Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 2002/2003
Michal Marvan

–1. Tvrzení a důkazy

Petitem (malým písmem) vyznačujeme části textu, které obsahují doplňující a rozšiřující výklad. Je možné (a někdy nutné) je při prvním čtení vynechat. Toto pravidlo neplatí pro příklady, cvičení a následující odstavec.

Matematika je deduktivní věda a algebra je její součást. Všechny pojmy jsou vymezeny *definicí*. Kriteriem pravdivosti matematického tvrzení je *důkaz*. To je potřeba brát smrtelně vážně.

Matematická tvrzení jsou zpravidla výroky: mohou být buď pravdivé nebo nepravdivé, přičemž vždy nastane právě jedna z těchto dvou možností (přestože nemusí být známo která).

Předpokládáme, že čtenář zná ze střední školy základy výrokového počtu (logické spojky negace $\neg$, konjunkce $\wedge$, disjunkce $\vee$, implikace $\Rightarrow$, ekvivalence $\Leftrightarrow$ výroků; obecný kvantifikátor $\forall$, existenční kvantifikátor $\exists$). Čtenář zběhlý v ověřování ekvivalence výroků pomocí pravdivostních tabulek může této dovednosti využít, ale není to podmínkou.

Výrokový počet stojí v pozadí všech dokazovacích metod. Nejčastěji mají matematická tvrzení podobu implikace $\alpha \Rightarrow \beta$ a umožňují tak provádět přímé a nepřímé důkazy dalších tvrzení.

Přímý důkaz pravdivosti tvrzení β spočívá v důkazu pravdivosti tvrzení $\alpha \Rightarrow \beta$ a v důkazu pravdivosti tvrzení α. Jinak řečeno, máme-li dokázat, že β platí, stačí dokázat, že platí α a že platí $\alpha \Rightarrow \beta$.

Příklad. Nechť platí tvrzení: „Kdo lže, ten krade.“ Nechť dále platí „x lže.“ Potom platí i „x krade.“

Nepřímý důkaz pravdivosti tvrzení β spočívá v důkazu pravdivosti tvrzení $\neg\beta \Rightarrow \neg\gamma$ a v důkazu pravdivosti tvrzení γ (pak β skutečně platí, protože kdyby β neplatilo, pak by neplatilo i γ). Jinak řečeno, máme-li dokázat, že β platí, stačí dokázat, že platí γ a že platí $\neg\beta \Rightarrow \neg\gamma$.

Příklad. Nechť platí tvrzení: „Kdo lže, ten krade.“ Nechť dále platí „x nekrade.“ Potom platí i „x nelže“ (protože kdyby lhal, pak by i kradl).

Podstatnou roli v důkazech sporem hraje negace. Všechna důležitá pravidla pro negování výroků jsou uvedena v následující tabulce:

	ϕ	$\neg\phi$
negace	$\neg\alpha$	α
konjunkce	$\alpha \wedge \beta$	$\neg\alpha \vee \neg\beta$
disjunkce	$\alpha \vee \beta$	$\neg\alpha \wedge \neg\beta$
implikace	$\alpha \Rightarrow \beta$	$\alpha \wedge \neg\beta$
obecný kvantifikátor	$\forall_x \alpha(x)$	$\exists_x \neg\alpha(x)$
existenční kvantifikátor	$\exists_x \alpha(x)$	$\forall_x \neg\alpha(x)$

K pravidlu o negaci implikace lze dojít následující úvahou: Implikace $\alpha \Rightarrow \beta$ je pravdivá právě tehdy, když při každém výskytu α nastane i β. Tudíž, *tvrzení $\alpha \Rightarrow \beta$ je vyvráceno, jestliže předpoklad α nastane, ale důsledek β se nedostaví.* Všimněte si, že pokud α vůbec nenastane, je nutno implikaci považovat za pravdivou.

Příklad. Negujte výrok: „Nebude-li pršet, nezmoknem."

Řešení: (1) Úvahou: Tvrzení je vyvráceno, jestliže nebude pršet (splněný předpoklad), a přesto zmokneme (nesplněný závěr).

(2) Výpočtem: Jde o výrok „$\neg$ pršet $\Rightarrow$ $\neg$ zmoknem." Negaci výroku $\neg\alpha \Rightarrow \neg\beta$ obdržíme výpočtem $\neg(\neg\alpha \Rightarrow \neg\beta) \equiv \neg\alpha \wedge \neg\neg\beta \equiv \neg\alpha \wedge \beta$ v souladu s pravidly uvedenými v tabulce. Výsledkem je „$\neg$ pršet $\wedge$ zmoknem."

Cvičení. Ukažte, že negací ekvivalence $\alpha \Leftrightarrow \beta$ je výrok $(\alpha \wedge \neg\beta) \vee (\beta \wedge \neg\alpha)$.

K pravidlu o negaci obecného kvantifikátoru dojdeme podobnou úvahou: Tvrzení $\forall_x\, \alpha(x)$ je vyvráceno, jestliže nalezneme x, pro něž $\alpha(x)$ neplatí. Takové x se nazývá *protipříklad* k tvrzení $\forall_x\, \alpha(x)$.

Příklad. Negujte výrok: „Kdo lže, ten krade."

Řešení: Jde o výrok „$\forall_x (x$ lže $\Rightarrow x$ krade)." Negací výroku $\forall_x[\alpha(x) \Rightarrow \beta(x)]$ je výrok $\exists_x[\alpha(x) \wedge \neg\beta(x)]$. V našem případě: „Existuje někdo, kdo lže, ale nekrade." Člověk, který lže a přitom nekrade pak slouží jako protipříklad k tvrzení „Kdo lže, ten krade." (Tento příklad relativizuje poněkud radikální závěry učiněné na předchozí straně.)

Poznámka o roli kvantifikátorů: Pravdivost výroku závislého na proměnné x závisí na konkrétní hodnotě proměnné x. „Výrok" $x > 0$ není pravdivý ani nepravdivý, pokud není známo x, nebo dokud není proměnná x kvantifikována.

Příklad. $\exists_{x\in\mathbf{R}}\, x > 0$ je pravdivý výrok (platí například $1 > 0$).

$\forall_{x\in\mathbf{R}}\, x > 0$ je nepravdivý výrok (máme protipříklad: neplatí $-1 > 0$).

Obecný kvantifikátor se často vynechává, je-li zřejmý z kontextu. Implikace $x > 0 \Rightarrow x > -1$ je pravdivá bez ohledu na konkrétní hodnotu x (je-li x reálné číslo), striktně vzato bychom však měli psát $\forall_{x\in\mathbf{R}}(x > 0 \Rightarrow x > -1)$.

V kombinaci s implikací lze předpoklady implikace přesunout do obecného kvantifikátoru:

$$\forall_{\substack{x\in\mathbf{R}\\ x>0}} x > -1.$$

Podobně lze upravit existenční kvantifikátor v kombinaci s konjunkcí: $\exists_{x\in\mathbf{R}}(x > 0 \wedge x^2 = 2)$ lze psát jako

$$\exists_{\substack{x\in\mathbf{R}\\ x>0}} x^2 = 2.$$

Existují standardní postupy důkazů tvrzení, jež mají podobu složeného výroku s některou z logických spojek či kvantifikátorů. V případě kvantifikovaných výroků máme následující možnosti přímého důkazu:

1. Výrok $\forall_{x\in X}\, \psi(x)$ dokážeme tak, že zvolíme libovolný prvek $x_0 \in X$ a dokážeme $\psi(x_0)$.
2. Výrok $\exists_{x\in X}\, \psi(x)$ dokážeme tak, že najdeme prvek $x_0 \in X$ takový, že platí $\psi(x_0)$.

Je-li výrok $\psi(x)$ opět kvantifikován, postupujeme opět podle týchž pravidel. Je-li výrok $\psi(x)$ složen z výroků $\alpha(x)$ a $\beta(x)$ pomocí logických spojek, máme následující možnosti:

3. Konjunkci $\alpha \wedge \beta$ dokazujeme tak, že dokážeme pravdivost obou výroků α a β.
4. Disjunkci $\alpha \vee \beta$ dokazujeme tak, že dokážeme pravdivost alespoň jednoho z výroků α, β; často se toho dosáhne rozdělením důkazu na dva vzájemně se doplňující případy, kdy první z nich vede k α a druhý k β.
5. Implikaci $\alpha \Rightarrow \beta$ dokazujeme tak, že výrok α dočasně (v průběhu důkazu) považujeme za pravdivé tvrzení a dokazujeme tvrzení β.

6. Ekvivalenci $\alpha \Leftrightarrow \beta$ dokazujeme tak, že dokážeme obě implikace $\alpha \Rightarrow \beta$ a $\beta \Rightarrow \alpha$.
V důkazech smíme použít i všechna již dokázaná tvrzení budované teorie.

Vytvoření schematu přímého důkazu je automatizovatelné (schema by mohl vytvořit počítač) a závisí jen na vyskytujících se logických spojkách a kvantifikátorech a nezávisí na konkrétním obsahu výroků, z nichž je dokazované tvrzení složeno.

7. Nepřímý důkaz tvrzení α konstruujeme tak, že připustíme, že tvrzení α neplatí (tj. dočasně považujeme $\neg\alpha$ za pravdivé tvrzení) a dojdeme ke sporu s některým pravdivým tvrzením.

Příklad. Předpokládejme, že platí obvyklá aritmetika reálných čísel, a že již byla dokázána pravdivost tvrzení:

A. Součet kladného reálého čísla s nezáporným reálným číslem je kladné reálné číslo.

B. Dvojmoc reálného čísla je nezáporné reálné číslo.

C. Dvojmoc nenulového reálného čísla je kladné reálné číslo.

D. Nula není kladné číslo.

Dokažme pravdivost tvrzení

E. Pro libovolná reálná čísla x, y platí: $x^2 + y^2 = 0$ právě tehdy, když $x = 0$ a zároveň $y = 0$.

Důkaz: Níže uvedený text zapsaný *kurzívou* představuje důkaz tvrzení **E**, text zapsaný obyčejnou antikvou představuje komentář. Tvrzení **E** má podobu

$$\underset{x\in\mathbf{R}}{\forall}\ \underset{y\in\mathbf{R}}{\forall}\ [x^2 + y^2 = 0 \Leftrightarrow (x = 0 \wedge y = 0)].$$

Tvrzení je uvedeno obecným kvantifikátorem, proto podle pravidla 1 začneme předpokladem: „*Buď x libovolné reálné číslo.*“ Poté následuje další obecný kvantifikátor, proto podle pravidla 1 pokračujeme analogickým předpokladem: „*Buď y libovolné reálné číslo.*“

Následuje ekvivalence, kterou podle pravidla 6 rozdělíme na dvě implikace. Začneme tou jednodušší: „*Dokazujme nejprve implikaci ‚$\Leftarrow$‘.*“ Podle pravidla 5 začneme dočasným zavedením předpokladu mezi pravdivá tvrzení: „*Nechť $x = 0$ a $y = 0$.*“ K závěru „$x^2 + y^2 = 0$,“ pak snadno dojdeme dosazením za x a y s použitím aritmetiky reálných čísel: „*Pak $x^2 + y^2 = 0^2 + 0^2 = 0 + 0 = 0$ a implikace je dokázána.*“

Dokazujme implikaci ‚$\Rightarrow$‘. Podle pravidla 5 začneme dočasným zavedením předpokladu mezi pravdivá tvrzení: „*Nechť $x^2+y^2 = 0$.*“ Máme dokázat konjunkci „$x = 0 \wedge y = 0$,“ ale žádné z tvrzení **A**, **B**, **C**, **D** k ní přímo nevede. Můžeme však provést důkaz nepřímý, což podle pravidla 7 znamená, že zavedeme negaci výroku „$x = 0 \wedge y = 0$“ jako dočasně pravdivé tvrzení a pokusíme se nalézt spor. Negací konjunkce „$x = 0 \wedge y = 0$“ je přitom disjunkce „$x \neq 0 \vee y \neq 0$.“ Pokračujeme slovem „připusťme“ na znamení, že formulujeme tvrzení, jež bude nakonec vyvráceno: „*Připusťme, že $x \neq 0$ nebo $y \neq 0$.*“ Jde o disjunkci, proto podobně jako v pravidle 4 postupujeme dále ve dvou alternativách: „*Jestliže $x \neq 0$, pak podle tvrzení* **C** *je x^2 kladné číslo, zatímco y^2 je nezáporné číslo podle* **B**. *Tudíž, podle* **A** *je $x^2 + y^2$ kladné číslo, což je podle* **D** *ve sporu s učiněným předpokladem $x^2 + y^2 = 0$. Tím je hotov důkaz implikace ‚$\Rightarrow$‘ v případě, že $x \neq 0$.*“ Druhá alternativa se dokazuje slovo od slova stejně, zaměníme-li všude x za y a naopak. Proto pokračujeme: „*V případě, že $y \neq 0$, se implikace ‚$\Rightarrow$‘ dokazuje analogicky.*“

Matematické vědomosti lidstva se neustále rozšiřují – díky důkazům neustále přibývá matematických tvrzení, která platí. Ne všechny pojmy však lze definovat a ne všechna tvrzení lze dokázat. Nejvíce mezer zeje právě v základech matematiky – evidentně nelze definovat definici, evidentně nelze dokázat správnost všech pravidel, podle kterých dokazujeme. V samotných základech matemtiky tak nutně stojí jistý soubor tvrzení, která dokázat nelze (není z čeho) a nezbývá, než je přijmout v dobré víře, že jsou správná a nevedou k rozporům.

Pro potřeby této přednášky si soubor tvrzení přijatých v dobré víře rozšíříme o celou aritmetiku reálných čísel. Budeme tedy předpokládat, že jsou známy pojmy přirozené, celé, racionální, reálné a komplexní číslo, že jsou známy základní aritmetické operace s nimi a jejich vlastnosti včetně dělení přirozených čísel se zbytkem, a že jsou známy vlastnosti uspořádání reálných čísel podle velikosti.