Úvod do Matematiky

Lev Bukovský

Katedra matematickej informatiky, Prírodovedecká fakulta UPJŠ

Košice, 2001

Obsah

1 Výrok

Výrok je gramatická veta, ktorá je pravdivá alebo nepravdivá. Hovoríme, že výrok má **pravdivostnú hodnotu: pravdivý, nepravdivý**. Píšeme 1, 0 alebo P, N.

Z daných výrokov môžeme utvoriť výroky nové pomocou logických operácií. Ak máme výrok $\mathcal{V}$, tak jeho **negácia** $\neg\mathcal{V}$ je výrok "Neplatí $\mathcal{V}$". Ak máme dva výroky $\mathcal{V}$, $\mathcal{W}$, tak môžeme utvoriť:

konjunkciu	$(\mathcal{V} \wedge \mathcal{W})$	$\mathcal{V}$ a $\mathcal{W}$.
disjunkciu	$(\mathcal{V} \vee \mathcal{W})$	$\mathcal{V}$ alebo $\mathcal{W}$.
implikáciu	$(\mathcal{V} \rightarrow \mathcal{W})$	Ak $\mathcal{V}$ tak $\mathcal{W}$.
ekvivalenciu	$(\mathcal{V} \equiv \mathcal{W})$	$\mathcal{V}$ vtedy a len vtedy, keď $\mathcal{W}$.

Vonkajšie zátvorky obyčajne vynecháme, napríklad $\mathcal{V} \wedge \mathcal{W}$, ale $(\mathcal{V} \wedge \mathcal{W}) \rightarrow \mathcal{Z}$.

Fakt: *Pravdivostná hodnota výroku utvoreného z iných výrokov pomocou logických operácií je určená pravdivostnými hodnotami týchto výrokov a nezávisí od ich obsahu.*

To nám umožňuje utvoriť známe tabuľky.

$\mathcal{V}$	$\mathcal{W}$	$\mathcal{V} \wedge \mathcal{W}$	$\mathcal{V} \vee \mathcal{W}$	$\mathcal{V} \rightarrow \mathcal{W}$	$\mathcal{V} \equiv \mathcal{W}$	$\neg\mathcal{V}$
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

V hovorovej reči logické operácie nie vždy vyjadrujeme pomocou uvedených oficiálnych spojok. Často používame iné vyjadrenie.

Negácia $\neg\mathcal{V}$:
"Nie $\mathcal{V}$"."Nie je pravda $\mathcal{V}$". Často negovanú vetu gramaticky upravíme.

Konjunkcia $\mathcal{V} \wedge \mathcal{W}$:
"$\mathcal{V}$ a súčasne $\mathcal{W}$". "Platia obidve $\mathcal{V}$ a $\mathcal{W}$". Často napíšeme len "$\mathcal{V}$, $\mathcal{W}$".

Disjunkcia $\mathcal{V} \vee \mathcal{W}$:
Je väčšinou vyjadrená pomocou spojky "alebo" a rozumie sa v nevylučovacom zmysle, t.j. je pravdivá aj keď sú pravdivé obidva výroky $\mathcal{V}, \mathcal{W}$. Pre vylučovací zmysel používame spojky "Buď... alebo ." Aj keď podľa pravidiel slovenskej gramatiky sa má hovoriť "Buď... buď... ." alebo "Alebo ... alebo ... .", matematika má výnimku. Iné možné vyjadrenie disjunkcie v nevylučovacom zmysle: "Platí aspoň jedna z $\mathcal{V}, \mathcal{W}$".

Implikácia $\mathcal{V} \rightarrow \mathcal{W}$:
"Za predpokladu $\mathcal{V}$ platí $\mathcal{W}$"."$\mathcal{W}$ ak $\mathcal{V}$".

Ekvivalencia $\mathcal{V} \equiv \mathcal{W}$: "$\mathcal{V}$ práve vtedy, keď $\mathcal{W}$".

Ak matematik vysloví alebo napíše výrok, tak obyčajne zamlčí predpoklad, že povedal alebo napísal pravdivý výrok. To sa pokladá v danom kontexte za samozrejmé. V takomto prípade však zvykneme použiť iné výrazové prostriedky. Je potrebné rozlišovať medzi implikáciou (ekvivalenciou) ako logickou operáciou a vyslovením pravdivej implikácie (ekvivalencie). V tomto prípade implikáciu vyjadrujeme "$\mathcal{V}$ implikuje $\mathcal{W}$", "$\mathcal{W}$

vyplýva z $\mathcal{V}$", "$\mathcal{V}$ je postačujúca podmienka pre $\mathcal{W}$", "$\mathcal{W}$ je nutná[1] podmienka pre $\mathcal{V}$". Pravdivú ekvivalenciu vyjadrujeme "$\mathcal{V}$ je ekvivalentné $\mathcal{W}$".

V definícii ekvivalenciu vyjadrujeme stručne "$\mathcal{V}$ ak $\mathcal{W}$".

Ešte jednu poznámku k vyjadreniu konjunkcie. Ak matematik chce napísať, že konjunkcia $\mathcal{V} \wedge \mathcal{W}$ je pravdivá, tak napíše $\mathcal{V}$, $\mathcal{W}$.

Niektoré výroky sú pravdivé vďaka svojmu tvaru, teda nezávisle od obsahu. Nazývajú sa **tautológie**. Napríklad výroky tvaru

$$\mathcal{V}_1 \to (\mathcal{V}_2 \to \mathcal{V}_1), \qquad (\mathcal{V}_1 \to \mathcal{V}_2) \to ((\mathcal{V}_2 \to \mathcal{V}_3) \to (\mathcal{V}_1 \to \mathcal{V}_3),$$

$$\mathcal{V}_1 \to (\mathcal{V}_2 \to (\mathcal{V}_1 \wedge \mathcal{V}_2)), \qquad (\mathcal{V}_1 \to \mathcal{V}_3) \to ((\mathcal{V}_2 \to \mathcal{V}_3) \to ((\mathcal{V}_1 \vee \mathcal{V}_2) \to \mathcal{V}_3))$$

sú tautológie – sú pravdivé nezávisle od toho, aké sú výroky $\mathcal{V}_1$, $\mathcal{V}_2$ a $\mathcal{V}_3$ (čo označujú a či sú pravdivé ale nie).

2 Výroková funkcia a kvantifikátory

Gramatická veta, ktorá závisí od niekoľkých premenných, sa nazýva **výroková funkcia**, ak po adekvátnom dosadení konkrétnych objektov (presnejšie, ich názvov) za tieto premenné dostaneme výrok. Z daných výrokových funkcií môžeme pomocou logických operácií utvoriť nové výrokové funkcie rovnako, ako vytvárame nové výroky. Ak $\mathcal{V}(x, y)$ a $\mathcal{W}(x, z)$ sú výrokové funkcie (závislé na premenných x, y a x, z), tak môžeme utvoriť konjunkciu $\mathcal{V}(x, y) \wedge \mathcal{W}(x, z)$, ktorá závisí na premenných x, y, z. Podobne môžeme utvoriť nové výrokové funkcie

$$\mathcal{V}(x, y) \vee \mathcal{W}(x, z), \quad \mathcal{V}(x, y) \to \mathcal{W}(x, z), \quad \mathcal{V}(x, y) \equiv \mathcal{W}(x, z), \quad \neg\mathcal{V}(x, y).$$

Pre používanie zátvoriek platia rovnaké dohody ako v prípade výrokov.

Ak $\mathcal{V}(x, y_1, \ldots, y_k)$ je výroková funkcia premenných $x, y_1, \ldots, y_k$, tak výrokovú funkciu "Pre každé x platí $\mathcal{V}(x, y_1, \ldots, y_k)$" zapíšeme jednoducho

$$(\forall x)\, \mathcal{V}(x, y_1, \ldots, y_k). \tag{2.1}$$

Táto výroková funkcia už nezávisí od premennej x. Tú istú výrokovú funkciu môžeme vyjadriť aj vetou "Pre každé u platí $\mathcal{V}(u, y_1, \ldots, y_k)$". Naviac, ak do výrokovej funkcie (2.1) môžeme za premenné $y_1, \ldots, y_k$ dosadiť nejaké konkrétne objekty, za premennú x nemôžeme dosadzovať.

Podobne výrokovú funkciu "Existuje x také, že platí $\mathcal{V}(x, y_1, \ldots, y_k)$ " zapíšeme jednoducho

$$(\exists x)\, \mathcal{V}(x, y_1, \ldots, y_k). \tag{2.2}$$

Ani táto výroková funkcia nezávisí od premennej x a za túto premennú do výrokovej funkcie (2.2) nemôžeme dosadzovať.

Matematici často šetria písanie a nepíšu zátvorky okolo kvantifikátorov. Je to vec individuálnej dohody, pokiaľ to nevedie k nedorozumeniu (najčastejšie k nejednoznačnosti). Výrokové funkcie (2.1) a (2.2) sa často skrátene píšu napríklad takto:

$$\forall x : \mathcal{V}(x, y_1, \ldots, y_k), \qquad \exists x : \mathcal{V}(x, y_1, \ldots, y_k).$$

Uvažujme číselný výraz

$$\sum_{i=n}^{m} i^2. \tag{2.3}$$

[1] Aj keď odborníci na slovenský jazyk dlho namietali proti termínu "nutná" a tvrdili, že je to "nevyhnutná podmienka", dnes v slovníkoch slovenského jazyka sa vyskytuje slovo "nutný". Teda matematici môžu znovu hovoriť o nutnej podmienke.

Tento výraz závisí od čísiel n, m a nezávisí od premennej i. Naviac, za premenné n, m môžeme dosadiť nejaké konkrétne prirodzené (alebo celé) čísla. Za premennú i nemôžeme dosadzovať. Premennú i môžeme vo všetkých jej výskytoch premenovať a výraz sa nezmení:

$$\sum_{i=n}^{m} i^2 = \sum_{j=n}^{m} j^2 = \sum_{\square=n}^{m} \square^2 = \sum_{\heartsuit=n}^{m} \heartsuit^2.$$

Číselný výraz (2.3) vieme opísať aj bez použitia premennej i, napríklad takto: "(2.3) je súčet druhých mocnín čísiel od n po m". Podobne je to aj s premenou x vo výraze

$$\int_a^b x^2\,dx.$$

Hovoríme, že premenná x (v prípade výrazu (2.3) premenná i) je **viazaná**. Premenné, ktoré sa vyskytujú vo výrokovej funkcii a nie sú viazané, sú **voľné**. Operátor $\forall$ sa nazýva **veľký** alebo **všeobecný kvantifikátor** a $\exists$ sa nazýva **malý** alebo **existenčný kvantifikátor**. Kvantifikátor premennú **viaže**, teda mení ju z voľnej na viazanú. Ak viazanú premennú vo všetkých jej výskytoch nahradíme premennou, ktorá sa ešte v danej situácii nevyskytla, tak sa výroková funkcia nezmení. Za viazanú premennú nemôžeme dosadzovať. Výroková funkcia závisí od voľných premenných, nezávisí od viazaných premenných.

Príklad 2.1 Ak nahradíme každý výskyt premennej x premennou z, tak sa daný výraz alebo výroková funkcia nezmení:

$$\int_0^1 x^2\,dx, \qquad \sum_{x=0}^{n} \frac{1}{x^2}, \qquad (\forall x)\, x^2 \geq 0, \qquad (\forall x)(\exists y)\, x + y = a$$

$$\int_0^1 z^2\,dz, \qquad \sum_{z=0}^{n} \frac{1}{z^2}, \qquad (\forall z)\, z^2 \geq 0, \qquad (\forall z)(\exists y)\, z + y = a$$

Naproti tomu dosadenie za viazanú premennú dáva nezmysel:

$$\int_0^1 7^2\,d7, \qquad \sum_{3=0}^{n} \frac{1}{3^2}, \qquad (\forall 1)\, 1^2 \geq 0, \qquad ,(\forall 0)(\exists y)\, 0 + y = a$$

Ak urobíme konjunkciu výrokových funkcií

$$x^2 > 3, \qquad (\forall x)(\exists y)\,(x + y < z)$$

tak vo výrokovej funkcii

$$x^2 > 3 \wedge (\forall x)(\exists y)\,(x + y < z) \tag{2.4}$$

premenná x sa vyskytuje dvojako: pred spojkou $\wedge$ je voľná a po spojke $\wedge$ je viazaná. Môže to spôsobiť nedorozumenie a preto sa takejto kolízii vyhýbame. Podľa potreby viazané premenné najprv premenujeme a až potom utvoríme konjunkciu. Výrokovú funkciu (2.4) môžeme bez kolízie premenných vyjadriť napríklad takto:

$$x^2 > 3 \wedge (\forall u)(\exists y)\,(u + y < z).$$

Niekedy je výhodné, aby niekoľko výrokových funkcií záviselo od tých istých premenných. Dosiahneme to **fiktívnymi** voľnými premennými. Napríklad výroková funkcia $(\forall x)\,(x^2 + y = z)$ závisí od voľných premenných y, z. Môžeme však povedať, že je to výroková funkcia premenných u, y, z. Ak by sa to niekomu zdalo divné, stačí

pôvodnú výrokovú funkciu nahradiť výrokovou funkciou $(\forall x)\,(x^2 + y = z) \wedge u = u$, ktorá je s ňou ekvivalentná. Posledná zrejme závisí od premenných u, y, z, aj keď od u len fiktívne.

Všeobecný kvantifikátor $(\forall x)$ často vyjadrujeme slovami:
"pre ľubovoľné x", "pre všetky x", "pre akékoľvek x". Ak nasleduje záporná veta, tak slovenčina si vyžaduje vyjadrenie "pre žiadne x".

Existenčný kvantifikátor $(\exists x)$ často vyjadrujeme slovami:
"pre nejaké x", "nájde sa také x, že", "aspoň pre jedno x".

Gramaticky správne vyjadrenie všeobecného kvantifikátora v zápornom prípade slovami "pre nijaké x" nie je vhodné, lebo je ľahko zameniteľné so svojím opakom "pre nejaké x". Nie je tam žiadna redundancia informácie[2]!

Matematika často používa kvantifikátory s podmienkou. Podmienený veľký kvantifikátor

$$(\forall x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$$

je skratka výrokovej funkcie

$$(\forall x)\,(\mathcal{V}(x) \to \mathcal{W}(x, y_1, \ldots, y_k))$$

a podmienený malý kvantifikátor

$$(\exists x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$$

je skratka výrokovej funkcie

$$(\exists x)\,(\mathcal{V}(x) \wedge \mathcal{W}(x, y_1, \ldots, y_k)).$$

Príklad 2.2 Definícia limity postupnosti, by mala byť formulovaná takto:

$$\lim_{n\to\infty} a_n = a \text{ ak } (\forall \varepsilon)\,(\varepsilon > 0 \to (\exists n_0)(\forall n)\,(n > n_0 \to |a_n - a| < \varepsilon)).$$

Táto neprehľadná forma sa dá prehľadnejšie napísať pomocou kvantifikátorov s podmienkou takto:

$$\lim_{n\to\infty} a_n = a \text{ ak } (\forall \varepsilon, \varepsilon > 0)(\exists n_0)(\forall n, n > n_0)\,(|a_n - a| < \varepsilon).$$

Matematici to napíšu spravidla ešte jednoduchšie

$$\lim_{n\to\infty} a_n = a \text{ ak } (\forall \varepsilon > 0)(\exists n_0)(\forall n > n_0)\,(|a_n - a| < \varepsilon).$$

Podobne, ako v prípade výrokov, existujú výrokové funkcie, ktoré sú pravdivé vďaka svojmu tvaru pre ľubovoľné hodnoty premenných. Najjednoduchšími príkladmi takýchto výrokových funkcií sú výrokové funkcie, ktoré vznikli z výrokov – tautológií, napríklad

$$(\mathcal{V}_1(x) \to \mathcal{V}_3(x)) \to ((\mathcal{V}_2(x) \to \mathcal{V}_3(x)) \to ((\mathcal{V}_1(x) \vee \mathcal{V}_2(x)) \to \mathcal{V}_3(x))).$$

Existujú aj iné výrokové funkcie, ktoré sú takto pravdivé, napríklad

$$(\forall x)\,\mathcal{V}(x) \to \mathcal{V}(y), \quad \neg(\forall x)\,\mathcal{V}(x) \equiv (\exists x)\,\neg\mathcal{V}(x), \quad \neg(\exists x)\,\mathcal{V}(x) \equiv (\forall x)\,\neg\mathcal{V}(x).$$

Budeme hovoriť, že takéto výrokové funkcie sú **logicky pravdivé**.

[2]Redundancia znamená nadbytočnosť, ktorá je potrebná k tomu, aby sme si mohli pri šume – nedobrom vyslovení alebo zlom počutí – domyslieť správnu informáciu.

3 Ešte raz o kvantifikátoroch

Ak výroková funkcia začína jedným alebo viacerými veľkými kvantifikátormi za sebou a za nimi nasleduje výroková funkcia bez kvantifikátorov, tak matematici obyčajne tieto kvantifikátory **zamlčia**. Napríklad, ak matematik chce povedať, že "Pre každé x, y, z, ak $x < y$ a $y < z$, tak $x < z$.", tak povie skrátene "Ak $x < y$ a $y < z$, tak $x < z$." Hovoríme tomu **interpretácia všeobecnosti**. Podobne to platí aj pri vyjadrení implikácie alebo ekvivalencie. Ak chceme povedať, že "Výroková funkcia $(\forall x)\,(\mathcal{V}(x) \to \mathcal{W}(x))$ je pravdivá", povieme obyčajne "Platí $\mathcal{V}(x) \to \mathcal{W}(x)$". Podobne pre ekvivalenciu. Nesmieme to urobiť, ak výroková funkcia obsahuje malý kvantifikátor. Mohlo by to viesť k nedorozumeniu.

Negácia výrokovej funkcie

$$\neg(\forall x)\,\mathcal{V}(x, y_1, \ldots, y_k)$$

je ekvivalentná výrokovej funkcii

$$(\exists x)\,\neg\mathcal{V}(x, y_1, \ldots, y_k).$$

Podobne, negácia výrokovej funkcie

$$\neg(\exists x)\,\mathcal{V}(x, y_1, \ldots, y_k)$$

je ekvivalentný výrokovej funkcii

$$(\forall x)\,\neg\mathcal{V}(x, y_1, \ldots, y_k).$$

Teda výroková funkcia

$$\neg(\forall x)(\exists y)(\exists u)(\forall v)\,\mathcal{V}(x, y, u, v)$$

je ekvivalentná výrokovej funkcii

$$(\exists x)(\forall y)(\forall u)(\exists v)\,\neg\mathcal{V}(x, y, u, v).$$

Čitateľ si ľahko overí, že negácie výrokových funkcií začínajúcich kvantifikátorom s podmienkou

$$(\forall x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k), \qquad (\exists x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$$

sú postupne ekvivalentné

$$(\exists x, \mathcal{V}(x))\,\neg\mathcal{W}(x, y_1, \ldots, y_k), \qquad (\forall x, \mathcal{V}(x))\,\neg\mathcal{W}(x, y_1, \ldots, y_k).$$

Napríklad, výroková funkcia $(\forall x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$ s kvantifikátorom s podmienkou je skratkou pre výrok $(\forall x)\,(\mathcal{V}(x) \to \mathcal{W}(x, y_1, \ldots, y_k))$. Negáciou tejto výrokovej funkcie je výroková funkcia $(\exists x)\,\neg(\mathcal{V}(x) \to \mathcal{W}(x, y_1, \ldots, y_k))$. Negácia implikácie je ekvivalentná výrokovej funkcii $\mathcal{V}(x) \wedge \neg\mathcal{W}(x, y_1, \ldots, y_k))$, teda skúmaná negácia je ekvivalentná výrokovej funkcii $(\exists x)\,(\mathcal{V}(x) \wedge \neg\mathcal{W}(x, y_1, \ldots, y_k))$. My sme sa dohodli, že túto výrokovú funkciu skrátene označíme

$$(\forall x, \mathcal{V}(x))\,\neg\mathcal{W}(x, y_1, \ldots, y_k).$$

Podobne by sme postupovali pre negovanie malého kvantifikátora s podmienkou. Teda, kvantifikátory s podmienkou negujeme rovnako, ako kvantifikátory bez podmienky.

Príklad 3.1 Výroková funkcia $\neg(\lim_{n\to\infty} a_n = a)$ je ekvivalentná výrokovej funkcii

$$(\exists \varepsilon > 0)(\forall n_0)(\exists n > n_0)\,(|a_n - a| \geq \varepsilon).$$

4 Množiny

Množina je súhrn nejakých objektov. Je to základný pojem, ktorý nemôžeme definovať. Niektoré objekty do danej množiny patria a niektoré nepatria. Ak objekt x do množiny A patrí, píšeme $x \in A$ a hovoríme tiež, že x je **prvok množiny** A. Negáciu $\neg x \in A$ označujeme jednoducho $x \notin A$. Množinu poznáme, ak vieme čo do nej patrí a čo do nej nepatrí. Teda dve množiny sa rovnajú, ak majú tie isté prvky:

$$A = B \text{ vtedy a len vtedy, ak } \ (\forall x)\,(x \in A \equiv x \in B).$$

Množinu A môžeme určiť napríklad vymenovaním jej prvkov:

$$A = \{0, 2, 4, 6, \ldots, 100\}, \qquad B = \{0, 2, 4, 6, \ldots\}.$$

Množinu môžeme určiť **charakteristickou vlastnosťou** jej prvkov:

$$(\forall x)\,(x \in A \equiv x \text{ je párne prirodzené číslo nie väčšie ako } 100),$$

$$(\forall x)\,(x \in B \equiv x \text{ je párne prirodzené číslo}).$$

Ukážeme, že nie každá "charakteristická vlastnosť" určuje množinu. Uvažujme charakteristickú vlastnosť $\mathcal{V}(x)$ množiny x vyjadrenú vzťahom " nepatrí do seba", t.j. $\mathcal{V}(x)$ označuje výrokovú funkciu $\neg x \in x$. Nech A je množina všetkých množín, ktoré majú túto vlastnosť, teda pre každé x platí

$$x \in A \equiv \neg x \in x.$$

Ak dosadíme za x množinu A, tak dostaneme spor

$$A \in A \equiv \neg A \in A.$$

Jediné možné vysvetlenie je také, že množina s uvedenou vlastnosťou neexistuje.

Zdanlivé protirečenie, paradox, v predchádzajúcej úvahe možno vysloviť aj bez pojmu množina. Bertrand Russel vymyslel takýto paradox: v dedine žil holič, ktorý holil všetkých mužov, ktorí neholili seba. Kto holil holiča?

Jeden z dôvodov neexistencie množiny v predchádzajúcom paradoxe je to, že táto množina by bola "veľmi veľká". Veď asi žiadna množina nepatrí do seba a teda množina A by obsahovala takmer všetky množiny. Dá sa ukázať, že nemôže existovať množina všetkých množín. Preto modifikujeme definíciu množiny pomocou charakteristickej vlastnosti takto. Ak B je množina a $\mathcal{V}(x)$ je výroková funkcia, tak utvoríme množinu A všetkých tých prvkov množiny B, ktoré majú charakteristickú vlastnosť $\mathcal{V}(x)$. Budeme písať

$$A = \{x \in B; \mathcal{V}(x)\}. \tag{4.5}$$

Pri takomto ohraničení na definíciu množiny pomocou charakteristickej vlastnosti a pri opatrnom zaobchádzaní s pojmom výroková funkcia sa nedostaneme do paradoxu.

Ak máme množiny A, B, tak môžeme utvoriť ich **prienik** $A \cap B$ a **rozdiel** $A \setminus B$ pomocou (4.5) takto:

$$A \cap B = \{x \in A; x \in B\},$$
$$A \setminus B = \{x \in A; x \notin B\}.$$

Ak A, B sú množiny, tak existuje ich **zjednotenie** $A \cup B$, pre ktoré platí

$$x \in A \cup B \equiv (x \in A \vee x \in B).$$

Ak x, y sú nejaké objekty, tak označíme $\{x, y\}$ množinu, ktorej prvkami sú len tieto dva objekty, teda

$$z \in \{x, y\} \equiv (z = x \vee z = y).$$

Podobne pre tri a viac objektov.

Množina A sa nazýva **podmnožina** množiny B, ak každý prvok množiny A je aj prvkom množiny B. Píšeme $A \subseteq B$. Uvedomte si, že platí

$$A = B \equiv (A \subseteq B \wedge B \subseteq A).$$

Ak x, y sú nejaké objekty, tak $[x, y]$ je **usporiadaná dvojica**[3] x je jej **prvá zložka** a y je **druhá zložka**. Základná vlastnosť usporiadanej dvojice je vyjadrená ekvivalenciou

$$[x, y] = [u, v] \equiv (x = u \wedge y = v).$$

Ak A, B sú množiny, tak $A \times B$ je množina všetkých usporiadaných dvojíc, ktorých prvá zložka patrí do množiny A a druhá zložka patrí do množiny B. Teda

$$u \in A \times B \equiv (\exists x \in A)(\exists y \in B)\, u = [x, y].$$

5 Reálne čísla

Množine reálnych čísiel $\mathbb{R}$ je opatrená rovnosťou "$=$", nerovnosťou "$\leq$", operáciami sčítania "$+$" a násobenia "$\cdot$" a obsahuje dve špeciálne reálne čísla nulu "0" a jednotku "1". Ak $x, y \in \mathbb{R}$ sú reálne čísla, tak platí alebo neplatí rovnosť $x = y$ alebo nerovnosť $x \leq y$. Namiesto negácie $\neg x = y$ píšeme $x \neq y$. Často bude potrebná **ostrá nerovnosť** $x < y$, ktorá je skratkou pre konjunkciu $x \leq y \wedge x \neq y$. Teda, definujeme

$$x < y \equiv (x \leq y \wedge \neg x = y).$$

Reálne čísla vieme sčítať a násobiť. Teda pre každé dve reálne čísla $x, y \in \mathbb{R}$ sú určené čísla $x + y$ a $x \cdot y$. Posledné sa skrátene označuje xy.

Množina reálnych čísiel opatrená uvedenou štruktúrou spĺňa nasledujúce **axiómy**, ktorými je v určitom zmysle jednoznačne charakterizovaná. Axiómy reálnych čísiel rozdelíme do viacerých skupín.

Prvú skupinu tvoria základné vlastnosti rovnosti (reflexívnosť, symetria a tranzitívnosť rovnosti):

(1) $(\forall x \in \mathbb{R})\, x = x$,

(2) $(\forall x, y \in \mathbb{R})\, (x = y \rightarrow y = x)$,

(3) $(\forall x, y, z \in \mathbb{R})\, (x = y \rightarrow (y = z \rightarrow x = z))$.

Ďalšiu skupinu tvoria axiómy, ktoré "spájajú" rovnosť s nerovnosťou a operáciami sčítania a násobenia. Často sa nazývajú **dosadzovacie pravidlá**:

(4) $(\forall x, y, u, v \in \mathbb{R})\, ((x = u \wedge y = v \wedge x \leq y) \rightarrow u \leq v)$

(5) $(\forall x, y, u, v \in \mathbb{R})\, ((x = u \wedge y = v) \rightarrow x + y = u + v)$

(6) $(\forall x, y, u, v \in \mathbb{R})\, ((x = u \wedge y = v) \rightarrow x \cdot y = u \cdot v)$

[3] Usporiadaná dvojica je nový pojem. Dá sa definovať. Nebudeme to robiť, stačí nám jeho základná vlastnosť.

Nasledujú základné vlastnosti nerovnosti (reflexívnosť, antisymetria a tranzitívnosť nerovnosti a zákon dichotómie):

(7) $(\forall x \in \mathbb{R})\, x \leq x$,

(8) $(\forall x, y \in \mathbb{R})\, ((x \leq y \wedge y \leq x) \rightarrow x = y)$,

(9) $(\forall x, y, z \in \mathbb{R})\, ((x \leq y \wedge y \leq z) \rightarrow x \leq z)$,

(10) $(\forall x, y \in \mathbb{R})\, (x \leq y \vee y \leq x)$.

Ľahko sa overí, že axióma (10)je ekvivalentná axióme $(10)^\star$, ktorá sa nazýva zákon trichotómie pre ostrú nerovnosť:

$(10)^\star$ $(\forall x, y \in \mathbb{R})\, (x < y \vee x = y \vee y < x)$.

Ďalšia skupina axióm dáva nerovnosť do vzťahu s operáciami (monotónnosť sčítania a násobenia):

(11) $(\forall x, y, z)\, (x \leq y \rightarrow x + z \leq y + z)$,

(12) $(\forall x, y, z)\, ((x \leq y \wedge z \geq 0) \rightarrow x \cdot z \leq y \cdot z)$.

Operácie sčítania a násobenia majú tieto základné vlastnosti (asociatívny a komutatívny zákon):

(13) $(\forall x, y, z \in \mathbb{R})\, x + (y + z) = (x + y) + z$,

(14) $(\forall x, y, z \in \mathbb{R})\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

(15) $(\forall x, y \in \mathbb{R})\, x + y = y + x$,

(16) $(\forall x, y \in \mathbb{R})\, x \cdot y = y \cdot x$.

Asociatívne zákony pre sčítanie a násobenie nám umožňujú nepísať zátvorky. Ak totiž napíšeme $x + y + z$, tak môžeme vložiť zátvorky dvojakým spôsobom: $x + (y + z)$ alebo $(x + y) + z$. Podľa asociatívneho zákona však obidva výrazy predstavujú to isté číslo. Podobne pre násobenie.

Ďalšia axióma spája sčítanie a násobenie (distributívny zákon):

(17) $(\forall x, y, z \in \mathbb{R})\, x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Špeciálne reálne čísla 0, 1 majú tieto vlastnosti:

(18) $(\forall x \in \mathbb{R})\, x + 0 = x$,

(19) $(\forall x \in \mathbb{R})\, x \cdot 1 = x$,

(20) $0 < 1$.

Existenciu opačného a inverzného prvku zabezpečujú axiómy

(21) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})\, x + y = 0$,

(22) $(\forall x \in \mathbb{R}, x \neq 0)(\exists y \in \mathbb{R})\, x \cdot y = 1$.

V príklade 13.2 ukážeme, že číslo s vlastnosťou (21) je jediné a označujeme ho $-x$. Teda

$$x + (-x) = 0.$$

Podobne sa dá ukázať, že číslo v (21) je jediné a označujeme ho $1/x$ alebo $1 : x$. Namiesto $x+(-y)$ píšeme $x-y$ a namiesto $x \cdot (1/y)$ píšeme x/y alebo $x : y$. Pozor, operácie $-$ a $:$ nie sú asociatívne.

Pre formuláciu poslednej axiómy potrebujeme definovať niekoľko pojmov. Číslo $a \in \mathbb{R}$ sa nazýva **horné ohraničenie** množiny $A \subseteq \mathbb{R}$, ak pre každé $x \in A$ platí $x \leq a$. Podobne môžeme definovať pojem **dolné ohraničenie**. Číslo a sa nazýva **supremum** množiny $A \subseteq \mathbb{R}$, píšeme

$$a = \sup A,$$

ak a je najmenšie horné ohraničenie množiny A, t.j.

(a) a je horné ohraničenie množiny A,

(b) ak b je horné ohraničenie množiny A, tak $a \leq b$.

Množina sa nazýva **zhora ohraničená**, ak existuje reálne číslo, ktoré je jej horným ohraničením. Ak $a \in A$ je horné ohraničenie množiny A, tak zrejme a je **najväčší prvok** množiny, niekedy sa nazýva **maximum**. Maximum je vždy supremum. Naopak nie. Podobne definujeme **infimum**, **zdola ohraničená**, **najmenší prvok**.

Prázdna ani zhora neohraničená množina nemôže mať supremum. Vysvetlite prečo?

Príklad 5.1 0 je infimum a 1 supremum množín $(0, 1)$, $(0, 1>$, $<0, 1)$ a $<0, 1>$. Ktorá z nich má najväčší a najmenší prvok?

Bernard Bolzano (1781 – 1848) v roku 1817 v práci *Rein Analytischer Beweiss des Lehrsatzes das Zwischen je zwey Werthen, die ein entgegengesetzes Resultat gewährten, wenigstens einer reelle Wurzel der Gleichung liege* sformuloval (a "dokázal"[4]) základnú vlastnosť množiny reálnych čísiel $\mathbb{R}$, ktorú uvedieme ako poslednú axiómu o reálnych číslach.

Bolzanov princíp: *Každá neprázdna zhora ohraničená množina reálnych čísiel má supremum.*

Na záver tejto časti pripomenieme definíciu intervalov. Nech $a < b$ sú reálne čísla. Označíme

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R}; a < x < b\}, & \langle a, b\rangle &= \{x \in \mathbb{R}; a \leq x \leq b\},\\
(a, b\rangle &= \{x \in \mathbb{R}; a < x \leq b\}, & \langle a, b) &= \{x \in \mathbb{R}; a \leq x < b\},\\
(a, +\infty) &= \{x \in \mathbb{R}; a < x\}, & \langle a, +\infty) &= \{x \in \mathbb{R}; a \leq x\},\\
(-\infty, b) &= \{x \in \mathbb{R}; x < b\}, & (-\infty, b\rangle &= \{x \in \mathbb{R}; x \leq b\}.
\end{aligned}$$

6 Prirodzené čísla a matematická indukcia

Množinu prirodzených čísiel $\mathbb{N}$ definujeme takto: $\mathbb{N}$ je najmenšia podmnožina množiny $\mathbb{R}$, ktorá má tieto dve vlastnosti

(a) $0 \in \mathbb{N}$,

(b) ak $n \in \mathbb{N}$, tak aj $n + 1 \in \mathbb{N}$.

Teda, $\mathbb{N}$ má vlastnosti (a), (b) a ak nejaká množina $X \subseteq \mathbb{R}$ má vlastnosti

[4] Dokázal to na základe iného predpokladu.

(c) $0 \in X$,

(d) ak $n \in X$, tak aj $n+1 \in X$,

tak $\mathbb{N} \subseteq X$.

Veta 6.1 (Prvá metaveta o matematickej indukcii): *Nech $\mathcal{V}(x)$ je výroková funkcia. Ak*
IK_1: *platí $\mathcal{V}(0)$,*
IK_2: *z $\mathcal{V}(n)$ vyplýva $\mathcal{V}(n+1)$ pre každé $n \in \mathbb{N}$,*
potom platí $\mathcal{V}(n)$ pre každé prirodzené číslo n.

Dôkaz: Položíme

$$X = \{n \in \mathbb{N}; \mathcal{V}(n)\}.$$

Podľa IK_1 je $0 \in X$. Podľa IK_2 množina X má aj vlastnosť (d) a teda $\mathbb{N} \subseteq X$. To ale znamená, že $\mathcal{V}(n)$ platí pre každé $n \in \mathbb{N}$.

q.e.d.

IK_1 sa nazýva **prvý indukčný krok** a IK_2 sa nazýva **druhý indukčný krok**. Keď dokazujeme druhý indukčný krok, tak spravidla postupujeme tak, že urobíme **indukčný predpoklad** $\mathcal{V}(n)$ a dokážeme $\mathcal{V}(n+1)$.

Príklad 6.1 Ukážeme, že 0 je najmenšie prirodzené číslo, teda, pre každé prirodzené číslo n platí $0 \leq n$.

Nech $\mathcal{V}(n)$ označuje výrokovú funkciu $0 \leq n$. Zrejme platí $\mathcal{V}(0)$. Predpokladajme, že platí $\mathcal{V}(n)$, t.j. $0 \leq n$. Podľa axiómy (20) je $0 < 1$ a podľa axiómy (11) je $0 + n \leq 1 + n$ (dokonca $0 + n < 1 + n$). Podľa axiómy (15) platí $0 + n = n + 0$ a $1 + n = n + 1$. Potom podľa axiómy (4) je $n + 0 \leq n + 1$. Podľa axiómy (18) je $n + 0 = n$. Potom pomocou axióm (2) a (3) dostávame $n \leq n + 1$. Axióma (9) spolu s indukčným predpokladom dáva $0 \leq n + 1$, t.j. platí $\mathcal{V}(n+1)$.

Podľa vety 6.1 o matematickej indukcii potom pre každé prirodzené číslo n platí $\mathcal{V}(n)$ a to sme mali dokázať.

Niekedy je potrebné indukčný krok rozdeliť na dva alebo viac prípadov. Bez komentára uvediem jednoduchý príklad.

Príklad 6.2 Ak $p > 1$ je prirodzené číslo, tak pre každé $n \in \mathbb{N}$ platí $n \cdot p \leq p^n$.

Pre $n = 0$ platí $0 \cdot p = 0 < p^0 = 1$.

Pre $n = 1$ platí $1 \cdot p = p \leq p^1 = p$.

Predpokladajme teraz, že $n \geq 1$ a platí $n \cdot p \leq p^n$. Potom je $p \leq p^n$ a dostávame

$$(n+1) \cdot p = n \cdot p + p \leq p^n + p \leq p^n + p^n = 2 \cdot p^n \leq p \cdot p^n = p^{n+1},$$

čo sme chceli dokázať.

Veta 6.2 *: Každá neprázdna množina prirodzených čísiel má najmenší prvok.*

Dôkaz: Nech $A \subseteq \mathbb{N}$ je neprázdna množina. Nech $\mathcal{V}(n)$ označuje výrokovú funkciu – implikáciu "Ak existuje $k \leq n$, $k \in A$, tak množina A má najmenší prvok."

Zrejme platí $\mathcal{V}(0)$: ak existuje $k \leq 0$, $k \in A$, tak $0 \in A$ a 0 je najmenšie prirodzené číslo a teda aj najmenší prvok množiny A.

Predpokladajme teraz, že platí $\mathcal{V}(n)$. Nech existuje $k \leq n+1$ také, že $k \in A$. Máme dve možnosti:

a) Existuje $k \leq n$, $k \in A$. Potom podľa indukčného predpokladu $\mathcal{V}(n)$ množina A má najmenší prvok.

b) Neexistuje $k \leq n, k \in A$. Potom $k = n + 1 \in \mathbb{N}$ a je to najmenší prvok množiny A.

Teda $\mathcal{V}(n)$ platí pre každé $n \in \mathbb{N}$. Keďže množina A je neprázdna, tak existuje $n \in A$. Potom platí predpoklad implikácie $\mathcal{V}(n)$ a teda aj jej záver: množina A má najmenší prvok.

q.e.d.

Veta 6.3 (Druhá metaveta o matematickej indukcii): *Nech $\mathcal{V}(x)$ je výroková funkcia. Ak pre každé $n \in \mathbb{N}$*
IK: *z platnosti $\mathcal{V}(k)$ pre každé $k < n$ vyplýva $\mathcal{V}(n)$,*
potom platí $\mathcal{V}(n)$ pre každé prirodzené číslo n.

Dôkaz: Teraz položíme

$$X = \{n \in \mathbb{N}; \neg\, \mathcal{V}(n)\}$$

a chceme ukázať, že $X = \emptyset$.

Keby $X \neq \emptyset$, tak podľa vety 6.2 množina X má najmenší prvok $n \in X$. Potom pre každé $k < n$ platí $\mathcal{V}(k)$ a neplatí $\mathcal{V}(n)$ – to je však spor s IK.

q.e.d.

Táto forma matematickej indukcie má len jeden indukčný krok. Indukčný predpoklad v tomto prípade je však "pre každé $k < n$ platí $\mathcal{V}(k)$".

Príklad 6.3 Každé prirodzené číslo $n > 1$ je deliteľné nejakým prvočíslom[5].

Výrokovú funkciu "ak $n > 1$, tak existuje prvočíslo, ktoré delí n" označíme $\mathcal{V}(n)$. Indukčný predpoklad bude "pre každé $k < n$, $k > 1$, existuje prvočíslo, ktoré delí číslo k".

Nech $n > 1$. Ak n je prvočíslo, tak n delí samé seba a teda je deliteľné prvočíslom. Ak n nie je prvočíslo, tak existuje prirodzené číslo k, $1 < k < n$, ktoré delí číslo n. Podľa indukčného predpokladu existuje prvočíslo p, ktoré delí číslo k. Potom však prvočíslo p delí aj číslo n.

Teda, dokázali sme, že platí indukčný krok IK. Podľa vety 6.3 platí $\mathcal{V}(n)$ pre každé n. A to sme chceli dokázať.

Ukážeme inú dôležitú vlastnosť prirodzených čísiel.

Lema 6.4 *Množina prirodzených čísiel $\mathbb{N}$ nie je zhora ohraničená.*

Dôkaz: Keby množina $\mathbb{N}$ bola zhora ohraničená, tak existuje $a = \sup \mathbb{N}$. Číslo $a - 1 < a$ potom nie je horné ohraničenie množiny $\mathbb{N}$ a teda existuje $n \in \mathbb{N}$ také, že $n > a - 1$. Potom ale $n + 1 > a$ a $n + 1 \in \mathbb{N}$, čo je spor.

q.e.d.

Veta 6.5 (Archimedov princíp) *Nech $a \in \mathbb{R}$, $\varepsilon > 0$. Potom existuje prirodzené číslo n také, že $n \cdot \varepsilon > a$.*

Dôkaz: Podľa lemy číslo a/ε nie je horné ohraničenie množiny $\mathbb{N}$. Teda existuje $n \in \mathbb{N}$ také, že $a/\varepsilon < n$. Potom $a < n \cdot \varepsilon$.

q.e.d.

Často budeme potrebovať jeden špeciálny dôsledok Archimedovho princípu.

Dôsledok 6.6 a) *Nech $p > 1$ je prirodzené číslo a $a \in \mathbb{R}$. Potom existuje prirodzené číslo n také, že $p^n > a$.*

b) *Nech $p > 1$ je prirodzené číslo a $a \in \mathbb{R}$, $a > 0$. Potom existuje prirodzené číslo n také, že $p^{-n} < a$.*

Dôkaz: a) Podľa Archimedovho princípu existuje prirodzené číslo n také, že platí $n \cdot p > a$. Podľa príkladu 6.2 platí $n \cdot p \leq p^n$.

b) Podľa časti a) existuje prirodzené číslo n také, že $p^n > 1/a$. Potom $p^{-n} < a$.

q.e.d.

Cvičenie 6.1 Súčet a súčin dvoch prirodzených čísiel je číslo prirodzené. Dokážte matematickou indukciou!

[5] Pripomeňme si definíciu prvočísla. Prirodzené číslo n sa nazýva prvočíslo, ak neexistuje prirodzené číslo k, $1 < k < n$, ktoré delí číslo n.

Cvičenie 6.2 Ak $n \leq m$ a $n + x = m$, tak x je prirodzené číslo.

Rozdiel dvoch prirodzených čísiel však nemusí byť prirodzené číslo. Množina **celých čísiel** je definovaná ekvivalenciou

$$z \in \mathbb{Z} \equiv z \in \mathbb{N} \vee -z \in \mathbb{N}.$$

Veta 6.7 *Pre každé reálne číslo x existuje jediné celé číslo z také, že*

$$z \leq x < z + 1. \tag{6.6}$$

Dôkaz: xxx QED Jediné celé číslo z pre ktoré platí (6.6), budeme označovať $[x]$ a nazývať **dolná celá časť** čísla x. Niekedy sa slovo "dolná" vynecháva a hovorí sa jednoducho "celá časť".

7 p–adický zápis prirodzeného čísla

V bežnom živote používame desiatkový (dekadický) zápis prirodzeného čísla. Prirodzené číslo

$$x = \sum_{i=0}^{n} x_i 10^i = x_0 + x_1 \cdot 10 + x_2 \cdot 10^2 + \ldots + x_n \cdot 10^n,$$

kde x_i sú číslice $0, 1, 2, \ldots, 9$ a $x_n \neq 0$, bežne zapisujeme

$$x = x_n x_{n-1} \ldots x_1 x_0.$$

Napríklad číslo $x = 7 + 8 \cdot 10 + 9 \cdot 10^2 + 1 \cdot 10^3$ zapisujeme ako 1987.

V tomto zápise číslo 10 je **základ**, čísla $0, 1, \ldots, 9$ sú **dekadické číslice**. Často potrebujeme zápis s iným základom, napríklad dvojkový, trojkový zápis. Pre počítače je užitočný zápis so základom 16.

Nech **základ** je prirodzené číslo $p > 1$. p–**adický zápis** čísla x je postupnosť $x_n, \ldots, x_0$ p–**adických číslic** $x_i \in \{0, \ldots, p-1\}$ taká, že platí

a) $x = \sum_{i=0}^{n} x_i \cdot p^i$,

b) ak $x = 0$, tak $n = 0$ a $x_0 = 0$,

c) ak $x \neq 0$, tak $x_n \neq 0$.

Píšeme

$$x = x_n x_{n-1} \ldots x_0|_p.$$

Ak z kontextu vieme, čo je základ, tak $|_p$ nepíšeme. Naviac, ak nepovieme, čo je základ, tak je to číslo 10.

Východiskom pre naše ďalšie úvahy je známa rovnosť pre súčet geometrického radu

$$\sum_{i=0}^{n} p^i = \frac{p^{n+1} - 1}{p - 1}$$

a z nej vyplývajúca rovnosť

$$\sum_{i=0}^{n} (p-1) \cdot p^i = p^{n+1} - 1.$$

Z tejto rovnosti bezprostredne dostávame nerovnosť

$$x = \sum_{i=0}^{n} x_i \cdot p^i < p^{n+1}, \tag{7.7}$$

ak $x_0, \ldots, x_n$ sú p–adické číslice, t.j. $x_i = 0, \ldots, p-1$.

Veta 7.1 *Pre každé prirodzené číslo x existuje jediný p–adický zápis*

$$x = \sum_{i=0}^{n} x_i \cdot p^i \tag{7.8}$$

Dôkaz Najprv ukážeme, že ak $x_n, \ldots, x_0$ a $y_m, \ldots, y_0$ sú p–adické zápisy toho istého čísla x, tak $n = m$ a $x_i = y_i$ pre každé $i \leq n$. Ukážeme to sporom. Predpokladajme, že to neplatí. Teda $n \neq m$ alebo existuje i také, že $x_i \neq y_i$.

Ak $n \neq m$, tak platí $n < m$ alebo $n > m$. Bez ujmy na všeobecnosti môžeme predpokladať, že $n < m$. Potom $m > 0$ a podľa b) je $x_m > 0$ a teda

$$x = \sum_{i=0}^{m} y_i \cdot y_i \geq x_m \cdot p^m \geq p^m.$$

Podľa (7.8) však platí

$$\sum_{i=0}^{n} x_i \cdot p^i < p^{n+1} \leq p^m,$$

čo je hľadaný spor. Teda $n = m$.

Predpokladajme teraz, že existuje $j \leq n$ také, že $x_j \neq y_j$. Nech j je najmenšie také a nech $x_j < y_j$. Označíme

$$x' = \sum_{i=0}^{j} x_i \cdot p^i, \quad x'' = \sum_{i=j+1}^{n} x_{i+j+1} \cdot p^i, \quad y' = \sum_{i=0}^{j} y_i \cdot p^i, \quad y'' = \sum_{i=j+1}^{n} y_{i+j+1} \cdot p^i.$$

Ak $j = n$ tak $x'' = y'' = 0$. Zrejme $x = x' + x'' = y' + y''$. Keďže $x_i = y_i$ pre $i < j$, tak $0 < y' - x' = (y_j - x_j)p^j < p^{j+1}$. Teda $0 < x'' - y'' < p^{j+1}$. Ale

$$y'' - x'' = p^{j+1} \cdot \sum_{i=0}^{n-j-1} (y_{i+j+1} - x_{i+j+1}) \cdot p^i.$$

Číslo $\sum_{i=0}^{n-j-1} (y_{i+j+1} - x_{i+j+1}) \cdot p^i$ je kladné a prirodzené, teda je ≥ 1. Potom $y'' - x'' \geq p^{j+1}$, čo je hľadaný spor.

Ukážeme teraz, že požadovaný p–adický zápis existuje. Náš dôkaz bude súčasne návod, ako ho zostrojiť.

Pre $x = 0$ stačí položiť $n = 0$ a $x_0 = 0$. Teda budeme predpokladať, že $x > 0$. Podľa dôsledku 6.6 existuje prirodzené číslo m také, že platí $p^m > x$. Nech m je najmenšie také číslo. Keďže $x > 0$, tak $m > 0$ a teda $m = n + 1$, kde n je prirodzené číslo. Zrejme $p^n \leq x$. Budeme "skúšať, koľkokrát sa p^n zmestí do x". Odpoveď je číslo x_n. Teda, x_n je najväčšie prirodzené číslo také, že $x_n \cdot p^n \leq x$. Zrejme je $x_n > 0$ a platí

$$x_n < p, \qquad x - x_n \cdot p^n < p^n.$$

Predpokladajme, že už sme našli čísla $x_n, \ldots, x_{i+1} \in \{0, \ldots . p-1\}$ také, že

$$x - (x_n \cdot p^n + \ldots + x_{i+1} \cdot p^{i+1}) < p^{i+1}.$$

Zase budeme "skúšať, koľkokrát sa p^i zmestí do $x - (x_n \cdot p^n + \ldots x_{i+1} \cdot p^{i+1})$". Odpoveď je najväčšie prirodzené číslo x_i také, že

$$x_i \cdot p^i \leq x - (x_n \cdot p^n + \ldots x_{i+1} \cdot p^{i+1}). \tag{7.9}$$

Ľahko vidieť, že $x_i < p$ a platí

$$x - (x_n \cdot p^n + \ldots + x_i \cdot p^i) < p^i.$$

Ak $i = 0$, tak $p^i = 1$ a najväčšie x_i také, že platí (7.9) je

$$x_0 = x - (x_n \cdot p^n + \ldots + x_1 \cdot p^1)$$

a teda platí (7.8).

q.e.d.

Príklad 7.1 Ilustrujeme dôkaz vety na príklade. Nájdeme trojkový zápis čísla 227 (číslo je dané v desiatkovom zápise). Začneme počítaním mocním čísla $p = 3$, pokiaľ "neprekročíme" naše číslo 227. Teda

$$3^0 = 1,\ 3^1 = 3,\ 3^2 = 9,\ 3^3 = 27,\ 3^4 = 81,\ 3^5 = 243.$$

Takže $m = 5$ a $n = 4$. Platí $3^n = 3^4 = 81 \leq 227$. Číslo 81 sa "zmestí" dvakrát do čísla 227, lebo $2 \cdot 81 = 162 < 227$ a $3 \cdot 81 = 243 > 227$. Teda $x_4 = 2$. Ďalej skúšame, koľkokrát sa "zmestí" číslo $3^3 = 27$ do čísla $227 - 2 \cdot 3^4 = 227 - 162 = 65$. Zrejme $x_3 = 2$. Pokračujeme skúšaním, koľkokrát sa zmestí číslo $3^2 = 9$ do čísla $227 - (2 \cdot 3^4 + 2 \cdot 3^3) = 65 - 2 \cdot 27 = 11$. Teraz je to $x_2 = 1$. Ďalej skúšame, koľkokrát sa zmestí $3^1 = 3$ do čísla $227 - (2 \cdot 3^4 + 2 \cdot 3^3 + 1 \cdot 3^2) = 11 - 9 = 2$. Ani raz, teda $x_1 = 0$. Potom $x_0 = 2$ a máme výsledok

$$2 \cdot 10^2 + 2 \cdot 10^1 + 7 \cdot 10^0 = 227|_{10} = 22102|_3 = 2 \cdot 2^4 + 2 \cdot 2^3 + 1 \cdot 3^2 + 0 \cdot 3^1 + 2 \cdot 3^0.$$

Prevod z p–adického zápisu do desiatkového je jednoduchý, lebo všetky výpočty (my, nie počítač) robíme automaticky v desiatkovom zápise.

Príklad 7.2 Číslo 6203 v semdičkovom zápise je číslo

$$6 \cdot 7^3 + 2 \cdot 7^2 + 0 \cdot 7^1 + 3 \cdot 7^0 = 6 \cdot 343 + 2 \cdot 49 + 0 \cdot 7 + 3 \cdot 3 = 2159$$

vyjadrené v desiatkovom zápise. Podobne číslo 10110010 v dvojkovom zápise je číslo

$$1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 128 + 32 + 16 + 2 = 178$$

vyjadrené v desiatkovom zápise.

Príklad 7.3 Prevod p–adického zápisu čísla x do dvojkového zápisu sa dá zjednodušiť. Nech $x = x_n x_{n-1} \ldots x_1 x_0|_2$ je dvojkový zápis. Definujeme postupnosť $\{a_i\}_{i=0}^{\infty}$ takto:

$$a_0 = x, \qquad a_{i+1} = \left[\frac{a_i}{2}\right].$$

Ľahko vidieť, že pre $i < n$ platí $a_i = x_n \ldots x_i|_2$ a $a_n = x_n = 1$. Odtiaľ bezprostredne vyplýva, že pre $i \leq n$ platí

číslo a_i je párne vtedy a len vtedy, keď $x_i = 0$.

Teda dvojkový zápis získame tak, že číslo delíme číslom 2 (zvyšok zanedbávame), pokiaľ nedostaneme výsledok 1 (dostaneme tak postupnosť $a_0, \ldots, a_n$). Dvojkový zápis $x_0, \ldots, x_n$ získame na základe parity medzivýsledkov delenia $a_0, \ldots, a_n$. Ak základ p je párne číslo, tak parita čísla v p–adickom zápise je daná jeho poslednou p–adickou číslicou.

Ilustrujeme to na príklade. Prevedieme do dvojkového zápisu číslo 726:

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
726	363	181	90	45	22	11	5	2	1
x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
0	1	1	0	1	0	1	1	0	1

Teda

$$726|_{10} = 1011010110|_2.$$

Príklad 7.4 Jeden africký kmeň vraj používa násobenie, ktoré využíva dvojkový zápis. Príslušníci tohoto kmeňa to však nevedia. Oni sa naučili počítať od svojich predkov a všetko naznačuje, že prapôvod je v starom Egypte, kde poznali osobitnú operáciu – zdvojnásobenie čísla.

Metódu najprv ilustrujeme na príklade. Máme vynásobiť čísla 178 a 37. Budeme písať dva stĺpce, ktoré začnú týmito číslami. V prvom stĺpci budeme číslo 178 postupne deliť dvomi – zvyšok zanedbáme – a v druhom stĺpci budeme číslo 37 postupne zdvojnásobovať. Keď pri delení dôjdeme k číslu 1, skončíme. Potom vyškrtneme riadky, v ktorých sú v ľavom stĺpci "nešťastné"[6] párne čísla. Ak spočítame čísla pravého stĺpca, ktoré po vyškrtnutí zostali, dostaneme výsledok. Teda

178	37	*po vyškrtnutí*	–
89	74		74
44	148		–
22	296		–
11	592		592
5	1184		1184
2	2368		–
1	4736		4736
		spolu	6586

Vysvetlenie je jednoduché. Nech $x = x_n \dots x_0|_2$ a y sú čísla, ktoré chceme vynásobiť. Definujeme dve postupnosti $\{a_i\}_{i=0}^n$ a $\{b_i\}_{i=0}^n$, ktoré tvoria tabuľku:

$$a_0 = x, \quad a_{i+1} = \left[\frac{a_i}{2}\right], \qquad b_0 = y, \quad b_{i+1} = 2 \cdot b_i.$$

Zrejme platí

$$x \cdot y = (\sum_{i=0}^{n} x_i \cdot 2^i) \cdot y = \sum_{i=0}^{n} x_i \cdot (2^i \cdot y) = \sum_{i=0}^{n} x_i \cdot b_i = x_0 \cdot b_0 + x_1 \cdot b_1 + \dots x_n \cdot b_n.$$

Čísla x_i nadobúdajú hodnoty 0, 1. Vieme, že $x_i = 1$ práve vtedy, keď a_i je nepárne. Teda súčin $x \cdot y$ je rovný súčtu tých b_i, pre ktoré je a_i párne.

8 Racionálne čísla

Súčet, súčin a rozdiel dvoch celých čísiel je číslo celé. Stále však podiel dvoch celých čísiel nemusí byť číslo celé. Číslo r je **racionálne**, ak existuje číslo celé $p \in \mathbb{Z}$ a nenulové prirodzené číslo $q \in \mathbb{N}$ také, že $r = p/q$. Množinu **racionálnych čísiel** označíme $\mathbb{Q}$. Teda

$$\mathbb{Q} = \{x \in \mathbb{R}; (\exists p \in \mathbb{Z})(\exists q \in \mathbb{N}, q \neq 0)\, x = \frac{p}{q}\}.$$

Zrejme súčet, súčin, rozdiel a podiel (nenulovým číslom) racionálnych čísiel je číslo racionálne.

Pripomeňme, že ak $a > 0$ tak $\sqrt{a}$ je také kladné číslo x, pre ktoré platí $x^2 = a$. V matematickej analýze sa dokazuje, že funkcia $x^2 - 2$ má kladný nulový bod, teda existuje číslo $\sqrt{2}$.

Veta 8.1 *Číslo $\sqrt{2}$ nie je racionálne.*

[6] Kmeň veril, že párne čísla sú nešťastné.

Dôkaz je založený na vete 6.2 a robí sa sporom [7]. Predpokladajme, že $\sqrt{2}$ je racionálne číslo - teda $\sqrt{2} = n/m$ pre nejaké prirodzené čísla n, m. Môžeme naviac predpokladať, že zlomok už nemožno krátiť. Presnejšie, podľa vety 6.2 vezmeme najmenšie m také, pre ktoré existuje n s vlastnosťou $\sqrt{2} = n/m$. Potom $n^2 = 2m^2$ a teda n je párne, teda existuje prirodzené číslo k také, že $n = 2k$. Z toho zase $2k^2 = m^2$ a teda aj m je párne, t.j. existuje prirodzené číslo l také, že platí $m = 2l$. Potom $\sqrt{2} = 2k/2l = k/l$, čo je spor s výberom čísla m.

q.e.d.

Veta 8.2 (Hustota racionálnych čísiel) *Pre ľubovoľné dve reálne čísla $a < b$ existuje racionálne číslo $r \in \mathbb{Q}$ také, že $a < r < b$.*

Dôkaz: Budeme rozlišovať tri prípady:

a) $0 \leq a < b$,

b) $a < 0 < b$,

c) $a < b \leq 0$.

Nech platí a). Podľa Archimedovho princípu existuje prirodzené číslo $n > 1/(b-a)$. Potom $1/n < b - a$. Znova podľa Archimedovho princípu existuje $m \in \mathbb{N}$ také, že $m \cdot 1/n > a$. Nech m je najmenšie prirodzené číslo s touto vlastnosťou. Potom $m > 0$ a teda $m - 1$ je prirodzené číslo a $(m-1) \cdot 1/n \leq a$. Potom

$$m \cdot 1/n < a + (b - a) = b.$$

Teda $r = m/n$ je hľadané číslo.

V prípade b) stačí položiť $r = 0$.

Podľa a) existuje racionálne číslo r také, že $0 \leq -b < r < -a$. Potom aj $-r$ je racionálne číslo a platí $a < -r < b$.

q.e.d.

Dôsledok 8.3 (Hustota iracionálnych čísiel) *Pre ľubovoľné dve reálne čísla $a < b$ existuje iracionálne číslo x také, že $a < x < b$.*

Dôkaz: Podľa vety 8.2 existuje racionálne číslo r také, že $a/\sqrt{2} < r < b/\sqrt{2}$. Potom $x = r \cdot \sqrt{2}$ je iracionálne číslo a platí $a < x < b$.

q.e.d.

Ľahko vidieť, že množina racionálnych čísiel $\mathbb{Q}$ má všetky vlastnosti (1) – (22). Na množine $\mathbb{Q}$ neplatí Bolzanov princíp: stačí zobrať množinu

$$A = \{r \in \mathbb{Q}; r^2 \leq 2\}.$$

Množina A je neprázdna a zhora ohraničená, nemá však v $\mathbb{Q}$ supremum - jej supremum je $\sqrt{2} \notin \mathbb{Q}$.

9 p–adický zápis reálneho čísla

Ak x je reálne číslo, tak $x = [x] + (x - [x])$. Zrejme $0 \leq (x - [x]) < 1$. Ak x je nezáporné, tak [x] je prirodzené číslo a v časti 7 sme opísali p–adický zápis prirodzeného čísla. V tejto časti opíšeme p–adický zápis čísla z intervalu $\langle 0, 1 \rangle$.

[7] Dôkaz poznal už Pytagoras (585? – 497? pred Kr.) a jeho žiaci. Tento výsledok bol veľmi nevhodný pre pytagorovcov, ktorí verili v určitú moc prirodzených čísiel. Báj hovorí, že Hippasosa, ktorý to objavil, hodili z lode do mora žralokom.

Nech p je prirodzené číslo väčšie ako 1. Nech $x \in \langle 0,1\rangle$. Postupnosť $\{x_i\}_{i=1}^{\infty}$ p–adických číslic $x_i \in \{0,\dots,p-1\}$ sa nazýva **p–adický zápis čísla** x, píšeme

$$x = 0,x_1x_2\dots x_i\dots|_p,$$

ak

$$x = \sum_{i=1}^{\infty} x_i \cdot p^{-i}. \tag{9.10}$$

Ak existuje n také, že pre $i > n$ je $x_i = 0$, tak píšeme

$$x = 0,x_1x_2\dots x_n|_p.$$

V tomto prípade totiž

$$x = \sum_{i=0}^{n} x_i \cdot p^{-i}.$$

Hovoríme, že číslo x má **konečný p–adický zápis**. V opačnom prípade je zápis **nekonečný**

Príklad 9.1 Číslo $\frac{1}{5}$ má konečný desiatkový zápis

$$0,2 = 0,2000\dots0\dots = 2\cdot 10^{-1} + 0\cdot 10^{-2} + 0\cdot 10^{-3} + \dots + 0\cdot 10^{-i} + \dots = \frac{2}{10} = \frac{1}{5}.$$

To isté číslo má aj nekonečný desiatkový zápis:

$$\begin{aligned} 0,1999\dots9\dots &= 1\cdot 10^{-1} + 9\cdot 10^{-2} + 9\cdot 10^{-3} + \dots + 9\cdot 10^{-i} + \dots = \\ &= \frac{1}{10} + \frac{9}{10^2}(1 + 10^{-1} + 10^{-2} + \dots + 10^{-i} + \dots). \end{aligned}$$

V zátvorke je súčet geometrického radu s kvocientom 10^{-1} a ten je rovný číslu

$$\frac{1}{1-10^{-1}} = \frac{1}{1-\frac{1}{10}} = \frac{10}{10-1} = \frac{10}{9}.$$

Teda

$$0,1999\dots9\dots = \frac{1}{10} + \frac{9}{10^2}\cdot\frac{10}{9} = \frac{1}{10} + \frac{1}{10} = \frac{1}{5}.$$

Podobne možno vypočítať, že $0,999\dots9\dots = 1$. Naozaj

$$\begin{aligned} 0,999\dots9\dots &= 9\cdot 10^{-1} + 9\cdot 10^{-2} + \dots + 9\cdot 10^{-i} + \dots = \\ &= \frac{9}{10}\cdot(1 + 10^{-1} + \dots + 10^{-i} + \dots = \\ &= \frac{9}{10}\cdot\frac{1}{1-10^{-1}} = \frac{9}{10}\cdot\frac{10}{9} = 1. \end{aligned}$$

Tento výsledok môžeme zovšeobecniť takto:

$$1 = 0,(p-1)(p-1)\dots(p-1)\dots|_p.$$

Podobne možno ukázať, že ak $x_i = p-1$ pre $i > m$ a $x_m < p-1$, tak

$$\begin{aligned} 0,x_1x_2\dots x_m(p-1)(p-1)\dots|_p &= 0,x_1x_2\dots(x_m+1)00\dots|_p = \\ &= 0,x_1x_2\dots(x_m+1)|_p. \end{aligned}$$

Veta 9.1 *Nech $p > 1$ je prirodzené číslo. Ak $x \in \langle 0, 1\rangle$ tak existuje p–adický zápis čísla x. Naviac tento zápis je jediný okrem nasledujúceho prípadu:*

$$x = 0, x_1 x_2 \ldots x_n \ldots |_p = 0, y_1 y_2 \ldots y_n \ldots |_p$$

a existuje kladné prirodzené číslo m také, že

$$x_i = y_i \text{ pre } i < m, \tag{9.11}$$

$$x_m = y_m + 1, \tag{9.12}$$

$$x_i = 0 \text{ pre } i > m, \tag{9.13}$$

$$y_i = p - 1 \text{ pre } i > m. \tag{9.14}$$

Dôkaz: Vzhľadom na výsledok príkladu 9.1 stačí uvažovať $x \in \langle 0, 1)$. Postupnosť $\{x_i\}_{i=1}^{\infty}$ zostrojíme matematickou indukciou podobne, ako v dôkaze vety 7.1. Nech x_1 je najväčšie prirodzené číslo také, že $x_1 \cdot p^{-1} \leq x$. Zrejme $x_1 < p$. Ak už máme zostrojené čísla $x_1, \ldots, x_i$, zostrojíme číslo x_{i+1} takto: x_{i+1} je najväčšie prirodzené číslo také, že

$$x_{i+1} \cdot p^{-i-1} \leq x - (x_1 \cdot p^{-1} + \ldots + x_i \cdot p^{-i}). \tag{9.15}$$

Ľahko vidieť[8], že $x_{i+1} < p$.

Podľa (9.15) pre každé n platí $\sum_{i=1}^{n} x_i \cdot p^{-i} \leq x$ a teda aj

$$\sum_{i=1}^{\infty} x_i \cdot p^{-i} \leq x.$$

Keby bolo $\sum_{i=1}^{\infty} x_i \cdot p^{-i} < x$, tak podľa dôsledku 6.6 existuje prirodzené číslo n také, že

$$p^{-n} < x - \sum_{i=1}^{\infty} x_i \cdot p^{-i} \leq x - \sum_{i=1}^{n} x_i \cdot p^{-i}$$

a teda

$$(x_n + 1) \cdot p^{-n} \leq x - \sum_{i=1}^{n-1} x_i \cdot p^{-i},$$

čo je spor s definíciou čísla x_n.

Ak existuje prirodzené číslo $m > 0$ také, že platí (9.11)–(9.14), tak jednoduchým výpočtom (súčet geometrického radu) možno zistiť, že

$$0, x_1 x_2 \ldots x_n \ldots |_p = 0, y_1 y_2 \ldots y_n \ldots |_p. \tag{9.16}$$

Predpokladajme teraz, že platí (9.16) a existuje také $m > 0$, že $x_m \neq y_m$. Bez ujmy na všeobecnosti môžeme predpokladať, že m je najmenšie také, teda $x_i = y_i$ pre $0 < i < m$ a že $x_i < y_i$. Potom dostávame

$$\begin{aligned} 0, x_1 x_2 \ldots x_m x_{m+1} x_{m+2} \ldots |_p &\leq 0, x_1 x_2 \ldots x_m (p-1)(p-1) \ldots |_p = \\ = 0, x_1 x_2 \ldots (x_m + 1) vert_p &\leq 0, x_1 x_2 \ldots x_{m-1} y_m |_p = \\ = 0, y_1, y_2 \ldots y_m |_p &\leq 0, y_1 y_2 \ldots y_m y_{m+1} \ldots |_p. \end{aligned}$$

Podľa predpokladu prvé a posledné čísla sa rovnajú a teda všetky tri nerovnosti $\leq$ musia byť rovnosti. Z toho postupne vyplýva, že $x_i = p - 1$ pre $i > m$, $x_m + 1 = y_m$ a konečne $y_i = 0$ pre $i > 0$.

q.e.d.

[8] Keby bolo $x_{i+1} \geq p$, tak $(x_i + 1) \cdot p^{-i} \leq x - (x_1 \cdot p^{-1} + \ldots + x_{i-1} \cdot p^{-p+1})$, čo je v spore s definíciou čísla x_i.

10 Zobrazenie

Zobrazenie f z množiny X do množiny Y je pravidlo, ktoré každému prvku x množiny X priradí určitý prvok $f(x)$ množiny Y. Budeme písať

$$f : X \longrightarrow Y.$$

Množina X sa nazýva obor definície zobrazenia f. Vzniká samozrejmá otázka, čo je to pravidlo. Pre naše potreby sa uspokojíme s tým, že to "nejako vieme".

Príklad 10.1 Zobrazenie f priradí každému prvku z množiny všetkých celých čísiel $\mathbb{Z}$ jeho druhú mocninu $f(z) = z^2$. f je zobrazenie z množiny $\mathbb{Z}$ do množiny $\mathbb{Z}$. Ale pozor, f je aj zobrazenie z množiny $\mathbb{Z}$ do množiny $\mathbb{N}$.
Zobrazenie definované predpisom

$$h(x) = \frac{x^2 - 6}{x^2 - 4x + 3}$$

je zobrazenie z množiny $(-\infty, 1) \cup (1, 3) \cup (3, \infty)$ do množiny $\mathbb{R}$, lebo výraz v menovateľovi je rovný 0 pre $x = 1$ a $x = 3$.

Ak chceme poznať zobrazenie f musíme vedieť pre aké prvky je definované, teda poznať jeho obor definície, t.j. množinu X s vlastnosťou, že pre každý prvok x množiny X je definovaná hodnota $f(x)$ a pre prvok x, ktorý nepatrí do množiny X nie je definovaná hodnota $f(x)$. Samozrejme, pre $x \in X$ musíme vedieť čo je to $f(x)$. Ak množina X je podmnožina $\mathbb{R}$ a hodnoty f sú tiež reálne čísla, tak môžeme nakresliť **graf** zobrazenia f. Graf G_f je množina bodov v rovine so súradnicami $x, f(x)$, kde $x \in X$. Ak stotožníme body so súradnicami $x, f(x)$ s usporiadanou dvojicou $[x, f(x)]$ (to je bežný postup v matematike, ktorý do matematiky zaviedol René Descartes (1596 – 1650)), tak graf G_f zobrazenia stotožníme s množinou usporiadaných dvojíc. Takto získaná množina usporiadaných dvojíc G_f nám dáva všetky informácie o zobrazení f. Vieme určiť obor definície, t.j. vieme určiť pre ktoré x je zobrazenie f definované – pre tie x, pre ktoré existuje y také, že $[x, y] \in G_f$ a pre $x \in X$ vieme z grafu určiť hodnotu $f(x)$ – je to jediné y také, že $[x, y] \in G_f$. Nič nám nebráni stotožniť zobrazenie s jeho grafom, teda s množinou usporiadaných dvojíc s určitou vlastnosťou.

Zhrnieme: množina $f \subseteq A \times B$ sa nazýva **zobrazenie**, ak pre ľubovoľné $[x, y_1] \in f$, $[x, y_2] \in f$ platí $y_1 = y_2$. **Obor definície** zobrazenia f je množina

$$\mathcal{D}(f) = \{x \in A; (\exists y)\, [x, y] \in f\}.$$

Ak $x \in \mathcal{D}(f)$, tak jediný prvok $y \in B$ taký, že $[x, y] \in f$, označíme $f(x)$ a nazývame ho **hodnota** f v bode (prvku) x. **Obor hodnôt** zobrazenia f je množina

$$\mathcal{H}(f) = \{z \in B; (\exists x)\, [x, y] \in f\}.$$

Píšeme

$$f : \mathcal{D}(f) \longrightarrow B.$$

Ak platí $f : X \longrightarrow Y$, tak množina X je jednoznačne určená. Zápis $f : X \longrightarrow Y$ tvrdí $\mathcal{D}(f) = X$ a $\mathcal{H}(f) \subseteq Y$. Ak $Y \subseteq Z$, tak $\mathcal{H}(f) \subseteq Z$ a môžeme písať aj $f : X \longrightarrow Z$. Teda množina Y (množina, v ktorej má zobrazenie hodnoty) nie je jednoznačne určená.

Namiesto slova zobrazenie často používame slovo **funkcia**.

Ak máme dve zobrazenia $f : A \longrightarrow B$, $g : B \longrightarrow C$, tak môžeme zostrojiť zložené zobrazenie $f \circ g : A \longrightarrow C$ jednoduchým predpisom $f \circ g(x) = g(f(x))$ pre $x \in A$ (pozor na zmenu poradia!). Pre každú množinu X existuje identické zobrazenie id_X tejto množiny do seba, ktoré každému prvku $x \in X$ priradí $\mathrm{id}_X(x) = x$.

Zobrazenie $g : B \longrightarrow A$ sa nazýva **inverzné** k zobrazeniu $f : A \longrightarrow B$, ak platí $f \circ g = \mathrm{id}_A$ a $g \circ f = \mathrm{id}_B$. Pojem inverzného zobrazenia závisí nie len od zobrazenia f, ale aj od množín A, B.

Príklad 10.2 Zobrazenie $f : \mathbb{R} \longrightarrow \mathbb{R}$ definované predpisom $f(x) = 2^x$ nemá inverzné zobrazenie. Ale platí aj $f : \mathbb{R} \longrightarrow (0, +\infty)$. Toto zobrazenie má inverzné zobrazenie $g : (0, +\infty) \longrightarrow \mathbb{R}$ definované predpisom $g(x) = \log_2(x)$.

Zobrazenie $f : \mathbb{R} \longrightarrow \langle 0, +\infty)$ definované predpisom $f(x) = x^2$ nemá inverzné zobrazenie. Jeho "časť", zobrazenie $h : \langle 0, +\infty) \longrightarrow \langle 0, +\infty)$ definované rovnakým predpisom "$h(x) = x^2$ pre $x \in \langle 0, +\infty)$" má inverzné zobrazenie $g : \langle 0, +\infty) \longrightarrow \langle 0, +\infty)$ definované predpisom $g(x) = \sqrt{x}$.

Zobrazenie $f : A \longrightarrow B$ sa nazýva prosté, ak pre každé $x_1, x_2 \in A$, $x_1 \neq x_2$, hodnoty $f(x_1) \neq f(x_2)$ sú rozličné. Píšeme

$$f : A \xrightarrow{1-1} B.$$

Konečne, hovoríme, že zobrazenie f je zobrazenie na množinu B, ak pre každé $y \in B$ existuje $x \in A$ také, že $y = f(x)$. Píšeme

$$f : A \xrightarrow{na} B.$$

Veta 10.1 *K zobrazeniu $f : A \longrightarrow B$ existuje inverzné zobrazenie vtedy a len vtedy, keď f je prosté zobrazenie na množinu B.*

Príklad 10.3 V príklade 10.2 sme v prvej časti zmenili množinu tak, aby skúmané zobrazenie bolo "na". Potom už existovalo inverzné zobrazenie. V druhej časti zobrazenie nebolo prosté a preto sme ho uvažovali na "menšej" množine, kde bolo prosté a teda existovalo inverzné.

Ak k zobrazeniu $f : A \longrightarrow B$ existuje inverzné zobrazenie, tak je jediné a označujeme ho f^{-1}. Ak $f : A \longrightarrow B$, $g : B \longrightarrow C$ a existujú inverzné zobrazenia f^{-1} a g^{-1}, tak existuje aj inverzné zobrazenie k zloženému zobrazeniu $f \circ g$ a platí $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

V matematickej analýze sú dôležité zobrazenia (funkcie), ktoré sú rastúce alebo klesajúce. Zrejme rastúce a klesajúce zobrazenie je prosté.

Uvedomte si, že postupnosť, napríklad reálnych čísiel, je zobrazenie z množiny $\mathbb{N}$ do množiny $\mathbb{R}$.

11 Konečné a spočítateľné množiny

Budeme hovoriť, že množiny A, B majú **rovnakú mohutnosť**[9], písať $|A| = |B|$, ak existuje prosté zobrazenie f z množiny A na množinu B. Ľahko sa overí, že vzťah je reflexívny, symetrický a tranzitívny.

Príklad 11.1 Intervaly $\langle 0, 1\rangle$, $\langle 0, 10\rangle$ majú rovnakú mohutnosť, lebo zobrazenie $f(x) = 10x$ pre $x \in \langle 0, 1\rangle$ je prosté a na množinu $\langle 0, 10\rangle$. Podobne možno zistiť, že pre ľubovoľné reálne čísla $a < b$, $c < d$ platí $|\langle a, b\rangle| = |\langle c, d\rangle|$.
Zobrazenie f množiny prirodzených čísiel $\mathbb{N}$ na množinu celých čísiel $\mathbb{Z}$ môžeme najjednoduchšie opísať nasledujúcou schémou:

$$\begin{array}{ccccccccc} 0, & 1, & 2, & 3, & 4, & \dots & 2n, & 2n+1, & \dots \\ 0, & -1, & 1, & -2, & 2, & \dots & n, & -n-1, & \dots \end{array}$$

Teda $|\mathbb{N}| = |\mathbb{Z}|$.

Budeme hovoriť, že množina A má **mohutnosť menšiu alebo rovnakú** ako množina B, ak existuje prosté zobrazenie $f : A \xrightarrow{1-1} B$. Píšeme $|A| \leq |B|$. Konečne, množina A má **mohutnosť menšiu** ako množina B, ak platí $|A| \leq |B|$ a nie je $|A| = |B|$. Píšeme $|A| < |B|$.

Ľahko sa zistí, že nerovnosť je reflexívna a tranzitívna. Platí netriviálne tvrdenie o antisymetrii relácie $\leq$ pre mohutnosti.

[9] rovnaký počet prvkov. Ale pozor, nevieme, čo je to počet prvkov množiny!

Veta 11.1 (Cantorova – Bernsteinova) *Ak* $|A| \leq |B|$ *a* $|B| \leq |A|$, *tak* $|A| = |B|$.

Zákon dichotómie (pre každé dve množiny platí $|A| \leq |B|$ alebo $|B| \leq |A|$) sa nedá dokázať.

Ak má množina X rovnakú mohutnosť ako množina

$$\mathbb{N}_n = \{k \in \mathbb{N} : k < n\} = \{0, 1, \ldots, n-1\},$$

tak hovoríme, že **má** n **prvkov**. Budeme hovoriť, že množina X je **konečná**, ak platí $|X| < |\mathbb{N}|$. Množina, ktorá nie je konečná, sa nazýva **nekonečná**.

Veta 11.2 *Množina* X *je konečná vtedy a len vtedy, keď existuje prirodzené číslo* n *také, že množina* X *má* n *prvkov.*

Budeme hovoriť, že množina X je **spočítateľná**, ak platí $|X| \leq |\mathbb{N}|$. Množina, ktorá nie je spočítateľná, sa nazýva **nespočítateľná**. Každá konečná množina je spočítateľná, ale napríklad množina $\mathbb{N}$ je spočítateľná a nie je konečná.

Uvedieme jedno jednoduché užitočné kritérium pre spočítateľnosť množiny. Budeme hovoriť, že množina X sa **dá zoradiť do postupnosti**, ak existuje zobrazenie f z množiny $\mathbb{N}$ na množinu X.

Veta 11.3 *Množina je spočítateľná vtedy a len vtedy, keď je prázdna alebo sa dá zoradiť do postupnosti.*

Príklad 11.2 Množina celých čísiel $\mathbb{Z}$ je podľa príkladu 11.1 spočítateľná. Ukážeme, že množina $\mathbb{Q} \cap \langle 0, 1\rangle$ racionálnych čísiel z intervalu $\langle 0, 1\rangle$ je spočítateľná. Ľahko vidieť, že túto množinu tvoria čísla 0, 1 a **pravé zlomky**, t.j. zlomky tvaru n/m, kde n, m sú nenulové prirodzené čísla a $n < m$. Tieto čísla zoradíme do postupnosti tak, že najprv napíšeme čísla 0, 1. Potom napíšeme všetky pravé zlomky s menovateľom 2 (existuje jediný), potom všetky pravé zlomky s menovateľom 3 (tie sú dva), atď. Pravých zlomkov s menovateľom n je totiž $n - 1$.

$$0,\ 1,\ \frac{1}{2},\ \frac{1}{3},\ \frac{2}{3},\ \frac{1}{4},\ \frac{2}{4},\ \frac{3}{4},\ \ldots,\ \frac{1}{n},\ \frac{2}{n},\ \ldots,\ \frac{n-1}{n},\ \ldots\ .$$

Podobne možno zoradiť do postupnosti celú množinu $\mathbb{Q}$.

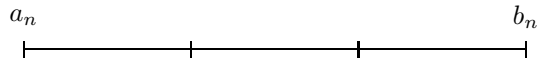
Veta 11.4 *Množina reálnych čísiel* $\mathbb{R}$ *nie je spočítateľná.*

Dôkaz urobíme sporom. Predpokladajme, že množina $\mathbb{R}$ je spočítateľná. Teda $|\mathbb{R}| \leq |\mathbb{N}|$. Keďže $\mathbb{N} \subseteq \mathbb{R}$, tak $|\mathbb{N}| \leq |\mathbb{R}|$. Podľa Cantorovej – Bernsteinovej vety platí $|\mathbb{R}| = |\mathbb{N}|$, teda existuje prosté zobrazenie f množiny $\mathbb{N}$ na množinu $\mathbb{R}$. Zostrojíme reálne číslo, ktoré nie je hodnotou zobrazenia, čo bude hľadaný spor.

Najprv indukciou zostrojíme dve postupnosti reálnych čísiel $\{a_n\}_{n=0}^{\infty}$, $\{b_n\}_{n=0}^{\infty}$ také, že platí

$$a_0 \leq a_1 \leq \ldots \leq a_n \leq a_{n+1} \leq \ldots \leq b_{n+1} \leq b_n \leq \ldots \leq b_1 \leq b_0$$

a pre každé $n \in \mathbb{N}$ je $f(n) \notin \langle a_n, b_n\rangle$. Konštrukcia je jednoduchá. Začneme s ľubovoľným intervalom $\langle a_0, b_0\rangle$, ktorý neobsahuje číslo $f(0)$. Ak už máme zostrojené čísla $a_n < b_n$ s požadovanými vlastnosťami, tak interval $\langle a_n, b_n\rangle$ rozdelíme na tri (napríklad rovnaké) uzavreté intervaly:



Aspoň do jedného z týchto troch intervalov nepatrí číslo $f(n+1)$. Vyberieme jeden taký a jeho koncové body označíme a_{n+1}, b_{n+1}.

Nech $c = \sup\{a_0, a_1, \ldots, a_n, \ldots\}$. Potom platí

$$a_0 \leq a_1 \leq \ldots \leq a_n \leq a_{n+1} \leq \ldots \leq c \leq \ldots \leq b_{n+1} \leq b_n \leq \ldots \leq b_1 \leq b_0.$$

Keby číslo c bolo hodnotou zobrazenia f, tak by existovalo také prirodzené číslo n, že $c = f(n)$. Čísla a_n, b_n sme zostrojili tak, aby $f(n) \notin \langle a_n, b_n \rangle$. Číslo c však patrí do intervalu $\langle a_n, b_n \rangle$, čo je hľadaný spor.

q.e.d.

Pozorný čitateľ si všimne, že sme dokázali podstatne viac: ak $f : \mathbb{N} \longrightarrow \mathbb{R}$ je zobrazenie z množiny prirodzených čísiel do množiny reálnych čísiel, tak v každom otvorenom intervale existuje číslo, ktoré nie je hodnotou zobrazenia f.

12 Čo je to dôkaz

Začneme jednoduchým príkladom. Priznávam určitú nepresnosť, ale tá je v záujme zjednodušenia a tak ľahšieho pochopenia.

Príklad 12.1 Dokážeme, že pre ľubovoľné reálne čísla x, y, z platí

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

Podľa axiómy (16) platí	$(y + z) \cdot x = x \cdot (y + z).$
Podľa axiómy (17) platí	$x \cdot (y + z) = x \cdot y + x \cdot z.$
Podľa axiómy (16) platí	$x \cdot y = y \cdot x, \quad x \cdot z = z \cdot x.$
Potom podľa axiómy (5) platí	$x \cdot y + x \cdot z = y \cdot x + z \cdot x.$
Podľa axiómy (3) platí	$(y + z) \cdot x = x \cdot y + x \cdot z,$
a podľa tej istej axiómy platí	$(y + z) \cdot x = y \cdot x + z \cdot x,$

čo sme chceli dokázať.

Matematická logika vie presne definovať, čo je to dôkaz. Pretože nemáme vybudovaný potrebný aparát, takúto definíciu nemôžeme urobiť. Pokúsime sa však vymedziť pojem dôkazu v matematike. Teda to, čo bude nasledovať, nie je definícia, ale len vymedzenie pojmu dôkaz v rámci možností a poznatkov, ktoré máme k dispozícii.

Najprv urobíme jednu dôležitú poznámku. V matematike máme určité **prvotné pojmy**[10], ktoré nedefinujeme. Príkladom takýchto pojmov je pojem "množina", "reálne číslo" a podobne. Prvotné pojmy majú svoje základné vlastnosti, ktoré sa nazývajú **axiómy**. My sme v 5. časti uviedli axiómy pre reálne čísla, ktoré používa celá dnešná matematika. Iné axiómy by sme museli uviesť, keby sme pracovali s prvotnými pojmami bod, priamka, rovina. Matematik vždy (aj keď to explicitne nepovie) pracuje v nejakej matematickej teórii, ktorá má určité prvotné pojmy a axiómy, ktoré určujú ich základné vlastnosti. Matematickou teóriou rozumieme systém axióm, ktoré pokladáme za pravdivé. Matematickú teóriu označujeme obyčajne $\mathbb{T}$ alebo s príslušným indexom, napríklad systém axióm "(1) – (22) + Bolzanov princíp" pre reálne čísla je prirodzené označiť $\mathbb{T}_{\text{reálne čísla}}$ a nazvať teória reálnych čísiel[11]. Dôkaz, ktorý matematik robí, závisí od použitých prvotných pojmov a ich základných vlastností vyjadrených axiómami. Teda dôkaz je vždy dôkaz v určitej matematickej teórii. V základnom kurze matematickej analýzy obyčajne pracujeme v teórii, ktorá má základné pojmy "množina", "reálne číslo" a axiómy uvedené v 4. a 5. časti. V základnom kurze geometrie máme iné axiómy – obyčajne sú to axiómy euklidovskej geometrie.

Ďalšie pojmy sme už definovali pomocou prvotných pojmov: "prirodzené číslo", "racionálne číslo", "zobrazenie" a podobne. Napríklad, (reálne) číslo sme nazvali prirodzeným číslom, ak patrilo do každej množiny

[10] Podľa slovníka slovenského jazyka je to pojem, ktorý je na začiatku.

[11] Dopúšťame sa určitej nepresnosti. Bolzanov princíp využíva pojem množina. Teda musíme pridať nejaké axiómy o množinách

X s vlastnosťami (c) a (d). Stručne povieme čo je to **definícia**. Mierne vulgarizované, definícia je **skratka**. Namiesto toho, aby sme hovorili že platí

$$(\forall \varepsilon > 0)(\exists n_0)(\forall n > n_0)\, |a_n - a| < \varepsilon)),$$

hovoríme stručne (skratkou), že $\lim_{n\to\infty} a_n = a$. Namiesto toho, aby sme hovorili, že platí

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x, |x - a| < \delta)\, |f(x) - f(a)| < \varepsilon,$$

hovoríme, že funkcia f je spojitá v čísle a. Podobne, jediné reálne číslo z také, že platí $x + z = y$ označujeme $y - x$. Teda v dôkaze je potrebné definíciu "dešifrovať": uvedomiť si a povedať alebo napísať, čo sme skrátili.

Dôkaz v matematickej teórii $\mathbb{T}$ je postupnosť argumentov – výrokových funkcií:

$$\mathcal{V}_1,\, \mathcal{V}_2,\, \ldots,\, \mathcal{V}_n.$$

Argumenty sú troch typov. Inými slovami, každý člen $\mathcal{V}_i$, $i = 1, 2, \ldots, n$ tejto postupnosti má aspoň jednu z nasledujúcich troch vlastností:

a) $\mathcal{V}_i$ je logicky pravdivá výroková funkcia,

b) $\mathcal{V}_i$ je axióma matematickej teórie $\mathbb{T}$, alebo už bola dokázaná v matematickej teórii $\mathbb{T}$.

c) $\mathcal{V}_i$ sme získali z nejakých predchádzajúcich členov dôkazu pomocou odvodzovacieho pravidla.

Ak nejaká výroková funkcia $\mathcal{V}$ bola dokázaná v matematickej teórii $\mathbb{T}$, t.j. už sme zostrojili taký dôkaz

$$\mathcal{V}_1,\, \mathcal{V}_2,\, \ldots,\, \mathcal{V}_n,$$

v matematickej teórii $\mathbb{T}$, že jeho posledný člen $\mathcal{V}_n$ je $\mathcal{V}$, tak $\mathcal{V}$ sa volá **veta** matematickej teórie $\mathbb{T}$. Píšeme $\mathbb{T} \vdash \mathcal{V}$. Zrejme každá axióma je veta. Teda podmienka b) žiada, aby $\mathcal{V}_i$ bola vetou.

Pojem **odvodzovacie pravidlo** sa dá exaktne definovať. Vo všeobecnosti odvodzovacie pravidlo

$$\frac{\mathcal{V}_1, \ldots, \mathcal{V}_k}{\mathcal{W}}$$

hovorí toto: ak výrokové funkcie nad čiarou $\mathcal{V}_1, \ldots, \mathcal{V}_k$ možno dokázať, tak možno dokázať aj výrokovú funkciu pod čiarou $\mathcal{W}$. Základným odvodzovacím pravidlom logiky a aj matematiky je **modus ponens**. Toto pravidlo spočíva v nasledujúcom: ak už máme dokázané výrokové funkcie $\mathcal{V}$, $\mathcal{V} \to \mathcal{W}$, tak pokladáme za dokázanú aj výrokovú funkciu $\mathcal{W}$. Toto pravidlo symbolicky vyjadrujeme zápisom

$$\frac{\mathcal{V},\, \mathcal{V} \to \mathcal{W}}{\mathcal{W}}.$$

Ďalšie dve dôležité pravidlá pomáhajú pracovať s veľkými kvantifikátormi. Jedno je o vynechaní veľkých kvantifikátorov. Predpokladám, že rozumieme, čo je to **číselný výraz**. Zhruba povedané, je to premenná, špeciálne čísla 0,1 a to, čo vzniklo postupne použitím operácií sčítania, odčítania, násobenia a delenia (ak malo zmysel – nedelili sme nulou). Nech $\mathcal{V}(x_1, \ldots, x_k)$ je výroková funkcia a $t_1, \ldots, t_k$ sú číselné výrazy. Potom odvodzovacie pravidlo o vynechaní veľkých kvantifikátorov[12] budeme skrátene nazývať "vyn $\forall$" a znie

$$\frac{(\forall x_1)\, \ldots\, (\forall x_k)\, \mathcal{V}(x_1, \ldots, x_k)}{\mathcal{V}(t_1, \ldots, t_k)}.$$

[12] Vo všeobecnosti namiesto pojmu číselný výraz je potrebné použiť pojem term. Pre naše potreby to však stačí.

Nech $\mathcal{V}(x_1, \ldots, x_k)$ je výroková funkcia. Potom odvodzovacie o zavedení veľkých kvantifikátorov – budeme ho skrátene nazývať "zav $\forall$" – je

$$\frac{\mathcal{V}(x_1, \ldots, x_k)}{(\forall x_1) \ldots (\forall x_k)\, \mathcal{V}(x_1, \ldots, x_k)},$$

Druhé dve odvodzovacie pravidlá sú spojené s malým kvantifikátorom. Nech $\mathcal{V}(x_1, \ldots, x_k)$ je výroková funkcia a t je číselný výraz. Odvodzovacie o zavedení malého kvantifikátora, ktoré nazveme "zav $\exists$" je

$$\frac{\mathcal{V}(t, x_1, \ldots, x_k)}{(\exists y)\, \mathcal{V}(y, x_1, \ldots, x_k)}.$$

Nech $\mathcal{V}(y, x_1, \ldots, x_k)$, $\mathcal{W}(x_1, \ldots, x_k)$ sú výrokové funkcie. Predpokladajme, že vo výrokovej funkcii $\mathcal{W}$ sa premenná y nevyskytuje ani voľne (to už vyplýva zo zápisu) a ani viazane. Potom nasledujúce odvodzovacie pravidlo o zavedení malého kvantifikátora nazveme "$\exists$ zav"

$$\frac{\mathcal{V}(y, x_1, \ldots, x_k) \to \mathcal{W}(x_1, \ldots, x_k)}{(\exists y)\, \mathcal{V}(y, x_1, \ldots, x_k) \to \mathcal{W}(x_1, \ldots, x_k)}.$$

Niektoré odvodzovacie pravidlá sú viazané na matematickú teóriu $\mathbb{T}$, v ktorej pracujeme. Zo strednej školy poznáte odvodzovacie pravidlá matematickej teórie $\mathbb{T}_{\text{reálne čísla}}$, ($t_1$, t_2, t sú číselné výrazy)

$$\frac{t_1 = t_2}{t_1 + t = t_2 + t}, \qquad \frac{t_1 = t_2}{t_1 \cdot t = t_2 \cdot t}, \qquad \frac{t_1 \leq t_2}{t_1 + t \leq t_2 + t}, \qquad \frac{t_1 \leq t_2, \quad 0 \leq t}{t_1 \cdot t \leq t_2 \cdot t}$$

o pripočítaní čísla k rovnosti, o vynásobení rovnosti, o pripočítaní čísla k nerovnosti, o vynásobení nerovnosti nezáporným číslom.

Rozoberieme z uvedeného pohľadu dôkaz uvedený v príklade 12.1. Prezentovaný dôkaz nie je dôkaz v zmysle nášho vymedzenia pojmu "dôkaz". Dôvod je jednoduchý: tak ako to robí väčšina matematikov, mnohé evidentné fakty sme si len mysleli a nenapísali. Doplníme teda to myslené a ukážeme, že to čo získame, už vyhovuje nášmu vymedzeniu pojmu dôkaz.

1°	$(\forall x, y \in \mathbb{R})\, x \cdot y = y \cdot x$	axióma (16)
2°	$(y + z) \cdot x = x \cdot (y + z)$	1° vyn $\forall$
3°	$(\forall x, y, z \in \mathbb{R})\, x \cdot (y + z) = x \cdot y + x \cdot z$	axióma (17)
4°	$x \cdot (y + z) = x \cdot y + x \cdot z$	3° vyn $\forall$
5°	$x \cdot y = y \cdot x$	1° vyn $\forall$
6°	$x \cdot z = z \cdot x$	1° vyn $\forall$
7°	$(\forall x, y, u, v \in \mathbb{R})\, ((x = u \wedge y = v) \to x + y = u + v)$	axióma (5)
8°	$(x \cdot y = y \cdot x \wedge x \cdot z = z \cdot x) \to x \cdot y + x \cdot z = y \cdot x + z \cdot x$	7° vyn $\forall$
9°	$x \cdot y = y \cdot x \to (x \cdot z = z \cdot x \to (x \cdot y = y \cdot x \wedge x \cdot z = z \cdot x))$	tautológia
10°	$x \cdot z = z \cdot x \to (x \cdot y = y \cdot x \wedge x \cdot z = z \cdot x)$	5°, 9° m.p.
11°	$x \cdot y = y \cdot x \wedge x \cdot z = z \cdot x$	6°, 10° m.p.
12°	$x \cdot y + x \cdot z = y \cdot x + z \cdot x$	11°, 8° m.p.
13°	$(\forall x, y, z \in \mathbb{R})\, (x = y \to (y = z \to x = z))$	axióma (3)
14°	$(y + z) \cdot x = x \cdot (y + z) \to$	
	$\to (x \cdot (y + z) = x \cdot y + x \cdot z \to (y + z) \cdot x = x \cdot y + x \cdot z)$	13° vyn $\forall$
15°	$x \cdot (y + z) = x \cdot y + x \cdot z \to (y + z) \cdot x = x \cdot y + x \cdot z$	2°, 13° m.p.
16°	$(y + z) \cdot x = x \cdot y + x \cdot z$	4°, 15° m.p.
17°	$(y + z) \cdot x = x \cdot y + x \cdot z$	
	$\to (x \cdot y + x \cdot z = y \cdot x + z \cdot x \to (y + z) \cdot x = y \cdot x + z \cdot x)$	13° vyn $\forall$
18°	$x \cdot y + x \cdot z = y \cdot x + z \cdot x \to (y + z) \cdot x = y \cdot x + z \cdot x$	16°, 17° m.p.
19°	$(y + z) \cdot x = y \cdot x + z \cdot x$	12°, 18° m.p.
20°	$(\forall x)(\forall y)(\forall z)\, ((y + z) \cdot x = y \cdot x + z \cdot x)$	!(° zav $\forall$

Posledný stĺpec obsahuje **komentár k dôkazu**. Uvádza, ktorá z troch podmienok vymedzenia pojmu dôkaz je splnená a prečo. Napríklad, výroková funkcia 1° je axióma (16) pre množinu reálnych čísiel. Výrokovú funkciu 2° sme získali z výrokovej funkcie d1° pomocou odvodzovacieho pravidla "vynechanie veľkého kvantifikátora" a to tak, že sme za x dosadili číselný výraz $y + z$ a za y číselný výraz x. Výroková funkcia 9° je logicky pravdivá – vznikla z tautológie tvaru $\mathcal{V} \to (\mathcal{W} \to (\mathcal{V} \wedge \mathcal{W}))$. Výroková funkcia 10° vznikla pomocou odvodzovacieho pravidla modus ponens z výrokových funkcií 5° a 9°. Podobne z komentáru vyplýva o ostatných výrokových funkciách, že spĺňajú jednu z troch podmienok položených na členy dôkazu v matematickej teórii $\mathbb{T}_{\text{reálne čísla}}$.

Ak sa pozriete na príklad 12.1, tak vidíte, že sme napísali len sedem členov tohoto dôkazu: 2°, 4°, 5°, 6°, 12°, 16°, 19°. Ostatné sme si len mysleli. Tak sa to obyčajne v matematickej praxi robí.

13 Metódy dôkazu

Z hľadiska metódy, dôkaz, ktorý sme prezentovali v predchádzajúcej časti sa nazýva **priamy dôkaz**. Obyčajne zostrojiť priamy dôkaz nie je jednoduché: potrebujeme prezentovať argumenty a na ich konci má byť dopredu stanovená výroková funkcia. Matematici si uľahčujú prácu tak, že používajú niekoľko málo metód dôkazu a ich kombináciou ľahšie dosiahnu cieľ. Teraz opíšeme základné metódy dôkazu a ilustrujeme ich použitie na príkladoch. Možno budete prekvapení, že existujú v podstate asi len tri[13] metódy dôkazu (okrem priameho dôkazu) a ostatné sú len ich kombináciou.

Prvá metóda dôkazu sa nazýva **veta o dedukcii** a tvrdí toto:

Nech $\mathcal{V}$, $\mathcal{W}$ sú výroky. Ak v matematickej teórii $\mathbb{T}$ s pridanou axiómou $\mathcal{V}$ sa dá dokázať výrok $\mathcal{W}$, tak v matematickej teórii $\mathbb{T}$ sa dá dokázať implikácia $\mathcal{V} \to \mathcal{W}$.

Ak matematik má dokázať implikáciu $\mathcal{V} \to \mathcal{W}$, tak začne svoj dôkaz slovami "nech platí $\mathcal{V}$" a dokáže $\mathcal{W}$. Teda výrok $\mathcal{W}$ dokázal v matematickej teórii rozšírenej o axiómu $\mathcal{V}$. Ani sa nenamáha povedať, že podľa vety o dedukcii sa potom dá dokázať implikácia $\mathcal{V} \to \mathcal{W}$.

Častejšie sa v matematike používa modifikácia vety o dedukcii, v ktorej vystupujú výrokové funkcie. Z určitých dôvodov[14] sa nazýva **metóda pomocných konštánt** a hovorí toto:

Nech $\mathcal{V}(y_1, \ldots, y_l, x_1, \ldots, x_k)$, $\mathcal{W}(y_1, \ldots, y_l, x_1, \ldots, x_k)$ sú výrokové funkcie a $\mathbb{T}$ je matematická teória. Ak

(a) *žiadna axióma teórie $\mathbb{T}$ neobsahuje premenné $y_1, \ldots, y_l$,*

(b) *v matematickej teórii $\mathbb{T}$ rozšírenej o axiómu $\mathcal{V}(y_1, \ldots, y_l, x_1, \ldots, x_k)$ sa dá dokázať výroková funkcia $\mathcal{W}(y_1, \ldots, y_l, x_1, \ldots, x_k)$, pričom v dôkaze nebol použitý kvantifikátor na premenné $y_1, \ldots, y_l$,*

tak v matematickej teórii $\mathbb{T}$ sa dá dokázať výroková funkcia

$$(\forall y_1) \ldots (\forall y_l)\, (\mathcal{V}(y_1, \ldots, y_l, x_1, \ldots, x_k) \to \mathcal{W}(y_1, \ldots, y_l, x_1, \ldots, x_k)).$$

Táto metóda dôkazu sa používa v matematike veľmi často a jej použitie je charakterizované slovným spojením "zvolíme si ľubovoľné ale pevné y". Slovom "ľubovoľné" chceme si zabezpečiť platnosť podmienky (a) – na premennú y nebol urobený žiadny predpoklad (nevyskytuje sa v žiadnej axióme) a slovom "pevné" zabezpečujeme, že počas dôkazu na premennú y nebude použitý kvantifikátor. Mnoho dôkazov v matematickej analýze začína slovami "Zvolíme si ľubovoľné ale pevné ε kladné".

[13] Ak nebudeme rozlišovať medzi vetou o dedukcii a metódou pomocnej konštanty, tak existujú len dve metódy dôkazu.
[14] V základnom kurze matematickej logiky sa tieto dôvody poznajú.

Príklad 13.1 Dokážeme (v teórii reálnych čísiel), že pre ľubovoľné nezáporné čísla x, y, ak $x \leq y$, tak aj $x^2 \leq y^2$. Teda, chceme dokázať

$$(\forall x)(\forall y)\,((x \geq 0 \wedge y \geq 0 \wedge x \leq y) \rightarrow x^2 \leq y^2). \tag{13.17}$$

Nech x, y sú ľubovoľné pevné nezáporné reálne čísla, $x \leq y$. Podľa axiómy (12) máme $x^2 \leq x \cdot y$. Podľa tej istej axiómy máme $x \cdot y \leq y^2$. Podľa axiómy (9) potom platí $x^2 \leq y^2$ Na základe metódy pomocných konštánt dostávame tvrdenie (13.17).

Príklad 13.2 Ukážeme, že pre každé reálne číslo x existuje jediné reálne číslo y také, že $x + y = 0$.

Najprv je potrebné upresniť, čo chceme dokázať. Chceme ukázať dve veci:

(i) pre každé reálne číslo x existuje reálne číslo y také, že $x + y = 0$;

(ii) pre každé x, y_1, $y_2 \in \mathbb{R}$ platí: ak $x + y_1 = 0$ a $x + y_2 = 0$, tak $y_1 = y_2$.

Prvé tvrdenie je axióma (21). Ukážeme druhé tvrdenie.

Nech x, y_1, y_2 sú ľubovoľné pevné reálne čísla, pre ktoré platí

$$\text{(a)} \quad x + y_1 = 0, \qquad \text{(b)} \quad x + y_2 = 0.$$

Ukážeme, že $y_1 = y_2$. Budeme písať očíslovanú sériu rovností a u každej napíšeme číslo axiómy alebo predpokladu, z ktorej bezprostredne vyplýva:

1°	$y_1 + 0 = y_1$	(18)	2°	$y_1 = y_1 + 0$	(2)
3°	$0 = x + y_2$	(b),(2)	4°	$y_1 = y_1$	(1)
5°	$y_1 + 0 = y_1 + (x + y_2)$	(5)	6°	$y_1 = y_1 + (x + y_2)$	(3)
7°	$y_1 + (x + y_2) = (y_1 + x) + y_2$	(13)	8°	$y_1 = (y_1 + x) + y_2$	(3)
9°	$y_1 + x = x + y_1$	(15)	10°	$y_1 + x = 0$	(a),(3)
11°	$y_2 = y_2$	(1)	12°	$(y_1 + x) + y_2 = 0 + y_2$	(5)
13°	$y_1 = 0 + y_2$	(3)	14°	$y_2 + 0 = y_2$	(18)
15°	$0 + y_2 = y_2 + 0$	(2)	16°	$0 + y_2 = y_2$	(3)
17°	$y_1 = y_2$	(3)			

Podľa metódy pomocných konštánt máme tvrdenie (2).

Niekedy je potrebné kombinovať viacej metód.

Príklad 13.3 Dokážeme, že pre ľubovoľné reálne čísla x, y existuje číslo u také, že $x + u = y$. Budeme ho označovať $y - x$. Teda $x + (y - x) = y$.

Podľa axiómy (21) existuje reálne číslo v také, že platí $x+v = 0$. Podľa axiómy (5) platí $(x+v)+y = 0+y$. Podľa axiómy (13) je $x + (v + y) = (x + v) + y$ a podľa axiómy (15) je $0 + y = y + 0$. Podľa axiómy (18) platí $y + 0 = y$. Opakovaným použitím axiómy (3) postupne dostávame $x + (v + y) = y + 0$ a $x + (v + y) = y$. Ak označíme $u = v + y$, tak podľa axiómy (5) platí $x + u = x + (v + y)$ a podľa axiómy (3) máme požadovanú rovnosť $x + u = y$.

Náš postup bol takýto: k teórii reálnych čísiel sme pridali predpoklad $x + v = 0$, kde x, v sú ľubovoľné pevné reálne čísla. V tejto rozšírenej teórii sme ukázali, že $x + (v + y) = y$ a podľa odvodzovacieho pravidla "zav $\exists$" máme $(\exists u)\, x + u = y$. Podľa metódy pomocných konštánt (a odvodzovacieho pravidla "vyn $\forall$") v teórii reálnych čísiel máme dokázanú implikáciu $x + v = 0 \rightarrow (\exists u)\, x + u = y$. Podľa odvodzovacieho pravidla "$zav\exists$" máme

$$(\exists v)\, x + v = 0 \rightarrow (\exists u)\, x + u = y.$$

Predpoklad implikácie je však axióma (21) a teda podľa modus ponens dostávame požadované tvrdenie.

Metódu dôkazu, ktorú teraz opíšeme, poznali už pytagorovci v 6. storočí pred Kr. Je to **metóda dôkazu sporom** a znie takto:

Nech $\mathbb{T}$ je matematická teória, $\mathcal{V}$, $\mathcal{W}$ sú výroky. Ak v matematickej teórii $\mathbb{T}$ rozšírenej o axiómu $\neg\mathcal{V}$ sa dá dokázať $\mathcal{W}$ aj $\neg\mathcal{W}$, tak v matematickej teórii $\mathbb{T}$ sa dá dokázať výrok $\mathcal{V}$.

Ak sa v matematickej teórii dá dokázať nejaký výrok a aj jeho negácia, tak hovoríme, že sa dá dokázať **spor** a matematická teória je **protirečivá**. Teda metóda dôkazu sporom je založená na tom, že k teórii, v ktorej chceme náš výrok dokázať, pridáme jeho negáciu a ukážeme, že takto rozšírená teória je protirečivá.

Príklad 13.4 Typický a historicky asi najstarší dôkaz sporom je dôkaz vety 8.1. Úlohu výroku $\mathcal{V}$ hral výrok "$\sqrt{2}$ nie je racionálne číslo" a úlohu výroku $\mathcal{W}$ hral výrok "m je najmenšie prirodzené číslo také, že existuje prirodzené číslo n s vlastnosťou $\sqrt{2} = n/m$". K matematickej teórii $\mathcal{T}_{\textit{reálne čísla}}$ sme pridali predpoklad $\neg\mathcal{V}$. Podľa vety 6.2 sme bezprostredne dostali výrok $\mathcal{W}$. Potom sme ukázali spor – že platí aj $\neg\mathcal{W}$.

Príklad 13.5 Dôkaz vety 11.4 je tiež jeden z typických dôkazov metódou dôkazu sporom. Predpokladali sme, že neplatí tvrdenie vety a dokázali sme spor: zobrazenie f je na množinu $\mathbb{R}$ a existuje reálne číslo $c \in \mathbb{R}$, ktoré nie je hodnota zobrazenia f.

Príklad 13.6 Dokážeme, že pre ľubovoľné reálne čísla x, y, z platí: ak $x < y$, $z > 0$, tak $x \cdot z < y \cdot z$.

Nech x, y, z sú ľubovoľné pevné reálne čísla také, že $x < y$ a $z > 0$. Podľa definície ostrej nerovnosti $<$ máme $x \leq y$ a $z \geq 0$. Potom podľa axiómy (12) máme $x \cdot z \leq y \cdot z$. Potrebujeme ukázať, že

$$? \quad \neg\, x \cdot z = y \cdot z. \quad ? \tag{13.18}$$

S úmyslom dosiahnuť spor, budeme predpokladať, že platí

$$x \cdot z = y \cdot z. \tag{13.19}$$

Z definície ostrej nerovnosti vyplýva, že $\neg\, z = 0$. Podľa axiómy (22) existuje reálne číslo u také, že

$$z \cdot u = 1. \tag{13.20}$$

Podobne, ako v predchádzajúcich príkladoch, budeme písať sériu rovností alebo nerovností s odvolaním sa na príslušnú axiómu:

1°	$u = u$	(1)
2°	$(x \cdot z) \cdot u = (y \cdot z) \cdot u$	(6)
3°	$x \cdot (z \cdot u) = (x \cdot z) \cdot u$	(14)
4°	$x \cdot (z \cdot u) = (y \cdot z) \cdot u$	(3)
5°	$y \cdot (z \cdot u) = (y \cdot z) \cdot u$	(14)
6°	$x \cdot (z \cdot u) = y \cdot (z \cdot u)$	(3)
7°	$x = x$	(1)
8°	$x \cdot 1 = x$	(19)
9°	$x \cdot (z \cdot u) = x \cdot 1$	(13.20) *a* (3)
10°	$x \cdot (z \cdot u) = x$	(3)
11°	$x = x \cdot (z \cdot u)$	(2)
12°	$y = y$	(1)
13°	$y \cdot (z \cdot u) = y \cdot 1$	(6)
14°	$y \cdot 1 = y$	(19)
15°	$y \cdot (z \cdot u) = y$	(3)
16°	$x \cdot (z \cdot u) = y$	(3)
17°	$x = y$	(3)

Podľa predpokladu $x < y$ platí $\neg\, x = y$ a to je hľadaný spor.

Ľahko vidieť, že sme kombinovali metódu pomocných konštánt a metódu dôkazu sporom.

Ďalšie spôsoby (nie metódy) sú založené na využívaní niektorých tautológií alebo odvodzovacích pravidiel. Dôkaz vety 8.2 bol založený na odvodzovacom pravidle

$$\frac{\mathcal{V}_1 \to \mathcal{W}, \ldots, \mathcal{V}_k \to \mathcal{W},\ \mathcal{V}_1 \vee \ldots \vee \mathcal{V}_k}{\mathcal{W}}.$$

Nazývame ho **rozbor prípadov**.

Príklad 13.7 Typický dôkaz rozborom prípadov bol dôkaz vety 8.2. Mali sme tri výroky (čísla $a < b$ boli pevne zvolené) $\mathcal{V}_1$, $\mathcal{V}_2$ a $\mathcal{V}_3$:

$$0 \leq a < b, \qquad a < 0 < b, \qquad a < b \leq 0.$$

Výrok $\mathcal{W}$ je výrok $(\exists r \in \mathbb{Q})\, a < r < b$. Metódou pomocných konštánt sme dokázali, tri implikácie:

$$\mathcal{V}_1 \to \mathcal{W}, \qquad \mathcal{V}_2 \to \mathcal{W}, \qquad \mathcal{V}_3 \to \mathcal{W}.$$

Podľa axiómy $(10)^*$ platí

$$\mathcal{V}_1 \vee \mathcal{V}_2 \vee \mathcal{V}_3.$$

Použitím špeciálneho prípadu odvodzovacieho pravidla "rozbor prípadov"

$$\frac{\mathcal{V}_1 \to \mathcal{W}, \quad \mathcal{V}_2 \to \mathcal{W}, \quad \mathcal{V}_3 \to \mathcal{W}, \qquad \mathcal{V}_1 \vee \mathcal{V}_2 \vee \mathcal{V}_3}{\mathcal{W}}$$

sme dostali tvrdenie vety.

Na záver uvedieme často používané spôsoby dôkazu implikácie. Ak v matematickej teórii $\mathbb{T}$ chceme dokázať implikáciu $\mathcal{V} \to \mathcal{W}$, tak môžeme využiť odvodzovacie pravidlo o dôkaze nepriamo

$$\frac{\neg\mathcal{W} \to \neg\mathcal{V}}{\mathcal{V} \to \mathcal{W}}$$

a dokazovať **obrátenú implikáciu** $\neg\mathcal{W} \to \neg\mathcal{V}$. Často to kombinujeme s vetou o dedukcii a v matematickej teórii $\mathbb{T}$ s pridanou axiómou $\neg\mathcal{W}$ dokazujeme $\neg\mathcal{V}$.

Iný spôsob dôkazu implikácie je založený na metóde dôkazu sporom. K matematickej teórii pridáme predpoklad neplatnosti implikácie, obyčajne v tvare dvoch predpokladov $\mathcal{V}$ a $\neg\mathcal{W}$ a dokážeme spor.

Príklad 13.8 Matematika používa veľmi často matematickú indukciu buď v tvare vety 6.1 alebo v tvare vety 6.3. Z hľadiska matematickej logiky (alebo ak chcete, z hľadiska teórie dôkazu), to nie je nová metóda dôkazu. Je to dôkaz založený na využití odvodzovacieho pravidla ($\mathcal{V}(x)$ je výroková funkcia) – v prvom prípade s dvomi indukčnými krokmi:

$$\frac{\mathcal{V}(0), \quad (\forall n \in \mathbb{N})\,(\mathcal{V}(n) \to \mathcal{V}(n+1))}{(\forall \in \mathbb{N})\,\mathcal{V}(n)}$$

a v druhom prípade s jedným indukčným krokom:

$$\frac{(\forall n \in \mathbb{N})\,((\forall k < n, k \in \mathbb{N})\,\mathcal{V}(k) \to \mathcal{V}(n))}{(\forall n \in \mathbb{N})\,\mathcal{V}(n)}.$$

Naviac, takmer vždy je použitie takýchto odvodzovacích pravidiel kombinované s použitím metódy pomocnej konštanty.

Analyzujte z tohoto pohľadu dôkazy v príkladoch 6.1 a 6.3!

Odporúčam čitateľovi, aby si zobral skriptá [MO] (ku ktorým asi aj tak siahne pri príprave na skúšku z matematickej analýzy) a analyzoval v duchu uvedených príkladov dôkazy časti 1 týchto skrípt, alebo dôkazy viet 2.3.6, 2.4.6 a 2.4.8. Samozrejme, aj analýza iných dôkazov alebo analýza dôkazov tvrdení prezentovaných v prednáškach z algebry je dobrým cvičením pre pochopenie a naštudovanie problematiky.

Literatúra

[Bu] Bukovský L., *Množiny a všeličo okolo nich,* Alfa, Bratislava 1985

[MO] Mihalíková B. a Ohriska J., *Matematická analýza 1,* PF UPJŠ, Košice 1994