

a) ak $a < -1$, $b > 2$, tak $2a + 2 - b - ab > 0$,

b) ak $1 < a < b + c < a + 1$, $b < c$, tak $b < a$,

c) ak $a + b \geq 0$, tak $a^3 + b^3 \geq a^2b + ab^2$,

d) ak $a > 1$, $b > 1$, tak $4a^4b^2 + 1 - a^2(4b^2 + 1) > 0$.

12. Dokážte, že pre každé kladné reálne a, b je $(a + b) \cdot (\frac{1}{a} + \frac{1}{b}) \geq 4$.

13. Dokážte, že pre ľubovoľné reálne číslo $a \neq 0$, $a > -1$ a všetky prirodzené čísla $n \geq 2$ platí tzv. Bernoulliho nerovnosť $(1 + a)^n > 1 + an$.

14. Nájdite reálne čísla x, y, ktoré vyhovujú rovnici

$$(1 + 2i)x + (3 - 5i)y = 1 - 3i.$$

15. Vypočítajte:

a) $(2 - 6i) + (5 + 2i) - (7 - 5i)$, b) $(5 + 3i)(2 + 2i)$, c) $\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^3$,

d) $(1 + 2i)^6$, e) $(1 + 2i)^5 - (1 - 2i)^5$,

f) $\frac{4 - 3i}{4 + 3i}$, g) $\frac{a + bi}{a - bi}$, h) $\frac{(1 + 2i)^2 - (1 - i)^3}{(3 + 2i)^3 - (2 + i)^2}$.

16. Riešte sústavu rovníc

$$(3-i)x+(4+2i)y=2+6i,$$
$$(4+2i)x-(2+3i)y=5+4i.$$

17. Vypočítajte:
a) $\sqrt{2i}$, b) $\sqrt{8-6i}$, c) $\sqrt{2-3i}$, d) $\sqrt{1-i\sqrt{3}}$.
18. Vyjadrite v trigonometrickom tvare komplexné čísla $1+i$, $1-i$, $-1+i$, $-1-i$, $-1+i\sqrt{3}$, $1-i\sqrt{3}$.
19. Riešte rovnice:
a) $|x|-x=1+2i$, b) $|x|+x=2+i$.
20. Vypočítajte:
a) $(1+i)^{25}$, b) $\left(\dfrac{1+i\sqrt{3}}{1-i}\right)^{20}$, c) $\dfrac{(-1+i\sqrt{3})^{15}}{(1-i)^{20}}+\dfrac{(-1-i\sqrt{3})^{15}}{(1+i)^{20}}$.

2. Deliteľnosť celých čísel

V tejto časti pod pojmom číslo budeme rozumieť celé číslo.

Zo strednej aj zo základnej školy poznáte delenie so zvyškom. Napríklad $70 : 11 = 6$, zv. 4, t.j. $70 = 11 \cdot 6 + 4$. Na základe takéhoto delenia môžeme riešiť napríklad nasledovnú úlohu. Aký deň a koľko hodín bude o 194 hodín, ak je dnes štvrtok 8 hodín ráno? Číslo 194 zapíšeme v tvare $194 = 24 \cdot 8 + 2$. Znamená to, že o 194 hodín bude piatok 10 hodín dopoludnia, čo je hľadané riešenie našej úlohy. Pri riešení sme využili nasledovné tvrdenie.

VETA 1 (O DELENÍ SO ZVYŠKOM). *Ku každým dvom celým číslam a, b, $b > 0$, existuje jediná dvojica celých čísel q, r, pre ktoré platí:*

$$a = b \cdot q + r, \qquad 0 \leq r < b. \tag{1}$$

DÔKAZ. 1. Najskôr dokážeme existenciu takej dvojice. Pretože $b > 0$, tak $b \geq 1$, z čoho dostávame, že $-|a| \cdot b \leq -|a| \leq a$. To znamená, že existuje nejaký celočíselný násobok čísla b, ktorý je menší alebo rovný ako číslo a. Preto množina všetkých čísel (rozdielov) tvaru $a - bx$ obsahuje aspoň jedno celé nezáporné (t.j. prirodzené) číslo. Na základe princípu dobrého usporiadania existuje medzi číslami tvaru $a - bx$ najmenšie prirodzené číslo. Označme ho r (nech je to napr. pre $x = q$). Máme teda $r = a - bq \geq 0$. Ďalej ukážeme, že $r < b$. Ak by bolo $r \geq b$, tak číslo

$$r - b = a - bq - b = a - b(q + 1) \geq 0$$

a

$$a - b(q + 1) < a - bq$$

čo nie je možné, lebo $a - bq$ je najmenšie nezáporné z čísel tvaru $a - bx$. Preto $r < b$.

2. Dokážeme jednoznačnosť. Predpokladajme, že okrem dvojice čísel q, r, pre ktoré platí (1) a r je najmenšie z čísel tvaru $a - bx$, existuje aj dvojica čísel q', r', pre ktoré platí

$$a = b \cdot q' + r', \qquad 0 \leq r' < b.$$

Pretože číslo r' je tiež číslom tvaru $a - bx$ je $r \leq r'$. Potom $r' - r = b \cdot (q - q')$ a $0 \leq r' - r < b$. Odtiaľ dostávame $0 \leq b \cdot (q - q') < b$, čo je možné len pre $q - q' = 0$, t.j. pre $q' = q$ (podrobne to overte). Potom aj $r' - r = 0$, t.j. $r' = r$. □

POZNÁMKA. Ak a, b sú celé čísla, $b < 0$, tak podľa predchádzajúcej vety existuje jediná dvojica q, r, že $a = |b|q + r$, $0 \leq r < |b|$. Potom $a = b(-q) + r$, $0 \leq r < |b|$.

PRÍKLAD 1. a) Ak $a = 29$, $b = 8$, tak $29 = 8 \cdot 3 + 5$, teda $q = 3$, $r = 5$.
b) Ak $a = -29$, $b = -8$, tak $-29 = (-8) \cdot 4 + 3$, teda $q = 4$, $r = 3$.
c) Ak $a = -29$, $b = 8$, tak $-29 = 8 \cdot (-4) + 3$, teda $q = -4$, $r = 3$.
d) Ak $a = 29$, $b = -8$, tak $29 = (-8) \cdot (-3) + 5$, teda $q = -3$, $r = 5$.

Budeme hovoriť, že *číslo $a \neq 0$ delí číslo b* keď existuje také číslo q, že $b = a \cdot q$.

Skutočnosť, že číslo a delí číslo b budeme zapisovať $a \mid b$ a hovoriť tiež, že číslo b je deliteľné číslom a alebo číslo b je násobkom čísla a. Symbol $a \nmid b$ bude znamenať, že a nedelí b.

V nasledujúcej vete zhrnieme niektoré základné vlastnosti deliteľnosti.

VETA 2. *Pre každé $a, b, c \in Z$ platí:*

a) $1 \mid a$; *ak* $a \neq 0$, *tak* $a \mid a$, $a \mid 0$,
b) *ak* $a \mid b$, $b \neq 0$ *tak* $|a| \leq |b|$,
c) *ak* $a \mid b$, *tak* $a \mid -b$, $-a \mid b$, $-a \mid -b$,
d) *ak* $a \mid b$, $b \mid c$, *tak* $a \mid c$,
e) *ak* $a \mid b$, $c \neq 0$, *tak* $a \cdot c \mid b \cdot c$,
f) *ak* $a \mid b$, $a \mid c$, *tak* $a \mid b \cdot x + c \cdot y$ *pre ľubovoľné* $x, y \in Z$.

Na ukážku urobíme dôkaz častí b) a d).

DÔKAZ. b) Ak $a \mid b$, $b \neq 0$, tak existuje $q \in Z$, že $b = a \cdot q$. Potom $|b| = |a| \cdot |q|$. Pretože $b \neq 0$, tak $1 \leq |q|$, z čoho $|a| \leq |a| \cdot |q| = |b|$.

d) Ak $a \mid b$, $b \mid c$, tak existujú $q_1, q_2 \in Z$, že $b = a \cdot q_1$, $c = b \cdot q_2$, z čoho $c = a \cdot q_1 \cdot q_2$, kde $q_1 \cdot q_2 \in Z$, čo znamená, že $a \mid c$. □

Číslo d sa nazýva *spoločným deliteľom* čísel a, b, ak $d \mid a$, $d \mid b$. Z vety 2 b) vyplýva, že množina všetkých spoločných deliteľov čísel a, b, z ktorých aspoň jedno je nenulové je konečná. Najväčší prvok tejto množiny nazveme *najväčším spoločným deliteľom* čísel a, b a budeme ho označovať $\mathrm{D}(a, b)$.

Analogicky môžeme zaviesť aj najväčšieho spoločného deliteľa troch a viac čísel.

Z vety 2 b), c) vyplývajú nasledovné tvrdenia.

LEMA 1. *Ak* $a \mid b$, *tak* $\mathrm{D}(a, b) = |a|$.

LEMA 2. *Pre všetky* $a, b \in Z$ *také, že* $a \neq 0$ *alebo* $b \neq 0$ *je* $\mathrm{D}(a, b) = \mathrm{D}(|a|, |b|)$.

Z lemy 2 vyplýva, že pri určovaní najväčšieho spoločného deliteľa sa môžeme obmedziť na prirodzené čísla a tak to budeme väčšinou aj robiť.

LEMA 3. *Ak* $a = b \cdot q + r$, *tak* $\mathrm{D}(a, b) = \mathrm{D}(b, r)$.

DÔKAZ. Ak $d \mid a$, $d \mid b$, tak podľa vety 2 f) $d \mid r$. Ak $d \mid b$, $d \mid r$, tak (opäť podľa vety 2 f)) $d \mid a$. To znamená, že množina všetkých spoločných deliteľov čísel a, b sa rovná množine všetkých spoločných deliteľov čísel b, r, z čoho už vyplýva, že $\mathrm{D}(a, b) = \mathrm{D}(b, r)$. □

Na výpočet najväčšieho spoločného deliteľa dvoch čísel existuje metóda, ktorá sa nazýva *Euklidov algoritmus*.

Nech a, $b \neq 0$ sú prirodzené čísla. Potom, podľa vety 1, existujú prirodzené čísla q_1, r_1, že

$$a = b \cdot q_1 + r_1, \qquad 0 \leq r_1 < b.$$

Ak $r_1 \neq 0$, k číslam b, r_1 existujú prirodzené čísla q_2, r_2, že

$$b = r_1 \cdot q_2 + r_2, \qquad 0 \leq r_2 < r_1.$$

Podobne, ak $r_2 \neq 0$ aj k číslam r_1, r_2 existujú čísla q_3, r_3, že

$$r_1 = r_2 \cdot q_3 + r_3, \qquad 0 \leq r_3 < r_2.$$

Takto môžeme postupovať ďalej. Pretože čísla $b, r_1, r_2, r_3, \ldots$ tvoria klesajúcu postupnosť prirodzených čísel, bude po konečnom počte krokov niektorý zvyšok r_n

nulový. Dostaneme tak sústavu

$$\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 \leq r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 \leq r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 \leq r_3 < r_2,\\
&\dots & \dots\\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2},\\
r_{n-2} &= r_{n-1} \cdot q_n + 0.
\end{aligned}$$

Z lemy 1 a lemy 3 dostávame, že

$$\mathrm{D}(a,b) = \mathrm{D}(b,r_1) = \mathrm{D}(r_1,r_2) = \cdots = \mathrm{D}(r_{n-2},r_{n-1}) = \mathrm{D}(r_{n-1},0) = r_{n-1}.$$

Opísaný postup hľadania najväčšieho spoločného deliteľa sa nazýva Euklidov algoritmus. Najväčší spoločný deliteľ čísel a, b je teda posledný nenulový zvyšok v Euklidovom algoritme.

Veta 3. *Ak najväčší spoločný deliteľ čísel $a, b \in N$ je číslo $\mathrm{D}(a,b)$, tak existujú také celé čísla x, y, že $\mathrm{D}(a,b) = x \cdot a + y \cdot b$.*

Dôkaz. Ak $b = 0$, tak $\mathrm{D}(a,b) = a = 1 \cdot a + 0 \cdot b$. V prípade, keď $b \neq 0$ urobíme dôkaz matematickou indukciou vzhľadom na počet krokov potrebných na výpočet najväčšieho spoločného deliteľa čísel a, b.

1. Ak je na výpočet potrebný jeden krok, t. j. ak $a = bq$, tak $\mathrm{D}(a,b) = b = 0 \cdot a + 1 \cdot b$.

2. Predpokladajme, že tvrdenie platí, ak najväčší spoločný deliteľ môžeme vyjadriť v menej ako k krokoch, $k > 1$. Nech najväčší spoločný deliteľ čísel a, b môžeme vypočítať v k krokoch. K číslam a, b existujú čísla q, r, že

(a) $$a = b \cdot q + r, \qquad 0 < r < b.$$

$\mathrm{D}(b,r)$ môžeme vypočítať použitím Euklidovho algoritmu v $k-1$ krokoch, preto podľa indukčného predpokladu existujú také čísla u, v, že

(b) $$\mathrm{D}(b,r) = u \cdot b + v \cdot r.$$

Z (a) a (b) potom dostávame

$$\begin{aligned}
\mathrm{D}(a,b) = \mathrm{D}(b,r) =& u \cdot b + v \cdot r = u \cdot b + v \cdot (a - b \cdot q) =\\
=& v \cdot a + (u - q \cdot v) \cdot b = x \cdot a + y \cdot b,
\end{aligned}$$

kde $x = v$, $y = u - qv \in Z$. □

Ak $\mathrm{D}(a,b) = 1$, tak hovoríme, že čísla a, b sú *nesúdeliteľné*.

Príklad 2. Najväčší spoločný deliteľ čísel 754 a 221 vyjadrite v tvare $754x + 221y$, $x, y \in Z$.

Riešenie. Najprv pomocou Euklidovho algoritmu vypočítame $\mathrm{D}(754, 221)$.

$$\begin{aligned}
754 &= 3 \cdot 221 + 91,\\
221 &= 2 \cdot 91 + 39,\\
91 &= 2 \cdot 39 + 13,\\
39 &= 3 \cdot 13,
\end{aligned}$$

teda $\mathrm{D}(754, 221) = 13$. Z predposlednej rovnosti vyjadríme číslo 13 a postupne dosadzujeme z druhej rovnosti za číslo 39 a z prvej rovnosti za číslo 91. Dostávame, $13 = 91 - 2 \cdot 39 = 91 - 2 \cdot (221 - 2 \cdot 91) = 5 \cdot 91 - 2 \cdot 221 = 5 \cdot (754 - 3 \cdot 221) - 2 \cdot 221 = 5 \cdot 754 + (-17) \cdot 221$. □

S využitím vety 3 môžeme odvodiť nasledovné dve tvrdenia.

VETA 4. *Ak* $a \mid b \cdot c$ a $\mathrm{D}(a, b) = 1$, *tak* $a \mid c$.

DÔKAZ. Podľa vety 3 existujú celé čísla x, y, že $1 = ax + by$. Potom $c = axc + bcy$. Pretože podľa predpokladu $a \mid bc$, je pravá strana poslednej rovnosti deliteľná číslom a a teda aj $a \mid c$. □

VETA 5. *Ak* $a \mid c$, $b \mid c$ a $\mathrm{D}(a, b) = 1$, *tak* $ab \mid c$.

DÔKAZ. Ak $a \mid c$, $b \mid c$, tak $c = ax$, $c = by$, teda $ax = by$, čo znamená, že $a \mid by$. Pretože $\mathrm{D}(a, b) = 1$, tak podľa predchádzajúcej vety $a \mid y$, teda $y = az$. Potom $c = by = baz$, čo znamená, že $ab \mid c$. □

PRÍKLAD 3. Dokážte, že pre každé celé číslo n je $n^3 + 11n$ násobkom čísla 6.

RIEŠENIE. Výraz $n^3 + 11n$ upravíme takto:

$$n^3 + 11n = n^3 - n + 12n = (n - 1)n(n + 1) + 12n.$$

Súčin $(n - 1)n(n + 1)$ je deliteľný dvoma aj troma lebo z dvoch po sebe idúcich (celých) čísel je jedno párne a z troch po sebe idúcich čísel je jedno deliteľné tromi (podrobne to preverte a zapíšte). Potom podľa vety 5 číslo $2 \cdot 3 = 6$ delí $(n - 1)n(n + 1)$ a pretože $6 \mid 12n$, tak (podľa vety 2 f)) $6 \mid (n^3 + 11n)$. □

VETA 6. *Nech* $a, b \in Z$, $a \neq 0$ *alebo* $b \neq 0$. *Číslo* $d > 0$ *je najväčším spoločným deliteľom čísel* a, b *vtedy a len vtedy, ak má nasledujúce dve vlastnosti*

a) $d \mid a$, $d \mid b$,

b) *ak* $c \mid a$, $c \mid b$, *tak* $c \mid d$.

DÔKAZ. 1. Nech d je najväčší spoločný deliteľ čísel a, b. Vlastnosť a) je splnená a naviac $d = ax_0 + by_0$ $(x_0, y_0 \in Z)$. Ak $c \mid a$, $c \mid b$, tak podľa vety 2 f) $c \mid d$ a teda aj vlastnosť b) je splnená.

2. Nech číslo d má vlastnosti a), b). Ak c je spoločný deliteľ čísel a, b, tak podľa vety 2 b) dostávame, že $c \leq |c| \leq d$, čo znamená, že d je najväčší spoločný deliteľ čísel a, b. □

Číslo m sa volá *spoločným násobkom* čísel $a \neq 0$, $b \neq 0$, ak $a \mid m$ aj $b \mid m$. Najmenší prvok z množiny kladných spoločných násobkov čísel a, b nazveme *najmenším spoločným násobkom* čísel a, b a budeme ho označovať $\mathrm{n}(a, b)$.

Analogicky môžeme zaviesť najmenší spoločný násobok troch a viac čísel.

POZNÁMKA. V tomto texte sme definovali $a \mid b$ len pre $a \neq 0$ a najväčší spoločný deliteľ a najmenší spoločný násobok sme definovali jednoznačne. Tento prístup je obvyklý v teórii čísel (kráľovskej disciplíne matematiky s veľkým počtom stáročia otvorených problémov). V modernej algebre sa skúma deliteľnosť aj u iných objektov ako celé čísla a tam sa stretnete s modifikovanými definíciami, podľa ktorých napríklad $0 \mid 0$ alebo $\mathrm{n}(4, 6)$ môže byť aj -12.

VETA 7. *Nech* $a, b \in Z$. *Číslo* $n > 0$ *je najmenším spoločným násobkom čísel* a, b *vtedy a len vtedy, ak má nasledovné dve vlastnosti*

a) $a \mid n$, $b \mid n$,

b) $ak \quad a \mid m,\ b \mid m \quad tak \quad n \mid m.$

Dôkaz. 1. Nech n je najmenší spoločný násobok čísel a, b. Zrejme vlastnosť a) je splnená. Nech m je spoločný násobok čísel a, b. Pre m, n existuje jediná dvojica celých čísel q, r taká, že

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

Z toho vyplýva, že $a \mid r$ aj $b \mid r$. Pretože n je najmenší spoločný násobok čísel a, b je $r = 0$ a teda $n \mid m$.

2. Nech pre n platí a), b). Ak m je kladný spoločný násobok čísel a, b tak podľa b) $n \mid m$, čo znamená, že $n \leq m$ a teda n je najmenší spoločný násobok. □

Nasledujúce tvrdenie opisuje súvis medzi najväčším spoločným deliteľom a najmenším spoločným násobkom.

Veta 8. *Pre ľubovoľné dve kladné celé čísla a, b platí*

$$\frac{a \cdot b}{\mathrm{D}(a,b)} = \mathrm{n}(a,b)\,.$$

Dôkaz. Označme $d = \mathrm{D}(a,b)$. Potom $a = d \cdot a'$, $b = d \cdot b'$, pričom zrejme $\mathrm{D}(a',b') = 1$ (lebo v opačnom prípade by číslo d nebolo najväčším spoločným deliteľom). Pretože

$$\frac{a \cdot b}{d} = \frac{d \cdot a' \cdot b}{d} = a' \cdot b, \qquad \frac{a \cdot b}{d} = \frac{a \cdot d \cdot b'}{d} = a \cdot b'\,,$$

je $\frac{a \cdot b}{d}$ celé číslo a je spoločným násobkom čísel a, b.

Nech aj m je spoločný násobok čísel a, b, t.j. $m = a \cdot u$, $m = b \cdot v$. Potom $a \cdot u = b \cdot v$, z čoho po dosadení a krátení dostávame $a' \cdot u = b' \cdot v$. Pretože $\mathrm{D}(a',b') = 1$, tak $a' \mid v$, t.j. $v = a' \cdot r$ a $m = b \cdot a' \cdot r = \frac{a \cdot b}{d} \cdot r$. Číslo $\frac{a \cdot b}{d}$ teda delí m, čo podľa vety 7 znamená, že $\frac{a \cdot b}{d}$ je najmenší spoločný násobok čísel a, b. □

Každé prirodzené číslo $n \geq 1$ je deliteľné číslami 1 a n. Nazývame ich *triviálnymi deliteľmi* čísla n.

Prirodzené číslo $n > 1$, ktoré je deliteľné len číslami 1 a n sa nazýva *prvočíslo*. Prirodzené číslo $n > 1$, ktoré nie je prvočíslom sa nazýva *zložené číslo*.

Veta 9. *Ak je prirodzené číslo a zložené, tak jeho najmenší kladný netriviálny deliteľ je prvočíslo p, pre ktoré platí $p^2 \leq a$.*

Dôkaz. Ak p je najmenší kladný netriviálny deliteľ čísla a, tak $a = px$, kde $p \leq x$. Ak by p nebolo prvočíslo, tak $p = p_1 \cdot p_2$, kde $1 < p_1 < p$, $1 < p_2 < p$. Potom $a = p_1 \cdot p_2 \cdot x$ a p by nebol najmenší kladný netriviálny deliteľ čísla a. Preto je p prvočíslo. Pretože $p \leq x$, tak $p^2 \leq px = a$. □

Veta 10. *Existuje nekonečne mnoho prvočísel.*

Dôkaz. (Sporom.) Predpokladajme, že všetkých prvočísel je konečne mnoho, t.j., že existuje $k \in N^+$, že $p_1, p_2, \ldots, p_k$ sú práve všetky prvočísla. Potom číslo $p = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ je prirodzené číslo a $p > p_i$ pre každé $i \in \{1, 2, \ldots, k\}$. Ak je p zložené číslo, tak je deliteľné niektorým z uvedených prvočísel, teda existuje $j \in \{1, 2, \ldots, k\}$, že $p_j \mid p$. Potom podľa vety 2 platí, že p_j delí číslo $p - p_1 \cdot p_2 \cdot \ldots \cdot p_k = 1$, čo je spor. □

Aj keď prvočísel je nekonečne veľa, existujú ľubovoľne dlhé úseky po sebe idúcich čísel, z ktorých ani jedno nie je prvočíslo.

VETA 11. *Ku každému prirodzenému číslu n existuje postupnosť n po sebe idúcich zložených prirodzených čísel.*

DÔKAZ. Skúmajme n za sebou idúcich čísel

$$(n+1)!+2, \quad (n+1)!+3, \quad \ldots, \quad (n+1)!+n+1.$$

Všetky tieto čísla sú zložené, lebo číslo $(n+1)!+i$ je deliteľné číslom i, $i \in \{2,3,\ldots,n+1\}$. □

VETA 12. *Nech $a_1, a_2, \ldots, a_n$ sú prirodzené čísla a nech p je prvočíslo. Ak $p \mid a_1 a_2 \ldots a_n$, tak pre niektorý činiteľ a_i platí $p \mid a_i$.*

DÔKAZ. (Matematickou indukciou.) 1. Nech $p \mid a_1 a_2$. Ak $p \nmid a_1$, tak $\mathrm{D}(p, a_1) = 1$ a podľa vety 4 platí $p \mid a_2$.

2. Predpokladajme, že tvrdenie platí pre $n-1$ činiteľov. Nech $p \mid a_1 a_2 \ldots a_n$. Označme $a = a_1 a_2 \ldots a_{n-1}$. Pretože $p \mid a \cdot a_n$ z prvej časti dôkazu vyplýva, že $p \mid a$ alebo $p \mid a_n$. Číslo a je súčin $n-1$ činiteľov, s využitím indukčného predpokladu teda dostávame, že pre niektorý činiteľ platí $p \mid a_i$. □

VETA 13. *Každé zložené prirodzené číslo je súčinom konečného počtu prvočísel.*

DÔKAZ. (Matematickou indukciou.) 1. Pre najmenšie zložené prirodzené číslo tvrdenie platí, lebo $4 = 2 \cdot 2$.

2. Nech n je zložené číslo a každé zložené číslo menšie ako n nech má uvedenú vlastnosť. Podľa vety 9 je $n = p \cdot n_1$, kde p je prvočíslo. Pretože $n_1 < n$, na základe indukčného predpokladu dostávame, že ak n_1 nie je prvočíslo, tak n_1 je súčinom konečného počtu prvočísel. Z toho vyplýva, že aj n je súčinom konečného počtu prvočísel. □

DÔSLEDOK. *Každé prirodzené číslo n môžeme zapísať v tvare*

$$p_1^{z_1} \cdot p_2^{z_2} \cdot \ldots \cdot p_n^{z_n}, \tag{1}$$

kde $p_1 < p_2 < \cdots < p_n$ sú prvočísla a $z_1, z_2, \ldots, z_n$ sú kladné celé čísla.

Súčin (1) voláme *kanonický rozklad*. Ak pripustíme aj nulové exponenty, tak hovoríme o *zovšeobecnenom rozklade* alebo krátko o *rozklade*.

VETA 14. *(*Základná veta aritmetiky*.) Každé prirodzené číslo n má jediný kanonický rozklad.*

DÔKAZ. Vzhľadom na predchádzajúci dôsledok už stačí dokázať len jednoznačnosť.

Predpokladajme, že n má dva rozklady

$$n = p_1^{r_1} \ldots p_k^{r_k} \quad \text{aj} \quad n = q_1^{s_1} \ldots q_l^{s_l}.$$

Potom

$$p_1^{r_1} \ldots p_k^{r_k} = q_1^{s_1} \ldots q_l^{s_l}. \tag{2}$$

Z toho vyplýva, že $p_1 \mid q_1^{s_1} \ldots q_l^{s_l}$ a teda podľa vety 12 existuje $j \in \{1, \ldots l\}$, že $p_1 \mid q_j$ a pretože p_1, q_j sú prvočísla, tak $p_1 = q_j$. Podobne, každé z čísel $p_2 \ldots p_k$

je rovné niektorému z čísel $q_1 \dots q_l$, čiže $k \leq l$. Analogicky $l \leq k$, teda $k = l$. Pretože $p_1 < \dots < p_k$, $q_1 < \dots < q_l$, tak $p_1 = q_1, \dots, p_k = q_k$. Ostáva dokázať, že $r_1 = s_1, \dots, r_k = s_k$. Nech pre nejaké $i \in \{1, 2, \dots, k\}$ je $r_i > s_i$, t.j. $r_i - s_i > 0$. Vydeľme obidve strany rovnosti (2) číslom $p_i^{s_i}$. Dostávame

$$p_1^{r_1} \dots p_i^{r_i - s_i} \dots p_k^{r_k} = p_1^{s_1} \dots p_{i-1}^{s_{i-1}} \cdot p_{i+1}^{s_{i+1}} \dots p_k^{s_k}. \tag{3}$$

Ľavá strana rovnosti (3) je deliteľná číslom p_i, ale pravá nie, čo je spor. Platí teda $r_1 = s_1, \dots, r_k = s_k$. □

VETA 15. *Nech $a = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_n^{r_n}$ je kanonický rozklad čísla $a \in N^+$. Potom $b \in N^+$ delí a práve vtedy, keď má zovšeobecnený rozklad tvaru*

$$b = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_n^{s_n}, \tag{4}$$

kde $0 \leq s_i \leq r_i$ pre $i = 1, 2, \dots, n$.

DÔKAZ. 1. Predpokladajme, že $b \mid a$, t.j., že $a = b \cdot c$. Potom kanonický rozklad čísla a dostaneme úpravou súčinu kanonických rozkladov čísel b, c. Z jednoznač nosti rozkladu čísla a vyplýva, že číslo b môže mať len rozklad (4), pričom $s_i \leq r_i$ pre $i = 1, \dots, n$.

2. Nech b má rozklad (4). Potom

$$\begin{aligned} a =& p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_n^{r_n} = p_1^{s_1 + r_1 - s_1} \cdot p_2^{s_2 + r_2 - s_2} \cdot \dots \cdot p_n^{s_n + r_n - s_n} = \\ =& p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_n^{s_n} \cdot p_1^{r_1 - s_1} \cdot p_2^{r_2 - s_2} \cdot \dots \cdot p_n^{r_n - s_n} = b \cdot q \end{aligned}$$

kde $q = p_1^{r_1 - s_1} \cdot p_2^{r_2 - s_2} \cdot \dots \cdot p_n^{r_n - s_n} \in N^+$ a teda $b \mid a$. □

Vzhľadom na to, že sa pri rozklade pripúšťajú aj nulové exponenty môžeme predpokladať (bez ujmy na všeobecnosti), že v rozkladoch dvoch rôznych prirodzených čísel sú rovnaké prvočísla.

VETA 16. *Ak a, b sú nenulové prirodzené čísla a*

$$a = p_1^{r_1} \dots p_n^{r_n}, \qquad b = p_1^{s_1} \dots p_n^{s_n}$$

sú ich zovšeobecnené rozklady, tak $\mathrm{D}(a, b) = p_1^{t_1} \dots p_n^{t_n}$, $\mathrm{n}(a, b) = p_1^{u_1} \dots p_n^{u_n}$, *kde*

$$t_i = \min(r_i, s_i), \quad u_i = \max(r_i, s_i), \quad i = 1, 2, \dots, n.$$

DÔKAZ. Označme $d = p_1^{t_1} \dots p_n^{t_n}$. Podľa vety 15 platí $d \mid a$, $d \mid b$. Nech $g \mid a$, $g \mid b$. Potom $g = p_1^{k_1} \dots p_n^{k_n}$, kde $k_i \leq r_i$, $k_i \leq s_i$, $i = 1, 2 \dots n$, z čoho vyplýva, že $k_i \leq t_i$, $i = 1, 2, \dots, n$, čo znamená, že $g \mid d$. Podľa vety 6 je teda $d = \mathrm{D}(a, b)$.

Analogicky sa dokáže aj časť tvrdenia týkajúca sa najmenšieho spoločného násobku. □

S využitím poznatkov o rozkladoch je dôkaz vety 8 jednoduchý, podrobne si ho zapíšte.

POZNÁMKA. Uvedený spôsob určenia najväčšieho spoločného deliteľa a najmenšieho spoločného násobku pomocou kanonických rozkladov je možné prirodzeným spôsobom zovšeobecniť pre ľubovoľný konečný počet čísel.

Cvičenia

1. Dokážte, že druhú mocninu každého prirodzeného čísla možno napísať buď v tvare $4k$ alebo v tvare $4k+1$, $k \in N$.

2. Dokážte, že súčet štvorcov štyroch po sebe idúcich čísel nemôže byť štvorcom celého čísla.

3. Dokážte, že z n po sebe idúcich celých čísel je práve jedno deliteľné číslom n.

4. Dokážte, že pre každé $n \in N$ je $n^3 + 17n$ násobkom čísla 6.

5. Dokážte, že súčet tretích mocnín troch po sebe idúcich čísel je násobkom čísla 9.

6. Dokážte, že ak $a, b \in Z$ nie sú násobkom troch, tak $a^2 + b^2 + 1$ je násobkom troch.

7. Dokážte, že pre každé $n \in N$ je $3^n + 5 \cdot 2^{8n+5}$ násobkom čísla 23.

8. Zistite, či pre nejaké $n \in N$ sa dá krátiť zlomok $\frac{14n+3}{21n+4}$.

9. Nájdite také dve čísla, že ich súčet je 60 a súčet ich najväčšieho deliteľa a najmenšieho násobku je 84.

10. Je daný trojčlen $2x^2 - x - 36$. Nájdite všetky prirodzené čísla, pre ktoré je hodnota daného trojčlena rovná druhej mocnine prvočísla.

11. Nájdite najväčší spoločný deliteľ a najmenší spoločný násobok čísel
a) 32, 40, 54; b)840, 900, 1100.

12. Ktorým najmenším prirodzeným číslom je treba násobiť číslo 9450, aby sme dostali druhú mocninu prirodzeného čísla?

13. Nájdite najväčšieho spoločného deliteľa čísel $f(n) = 5^{3n+5} - 2^{2n}$, $n \in N$.

14. Nájdite najmenšie prirodzené číslo n s touto vlastnosťou. Číslo $\frac{n}{2}$ je druhá mocnina, $\frac{n}{3}$ tretia mocnina a $\frac{n}{5}$ piata mocnina prirodzeného čísla.

15. Dokážte, že existuje práve jedno prirodzené číslo n, že $2^8 + 2^{11} + 2^n$ je druhá mocnina prirodzeného čísla.

16. Dokážte, že pre ľubovoľné čísla a, b, c platí

$$\mathrm{D}(\mathrm{D}(a,b),c) = \mathrm{D}(a,b,c) = \mathrm{D}(a,\mathrm{D}(b,c)), \quad \mathrm{n}(\mathrm{n}(a,b),c) = \mathrm{n}(a,b,c) = \mathrm{n}(a,\mathrm{n}(b,c)).$$

17. Pomocou vety 16 ukážte, že

$$\mathrm{D}(a,\mathrm{n}(b,c)) = \mathrm{n}(\mathrm{D}(a,b),\mathrm{D}(a,c)), \qquad \mathrm{n}(a,\mathrm{D}(b,c)) = \mathrm{D}(\mathrm{n}(a,b),\mathrm{n}(a,c)).$$

3. Základné pojmy teórie množín

Skúmanie nekonečných súborov bolo pre nemeckého matematika G. Cantora impulzom pre zavedenie pojmu množina. S úvahami týkajúcimi sa množín sa možno stretnúť už aj u jeho predchodcov, ale až Cantor ukázal aký silný aparát z hľadiska skúmania nekonečna, ale aj z hľadiska rozvoja všetkých matematických disciplín, možno získať zavedením pojmu množina. Za zrod teórie množín možno preto pokladať rok 1872, kedy Cantor uverejnil prvú prácu o množinách. V súčasnosti možno teóriu množín a matematickú logiku pokladať za východiská (základy) matematiky. So základnými pojmami, ktoré zavedieme v tomto článku sa budeme v matematike stretávať počas celého štúdia.

Primitívnymi pojmami teórie množín (ktoré nedefinujeme) sú: *množina, prvok množiny, je prvok množiny* (príslušnosť prvku množine). Rozsah a zmysel týchto pojmov sa v teórii množín vymedzuje pomocou základných postulátov-axióm, ktoré o nich predpokladáme. Všetky ostatné pojmy teórie množín a dokonca aj všetky ostatné matematické pojmy možno pomocou nich postupne definovať. S axiómami teórie množín sa však zoznámite až neskôr. Zatiaľ sa uspokojíme s tým, že pojmy množina, prvok množiny, príslušnosť prvku množine (vzťah byť prvkom množiny) dobre poznáte z predchádzajúceho štúdia. Tiež predpokladáme, že ste si už osvojili aj elementárne poznatky o množinách. Napriek tomu si niektoré z nich pripomenieme.

Množina je určená (daná) vtedy, keď o každom objekte možno rozhodnúť (aspoň v princípe), či je jej prvkom, alebo nie je jej prvkom. Napríklad, nevieme zatiaľ rozhodnúť, či číslo $3^{1000!}+2$ je alebo nie je prvočíslom, ale je to len dôsledok našich súčasných ohraničených možností. Napriek tomu úvahy o množine všetkých prvočísel sú v matematike bežné.

Ak x je prvkom množiny A píšeme $x \in A$, v opačnom prípade píšeme $x \notin A$. Ak prvkami množiny A sú čísla 1, 2, 3 a iné prvky množina A nemá, píšeme $A = \{1,2,3\}$ alebo $A = \{1,3,2\}$ a pod. V takomto prípade hovoríme, že množina je daná *vymenovaním prvkov*. Prázdnu množinu (t.j. množinu, ktorá nemá žiadny prvok) budeme označovať symbolom $\emptyset$.

Definícia 1. Hovoríme, že množina A je podmnožinou množiny B a píšeme $A \subseteq B$, ak každý prvok množiny A je prvkom množiny B.

Keď chceme zdôrazniť, že $A \subseteq B$ a $A \neq B$, tak píšeme $A \subset B$ a hovoríme, že A je vlastnou podmnožinou množiny B.

Poznámka. V niektorej literatúre (včítane stredoškolských učebníc) sa však namiesto $A \subseteq B$ píše $A \subset B$ a namiesto $A \subset B$ sa potom píše $A \subsetneq B$.

Rovnosť množín je charakterizovaná nasledovne:

$$A = B \quad \text{práve vtedy, keď} \quad A \subseteq B \quad \text{a zároveň} \quad B \subseteq A.$$

Teda množina je, na rozdiel napríklad od spolku (ľudí), jednoznačne daná svojimi prvkami (rôzne spolky môžu mať tých istých členov, ale rôzne množiny nemôžu mať presne tie isté prvky).

Veľmi užitočným matematickým pojmom je pojem *usporiadaná dvojica.* Pre usporiadané dvojice je charakteristickou nasledujúca vlastnosť:

(1) $\quad [x_1,x_2] = [y_1,y_2]$ práve vtedy, keď $x_1 = y_1$ a tiež $x_2 = y_2$.

Naproti tomu $\{x_1,x_2\} = \{y_1,y_2\}$ ak $x_1 = y_1$ alebo $x_1 = y_2$ a zároveň $x_2 = y_1$ alebo $x_2 = y_2$.

Pomocou pojmu množina môžeme usporiadanú dvojicu definovať napríklad takto.

DEFINÍCIA 2. Usporiadanou dvojicou $[x_1, x_2]$ s prvou zložkou x_1 a s druhou zložkou x_2 nazývame množinu $\{\{x_1, x_2\}, \{x_2\}\}$.

Overte, že pre uvedeným spôsobom zavedené usporiadané dvojice naozaj platí (1).

Pod usporiadanou trojicou $[x_1, x_2, x_3]$ s prvou zložkou x_1, s druhou x_2 a s treťou x_3 budeme rozumieť usporiadanú dvojicu $[[x_1, x_2], x_3]$. Analogicky môžeme zaviesť usporiadanú štvoricu, päticu, atď.

DEFINÍCIA 3. Nech n je kladné prirodzené číslo. Usporiadanú n-ticu $[x_1, x_2, \ldots, x_n]$ definujeme indukciou takto:

1. $[x_1] = x_1$.
2. Ak $n > 1$, tak $[x_1, x_2, \ldots, x_n] = [[x_1, x_2, \ldots, x_{n-1}], x_n]$.

PRÍKLAD 1. $[a, b, c, d] = [[a, b, c], d] = [[[a, b], c], d]$. □

Zrejme platí
$[x_1, \ldots, x_n] = [y_1, \ldots, y_n]$ vtedy a len vtedy, keď $x_1 = y_1, \ldots, x_n = y_n$.

POZNÁMKA. U zápisov typu $[x_1, \ldots, x_n]$ nevylučujeme ani možnosti $n = 1$ a $n = 2$. V prípade $n = 1$ chápeme zápis $[x_1, \ldots, x_n]$ ako $[x_1]$, v prípade $n = 2$ ako $[x_1, x_2]$.

U zápisov množín daných vymenovaním prvkov nie je zvykom používať zápisy typu $\{1, 2, 2, 3\}$, kde sa opakuje zápis čísla 2. Ak by sme však takúto dohodu vždy dodržali, mali by sme komplikáciu napríklad s uvedením množinového modelu usporiadanej dvojice. Preto teória množín uvedený zápis nezakazuje. Pritom zápis $\{1, 2, 2, 3\}$ reprezentuje trojprvkovú a nie štvorprvkovú množinu, jej prvkami sú čísla, nie symboly (číslice) vytlačené na papieri. V ďalšom texte však aj my napríklad u zápisu $\{a, b, c\}$ budeme predpokladať, že $a \neq b \neq c \neq a$.

DEFINÍCIA 4. Nech A, B sú množiny. Pod karteziánskym súčinom $A \times B$ množiny A a množiny B rozumieme množinu všetkých usporiadaných dvojíc, ktorých prvá zložka je prvkom množiny A a druhá je prvkom množiny B.

PRÍKLAD 2. $\{1, 2, 3\} \times \{a, b\} = \{[1, a], [1, b], [2, a], [2, b], [3, a], [3, b]\}$. □

Karteziánsky súčin $A \times A$ často zapisujeme stručne A^2. Napríklad $\{3, 5\}^2 = \{[3, 3], [3, 5], [5, 3], [5, 5]\}$.

Podobne možno definovať karteziánsky súčin $A \times B \times C$ troch množín (ako množinu usporiadaných trojíc), štyroch množín, atď. Upozorňujeme, že v súlade s definíciou 3 platí $A \times B \times C = (A \times B) \times C$, ale $(A \times B) \times C \neq A \times (B \times C)$.

Všimnite si, že $A \times B = B \times A$ vtedy a len vtedy, keď $A = B$ alebo niektorá z množín A, B je prázdna.

V matematike sa často zaoberáme skúmaním vzťahov medzi objektami (číslami, priamkami, geometrickými útvarmi a číslami, atď.) Rozsah pojmu vzťah však nie je vymedzený ani žiadnou definíciou ani skupinou nejakých základných postulátov (axióm). Preto zavedieme pojem *relácia*, ktorý možno definovať pomocou už skôr uvedených pojmov a ktorý pojem vzťahu vhodne reprezentuje (a môže ho nahrádzať).

DEFINÍCIA 5. Binárnou reláciou (stručne reláciou) nazývame každú množinu usporiadaných dvojíc.

Ak R je relácia a $[a,b] \in R$ často píšeme $a\,R\,b$ a hovoríme, že prvok a je v relácii R s prvkom b, alebo, že relácia R priraďuje k prvku a prvok b.

PRÍKLAD 3. Vzťah byť menším na množine čísel $\{1,2,3,4\}$ je reprezentovaný reláciou

$\{[1,2],[1,3],[1,4],[2,3],[2,4],[3,4]\}$

Vzťah byť násobkom je (na tej istej množine) reprezentovaný reláciou

$\{[1,1],[2,1],[3,1],[4,1],[2,2],[4,2],[3,3],[4,4]\}$. □

Počas predchádzajúceho štúdia matematiky ste sa oboznámili napríklad s reláciami, ktoré označujeme symbolmi $<$, $\leq$, $\in$, $\subset$, $\perp$, $\parallel$, $\cong$, $\sim$.

DEFINÍCIA 6. Nech R je binárna relácia. Definičným oborom (prvým oborom) relácie R nazývame množinu $\mathcal{D}(R)$, ktorá je daná takto:

$a \in \mathcal{D}(R)$ vtedy a len vtedy, keď existuje prvok b o ktorom platí $[a,b] \in R$.

Obor hodnôt (druhý obor) relácie R je množina $\mathcal{H}(R)$ daná takto:

$b \in \mathcal{H}(R)$ vtedy a len vtedy, keď existuje prvok a, o ktorom platí $[a,b] \in R$.

PRÍKLAD 4. Ak $R = \{[0,0],[0,1],[1,1],[1,2],[1,3]\}$, tak $\mathcal{D}(R) = \{0,1\}$, $\mathcal{H}(R) = \{0,1,2,3\}$. □

Ak R je relácia a A, B sú množiny, o ktorých platí $\mathcal{D}(R) \subseteq A$, $\mathcal{H}(R) \subseteq B$ hovoríme, že R je *relácia z množiny A do B*. Ak R je relácia z A do A hovoríme, že R je *relácia na množine A*. Napríklad relácia, ktorá bola daná v predchádzajúcom príklade, je reláciou z množiny $\{0,1\}$ do $\{0,1,2,3\}$, ale aj reláciou z $\{0,1,2\}$ do $\{0,1,2,3,4,10,11\}$, aj reláciou na množine N, atď.

PRÍKLAD 5. Nech R je relácia z E do E definovaná takto:

$[x,y] \in R$ vtedy a len vtedy, keď $x^2 - 2xy + y^2 - 2x - y = 20$.

Určte prvý a druhý obor relácie R.

RIEŠENIE. Uvedenú podmienku môžeme zapísať v tvare

(a) $$x^2 - x.(2y+2) + y^2 - y - 20 = 0$$

aj v tvare

(b) $$y^2 - y.(2x+1) + x^2 - 2x - 20 = 0.$$

Ak (a) pokladáme za kvadratickú rovnicu s neznámou x zistíme, že číslo x spĺňajúce (a) existuje práve vtedy, keď diskriminant tejto rovnice je nezáporný, t. j. keď $[-(2y+2)]^2 - 4y^2 + 4y + 80 \geq 0$. Po úprave dostaneme $y \geq -7$. Analogicky z (b) možno dostať, že $x \geq -\frac{27}{4}$.

Z uvedeného vyplýva, že $\mathcal{D}(R) = \langle -\frac{27}{4}, \infty)$, $\mathcal{H}(R) = \langle -7, \infty)$. □

S inými, ako binárnymi vzťahmi (v ktorých nie sú dvojice, ale iné skupiny objektov) sa stretávame v matematike dosť zriedka, preto ternárne, prípadne n-árne ($n \geq 3$) relácie v tomto texte nedefinujeme.

Osobitný význam majú v matematike také binárne relácie, ktoré k ľubovoľnému prvku priraďujú najviac jeden prvok.

DEFINÍCIA 7. Binárnu reláciu f nazývame zobrazenie, ak f priraďuje ku každému prvku z $D(f)$ práve jeden prvok, t. j. ak o relácii f platí

$$[a,b] \in f \quad \& \quad [a,c] \in f \quad \Longrightarrow \quad b = c.$$

Ak A, B sú množiny a f je relácia z A do B, ktorá je zobrazením, hovoríme, že f je *zobrazenie z A do B* a píšeme $f : A \xrightarrow{z} B$. Množinu $\mathcal{D}(f)$ nazývame *definičný obor zobrazenia f* a množinu $\mathcal{H}(f)$ *obor hodnôt zobrazenia f*. Ak $\mathcal{D}(f) = A$ tak hovoríme, že f je *zobrazenie množiny A do množiny B* a píšeme $f : A \to B$. Ak $[a,b] \in f$, obyčajne píšeme $b = f(a)$ alebo $b = af$ alebo $f : a \mapsto b$ a hovoríme, že prvok b je *obraz prvku a* v zobrazení f, resp. že a je *vzor prvku b* v zobrazení f. Z definície vyplýva, že ľubovoľný prvok z $D(f)$ má v zobrazení f len jeden obraz, ale prvok z $H(f)$ môže mať v zobrazení f aj viac vzorov.

PRÍKLAD 6. Nech $\mathcal{S}$ je zvolený systém konečných množín (napríklad $\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$) a nech f je relácia z $\mathcal{S}$ do N, ktorá priraďuje každej množine počet jej prvkov. Relácia f je zrejme zobrazenie. □

PRÍKLAD 7. Nech F je relácia, ktorá ku každému reálnemu číslu priraďuje jeho dekadický zápis. Relácia F nie je zobrazenie, pretože napríklad k číslu 2 sú priradené zápisy $2,0$ aj $1,\bar{9}$. □

Namiesto názvu zobrazenie často používame názov *funkcia*. Vtedy namiesto „b je obraz prvku a v zobrazení f“ hovoríme „b je *hodnota* funkcie f v bode a“.

POZNÁMKA. Na strednej škole ste používali názov funkcia len u zobrazení z množiny E do E.

PRÍKLAD 8. Daná je relácia R z množiny Z do Z takto:

$$[x,y] \in R \quad \text{práve vtedy, keď} \quad 15x^2 - xy - 2y^2 - 5 = 0.$$

Zistite, či relácia R je zobrazenie.

RIEŠENIE. Uvedenú rovnosť môžeme upraviť na tvar $(5x - 2y).(3x + y) = 5$. Pretože hodnoty x, y sú celé čísla dostávame 4 možnosti :

a) $5x - 2y = 1$ a $3x + y = 5$
b) $5x - 2y = -1$ a $3x + y = -5$
c) $5x - 2y = 5$ a $3x + y = 1$
d) $5x - 2y = -5$ a $3x + y = -1$.

Prvé dve sústavy rovníc majú riešenia $x_1 = 1$, $y_1 = 2$ a $x_2 = -1$, $y_2 = -2$, ďalšie dve sústavy nemajú nad oborom celých čísel riešenie. Z uvedeného vyplýva, že $R = \{[1,2], [-1,-2]\}$, teda relácia R je zobrazenie. (Ako sa zmení výsledok keď množinu Z nahradíme v zadaní množinou E ?) □

Fundamentálnym pojmom algebry je pojem *operácia*.

DEFINÍCIA 8. Zobrazenie, ktorého definičný obor je množina usporiadaných dvojíc, sa nazýva binárna operácia (stručne operácia).

Ak f je binárna operácia a ak $f : [a,b] \mapsto c$ píšeme $f(a,b) = c$, alebo $afb = c$. Posledný typ zápisu používame najmä vtedy, keď je binárna operácia označená niektorým zo symbolov $+, \cdot, -, \circ, \cup, \cap, \star$ a pod.

PRÍKLAD 9. Obvyklé sčítanie prirodzených čísel je binárnou operáciou. Zápis $2 + 7 = 9$ znamená, že u tejto operácie je obrazom usporiadanej dvojice $[2,7]$ číslo 9. □

PRÍKLAD 10. Nech $\circ$ je operácia na množine N^+ daná predpisom

(c) $$a \circ b = 2a + b - 1$$

Určte

a) $(3 \circ 4) \circ (1 \circ 2)$

b) $((3 \circ 4) \circ 1) \circ 2$,

c) $3 \circ (4 \circ (1 \circ 2))$.

RIEŠENIE. a) Využitím (c) dostávame

$(3 \circ 4) \circ (1 \circ 2) = (2.3 + 4 - 1) \circ (2.1 + 2 - 1) = 9 \circ 3 = 2.9 + 3 - 1 = 20.$

b) Podobne pomocou (c) postupne dostávame $3 \circ 4 = 2.3 + 4 - 1 = 9$,
$9 \circ 1 = 2.9 + 1 - 1 = 18$, $18 \circ 2 = 2.18 + 2 - 1 = 37$.

c) Analogickým postupom dostaneme výsledok 15 (overte si to). □

Popri binárnych operáciach (s ktorými sa budeme stretávať najčastejšie) sa v matematike vyskytujú aj iné typy operácií (u ktorých vzory sú usporiadané trojice, alebo štvorice a pod.), ale v tomto texte sa takými nebudeme zaoberať. Binárnymi operáciami sa budeme podrobnejšie zaoberať v 12. kapitole.

Cvičenia

1. Vymenovaním prvkov určte nasledujúce množiny.

a) $A = \left\{x \in Q; \sqrt{4x^2 - \sqrt{8x+5}} = 2x + 1\right\}$,

b) $B = \{x \in N; \sqrt[3]{2x+17} - \sqrt[3]{2x-9} = 2\}$,

c) $M = \left\{x \in N; \left(\frac{3}{4}\right)^{x+2} \cdot \sqrt[x]{\frac{4}{3}} = \frac{9}{16}\right\}$,

d) $D = \{x \in Q; x^{3+2.\log x} = 100.x^{2+\log x}\}$,

e) $K = \{x \in Q; x^{\log x} + 10.x^{-\log x} = 11\}$.

2. V priestore sú dané nekolineárne body A, B, C. Pomenujte geometrické útvary, ktoré sú identické s množinami bodov

a) $\{P; |PA| = |PB|\}$, b) $\{P; |PA| = |PB| = 5cm\}$,

c) $\{P; |PA| = |PB| = |PC|\}$, d) $\{P; |PA| = |PB| = |PC| = 5cm\}$,

e) $\{P; |PA| = |PB| > |PC|\}$, f) $\{P; |PA| \geq |PB| \geq |PC|\}$.

3. Zapíšte nasledujúce množiny ako intervaly alebo zjednotenia intervalov.

a) $A = \{x \in E; ||x+1| - |x-1|| < 1\}$,

b) $B = \{x \in E; \frac{2x-1}{x+2} - \frac{x+3}{x-1} > 1\}$,

c) $D = \{x \in E; |-\frac{5}{x+2}| < |\frac{10}{x-1}|\}$.

4. Vymenovaním prvkov zapíšte množiny

a) $[a, b, c]$, b) $[a, b, c, d]$.

5. Dokážte, že

a) $\{\{a, b\}, \{b\}\} = \{\{c, d\}, \{d\}\} \Longleftrightarrow a = c \ \& \ b = d$,

b) $[a, b, c] = [x, y, z] \Longleftrightarrow a = x \ \& \ b = y \ \& \ c = z$.

6. Určte vymenovaním všetky (binárne) relácie na množine $A = \{0, 1\}$.

7. Určte všetky zobrazenia z množiny $\{0, 1\}$ do množiny $\{a, b\}$.

8. Určte definičné obory a obory hodnôt nasledujúcich relácii:

a) $R = \{[x, y] \in E^2; y = \sqrt{x-1}\}$,

b) $S = \{[x, y] \in E^2; x^2 - 2x + y^2 + xy = 20\}$,

c) $T = \{[x, y] \in E^2; y = \frac{2x}{x^2+1}\}$.

9. Rozhodnite, ktoré z nasledujúcich relácii sú zobrazenia.

a) $R = \{[x, y] \in E^2; x^3 = y^3\}$,

b) $S = \{[x, y] \in E^2; x^2 = y^3\}$,

c) $T = \{[x, y] \in E^2; x + 2 = |y|\}$.

10. Nájdite definičný obor a obor hodnôt reálnej funkcie reálnej premennej.

a) $y = \frac{x^2-1}{x^2-3}$, b) $y = \frac{3}{1-x^2}$.

11. Dohodneme sa, že A_x bude označovať obraz čísla x na zvolenej číselnej osi. Na množine E definujeme operácie $\circ$ a $*$ takto:

$x \circ y = z$, ak A_z je stred úsečky A_xA_y,

$x \circ x = x$,

$x * y = z$, ak A_z je obraz bodu A_x v súmernosti so stredom A_y.

Vypočítajte

a) $(11 \circ 5) \circ (-2 \circ 10)$, b) $(-2) \circ (10 \circ (5 \circ 11))$,

c) $(11 * 5) * (-2 * 10)$, d) $(-2) * (10 * (5 * 11))$.

4. Výrokový počet

Primitívnym pojmom, ktorý vo výrokovom počte nedefinujeme, je pojem *výrok*. Pod výrokom rozumieme každý oznam, u ktorého má zmysel hovoriť, či je pravdivý, alebo nepravdivý, pričom z oboch možností nastáva práve jedna. Vo výrokovom počte sa však nebudeme zaoberať otázkou, či je určitý výrok pravdivý, resp. nepravdivý. Podotýkame len, že v matematike sa (prirodzene) stretávame aj s takými výrokmi, u ktorých v súčasnosti ani nevieme určiť, či sú pravdivé alebo nie. Príkladom je výrok: každé párne prirodzené číslo väčšie ako 2 je súčtom dvoch prvočísel (Goldbachov problém z roku 1742).

Ak písmeno p označuje výrok, tak zápis $\mathrm{ph}(p) = 1$ znamená, že výrok p je pravdivý (*má pravdivostnú hodnotu* 1). Analogicky $\mathrm{ph}(p) = 0$ znamená, že výrok p je nepravdivý (*má pravdivostnú hodnotu* 0).

Ak p je výrok, tak $\neg p$ je označenie tzv. *negácie* výroku p. O pravdivostných hodnotách výroku p a jeho negácie $\neg p$ platí: ak p je pravdivý, tak $\neg p$ je nepravdivý, ak p je nepravdivý, tak $\neg p$ je pravdivý. Ak je výrok p zapísaný prirodzeným jazykom, tak pre utvorenie jeho negácie máme viac možností. Často ju tvoríme pomocou „nie je pravda, že“, zámenou „nie je“ za „je“ alebo pomocou predpony ne.

Príklad 1. Číslo 2 je párne. Negácia uvedeného výroku: číslo 2 nie je párne (alebo „číslo 2 je nepárne“). □

Ak p, q sú výroky zapísané prirodzeným jazykom, tak „p a q“ je opäť výrok a nazývame ho *konjunkcia výrokov* p, q. Namiesto „p a q“ používame tiež spojenie „p aj q“, alebo „p a zároveň q“. Keď sú výroky p, q zapísané formalizovane (nie prirodzeným jazykom, ale pomocou matematických symbolov), tak namiesto „p a q“ píšeme „p & q“ alebo „$p \wedge q$“.

Ďalším častým spojením výrokov p, q je výrok „p alebo q“, ktorý nazývame *disjunkciou* (prípadne *alternatívou) výrokov* p, q. V symbolických zápisoch píšeme „$p \vee q$“.

Poznámka. Niekedy rozlišujeme disjunkciu a alternatívu, ale v tomto texte to nepokladáme za potrebné z viacerých dôvodov.

Najčastejšie sa v matematike stretávame so spojením „ak p, tak q“. Toto spojenie označíme $p \Longrightarrow q$. Výrok „ak p, tak q“ nazývame *implikácia* s *predpokladom* p a s *tvrdením* q. Namiesto „ak p, tak q“, hovoríme tiež „keď p potom q“, „z p vyplýva q“, alebo „p implikuje q“.

Posledným často používaným spojením výrokov p, q je „p práve vtedy, keď q“, resp. „p vtedy a len vtedy, keď q“. Nazývame ho *ekvivalencia výrokov* p, q. Symbolicky ho zapíšeme $p \Longleftrightarrow q$.

Znaky $\neg$, &, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ nazývame *logické spojky*.

Výroky typu p a q, p alebo q, z p vyplýva q, p práve vtedy, keď q, nie je pravda, že p (pričom p, q sú výroky), nazývame *zložené výroky*. Výrok, ktorý nie je zloženým výrokom, nazývame *atomárny výrok*.

V matematike je daná závislosť pravdivosti zložených výrokov od pravdivosti

ich zložiek nasledujúcou tabuľkou.

ph(p)	ph(q)	ph($p \ \& \ q$)	ph($p \vee q$)	ph($p \Longrightarrow q$)	ph($p \Longleftrightarrow q$)	ph($\neg p$)
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

Tab. 1

POZNÁMKA. Mimo matematiky niekedy chápeme pravdivosť zložených výrokov inak (najmä u disjunkcie a implikácie), ale v matematike vždy budeme rešpektovať dohodu o pravdivosti podľa uvedenej tabuľky.

Tvorenie zložených výrokov nepodmieňujeme ani obsahovou ani formálnou súvislosťou ich zložiek. Teda z hľadiska matematickej logiky je korektným aj výrok: „ak $2 + 2 = 5$, tak existuje trojuholník, u ktorého sú všetky vnútorné uhly pravé“ (a dokonca je to pravdivý výrok).

Premennú, ktorej oborom je množina výrokov, nazývame *výroková premenná*. Z výrokových premenných tvoríme pomocou logických spojok $\neg$, $\&$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ *výrokové formuly*.

DEFINÍCIA VÝROKOVEJ FORMULY.

(1) Každá výroková premenná je výroková formula.

(2) Ak Φ a Ψ sú výrokové formuly, tak aj $\neg(\Phi)$, $(\Phi) \ \& \ (\Psi)$, $(\Phi) \vee (\Psi)$, $(\Phi) \Longrightarrow (\Psi)$, $(\Phi) \Longleftrightarrow (\Psi)$ sú výrokové formuly.

POZNÁMKA. V definícii výrokovej formuly sa nehovorí o tom, ktorý zápis nie je výrokovou formulou. V takomto prípade v matematike predpokladáme, že výrokovými formulami sú len také zápisy, u ktorých to možno uvedenými kritériami (1) a (2) zdôvodniť. Teda predpokladáme, že každú výrokovú formulu možno utvoriť postupným aplikovaním uvedených dvoch pravidiel (1) a (2).

Ak p, q sú výrokové premenné, tak namiesto $\neg(p)$, $(p) \ \& \ (q)$ stručne píšeme $\neg p$, $p \ \& \ q$ a podobne v iných prípadoch.

PRÍKLAD 2. Nech p, q, r sú výrokové premenné. Potom

$$((p \Longrightarrow q) \ \& \ (q \Longrightarrow r)) \Longrightarrow (p \Longrightarrow r) \tag{3}$$

je výroková formula (niekedy hovoríme formula výrokového počtu). Vyplýva to z nasledujúceho:

a) p, q, r sú výrokové formuly (ďalej stručne len formuly) podľa (1).

b) Z a) vyplýva podľa (2), že aj $p \Longrightarrow q$, $q \Longrightarrow r$, $p \Longrightarrow r$ sú formuly.

c) Z b) vyplýva podľa (2), že aj $(p \Longrightarrow q) \ \& \ (q \Longrightarrow r)$ je formula.

d) Z b), c) podľa (2) vyplýva, že aj (3) je formula. □

Postupnosť p, q, r, $p \Longrightarrow q$, $q \Longrightarrow r$, $p \Longrightarrow r$, $(p \Longrightarrow q) \ \& \ (q \Longrightarrow r)$, celá formula (3), sa nazýva *vytvárajúcou postupnosťou formuly* (3).

Ku každej výrokovej formule môžeme priradiť *tabuľku pravdivostných hodnôt*, ktorú zostavujeme nasledujúcim spôsobom:

1. Do záhlavia napíšeme členy vytvárajúcej postupnosti formuly (pričom symbol ph kvôli stručnosti obvykle vynechávame).

2. Pod premenné napíšeme do riadkov všetky (usporiadané) n-tice utvorené z pravdivostných hodnôt 0, 1. Ak má formula n premenných, tak usporiadaných n-tíc je 2^n (t.j. tabuľka má pod záhlavím 2^n riadkov).

3. V zhode s tabuľkou 1 postupne vypĺňame stĺpce pod ostatnými členmi vytvárajúcej postupnosti (podrobne sa s tým čitateľ oboznámi na cvičení). K formule (3) prislúcha nasledujúca tabuľka pravdivostných hodnôt.

p	q	r	$p \Longrightarrow q$	$q \Longrightarrow r$	$p \Longrightarrow r$	$(p \Longrightarrow q)$ & $(q \Longrightarrow r)$	F
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	1	0	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	1	0	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

Tab. 2

Poznámka. Písmenom F je v tabuľke 2 označená formula (3).

Niekedy tabuľku 2 zapisujeme v nasledujúcom skrátenom tvare.

$$((p \Longrightarrow q)\ \&\ (q \Longrightarrow r)) \Longrightarrow (p \Longrightarrow r)$$

1	1	1	1	1	1	1	1	1	1	1
1	1	1	0	1	0	0	1	1	0	0
1	0	0	0	0	1	1	1	1	1	1
1	0	0	0	0	1	0	1	1	0	0
0	1	1	1	1	1	1	1	0	1	1
0	1	1	0	1	0	0	1	0	1	0
0	1	0	1	0	1	1	1	0	1	1
0	1	0	1	0	1	0	1	0	1	0

V zápisoch zložitejších formúl je veľa zátvoriek, čo zmenšuje prehľadnosť zápisov. Preto je zvykom prijať aj ďalšiu dohodu, umožňujúcu ich vynechávanie.

Dohovor: a) Logické spojky & a $\vee$ viažu tesnejšie, ako $\Longrightarrow$ a $\Longleftrightarrow$.

b) Logická spojka $\neg$ viaže tesnejšie, než ostatné logické spojky.

Na základe uvedeného dohovoru môžeme formulu

$$(\neg(p\ \&\ q)) \Longleftrightarrow ((\neg p) \vee (\neg q))$$

napísať v tvare

$$\neg(p\ \&\ q) \Longleftrightarrow \neg p \vee \neg q.$$

Príklad 3. Pri vyšetrovaní krádeže sa zistili nasledujúce skutočnosti:

1. Podozrivé sú len štyri osoby A, B, C, D.
2. Ak A aj B kradli, tak C bol ich spoločníkom.
3. Ak A kradol, bol jeho spoločníkom aspoň jeden z dvojice B, C.
4. C nekradol bez D.

5. Ak A je nevinný, tak kradol D.

Ktorú z osôb A, B, C, D môže sudca jednoznačne obviniť z krádeže?

RIEŠENIE. Najskôr uvedieme riešenie „úvahou“, potom riešenie pomocou tabuľky pravdivostných hodnôt.

a) Najskôr zdôvodníme, že ak A kradol, tak aj C kradol. Predpokladajme, že A kradol. Potom podľa 3. je vinný aj B alebo C. Ak B kradol, tak podľa 2. aj C kradol. Z posledných dvoch výrokov vyplýva, že C kradol. Potom však podľa 4. dostávame, že ak A kradol, tak kradol aj D. Z 5. vyplýva, že aj v prípade, že A je nevinný D kradol.

Sudca môže jednoznačne obviniť len osobu D.

b) Písmenom a označíme výrok "A kradol". Analogický význam majú symboly b, c, d. Ak výsledky vyšetrovania zapíšeme do tabuľky pravdivostných hodnôt dostaneme tabuľku 3.

a	b	c	d	$(a \ \& \ b) \Rightarrow c$	$a \Rightarrow (b \vee c)$	$c \Rightarrow d$	$\neg a \Rightarrow d$
1	1	1	1	1	1	1	1
1	1	1	0	1	1	0	1
1	1	0	1	0	1	1	1
1	1	0	0	0	1	1	1
1	0	1	1	1	1	1	1
1	0	1	0	1	1	0	1
1	0	0	1	1	0	1	1
1	0	0	0	1	0	1	1
0	1	1	1	1	1	1	1
0	1	1	0	1	1	0	0
0	1	0	1	1	1	1	1
0	1	0	0	1	1	1	0
0	0	1	1	1	1	1	1
0	0	1	0	1	1	0	0
0	0	0	1	1	1	1	1
0	0	0	0	1	1	1	0

Tab. 3

Predpokladáme, že vyšetrovaním sa zistili pravdivé údaje, preto si všímame len tie riadky tabuľky, v ktorých sú v posledných štyroch stĺpcoch len hodnoty 1, teda riadky 1., 5., 9., 11., 13. a 15. Vo všetkých týchto riadkoch je pravdivostná hodnota 1 zakaždým v prvých štyroch stĺpcoch len pod výrokom d, teda sudca môže jednoznačne obviniť len D. □

V matematike sú osobitne dôležité také formuly výrokového počtu, u ktorých tabuľka pravdivostných hodnôt má v poslednom stĺpci (resp. pri skrátenom zápise v naposledy vypĺňanom stĺpci) len hodnoty 1. Takéto formuly nazývame *tautológie* (výrokového počtu).

Formula F je tautológiou práve vtedy, keď po dosadení ľubovoľných výrokov za premenné dostaneme vždy pravdivý výrok (samozrejme pri správnej interpretácii logických spojok).

Ak Φ a Ψ sú výrokové formuly a ak $(\Phi \Longleftrightarrow \Psi)$ je tautológia, hovoríme, že formuly Φ a Ψ sú *logicky ekvivalentné* a píšeme $\Phi \equiv \Psi$, resp. $\Phi \sim \Psi$. Ak $(\Phi) \Longrightarrow (\Psi)$ je tautológia hovoríme, že Ψ je *logickým dôsledkom* Φ.

Pomocou tabuliek pravdivostných hodnôt sa možno presvedčiť že platí:

$$
\begin{array}{lll}
T_1 & p \equiv \neg(\neg p), & \\
T_2 & p \ \& \ q \equiv q \ \& \ p, & p \vee q \equiv q \vee p, \\
T_3 & p \ \& \ (q \ \& \ r) \equiv (p \ \& \ q) \ \& \ r, & p \vee (q \vee r) \equiv (p \vee q) \vee r, \\
T_4 & p \ \& \ (q \vee r) \equiv (p \ \& \ q) \vee (p \ \& \ r), & p \vee (q \ \& \ r) \equiv (p \vee q) \ \& \ (p \vee r), \\
T_5 & \neg(p \ \& \ q) \equiv \neg p \vee \neg q, & \neg(p \vee q) \equiv \neg p \ \& \ \neg q, \\
T_6 & p \Longleftrightarrow q \equiv (p \Longrightarrow q) \ \& \ (q \Longrightarrow p), & \\
T_7 & \neg(p \Longrightarrow q) \equiv p \ \& \ \neg q, & \\
T_8 & p \Longrightarrow q \equiv \neg q \Longrightarrow \neg p, &
\end{array}
$$

pričom p, q, r sú výrokové premenné.

Keď chceme zdôrazniť, že Φ je výroková formula, ktorá obsahuje výrokové premenné $A_1, \ldots, A_n$ a žiadne iné, často namiesto Φ napíšeme $\Phi(A_1, \ldots, A_n)$.

O tautológiach možno dokázať nasledujúce tvrdenia:

a) Ak $\Phi(A_1, \ldots, A_n)$ je tautológia a $\Phi_1, \ldots, \Phi_n$ sú ľubovoľné formuly, tak po dosadení Φ_1 za A_1, ... , Φ_n za A_n do formuly Φ dostaneme opäť tautológiu (tzv. *dosadzovacie pravidlo*).

b) Ak Φ aj $\Phi \Longrightarrow \Psi$ sú tautológie, tak aj Ψ je tautológia (tzv. *pravidlo odlúčenia – modus ponens*).

Pri dokazovaní matematických poznatkov okrem poznatkov už predtým dokázaných (resp. uvedených ako axiómy) používame aj logické úvahy (logické úsudky). Zaiste ste si už osvojili mnohé matematické dôkazy, sotva by ste však vedeli presne charakterizovať aké logické úvahy sa pri nich využívajú a z čoho vyplýva ich oprávnenosť. Podrobne sa s tým ani v tomto texte zaoberať nebudeme. Zdôrazňujeme však, že prípustné logické úvahy sú tie, ktoré sú v súlade s tautológiami (nielen výrokového, ale aj predikátového počtu, ktorý je obsahom nasledujúcej kapitoly). Preto v niektorej literatúre sa nazývajú tautológie *logickými zákonmi*. Z tautológii uvedených v tomto texte si všimnite najmä T_1, T_7 a T_8, na ktorých sú založené nepriame dôkazy.

Aby sme pomohli čitateľovi pri riešení cvičení uvedieme riešenie ešte aspoň jedného jednoduchého príkladu.

PRÍKLAD 4. V stredoveku vyrábali umelecké skrinky slávni majstri Bellini a Cellini. Zatiaľ čo Bellini napísal na zhotovenú skrinku vždy nejaký pravdivý výrok, Cellini napísal na zhotovenú skrinku vždy nepravdivý výrok. Každý z nich mal syna, ktorý pokračoval v činnosti otca a dodržiaval jeho zásady.

Na výstave umeleckých predmetov som uvidel skrinku vyrobenú niektorým z nich štyroch a na nej nápis „Túto skrinku nevyrobil Bellini ml.“ Môžeme z toho vyvodiť kto skrinku vyrobil ?

RIEŠENIE. Hoci zdanlivo by malo ist' o $2^4 = 16$ možností, stači uvažovať len o štyroch, pretože predpokladáme že skrinku vyrobil len jeden zo štvorice Bellini starší, Bellini mladší, Cellini mladší, Cellini starší.

Keby skrinku zhotovil Bellini ml., nenapísal by na skrinku nepravdivý výrok, teda on ju nevyrobil. Keby skrinku vyrobil niektorí Cellini, bol by výrok na skrinke pravdivý, ale oni na skrinky pravdivé výroky nepísali. Z toho vyplýva, že skrinku vyrobil Bellini starší. □

Cvičenia

1. Ukážte, že nasledujúce formuly sú tautológie:

a) $(p \Longrightarrow q) \Longleftrightarrow (\neg p \vee q)$,

b) $(p \Longleftrightarrow q) \Longleftrightarrow ((p \ \& \ q) \vee (\neg q \ \& \ \neg q))$,

c) $(p \Longleftrightarrow r) \Longrightarrow ((q \Longleftrightarrow r) \Longrightarrow (p \Longleftrightarrow q))$,

d) $(p \Longleftrightarrow q) \Longrightarrow (p \ \& \ r \Longleftrightarrow r \ \& \ q)$.

2. Napíšte formulu, ktorá obsahuje len výrokové premenné, logické spojky $\neg$, $\vee$ a zátvorky a je ekvivalentná s formulou

a) $p \Longrightarrow q$, b) $p \ \& \ q$

c) $(p \Longrightarrow q) \Longrightarrow r$ d) $p \Longrightarrow (q \Longrightarrow r)$.

3. Dané sú pravdivostné hodnoty formuly F v závislosti od hodnôt jej premenných p, q nasledovne:

a)
p	q	F
1	1	1
1	0	0
0	1	1
0	0	0

b)
p	q	F
1	1	0
1	0	0
0	1	1
0	0	0

Nájdite formulu F.

4. Pred sudcom stáli traja obžalovaní. Vyšetrovaním sa zistilo, že

a) Ak je A nevinný alebo B vinný, tak C je vinný.

b) Ak A je nevinný, tak nevinný je aj C.

Koho z nich má sudca odsúdiť?

5. Inšpektor Sherlock Holmes zistil

a) Ak A je vinný a B je nevinný, tak C je vinný.

b) C nikdy nie je v akcii sám.

c) A nikdy nespolupracuje s C.

d) Okrem A, B, C nie sú do prípadu zapletení d'alší l'udia, teda aspoň jeden z A, B, C je vinný.

Koho obvinil Sherlock Holmes ?

6. V texte úlohy sa hovorí o skrinkách zhotovených niektorým zo slávnych majstrov Bellini ml., Bellini st., Cellini ml., Cellini st. (prečitajte si text príkladu 4, ktorý je uvedený pred cvičeniami).

V múzeu boli vystavené dve skrinky s nápismi:

Každú skrinku z tejto súpravy vyrobil Cellini - nápis na prvej.

Žiadnu z týchto skriniek nevyrobil Bellini ml. ani Cellini ml. - nápis na druhej.

Viete z toho usúdit' kto vyrobil prvú a kto druhú skrinku ?

7. Na výstave boli vedl'a seba umiestnené tri skrinky vyrobené už spomínanými majstrami. Riaditeľ výstavy vložil do jednej z nich šperk, pričom dbal aby tradícia o nápisoch ostala zachovaná. Na skrinkách boli nápisy:

V tejto skrinke je šperk - prvá skrinka,

V tejto skrinke je šperk - druhá skrinka,

Aspoň dve z týchto skriniek zhotovil Cellini - tretia skrinka.

Vašou úlohou je určit'

a) V ktorej skrinke je šperk.

b) Určit' výrobcov jednotlivých skriniek.

8. Účast' Anny, Barbary, Cyrila a Dušana na koncerte bola podmienená týmito záväzkami. Na koncert pôjde aspoň jeden chlapec a najviac jedno dievča. Zo

súrodencov Anna - Cyril pôjde práve jeden. Barbara nepôjde bez Dušana, ale Anna zasa nepôjde v žiadnom prípade spolu s Dušanom. Kto z nich sa na koncerte určite zúčastní ?

5. Predikátový počet.

Jednou z charakteristických čŕt matematiky nášho storočia je úsilie preskúmať základy (východiská) matematiky a precizovať vyjadrovacie prostriedky používané v matematike. Dôsledkom týchto snáh bolo odlíšenie tzv. matematického jazyka od bežne používaného nematematického jazyka (tzv. metajazyka). Dôvodov pre takéto rozlišovanie je viac, jedným je možnosť formulovania paradoxov nasledujúceho typu:

Nech m je najmenšie prirodzené číslo, ktoré nemožno určiť pomocov menej ako dvadsať slov slovenského jazyka.

Určili sme tým číslo m ? Pretože prirodzených čísel je nekonečne veľa zrejme nie každé možno určiť pomocou vety s najviac 20 slovami, t.j. množina takých prirodzených čísel, ktoré nemožno takto určiť je neprázdna a má najmenší prvok m. Na druhej strane vidíme, že m je určené menej ako dvadsiatimi slovami slovenského jazyka.

Významným medzníkom vo vývoji matematiky bolo zavedenie symbolov vo význame *premenných* (Descartes 1596-1650). Pod premennou (v zmysle tzv. voľnej premennej) rozumieme taký symbol, ktorý reprezentuje ľubovoľný prvok určitej množiny nazývanej *obor premennej*. Napríklad do vzorca $P = \pi.r^2$ môžeme za r dosadiť hocijaké kladné reálne číslo a vypočítame obsah kruhu, ktorého polomerom je toto číslo. Teda r je premenná, ktorej oborom je množina kladných reálnych čísel. Naproti tomu za π nedosadzujeme hocijaké čísla, vieme, že π je (vo vyššie uvedenom vzorci) konštanta (Ludolfovo číslo). Niekedy však (ak to nie je explicitne povedané) si vieme domyslieť len z kontextu, či nejaký symbol je premennou alebo konštantou. Napríklad v Ohmovom zákone $U = R.I$ môžu byť premennými symboly U, I a konštantou R, ale v iných úvahách sú premenné R, I a konštanta U (resp. U, R aj I sú premenné). Dohodneme sa, že obor premennej x budeme označovať $O(x)$.

Východiskom pri budovaní matematického jazyka sú premenné a konštanty. Z nich pomocou symbolov operácií tvoríme *termy* (výrazy) a z termov pomocou symbolov relácií a kvantifikátorov tvoríme *formuly (predikátového počtu)*, prostredníctvom ktorých sa vyjadrujeme. V logike sa namiesto o symboloch operácií a relácií hovorí o funkcionálnych a predikátových symboloch, ale my uprednostníme terminológiu bežne používanú v matematike (napriek tomu, že n-árne relácie sa často definujú len pre $n > 1$.)

DEFINÍCIA (TERMU). Nech A je množina. Term (nad A) je definovaný takto:

1. Každá premenná ktorej oborom je množina A je term (nad A).
2. Každá konštanta (z A) je term (nad A).
3. Ak $*$ je binárna operácia na množine A a ak t, w sú termy (nad A), tak aj $(t) * (w)$ je term (nad A).

POZNÁMKA. a) Ak t, w sú premenné alebo konštanty, tak namiesto $(t) * (w)$ píšeme stručne $t * w$.

b) V matematike okrem binárnych operácií používame aj operácie unárne, ternárne atď., preto posledná časť definície by mala byť formulovaná všeobecnejšie, ale v tomto úvodnom texte to robiť nebudeme.

PRÍKLAD 1. Nech x, y, z sú reálne premenné. Potom
(a) $((2.x) + (y.z)) : (x + y)$
je term (nad E). Odôvodnit' to môžeme nasledovne:
a) x, y, z sú termy (nad E) podľa 1.
b) Konštanta 2 je term (nad E) podľa 2.
c) Z a), b) podľa 3. vyplýva, že aj $2.x$, $y.z$, $x + y$ sú termy (nad E).
d) Z c) vyplýva podľa 3., že aj $(2.x) + (y.z)$ je term (nad E).
e) Z c), d) podľa 3. dostávame, že aj (a) je term nad E.
Postupnost' x, y, z, $2.x$, $y.z$, $x + y$, $(2.x) + (y.z)$, $((2x) + (y.z)) : (x + y)$ sa nazýva *vytvárajúca postupnost' termu* (a). □

V zápisoch termov je zvykom predpokladat', že znaky operácií $\cdot$ a $:$ viažu tesnejšie ako znaky operácií $+$ a $-$. Dokonca písanie znaku . často vynechávame. Teda term (a) zvykneme zapisovat' v tvare:

$$(2x + yz) : (x + y).$$

S termami sa stretávame napríklad pri riešení rovníc a nerovníc, pretože pravou aj ľavou stranou rovnice, resp. nerovnice, sú termy. V algebre ste nacvičovali úpravy termov, ktoré ste nazývali algebraické výrazy.

O termoch možno stručne povedat', že sú to korektne zostavené zápisy z premenných s rovnakým oborom A, zo symbolov prvkov množiny A (konštánt), znakov operácií na A a zátvoriek.

DEFINÍCIA 2. Nech A je množina. Ak t, w sú termy nad A a R je binárna relácia na A, tak zápis tRw nazývame atomická formula predikátového počtu (nad A).

Príkladmi atomických formúl predikátového počtu sú rovnice a nerovnice. Iné príklady atomických formúl : $a \in A$, $\{1, 2\} \subseteq B$, $1 < 4$, $a \parallel b$, $a \perp \alpha$ (obory premenných si môžeme vhodne zvolit').

Z predchádzajúceho štúdia poznáte kvantifikátory:
a) všeobecný, označovaný $\forall$, obvykle ho interpretujeme slovami „pre každé“,
b) existenčný, označovaný $\exists$, spravidla interpretujeme slovom „existuje“.
Logické spojky a kvantifikátory nám umožňujú rozšíť pojem formuly predikátového počtu (stručne formuly) nasledujúcim spôsobom.

DEFINÍCIA 3. 1. Každá atomická formula predikátového počtu (nad A) je formula.
2. Ak U, V sú formuly (nad A), tak aj $\neg(U)$, (U) & (V), $(U) \vee (V)$, $(U) \Longrightarrow (V)$, $(U) \Longleftrightarrow (V)$ sú formuly.
3. Ak x je premenná s oborom A a V je formula (nad A), ktorá neobsahuje výraz $\forall x$ ani $\exists x$, tak aj $\forall x$ (V) a $\exists x$ (V) sú formuly (nad A).

PRÍKLAD 2. Nech x, y, z sú reálne premenné (t.j. ich oborom je množina reálnych čísel E). Zápisy
(b) $(x < y) \Longrightarrow ((x + z) < (y + z))$,
(c) $\exists x \quad (x^2 + x + 1 = 0)$,
(d) $\forall x \quad (\exists y \quad (x = y^2))$
sú formuly (nad E). □

Ak nehrozí nedorozumenie, tak u formúl predikátového počtu niektoré zátvorky vynechávame. Napríklad namiesto $\forall x\,(\forall y\,(U))$ zvykneme písať $\forall x, y\,(U)$ a pod. Ďalej zvykneme predpokladať, že znaky operácií viažu tesnejšie, než znaky relácií a znaky relácií viažu tesnejšie ako logické spojky. Napríklad formulu (b) môžeme na základe tejto dohody zapísať v tvare

(e) $$x < y \Longrightarrow x + z < y + z.$$

Ak je oborom premennej x množina A, tak zápis „$\forall x$“ čítame „pre každé x z množiny A“ a zápis „$\exists x$“ čítame „existuje x z množiny A“. Napríklad zápis (c) čítame „existuje reálne číslo x, o ktorom platí $x^2 + x + 1 = 0$“. Keď chceme zdôrazniť, že oborom premennej x je množina A, tak namiesto „$\forall x$“ napíšeme „$\forall x \in A$“. Napríklad formulu (d) môžeme zapísať v tvare

$$\forall x \in E\, \exists y \in E \quad x = y^2.$$

Nech Φ, Ψ sú formuly. Hovoríme, že Ψ je *podformula* formuly Φ ak Ψ môžeme získať z Φ tak, že vo Φ vynecháme niekoľko symbolov na začiatku aj na konci (niekoľko môže znamenať aj 0, t.j. žiadne). Napríklad $x < y$ je podformula formuly (e).

V ďalšom texte budeme kvantifikátormi nazývať nielen symboly $\forall$ a $\exists$, ale aj $\forall x$, $\exists y$ a pod. *Dosahom kvantifikátora* $\forall x$, resp. $\exists x$ nazývame tú podformulu, ktorej zápis bezprostredne nasleduje za $\forall x$, resp. $\exists x$. Napríklad dosah kvantifikátora $\exists y$ vo formule (d) je podformula $x = y^2$.

Výskyt premennej x (ktorý nie je súčasťou kvantifikátora $\forall x$ resp. $\exists x$) vo formule V sa nazýva:

1. *viazaným*, ak sa nachádza v dosahu kvantifikátora $\forall x$ alebo $\exists x$.
2. *voľným*, ak nie je viazaný.

Premenná x je voľnou vo formule V, ak má aspoň jeden voľný výskyt vo formule V. *Premenná x je viazaná* vo formule V, ak všetky jej výskyty vo V sú viazané. Napríklad premenná x je vo formule (b) voľná, ale vo formulách (c) a (d) je viazaná.

Z hľadiska voľných a viazaných premenných delíme formuly na:

a) *uzavreté formuly*, u ktorých všetky premenné sú viazané (také sú formuly (c) a (d))

b) *výrokové formy*, u ktorých aspoň jedna premenná je voľnou premennou (takou je formula (b)).

Pri našom chápaní formúl sú uzavreté formuly výrokmi. Často ich nazývame *kvantifikované výroky*. Väčšina matematických viet má tvar kvantifikovaných výrokov, alebo ich možno na tento tvar prepísať. Napríklad

(i) $\forall x \forall y \exists z \qquad x + z = y, \quad$ kde $\quad O(x) = O(y) = O(z) = Z,$

(j) $\forall a \forall b \forall c \qquad a \parallel b \ \ \& \ \ b \parallel c \Longrightarrow a \parallel c, \quad$ kde $\quad O(a) = O(b) = O(c) = P,$

kde P je množina všetkých priamok zvolenej roviny,

(k) $\forall u \forall v \qquad (u < v \Longrightarrow \exists w\,(u < w < v)), \quad$ kde $\quad O(u) = O(v) = O(w) = Q.$

Nech $V(x)$ je výroková forma (s jedinou voľnou premennou x), pričom obor premennej $O(x) = A$. Ak dosadíme za x (t.j. za všetky voľné výskyty premennej x) nejaký prvok $a \in A$, tak môžeme (ale nemusíme) dostať výrok. Napríklad ak dosadíme do výrokovej formy (rovnice)

(g) $$4 - x = \frac{3}{x}$$

(s reálnymi premennými) za x číslo 1 dostaneme pravdivý výrok $4-1=\frac{3}{1}$. Ak však dosadíme za x číslo 0, nedostaneme výrok, pretože na pravej strane dostaneme zápis $\frac{3}{0}$, ktorý nereprezentuje žiadne číslo.

Množinu všetkých prvkov $a \in A$, po dosadení ktorých do $V(x)$ dostaneme výrok $V(a)$, nazývame *definičný obor výrokovej formy* $V(x)$.

Výroková forma (g) má definičný obor $E-\{0\}$.

Množinu všetkých tých prvkov a z definičného oboru formy $V(x)$ po dosadení ktorých do $V(x)$ dostaneme pravdivý výrok $V(a)$, nazývame *obor pravdivosti výrokovej formy* $V(x)$.

Ak je oborom pravdivosti výrokovej formy $V(x)$ množina M, píšeme

$M=\{x \in A; V(x)\}$ alebo stručne $\{x;\, V(x)\}$

a čítame „M je množina všetkých (takých) prvkov x (z množiny A), o ktorých platí $V(x)$“.

Oborom pravdivosti výrokovej formy (g) je množina $\{1,3\}$ (t. j. rovnica (g) má korene $x_1=1,\ x_2=3$).

Analogicky, ako hovoríme o definičnom obore a o obore pravdivosti u výrokových foriem s jednou voľnou premennou, môžeme hovoriť o definičnom obore a o obore pravdivosti aj u výrokových foriem s viacerými premennými.

Napríklad do definičného oboru výrokovej formy

$$\text{(h)} \qquad \sqrt{x^2-y} < z+x$$

(s reálnymi premennými) nepatrí usporiadaná trojica $[1,2,3]$ (pretože $\sqrt{1-2}$ u formúl uvedeného typu nie je definované), ale patrí usporiadaná trojica $[2,3,1]$. Po dosadení usporiadanej trojice $[2,3,1]$ do (h) dokonca dostaneme pravdivý výrok $\sqrt{2^2-3}<1+2$ preto $[2,3,1]$ patrí do oboru pravdivosti formy (h).

Ak do výrokovej formy s viacerými voľnými premennými dosadíme konštanty len za niektoré premenné, opäť dostaneme výrokovú formu. Napríklad, ak dosadíme do (h) len za z číslo 0 (t.j. ak dosadíme do (h) usporiadanú trojicu $[x,y,0]$), dostaneme výrokovú formu s dvoma (voľnými) premennými $\sqrt{x^2-y}<x$.

Ak $V(x)$ aj $W(x)$ sú výrokové formy, tak zrejme aj $\neg V(x)$, $V(x)\ \&\ W(x)$, $V(x) \vee W(x)$, $V(x) \Longrightarrow W(x)$, $V(x) \Longleftrightarrow W(x)$ sú výrokové formy.

Výrokovú formu $\neg V(x)$ zvykneme nazývať *negácia výrokovej formy* $V(x)$. Pri negáciách výrokových foriem však často používame aj špeciálne zápisy, napríklad namiesto $\neg(x=y)$ stručne píšeme $x \neq y$, alebo $\neg(x \leq y)$ nahradzujeme zápisom $x>y$. Stručne môžeme negáciu výrokovej formy $V(x)$ charakterizovať ako výrokovú formu $W(x)$, ktorá má rovnaký definičný obor D a pre každý prvok $a \in D$ platí, že $V(a)$ je pravdivý výrok práve vtedy, keď $W(a)$ je nepravdivý výrok.

Poznámka. Poznatky uvedené v predchádzajúcich odstavcoch môžeme zovšeobecniť aj pre výrokové formy s viacerými premennými (ale prenechávame to čitateľovi).

Na základe definície pravdivosti zložených výrokov (vo výrokovom počte) je čitateľovi zaiste jasné, kedy je pravdivý napríklad výrok tvaru

$\forall x \quad V(x)\ \&\ W(x)$, alebo $\forall x \exists y \quad V(x,y) \vee W(x,y)$,

$\forall x \forall y \quad V(x,y) \Longrightarrow W(x,y)$ a pod.

Príklad 3. Výroky zapísané formulami

a) $\forall x \quad (x-2<0 \iff x<2)$,

b) $\forall x \forall y \qquad (\sqrt{x^2} = x \quad \& \quad \sqrt{y^2} = y \qquad \Longrightarrow \quad \sqrt{(x.y)^2} = x.y)$,
kde x, y sú reálne premenné, sú pravdivé výroky. $\square$

POZNÁMKA. V matematických formuláciách si však často treba „domysliet" nielen zátvorky, ale aj logické spojky a kvantifikátory. Známu vetu „uhlopriečky rovnobežníka sa rozpoľujú" nechápeme ako tvrdenie o rovnobežníku, ktorý sme mali v texte naposledy narysovaný, ale v zmysle „pre každý rovnobežník platí, že jeho uhlopriečky sa rozpoľujú".

Poradie kvantifikátorov rovnakého typu môžeme u formúl menit' bez toho, že by sme zmenili zmysel zápisu. Zmenou poradia rôznych kvantifikátorov môžeme však dostat' z pravdivého výroku nepravdivý výrok, alebo naopak. Napríklad

$\forall x \exists y \qquad x < y, \quad$ kde $\quad O(x) = O(y) = E,$

je pravdivý výrok, kdežto

$\exists y \forall x \qquad x < y, \qquad O(x) = O(y) = E,$

je nepravdivý výrok.

Pri negovaní kvantifikovaných výrokov používame tzv. *de Morganove pravidlo*: všeobecné kvantifikátory nahradíme existenčnými a naopak a príslušnú výrokovú formu V nahradíme formou $\neg V$. Napríklad negáciou kvantifikovaného výroku

$$\forall x \forall y \exists z \qquad x + z = y, \quad \text{kde} \quad O(x) = O(y) = O(z) = Z$$

dostaneme výrok

$$\exists x \exists y \forall z \qquad x + z \neq y, \qquad O(x) = O(y) = O(z) = Z.$$

POZNÁMKA. V matematickej logike sa nezvykne pojem termu a formuly viazat' k určitej množine. V takom prípade formula (predikátového počtu) je korektne zostavený zápis z (predmetových) premenných, symbolov operácií, relácií, logických spojok, kvantifikátorov a zátvoriek, a až ked' sa hovorí o interpretácii priraďujeme premenným obor (t.j. určitú množinu). Symboly operácií a relácií sa až potom stávajú reprezentantmi konkrétnych operácií a relácií na obore premenných. V takom prípade sa aj u formúl predikátového počtu uvádzajú tautológie. Ide o formuly, ktoré sú pravdivé pri l'ubovoľnej interpretácii. Príkladom je formula

$$x_1 = y_1 \ \ \& \ \ x_2 = y_2 \quad \Longrightarrow x_1 \circ x_2 = y_1 \circ y_2$$

pričom $\circ$ je symbol l'ubovoľnej (binárnej) operácie.

Formuly predikátového počtu sa v matematike stali často používaným vyjadrovacím prostriedkom. Preto sme sa podrobnejšie zaoberali ich štruktúrou a významovou stránkou. Záverom však treba poznamenat', že sme sa zamerali len na najjednoduchšie typy takýchto formúl. V súčasnej matematike sa v súvislosti so skúmaním operácií a relácií napríklad popri operáciách a reláciách na množine reálnych čísel skúmajú aj operácie a relácie na systéme reálnych funkcií. Tomu potom zodpovedá aj štruktúra formúl, v ktorých vystupujú premenné s rôznymi obormi, operácie na rôznych množinách a relácie medzi množinami. V zložitejších úvahách dokonca operačné a relačné symboly môžu byt' uvažované ako premenné, ktoré môžu byt' voľné alebo viazané kvantifikátormi, to však už presahuje rámec tohto textu (my sme sa zamerali len na tzv. jazyk prvého rádu).

Cvičenia.

1. Nech x, y, z sú reálne premenné. Rozhodnite, ktorý z nasledujúcich zápisov (pri obvyklom chápaní znakov, z ktorých je zložený) je term, ktorý je výroková forma a ktorý je výrokom:

$3x - 1, \qquad |x + y| = |x| + |y|, \qquad \forall x \quad \sqrt{x + y} = \sqrt{x} + \sqrt{y},$
$\forall x \exists y, \quad x < y, \qquad (x + y).z - 2xy, \qquad \exists x \forall y \quad x + y = 0,$
$\forall x \forall y \quad (x < y \Longrightarrow \exists z \quad x < z < y), \qquad \forall x \quad x - y < y,$
$\forall x \forall y \quad x.z = y.z \Longrightarrow x = y, \qquad \sqrt{x^2.y^2} = x.y.$

2. Posúďte pravdivosť výrokov z cvičenia 1 a napíšte ich negácie.

3. Nech A, B, C sú množinové premenné. Rozhodnite, ktorý z nasledujúcich zápisov je term, ktorý je výroková forma a ktorý je výrok:

$\forall A \forall B \quad A \cup B = B \cup A, \qquad (A \cap B) \cup C, \qquad A - B \subseteq \emptyset,$
$\forall A \exists B \quad A \subseteq B, \qquad A - (B \cup C) = (A - B) \cup (A - C),$
$\forall A \forall B \quad A - C = B - C \Longrightarrow A = B, \qquad \exists A \exists C \quad A \cup C \subseteq A \cap C.$

4. Rozhodnite o pravdivosti výrokov z cvičenia 3 a napíšte ich negácie.

5. Daná je výroková forma $6|x, \qquad O(x) = \{0, 3, 6, 9, 12, 15\}$. Bez použitia kvantifikátorov zapíšte výroky: $\forall x \quad 6|x, \qquad \exists x \quad 6|x.$

6. Z nasledujúcich výrokových foriem s celočíselnými premennými utvorte výroky

a) dosadením,
b) pomocou kvantifikátorov,
c) kombináciou predchádzajúcich spôsobov

$x|y, \qquad x.y = 10, \qquad x < x^2, \qquad x - y = z.$

7. Rozhodnite o pravdivosti výrokov, ktoré ste napísali, pri riešení predchádzajúceho cvičenia.

8. Formulami predikátového počtu zapíšte:

a) Rovnica $x^3 - 6x + 4 = 0$ má aspoň jeden reálny koreň.
b) Rovnica $x^2 + x + 1 = 0$ nemá reálny koreň.
c) Pre niektoré reálne čísla platí $(a + b)^2 = a^2 + b^2$.
d) Pre sčítanie reálnych čísel platí asociatívny zákon.
e) Ak obidve strany nerovnosti (medzi reálnymi číslami) vynásobíme záporným (reálnym) číslom, znak nerovnosti sa obráti.
f) Súhlasné nerovnosti (medzi reálnymi číslami) môžeme sčítať.
g) Neexistuje najmenšie reálne číslo.
h) Existuje (celé) číslo, ktoré je deliteľom každého (celého) čísla.
i) Existuje (celé) číslo, ktoré je deliteľné každým (celým) číslom.
j) Prirodzené číslo je deliteľné šiestimi, práve vtedy, keď je deliteľné dvoma a troma.
k) $\lim\limits_{n \to \infty} a_n = a, \qquad a \in E.$
m) $\lim\limits_{n \to \infty} a_n = -\infty.$
n) $\lim\limits_{x \to a} f(x) = b, \qquad a, b \in E.$

9. Oborom premenných a, b, c nech je množina strán daného štvorca a oborom premenných p, q, r nech je množina jeho uhlopriečok (urobte si náčrt). Posúďte pravdivosť nasledujúcich výrokov a zapíšte ich negácie.

a) $\forall a \exists b \quad a \parallel b$ b) $\exists a \exists b \exists c \quad a \parallel b \parallel c$

c) $\exists a \forall b \quad a \perp b$ d) $\forall a \forall p \quad \neg(a \parallel p)$
e) $\forall p \exists r \quad p \perp r$ f) $\forall p \exists q \quad p \parallel q$
g) $\exists a \exists p \quad a \perp p$ h) $\forall p \exists q \exists r \quad p \perp q \perp r$.

10. Určte obory číselných premenných tak, aby nasledujúce formuly boli zápismi pravdivých výrokov:

a) $\forall x \exists y \quad x = y^2$ b) $\forall x \exists y \quad x = y^3$
c) $\forall x \exists y \forall z \quad x < z \Longrightarrow y \leq z$
d) $\forall x \forall y \quad x < y \Longrightarrow \exists z \quad x < z < y$.
e) $\forall x \exists y \exists z \quad y \neq z \ \& \ y^2 = z^2 = x$
f) $\forall x \forall y \forall z \quad x.z = y.z \Longrightarrow x = y$.

6. Ďalšie poznatky o množinách

Pripomeňme si, že dve množiny sa rovnajú práve vtedy, keď obsahujú tie isté prvky, t.j.

(1) $$A = B \iff (\forall x \quad x \in A \Leftrightarrow x \in B).$$

Ak $A = B$, tak symboly (písmená) A, B označujú tú istú množinu, preto implikácia $\Longrightarrow$ je zrejmá a je len špeciálnym prípadom tautológie o rovnosti z predikátového počtu. Z hľadiska teórie množín je podstatná obrátená implikácia $\Longleftarrow$, z ktorej vyplýva, že množina je jednoznačne určená svojimi prvkami, pričom charakter prvkov a vzťahy medzi nimi sú z hľadiska „konštituovania“ množiny úplne nepodstatné. Teda prvky sa na vytvorení množiny podieľajú len svojou prítomnosťou [36]. Z uvedeného vyplýva, že množina je určená (ako sme už uviedli v tretej kapitole), ak o každom objekte možno (aspoň v princípe) rozhodnúť, či je alebo nie je jej prvkom.

PRÍKLAD 1. Množina A všetkých prirodzených čísel deliteľných šiestimi a množina B všetkých párnych prirodzených čísel sa nerovnajú, lebo $8 \in B$ ale $8 \notin A$.

Množina C všetkých prirodzených čísel deliteľných súčasne dvoma a troma je rovná množine A lebo (podľa vety 2.5) prirodzené číslo je deliteľné šiestimi práve vtedy, keď je deliteľné dvoma a troma. □

Vzťah inklúzie (byť podmnožinou), ktorý sme zaviedli už v tretej kapitole má nasledujúce základné vlastnosti, ktorých dôkazy si čitateľ ľahko urobí aj sám.

VETA 1. *Nech A, B, C sú ľubovoľné množiny. Potom platí:*

a) $A \subseteq A$,

b) *ak* $A \subseteq B$, $B \subseteq A$, *tak* $A = B$,

c) *ak* $A \subseteq B$, $B \subseteq C$, *tak* $A \subseteq C$,

d) $\emptyset \subseteq A$.

Pri dôkazoch rovnosti dvoch množín sa (ako vieme) často používa vlastnosť b).

Uviedli sme už, že množina môže byť daná vymenovaním prvkov (kapitola 3) alebo charakteristickou vlastnosťou, t.j. ako obor pravdivosti nejakej výrokovej formy (kapitola 5). V matematických textoch sa však stretávame aj s rôznymi obmenami uvedených spôsobov. Napríklad, ak napíšeme

$$A = \{0, 1, \ldots, 100\}, \qquad B_n = \{5, 6, \ldots, n\}$$

znamená to, že

$$A = \{n \in N;\ n \leq 100\}, \qquad B_n = \{m \in N;\ 5 \leq m \leq n\}.$$

Niekedy takto zadáme aj množinu, ktorá obsahuje „nekonečne veľa“ prvkov. Napr. $\{0, 2, 4, \ldots, 2k, \ldots\}$ je množina všetkých párnych prirodzených čísel. Ďalej sa stretávame aj so zápismi typu

(a) $$M = \{V(x);\ x \in A\},$$

kde $V(x)$ je tzv menná forma s jedinou voľnou premennou x. Pod *mennou formou* rozumieme výraz obsahujúci jednu alebo viac voľných premenných, z ktorého po dosadení prípustných hodnôt za všetky voľné premenné dostaneme zápis (meno) jediného matematického objektu (čísla, množiny, bodu a pod.). Špeciálnym prípadom mennej formy je term. Zápis (a) teda znamená, že $M = \{b;\ \exists a \in A \quad b = V(a)\}$. Ak napr. $M = \{[x, x+1];\ x \in Z\}$, tak v tomto prípade je M množina všetkých usporiadaných dvojíc, ktoré dostaneme po dosadení celých čísel do výrazu $[x, x+1]$. Napríklad $[2, 3] \in M$, $[2, 4] \notin M$.

PRÍKLAD 2. a) Množinu všetkých prirodzených čísel, ktoré pri delení tromi majú zvyšok 1 môžeme zapísať v tvare $\{x \in Z; \exists k \in N \quad x = 3k + 1\}$ alebo v tvare $\{3k + 1; k \in Z\}$.

b) Množinu kZ všetkých celých čísel deliteľných daným celým číslom k môžeme zapísať napr. v tvare $kZ = \{y \in Z; \exists x \in Z \quad y = k \cdot x\}$ alebo $kZ = \{k \cdot x; x \in Z\}$. □

Ak A je množina, tak môžeme uvažovať o množine $P(A)$ všetkých podmnožín množiny A. Nazývame ju *potenčná množina* množiny A. Symbolicky $P(A) = \{B; B \subseteq A\}$. V takomto prípade namiesto názvu množina množín používame radšej termín systém množín. Napr. $P(\emptyset) = \{\emptyset\}$, $P(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Ku každým dvom množinám A, B môžeme priradiť:

1. množinu $A \cup B = \{x; x \in A \vee x \in B\}$, ktorú nazývame *zjednotenie množín* A, B,
2. množinu $A \cap B = \{x; x \in A \ \& \ x \in B\}$, ktorú nazývame *prienik množín* A, B,
3. množinu $A - B = \{x; x \in A \ \& \ x \notin B\}$, ktorú nazývame *rozdiel množiny* A *a množiny* B. (Miesto $A - B$ sa niekedy píše aj $A \setminus B$).

Ak o množinách A, B platí $A \cap B = \emptyset$, hovoríme, že množiny A, B sú *disjunktné*. V nasledujúcej vete sú zhrnuté niektoré vlastnosti prieniku a zjednotenia.

VETA 2. *Nech* A, B, C *sú ľubovoľné množiny. Potom*

a) $A \cup B = B \cup A, \quad A \cap B = B \cap A,$
b) $(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C),$
c) $A \cup A = A, \quad A \cap A = A,$
d) $A \cup \emptyset = A, \quad A \cap \emptyset = \emptyset,$
e) $A \subseteq A \cup B, \quad A \cap B \subseteq A,$
f) *ak* $A \subseteq B$, *tak* $A \cup C \subseteq B \cup C,$
g) *ak* $A \subseteq B$, *tak* $A \cap C \subseteq B \cap C,$
h) $A \subseteq B$ *práve vtedy, keď* $A \cup B = B,$
i) $A \subseteq B$ *práve vtedy, keď* $A \cap B = A.$

DÔKAZ. Dôkazy týchto tvrdení sú jednoduché. Pre ilustráciu dokážeme vzťah f).

Nech $A \subseteq B$ a nech x je ľubovoľný prvok množiny $A \cup C$. Potom $x \in A$ alebo $x \in C$. Z využitím predpokladu $(A \subseteq B)$ dostávame $x \in B$ alebo $x \in C$, t.j. $x \in B \cup C$. Z toho vyplýva $A \cup C \subseteq B \cup C$. □

V a) sú uvedené *komutatívne zákony* (prvý zo vzťahov pre zjednotenie a druhý pre prienik), v b) *asociatívne zákony* a v c) sú tzv. *zákony idempotencie*.

Vzájomné vzťahy operácií zjednotenia a prieniku (tzv. *distributívne zákony*) sú uvedené v nasledujúcej vete.

VETA 3. *Nech* A, B, C *sú ľubovoľné množiny. Potom*

a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$
b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

DÔKAZ. Dokážeme tvrdenie a), tvrdenie b) sa dokazuje analogicky.

S využitím definície prieniku, zjednotenia a tautológie

$$p \ \& \ (q \vee r) \implies (p \ \& \ q) \vee (p \ \& \ r)$$

môžeme napísať nasledovný reťazec implikácií:

$$x \in A \cap (B \cup C) \implies x \in A \ \& \ x \in B \cup C \implies x \in A \ \& \ (x \in B \vee x \in C) \implies$$
$$\implies (x \in A \ \& \ x \in B) \vee (x \in A \ \& \ x \in C) \implies x \in A \cap B \vee x \in A \cap C \implies$$
$$\implies x \in (A \cap B) \cup (A \cap C).$$

Z toho vyplýva, že $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Pretože všetky implikácie v uvedenom reťazci je možné obrátiť (podrobne to preverte, lebo nie vždy je to možné) dostávame, že aj $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Podľa vety 1 b) je teda $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$. $\square$

Operácie zjednotenia a prieniku množín možno zovšeobecniť nasledujúcim spôsobom.

Nech I je nejaká množina a ku každému prvku $i \in I$ nech je priradená práve jedna množina A_i. Potom množinu

$$\bigcup_{i \in I} A_i = \{x;\, \exists i \in I \quad x \in A_i\}$$

nazývame zjednotenie množín A_i. Množinu

$$\bigcap_{i \in I} A_i = \{x;\, \forall i \in I \quad x \in A_i\}$$

nazývame prienik množín A_i.

Ak systém množín $\{A_i;\, i \in I\}$ je označený $\mathcal{S}$, tak namiesto $\bigcup_{i \in I} A_i$ píšeme tiež $\bigcup_{A_i \in \mathcal{S}} A_i$ alebo skrátene $\bigcup \mathcal{S}$ a čítame *zjednotenie systému* $\mathcal{S}$. Podobne namiesto $\bigcap_{i \in I} A_i$ píšeme $\bigcap \mathcal{S}$ a čítame *prienik systému* $\mathcal{S}$.

Ak $I = N$, tak namiesto $\bigcup_{i \in I} A_i$ obyčajne píšeme $\bigcup_{i=1}^{\infty} A_i$ alebo $A_1 \cup A_2 \cup \cdots \cup A_n \cup \ldots$; podobne používame zápisy $\bigcap_{i=1}^{\infty} A_i$, resp. $A_1 \cap A_2 \cap \cdots \cap A_n \cap \ldots$.

Ak $I = \{1, 2 \ldots, n\}$, tak namiesto $\bigcup_{i \in I} A_i$ píšeme $\bigcup_{i=1}^{n} A_i$ alebo jednoducho $A_1 \cup A_2 \cup \cdots \cup A_n$. Analogický zmysel majú zápisy $\bigcap_{i=1}^{n} A_i$, $A_1 \cap A_2 \cap \cdots \cap A_n$.

PRÍKLAD 3. Nech pre každé $t \in E^+$ je $A_t = \left(-\infty, \frac{2t+3}{t}\right)$. Ukážte, že

$$\bigcap_{t \in E^+} A_t = (-\infty, 2\rangle.$$

RIEŠENIE. Najprv nepriamo ukážeme, že ak $x \in \bigcap_{t \in E^+} A_t$, tak $x \in (-\infty, 2\rangle$. Predpokladajme, že $x \notin (-\infty, 2\rangle$, t.j., že $x > 2$. Ukážeme, že v tomto prípade existuje $t_0 \in E^+$, pre ktoré $x \notin A_{t_0} = \left(-\infty, \frac{2t_0+3}{t_0}\right)$. Za predpokladu $x > 2$ platí

$$x \geq \frac{2t_0 + 3}{t_0} \quad \Leftrightarrow \quad xt_0 \geq 2t_0 + 3 \quad \Leftrightarrow \quad t_0(x-2) \geq 3 \quad \Leftrightarrow \quad t_0 \geq \frac{3}{x-2}.$$

Teda ak $x > 2$, môžeme zvoliť $t_0 \geq \frac{3}{x-2}$ a potom $x \notin A_{t_0}$, čiže $x \notin \bigcap_{t \in E^+} A_t$.

Dokázali sme, že $\bigcap_{t \in E^+} A_t \subseteq \left(-\infty, \frac{2t+3}{t}\right)$.

Naopak, ak $x \in (-\infty, 2\rangle$, t.j. ak $x \leq 2$, tak pre každé $t \in E^+$ je $x < \frac{2t+3}{t}$ (lebo pre každé $t \in E^+$ je $2 < \frac{2t+3}{t}$), čo znamená, že $x \in \left(-\infty, \frac{2t+3}{t}\right)$ a teda $x \in \bigcap_{t \in E^+} A_t$. Dokázali sme teda aj obrátenú inklúziu, z čoho už vyplýva požadovaná rovnosť.

Odporúčame, aby ste si danú situáciu znázornili na číselnej osi a podrobne si všímali, ako sme pri dôkaze postupovali. □

Nech $I \neq \emptyset$ je množina. Budeme hovoriť, že systém množín A_i, $i \in I$ je disjunktný, ak $\bigcap_{i \in I} A_i = \emptyset$ a budeme hovoriť, že množiny A_i, $i \in I$ sú po dvoch disjunktné, ak pre každé dva navzájom rôzne prvky $i, j \in I$ platí $A_i \cap A_j = \emptyset$.

Ak sú množiny A_i, $i \in I$ po dvoch disjunktné, tak systém množín A_i, $i \in I$ je zrejme disjunktný. Obrátené tvrdenie, ako ukazuje aj nasledujúci príklad, však neplatí.

Príklad 4. Nech pre každé $n \in N$ je $A_n = (n, \infty)$. Potom $\bigcap_{n=0}^{\infty} A_n = \emptyset$. Daný systém je teda disjunktný, ale pre ľubovoľné $m, n \in N$, $m < n$ je $A_m \cap A_n = A_n$, čiže množiny A_i nie sú po dvoch disjunktné. □

V ďalších tvrdeniach uvedieme niektoré dôležité vlastnosti týkajúce sa rozdielu množín.

Veta 4. *Nech A, B sú ľubovoľné množiny. Potom*

$$A - B = A - (A \cap B).$$

Dôkaz. Tvrdenie vyplýva z nasledovného reťazca ekvivalencií: $x \in A - B \Leftrightarrow x \in A \ \& \ x \notin B \Leftrightarrow x \in A \ \& \ x \notin A \cap B \Leftrightarrow x \in A - (A \cap B)$. □

Veta 5 (De Morganove pravidlá). *Nech A, B, C sú ľubovoľné množiny. Potom*

a) $A - (B \cup C) = (A - B) \cap (A - C)$,

b) $A - (B \cap C) = (A - B) \cup (A - C)$.

Dôkaz. Na ukážku urobíme dôkaz tvrdenia b): $x \in A - (B \cap C) \Leftrightarrow x \in A \ \& \ x \notin (B \cap C) \Leftrightarrow x \in A \ \& \ \neg(x \in B \ \& \ x \in C) \Leftrightarrow x \in A \ \& \ (x \notin B \vee x \notin C) \Leftrightarrow (x \in A \ \& \ x \notin B) \vee (x \in A \ \& \ x \notin C) \Leftrightarrow x \in A - B \vee x \in A - C \Leftrightarrow x \in (A - B) \cup (A - C)$. □

Pri elementárnych aplikáciách teórie množín sa najčastejšie stretneme so situáciou, že všetky uvažované množiny sú podmnožinami istej pevne zvolenej (základnej) množiny M (napr. v teórii čísel uvažujeme podmnožiny množiny celých čísel, v planimetrii podmnožiny roviny a pod.). V takých prípadoch často označujeme množinu $M - A$ symbolom A' a nazývame ju doplnkom alebo komplementom množiny A (v množine M). Množinu $A - B$ môžeme napríklad zapísať pomocou komplementu v tvare $A \cap B'$. De Morganove pravidlá môžeme zapísať v nasledovnom tvare.

DÔSLEDOK. *Nech A, B sú ľubovoľné podmnožiny množiny M. Potom*

$$(A \cup B)' = A' \cap B', \qquad (A \cap B)' = A' \cup B'$$

(kde komplementy sa vzťahujú k základnej množine M).

Pri riešení úloh o množinách sú užitočné tzv. množinové diagramy. Predpokladáme, že pre 1, 2, 3 a 4 množiny ich poznáte z predchádzajúceho štúdia. Bude užitočné, ak si jednotlivé tvrdenia týkajúce sa množín budete ilustrovať šrafovaním na množinových diagramoch.

Pomocou operácií rozdielu a zjednotenia sa často zavádza tzv. symetrická diferencia (symetrický rozdiel) množín. *Symetrickou diferenciou* množín A, B nazývame množinu

$$A \triangle B = (A - B) \cup (B - A).$$

VETA 6. *Nech A, B, C sú ľubovoľné množiny. Potom*

a) $A \triangle B = B \triangle A$,

b) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$,

c) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

DÔKAZ. Dôkazy tvrdení a), c) sú jednoduché, pokúste sa ich podrobne zapísať.

Dôkaz časti b). Predpokladáme, že čitateľ si už urobil dôkazy jednoduchších vzťahov, preto (kvôli prehľadnosti) budeme stručnejší. Platí

$$\begin{aligned}
&x \in A\triangle(B\triangle C) \Leftrightarrow (x \in A \ \&\ x \notin B\triangle C) \vee (x \notin A \ \&\ x \in B\triangle C) \Leftrightarrow \\
&[x \in A \ \&\ \neg((x \in B \ \&\ x \notin C) \vee (x \notin B \ \&\ x \in C))]\vee \\
&[(x \notin A \ \&\ ((x \in B \ \&\ x \notin C) \vee (x \notin B \ \&\ x \in C))] \Leftrightarrow \\
&[x \in A \ \&\ (x \notin B \vee x \in C) \ \&\ (x \in B \vee x \notin C)]\vee \\
&(x \notin A \ \&\ x \in B \ \&\ x \notin C) \vee (x \notin A \ \&\ x \notin B \ \&\ x \in C) \Leftrightarrow \\
&(x \in A \ \&\ x \notin B \ \&\ x \notin C) \vee (x \in A \ \&\ x \in C \ \&\ x \in B)\vee \\
&(x \notin A \ \&\ x \in B \ \&\ x \notin C) \vee (x \notin A \ \&\ x \notin B \ \&\ x \in C).
\end{aligned}$$

Analogicky možno ukázať, že $x \in (A\triangle B)\triangle C$ práve vtedy, keď x je prvkom buď všetkých troch množín A, B, C alebo patrí len do jednej z nich (presvedčte sa o tom). Teda platí

$$x \in A\triangle(B\triangle C) \quad \Longleftrightarrow \quad x \in (A\triangle B)\triangle C$$

(znázornite množinový diagram pre množiny A, B, C a postupne vyšrafujte množinu $A\triangle(B\triangle C)$ a množinu $(A\triangle B)\triangle C$). □

Ako už vieme, logické spojky a množinové operácie spolu súvisia. Nech obor pravdivosti výrokovej formy $A(x)$ (nad M) je množina A, obor pravdivosti výrokovej formy $B(x)$ množina B, t.j.

$$A = \{x \in M;\ A(x)\}, \qquad B = \{x \in M;\ B(x)\}.$$

Potom

$$\begin{aligned}
A \cup B &= \{x \in M;\ A(x) \vee B(x)\}, \\
A \cap B &= \{x \in M;\ A(x) \ \&\ B(x)\}, \\
A' &= \{x \in M;\ \neg A(x)\}.
\end{aligned}$$

PRÍKLAD 5. Nech $M = \{0, 1, 2, \ldots, 20\}$. Označme $A = \{x \in M;\ x \leq 18\}$, $B = \{x \in M;\ 3 \mid x\}$. Určte vymenovaním množinu $C = \{x \in M;\ x \leq 18 \implies 3 \mid x\}$.

RIEŠENIE.

$$\begin{aligned} C &= \{x \in M;\ x \leq 18 \implies 3 \mid x\} = \{x \in M;\ x \in A \implies x \in B\} = \\ &= \{x \in M;\ x \notin A \vee x \in B\} = \{19, 20\} \cup \{0, 3, 6, 9, 12, 15, 18\} = \\ &= \{0, 3, 6, 9, 12, 15, 18, 19, 20\}, \end{aligned}$$

využili sme tautológiu $(p \implies q) \iff (\neg p \vee q)$. $\square$

Na záver uvedieme niekoľko informatívnych poznámok, ktoré môže čitateľ vynechať (podrobne sa s tým oboznámi až neskôr).

Slávny Russelov paradox ukazuje, že existujú „veľmi veľké" systémy objektov, ktoré netvoria množiny. V úvode tejto časti oboznámime čitateľa so spomínaným paradoxom.

Nech $\mathcal{S}$ je systém všetkých množín M, ktoré majú vlastnosť $M \notin M$. (Všetky množiny, na ktoré si spomeniete majú túto vlastnosť a teda patria do systému $\mathcal{S}$). Predpokladajme, že systém $\mathcal{S}$ je množinou. Potom buď $\mathcal{S} \in \mathcal{S}$ alebo $\mathcal{S} \notin \mathcal{S}$ (množina $\mathcal{S}$ do systému $\mathcal{S}$ buď patrí alebo nepatrí).

1. Ak $\mathcal{S} \in \mathcal{S}$, tak podľa definície systému $\mathcal{S}$ platí $\mathcal{S} \notin \mathcal{S}$, čo je spor.
2. Ak $\mathcal{S} \notin \mathcal{S}$ tak množina $\mathcal{S}$ má vlastnosť objektov systému $\mathcal{S}$, preto platí $\mathcal{S} \in \mathcal{S}$, opäť spor.

Z uvedeného vyplýva, že systém $\mathcal{S}$ nemôže byť množinou. Pojem množiny teda nezahŕňa tak veľké systémy objektov ako je systém všetkých množín. Pretože ku každej množine A môžeme jednojednoznačne priradiť jednoprvkovú množinu $\{A\}$ je zrejmé, že ani systém všetkých jednoprvkových množín nie je množinou. Pre takéto systémy sa zaviedol pojem trieda (ktorý však kvôli dodržaniu obvyklej terminológie budeme používať v inom zmysle).

Koncom 19. a začiatkom 20. storočia boli formulované aj ďalšie paradoxy, ktoré poukázali, že Cantorovo vymedzenie (charakterizovanie) pojmu množina („množina je súhrn predmetov, vecí dobre rozlíšiteľných našou mysľou alebo intuíciou") je pre korektné matematické úvahy nepostačujúce. Vznikla tzv. kríza teórie množín, ktorej dôsledkom bolo axiomatické vymedzenie základných poznatkov o množinách. Aby ste už teraz získali aspoň približnú predstavu o tom, ktoré poznatky o množinách sú východiskom pri budovaní (rozvíjaní) teórie množín, najznámejšie axiómy teraz uvedieme.

AXIOMA EXTENZIONALITY (ROVNOSTI). Pre každé dve množiny A, B platí (1).

AXIÓMA ZJEDNOTENIA. Nech $\mathcal{S}$ je systém množín. Potom existuje taká množina M, ktorá obsahuje práve tie prvky, ktoré patria aspoň do jednej množiny systému $\mathcal{S}$.

AXIÓMA DVOJICE. Nech a, b sú množiny. Potom existuje množina A, ktorej prvkami sú množiny a, b a ktorá iné prvky nemá, t.j. $A = \{a, b\}$. (V tejto súvislosti upozorňujeme, že v klasickej teórii množín sú prvkami množín kvôli jednoduchosti opäť len množiny.)

ZERMELOVA METAAXIÓMA. Nech $\Gamma(x)$ je výroková forma s jedinou voľnou množinovou premennou x. Potom ku každej množine A existuje množina B tých prvkov $a \in A$, pre ktoré je $\Gamma(a)$ pravdivý výrok. Túto množinu zapisujeme v tvare

$$B = \{x \in A;\ \Gamma(x)\}.$$

(V tomto prípade ide o schému axióm, pre každú konkrétnu výrokovú formu $\Gamma(x)$ ide o jednu axiómu – kvantifikátory v bežnom jazyku sa vzťahujú len na predmetové premenné a nie napríklad na výrokové formy.)

AXIÓMA O PODMNOŽINÁCH. Ku každej množine A existuje taká množina $P(A)$, ktorej prvkami sú práve všetky podmnožiny množiny A.

Okrem uvedených najznámejších axióm, ktoré sú prijaté bez výhrad, niektoré axiomy sú prijaté s výhradami. Napríklad nasledujúca.

AXIÓMA VÝBERU. Nech $\mathcal{S}$ je neprázdny systém neprázdnych navzájom disjunktných množín. Potom existuje taká množina V, že jej prienik s každou množinou $A \in \mathcal{S}$ je jednoprvková množina.

Cvičenia

1. Dané sú množiny $A = \{1,4,5,6\}$, $B = \{3,4,6,7\}$, $C = \{2,5,6\}$. Určte $A \cup B$, $A \cap C$, $C - B$, $A - (C - B)$, $A \cap (B - C)$, $A \triangle B$.

2. Dané sú množiny $A = (1,3\rangle$, $B = \langle 2,5)$. Určte $A \cup B$, $A \cap B$, $B - A$, $A - (A - B)$, $B - (B - A)$, $A - (B - A)$, $B - (A - B)$, $(A - B) \cap (B - A)$, $A \triangle B$.

3. Dokážte, že pre ľubovoľné množiny A, B platí
a) $A \cap (A \cup B) = A$, $\quad A \cup (A \cap B) = A$,
b) $A - B = (A \cup B) - B$,
c) $A - (A - B) = B - (B - A) = A \cap B$,
d) $A - (B - A) = A$,
e) $(A - B) \cap (B - A) = \emptyset$.

4. Určte vymenovaním prvkov množinu
a) $P(\{1\})$, $\quad$ b) $P(\{1,2,3\})$.

5. Dokážte, že pre ľubovoľné množiny A, B, C platí
a) $(A \cup B) - C = (A - C) \cup (B - C)$,
b) $(A \cap B) - C = A \cap (B - C) = (A - C) \cap (B - C)$,
c) $A - (B \cup C) = (A - B) \cap (A - C) = (A - B) - C$,
d) $A - (B \cap C) = (A - B) \cup (A - C)$,
e) $(A - B) \cap C = (A \cap C) - (B \cap C) = (A \cap C) - B$,
f) $A - (B - C) = (A - B) \cup (A \cap C)$,
g) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$,
h) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
i) $(A - B) \times C = (A \times C) - (B \times C)$.

6. a) Dokážte, že pre ľubovoľné množiny A, B platí $P(A \cap B) = P(A) \cap P(B)$.
b) Zistite, či $P(A \cup B) = P(A) \cup P(B)$.

7. Rozhodnite, či pre ľubovoľné množiny A, B, C, D platia nasledujúce rovnosti:
a) $A \times (B \triangle C) = (A \times B) \triangle (A \times C)$,

b) $(A \times B) - (C \times D) = (A - C) \times (B - D)$,
c) $(A \times B) \cup (C \times D) = (A \times C) \cup (B \times D)$.

8. Určte $\bigcup_{t \in T} A_t$, $\bigcap_{t \in T} A_t$, ked'

a) $T = (0, \infty)$, $A_t = \langle -t, t \rangle$,
b) $T = (0, 1)$, $A_t = (t, t + 1)$,
c) $T = E^+$, $A_t = \left(1 - \frac{1}{t}, 2 + \frac{3}{t}\right)$,
d) $T = (0, 2\rangle$, $A_t = \left(1 - \frac{1}{t}, 2 + \frac{3}{t}\right)$,
e) $T = E$, $A_t = \{[x, y] \in E^2;\ x^2 + y^2 \geq t^2\}$,
f) $T = E^+$ $A_t = \{[x, y] \in E^2;\ y = tx^2\}$.

9. Ak pre každé $i \in \{1, 2, \ldots, n - 1\}$ je $A_{i+1} \subseteq A_i$, $B_{i+1} \subseteq B_i$, tak $\bigcap_{i=1}^{n} (A_i \cup B_i) = (\bigcap_{i=1}^{n} A_i) \cup (\bigcap_{i=1}^{n} B_i)$. Dokážte.

10. Dokážte, že pre l'ubovoľné množiny platí

a) $A \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (A \cup A_i)$,
b) $A - \bigcup_{i \in I} A_i = \bigcap_{i \in I} (A - A_i)$.

7. Definície, vety, dôkazy

Pri odovzdávaní (sprístupňovaní) matematických poznatkov, či už písomnom alebo ústnom, sa ustálila určitá forma, ktorú už čitateľ pozná. Zjednodušene ju možno charakterizovať takto: pojmy sa presne vymedzujú a pomenúvajú v *definíciách*, poznatky o nich sa formulujú v *matematických vetách* a ich správnosť sa overuje v *dôkazoch*. Najprv si všimneme zmysel a formu definície.

Definícia je presné určenie (vymedzenie) významu nejakého výrazu (názvu) pomocou výrazov, ktorých význam pokladáme za známy. Určovaný (definovaný) výraz je vlastne nový názov, ktorý dávame definovanému pojmu a nazýva sa *definiendum*. Určujúci výraz, pomocou ktorého pojem vymedzujeme, voláme *definiens*. Oba sú spojené slovne alebo symbolom vyjadrenou *definičnou rovnosťou* alebo *definičnou ekvivalenciou*. O rovnosť ide obyčajne vtedy, keď definujeme „objekt“, o ekvivalenciu spravidla vtedy, keď definujeme nejaký vzťah medzi objektami (keď ide o reláciu).

V učebniciach matematiky pre stredné školy sa môžeme stretnúť s definíciou: „Geometrickým priemerom nezáporných čísel x, y nazývame $\sqrt{x \cdot y}$“. V tejto definícii ide o definičnú rovnosť, ktoré je vyjadrená slovne „nazývame“. Definiendum je názvová (menná) forma „geometrický priemer nezáporných čísel x, y“ a definiens je menná forma (term) „$\sqrt{x \cdot y}$“. V takomto prípade často vyslovujeme definíciu aj v nasledujúcom tvare

„Geometrickým priemerom nezáporných čísel x, y voláme číslo

(a) $$G(x, y) = \sqrt{x \cdot y}“.$$

V tomto prípade sme naviac urobili dohodu, že geometrický priemer nezáporných čísel x, y budeme (stručne) označovať $G(x, y)$ a zdôraznili sme, že hodnoty $G(x, y)$ (t.j. geometrické priemery zvolených čísel) budú opäť čísla. V zápisoch typu (a) sa tiež v matematickej literatúre používa namiesto symbolu $=$ aj symbol $=:$ alebo $=_{df}$ (aby sa zdôraznilo, že ide o definičnú rovnosť).

S definičnou ekvivalenciou sa stretávame v nasledujúcej definícii: „hovoríme, že číslo a delí b a píšeme $a \mid b$, práve vtedy, keď existuje číslo c, o ktorom platí $a \cdot c = b$“. Definičná ekvivalencia je vyjadrená slovne „práve vtedy, keď“. Definiendum je výroková forma „číslo a delí číslo b“ a definiens je výroková forma „existuje číslo c, o ktorom platí $a \cdot c = b$“. V tejto definícii si treba domyslieť, že oborom premenných je množina celých čísel Z (alebo z kontextu, v ktorom je definícia uvedená je jasné, ktorá iná množina je oborom premenných). Uvedenú definíciu možno formulovať aj takto: „Nech a, b sú celé čísla. Potom definujeme

(b) $$a \mid b \iff \exists c \in Z \quad a \cdot c = b“.$$

V takomto prípade si treba uvedomiť, že symbol $\iff$ tu chápeme inak ako vo výrokovom alebo predikátovom počte (aj keď ho čítame rovnako). Ide o spomínanú definičnú ekvivalenciu a preto v takýchto prípadoch niekedy radšej píšeme $\iff_{df}$.

Poznámka. V matematickej literatúre je zvykom používať v takejto definícii namiesto slovného vyjadrenia „práve vtedy, keď“ stručnejšie vyjadrenie „ak“.

Osobitnú formu má tzv. *definícia indukciou*. Ak $V(n)$ je názvová forma s voľnou premennou n, ktorej oborom je množina $\{k \in N;\ k \geq n_0\}$, pričom n_0 je určité číslo z N (často $n_0 = 0$ alebo $n_0 = 1$), zvykneme zmysel výrazu $V(n)$ definovať takto:

1. definujeme $V(n_0)$,
2. pre $n > n_0$ definujeme $V(n)$ pomocou $V(n-1)$.

Napríklad mocninu a^n, pričom $a \in E$, môžeme pre exponenty $n \in N^+$ definovať takto:

1. $a^1 = a$,
2. $a^n = a^{n-1} \cdot a$, pre $n > 1$.

Od všetkých definícií požadujeme, aby boli presné (jednoznačne stanovili rozsah) a adekvátne (aby pokiaľ možno čo najlepšie vyjadrovali naše intuitívne predstavy o pojme). Najmä v novších matematických teóriách (akou je napr. teória množín) nie sú v rôznych učebniciach vymedzené tie isté pojmy rovnako. Preto pri štúdiu matematickej literatúry si treba definície aj „známych pojmov" starostlivo všímať. Sú to v podstate len dohovory medzi autorom knihy, ktorú práve študujete a vami, ako jej čitateľom.

Matematické vety (tvrdenia) vyjadrujú dôležité vlastnosti matematických objektov a ich vzájomné vzťahy a súvislosti. Základné matematické tvrdenia, z ktorých vychádza ľubovoľná oblasť matematiky sú axiómy uvedené v kapitole 6 (tzv. axiómy teórie množín) a prípadne niekoľko ďalších axióm patriacich danej oblasti (ak napr. tou oblasťou je geometria, tak geometrických axióm). Budovanie danej oblasti matematiky (matematickej teórie) spočíva v tom, že sa z axióm pomocou logických pravidiel odvádzajú (dokazujú) nové tvrdenia – matematické vety. Ony vlastne tvoria danú matematickú teóriu. Preto aj v centre našej pozornosti budú predovšetkým (matematické) vety a ich dôkazy.

Vety, ktoré majú význam hlavne z hľadiska ich využívania v dôkazoch ďalších viet, ale samy o sebe nevyjadrujú obzvlášť dôležité (alebo zaujímavé) tvrdenia sa obyčajne nazývajú lemy. Forma viet najčastejšie zodpovedá uzavretým formulám predikátového počtu.

Pri dôkazoch využívame tzv. odvodzovacie pravidlá. Jedno z nich je známe pravidlo odlúčenia (modus ponens):

(a) $$\frac{A,\ A \implies B}{B}.$$

Tento zápis čítame takto: ak výroky (môže sa jednať aj o kvantifikované výroky) A a $A \implies B$ sú pravdivé, tak aj výrok B je pravdivý. Ďalšie často používané odvodzovacie pravidlá sú

(b) $$\frac{A \implies B,\ B \implies C}{A \implies C}$$

a jeho zovšeobecnenie

(c) $$\frac{A_1 \implies A_2,\ A_2 \implies A_3,\ \ldots,\ A_{k-1} \implies A_k}{A_1 \implies A_k}.$$

Pri priamom dôkaze tvrdenia $A \implies B$ (t.j. výroku v tvare implikácie) postupujeme takto: Vyhľadáme reťazec platných implikácií (môžu to niekedy byť napr. dôsledkové úpravy nerovnosti) $A \implies B_1, B_1 \implies B_2, \ldots, B_n \implies B$. Z (c) potom vyplýva, že platí $A \implies B$.

S tvrdením $A \implies B$ je ekvivalentné tvrdenie $\neg B \implies \neg A$. Dôkaz tvrdenia $\neg B \implies \neg A$ sa volá nepriamym dôkazom tvrdenia $A \implies B$.

Pri priamom dôkaze tvrdenia V (výroku, ktorý ktorý nie je vyjadrený v tvare implikácie) postupujeme takto: Zvolíme (vyhľadáme) vhodný pravdivý výrok A. Odvodíme (pomocou reťazca implikácií), že platí $A \implies V$. Z (a) potom vyplýva, že platí V.

V matematike používame aj tzv. dôkazy sporom. Ich východiskom je odvodzovacie pravidlo

$$\text{(d)} \qquad \frac{\neg A \implies B,\ \neg B}{A}.$$

Pri dôkaze sporom predpokladáme, že tvrdenie A, ktoré treba dokázať neplatí (t.j. platí $\neg A$). Odvodíme (pomocou reťazca implikácií), že platí $\neg A \implies B$, pričom o B vieme, že je nepravdivé (t.j. $\neg B$ je pravdivé). Z (d) potom vyplýva, že platí A.

Pri dôkaze tvrdenia typu $A \iff B$ dokážeme $A \implies B$ aj $B \implies A$. Niekedy sa však v takomto prípade dajú dokazovať obidve implikácie súčasne.

Pri dôkaze tvrdenia typu $A_1 \iff A_2 \iff \cdots \iff A_n$ stačí napríklad ukázať $A_1 \implies A_2 \implies \cdots \implies A_n \implies A_1$ (niekedy tomu hovoríme *kruhový dôkaz*).

Ak platí, že z A vyplýva B hovoríme, že A je *postačujúca podmienka* pre B a že B je *nutná podmienka* pre A. Napr. „$6 \mid x$“ je postačujúca (ale nie nutná) podmienka pre „$2 \mid x$“ a „$2 \mid x$“ je nutná (ale nie postačujúca) podmienka pre „$6 \mid x$“. Nutnou a postačujúcou podmienkou pre „$6 \mid x$“ je „$2 \mid x \wedge 3 \mid x$“.

Podrobnejšie sa o rôznych typoch dôkazov môžete dozvedieť napr. v učebnici [29] alebo v [14]. Všetky spomenuté typy dôkazov, ich rôzne varianty a kombinácie (včítane matematickej indukcie, o ktorej sme hovorili už v prvej kapitole) nájdete aj v týchto skriptách a budú vás samozrejme sprevádzať počas celého štúdia, lebo to (alebo lepšie povedané aj to) je matematika.

8. Binárne relácie

Pripomeňme si, že binárnou reláciou nazývame ľubovoľnú množinu usporiadaných dvojíc. Definičným oborom relácie R (alebo prvým oborom relácie R) nazývame množinu $\mathcal{D}(R) = \{a; \exists b\, [a,b] \in R\}$. Množinu $\mathcal{H}(R) = \{b; \exists a\, [a,b] \in R\}$ nazývame obor hodnôt (alebo druhý obor) relácie R.

Nech A, B sú množiny a R binárna relácia (ďalej stručne len relácia). Ak $\mathcal{D}(R) \subseteq A$ a $\mathcal{H}(R) \subseteq B$ hovoríme (ako sme už poznamenali v kapitole 3), že R je relácia z množiny A do B. Ak R, S sú relácie z A do B, tak zrejme aj $R \cup S$, $R \cap S$, $R - S$ sú relácie z A do B.

Definícia 1. Nech R je relácia. Reláciu

$$R^{-1} = \{[a,b]; [b,a] \in R\}$$

nazývame inverzná relácia k relácii R.

Príklad 1. a) Nech $R = \{[1,1],[1,2],[2,3],[1,3]\}$. Potom
$R^{-1} = \{[1,1],[2,1].[3,2],[3,1]\}$.

b) Nech $R = \{[x,y] \in E^2; x^2 + y > x - y^2 + 1\}$. Potom
$R^{-1} = \{[x,y] \in E^2; y^2 + x > y - x^2 + 1\} = \{[y,x] \in E^2; x^2 + y > x - y^2 + 1\}$.

c) Nech $R = \{[a,b] \in E^2; b = 2a + 1\}$. Potom
$R^{-1} = \{[a,b] \in E^2; a = 2b + 1\}$ alebo $R^{-1} = \left\{[a,b] \in E^2; b = \frac{a-1}{2}\right\}$.

d) Nech $R = \{[x,y] \in E^2; y = \log(x+3)\}$. Potom
$R^{-1} = \{[x,y] \in E^2; x = \log(y+3)\}$ alebo $R^{-1} = \{[x,y] \in E^2; y = 10^x - 3\}$. □

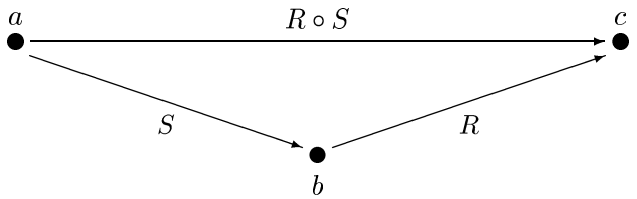
Zrejme platí $\left(R^{-1}\right)^{-1} = R$. Ďalej, ak R je relácia z množiny A do B, tak R^{-1} môžeme pokladať za reláciu z množiny B do A a naviac $\mathcal{D}(R) = \mathcal{H}(R^{-1})$, $\mathcal{H}(R) = \mathcal{D}(R^{-1})$ (podrobne si to premyslite).

Definícia 2. Nech R, S sú relácie. Reláciu

$$R \circ S = \{[a,c]; \exists b \quad [a,b] \in S \wedge [b,c] \in R\}$$

nazývame zloženou reláciou z relácie R a relácie S.

Reláciu $R \circ S$ môžeme schematicky znázorniť takto:



Reláciu $R \circ S$ často zapisujeme (najmä v algebre) v tvare $R \cdot S$ alebo stručne RS a vtedy ju nazývame *súčinom* relácie R a relácie S.

Poznámka. V niektorej literatúre sa definuje relácia $R \circ S$ takto:

$$R \circ S = \{[a,c]; \exists b \quad [a,b] \in R \wedge [b,c] \in S\}.$$

Binárne relácie sú obyčajne dané ako obory pravdivosti výrokových foriem s dvomi premennými.

PRÍKLAD 2. Nech $R = \{[x,y] \in E^2;\ y = x^2 + 1\}$, $S = \{[x,y] \in E^2;\ y = 3x\}$. Potom

$$R \circ S = \{[x,y] \in E^2;\ y = 9x^2 + 1\}, \quad S \circ R = \{[x,y] \in E^2;\ y = 3x^2 + 3\}.$$

VETA 1. *Pre ľubovoľné relácie R, S, T platí:*

a) $(R \circ S) \circ T = R \circ (S \circ T)$ *(asociatívny zákon),*

b) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

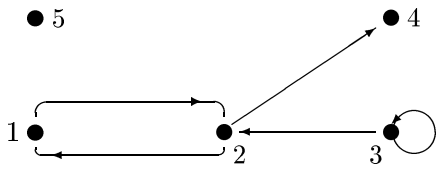
DÔKAZ. $[a,b] \in (R \circ S) \circ T \Leftrightarrow \exists c\, [a,c] \in T \wedge [c,b] \in R \circ S \Leftrightarrow \exists c,d\ [a,c] \in T \wedge [c,d] \in S \wedge [d,b] \in R \Leftrightarrow \exists d\, [a,d] \in S \circ T \wedge [d,b] \in R \Leftrightarrow [a,b] \in R \circ (S \circ T)$.

Druhú rovnosť možno dokázať podobne. □

Relácie často znázorňujeme pomocou *orientovaných grafov* alebo *karteziánskych grafov*. Karteziánske grafy pozná čitateľ z predchádzajúceho štúdia. Preto si pripomenieme len konštrukciu uzlového grafu. Uzlový graf relácie R z množiny A do B zostrojíme takto:

1. Každému prvku množiny $A \cup B$ priradíme v nákresni krúžok.
2. Ak $[a,b] \in R$, $a \neq b$, tak zostrojíme šípku (orientovanú hranu) idúcu od obrazu prvku a (od krúžku priradeného prvku a) k obrazu prvku b.
3. Ak $[a,a] \in R$, tak zostrojíme šípku (tzv. slučku) idúcu od obrazu prvku a opäť k obrazu prvku a.

PRÍKLAD 3. Relácia $R = \{[1,2],[2,1],[2,4],[3,2],[3,3]\}$, ktorá je definovaná na množine $A = \{1,2,3,4,5\}$, má graf na nasledovnom obrázku.



Obr.

□

Uvedomte si, že pomocou uzlového grafu je možné binárnu reláciu aj definovať (zadať).

Ak R je relácia na množine A, tak aj $R' = A^2 - R$ je relácia na A. Reláciu R' nazývame *doplnkovou (komplementárnou)* reláciou k relácii R na množine A.

Identickou (diagonálnou) reláciou na množine A nazývame reláciu

$$\triangle_A = \{[a,a];\ a \in A\}.$$

VETA 2. *Ak R je relácia z A do B, tak $R \circ \triangle_A = \triangle_B \circ R = R$.*

DÔKAZ. Nech $[x,y] \in R \circ \triangle_A$. Potom existuje z, že $[x,z] \in \triangle_A$, $[z,y] \in R$. Z toho dostávame, že $x = z$, teda $[x,y] \in R$, z čoho vyplýva $R \circ \triangle_A \subseteq R$.

Nech $[x,y] \in R$. Pretože $[x,x] \in \triangle_A$, tak $[x,y] \in R \circ \triangle_A$, čo znamená, že aj $R \subseteq R \circ \triangle_A$.

Druhá rovnosť sa dokáže analogicky. □

Relácie môžu mať rôzne špeciálne vlastnosti. S najdôležitejšími z nich sa teraz oboznámime.

DEFINÍCIA 3. Nech R je relácia na množine A. Hovoríme, že relácia R je

a) reflexívna na A, ak
$\forall a \in A \quad aRa$,
b) symetrická, ak
$\forall a, b \in A \quad aRb \implies bRa$,
c) tranzitívna, ak
$\forall a, b, c \in A \quad aRb \wedge bRc \implies aRc$,
d) antisymetrická, ak
$\forall a, b \in A \quad aRb \wedge bRa \implies a = b$,
e) ireflexívna (antireflexívna), ak
$\forall a \in A \quad aR'a$,
f) súvislá, ak
$\forall a, b \in A \quad a \neq b \implies aRb \vee bRa$,
g) trichotomická, ak pre každé dva prvky $a, b \in A$ platí práve jeden zo vzťahov aRb, $a = b$, bRa (t.j. ak je ireflexívna, antisymetrická a súvislá).

Z tautológií T8 a T5 z kapitoly 4 vyplýva, že relácia R je antisymetrická práve vtedy, keď o nej platí

$$\forall a, b \in A \quad a \neq b \implies aR'b \vee bR'a$$

(t.j. ak a, b sú rôzne prvky, tak platí najviac jeden zo vzťahov aRb, bRa).
V nasledujúcich dvoch príkladoch budeme ilustrovať ako odôvodníme, že daná relácia nejakú vlastnosť nemá (t.j. ako dokážeme, neplatnosť všeobecného výroku), resp. ako postupovať pri dôkazoch vlastností relácie (t.j. ako dokazovať platnosť všeobecného výroku).

PRÍKLAD 4. Zistite, ktorú z vlastností a) – f) (z definície 3) má relácia

$$R = \{[x, y] \in Z^2;\ x \geq 2y - 1\}.$$

RIEŠENIE. Relácia R nie je reflexívna, lebo napr. $[2, 2] \notin R$. Nie je symetrická, lebo napr. $[1, 0] \in R$, ale $[0, 1] \notin R$. Nie je tranzitívna, lebo napr. $[-2, -1] \in R$ aj $[-1, 0] \in R$, ale $[-2, 0] \notin R$. Nie je antisymetrická, lebo napr. $[-1, 0] \in R$ aj $[0, -1] \in R$. Nie je ireflexívna, lebo napr. $[0, 0] \in R$. Nie je súvislá, lebo napr. $[4, 3] \notin R$, $[3, 4] \notin R$. □

PRÍKLAD 5. Dokážte, že relácia $S = \{[x, y] \in N^2;\ x \geq 2y - 1\}$ je a) tranzitívna, b) antisymetrická.

RIEŠENIE. a) Nech $[x, y] \in S$, $[y, z] \in S$. Potom $x \geq 2y - 1$, $y \geq 2z - 1$. Po úprave dostávame, že $x \geq 2y - 1$, $2y - 1 \geq 4z - 3$, teda $x \geq 4z - 3$ (lebo relácia $\geq$ je tranzitívna).

1. Ak $z \geq 1$, tak $4z - 3 \geq 2z - 1$ (podrobne sa presvedčte) a z tranzitívnosti relácie $\geq$ vyplýva, že $x \geq 2z - 1$.
2. Ak $z = 0$, tak pre každé $x \in N$ je $x \geq 2z - 1 = -1$.

Z 1. a 2. vyplýva, že ak $[x, y] \in S$, $[y, z] \in S$, tak aj $[x, z] \in S$ a relácia S je teda tranzitívna.

b) Nech $[x, y] \in S$ a $[y, x] \in S$. Potom $x \geq 2y - 1$ a $y \geq 2x - 1$. Z toho vyplýva, že $x \geq 2y - 1$ a $2y - 1 \geq 4x - 3$, t.j. $x \geq 4x - 3$, teda $x \leq 1$. Analogicky dostaneme $y \leq 1$.

Ak $x = 1$, $y = 0$ neplatí $[y, x] \in S$, ak $x = 0$, $y = 1$ neplatí $[x, y] \in S$. Teda z predpokladu $[x, y] \in S$ a $[y, x] \in S$ vyplýva, že buď $x = y = 1$ alebo $x = y = 0$. □

Z mnohými zo známych relácií a s ich vlastnosťami ste sa už stretli. Napríklad relácia $\perp$ (kolmosti) na množine všetkých priamok zvolenej roviny je symetrická a ireflexívna. Žiadnu z ďalších menovaných vlastností nemá. Relácia $|$ (byť deliteľom) na množine N je reflexívna, tranzitívna a antisymetrická. Ďalšie zo spomínaných vlastností nemá.

VETA 3. *Nech R je binárna relácia na množine A. Potom*
a) R je reflexívna práve vtedy, keď $\triangle_A \subseteq R$,
b) R je symetrická práve vtedy, keď $R = R^{-1}$,
c) R je tranzitívna práve vtedy, keď $R \circ R \subseteq R$,
d) R je antisymetrická práve vtedy, keď $R \cap R^{-1} \subseteq \triangle_A$,
e) R je ireflexívna práve vtedy, keď $R \cap \triangle_A = \emptyset$,
f) R je súvislá práve vtedy, keď $A^2 - \triangle_A \subseteq R \cup R^{-1}$.

DÔKAZ. Uvedieme dôkaz časti c). Ostatné časti dôkazu prenechávame čitateľovi ako cvičenie.

c) Nech R je tranzitívna relácia a nech $[x, y] \in R \circ R$. Potom existuje $z \in A$, že $[x, z] \in R$, $[z, y] \in R$. Pretože R je tranzitívna, tak $[x, y] \in R$. Dokázali sme, že $R \circ R \subseteq R$.

Nech $R \circ R \subseteq R$ a nech $[x, y] \in R$, $[y, z] \in R$. Potom je $[x, z] \in R \circ R \subseteq R$, teda R je tranzitívna relácia. □

Nech R je relácia na množine A a nech $B \subseteq A$. Potom $R \cap B^2$ je zrejme relácia na množine B. Nazývame ju *zúženie (reštrikcia)* relácie R na množinu B a označujeme $R \restriction B$ alebo R_B alebo (ak nehrozí nedorozumenie) tiež písmenom R.

PRÍKLAD 6. Nech $\mid$ je relácia delí na množine N. Jej zúžením na množinu $M = \{1, 2, 3, 6\}$ je relácia

$$\triangle_M \cup \{[1, 2], [1, 3], [1, 6], [2, 6], [3, 6]\}.$$

□

Jednoduchý dôkaz nasledovného tvrdenia prenechávame čitateľovi ako cvičenie.

VETA 4. *Nech R je relácia na množine A a nech R_B je jej zúženie. Ak relácia R má niektorú z vlastností a) – g) (uvedených v definícii 3), tak tú istú vlastnosť má aj relácia R_B (chápaná ako relácia na množine B) aj relácia R^{-1}.*

Cvičenia

1. Na množine $\{1, 2, 3, 4, 5, 6\}$ sú dané relácie R, S takto:

$$R = \{[1, 2], [2, 3], [3, 1], [4, 5], [5, 5], [6, 6]\},$$
$$S = \{[1, 6], [2, 4], [3, 5], [4, 2], [4, 4], [5, 3], [5, 5], [6, 1]\}.$$

a) Nakreslite uzlový a karteziánsky graf relácií R, S.
b) Určte (vymenovaním prvkov aj graficky) relácie R^{-1}, S^{-1}.
c) Určte relácie $R \circ S$, $S \circ R$, $S \circ R^{-1}$, $R \circ S^{-1}$, $(R \circ S)^{-1}$, $S^{-1} \circ R^{-1}$.

2. Načrtnite karteziánske grafy nasledovných relácií:
a) $R = \{[x, y] \in E^2;\ \log xy \leq 0 \ \ \& \ \ |y| < x + 1\}$,
b) $R = \{[x, y] \in E^2;\ y \leq |x^2 - |x| - 2| \ \ \& \ \ x^2 + y^2 \leq 4\}$,
c) $R = \{[x, y] \in Z^2;\ \frac{x+y}{x} \in Z\}$.

3. Nech $A = \{a, b, c\}$. Daná je relácia $R = \{[X, Y] \in (P(A))^2;\ X \subseteq Y\}$ (t.j. relácia inklúzie množín na $P(A)$). Nakreslite jej uzlový graf a zistite jej vlastnosti.

4. Nájdite všetky relácie na množine $\{a, b\}$ a určte ich vlastnosti.

5. Ukážte, že na každej množine, ktorá má aspoň dva prvky existujú také relácie R, S, že $R \circ S \neq S \circ R$.

6. Dokážte, že

a) ak relácie R, S sú na množine A reflexívne, tak aj relácia $R \circ S$ je reflexívna,

b) ak relácie R, S sú symetrické, tak relácia $R \circ S$ nemusí byť symetrická.

7. Nech $A = \{n \in N;\ n < 10\}$, $B = \{n \in N;\ n \geq 12\}$,
$R = \{[m, n] \in A \times B;\ m + 1 = n\}$, $S = \{[m, n] \in A \times B;\ m^2 = n\}$.

a) Zapíšte relácie R, S vymenovaním prvkov.

b) Zostrojte uzlové grafy relácií R, S.

c) Určte (vymenovaním prvkov) relácie $R \circ S$ a $S \circ R$.

8. Nech $R = \{[x, y] \in E^2;\ y = 2x\}$, $S = \{[x, y] \in E^2;\ y = x^2\}$,
$T = \{[x, y] \in E^2;\ y = \sqrt{x}\}$.

a) Zostrojte karteziánske grafy relácií R, S, T.

b) Určte relácie $R \circ S$, $S \circ R$, $S \circ T$, $R \circ T$, $T \circ R$, $T \circ S$.

c) Zostrojte karteziánske grafy relácií nájdených v predchádzajúcej časti.

9. Dokážte, že pre ľubovoľné relácie platí

a) $R \circ (S \cup T) = R \circ S) \cup R \circ T$,

b) $(R - S)^{-1} = R^{-1} - S^{-1}$,

c) $(R^{-1})^{-1} = R$, $(R')^{-1} = (R^{-1})'$ (pričom $R \subseteq A^2$),

d) $R \circ (\bigcup_{i \in I} S_i) = \bigcup_{i \in I} R \circ S_i$, $(\bigcup_{i \in I} R_i)^{-1} = \bigcup_{i \in I} R_i^{-1}$.

10. a) Ukážte, že pre ľubovoľné relácie R, R_1, R_2, S, S_1, S_2 platia nasledujúce vzťahy:

$R \circ (S_1 \cap S_2) \subseteq R \circ S_1 \cap R \circ S_2$,

$(R_1 \cap R_2) \circ S \subseteq R_1 \circ S \cap R_2 \circ S$,

$R \circ S_1 - R \circ S_2 \subseteq R \circ (S_1 - S_2)$.

b) Ukážte, že v uvedených vzťahoch nemožno (pre ľubovoľné relácie) nahradiť inklúziu rovnosťou.

11. Zistite, aké vlastnosti majú nasledovné relácie:

a) $R = \{[x, y] \in Z^2;\ x^2 = y\}$,

b) $R = \{[x, y] \in Z^2;\ |x - y| \geq 3\}$,

c) $R = \{[x, y] \in E^2;\ x^2 + y^2 - 1\}$.

12. Dokážte, že o ľubovoľnej relácii R platí:

a) $R \circ R^{-1}$ je symetrická relácia.

b) Ak R je tranzitívna a ireflexívna, tak R je antisymetrická.

13. Na množine $M = \{1, 2, 3\}$ je daná relácia $R = \{[1, 1], [1, 2], [2, 3]\}$. Určte najmenšiu (vzhľadom na inklúziu) reláciu S na M, o ktorej platí

a) $R \subseteq S$ a S je reflexívna aj symetrická,

b) $R \subseteq S$ a S je tranzitívna.

14. Na množine $M = \{0, 1, 2\}$ definujte (vymenovaním) reláciu, ktorá

a) je reflexívna a tranzitívna, ale nie je symetrická,

b) ktorá je reflexívna a symetrická, ale nie je tranzitívna,

c) ktorá je súvislá, tranzitívna a nerovná sa M^2.

15. Ak R_i, $i \in I$, je systém relácií, ktoré majú niektorú z vlastností reflexívnosť, symetričnosť, tranzitívnosť, tak ju má aj relácia $\bigcap_{i \in I} R_i$. Dokážte.

16. Dokážte, že ak sú relácie R, S reflexívne na A, tak aj relácia $R \circ S$ je reflexívna na A. Ukážte, že pre symetrické a tranzitívne relácie analogická vlastnosť neplatí.

17. Nech množina A má n prvkov, $n > 1$. Určte počet
a) všetkých relácií na A,
b) všetkých reflexívnych relácií na A,
c) všetkých symetrických relácií na A.

9. Zobrazenia

Pripomeňme si, že binárnu reláciu f, $f \subseteq A \times B$, nazývame zobrazenie (z A do B), keď o nej platí

$$[a,b] \in f \wedge [a,c] \in f \implies b = c. \tag{1}$$

Ak relácia f je zobrazením z A do B, tak píšeme $f : A \xrightarrow{z} B$.

Nech f je zobrazenie a nech $M \subseteq \mathcal{D}(f)$. Potom označíme

$$f(M) = \{b; \exists a \in M \quad f(a) = b\} = \{f(a); a \in M\}.$$

Množinu $f(M)$ nazývame obraz množiny M v zobrazení f. Ak $P \subseteq \mathcal{H}(f)$, tak označíme

$$f_{-1}(P) = \{a; \exists b \in P \quad f(a) = b\} = \{a; f(a) \in P\}.$$

Množinu $f_{-1}(P)$ nazývame (úplný) vzor množiny P v zobrazení f. Ak $P = \{b\}$, tak namiesto $f_{-1}(\{b\})$ stručne píšeme $f_{-1}(b)$.

Príklad 1. Ak $f = \{[x,y] \in E^2; y = x^2\}$, tak $f(\langle 0,2\rangle) = \langle 0,4\rangle$, $f_{-1}(\langle 0,4\rangle) = \langle -2,2\rangle$. □

Ak je binárna relácia f daná (podobne ako v predchádzajúcom príklade) ako obor pravdivosti výrokovej formy dvoch (voľných) premenných, t.j.

$$f = \{[x,y] \in A \times B; V(x,y)\},$$

tak podmienku (1) môžeme zapísať v tvare

$$V(x,y_1) \wedge V(x,y_2) \implies y_1 = y_2. \tag{2}$$

Príklad 2. Nech $f = \{[x,y] \in E^2; yx + 2 = x - 3y\}$. Určte prvý a druhý obor relácie f a zistite, či f je zobrazenie.

Riešenie. Po úprave výrokovej formy $yx+2 = x-3y$ dostávame $y(x+3) = x-2$. Pre $x \neq -3$ je $y = \frac{x-2}{x+3}$. Znamená to, že $\mathcal{O}_1(f) = \mathcal{D}(f) = E - \{-3\}$. Podobne môžeme ukázať (ak vyjadríme x) že $\mathcal{H}(f) = E - \{1\}$.

Pretože $y = \frac{x-2}{x+3}$ (pre $x \neq -3$) je zrejme relácia f zobrazením. □

Zobrazenie je obyčajne dané niektorým z týchto spôsobov:

1. Vymenovaním, napríklad $f = \{[0,0],[1,0],[2,1]\}$.
2. Definičným oborom a predpisom (pravidlom), ktorý ku každému prvku z definičného oboru priraďuje práve jeden prvok, napríklad
   $\mathcal{D}(g) = N, \quad \forall n \in N \quad g(n) = n^2$.
3. Výrokovou formou dvoch premenných, pričom sú určené (alebo sú známe z kontextu) obory premenných a to, ktorá z nich je tzv. nezávisle premenná a ktorá je závisle premenná, napríklad:
   a) $yx + 2 = x - 3y$, $x, y \in E$, x je nezávisle premenná,
   b) $h : E \xrightarrow{z} E$, $st + 2 = t - 3s$, t je nezávisle premenná.

POZNÁMKA. Ak v ďalšom texte určíme zobrazenie výrokovou formou $V(x,y)$ a explicitne neuvedieme obory premenných budeme predpokladať (ako v stredoškolskej matematike), že $\mathcal{O}(x) = \mathcal{O}(y) = E$, a že nezávisle premennou je premenná x.

V literatúre sa môžu samozrejme vyskytnúť aj rôzne obmeny spomenutých zápisov zobrazení.

Zobrazenie (v zmysle uvedenom v tomto texte) je množina, teda zobrazenia f, g sa rovnajú, ak obsahujú tie isté usporiadané dvojice, t.j.

$$f = g \iff \mathcal{D}(f) = \mathcal{D}(g) \wedge \forall x \in \mathcal{D}(f)\, f(x) = g(x). \tag{3}$$

DEFINÍCIA 1. Nech $f : A \xrightarrow{z} B$. Ak platí $\mathcal{H}(f) = B$, hovoríme, že f je zobrazenie z množiny A na množinu B. Ak $\mathcal{D}(f) = A$ hovoríme, že f je zobrazenie množiny A do množiny B a píšeme $f : A \to B$. Ak $\mathcal{D}(f) = A$ a $\mathcal{H}(f) = B$ hovoríme, že f je zobrazenie množiny A na B alebo, že f je surjekcia (množiny A na B).

Zobrazenie $f : A \to B$ je teda surjekcia, ak

$$\forall b \in B\, \exists a \in A \qquad f(a) = b.$$

Upozorňujeme čitateľa, že podľa predchádzajúcej definície je každé zobrazenie množiny A aj zobrazením z množiny A (pretože $\mathcal{D}(f) = A \implies \mathcal{D}(f) \subseteq A$) a každé zobrazenie na množinu B je aj zobrazením do množiny B (lebo $\mathcal{H}(f) = B \implies \mathcal{H}(f) \subseteq B$). Napríklad funkcia $y = \sqrt{x-1}$ je zobrazenie z E do E, funkcia $y = x^2 - 1$ je zobrazenie E do E (teda aj z E do E), atď. V ďalšom texte sa obmedzíme hlavne na zobrazenie A do B.

DEFINÍCIA 2. Nech $f : A \to B$. Ak

$$\forall a, b \in A \qquad a \neq b \implies f(a) \neq f(b)$$

hovoríme, že f je prosté zobrazenie (alebo, že f je injekcia).

Napríklad funkcia $y = 2^x$ je prosté zobrazenie, ale funkcia $y = x^2$ nie je prosté zobrazenie.

PRÍKLAD 3. Daná je funkcia $f : E - \{1\} \to E$, $y = \frac{|x|}{1-x}$. Určte obor hodnôt a zistite, či f je injekcia.

RIEŠENIE. Ak $1 \neq x \geq 0$, tak $y = \frac{x}{1-x}$ a po úprave dostávame $x = \frac{y}{y+1}$. Pretože $1 \neq \frac{y}{y+1} \geq 0$ dostávame $y \in (-\infty, -1) \cup \langle 0, \infty)$. Analogicky sa môžeme presvedčiť, že ak $x < 0$, tak $y \in (0, 1)$. Znamená to, že

$$\mathcal{H}(f) = (-\infty, -1) \cup \langle 0, \infty) \cup (0, 1) = (-\infty, -1) \cup \langle 0, \infty).$$

Predpokladajme, že $f(a) = f(b)$, t.j. $\frac{|a|}{1-a} = \frac{|b|}{1-b}$.

Ak $a \geq 0$ aj $b \geq 0$ tak po úprave dostávame $a = b$.

Ak $a < 0$ aj $b < 0$ tak opäť dostávame $a = b$.

Ak napr. $a \geq 0$, $b < 0$, tak $\frac{a}{1-a} = \frac{-b}{1-b}$ a po úprave dostávame $a = \frac{b}{2b-1}$ (pre $b \neq \frac{1}{2}$). Ak zvolíme napríklad $b = -1$, tak $a = \frac{1}{3}$ a $f(-1) = f(\frac{1}{3}) = \frac{1}{2}$, čo znamená, že f nie je injekcia. □

DEFINÍCIA 3. Ak zobrazenie $f : A \to B$ je injekcia aj surjekcia hovoríme, že f je bijekcia A na B.

PRÍKLAD 4. Nech $A = \{3a + 1; a \in Z\}$, $B = \{5a + 3; a \in Z\}$. Zistite, či zobrazenie $f = \{[x, y] \in A \times B; y = \frac{5x+4}{3}\}$ je bijekcia A na B.

RIEŠENIE. a) Ak $x \in A$, tak existuje $a \in Z$, že $x = 3a + 1$ a potom $y = \frac{5(3a+1)+4}{3} = 5a + 3 \in B$, teda f je zobrazenie množiny A do B.

b) Zo vzťahu $y = \frac{5x+4}{3}$ vyplýva $x = \frac{3y-4}{5}$. Ak $y \in B$, tak existuje $a \in Z$, že $y = 5a + 3$ a vtedy $x = \frac{3y-4}{5} = \frac{3(5a+3)-4}{5} = 3a + 1 \in A$, t.j. ľubovoľné číslo $y = 5a + 3 \in B$ má vzor $x = 3a + 1 \in A$, preto f je surjekcia.

c) Ak $f(x_1) = f(x_2)$, t.j. $\frac{5x_1+4}{3} = \frac{5x_2+4}{3}$, tak $x_1 = x_2$, teda f je injekcia (použili sme obmenu podmienky z definície 2). □

Ak relácia f je zobrazenie a $X \subseteq \mathcal{D}(f)$, tak jej zúženie $f \restriction X$ na množinu X je zrejme opäť zobrazenie. Nazývame ho *parciálne* zobrazenie k f na množine X. Napríklad zúžením funkcie $y = 2x$ na množinu N je postupnosť $(0, 2, 4, \dots, 2n, \dots)$, zúženie funkcie $y = \cos x$ (ktorá nie je prostá) na interval $\langle 0, \pi \rangle$ je prostá funkcia.

VETA 1. *Ak binárne relácie f, g sú zobrazenia, tak aj $f \circ g$ je zobrazenie a pre každé $x \in \mathcal{D}(f \circ g)$ platí*

$$(f \circ g)(x) = f(g(x)). \tag{3}$$

DÔKAZ. Nech $[a, b] \in f \circ g$ aj $[a, c] \in f \circ g$. Potom existujú prvky d, e, o ktorých platí

$$[a, d] \in g, \quad [d, b] \in f, \quad [a, e] \in g, \quad [e, c] \in f.$$

Keďže g je zobrazenie, tak $d = e$ a pretože aj f je zobrazenie, tak $b = c$.

Rovnosť (3) vyplýva z nasledovného reťazca ekvivalencií: $(f \circ g)(x) = y \Leftrightarrow [x, y] \in f \circ g \Leftrightarrow \exists z\, [x, z] \in g, [z, y] \in f \Leftrightarrow \exists z\, g(x) = z, f(z) = y \Leftrightarrow f(g(x)) = y$. □

Ak f, g sú zobrazenia, tak zobrazenie $f \circ g$ nazývame *zložené zobrazenie* alebo *kompozícia zobrazení*. Zobrazenie f voláme *vonkajšia zložka* a zobrazenie g *vnútorná zložka* zloženého zobrazenia $f \circ g$.

PRÍKLAD 5. Nech f, g sú funkcie, $f(x) = 2x - 1$, $g(x) = 1 - x^2$. Potom

$$(f \circ g)(x) = 2(1 - x^2) - 1 = 1 - 2x^2,$$
$$(g \circ f)(x) = 1 - (2x - 1)^2 = 4x - 4x^2.$$

□

POZNÁMKA. Pretože zobrazenia sú špeciálne prípady relácií (každé zobrazenie je reláciou), tak všeobecné tvrdenia o reláciách platia aj pre zobrazenia. Napríklad z vety 8.1 vyplýva, že pre ľubovoľné zobrazenia f, g, h platí: $(f \circ g) \circ h = f \circ (g \circ h)$.

Základné vlastnosti, ktoré majú zobrazenia sa zachovajú aj pre zložené zobrazenia.

VETA 2. *Nech $g : A \to B$, $f : B \to C$. Potom*
a) ak g, f sú injekcie, tak aj $f \circ g$ je injekcia,
b) ak g, f sú surjekcie, tak aj $f \circ g$ je surjekcia,
c) ak g, f sú bijekcie, tak aj $f \circ g$ je bijekcia.

DÔKAZ. a) Nech $a \neq b$. Potom $g(a) \neq g(b)$ (lebo g je injekcia) a preto aj $f(g(a)) \neq f(g(b))$ (lebo aj f je injekcia). Teda $(f \circ g)(a) \neq (f \circ g)(b)$, čo znamená, že $f \circ g$ je tiež injekcia.

b) Nech $c \in C$. Pretože f je surjekcia, existuje $b \in B$, že $f(b) = c$ a pretože aj g je surjekcia, existuje $a \in A$, že $g(a) = b$. Z toho vyplýva, že $f(g(a)) = (f \circ g)(a) = c$. Teda k ľubovoľnému prvku $c \in C$ existuje v zloženom zobrazení $f \circ g$ vzor $a \in A$. Preto $f \circ g$ je surjekcia

Tvrdenie c) vyplýva z a) a b). □

V predchádzajúcej kapitole bola zavedená identická (diagonálna) relácia $\triangle_A$. Je zrejmé, že $\triangle_A$ je bijekcia A na A; platí $\triangle_A(x) = x$ pre každé $x \in A$. Zobrazenie $\triangle_A$ sa nazýva *identické zobrazenie* množiny A.

Pripomeňme, že o ľubovoľnej relácii f z A do B (a teda aj o ľubovoľnom zobrazení) platí

$$f \circ \triangle_A = \triangle_B \circ f = f.$$

K ľubovoľnej binárnej relácii R existuje inverzná relácia R^{-1}. Ak R je zobrazenie, R^{-1} zobrazením byť nemusí.

VETA 3. *Ak zobrazenie $f : A \to B$ je injekcia, tak inverzná relácia f^{-1} je zobrazenie (z B do A).*

DÔKAZ. Nech $[a, b] \in f^{-1}$, $[a, c] \in f^{-1}$. Potom $[b, a] \in f$, $[c, a] \in f$, čiže $f(b) = f(c) = a$. Keďže f je injekcia, tak $b = c$ čo znamená, že f^{-1} je zobrazenie. □

DEFINÍCIA 4. Inverznú reláciu f^{-1} k prostému zobrazeniu f nazývame inverzné zobrazenie (k zobrazeniu f).

VETA 4. *Relácia f je bijekcia práve vtedy, keď f^{-1} je bijekcia.*

DÔKAZ. Nech f je bijekcia A na B. Z vety 3 vyplýva, že f^{-1} je zobrazenie (z B do A). Pretože $\mathcal{D}(f^{-1}) = \mathcal{H}(f) = B$, $\mathcal{H}(f^{-1}) = \mathcal{D}(f) = A$, je f^{-1} zobrazenie A na B (teda je surjekcia). Nakoniec, ak $f^{-1}(a) = f^{-1}(b) = c$, tak $a = f(c)$, $b = f(c)$ a teda (pretože f je zobrazenie) $a = b$ čo znamená, že f^{-1} je aj injekcia.

Obrátené tvrdenie vyplýva z toho, že $(f^{-1})^{-1} = f$. □

VETA 5. *Nech $f : A \to B$, $A \neq \emptyset$. Potom zobrazenie f je injekcia vtedy a len vtedy, keď existuje zobrazenie $g : B \to A$, že $g \circ f = \triangle_A$.*

DÔKAZ. a) Predpokladajme, že existuje zobrazenie g, o ktorom platí $g \circ f = \triangle_A$. Nech $f(a) = f(b)$. Potom $a = \triangle_A(a) = (g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b) = \triangle_A(b) = b$. Teda f je injekcia.

b) Obrátene, nech $f : A \to B$ je injekcia. Definujme zobrazenie $g : B \to A$ takto:

ak $b \in \mathcal{H}(f)$, tak $g(b) = f^{-1}(b)$,

ak $b \notin \mathcal{H}(f)$, tak $g(b) = c$, kde c je ľubovoľný ale pevne zvolený prvok z A.

Potom pre každé $a \in A$ je $(g \circ f)(a) = g(f(a)) = a$, teda $g \circ f = \triangle_A$. □

VETA 6. *Nech $f : A \to B$. Potom zobrazenie f je surjekcia vtedy a len vtedy, keď existuje zobrazenie $g : B \to A$, že $f \circ g = \triangle_B$.*

DÔKAZ. Predpokladajme, že k zobrazeniu f existuje také zobrazenie g, že $f \circ g = \triangle_B$. Potom $b = \triangle_B(b) = (f \circ g)(b) = f(g(b))$. Znamená to, že k ľubovoľnému $b \in B$ existuje v množine A jeho vzor v zobrazení f (je ním prvok $g(b)$), teda f je surjekcia.

Obrátene, nech f je surjekcia. Ak $b \in B$, tak existuje aspoň jeden prvok $a \in A$, že $f(a) = b$ (lebo f je surjekcia). Zvoľme (vyberme) ku každému prvku $b \in B$ jeden prvok $a_b \in A$ taký, že $f(a_b) = b$ a položme $g(b) = a_b$. Tým sme definovali zobrazenie $g : B \to A$. Pre každé $b \in B$ je $(f \circ g)(b) = f(g(b)) = f(a_b) = b$, teda $f \circ g = \triangle_B$. □

Z predchádzajúcich dvoch viet vyplýva

DÔSLEDOK. *Nech $f : A \to B$, $A \neq \emptyset$. Potom f je bijekcia A na B vtedy a len vtedy, keď existuje zobrazenie $g : B \to A$, že $g \circ f = \triangle_A$ a $f \circ g = \triangle_B$.*

VETA 7. *Nech $f : A \to B$, $g : B \to A$. Ak $f \circ g = \triangle_B$, $g \circ f = \triangle_A$, tak $g = f^{-1}$.*

DÔKAZ. Treba dokázať, že $[x, y] \in f$ práve vtedy, keď $[y, x] \in g$.

Nech $[x, y] \in f$. Pretože pre každé $x \in A$ je $[x, x] \in \triangle_A = g \circ f$, tak $[y, x] \in g$ (lebo $g \circ f$ je zobrazenie).

Obrátená implikácia sa dokáže analogicky. □

DEFINÍCIA 5. Ak existuje bijekcia množiny A na množinu B hovoríme, že množina A je ekvivalentná s množinou B a píšeme $A \sim B$.

VETA 8. *Pre ľubovoľné množiny A, B, C platí*

a) $A \sim A$,

b) $A \sim B \implies B \sim A$,

c) $A \sim B \wedge B \sim C \implies A \sim C$.

DÔKAZ. a) Zrejme $\triangle_A$ je bijekcia A na A, preto $A \sim A$.

b) Ak $A \sim B$, tak existuje bijekcia f množiny A na B. Potom f^{-1} je bijekcia B na A (veta 4), preto $B \sim A$.

c) Ak $A \sim B$, $B \sim C$, tak existujú bijekcie f množiny A na B a g množiny B na C. Potom, podľa vety 2, $g \circ f$ je bijekcia A na C, z čoho vyplýva $A \sim C$. □

Zobrazenia konečných a nekonečných množín. Symbolom $\boldsymbol{n}$ budeme označovať „štandardnú“ množinu $\boldsymbol{n} = \{m \in N;\ 1 \leq m \leq n\}$. Teda $\boldsymbol{n} = \{1, 2, \ldots, n\}$. Napríklad $\mathbf{1} = \{1\}$, $\mathbf{0} = \emptyset$, $\mathbf{3} = \{1, 2, 3\}$.

Množina A je *konečná*, ak existuje $n \in N$, že množina $\boldsymbol{n}$ je ekvivalentná s A. V takomto prípade hovoríme, že A je *n-prvková* množina. Ak zobrazenie $a : \boldsymbol{n} \to A$ je bijekcia, tak každý prvok $x \in A$ je obrazom nejakého čísla $i \in \boldsymbol{n}$, teda $x = a(i)$ čo často zapisujeme $x = a_i$. Množinu A môžeme potom zapísať v tvare $A = \{a_1, a_2, \ldots, a_n\}$ teda tak, ako sme to aj doteraz často robili.

POZNÁMKA. V teórii množín sa oboznámite aj s inými definíciami konečnej množiny, ktoré sú nezávislé od pojmu prirodzené číslo. Tam sa postupuje naopak, pomocou konečných množín sa vybuduje model množiny všetkých prirodzených čísel.

Zobrazenia konečných množín majú niektoré vlastnosti, ktoré zobrazenia nekonečných množín nemajú (a naopak). Niektoré z nich teraz uvedieme.

VETA 9. *Každé injektívne zobrazenie konečnej množiny do seba je aj surjekcia (t.j. bijekcia).*

DÔKAZ. (Matematickou indukciou.) Pre 0-prvkovú (t.j. prázdnu) množinu je tvrdenie zrejme pravdivé. Predpokladajme, že tvrdenie platí pre každú n-prvkovú množinu. Nech $B = \{b_1, b_2, \ldots, b_n, b_{n+1}\}$ je $n+1$-prvková množina a nech $f : B \to B$ je injekcia. Ak $b_{n+1} \notin \mathcal{H}(f)$, tak zúženie zobrazenia f na $B' = \{b_1, b_2, \ldots, b_n\}$ je prosté zobrazenie $B' \to B'$ a preto podľa indukčného predpokladu surjekcia. Potom $f(b_{n+1}) = f(b_k)$ pre nejaké $k < n+1$, spor (lebo f je prosté). Teda $b_{n+1} \in \mathcal{H}(f)$. Nech $f(b_k) = b_{n+1}$. Nepriamo ukážeme, že f je surjekcia. Ak existuje prvok b_j, ktorý nemá v zobrazení f vzor, môžeme definovať zobrazenie g takto:

$$g(b_k) = b_j, \qquad g(b_i) = f(b_i) \quad \text{pre} \quad i \neq k.$$

Potom g je injektívne zobrazenie $B \to B$ a $b_{n+1} \notin \mathcal{H}(g)$, čo podľa prvej časti dôkazu vedie k sporu. Teda f musí byť surjektívne zobrazenie. □

VETA 10. *Každé surjektívne zobrazenie konečnej množiny do seba je aj injektívne.*

DÔKAZ. Nech $A = \{a_1, a_2, \ldots, a_n\}$ a nech $f : A \to A$ je surjekcia. Podľa vety 6 existuje $g : A \to A$, že $f \circ g = \triangle_A$. Podľa vety 5 potom ale $g : A \to A$ je injekcia a preto (podľa vety 9) je aj surjekciou (a teda bijekciou). Preto g^{-1} je tiež bijekcia a z rovnosti $f \circ g = \triangle_A$ dostávame $f \circ g \circ g^{-1} = \triangle_A \circ g^{-1}$, t.j. $f = g^{-1}$ čo znamená, že f je tiež bijekcia. □

Na rozdiel od konečných množín u nekonečnej množiny, napríklad E, poznáme injektívne zobrazenie $E \to E$, ktoré nie je surjektívne, napríklad $y = 2^x$ a surjektívne zobrazenie, ktoré nie je injektívne, napríklad $y = x^3 - x$ (načrtnite si jeho graf).

Jednou z axióm gréckej matematiky bolo tvrdenie: „časť je menšia ako celok“. Pokiaľ si všímame len konečné množiny, tak toto tvrdenie naozaj odpovedá našej predstave a skúsenosti (ak A, B sú konečné množiny a A je vlastnou podmnožinou množiny B, tak neexistuje bijekcia A na B). U nekonečnej množiny je to inak. Napríklad zobrazenie $f : N \to Z$, $f = \{[0,0], [1,-1], [2,1], [3,-2], [4,2], \ldots\}$ t.j.

$f(n) = \frac{n}{2}$, ak n je párne,

$f(n) = -\frac{n+1}{2}$, ak n je nepárne

je bijekciou N na Z. Podobné poznatky boli dôvodom, že v roku 1848 pražský matematik Bertrand Bolzano uznáva existenciu nekonečnej množiny. Zavádza pojem ekvivalencie a zdôrazňuje, že sa musíme zmieriť s tým, že časť je ekvivalentná celku (teda napríklad množina všetkých prirodzených čísel je ekvivalentná s množinou všetkých celých čísel).

Na záver si všimnime bijektívne zobrazenia medzi intervalmi reálnych čísel.

Nech $a, b \in E$, $a < b$. Zobrazenie

$$f : (0,1) \to (a,b), \quad f(x) = a + (b-a)x$$

je bijekcia (načrtnite si graf tohto zobrazenia napr. pre $a = 2$, $b = 5$). Teda $(0,1) \sim (a,b)$. Z vety 8 vyplýva, že ak $a, b, c, d \in E$, $a < b$, $c < d$, tak $(a,b) \sim (c,d)$.

Zobrazenie (funkcia) tangens je bijekcia intervalu $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ na množinu reálnych čísel E (teda na interval $(-\infty, \infty)$). Teda (opäť podľa vety 8) je $(0,1) \sim E$.

Ak uvažujeme dva intervaly, ktoré sa líšia len „trochu“, napríklad intervaly $\langle 0,1)$ a $(0,1)$, tak príslušná bijekcia nemusí byť taká jednoduchá ako v predchádzajúcich prípadoch.

PRÍKLAD 6. Nájdite bijektívne zobrazenie intervalu $\langle 0,1)$ na interval $(0,1)$.

RIEŠENIE. Položíme
$f(0)=\frac{1}{2}$,
$f(\frac{1}{n})=\frac{1}{n+1}$ pre $n\in N$, $n\geq 2$,
$f(x)=x$ pre $x\in\langle 0,1)$, $x\neq 0$, $x\neq\frac{1}{n}$, pre každé $n\in N$.
Podrobne sa presvedčte, že takto definované zobrazenie f je bijekcia $\langle 0,1)$ na $(0,1)$. □

Tento príklad je aj návodom, ako riešiť ďalšie podobné úlohy. Pokúste sa napríklad ukázať, že $(0,1\rangle\sim(0,1)$ a $\langle 0,1\rangle\sim(0,1)$.

Cvičenia

1. Dané sú relácie
a) $f_1=\{[x,y]\in E^2;\ y=\sqrt{x+2}\}$,
b) $f_2=\{[x,y]\in E^2;\ x=(y-2)^2\}$,
c) $f_3=\{[x,y]\in E^2;\ |x|+|y|=1\}$,
d) $f_4=\left\{[x,y]\in E^2;\ y=\sqrt{(x-3)^2}-x\right\}$,
e) $f_5=\{[x,y]\in E^2;\ y=\log(x-2)+\log(3-x)\}$,
f) $f_6=\{[x,y]\in E^2;\ x=\sqrt{3-y}\cdot\log(y-3)\}$,
g) $f_7=\left\{[x,y]\in E^2;\ x=\frac{\sqrt{1-y^2}}{y-2}\right\}$.
Určte ich definičné obory a obory hodnôt. Zistite, ktoré z týchto relácií sú zobrazenia, a ktoré sú injekcie.

2. Zistite, či pre zobrazenia f, g z E do E platí $f=g$, ak
a) $f(x)=\frac{x^2-1}{x-1}$, $g(x)=x+1$,
b) $f(x)=\frac{x^4-1}{x^2+1}$, $g(x)=x^2-1$,
c) $f(x)=-\ln x$, $g(x)=\ln\frac{1}{x}$,
d) $f(x)=\sqrt{\frac{x+3}{x-3}}$, $g(x)=\frac{\sqrt{x+3}}{\sqrt{x-3}}$.

3. Dané sú zobrazenia
a) $f=\{[x,y]\in E^2;\ y=|x-1|-|2x+3|\}$,
b) $g=\{[x,y]\in E^2;\ y=(x-2)(x+3)\}$,
c) $h=\{[x,y]\in E^2;\ y=x^2+|x|-2\}$.
Načrtnite grafy týchto zobrazení a rozhodnite, ktoré z relácií f^{-1}, g^{-1}, h^{-1} sú zobrazenia.

4. Dané sú zobrazenia f, g množiny E do E takto:
a) $f(x)=|x|-2$, $g(x)=(x+2)(x-3)$,
b) $f(x)=|x-1|$, $g(x)=x^2$.
Určte $f\circ g$, $g\circ f$ a načrtnite ich grafy.

5. Nájdite $f\circ g$ a $\mathcal{D}(f\circ g)$ pre zobrazenia f, g z E do E, ak
a) $f(x)=\sqrt{x+1}$, $g(x)=x^2-2$,
b) $f=\{[x,y]\in N^2;\ x=2y+1\}$, $g=\{[x,y]\in N^2;\ x=2y\}$,

c) $f = \{[x,y] \in E^2;\, y = \ln(x-4)\}$, $\quad g = \{[x,y] \in E^2;\, y = \sqrt{x^2+x-2}\}$,
d) $f = \{[x,y] \in E^2;\, e^y = x\}$, $\quad g = \{[x,y] \in E^2; x(y-1) = 2\}$.

6. Daná je funkcia $f : E - \{1\} \to E$, $y = \frac{|x-3|}{1-x}$. Určte obor hodnôt a zistite, či f je injekcia.

7. Nech f, g sú zobrazenia.
a) Dokážte, že aj $f \cap g$ a $f - g$ sú zobrazenia.
b) Ukážte, že relácia $f \cup g$ nemusí byť zobrazením.

8. Nech f je kvadratická funkcia $y = x^2 - 1$. Určte $f(\langle -1, 2\rangle)$, $f(E)$, $f_{-1}(\langle -1, 1\rangle)$, $f_{-1}(\langle 0, 2\rangle)$.

9. Nech $f : A \to B$ a nech A_1, $A_2 \subseteq A$, B_1, $B_2 \subseteq B$. Dokážte, že platí:
a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$,
b) $f_{-1}(B_1 \cup B_2) = f_{-1}(B_1) \cup f_{-1}(B_2)$,
c) $f_{-1}(B_1 \cap B_2) = f_{-1}(B_1) \cap f_{-1}(B_2)$,
d) $f_{-1}(B_1 - B_2) = f_{-1}(B_1) - f_{-1}(B_2)$.
e) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$,
f) $f(A_1) - f(A_2) \subseteq f(A_1 - A_2)$,
g) $A_1 \subseteq f_{-1}(f(A_1))$.

10. Nájdite také zobrazenie f a množiny A_1, A_2, aby platilo:
a) $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$,
b) $f(A_1) - f(A_2) \neq f(A_1 - A_2)$,
c) $A_1 \neq f_{-1}(f(A_1))$.

11. Nech $f : A \to B$, $g : B \to C$. Dokážte, že
a) ak $g \circ f$ je injekcia, tak aj f je injekcia,
b) ak $g \circ f$ je surjekcia na C, tak aj g je surjekcia na C.

12. Nech f je zobrazenie neprázdnej množiny A do B. Ukážte, že nasledujúce podmienky sú ekvivalentné:

a) f je injekcia,
b) pre ľubovoľnú množinu C a pre ľubovoľné zobrazenia g, h množiny C do A z rovnosti $f \circ g = f \circ h$ vyplýva $g = h$.

13. Nech f je zobrazenie neprázdnej množiny A do B. Ukážte, že nasledujúce podmienky sú ekvivalentné:

a) f je surjekcia,
b) pre ľubovoľnú množinu C a pre ľubovoľné zobrazenia g, h množiny B do C z rovnosti $g \circ f = h \circ f$ vyplýva $g = h$.

14. Nech $f : A \to B$. Potom f je surjekcia práve vtedy, keď $f \circ f^{-1} = \triangle_B$. Dokážte.

15. Nech $f : A \to B$. Potom f je injekcia práve vtedy, keď $f^{-1} \circ f = \triangle_A$. Dokážte.

10. Relácie ekvivalencie a usporiadania

Prvky množiny často rozdeľujeme na základe nejakých kritérií do skupín. Napríklad množinu celých čísel môžeme rozdeliť na množinu kladných čísel, množinu záporných čísel a jednoprvkovú množinu $\{0\}$ alebo ju môžeme rozdeliť na množinu párnych čísel a množinu nepárnych čísel alebo nejakým iným spôsobom. V takýchto prípadoch hovoríme, že sme vytvorili rozklad množiny.

DEFINÍCIA 1. Nech A je neprázdna množina. Systém $\mathcal{S}$ podmnožín množiny A sa nazýva rozklad množiny A, ak

1. $\emptyset \notin \mathcal{S}$,
2. $\forall B, C \in \mathcal{S}, \quad B \neq C \implies B \cap C = \emptyset$,
3. $\bigcup \mathcal{S} = A$.

Ak $\mathcal{S}$ je rozklad množiny A, tak podmnožiny patriace do $\mathcal{S}$ obyčajne nazývame *triedy rozkladu (alebo bloky).*

Pri rozdeľovaní prvkov množiny do skupín (blokov) si obyčajne zvolíme nejaké kritérium a do jednej triedy zaradíme tie prvky, ktoré z hľadiska zvoleného kritéria majú rovnakú vlastnosť. Pri delení detských guličiek môže byť kritérium farba a do jednej skupiny dáme červené guličky, do druhej zelené, atď. Pri prirodzených číslach môže byť kritérium počet deliteľov (do jednej skupiny bude patriť len číslo 1, ktoré má jediného deliteľa, do druhej číslo 0, ktoré má nekonečný počet deliteľov do tretej budú patriť prvočísla, ktoré majú po dvoch deliteľoch a do štvrtej zložené čísla, ktoré majú konečný počet deliteľov väčší ako 2. Všimnite si, že pritom platí:

ak objekt a má takú vlastnosť ako b, tak aj b má takú vlastnosť ako a,

ak a, b majú tú istú (rovnakú) vlastnosť aj b, c majú rovnakú vlastnosť, tak aj a, c majú rovnakú vlastnosť.

Teda relácia obsahujúca usporiadané dvojice prvkov majúcich rovnakú vlastnosť je symetrická, tranzitívna a zrejme je aj reflexívna.

DEFINÍCIA 2. Nech R je relácia na množine A. Hovoríme, že R je ekvivalencia (relácia ekvivalencie) na A, ak je reflexívna na A, symetrická a tranzitívna.

Ukážeme teraz, že rozklady množín a relácie ekvivalencie spolu súvisia. Tento súvis je dosť dôležitý, často sa využíva a aj vy sa s ním pri štúdiu matematiky často stretnete.

VETA 1. *Nech $\sim$ je ekvivalencia na množine A. Pre ľubovoľný prvok $a \in A$ označíme $\overline{a} = \{x \in A;\, x \sim a\}$. Potom $\mathcal{S} = \{\overline{a};\, a \in A\}$ je rozklad množiny A.*

DÔKAZ. $\mathcal{S}$ je zrejme systém podmnožín množiny A. Pretože $a \in \overline{a}$ (lebo $\sim$ je reflexívna), tak $\emptyset \notin \mathcal{S}$ a $\bigcup \mathcal{S} = A$. Treba ešte ukázať, že ak $\overline{a}, \overline{b} \in \mathcal{S}$, $\overline{a} \cap \overline{b} \neq \emptyset$, tak $\overline{a} = \overline{b}$. Ak $\overline{a} \cap \overline{b} \neq \emptyset$, tak existuje c, že $c \in \overline{a}$ aj $c \in \overline{b}$. Z toho vyplýva, že $c \sim a$, $c \sim b$ a pretože $\sim$ je symetrická, platí aj $a \sim c$. Nech $x \in \overline{a}$. Potom $x \sim a$ a pretože $\sim$ je tranzitívna relácia, tak zo vzťahov $x \sim a$, $a \sim c$, $c \sim b$ vyplýva $x \sim b$, t.j. $x \in \overline{b}$. Tým sme ukázali, že $\overline{a} \subseteq \overline{b}$. Analogicky možno ukázať, že aj $\overline{b} \subseteq \overline{a}$. $\square$

Nech $\sim$ je ekvivalencia na množine A a nech $a \in A$. Množinu $\overline{a} = \{x \in A;\, x \sim a\}$ nazývame *trieda (blok) rozkladu* množiny A podľa ekvivalencie $\sim$, daná (daný) prvkom a. Systém $\{\overline{a};\, a \in A\}$ budeme označovať $A/\sim$ a nazývať *faktorová množina* množiny A podľa $\sim$.

Ak R je ekvivalencia (na nejakej množine), tak namiesto aRb niekedy píšeme $a \equiv b \pmod{R}$.

VETA 2. *Nech $\mathcal{S}$ je rozklad množiny A. Nech pre ľubovoľné $a, b \in A$ je $a \sim b$ práve vtedy, keď existuje množina $X \in \mathcal{S}$ tak, že $a, b \in X$. Potom relácia $\sim$ je ekvivalencia na A.*

DÔKAZ. Každý prvok $a \in A$ patrí do nejakej množiny systému $\mathcal{S}$, teda $a \sim a$ čo znamená, že $\sim$ je reflexívna relácia. Je zrejmé, že relácia $\sim$ je symetrická. Nech $x \sim y$, $y \sim z$. Potom existujú množiny X, Y systému $\mathcal{S}$, že $x, y \in X$, $y, z \in Y$. Pretože $X \cap Y \neq \emptyset$ (lebo $y \in X \cap Y$), tak $X = Y$ a teda $x, z \in X$ čo znamená, že $x \sim z$. Ukázali sme, že relácia $\sim$ je aj tranzitívna. □

Vo vete 1 a vete 2 sú dva prvky v relácii práve vtedy, keď sú prvkami tej istej triedy rozkladu. Z predchádzajúcich poznatkov teda vyplýva, že medzi rozkladmi množiny A a ekvivalenciami na A je vzájomne jednoznačná korešpodencia: každému rozkladu množiny A prislúcha práve jedna ekvivalencia na A (ním určená) a naopak.

PRÍKLAD 1. Na množine Z definujeme reláciu $\equiv$ takto:

$$a \equiv b \iff 5 \mid (a - b).$$

Pre každé číslo $a \in Z$ platí $5 \mid (a - a)$, t.j. $a \equiv a$. Ak $a \equiv b$, tak $5 \mid (a - b)$, z čoho vyplýva $5 \mid (b - a)$, t.j. $b \equiv a$. Ak $a \equiv b$ aj $b \equiv c$, tak $5 \mid (a - b)$, $5 \mid (b - c)$, z čoho vyplýva $5 \mid ((a - b) + (b - c))$, t.j. $5 \mid (a - c)$, teda $a \equiv c$. Tým sme ukázali, že $\equiv$ je ekvivalencia. Ona určuje rozklad (faktorovú množinu) $Z/\equiv = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, pričom

$$\begin{aligned}
\overline{0} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\}, \\
\overline{1} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\}, \\
\overline{2} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\}, \\
\overline{3} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\}, \\
\overline{4} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

Všimnite si, že dve celé čísla patria do tej istej triedy rozkladu práve vtedy, keď pri ich delení číslom 5 dostaneme rovnaký zvyšok. Preto $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ sa nazývajú *zvyškové triedy* (podľa modulu 5). □

Pri uvedenom spôsobe označovania tried rozkladu je možné tú istú triedu označiť viacerými symbolmi. Ak a, b sú prvky tej istej triedy, tak $\overline{a} = \overline{b}$. Napríklad v rozklade z predchádzajúceho príkladu je $\overline{1} = \overline{6} = \overline{-4} = \overline{11} = \ldots$.

Pri riešení niektorých matematických úloh uvádzame v závere počet riešení danej úlohy. Napríklad v geometrii pri úlohe „zostrojte trojuholník ABC so stranami $a = 4cm$, $b = 5cm$, $c = 6cm$“ sa zvykne uviesť, že úloha má jedno riešenie, hoci trojuholníkov, ktoré spĺňajú uvedené podmienky je nekonečne veľa. V takomto prípade však ide v skutočnosti o nájdenie reprezentanta triedy rozkladu, daného na množine všetkých trojuholníkov (vo zvolenej rovine) reláciou zhodnosť.

Relácia $\sim$ (ekvivalencia množín) daná v definícii 9.5 je, ako vyplýva z vety 9.10, reláciou ekvivalencie. Vytvára teda na ľubovoľnom systéme množín, ktorý je opäť množinou, rozklad podľa vety 1. Do jednej triedy rozkladu patria všetky navzájom ekvivalentné množiny. Hovoríme, že tieto množiny majú rovnakú *mohutnosť* alebo rovnaké *kardinálne číslo* (u konečných množín rovnaký *počet prvkov*). V predchádzajúcej kapitole sme sa niektorými takýmito množinami reálnych čísel zaoberali.

Ak je dané zobrazenie f množiny A na množinu B, tak je možné definovať na A (prirodzeným spôsobom) reláciu ekvivalencie.

VETA 3. *Nech je dané zobrazenie $f : A \to B$. Na množine A definujeme reláciu $\sim$ podmienkou*

$$a \sim b \iff f(a) = f(b). \tag{1}$$

Relácia $\sim$ je ekvivalenciou na A a faktorová množina $A/\sim$ je ekvivalentná s oborom hodnôt $\mathcal{H}(f)$. Bijekciou $A/\sim$ na $\mathcal{H}(f)$ je (napríklad) zobrazenie g, ktoré je dané predpisom

$$\forall\, \overline{a} \in A/\sim \qquad g(\overline{a}) = f(a). \tag{2}$$

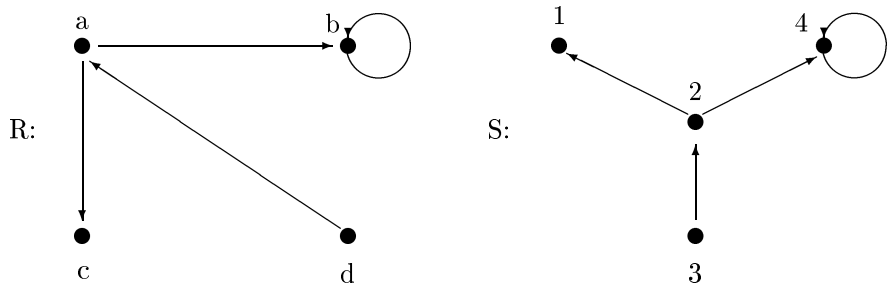
DÔKAZ. Overenie reflexívnosti, symetričnosti a tranzitívnosti relácie $\sim$ prenechávame čitateľovi ako ľahké cvičenie. Ďalej treba ukázať, že g je bijekcia $A/\sim$ na $\mathcal{H}(f)$. Platí

$$\overline{a} = \overline{b} \iff a \sim b \iff f(a) = f(b).$$

Z toho vyplýva, že g je *korektne definované* zobrazenie (rovnosť vzorov $\overline{a}$, $\overline{b}$ implikuje rovnosť ich obrazov $f(a)$, $f(b)$, t.j. relácia g je zobrazením), a že g je prosté zobrazenie. Z (2) vyplýva, že g je zobrazenie na množinu $\mathcal{H}(f)$, preto g je bijekcia $A/\sim$ na $\mathcal{H}(f)$. □

V matematike sa obvykle zaoberáme množinou nejakých objektov, pričom na tejto množine skúmame určité relácie a operácie. Napríklad na množine celých čísel sa obyčajne zaoberáme reláciami usporiadania a deliteľnosti a operáciami sčítania, násobenia a odčítania, na množine vektorov reláciou kolmosti a operáciou sčítania, na množine geometrických útvarov reláciami zhodnosti a podobnosti, atď. Množinu spolu s usporiadaným systémom relácií a operácií na nej definovaných voláme *algebraická štruktúra.* V závislosti od počtu relácií a operácií a od vlastností relácií a operácií majú algebraické štruktúry rôzne pomenovania (grupy, usporiadané polia, euklidovské priestory, atď.) Kvôli jednoduchosti si na začiatku budeme všímať na množine len jedinú binárnu reláciu.

Na obrázku 1 sú pomocou uzlových grafov dané binárne relácie R, S. Relácia R na množine $A = \{a, b, c, d\}$, relácia S na množine $B = \{1, 2, 3, 4\}$.



Obr. 1

Všimnime si, že „vhodným prekreslením“ jedného z týchto grafov môžeme docieliť to, že obrázky grafov týchto dvoch relácií budú „rovnaké“. Podrobnejšie sa budeme zaoberať tým, čo to znamená.

Nech R je relácia na množine A. Usporiadaná dvojica (A, R) sa volá *relačná štruktúra*, množina A sa volá *nosič* tejto štruktúry.

DEFINÍCIA 3. Nech (A, R), (B, S) sú relačné štruktúry. Bijektívne zobrazenie $f : A \to B$, o ktorom platí

$$\forall a, b \in A \qquad [a, b] \in R \Longleftrightarrow [f(a), f(b)] \in S$$

nazývame izomorfné zobrazenie (izomorfizmus) relačnej štruktúry (A, R) na relačnú štruktúru (B, S).

Prvý z grafov na obrázku 1 znázorňuje relačnú štruktúru

$$(\{a, b, c, d\}, \{[a, b], [a, c], [b, b], [d, a]\}).$$

Zobrazenie $f = \{[a, 2], [b, 4], [c, 1], [d, 3]\}$ je izomorfné zobrazenie tejto relačnej štruktúry na relačnú štruktúru (B, S). Všimnime si, že zobrazenie k nemu inverzné, t.j. $f^{-1} = \{[2, a], [4, b], [1, c], [3, d]\}$ je izomorfným zobrazením relačnej štruktúry (B, S) na (A, R).

VETA 4. *a) Ak f je izomorfné zobrazenie relačnej štruktúry (A, R), na (B, S), tak f^{-1} je izomorfné zobrazenie relačnej štruktúry (B, S) na (A, R).*

b) Ak f je izomorfné zobrazenie relačnej štruktúry (A, R), na (B, S) a g je izomorfné zobrazenie relačnej štruktúry (B, S) na (C, Q), tak $g \circ f$ je izomorfné zobrazenie (A, R) na (C, Q).

DÔKAZ. a) Ak $f : A \to B$ je bijekcia, tak aj $f^{-1} : B \to A$ je bijekcia. Nech x, y sú ľubovoľné prvky z B. Potom existujú prvky $a, b \in A$, že $f(a) = x$, $f(b) = y$, teda $a = f^{-1}(x)$, $b = f^{-1}(y)$. To, že f^{-1} je izomorfizmus vyplýva z nasledovného reťazca ekvivalencií

$$[x, y] \in S \quad \Leftrightarrow \quad [f(a), f(b)] \in S \quad \Leftrightarrow \quad [a, b] \in R \quad \Leftrightarrow \quad [f^{-1}(x), f^{-1}(y)] \in R.$$

b) Ak $f : A \to B$, $g : B \to C$ sú bijekcie, tak aj $g \circ f : A \to C$ je bijekcia. Nech $x, y \in A$. Potom $[x, y] \in R$ práve vtedy, keď $[f(x), f(y)] \in S$ (lebo f je izomorfizmus) a $[f(x), f(y)] \in S$ práve vtedy, keď $[g(f(x)), g(f(y))] \in Q$, t.j. $[(g \circ f)(x), (g \circ f)(y)] \in Q$ (lebo aj g je izomorfizmus). Z toho vyplýva, že aj $g \circ f$ je izomorfizmus. □

DEFINÍCIA 4. Ak existuje izomorfné zobrazenie relačnej štruktúry (A, R) na (B, S) hovoríme, že relačné štruktúry (A, R), (B, S) sú izomorfné a píšeme $(A, R) \simeq (B, S)$

Nech $\mathcal{S}$ je ľubovoľný neprázdny systém relačných štruktúr, ktorý je množinou. Relácia $\simeq$ je reflexívna, lebo každá relačná štruktúra (A, R) je izomorfná sama so sebou (izomorfizmom je identita $\triangle_A$). Z vety 4 vyplýva, že relácia $\simeq$ je aj symetrická aj tranzitívna. Teda relácia $\simeq$ je reláciou ekvivalencie, t.j. určuje rozklad systému $\mathcal{S}$. Pritom dve relačné štruktúry patria do tej istej triedy rozkladu práve vtedy, keď sú izomorfné. Izomorfné relačné štruktúry nepokladáme obyčajne za rôzne. Zvyčajne sa teda nezaoberáme skúmaním jednotlivých relačných štruktúr, ale skúmaním tried daných reláciou $\simeq$, resp. skúmaním takých vlastností relačných štruktúr, ktoré sa pri izomorfizmoch zachovávajú (sú vzhľadom na izomorfizmy invariantné). Takýmito vlastnosťami sú (ako vyplýva z nasledovnej vety) aj všetky vlastnosti zavedené v definícii 8.3.

VETA 5. *Nech (A, R), (B, S) sú izomorfné relačné štruktúry. Ak relácia R má niektorú z vlastností a) – g) z definície 8.3, tak ju má aj relácia S.*

DÔKAZ. Dokážeme invariantnosť tranzitívnosti. Ostatné vlastnosti sa dokážu analogicky.

Nech relácia R je tranzitívna a nech pre $a, b, c \in B$ je $[a, b] \in S$ aj $[b, c] \in S$. Pretože $(A, R) \simeq (B, S)$, existuje izomorfizmus f relačnej štruktúry (A, R) na (B, S), teda existujú aj prvky $x, y, z \in A$, že $f(x) = a$, $f(y) = b$, $f(z) = c$ a $[x, y] \in R$, $[y, z] \in R$. Relácia R je tranzitívna, teda $[x, z] \in R$ z čoho vyplýva, že $[f(x), f(z)] = [a, c] \in S$ čo znamená, že aj relácia S je tranzitívna. □

V závere tohto článku sa oboznámime s často používanou relačnou štruktúrou, s tzv. usporiadanou množinou.

V matematike, ale aj v iných oblastiach, často prvky množín nejakým spôsobom usporiadame. Napríklad v slovníku sú slová usporiadané na základe tzv. abecedného poradia, cvičenci sa zvyknú zoradiť podľa ich výšky, prirodzené čísla podľa veľkosti atď. V takýchto prípadoch pre každé dva prvky (slová, cvičencov, čísla) a, b platí, že buď „a je pred b“ alebo „b je pred a“. Často sa však stretávame aj s takými usporiadaniami, kde táto vlastnosť nie je splnená. Napríklad, ak podmnožiny množiny $M = \{1, 2, 3\}$ usporiadame na základe množinovej inklúzie, tak $\emptyset$ je pred $\{1\}$, táto je pred $\{1, 2\}$ atď., ale z podmnožín $\{1\}$, $\{2\}$ nie je ani jedna pred druhou. U usporiadania vždy požadujeme, aby zo vzťahov „a je pred b“ a „b je pred c“ vyplývalo „a je pred c“ a aby pre rôzne prvky a, b neplatilo „a je pred b“ aj „b je pred a“.

DEFINÍCIA 5. Nech A je množina. Reflexívnu, antisymetrickú a tranzitívnu reláciu na A nazývame (neostré) usporiadanie na množine A (alebo usporiadanie množiny A). Ak $\leq$ je usporiadanie na množine A, tak relačnú štruktúru $(A, \leq)$ nazývame usporiadaná množina. Ak $x \in A$ hovoríme, že x je prvok usporiadanej množiny $(A, \leq)$.

POZNÁMKA. Usporiadanie zavedené v predchádzajúcej definícii sa často nazýva čiastočným usporiadaním.

PRÍKLAD 2. a) Množina reálnych čísel s tzv. „prirodzeným“ usporiadaním $\leq$ (t.j. usporiadaním podľa veľkosti) je usporiadanou množinou.

b) Nech A je ľubovoľná množina. Z vety 6.1 vyplýva, že $(P(A), \subseteq)$ je usporiadaná množina.

c) Z vety 2.2 vyplýva, že $(N^+, |)$ je usporiadaná množina. □

Nech $(A, \leq)$ je usporiadaná množina. Potom symbolom $<$ označujeme reláciu na A, ktorá je definovaná takto:

$$a < b \iff a \leq b \wedge a \neq b. \tag{3}$$

Z (3) a definície 5 vyplýva, že relácia $<$ je ireflexívna a tranzitívna a preto je aj antisymetrická (podrobne sa presvedčte). Nazývame ju *ostré usporiadanie* na množine A. Ak $<$ je ostré usporiadanie na A, tak aj relačnú štruktúru $(A, <)$ nazývame usporiadaná množina.

Ak o prvkoch a, b usporiadanej množiny $(A, \leq)$ platí $a \leq b$, píšeme niekedy $b \geq a$ a podobne, ak $a < b$ píšeme $b > a$. V takomto prípade namiesto „a je pred b“ zvykneme hovoriť „b je za a“.

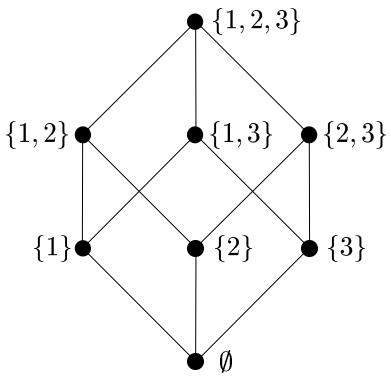
Poznámka. Na číselnej množine budeme symbolmi $\leq$, $<$ vždy označovať obvyklé usporiadanie (ktoré čitateľ pozná z predchádzajúceho štúdia).

Ak $(A, \leq)$ je usporiadaná množina a $B \subseteq A$, tak podľa vety 8.4 aj množina B so zúžením relácie $\leq$ na množinu B je usporiadaná množina, t.j. $(B, \leq_B)$ je usporiadaná množina. O usporiadaní $\leq_B$ hovoríme, že je *indukované* usporiadaním $\leq$.

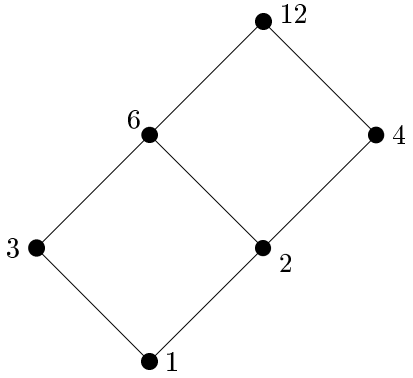
Ak $\leq$ je relácia usporiadania na konečnej množine A, tak usporiadanú množinu $(A, \leq)$ často znázorňujeme pomocou tzv. Hasseho diagramu, ktorý zostrojíme takto:

1. Ku každému prvku z A priradíme v rovine krúžok tak, aby v prípade, keď $a < b$ ležal krúžok priradený k prvku b vyššie ako krúžok priradený k prvku a,
2. ak $a < b$ a neexistuje v A prvok c, o ktorom platí $a < c < b$, tak krúžky znázorňujúce prvky a, b spojíme úsečkou.

Na obrázku 2 je Hasseho diagram usporiadanej množiny $(P(\{1,2,3\}, \subseteq)$ a na obrázku 3 je Hasseho diagram usporiadanej množiny $(\{1,2,3,4,6,12\}, |)$.



Obr. 2



Obr. 3

Zadaním Hasseho diagramu môžeme tiež veľmi jednoducho usporiadanie na danej množine definovať.

Ak o prvkoch a, b usporiadanej množiny $(A, \leq)$ neplatí ani $a \leq b$ ani $b \leq a$ hovoríme, že a, b sú *neporovnateľné* prvky. Neporovnateľnými prvkami sú napr. prvky $\{1,2\}$ a $\{3\}$ usporiadanej množiny na obrázku 2 alebo napr. čísla 3, 4 usporiadanej množiny na obrázku 3.

Definícia 6. Nech $(A, \leq)$ je usporiadaná množina. Prvok $a \in A$ sa nazýva:
a) prvý (najmenší) prvok množiny A, ak $a \leq x$ pre každý prvok $x \in A$,
b) posledný (najväčší) prvok množiny A, ak $x \leq a$ pre každý prvok $x \in A$.

V usporiadanej množine s Hasseho diagramom na obrázku 2 je prvým (najmenším) prvkom $\emptyset$, posledným (najväčším) prvkom množina $\{1,2,3\}$. Jej podmnožina $B = \{\emptyset, \{1\}, \{3\}\}$ (s indukovaným usporiadaním) má prvý prvok $\emptyset$, posledný prvok nemá. Množina všetkých celých čísel s obvyklým usporiadaním, t.j. usporiadaná množina $(Z, \leq)$ nemá ani prvý ani posledný prvok. Jej podmnožina N má prvý prvok 0, ale posledný prvok nemá.

Ak v usporiadanej množine $(A, \leq)$ neexistujú neporovnateľné prvky (t.j. relácia $\leq$ je aj súvislá) hovoríme, že $\leq$ je *úplné* usporiadanie na A a že $(A, \leq)$ je *úplne* usporiadaná množina (alebo *ret'azec*).

Definícia 7. Nech $(A, \leq_1)$, $(B, \leq_2)$ sú usporiadané množiny. Zobrazenie $f : A \to B$ sa nazýva izotónne zobrazenie, ak

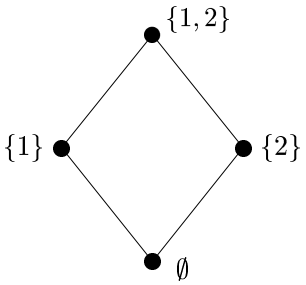
$$\forall x, y \in A; \quad x \leq_1 y \implies f(x) \leq_2 f(y).$$

V definícii 3 je zavedený izomorfizmus relačných štruktúr. Je zrejmé, že zobrazenie $f : A \to B$ je izomorfizmus usporiadanej množiny $(A, \leq_1)$ na usporiadanú množinu $(B, \leq_2)$ ak f je bijekcia a zobrazenia f a f^{-1} sú izotónne.

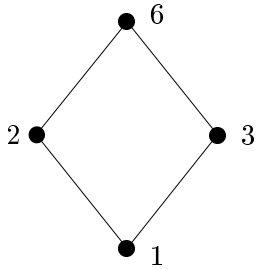
Príklad 2. Dané sú usporiadané množiny

$$(P(\{1, 2, \}), \subseteq), \qquad (\{1, 2, 3, 6\}, |), \qquad (\{1, 2, 3, 4\}, \leq),$$

ktorých Hasseho diagramy sú na obrázkoch 4, 5, 6.



Obr. 4



Obr. 5

Obr. 6

Zobrazenie $f = \{[1, 1], [2, 2], [3, 3], [6, 4]\}$ je izotónnym zobrazením usporiadanej množiny na obr. 5 do usporiadanej množiny na obr. 6 ale nie je izomorfným zobrazením usporiadanej množiny $(\{1, 2, 3, 6\}, |)$ na $(\{1, 2, 3, 4\}, \leq)$, pretože $f(2) \leq f(3)$ ale neplatí $2 \mid 3$ (zobrazenie f^{-1} nie je izotónne).

Zobrazenie $g = \{[\emptyset, 1], [\{1\}, 2], [\{2\}, 3], [\{1, 2\}, 6]\}$ je izomorfným zobrazením usporiadanej množiny $(P(\{1, 2, \}), \subseteq)$ na $(\{1, 2, 3, 6\}, |)$. □

Cvičenia

1. Určte vymenovaním všetky rozklady množiny
a) $\{1,2\}$, b) $\{1,2,3\}$, c) $\{1,2,3,4\}$.

2. Určte (vymenovaním) relácie ekvivalencie dané rozkladmi nájdenými pri riešení cvičenia 1.

3. Nájdite aspoň tri rôzne rozklady množiny Z.

4. Zistite, ktoré z nasledujúcich relácií sú ekvivalenciami na množine E.

a) $\{[x,y] \in E^2;\ \frac{x}{y} = 1\}$, b) $\{[x,y] \in E^2;\ |x-y| \leq 1\}$,
c) $\{[x,y] \in E^2;\ |x| = |y|\}$, d) $\{[x,y] \in E^2;\ x^3 = y^3\}$.

5. Na množine $A = \{1,2,\ldots,20\}$ definujeme reláciu R takto:
a) xRy práve vtedy, keď čísla x, y majú rovnaký súčet cifier,
b) xRy práve vtedy, keď čísla x, y majú rovnaký súčin cifier.
Dokážte, že R je ekvivalencia a napíšte príslušný rozklad.

6. Na množine N definujeme relácie:
a) mR_1n práve vtedy, keď dekadický zápis čísla m sa končí rovnakou číslicou ako dekadický zápis čísla n,
b) mR_2n práve vtedy, keď dekadický zápis čísla m má rovnaký počet (platných) cifier ako zápis čísla n,
c) mR_3n práve vtedy, keď číslo m má rovnaký ciferný súčet ako n.
Ukážte, že R_1, R_2, R_3 sú relácie ekvivalencie a nájdite príslušné triedy rozkladov.

7. Nech vo zvolenej rovine α je daná priamka p. Na množine α definujeme reláciu $\sim$ takto:

$$A \sim B \iff A = B \vee (A \neq B \wedge AB \parallel p).$$

Ukážte, že $\sim$ je reláciou ekvivalencie a nájdite triedy rozkladu daného touto ekvivalenciou.

8. Na množine Z je daná relácia $\equiv$ takto:

$$a \equiv b \iff 6 \mid a-b.$$

Dokážte, že $\equiv$ je relácia ekvivalencie a určte faktorovú množinu $Z/\equiv$.

9. Daná je relácia $R = \{[x,y] \in Z^2;\ 2 \mid x^2 - y^2\}$. Ukážte, že R je ekvivalencia a nájdite príslušný rozklad množiny celých čísel.

10. Na množine zlomkov $\left\{\frac{m}{n};\ m \in Z,\ n \in N^+\right\}$ je daná relácia $\sim$ takto:

$$\frac{m}{n} \sim \frac{m'}{n'} \iff m \cdot n' = m' \cdot n.$$

a) Ukážte, že $\sim$ je relácia ekvivalencie.
b) Kedy dva zlomky patria do tej istej triedy rozkladu daného reláciou $\sim$?

11. Na množine $N \times N$ definujeme reláciu $\sim$ takto:

$$[a,b] \sim [c,d] \iff a + d = b + c.$$

a) Ukážte, že $\sim$ je na $N \times N$ ekvivalencia.
b) Kedy patria dve usporiadané dvojice do tej istej triedy rozkladu?

12. Nech $A = \{-5,-4,\ldots,4,5\}$, $B = \{0,1,2,3,4,5\}$ a nech zobrazenie $f : A \to B$ je dané predpisom $f(x) = |x|$.
a) Určte (vymenovaním) faktorovú množinu $A/\sim$, pričom relácia $\sim$ je daná podmienkou (1) vo vete 3.

b) Určte (vymenovaním dvojíc) bijekciu g, faktorovej množiny $A/\sim$ na $\mathcal{H}(f) = B$, pričom bijekcia g je daná podmienkou (2) vo vete 3.

13. Nakreslite diagramy všetkých (navzájom neizomorfných)
a) dvojprvkových usporiadaných množín,
b) trojprvkových usporiadaných množín,
a) štvorprvkových usporiadaných množín.

14. Koľko rôznych úplných usporiadaní možno definovať
a) na trojprvkovej množine $\{1, 2, 3\}$
b) na n-prvkovej množine $\{1, 2, \ldots, n\}$.

15. Na množine $\{a, b, c, d\}$ určte reláciu usporiadania (pomocou Hasseho diagramu) tak, aby
a) existoval prvý aj posledný prvok,
b) existoval prvý, ale neexistoval posledný prvok,
c) existoval posledný, ale neexistoval prvý prvok,
d) neexistoval ani prvý ani posledný prvok.

16. Je daná množina zobrazení $F = \{f_1, f_2, \ldots, f_9\}$ s definičným oborom $\langle -2, 2\rangle$ definovaných takto:

$$\begin{array}{lll} f_1(x) = |x| - 4, & f_2(x) = |x| - 3, & f_3(x) = |x| - 2, \\ f_4(x) = -|x| + 4, & f_5(x) = -|x| + 3, & f_6(x) = -|x| + 2, \\ f_7(x) = -|x|, & f_8(x) = |x + 2|, & f_9(x) = 2. \end{array}$$

Na množine F definujeme reláciu ρ takto:

$f_i \rho f_j$ práve vtedy, keď pre každé $x \in \langle -2, 2\rangle$ je $f_i(x) \leq f_j(x)$.

Ukážte, že (F, ρ) je usporiadaná množina, nakreslite jej Hasseho diagram a zistite, či má najmenší a najväčší prvok.

17. Nakreslite Hasseho diagram usporiadanej množiny $(A, |)$, ak
a) $A = \{3, 6, 9, 12, 15, 18\}$, b) $A = \{2, 3, 5, 7, 11, 13\}$,
c) $A = \{1, 2, 3, 10, 14, 15, 21, 30, 45, 105, 140\}$.

18. Zistite, či usporiadaná množina $(N^+, \leq)$ je izomorfná s usporiadanou množinou
a) $(A, \geq)$, kde $A = \{1 - 2x;\ x \in N^+\}$, b) $(B, \geq)$, kde $B = \left\{\frac{1}{3x+1};\ x \in N^+\right\}$,
c) $(C, \leq)$, kde $C = \{2 - 3x;\ x \in N^+\}$, d) $(D, \leq)$, kde $D = \left\{\frac{1}{1-3x};\ x \in N^+\right\}$.

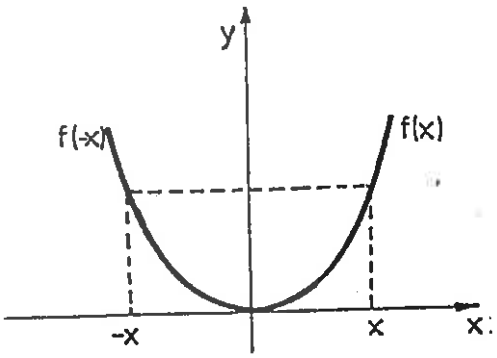
19. Nech (P, R) je čiastočne usporiadaná množina a nech $[x, y] \in R$. Zistite, kedy je $(P, R \setminus \{[x, y]\})$ čiastočne usporiadaná množina.

20. Nech $P = \{a, b, c, d, e\}$, $R = \triangle_P \cup \{[d, e], [d, c], [b, c], [b, e], [a, b], [a, c], [a, e]\}$.
a) Nakreslite Hasseho diagram čiastočne usporiadanej množiny (P, R).
b) Nájdite všetky usporiadané dvojice $[x, y] \in R$ pre ktoré je $(P, R \setminus \{[x, y]\})$ čiastočne usporiadaná množina a nakreslite príslušné Hasseho diagramy. Ktoré z týchto usporiadaných množín sú neizomorfné?

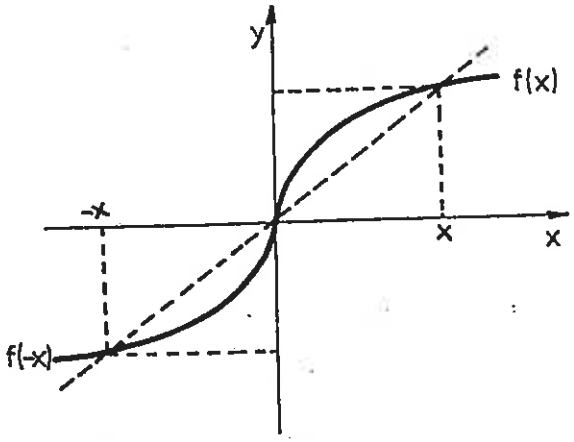
21. Nájdite všetky izomorfné zobrazenia usporiadanej množiny $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ na usporiadanú množinu $(\{1, 2, 3, 5, 6, 10, 15, 30\}, |)$.

11. Elementárne funkcie

V tomto učebnom texte ste sa už viackrát stretli s poznatkami o zobrazeniach a na strednej škole ste venovali osobitnú pozornosť zobrazeniam, ktoré sa nazývajú reálne funkcie reálnej premennej. Už názov hovorí, že ide o zobrazenia, u ktorých definičný obor aj obor hodnôt sú nejaké množiny reálnych čísel. Ak f je reálna funkcia reálnej premennej a ak v rovine s pravouhlým súradnicovým systémom každej dvojici $[x, y] \in f$ (namiesto y budeme často písať $f(x)$) priradíme bod so súradnicami x, y, dostaneme *graf funkcie* f. Na obr. 1 je načrtnutý graf funkcie $f(x) = x^2$.



Obr. 1



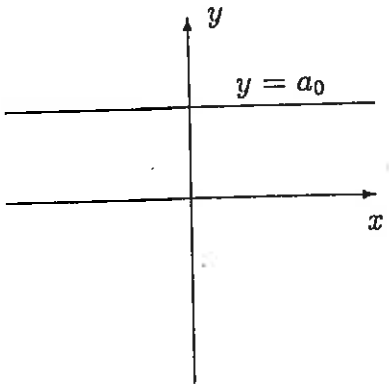
Obr. 2

Náčrt grafu funkcie, ak sa dá urobiť, nás (poskytnutím vizuálnej predstavy funkcie) často lepšie „zoznámi“ s funkciou než jej predpis. Napríklad pri pohľade na obr. 1 je vidieť, že definičným oborom funkcie $f(x) = x^2$ je celá množina E, zatiaľ čo oborom hodnôt je zrejme interval $\langle 0, \infty)$. Je tiež vidieť, že na intervale $(-\infty, 0\rangle$ s rastúcimi hodnotami premennej x funkčné hodnoty $f(x)$ klesajú (hovoríme, že funkcia f je na tomto intervale *klesajúca*), zatiaľ čo na intervale $\langle 0, \infty)$ rastú (funkcia f je na ňom *rastúca*). Pretože funkčné hodnoty nie sú zrejme zhora ohraničené žiadnou konštantou, hovoríme, že f je *zhora neohraničená*. Existuje však konštanta, ktorá zdola ohraničuje funkčné hodnoty (t.j. $\exists c \in E\, \forall x \in E\ c \leq f(x)$; napr. $c = 0$), preto hovoríme, že f je *zdola ohraničená*. Graf funkcie je súmerný podľa osi y, čo korešponduje s faktom, že $f(-x) = f(x)$ pre všetky $x \in E$. V takom prípade hovoríme, že funkcia je *párna*. Ak graf funkcie je súmerný podľa počiatku súradnicovej sústavy $[0, 0]$, t.j. $f(-x) = -f(x)$ pre všetky $x \in E$, hovoríme, že funkcia je *nepárna* (obr. 2).

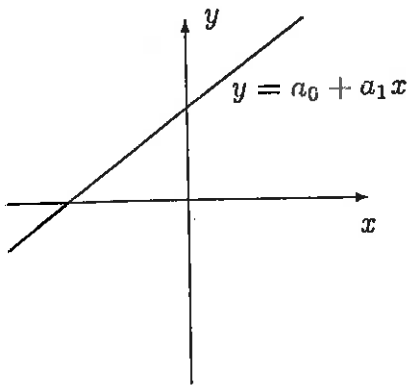
V tejto kapitole vymenujeme najzákladnejšie reálne funkcie reálnej premennej, niektoré ich vlastnosti a načrtneme ich grafy. *Elementárnymi funkciami* nazveme všetky funkcie, ktoré možno z funkcií v 1.-12. nasledujúceho zoznamu dostať pomocou konečného počtu operácií súčtu, súčinu, podielu, odmocňovania a tvorenia zloženej funkcie.

1. **Konštantná funkcia:** $f(x) = a_0$ $(a_0 \in E)$. $\mathcal{D}(f) = E$, $\mathcal{H}(f) = \{a_0\}$. Jej

grafom (obr. 3) je priamka prechádzajúca bodom $[0, a_0]$ na osi y a rovnobežná s osou x. Táto funkcia je ohraničená (zhora i zdola), nie je ani rastúca ani klesajúca (na žiadnom intervale) a je párna.



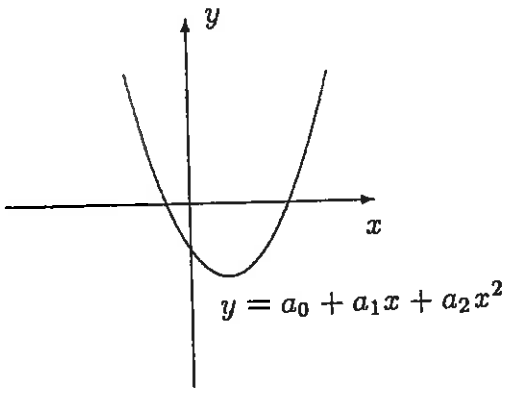
Obr. 3



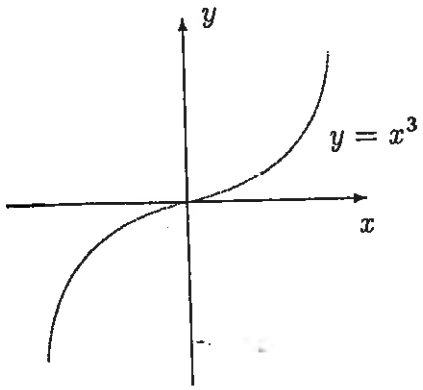
Obr. 4

2. **Lineárna funkcia:** $f(x) = a_0 + a_1.x$ $(a_0, a_1 \in E,\ a_1 \neq 0)$. $\mathcal{D}(f) = E$, $\mathcal{H}(f) = E$. Jej grafom (obr. 4) je priamka prechádzajúca bodmi $[-\frac{a_0}{a_1}, 0]$ a $[0, a_0]$. Je zhora i zdola neohraničená. Na celom intervale $(-\infty, \infty)$ je pre $a_1 > 0$ rastúca a pre $a_1 < 0$ klesajúca. Pre $a_0 = 0$ je nepárna.

3. **Kvadratická funkcia:** $f(x) = a_0 + a_1.x + a_2.x^2$ $(a_0, a_1, a_2 \in E,\ a_2 \neq 0)$. $\mathcal{D}(f) = E$, $\mathcal{H}(f) = \langle a_0 - \frac{a_1^2}{4a_2}, \infty)$ pre $a_2 > 0$ a $\mathcal{H}(f) = (-\infty, a_0 - \frac{a_1^2}{4a_2}\rangle$ pre $a_2 < 0$. Jej grafom (obr. 5) je parabola s osou súmernosti, ktorá prechádza vrcholom $[-\frac{a_1}{2a_2}, a_0 - \frac{a_1^2}{4a_2}]$ paraboly a je rovnobežná s osou y. V prípade $a_2 > 0$ je zdola ohraničená a zhora neohraničená, v prípade $a_2 < 0$ je to naopak. Pre $a_2 > 0$ je na intervale $(-\infty, -\frac{a_1}{2a_2}\rangle$ klesajúca a na intervale $\langle -\frac{a_1}{2a_2}, \infty)$ rastúca, pre $a_2 < 0$ naopak. Ak $a_1 = 0$ (t.j. vrchol paraboly je na osi y), je párna.



Obr. 5



Obr. 6

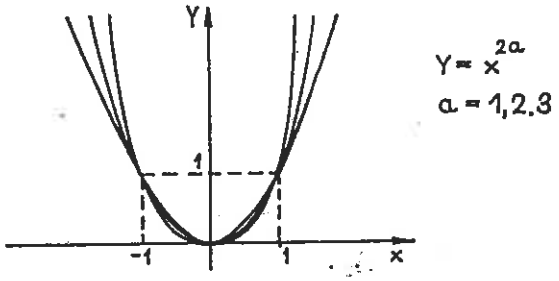
4. **Kubická funkcia:** $f(x) = a_0 + a_1.x + a_2.x^2 + a_3.x^3$ $(a_0, a_1, a_2, a_3 \in E,\ a_3 \neq 0)$. $\mathcal{D}(f) = E$, $\mathcal{H}(f) = E$. Podobne ako lineárna funkcia je zdola i zhora neohraničená. Jej graf prechádza bodom $[0, a_0]$. Na obr. 6 je graf funkcie $f(x) = x^3$,

ktorá je nepárna.

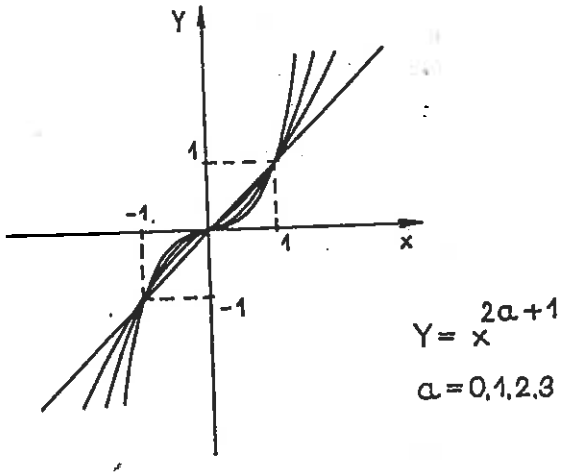
Predchádzajúce 4 typy funkcií sú špeciálnymi prípadmi **polynomickej funkcie** $f(x) = a_0 + a_1.x + a_2.x^2 + \cdots + a_n.x^n$ $(a_0, a_1, a_2, \ldots, a_n \in E,\ a_n \neq 0,\ n \in N)$. Jej definičným oborom je celá množina E. Náčrt jej grafu a popis vlastností je zrejme tým menej komplikovaný, čím menšie je n a čím menej má nenulových koeficientov a_i.

5. **Racionálna funkcia:** $f(x) = \frac{p(x)}{q(x)}$, kde $p(x), q(x)$ sú polynomické funkcie a $q(x)$ nie je polynomická funkcia rovná nule. Jej definičným oborom je množina E okrem koreňov polynómu $q(x)$, t.j. okrem $x \in E$ pre ktoré $q(x) = 0$. Jej graf je vo všeobecnosti nesúmerný.

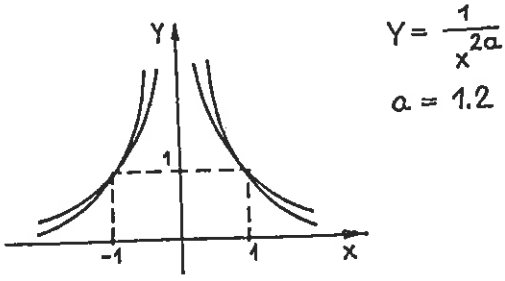
6. **Mocninová funkcia s celočíselným exponentom:** $f(x) = x^n$ $(n \in Z)$. Pre $n > 0$ je to polynomická funkcia s jediným nenulovým koeficientom $a_n = 1$, preto náčrt jej grafu nie je príliš komplikovaný (pozri obr. 7 pre $n = 2, 4, 6$ a obr. 8 pre $n = 1, 3, 5, 7$).



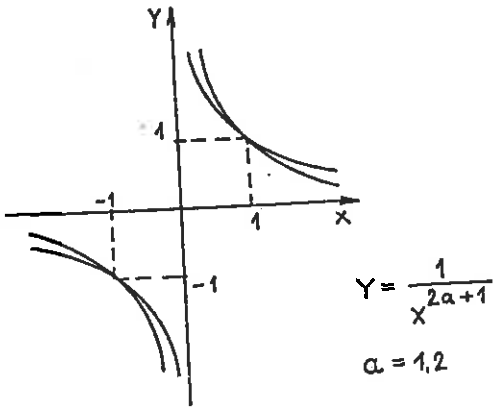
Obr. 7



Obr. 8



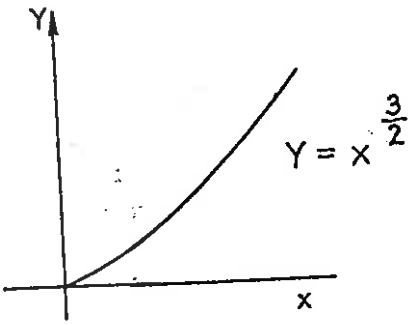
Obr. 9



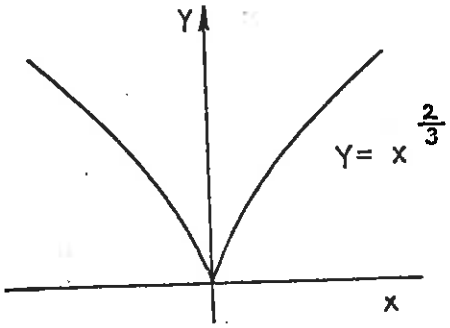
Obr. 10

V prípade párneho n je $\mathcal{H}(f) = \langle 0, \infty)$ a (podobne ako kvadratická funkcia s $a_2 > 0$, $a_1 = 0$) je zdola ohraničená, zhora neohraničená, párna a na intervale $(-\infty, 0\rangle$ klesajúca. V prípade nepárneho n má (podobne ako lineárna funkcia s $a_1 > 0$) obor hodnôt $\mathcal{H}(f) = E$, je zhora i zdola neohraničená a rastúca. Je nepárna. Pre $n = 0$ je to konštantná funkcia rovná 1 s definičným oborom $E - \{0\}$. Pre $n < 0$ je to racionálna funkcia $\frac{1}{x^{-n}}$ s definičným oborom $\mathcal{D}(f) = E - \{0\}$, ktorej graf vieme opäť bez väčších komplikácií načrtnúť (pre $n = -2, -4$ pozri obr. 9 a pre $n = -3, -5$ pozri obr. 10). Vlastnosti tejto funkcie zrejme opäť súvisia s paritou čísla n a na základe obr. 9, 10 niektoré z nich čitateľ ľahko „odhalí".

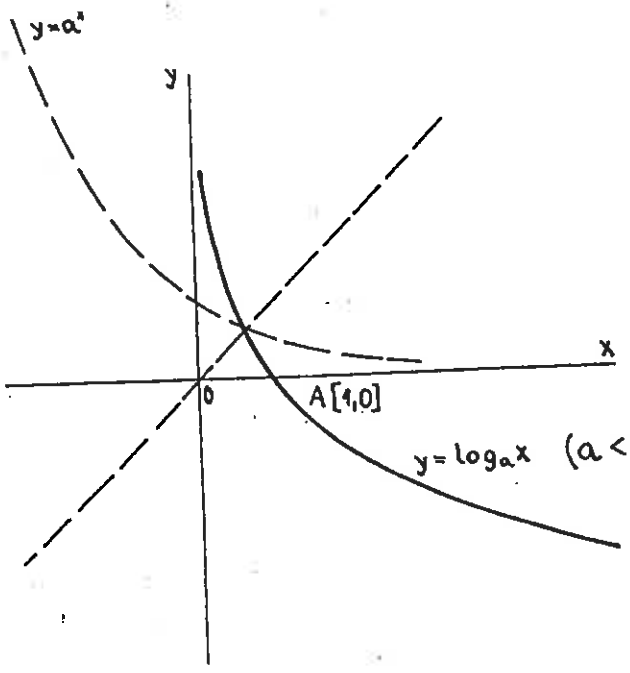
7. **Odmocninová funkcia:** $f(x) = \sqrt[n]{x}$ $(n \in N)$. Pre párne n je definovaná len na intervale $\langle 0, \infty)$ (a $f(x)$ je také nezáporné reálne číslo, že $f(x)^n = x$), zatiaľ čo pre nepárne n jej definičným oborom je celá množina E (a $f(x)$ je také reálne číslo, že $f(x)^n = x$).



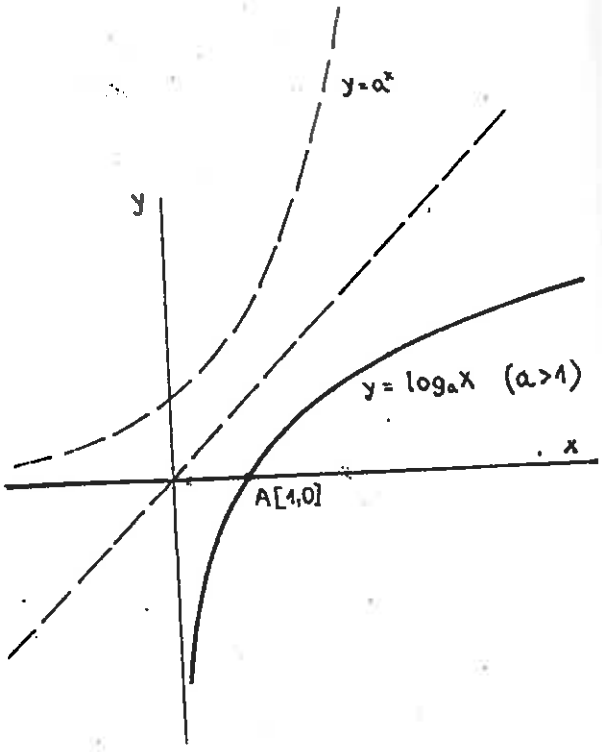
Obr. 11



Obr. 12



Obr. 13



Obr. 14

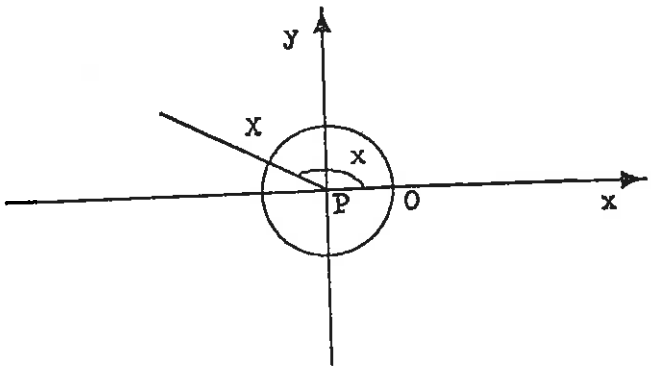
8. **Mocninová funkcia s racionálnym exponentom:** $f(x) = x^{\frac{p}{q}} = \sqrt[q]{x^p}$ ($p \in Z$, $q \in N$, $q \neq 0$, p, q sú nesúdeliteľné). V prípade $p > 0$ je pre párne q definovaná na intervale $\langle 0, \infty)$ (pozri obr. 11), pre nepárne q na celej množine E (pozri obr. 12) a pri pohľade na obr. 11, 12 čitateľ zaiste vidí niektoré jej vlastnosti. Ak $p \leq 0$ tak z definičného oboru treba naviac vynechať číslo 0.

9. **Exponenciálna funkcia:** $f(x) = a^x$ ($a \in E^+ - \{1\}$). $\mathcal{D}(f) = E$, $\mathcal{H}(f) = (0, \infty)$. Jej graf vždy prechádza bodom $[0, 1]$. Pre $a = 1$ je to konštantná funkcia rovná 1. Pre $0 < a < 1$ náčrt jej grafu vidíme na obr. 13. Je zhora neohraničená, zdola ohraničená (nie však žiadnou kladnou konštantou!) a klesajúca. Pre $a > 1$ je náčrt jej grafu na obr. 14, je rastúca a vlastnosti ohraničenosti sú rovnaké ako v predchádzajúcom prípade.

10. **Logaritmická funkcia:** $f(x) = \log_a x$ ($a \in E^+$, $a \neq 1$). $\mathcal{D}(f) = (0, \infty)$, $\mathcal{H}(f) = E$. Je to inverzná funkcia (inverzné zobrazenie) k exponenciálnej funkcii $y = a^x$, t.j. $f(x)$ je také reálne číslo, že $x = a^{f(x)}$. Jej graf vždy prechádza bodom $[1, 0]$. Pre $0 < a < 1$ náčrt jej grafu (a inverznosť k funkcii $y = a^x$) vidíme na obr. 13 a pre $a > 1$ na obr. 14. Jej základné vlastnosti vidíme na týchto obrázkoch a ľahko ich možno odvodiť z vlastností exponenciálnej funkcie na základe inverznosti. Pre $a = 10$ jej hodnoty nazývame dekadické logaritmy a označujeme $\log x$ (symbol $a = 10$ nepíšeme) a pre $a = e \doteq 2,71828$ jej hodnoty nazývame prirodzené logaritmy a označujeme $\ln x$.

11. **Goniometrické funkcie:** a) $f(x) = \sin x$, $f(x) = \cos x$.

Pre ľubovoľné $x \in E$ možno hodnoty $\sin x$ a $\cos x$ definovať geometricky takto: V rovine s pravouhlým súradnicovým systémom zvoľme kružnicu so stredom v počiatku $P \equiv [0, 0]$ a polomerom 1 a na nej bod $O \equiv [1, 0]$. Nech X je taký bod na kružnici, že veľkosť uhla $\angle OPX$ v radiánoch je dané reálne číslo x. Potom $X \equiv [\cos x, \sin x]$, t.j. hodnoty $\sin x$ a $\cos x$ sa určia ako druhá a prvá súradnica bodu X.



Z definície vyplýva, že

(i) $\sin(x + 2k\pi) = \sin x$ a $\cos(x + 2k\pi) = \cos x$ pre ľubovoľné $x \in E$ a $k \in Z$ - hovoríme, že funkcie sínus a kosínus sú *periodické s periódou* 2π.

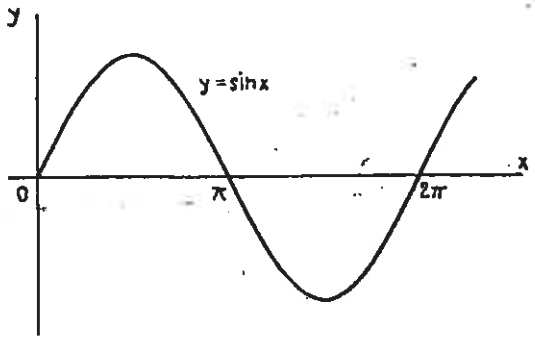
(ii) $\sin(-x) = -\sin x$ a $\cos(-x) = \cos x$ pre ľubovoľné $x \in E$, t.j. funkcia sínus

je nepárna a funkcia kosínus je párna.

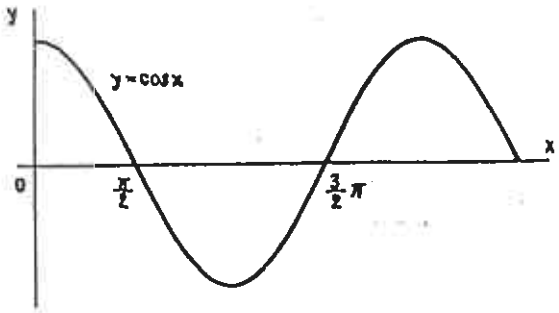
(iii) funkcia sínus je rastúca na intervaloch $\langle -\frac{\pi}{2} + 2k\pi, \frac{\pi}{2} + 2k\pi \rangle$ a klesajúca na intervaloch $\langle \frac{\pi}{2} + 2k\pi, \frac{3\pi}{2} + 2k\pi \rangle$ $(k \in Z)$; funkcia kosínus je klesajúca na intervaloch $\langle 0 + 2k\pi, \pi + 2k\pi \rangle$ a rastúca na intervaloch $\langle \pi + 2k\pi, 2\pi + 2k\pi \rangle$ $(k \in Z)$.

(iv) $\sin^2 x + \cos^2 x = 1$ - užitočný vzorec, ktorý ľahko odvodíme na základe Pytagorovej vety.

Funkcie sínus a kosínus majú teda definičný obor E, obor hodnôt $\langle -1, 1 \rangle$ a náčrty ich grafov sú na obr. 15, 16 (keďže funkcia sínus je nepárna a funkcia kosínus je párna a obe sú periodické, na obr. 15 a 16 si „chýbajúcu" časť grafu na intervale $(-\infty, 0\rangle$ vieme predstaviť).

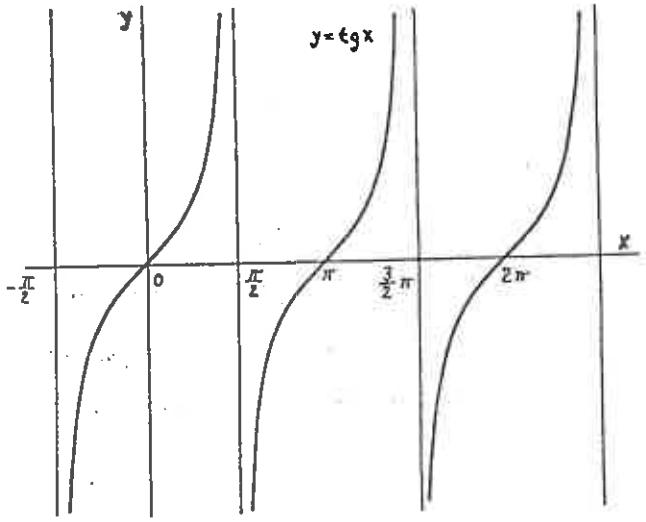


Obr. 15

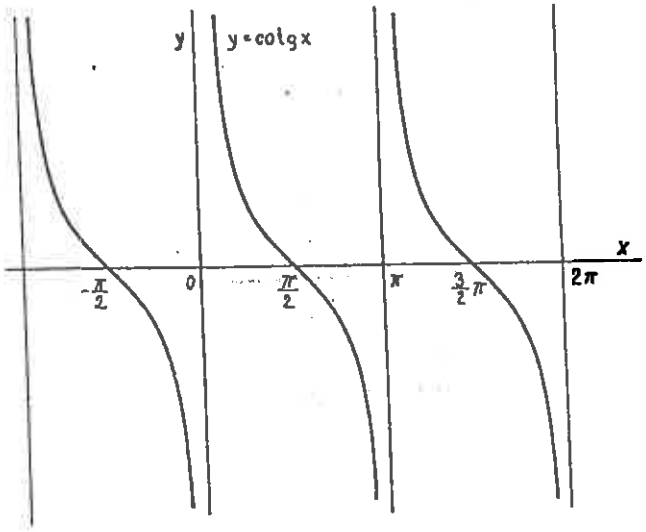


Obr. 16

b) $f(x) = \operatorname{tg} x$ a $f(x) = \operatorname{cotg} x$. Funkcia $f(x) = \operatorname{tg} x = \frac{\sin x}{\cos x}$ je definovaná pre všetky $x \in E$ pre ktoré $\cos x \neq 0$, t.j. jej definičným oborom je $E - \{(2k+1)\frac{\pi}{2};\ k \in Z\}$ (obr. 17). Funkcia $f(x) = \operatorname{cotg} x = \frac{\cos x}{\sin x}$ je definovaná pre všetky $x \in E$ pre ktoré $\sin x \neq 0$, t.j. jej definičným oborom je $E - \{k\pi;\ k \in Z\}$ (obr. 18).



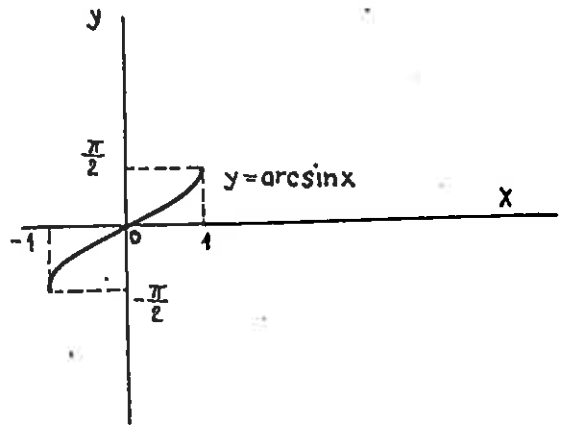
Obr. 17



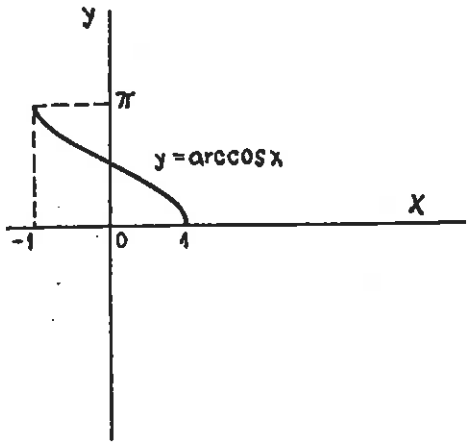
Obr. 18

Z obr. 17, 18 je možné usúdiť, ktoré základné vlastnosti majú funkcie tangens a kotangens. (Pokúste sa o to).

12. **Cyklometrické funkcie:** $f(x) = \arcsin x$, $f(x) = \arccos x$, $f(x) = \operatorname{arctg} x$ a $f(x) = \operatorname{arccotg} x$. Sú to inverzné funkcie (inverzné zobrazenia) postupne k zúženiu funkcie sínus na interval $\langle -\frac{\pi}{2}, \frac{\pi}{2} \rangle$, k zúženiu funkcie kosínus na interval $\langle 0, \pi \rangle$, k zúženiu funkcie tangens na interval $(-\frac{\pi}{2}, \frac{\pi}{2})$ a k zúženiu funkcie kotangens na interval $(0, \pi)$. Preto definičným oborom funkcií arkussínus resp. arkuskosínus je interval $\langle -1, 1 \rangle$ a tento zobrazujú na interval $\langle -\frac{\pi}{2}, \frac{\pi}{2} \rangle$ resp. $\langle 0, \pi \rangle$ (pozri obr. 19 a obr. 20). Ich základné vlastnosti možno odvodiť z vlastností funkcií sínus resp. kosínus na základe inverznosti.

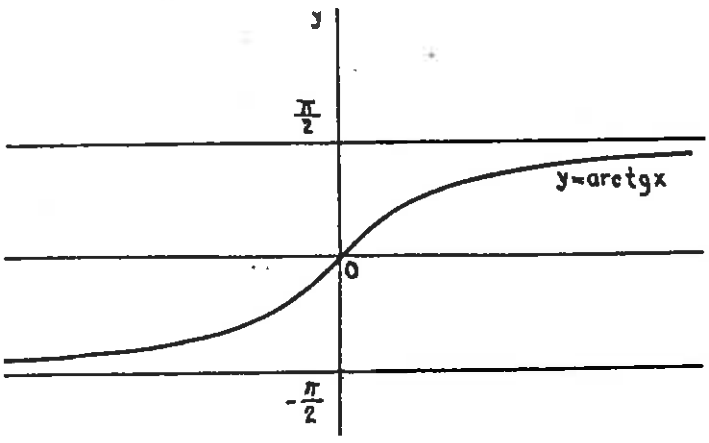


Obr. 19

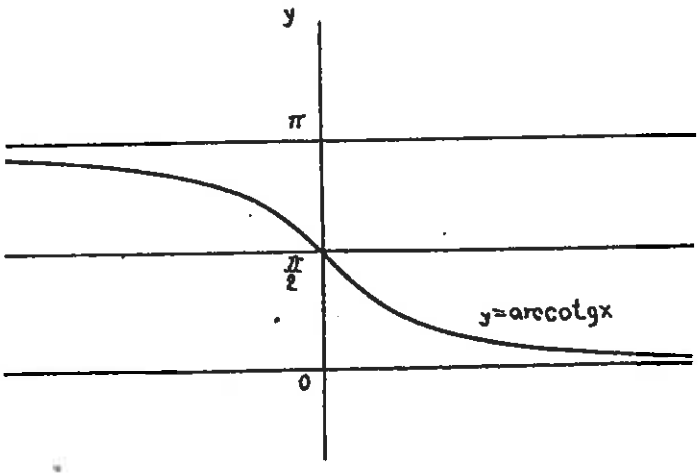


Obr. 20

Funkcia arkustangens zobrazuje E na interval $(-\frac{\pi}{2}, \frac{\pi}{2})$ (obr. 21) a funkcia arkuskotangens zobrazuje E na interval $(0, \pi)$ (obr. 22). Funkcie arkussínus a arkustangens sú nepárne.



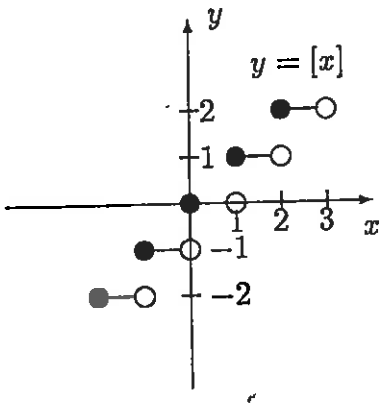
Obr. 21



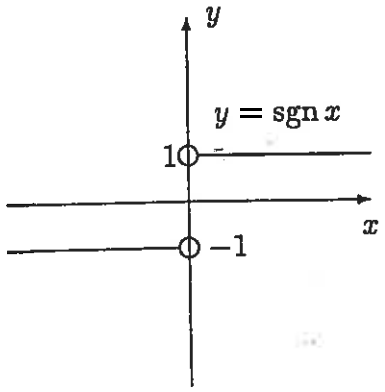
Obr. 22

Na záver nášho zoznamu sme zaradili funkcie ktoré síce nepatria do triedy elementárnych funkcií, avšak často sa s nimi v matematike stretávame.

13. **Funkcia celá časť**: $f(x) = [x]$. $\mathcal{D}(f) = E$, $\mathcal{H}(f) = Z$. Celá časť $[x]$ reálneho čísla x je definovaná ako „najbližšie" celé číslo, ktoré predchádza x, t.j. $[x] = n \in Z$, kde $n \leq x < n + 1$. Jej graf je načrtnutý na obr. 23. Je zdola i zhora neohraničená, „po častiach" konštantná (na každom podintervale $\langle n, n+1)$), $(n \in Z)$, neklesajúca.



Obr. 23



Obr. 24

14. **Funkcia signum**: $f(x) = \operatorname{sgn}(x)$ s definičným oborom E, kde

$$sgn(x) = \begin{cases} 1, & \text{ak } x > 0, \\ 0, & \text{ak } x = 0, \\ -1, & \text{ak } x < 0. \end{cases}$$

Teda $\mathcal{H}(f) = \{-1, 0, 1\}$. Jej graf je načrtnutý na obr. 24. Táto funkcia je tiež „po častiach" konštantná (na intervaloch $(-\infty, 0)$ a $(0, \infty)$) a neklesajúca, preto je zhora i zdola ohraničená.

15. **Charakteristická funkcia množiny** A, $A \subseteq E$: $f(x) = \chi_A(x)$ s definičným oborom E, kde

$$\chi_A(x) = \begin{cases} 1, & \text{ak } x \in A, \\ 0, & \text{ak } x \in E - A. \end{cases}$$

Teda $\mathcal{H}(f) = \{0, 1\}$ a funkcia je (zhora i zdola) ohraničená. Ak A je interval tvaru $(-\infty, x_0)$ alebo $(-\infty, x_0\rangle$ $(x_0 \in E)$ tak f je „po častiach" konštantná a nerastúca; ak A je interval tvaru (x_0, ∞) alebo $\langle x_0, \infty)$ $(x_o \in E)$ tak f je „po častiach" konštantná a neklesajúca; v ostatných prípadoch nie je klesajúca ani rastúca.

Charakteristická funkcia množiny Q racionálnych čísel sa nazýva **Dirichletova funkcia**. (Dá sa načrtnúť jej graf?)

Cvičenia

1. V každom z nasledujúcich príkladov elementárnej funkcie f je vašou úlohou:

(i) určiť definičný obor $\mathcal{D}(f)$;
(ii) určiť obor hondôt $\mathcal{H}(f)$;
(iii) určiť ohraničenosť (zdola, zhora) funkcie f;
(iv) určiť či je alebo nie je párna resp. nepárna;
(v) pokúsiť sa načrtnúť jej graf (začnite výpočtom $f(x)$ pre $x = -3, -2, -1, 0, 1, 2, 3$);
(vi) pokúsiť sa určiť intervaly monotónnosti (t.j. na ktorých intervaloch je rastúca či klesajúca).

a) $f(x) = 2x - 3$,
b) $f(x) = -x^2 + 4x - 5$,
c) $f(x) = x^3 - 6x^2 + 12x - 9$,
d) $f(x) = x^4 + 2x - \frac{3}{2}$,
e) $f(x) = \frac{1}{-x+2}$,
f) $f(x) = \frac{3x-5}{2x+1}$,
g) $f(x) = \frac{2}{(x-1)^2+1}$,
h) $f(x) = x^{-\frac{4}{3}} - 2$,
j) $f(x) = -2^x$,
k) $f(x) = (\frac{1}{2})^x - 1$,
l) $f(x) = \log_2(-x)$,
m) $f(x) = \log_{\frac{1}{2}}(x + 1)$,
n) $f(x) = \log x - ln x$,
o) $f(x) = \sin 2x + \frac{1}{2}$,
p) $f(x) = -\mathrm{tg}(x - \frac{\pi}{2})$,
r) $f(x) = \arccos(x + 1)$,
s) $f(x) = \mathrm{arccotg}(-x) + \frac{\pi}{2}$,
t) $f(x) = -[x] + 1$,
u) $f(x) = \mathrm{sgn}(\frac{2x-3}{x+1})$,
v) $f(x) = \chi_{\bigcup_{k\in Z}(-1+2k, \frac{1}{2}+2k)}(x)$.

2. Určte definičný obor a obor hodnôt funkcie f danej predpisom

a) $y = 3^x + \sin 2x$,
b) $y = \sqrt{4 - 2x - x^2} + \log(1 - x)$,
c) $y = \arccos(2x - 3)$,
d) $y = \ln(e^x - e^{-x}) + \mathrm{cotg}\sqrt{x^3}$,
e) $y = \mathrm{arctg}\frac{x+1}{x-1} + \cos(\log_{\frac{1}{2x+3}})$,
f) $y = \sqrt{\ln \sin x}$.

3. Zistite, či nasledujúce funkcie sú párne alebo nepárne:

a) $f(x) = \frac{x}{\cos x}$,
b) $g(x) = \sin x^2 - \cos 2x$,
c) $h(x) = \frac{e^x-1}{e^x+1}$,
d) $k(x) = \ln\frac{x}{|x|}$,
e) $l(x) = -\frac{2^x}{2^{-x}}$,

f) $m(x) = \frac{x+\mathrm{tg}x}{\sqrt{1-x^2}} + x.\ln|x|$.

4. Pre každú podmnožinu U množiny V nasledujúcich vlastností funkcií nájdite príklad funkcie, ktorá má vlastnosti z U a nemá vlastnosti z $V - U$:

a) $V = \{$zdola ohraničená, rastúca, párna$\}$;

b) $V = \{$ohraničená, monotónna, nepárna$\}$.

UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI

Pedagogická fakulta

ÚVOD DO ŠTÚDIA MATEMATIKY

P. Klenovčan, A. Haviar, M. Haviar

1996

Obsah

12. Binárne operácie a algebry

Špeciálnym typom zobrazení sú operácie, o ktorých sme sa krátko zmienili v závere kapitoly 3. S niektorými operáciami ste sa oboznámili už na základnej a strednej škole. Napríklad odčítanie prirodzených čísel možno chápať ako zobrazenie, ktoré k usporiadanej dvojici $[a, b]$ prirodzených čísel, v prípade $a > b$, priradí prirodzené číslo $a - b$. Skalárny súčin vektorov je zobrazenie, ktoré k usporiadanej dvojici vektorov $[\vec{u}, \vec{v}]$ priradí ich skalárny súčin (reálne číslo) $\vec{u}.\vec{v}$, atď. Pri skúmaní vlastností binárnych operácií sa však kvôli jednoduchosti obmedzíme len na také operácie akými sú napríklad sčítanie a násobenie čísel (prirodzených, celých, racionálnych, reálnych), ktoré možno chápať ako zobrazenia priraďujúce každej dvojici čísel a, b z daného číselného oboru A ich súčet $a + b$ resp. ich súčin $a.b$, t.j opäť číslo z A. Sú to zobrazenia množiny $A \times A$ do A. Podobne napríklad zjednotenie a prienik množín sú zobrazenia, ktoré každej dvojici prvkov $A, B \in P(M)$ ($P(M)$ je potenčná množina nejakej množiny M) priradia prvok $A \cup B \in P(M)$ resp. $A \cap B \in P(M)$. Sú to zobrazenia množiny $P(M) \times P(M)$ do množiny $P(M)$.

Definícia 1. Binárna operácia na množine A je zobrazenie množiny $A \times A$ do A.

Binárna operácia priraďuje teda každej dvojici prvkov $[a, b] \in A \times A$ nejaký prvok, „výsledok", ktorý opäť patrí do A. Obvyklé sčítanie, odčítanie a násobenie sú preto binárnymi operáciami na množinách celých, racionálnych a reálnych čísel, ale odčítanie nie je binárna operácia na množine prirodzených čísel. Podobne delenie nie je binárna operácia na množine nenulových celých čísel, ale je binárna operácia na množine nenulových racionálnych čísel (cvičenie 1a).

Binárne operácie označujeme symbolmi $+, ., \cup, \cap, \circ, \Box, *, \triangle, \oplus, \odot$ a pod. Obraz usporiadanej dvojice $[a, b]$ napr. v operácii $*$ budeme označovať $a * b$ (podobne ako obraz usporiadanej dvojice [a,b] pri sčitovaní sme zvyknutí označovať $a + b$ a nie $+([a, b])$).

Vieme, že pri sčítaní alebo násobení dvoch čísel a, b je $a + b = b + a$ a $a.b = b.a$. Tiež vieme, že pri sčítaní viacerých čísel alebo pri násobení viacerých čísel nemusíme používať zátvorky, pretože bez ohľadu na to v akom poradí prevádzame jednotlivé sčítania resp. násobenia, výsledok je vždy rovnaký. Toto pozorovanie teraz zovšeobecníme.

Definícia 2. Binárna operácia $*$ na množine A je komutatívna, ak

$$\forall a, b \in A \quad a * b = b * a.$$

Definícia 3. Binárna operácia $*$ na množine A je asociatívna, ak

$$\forall a, b, c \in A \quad (a * b) * c = a * (b * c).$$

Komutatívnosť a asociatívnosť sú dôležité vlastnosti binárnych operácií. Mnohé známe operácie tieto vlastnosti majú – operácie sčítania a násobenia reálnych čísel, zjednotenia a prieniku množín a pod. Iné známe operácie tieto vlastnosti nemajú ako ukazuje aj nasledujúci príklad.

Príklad 1. a) Umocňovanie na množine N^+ kladných prirodzených čísel je zobrazenie $N^+ \times N^+ \to N^+$ dané predpisom

$$a * b = a^b.$$

Je to binárna operácia, ktorá nie je komutatívna ($1 * 2 = 1 \neq 2 = 2 * 1$) ani asociatívna ($(2 * 1) * 2 = 4 \neq 2 = 2 * (1 * 2)$).

b) Odčítanie na množine celých čísel je binárna operácia, ktorá nie je komutatívna ($1 - 2 \neq 2 - 1$) ani asociatívna ($(1 - 2) - 3 \neq 1 - (2 - 3)$).

c) Analogicky možno overiť, že operácia (slovo „binárna" budeme často vynechávať) delenia na množine nenulových racionálnych čísel nie je komutatívna ani asociatívna (cvičenie 1b). □

Nasledujúci príklad dáva návod ako možno ľubovoľnú operáciu na danom číselnom obore „preniesť" na množinu všetkých zobrazení (funkcií) na tomto číselnom obore.

Príklad 2. Nech R^R označuje množinu všetkých reálnych funkcií reálnej premennej, t.j. všetkých zobrazení $R \to R$. Operácia sčítania $\oplus$ a operácia násobenia $\odot$ funkcií sú definované „bodovo", t.j. predpisom

$$(f \oplus g)(x) = f(x) + g(x) \quad \text{a} \quad (f \odot g)(x) = f(x) \cdot g(x) \quad \text{pre všetky } x \in R.$$

Teda hodnotu funkcie $f \oplus g$ v bode $x \in R$ vypočítame tak, že určíme hodnotu funkcie f a funkcie g v bode x a tieto dve reálne čísla sčítame obvyklým spôsobom. Podobne postupujeme pri násobení.

Pretože obvyklé sčítanie a násobenie reálnych čísel sú komutatívne operácie, platí pre všetky $x \in R$

$$(f \oplus g)(x) = f(x) + g(x) = g(x) + f(x) = (g \oplus f)(x),$$
$$(f \odot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \odot f)(x).$$

Preto $f \oplus g = g \oplus f$ a $f \odot g = g \odot f$, teda aj operácie $\oplus$ a $\odot$ sčítania resp. násobenia reálnych funkcií sú komutatívne. Analogicky možno ukázať, že operácie $\oplus$ a $\odot$ sú asociatívne (cvičenie 1c). □

Ak množina A, na ktorej je binárna operácia $*$ definovaná je konečná (a nemá veľa prvkov), je zaužívané operáciu $*$ opísať tzv. operačnou (alebo Cayleyho) tabuľkou. Horné a ľavé záhlavie tejto tabuľky obsahuje zoznam prvkov množiny A. (Pritom na poradí vymenovania prvkov A nezáleží, ale je zvykom dodržať rovnaké poradie prvkov pre horné i ľavé záhlavie tabuľky – pozri tab. 1.) Do priesečníka oboch záhlaví píšeme operačný symbol a do priesečníka riadka obsahujúceho prvok a a stĺpca obsahujúceho prvok b vpisujeme „výsledok" $a * b$. Operačná tabuľka prehľadným spôsobom vyjadruje, na akej množine je operácia definovaná a ako na nej „funguje", preto niekedy definujeme operáciu priamo prostredníctvom operačnej tabuľky.

Príklad 3. Nech $A = \{a, b, c, d\}$. Zobrazenie $o : A \times A \to A$ je dané „vymenovaním prvkov“: $o = \{[(a,a),c], [(a,b),a], [(a,c),d], [(a,d),c], [(b,a),a], [(b,b),b], [(b,c),c], [(b,d),d], [(c,a),d], [(c,b),c], [(c,c),b], [(c,d),b], [(d,a),c], [(d,b),d], [(d,c),b], [(d,d),a]\}$. Ak sa na zobrazenie o pozeráme ako na operáciu na A, zapíšeme ho operačnou tabuľkou

o	a	b	c	d
a	c	a	d	c
b	a	b	c	d
c	d	c	b	b
d	c	d	b	a

Tab. 1

Toto vyjadrenie operácie (zobrazenia) o je prehľadné a niektoré jej (jeho) vlastnosti z neho možno ľahko vidieť. Napríklad vidíme, že tabuľka je súmerná podľa diagonály prechádzajúcej operačným symbolom o, čo znamená, že operácia o je komutatívna. (Presvedčte sa o tom.) Operácia o nie je asociatívna (čo v tomto prípade z tabuľky hneď nevidíme a môžeme zistiť zrejme iba postupným preverovaním podľa definície 3), lebo napr. $(d \circ c) \circ c = b \circ c = c \neq d \circ (c \circ c) = d \circ b = d$. □

Osobitnú pozornosť si pri binárnych operáciach zasluhuje prvok, ktorý „neovplyvňuje výsledok operácie“. Pri sčitovaní čísel je takým prvkom 0, pri násobení 1, pri zjednotení množín $\emptyset$ a pri skladaní zobrazení identické zobrazenie.

Definícia 4. Nech $*$ je binárna operácia na množine A. Ak v množine A existuje prvok e, o ktorom platí

$$\forall a \in A \quad a * e = e * a = a$$

tak ho nazývame neutrálnym prvkom operácie $*$.

Príklad 4. Operácia o z príkladu 3 má neutrálny prvok b. Spoznáme ho na operačnej tabuľke podľa toho, že riadok i stĺpec tabuľky odpovedajúci prvku b je totožný s príslušným záhlavím tabuľky. Aj v príklade 2 majú operácie $\oplus$ a $\odot$ neutrálne prvky. U operácie $\oplus$ je to konštantná funkcia nadobúdajúca v každom bode hodnotu 0 (jej grafom je „os x“) a u operácie $\odot$ je to konštantná funkcia nadobúdajúca v každom bode hodnotu 1. □

Z nasledujúceho tvrdenia vyplýva, že binárna operácia na množine buď nemá neutrálny prvok alebo má jediný neutrálny prvok.

Veta 1. *Každá binárna operácia môže mať najviac jeden neutrálny prvok.*

Dôkaz. Predpokladajme, ze by nejaká binárna operácia $*$ na množine A mala neutrálne prvky e_1, e_2. Potom $e_1 * e_2 = e_1$, lebo e_2 je neutrálny prvok a podobne $e_1 * e_2 = e_2$, lebo e_1 je neutrálny prvok. Teda $e_1 = e_2$. □

Definícia 5. Nech $*$ je binárna operácia na množine A s neutrálnym prvkom e. Ak k prvku $a \in A$ existuje prvok $b \in A$ tak, že platí

$$a * b = b * a = e$$

tak prvok b nazývame inverzným prvkom k prvku a (vzhľadom na operáciu $*$).

Z definície 5 vidíme, že ak b je inverzným prvkom k a, tak aj obrátene, a je inverzným prvkom k b. Tiež vidíme, že neutrálny prvok e (ak existuje) má vždy inverzný prvok, ktorým je opäť e.

Príklad 5. a) U operácie sčítania celých (racionálnych, reálnych) čísel je číslo $-a$ inverzným prvkom k číslu a. Všimnime si, že u operácie sčítania prirodzených čísel má jedine číslo 0 (neutrálny prvok operácie sčítania) inverzný prvok.

b) U operácie násobenia na množine celých čísel majú len prvky 1 a -1 inverzné prvky. U operácie násobenia racionálnych (reálnych) čísel má každé číslo $a \neq 0$ inverzný prvok $\frac{1}{a}$. Číslo 0 nemá inverzný prvok vzhľadom na operáciu násobenia.

c) V príklade 2 je k ľubovoľnej funkcii f inverzným prvkom vzhľadom na operáciu $\oplus$ funkcia $-f$ definovaná predpisom $(-f)(x) = -(f(x))$ pre všetky $x \in R$. Jej graf je súmerný s grafom funkcie f podľa osi x.

Inverzné prvky vzhľadom na operáciu $\odot$ existujú len k tým funkciám $f \in R^R$, ktoré nenadobúdajú v žiadnom bode nulovú hodnotu (ich graf nepretína os x). Inverzným prvkom k takej funkcii f je funkcia $\frac{1}{f}$ definovaná predpisom $\frac{1}{f}(x) = \frac{1}{f(x)}$ pre všetky $x \in R$.

d) V príklade 3 prvok a nemá inverzný prvok, k prvku b (neutrálnemu) je inverzným prvkom (nutne) b, prvok d má inverzný prvok c a prvok c má dva inverzné prvky c a d. □

Ak operácia je asociatívna, nemôže nastať situácia ako v príklade 5d, že niektorý prvok má viac ako jeden inverzný prvok.

Veta 2. *Ak binárna operácia na množine A je asociatívna, tak každý prvok množiny A má nanajvýš jeden inverzný prvok.*

Dôkaz. Predpokladajme, že a_1, a_2 sú inverzné prvky k prvku a vzhľadom na asociatívnu operáciu $*$ s neutrálnym prvkom e. Potom s využitím asociatívnosti dostávame

$$a_1 = a_1 * e = a_1 * (a * a_2) = (a_1 * a) * a_2 = e * a_2 = a_2. \quad \square$$

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*. Množinu A nazývame *nosičom* danej algebry. V druhej časti tejto kapitoly sa budeme zaoberať niektorými najzákladnejšími typmi (binárnych) algebier.

Definícia 6. Algebru $(A, *)$ s jednou binárnou operáciou nazývame grupoid.

Niekedy hovoríme stručne, že A je grupoid, ak je z kontextu jasné, ktorú operáciu na A máme na mysli.

Príklad 6. Algebry $(N,+),(N,.),(Z,-),(Q-\{0\},:),(R^R,\oplus),(R^R,\odot)$ sú grupoidy. □

Pri skúmaní algebier často pracujeme s grupoidami, ktoré sú „časťou" daného grupoidu. Napríklad namiesto grupoidu $(N,+)$ nás často zaujíma len podmnožina $kN = \{k.n;\ n \in N\}$ k-násobkov prirodzených čísel (všimnime si, že $2N$ je množina párnych prirodzených čísel). Ľahko sa nahliadne (pozri príklad 7a), že pre ľubovoľné prirodzené číslo k množina kN s operáciou $+$ obvyklého sčítania je opäť grupoid. Budeme hovoriť, že $(kN,+)$ je podgrupoid grupoidu $(N,+)$ v zmysle nasledujúcej definície.

Definícia 7. Nech $(A,*)$ je grupoid a nech $\emptyset \neq B \subseteq A$. Ak operáciu $*$ možno *zúžiť* na podmnožinu B, t.j. ak platí

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

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

V uvedenej definícii sme operáciu na A aj jej zúženie na B označili rovnako. V matematike je takéto označenie obvyklé.

Príklad 7. a) Podmnožina $kN = \{k.n;\ n \in N\}$ k-násobkov prirodzených čísel je podgrupoid grupoidu $(N,+)$ a $(kN,.)$ je podgrupoid grupoidu $(N,.)$, lebo pre všetky
$a = k.n$, $b = k.m$ $(n,m \in N)$ platí $a+b = k.n + k.m = k.(n+m) \in kN$ a $a.b = k.n.k.m = k.(k.n.m) \in kN$, t.j. sčítaním a násobením k-násobkov prirodzených čísel dostaneme vždy opäť k-násobok prirodzeného čísla.

b) podmnožina kZ k-násobkov celých čísel je podgrupoid grupoidu $(Z,-)$. Avšak N ani žiadna z jej podmnožín kN nie sú podgrupoidy grupoidu $(Z,-)$ (cvičenie 6a).

c) Podgrupoidmi grupoidu $(R,.)$ sú napr. podmnožiny R^+, Q, $Q-\{0\}$, Z, N, $\{1,-1\}$. Podmnožina R^- nie je podgrupoidom grupoidu $(R,.)$, na druhej strane je ale podgrupoidom grupoidu $(R,+)$ (cvičenie 6b). □

Ak $(A,*)$ je grupoid a neprázdna podmnožina $B \subseteq A$ netvorí jeho podgrupoid, t.j. existujú prvky $a,b \in B$ tak, že $a*b \notin B$, zaujíma nás ako vyzerá najmenší podgrupoid grupoidu A obsahujúci množinu B. Najmenší podgrupoid grupoidu A obsahujúci množinu B nazývame *podgrupoid generovaný množinou* B a označujeme ho $[B]$. Prvky množiny B nazývame *generátory* grupoidu $([B],*)$. Ak množina B je konečná, napr. $B = \{b_1,\ldots,b_n\}$, namiesto označenia $[\{b_1,\ldots,b_n\}]$ používame označenie $[b_1,\ldots,b_n]$. Jednoznačnú existenciu podgrupoidu $[B]$ nám zaručuje nasledujúca veta (uvedieme ju bez dôkazu).

Veta 3. *Nech $(A,*)$ je grupoid a B je ľubovoľná jeho neprázdna podmnožina. Potom podgrupoid generovaný množinou B je jednoznačne určený vzťahom*

$$[B] = \bigcap\{A';\ A' \text{je podgrupoid } A \text{ a } B \subseteq A'\}.$$

Teda $[B]$ je prienikom všetkých podgrupoidov grupoidu A, ktoré obsahujú množinu generátorov B.

Príklad 8. a) Ukážeme, že podgrupoid [2] grupoidu $(N,+)$ generovaný prvkom $2 \in N$ je množina $2N^+ = \{2n \mid n \in N^+\}$ párnych kladných prirodzených čísel. Najprv si všimnime, že podmnožina $2N^+$ je podgrupoid grupoidu $(N,+)$, lebo pre všetky $2n, 2m \in 2N^+$ je $2n + 2m = 2(n+m) \in 2N^+$. Podľa definície 7, každý podgrupoid B grupoidu N obsahujúci číslo 2 musí obsahovať aj všetky súčty $2+2$, $2+2+2, \ldots$, t.j. čísla $2n$ pre každé $n \in N^+$, čiže musí obsahovať množinu $2N^+$. Z toho jasne vyplýva, že $2N^+$ je najmenší podgrupoid (vzhľadom na usporiadanie dané inklúziou) grupoidu N obsahujúci číslo 2. Teda $[2] = 2N^+$.

b) Podgrupoid grupoidu $(N,.)$ generovaný prvkom $2 \in N$ je množina $\{2^n;\ n \in N^+\}$ všetkých kladných mocnín čísla 2 a podgrupoid grupoidu $(Z,-)$ generovaný množinou $\{-2,2\}$ je množina $2Z$ všetkých párnych celých čísel (cvičenie 7a).

c) Z tabuľky operácie $\circ$ v príklade 3 vidíme, že podgrupoid $[b]$ grupoidu $(A,\circ)$ generovaný prvkom b je $[b] = \{b\}$, zatiaľčo $[c] = \{b,c\} = [b,c]$ ($b \in [c]$, lebo $c \circ c = b$ ale ďalšie prvky už do $[c]$ nepatria lebo $b \circ b = b$, $b \circ c = c \circ b = c$). Ďalej si všimnime, že $[a] = [c,d] = \{a,b,c,d\} = A$ (lebo napríklad $a \circ a = c$, $a \circ c = d$, $c \circ d = b$, $d \circ d = a$). Hovoríme, že prvok a resp. množina $\{c,d\}$ generuje grupoid A alebo, že grupoid A je generovaný prvkom a resp. prvkami c, d. Dá sa ľahko presvedčiť, že grupoid A je generovaný aj prvkom d a množinami $\{a,b\}$, $\{a,c\}$, $\{a,d\}$ a $\{b,d\}$ a tiež, že je generovaný každou svojou 3-prvkovou podmnožinou (cvičenie 8). □

Všimnime si, že všetky podgrupoidy v príklade 8 sú komutatívne. Pretože ide o podgrupoidy komutatívneho grupoidu, komutatívnosť vlastne „zdedili". Podobné „dedenie" sa týka aj asociatívnosti. (Nie však neasociatívnosti - všimnime si, že podgrupoid $\{b,c\}$ neasociatívneho grupoidu A v príklade 3 je asociatívny.) Zdôvodnenie nasledujúceho tvrdenia prenechávame na čitateľa.

Veta 4. *Nech $(A,*)$ je grupoid, ktorý je komutatívny (asociatívny) a má neutrálny prvok e. Potom každý jeho podgrupoid je komutatívny (asociatívny) a ak obsahuje prvok e, tak tento je jeho neutrálnym prvkom.*

Videli sme, že mnohé grupoidy okrem splnenia asociatívnosti obsahujú neutrálny prvok a s každým prvkom aj k nemu inverzný prvok. V zmysle nasledujúcej definície ich nazývame grupami.

Definícia 8. Grupoid $(A,*)$, o ktorom platí

1. operácia $*$ je asociatívna,
2. obsahuje neutrálny prvok operácie $*$,
3. obsahuje s každým prvkom aj k nemu inverzný prvok (vzhľadom na $*$)

nazývame grupou.

Definícia 9. Ak grupa $(B,*)$ je obsiahnutá v grupe $(A,*)$, t.j. $B \subseteq A$ a operácia na B je zúžením operácie na A hovoríme, že B je podgrupou A.

Ak máme grupu $(A,*)$ a nejakú jej podmnožinu $\emptyset \neq B \subseteq A$, tak ľahko vidieť, že B je podgrupou grupy A práve vtedy, keď B je podgrupoidom A, t.j.

(i) $\forall a,b \in B;\ a * b \in B$

a inverzné prvky (v grupe A) ku všetkým prvkom množiny B sú opäť v B, t.j.

(ii) $\forall b \in B;\ b^{-1} \in B$.

Skutočne, každá grupa $(B,*)$ obsiahnutá v grupe $(A,*)$ spĺňa (i), (ii) a obrátene, ak neprázdna podmnožina B grupy $(A,*)$ spĺňa (i) a (ii), tak $(B,*)$ je grupoid spĺňajúci 1. – 3. definície 8. (Prečo je splnené 2.?)

Príklad 9. a) Grupoidy $(Z,+)$, $(Q,+)$, $(R,+)$ sú grupy, pričom každá z nich je podgrupou nasledujúcej (vzhľadom na poradie v akom sme ich vymenovali). Grupoid $(N,+)$ nie je grupa.

b) Grupoidy $(Q-\{0\},.)$, $(R-\{0\},.)$ sú grupy, pričom $Q-\{0\}$ je podgrupou $R-\{0\}$. Grupoidy $(N-\{0\},.)$ a $(Z-\{0\},.)$ nie sú grupami.

c) Grupoid $(R^R,\oplus)$ z príkladu 2 je grupa, avšak grupoid $(R^R,\odot)$ nie je grupou.

d) Podgrupoid $\{b,c\}$ grupoidu $(A,\circ)$ v príklade 3 je grupa, avšak nie je podgrupou A, lebo A nie je grupa. □

Príklad 10. Nech pre ľubovoľné kladné prirodzené číslo n, označuje Z_n množinu $\{0,1,\ldots,n-1\}$. Na množine Z_n možno definovať operácie $\oplus$ a $\odot$ nasledovne: nech pre všetky $a,b\in Z_n$

$$a\oplus b=a+b\ (\mathrm{mod}\ n),\quad a\odot b=a.b\ (\mathrm{mod}\ n),$$

kde $+$ a $\cdot$ označujú obyklé sčítanie a násobenie a mod n v zátvorke znamená, že číslo pred zátvorkou vydelíme číslom n a zoberieme len zvyšok po tomto delení, čo je vždy číslo z $\{0,1,\ldots,n-1\}$. Tým, že „výsledok" bude vždy zo Z_n zabezpečíme, že $\oplus$ a $\odot$ budú operácie na Z_n. Počítanie mod 4 je ilustrované tabuľkami grupoidov $(Z_4,\oplus)$ (Tab. 2) a $(Z_4,\odot)$ (Tab. 3).

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tab. 2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tab. 3

Možno ukázať, že pre každé $n\in N^+$ je $(Z_n,\oplus)$ grupa a že $(Z_n,\odot)$ je grupa práve vtedy, keď n je prvočíslo (cvičenie 11). □

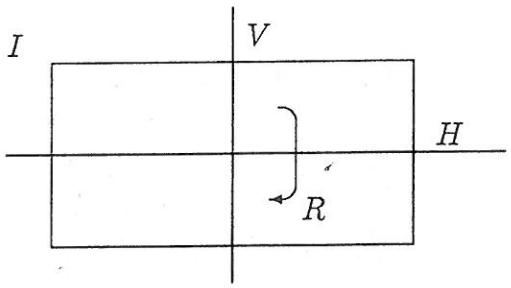
Grupy patria medzi najznámejšie algebraické štruktúry (algebry). Začali sa skúmať v 1. polovici minulého storočia, kedy dvaja mladí matematici, Francúz E. Galois (1811-1832) a Nór H. Abel (1802-1829) za pomoci grúp ukázali, že korene rovnice 5. stupňa s komplexnými koeficientami nemožno už vo všeobecnosti vypočítať z jej koeficientov pomocou operácií sčítania, odčítania, násobenia, delenia a odmocnín (tak ako vieme vypočítať podľa všeobecného vzorca korene kvadratickej rovnice a ako sa ukázalo už v 16. storočí, aj korene rovníc 3. a 4. stupňa). Galoisova teória, ktorá patrí dodnes k najkrajším výtvorom matematiky a ľudského myslenia vôbec, dala impulz mohutnému rozvoju modernej algebry, pod čím myslíme najmä skúmanie algebraických štruktúr (algebier). V tejto kapitole

je naším cieľom predovšetkým na príkladoch číselných štruktúr ilustrovať aspoň niektoré najzákladnejšie pojmy modernej algebry.

Okrem číselných štruktúr sú významnými príkladmi grúp symetrie geometrických útvarov.

Príklad 11. Pripomeňme, že pod symetriou geometrického útvaru U v rovine rozumieme zhodné zobrazenie útvaru U na seba, t.j. také zobrazenie $U \to U$, ktoré zachováva vzdialenosti bodov. Zrejme symetrie sú bijektívne zobrazenia a skladanie zobrazení $\circ$ je operácia na množine S_U všetkých symetrií útvaru U (cvičenie 12). V tomto príklade budeme skúmať štruktúru všetkých symetrií obdĺžnika vzhľadom na operáciu skladania zobrazení.

Ľahko sa presvedčíme, že jedinými symetriami (ľubovoľného) obdĺžnika sú identické zobrazenie I, otočenie o 180 stupňov R a osové súmernosti H a V podľa horizontálnej a vertikálnej osi prechádzajúcej stredom obdĺžnika (Obr. 1).



Obr. 1

$\circ$	I	R	H	V
I	I	R	H	V
R	R	I	V	H
H	H	V	I	R
V	V	H	R	I

Tab. 4

Zostavme tabuľku operácie $\circ$ na množine $S_{\square\square} = \{I, R, H, V\}$ (Tab. 4). Z tabuľky možno ľahko vidieť, že operácia $\circ$ na $S_{\square\square}$ je komutatívna, má neutrálny prvok I a každý prvok je sám k sebe inverzným prvkom. Pretože skladanie zobrazení je vždy asociatívne, $(S_{\square\square}, \circ)$ je grupa. Ľahko sa možno presvedčiť, že jej podgrupami sú $(\{I\}, \circ)$, $(\{I, R\}, \circ)$, $(\{I, H\}, \circ)$, $(\{I, V\}, \circ)$ a $(S_{\square\square}, \circ)$. □

V predchádzajúcom príklade sme sa presvedčili, že $(S_{\square\square}, \circ)$ je grupa. Teraz toto tvrdenie zovšeobecníme.

Veta 5. *$(S_U, \circ)$ je grupa pre ľubovoľný geometrický útvar U.*

Dôkaz. Pretože skladanie zobrazení je asociatívna operácia a identické zobrazenie je evidentne symetriou každého geometrického útvaru U, ostáva sa presvedčiť, že výsledkom skladania dvoch symetrií útvaru U je opäť symetria útvaru U (cvičenie 12) a že inverzné zobrazenie f^{-1} k ľubovoľnej symetrii $f \in S_U$ je bijekciou (kapitola 8) a zachováva vzdialenosti bodov útvaru U. Ukázať posledné znamená odvodiť rovnosť

$$(1) \quad d(f^{-1}(X), f^{-1}(Y)) = d(X, Y),$$

kde $d(\ ,\ )$ je reálne číslo označujúce vzdialenosť bodov v zátvorke. Pretože f je symetria, t.j. zachováva vzdialenosť bodov $f^{-1}(X)$ a $f^{-1}(Y)$, máme

$$(2) \quad d(f(f^{-1}(X)), f(f^{-1}(Y))) = d(f^{-1}(X), f^{-1}(Y)).$$

Pretože $f(f^{-1}(X)) = X$, $f(f^{-1}(Y)) = Y$, dostávame z (2) vzťah (1) a dôkaz je hotový. □

Vetu 5 možno ďalej zovšeobecniť nasledovne: namiesto geometrického útvaru U uvažujme o ľubovoľnej množine M a namiesto symetrií ako zhodných bijektívnych zobrazeniach uvažujme o všetkých bijektívnych zobrazeniach $M \to M$ (nazývame ich *transformáciami* množiny M). Dá sa ľahko ukázať, že platí

Veta 6. *Nech M je ľubovoľná neprázdna množina. Množina T_U všetkých bijektívnych zobrazení $M \to M$ s operáciou skladania zobrazení je grupa (transformácií množiny M).*

Pre daný geometrický útvar U sú teda grupa symetrií útvaru U a grupa transformácií množiny U v nasledovnom vzťahu:

Veta 7. *Grupa symetrií geometrického útvaru U je podgrupou grupy transformácií množiny U.*

V modernej algebre (teórii algebraických štruktúr) zvyčajne nerozlišujeme tie algebraické štruktúry (algebry), ktoré sa líšia iba označením prvkov a prípadne operácií. Tak napríklad grupa symetrií obdĺžnika (príklad 11) sa od grupy K_4 s operačnou tabuľkou 5 (nazývame ju Kleinova 4-prvková grupa alebo len štvorgrupa) líši len tým, že prvky I, R, H, V sú premenované postupne na $0, a, b, c$ a operácia $\circ$ na operáciu $*$. (Presvedčte sa o tom porovnaním tabuliek 4 a 5).

$*$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

Tab. 5

Fakt, že Tab. 5 je kópiou Tab. 4 (až na označenie) možno vyjadriť nasledovne: existuje bijektívne zobrazenie $f : S_{\sqsubset\sqsupset} = \{I, R, H, V\} \to \{0, a, b, c\} = K_4$ tak, že

$$\forall x, y \in S_{\sqsubset\sqsupset}; \quad f(x \circ y) = f(x) * f(y).$$

Ľahko sa napr. overí, že zobrazenie $f = \{[I, 0], [R, a], [H, b], [V, c]\}$ spĺňa túto podmienku.

Definícia 10. Nech $(A, \circ)$ a $(B, *)$ sú grupoidy (grupy). Ak existuje bijektívne zobrazenie $f : A \to B$, ktoré zachováva operáciu, t.j.

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

tak f nazývame izomorfizmus grupoidu (grupy) $(A, \circ)$ na grupoid (grupu) $(B, *)$ a hovoríme, že grupoidy (grupy) A a B sú izomorfné (označenie $A \cong B$).

Možno ukázať (podobne ako v kapitole 9 u relačných štruktúr), že ak f je izomorfizmus grupoidu (grupy) $(A, \circ)$ na grupoid (grupu) $(B, *)$, tak inverzné zobrazenie f^{-1} je izomorfizmus $(B, *)$ na $(A, \circ)$ (cvičenie 16a). Tiež sa dá ľahko ukázať, že pri izomorfizme dvoch grúp sa neutrálny prvok jednej grupy vždy zobrazuje na neutrálny prvok druhej grupy (cvičenie 16b).

Príklad 12. a) Podgrupoid $(\{b, c\}, *)$ grupoidu $(A, *)$ v príklade 3 je grupou a je izomorfný s grupou $(Z_2, \oplus)$ (príklad 10) pri izomorfizme $f = \{(b, 0), (c, 1)\}$.

b) Grupa $(S_{\square\square}, \circ)$ symetrií obdĺžnika je izomorfná s Kleinovou grupou $(K_4, *)$ (štvorgrupou). Okrem izomorfizmu f uvedeného pred definíciou 10 možno ľahko nájsť 5 ďalších izomorfizmov oboch grúp (cvičenie 17). Podgrupy $\{I, R\}$, $\{I, H\}$ a $\{I, V\}$ grupy $S_{\square\square}$ sú navzájom izomorfné a každá z nich je izomorfná s každou z podgrúp $\{0, a\}$, $\{0, b\}$, $\{0, c\}$ grupy K_4, pričom neutrálny prvok sa vždy zobrazí na neutrálny prvok.

c) Príkladom izomorfizmu grúp je aj známa logaritmická funkcia $\log : R^+ \to R$. Zobrazenie log je bijektívne a naviac platí

$$\log(x.y) = \log(x) + \log(y).$$

Preto funkcia log je izomorfizmus grupy $(R^+, .)$ na grupu $(R, +)$. □

Možno ukázať, že na ľubovoľnej množine grupoidov (grúp) je binárna relácia $\cong$ („sú izomorfné“) nielen symetrická ale aj reflexívna a tranzitívna (cvičenie 19). Teda je reláciou ekvivalencie a určuje rozklad danej množiny grupoidov (grúp), pričom do jednej triedy rozkladu patria grupoidy (grupy) navzájom izomorfné. Pri skúmaní algebraických štruktúr (ako sme už uviedli) zvyčajne grupoidy (grupy) v tej istej triede rozkladu podľa $\cong$ stotožňujeme (nepokladáme za rôzne). „Zaradenie“ jednotlivých konečných grúp do tried ekvivalencie podľa relácie $\cong$ nazývame *klasifikáciou* konečných grúp. Dá sa napríklad ukázať, že

1. Každá grupa s prvočíselným počtom prvkov p je izomorfná s grupou $(Z_p, \oplus)$.
2. Každá štvorprvková grupa je izomorfná buď s grupou $(Z_4, \oplus)$ alebo s grupou symetrií obdĺžnika (štvorgrupou).
3. Každá šesťprvková grupa je izomorfná s grupou $(Z_6, \oplus)$ alebo s grupou symetrií rovnostranného trojuholníka $(S_\triangle, \circ)$.

Tieto tvrdenia (ich dôkaz možno nájsť v niektorých učebniciach algebry) interpretujeme tak, že (až na izomorfizmus) $(Z_p, \oplus)$ je jediná grupa s prvočíselným počtom prvkov p, $(Z_4, \oplus)$ a štvorgrupa sú jediné štvorprvkové grupy a $(Z_6, \oplus)$ a $(S_\triangle, \circ)$ sú jediné šesťprvkové grupy. Tieto tvrdenia znamenajú klasifikáciu všetkých konečných grúp majúcich nanajvýš 7 prvkov. (Je ich teda deväť. Urobte tabuľky všetkých týchto „malých“ grúp (cvičenie 20.) Klasifikácia všetkých konečných grúp je pravdepodobne jeden z najťažších **otvorených** (t.j. nevyriešených) problémov súčasnej matematiky. Nepoznáme zatiaľ ani vzorec, ktorý by pre ľubovoľné prirodzené číslo n určoval, koľko je (až na izomorfizmus) konečných grúp s n prvkami.

Cvičenia.

1. a) Ukážte, že delenie nie je binárna operácia na množine nenulových celých čísel, ale je binárna operácia na množine nenulových racionálnych čísel.

b) Ukážte, že delenie na množine nenulových racionálnych čísel nie je komutatívna ani asociatívna operácia.

c) Ukážte, že operácie $\oplus$ a $\odot$ v príklade 2 sú asociatívne.

2. Vyšetrite vlastnosti binárnej operácie $\triangle$ symetrického rozdielu množín na potenčnej množine $P(M)$ množiny M, ak $\triangle$ je definovaná predpisom

$$A \triangle B := (A - B) \cup (B - A) = (A \cup B) - (A \cap B).$$

(Pozri aj vetu 7.6.)

3. Nech operácie $\oplus$ a $\odot$ sú definované „bodovo" tak ako v príklade 2 na množine

a) R^N všetkých zobrazení $N \to R$ (t.j. všetkých postupností $(a_1, a_2, a_3, \dots)$ reálnych čísel);

b) Z^N všetkých zobrazení $N \to Z$ (postupností celých čísel);

c) N^N všetkých zobrazení $N \to N$ (postupností prirodzených čísel);

Vyšetrite vlastnosti operácí $\oplus$ a $\odot$ v každom z uvedených prípadov. V ktorom z uvedených prípadov je $\oplus$ resp. $\odot$ grupovou operáciou?

4. Nech M je ľubovoľná neprázdna množina. Dokážte, že na množine M^M všetkých zobrazení $M \to M$ má operácia $\circ$ skladania zobrazení tieto vlastnosti:

a) nie je komutatívna, ak M je aspoň dvojprvková;

b) má neutrálny prvok id_M (identické zobrazenie na M);

c) Ak existuje inverzné zobrazenie f^{-1} k zobrazeniu $f : M \to M$, tak f a f^{-1} sú navzájom inverzné prvky vzhľadom na operáciu $\circ$. Na akých podmnožinách M^M je $\circ$ grupovou operáciou?

5. Určte neutrálne a inverzné prvky u grupoidov $(N, +)$, $(N, .)$, $(Z, -)$ a $(Q - \{0\}, :)$ z príkladu 6. Ktoré z nich sú grupami? Vymenujte aspoň tri podgrupoidy (v prípade grupy tri podgrupy) u každého z nich.

6. a) Overte tvrdenia v príklade 7b. Naviac ukážte, že množina kZ je podgrupou grupy $(Z, +)$;

b) Overte tvrdenia v príklade 7c. Zistite v ktorých prípadoch sa jedná o podgrupu.

7. a) Overte tvrdenia v príklade 8b.

b) Nájdite podgrupoidy grupy $(R, +)$ generované množinami $\{-1, 1\}$, $\{-3, 3\}$ a $\{-1\} \cup N^+$. Zistite, či sú aj jej podgrupami.

c) Nájdite podgrupoidy grupy $(R, .)$ a $(R - \{0\}, :)$ generované množinou $\{-1\} \cup N^+$ a zistite, či sú aj podgrupami.

8. Podrobne overte tvrdenia v príklade 8c.

9. Odôvodnite tvrdenia vo vete 4.

10. Podrobne overte tvrdenia v príklade 9.

11. Podrobne overte, že grupoid $(Z_4, \oplus)$ v príklade 10 je grupa a že grupoid $(Z_4, \odot)$ nie je grupa. Dokážte tvrdenia vyslovené v závere príkladu 10.

12. Zdôvodnite, prečo symetria geometrického útvaru U na seba je prosté zobrazenie a ukážte, že výsledkom skladania dvoch symetrií útvaru U je opäť symetria útvaru U.

13. Dokážte vetu 5.

14. Na množine $Z_2 \times Z_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ sú dané operácie $+$ a $\cdot$ „po zložkách", t.j.

$(a,b)+(c,d)=(a\oplus c, b\oplus d)$, $\quad (a,b)\cdot(c,d)=(a\odot c, b\odot d)$.
Zostavte Cayleyho tabuľku pre operácie $+$ a $\cdot$ a zistite, či $(Z_2\times Z_2,+)$ a $(Z_2\times Z_2,\cdot)$ sú grupy.

15. a) Ukážte, že ak f je izomorfizmus grupoidu (grupy) $(A,\circ)$ na grupoid (grupu) $(B,*)$, tak inverzné zobrazenie f^{-1} je izomorfizmus $(B,*)$ na $(A,\circ)$;

b) Dokážte, že pri izomorfizme dvoch grúp sa neutrálny prvok jednej grupy vždy zobrazuje na neutrálny prvok druhej grupy.

16. Vymenujte všetkých 6 izomorfizmov grupy $(S_{\sqsubset\sqsupset},\circ)$ na grupu $(K_4,*)$ (pozri príklad 12b).

17. Ukážte, že

a) grupa symetrií obdĺžnika (príklad 11) je izomorfná s grupou $(Z_2\times Z_2,+)$;

b) grupa symetrií rovnostranného trojuholníka je izomorfná s grupou transformácií 3-prvkovej množiny;

c) grupa $(Z_4,\oplus)$ je izomorfná s grupou komplexných jednotiek $(\{1,-1,i,-i\},.)$.
V každom z uvedených prípadov nájdite všetky izomorfizmy.

18. Ukážte, že na ľubovoľnej množine grupoidov (grúp) je binárna relácia $\cong$ („sú izomorfné“) reflexívna a tranzitívna.

19. Zostavte tabuľky všetkých deviatich (navzájom neizomorfných) grúp majúcich nanajvýš 7 prvkov. Operácie definujte na množinách:
$\{0\},\{0,1\},\ldots,\{0,1,2,3,4,5,6\}$.