Úvodní kurz z matematiky

Věty a důkazy

Dalibor Šmíd

MFF UK

Styl výkladu matematiky na VŠ typu MFF se výrazně liší od středoškolské matematiky, a blíží se tomu, jakým způsobem se matematika standardně zapisuje v odborné literatuře. Více abstrakce, rigoróznější vyjadřování a větší samostatnost očekávaná od studentů bývají pro většinu tím nejtěžším, s čím se musejí v prvním semestru vyrovnat. Tato přednáška má poskytnout základní přehled, který vám usnadní čtení učebních textů a sledování přednášek.

Základní doporučení

1. Nečekejte, že všechno pochopíte na první přečtení/poslech. Napoprvé se snažte především porozumět definicím, zněním jednotlivých tvrzení, ilustrativním příkladům a motivaci, proč se to celé dělá.
2. Pište si vlastní poznámky, vracejte se k nim a doplňujte je s pomocí literatury.
3. Ptejte se. Během přednášky, po ní, na cvičeních, ostatních studentů.
4. U důkazů se snažte pochopit každý jednotlivý krok a uvědomit si, jaké předpoklady ze znění tvrzení se při něm použijí. Pojmenujte si pro sebe neformálně základní myšlenku důkazu a pak se pokuste ji rozvinout a důkaz rigorózně zapsat. Chce to trénink jako všechno.

Matematický výklad obsahuje určité standardizované elementy, které tvoří jeho kostru:

Definice je zavedení a přesné vymezení pojmu a obvykle i jeho označení

Tvrzení je výrok, který říká něco o dříve zavedených pojmech a jejich vlastnostech či vztazích, jeho platnost musí být stvrzena důkazem, který obvykle bezprostředně následuje.

Věta je významnější tvrzení, mající často standardizovaný název („Bolzano-Weierstrassova věta“, „Věta o dimenzi jádra a obrazu“).

Lemma je pomocné tvrzení, které se použije v důkazu jiného tvrzení nebo věty. Existují ale lemmata, která v průběhu let nabyla většího významu a získala pak i speciální pojmenování.

Důsledek je tvrzení plynoucí z předchozího tvrzení, obvykle natolik přímočaře, že se nepíše samostatný důkaz.

Tato kostra je pak obalena „masem“, které se liší podle typu tématu a stylu přednášejícího. Obvykle jsou zastoupeny *Příklady* motivační a ilustrační, *Cvičení*, na nichž si čtenář může otestovat své porozumění nebo si výklad sám doplnit, různé formy úvodů, poznámek, komentářů a shrnutí, často bez výslovného označení, obrázky a schémata mající vizualizovat některé pojmy a myšlenky apod.

Důkaz standardně bezprostředně následuje dokazované tvrzení a využívá v něm použitého označení. Občas ale může být *odložen* (až po dokázání nějakých lemmat nebo dobudování teorie), *nastíněn* nebo část či celý *vynechán* (pokud autor věří, že čtenář zvládne detaily doplnit sám), nebo dokonce proveden ještě před tvrzením ve formě jakéhosi odvození. Pokud si nejste jisti, se kterou z možností máte právě tu čest, ptejte se.

Důležitou součástí matematiky jsou *protipříklady*, které ilustrují, proč tvrzení neplatí, když se vynechá některý předpoklad. Vymýšlejte si je i sami pro sebe!

Tvorba důkazů zajímavějších tvrzení je do značné míry kreativní proces, má ale solidní řemeslný základ, který si nejlépe osvojíte na tvrzeních jednodušších. V první řadě jde o:

- rozlišování, kdy má tvrzení formu implikace a kdy ekvivalence a která část důkazu dokazuje který směr ekvivalence
- rozlišování logické formy důkazu jedné implikace: důkaz *přímý*, *nepřímý*, *sporem*
- schopnost zkontrolovat (a časem samostatně sepsat) důkaz „z definic“, tj. bez použití netriviálních tvrzení
- porozumění různým formám matematické indukce

Mějme tvrzení ve tvaru $A \Rightarrow B$, kde A, B jsou výroky. Jeho *přímý důkaz* spočívá v nalezení výroků $A_1, A_2, \dots, A_k$ takových, že výroky $A \Rightarrow A_1$, $A_1 \Rightarrow A_2, \dots, A \Rightarrow B$ jsou platné a přímo plynou z definic nebo dříve dokázaných tvrzení. Jednoduchým příkladem budiž

Tvrzení
Je-li přirozené číslo n liché, pak je i n^2 liché.

Důkaz.
Pokud je n liché, pak existuje $k \in \mathbb{N}$ takové, že $n = 2k - 1$. Pro takové n platí, že $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2K - 1$, kde $K = 2k^2 - 2k + 1$. Protože K je přirozené číslo, je n^2 liché přirozené číslo. $\square$

Nepřímý důkaz se opírá o logickou ekvivalenci výroků $A \Rightarrow B$ a $B' \Rightarrow A'$ („z negace B plyne negace A“). Tomu se říká *obměna implikace* (neplést s *opačnou* neboli *obrácenou* implikací $B \Rightarrow A$, která s $A \Rightarrow B$ logicky ekvivalentní není). Jednoduchý příklad:

TVRZENÍ
Nechť $n \in \mathbb{N}$. Je-li $5n + 3$ sudé, pak je n liché.

DŮKAZ.
Obměněná implikace zní: je-li n sudé, pak je $5n + 3$ liché. Pro n sudé existuje $k \in \mathbb{N}$ takové, že $n = 2k$. Pak $5n + 3 = 10k + 3 = 2(5k + 2) - 1$. Protože $K := 5k + 2$ je přirozené, je $2K - 1$ liché. $\square$

Obě zmíněná tvrzení se dají zesílit na ekvivalence:

Tvrzení

Přirozené číslo n je liché tehdy a jen tehdy, je-li n^2 liché.

Tvrzení

Nechť $n \in \mathbb{N}$. Pak $5n + 3$ je sudé, právě když je n liché.

V angličtině vyjadřují ekvivalenci spojka „if and only if" a její zkratka „iff".

Dokážeme jen první tvrzení. Implikaci „n liché" $\Rightarrow$ „n^2 liché" už máme, opačnou implikaci „n^2 liché" $\Rightarrow$ „n liché" nahradíme její obměnou „n sudé" $\Rightarrow$ „n^2 sudé". Pro tu stačí přepsat druhou mocninu sudého čísla $n = 2k$ jako $n^2 = 4k^2 = 2(2k^2)$.

Důkaz sporem je aplikací logické ekvivalence mezi $A \Rightarrow B$ a $(A \wedge B')'$. Ukazujeme při něm tedy neplatnost výroku „A a zároveň negace B“, obvykle tím, že z něj odvodíme nějaký důsledek, který je v rozporu s předpoklady tvrzení, definicemi nebo dříve dokázanými tvrzeními.

Tvrzení

Jsou-li $x_1, x_2, \ldots, x_n$ reálná čísla, pak existuje $i \in \{1, \ldots, n\}$ takové, že $x_i \geq \frac{1}{n}(x_1 + \ldots + x_n)$.

Důkaz.

Předpokládejme, že pro všechna $i \in \{1, \ldots, n\}$ je $x_i < \frac{1}{n}(x_1 + \ldots + x_n)$. Sečteme-li těchto n nerovností, vychází nám, že reálné číslo $x_1 + \ldots + x_n$ je menší než ono samo. To je spor se základními vlastnostmi relace $<$ na reálných číslech. $\square$

Trochu odlišná varianta důkazu sporem se používá v důkazu iracionality $\sqrt{2}$:

TVRZENÍ
Neexistuje žádná dvojice přirozených čísel (m, n) *taková, že* $\frac{m^2}{n^2} = 2$.

DŮKAZ.
Pro spor předpokládejme, že aspoň jedna taková dvojice (m, n) existuje a zároveň je to taková, že n je nejmenší možné. Protože $m^2 = 2n^2$, je m^2 sudé a dle dříve dokázaného tvrzení je i m sudé. Dosazením $m = 2k$ do $m^2 = 2n^2$ a vykrácením dvojky dostáváme, že $n^2 = 2k^2$. Opakováním stejné úvahy zjistíme, že $n = 2l$ pro nějaké $l \in \mathbb{N}$. Zjevně $l < n$ a $k^2 = 2l^2$, tedy (k, l) je dvojice splňující předpoklad, jejíž druhá složka je menší než n, což je spor. $\square$

Matematická indukce se používá pro důkaz tvrzení typu „pro každé $n \in \mathbb{N}$ platí $V(n)$", kde $V(n)$ je nějaký výrok závislý na proměnné n. Sestává ze dvou částí:

1. Důkaz výroku $V(1)$.
2. Důkaz výroku $\forall n \in \mathbb{N} : (V(n) \Rightarrow V(n+1))$

Druhá část je tedy důkazem výroku $V(n+1)$ za předpokladu, že platí výrok $V(n)$.

TVRZENÍ
Pro každé $n \in \mathbb{N}$ je číslo $10^n - 4$ dělitelné šesti.

DŮKAZ.
Výrok $V(1)$=„$10^1 - 4$ je dělitelné šesti" zjevně platí.
Předpokládejme, že platí $V(n)$, tedy že $10^n - 4 = 6k$ pro nějaké k celé. Pak

$$10^{n+1} - 4 = 10 \cdot (10^n - 4) + 40 - 4 = 10 \cdot 6k + 36$$

je dělitelné šesti, přičemž ve druhé rovnosti jsme využili indukční předpoklad. Platí tedy $V(n+1)$ a tím i $\forall n \in \mathbb{N} : V(n)$. $\square$

TVRZENÍ
Pro každé $n \in \mathbb{N}$ je $2^n > n$.

DŮKAZ.
Pro $n = 1$ dostáváme výrok $2 > 1$, který jistě platí.
Předpokládejme, že pro nějaké n je $2^n > n$. Potom

$$2^{n+1} = 2 \cdot 2^n = 2^n + 2^n > n + 1$$

V posledním kroku jsme využili platnost výroků $2^n > n$ (indukční předpoklad) a $2^n > 1$ (platí pro všechna $n \in \mathbb{N}$).
Celkově dostáváme, že $2^{n+1} > n + 1$. $\square$

Často vídanou variantou matematické indukce je *silná* nebo též *složená* indukce, kde se v indukčním kroku namísto pouze $V(n)$ předpokládá platnost $V(k)$ pro všechna k od 1 až do n.
Snadným příkladem je důkaz explicitního tvaru n-tého členu Fibonacciho posloupnosti, v němž se do rekurentního předpisu $a_{n+1} = a_n + a_{n-1}$ dosadí explicitní vztahy pro a_n a a_{n-1}.

Další čtení:

- Portál středoškolské matematiky
  `https://www2.karlin.mff.cuni.cz/~portal/logika/`
- How do undergraduates do mathematics
  `https://www.maths.ox.ac.uk/system/files/attachments/study_public_0.pdf`
- Úvodní kapitola z
  `https://www2.karlin.mff.cuni.cz/~pick/analyza.pdf`