Katedra informatiky Fakulty matematiky, fyziky a informatiky
Univerzity Komenského v Bratislave

ÚVOD DO DISKRÉTNYCH ŠTRUKTÚR

Eduard Toman

BRATISLAVA 2008

OBSAH

Predhovor

Predložený učebný text je napísaný pre predmet Úvod do diskrétnych štruktúr, študijný odbor Informatika, prvý ročník na Fakulte matematiky, fyziky a informatiky v Bratislave. V podstate ide o rozšírený a upravený zápis viacerých prednášok autora z diskrétnej matematiky na tejto fakulte.

Diskrétna matematika predstavuje základ teoretických disciplín pre vedu o počítačoch, pre ktorú používame označenie informatika, ktorá sa zaoberá všetkým tým, čo súvisí s počítačmi a vyčísliteľnými procesmi.

Diskrétna matematika sa zaoberá skúmaním najmä diskrétnych (nespojitých) štruktúr. Práve v súvislosti s intenzívnym využívaním počítačov pri riešení problémov a úloh najrozličnejších typov, diskrétna matematika presiahla rámec diskrétnej analýzy a zahrňuje dnes aj rad metód konštruktívnych, vytvorených pre bezprostredné využívanie počítačov.

Diskrétna matematika je relatívne samostatná súčasť matematiky. Jej začiatky sú začiatkami matematiky. Hlavnou špecifikou je diskrétnosť, t.j. opak spojitosti a v širšom zmysle zahrňuje aj také disciplíny ako teória čísel, algebra, matematická logika, kombinatorika, teória grafov, teória množín a rad ďalších disciplín, ktoré sa začali najintenzívnejšie rozvíjať v polovici dvadsiateho storočia spojených s využívaním počítačov.

Dosiahnutie určitého stupňa matematickej zrelosti tvorí v značnej miere súčasť odbornej kvalifikácie každého, kto chce s počítačmi systematicky pracovať. Prirodzené východisko pre štúdium informatiky predstavujú matematická logika a teória množín, ktoré zo všeobecného hľadiska tvoria vyjadrovacie prostriedky a pracovné postupy. Životnosť týchto teórií sa prejavuje v tom, že ony samy, ale aj disciplíny, ktorých vznik podmienili prenikli do celej matematiky i informatiky a v istom rozsahu sa dostávajú do učiva prvých ročníkov vysokoškolského štúdia na fakultách rôznych zameraní.

V učebnom texte je iste mnoho nedostatkov, nejasných formulácií, nepresností, alebo chýb. Veríme však, že sa dajú odstrániť pomerne rýchlo a pohodlne. Čitateľovi, ktorý ma na tieto nedostatky upozorní, budem veľmi povďačný.

V Bratislave, 21.9. 2008 Doc. RNDr. E. Toman, CSc.,

Prehľad označení

Symbol	Význam, prípadne názov
$A, B, C, \ldots$	množiny
$a \in A$	prvok a patrí do množiny A
$a_1, a_2, \ldots, a_n \in A$	prvky $a_1, a_2, \ldots, a_n$ patria do množiny A
$a \notin A,\ \neg(a \in A)$	prvok a nepatrí do množiny A
$A = \{a_1, a_2, \ldots, a_n\}$	množina A obsahuje práve prvky $a_1, a_2, \ldots, a_n$
$\{a \in A \mid V(a)\}$	množina práve tých prvkov množiny A, ktoré majú vlastnosť V
$\emptyset$	prázdna množina
$A = B$	množina A sa rovná množine B
$A \neq B$	množina A sa nerovná množine B
$A \subseteq B$	množina A je obsiahnutá v množine B
$A \not\subseteq B$	množina A nie je obsiahnutá v množine B
$A \subset B$, $A \subsetneq B$	množina A je vlastnou, (pravou) podmnožinou množiny B
$\mathcal{P}$, $\mathcal{S}$	systémy množín
$\mathcal{P}(A)$	množina všetkých podmnožín množiny A
$A \cup B$	zjednotenie množín A a B
$A \cap B$	prienik množín A a B
$A \setminus B$, $A - B$	rozdiel množín A a B
$A \div B$	symetrická diferencia množín A a B
$\bigcup_{A \in \mathcal{S}} A$	zjednotenie systému množín
$\bigcap_{A \in \mathcal{S}} A$	prienik systému množín
(a, b)	usporiadaná dvojica
$(a_1, a_2, \ldots, a_n)$	usporiadaná n-tica
$A \times B$	Karteziánsky súčin množín A a B
$A_1 \times A_2 \times \ldots \times A_n$	Karteziánsky súčin množín $A_1, A_2, \ldots, A_n$
$\lvert A \rvert$	mohutnosť množiny A
$N_n,\ n \geq 1$	množina $\{0, 1, 2, \ldots, n-1\}$

$\aleph_0$	alef nula, mohutnosť množiny N
$f : A \to B$	zobrazenie f množiny A do množiny B
$g = f \mid A$	parciálna funkcia k funkcií f
B^A	množina zobrazení $f : A \to B$
p, q, r	výroková premenná
$\neg p$	negácia výroku p
$p \wedge q$	konjunkcia výrokov p a q
$p \vee q$	disjunkcia výrokov p a q
$p \Rightarrow q$, $p \to q$	implikácia výrokov p a q
$p \Leftrightarrow q$, $p \leftrightarrow q$	ekvivalencia výrokov p a q
$\uparrow$	Shafferova spojka
$\downarrow$	Pierce – Lukasiewicsova spojka
$\forall$	veľký (všeobecný, univerzálny) kvantifikátor
$\forall a \in A : V(a)$	všetky prvky a množiny A majú vlastnosť V
$\exists$	malý (existenčný) kvantifikátor
$\exists a \in A : V(a)$	v množine A existuje aspoň jeden prvok a s vlastnosťou V
$\exists! a \in A : V(a)$	v množine A existuje práve jeden prvok a s vlastnosťou V

1. Základy matematickej logiky

V matematike pracujeme so súbormi objektov, ktoré sú idealizované a abstraktné, čo do mohutnosti môžu byť konečné, alebo nekonečné.

Matematika je deduktívna veda, na rozdiel od experimentálnych vied nové tvrdenia, ak chceme začleniť do matematickej teórie, musíme ich najskôr dokázať.

Ak niekto chce študovať matematiku, rozumieť jej tvrdeniam a správne ich interpretovať, musí mať základné vedomosti o výstavbe matematických teórií.

V našom výklade nepôjdeme až do takých podrobností. Máme na to niekoľko dôvodov; prvý dôvod je časový, druhý dôvod je, že ešte nepoznáme dôkladne žiadnu matematickú teóriu a tretí dôvod je, že problematika spadá do matematickej logiky, ktorá v širšom zmysle slova taktiež patrí do oblasti diskrétnej matematiky.

Niekoľko slov k logickej výstavbe matematických teórií povieme. Keď sa zaoberáme logickou výstavbou matematiky stojíme predovšetkým pred dvoma otázkami:

1. Ako sa odvodzujú matematické tvrdenia (vety) ?
2. Aké sú logické základy matematiky?

Keď študujeme odvodzovanie matematických viet, tak sa musíme pýtať, aké typy logických záverov (úsudkov) poznáme, aké metódy dôkazov rozoznávame, atď. Ako vidíme sú to čisto logické otázky. Nemusíme sa preto zaoberať logickým odvodzovaním (dedukciou) vôbec a pritom súčasne spoznáme ako sa odvodzujú matematické vety. Vlastnému výkladu o logickej dedukcií treba predoslať akúsi "hovorkyňu logiky", totiž výklad o tvare a druhoch viet (výrokov).

Základom každej matematickej teórie sú, ako je známe určité axiómy, pre jeho ďalšiu výstavbu potom sú dôležité definície, ktorými zavádzame nové "matematické objekty". Ak sa obrátime k logickým základom matematiky, prehovoríme teda o tom, aké definície rozoznávame a aké vlastnosti definície musia mať. Potom sa môžme zaoberať systémom axióm a dotknúť sa požiadaviek, ktoré na ne kladieme (bezospornosť, úplnosť, nezávislosť).

Napokon možno zaviesť niektoré matematické pojmy, napr. pojem množiny, relácie, zobrazenie, funkcie, mohutnosť množiny, prirodzené čísla atď., ktoré sa vyskytujú vo všetkých odboroch matematiky a majú pre jej výstavbu základnú dôležitosť. Musíme preto venovať pozornosť aj týmto pojmom.

Ako sme už povedali vyššie, výstavbu matematických teórií nebudeme študovať podrobne, uspokojíme sa s tým, že sa naučíme rozpoznávať logickú štruktúru a základné typy dôkazov matematických tvrdení. Teraz sa bližšie pozrieme na logický aparát matematických teórií.

1.1. Výroky

Matematické poznatky formulujeme v podobe výrokov. Výrok je tvrdenie, o ktorého pravdivosti alebo nepravdivosti má zmysel uvažovať. Výrok ma spravidla tvar gramatickej oznamovacej vety. Výrokmi nie sú otázky, rozkazovacie vety, ale ani oznamovacie vety, pokiaľ im nemožno jednoznačne priradiť pravdivostnú hodnotu. (Napr. „Táto veta je nepravdivá".)

Výrok je buď pravdivý, buď je nepravdivý (princíp dvojhodnotovosti), výrok nemôže byť súčasne pravdivý i nepravdivý (zákon o vylúčení sporu), ale platí práve jedna z týchto možností (zákon vylúčenia tretieho).

Pravdivostná hodnota "pravdivý" sa označuje symbolom 1 (alebo T - true), pravdivostná hodnota „nepravdivý" sa označuje symbolom 0 (alebo F - false). Pri rozhodovaní, či nejaké tvrdenie má pravdivostnú hodnotu 0 alebo 1, t. j. či tvrdenie je výrokom z hľadiska výrokového počtu nezáleží na tom, akým spôsobom zistíme pravdivostnú hodnotu daného tvrdenia, dokonca nezáleží na tom, či vôbec vieme pravdivostnú hodnotu tvrdenia určiť.

V matematike výroky najčastejšie obsahujú tvrdenia, či nejaký objekt alebo množina objektov má resp. nemá istú vlastnosť, alebo vlastnosti.

Výroky, ktorých pravdivostnú hodnotu nepoznáme nazývame hypotézami. (Napríklad: Existuje nekonečne veľa prirodzených čísel p takých, že aj číslo $p+2$ je prvočíslo). Teda prvočíselných dvojčiat je nekonečne veľa.

Napríklad problém v matematike známy ako „problém štyroch farieb“ bol pokladaný dlho za otvorený, napokon sa ho v roku 1976 podarilo úspešne vyriešiť.

Pojem výroku patrí k základným matematickým pojmom, presná definícia výroku je zložitejším problémom, ktorý spadá do oblasti skúmania matematickej logiky. My v našich úvahách vystačíme s intuitívnym pojmom výroku.

Nasledujúce tvrdenia sú výroky:

1. Bratislava je hlavné mesto Slovenskej republiky.
2. Číslo 255 je deliteľné piatimi.
3. Každé prirodzené číslo je menšie ako číslo 125.
4. Prvočísel je nekonečne veľa.
5. Množina {3,4,11} je konečná, spočítateľná.

Nasledujúce gramatické vety nie sú výroky:

1. Požičaj mi učebnicu zo slovenského jazyka.
2. Prines mi pohár dobrej minerálky.
3. Táto veta je zelená.
4. Všetci Kréťania vždy klamú.

Výroky označujeme malými písmenami latinskej abecedy: *a, b, c, d, ...* najčastejšie však z konca abecedy *p, q, r, s, ...* (Symboly *a, b, c, …* používané na označenie výrokov, nazývame tiež výrokovými premennými. Niekedy výrokové premenné aj indexujeme $a_1, a_2, ..., a_n$. Pravdivostnú hodnotu (valuáciu) výroku *a* budeme označovať symbolom v(*a*). Poznamenávame, že ak výrok a je pravdivý, tak potom v(*a*) =1, v opačnom prípade v(*a*) = 0.

Z výrokov pomocou logických spojok môžeme tvoriť nové, zložitejšie výroky. Najjednoduchší spôsob ako z daného výroku utvoriť nový výrok je popretie skutočnosti, ktorú vyjadruje pôvodný výrok. Napríklad, ak máme výrok: „číslo 5 je väčšie ako číslo 2“, popretím skutočnosti, ktorú tvrdí dostávame výrok „nie je pravda, že číslo 5 je väčšie ako číslo 2“, alebo používame aj slovný obrat „neplatí, že číslo 5 je väčšie ako číslo 2“. Hovoríme, že druhý výrok vznikol z prvého výroku negovaním, teda negáciou prvého výroku. Ak prvý výrok označíme *p*, tak jeho **negáciu** budeme označovať $\neg p$. (V literatúre sa používa pre negáciu výroku aj označenie p', $\overline{p}$, non p, v programovacích jazykoch NOT *p*). Poznamenávame, že výrok je pravdivý práve vtedy, ak jeho negácia je nepravdivá, je nepravdivý v opačnom prípade.

Ak sú *p*, *q* ľubovoľné výroky, **konjunkcia** spája výroky *p*, *q* do nového výroku “*p* a *q*” čítame “*p* súčasne *q*”. Konjunkciu výrokov *p*, *q* označujeme $p \wedge q$ (*p* & *q*, *p*.*q*, *p* and *q*). Konjunkcia $p \wedge q$ je pravdivá práve vtedy, ak výroky *p*, *q* sú pravdivé súčasne. V opačnom prípade je konjunkcia $p \wedge q$ nepravdivá.

Disjunkciu výrokov *p*, *q* zapisujeme výrazom $p \vee q$ (*p* or *q*). Disjunkciu výrokov *p*, *q* čítame „ *p* alebo *q*“. Disjunkcia výrokov *p*, *q* je pravdivá práve vtedy, ak aspoň jeden z výrokov *p*, *q* je pravdivý, v opačnom prípade je disjunkcia výrokov *p*, *q* nepravdivá. Okrem disjunkcie výrokov sa niekedy používa aj alternatíva výrokov (výlučné alebo, XOR, sčítanie podľa modulu 2, negácia ekvivalencie). **Alternatívu** výrokov *p*, *q* označujeme $p \oplus q$ a čítame „buď platí výrok *p* alebo platí výrok *q*, ale výroky *p* a *q* neplatia súčasne“. Výrok $p \oplus q$ je pravdivý práve vtedy, ak je pravdivý práve jeden z výrokov *p*, *q*. V opačnom prípade je výrok $p \oplus q$ nepravdivý.

Matematické tvrdenia majú spravidla tvar implikácie alebo ekvivalencie. Preto v matematických dôkazoch zohráva veľmi dôležitú úlohu implikácia. **Implikácia** výrokov p, q sa označuje symbolicky ako $p \to q$ a číta sa „ak p, tak q“, „p implikuje q“, „z p vyplýva q“. Výrok p v implikácií $p \to q$ nazývame predpoklad a výrok q záver, alebo tvrdenie, dôsledok. Implikácia výrokov p, q je nepravdivá, ak predpoklad p je pravdivý a záver q je nepravdivý, v opačnom prípade je implikácia pravdivá. Implikáciu $\neg q \to \neg p$ nazývame obmenou implikácie $p \to q$, implikáciu $q \to p$ nazývame obrátením implikácie $p \to q$.

Treba upozorniť na istú odlišnosť v chápaní výrokov $p \vee q$ a $p \to q$ od ich chápania v bežnej hovorovej reči. Tak napríklad spojka alebo sa v bežnej reči používa vo vylučovacom zmysle, t.j. p alebo q znamená, že platí práve jeden z výrokov. Implikácia sa v bežnej reči chápe tak, že z pravdivosti predpokladu možno naozaj odvodiť pravdivosť tvrdenia, dôsledku, záveru. No v matematike chápeme implikáciu trocha inak. Ilustrujeme to na elementárnom príklade zo školského učiva.

Ak prirodzené číslo n je deliteľné číslom 10, tak je deliteľné aj číslom 5. Tento výrok v matematike pokladáme za pravdivý, teda ak za n dosadíme ľubovoľné prirodzené číslo, tak dostávame vždy pravdivý výrok. Špeciálne pri dosadení čísla 4 dostaneme výrok typu $0 \to 0$, pri dosadení čísla 5 výrok typu $0 \to 1$, pri dosadení čísla 30 výrok typu $1 \to 1$, všimnime si, že pri ľubovoľnom dosadení prirodzeného čísla nikdy nedostaneme výrok typu $1 \to 0$, teda nepravdivý výrok.

Ekvivalenciu výrokov p, q zapisujeme výrazom $p \leftrightarrow q$ (niekedy sa používajú aj výrazy $p \equiv q$, alebo $p \sim q$) a čítame ako „p je ekvivalentné s q“, „p práve vtedy, keď q“, „p vtedy a len vtedy, keď q“. Ekvivalencia $p \leftrightarrow q$ je pravdivá práve vtedy, keď výroky p a q majú rovnakú pravdivostnú hodnotu, ekvivalencia neplatí v opačnom prípade. Výroky, ktoré majú rovnakú pravdivostnú hodnotu sa nazývajú logicky rovnocenné (ekvivalentné). To, že výroky majú rovnakú pravdivostnú hodnotu znamená, že jeden z nich môže byť napríklad v zloženom výroku nahradený druhým výrokom bez toho, aby sa zmenila pravdivostná hodnota zloženého výroku. Na druhej strane však logicky ekvivalentné výroky nemusia mať rovnaký zmysel. Napríklad výrok „Bratislava je hlavné mesto Slovenskej republiky“ a výrok „Prirodzené číslo 6 je párne číslo“ sú pravdivé výroky a teda aj ekvivalentné výroky, ktoré však majú rozličný zmysel. Nahradzovanie výrokov ekvivalentnými výrokmi využívame pri zjednodušovaní výrokov, z dôvodu prehľadnejšieho a vhodnejšieho zápisu.

Poznámka. V literatúre sa stretávame pri implikácií aj s označením $\Rightarrow$ a pre ekvivalenciu s označením $\Leftrightarrow$. My prednostne používame označenia $\to$, $\leftrightarrow$.

Napokon uvedieme dve dôležité binárne spojky: Shafferovu a Pierce-Lukasiewiçsovu.

Shafferova spojka $\uparrow$ je pre výroky p, q definovaná takto: $(p \uparrow q) \leftrightarrow \neg(p \wedge q)$, čiže $p \uparrow q$ je pravdivá práve vtedy, keď $p \wedge q$ je nepravdivá a je nepravdivá v opačnom prípade.

Pierce – Lukasiewiçsova spojka $\downarrow$ je pre výroky p, q definovaná takto: $(p \downarrow q) \leftrightarrow \neg(p \vee q)$, čiže $p \downarrow q$ je pravdivá práve vtedy, keď $p \vee q$ je nepravdivá a je nepravdivá v opačnom prípade.

Obidvom uvedeným spojkám budeme venovať zvláštnu pozornosť, pre ich dôležitú vlastnosť, o niečo neskôr v texte nižšie.

Ak sa pravdivostná hodnota výroku p (označenie v(p)) identicky rovná 1, t.j. výrok p je pravdivý pre všetky možné kombinácie pravdivostných hodnôt výrokov, z ktorých je zložený, nazývame ho **tautológia**. Zložený výrok p nazývame **kontradikcia**, ak v(p) = 0 bez ohľadu na pravdivostné hodnoty výrokov, z ktorých pozostáva. Zložený výrok je **splniteľný**, ak v(p) = 1 aspoň pre jednu kombináciu pravdivostných hodnôt výrokov, z ktorých sa skladá.

Uvedieme niektoré významné logické tautológie, ktoré budeme v ďalšom výklade používať a potrebovať. Nech sú p, q, r ľubovoľné výroky (výrokové premenné) a nech výroky 0 (1) označujú ľubovoľnú kontradikciu (tautológiu), potom sú nasledujúce výroky tautológie.

1. Idempotentnosť $(p \wedge p) \leftrightarrow p$
   $(p \vee p) \leftrightarrow p$
2. Komutatívnosť $(p \wedge q) \leftrightarrow (q \wedge p)$
   $(p \vee q) \leftrightarrow (q \vee p)$
   $(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$
3. Asociatívnosť $(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r)$
   $(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r)$
4. Distributívne zákony $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$
   $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$
5. Absorbčné zákony $(p \wedge (q \vee p)) \leftrightarrow p$
   $(p \vee (q \wedge p)) \leftrightarrow p$
6. Zákon dvojitej negácie $\neg\neg p \leftrightarrow p$
7. Zákon vylúčenia tretieho $(p \vee \neg p) \leftrightarrow 1$
8. Zákon o vylúčení sporu $(p \wedge \neg p) \leftrightarrow 0$
9. De Morganove zákony $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
   $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
10. Kontrapozícia negácie $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$
11. Reductio ad absurdum $(\neg p \rightarrow p) \rightarrow p$
12. $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$
13. $(p \rightarrow q) \leftrightarrow \neg(p \wedge \neg q)$
14. $(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q)$
15. $(p \vee q) \leftrightarrow (\neg p \rightarrow q)$
16. $(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$

V nasledujúcej tabuľke uvádzame pravdivostné hodnoty základných zložených výrokov, závisiacich od pravdivostných hodnôt ich prvotných zložiek.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$	$p \uparrow q$	$p \downarrow q$
0	0	1	0	0	0	1	1	1	1
0	1	1	0	1	1	1	0	1	0
1	0	0	0	1	1	0	0	1	0
1	1	0	1	1	0	1	1	0	0

Obr. 1. Tabuľka pravdivostných hodnôt

Z vyššie uvedených základných tautológií ihneď vidno, že ľubovoľnú binárnu spojku možno nahradiť nasledujúcimi dvojicami spojok $\{\neg, \rightarrow\}, \{\neg, \wedge\}, \{\neg, \vee\}$.

Ukážeme, že $\downarrow$a $\uparrow$ a sú jediné binárne spojky, ktoré túto vlastnosť majú, t.j. ľubovoľnú binárnu spojku môžeme vyjadriť len pomocou jedinej z uvedených spojok. Nato, aby sme sa o tom presvedčili, pomocou každej spojky $\downarrow$a $\uparrow$ vyjadríme $\neg, \wedge, \vee$.

$\neg p \leftrightarrow p \downarrow q,\ \neg p \leftrightarrow p \uparrow q,\ p \vee q \leftrightarrow (p \uparrow p) \uparrow (q \uparrow q).$
$p \wedge q \leftrightarrow (p \downarrow p) \downarrow (q \downarrow q),\ p \vee q \leftrightarrow (p \downarrow q) \downarrow (p \downarrow q),$
$p \wedge q \leftrightarrow (p \uparrow q) \uparrow (p \uparrow q).$

Ukážeme, že žiadna iná spojka túto vlastnosť nemá. Uvažujeme nasledujúcu pravdivostnú tabuľku pre logickú spojku Δ s uvedenou vlastnosťou.

p	q	$p \Delta q$		$p \downarrow q$	$p \uparrow q$
0	0	1		1	1
0	1	0	1	0	1
1	0	1	0	0	1
1	1	0		0	0

Obr. 2. Pravdivostné hodnoty pre logickú spojku Δ

Ak v(p) = v(q) = 0, tak $p \Delta q$ musí byť pravdivý výrok, inak by sa pomocou Δ nedal vyjadriť výrok $\neg p$. Taktiež z toho istého dôvodu musí platiť, že ak v(p) = v(q) = 1, tak $p \Delta q$ je nepravdivý výrok. Ak pre zvyšné pravdivostné hodnoty p, q doplníme chýbajúce pravdivostné hodnoty pre Δ, tak, že jednotlivé stĺpce budú vyzerať takto: Δ (0,1) = 0, Δ (1,0) = 1, tak bude spojka Δ totožná s $\neg$ a $p \wedge q \leftrightarrow \neg q$, ak Δ (0,1) = 1, Δ (1,0) = 0, tak $p \wedge q \leftrightarrow \neg p$. V prípade, že Δ (0,1) = 0, Δ (1,0) = 0, je Δ totožná s $\downarrow$, v prípade, že Δ (0,1) = 1, Δ (1,0) = 1, je Δ totožná s $\uparrow$.

Pomocou logickej spojky $\neg$ môžeme vyjadriť výrok identicky rovný premennej alebo identicky rovný negácií premennej. Ale výrok identicky rovný 0, alebo identicky rovný 1 nedokážeme len pomocou negácie napísať.

1.2. Výrokové formy

Výrokovou formou $a(x)$ s premennou x nazývame takú oznamovaciu vetu (formálny výraz, formulu), ktorá obsahuje premennú x, sama nie je výrokom, a stane sa výrokom vždy vtedy, keď za premennú x dosadíme konkrétny objekt z vopred danej vhodne vybratej množiny.

Príklad: 1. „x je väčšie ako číslo 5“
2. „x je hlavné mesto SR“
3. „x je prvočíslom“
4. „$|x+5| \leq 3$“

Ku každej výrokovej forme existuje nejaká množina prvkov, ktoré má zmysel do výrokovej formy dosadzovať. Napríklad v príkladoch 1. a 4. to môže byť množina reálnych čísel. V príklade 2. množina miest na Slovensku, v príklade 3. množina prirodzených čísel.

Označíme $a(x)$ výrokovú formu definovanú na množine prirodzených čísel takto:

$a(x)$: „x je väčšie ako 3 a menšie alebo rovné 7“.

Dosadením prirodzených čísel do formuly $a(x)$ dostávame nasledujúce výroky:

$a(0)$..... $3 < 0 \leq 7$
$a(1)$..... $3 < 1 \leq 7$
$a(2)$..... $3 < 2 \leq 7$
$a(3)$..... $3 < 3 \leq 7$
$a(4)$..... $3 < 4 \leq 7$
$a(5)$..... $3 < 5 \leq 7$
.
.
.

Je zrejmé, že prvé štyri výroky sú nepravdivé, ak budeme dosadzovať ďalej ľahko uvidíme, že ďalšie štyri výroky sú pravdivé a všetky ostatné výroky už budú nepravdivé.

V matematike sa často vyskytujú výroky, o ktorých hovoríme, že v danej množine existuje objekt istých vlastností alebo, že všetky objekty z istej množiny majú istú vlastnosť. Inak povedané, že z výrokovej formy môžeme dostať výrok nielen dosadením, ale aj tým, že určíme (kvantifikujeme),

pre koľko (aké množstvo) prvkov z vhodnej množiny dáva daná výroková formula pravdivý výrok. Pri zápise týchto výrokov používame **kvantifikátory**.

Existenčný kvantifikátor $\exists$ čítame „existuje“. Zápis $(\exists x)\, a(x)$ má význam „existuje aspoň jedno také x, pre ktoré platí $a(x)$ “, t.j. existuje aspoň jeden taký prvok, ktorý keď dosadíme do výrokovej formy $a(x)$ za premennú x, dostaneme pravdivý výrok.

Všeobecný kvantifikátor $\forall$ čítame „pre všetky“, alebo „pre každé“. Zápis $(\forall x)\, a(x)$ má význam: „pre každé x platí $a(x)$“.

Výroky obsahujúce kvantifikátory nazývame **kvantifikované výroky.** Poznamenávame, že existenčný kvantifikátor niekedy nazývajú aj malý kvantifikátor a všeobecný kvantifikátor veľký alebo univerzálny kvantifikátor.

Príklad 1. Nech N označuje množinu všetkých prirodzených čísel. Nech na množine N je definovaná výroková forma $a(x)$: „ x+1 je väčšie ako 5“. Kvantifikovaný výrok: „existuje aspoň jedno prirodzené číslo x, pre ktoré platí, že je väčšie ako 5“, formálne zapisujeme takto: $(\exists x)((x \in N) \wedge (x+1) > 5)$.

Príklad 2. Nech R označuje množinu všetkých racionálnych čísel. Nech na množine R je definovaná výroková forma $b(x)$: „ x+1 v absolútnej hodnote je väčšie ako číslo 5“. Kvantifikovaný výrok: „pre každé reálne číslo x platí, že $|x+1| > 5$ “ formálne zapíšeme takto: $(\forall x)((x \in R) \rightarrow |x+1| > 5)$.

Poznamenávame, že kvantifikovaný výrok z príkladu 1. je pravdivý, stačí nám položiť napr. $x = 6$, kvantifikovaný výrok z príkladu 2. je nepravdivý, stačí nám položiť napríklad $x = 3{,}5$.

Kvantifikované výroky môžeme spájať pomocou logických spojok a tak vytvoriť **zložené kvantifikované výroky**. Zvláštnu pozornosť si zasluhuje **negovanie kvantifikovaných výrokov**. Nech $a(x)$ označuje ľubovoľnú výrokovú formu.

Jednoduché kvantifikované výroky (t.j. obsahujúce jeden kvantifikátor) negujeme podľa nasledujúcich pravidiel:

$$\neg(\exists x)a(x) \leftrightarrow (\forall x)(\neg a(x)) \qquad (1)$$

$$\neg(\forall x)a(x) \leftrightarrow (\exists x)(\neg a(x)) \qquad (2)$$

Príklad 3. Nech $a(x)$ je výroková forma definovaná na množine prirodzených čísel, ktorá hovorí, že „x je nepárne číslo“. Vieme, že párne číslo je také prirodzené číslo, ktoré sa dá vyjadriť v tvare $2k$, kde k je ľubovoľné prirodzené číslo. Uvažujme kvantifikovaný výrok „existuje prirodzené číslo x, ktoré je zároveň aj párne číslo. Formálne môžeme tento výrok zapísať takto: $(\exists x)((x \in N) \wedge (x \text{ je párne číslo}))$. Urobme negáciu tohto kvantifikovaného výroku. Podľa vyššie uvedeného pravidla dostávame:

$$\neg(\exists x)((x \in N) \wedge (x \text{ je párne číslo})) \leftrightarrow (\forall x)\neg((x \in N) \wedge (x \text{ je párne číslo}))$$

Uplatníme teraz de Morganov zákon:

$$(\forall x)\neg((x \in N) \wedge (x \text{ je párne číslo})) \leftrightarrow (\forall x)(\neg(x \in N) \vee \neg(x \text{ je párne číslo}))$$

$$\leftrightarrow (\forall x)((x \notin N) \vee \neg(x \text{ je párne číslo})) \leftrightarrow (\forall x)((x \in N) \rightarrow (x \text{ je nepárne číslo}))\,.$$

V poslednej úprave sme použili tautológiu $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$.

Poznamenávame, že pôvodný kvantifikovaný výrok je pravdivý, teda jeho negáciou sme dostali nepravdivý výrok.

Príklad 4. Uvažujme teraz kvantifikovaný výrok: $(\forall x)((x \in N) \rightarrow (x \text{ je párne číslo}))$. Výrok nám hovorí, že každé prirodzené číslo je párne, je to zrejme výrok nepravdivý. Negujme tento výrok,

použitím najprv tautológie $(p \to q) \leftrightarrow (\neg p \vee q)$, zákonu dvojitej negácie a de Morganovho zákona, dostávame

$$\neg(\forall x)((x \in N) \to (x \text{ je párne číslo})) \leftrightarrow (\exists x)\neg((x \in N) \to (x \text{ je párne číslo})) \leftrightarrow$$
$$(\exists x)\neg(\neg(x \in N) \vee (x \text{ je párne číslo})) \leftrightarrow (\exists x)\ (\neg\neg(x \in N) \wedge \neg(x \text{ je párne číslo})) \leftrightarrow$$
$$(\exists x)\ ((x \in N) \wedge \neg(x \text{ je párne číslo})) \leftrightarrow (\exists x)\ ((x \in N) \wedge (x \text{ je nepárne číslo}))\,,$$

kvantifikovaný výrok, ktorý hovorí, že existuje také prirodzené číslo *x*, ktoré nie je párne, teda je nepárne číslo. Ľahko vidno, že je výrok pravdivý.

Ako sme už uviedli, kvantifikované výroky môžeme spájať pomocou logických spojok. Nech *a*(*x*) je ľubovoľná výroková forma definovaná na množine A a kvantifikované výroky $(\forall x)\ a(x)$, $(\exists x)\ a(x)$. Pomocou implikácie môžeme vytvoriť nasledujúce zložené kvantifikované výroky:

$$(\forall x)a(x) \to (\exists x)a(x)$$
$$(\exists x)a(x) \to (\forall x)a(x)$$

Všimnime si, že, že kvantifikovaný výrok $(\forall x)a(x) \to (\exists x)a(x)$ je pravdivý pre ľubovoľnú výrokovú formu *a*(*x*) a pre ľubovoľnú množinu prvkov A, na ktorej je výroková forma *a*(*x*) definovaná, teda kvantifikovaný výrok je tautológia. Nech A je ľubovoľná množina, na ktorej je výroková forma *a*(*x*) definovaná, ak *a*(*x*) je pravdivá pre ľubovoľné $x \in A$, teda je pravdivý predpoklad $(\forall x)a(x)$, tak potom je pravdivý aj záver $(\exists x)a(x)$, dôsledok danej implikácie.

V prípade výroku $(\exists x)a(x) \to (\forall x)a(x)$, môže nastať taká situácia, že pre niektoré $x \in A$ je *a*(*x*) nepravdivý výrok. V tomto prípade je implikácia $(\exists x)a(x) \to (\forall x)a(x)$ nepravdivá, teda kvantifikovaný výrok $(\exists x)a(x) \to (\forall x)a(x)$ nie je tautológia.

Príklad 5. Nech *a*(*x*), b(*x*) sú ľubovoľné výrokové formy definované na množine A. Ukážte, že nasledujúce kvantifikované výroky sú tautológie:

1. $(\forall x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\forall x)\,b(x))$
2. $(\exists x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\exists x)\,b(x))$

Riešenie.

1. Predpokladajme, že kvantifikovaný výrok $(\forall x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\forall x)\,b(x))$ nie je tautológia. To znamená, že existujú také *a*(*x*), b(*x*) definované na množine A, že kvantifikovaný výrok $(\forall x)\,a(x) \to (\forall x)\,b(x)$ je nepravdivý, t.j. výrok $(\forall x)\ a(x)$ je pravdivý a $(\forall x)\,b(x)$ je nepravdivý výrok, to znamená, že existuje aspoň jedno také $x \in A$, označme ho x_0, že výrok $b(x_0)$ je nepravdivý. Položme si otázku, či v tomto prípade môže byť kvantifikovaný výrok $(\forall x)(a(x) \to b(x))$ pravdivý, t. j. či implikácia $a(x) \to b(x)$ je pravdivá pre každé $x \in A$. Vezmime $x_0 \in A$, v tomto prípade je $a(x_0)$ pravdivý výrok, $b(x_0)$ nepravdivý výrok, teda implikácia $a(x_0) \to b(x_0)$ je nepravdivá. To znamená, že v kvantifikovanom výroku $(\forall x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\forall x)\,b(x))$ nemôže nastať prípad, že záver – v našom prípade kvantifikovaný výrok $(\forall x)\,a(x) \to (\forall x)\,b(x)$ je nepravdivý a predpoklad – kvantifikovaný výrok $(\forall x)(a(x) \to b(x))$ je pravdivý výrok. Čiže implikácia $(\forall x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\forall x)\,b(x))$ je vždy pravdivý kvantifikovaný výrok, teda tautológia.

2. To, že kvantifikovaný výrok $(\exists x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\exists x)\,b(x))$ je tautológia dokážeme priamo. Ak uvedený kvantifikovaný výrok je tautológia, tak potom jeho negácia je kontradikcia. Najprv pomocou známych tautológií budeme upravovať uvažovaný kvantifikovaný výrok. Postupnými ekvivalentnými úpravami dostávame:

$$[(\exists x)(a(x) \to b(x)) \to ((\forall x)\,a(x) \to (\exists x)\,b(x))] \leftrightarrow$$

$$[(\exists x)(\neg a(x) \vee b(x)) \rightarrow (\neg(\forall x)\, a(x) \vee (\exists x)\, b(x))] \leftrightarrow$$
$$[\neg(\exists x)(\neg a(x) \vee b(x)) \vee ((\exists x) \neg a(x) \vee (\exists x)\, b(x))] \leftrightarrow$$
$$[(\forall x) \neg(\neg a(x) \vee b(x)) \vee ((\exists x) \neg a(x) \vee (\exists x)\, b(x))] \leftrightarrow$$
$$[(\forall x)\, (\neg\neg a(x) \wedge \neg b(x)) \vee ((\exists x) \neg a(x) \vee (\exists x)\, b(x))] \leftrightarrow$$
$$[(\forall x)\, (a(x) \wedge \neg b(x)) \vee ((\exists x) \neg a(x) \vee (\exists x)\, b(x))].$$

Negáciou posledného výroku postupnými ekvivalentnými úpravami dostávame:

$$\neg[(\forall x)\, (a(x) \wedge \neg b(x)) \vee ((\exists x) \neg a(x) \vee (\exists x)\, b(x))] \leftrightarrow$$
$$\neg(\forall x)\, (a(x) \wedge \neg b(x)) \wedge \neg((\exists x) \neg a(x) \vee (\exists x)\, b(x)) \leftrightarrow$$
$$(\exists x)\, (\neg a(x) \vee b(x)) \wedge ((\forall x)\, a(x) \wedge (\forall x) \neg b(x)).$$

Je zrejmé, že posledný výrok je vždy nepravdivý preľubovoľné $x \in A$.

Príklad 6. Nech $a(x)$, b(x) sú ľubovoľné výrokové formy definované na množine A. Ukážeme, že kvantifikovaný výrok

$$(\exists x)(a(x) \rightarrow b(x)) \rightarrow ((\exists x)\, a(x) \rightarrow (\exists x)\, b(x))$$

nie je tautológia.

Riešenie. Stačí nám uviesť výrokové výrokové formy $a(x)$, b(x) a množinu A, na ktorej sú $a(x)$, b(x) definované tak, že uvedený kvantifikovaný výrok nebude pravdivý. Zvolíme napríklad množinu $A = \{u, v\}$. Teda množina A pozostáva z dvoch prvkov u a v. Nech ďalej $a(u)$ je pravdivý výrok, $a(v)$ nepravdivý výrok, $b(u)$, $b(v)$ nepravdivé výroky. V tomto prípade kvantifikovaný výrok $(\exists x)(a(x) \rightarrow b(x))$ je pravdivý výrok, zabezpečuje nám ho pravdivá implikácia $a(v) \rightarrow b(v)$. Kvantifikovaný výrok $(\exists x)\, a(x) \rightarrow (\exists x)\, b(x)$ je nepravdivý výrok, pretože $(\exists x)\, a(x)$ je pravdivý výrok a $(\exists x)\, b(x)$ je v danom prípade nepravdivý výrok. Zhrnutím dostávame, že implikácia $(\exists x)(a(x) \rightarrow b(x)) \rightarrow ((\exists x)\, a(x) \rightarrow (\exists x)\, b(x))$ je v uvažovanom prípade nepravdivá.

Doteraz sme uvažovali výrokové formy jednej premennej. Poznamenávame, že v matematike sa stretávame s výrokovými formami dvoch, troch, vo všeobecnosti n- premenných.

Poznámka: Upozorňujeme čitateľa, že pri kvantifikovaných výrokoch si treba uvedomiť nasledujúcu vec. Ak máme ľubovoľnú výrokovú formu $a(x)$, tak bežne v odbornej reči sa stretávame s nasledujúcou formuláciou: „Pre žiadne x neplatí $a(x)$." Formálne tento kvantifikovaný výrok môžeme skrátene zapísať $(\forall x) \neg a(x)$, teda v skutočnosti nepoužijeme dve negácie v kvantifikovanom výroku.

Poznamenávame, že horeuvedený kvantifikovaný výrok možno ekvivalentne v slovenskom jazyku vyjadriť aj nasledovne : „Pre každé x, neplatí c alebo „Pre žiadne x platí $a(x)$." Najpoužívanejšie je však vyjadrenie „Pre žiadne x neplatí $a(x)$", ktoré podľa mienky autora vyplýva zo zvyklostí vyjadrovania sa v slovenskom jazyku, v iných jazykoch napríklad v angličtine je to inak.

Na záver tejto poznámky uvedieme nasledujúci konkrétny príklad. Nech $a(x)$ označuje, že prirodzené číslo x je prvočíslo. Uvažujme kvantifikovaný výrok: „Žiadne x nie je prvočíslo". Formálne výrok zapíšeme takto: $(\forall x)((x \in N) \rightarrow \neg a(x))$, alebo skrátene $(\forall x) \neg a(x)$, ak v danom prípade použijeme dve negácie, tak dostávame:

$$\neg(\exists x)((x \in N) \wedge \neg a(x)) \leftrightarrow (\forall x)(\neg(x \in N) \vee \neg\neg a(x)) \leftrightarrow (\forall x)((x \in N) \rightarrow a(x))$$

a teda skrátene $(\forall x)\, a(x)$ a to sme nechceli povedať.

1.1. - 1.2. CVIČENIA

1) Udajte príklady dvoch výrokov a utvorte z nich konjunkciu, disjunkciu, implikáciu, ekvivalenciu.

2) Prepíšte z prirodzeného jazyka do jazyka výrokovej logiky nasledujúce výroky a negujte ich.

a) Mama nepôjde na výlet bez otca.
b) Ak nepôjde na výlet Katka, tak nepôjde ani Jano.
c) Jano pôjde práve vtedy, keď pôjde Zuzka.
d) Anka na výlet pôjde a Eva na výlet nepôjde.

3) Negujte nasledujúce výroky:

a) Na výlet pôjdem iba vtedy, keď nebude pršať.
b) Všetky okná v miestnosti sú zatvorené.
c) Nórsko má aspoň 15 tisíc obyvateľov.
d) V závode pracuje najviac 9 inžinierov.

4) Napíšte obrátenie, obmenu a negáciu výrokov.

a) Ak je číslo deliteľné desiatimi, tak je deliteľné aj piatimi.
b) Ak je štvoruholník ABCD štvorec, tak všetky jeho štyri strany majú rovnakú veľkosť

5) Preverte, pomocou tabuľkovej metódy, ktoré formuly sú tautológie, kontradikcie a splniteľné.

a) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
b) $p \rightarrow (q \rightarrow p)$
c) $(p \rightarrow q) \rightarrow (\neg q \rightarrow p)$
d) $p \wedge \neg q$
e) $p \wedge (q \wedge \neg p)$

6) Negujte dané výroky. Vyjadrite slovne ich obsah, určite ich pravdivostnú hodnotu.

a) $(\exists x)((x \in N) \wedge (x > 5))$
b) $(\forall x)((x \in N) \rightarrow (x \bmod 2 = 0 \vee x \bmod 2 = 1))$
c) $(\exists x)\left((x \in R) \wedge \left(x^2 + 2x + 1 \geq 0\right)\right)$

7) Zistite, či pre ľubovoľné výrokové formy $a(x)$, $b(x)$, definované na množine A sú nasledujúce kvantifikované výroky tautológie.

a) $((\forall x)\, a(x) \rightarrow (\forall x)\, b(x)) \rightarrow (\forall x)(a(x) \rightarrow b(x))$
b) $((\forall x)\, a(x) \rightarrow (\exists x)\, b(x)) \rightarrow (\exists x)(a(x) \rightarrow b(x))$
c) $(\forall x)(a(x) \rightarrow b(x)) \rightarrow ((\exists x)\, a(x) \rightarrow (\exists x)\, b(x))$

8) Dokážte pomocou pravdivostných tabuliek, že uvedené výroky sú tautológie.

a) $(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r)$
b) $(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r)$
c) $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$
d) $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$
e) $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$
f) $(p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow (q \wedge r)))$

g) $(p \to q) \to ((q \to r) \to ((p \vee q) \to r))$

1.3. Matematické dôkazy

V predchádzajúcej časti sme uviedli, že matematika ako exaktná veda je vybudovaná deduktívne.

Základy každej matematickej teórie tvoria základné pojmy, ktoré sú intuitívne jasné a názorné (napr. prirodzené číslo, reálne číslo, zlomok, bod, priamka, rovina, ...). Tieto základné pojmy nedefinujeme, ale pomocou nich definujeme ostatné pojmy, ktoré sa v teórií vyskytujú.

Niekoľko elementárnych tvrdení o vlastnostiach základných pojmov prijmeme za **axiómy**. Znamená to, že ich považujeme za natoľko zrozumiteľné, že sme ochotní prijať ich pravdivosť z názoru, bez ďalšej argumentácie.

Budovať, rozvíjať, zdokonaľovať teóriu, znamená odhaľovať stále nové pravdivé tvrdenia o vlastnostiach základných pojmov a ďalších definovaných pojmov, pričom najčastejšie postupujeme tak, že sformulujeme **hypotézu**, t. j. výrok , ktorého pravdivostnú hodnotu zatiaľ nepoznáme, potom sa snažíme hypotézu dokázať, alebo vyvrátiť.

Dôkazom ľubovoľného tvrdenia a rozumieme postupnosť logických úvah, ktoré ukazujú, že platnosť tvrdenia a logicky vyplýva z platnosti prijatých axióm a z tvrdení, ktoré už boli skôr dokázané. Deduktívnosť výstavby matematických teórií je v tom, že každé tvrdenie, ktoré chceme do teórie začleniť, musí byť najskôr dokázané (jedinou výnimkou sú axiómy).

Teda zjednodušene, pod matematickým dôkazom tvrdenia a si budeme predstavovať konečnú postupnosť tvrdení $a_1, a_2, ..., a_n = a$, kde a_i sú nejaké výroky, alebo výrokové formy a pre všetky i, $i = 1, 2, ..., n\text{-}1$ sú implikácie $a_i \to a_{i+1}$ tautológie. Pričom a_1 je pravdivý výrok a nazývame ho predpoklad.

Pri takomto poňatí matematického dôkazu si treba uvedomiť, že sme zohľadnili finitné hľadisko a odvolávame sa na sémantiku, uvažované implikácie sú tautológie.

Jedným z našich cieľov je upresniť túto predstavu a naučiť čitateľa niektorým štandardným postupom, ktoré sa pri dôkazoch matematických tvrdení používajú.

Ak stojíme pred problémom, ako dokázať dané tvrdenie a (výrok a) odporúčame postupovať nasledujúcim spôsobom.

Najprv uvedieme základné typy matematických dôkazov, ktoré postupne popíšeme a bližšie špecifikujeme.

1) Priamy dôkaz tvrdenia a (pokúsiť sa dokázať tvrdenie a priamo).
2) Utvoriť negáciu tvrdenia a, tú sa pokúsiť doviesť do sporu.
3) Utvoriť obmenu tvrdenia a (výrok ekvivalentný s a), tento výrok dokázať priamo, alebo sporom.
4) Dôkaz tvrdenia a vykonať matematickou indukciou.

Ak dokazujeme tvrdenie a sporom, alebo ak dokazujeme jeho obmenu, takýto dôkaz nazývame nepriamy.

Vo všetkých typoch deduktívnych dôkazov potrebujeme mať k dispozícií odvodzovacie pravidlá, ktoré nám umožnia prejsť od pravdivých tvrdení k novým pravdivým tvrdeniam. Hovoríme, že uvedené pravidlá sú korektné.

Najdôležitejším odvodzovacím pravidlom, ktoré budeme používať je tzv. **pravidlo odlúčenia**, **modus ponens**, ktoré symbolicky zapisujeme v tvare $\dfrac{a, a \to b}{b}$ a čítame „z predpokladov $a, a \to b$ odvoď b“.

Zmysel tohto pravidla je teda nasledujúci, ak platia výroky napísané nad čiarou (predpoklady), tak potom musí platiť aj záver, t. j. výrok b. Ihneď sa o tom presvedčíme, ak si vezmeme na pomoc pravdivostnú tabuľku implikácie.

Pravidlo modus ponens možno zapísať aj v nasledujúcom tvare $\frac{\neg b \to a, \neg b}{\neg a}$, ak na implikáciu v predpoklade použijeme zákon kontrapozície negácie dostávame pravidlo nazývané **modus tolens** $\frac{a \to b, \neg b}{\neg a}$, nazývame ho **pravidlo zamietnutia**.

Veľmi užitočné pravidlo, pre skracovanie implikácie je **pravidlo jednoduchého sylogizmu**, ktoré hovorí, z predpokladov $a \to b,\ b \to c$ odvoď $a \to c$, symbolicky zapísané $\frac{a \to b, b \to c}{a \to c}$.

Nakoniec uvedieme **pravidlo reductio ad absurdum**, ktoré hovorí, že ak z negácie tvrdenia a odvodíme tvrdenie a, tak potom platí tvrdenie a. Formálne $\frac{\neg a \to a}{a}$.

V matematike, ako aj v bežnom živote často treba riešiť otázku, či dané tvrdenie vyplýva, je dôsledok nejakých iných tvrdení. To nás privádza k pojmu „logický dôsledok“.

Skôr, než si tento pojem presne definujeme, objasníme pojem **interpretácia** (označujeme I), ak povieme interpretácia, tak máme na mysli nejakú konkrétnu kombináciu pravdivostných hodnôt výrokov, ktoré vytvárajú zložený výrok. (V prípade pravdivostnej tabuľky je to jeden konkrétny riadok).

Definícia 1.3.1 Nech sú dané výroky $a_1, a_2, ..., a_n$ a výrok a. Hovoríme, že **výrok** a je **logickým dôsledkom výrokov** $a_1, a_2, ..., a_n$ (alebo že a logicky vyplýva z $a_1, a_2, ..., a_n$), ak pre každú interpretáciu, v ktorej každý výrok $a_1, a_2, ..., a_n$ je pravdivý, výrok a je taktiež pravdivý. Výroky $a_1, a_2, ..., a_n$ nazývame postulátmi, alebo predpokladmi tvrdenia a.

Veta 1.3.1 Nech sú dané výroky $a_1, a_2, ..., a_n$, a, potom výrok a je logickým dôsledkom $a_1, a_2, ..., a_n$ práve vtedy, keď $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je tautológia.

Dôkaz: Predpokladajme, že a je logickým dôsledkom $a_1, a_2, ..., a_n$. Nech I je ľubovoľná interpretácia a nech výroky $a_1, a_2, ..., a_n$ sú v nej pravdivé, tak potom podľa definície logického dôsledku je výrok $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ pravdivý v interpretácií I, ak nie všetky výroky $a_1, a_2, ..., a_n$ nie sú pravdivé v I, t.j. aspoň jeden z nich nie je pravdivý v I, potom výrok $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je pravdivý v I a teda výrok $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je pravdivý pri každej interpretácií I výrokov $a_1, a_2, ..., a_n$, t. j. zložený výrok $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je tautológia.

Z druhej strany predpokladajme, že $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je tautológia, teda, ak $a_1, a_2, ..., a_n$ sú pravdivé výroky, pravdivý výrok je aj $a_1 \wedge a_2 \wedge ... \wedge a_n$, potom aj a je pravdivý výrok, teda a je logický dôsledok výrokov $a_1, a_2, ..., a_n$.

Veta 1.3.2 Nech sú dané výroky $a_1, a_2, ..., a_n$, a, potom výrok a je logickým dôsledkom $a_1, a_2, ..., a_n$ práve vtedy, ak $(a_1 \wedge a_2 \wedge ... \wedge a_n) \wedge \neg a$ je kontradikcia, nesplniteľný, t. j. nie je pravdivý v žiadnej interpretácií.

Dôkaz: Podľa predchádzajúcej vety výrok a je logickým dôsledkom výrokov $a_1, a_2, ..., a_n$ práve vtedy, ak $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je tautológia. Z toho vyplýva, že a je logický dôsledok $a_1, a_2, ..., a_n$ práve vtedy, keď negácia výroku $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ je nesplniteľná. Počítajme
$\neg((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a) \leftrightarrow \neg(\neg(a_1 \wedge a_2 \wedge ... \wedge a_n) \vee a) \leftrightarrow (\neg\neg(a_1 \wedge a_2 \wedge ... \wedge a_n) \wedge \neg a) \leftrightarrow$
$((a_1 \wedge a_2 \wedge ... \wedge a_n) \wedge \neg a) \leftrightarrow 0$.

Poznamenávame, že u všetkých odvodzovacích pravidiel výrok napísaný pod čiarou je logickým dôsledkom výrokov zapísaných nad čiarou.

Príklad: Nech výrok *a*: $(p \to (q \to r))$, *b*: $(p \to q)$, *c*: $(p \to r)$. Výrok *c* je logický dôsledok výrokov *a*, *b*.

Poznámka 1. Z predchádzajúcich viet vyplýva, ak potrebujeme dokázať, že nejaký výrok je logický dôsledok konečnej množiny výrokov, je ekvivalentné dôkazu toho, že niektorý s ním spojený zložený výrok je tautológia, alebo kontradikcia.

Poznámka 2. Ak a je logický dôsledok $a_1, a_2, ..., a_n$, potom výrok $((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$ nazývame teorémou a v matematickej logike často označujeme symbolicky $\vdash ((a_1 \wedge a_2 \wedge ... \wedge a_n) \to a)$.

Teraz podrobnejšie popíšeme jednotlivé metódy dôkazov v matematike.

1.4. Základné metódy dôkazov v matematike

I. Priamy dôkaz tvrdenia *a*

Pozostáva z konečného reťazca implikácií $a_1 \to a_2 \to ... \to a_n \to a$, ktorého prvý člen je axióma, alebo už dokázané tvrdenie, alebo pravdivé tvrdenie, výrok a každé ďalšie tvrdenie je logickým dôsledkom predchádzajúcich, pričom posledným členom reťazca (postupnosti) je dokazované tvrdenia *a*.

Všimnime si, že ak v uvedenej postupnosti implikácií použijeme dostatočný počet krát pravidlo jednoduchého sylogizmu dostávame platnosť implikácie $a_1 \to a$. O tvrdení, výroku a_1 predpokladáme, že je pravdivé, tak potom použitím pravidla modus ponens dostávame platnosť tvrdenia *a*.

Príklad 1. Ak prirodzené číslo *n* je deliteľné súčasne číslami 2 a 3, tak potom je deliteľné aj číslom 6. Dokážte.

Dôkaz vykonáme priamo. Ak číslo *n* je deliteľné číslom 2, tak ho môžeme vyjadriť v tvare $n = 2 \cdot k$, *k* je prirodzené číslo. Súčasne je číslo *n* deliteľné aj číslom 3, tak potom $n = 3 \cdot l$, kde *l* je prirodzené číslo, pretože číslo 2 nie je deliteľné číslom 3, tak potom číslo 3 musí deliť číslo *k*, teda číslo *k* môžeme vyjadriť v tvare $k = 3 \cdot r$. Zhrnutím dostávame, že číslo *n* môžeme napísať v tvare $n = 2 \cdot 3 \cdot r = 6 \cdot r$. Z toho vyplýva, že číslo 6 delí číslo *n*.

II. Nepriamy dôkaz tvrdenia *a* sporom

Založený je na zákone vylúčenia tretieho, podľa ktorého z dvojice výrokov $a, \neg a$ musí byť práve jeden pravdivý. Keď teda dokážeme, že výrok $\neg a$ nie je pravdivý, vyplýva z toho pravdivosť tvrdenia *a*. Pri dôkaze sporom postupujeme takto: Predpokladajme platnosť tvrdenia $\neg a$, odvodzujeme z neho logické dôsledky tak dlho, až sa nám podarí odvodiť tvrdenie *b*, o ktorom vieme, že je nepravdivé (pretože jeho negácia $\neg b$ bola už skôr dokázaná). V tom prípade hovoríme, že sme dospeli ku sporu. Keby sme v tejto situácií pokladali $\neg a$ za pravdivé tvrdenie, boli by v našej teórií dokázateľné tvrdenia *b* aj $\neg b$, a teda aj tvrdenie $b \wedge \neg b$, ktoré je nepravdivé. Teória by bola preto sporná (všetky tvrdenia by v nej boli dokazateľné a teda aj pravdivé), ľahko to možno nahliadnuť takto, nech *a* je ľubovoľné tvrdenie, výrok, zložený výrok $(\neg b \to (b \to c))$ je tautológia, použitím pravidla modus ponens, dvakrát, dostávame platnosť tvrdenia *c*, ktoré sme vzali ľubovoľné. Teda zhrnutím dostávame, že predpoklad o pravdivosti tvrdenia $\neg a$ neplatí, z čoho vyplýva, že *a* je pravdivé tvrdenie.

Príklad 2. Ak *n* je párne prvočíslo, tak potom nie je deliteľné tromi.

Dôkaz vykonáme sporom. Predpokladajme, že párne prvočíslo *n* je deliteľné 3. Dostávame, že párne prvočíslo *n* má aspoň troch deliteľov a to čísla 1, 2 a 3. To je spor s tým, že *n* je prvočíslo, pričom každé prvočíslo má práve dvoch rôznych deliteľov, číslo 1 a seba samého.

V matematike majú tvrdenia spravidla tvar implikácie. Poznamenávame, že obe uvedené metódy dôkazov možno použiť aj v prípade, keď dokazované tvrdenie má tvar implikácie $a \to b$.

III. Priamy dôkaz implikácie $a \to b$

Predpokladajme, že tvrdenie *a* platí (v prípade, že *a* je nepravdivé je implikácia $a \to b$ pravdivá, niet čo dokazovať), nájdeme postupnosť implikácií začínajúcu tvrdením *a*, končiacu tvrdením *b*, v ktorej každý člen je logickým dôsledkom predchádzajúcich tvrdení a axióm, resp. skôr dokázaných tvrdení. Niekoľkonásobným použitím pravidla jednoduchého sylogizmu dostávame platnosť implikácie $a \to b$.

IV. Nepriamy dôkaz implikácie $a \to b$ sporom.

Podobne ako v opísanej schéme dôkazu sporom predpokladáme platnosť negácie dokazovanej implikácie, t. j. predpokladáme platnosť tvrdenia $\neg(a \to b)$, ktoré je ekvivalentné tvrdeniu $a \wedge \neg b$. Z tohto tvrdenia postupne odvodzujeme logické dôsledky tak dlho, pokým dospejeme k sporu. Môžu tu nastať tri prípady:
- dôjdeme do sporu s tvrdením *a*,
- dôjdeme do sporu s tvrdením $\neg b$
- napokon môžeme dokázať dve navzájom odporujúce si tvrdenia *c*, $\neg c$.

Všetky tri prípady vedú na platnosť tvrdenia $a \to b$, čo teraz postupne dokážeme.

V prvom prípade sme dokázali pravdivosť implikácie

$$\neg(a \to b) \to \neg a .$$

Ak použijeme na uvedenú implikáciu zákon kontrapozície, tak dostávame

$$a \to (a \to b),$$

Zo známych dôvodov predpokladáme, že výrok *a* je pravdivý, aplikáciou pravidla modus ponens dostávame pravdivosť implikácie $a \to b$.

V druhom prípade sme odvodili implikáciu

$$\neg(a \to b) \to b$$

Použijeme tautológiu $b \to (a \to b)$, aplikáciou pravidla jednoduchého sylogizmu dostávame platnosť implikácie $a \to b$.

V treťom prípade sme odvodili implikáciu

$$\neg(a \to b) \to (c \wedge \neg c)$$

Ak použijeme kontrapozíciu negácie, tak dostávame implikáciu

$$\neg(c \wedge \neg c) \to (a \to b).$$

Výrok $\neg(c \wedge \neg c)$ je podľa de Morganovho zákona ekvivalentný s výrokom $\neg c \vee c$, ktorý je tautológia. Pomocou pravidla modus ponens opäť dostávame pravdivosť výroku $a \to b$, čo bolo treba dokázať.

V prípade, že dokazovaným tvrdením je implikácia, môžeme použiť aj nepriamy dôkaz pomocou obmeny, ak je to výhodnejšie (autor tento typ dôkazu zaradil aj z toho dôvodu, že sa vyskytuje v stredoškolskom učive).

V. Nepriamy dôkaz implikácie $a \to b$ pomocou obmeny.

Zakladá sa na skutočnosti, že implikácia $a \to b$ a jej obmena $\neg b \to \neg a$ sú ekvivalentné, t.j. majú vždy rovnakú pravdivostnú hodnotu. To znamená, že namiesto implikácie $a \to b$, môžeme

dokazovať jej obmenu $\neg b \to \neg a$, ak je to výhodnejšie. Nepriamym dôkazom implikácie $a \to b$ je teda reťazec (postupnosť) implikácií $\neg b \to a_1 \to a_2 \to ... \to a_n \to \neg a$.
Do predpokladu sme dali $\neg b$ a odvodili sme $\neg a$. Dokázali sme teda implikáciu $\neg b \to \neg a$, ktorá je obmenou implikácie $a \to b$, teda z $a \to b$, a vyplýva b. Prakticky to znamená, že nepriamy dôkaz implikácie obmenou ukončíme odkazom na spor, pretože z negovaného tvrdenia $\neg b$ sme odvodili platnosť nepravdivého tvrdenia $\neg a$. (Pritom sa neodvolávame na kontrapozíciu negácie). Náš spor spočíva v tom, že o tvrdení a v implikácií $a \to b$ predpokladáme, že je pravdivé (zo známych dôvodov), zároveň sme však dokázali, že aj $a \wedge \neg a$ je pravdivé tvrdenie, čo ale nie je pravda.

Poznamenávame, že účinnosť nepriamych dôkazov závisí podstatne na tom, či okrem daných predpokladov sa naviac ako predpoklad príjme nepravdivosť toho, čo chceme dokázať a vychádzame z väčšieho počtu predpokladov. Vďaka tomu sa mnohé tvrdenia dokazujú ľahšie nepriamo, ako keby sme ich chceli dokázať priamo, neplatí to však všeobecne.

Príklad 3. Ak prirodzené číslo n je deliteľné 2 a 3 súčasne, tak potom je deliteľné aj 6.
Riešenie: Utvoríme obmenu tohto výroku, dostávame výrok: ak prirodzené číslo n nie je deliteľné 6, tak potom nie je deliteľné 2 alebo nie je deliteľné 3. To znamená, že ak číslo n sa nedá vyjadriť v tvare $6.x$, tak potom sa nedá vyjadriť v tvare $2.y$, alebo sa nedá vyjadriť v tvare $3.z$.

V ďalšom uvedieme niekoľko príkladov na rôzne typy matematických dôkazov.
Príklad 4. Dokážte, že pre každé dve reálne čísla $a > 1, b > 1$ platí:

$$\log_a b + \log_b a \geq 2$$

Najskôr urobíme rozbor úlohy. Pretože $a > 1, b > 1$, sú oba logaritmy kladné čísla. Ak označíme $\log_a b = x$, to znamená, že $a^x = b$, ak označíme $\log_b a = y$, teda $b^y = a$, tak dostávame, že $\left(b^y\right)^x = b$, a teda $b^{x.y} = b$, čiže $x.y = 1$. Z vyššie uvedeného vyplýva, že

$$\log_a b = \frac{1}{\log_b a}.$$

Ak zostaneme pri označení $\log_a b = x$, potom nám stačí dokázať, že

$$x + \frac{1}{x} \geq 2$$

pre každé x. Postupnými úpravami dostaneme

$$x^2 + 1 \geq 2x$$
$$x^2 - 2x + 1 \geq 0$$
$$(x-1)^2 \geq 0$$

čo platí pre každé reálne x. Tým sme s rozborom hotoví a v opačnom smere môžeme vykonať priamy dôkaz. (Rozbor sám o sebe nie je dôkaz.)

Platí $(\log_a b - 1)^2 \geq 0$ a postupne dostávame $(\log_a b)^2 - 2\log_a b + 1 \geq 0$ a teda $(\log_a b)^2 + 1 \geq 2\log_a b$. Z toho vyplýva, že $\log_a b + \frac{1}{\log_a b} \geq 2$, čo bolo treba dokázať.

Príklad 5. Dokážte, že prvočísel je nekonečne veľa.
Riešenie: Dôkaz vykonáme sporom. Predpokladajme, že prvočísel je konečne veľa. Označme ich $p_1, p_2, ..., p_n$, kde $n \in N$. Označme $m = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. Číslo $m \in N$, teda môžu nastať pre prirodzené číslo tieto prípady:

1. číslo $m = 0$
2. číslo $m = 1$
3. číslo m je prvočíslo
4. číslo m je zložené číslo

Nemôže nastať prípad 1. ani 2., je to v spore s voľbou čísla *m*, číslo *m* je vždy väčšie ako 1. Číslo *m* nie je ani zložené číslo, pretože nie je deliteľné žiadnym z prvočísel $p_1, p_2, ..., p_n$. (Po delení čísla *m* ľubovoľným prvočíslom dostaneme vždy zvyšok 1).

Teda predpoklad o konečnom počte prvočísel je nepravdivý. Platí, že prvočísel je nekonečne veľa, čo bolo treba dokázať.

Príklad 6. Dokážte, že $\sqrt{5}$ je iracionálne číslo.

Dôkaz: Tvrdenie dokážeme sporom. Predpokladajme, že $\sqrt{5}$ je racionálne číslo, teda existujú také prirodzené čísla *p*, *q*, že $\frac{p}{q} = \sqrt{5}$. Súčasne predpokladáme, že zlomok je v základnom tvare, teda *p*, *q* sú nesúdeliteľné. Úpravou dostaneme, že $p = q\sqrt{5}$ a teda $p^2 = 5q^2$.

Z toho vidíme, že p^2 je deliteľné piatimi a pretože 5 je prvočíslo musí platiť, že aj p je deliteľné piatimi. (Ak by p nebolo deliteľné piatimi, nebolo by ani p^2 deliteľné piatimi.) Teda $p = 5k$, $k \in N$. Ak dosadíme do predošlej rovnosti, dostaneme $25k^2 = 5q^2$ a teda $5k^2 = q^2$, číslo q^2 je deliteľné piatimi, teda aj q je deliteľné piatimi. To je ale spor s predpokladom, že *p*, *q* sú nesúdeliteľné. $\sqrt{5}$ sa teda nedá zapísať v tvare p/q, teda nie je racionálne číslo, ale iracionálne, čo bolo treba dokázať.

Príklad 7. Dokážte, že funkcia $f : y = -2x^2$ je na intervale $(-\infty, 0)$ rastúca.

Riešenie: Máme dokázať implikáciu

$$x \in (-\infty, 0);\ x_1 < x_2 \rightarrow -2x_1^2 < -2x_2^2.$$

Implikáciu dokážeme priamo.

Nech platí $x_1 < x_2 < 0$.

Postupne dostávame

$$|x_1| > |x_2| > 0$$

$$|x_1|^2 > |x_2|^2$$

$$x_1^2 > x_2^2 \text{ pretože } x^2 \geq 0$$

$$-2x_1^2 < -2x_2^2$$

Tým je tvrdenie dokázané.

Príklad 8. Šesť družstiev sa zúčastnilo turnaja, ktorý sa hral systémom „každý s každým jeden zápas“. Turnaj trval dva dni. Dokážte, že existujú tri družstvá, ktoré odohrali všetky svoje zápasy počas jedného dňa.

Riešenie: Každé družstvo hralo 5 zápasov, teda existuje také družstvo, ktoré odohralo aspoň 3 zápasy v jeden deň, pretože keby odohralo denne najviac 2, boli by to celkove iba 4 zápasy. (Takýto úsudok nazývame Dirichletov princíp.) Označme ho družstvo *A* (ľahko sa možno presvedčiť, že to môže byť ľubovoľné z piatich družstiev) a deň, v ktorý odohralo aspoň tri zápasy označme *d*. Nech súpermi družstva *A* v deň *d* sú družstvá *B*, *C*, *D*. Skúmajme vzájomné zápasy týchto štyroch družstiev. V deň *d* sa odohrali zápasy $A-B$, $A-C$, $A-D$. Súperi družstva *A* zohrali ešte v dvoch dňoch zápasy medzi sebou, teda $B-C$, $B-D$, $C-D$. Ak sa ani jeden z týchto zápasov nehral v deň *d*, máme tri družstvá *B*, *C*, *D*, ktoré odohrali svoje vzájomné zápasy jeden deň, iný ako *d*. Ak by napríklad zápas $B-C$ odohrali v deň *d*, tak v tomto dni sa odohrajú všetky tri vzájomné zápasy družstiev *A*, *B*, *C*. Teda v každom prípade existujú také tri družstvá, ktoré odohrali všetky vzájomné zápasy v jeden deň, čo bolo treba dokázať.

Príklad 9. Máme $2k+1$ lístkov očíslovaných prirodzenými číslami $1,2,...,2k+1$. Aký najväčší počet lístkov možno vybrať tak, aby sa žiadne vybraté číslo nerovnalo súčtu dvoch vybratých čísel?

Riešenie: Podmienku úlohy spĺňajú napríklad lístky s číslami $k+1, k+2, ..., 2k+1$. Ich počet je $k+1$. Dokážeme, že väčší počet lístkov sa už nedá vybrať. Predpokladáme opak, t. j. že možno vybrať $k+r$ lístkov, ktoré spĺňajú podmienku úlohy, pričom $r>1$. Nech n je najväčšie číslo, napísané na tých lístkoch. Uvažujme rozdiely medzi n a ostatnými členmi na vybratých $k+r$ lístkoch. Týchto rozdielov je $k+r-1$ a musia byť napísané na ostatných $2k+1-(k+r)$ lístkoch. To znamená, že musí byť splnená nerovnosť $k+r-1 \le 2k+1-k-r = k-r+1$, čiže $r \le 1$, čo je spor.

Poznamenávame, že podmienku úlohy spĺňajú aj lístky s číslami $1,3,5,...,2k+1$, ktorých je taktiež $k+1$.

Na záver tejto časti uvedieme ešte jeden príklad zo školského učiva.

Príklad 10. Dokážte, že ak nemožno pravítkom a kružidlom zostrojiť uhol s veľkosťou 1º, nemožno zostrojiť ani uhol s veľkosťou 19 º.

Riešenie: Tvrdenie dokážeme nepriamo. Namiesto implikácie $a \to b$, dokážeme jej obmenu $\neg b \to \neg a$, v našom prípade tvrdenie: "Ak možno zostrojiť uhol s veľkosťou 19º, možno zostrojiť aj uhol s veľkosťou 1º.

Predpokladajme teda, že vieme zostrojiť uhol s veľkosťou 19º. Potom vieme zostrojiť aj uhol s veľkosťou 19. 19 º = 361º, a teda aj uhol s veľkosťou 1º. Tým je tvrdenie dokázané.

VI. Matematická indukcia.

Ak nám treba dokázať platnosť nejakého tvrdenia (vety), ktoré je typu (alebo sa dá sformulovať tak, aby bolo tohto typu) „pre každé prirodzené číslo platí ...", budeme sa pridržiavať princípu na ktorom je založená metóda dokazovania tvrdení nazývaná **matematická indukcia**. Pričom pod prirodzenými číslami rozumieme $0,1,2,...,n, ...$, teda aj 0 pokladáme za prirodzené číslo.

Princíp môžeme sformulovať takto:

Majme množinu M, ktorá má tieto dve vlastnosti:

1) $0 \in M$
2) Pre každé prirodzené číslo n platí: Ak $n \in M$, tak aj $n+1 \in M$.

Množina M obsahuje všetky prirodzené čísla.

Ľahko sa o tom presvedčíme. Podľa 1) je $0 \in M$. Podľa 2) z toho vyplýva, že $1 \in M$. Z toho znovu podľa 2) vyplýva, že $2 \in M$, odtiaľ $3 \in M$, atď. Takto môžeme prísť postupne ku ktorémukoľvek prirodzenému číslu, takže množina M obsahuje všetky prirodzené čísla.

Môžeme uvažovať aj inak. Predpokladajme, že existujú prirodzené čísla, ktoré do M nepatria, najmenšie z nich označme p. Podľa 1) je $p>0$. Číslo $p-1$ je teda prirodzené číslo a podľa toho ako sme zaviedli číslo p, je $p-1 \in M$. Podľa 2) z toho vyplýva, že $p \in M$ a to je spor.

Nech $a(n)$ označuje výrokovú formu, definovanú na množine prirodzených čísel. Máme dokázať tvrdenie, že $a(n)$ platí pre každé prirodzené číslo n, tak postupujeme nasledujúcim spôsobom:

1º Dokážeme, že $a(n)$ platí pre $n = 0$. Tento krok nazývame **báza matematickej indukcie**.

2º Dokážeme nasledujúce tvrdenie. Pre každé prirodzené číslo n platí: ak platí $a(n)$ pre číslo n, tak platí aj pre $n + 1$.

Tvrdenie, ktoré dokazujeme v 2º nazývame **indukčný krok** a jej predpoklad „$a(n)$ platí pre číslo n" nazývame **indukčný predpoklad**.

Záver: Výroková forma $a(n)$ platí pre každé prirodzené číslo.

Dôkaz matematickou indukciou ukážeme na niekoľkých typických príkladoch.

Príklad 1. Dokážte, že číslo $2^{3n}+3^{4n}$ nie je pre nijaké prirodzené číslo n deliteľné číslom 73.

Riešenie: Pre $n = 0$ tvrdenie platí, pretože $2^0 + 3^0 = 2$, a to nie je číslo deliteľné 73. Báza indukcie platí. Zostáva nám preveriť platnosť indukčného kroku. Nech n je prirodzené číslo, predpokladajme, že $2^{3n} + 3^{4n}$ nie je deliteľné číslom 73. Ako je to s číslom $2^3.2^{3n} + 3^4.3^{4n} = 8.2^{3n} + 81.3^{4n} = 8\left(2^{3n} + 3^{4n}\right) + 73.3^{4n}$. Prvý zo sčítancov nie je podľa indukčného predpokladu deliteľný 73, druhý je deliteľný 73. Preto ich súčet nie je deliteľný číslom 73. Dokázali sme platnosť indukčného kroku. Tým sme dôkaz tvrdenia vykonali.

Príklad 2. Dokážte, že pre každé prirodzené číslo n a reálne $q \neq 1$ je súčet

$$1 + q + q^2 + ... + q^n = \frac{q^{n+1} - 1}{q - 1}.$$

Riešenie: Pre $n = 0$ tvrdenie platí, pretože $1 = \frac{q-1}{q-1}$. Báza indukcie platí. Preveríme platnosť indukčného kroku. Nech n je prirodzené číslo, predpokladajme, že $1 + q + q^2 + ... + q^n =$.

$= \frac{q^{n+1} - 1}{q - 1}$. Ako je to v prípade $1 + q + q^2 + ... + q^n + q^{n+1}$. Využitím indukčného predpokladu dostávame $\frac{q^{n+1} - 1}{q - 1} + q^{n+1} = \frac{q^{n+1}(q-1) + q^{n+1} - 1}{q - 1} = \frac{q^{n+2} - 1}{q - 1}$. Teda dokázali sme platnosť indukčného kroku.

Záver: Uvedené tvrdenie platí pre každé prirodzené číslo n a reálne číslo $q \neq 1$.

Predovšetkým si treba uvedomiť, že na princípe matematickej indukcie nie je podstatné, že sa začína od čísla 0. Úplne rovnako, ako v pôvodnom znení 1° a 2° možno overiť pravdivosť všeobecnejšieho variantu matematickej indukcie.

Uvažujme o množine M, ktorá má tieto vlastnosti:

3) Pre každé celé číslo k platí, $k \in M$

4) Pre každé celé číslo $r \geq k$ platí: Ak $r \in M$, tak aj $r + 1 \in M$.

Množina M potom obsahuje všetky celé čísla väčšie, alebo rovnajúce sa číslu k.

To umožňuje dokazovať vety typu: „Pre každé celé číslo väčšie alebo rovnajúce sa číslu k platí ...“, tak, že preveríme platnosť výrokovej formy $a(k)$, kde k je celé číslo.

1° Výroková forma $a(k)$ platí pre celé číslo k. **Báza matematickej indukcie**.

2° Pre každé celé číslo $r \geq k$ platí: Ak $a(k)$ platí pre celé číslo r, tak platí aj pre celé číslo $r + 1$. **Indukčný krok.**

Záver: Výroková forma $a(k)$ platí pre každé celé číslo $r \geq k$.

Na ilustráciu dôkazu matematickou indukciou uvedieme ďalšie príklady.

Príklad 3. Dokážte, že pre každé celé číslo x väčšie alebo rovné -8 platí nerovnosť $x - 1 > -10$.

Riešenie: Nech $x = -8$, dostávame $-9 > -10$. Báza indukcie platí. Nech pre celé číslo $k \geq -8$ platí nerovnosť $k - 1 > -10$. Potom pre $k + 1$ dostávame $k + 1 - 1 = k \geq -8 > -10$. Platí aj indukčný krok.

Záver: Uvedená nerovnosť platí pre každé celé číslo väčšie alebo rovné -8.

Príklad 4. Dokážte, že pre každé prirodzené číslo $n \geq 1$ platí, že číslo 31 delí $5^{n+1} + 6^{2n-1}$.

Riešenie: Preveríme platnosť tvrdenia pre $n = 1$, dostávame, že $31 \mid 5^2 + 6 = 31$. Báza indukcie platí.

Nech $n \in N$ a tvrdenie platí pre n, teda $31 \mid 5^{n+1} + 6^{2n-1}$. Pre $n + 1$ dostávame

$$5^{(n+1)+1}+6^{2(n+1)-1}=5^{n+1}.5+6^{2n-1}.6^2=5^{n+1}.5+6^{2n-1}.(5+31)=5.\left(5^{n+1}+6^{2n-1}\right)+6^{2n-1}.31$$

Číslo $5^{n+1}+6^{2n-1}$ je deliteľné číslom 31 podľa indukčného predpokladu. V poslednom výraze sú oba sčítance deliteľné 31, teda aj ich súčet je deliteľný číslom 31.

Záver: Pre každé prirodzené číslo $n \geq 1$ platí, že 31 delí $5^{n+1}+6^{2n-1}$.

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

$$\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)}<1.$$

Riešenie: 1° $a(1)$: $\frac{1}{1.2}=\frac{1}{2}<1$. Báza indukcie platí.

2° Nech $n \in N$ a platí $a(n)$ t. j. $\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)}<1$.

Počítajme $a(n+1)$: $\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)}<1+\frac{1}{(n+1)(n+2)}$.

Vyjadrime $\frac{1}{n(n+1)}$ v tvare $\frac{1}{n}-\frac{1}{n+1}$. Ďalej ukážeme, že platí $a^*(n)$: $\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)} \leq 1-\frac{1}{n+1}<1$. Matematickou indukciou teraz dokážeme uvedenú nerovnosť.

1° Báza indukcie. $a^*(1)$: $\frac{1}{1.2}=\frac{1}{2} \leq 1-\frac{1}{2}$. Báza indukcie platí. Predpokladajme, že platí $a^*(n)$ indukčný predpoklad, t.j. $\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)} \leq 1-\frac{1}{n+1}$. Počítajme $a^*(n+1)$:

$$\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)}<1-\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}=1-\frac{1}{n+1}+\frac{1}{n+1}-\frac{1}{n+2}=1-\frac{1}{n+2}<1$$

Platí aj indukčný krok.

Záver: Pre každé prirodzené číslo $n \geq 1$ platí nerovnosť: $\frac{1}{1.2}+\frac{1}{2.3}+...+\frac{1}{n(n+1)}<1$.

Uvedieme ešte jeden variant princípu matematickej indukcie. Uvažujeme množinu *M*, ktorá má tieto dve vlastnosti:

5) $0 \in M$

6) Pre každé prirodzené číslo *n* platí: Ak $k \in M$ pre všetky prirodzené čísla $k \leq n$, tak aj $n+1 \in M$.

Potom množina *M* obsahuje všetky prirodzené čísla.

Uvedený variant umožňuje dokazovať tvrdenia typu, ktorý už poznáme: „Pre každé prirodzené číslo *n* platí... “ tak, že dokážeme dve pomocné tvrdenia:

1° Výroková forma *a*(*n*) platí pre *n* = 0. **Báza matematickej indukcie**.

2° **Indukčný krok.** Pre každé prirodzené číslo *n* platí: Ak *a*(*n*) platí pre všetky prirodzené čísla menšie ako *n* + 1, tak platí aj pre číslo *n* + 1.

Záver: Výroková forma *a*(*n*) platí pre všetky prirodzené čísla.

Poznamenávame, že indukčný predpoklad je v tomto prípade silnejší ako v predchádzajúcich variantoch matematickej indukcie. Namiesto platnosti výrokovej formy *a*(*n*) pre *n*, požadujeme platnosť výrokovej formy *a*(*n*) pre $0,1,...,n$ súčasne, naraz.

Príklad 6. Každé prirodzené číslo $n > 1$ je možné vyjadriť v tvare súčinu mocnín prvočísel

$n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$, kde $\alpha_1, \alpha_2, ..., \alpha_k$ sú prirodzené čísla a $p_1, p_2, ..., p_k$ sú navzájom rôzne prvočísla.

Riešenie: Nech $n = 2$, $a(2)$ platí, 2 = 2. Báza indukcie platí. Nech tvrdenie platí pre $n \geq 2$. Ukážeme platnosť $a(n+1)$. Ak $n+1$ je prvočíslo, tak indukčný krok platí. Ak $n+1$ nie je prvočíslo, tak vyjadríme číslo $n+1$ v tvare súčinu dvoch prirodzených čísel *r*, *l*, o ktorých vieme, že platí $a(r)$, aj $a(l)$ podľa indukčného predpokladu modifikovaného princípu matematickej indukcie, $r < n+1, l < n+1$.

$$r = p_{i_1}^{\alpha_{i1}}.p_{i_2}^{\alpha_{i2}}.....p_{i_r}^{\alpha_{ir}}, \quad l = p_{j_1}^{\alpha_{j1}}.p_{j_2}^{\alpha_{j2}}.....p_{j_l}^{\alpha_{jl}}.$$

Teda $n+1 = p_{i_1}^{\alpha_{i1}}.....p_{i_r}^{\alpha_{ir}}.p_{j_1}^{\alpha_{j1}}.....p_{j_l}^{\alpha_{jl}} = p_{k_1}^{\alpha_{k1}}.p_{k_2}^{\alpha_{k2}}.....p_{k_n}^{\alpha_{kn}}$. Platí aj indukčný krok. Poznamenávame, že vyjadrenie ľubovoľného prirodzeného čísla $n > 1$ v tvare súčinu prirodzených mocnín prvočísel je jednoznačné ažna poradie činiteľov.

Poznamenávame, že pri dôkaze matematickou indukciou je treba vykonať bázu indukcie aj indukčný krok. Aj keď je dôkaz bázy indukcie vo všeobecnosti podstatne ľahší (netvrdíme, že tak vždy musí byť) ako dôkaz indukčného kroku, nie je rozumné túto etapu podceňovať alebo dokonca vynechávať. Skúsme dokázať nasledujúce tvrdenie:

„Pre každé prirodzené číslo *n* je číslo $2^{3n} + 3^{4n}$ deliteľné číslom 73“. Ako vieme toto tvrdenie neplatí, v príklade 1. sme dokázali opačné tvrdenie. Ak vynecháme bázu indukcie a budeme predpokladať, že pre každé *n* je $2^{3n} + 3^{4n}$ deliteľné číslom 73, tak dostávame, že aj $2^{3(n+1)} + 3^{4(n+1)} = 8.\left(2^{3n} + 3^{4n}\right) + 73.3^{4n}$ je deliteľné číslom 73.

Podobne, ak v príklade 2. vynecháme bázu indukcie, tak dokážeme nesprávne tvrdenie, že súčet $1 + q + q^2 + ... + q^n = \frac{q^{n+1} - q}{q-1}$ pre $q \neq 1$.

Ďalej na príklade ukážeme, aké dôležité sú v indukčnom kroku slová „pre každé prirodzené číslo“. „Dokážeme“, že pre každé prirodzené číslo $n \geq 1$ platí: Ľubovoľných *n* prirodzených čísel sa navzájom rovná. Pre $n = 1$ toto tvrdenie platí, každé prirodzené číslo sa rovná samo sebe. Majme teraz $n+1$ prirodzených čísel $c_1, c_2, ..., c_{n+1}$. Podľa indukčného predpokladu platí:

$$c_1 = c_2 = ... = c_n$$

a tiež $$c_2 = c_3 = ... = c_{n+1}$$

Preto $$c_1 = c_2 = ... = c_n = c_{n+1}.$$

Tým sme dôkaz vykonali. Chyba v tomto prípade nastala v tom, že indukčný krok neplatí pre $n = 1$. Z toho, že každé číslo sa rovná samo sebe ešte nevyplýva, že každé dve čísla sa navzájom rovnajú.

Poznamenávame, že pri dôkaze tvrdení matematickou indukciou je veľmi dôležité správne zvoliť bázu matematickej indukcie o čom svedčí aj predchádzajúci príklad, pretože vo všeobecnosti výroková forma *a*(*n*) platí od určitého celého *n*.

V úvode nášho textu sme uviedli, že matematika je exaktná deduktívna veda, že každé tvrdenie, ktoré chceme do matematickej teórie začleniť, musíme logicky odvodiť, dokázať. Ako je to v súlade s názvom metódy dokazovania matematickou indukciou? Ak si bližšie všimneme spôsob uvažovania pri dokazovaní matematickou indukciou, vidíme, že usudzovanie má čisto deduktívny charakter a dôkaz matematickou indukciou nie je podľa toho nijaká indukcia, ale dedukcia.

Názov indukcia je zrejme vyvolaný tým, že v matematike niekedy pri formulácií úlohy typu „Pre každé prirodzené číslo platí ...“ uvažujú induktívne, najprv pre prirodzené číslo *n* preverujú platnosť tvrdenia, sformulujú samotné tvrdenie a potom nasleduje deduktívne odvodenie tvrdenia.

Na záver tejto časti uvedieme ešte dva dôkazy tvrdení pomocou matematickej indukcie.

Príklad 7. Bernoulliho nerovnosť. Nech $x \in R, x > -1, x \neq 0$, tak pre každé prirodzené číslo $n > 1$ platí $(1+x)^n > 1+nx$.

Riešenie: Nech $n = 2$ $a(2): (1+x)^2 = (1+2x+x^2) > 1+2x$, pretože $x^2 > 0$. Báza indukcie platí. Nech platí $a(n)$, $n \geq 2$, overíme platnosť $a(n+1)$: Počítajme $(1+x)^n > 1+nx$ podľa indukčného predpokladu. Pri podmienke $x > -1, x \neq 0$ platí nerovnosť $1+x > 0$. Vynásobením poslednej nerovnosti $1+x$ dostávame $(1+x)^{n+1} > (1+nx)(1+x) = 1+(n+1)x+nx^2 > 1+(n+1)x$. Platí aj indukčný krok.

Príklad 8. Prvočísel je nekonečne veľa.

Riešenie: Dôkaz vykonáme priamo, pričom použijeme aj matematickú indukciu. Položíme $F_n = 2^{2^n}+1$, pre $n = 0,1,2,...$ dostávame $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, ...$. Najprv ukážeme, že platí: $\prod_{k=0}^{n-1} F_k = F_n - 2,\ n \geq 1$.

1° $n = 1,\ F_0 = 3,\ F_1 - 2 = 3$. Báza indukcie platí.

2° $\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n = (F_n - 2).F_n = \left(2^{2^n}-1\right)\left(2^{2^n}+1\right) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$.

Ďalej ukážeme, že pre $n \neq m$ platí, že F_n, F_m sú nesúdeliteľné. Nech $n < m$, $F_n - 2 = \prod_{k=0}^{n-1} F_k$, teda jeden činiteľ v pravo je F_m. Nech $d \mid F_n \wedge d \mid F_m$. Z toho vyplýva, že $d \mid \prod_{k=0}^{n-1} F_k$. Potom $d \mid \left(F_n - \prod_{k=0}^{n-1} F_k\right) = 2$. Teda $d = 1$ alebo $d = 2$. Keďže $d \mid F_n$, ale F_n je nepárne číslo, preto $d = 1$. Keďže F sú navzájom nesúdeliteľné čísla, a každé z nich je deliteľné nejakým prvočíslom, dostávame že prvočísel je nekonečne veľa, pretože čísel F_n je nekonečne veľa.

***Poznámka*:** Fermat (16. – 17. storočie) vyslovil hypotézu, že každé jeho číslo F_n je prvočíslo. Euler dokázal, že F_5 nie je prvočíslo, je deliteľné číslom 641. Nevie sa zatiaľ, či existuje nekonečne veľa Fermatových prvočísel.

1.3. - 1.4. CVIČENIA

1) Dokážte, že funkcia $y = 2/x$ je klesajúca na intervale $(-\infty, 0)$ aj na intervale $(0, \infty)$.

2) Pre každé dve reálne čísla *a*, *b* platí $|a| + |b| \geq |a+b|$. Dokážte.

3) Dokážte nerovnosť medziaritmetickým a geometrickým priemerom. Pre kladné reálne čísla *a*, *b* platí $(a+b)/2 \geq \sqrt{ab}$. Kedy platí rovnosť?

4) Nech ABC je trojuholník, *a*, *b*, *c* sú jeho strany a t_a, t_b, t_c sú prislúchajúce ťažnice. Dokážte, že v trojuholníku ABC platí: $a + b > 2t_c$.

5) Dokážte, že ak má geometrický útvar dve na seba kolmé osi súmernosti, tak je stredovo súmerný. Platí aj obrátená veta ?

Nasledujúce cvičenia dokážte matematickou indukciou:

6) Nech $n \geq 1$ je prirodzené číslo a $x_1, x_2, ..., x_n$ sú kladné reálne čísla. Potom platí

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + ... + \frac{x_{n-1}}{x_n} + \frac{x_n}{x_1} \geq n .$$

7) Nech $n \geq 1$ je prirodzené číslo, dokážte, že pre každých *n* reálnych čísel $x_1, x_2, ..., x_n$ platí $(x_1 + x_2 + ... + x_n)^2 \leq n\left(x_1{}^2 + x_2{}^2 + ... + x_n{}^2\right)$. Kedy nastane rovnosť ?

8) Dokážte, že pre každé prirodzené číslo $n \geq 2$ platí

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}} .$$

9) Pre každé prirodzené číslo $n \geq 2$ platí

$$\sqrt{n} < 1 + \frac{1}{\sqrt{2}} + ... + \frac{1}{\sqrt{n}} < 2\sqrt{n} .$$

Dokážte.

10) Dokážte, že ak sú $x_1, x_2, ..., x_n$ kladné reálne čísla, pre ktoré platí $x_1 \cdot x_2 \cdot ... \cdot x_n = 1$, tak $x_1 + x_2 + ... + x_n \geq n$.

11) Dokážte, že pre každé prirodzené číslo $n \geq 1$ platí

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

12) Dokážte, že pre každé prirodzené číslo $n \geq 1$ platí

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

13) Dokážte, že pre každé prirodzené číslo $n \geq 1$ platí

$$\sum_{i=1}^{n} 2.3^{i-1} = 3^n - 1$$

2. Úvod do teórie množín

2.1. Základné pojmy a označenia teórie množín

V modernom svete nadobúda matematika čoraz väčší význam. Súčasná matematika je budovaná na základe poznatkov z teórie množín. Tento spôsob pojatia matematiky, pôvodne obmedzený len na teoretickú matematiku,preniká do všetkých vedných oblastí.

Začiatky teórie množín siahajú do 19. storočia. Cantor publikoval prvú prácu z teórie množín v roku 1872 a v priebehu ďalších rokov vytvoril teóriu, ktorá po obsahovej stránke tvorí základ súčasnej matematiky.

Na intuitívnej úrovni chápeme pojem množiny takto: Množina je súbor prvkov, ktoré majú istú spoločnú vlastnosť a tvoria určitý celok.

Napríklad množina obyvateľov mesta Bratislavy, množina všetkých priamok v rovine, množina všetkých celých čísel, atď.

Formulácia pojmu množiny ako súboru vecí je všeobecná a neurčitá, nedáva informáciu o spôsobe tvorby množín, pripúšťa neobmedzenú možnosť tejto tvorby, teda aj možnosť takých množín ako je množina všetkých množín,ktorej existencia sa ukázala byť sporná.

V teórií množín vznikali antinómie, ktoré pripomínali staroveké paradoxy a vynútili potrebu položiť solídnejšie základy teórie množín. Východiskom sa stalo budovanie teórie množín na axiomatickom základe. Axiomatická metóda našla už predtým uplatnenie v matematike.

Množiny budeme označovať veľkými písmenami latinskej abecedy A, B, C, ..., prípadne veľkými písmenami s indexami: $A_1, A_2, ..., A_n, ...$.

Objekty, ktoré tvoria množinu nazývame prvkami danej množiny. Prvky množiny označujeme malými písmenami latinskej abecedy $a, b, c, ...$, $x, y, z, ...$, v prípade potreby ich tiež indexujeme. Skutočnosť, že prvok x patrí do množiny A zapisujeme symbolicky $x \in A$. (Znak $\in$ nazývame binárny predikát patričnosti, prináležitosti), hovoríme tiež, že prvok x je elementom množiny A (množina A obsahuje (prvok) x, x patrí do (množiny) A). Ak x nie je prvkom množiny A, zapisujeme $x \notin A$, alebo niekedy je výhodné zapísať $\neg(x \in A)$.

Akým spôsobom môžeme opísať množinu, t.j. aké prvky množina obsahuje?

Opísať množinu možno v podstate dvomi spôsobmi a to buď vymenovaním jej prvkov, alebo charakterizáciou jej prvkov pomocou nejakej spoločnej vlastnosti. V prvom prípade do zložených zátvoriek vypíšeme všetky prvky danej množiny, v prípade, že množina je konečná, nie príliš veľká; zložené zátvorky môžeme použiť aj v prípade, keď množina je nekonečná spočítateľná. (Presnú definíciu uvedených pojmov uvedieme neskôr).

Príklad 1. $A_1 = \{a_1, a_2, a_3, a_4, a_5\}$

$A_2 = \{\text{Bratislava, B. Bystrica, Košice}\}$

$A_3 = \{a, b, c, d\}$.

V matematike sa však často stretávame s veľmi veľkými alebo nekonečnými množinami, ktoré z pochopiteľných dôvodov nemožno zadať vymenovaním prvkov.

Niektoré z nich sú všeobecne známe a majú zaužívané označenie, napríklad číselné množiny:

N – množina prirodzených čísel

Z - množina celých čísel

Q – množina racionálnych čísel

I – množina iracionálnych čísel

R – množina reálnych čísel

C – množina komplexných čísel.

Iné množiny je potrebné definovať tak, že zadáme vlastnosti, ktoré musia spĺňať všetky prvky danej množiny. Využívame tu takzvanú axiómu (Zermelovu schému separácie), ktorá hovorí, že každá rozumná vlastnosť určuje množinu. Poznamenávame, že rozumná vlastnosť je daná výrokovou formou $V(x)$, pričom x je množinová premenná (t.j. $V(x)$ je výrok, či už pravdivý alebo nepravdivý, ak za x dosadíme ľubovoľnú množinu). Potom ku každej množine A existuje množina B všetkých tých prvkov $a \in A$, pre ktoré je $V(a)$ pravdivý výrok. Množinu B označujeme znakom

$$\{x \in A \mid V(x)\} \qquad (1)$$

Napríklad: $\{x \in R \mid 5 \le x \le 10\}$

(V literatúre sa používajú aj zápisy $\{x \in A : V(x)\}$ a $\{x \in A, V(x)\}$, $\{x \in A; V(x)\}$

Ďalej uvedieme príklady množín určené vyššie uvedeným spôsobom.

$$A_4 = \{x \in N \mid (x \text{ je deliteľné dvomi})\}$$

$$A_5 = \left\{x \in R \mid \left(x^2 - 2x + 1 \ge 0\right)\right\}$$

Keď si všimneme predchádzajúce príklady vidíme, že výraz (1) je ich zovšeobecnený zápis, ktorý označuje, že príslušnú množinu tvoria prvky, ktoré majú istú rozumnú vlastnosť a do množiny nepatria tie prvky z vybratej množiny, ktoré danú vlastnosť reprezentovanú výrokovou formou $V(x)$ nemajú.

Cantor používal intuitívny pojem množiny a nehovoril nič o spôsobe tvorby množín z ľubovoľných objektov. To viedlo k niektorým ťažkostiam – paradoxom v teórii množín a podnietilo vznik axiomatickej teórie množín. Ako príklad uvádzame Russellov paradox.

Poznamenávame, že v axióme separácie je veľmi dôležité, že prvky x, ktoré tvoria množinu B, berieme z množiny (v našom prípade z množiny A). Bez tohto obmedzenia axióma neplatí! Dokážeme to pomocou Russellovho paradoxu. Nech X je množina a $V(x)$ je výroková forma $x \notin X$ (je to zrejme výroková forma (funkcia) jednej voľnej premennej). Nech by existovala množina M všetkých tých x, pre ktoré $V(x)$ je pravdivá, t.j. nech $M = \{x \mid x \notin X\}$ (do $V(x)$ dosadzujeme všetky možné množiny bez obmedzenia). Podľa definície teda máme pre každé x, $x \in M$ práve vtedy, keď $V(x)$, t.j. $x \in M \leftrightarrow x \notin X$. Ak za x dosadíme špeciálne množinu M, tu sme aj za X dosadili, dostaneme výrok $M \in M \leftrightarrow M \notin M$, ktorý je nepravdivý.

Poznamenávame, že pomocou vyššie uvedeného príkladu sa dá ukázať, že neexistuje množina, ktorej prvkami by boli všetky množiny.

Ďalej si treba všimnúť, že axióma separácie vlastne predstavuje nekonečne veľa axióm (ku každej výrokovej funkcii jednu).

Podľa Cantora môžeme vytvoriť množinu, ktorej prvkami sú všetky množiny. Označme ju znakom M. Pretože M je množina, tak je aj prvkom množiny všetkých množín, teda $M \in M$. Pre množinu N všetkých prirodzených čísel zasa platí $N \notin N$. Rozdelíme teda množinu M všetkých množín na množiny U a V, pričom U je množina tých prvkov $x \in M$ pre ktoré platí $x \notin X$ a V je množina tých prvkov $x \in M$, pre ktoré platí $x \in X$. Platia tieto vzťahy:

$$M = \mathrm{U} \cup \mathrm{V}, \quad \mathrm{U} \cap \mathrm{V} = \emptyset$$

Množiny U, V sú neprázdne, lebo $M \in \mathrm{V}$ a $N \in \mathrm{U}$. Každá množina patrí do U alebo do V. Kam patrí množina U ?

Ak $\mathrm{U} \in \mathrm{V}$, tak podľa definície V je $\mathrm{U} \in \mathrm{U}$. Ale $\mathrm{U} \cap \mathrm{V} = \emptyset$ tak ak $\mathrm{U} \in \mathrm{V}$, potom $\mathrm{U} \notin \mathrm{U}$. Máme spor $\mathrm{U} \in \mathrm{U}$ a súčasne $\mathrm{U} \notin \mathrm{U}$. Teda nie je možné, aby $\mathrm{U} \in \mathrm{V}$.

Ak $\mathrm{U} \notin \mathrm{V}$, tak $\mathrm{U} \in \mathrm{U}$ a podľa definície U, $\mathrm{U} \notin \mathrm{U}$. Opäť máme spor.

Máme teda množinu U, ktorá nie je prvkom *M*, čo je v rozpore s tým, že *M* je množina všetkých množín, *M* potom ale nemôže byť množina.

2.2. Základné množinové operácie a vzťahy

Definícia 2.2.1 Nech sú *A*, *B* ľubovoľné množiny. Hovoríme, že množina ***A* sa rovná** množine ***B***, označujeme $A = B$ práve vtedy, ak každý prvok z množiny *A* je súčasne prvkom množiny *B* a každý prvok z množiny *B* je súčasne prvkom množiny *A*.

Formálne možno vyššie uvedenú definíciu zapísať takto:
$A = B \leftrightarrow (\forall x)[((x \in A) \rightarrow (x \in B)) \wedge ((x \in B) \rightarrow (x \in A))]$ resp. skrátene $A = B \leftrightarrow (\forall x)((x \in A) \leftrightarrow (x \in B))$.

Príklad 1. Množina $A=\{x|\ (x \in N) \wedge (x \text{ je deliteľné dvomi})\}$ a množina $B = \{0,2,4,...,2n,...\}$ sa rovnajú.

Definícia 2.2.2 Nech sú *A*, *B* ľubovoľné množiny. Ak pre každý prvok $x \in A$ platí, že *x* je prvkom *B*, tak potom hovoríme, že množina ***A* je podmnožinou** množiny ***B*** alebo tiež, že *A* je v inklúzii s *B*, označenie $A \subseteq B$.

Ak $A \subseteq B$ a existuje prvok množiny *B* taký, ktorý nepatrí do množiny *A* (t.j. neplatí $B \subseteq A$), tak hovoríme, že ***A* je vlastná alebo pravá podmnožina** množiny ***B*** a označujeme $A \subset B$.

Poznamenávame, že niekedy namiesto $A \subseteq B$ sa v literatúre píše $A \subset B$. Vtedy namiesto $A \subset B$ píšeme $A \subsetneq B$.

Skutočnosť, že $A \subseteq B$ zapisujeme formálne takto:

$$A \subseteq B \leftrightarrow (\forall x)((x \in A) \rightarrow (x \in B))$$

Príklad 2. Pre množiny *A*, *B* z predchádzajúceho príkladu platí, že $A \subseteq B$.

Príklad 3. Pre množiny $A = \{0,2,4,...,2n,...\}$ a $B = N$ platí že, $A \subset B$.

Treba si všimnúť, že z porovnania predchádzajúcich definícií vyplýva, že rovnosť množín $A = B$ možno zapísať aj pomocou vzťahu inklúzie:

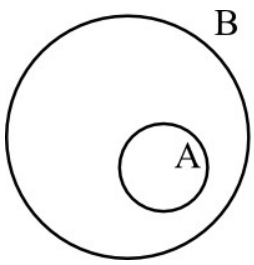
$$A = B \leftrightarrow ((A \subseteq B) \wedge (B \subseteq A))$$

Tento posledný vzťah budeme často používať pri dokazovaní vlastností nejakých dvoch množín.

Všimnime si, že v prípade rovnosti množín *A*, *B* z Príkladu 1., nám platia obe inklúzie, $A \subseteq B$, $B \subseteq A$.

V ďalšom budeme predpokladať, že množiny s ktorými pracujeme tvoria podmnožiny nejakej univerzálnej množiny U. Poznamenávame, že množina U nie je množina, ktorá obsahuje všetky množiny, ako uvidíme neskôr, taká množina neexistuje.

Niektoré vzťahy medzi množinami, množinové operácie možno názorne reprezentovať pomocou Vennových diagramov. Množiny budeme reprezentovať spojitými olasťami roviny (kruhmi). Na obr. 1 sú znázornené dve množiny *A*, *B* také, že $A \subseteq B$.



Obr. 1

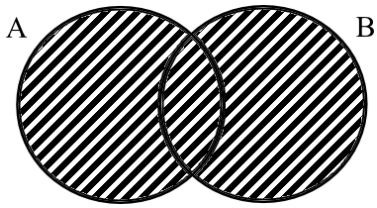
Zavedieme teraz operácie zjednotenia, prieniku, doplnku, rozdielu množín, symetrickej diferencie a karteziánskeho súčinu.

Definícia 2.2.3 Nech sú A a B ľubovoľné množiny. **Zjednotením množín *A*, *B*** nazveme množinu všetkých prvkov, ktoré patria aspoň do jednej z množín A, B. Označenie: $A \cup B$.

Formálne zapísané zjednotenie množín:

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$$

Pomocou Vennových diagramov zjednotenie znázorňujeme takto:



Obr. 2

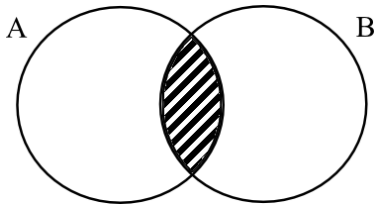
Príklad 4. $A = \{x \mid x = 2k, k \in n\}$, $B = \{x \mid x = 2k+1, k \in n\}$. $A \cup B = N$.

Definícia 2.2.4 Nech sú A a B ľubovoľné množiny. **Prienikom množín *A*, *B*** nazveme množinu všetkých prvkov, ktoré patria súčasne do oboch množín A, B. Označenie: $A \cap B$.

Formálne zapisujeme prienik množín:

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

Pomocou Vennových diagramov prienik množín znázorňujeme takto:



Obr. 3

Príklad 5. Nech $A = \{x \mid (x \in N) \wedge x \geq 5\}$, $B = \{x \mid (x \in Z) \wedge x \leq 9\}$. Potom $A \cap B = \{x \mid x \in N, 5 \leq x \leq 9\}$.

Nech A a B sú ľubovoľné množiny, ak neexistuje taký prvok, ktorý súčasne patrí do množiny A aj B, teda množiny A, B nemajú spoločný prvok, v tomto prípade hovoríme, že množiny sú **disjunktné** a ich prienikom je množina, ktorá neobsahuje žiaden prvok.

Definícia 2.2.5 Množina, ktorá neobsahuje žiaden prvok sa nazýva **prázdna množina** a označujeme ju $\emptyset$.

Poznamenávame, že prázdnu množinu môžeme definovať pomocou ľubovoľnej vlastnosti, ktorú nespĺňa žiaden prvok.

V nasledujúcom tvrdení ukážeme dve dôležité vlastnosti prázdnej množiny.

Veta 2.2.1 a) Prázdna množina je podmnožina ľubovoľnej množiny
b) Existuje práve jedna prázdna množina

Dôkaz: Najprv dokážeme tvrdenie a) priamo a potom sporom.

Nech X je ľubovoľná množina, máme dokázať, že $\emptyset \subseteq X$. Z definície vyplýva, že $\emptyset \subseteq X \leftrightarrow (\forall x)(x \in \emptyset \rightarrow x \in X)$. Všimnime si, že kvantifikovaný výrok na pravej strane ekvivalencie je vždy pravdivý, pre ľubovoľnú množinu X, teda je tautológia, pretože implikácia $x \in \emptyset \rightarrow x \in X$ je vždy pravdivý výrok, lebo výrok $x \in \emptyset$ má pravdivostnú hodnotu 0.

Ďalej dokážeme tvrdenie a) sporom. Predpokladajme, že tvrdenie vety neplatí. To znamená, že platí jeho negácia.

$$\neg(\forall X)\{\varnothing \subseteq X\} \leftrightarrow (\exists X)\neg\{\varnothing \subseteq X\},$$

čiže slovne povedané; existuje taká množina X, že prázdna množina nie je podmnožinou X, to ale znamená, že prázdna množina obsahuje prvok, ktorý nepatrí do X. To ale nie je možné, pretože prázdna množina neobsahuje žiaden prvok. Dostali sme spor, čiže platí tvrdenie $(\forall X)\{\varnothing \subseteq X\}$ a nie jeho negácia.

Tvrdenie b) dokážeme sporom. Predpokladajme, že existujú dve rôzne prázdne množiny A_1, A_2. Vzhľadom na to, že A_1, A_2 sú prázdne množiny, podľa predchádzajúceho tvrdenia platí $A_1 \subseteq A_2$ a súčasne $A_2 \subseteq A_1$, z toho vyplýva, že $A_1 = A_2$, čo je v spore s predpokladom. Teda existuje práve jedna prázdna množina.

Definícia 2.2.6 Nech A je ľubovoľná množina, $A \subseteq \mathrm{U}$. **Doplnkom množiny *A*** vzhľadom na množinu U nazývame množinu všetkých tých prvkov univerzálnej množiny U, ktoré nepatria do množiny A. Označenie A'.

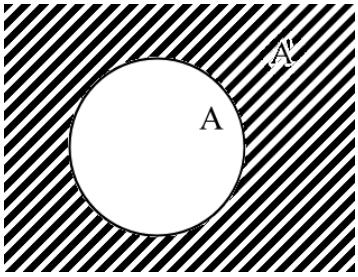
Formálny zápis:

$$A' = \{x \mid x \in \mathrm{U} \wedge x \notin A\}.$$

V literatúre označujú doplnok (komplement) množiny A aj ako $\overline{A}$ alebo A^C.

Keďže uvažujeme doplnok (komplement) množiny vzhľadom na univerzálnu množinu U, často používame aj skrátený formálny zápis

$$A' = \{x \mid x \notin A\}.$$



Obr. 4

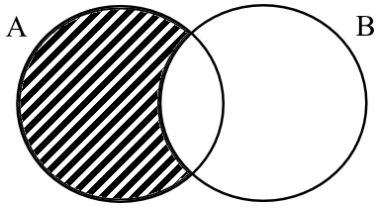
Poznamenávame, že pojem doplnok množiny možno zovšeobecniť, t.j. vyjadriť nielen vzhľadom na univerzálnu množinu, ale aj vzhľadom na ľubovoľnú inú množinu. Na to uvedieme ďalšiu množinovú operáciu rozdiel množín.

Definícia 2.2.7 Nech sú A, B ľubovoľné množiny. **Rozdielom množín *A*, *B*** nazveme množinu všetkých tých prvkov množiny A, ktoré nepatria do B. Označenie $A \setminus B$, alebo aj $A - B$.

Formálny zápis:

$$A - B = \{x \mid (x \in A) \wedge (x \notin B)\}.$$

Znázornenie pomocou Vennových diagramov:



Obr. 5

Príklad 6. Nech $A = \langle 5,12\rangle$, $B = \langle 7,15\rangle$. Potom $A - B = \langle 5,7\rangle$.

Ľahko vidno, že rozdiel množín môžeme vyjadriť pomocou prieniku a doplnku nasledovne:

$$A - B = A \cap B'$$

V takomto prípade doplnok A' množiny A vzhľadom na univerzálnu množinu U nie je nič iné ako $U - A = U \cap A' = A'$.

Pomocou rozdielu dvoch množín budeme definovať ďalšiu množinovú operáciu, symetrickú diferenciu množín.

Definícia 2.2.8 Nech sú A, B ľubovoľné množiny. **Symetrickou diferenciou množín *A*, *B*** nazveme množinu

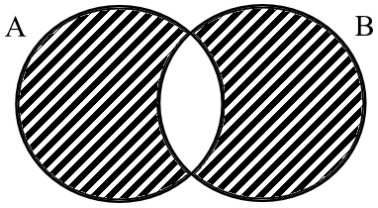
$$A \div B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}.$$

Symetrickú diferenciu množín A, B možno vyjadriť pomocou rozdielu a zjednotenia množín skrátene takto:

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

Príklad 7. Nech $A = \langle 5,12\rangle$, $B = \langle 7,15\rangle$. Potom $A \div B = \langle 5,7) \cup (12,15\rangle$.

Grafické znázornenie symetrickej diferenciemnožín A, B.



Obr. 6

Na záver tejto časti uvedieme ďalší typ dôležitej množiny. Videli sme už, že prvkami množiny môžu byť aj iné množiny. Medzi množinami, ktorých prvkami sú množiny majú zvláštny význam tzv. potenčné množiny.

Definícia 2.2.9 Nech je daná množina A. **Potenčnou množinou** množiny ***A*** nazveme množinu všetkých podmnožín množiny A. Označenie $\mathcal{P}(A)$. Teda

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

Príklad 8. Nech $A = \{a_1, a_2, a_3\}$. Potom

$$\mathcal{P}(A) = \{\emptyset, \{a_1\}, \{a_2\}, \{a_3\}, \{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}, \{a_1, a_2, a_3\}\}.$$

2.3. Základné vlastnosti množinových operácií

Uvedieme najprv niekoľko jednoduchých vlastností základných množinových operácií. Treba si uvedomiť, že jednu a tú istú množinu môžeme vyjadriť rôznymi spôsobmi. Je pochopiteľné, že sa snažíme získať vyjadrenie čo najjednoduchšie a najprehľadnejšie. Podľa toho aký typ úlohy riešime, podľa toho hľadáme aj vhodné vyjadrenie množiny, s ktorou pracujeme.

Veta 2.3.1 Nech A, B, C sú ľubovoľné množiny, potom platia nasledujúce rovnosti:

1) $A \cup B = B \cup A$, $A \cap B = B \cap A$ **komutatívnosť**
2) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ **asociatívnosť**
3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ **distributívnosť**
4) $A \cup A = A$, $A \cap A = A$ **idempotentnosť**
5) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$
6) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$ **de Morganove zákony**

Dôkaz: Dokážeme len tvrdenie 1) a 6). Ostatné tvrdenia nechávame usilovnému čitateľovi. Pri dôkazoch uvedených tvrdení budeme vychádzať z definície uvedených množinových operácií a z vlastností výrokovej logiky. Najprv ukážeme, že platí $A \cup B = B \cup A$. Treba nám teda dokázať, že platí $A \cup B \subseteq B \cup A$ a súčasne $B \cup A \subseteq A \cup B$. Nech $x \in A \cup B$, x je ľubovoľný prvok, $x \in A \cup B \to x \in A \vee x \in B \to x \in B \vee x \in A \to x \in B \cup A$. Teraz obrátená inklúzia, nech $x \in B \cup A \to x \in B \vee x \in A \to x \in A \vee x \in B \to x \in A \cup B$. Mohli by sme uvažovať aj takto: $x \in A \cup B \leftrightarrow x \in A \vee x \in B \leftrightarrow x \in B \vee x \in A \leftrightarrow x \in B \cup A$. Využili sme pritom ekvivalenciu výrokov $p \vee q \leftrightarrow q \vee p$.

Ďalej dokážeme, že $\overline{A \cap B} = \overline{A} \cup \overline{B}$, máme teda opäť dokazovať inklúzie $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$, $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. Obe inklúzie dokážeme súčasne, nie oddelene. Nech x je ľubovoľný prvok, pričom $x \in \overline{A \cap B} \leftrightarrow \neg(x \in A \cap B) \leftrightarrow \neg(x \in A \wedge x \in B) \leftrightarrow \neg(x \in A) \vee \neg(x \in B) \leftrightarrow x \in \overline{A} \vee x \in \overline{B} \leftrightarrow$ $x \in \overline{A} \cup \overline{B}$. Pri dôkaze sme využili ekvivalenciu výrokov $\overline{p \wedge q} \leftrightarrow \overline{p} \vee \overline{q}$.

Poznamenávame, že pri tomto spôsobe dôkazov musíme dávať veľký pozor, či využívame ekvivalenciu výrokov, alebo len platnosť implikácie istých výrokov. Napríklad vo všeobecnosti neplatí rovnosť $A \cap B = A$, pretože platí implikácia $p \wedge q \to p$ a teda $A \cap B \subseteq A$, neplatí ekvivalencia $p \wedge q \leftrightarrow p$.

Príklad 1. Nech A, B, C sú ľubovoľné množiny, potom platí $(A \cap B) - C = (A - C) \cap (B - C)$

Riešenie: Pri dôkaze tejto identity využívame platnosť už dokázaných identít z predošlej vety a rovnosť $A - B = A \cap \overline{B}$. Postupujeme nasledujúcim spôsobom. Vezmime výrok na ľubovoľnej strane rovnosti a pomocou ekvivalentných množinových úprav sa snažíme získať druhú stranu, takýmto spôsobom dostávame:

$(A - C) \cap (B - C) = (A \cap \overline{C}) \cap (B \cap \overline{C}) = ((A \cap \overline{C}) \cap B) \cap \overline{C} = (A \cap \overline{C} \cap B) \cap \overline{C} = (A \cap B) \cap (\overline{C} \cap \overline{C}) =$
$(A \cap B) \cap \overline{C} = (A \cap B) - C$.

Poznámka: Všimnime si podstatný rozdiel pri dokazovaní množinových identít. Vo vete sme vychádzali z definícií množinových operácií a vykonali sme ekvivalentné úpravy výrokov, v príklade sme robili ekvivalentné úpravy s množinovými operáciami. Pri dôkazoch množinových identít sa musíme vyvarovať používaniu nasledujúcich zápisov, napríklad $A \cup B = x \in A \vee x \in B$. Zápis nie je správny, pretože na ľavej strane je množina a na pravej strane zložený výrok v tvare disjunkcie výrokov. Správne zápisy sú $A \cap B = \{x \mid x \in A \wedge x \in B\}$ a $x \in A \cup B \leftrightarrow x \in A \vee x \in B$.

Príklad 2. Nech A, B sú ľubovoľné množiny, potom platí $A \div B = (A \cup B) - (A \cap B)$.

Riešenie: Upravíme pravú stranu identity: $(A \cup B) - (A \cap B) = (A \cup B) \cap \overline{(A \cap B)} =$
$= (A \cup B) \cap (\overline{A} \cup \overline{B}) = [(A \cup B) \cap \overline{A}] \cup [(A \cup B) \cap \overline{B}] = [((A \cap \overline{A}) \cup (B \cap \overline{A}))] \cup [(A \cap \overline{B}) \cup (B \cap \overline{B})] =$
$= [\varnothing \cup (B \cap \overline{A})] \cup [(A \cap \overline{B}) \cup \varnothing] = (B \cap \overline{A}) \cup (A \cap \overline{B}) = (B - A) \cup (A - B) = (A - B) \cup (B - A) = A \div B$.
Najprv sme použili identitu $X - Y = X \cap \overline{Y}$, potom de Morganov zákon, distributívny zákon, identitu $\varnothing \cup X = X$, komutatívny zákon a definíciu symetrickej diferencie.

Príklad 3. Nech A, B sú ľubovoľné množiny, dokážte, že nasledujúce výroky sú ekvivalentné: $A \subseteq B$ a $A \cap B = A$.

Riešenie: Máme teda dokázať, že $A \subseteq B$ platí práve vtedy, keď $A \cap B = A$. Predpokladajme, že $A \subseteq B$, potrebujeme dokázať inklúzie $A \cap B \subseteq A$ a $A \subseteq A \cap B$. Prvá inklúzia platí pre ľubovoľné množiny A, B (pretože implikácia $p \wedge q \to p$ je tautológia), druhú inklúziu dokážeme sporom. Nech $A \subseteq B$ a nech súčasne $\neg(A \subseteq A \cap B)$, to sú naše predpoklady. Podrobne rozpíšeme druhý predpoklad: $\neg(A \subseteq A \cap B) \leftrightarrow \neg(\forall x)((x \in A) \to (x \in A \cap B)) \leftrightarrow$
$(\exists x)\neg(\neg(x \in A) \vee x \in A \cap B) \leftrightarrow (\exists x)((x \in A) \wedge \neg(x \in A \cap B))$.

To znamená, že existuje prvok *u*, ktorý patrí do množiny *A* a súčasne nepatrí do množiny $A \cap B$, t.j. $(u \in A) \wedge \neg(u \in A \wedge u \in B) \leftrightarrow (u \in A) \wedge ((u \notin A) \vee (u \notin B)) \leftrightarrow$
$((u \in A) \wedge (u \notin A)) \vee ((u \in A) \wedge (u \notin B)) \leftrightarrow (u \in A) \wedge (u \notin B)$.
Predpokladali sme však, že $A \subseteq B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$. Tvrdenie, ktoré sme odvodili je negáciou $u \in A \rightarrow u \in B$. Teda $\neg(u \in A \rightarrow u \in B) \leftrightarrow (u \in A \wedge u \notin B)$. Dostali sme spor, ktorý poukazuje na to, že z predpokladu $A \subseteq B$ musí platiť aj $A \subseteq A \cap B$.

Ďalej budeme dokazovať obrátenú implikáciu, t. j. že z predpokladu $A \cap B = A$ vyplýva $A \subseteq B$. Implikáciu budeme dokazovať priamo. Nech platí výrok $A \cap B = A$, to znamená, že pre každé x platí $x \in A \cap B \leftrightarrow x \in A$, teda $x \in A \wedge x \in B \leftrightarrow x \in A$. Z pravdivosti uvedeného výroku vyplýva platnosť výroku $x \in A \rightarrow x \in B$, uvedená implikácia platí z nasledujúcej úvahy: ak výrok $x \in A$ je pravdivý, potom musí byť pravdivý aj výrok $x \in A \wedge x \in B$ (keďže sú oba výroky ekvivalentné) a teda aj výrok $x \in B$. V prípade, že $x \in A$ je nepravdivý výrok, implikácia $x \in A \rightarrow x \in B$ je opäť pravdivá, teda za uvedeného predpokladu, že $x \in A \wedge x \in B \leftrightarrow x \in A$ je implikácia $x \in A \rightarrow x \in B$ tautológia, teda $A \subseteq B$.

Príklad 4. Nech *A*, *B*, *C* sú ľubovoľné množiny. Dokážte, že inklúzia $A \cup B \subseteq C$ platí práve vtedy, ak $A \subseteq C$ a $B \subseteq C$.

Riešenie: Skôr, než začneme úlohu riešiť, všimnime si štruktúru tohto tvrdenia. Označme symbolom:

p výrok $A \cup B \subseteq C$
q výrok $A \subseteq C$
r výrok $B \subseteq C$
s výrok „*A*, *B*, *C* sú ľubovoľné množiny“

Potom tvrdenie môžeme schématicky zapísať takto:

$$\frac{s}{p \leftrightarrow (q \wedge r)}$$

Výrok s je predpoklad a tvrdenie, ktoré treba dokázať je $(p \rightarrow (q \wedge r)) \wedge ((q \wedge r) \rightarrow p)$. Implikáciu $p \rightarrow (q \wedge r)$ dokážeme sporom. Nech $A \cup B \subseteq C$ a $\neg(A \subseteq C \wedge B \subseteq C)$. To znamená, že platí tvrdenie $\neg(A \subseteq C) \vee \neg(B \subseteq C)$, teda buď existuje prvok $a \in A - C$ alebo $b \in B - C$. Keďže $A - C \subseteq A \cup B$ a $B - C \subseteq A \cup B$, prvok *a* nepatrí do *C* ale patrí do *A*, prvok *b* nepatrí do *C* ale patrí do *B*, teda *a* alebo *b* patrí do $A \cup B \subseteq C$, teda *a* alebo *b* patrí aj do *C*, čo je spor.

Implikáciu $(q \wedge r) \rightarrow p$ dokážeme priamo. Nech platí $A \subseteq C$ a $B \subseteq C$. To znamená $A \cup C = C$, $B \cup C = C$, potom aj $(A \cup B) \cup C = A \cup (B \cup C) = A \cup C = C$ a teda aj $A \cup B \subseteq C$.

2.4. Usporiadaná dvojica a karteziánsky súčin

Ak chceme na množinovom jazyku bližšie skúmať a popisovať vlastnosti, vzťahy a štruktúru jednotlivých množín je potrebné zaviesť niektoré ďalšie dôležité pojmy. K novým pojmom bezprostredne patrí usporiadaná dvojica, vo všeobecnosti usporiadaná *n*-tica a pomocou nich definovaný karteziánsky súčin množín.

Pojem usporiadanej dvojice (*n*-tice) je čitateľovi zrejme na intuitívnej úrovni jasný. Pod usporiadanou *n*-ticou si môžeme predstaviť konečnú postupnosť o *n*-členoch. Usporiadanú *n*-ticu pre $n \geq 1$ budeme označovať $(a_1, a_2, ..., a_n)$, čo predstavuje aj *n*-rozmerný vektor. Pojem usporiadanej *n*-tice sa dá definovať rôznym spôsobom. Pri definovaní usporiadanej *n*-tice dbáme predovšetkým na to, aby bola zachovaná nasledujúca vlastnosť: Nech $(a_1, a_2, ..., a_n)$, $(b_1, b_2, ..., b_n)$ sú dve usporiadané *n*-tice, tieto sa rovnajú práve vtedy, ak $a_i = b_i$, pre $i = 1,2,...,n$.

Na jazyku teórie množín môžeme podobne definovať pojem usporiadanej dvojice (a_1, a_2) nasledujúcim spôsobom.

Definícia 2.4.1 Nech sú a_1, a_2 ľubovoľné prvky. Množinu $\{\{a_1\},\{a_1, a_2\}\}$ nazývame **usporiadanou dvojicou**, označenie (a_1, a_2), pričom a_1 nazývame prvou súradnicou (zložkou), a_2 druhou súradnicou (zložkou).

Usporiadanú *n*-ticu, pre $n \geq 1$ môžeme teraz definovať induktívne takto:

$$(a_1) = a_1$$
$$(a_1, a_2) = \{\{a_1\},\{a_1, a_2\}\}$$
$$\vdots$$
$$(a_1, a_2, ..., a_n) = ((a_1, \ldots, a_{n-1}), a_n).$$

Platí nasledujúce tvrdenie, charakterizujúce základnú vlastnosť usporiadanej dvojice.

Veta 2.4.1 Nech (a_1, a_2), (b_1, b_2) sú dve usporiadané dvojice. $(a_1, a_2) = (b_1, b_2)$ práve vtedy, ak $a_1 = b_1$, $a_2 = b_2$.

Dôkaz: Ak platí, že $a_1 = b_1$ súčasne $a_2 = b_2$, tak zrejme platí $\{\{a_1\},\{a_1, a_2\}\} = \{\{b_1\},\{b_1, b_2\}\}$. Nech teraz $(a_1, a_2) = (b_1, b_2)$, dôkaz rozdelíme na dve časti.

1) Nech $a_1 = a_2$. Potom dostávame $\{\{a_1\}\} = \{\{b_1\},\{b_1, b_2\}\}$. Odtiaľ dostávame, že $b_1 = b_2$, súčasne $a_1 = b_1$.

2) Nech $a_1 \neq a_2$, potom z rovnosti $(a_1, a_2) = (b_1, b_2)$ dostávame, že $b_1 \neq b_2$, $a_1 = b_1$, $a_2 = b_2$.

Tým je dôkaz vety ukončený.

Poznamenávame, že prvky usporiadanej dvojice, *n*-tice nemusia byť navzájom rôzne.

Pomocou pojmu usporiadanej dvojice zavedieme pojem karteziánskeho súčinu.

Definícia 2.4.2 **Karteziánskym súčinom množín** *A*, *B* nazveme množinu

$$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}.$$

Príklad 1. $A = \{a_1, a_2\}$, $B = \{b_1, b_2, b_3\}$;

$A \times B = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3)\}$.

Definíciu karteziánskeho súčinu môžeme rozšíriť aj pre prípad *n* množín, môžeme postupovať induktívne, ako v prípade usporiadanej *n*-tice. Teda

$$A = \{(a) \mid a \in A\}$$
$$A_1 \times A_2 = \{(a_1, a_2) \mid a_1 \in A_1 \wedge a_2 \in A_2\}$$
$$\vdots$$
$$A_1 \times A_2 \times \ldots \times A_n = (A_1 \times A_2 \times \ldots \times A_{n-1}) \times A_n$$

Pri definovaní karteziánskeho súčinu *n* – množín môžeme postupovať aj jednoduchšie, budeme vychádzať z pojmu usporiadanej *n* – tice, pričom budeme mať na zreteli základnú vlastnosť usporiadaných *n* – tíc, usporiadané *n* – tice $(a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_n)$ práve vtedy, ak $a_i = b_i$, pre $i = 1,2,...,n$, pričom všetky $a_1, a_2, ..., a_n$ nemusia byť navzájom rôzne. **Karteziánsky súčin množín** $A_1, A_2, ..., A_n$ môžeme definovať ako množinu

$$A_1 \times A_2 \times ... \times A_n = \left\{ (a_1, a_2, ..., a_n) \mid a_i \in A_i, i = \overline{1,n} \right\}.$$

Poznámka: Všimnime si, že ak máme dané dve konečné množiny: $A = \{a_1, a_2, ..., a_n\}$, $B = \{b_1, b_2, ..., b_m\}$, tak karteziánsky súčin množín $A \times B$ je vhodné niekedy reprezentovať obdĺžnikovou maticou typu $n \times m$, na priesečníku *i*–teho riadku a *j*-teho stĺpca bude prvok (a_i, b_j). Nie je ťažké vidieť, že medzi $A \times B$ a obdĺžnikovou maticou je vzájomne jednoznačné priradenie.

Príklad 2. Nech *A*, *B*, *C* sú ľubovoľné množiny. Ukážeme, že vo všeobecnosti neplatí $A \times B = B \times A$, komutatívny zákon pre karteziánsky súčin množín a taktiež neplatí $A \times (B \times C) = (A \times B) \times C$, asociatívny zákon pre karteziánsky súčin množín.

Riešenie: Najprv ukážeme, že $A \times B \neq B \times A$, ak $A = \{a\}$, $B = \{b\}$, pričom predpokladáme, že $a \neq b$, $A \times B = \{(a,b)\}$, $B \times A = \{(b,a)\}$, odtiaľ $\{(a,b)\} \neq \{(b,a)\}$. Ďalej uvažujme množinu $C = \{c\}$, pričom predpokladáme, že $c \neq a$, $c \neq b$,. Potom $A \times (B \times C) = \{(a,(b,c))\}$, $(A \times B) \times C = \{((a,b),c)\}$, $\{(a,(b,c))\} \neq \{((a,b),c)\}$.

Príklad 3. Ukážeme, že ak aspoň jedna z množín *A*, *B* je prázdna, tak potom $A \times B = \varnothing$.

Riešenie: Trvrdenie dokážeme sporom. Bez ujmy na všeobecnosti predpokladajme, že $A = \varnothing$, a pre spor nech $A \times B \neq \varnothing$. To znamená, že existuje $(a,b) \in A \times B$ je pravdivý výrok. Potom ale platí, že $a \in A$ a súčasne $b \in B$, to je výrok nepravdivý, čiže dostávame sa do sporu. Implikácia je nepravdivá, ak predpoklad $(a,b) \in A \times B$ je pravdivý a záver $a \in A \wedge b \in B$ je nepravdivý.

Príklad 4. Nech *A*, *B*, *C* sú ľubovoľné množiny, potom platí nasledujúca rovnosť:

$$(A \cup B) \times C = (A \times C) \cup (B \times C).$$

Riešenie: Zvolíme nasledujúci postup, vezmeme ľubovoľný prvok $(x,y) \in (A \cup B) \times C$, využijeme definíciu množinových operácií a karteziánskeho súčinu množín, uskutočníme ekvivalentné úpravy výrokov a ukážeme, že prvok $(x,y) \in (A \times C) \cup (B \times C)$ a obrátene. Nech teda

$$(x,y) \in (A \cup B) \times C \leftrightarrow x \in (A \cup B) \wedge y \in C \leftrightarrow (x \in A \vee x \in B) \wedge y \in C \leftrightarrow$$
$$(x \in A \wedge y \in C) \vee (x \in B \wedge y \in C) \leftrightarrow (x,y) \in (A \times C) \vee (x,y) \in B \times C \leftrightarrow$$
$$\leftrightarrow (x,y) \in (A \times C) \cup (B \times C).$$

Ďalšie dôležité množinové identity a vzťahy uvádzame v cvičeniach. Odporúčame čitateľovi venovať im patričnú pozornosť.

2.1. – 2.4. CVIČENIA

1) Nech A, B sú ľubovoľné množiny. Dokážte, že platia nasledujúce vzťahy:

a) $A \cap B \subseteq A,\ A \cap B \subseteq B$

b) $A \subseteq A \cup B,\ B \subseteq A \cup B$

c) $\overline{\overline{A}} = A$

d) $A \cap \overline{A} = \emptyset,\ A \cup \overline{A} = \mathrm{U}$

e) $A \cap (A \cup B) = A,\ A \cup (A \cap B) = A$, absorbčné zákony.

2) Nech A, B, C sú ľubovoľné množiny. Dokážte, že platia nasledujúce vzťahy:

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

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

c) $C - (A \cap B) = (C - A) \cup (C - B)$

d) $C - (A \cup B) = (C - A) \cap (C - B)$

e) $A - B = A - (A \cap B) = (A \cup B) - B$

f) $A - (B - C) = (A - B) \cap (A \cap C)$

g) $(A - B) - C = A - (B \cup C)$

3) Nech A, B sú ľubovoľné množiny, dokážte, že platia nasledujúce vzťahy:

a) $A \div B = B \div A$ komutatívnosť

b) $A \div (B \div C) = (A \div B) \div C$ asociatívnosť

c) rovnica $X \div A = B$ má jediné riešenie $X = A \div B$.

4) Nech A, B sú ľubovoľné množiny a U univerzálna množina. Dokážte, že potom sú nasledujúce výroky ekvivalentné:

a) $A \subseteq B$

b) $A \cap B = A$

c) $A \cup B = B$

d) $A - B = \emptyset$

e) $\overline{A} \cup B = \mathrm{U}$

f) $A \div B = B - A$

5) Nech A, B, C sú ľubovoľné množiny. Dokážte, že platí inklúzia $C \subseteq A \cap B$ práve vtedy, ak $C \subseteq A$ a $C \subseteq B$.

6) Nech A, B sú ľubovoľné množiny.

a) Zapíšte formálne negáciu tvrdení $A \subseteq B$, $A = B$.

b) Slovne vyjadrite negáciu uvedených tvrdení

7) Zistite, či platí: Ak $C \neq \emptyset$ a $A \times C = B \times C$, tak $A = B$.

8) Nech A, B, C sú ľubovoľné množiny, potom platia nasledujúce tvrdenia:

a) Ak $A \subseteq B$, tak pre každú množinu C platí $A \times C \subseteq B \times C$

b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

c) $(A-B)\times C=(A\times C)-(B\times C)$

d) Množiny A, B sú disjunktné práve vtedy, keď $A\times B\cap B\times A=\varnothing$

9) Zistite, pre aké množiny A, B, C platí resp. neplatí:

a) $A\cup(B\times C)=(A\cup B)\times(A\cup C)$

b) $A\cap(B\times C)=(A\cap B)\times(A\cap C)$

c) $A-(B\times C)=(A-B)\times(A-C)$

d) $(A\div B)\times C=(A\div C)\times(B\div C)$

2.5. Relácie

Pojem relácie má v matematike a v takých príbuzných vedách ako je informatika základný význam. Veľmi úzko súvisí s pojmom karteziánskeho súčinu množín. Najprv uvedieme definíciu a potom uvedieme príklady na rôzne typy relácií.

Definícia 2.5.1 Nech A, B sú ľubovoľné množiny. Množinu φ nazývame **binárnou reláciou** z množiny A do množiny B, alebo binárnou reláciou medzi prvkami množín A a B vtedy a len vtedy, keď $\varphi \subseteq A \times B$.

Príklad 1. Nech $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2\}$. Potom $\varphi_1 = \{(a_1, b_1), (a_1, b_2)\}$, $\varphi_2 = \{(a_1, b_1), (a_2, b_1)\}$, $\varphi_3 = \{(a_1, b_1), (a_2, b_2), (a_3, b_3)\}$, $\varphi_4 = \varnothing$, $\varphi_5 = A \times B$ sú relácie z množiny A do množiny B.

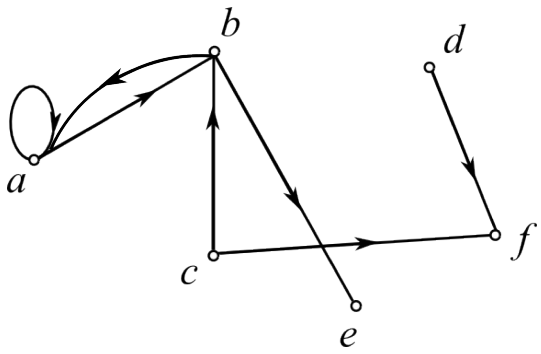
Poznámka: Z definície i uvedeného príkladu možno usudzovať, že ľubovoľná podmnožina (pravá, alebo nepravá) karteziánskeho súčinu množín je reláciou a že existujú rôzne druhy relácií. My sa budeme zaoberať rôznymi typmi relácií v súvislosti so špeciálnym typom relácií ako sú usporiadania, relácia ekvivalencie a zobrazenia.

Poznámka: Slovo binárna z definície znamená, že relácia je definovaná medzi dvomi množinami. Môžeme však zaviesť aj ***n* – árne relácie**, ktoré sú podmnožinami karteziánskeho súčinu n – množín $A_1, A_2, ..., A_n$. V tejto časti sa budeme zaoberať výlučne binárnymi reláciami a preto pojem relácia bude označovať binárnu reláciu.

Binárna relácia φ z n–prvkovej množiny A do m – prvkovej množiny B sa dá reprezentovať maticou M typu $n \times m$. Tie miesta v matici, ktoré zodpovedajú usporiadaným dvojiciam množiny φ označíme symbolom 1, na ostatné miesta v matici M napíšeme symbol 0. Miesto matice M ležiace na priesečníku i-teho riadku a j-teho stĺpca označíme symbolom (i, j) a jeho hodnotu symbolom m_{ij}. Maticu M budeme tiež označovať symbolom (m_{ij}), $i = 1,...,n$, $j = 1,...,m$. Maticu, ktorej prvky nadobúdajú hodnoty z množiny $\{0,1\}$ nazývame **booleovská**. *Maticovú reprezentáciu* relácie tiež nazývame tabuľkovou reprezentáciou.

Ďalšou veľmi názornou reprezentáciou je *grafová reprezentácia* binárnej relácie. Prvky množín označíme krúžkami, ktoré nazývame vrcholmi grafu a usporiadanú dvojicu znázorníme šípkou, ktorá ide z vrcholu odpovedajúceho prvému prvku dvojice k vrcholu, ktorý odpovedá druhému prvku dvojice. Táto šípka sa nazýva orientovanou hranou, v tom prípade, že oba vrcholy sú totožné ide o orientovanú slučku.

Príklad 1. Nech $A = \{a, b, c, d\}$ a $A = \{a, b, e, f\}$, $\varphi = \{(a, a), (a, b), (b, e), (c, b), (d, f), (b, a)\}$.



Obr. 7. Graf relácie φ z príkladu 1.

Poznámka: Teda reláciou medzi prvkami množín A, B (v tomto poradí) nazývame akúkoľvek podmnožinu karteziánskeho súčinu $\varphi \subseteq A \times B$. Ak $A = B$, tak hovoríme o relácii na množine A (alebo medzi prvkami množiny A). Relácia medzi prvkami množín A, B je akákoľvek množina $\varphi \subseteq A \times B$, špeciálne $\varphi = \emptyset$ a $\varphi = A \times B$.

Príklad 2. a) Vymenujte niekoľko relácií medzi prvkami množín $A = \{a,b,c\}$ a $B = \{d,e\}$, kde a,b,c,d,e sú navzájom rôzne prvky.

b) Určte počet všetkých relácií na konečnej množine, ktorá má práve n prvkov.

Riešenie: a) Všetkých relácií je 64. Niektoré z nich sú
$\{(a,d),(b,e)\},\{(a,e),(b,e)\},\{(a,d),(b,d),(c,e)\},\{(b,e)\},...$

b) Ak A je n – prvková množina, tak $A \times A$ má n^2 prvkov a systém $P(A \times A)$ všetkých jej podmnožín má 2^{n^2} prvkov. Teda počet relácií na množine A je 2^{n^2}.

Aby sme mohli neskôr podrobnejšie skúmať relácie na danej množine, ktoré majú veľký význam takmer vo všetkých oblastiach matematiky a informatiky, zavedieme potrebnú terminológiu.

Definícia 2.5.2 Nech φ je relácia na množine A.

a) Relácia φ je **reflexívna**, ak pre každé $x \in A$ platí $(x,x) \in \varphi$;
b) Relácia φ je **ireflexívna**, ak pre žiadne $x \in A$ neplatí $(x,x) \in \varphi$;
c) Relácia φ je **symetrická**, ak z podmienky $(x,y) \in \varphi$ vyplýva $(y,x) \in \varphi$;
d) Relácia φ je **asymetrická**, ak pre každé $(x,y) \in \varphi$ platí $(y,x) \notin \varphi$;
e) Relácia φ je **tranzitívna**, ak $((x,y) \in \varphi \wedge (y,z) \in \varphi) \Rightarrow (x,z) \in \varphi)$
f) Relácia φ je **atranzitívna**, ak $((x,y) \in \varphi \wedge (y,z) \in \varphi) \Rightarrow (x,z) \notin \varphi$
g) Relácia φ je **trichotomická**, ak pre každé $x,y \in A$ platí:
$$x \neq y \Rightarrow ((x,y) \in \varphi \vee (y,x) \in \varphi)$$
$$[\ (x = y) \vee (x,y) \in \varphi \vee (y,x) \in \varphi\ ]$$
h) Relácia φ je **antisymetrická**, ak pre každé $x,y \in A$ platí:
$$((x,y) \in \varphi \wedge (y,x) \in \varphi) \Rightarrow x = y$$

Poznámka: Všimnime si, že reflexívnosť (ireflexívnosť) relácie nedostaneme prostou negáciou reflexívnosti. Podobný je aj vzťah medzi vlastnosťami c) a d), resp. e) a f).

Zapíšme formálnejšie definíciu reflexívnosti a ireflexívnosti relácie φ na množine A. Relácia φ na množine A je reflexívna, ak pre $(\forall x)((x \in A) \Rightarrow (x,x) \in \varphi)$. Relácia φ na množine A je ireflexívna, ak pre $(\forall x)((x \in A) \Rightarrow (x,x) \notin \varphi)$. Ak urobíme negáciu prvého výroku, tak dostávame kvantifikovaný výrok: $(\exists x)((x \in A) \wedge (x,x) \notin \varphi)$. Presvedčte sa o správnosti tvrdenia poznámky aj v ostatných prípadoch

Zavedieme ešte pojem inverznej relácie a zloženej relácie.

Definícia 2.5.3 **a)** Nech φ je relácia medzi prvkami množín A, B a nech ψ je relácia medzi prvkami množín B, C. Potom
$$\{(a,c) \in A \times C : (\exists b)(b \in B \wedge (a,b) \in \varphi \wedge (b,c) \in \psi)\}$$
(je to relácia medzi prvkami množín A a C) sa nazýva **zložená relácia (zložená z relácií φ a ψ)** a označujeme ju $\psi \circ \varphi$.

b) Nech φ je relácia medzi prvkami množín A, B. Potom
$$\{(b,a) \in B \times A, (a,b) \in \varphi\}$$

(je to relácia medzi prvkami množín B a A) sa nazýva **inverzná relácia** k relácií φ a označujeme ju symbolom φ^{-1}.

Príklad 3. **a)** Nech $A=\{a_1,a_2,a_3,a_4\}$, $B=\{b_1,b_2,b_3\}$, $C=\{c_1,c_2\}$.
Nech $\varphi=\{(a_1,b_1),(a_2,b_2),(a_4,b_3)\}$, $\psi=\{(b_1,c_1),(b_2,c_2),(b_3,c_1)\}$. Potom
$\psi\circ\varphi=\{(a_1,c_1),(a_2,c_2),(a_4,c_1)\}$

b) Nech $\varphi\subseteq A\times B$ uvedená vyššie, potom $\varphi^{-1}=\{(b_1,a_1),(b_2,a_2),(b_3,a_4)\}$.

Bezprostredne so skladaním relácií na množine súvisí pojem **tranzitívny uzáver relácie** na množine, resp. **reflexívno-tranzitívny uzáver relácie** na množine. Tieto pojmy sa významne využívajú v takých informatických disciplínach, ako napr. formálne jazyky a automaty. Teraz budeme tieto pojmy formálne definovať.

Definícia 2.5.4 Nech φ je relácia na množine A. **Tranzitívnym**, resp. **reflexívno-tranzitívnym uzáverom relácie** φ nazývame relácie φ^+, resp. φ^* definované nasledujúcimi vzťahmi:

$$\varphi^+=\varphi^1\cup\varphi^2\cup\ldots=\bigcup_{k\geq 1}\varphi^k$$

$$\varphi^*=I_A\cup\varphi^1\cup\varphi^2\cup\ldots=\bigcup_{k\geq 0}\varphi^k$$

$I_A=\{(x,x)\mid x\in A\}$, $\varphi^0=I_A$, $\varphi^i=\varphi^{i-1}\circ\varphi$ pre $i>0$, t.j. $(x,y)\in\varphi^k$ pre nejaké $k>0$ $\Leftrightarrow$ ak existuje postupnosť prvkov $x=x_0,x_1,\ldots,x_{k-1},x_k=y$ taká, že platí $(x_0,x_1)\in\varphi$, $(x_1,x_2)\in\varphi$, ..., $(x_{k-1},x_k)\in\varphi$.

Príklad 4. **a)** Nech φ je relácia na množine A. Dokážte, že φ^+ je tranzitívna relácia na množine A a φ^* reflexívna aj tranzitívna relácia na množine A.

b) Nech φ^+ je tranzitívny uzáver relácie φ na množine A. Ak S je taká tranzitívna relácia na A, že $\varphi\subseteq S$, potom aj $\varphi^+\subseteq S$.

c) Nech φ^* je reflexívno – tranzitívna relácia na množine A. Ak S je taká reflexívno – tranzitívna relácia na množine A, že $\varphi\subseteq S$, potom aj $\varphi^*\subseteq S$.

Riešenie: **b)** Nech φ^+ je tranzitívny uzáver relácie φ na množine A. Podľa **a)** je to tranzitívna relácia na A. Nech S je tranzitívna relácia na A taká, že $\varphi\subseteq S$, ukážeme, že aj $\varphi^+\subseteq S$.
Nech $(x,y)\in\varphi^+$, potom existuje také $k>0$, že $(x,y)\in\varphi^k$ práve vtedy, ak existuje postupnosť $x=x_0,x_1,\ldots,x_{k-1},x_k=y$, že platí $(x_{i-1},x_i)\in\varphi$ pre $i=\overline{1,k}$. Keďže $\varphi\subseteq S$, tak $(x_{i-1},x_i)\in S$ a S je tranzitívna relácia na A, tak potom aj $(x,y)\in S$.

Časť **a)** a **c)** odporúčame čitateľovi ako domáce cvičenie.

Poznamenávame, že z vyššie uvedených tvrdení vyplýva, že tranzitívny uzáver, resp. reflexívno – tranzitívny uzáver relácie φ na množine A je najmenšia (v zmysle inklúzie) tranzitívna, resp. reflexívno – tranzitívna relácia na množine A, obsahujúca φ.

Ako sme už vyššie povedali s uvedenými reláciami sa často stretávame v teórií formálnych jazykov a automatov.

2.6. Relácia ekvivalencie a rozklad množiny

V predchádzajúcej časti sme zaviedli viaceré vlastnosti relácií na množine. Pomocou nich možno definovať isté typy relácií. V ďalších častiach budeme podrobne rozoberať najdôležitejšie typy.

Definícia 2.6.1 Relácia φ na množine A sa nazýva **relácia ekvivalencie** na A, ak je reflexívna, symetrická a tranzitívna.

Teda φ je relácia ekvivalencie na A, ak $\varphi \in A \times A$ a pre každé $x, y, z \in A$ platí:

1. $(x,x) \in \varphi$
2. $(x,y) \in \varphi \rightarrow (y,x) \in \varphi$
3. $((x,y) \in \varphi \wedge (y,z) \in \varphi) \rightarrow (x,z) \in \varphi$.

Ak φ je relácia ekvivalencie na množine A, tak namiesto $(x,y) \in \varphi$ niekedy píšeme aj $x \sim y$ alebo $x \equiv y$. Zapíšte predchádzajúce vlastnosti ekvivalencie pomocou uvedených symbobv.

Definícia 2.6.2 Nech A je neprázdna množina. Systém $S \subseteq P(A)$ sa nazýva **rozklad množiny** A, ak každá množina systému S je neprázdna. Pričom S je systém po dvoch disjunktných množín s vlastnosťou $\bigcup_{M \in S} M = A$.

Teda rozklad množiny A je taký systém neprázdnych podmnožín množiny A, že každý prvok $x \in A$ patrí práve do jednej množiny tohto systému.

Príklad 1. Nech Z označuje množinu všetkých celých čísel a nech m je prirodzené číslo, $m > 1$. Označme symbolom $\bar{r}$ $(0 \le r < m)$ zvyškovú triedu (mod m), t.j. množinu všetkých tých celých čísel a, ktoré majú tvar $a = k \cdot m + r$, $k \in Z$. Potom $S = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$ je rozklad množiny Z.

Nasledujúca veta ukazuje súvis medzi reláciou ekvivalencie a rozkladom príslušnej množiny. S touto vetou sa často stretávame v algebre a v informatických disciplínach.

Veta 2.6.1 Nech φ je relácia ekvivalencie na neprázdnej množine A. Pre $x \in A$ označme $A(x) = \{y \in A, (x,y) \in \varphi\}$. Potom systém množín $S = \{A(x) \in P(A), x \in A\}$ je rozklad množiny A (nazýva sa rozklad množiny A indukovaný ekvivalenciou φ, alebo patriaci k ekvivalencií φ).

Dôkaz: Každá množina $A(x) \in S$ je neprázdna, pretože $x \in A(x)$. Ďalej ak $(x,x') \in \varphi$, tak $A(x) = A(x')$. Skutočne, nech $y \in A(x)$. Potom $(y,x) \in \varphi$ a keďže $(x,x') \in \varphi$, tak aj $(y,x') \in \varphi$, relácia φ je tranzitívnou, teda $y \in A(x')$. To znamená, že $A(x) \subseteq A(x')$. Podobne sa dokáže, že $A(x') \subseteq A(x)$.

Nech teraz $(x,x') \notin \varphi$, tak $A(x) \cap A(x') = \varnothing$. Ak by totiž nejaké y patrilo do $A(x) \cap A(x')$, tak by platilo $(x,y) \in \varphi$ a $(y,x) \in \varphi$ a preto aj $(x,x') \in \varphi$, čo je v spore s predpokladom.

Teda množiny $A(x)$, $(x \in A)$ sú navzájom disjunktné a keďže $x \in A(x)$ pre každé $x \in A$, platí $\cup S = A$. Teda S je rozkladom množiny A.

Príklad 2. Nech Z má rovnaký význam ako v predchádzajúcom príklade, nech m je prirodzené číslo, $m > 1$. Hovoríme, že číslo $a \in Z$ kongruentné s číslom $b \in Z$ podľa modulu m (v označení $a \equiv m \pmod m$), ak m delí rozdiel $a - b$. Označme $\varphi = \{(a,b) \in Z \times Z, a \equiv b \pmod m\}$. Ľahko zistíme, že φ je relácia ekvivalencie na Z a ňou indukovaný rozklad je práve rozklad uvedený v predchádzajúcom príklade.

Nasledujúca veta je v istom zmysle obrátená k poslednej vete.

Veta 2.6.2 Nech A je neprázdna množina a S je jej rozklad. Definujme na množine A reláciu φ takto:

$$\varphi = \{(x,y) \in A \times A \mid \exists M \in S \wedge x \in M \wedge y \in M)\}$$

Potom φ je relácia ekvivalencie na množine A a φ je ňou indukovaný rozklad.

Dôkaz: Keďže množiny systému S sú navzájom disjunktné je definícia relácie φ korektná. Ľahko možno overiť, že φ je reflexívna, symetrická a tranzitívna relácia.

Označme S_0 rozklad množiny A indukovaný ekvivalenciou φ. Dokážeme, že $S = S_0$. Nech $A(x) \in S_0$, potom x patrí do nejakej množiny systému S, povedzme $x \in M$, $M \in S$. Nech $y \in M$. Potom zrejme $y \in A(x)$ a obrátene, ak $y \in A(x)$, tak y patrí do tej istej množiny ako x, t.j. $y \in M$. Teda $A(x) = M$, a tak $A(x) \in S$.

Nech obrátene $H \in S$, potom $H \neq \emptyset$ a tak existuje $x \in H$. Na základe definície φ potom platí $H = A(x)$, a tak $H \in S_0$.

Príklad 3. Nech $A = \{0,1,2\}$. Zostrojme všetky rozklady množiny A: $S_1 = \{\{0\},\{1\},\{2\}\}$, $S_2 = \{\{0,1\},\{2\}\}$, $S_3 = \{\{0,2\},\{1\}\}$, $S_4 = \{\{1,2\},\{0\}\}$, $S_5 = \{\{0,1,2\}\}$. Príslušné relácie ekvivalencie vyzerajú takto:

$\varphi_1 = I_A = \{(0,0),(1,1),(2,2)\}$
$\varphi_2 = I_A \cup \{(0,1),(1,0)\}$
$\varphi_2 = I_A \cup \{(0,2),(2,0)\}$
$\varphi_4 = I_A \cup \{(1,2),(2,1)\}$
$\varphi_5 = A \times A$.

Príklad 4. Ktorým ilustrujeme vyššie uvedené výsledky poznáte už zo strednej školy. Ide o príklad, ktorý objasňuje rozdiel medzi zlomkom a racionálnym číslom. Označme znakom W množinu všetkých zlomkov p/q, $p, q \in Z$, $q \neq 0$. Píšeme $\left(p/q, p'/q'\right) \in \varphi$, ak $pq' = p'q$. Ihneď vidno, že takto definovaná relácia na množine W je reflexívna a symetrická. Ukážeme, že je aj tranzitívna. Nech teda $\left(p/q, p'/q'\right) \in \varphi$ a súčasne aj $\left(p'/q', p''/q''\right) \in \varphi$. Potom $pq' = p'q$ a $p'q'' = p''q'$. Násobme prvú rovnosť $q'' \neq 0$. Dostávame $pq'q'' = p'qq''$. Ak dosadíme za $p'q''$ z druhej rovnosti, dostaneme $p'q'' = p''q$, teda $\left(p/q, p''/q''\right) \in \varphi$. Teda relácia φ je relácia ekvivalencie na množine W.

Na základe vyššie uvedeného tvrdenia sa množina W rozpadá na triedy navzájom ekvivalentných prvkov, každú z týchto tried nazývame racionálnym číslom. Za jej reprezentanta možno vziať jej ľubovoľný prvok a každé racionálne číslo možno vyjadriť hociktorým z nekonečne mnoho (navzájom ekvivalentných) zlomkov.

2.7. Čiastočné usporiadanie a usporiadanie množiny

V tejto časti vyložíme základné poznatky o ďalšom dôležitom type relácií a usporiadaní.

Definícia 2.7.1 Relácia na množine A sa nazýva **čiastočné usporiadanie množiny** A, ak je asymetrická a tranzitívna. Relácia na množine A sa nazýva **(lineárne) usporiadanie množiny** A, ak je asymetrická tranzitívna a trichotomická. Teda usporiadanie množiny A je každé čiastočné usporiadanie, ktoré je trichotomické na množine A.

Formálnejšie, relácia φ na množine A je čiastočné usporiadanie množiny A, ak pre každé $x, y, z \in A$ platí:

1. $(x,y) \in \varphi \rightarrow (y,x) \notin \varphi$
2. $(x,y) \in \varphi \wedge (y,z) \in \varphi \rightarrow (x,z) \in \varphi$.

Ak navyše pre každé $x, y \in A$ platí:

3. $(x = y) \vee (x, y) \in \varphi \vee (y, x) \in \varphi$, čo je ekvivalentné

3´. $x \neq y \rightarrow ((x, y) \in \varphi \vee (y, x) \in \varphi)$,

tak φ je **usporiadanie množiny *A***.

Ak A je množina a φ je jej usporiadanie (resp. čiastočné usporiadanie), tak hovoríme, že **množina *A* je usporiadaná** (resp. čiastočne usporiadaná) **reláciou** φ a zapisujeme to v tvare (A, φ), alebo $(A, <)$, ak namiesto $(x, y) \in \varphi$ píšeme $x < y$. Uvedený zápis je motivovaný tým, že pre tú istú množinu možno vo všeobecnosti definovať viacero čiastočných usporiadaní. Presnejšie, usporiadaná množina A je vlastne usporiadaná dvojica (A, φ), kde relácia φ je usporiadanie množiny A.

Ak namiesto $(x, y) \in \varphi$ píšeme $x < y$, tak je prirodzené stotožniť znak φ so znakom <, teda napr. $(<) \subseteq A \times A$, ak $<$ je usporiadanie množiny A a pod.

Poznámka: V matematickej literatúre niektorí autori namiesto termínu čiastočne usporiadanie používajú termín usporiadanie a v tomto prípade sa namiesto termínu usporiadanie hovorí lineárne (alebo totálne) usporiadanie. My sa budeme držať v našom texte definície, ktorú sme zaviedli vyššie.

Príklad 1. a) Nech N je množina prirodzených čísel, definujme na N reláciu φ takto: $(x, y) \in \varphi \Leftrightarrow y - x > 0$. Ľahko nahliadneme, že uvedená relácia je asymetrická a tranzitívna, ak $x \neq y$ pre $x, y \in N$, tak buď $x - y > 0$ alebo $y - x > 0$, teda φ je usporiadanie množiny N.

b) Na množine N všetkých prirodzených čísel definujme reláciu φ takto; ak $a, b \in N$, tak $(a, b) \in \varphi$ práve vtedy, keď $a \mid b$ (t.j. a delí b) a $a \neq b$. Zrejme φ je čiastočné usporiadanie množiny N. Nie je to ale usporiadanie množiny N, pretože napríklad $(3,5) \notin \varphi$ a súčasne $(5,3) \notin \varphi$.

c) Nech $\mathcal{S}$ je systém množín. Definujeme na $\mathcal{S}$ reláciu φ takto. Pre $A, B \in \mathcal{S}$ je $(A, B) \in \varphi$ práve vtedy, keď $A \subseteq B$ a súčasne $A \neq B$, t.j. práve vtedy, ak $A \subset B$. Ľahko sa môžeme presvedčiť, že φ je čiastočné usporiadanie množiny $\mathcal{S}$ (hovoríme tiež, že v tomto prípade množina $\mathcal{S}$ je čiastočne usporiadaná inklúziou). Namiesto $(\mathcal{S}, \varphi)$ sa zvykne písať aj $(\mathcal{S}, \subset)$, aj keď presne vzaté $\subset$ nie je relácia. K omylu však nemôže dôjsť. Ľahko zistíme, že čiastočné usporiadanie generované inklúziou $\subset$ nemusí byť lineárnym usporiadaním každého systému množín, stačí ak vezmeme systém $\mathcal{P}(A)$, kde A je aspoň dvojprvková množina. V prípade, že $A = \{a, b\}$, tak množiny $\{a\}, \{b\}$ nie sú v inklúzii.

Poznámka: Všimnime si, že v čiastočne usporiadanej množine $(A, <)$ pre žiaden prvok x neplatí $x < x$, je to dôsledok asymetričnosti čiastočného usporiadania. Takisto, ak by platil výrok $x < x$, tak potom výrok $\neg x < x$ je nepravdivý a implikácia $x < x \rightarrow \neg x < x$ by bola v tomto prípade nepravdivá, čo je v spore s tým, že čiastočné usporiadanie je asymetrická relácia na množine.

Ak $(A, <)$ je (čiastočne) usporiadaná množina a $x, y \in A$, tak definujeme nerovnosť $x \leq y$ vzťahom

$$x \leq y \leftrightarrow (x < y) \vee (x = y)$$

Všimnime si, že z podmienky $x < y$ vyplýva $x \leq y$, ale obrátene nie, teda $x \leq y$ neimplikuje vo všeobecnosti $x < y$.

Poznámka: V niektorých knihách sa pod čiastočným usporiadaním množiny A rozumie taká relácia φ, ktorá je reflexívna, tranzitívna a antisymetrická, t.j.

$$(x, y) \in \varphi \wedge (y, x) \in \varphi \rightarrow x = y$$

V tom prípade je φ usporiadanie, ak navyše φ je trichotomická relácia. Ľahko sa môžeme presvedčiť, že takto chápané čiastočné usporiadanie a usporiadanie zodpovedá „neostrej“ nerovnosti $\leq$. V našom texte povieme vždy o aký druh čiastočného usporiadanie a usporiadania ide, t.j. či ide o „ostrú“ nerovnosť $<$, alebo „neostrú“ $\leq$ nerovnosť.

Nakoniec ešte zavedieme dva dôležité pojmy. Prvok a čiastočne usporiadanej množiny $(A,<)$ sa nazýva **minimálny** (resp. **maximálny**) **prvok**, ak pre žiadne $x \in A$ neplatí $x < a$ (resp. $a < x$). Prvok b čiastočne usporiadanej množiny $(A,<)$ sa nazýva **prvý** alebo **najmenší prvok** množiny A, ak pre každý prvok $x \in A$, $x \neq b$ platí $b < x$. Podobne b je **najväčší** alebo **posledný prvok** množiny A, ak pre každé $x \in A$, $x \neq b$ platí $x < b$.

Všimnime si, že najmenší (najväčší) prvok čiastočne usporiadanej množiny je súčasne jej minimálnym (resp. maximálnym) prvkom. Obrátené tvrdenie neplatí, ako vidieť z tohto príkladu.

Príklad 2. Nech A je množina všetkých prirodzených čísel väčších ako 1. Potom A je podmnožinou množiny N čiastočne usporiadanou reláciou $\varphi = \{(a,b) \in A \times A,\ a \text{ delí } b,\ \text{súčasne } a \neq b\}$. Je zrejmé, že každé prvočíslo je minimálnym prvkom množiny A a pritom A nemá najmenší prvok. Naproti tomu množina $N^+ = \{1,2,3,...,n,...\}$ čiastočne usporiadaná reláciou φ má najmenší prvok, je ním číslo 1, ktoré je súčasne aj minimálnym prvkom (jediným) množiny N^+. Ďalej si všimnime, že množina A nemá maximálny a teda ani najväčší prvok.

Poznámka: Celkom na záver tejto časti poznamenávame, že pojem prvý prvok je dôležitý pri zavádzaní takých pojmov ako je dobre usporiadaná množina a s tým súvisiaci ordinálny typ.

2.5. – 2.7. CVIČENIA

1) Zistite, či relácia $\varphi \subseteq R \times R$, $\varphi = \{(x,y), x \leq y\}$ je reflexívna, symetrická, antisymetrická, tranzitívna

2) Dokážte, že relácia $\varphi \subseteq Z \times Z$, $(x,y) \in \varphi$ práve vtedy, keď 3 delí $x - y$ je reflexívna, symetrická, tranzitívna.

3) Ukážte, že ak relácia $\varphi \subseteq A \times A$ je symetrická a antisymetrická, tak $\varphi \subseteq \{(a,a); a \in A\}$.

4) Ak φ a ψ sú relácie ekvivalencie na množine A, tak $\varphi \cap \psi$ je relácia ekvivalencie na A, $\varphi \cup \psi$ nemusí byť relácia ekvivalencie na A.

5) Nakreslite orientovaný graf relácie φ na množine A, keď

a) $A = \{1,2,...,10\}$, $\varphi = \{(1,2),(3,5),(2,2),(5,3),(8,9)\}$

b) $A = \{a,b,c\}$, $\varphi = \{(a,a),(a,b),(b,c),(c,a),(a,c)\}$.

6) Zistite, či relácia φ na množine R je reflexívna, symetrická, tranzitívna, ak:

a) $(x,y) \in \varphi$ práve vtedy, keď $2x = 3y$

b) $(x,y) \in \varphi$ práve vtedy, keď $x \geq y$, $x \neq y$

c) $(x,y) \in \varphi$ práve vtedy, keď $|x| \leq |y|$

d) $(x,y) \in \varphi$ práve vtedy, keď $x \leq y$ alebo $x = 3y$.

7) Zistite, či relácia φ je na množine N^+ ekvivalencia, ostré alebo neostré čiastočné usporiadanie alebo lineárne usporiadanie.

a) $(x,y) \in \varphi$ práve vtedy, keď $y - x = 0$

b) $(x,y) \in \varphi$ práve vtedy, keď $x - y = 2$

c) $(x,y) \in \varphi$ práve vtedy, keď x, y sú nesúdeliteľné.

d) $(x,y) \in \varphi$ práve vtedy, keď $x = y^2$

8) Koľko relácií ekvivalencie je možné definovať na množine A, ak $A = \{1,2,3,4\}$.

9) Zistite, či relácia φ na množine A je reláciou ekvivalencie, pričom
a) $A = \{1,2,3,4,5,6,7,8,9,10\}$ a platí $(x, y) \in \varphi$ práve vtedy, keď 2 delí $x + y$
b) $A = N^+$ a $(x, y) \in \varphi$ práve vtedy, keď x delí y alebo y delí x.
c) $A = R$ a $(x, y) \in \varphi$ práve vtedy, keď x delí y alebo y delí x

10) Nech φ je relácia ekvivalencie na množine A. Je φ^{-1} tiež relácia ekvivalencie na množine A?

11) Nech $A \neq \emptyset$. Je niektorá z relácií $\emptyset$, $A \times A$ relácia ekvivalencie na A?

12) Nech Z, Q, R je množina všetkých celých, racionálnych, resp. všetkých reálnych čísel. Označme
$\varphi = \{(x, y) \in R \times R;\ x - y \in Z\}$
$\psi = \{(x, y) \in R \times R;\ x - y \in Q\}$
Dokážte, že φ a ψ sú relácie ekvivalencie na R. Opíšte rozklady množín R indukované týmito reláciami.

13) Nech A je množina. Je $\emptyset$, resp. $A \times A$ čiastočné usporiadanie množiny A? Je to usporiadanie množiny A?

14) Nech φ je neprázdny systém čiastočných usporiadaní množiny. Dokážte, že aj $\cap\varphi$ je čiastočné usporiadanie množiny. Platí podobné tvrdenie aj pre neprázdny systém usporiadaní množiny A?

15) Dokážte, že ak φ je usporiadanie množiny A, tak aj φ^{-1} je usporiadanie množiny A. (Usporiadanie φ^{-1} sa nazýva opačné usporiadanie k usporiadaniu φ).

16) Nech φ je čiastočné usporiadanie neprázdnej množiny A. Dokážte, že φ nie je relácia ekvivalencie na A. Ako je to v prípade $A \neq \emptyset$?

17) Nájdite príklad relácie na neprázdnej množine A, ktorá nie je ani čiastočným usporiadaním, ani reláciou ekvivalencie.

18) a) Dokážte, že v usporiadanej množine sa pojem minimálneho prvku zhoduje s pojmom najmenšieho (prvého) prvku a pojem maximálneho prvku s pojmom najväčšieho (posledného prvku).

b) Dokážte, že usporiadaná množina má najviac jeden maximálny a najviac jeden minimálny prvok.

c) Nech A je čiastočne usporiadaná množina, ktorá má práve jeden minimálny prvok a. Je pravda, že potom a je najmenším prvkom množiny A?

2.8. Zobrazenie

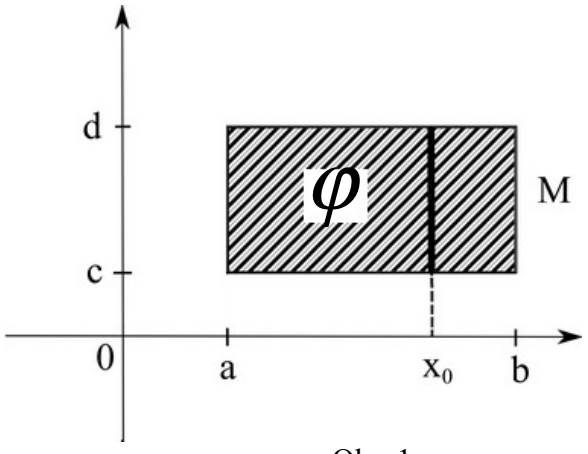
Veľmi dôležitým prípadom relácií sú zobrazenia alebo funkcie, ktoré predstavujú jeden z najdôležitejších pojmov súčasnej matematiky. S pojmom zobrazenia sme sa už oboznámili na strednej škole. Pod zobrazením $f : X \to Y$ sme chápali akýsi predpis, ktorý každému prvku $x \in X$ priradí nejaký prvok $y \in Y$. Aby naša predstava o zobrazení bola korektná je potrebné upresniť, čo je to predpis. Ďalej na strednej škole nám povedali, čo je to graf funkcie, zobrazenia. V podstate, je to definovanie funkcie, zobrazenia ako špeciálnej relácie. S takýmto poňatím vystačíme, ak sa zaoberáme funkciami, zobrazeniami definovanými na množinách. Keďže v našich úvahách sa zaoberáme v prevažnej miere funkciami definovanými na množinách, budeme definovať zobrazenie ako špeciálny typ relácie. Skôr než to urobíme poznamenávame, že ak niekedy v matematike používame zobrazenia definované na všetkých množinách (t.j. zobrazenia, ktoré každej množine priradia nejakú hodnotu), vieme, že všetky množiny netvoria množinu. Napríklad v nasledujúcich častiach nášho textu v prípade, keď každej množine priradzujeme jej mohutnosť. V takýchto prípadoch treba interpretovať zobrazenie ako predpis. Treba ale presne povedať, čo je to dovolený predpis. Poznamenávame, že termíny zobrazenie a funkcia sú synonymami.

Definícia 2.8.1 Zobrazením f z množiny X do množiny Y nazývame reláciu $f \subseteq X \times Y$ ak ku každému $x \in X$ existuje práve jedno také $y \in Y$, že dvojica $(x, y) \in f$.

Podrobnejšie: relácia f z množiny X do množiny Y (alebo medzi prvkami množín X a Y v uvedenom poradí) sa nazýva **zobrazenie** (**funkcia**) množiny X do Y, ak platí:

1. $\underset{x\in X}{\forall}\ \underset{y\in Y}{\exists} (x, y) \in f$
2. $\underset{x\in X}{\forall}\ \underset{y\in Y}{\forall}\ \underset{y'\in Y}{\forall} \left((x, y) \in f \wedge (x, y') \in f\right) \to y = y'$.

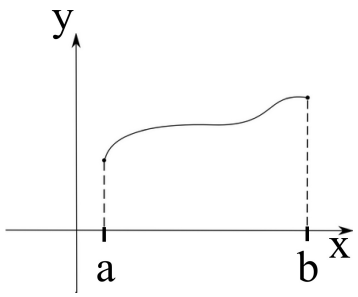
Názornú predstavu o zobrazeniach (funkciách) získame v prípade, keď $X = Y = R$, vtedy hovoríme, že ide o funkcie reálnej premennej s reálnymi hodnotami. Ak použijeme obvyklú pravouhlú súradnicovú sústavu, potom každá relácia $\varphi \subseteq R \times R$ sa javí ako istá podmnožina roviny. Na obr.1 je graficky znázornená relácia φ, jej graf tvoria body obdĺžnika M.



Obr. 1

Táto relácia nie je zobrazenie, pretože napr. k bodu x_0 existuje nekonečne veľa y, že $(x_0, y) \in \varphi$ (tieto body y vypĺňajú celý interval na osi y a to interval $\langle c, d \rangle$.

Naproti tomu relácia znázornená na obr. 2 je zobrazenie.



Obr. 2

Pripomíname niektoré označenia. Ak f je zobrazenie množiny X do množiny Y, tak tento fakt zapisujeme $f : X \to Y$. Namiesto $(x, y) \in f$ píšeme $f(x) = y$. Prvok $y \in Y$ sa nazýva hodnota zobrazenia f v prvku x.

Ďalej, ak $A \subseteq X$, tak znakom $f(A)$ označujeme množinu všetkých tých $y \in Y$, ku ktorým existuje $x \in A$, že $y = f(x)$. Teda:

$$f(A) = \left\{ y \in Y; \underset{x}{\exists} x \in A \wedge y = f(x) \right\}$$

Množina $f(A)$ sa nazýva obraz množiny A v zobrazení f. Množina X sa nazýva obor definície zobrazenia $f : X \to Y$, Y sa nazýva obor hodnôt zobrazenia f. Pripúšťame aj možnosť $Y \neq f(X)$ (t.j. platí $f(X) \subseteq Y$). Ak $f(X) = Y$, tak f sa nazýva **surjektívne zobrazenie**, alebo skrátene surjekcia (niekedy sa surjekcií hovorí aj **zobrazenie** množiny X **na** množinu Y). Pripomíname ešte, že zobrazenie $f : X \to Y$ je **prosté** alebo **injektívne** (niekedy hovoríme tiež, že f je injekcia), ak f nadobúda v rôznych prvkoch množiny X rôzne hodnoty. Presnejšie, ak $x, y \in X$ a $x \neq y$, tak $f(x) \neq f(y)$. Zobrazenie $f : X \to Y$ nazývame **bijektívne**, ak je injektívne a súčasne surjektívne.

Niekedy je účelné zmenšiť obor definície danej funkcie, s týmto typom funkcií sa stretávame často v teoretickej informatike, napríklad v teórií algoritmov.

Definícia 2.8.2 Ak $f : X \to Y$ je funkcia a $A \subseteq X$, tak znakom $f \mid A$ označujeme funkciu $g : A \to Y$ definovanú takto; pre $x \in A$ platí $f(x) = g(x)$, t.j. $f \mid A = f \cap (A \times Y)$. Funkcia $g = f \mid A$ sa nazýva parciálna funkcia k funkcií f, alebo zúženie funkcie f (na množine A).

Poznámka: V teórií rekurzívnych funkcií sa parciálne funkcie nazývajú čiastočné.

Príklad 1. Nech R je množina všetkých reálnych čísel a R_0^+ množina všetkých nezáporných reálnych čísel. Nech

$$f_1 : R \to R,\ f_2 : R \to R_0^+,\ f_3 : R_0^+ \to R,\ f_4 : R_0^+ \to R_0^+$$

sú zobrazenia definované rovnakým predpisom $f_i(x) = x^2$ pre $i = 1, 2, 3, 4$. Všimnime si predovšetkým to, že všetky štyri zobrazenia sú zobrazenia v zmysle našej definície, napríklad

$$f_1 = \left\{ (x, y) \in R \times R; y = x^2 \right\}$$

pričom množina vpravo existuje na základe axiómy teórie množín (pričom využívame tú skutočnosť, že R je množina a že $y = x^2$ je prípustná funkcia – to ale je možné v rámci teórie množín dokázať).

Ďalej $f_3 = f_1 \mid R_0^+$ a $f_4 = f_2 \mid R_0^+$ sú zúženia funkcií. Zobrazenie f_1 nie je ani surjektívne, ani injektívne, f_2 je surjektívne, ale nie je injektívne, f_3 je injektívne, ale nie je surjektívne a napokon f_4 je bijektívne. Sú to teda štyri rôzne funkcie (ak berieme do úvahy ich obory definície a obory hodnôt).

Pravda, z hľadiska teórie množín je $f_1 = f_2$ tá istá relácia a podobne aj $f_3 = f_4$.

Tento zdanlivý rozpor možno jednoducho vysvetliť. Zobrazenie $f : X \to Y$ je vlastne usporiadaná trojica (f, X, Y). Množina X je ale jednoznačne určená reláciou f - je to množina všetkých prvých súradníc prvkov (t.j. dvojíc) množiny f. Preto každé zobrazenie $f : X \to Y$ môžme jednoznačne reprezentovať usporiadanou dvojicou (f, Y) a rovnosť dvoch zobrazení potom chápeme ako rovnosť dvoch usporiadaných dvojíc. Len v tomto prípade má zmysel hovoriť o tom, či zobrazenie je surjekcia alebo bijekcia (to, či je zobrazenie injektívne, nezávisí od oboru hodnôt *Y*).

Poznamenávame, že v matematickej literatúre sa môžeme stretnúť s obidvoma chápaniami rovnosti zobrazení. V algebre a príbuzných odboroch sa obyčajne zobrazenie chápe ako usporiadaná dvojica, v matematickej analýze sa naproti tomu pokladajú za rovnaké aj funkcie, ktoré nemajú rovnaký obor hodnôt. Má to svoje opodstatnenie.

V našom texte budeme väčšinou chápať rovnosť zobrazení ako rovnosť relácií, t.j. nebudeme brať do úvahy obor hodnôt. V tých prípadoch, keď použijeme „algebraickú“ interpretáciu rovnosti dvoch funkcií, to bude z kontextu zrejmé.

Pre úplnosť ešte uvedieme niektoré vlastnosti funkcií známe zo stredoškolského učiva.

Veta 2.8.1 Ak f je injektívne zobrazenie množiny *X* do *Y*, tak f^{-1} je bijektívne zobrazenie množiny $f(X)$ do *X*.

Dôkaz: Nech $Z = f(X)$. Nech $z \in Z$. Potom existuje také $x \in X$, že platí $f(x) = z$. (Využili sme definíciu množiny Z), teda $(x, z) \in f$, a preto $(z, x) \in f^{-1}$. Teda relácia f^{-1} má prvú vlastnosť definície zobrazenia. Ak by platilo, že $(z, x_1) \in f^{-1}$ a súčasne aj $(z, x_2) \in f^{-1}$, tak $(x_1, z) \in f$ a $(x_2, z) \in f$, keďže f je prosté zobrazenie, dostávame $x_1 = x_2$. Teda f^{-1} má aj druhú vlastnosť zobrazenia. To že f^{-1} je surjektívne zobrazenie vyplýva z toho, že zobrazenie f je definované na množine *X*. Nakoniec dokážeme, že f^{-1} je aj injektívne zobrazenie. Ak totiž $(y_1, x) \in f^{-1}$ a súčasne aj $(y_2, x) \in f^{-1}$ a $y_1 \neq y_2$, potom keďže f je zobrazenie $(x, y_1) \in f$ a $(x, y_2) \in f$ dostávame, že $y_1 = y_2$, čo je spor z predpokladom.

Ako dôsledok predchádzajúcej vety uvádzame tvrdenie.

Veta 2.8.2 Ak je f bijekcia množiny *X* na *Y*, tak f^{-1} je bijekcia množiny Y do *X*.

Poznamenávame, že $f^{-1} = \{(y, x) \in Y \times X, (x, y) \in f\}$.

Veta 2.8.3 Nech $f : X \to Y$ a $g : Y \to Z$. Potom zložená relácia $g \circ f$ je zobrazenie množiny *X* do *Z*. Poznamenávame, že $g \circ f = \{(x, z) \in (X, Z) \mid \exists y, y \in Y, (x, y) \in f \wedge (y, z) \in g\}$.

Dôkaz: Ukážeme, že $g \circ f$ spĺňa obidve podmienky zobrazenia. Nech *x* je ľubovoľný prvok množiny *X*, keďže f je zobrazenie množiny *X* do množiny *Y*, tak existuje práve jedno $y \in Y$, že $(x, y) \in f$, súčasne *g* je zobrazenie množiny *Y* do *Z*, tak existuje práve jedno $z \in Z$, že $(y, z) \in g$, a teda $(x, z) \in g \circ f$.

Zhrnutím dostávame: pre ľubovoľné *x* patriace *X* existuje práve jedno $z \in Z$, že platí $(x, z) \in g \circ f$.

Poznámka: Všimnime si, že pri označení použitom vo vyššie uvedenej vete pre každé $x \in X$ platí $(g \circ f)(x) = g(f(x))$.

Zobrazenie $g \circ f$ sa nazýva **zložené zobrazenie** alebo **kompozícia zobrazení** f a *g*. V mnohých matematických knihách sa to isté zobrazenie zapisuje aj v tvare $f \circ g$, t.j. v obrátenom poradí. My

budeme zásadne používať označenie $g \circ f$, t.j. zložené zobrazenie aplikujeme tak, že najskôr aplikujeme pravé zobrazenie f a potom ľavé zobrazenie *g*. V analýze nazývajú f vnútorná zložka a *g* vonkajšia zložka zloženého zobrazenia $g \circ f$.

Na záver tejto časti ešte uvedieme tvrdenie, ktoré charakterizuje skladanie zobrazení.

Veta 2.8.4 Nech $f : X \to Y$ a $g : Y \to Z$

a) Ak f, g sú injektívne zobrazenia, tak aj $g \circ f$ je injektívne zobrazenie

b) Ak f, g sú surjektívne zobrazenia, tak aj $g \circ f$ je surjektívne zobrazenie

c) Ak f, g sú bijektívne zobrazenia, tak aj $g \circ f$ je bijektívne zobrazenie

Dôkaz: Uvedieme stručný dôkaz týchto tvrdení. Všimnime si, že posledné tvrdenie vyplýva z predchádzajúcich dvoch tvrdení. Nech x_1, x_2 sú dva rôzne prvky množiny *X*, keďže f je injektívne zobrazenie množiny *X* do množiny *Y*, tak aj $y_1, y_2 \in Y$ sú rôzne, pričom platí $y_1 = f(x_1)$ a $y_2 = f(x_2)$. Keďže zobrazenie *g* je injektívne zobrazenie množiny *Y* do množiny *Z*, tak dva rôzne prvky $y_1, y_2 \in Y$ sa zobrazením *g* zobrazia na dva rôzne prvky $z_1, z_2 \in Z$. Zhrnutím dostávame, že ľubovoľné dva rôzne prvky $x_1, x_2 \in X$ sa zobrazením $g \circ f$ zobrazia na dva rôzne prvky $z_1, z_2 \in Z$. Teda $g \circ f$ je injektívne zobrazenie množiny *X* do *Z*. Obdobne postupujeme aj v prípade dôkazu surjetívnosti zobrazenia $g \circ f$. Keďže f je surjektívne zobrazenie množiny *X* na *Y*, tak ku každému prvku $y \in Y$, existuje aspoň jedno také $x \in X$, že $y = f(x)$, ďalej *g* je surjektívne zobrazenie množiny *Y* na *Z*, t.j. ku každému prvku $z \in Z$ existuje aspoň jedno také $y \in Y$, že platí $z = g(y)$, z uvedeného vyplýva, že pre každé $z \in Z$ existuje aspoň jedno $x \in X$, že platí $z = g(f(x))$. Teda $g \circ f$ je surjektívne zobrazenie množiny *X* na *Z*.

2.8. CVIČENIA

1) Rozhodnite, ktoré z uvedených relácií sú zobrazenia

a) $\{(x, y) \in R^2 \mid x^2 = y^2\}$

b) $\{(x, y) \in R^2 \mid x^2 = y^2 \wedge y \geq 0\}$

c) $\{(x, y) \in Z \times N \mid x = y \vee x = -y\}$

d) $\{(x, y) \in Z \times Z \mid x \text{ delí } y\}$

2) Nájdite obor definície a obor hodnôt týchto zobrazení (určte, ktoré sú injektívne):

a) $\{(x, y) \in R^2 \mid \ln x = y^2 \wedge y \geq 0\}$

b) $\{(n, m) \in N^2 \mid n = 2m + 1\}$

c) $\left\{(x, y) \in R^2 \mid y = \frac{x^2 - 1}{x - 1}\right\}$

d) $\{(x, y) \in R^2 \mid y = x + 1\}$

3) Zostrojte prosté zobrazenie množiny *A* na množinu *B*, keď

a) *A* je množina všetkých priamok v rovine, $B = R \times R$

b) *A* je množina všetkých kruhov v rovine $B = R \times R \times (0, \infty)$

c) $A = \{(x, y) \in R^2;\ x^2 + y^2 \leq 1\}$, $B = \langle -1,1 \rangle \times \langle -1,1 \rangle$.

4) Rozhodnite, či platí $f = g$. Svoje tvrdenie zdôvodnite.

a) $f(x) = \frac{x^2 - 1}{x - 1}$, $g(x) = x + 1$

b) $f(x)=\frac{1}{|x|}$, $g(x)=\frac{1}{|x|}$, pre $x\neq 0$, $g(x)=1$, pre $x=0$

c) $f(x)=-\ln x$, $g(x)=\ln\frac{1}{x}$

d) $f(x,y)=\frac{x^4-1}{x^2+1}$, $g(x)=x^2-1$

5) Zostrojte množiny X, Y a zobrazenie $f: X\to Y$, tak, aby relácia f^{-1} nebola zobrazenie.

6) Môže byť čiastočné usporiadanie množiny A zobrazením A do A ?

7) Nech $f: X\to Y$ a nech $\varphi=\{(x,y)\in X\times Y \mid f(x)=f(y)\}$. Dokážte, že φ je relácia ekvivalencie na X a opíšte rozklad množiny X indukovaný touto ekvivalenciou.

8) Nech $A\neq\emptyset$. Dokážte, že zobrazenie $f: A\to A$ je reláciou ekvivalencie na množine A práve vtedy, keď pre každé $x\in A$ platí $f(x)=x$, t.j. keď f je identické zobrazenie.

9) Ak f je prosté zobrazenie, tak pre $A, A'\subseteq X$ platí $f(A)-f(A')=f(A-A')$.

10) Nech A je množina. Dokážte, že $\emptyset$ je jediné zobrazenie množiny $\emptyset$ do A. Je to injektívne zobrazenie ?

11) Dokážte, že ak $A\neq\emptyset$, tak neexistuje zobrazenie $f: A\to\emptyset$.

12) Nech zobrazenie $f: X\to Y$ nie je injektívne. Dokážte, že potom $X\neq\emptyset\neq Y$

13) Nech $f: X\to Y$ a $g: Y\to X$ a nech $g\circ f$ je identické zobrazenie. Dokážte, že f je injekcia a g surjekcia. Dokážte, že f nemusí byť surjekcia a g injekcia.

14) Nech $f: X\to Y$ a $g: Y\to X$. Nech $g\circ f$ a $f\circ g$ sú identické zobrazenia. Dokážte, že f a g sú bijekcie a $g=f^{-1}$.

15) Nech $h: X\to X$. Dokáže, že výrok $h\circ f=h\circ g\Rightarrow f=g$ platí pre každé dve zobrazenia $f, g: X\to X$ práve vtedy, keď h je injektívne zobrazenie.

16) Nech $h: X\to X$. Dokážte, že výrok $f\circ h=g\circ h\to f=g$ platí pre každé dve funkcie $f, g: X\to X$ práve vtedy, keď h je surjekcia.

17) Nech $f: X\to X$. Potom

a) f je surjekcia práve vtedy, keď existuje také $g: X\to X$, $f\circ g$ je identické zobrazenie I_x

b) f je injekcia práve vtedy, keď existuje také $g: X\to X$, že $g\circ f=I_x$

2.9. Mohutnosti množín

Mohutnosť množiny alebo kardinálne číslo množiny je zovšeobecnenie pojmu počet prvkov množiny. Ak si všimneme rozličné množiny, vidíme, že niekedy možno (aspoň teoreticky) určiť počet prvkov v množine. K takým množinám patrí množina všetkých študentov príslušnej fakulty, množina účastníkov – divákov futbalového zápasu, divadelného predstavenia, koncertu, atď.

Každá z týchto množín obsahuje konečný, aj keď možno pre nás neznámy počet prvkov. Naproti tomu existujú nekonečné množiny, ako napríklad množina všetkých prirodzených čísel, reálnych čísel, priamok v rovine a podobne. Ak hovoríme, že množina obsahuje nekonečný počet prvkov alebo, že je nekonečná, myslíme tým, že ak vyberáme postupne po jednom rozličné prvky danej množiny, po každom výbere v tejto množine ešte zostanú prvky.

V súlade s vyššie povedaným uvedieme najskôr, kedy dve množiny majú rovnakú mohutnosť.

Definícia 2.9.1 Nech A, B sú dve množiny. Budeme hovoriť, že množiny ***A, B* majú rovnakú mohutnosť** alebo rovnaký počet prvkov, píšeme $|A| = |B|$, ak existuje prosté zobrazenie množiny A na množinu B, teda bijekcia.

Príklad 1. Množiny $\{0,1,2\}$ a $\{3,4,5\}$ majú rovnakú mohutnosť lebo existuje prosté zobrazenie f množiny $\{0,1,2\}$ ma množinu $\{3,4,5\}$ napríklad $f(0) = 3, f(1) = 4, f(2) = 5$. Podobne množiny $(0,1)$ a $(0,2)$ majú rovnakú mohutnosť lebo zobrazenie $f(x) = 2x$ proste zobrazuje množinu $(0,1)$ na $(0,2)$. Taktiež množiny N a N^+ majú rovnakú mohutnosť, lebo zobrazenie $f(n) = n+1$ je bijekcia medzi N a N^+.

Vzťah „mať rovnakú mohutnosť“ je reflexívny, symetrický a tranzitívny. Vyjadruje ho nasledujúca veta.

Veta 2.9.1:

a) Pre každú množinu A platí $|A| = |A|$,

b) Ak $|A| = |B|$, potom $|B| = |A|$,

c) Ak $|A| = |B|$, $|B| = |C|$, tak $|A| = |C|$.

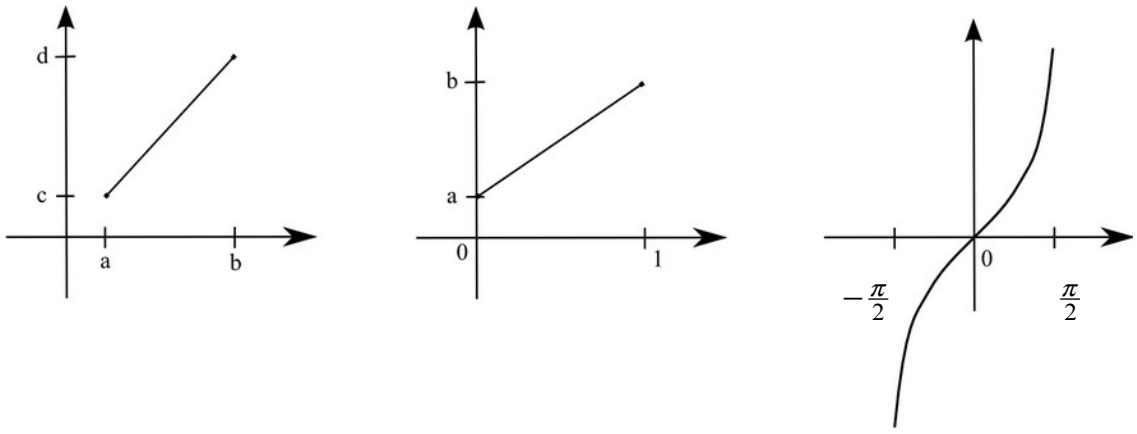
Dôkaz: a) Zobrazenie $I_x(x) = x,\ x \in A$ je prosté a na množine A.

b) Ak $|A| = |B|$, tak podľa definície existuje prosté zobrazenie $f : A \to B$. Ľahko možno nahliadnuť, že inverzné zobrazenie $f^{-1} : B \to A$ existuje, ktoré je prosté a na množine A.

c) Ak $|A| = |B|$, $|B| = |C|$, tak existujú zobrazenia $f : A \to B$ a $g : B \to C$, ktoré sú bijekcie. Potom aj $g \circ f$ je bijekcia medzi množinami A a C.

Príklad 2. a) Ak $a < b$, tak existuje bijektívne zobrazenie $f : (0,1) \to (a,b)$. Stačí položiť $f(x) = a + (b-a)x$ pre $x \in (0,1)$, (pozri obr. 1). Podľa vyššie uvedenej vety potom aj pre ľubovoľné dva otvorené intervaly (a,b), (c,d), $a < b$, $c < d$, platí $|(a,b)| = |(c,d)|$. Nech $f : (a,b) \to (0,1)$ je bijektívne zobrazenie, potom aj $g : (0,1) \to (c,d)$, potom $g \circ f : (a,b) \to (c,d)$ je bijektívne zobrazenie.

b) Funkcia $tg\,x$ proste zobrazuje interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ na množinu R (pozri obr.1). Teda $\left|\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)\right| = |R|$. Podľa predchádzajúcej vety a časti a) nášho príkladu platí, že $|(0,1)| = |R|$.



Obr. 1

Poznámka: Uvedený výsledok hovorí o tom, že „časť“ $(0,1)$ má rovnakú mohutnosť, ako „celok“ R – množina všetkých reálnych čísel. Je to trocha v spore s našou predstavou, že „časť“ je menšia ako „celok“, teda podmnožina má menšiu mohutnosť ako množina.

Po matematickej stránke je všetko v poriadku, nemôžu byť, proti presne sformulovanému matematickému výsledku ako faktu, žiadne námietky.

Zavedieme ďalšie pojmy týkajúce sa porovnania mohutnosti množín.

Definícia 2.9.2 Nech A, B sú množiny. Budeme hovoriť, že množina A má **mohutnosť menšiu alebo rovnú ako** množina B a písať $|A| \le |B|$, ak existuje injektívne zobrazenie $f : A \to B$. Množina A má **mohutnosť menšiu ako** množina B, píšeme $|A| < |B|$, ak $|A| \le |B|$ a nie je $|A| = |B|$.

Príklad 3. a) Interval $(0,1)$ má mohutnosť menšiu alebo rovnakú ako interval $\langle 0,1\rangle$, lebo $I_{(0,1)}$ je prosté zobrazenie množiny $(0,1)$ do $\langle 0,1\rangle$.

b) Množina $\{0\}$ má mohutnosť menšiu ako množina $\langle 0,1\rangle$. Existuje prosté zobrazenie $f : \{0\} \to \langle 0,1\rangle$, napríklad $f(0) = \frac{1}{2}$. Teda $|\{0\}| \le |\langle 0,1\rangle|$. Ale neplatí $|\{0\}| = |\langle 0,1\rangle|$. Ak g je zobrazenie z $\langle 0,1\rangle$ na $\{0\}$, tak nutne $g(0) = g(1) = 0$ a teda nie je prosté.

Poznámka: Všimnime si nasledujúci fakt: $|A| \le |B|$ vtedy a len vtedy, ak existuje $C \subseteq B$ taká, že $|A| = |C|$. Skutočne, ak $|A| \le |B|$, tak existuje prosté zobrazenie $f : A \to B$. Ak označíme $C = f(A)$, tak $C \subseteq B$ a f je prosté zobrazenie na množinu C, t.j. $|A| = |C|$. Ak zase naspäť existuje $C \subseteq B$ taká, že $|A| = |C|$, tak existuje prosté zobrazenie g z A na C. Potom g je prosté zobrazenie A do B a teda $|A| \le |B|$. Na základe tejto poznámky dokážeme nasledujúcu vetu.

Veta 2.9.2 Nech A, B, C sú množiny potom platí:

a) Ak $|A| = |B|$, tak $|A| \le |B|$,

b) Ak $|A| \le |B|$ a $|B| \le |C|$, tak $|A| \le |C|$,

c) Ak $|A| = |B|$ a $|B| < |C|$, tak $|A| < |C|$.

Dôkaz: a) Ak $|A| = |B|$, tak existuje bijektívne zobrazenie $f : A \to B$, ktoré je samozrejme aj injektívne a teda $|A| \le |B|$.

b) Ak $|A| \le |B|$, tak existuje $B' \subseteq B$, že $|A| = |B'|$, ak $|B| \le |C|$, tak existuje $C' \subseteq C$, že $|B| = |C'|$. Teda $f : A \to B'$ je bijekcia a taktiež $g : B \to C'$ je bijekcia. Potom $g \mid B' \circ f : A \to C$ je injektívne zobrazenie množiny A do množiny C a teda $|A| \le |C|$.

c) Ak $|A| = |B|$, tak $f : A \to B$ je bijekcia, ak $|B| < |C|$, tak $g : B \to C$ je injektívne zobrazenie, ktoré nie je surjektívne. Označme $g(B) = C' \subset C$, $C' \neq C$. Potom $g \circ f : A \to C'$ je bijekcia medzi množinami A a C' a injekcia medzi množinami A a C, teda $|A| < |C|$.

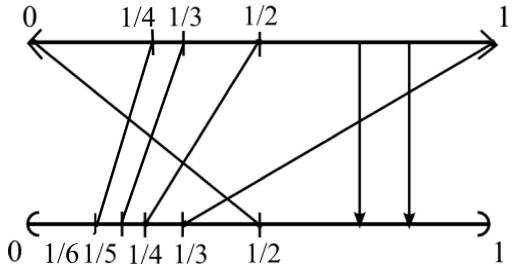
Dá sa čakať, že vzťah „$|A| \le |B|$“ je antisymetrický, t.j. ak $|A| \le |B|$ a súčasne $|B| \le |A|$, tak $|A| = |B|$. Ako uvidíme, je to pravda, ale dôkaz nie je celkom triviálny.

Príklad 4. Zrejme platí $|(0,1)| \le |\langle 0,1\rangle|$ a $|\langle 0,1\rangle| \le |(0,1)|$. Prvá nerovnosť je zrejmá z toho, že $(0,1) \subseteq \langle 0,1\rangle$ a druhá nerovnosť vyplýva z nasledujúceho, uvažujme $a < b$, pričom $0 < a < b < 1$ a definujme zobrazenie $f : \langle 0,1\rangle \to \langle a,b\rangle$ takto: $f(x) = a + (b-a)x$, toto zobrazenie je prosté a na, tým sme zaručili existenciu prostého zobrazenia intervalu $\langle 0,1\rangle$ do intervalu $(0,1)$. Ako však teraz nájsť prosté zobrazenie z $\langle 0,1\rangle$ na $(0,1)$? Neskôr takéto zobrazenie nájdeme. Poznamenávame, že také zobrazenie nemôže byť spojité.

Potiaž spočíva v tom, že z dvoch prostých zobrazení $f : A \to B$ a $g : B \to A$ chceme zostrojiť jedno prosté zobrazenie $h : A \to B$ množiny A na množinu B. Zobrazenie f je prosté, ale k tomu aby bolo „na“, mu „niečo“ chýba: $B - f(A)$. Tam je síce definované prosté zobrazenie g. Keby sme zobrali prosté zobrazenie $g^{-1} : g(B) \to B$, tak je síce „na“ množinu B, ale zasa „niečo“ zostalo $A - g(B)$. Mohli by sme postupovať takto: Označíme $X_0 = B - f(A)$ a $Y_0 = g(X_0)$. Potom g^{-1} zobrazí Y_0 na $B - f(A)$ (to nám chýbalo). Ale f môžeme uvažovať len na $A - Y_0$ a vznikne nový dlh $B - X_0 - f(A - Y_0) = f(A) - f(A - Y_0) = f(Y_0)$, ktorý treba zaplatiť. (Rôzny podvodníci a kriminálne živly už dávno objavili túto vlastnosť „nekonečna“). Treba na zaplatenie urobiť opäť nový dlh a týmto spôsobom požičiavania si do nekonečna môžeme postupovať ďalej. Podobný princíp „požičiavania si do nekonečna“ môžme použiť na konštrukciu hľadaného prostého zobrazenia $h : \langle 0,1\rangle \to (0,1)$.

Príklad 5. Zostrojíme prosté zobrazenie f intervalu $\langle 0,1\rangle$ na $(0,1)$.

Riešenie: Problémy nám robia čísla 0 a 1, ktoré nemáme kam zobraziť. Požičiame si čísla $\frac{1}{2}$ a $\frac{1}{3}$, položíme $f(0) = \frac{1}{2}$ a $f(1) = \frac{1}{3}$. Vznikne nám dlžoba $\frac{1}{2}$ a $\frac{1}{3}$, požičiame si $\frac{1}{4}$ a $\frac{1}{5}$ na jej zaplatenie. Teda položíme $f\left(\frac{1}{2}\right) = \frac{1}{4}$ a $f\left(\frac{1}{3}\right) = \frac{1}{5}$, a vo všeobecnosti $f\left(\frac{1}{n}\right) = \frac{1}{n+2}$ pre $n \in N, n \ge 2$. Ak pre $x \neq 0,\ x \neq 1,\ x \neq \frac{1}{n},\ n \ge 2,\ x \in \langle 0,1\rangle$ položíme $f(x) = x$, tak f je prosté zobrazenie z $\langle 0,1\rangle$ na $(0,1)$. Pozri obr. 2.



Obr. 2.

Prejdeme teraz k dôkazu všeobecného tvrdenia. Podstatnú časť tohto tvrdenia, ktorej dôkaz využíva vyššie uvedenú myšlienku, sformulujeme ako pomocné tvrdenie.

Lema 2.9.1 Nech f, g sú zobrazenia $f : A \to B$ a $g : B \to A$ a f je prosté. Potom existujú množiny A_1, A_2, B_1, B_2 také, že platí:

$$A_1 \cap A_2 = \emptyset,\ B_1 \cap B_2 = \emptyset \qquad (1a)$$

$$A_1 \cup A_2 = A,\ B_1 \cup B_2 = B \qquad (1b)$$

$$f(A_1) = B_1,\ g(B_2) = A_2 \qquad (1c)$$

Dôkaz: Keby f bolo zobrazenie na B, tak stačí položiť $A_1 = A,\ B_1 = B$ a $A_2 = B_2 = \emptyset$. Ak máme „dlžobu“ $X_0 = B - f(A)$, požičiame si $Y_0 = g(X_0)$ „na jej zaplatenie“. Ostane nám „ďalší dlh“ $X_1 = f(Y_0)$, ktorý zaplatíme „pôžičkou“ $Y_1 = g(X_1)$. Vo všeobecnosti položíme (pozri Obr. č. 3):

$$X_n = f(Y_{n-1}) \qquad (2a)$$

$$Y_n = g(X_n) \qquad (2b)$$

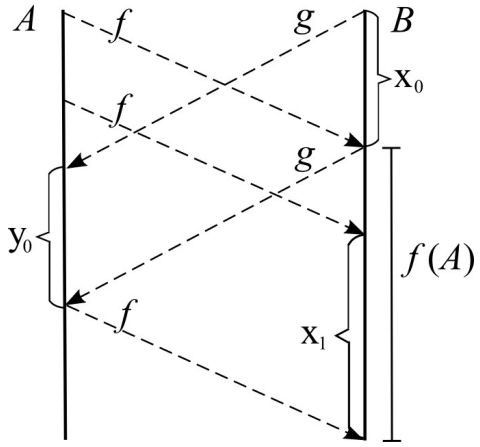
Označíme teraz

$$A_2 = \bigcup_{n=0}^{\infty} Y_n \qquad (3a)$$

$$A_1 = A - A_2 \qquad (3b)$$

$$B_2 = \bigcup_{n=0}^{\infty} X_n \qquad (3c)$$

$$B_1 = B - B_2 \qquad (3d)$$



Obr. 3.

Zrejme platí (1a) a (1b). Ukážeme, že platí (1c). K tomu stačí ukázať štyri inklúzie: 1) $f(A_1) \subseteq B_1$, 2) $B_1 \subseteq f(A_1)$, 3) $A_2 \subseteq g(B_2)$ a 4) $g(B_2) \subseteq A_2$.

1) Nech $x \in A_1$ a $y \in f(x)$. Keby $y \notin B_1$, tak $y \in B_2$ a teda existuje n také, že $y \in X_n$. Keďže $y \in f(A)$, tak $n > 0$. Podľa (2a) existuje $z \in Y_{n-1}$ také, že $y \in f(z)$. Ale f je prosté zobrazenie, teda $z = x$, čo je spor, lebo $x \in A_1$ a $z \in Y_{n-1} \subseteq A_2 = A - A_1$. Teda $f(A_1) \subseteq B_1$.

2) Nech $y \in B_1$. Zrejme $f(A) = B - X_0 \supseteq B_1$. Takže existuje $x \in A$ také, že $f(x) = y$. Stačí ukázať, že $x \in A_1$. Keby $x \notin A_1$, tak $x \in A_2$ a podľa (3a) a (2a) je $f(x) \in \bigcup_{n=0}^{\infty} X_n = B_2$, spor pretože $B_1 \cap B_2 = \emptyset$. Teda $x \in A_1$ a teda $B_1 \subseteq f(A_1)$.

3) Nech teraz $x \in A_2$. Potom existuje n také, že $x \in Y_n$, podľa (2b) existuje $y \in X_n$ také, že $x = g(y)$. Teda $x \in g(X_n)$, teda $A_2 \subseteq g(B_2)$.

4) Ak naopak je $x \in g(B_2)$, tak existuje n a existuje $y \in X_n$ také, že $x = g(y)$. Teda podľa (2b) $x \in Y_n \subseteq A_2$.

Veta 2.9.3 (Cantor - Bernstein) Nech A, B sú množiny. Ak platí $|A| \leq |B|$ a súčasne $|B| \leq |A|$, tak $|A| = |B|$.

Dôkaz 1: Nech platí $|A| \leq |B|$, $|B| \leq |A|$. Potom existujú injektívne zobrazenia f, g také, že $f : A \to B$ a $g : B \to A$. Podľa predchádzajúcej lemy existujú množiny A_1, A_2, B_1, B_2 také, že platí (1a) – (1c). Podľa (1c) zobrazenie g zobrazuje množinu B_2 injektívne na A_2. Teda existuje inverzné zobrazenie $g^{-1} : A_2 \to B_2$. Definujme zobrazenie h takto:

$$h(x) = f(x) \text{ pre } x \in A_1 \qquad (4a)$$

$$h(x) = g^{-1}(x) \text{ pre } x \in A_2 \qquad (4b)$$

Ukážeme, že h je prosté zobrazenie množiny A na množinu B. Nech $x_1, x_2 \in A$, $x_1 \neq x_2$. Máme štyri možnosti: 1) $x_1, x_2 \in A_1$, 2) $x_1, x_2 \in A_2$, 3) $x_1 \in A_1, x_2 \in A_2$ a 4) $x_1 \in A_2, x_2 \in A_1$. V prípadoch (1) a (2) je $h(x_1) \neq h(x_2)$ lebo f a g^{-1} sú injektívne zobrazenia. V prípadoch (3) a (4) jeden z prvkov $h(x_1), h(x_2)$ patrí do B_1 a druhý do B_2, teda sú rôzne. Z uvedeného vyplýva, že h je prosté zobrazenie.

Nech $y \in B$. Ak $y \in B_1$ tak podľa (1c) a (4a) je $y = f(x) = h(x)$ pre nejaké $x \in A_1$. Ak $y \in B_2$ potom podľa (1c) je $x = g(y) \in A_2$ a podľa (4b) je $h(x) = g^{-1}(x) = y$. Teda zobrazenie h je surjektívne zobrazenie množiny A na B.

Príklad 6. a) Zrejme platí, že $\{0,1\}^N \subseteq \{0,1,2\}^N$. Teda $\left|\{0,1\}^N\right| \leq \left|\{0,1,2\}^N\right|$.

b) Zostrojíme také prosté zobrazenie Φ z $\{0,1,2\}^N$ do $\{0,1\}^N$ takto:

$\Phi\left(\{a_n\}_{n=0}^{\infty}\right) = \{b_n\}_{n=0}^{\infty}$, kde $b_{2n} = 0$, ak $a_n = 0$ alebo 2; $b_{2n} = 1$, ak $a_n = 1$; $b_{2n+1} = 0$, ak $a_n = 0$ alebo 1; $b_{2n+1} = 1$ ak $a_n = 2$. Teda $\left|\{0,1,2\}^N\right| \leq \left|\{0,1\}^N\right|$.

Zhrnutím podľa Cantorovej – Bernsteinovej vety dostávame, že $\left|\{0,1\}^N\right| = \left|\{0,1,2\}^N\right|$.

Uvedieme ešte jeden dôkaz Cantorovej –Bernsteinovej vety.

Dôkaz 2: Každý prvok $y \in B$ je obrazom najviac jedného prvku $x \in A$ v zobrazení f. Ak taký prvok x jestvuje, nazveme ho rodičom prvku y. Podobne je každý prvok $x \in A$ obrazom najviac jedného prvku $y \in B$ v zobrazení g. Tento prvok, ak existuje, sa tiež bude nazývať rodičom prvku x.

Pre každý prvok t z množiny A, alebo z množiny B budeme sledovať reťazec jeho predkov. Formálne prvok z nazveme predkom prvku t, ak existuje postupnosť $z = z_n, z_{n-1}, ..., z_1, z_0 = t$ prvkov množiny $A \cup B$ taká, že pre každé $i = 0,1,...,n-1$ je prvok z_{i+1} rodičom prvku z_i. Pre ľubovoľný prvok $t \in A \cup B$ môžu nastať tri navzájom sa vylučujúce prípady.

1. t má nekonečne veľa predkov, inými slovami, každý predok prvku t má rodiča.
2. Existuje taký predok z prvku t, ktorý už nemá rodiča pričom $z \in A$.
3. Existuje taký predok z prvku t, ktorý nemá rodiča, pričom $z \in B$.

Nech teraz $A_i, i = 1,2,3$ je množina všetkých $t \in A$, ktoré majú vyššie uvedenú vlastnosť i. Podobne definujeme aj množiny $B_i, i = 1,2,3$. Keďže sa prípady vylučujú, sú množiny A_i ako aj B_i po dvoch disjunktné.

Ľahko nahliadneme, že predok prvku $t \in A_i$ patriaci do A tiež leží v A_i. Podobné tvrdenie platí aj o $t \in B_i$. Preto $f \mid A_1 : A_1 \to B_1$ je bijekcia, $f \mid A_2 : A_2 \to B_2$ je bijekcia a $g \mid B_3 : B_3 \to A_3$ je bijekcia.

Napokon uvidíme, že zobrazenie $h : A \to B$ definované predpisom

$$h(x) = f(x), \text{ ak } x \in A_1 \cup A_2$$
$$g^{-1}(x), \text{ ak } x \in A_3$$

je bijekcia.

Poznámka: Nestalo sa náhodou, že sme skúmanie vlastnosti „ostrej“ nerovnosti medzi mohutnosťami nechali až na teraz. Bez predchádzajúcej vety sa tvrdenia o „ostrej“ nerovnosti dokazujú omnoho ťažšie.

Veta 2.9.4 Nech A, B, C sú množiny. Ak $|A| \le |B|$ a $|B| < |C|$ (alebo $|A| < |B|$ a $|B| \le |C|$), tak $|A| < |C|$.

Dôkaz: Ak $|A| \le |B|$ a $|B| < |C|$, tak $|A| \le |C|$ vyplýva z vety, ktorú sme dokázali skôr. Keby platilo $|A| = |C|$ a teda aj $|C| \le |A|$, tak dostávame $|C| \le |B|$ a súčasne $|B| < |C|$, podľa Cantorovej-Bersteinovej vety je $|B| = |C|$, čo je v spore s predpokladom vety.

V súlade s tým, čo sme povedali na úvod o mohutnostiach, uvažovali sme vzťah „dve množiny majú rovnakú mohutnosť“ alebo vzťah „mohutnosť jednej množiny je menšia ako mohutnosť druhej množiny“ bez toho, aby sme vedeli čo je to „mohutnosť“. Zatiaľ sme to nepotrebovali a ani to potrebovať nebudeme. V niektorých špeciálnych prípadoch budeme postupovať zdanlivo inak, ale vždy to bude len vyjadrenie (skratka) pre vzťah „mať rovnakú mohutnosť“.

Vo filozofii sa hovorí o definícií abstrakciou, „mohutnosť“ je to čo je spoločné všetkým množinám rovnakej mohutnosti, nepotrebujeme tento pojem mať ako presne definovaný matematický pojem. S podobnou situáciou sa stretávame v bežnom živote často: asi by ste ťažko vysvetlili, čo je to „pekné“, ale viete posúdiť, či je hudba pekná, či sú pekné kvety na lúke, alebo či je pekné dievča, mládenec. „Pekné“ je tá vlastnosť týmto všetkým spoločná. Preto mnohí matematici často pod mohutnosťou množiny A nazývajú symbol, priradený všetkým množinám s rovnakou mohutnosťou ako množina A. Ak sa vrátime do matematiky, môžeme si všimnúť, že nevieme, čo je to prirodzené číslo, ale vieme (aspoň čiastočne), čo je to množina všetkých prirodzených čísel. Príslušné pojmy (mohutnosť, číslo) vieme posúdiť v súvislostiach a nie oddelene.

2.10. Počítanie s mohutnosťami

Naučíme sa teraz počítať s mohutnosťami, počítanie bude veľmi jednoduché a v určitom zmysle prirodzené. Je to (prirodzené) zovšeobecnenie aritmetiky prirodzených čísel.

Definícia 2.10.1 Nech A, B, C sú množiny. Budeme hovoriť, že **mohutnosť** množiny ***C*** **je súčet mohutností** množín ***A*** a ***B***, písať $|C| = |A| + |B|$, ak existujú množiny A_1, B_1 také že

$$A_1 \cup B_1 = C \qquad (1a)$$

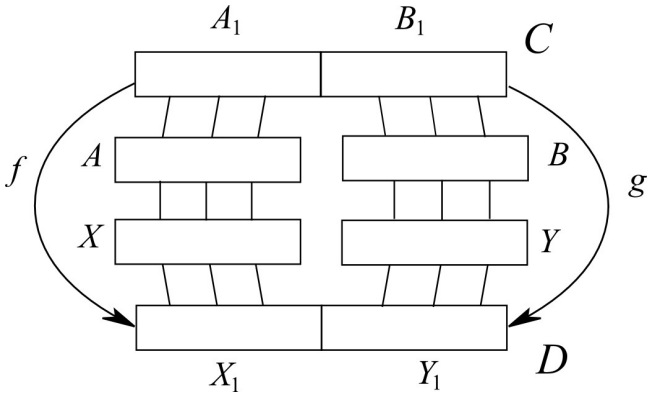
$$A_1 \cap B_1 = \emptyset \qquad (1b)$$

$$|A| = |A_1|, |B| = |B_1| \qquad (1c)$$

Najprv musíme overiť, či takáto definícia je korektná. Totiž súčet mohutností „$|A| + |B|$“ sme definovali pomocou množín A, B. Nezmení sa výsledok (definície), ak vezmeme iné množiny ako množiny A, B, ale tej istej mohutnosti? Presne povedané musíme dokázať toto:

Ak $|C| = |A| + |B|$, $|X| = |A|$, $|Y| = |B|$ a $|D| = |X| + |Y|$, potom aj $|C| = |D|$.

Nech $|C| = |A| + |B|$, $|X| = |A|$, $|Y| = |B|$ a $|D| = |X| + |Y|$. Teda existujú množiny A_1, B_1 s vlastnosťami (1a) – (1c) a množiny X_1, Y_1 také, že $|X_1| = |X|$, $|Y_1| = |Y|$, $X_1 \cap Y_1 = \emptyset$ a $X_1 \cup Y_1 = D$. Potom $|A_1| = |X_1|$ a $|B_1| = |Y_1|$ (pozri obr.1.) a teda existujú prosté zobrazenia f, g z A_1 resp. B_1 na množinu X_1 resp. Y_1.



Obr.1.

Položme

$$h(x) = f(x), \text{ pre } x \in A_1,$$
$$g(x), \text{ pre } x \in B_1,$$

t.j. $h = \{(x, y); (x \in A_1 \wedge y = f(x)) \vee (x \in B_1 \wedge y = g(x))\}$.

Ľahko sa za zistí, že h je prosté zobrazenie množiny C na množinu D. To sme však chceli ukázať.

Príklad 1. a) Nech $A = \{0,1,2\}$, $B = \{0,1,2,3,4\}$ a $C = \{0,1,2,3,4,5,6,7\}$. Potom $|C| = |A| + |B|$, lebo existujú množiny $A_1 = \{0,1,2\}$ a $B_1 = \{3,4,5,6,7\}$ spĺňajúce podmienky (1a)– (1c).

b) Platí $|(0,1)| = |(0,1)| + |(0,1)|$

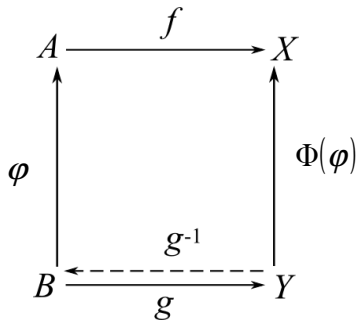
Stačí zvoliť napríklad $A_1 = (0, \frac{1}{2})$ a $B_1 = \langle \frac{1}{2}, 1)$ a použiť výsledky príkladov z predchádzajúcej časti.

Ďalšou operáciou je umocňovanie mohutnosti.

Definícia 2.10.2 Budeme hovoriť, že mohutnosť množiny C je **mohutnosť** množiny A **umocnená na mohutnosť** množiny B, písať $|C| = |A|^{|B|}$, ak $|C| = |A^B|$. Pričom A^B označujeme množinu všetkých zobrazení množiny B do množiny A.

Podobne ako v prípade súčtu mohutností, ukážeme korektnosť definície. Máme ukázať, že ak $|X| = |A|$, $|Y| = |B|$ a $|D| = |X^Y|$, tak $|D| = |C|$. K tomu stačí ukázať toto: ak $|A| = |X|$, $|B| = |Y|$, tak $|A^B| = |X^Y|$.

Nech teda $|A| = |X|$, $|B| = |Y|$, t.j. existujú prosté zobrazenia f, g množiny A, resp. B na množinu X, resp. Y. Zostrojíme zobrazenie $\Phi : A^B \to X^Y$ ľahko. Keďže g je prosté zobrazenie množiny B na množinu Y, existuje inverzné zobrazenie $g^{-1} : Y \to B$. Pre $\varphi \in A^B$ (t.j. $\varphi : B \to A$) položíme $\Phi(\varphi) = f \circ \varphi \circ g^{-1}$. Potom (pozri obr.2) $\Phi(\varphi) : Y \to X$, t.j. $\Phi(\varphi) \in X^Y$. Ak $\varphi_1, \varphi_2 \in A^B$, $\varphi_1 \neq \varphi_2$, tak existuje $x \in B$ také, že $\varphi_1(x) \neq \varphi_2(x)$.



Obr.2.

Nech $y = g(x)$. Potom (f je prosté) platí:
$\Phi(\varphi_1)(y) = f\left(\varphi_1\left(g^{-1}(y)\right)\right) = f(\varphi_1(x)) \neq f(\varphi_2(x)) = f\left(\varphi_2\left(g^{-1}(y)\right)\right) = \Phi(\varphi_2)(y)$. Teda $\Phi(\varphi_1) \neq \Phi(\varphi_2)$.
Odtiaľ vyplýva, že Φ je prosté zobrazenie množiny A^B do množiny X^Y.

Ukážeme ,že je zobrazením na množinu X^Y. Nech $\psi \in X^Y$. Potom (f má inverznú), nech $\psi \in X^Y$, tak $f^{-1} \circ \varphi \circ g^{-1} \in A^B$ (pozri Obr.2). $\Phi(\varphi) = f \circ \varphi \circ g^{-1} = f \circ f^{-1} \circ \psi \circ g \circ g^{-1} = \psi$.

Podobne definujeme súčin mohutností.

Definícia 2.10.3 Budeme hovoriť, že mohutnosť množiny C je **súčin mohutností** množín A a B, písať $|C| = |A| \cdot |B|$, ak platí

$$|C| = |A \times B|.$$

Aj tu je potrebné overiť korektnosť definície. Stačí ukázať, že ak $|A| = |X|$, $|B| = |Y|$, tak $|A \times B| = |X \times Y|$.

Avšak, ak f, g sú prosté zobrazenia z množiny A, resp. B na množinu X, resp. Y, tak položíme

$$h((x, y)) = (f(x), g(y))$$

pre $x \in A$ a $y \in B$. Ľahko možno overiť, že h je prosté zobrazenie množiny $A \times B$ na množinu $X \times Y$.

Príklad 2. a) $|\varnothing| \cdot |A| = |\varnothing|$. Skutočne, pre ľubovoľnú množinu A je $\varnothing \times A = \varnothing$.

b) Nech $A=\{a\}$, t.j. A má jeden prvok. Potom $|A|\cdot|B|=|B|$. Totiž zobrazenie $f(x)=(a,x)$ pre $x\in B$, je prosté a na množinu $A\times B$. Teda

$$|A|\cdot|B|=|A\times B|=|B|.$$

c) Nech $A=\{a,b\}$, $a\neq b$. Potom $|A|.|B|=|B|+|B|$. Skutočne, ak označíme

$$A_1=\{a\}\times B,\ B_1=\{b\}\times B,$$

tak $A_1\cup B_1=A\times B,\ A_1\cup B_1=\varnothing,\ |A_1|=|B_1|=|B|$. Podľa definície súčtu a súčinu mohutností dostávame $|A|\cdot|B|=|A\times B|=|A_1\cup B_1|=|A_1|+|B_1|=|B|+|B|$.

Príklad 3. a) Pre každú množinu A je $|A|^{|\varnothing|}=|\{\varnothing\}|$. Totiž $A^{\varnothing}=\{\varnothing\}$, čo teraz aj ukážeme. Inak povedané dokážeme, že prázdna množina $\varnothing$ je jediné zobrazenie prázdnej množiny $\varnothing$ do ľubovoľnej množiny A. Ukážeme, že $\varnothing$ spĺňa podmienky zobrazenia z definície. Teda nech x je ľubovoľný prvok patriaci do $\varnothing$, tak potom existuje práve jeden prvok $y\in A$, že $(x,y)\in\varnothing$. Formálnejšie zapísané:

$$(\forall x)(x\in\varnothing)\rightarrow((\exists!\,y\in A)\wedge(x,y)\in\varnothing)$$

Symbolom $\exists!\,a\in A:V(a)$ označujeme, že v množine A existuje práve jedno a s vlastnosťou V.
Ihneď vidno, že zložený kvantifikovaný výrok je tautológia, pretože výrok $x\in\varnothing$ pre ľubovoľné x je nepravdivý a teda implikácia je pravdivá ak predpoklad je nepravdivý. To, že prázdna množina je jediné zobrazenie vyplýva z toho, že $\varnothing\times A=\varnothing$.

b) $|A|^{|\{a\}|}=|A|$ pre ľubovoľnú množinu A. Vyplýva to z toho, že zobrazenie $\Phi:A\rightarrow A^{\{a\}}$ definované predpisom

$$\Phi(x)=\{(a,x)\}$$

je prosté zobrazenie na množine $A^{\{a\}}$.

Práve definované operácie majú bežné vlastnosti podobných vlastností na prirodzených číslach. Napr. všetky sú monotónne, t.j. ak $|A|\leq|X|,\ |B|\leq|Y|$, potom

$$|A|+|B|\leq|X|+|Y| \qquad (2a)$$

$$|A|\cdot|B|\leq|X|\cdot|Y| \qquad (2b)$$

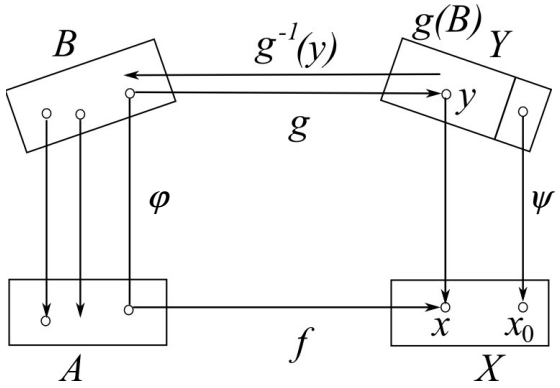
$$\left|A^B\right|\leq|X|^{|Y|} \qquad (2c)$$

Dokážeme napríklad (2c). Keďže $|A|\leq|X|,\ |B|\leq|Y|$, tak existujú prosté zobrazenia $f:A\rightarrow X$ a $g:B\rightarrow Y$. Ak g je zobrazenie na množinu Y, tak existuje g^{-1} a zobrazenie Φ definované predpisom

$$\Phi(\varphi)=f\circ\varphi\circ g^{-1}$$

je prosté zobrazenie množiny A^B do množiny X^Y. Ak je $g(B)\neq Y$, musíme postupovať zložitejšie. Ak $X=\varnothing$, tak nutne aj $A=\varnothing$, pretože $|A|\leq|X|$ a (2c) platí, lebo za predpokladu, že $B\neq\varnothing$, tak aj $Y\neq\varnothing$ zo známeho dôvodu, $\varnothing^B=\varnothing^Y=\varnothing$, t.j. neexistuje zobrazenie neprázdnej množiny do prázdnej (presvedčte sa o tom). V prípade, že $A=\varnothing,\ B=\varnothing,\ X=\varnothing,\ Y=\varnothing$ (2c) taktiež platí, lebo $\varnothing^{\varnothing}=\{\varnothing\}$, ak ale $A=\varnothing,\ B=\varnothing,\ X=\varnothing$ a $Y\neq\varnothing$, nerovnosť (2c) neplatí (prečo?). A^B do X^Y

definujeme teraz takto. Nech $\varphi \in A^B$. Zobrazenie $g : B \to g(B)$ má inverzné. Nech $\psi(y) = f\left(\varphi\left(g^{-1}(y)\right)\right)$ pre $y \in g(B)$ a $\psi(y) = x_0$ pre $y \in Y - g(B)$ (porovnaj Obr. 3). Položíme $\Phi(\varphi) = \psi$. Ľahko sa zistí, že Φ je prosté zobrazenie A^B do X^Y.



Obr.3.

Pre sčítanie a násobenie mohutností platia zákony aritmetiky, napr.

Sčítanie je *komutatívne* $|A| + |B| = |B| + |A|$, (3a)

asociatívne $|A| + (|B| + |C|) = (|A| + |B|) + |C|$. (3b)

Násobenie je *komutatívne* $|A| \cdot |B| = |B| \cdot |A|$, (3c)

asociatívne: $|A| \cdot (|B| \cdot |C|) = (|A| \cdot |B|) \cdot |C|$. (3d)

Platí *distributívny zákon*

$$|A| \cdot (|B| + |C|) = (|A| \cdot |B|) + (|A| \cdot |C|). \quad (3e)$$

Dokážeme napríklad asociatívnosť násobenia. Zrejme stačí ukázať:

$$|A \times (B \times C)| = |(A \times C) \times C|.$$

Nech $x \in A \times (B \times C)$. Potom existujú $a \in A, b \in B, c \in C$ také, že $x = (a,(b,c))$. Položíme $f(x) = ((a,b),c) \in (A \times B) \times C$. Ukážeme najprv, že f je prosté zobrazenie. Nech $x, x' \in A \times (B \times C)$, $x = (a,(b,c))$, $x' = (a',(b',c'))$. Teda $a \neq a'$ alebo $b \neq b'$ alebo $c \neq c'$. Potom aj $((a,b),c) \neq ((a',b'),c')$, t.j. $f(x) \neq f(x')$. Ak $y \in (A \times B) \times C$, tak existujú $a \in A$, $b \in B$ a $c \in C$ také, že $y = ((a,b),c)$. Potom $(a,(b,c)) \in A \times (B \times C)$ a $f(a,(b,c)) = y$. Teda f je zobrazenie na množinu $(A \times B) \times C$.

Pre umocňovanie platia tiež zákony aritmetiky

$$|A|^{|B|+|C|} = |A|^{|B|} \cdot |A|^{|C|} \quad (4a)$$

$$(|A| \cdot |B|)^{|C|} = |A|^{|C|} \cdot |B|^{|C|} \quad (4b)$$

$$\left(|A|^{|B|}\right)^{|C|} = |A|^{|B| \cdot |C|} \quad (4c)$$

Naznačíme dôkaz poslednej rovnosti. Zrejme stačí zostrojiť prosté zobrazenie množiny $\left(A^B\right)^C$ na množinu $A^{(B \times C)}$. Nech $\varphi \in \left(A^B\right)^C$. Pre každé $c \in C$ je $\varphi(c)$ zobrazenie $\varphi(c) : B \to A$.

Zobrazenie Ψ z $B\times C$ do A definujeme takto: $b\in B$, $c\in C$, tak položíme $\psi((b,c))=\varphi(c)(b)\in A$. Ak položíme $\Phi(\varphi)=\psi$, tak Φ je hľadané prosté zobrazenie množiny $\left(A^B\right)^C$ na množinu $A^{B\times C}$.

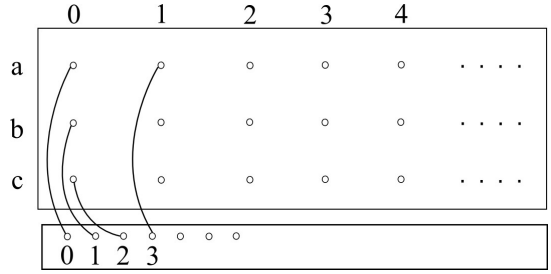
Príklad 4. Pre ľubovoľnú množinu X podľa práve dokázanej rovnosti platí:
$\left(|X|^{|N|}\right)^{|N|}=|X|^{|N|\cdot|N|}$.
Množina $\left(X^N\right)^N$ je množina všetkých postupností, ktorej členmi sú postupnosti prvkov množiny X. Teda typický prvok množiny $\left(X^N\right)^N$ je postupnosť $\{f_n\}_{n=0}^{\infty}$, kde každé f_n je postupnosť prvkov X, t.j. $f_n: N\to X$. Ak označíme $F(n,k)=f_k(n)\in X$ pre $n,k\in N$, tak F je „dvojitá postupnosť“, t.j. $F: N\times N\to X$. Všimnime si, že $F=\Phi\left(\{f_n\}_{n=0}^{\infty}\right)$, kde Φ je zobrazenie z dôkazu rovnosti (4c).

Odčítanie a delenie mohutnosti sa definovať nedá. Napríklad definícia odčítania $|X|-|Y|$ pre $|Y|\le|X|$ by vyžadovala existenciu „jedinej mohutnosti $|Z|$“ takej, že $|Y|+|Z|=|X|$. My už vieme, že napríklad

$$|\varnothing|+|(0,1)|=|(0,1)|+|(0,1)|=|(0,1)|$$

a teda nemôžeme definovať ani rozdiel $|(0,1)|-|(0,1)|$. Ukážeme podobnú vec pre násobenie.

Príklad 5. Nech $a\neq b$, $a\neq c$, $b\neq c$. Potom $|N|\le|\{a,b\}|\cdot|N|=|\{a,b,c\}|\cdot|N|$. Zrejme platí $|N|\le|\{a,b\}|\cdot|N|\le|\{a,b,c\}|\cdot|N|$, teda stačí ukázať, $|\{a,b,c\}|\cdot|N|\le|N|$. Zobrazenie $f:\{a,b,c\}\times N\to N$ definujeme takto: $f((a,n))=3n$, $f((b,n))=3n+1$, $f((c,n))=3n+2$.



Obr.4.

Uvedené príklady ukazujú tiež to, že monotónnosť sčítania a násobenia neplatí pre ostrú nerovnosť, napríklad podľa predchadzajúceho príkladu je $|\{a,b\}|<|\{a,b,c\}|$ ale $|\{a,b\}|\cdot|N|=|\{a,b,c\}|\cdot|N|$.

Bude nás teraz zaujímať mohutnosť množiny $P(X)$ vo vzťahu k mohutnosti množiny X. Na množinu X sa budeme pozerať teraz ako na „náhodný priestor“. Ak $A\subseteq X$, tak charakteristická funkcia χ_A množiny A je zobrazenie $\chi_A: X\to\{0,1\}$ s takouto vlastnosťou:

$$\chi_A(x)=1, \text{ ak } x\in A,$$

$$\chi_A(x)=0, \text{ ak } x\notin A, \text{ teda ak } x\in X-A.$$

Príklad 6. Nech základný priestor je $X=N$.

Postupnosť $\left\{\frac{1+(-1)^n}{2}\right\}_{n=0}^{\infty}$ je charakteristická funkcia množiny párnych prirodzených čísel. Ak $\{a_n\}_{n=0}^{\infty}$ je ľubovoľná postupnosť reálnych čísel, A je nejaká množina prirodzených čísel, tak znak $\sum_{n\in A} a_n$ zrejme označuje súčet radu $\sum_{n=0}^{\infty} \chi_A(n).a_n$.

Príklad 7. Nech X je základný priestor, $A, B \subseteq X$. Ľahko možno overiť, že platí:

$$\chi_{A\cap B} = \chi_A \cdot \chi_B$$

$$\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$$

$$\chi_{X-A} = 1 - \chi_A$$

$$A \subseteq B \leftrightarrow \chi_A \le \chi_B$$

Keďže je prirodzené považovať prirodzené číslo 2 za mohutnosť množiny $\{0,1\}$, tak budeme písať $|\{0,1\}|^{|X|} = 2^{|X|}$.

Lema 2.10.1 Pre ľubovoľnú množinu X platí $|P(X)| = 2^{|X|}$.

Dôkaz: Pre množinu $A \subseteq B$ položíme

$$\Phi(A) = \chi_A .$$

Zrejme Φ je prosté zobrazenie množiny $P(X)$ na množinu $\{0,1\}^X$. Napríklad, ak $\varphi \in \{0,1\}^X$, potom $S = \chi_A = \Phi(A)$, kde

$$A = \{x \in X; \varphi(x) = 1\} .$$

Príklad 8. Pre ľubovoľnú množinu X, pre ktorú $|X| \ge |\{0,1\}|$ platí

$$|X| \le 2^{|X|} \le |X|^{|X|} \le 2^{|X|\cdot|X|}$$

Nech $f : X \to P(X)$ je definované predpisom $f(x) = \{x\}$ pre $x \in X$. f je prosté zobrazenie a teda $|X| \le |P(X)| = 2^{|X|}$. Druhá nerovnosť vyplýva z platnosti nasledujúcich nerovností: ak $|A| \le |X|, |B| \le |Y|$, tak $|A|^{|B|} \le |X|^{|Y|}$. Ďalej ak si uvedomíme, že každé zobrazenie $g \in X^X$ je množina usporiadaných dvojíc prvkov množiny X, t.j. $g \subseteq X \times X$, tak dostávame $X^X \subseteq P(X, X)$, odtiaľ nám vyplýva tretia nerovnosť.

Vo všeobecnosti nevieme o sčítaní, násobení a umocňovaní mohutností takmer nič dokázať. Dokážeme niekoľko výsledkov pre konkrétne množiny, ktoré sú však veľmi dôležité.

Mohutnosť množiny N prirodzených čísel označujeme $\aleph_0$, čítame „alef nula“. $\aleph$ je prvé písmeno hebrejskej abecedy. Predpokladám, že vám nevadí ten fakt, že nevieme, čo to mohutnosť je, ale „mohutnosť N“ označujeme $\aleph_0$. Napríklad zápis „$\aleph_0 \neq \aleph_0^{\aleph_0}$“ znamená „$|N|^{|N|} \neq |N|$“, t.j. „neexistuje prosté zobrazenie N^N na N“.

Veta 2.10.1 $\aleph_0 = \aleph_0 + \aleph_0$.

Dôkaz: Máme ukázať, že $|N| + |N| = |N|$. Podľa definície stačí (a je nutné) nájsť dve disjunktné množiny A, B, také, že $A \cup B = N$ a $|A| = |B| = |N|$. Nech

$$A=\{m\in N;(\exists n)(n\in N\wedge m=2n)\},$$
$$B=\{m\in N;(\exists n)(n\in N\wedge m=2n+1)\},$$

t.j. A je množina párnych a B je množina nepárnych prirodzených čísel. Zrejme $A\cap B=\emptyset$ a $A\cup B=N$, (presvedčte sa o tom!). Nech $f=\{(n,2n),n\in N\}$ a $g=\{(n,2n+1),n\in N\}$, t.j. $f(n)=2n$ a $g(n)=2n+1$ pre $n\in N$. Ľahko vidieť, že f je prosté zobrazenie množiny N na množinu A a g je prosté zobrazenie množiny N na množinu B. Teda

$$|A|=|B|=|N|.$$

Príklad 9. $2^{\aleph_0}2=\aleph_0 2+\aleph_0$.

Zo známych nerovností pre mohutnosti dostávame $2^{\aleph_0}2\le\aleph_0 2+\aleph_0$, ďalej podľa tvrdenia ($A=\{a,b\}$, $a\neq b$, potom $|A|.|B|=|B|+|B|$) je $2^{\aleph_0}2.2=\aleph_0 2+\aleph_0$, platí $2.2^{\aleph_0}2=\aleph_0+\aleph_0 2=\aleph_0 2.\aleph_0 2\le\aleph_0$. Podľa Cantor – Bernsteinovej vety dostávame $2^{\aleph_0}2=\aleph_0 2+\aleph_0$.

Veta 2.10.2 $\aleph_0=\aleph_0.\aleph_0$.

Dôkaz: Máme ukázať $|N\times N|=|N|$, t.j. máme nájsť prosté zobrazenie $N\times N$ na N. Ukážeme viac takýchto zobrazení. Pripomíname, že používame skrátený zápis $f((x,y))=f(x,y)$.

a) Najjednoduchšie zobrazenie f je definované predpisom

$$f(n,m)=2^n(2m+1)-1.$$

Zrejme je f prosté (ak $2^{n_1}(2m_1+1)-1=2^{n_2}(2m_2+1)-1$, tak $n_1=n_2$ a $m_1=m_2$). Nech $k\in N$. Potom číslo $k+1$ možno (jediným spôsobom) napísať v tvare $2^n(2m+1)$. Zrejme $f(n,m)=k$. Teda f je zobrazenie $N\times N$ na množinu N.

b) Náročnejšie je zobrazenie g definované predpisom

$$g(n,m)=\frac{1}{2}(n+m)(n+m+1)+m$$

Môžeme ho zapísať takto. Nech

$$T(k)=0+1+\ldots+k=\frac{1}{2}k(k+1).$$

Potom $T(k+1)=T(k)+(k+1)$.

Všetkých dvojíc (n,m) takých, že $n+m=k$ je práve $k+1$: $(k,0),(k-1,1),\ldots,(0,k)$.

Čísla $T(k)+0,\ T(k)+1,\ldots,T(k)+k$, použijeme na ich číslovanie, t.j.

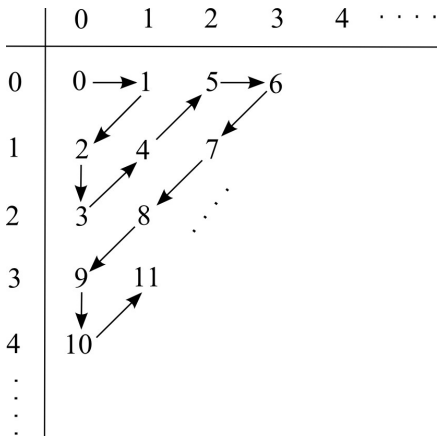
$$g(n,m)=T(n+m)+m$$

Dobrú predstavu o zobrazení g dáva obr. č.5.

	0	1	2	3	4	5	..	m	..
0	0	2	5	9	14	20		$k+m$	
1	1	4	8	13	19				
2	3	7	12	18		$k+5$			
3	6	11	17		$k+4$				
4	10	16		$k+3$					
5	15		$k+2$						
:		$k+1$						$k=\frac{1}{2}(n+m)(n+m+1)$	
n	k								
:									

Obr.5.

c) Historicky prvé známe zobrazenie je znázornené na obr. č.6.



Obr.6.

d) Zobrazenie znázornené na obr. č. 7. má dôležitú úlohu pri dobre usporiadaných množinách.

	0	1	2	3	4	...	n	...
0	0	1	4	9	16	...	n^2	
1	2	3	5	10	17	...	n^2+1	
2	6	7	8	11	18	...	n^2+2	
3	12	13	14	15	19	...	n^2+3	
4	20	21	22	23	24		⋮	
⋮							⋮	
n	n^2+n	n^2+n+1	...	...	...	...	n^2+2n	
⋮							⋮	

Obr.7.

Ľahko možno overiť, že všetky uvedené zobrazenia sú prosté na množinu *N*.

Príklad 10. $^{0}\aleph 2 = {}^{0}\aleph_0\,\aleph$.

Podľa známych nerovností a tvrdení pre mohutnosti množín máme:

$$^{0}\aleph 2 = {}^{0}\aleph.{}^{0}\aleph\, 2 = {}^{0}\aleph({}^{0}\aleph 2) \leq {}^{0}\aleph_0\,\aleph.$$

Keďže $2^{0}\aleph_0\,\aleph \leq {}^{0}\aleph$, tak podľa Cantorovej – Bernsteinovej vety platí $^{0}\aleph 2 = {}^{0}\aleph_0\,\aleph$.

Na záver dokážeme jednu všeobecnú vetu o umocňovaní, ktorá hrala a hrá dôležitú úlohu v teórii množín.

Veta 2.10.3 (Cantor) Pre každú množinu X platí $|X| < |P(X)|$.

Dôkaz: Vieme už, že existuje prosté zobrazenie $f : X \to P(X)$, stačí položiť $f(x) = \{x\}$. Teda $|X| \leq |P(X)|$. Ukážeme, že neplatí rovnosť $|X| = |P(X)|$. Budeme dokazovať sporom. Nech platí $|X| = |P(X)|$. Potom existuje prosté zobrazenie f množiny X na množinu $P(X)$. Uvažujme množinu:

$$E = \{x \in X,\ x \notin f(x)\}.$$

Zrejme $E \subseteq X$ a teda $E \in \mathcal{P}(X)$, keďže f je zobrazenie na množinu $\mathcal{P}(X)$, tak existuje $k \in X$ taký, že $f(k) = E$. Máme dve možnosti:

1) $k \in E$. Potom podľa definície množiny E platí, že $k \notin f(k)$. To však nie je možné, lebo $f(k) = E$.

Teda nutne platí:

2) $k \notin E$. Keďže $E = f(k)$, tak to znamená, že $k \notin f(k)$. Potom podľa definície množiny E platí $k \in E$. A to je hľadaný spor.

Dôsledok 1. Pre každú množinu X platí $|X| < 2^{|X|}$.

Dôsledok 2. Neexistuje množina všetkých množín.

Dôkaz: Vykonáme sporom. Nech A je množina, ktorá obsahuje všetky množiny, tak každá množina množín je jej podmnožina. Špeciálne $\mathcal{P}(A) \subseteq A$. Potom by však bola $|\mathcal{P}(A)| \leq |A|$, čo je spor s Cantorovou vetou.

Vzniká otázka, ktoré množiny nazvať konečné a ktoré nazvať nekonečné. Mnohé vlastnosti nekonečna sa ponúkajú za definíciu: napríklad zrejme „nekonečná“ množina R má rovnakú mohutnosť ako „jej časť“ $(0,1)$. To by sa konečnej množine nemalo stať. Za vyše sto rokov bádania v teórii množín sa však ukázalo, že práve uvedená vlastnosť nie je najvhodnejšia pre definíciu. Pojem nekonečna je schovaný vo vlastnostiach prirodzených čísel a princíp matematickej indukcie zaručuje, že $\aleph_0$ je v určitom zmysle najmenšie nekonečno.

Definícia 2.10.4 Množina ***A*** sa nazýva **konečná**, ak $|A| < \aleph_0$, t.j. ak $|A| < |N|$. Množina sa nazýva nekonečná, ak nie je konečná.

Príklad 11. Množiny $\emptyset, \{1\}, \{1,2\}, \{a,b\}$ sú konečné. Množiny N, R, Q, C sú nekonečné.

Definícia konečnej množiny je síce jednoduchá, ale mnoho nám nehovorí. Musíme preto príslušný pojem preskúmať. Prvé, čo nás napadá je, či „n prvková“ množina je konečná. Upresníme to. Označíme pre $n \in N$:

$$N_n = \{k \in N;\ k < n\} \qquad (1)$$

Teda napr. $N_0 = \emptyset$, $N_1 = \{0\}$, $N_2 = \{0,1\}$, $N_n = \{0,1,2,...,n-1\}$. Pre ľubovoľné $n \in N$ platí

$$N_{n+1} = N_n \cup \{n\} \qquad (2)$$

Skutočne, ak $k < n+1$, tak $k \leq n$, t.j. $k < n$ alebo $k = n$.

Definícia 2.10.5 Budeme hovoriť, že množina ***A*** **má *n* prvkov**, písať $|A| = n$, kde $n \in N$, ak $|A| = |N_n|$.

Chceme ukázať, že n prvková množina je konečná. K tomu bude užitočná nasledujúca lema.

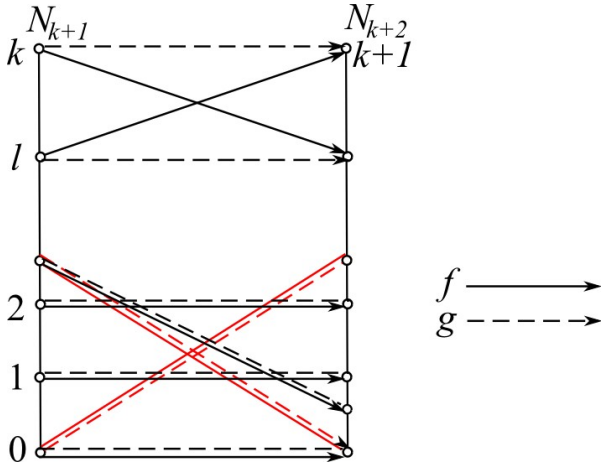
Lema 2.10.2 Pre každé $n \in N$ platí

$$|N_n| < |N_{n+1}| \qquad (3)$$

Dôkaz: Urobíme matematickou indukciou. Pre každé $n \in N$ platí $N_n \subseteq N_{n+1}$ a teda $|N_n| \leq |N_{n+1}|$. Stačí ukázať, že $|N_n| \neq |N_{n+1}|$.

Pre $n = 0$ je tvrdenie pravdivé, lebo prázdna množina N_0 nemôže mať rovnakú mohutnosť ako neprázdna množina N_1.

Predpokladajme, že (3) platí pre $n = k$ a dokážeme platnosť (3) pre $n = k+1$. Budeme dokazovať sporom. Nech $|N_{k+1}| = |N_{k+2}|$. Potom existuje prosté zobrazenie f množiny $N_{k+1} = \{0,1,2,...,k\}$ na množinu $N_{k+2} = \{0,1,2,...,k+1\}$. Keďže f je zobrazenie na množinu N_{k+2}, tak existuje $l \in N_{k+1}$ taký, že $f(l) = k+1$. Definujeme nové zobrazenie g takto: $g(x) = f(x)$ pre $x \in N_{k+1}$, $x \neq l$ $x \neq k$, $g(l) = f(k)$ a $g(k) = k+1$, $g(k) = f(l)$. (Pozri obr. č. 8).



Obr.8.

Zobrazenie f sme „pozmenili“, tak aby zobrazovalo k na $k+1$. Zrejme g je prosté zobrazenie na množinu N_{k+2}. Naviac g zobrazuje proste množinu $N_k = N_{k+1} - \{k\}$ na množinu $N_{k+1} = N_{k+2} - \{k+1\}$ a to je spor s indukčným predpokladom.

Veta 2.10.4 Ak má množina n prvkov, $n \in N$, tak je konečná.

Dôkaz: Nech množina A má n prvkov, t.j. $|A| = |N_n|$, tak každá množina N_k je podmnožinou N, tak z lemy 2.10.2 dostávame $|A| = |N_n| < |N_{n+1}| \leq |N|$. Podľa vety, ktorú sme dokázali pre mohutnosti predtým platí , že $|A| < |N|$. Lema má aj iný dôležitý dôsledok.

Veta 2.10.5 Pre $n, m \in N$ je $|N_n| = |N_m|$ vtedy a len vtedy, keď $n = m$.

Dôkaz: Ak $n \neq m$, tak platí $n < m$, alebo $m < n$. Nech $n < m$. Potom z vlastnosti prirodzených čísel platí, že $1 + n \leq m$ a teda $N_{n+1} \subseteq N_m$. Podľa lemy 2.10.2 dostávame spor.

$$|N_n| < |N_{n+1}| \leq |N_m|.$$

Teda $|N_n| < |N_m|$. Nech obrátene $n = m$, tak potom $|N_n| = |N_m|$, existuje prosté zobrazenie f množiny N_n na N_m, stačí položiť $f(k) = k$, pre ľubovoľné $k \in N_n$.

Ukážeme teraz vetu obrátenú k vete 2.10.4. Najprv dve pomocné tvrdenia.

Lema 2.10.3 Ak $A \subseteq N_n$, tak existuje k také, že $|A| = k$.

Dôkaz: Urobíme matematickou indukciou

1° Ak $A \subseteq N_0 = \emptyset$, tak $A = \emptyset$ a $|A| = 0$

2° Nech tvrdenie platí pre n a $A \subseteq N_{n+1} = \{0,1,2,...,n\}$. Ak $n \notin A$, tak $A \subseteq N_n$ a podľa indukčného predpokladu existuje k také, že $|A| = k$.

Nech teda $n \in A$. Rozlíšime dva prípady.

1) $A = N_{n+1}$. Stačí položiť $k = n+1$, lebo $|A| = |N_{n+1}| = n+1$

2) $A \neq N_{n+1}$. Teda existuje $l \in N_{n+1}$, také, že $l \notin A$. Množina $A' = A - \{n\} \cup \{l\}$ má rovnakú mohutnosť ako množina A (stačí položiť $f(i) = i$, pre $i \in A, i \neq n$, $f(n) = l$ a máme prosté zobrazenie f množiny A na A' - porovnaj dôkaz lemy 1. Zrejme však $A' \subseteq N_n$. Potom podľa indukčného predpokladu existuje $k \in N$ také, že $k = |A'| = |A|$.

Lema 2.10.4 Ak množina $A \subseteq N$ je zhora neohraničená, tak $|A| = |N|$.

Dôkaz: Nech $A \subseteq N$ nie je zhora ohraničená, t.j.

$$(\forall n)(\exists m)(m \in A \wedge m > n). \qquad (4)$$

Zostrojíme prosté zobrazenie f z N na A takto. Nech $f(0)$ je najmenší prvok množiny A. Ak $f(n)$ máme už definované, tak $f(n+1)$ bude najmenší prvok množiny A väčší ako $f(n)$. Jeho existencia je určená podmienkou (4).

Zobrazenie f je prosté lebo pre každé $n \in N$ je $f(n) < f(n+1)$ a teda aj $f(n) \neq f(n')$ pre $n \neq n'$.

Z definície f vyplýva, že $f(n) \geq n$ (ľahko sa dokáže matematickou indukciou).

Nech $k \in A$. Z vlastnosti prirodzených čísel existuje $n \in N$ také, že $k \leq n \leq f(n)$. Nech n je najmenšie také prirodzené číslo, že $k \leq f(n)$. Ak $n = 0$, tak nutne $k = f(0)$, lebo $f(0)$ je najmenšie číslo z A). Nech $n \neq 0$, t.j. $n = l+1$. Potom $l < n$ a teda $f(l) < k$. Keďže $f(l+1) = f(n)$ je najmenšie číslo z množiny A väčšie ako $f(l), k \in A, k \leq f(n)$ tak nutne $k = f(n)$. Tým sme dokázali, že f je zobrazenie na množinu A.

Teraz ľahko ukážeme sľúbené tvrdenie.

Veta 2.10.6 Ak množina A je konečná, tak existuje také prirodzené číslo n, že $|A| = n$.

Dôkaz: Nech $|A| = |N|$. Teda existuje prosté zobrazenie množiny A do množiny N. Označme $B = h(A)$. Zrejme $|B| = |A|$ a teda $|B| < |N|$. Taktiež, $B \subseteq N$. Podľa lemy 2.10.4 množina B je zhora ohraničená, teda existuje prirodzené číslo m také, že $B \subseteq N_m$. Podľa lemy 2.10.3 existuje prirodzené číslo n také, že $n = |B| = |A|$.

Dôsledok 1. Množina A je konečná vtedy a len vtedy, ak existuje prirodzené číslo $n \in N$ také, že A má n prvkov.

Zistili sme, že prirodzené čísla sú práve mohutnosti konečných množín. Pojem konečnej množiny bol definovaný pomocou množiny prirodzených čísel. Ako uvidíme neskôr, konečnú množinu možno definovať bez použitia prirodzených čísel.

Prirodzené čísla vieme sčítať, násobiť a umocňovať. Mohutnosti (konečných) množín vieme tiež sčítať, násobiť a umocňovať. Vzniká prirodzená otázka, aký je vzťah medzi týmito operáciami. Upresníme ho. Nech A, B sú dve konečné množiny, kvôli jednoduchosti disjunktné, t.j. $A \cap B = \emptyset$. Podľa vety 2.10.6. existujú prirodzené čísla n, m také, že $|A| = n$, $|B| = m$. Otázka znie: platí $|A| + |B| \left(= |A \cup B|\right) = n + m$, $|A| \cdot |B| \left(= |A \times B|\right) = n \cdot m$, $|A|^{|B|} \left(= \left|A^B\right|\right) = n^m$?

V ďalšom ukážeme, že odpoveď na otázku je pozitívna. Najprv ukážeme, že sčítanie, násobenie a umocňovanie na množine prirodzených čísel je jednoznačne charakterizované, každé dvomi jednoduchými vlastnosťami.

Lema 2.10.5 Nech f je zobrazenie z $N \times N$ do N také, že pre každé $n, m \in N$ platí

$$f(n,0) = n \qquad (5)$$

$$f(n,m+1) = f(n,m)+1 \qquad (6)$$

Potom, pre každé $n,m \in N$ platí

$$f(n,m) = n+m \qquad (7)$$

Poznámka: Všimnime si najprv, že ak položíme $f(n,m) = n+m$; tak platí (5) a (6).

$$n+0 = n \qquad (8)$$

$$n+(m+1) = (n+m)+1 \qquad (9)$$

Lema tvrdí, že tieto dve rovnosti sčítanie prirodzených čísel jednoznačne charakterizujú.

Dôkaz lemy 2.10.5 Tvrdenie dokážeme matematickou indukciou. Nech $V(m)$ označuje výrok „pre každé $k \in N$ platí $f(k,m) = k+m$ “. Chceme ukázať, že pre každé $m \in N$ platí $V(m)$.

Keďže $k+0 = k$, tak $V(0)$ platí podľa (5). Predpokladajme, že platí $V(m)$, t.j. pre každé $k \in N$ platí

$$f(k,m) = k+m$$

Z rovnosti (6) dostávame

$$f(k,m+1) = f(k,m)+1 = k+(m+1) = (k+m)+1$$

Teda platí aj $V(m+1)$.

Lema 2.10.6 Nech g je zobrazenie z $N \times N$ do N také, že pre každé $n,m \in N$ platí

$$g(n,0) = 0 \qquad (10)$$

$$g(n,m+1) = g(n,m)+n \qquad (11)$$

Potom, pre každé $n,m \in N$ platí

$$g(n,m) = n+m \qquad (12)$$

Dôkaz: Podobne ako vyššie označíme výrok „pre každé $k \in N$ platí $g(k,m) = k \cdot m$“ ako $V(m)$. Podľa (10) platí $V(0)$. Ak predpokladáme $V(m)$, tak z (11) dostávame $g(k,m+1) = g(k,m)+k = k \cdot m + k = k(m+1)$. Teda platí aj výrok $V(m+1)$.

Úplne rovnako sa dokáže podobná vlastnosť umocňovania.

Lema 2.10.7 Nech h je zobrazenie z $N \times N$ do N také, že pre každé $n,m \in N$ platí

$$h(n,0) = 0 \qquad (13)$$

$$h(n,m+1) = h(n,m) \cdot n \qquad (14)$$

Potom, pre každé $n,m \in N$ platí

$$h(n,m) = n^m \qquad (15)$$

Môžeme teraz dokázať sľubené tvrdenie.

Veta 2.10.7 Nech A, B sú konečné množiny, $|A| = n$, $|B| = m$.

a) Ak A, B sú disjunktné, tak $|A \cup B| = n+m$

b) $|A \times B| = n \cdot m$

c) $|A^B| = n^m$

Dôkaz: a) Zostrojíme zobrazenie f takto: Nech $n,m \in N$. Ak množina $N_n \cup (N_m \times \{0\})$ je konečná a $|N_n \cup (N_m \times \{0\})| = k$, tak položíme $f(n,m) = k$. Ak $N_n \cup (N_m \times \{0\})$ nie je konečná, tak $f(n,m)$ nie je definovaná. V skutočnosti uvedená množina nikdy nie je nekonečná, ale ešte sme to nedokázali. Vyplynie to až z tejto vety.

Ukážeme matematickou indukciou, že f je definovaná na $N \times N$ a spĺňa podmienky (5) a (6).

Pre ľubovoľné $n \in N$ platí

$$N_n \cup (N_0 \times \{0\}) = N_n$$

Teda $f(n,0)$ je definované a $f(n,0) = n$, t.j. platí (5).

Predpokladajme, že pre každé $n \in N$ je definované $f(n,m)$. Nech $f(n,m) = k$. Vieme, že

$$N_{m+1} = N_m \cup \{m\}.$$

Teda

$N_n \cup (N_{m+1} \times \{0\}) = N_n \cup (N_m \times \{0\}) \cup \{(m,0)\}$. Podľa predpokladu platí

$$|N_n \cup (N_m \times \{0\})| = k,$$

t.j. existuje prosté zobrazenie φ množiny N_k na množinu $N_n \cup (N_m \times \{0\})$.
Ak doplníme

$$\varphi(k) = (m,0)$$

tak φ bude prosté zobrazenie množiny $N_{k+1} = N_k \cup \{k\}$ na množinu $N_n \cup (N_{m+1} \times \{0\})$. Teda $f(n,m+1)$ je definovaná a platí

$$f(n,m+1) = |N_n \cup (N_{m+1} \times \{0\})| = k+1 = f(n,m)+1.$$

Platí teda aj (6). Podľa lemy 2.10.5 platí rovnosť (7) a tá je ekvivalentná nášmu tvrdeniu.

b) Zobrazenie *g* definujeme takto $g(n,m) = k$, ak $|N_n \times N_m| = k$. Rovnako ako vyššie sa dokáže, že *g* je definované na $N \times N$ a platí (10) a (11). Stačí si uvedomiť, že

$$N_n \times N_{m+1} = (N_n \times N_m) \cup (N_n \times \{m\})$$

a $|N_n \times \{m\}| = |N_n|$.

c) Zase položíme $h(n,m) = k$ ak $\left|N_n^{\,N_m}\right| = k$. Ku dôkazu matematickou indukciou je potrebná rovnosť

$$\left|N_n^{\,N_{m+1}}\right| = \left|N_n^{\,N_m \cup \{m\}}\right| = \left|N_n^{\,N_m} \times N_n^{\,\{m\}}\right|.$$

Dôsledok 2. Ak A, B sú konečné množiny, potom $A \cup B$, $A \times B$, A^B, $\mathcal{P}(A)$ sú konečné množiny .

Dôkaz: Ak A, B sú konečné, aj $B - A$ je konečná. Podľa vety je $|A \cup B| = |A| + |B - A|$. Podobne $|A \times B| = |A| \cdot |B|$ a $\left|A^B\right| = |A|^{|B|}$. $\mathcal{P}(A)$ je konečná, lebo $|\mathcal{P}(A)| = 2^{|A|}$.

V ďalších úvahách bude užitočné toto tvrdenie.

Veta 2.10.8 Nech A_k, $1 \le k \le n$ sú množiny také, že

a) $|A_k| = m$ pre $1 \le k \le n$

b) $A_k \cap A_{k'} = \emptyset$ pre $k \ne k'$

Potom $\left|\bigcup_{k=1}^{n} A_k\right| = n \cdot m$.

Dôkaz: Urobíme matematickou indukciou. Pre $n = 1$ je tvrdenie triviálne pravdivé. Predpokladajme, že platí pre *n*. Potom

$$\bigcup_{k=1}^{n+1} A_k = \bigcup_{k=1}^{n} A_k \cup A_{n+1}$$

Podľa indukčného predpokladu platí

$$\left|\bigcup_{k=1}^{n} A_k\right| = n \cdot m .$$

Podľa vety 2.10.7 potom dostávame

$$\left|\bigcup_{k=1}^{n+1} A_k\right| = n \cdot m + m = (n+1) \cdot m$$

Podobným spôsobom môžeme dokázať aj nasledujúce tvrdenie.

Veta 2.10.9 Ak A_k, $1 \le k \le n$ sú disjunktné množiny, $|A_k| \ge m$ pre každé k, $1 \le k \le n$, potom

$$\left|\bigcup_{k=1}^{n} A_k\right| \ge n \cdot m .$$

Na začiatku tejto časti sme poznamenali, že konečná množina by mala mať Euklidovu vlastnosť „časť je menšia ako celok“. R. Dedekind túto vlasnosť vzal za základ pre definíciu konečnosti. Nebudeme sa týmto pojmom podrobnejšie zaoberať. Ukážeme však, že konečné množiny naozaj túto požadovanú vlastnosť majú. Najprv definícia. Množina A sa nazýva konečná podľa Dedekinda, ak pre každú množinu $X \subseteq A$, $X \neq A$ platí $|X| < |A|$.

Teraz ukážeme sľúbené tvrdenie.

Veta 2.10.10 Každá konečná množina je konečná podľa Dedekinda.

Dôkaz: Predpokladajme, že A je konečná množina, $|A| = n$ a nie je konečná podľa Dedekinda. Potom existuje množina $X \subseteq A$, $X \neq A$ taká, že $|X| = |A|$. Nech $a \in A - X$. Potom $|X \cup \{a\}| = n+1$ a $X \cup \{a\} \subseteq A$, t.j. $|X \cup \{a\}| \le |A| = n$, to je spor s tvrdením lemy 2.10.2 $\left(\forall n \in N, |N_n| < |N_{n+1}|\right)$.

2.11. Spočítateľné množiny

Definícia 2.11.1 Množina A sa nazýva **spočítateľná**, ak platí $|A| \leq_0 \aleph_0$, t.j. ak existuje prosté zobrazenie množiny A do množiny N – prirodzených čísel. Množina sa nazýva **nespočítateľná**, ak nie je spočítateľná.

Zrejme každá konečná množina je spočítateľná. Podmnožina spočítateľnej množiny je spočítateľná. Množina N je nekonečná spočítateľná. Podľa Cantorovej vety množina $P(N)$ je nespočítateľná.

Definícia 2.11.2 Budeme hovoriť, že množina A **sa dá zoradiť do postupnosti**, ak existuje zobrazenie množiny N na množinu A, t.j. ak existuje postupnosť $\{a_n\}_{n=0}^{\infty}$ taká, že $A = \{a_n, n \in N\}$.

Príklad 1. Každá podmnožina N je spočítateľná. Množina Z je spočítateľná, lebo $Z = N \cup \{-n, n \in N \wedge n > 0\}$. Keďže $|\{-n, n \in N \wedge n > 0\}| = |N| = \aleph_0$, tak $|Z| = \aleph_0 = \aleph_0 + \aleph_0$.

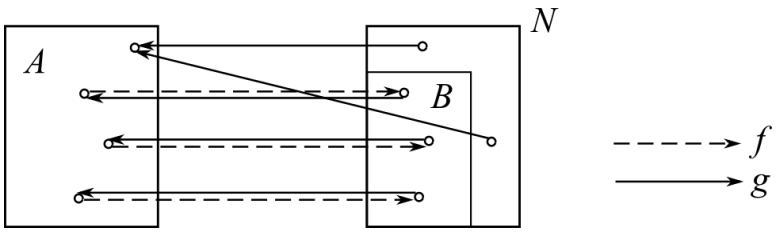
Príklad 2. Množinu $\langle 0,1\rangle \cap Q$ racionálnych čísel z intervalu $\langle 0,1\rangle$ ľahko zoradíme do postupnosti:
$$0, \frac{1}{1}, \frac{1}{2}, \frac{2}{2}, \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \ldots, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}, \ldots .$$

Pre praktické účely bude veľmi užitočná nasledujúca veta.

Veta 2.11.1 Neprázdna množina je spočítateľná vtedy a len vtedy, keď sa dá zoradiť do postupnosti.

Dôkaz: Nech A je neprázdna spočítateľná množina. Potom existuje prvok $a \in A$. Keďže $|A| \leq |N|$, tak existuje prosté zobrazenie f z A do N. Nech $B = f(A)$. Zobrazenie f je na množinu B a existuje inverzné zobrazenie $f^{-1} : B \to A$.

Zobrazenie g je zobrazenie množiny N na množinu A (pozri obr.č.1). Teda množina A sa dá zoradiť do postupnosti.



Obr. 1

Nech teraz naopak, A sa dá zoradiť do postupnosti, t.j. existuje zobrazenie h množiny N na množinu A. Označíme
$$C = \{n \in N, (\forall m)(m < n \to h(m) \neq h(n))\}.$$
Ak $n_1, n_2 \in C$ a napr. $n_1 < n_2$, tak nutne $h(n_1) \neq h(n_2)$. Teda zobrazenie $h \mid C$ je prosté. Ak $x \in A$, tak množina $\{n \in N, h(n) = x\}$ je neprázdna. Ak n je najmenší prvok tejto množiny, tak n je zrejme z množiny C. Takže h zobrazuje množinu C na množinu A. Podľa známych viet existuje zobrazenie $g = (h \mid C)^{-1} : A \to C \subseteq N$. Odtiaľ vyplýva, že $|A| \leq |N|$, t.j. A je spočítateľná množina.

Dôsledok 1. Ak existuje prosté zobrazenie f množiny A na množinu B a množina A je spočítateľná , potom aj množina B je spočítateľná.

Dôkaz: Ak A je prázdna aj B je prázdna teda spočítateľná. Ak A je neprázdna, tak podľa vety 2.11.1 existuje zobrazenie g množiny N na množinu A. Potom $f \circ g$ je zobrazenie N na množinu B a znovu podľa vety 2.11.1, množina B je spočítateľná.

Príklad 3. Podľa príkladu 2 množina $Q \cap \langle 0,1 \rangle$ je spočítateľná. Spočítateľnosť Z vyplýva podľa vety 2.11.1 tiež z toho, že ju ľahko vieme zoradiť do postupnosti

$$0, 1, -1, 2, -2, ..., n, -n, ...$$

Veta 2.11.2 Zjednotenie a karteziánsky súčin dvoch spočítateľných množín sú spočítateľné množiny.

Dôkaz: Nech A, B sú spočítateľné množiny. Ak aspoň jedna z nich, napríklad B je prázdna, tak tvrdenie je triviálne pravdivé, lebo

$$A \cup \emptyset = A, \quad A \times B = \emptyset$$

Predpokladajme, že obidve množiny A, B sú neprázdne. Potom obidve sa dajú zoradiť do postupnosti, t.j. existujú zobrazenia f, g a h, také že $f(N) = A$, $g(N) = B$.

Množinu $A \cup B$ môžeme potom zoradiť do postupnosti takto:

$$f(0), g(0), f(1), g(1), ..., f(n), g(n), ...$$

t.j. položíme

$$h(n) = f\left(\frac{n}{2}\right), \text{ pre } n \text{ párne},$$

$$h(n) = g\left(\frac{n-1}{2}\right), \text{ pre } n \text{ nepárne}.$$

Zrejme $h : N \to A \cup B$ je zobrazením na (ak $x \in A$, existuje n také, že $f(n) = x$ a potom $h(2n) = f(n) = x$, podobne pre $x \in B$, $h(2n+1) = g(n) = x$).

Podľa vety, ktorú sme dokázali už skôr existuje prosté zobrazenie π množniny N na $N \times N$. Ak $n \in N$, tak $\pi(n)$ je nejaká usporiadaná dvojica (k,l). Položíme

$$j(n) = (j(k), g(l)).$$

Zobrazenie j je zobrazenie množiny N na množinu $A \times B$. Ak totiž $z \in A \times B$, tak $z = (x,y)$, $x \in A$ a $y \in B$. Predpokladali sme $f(N) = A$ a $g(N) = B$. Teda existujú $k, l \in N$, také, že $f(k) = x$, $g(l) = y$. Nech $n \in N$ je také, že $\pi(n) = (k,l)$. Potom

$$j(n) = (f(k), g(l)) = (x,y) = z.$$

Príklad 4. Množina Q racionálnych čísel je spočítateľná. Podľa definície, množina Q je množina všetkých čísel tvaru $\frac{z}{n}$, kde $z \in Z$ a $n \in N$, $n \neq 0$. Teda zobrazenie f definované predpisom

$$f((z,n)) = \frac{z}{n+1} \text{ pre } z \in Z,\ n \in N$$

zobrazuje množinu $Z \times N$ na množinu Q. Tvrdenie vyplýva z vety 2.11.2 a dôsledku 1.

Veta 2.11.3 Zjednotenie spočítateľne mnoho spočítateľných množín je spočítateľná množina.

Dôkaz: Nech $A_n, n \in N$ sú spočítateľné množiny (je ich spočítateľne mnoho, teda sú zoradené do postupnosti). Chceme ukázať, že množina

$$A = \bigcup_{n=0}^{\infty} A_n$$

je spočítateľná. Bez ujmy na všeobecnosti môžeme predpokladať, že každá množina A_n je neprázdna (prázdnu by sme „vynechali“). Pre každé n potom existuje zobrazenie f_n množiny N na množinu A_n.

Nech zase π je zobrazenie N na $N \times N$. Ak $\pi(n) = (k,l)$, tak položíme

$$f(n) = f_k(l).$$

Ak $x \in A$, tak existuje také k, že $x \in A_k$. Zobrazenie f_k je na množinu A_k a teda existuje $l \in N$ také, že $f_k(l) = x$. Nech $n \in N$ je také, že $\pi(n) = (k,l)$. Potom

$$f(n) = f_k(l) = x.$$

Teda f je zobrazenie množiny N na množinu A.

Príklad 5. Nech F je množina všetkých konečných postupností prirodzených čísel.Ukážeme, že F je spočítateľná množina. Označíme

$$F_n = N^{N_n}$$

t.j. F_n je množina n-prvkových postupností prirodzených čísel. Potom platí

$$F = \bigcup_{n=0}^{\infty} F_n.$$

Zrejme $F_0 = \{\varnothing\}$. Ďalej $|F_1| = |N|$. Indukciou dostávame podľa viet predchádzajúcich častí a vety 2.11.2:

$$|F_{n+1}| = \left|N^{N_{n+1}}\right| = |N|^{|N_{n+1}|} = |N|^{|N_n|+|\{n\}|} = |N|^{|N_n|}.|N| = |F_n| \cdot |N| = |N| \cdot |N| = |N|.$$

Podľa vety 2.11.3 je $|F| = |N|$.

Príklad 6. Nech K je množina všetkých konečných podmnožín množiny N. Zobrazenie Φ z F na K definujeme takto; ak $f \in F$, t.j. f je funkcia z nejakého N_n do N, tak $\Phi(f) = f(N_n)$. Zrejme Φ je zobrazenie množiny F – spočítateľnej na množinu K. Podľa príkladu 5 a dôsledku 1 množina F je spočítateľná a množina K je taktiež spočítateľná.

Zrejme v obidvoch príkladoch množina N môže byť nahradená ľubovoľnou spočítateľnou množinou a tvrdenia zostanú pravdivé.

Príklad 7. Reálne číslo x sa nazýva algebraické, ak existujú také celé čísla $a_0, a_1, a_2, ..., a_n$, že pre x platí

$$a_0 + a_1 x + a_2 x^2 + ... + a_n x^n = 0.$$

Nech $f : N_n \to Z$ je n-prvková postupnosť celých čísel. Označíme

$$P_f = \{x \in R, f(0) + f(1)x + ... + f(n-1)x^{n-1} = 0\}.$$

Množina všetkých algebraických čísel sa dávyjadriť takto:

$$A \cup \left\{ P_f,\ f \in \bigcup_{n=0}^{\infty} Z^{N_n} \right\}.$$

Z – spočítateľná množina, Z^{N_n} - spočítateľná množina $\bigcup_{n=0}^{\infty} Z^{N_n}$ - spočítateľná množina. Každá P_f - spočítateľná (dokonca konečná) množina a teda množina A – algebraických čísel je spočítateľná množina.

Príklad 8. Ukážeme, že interval $\langle 0,1 \rangle$ nie je spočítateľná množina.

Dokážeme to sporom, predpokladajme, že interval $\langle 0,1 \rangle$ je spočítateľná množina a možno ho zoradiť do postupnosti

$$\langle 0,1 \rangle = \{a_n,\ n \in N\}.$$

Každé číslo a_n má dekadický zápis $a_n = \sum_{k=0}^{\infty} a_{nk}.10^{-k-1}$. Ak $a_n \neq 0$, tak vyberieme ten zápis, ktorý nemá samé nuly od určitého miesta, t.j. nie je konečný. Čísla a_n, $n \in N$ môžeme zoradiť do tabuľky – pozri obr.č.2. Teraz použijeme ***metódu Cantorovej diagonály***.

$a_0 = 0$	a_{00}	a_{01}	a_{02}	a_{03}	a_{04}	... a_{0n}	...
$a_1 = 0$	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	... a_{1n}	...
.	.	.	.	.	.		
.	.	.	.	.	.		
.	.	.	.	.	.		
$a_n = 0$	a_{n0}	a_{n1}	a_{n2}	a_{n3}	a_{n4}	... a_{nn}	...
.	.	.	.	.	.	.	
.	.	.	.	.	.	.	
.	.	.	.	.	.	.	

Obr. 2

Nech $b_n = 9$ ak $a_{nn} = 1$ a $b_n = 1$ ak $a_{nn} \neq 1$. Teda pre každé n platí

$$b_n \neq a_{nn} \qquad (*)$$

Číslo $b = \sum_{k=0}^{\infty} b_k.10^{-k-1}$ patrí do intervalu $\langle 0,1 \rangle$. Teda existuje $m \in N$, že $b = a_m$. Dekadický zápis čísla b je $0, b_0\, b_1\, b_2 \ldots b_n \ldots$ a neobsahuje nulu vôbec. Dekadický zápis čísla a_m je $0, a_{m0}\, a_{m1}\, a_{m2} \ldots a_{mn} \ldots$. Číslo a_m síce môže mať dva rôzne dekadické zápisy, my sme však vybrali ten, ktorý nie je konečný. Ani zápis $0, b_0\, b_1\, b_2 \ldots b_n \ldots$ nie je konečný (neobsahuje 0 vôbec). Keďže $a_m = b$, tak z uvedeného vyplýva, že obidva zápisy musia byť totožné, t.j. $b_k = a_{mk}$ pre každé $k \in N$. Pre $k = m$ dostávame

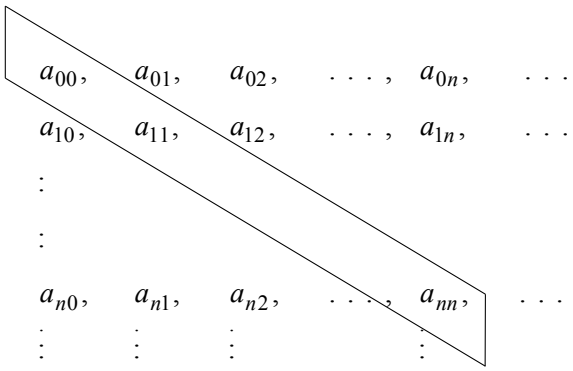
$$b_m = a_{mm},$$

čo je spor s (*).

Veta 2.11.4 (Cantorova) Množina všetkých reálnych čísel je nespočítateľná.

Dôkaz: Predpokladajme, že množina R je spočítateľná., keďže $|R| = |(0,1)|$ a $|(0,1)| = |\langle 0,1 \rangle|$, platilo by, že aj interval $\langle 0,1 \rangle$ je spočítateľná množina, čo je spor s predchádzajúcim príkladom.

Príklad 9. Množina všetkých postupností z prvkov množiny $\{0,1\}$ je nespočítateľná. Budeme pri dôkaze postupovať podobne ako v predchádzajúcom príklade. Predpokladajme, že množina uvažovaných postupností je spočítateľná, jej prvky môžeme zoradiť do tabuľky – pozri obr.č.3.- a použijeme Cantorovu diagonalizačnú metódu.



Obr. 3

Nech $b=\{b_0, b_1, b_2, ..., b_n, ...\}$ je postupnosť prvkov množiny $\{0,1\}$ definovaná takto: $b_{nn}=1-a_{nn}$. Ľahko vidno, že je rôzna od všetkých postupností, zapísaných vo vyššie uvedenej tabuľke, presnejšie $b \neq a_n$, $a_n=\{a_{ni}\}_{i=0}^{\infty}$, pre každé $n \in N$. To je spor.

2.9. - 2.11. CVIČENIA

1) Množina N všetkých prirodzených čísel je spočítateľná. Dokážte.

2) Množina $N^+=\{1,2,...,n,...\}$ je spočítateľná. Dokážte.

3) Množina Z celých čísel je spočítateľná. Dokážte.

4) Množiny N a N^+ majú rovnakú mohutnosť. Dokážte.

5) Množiny R a R^+ majú rovnakú mohutnosť. Dokážte.

6) Množiny $A=\{0,1,2\}$ a $B=\{a,b,c\}$ majú rovnakú mohutnosť. Zdôvodnite.

7) Intervaly $(0,1)$ a $(-\infty,0)$ majú rovnakú mohutnosť. Dokážte.

8) Interval $(1,\infty)$ a R^+ majú rovnakú mohutnosť. Dokážte.

9) Dokážte, že všetky intervaly (a,∞), kde a je reálne číslo, majú rovnakú mohutnosť.

10) Dokážte, že množina $\{x \mid x=3k+1,\ k \in N\}$ je spočítateľná.

11) Nech M je množina všetkých matíc stupňa 2, tvaru $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, kde $a,b \in N$. Dokážte, že M je spočítateľná.

12) Nech A je konečná množina. Potom platí:

a) Ak $f: A \to A$ je injektívne zobrazenie, tak f je aj surjektívne zobrazenie na množinu A.

b) Ak $f: A \to A$ je surjektívne zobrazenie, tak f je aj injektívne zobrazenie.

13) Dokážte, že:

a) Každá podmnožina konečnej množiny je konečná.

b) Zjednotenie konečného počtu konečných množín je konečná množina.

c) Karteziánsky súčin konečného počtu konečných množín je konečná množina.

14) a) Dokážte, že každá vlastná podmnožina konečnej množiny má mohutnosť menšiu ako množina.

b) Dokážte, že dve konečné množiny majú rovnakú mohutnosť práve vtedy, keď obsahujú rovnaký počet prvkov.

15) Dokážte, že z každej nekonečnej množiny možno vybrať spočítateľnú nekonečnú množinu.

16) Dokážte, že množina je nekonečná vtedy a len vtedy, keď má rovnakú mohutnosť ako jej niektorá podmnožina.

17) Dokážte, že množina všetkých postupností z 0 a 1 je nespočítateľná množina.

18) Dokážte, že interval $(0,1)$ je nespočítateľná množina.

Záver

Prirodzené východisko pre štúdium informatiky predstavujú matematická logika a taká jej príbuzná disciplína ako je teória množín.

Predložený učebný text je určený predovšetkým študentom prvého ročníka študijného odboru informatika, ale môže byť užitočný aj pre študentov rôznych matematických odborov.

Snahou autora bolo, usiloval sa napísať text, čo najzrozumiteľnejšie a pritom čo najpresnejšie, berúc do úvahy skutočnosť, že sa dnes žiaci s istými pojmami oboznamujú na základnej a strednej škole. Skriptá sú určené predovšetkým študentom, ktorí už viac-menej poznajú základné pojmy a je pre nich nevyhnutné si svoje znalosti v danej oblasti doplniť a prehĺbiť, správne pochopiť a rozumieť jazyku, ktorým matematika hovorí o abstraktných objektoch. Nezaoberáme sa axiomatickou výstavbou logiky a teórie množín, ani ich históriou a filozofiou.

Pri spracovaní a usporiadaní textu sme smerovali dosiahnuť čo najväčšiu logickú nadväznosť a to ako vo vnútri jednotlivých častí, tak i medzi jednotlivými časťami.

Patričnú pozornosť sme venovali výberu príkladov jednak riešených i príkladov uvádzaných na konci jednotlivých článkov na precvičenie si učiva. Na ich vyriešenie spravidla postačí použiť postup, ktorý je explicitne uvedený alebo naznačený v texte. V tomto smere v nadväznosti na predložený učebný text má autor rozpracovanú Zbierku úloh z diskrétnej matematiky, ktorá okrem úloh dotýkajúcich sa problematiky predloženého textu obsahuje úlohy a cvičenia z takých konkrétnych diskrétnych štruktúr ako sú kombinatorické a grafové štruktúry, ktoré sa hojne využívajú v informatike. Pričom každá časť zbierky je štruktúrovaná tak, že najprv sú uvedené základné pojmy, tvrdenia, riešené úlohy, úlohy s návodmi na riešenie a cvičenia s výsledkami.

Domnievam sa, že oba tieto texty budú užitočnou učebnou pomôckou preusilovných študentov na zvládnutie netriviálneho, no veľmi potrebného metodického nástroja abstrakcie ako je analýza a syntéza.

Resumé

Predložený text predstavuje úvod do výrokovej logiky a teórie množín na intuitívnej úrovni. Obsah zodpovedá prednáškam z predmetu diskrétna matematika pre študentov prvého ročníka odboru informatika.

V 1. časti Základy matematickej logiky je vyložený pojem výroku, pravdivostná hodnota výroku, zložené výroky, základné logické spojky, tabuľky pravdivostných hodnôt. Tautológia, kontradikcia, splniteľnosť výroku, dôležité tautológie, logické zákony a pravidlá. Kvantifikované výroky a operácie s nimi, pojem logického dôsledku.

V časti 1.a Základné metódy dôkazov v matematike sa zaoberáme pojmom matematického dôkazu, vysvetlujeme priamy dôkaz tvrdenia, nepriamy dôkaz sporom, priamy dôkaz implikácie, nepriamy dôkaz implikácie sporom a obmenou. Dôkaz matematickou indukciou. Všetky typy dôkazov sú ilustrované príkladmi.

V 2. časti Úvod do teórie množín sú najprv definované základné pojmy a označenia, množinové operácie a vzťahy, vlastnosti množinových operácii, pojem usporiadanej dvojice a karteziánskeho súčinu, relácie z množiny do množiny, na množine, skladanie relácii, inverzná relácia. Dôležité relácie na množine, relácia ekvivalencia a rozklad množiny, čiastočné usporiadanie a usporiadanie množiny, ako špeciálny typ relácie pojem zobrazenia. Nakoniec je vyložený pojem mohutnosti množiny, počítanie s mohutnosťami, konečné, spočítateľné a nespočítateľné množiny. Každá časť obsahuje riešené aj neriešené príklady uvádzané ako cvičenia.

Autor pracuje nad Zbierkou príkladov z diskrétnej matematiky, ktorá nadväzuje na predložený text s množstvom riešených a neriešených príkladov, návodov na riešenie a výsledkami riešení. Jej obsah je rozšírený o príklady z kombinatoriky a teórie grafov.

Literatúra

1) BIRKHOFF, G., BARTE, E.: Aplikovaná algebra. Alfa, Bratislava 1981. 389s.
2) BUKOVSKÝ, L.: Teória množín. Rektorát Univerzity P. J. Šafárika v Košiciach, 1980. 274 s.
3) BEČVAŘ, J. a kol.: Seznamujeme se s množinami. SNTL, Praha 1982. 176 s.
4) GALANOVÁ, J., KAPRÁLIK, P.: Diskrétna matematika. Fakulta elektrotechniky a informatiky, STU, Bratislava 1997. 144 s.
5) HAUPT, D.: Množinový počet zrozumiteľne. Alfa, Bratislava 1984. 145 s.
6) JABLONSKIJ, S. U.: Úvod do diskrétnej matematiky. Alfa, Bratislava 1984. 278 s.
7) JENDROĽ, S. a MIHÓK, P.: Diskrétna matematika I. Prírodovedecká fakulta UPJŠ, Košice 1992. 135 s.
8) KOLÁŘ, J., ŠTĚPÁNKOVÁ, O., CHYTIL, M.: Logika, algebry a grafy. SNTL, Alfa, Praha 1989. 434 s.
9) KOSMÁK, L.: Množinová algebra. Alfa, Bratislava 1978. 107 s.
10) MEDEK V. a kol.: Matematická terminológia. SPN, Bratislava 1975. 144 s.
11) OLEJÁR, D., ŠKOVIERA, M.: Diskrétna matematika I. Matematicko – fyzikálna fakulta UK, Bratislava 1991. 195 s.
12) PREPARATA, F. P.; YEH, R. T.: Úvod do teórie diskrétnych matematických štruktúr. Alfa, Bratislava 1982. 328 s.
13) SOCHOR, A.: Klasická matematická logika. Univerzita Karlova v Prahe, Nakladatelsví Karolínum, 2001. 403 s.
14) ŠALÁT, T., SMÍTAL, J.: Teória množín. Alfa, Bratislava 1986. 217 s.
15) ŠVEJDAR, V.: Logika, neúplnost, zložitost a nutnost. Academia, Praha 2002. 464 s.