1. Matematika, logika

Co je matematika? Rozhodně to nejsou vzorečky k učení nazpaměť—to jsou počty. Matematika je jazyk, který nám dovoluje vyjádřit, že mezi určitými objekty existují rozličné vztahy, popřípadě že tyto objekty spolu různě interagují a tyto interakce splňují rozličná pravidla. Výhodou tohoto jazyka je jeho přesnost, protože v matematice je přesně definováno (určeno), co jednotlivé pojmy a značky znamenají. Další výhodou je jeho stručnost.

Je například možné říci: „Uvažujme kvantitu takovou, že když udělám čtvercové pole o straně rovné této kvantitě, pak bude mít toto pole výměru 4 jednotky“. Matematika nám umožňuje namísto toho říct „uvažujme číslo $\sqrt{4}$.“ Mimochodem, není to umělý příklad. Ta dlouhá věta ukazuje, jak lidé s matematikou začínali, první spisky o výpočtech a algoritmech (starověký Egypt, Čína, Indie,…) takto fungovaly.

Kromě stručnosti a přesnosti má matematický jazyk ještě další podstatnou výhodu: Umožňuje relativně efektivně hledat způsoby, jak ze zachycených vztahů, interakcí a pravidel získat co nejvíce informací. Například víme, že ona kvantita musí být 2.

Nevýhodou matematického jazyka je, že mu normální člověk nerozumí. Pokud jej někdo potřebuje (vědci, inženýři), tak se jej musí (jako každý jiný jazyk) naučit, a to v zásadě klasickým způsobem. I matematický jazyk má svá slovíčka (pojmy, značení) a gramatiku (například pravidla logiky), jeho obtížnost je ale v tom, že se podstatně liší od ostatních lidských jazyků a navíc je při jeho používání nutno silně používat mozek, a to ještě jedním specifickým způsobem (v zásadě tím, co měří IQ testy), což pro hodně lidí představuje problém a pro některé problém nepřekonatelný. Jedním z cílů tohoto textu je tento jazyk čtenáře alespoň trochu naučit. Bude to od něj samozřejmě vyžadovat práci, protože nejlépe se člověk jazyk naučí tak, že jakmile jej trochu pochytí, začne jím mluvit.

Zkusme ukázat ještě jeden pohled na věc: Umět matematiku znamená především umět kolem sebe nacházet vztahy a pravidelnosti a vyjadřovat je matematickým jazykem, struktury vzniklé matematickým popisem pak prozkoumat a problém vyřešit. A naopak, je to i schopnost číst matematický jazyk, porozumět mu a překládat z něj do lidských, intuitivních pojmů, které je pak možno vztáhnout na svět kolem nás. Je to také schopnost umět odůvodnit, proč jsou metody použité k řešení problémů správné, protože základním prvkem matematiky je její spolehlivost. V matematice je přesně známo, která tvrzení platí, protože matematici vše dokazují.

Aby byly závěry matematiky spolehlivé, je potřeba přesně definovat pojmy a o nich pak tvrdit rozličné věci. Tímto se zabývá kapitola 1b. Spolehlivost matematických tvrzení se pak odvíjí od toho, že je jejich platnost nezvratně dokázána (v rámci přijatého výkladu světa, viz poznámky o axiomech v dalších kapitolách). O metodách důkazu se rozpovídáme v kapitole 1b, ale potřebujeme na to jako základní nástroj logiku. S ní tedy začneme.

1a. Průlet logikou

Znalost logiky je v matematice naprostou nutností. Zde je třeba říct, že logika jako taková je samostatný a obsáhlý obor, kterému je možné se plně věnovat několik semestrů, ale pro práci v matematice většinou stačí základní znalosti. V této kapitolce je přiblížíme pro ty, kdo se s formální logikou ještě nesetkali, ale hlouběji nepůjdeme. Jednak to není třeba a druhak ji studenti computer science často mají jako samostatný kurs, který se na ni podívá mnohem blíže, než tady vůbec potřebujeme, navíc jsou na to pěkné knihy a nemá tedy smysl to zde dělat znovu.

Co je tedy logika? Z praktického pohledu je to obor zabývající se zkoumáním situací, ve kterých dokážeme ze znalosti, zda jsou pravdivá určitá tvrzení, odvodit spolehlivě pravdivost či nepravdivost tvrzení jiných. Základem jsou výroky (značíme je malými písmeny), což je v zásadě nějaké vyjádření, o kterém lze rozhodnout, zda je pravdivé či ne. Příklady výroků: „$13 > 23$“, „Země je blíž ke Slunci než Jupiter“, „Právě čtu tato skripta“, „Žižka jedl 4. října 1424 jablka“. Všimněte si, že u posledního tvrzení nevíme, zda je pravdivé či ne (možné to je, umřel až o týden později), ale nějakou pravdivostní hodnotu to má, to je podstatné.

Toto pro změnu výroky nejsou: „Ahoj“, „31“, „Pavlač“, „Beze mne“, „Modrá je dobrá“, „Jsem normální“, „Prší“. Kupodivu se zrovna tvrzení „prší“ často v populárnějších rozpravách o logice používá jako příklad výroku, ale výrokem se to stane teprve ve chvíli, kdy řekneme, kde a kdy má pršet, jinak totiž nelze určit, zda je pravdivý či ne. „Tady a teď prší“ je výrok. Jenže lidé jsou líní to psát celé.

Rozmyslete si, že všechny ty výroky byly tak jednoduché, že už nešly dál zmenšit, aby ještě zůstaly výroky. Naopak „Právě ťukám do klávesnice a hraje mi Weird Al Yankovic“ se dá rozlousknout na dva výroky jednodušší. Přesně takové situace nás budou zajímat. Máme jednoduché výroky (atomární, ale nechceme zde začínat s odbornou terminologií) a zajímá nás, co se s nimi dá dělat a jak to pak dopadne. Jinými slovy, výroky různě modifikujeme a spojujeme a pak se ptáme, co se děje s pravdivostí. Přitom nás vůbec nebude zajímat, co vlastně jednotlivé výroky říkají, jen jestli jsou pravdivé či ne. Pravdivost výsledných tvrzení bude odvozována čistě z toho,

jakým způsobem jsou prvotní výroky poskládány, a z informace o jejich pravdivosti, dominantní je forma, nikoliv obsah. Proto se tomu říká formální logika.

Začneme tím nejjednodušším.

• Nechť je p výrok. Jeho **negace** se značí $\neg p$ a je to výrok, jehož pravdivostní hodnota je přesně opačná než pravdivostní hodnota p.

Takže $\neg p$ je takový výrok, který je pravdivý, když p pravdivý není, a naopak. Například negace výroku „Tady a teď prší“ je „Tady a teď neprší“. Rozhodně negací nebude „Nejsou tu teď mraky“, protože může nastat situace, kdy jsou tvrzení „Nejsou tu teď mraky“ a „Tady teď prší“ obě nepravdivá. Nás to samozřejmě nejvíce zajímá v matematice, takže například negace k „$13 > 23$“ není „$13 < 23$“, ale „$13 \leq 23$“.

Fungování negace se dá elegantně vyjádřit takzvanou pravdivostní tabulkou.

p	$\neg p$
0	1
1	0

V prvním sloupci si najdeme, co víme o p, a v druhém se ve stejném řádku dozvíme, jak se pak zachová $\neg p$. Jako obvykle používáme 0 pro nepravdu a 1 pro pravdu.

Výroky spojujeme logickými spojkami. Nejpoužívanější jsou tyto čtyři.

Nechť p a q jsou výroky.

• **konjunkce** značená „$p \wedge q$“ popř. „p & q“ či „p a q“ a čtená „p a q“ je výrok, který je pravdivý právě tehdy, když jsou pravdivé oba výroky p i q.

• **disjunkce** značená „$p \vee q$“ popř. „p nebo q“ a čtená „p nebo q“ je výrok, který je pravdivý v situaci, když je pravdivý alespoň jeden z výroků p či q.

• **implikace** značená „$p \Longrightarrow q$“ popř. „$p \rightarrow q$“ a čtená „jestliže p, pak q“ je výrok, který je pravdivý, když jsou pravdivé oba p i q nebo když je p nepravdivý.

• **ekvivalence** značená „$p \Longleftrightarrow q$“ popř. „$p \leftrightarrow q$“ a čtená „p právě tehdy, když q“ je výrok, který je pravdivý, když mají výroky p a q stejnou pravdivost, tedy jsou oba pravdivé či oba nepravdivé.

Fungování těchto operací se zase standardně vyjadřuje pomocí pravdivostních tabulek, které ukazují, jakou má ten který složený výrok pravdivost v závislosti na tom, co je zrovna známo o pravdivosti p a q.

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \Longrightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

p	q	$p \Longleftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Zkusme si to, uvažujme například výroky p: „Dnes je pátek“ a q: „Dnes je 13. den v měsíci“. Pak výrok $p \wedge q$ říká „Dnes je pátek třináctého“ a selský rozum ve shodě s tabulkou říká, že bude pravdivý jen tehdy, když jej řekneme v pátek, který je také třináctý den v měsíci. Naopak výrok $p \vee q$ bude pravdivý každý pátek a také každého třináctého, což zahrnuje i pátky třináctého. Na konjunkci a disjunkci asi není moc co řešit, jsou v zásadě jasné. Podívejme se blíže na ostatní dvě operace.

Implikace má jednu zajímavou vlastnost, v našem příkladě $p \Longrightarrow q$ znamená „Jestliže je pátek, tak je třináctého“. Podle tabulky je pravdivá v pátky třináctého, ale také od pondělí do čtvrtka a o víkendu, bez ohledu na to kolikátého je. Dostáváme se tím ke klíčové vlastnosti implikace, v případě neplatného předpokladu je implikace jako celek pravdivá. To může začátečníka zarazit, snad mu pomůže následující představa. Implikace se dá brát jako jakási forma slibu. Slibujeme, že jestliže se splní p, tak my uděláme věc q. Někdo se pak dívá, jak to proběhlo, a hodnotí, zda jsme svůj slib splnili (tedy implikace je pravdivá). Tabulka pak dává smysl: Pokud p nenastalo, tak nás slib k ničemu nezavazoval, tudíž ať už jsme q udělali či ne, tak ten slib nebyl porušen a dostává jedničku. Porušili jsme jej jedině v případě, kdyby p bylo splněno, ale my jsme neudělali q.

Toto chování je možná na první pohled divné, ale brzy uvidíme, že přesně vystihuje, co při logických úvahách často potřebujeme.

Při běžném hovoru si lidé často pletou implikaci s **ekvivalencí**. Například řeknou: „Když budeš hodný, dostaneš bonbón“, ale zároveň tím myslí, že když hodný nebude, tak bonbón nedostane, což ovšem ze zvolené formy implikace nevyplývá. Jak už jsme viděli, zlobivé dítě klidně bonbón dostat může a slib–implikace tím porušen nebude. Správné logické vyjádření tedy je „bonbón dostaneš právě tehdy, když budeš hodný“. Tím jsou obě základní fakta („hodný“ a „bonbón“) vzájemně zcela spojeny, pravdivostí si musí odpovídat, aby tento slib zůstal splněn.

Výroky sestavené pomocí základních čtyř spojek a negace je ovšem možné znovu spojovat a negovat, takže můžeme (podobně jako s čísly a operacemi v algebře) sestavovat komplikované konstrukce, i zde pořadí vyhodnocování vyznačujeme závorkami. Abychom jich trochu ušetřili, dává se negaci absolutní priorita nad ostatními operacemi. Přestavme si tedy takový obludný výrok vzniklý z určitých atomárních výroků p, q, ... , pak nás zajímá, jak jeho pravdivost závisí na vstupních datech neboli na pravdivostních hodnotách těch p, q, ... To se zase nejlépe vyjádří tabulkou. Ukážeme si to pro vcelku jednoduchý výrok $\neg p \vee q$, nejprve si uděláme pomocný sloupec pro tu negaci a pak jej „zdisjunktníme“ s q. Mimochodem, díky prioritě negace jsme nemuseli psát $(\neg p) \vee q$.

p	q	$\neg p$	$\neg p \vee q$
1	1	0	1
1	0	0	0
0	1	1	1
0	0	1	1

Tento příklad je typický, zkoumaný výrok je někdy pravdivý a někdy ne. Jsou ale výjimky. Dobrým příkladem je výrok „Teď tady prší nebo teď tady neprší“. Vzhledem k tomu, že třetí možnost není, tak jedna z těch dvou variant musí vždycky nastat a podle pravdivostní tabulky vidíme, že pak už je pravdivá celá disjunkce. Je to tedy výrok, který je za všech okolností pravdivý.

Je asi zjevné, že toto bude fungovat s libovolným výrokem p, výraz $p \vee \neg p$ bude vždy pravdivý už z principu. Logici takovýmto formálně vždy platným výrazům říkají tautologie, někdy se značí T jako Tautologie nebo taky True.

Rozmyslete si, že pro libovolný výrok p je naopak tvrzení $p \wedge \neg p$ vždy nepravdivé, třeba „Teď tady prší a neprší“. Tomu se v logice říká kontradikce a výrok, který je vždy nepravdivý, se značí F jako False.

Vraťme se k našemu příkladu. Všimněte si, že výraz $\neg p \vee q$ má přesně stejné pravdivostní hodnoty jako implikace $p \implies q$. To znamená, že z pohledu logiky jsou tyto dva výrazy naprosto rovnocenné a můžeme je zaměňovat dle libosti. Ten druhý výraz není tak výstižný, ale zase je v některých situacích praktičtější, protože disjunkce a negace jsou jednodušší operace, pohodlnější při úpravách.

Podobně se dá ekvivalence $p \iff q$ nahradit dvěma implikacemi $p \implies q$ a $q \implies p$, ostatně samo značení to naznačuje. Tyto implikace pak případně můžeme dále nahradit pomocí triku z předchozího odstavce.

V běžných matematických knihách by toto vyjádřili pomocí rovnosti, například takto: $(p \implies q) = (\neg p \vee q)$, ale to není úplně korektní z hlediska logického, ve formální logice se totiž musí dávat pozor na správný význam rovnítka. Matematici z jiných oborů, kteří logiku používají jen jako nástroj, nebývají při jejím použití tak formální, díky čemuž ušetří spoustu času různými šikovnými zkratkami, například tím rovnítkem. Tohle je matematická kniha, takže budeme většinu těch zkratek používat také, ale u logické rovnosti dvou výrazů uděláme výjimku. Ve formální logice se pro to zavádí značení $\models\!\!\models$, a protože se dá čekat, že studenti diskrétní matematiky formální logiku potkají, nebudeme jim v tom dělat zmatek a použijeme to také. Naše pozorování by se tedy zapsala takto:

- $(p \implies q) \;\models\!\!\models\; (\neg p \vee q)$
- $(p \iff q) \;\models\!\!\models\; ([p \implies q] \wedge [q \implies p])$

Z pohledu praktického se tato „rovnost“ chová stejně jako rovnost v algebře, vztah $\models\!\!\models$ nám umožňuje provádět s výroky logické úpravy a zjednodušování, podobně jako pomocí rovnítka děláme úpravy s čísly a využíváme identit jako $1 + 3 = 4$. A podobně jako pro algebraické operace máme určitá pravidla, existují (a jsou užitečná) i pro operace logické.

1a.1 Pravidla

Začneme tím nejednodušším.

- $p \wedge p \;\models\!\!\models\; p$, $\quad p \vee p \;\models\!\!\models\; p$, $\quad \neg\neg p \;\models\!\!\models\; p$;
- $p \wedge \neg p \;\models\!\!\models\; F$, $\quad p \vee \neg p \;\models\!\!\models\; T$;
- $p \wedge T \;\models\!\!\models\; p$, $\quad p \vee F \;\models\!\!\models\; p$;
- $p \wedge F \;\models\!\!\models\; F$, $\quad p \vee T \;\models\!\!\models\; T$.

Většina se dá rozmyslet selským rozumem. První vztahy ukazují, že zdvojováním výroků ani zdvojením negace nic nezískáme. Druhý řádek jsme již potkali (prší a/nebo neprší). Další dva řádky kombinují obecný výrok p s výroky, které jsou vždy pravda či vždy nepravda. I zde je to jasné po kratším rozmyšlení, například výrok $p \wedge T$ je pravdivý přesně tehdy, když jsou pravdivé oba výroky p a T, ale T je pravdivý vždy, takže pravdivost obou závisí čistě na pravdivosti p. Takovéto identity se občas hodí při úvahách, jak ještě uvidíme například v kapitole 2.

Jak už jsme obecně vyložili v úvodu, není cílem se všechny takovéto vlastnosti učit nazpaměť. Důležité je rozumět logice natolik, aby si to potřebné dokázal člověk rozmyslet ve chvíli, kdy to potřebuje. Pak ale pomůže, když to již předtím někde viděl a že je v takovém rozmýšlení trénovaný. Platí to i pro většinu vlastností zmíněných dále.

Podívejme se na další vlastnosti logických spojek:

- $p \wedge q \;\models\!\!\models\; q \wedge p, \quad p \vee q \;\models\!\!\models\; q \vee p;$
- $p \wedge (q \wedge r) \;\models\!\!\models\; (p \wedge q) \wedge r, \quad p \vee (q \vee r) \;\models\!\!\models\; (p \vee q) \vee r;$
- $p \wedge (q \vee r) \;\models\!\!\models\; (p \wedge q) \vee (p \wedge r), \quad p \vee (q \wedge r) \;\models\!\!\models\; (p \vee q) \wedge (p \vee r).$

Odborně řečeno, první odrážka ukazuje komutativitu spojek, druhá zase asociativitu a třetí ukazuje distributivní zákon. Tím prvním jsme asi nikoho nepřekvapili, i asociativitu znáte z běžných algebraických operací. Je užitečná například proto, že nám ušetří závorky, při opakované stejné spojce je díky asociativitě vůbec nemusíme psát, třeba takto: $p \wedge q \wedge r \wedge s$. Každý si to teď může ozávorkovat dle libosti.

Distributivní zákon vlastně student dobře zná, dotyčné logické spojky jsou spřízněny s operacemi, $\wedge$ se chová jako násobení a $\vee$ jako sčítání a první rovnost třetí odrážky je pak vlastně jen roznásobení závorky. Druhá rovnost je pak zajímavá, ukazuje, že u logiky se dá roznásobovat i v opačném umístění operací, což pro sčítání a násobení rozhodně neplatí.

Důležitá jsou také pravidla, která nám umožňují negovat operace.

- $\neg(\neg p) \;\models\!\!\models\; p;$
- $\neg(p \wedge q) \;\models\!\!\models\; \neg p \vee \neg q;$
- $\neg(p \vee q) \;\models\!\!\models\; \neg p \wedge \neg q;$
- $\neg(p \Longrightarrow q) \;\models\!\!\models\; p \wedge \neg q;$
- $\neg(p \Longleftrightarrow q) \;\models\!\!\models\; (p \wedge \neg q) \vee (\neg p \wedge q).$

Druhý a třetí vztah se jmenují **de Morganovy zákony** a budou se nám v knize hodit, je dobré si je pamatovat. Nejsou vlastně ničím záhadným. Představme si konjunkci $p \wedge q$. Ta platí, pokud jsou pravdivé obě složky p a q. Jestli ji tedy chceme zneplatnit, tak stačí zneplatnit alesoň jednu z těch složek. Konjunkce je tedy neplatná (znegovaná), když neplatí p nebo neplatí q, což je přesně to, co je na pravé straně v druhém řádku.

Podobně se dá rozmyslet i negace implikace. Potřebujeme vystihnout situaci, kdy implikace neplatí, a to je přesně situace, kdy platí předpoklad a neplatí závěr. Dá se k tomu dojít i formálně pomocí přepisu implikace na rovnocenný výraz a pak použitím de Morganových zákonů:

$$\neg(p \Longrightarrow q) \;\models\!\!\models\; \neg(\neg p \vee q) \;\models\!\!\models\; (\neg\neg p \wedge \neg q) \;\models\!\!\models\; (p \wedge \neg q).$$

Negace ekvivalence plyne z toho, že ekvivalence je vlastně oboustranná implikace, takže pokud se má pokazit, musí se pokazit jedna (či obě) z těch implikací, pro takovou negaci máme vzoreček o řádek výše. Dá se to také rozmyslet přímo, ekvivalence platí, pokud mají p a q stejnou pravdivostní hodnotu, negace tedy musí popisovat vztah, kde je jeden z p, q pravdivý a druhý ne. Můžeme si to odvodit i formálně, alespoň si naše nová pravidla trochu procvičíme.

$$\neg(p \Longleftrightarrow q) \;\models\!\!\models\; \neg[(p \Longrightarrow q) \wedge (q \Longrightarrow p)] \;\models\!\!\models\; [\neg(p \Longrightarrow q) \vee \neg(q \Longrightarrow p)] \;\models\!\!\models\; (p \wedge \neg q) \vee (q \wedge \neg p).$$

Na závěr si ukážeme ještě dva zajímavé vztahy. Následující implikace jsou vždy pravdivé.

- $p \Longrightarrow (p \vee q), \quad (p \wedge q) \Longrightarrow p.$

Podíváme se na tu první, rozebereme si možnosti pro p. Víme už, že pokud p neplatí, tak je celá implikace automaticky pravdivá. Pokud by p platilo, pak také platí i $p \vee q$ a implikace zase platí. Zkusíme to ukázat ještě pomocí pravdivostní tabulky.

p	q	$p \vee q$	$p \Longrightarrow (p \vee q)$
1	1	1	1
1	0	1	1
0	1	1	1
0	0	0	1

Daný výrok je tedy opravdu vždy pravdivý (je to tautologie), našim značením $[p \Longrightarrow (p \vee q)] \;\models\!\!\models\; T$. Rozmyslete si a tabulkou ověřte i platnost druhého výroku.

K čemu takováto tautologie může být? Když máme implikaci, která je vždy pravdivá, můžeme ji použít v logických úvahách, například pokud je dána pravdivost $p \wedge q$, tak můžeme podle první tautologie s jistotou odvodit platnost p. Ale to se již dostáváme k následujícím tématu.

1a.2 Logika v aplikacích

Formální logika se nezabývá obsahem výroků, proto nám tautologie neboli výroky, jejichž platnost plyne čistě z formální logiky, málokdy dají nějakou opravdu užitečnou informaci v aplikacích. Tam se snažíme logiku použít k poznávání světa (či jiných věcí) a obsah výroků začíná být důležitý. V aplikacích nás proto zajímají výroky, jejichž

pravdivost (v rámci zkoumaného světa!) vyplývá z informací, nikoliv chladné logiky. Jinak řečeno, zajímají nás situace, kdy ony řádky v tabulce, kde má dotyčný výrok nuly, jsou jen virtuální, nemohou nastat ve skutečnosti. Například výrok „Sekačka na trávu mi omylem usekla před rokem hlavu a já teď bez ní normálně chodím do školy“ je evidentně nepravdivý (alespoň tedy za současného stavu technologie). Něco pravdivého: „Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi“.

Zkusme si to rozebrat. Pokud opravdu je 29. února, pak musí nutně podle našeho kalendáře platit i to o dělitelnosti roku a implikace platí. Pokud naopak 29. února není, pak není splněn předpoklad implikace a tato implikace jako celek je tedy pravdivá. To znamená, že reálně nemůže nastat situace, kdy by tato konkrétní implikace neplatila.

Právě taková vždy pravdivá tvrzení nás zajímají nejvíce a většina matematických tvrzení je tohoto typu, pravdivé implikace. Ukážeme vzájemnou propojenost $p \implies q$ určitých věcí a ona pak čeká na uživatele. Pokud by se někomu přihodilo, že p platí, pak díky naší práci už hned ví, že mu platí i q. Například ona implikace o 29. únoru čeká na někoho, kdo si na ni jednoho krásného 29. února vzpomene, pak už rovnou ví něco o dělitelnosti roku, aniž by vlastně věděl, jaký rok přesně je. Čtenář se už setkal s implikací jinou, určitě ví, že když má kvadratickou rovnici a vyjde mu číslo $b^2 - 4ac$ kladné, tak už ta rovnice má dva reálné kořeny.

Všimněte si mimochodem, že v jiném kulturním okruhu, kde mají kalendář jinak, naše implikace pravdivá být nemusí. Když tedy v běžném hovoru mluvíme o tom, že určitý výrok je pravdivý, tak tím myslíme, že je vždy pravdivý v rámci dotyčného světa, přičemž ten svět nemusí být náš fyzický, ale třeba abstraktní matematický (viz zbytek této knihy). Pravdivost tvrzení tedy závisí na pravidlech, která fungování dotyčného světa určují. My se k tomu blíže dostaneme v povídání o axiomech v kapitole 3 o indukci.

Teď se podíváme na to, jak se z tvrzení, o kterém víme, že je (vždy) pravdivé, dá něco získat díky znalosti formální logiky. Nejčastěji se takto informačně vytěžují **implikace**, které jsou v matematice klíčové, tak se na ně zaměříme.

Máme-li pravdivou implikaci $p \implies q$, pak části p říkáme „postačující podmínka“ a části q říkáme „nutná podmínka“. Je to vlastně rovnocenné vyjádření, říct, že „p je postačující podmínka pro q“, je z hlediska logiky stejné, jako říct, že $p \implies q$ je vždy pravdivá, což je stejné, jako říct „q je nutná podmínka pro p“. Jak ještě uvidíme, pro matematiky je tato terminologie velmi užitečná. Odkud se to vzalo?

Je to přirozené. Pokud vím, že je dnes 29. února, tak to postačuje k jistotě, že je rok dělitelný čtyřmi. Toto je také hlavní způsob využití implikace, který jde zpět minimálně o tisíc let. Tradiční zápis vypadá nějak takto:

- Platí: Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi.
- Předpokládáme, že platí: Je 29. února.
- Závěr: Tento rok je dělitelný čtyřmi.

Ve středověku tomu říkali „modus ponens“. Využití implikace je tedy následující. Zajímá nás, zda je pravdivé tvrzení q, ale do jeho zkoumání se nám nechce. Naštěstí dostaneme k dispozici pravdivou implikaci $p \implies q$, kde p je mnohem příjemnější. Podíváme se tedy na p a pokud se ukáže pravdivým, pak je nutně pravdivé i q. Skvělé. Má to ale zádrhel. Pokud by se ukázalo, že p neplatí, tak o q nic nevíme. U našeho příkladu je to jasné:

- Platí: Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi.
- Předpokládáme, že platí: Není 29. února.
- Závěr: ????

Implikace tedy dokáže posouvat informaci z p do q, ale je to nástroj nedokonalý, posílá jen jeden typ informace. Tato nespolehlivost dokáže někdy docela potrápit. Tento problém se projeví ještě jedním způsobem. Máme-li pravdivou implikaci $p \implies q$, tak rozhodně neplatí, že závěr q je postačující pro q. Zase je to vidět na našem příkladě:

- Platí: Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi.
- Předpokládáme, že platí: Je rok dělitelný čtyřmi.
- Závěr: ????

Je to jasné, v roce dělitelném čtyřmi nemusí dnes být zrovna 29. února, klidně může být červen, dokonce v tom roce ani žádný 29. únor nemusí být (protože roky, které jsou kromě čtyř dělitelné i stem, ale už ne čtyřmi sty, žádný přechodný den nemají).

Toto se dá jinak vyjádřit pozorováním, že pravdivou implikaci nelze beztrestně obrátit. Mějme implikaci $p \implies q$, o které víme třeba to, že je (vždy) pravdivá. V okamžiku, kdy se ji pokusíme obrátit, tak všechny informace ztratíme, $q \implies p$ je úplně jiná věc, jejíž pravdivost nemá obecně s pravdivostí $p \implies q$ nic společného. Často tak dostaneme implikaci nepravdivou, jen v některých případech zjistíme, že je pravdivá $p \implies q$ i $q \implies p$. Pak musí mít p a q stejnou pravdivostní hodnotu a dostáváme vlastně ekvivalenci $p \iff q$, ale to musíme mít hodně štěstí. V obecném případě rozhodně implikace obracet nesmíme.

Teď se podíváme na vyjádření slovy nutná podmínka. Je jasné, že abychom si mohli užívat 29. února, tak musí být rok dělitelný čtyřmi, je to tedy nutné, bez toho to nejde. Nutné podmínky nebývají tak populární jako podmínky postačující, protože když víme, že je q pravdivé, tak nám to nepomůže odvodit nic o p kromě toho, že nám to umožňuje mít p pravdivé. Přesto ale bývají nutné podmínky užitečné. Když zkoumáme, za jakých okolností platí p, tak nám pravdivá implikace $p \implies q$ umožňuje omezit se pouze na situace, kde platí q, protože jinak rovnou víme, že p neplatí.

Už jsme poznamenali, že q postačující podmínkou není, tedy ze znalosti o pravdivosti q nic o p neodvodíme. Viděli jsme ale, že znalost o neplatnosti q již dává neplatnost p, takže dokážeme posílat jistou informaci z q na p. Vypadá to u našeho příkladu takto.

- Platí: Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi.
- Předpokládáme, že platí: Není rok dělitelný čtyřmi.
- Závěr: Dnes není 29. února.

Za středověku tomuto typu úvahy říkali „modus tollens“. Vlastně tak dostáváme novou implikaci.

- Máme: Jestliže je dnes 29. února, pak je rok dělitelný čtyřmi.
- Dostali jsme: Jestliže není rok dělitelný čtyřmi, pak dnes není 29. února.

Uděláme si to formálně. Je-li dána implikace $p \implies q$, pak se definuje její **obměna** jako $\neg q \implies \neg p$. Pomocí pravdivostní tabulky se hravě dokáže, že implikace a její obměna mají vždy nutně stejnou pravdivostní hodnotu, jde tedy o ekvivalentní výroky a lze je libovolně zaměňovat. Přechod k obměně je občas velice užitečný a setkáme se s ním u nepřímého důkazu níže.

> Čtenář si může předchozí úvahy procvičit na implikaci „Jestliže je mi přes 21, tak mi je přes 18“ neboli „Být přes 21 je postačující k tomu, abych byl přes 18“. Ta je dozajista pravdivá, ať už ji řekne kdokoliv. Je na ní zajímavé, že 21 bývá v mnoha zemích legálním věkem pro pití alkoholu, zatímco 18 bývá věkem pro získání řidičského průkazu. Tuto implikaci lze tedy vyjádřit slovy „Jestliže mohu pít, tak mohu řídit“, což je z logického pohledu pravdivá implikace, ale zní to podezřele.

Ekvivalence $p \iff q$ je podle definice situace, kdy mají výroky p a q vždy stejnou pravdivost. Již jsme uvedli, že pak máme implikace oběma směry. To znamená, že p je nutnou i postačující podmínkou pro q a naopak, ekvivalence je již z podstaty symetrická. V praxi je to skvělé, cokoliv se dozvíme o p platí i pro q. Jak se dá čekat, získat pravdivou ekvivalenci je mnohem obtížnější než získat pravdivou implikaci.

1a.3 Predikátová logika

Opravdu užitečné výroky nejsou „absolutní“, ale mají proměnnou. Už i to „teď tady prší“ vlastně mělo dvě proměnné, místo a čas, a podle toho, kde a kdy jsme tento výrok řekli, se měnila jeho pravdivost. Výroky s proměnnými značíme $p(x)$, $p(x,y)$ a podobně. Matematika je výroků s proměnnými plná. Třeba „$x > 13$“ někdy platí a někdy ne, podle toho, co dáme za x. Výrok „pro $x = 23$ je $x > 13$“ je pravdivý, výrok „pro $x = 3$ je $x > 13$“ pravdivý není. Toto ale moc užitečné není. Z hlediska teorie nás zajímají hlavně výroky, které by měly pravdivost stálou bez nutnosti volit nějaké konkrétní x. U výroků s jednou proměnnou se tak studují dvě situace:

1. Chceme vědět, jestli náhodou takový výrok neplatí úplně vždy, bez ohledu na naší volbu proměnné. To se vyjadřuje slovy „pro každé x platí $p(x)$“ a máme i pohodlnou zkratku „$\forall x\colon p(x)$“. Jestliže si například vezmeme výrok „$x^2 \geq 0$“, pak je pravdivý, ať už za x zvolíme jakékoliv reálné číslo. Běžný matematik by tedy napsal toto:

$$\forall x \in \mathbb{R}\colon x^2 \geq 0.$$

Čteme to: Pro každé x z množiny reálných čísel platí, že $x^2 \geq 0$. Ta dvojtečka je tedy jen zkratka pro slovo „platí“. Logici by zase měli nepříjemný pocit, hlavně z té dvojtečky, a dávali by přednost zápisu

$$\forall x\ (x \in \mathbb{R} \implies x^2 \geq 0).$$

Pro běžné matematiky (nelogiky) je první zápis dostačující a normálně jej používají, nicméně jsou situace (viz třeba důkaz Faktu 2a.1), kdy ten přesný logický zápis pomůže. Většinou ale i zde raději použijeme ten stručnější zápis, odpovídá lépe přirozenému jazyku. Podstatné je tomu zápisu dobře rozumět.

2. Mnoho tvrzení s argumentem ovšem takto pěkných není, aby platilo vždy, třeba zrovna to $x > 13$. Matematici se pak ptají, jestli by toto nemohlo být pravda alespoň někdy. Zkoumaný výrok je „existuje x, pro které platí $p(x)$“ a zapisujeme jej „$\exists x\colon p(x)$“. Příklad pravdivého výroku:

$$\exists x \in \mathbb{R}\colon x > 13.$$

Naopak $\exists x \in \mathbb{R}\colon x = x + 1$ je výrok nepravdivý, protože $x = x + 1$ se nedá splnit žádnou volbou reálného čísla x. I zde by logici raději viděli

$$\exists x\ (x \in \mathbb{R} \wedge x = x + 1)$$

a i zde je v této knize budeme opakovaně zklamávat. Značkám $\forall x$ a $\exists x$ se říká **kvantifikátory**, ten první je obecný, ten druhý existenční. Když je otočíte vzhůru nohama, dostanete písmena A a E jako „All“ a „Exists“, dobře se to pamatuje.

Zde bychom mohli uvést pravidla popisující, jak kvantifikátory interagují s logickými spojkami, ale podobně jako předtím není důležité si ta pravidla pamatovat, ale zamyslet se nad nimi a porozumět jim. Necháváme je proto jako cvičení 1a.3.

Důležité pro nás bude, jak se takové věci dokazují. Odpověď je jednoduchá: Přesně tak, jak by člověk čekal. V důkazu výroku $\forall x \in M\colon p(x)$ musíme nějak odůvodnit, že ať už si vezmeme z M cokoliv, vždy pro tento prvek bude platit p. Naopak k důkazu výroku $\exists x \in M\colon p(x)$ stačí nějaké takové x najít. Důkaz výroku $\exists x \in \mathbb{R}\colon x > 13$ zní: Zkuste $x = 14$.

Někdy potřebujeme naopak dokázat, že výrok neplatí, což je totéž jako dokazovat, že platí negace výroku. Pro negace výroků s kvantifikátory máme následující pravidla:

- $\neg(\forall x \in M\colon p(x)) \;\nleftrightarrow\; \exists x \in M\colon \neg p(x)$;
- $\neg(\exists x \in M\colon p(x)) \;\nleftrightarrow\; \forall x \in M\colon \neg p(x)$.

Opět je to selský rozum. Na to, abychom ukázali, že se někdo mýlí, když tvrdí, že vždy platí p, mu stačí ukázat jediný případ, kdy tomu tak není, což je přesně první řádek. Tomu jednomu příkladu se pak říká **protipříklad**.

Podobně jako u implikace, i zde máme jeden zvláštní případ, který se moc nevyskytuje, ale když už na něj narazíme, měli bychom vědět, co s ním. Jak fungují kvantifikátory, když se odkazují na prázdnou množinu? Jinými slovy, bude výrok $\forall x \in \emptyset\colon p(x)$ pravdivý? A výrok $\exists x \in \emptyset\colon p(x)$? Odpověď zní, že první vždy ano, druhý vždy ne. U toho druhého je to jasné, v prázdné množině nic nenajdeme, tudíž existence speciálního prvku nemůže být splněna, ale u toho prvního to tak jasné není. Jedna možnost je si říct, že vlastně ten výrok nejde pokazit, protože nenajdeme v prázdné množině x takové, aby pro něj p neplatilo. Jestliže nejde výrok pokazit, tak musí platit opak, tedy výrok je pravdivý. Naprosto jasné je to z toho správně logického přepisu $\forall x\ (x \in \emptyset \implies x^2 \geq 0)$. Předpoklad dotyčné implikace je vždy nepravdivý, tudíž je celá implikace automaticky pravdivá.

Zajímavá situace je, když máme výrok s více proměnnými. Pokud je uvozujeme kvantifikátory stejného typu, pak na pořadí nezáleží a obvykle je sloučíme do jednoho (pokud vybíráme ze stejné množiny):

$$\big(\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon p(x,y)\big) \;\nleftrightarrow\; \big(\forall y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon p(x,y)\big) \;\nleftrightarrow\; \big(\forall x, y \in \mathbb{R}\colon p(x,y)\big);$$
$$\big(\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon p(x,y)\big) \;\nleftrightarrow\; \big(\exists y \in \mathbb{R}\, \exists x \in \mathbb{R}\colon p(x,y)\big) \;\nleftrightarrow\; \big(\exists x, y \in \mathbb{R}\colon p(x,y)\big).$$

Například $\forall x, y \in \mathbb{R}\colon x^2 + y^2 \geq 0$ je pravdivý výrok. Naopak $\forall x, y \in \mathbb{R}\colon x^2 + y^2 = 5^2$ pravdivý výrok není. Volba $x = 3$, $y = 4$ ovšem ukazuje pravdivost výroku $\exists x, y \in \mathbb{R}\colon x^2 + y^2 = 5^2$.

Složitější situace je, když se smíchají kvantifikátory rozličných druhů, pak totiž na pořadí velice záleží. Základem je rozmyslet si dobře situaci pro dva kvantifikátory. Ukážeme si to na příkladech.

Výrok $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x^2 = 4y^2$ říká: „Pro každé reálné číslo x existuje reálné číslo y takové, že $x^2 = 4y^2$.“ Již samotná forma naznačuje, že y hledáme vždy k jistému konkrétnímu x. Vezmeme nějaké x a hledáme k němu y splňující specifikovanou vlastnost. Pak vezmeme jiné x a klidně se může stát (ale není to nutné), že k němu najdeme jiné y s požadovanou vlastností (nebo také nenajdeme, podle toho, zda daný výrok platí či ne). Je náš výrok vlastně platný? Ano. Když nám někdo dá x, tak stačí zvolit $y = \frac{1}{2}x$ a vlastnost je splněna, opravdu pak $x^2 = 4y^2$. Je také možné volit $y = -\frac{1}{2}x$, což ale vůbec nevadí, výrok toto neřeší. Pro něj je podstatné, aby alespoň nějaké takové y vždy pro dané x bylo. Můžeme si také všimnout, že pro některá x dostáváme stejné možnosti na y, třeba pro $x = 6$ a $x = -6$ máme vždy pro y kandidáty ± 3. Ani to ten výrok neřeší.

U tohoto pořadí kvantifikátorů tedy pravdivost výroku znamená, že vzniká jakési přiřazení $x \mapsto y$, které ale nemusí být jednoznačné.

Teď se podíváme na opačné pořadí: Výrok $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon x^2 = 4y^2$ říká: „Existuje reálné číslo y takové, že pak pro každé reálné číslo x platí $x^2 = 4y^2$.“ Zde již čeština naznačuje, že číslo y musí být univerzální, jedno číslo pro všechna x. Je zjevné, že v tomto případě takové univerzální číslo y nenajdeme. Vidíme tedy, že prohozením kvantifikátorů došlo ke změně pravdivosti výroku. Příklad pravdivého výroku tohoto typu: $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon (|y| + 1)^x = 1$. Stačí totiž zvolit $x = 0$ a vlastnost bude pro všechna reálná y platit.

Pro praktickou práci v matematice je proto důležité rozumět dobře těmto kombinacím kvantifikátorů a hlavně si pamatovat, že pořadí nelze zaměňovat. Pečlivější čtenář si nicméně může všimnout, že alespoň něco říct lze, jmenovitě platí toto:

- $[\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon p(x,y)] \implies [\forall y \in \mathbb{R}\, \exists x \in \mathbb{R}\colon p(x,y)]$.

Jinými slovy, jestliže máme univerzálně fungující prvek x, pak tento prvek bude samozřejmě také fungovat individuálně pro jednotlivce. Pro další pravidla, která jsou někdy užitečná, se podívejte na cvičení 1a.3. Jako obvykle nemá smysl se je učit, spíš si dobře rozmyslete, proč to vlastně nemůže být jinak, než je tam řečeno.

Existenční kvantifikátor má jednu užitečnou modifikaci. Když se za něj přidá vykřičník, tak se to čte „existuje právě jedno“, je to tedy spojení dvou věcí, „existuje“ a „není jich víc“. Například výrok $\exists! x \in \mathbb{R}\colon x+1=14$ je pravdivý, tato rovnice má přesně jedno řešení, ale výroky $\exists! x \in \mathbb{R}\colon x^2=13$ a $\exists! x \in \mathbb{R}\colon x^2=-13$ pravdivé nejsou. Ve formální logice tento kvantifikátor neexistuje, takže se náš pravdivý příklad musí zapsat například takto:

$$[\exists x\ (x \in \mathbb{R} \wedge x+1=14)] \wedge \neg[\exists x,y\ (x \in \mathbb{R} \wedge y \in \mathbb{R} \wedge x \neq y \wedge x+1=14 \wedge y+1=14)].$$

Už asi chápete, proč obyčejný matematik-nelogik radostně sáhne po $\exists!$, i když nutno přiznat, že logici mají dobré důvody, proč to do formální logiky nepřibírat.

O logice by se toho dala napsat spousta. Existuje více pravidel, existují další operace (užitečné v některých aplikacích), to už vůbec nemluvíme o tématech, která jsme tu ani nenačali (zvídavému čtenáři doporčujeme přečíst si nějakou pěknou knížku), ale pro běžnou matematickou práci v zásadě stačí to, co vidíme výše.

Na to, jak se logika v matematice opravdu používá, se blíže podíváme v příští kapitole, a v praxi to pak uvidíme ve větší či menší míře ve všech kapitolách následujících.

Cvičení

Cvičení 1a.1: Připomeňme, že $\mathbb{R}$ značí množinu všech reálných čísel a $\mathbb{Z}$ množinu všech celých čísel. Rozhodněte, zda jsou pravdivé následující výroky:

(i) $\forall x \in \mathbb{R}\colon (x \geq 3 \vee x < 5)$;
(ii) $\exists x \in \mathbb{R}\colon (x \geq 3 \wedge x < 0)$;
(iii) $\forall x \in \mathbb{Z}\colon (x > 3 \wedge x < 7)$;
(iv) $\exists x \in \mathbb{Z}\colon (x \geq 3 \wedge x < 5)$;
(v) $\forall x \in \mathbb{R}\colon (x > 3 \implies x^2 > 9)$;
(vi) $\forall x \in \mathbb{R}\colon (x^2 > 9 \implies x > 3)$;
(vii) $\forall x \in \mathbb{R}\colon (x^2 < 0 \implies x = 13)$;
(viii) $\exists x \in \mathbb{R}\colon (x \geq 5 \implies x^2 = 40)$;
(ix) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x+y=0$;
(x) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon x+y=0$;
(xi) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x \cdot y = 0$;
(xii) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon x \cdot y = 0$;
(xiii) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon \frac{x}{y} = 1$;
(xiv) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon \frac{x}{y} = 1$;
(xv) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x < 3y$;
(xvi) $\exists y \in \mathbb{Z}\, \exists x \in \mathbb{Z}\colon x^2 - y^2 = 3$.

Cvičení 1a.2: Následující výrazy s proměnnou z $\mathbb{R}$ upravte pomocí distributivního zákona a pak zjednodušte:
(i) $x > 3 \wedge (e^x = x^5 \vee x = 4)$;
(ii) $x < 13 \wedge (\sin(x) < \frac{1}{3} \vee x > 14)$;
(iii) $(\sin(x) < x^3 \wedge x < 3) \vee (\sin(x) < x^3 \wedge x > 1)$.

Cvičení 1a.3: Rozhodněte, zda platí obecně (tedy pro libovolné množiny M a výroky p, q) následující tvrzení o logické ekivalenci výroků. Pokud máte pocit, že některá dvojice výroků ekvivalentní není, tak najděte příklad takových výroků p, q, aby jeden z výroků platil a druhý ne.

(i) $\forall x \in M\colon p(x) \wedge q(x) \ \nleftrightarrow\ [\forall x \in M\colon p(x)] \wedge [\forall x \in M\colon q(x)]$;
(ii) $\forall x \in M\colon p(x) \vee q(x) \ \nleftrightarrow\ [\forall x \in M\colon p(x)] \vee [\forall x \in M\colon q(x)]$;
(iii) $\exists x \in M\colon p(x) \wedge q(x) \ \nleftrightarrow\ [\exists x \in M\colon p(x)] \wedge [\exists x \in M\colon q(x)]$;
(iv) $\exists x \in M\colon p(x) \vee q(x) \ \nleftrightarrow\ [\exists x \in M\colon p(x)] \vee [\exists x \in M\colon q(x)]$;
(v) $p \wedge \forall x \in M\colon q(x) \ \nleftrightarrow\ \forall x \in M\colon p \wedge q(x)$;
(vi) $p \vee \forall x \in M\colon q(x) \ \nleftrightarrow\ \forall x \in M\colon p \vee q(x)$;
(vii) $p \wedge \exists x \in M\colon q(x) \ \nleftrightarrow\ \exists x \in M\colon p \wedge q(x)$;
(viii) $p \vee \exists x \in M\colon q(x) \ \nleftrightarrow\ \exists x \in M\colon p \vee q(x)$.

Cvičení 1a.4: Znegujte formálně následující výroky. Pro každý výrok i jeho negaci si pak zvlášť rozmyslete, zda platí či ne, abyste se přesvědčili, že vždy mají opačnou pravdivost.

(i) $\exists x \in \mathbb{R}\colon x > 5$;
(ii) $\forall x \in \mathbb{Z}\colon (x > 5 \vee x^2 = 14)$;
(iii) $\exists x \in \mathbb{R}\colon (x < 3 \implies x = x - 1)$;
(iv) $(\forall x \in \mathbb{R}\colon x^2 \geq 0) \implies (\forall x \in \mathbb{R}\colon x < 0)$;
(v) $(\exists x \in \mathbb{R}\colon x = \frac{x}{2}) \implies (\forall x \in \mathbb{R}\colon x = 13x)$;
(vi) $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon x < y$;
(vii) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon x^2 + y^2 \geq 0$;
(viii) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon \sin(x) = \cos(y)$.

Řešení:
1a.1: (i): platí; (ii): neplatí (podmínky se vylučují); (iii): neplatí (pro některá x obě nerovnosti platí, ale to nestačí); (iv): platí, $x = 3$ nebo $x = 4$; (v): platí; (vi): neplatí, protipříklad $x = -4$; (vii): platí (předpoklad není nikdy splněn, proto je implikace pravdivá); (viii): platí, $x = \sqrt{40}$ nebo třeba $x = 0$; (ix): platí, $y = -x$; (x): neplatí; (xi): platí, $y = 0$; (xii): platí, $y = 0$; (xiii): neplatí, pro $x \neq 0$ sice najdeme $y = x$, ale pro $x = 0$ to zařídit nejde; (xiv): neplatí; (xv): platí, stačí zvolit třeba $y = |x| + 1$; (xvi): platí, $x = 2$ a $y = 1$ (všimněte si, že kdyby tam bylo $x^2 - y^2 = 2$, tak už by to neplatilo).
1a.2: (i): $\nleftrightarrow\ (x > 3 \wedge e^x = x^5) \vee (x > 3 \wedge x = 4) \ \nleftrightarrow\ (x > 3 \wedge e^x = x^5) \vee x = 4$.

(ii): $\nexists\ (x < 13 \wedge \sin(x) < \frac{1}{3}) \vee (x < 13 \wedge x > 14)\ \nexists\ \nexists\ (x < 13 \wedge \sin(x) < \frac{1}{3}) \vee F\ \nexists\ x < 13 \wedge \sin(x) < \frac{1}{3}$.
(iii): $\nexists\ \sin(x) < x^3 \wedge (x < 3 \vee x > 1)\ \nexists\ \sin(x) < x^3 \wedge T\ \nexists\ \nexists\ \sin(x) < x^3$.

1a.3: (i): platí. Oba výrazy vyžadují platnost p i q pro všechna x.
(ii): neplatí, jde jen v jednom směru. Pokud platí výrok napravo, tak už platí i výrok nalevo. Pravý výrok totiž vynutí platnost jednoho z p, q vždy, díky tomu platí i $p \vee q$ vždy. Naopak to ale nejde, pokud platí výraz nalevo, tak je $p \vee q$ splněno vždy, ale nepřinutí to jeden z nich, aby platil vždy. Příklad: $M = \mathbb{R}$, $p(x)$: $x \geq 13$, $q(x)$: $x < 13$.
(iii): neplatí, jde jen v jednom směru. Pokud platí výrok nalevo, tak existuje x, pro které platí $p \wedge q$, pro toto x pak platí oba výroky. Naopak to nejde, pokud platí výrok napravo, tak jde p i q nějakou volbou x splnit, ale nikde není zaručeno, že to bude totéž x, aby tak platil i výrok nalevo. Příklad: $M = \mathbb{R}$, $p(x)$: $x = 13$, $q(x)$: $x = 14$.
(iv): platí. Výrok nalevo i výrok napravo požadují, aby šlo alespoň jeden p, q alespoň jednou volbou x splnit.
(v): platí. Výrok nalevo i výrok napravo požadují, aby platilo jak p, tak $q(x)$ pro všechna x.
(vi): platí. Pokud platí p, tak jsou pravdivé výroky na obou stranách. Pokud p neplatí, ale $q(x)$ vždy platí, tak jsou zase výroky na obou stranách pravdivé. Pokud p neplatí a také $q(x)$ alespoň pro jedno x neplatí, tak jsou výroky na obou stranách nepravdivé. Mají tedy vždy stejnou pravdivost.
(vii): platí. Oba výroky požadují, aby platilo jak p, tak $q(x)$ pro nějaké x.
(viii): platí. Pokud platí p, tak jsou výroky na obou stranách pravdivé. Pokud p neplatí a q platí alespoň pro jedno x, tak jsou zase výroky na obou stranách pravdivé. Pokud neplatí ani p, ani $q(x)$ pro žádné x, pak jsou výroky na obou stranách nepravdivé. Mají tedy vždy stejnou pravdivost.

1a.4: (i): negace: $\forall x \in \mathbb{R}$: $x \leq 5$. Výrok platí, negace ne, třeba $x = 7$.
(ii): negace: $\exists x \in \mathbb{Z}$: $(x \leq 5 \wedge x^2 \neq 14)$. Výrok neplatí, negace ano, třeba $x = 2$.
(iii): negace: $\forall x \in \mathbb{R}$: $(x < 3 \wedge x \neq x - 1)$. Výrok platí (třeba $x = 0$, pak má implikace nesplněný předpoklad a tudíž platí), negace ne.
(iv): negace: $(\forall x \in \mathbb{R}$: $x^2 \geq 0) \wedge (\exists x \in \mathbb{R}$: $x \geq 0)$. Výrok neplatí, negace ano.
(v): negace: $(\exists x \in \mathbb{R}$: $x = \frac{x}{2}) \wedge (\exists x \in \mathbb{R}$: $x \neq 13x)$. Výrok neplatí (předpoklad splněn $x = 0$, závěr ne), negace ano (první výrok splněn $x = 0$, druhý také $x = 1$).
(vi): negace: $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}$: $x \geq y$. Výrok neplatí (to by muselo existovat jedno číslo, které je nejmenší ze všech reálných), negace ano (pro dané x stačí zvolit $y = x - 1$).
(vii): negace: $\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}$: $x^2 + y^2 < 0$. Výrok platí, negace ne.
(viii): negace: $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}$: $\sin(x) \neq \cos(y)$. Výrok platí (pro dané x stačí zvolit $y = \arccos(\sin(x))$), negace ne (ať zkusíme jakékoliv x, vždy nám jeho volbu zkazí nějaké y, které se hodnotou cosinu trefí do $\sin(x)$).

1b. Logika a matematika

Zde se podíváme, jak požadavek na přesnost a logickou správnost ovlivňuje strukturu matematiky a naopak jak matematika ovlivňuje použití logiky. Ukážeme také praktické rady, které ocení zejména ti, kdo se budou snažit psát důkazy. Některé části možná čtenář lépe docení, když se k nim zase vrátí po nabytí zkušeností v několika dalších kapitolách.

Matematika se dělí na rozličné obory podle toho, jaké objekty se zkoumají, například (zhruba řečeno) analýza zkoumá funkce, algebra struktury s operacemi, lineární algebra lineární prostory atd. Matematika ovšem nezkoumá objekty konkrétní, ale objekty abstraktní, dá se říci typy objektů. Každý výklad určitého oboru tak musí začít úmluvou, jaké objekty se budou zkoumat. Protože chceme, aby závěry matematiky byly naprosto spolehlivé, musí být také popis zkoumaných objektů zcela přesný, aby bylo vždy jasné, co je pravda a co ne (abstraktní svět matematiky je nutně černobílý).

Rozmyslete si například, že není možné se spolehlivě rozhodnout, zda autor této knihy je normální, protože nikdo přesně neví, co to vlastně je (hodně lidí si myslí, že ví, co je to normální, ale nějak se neshodnou). Zato všichni poznají, co je to sudé číslo, protože na to je přesná specifikace.

Specifikaci nových pojmů se v matematice říká **definice**. Většinou je nový pojem charakterizován vlastností, podle které se dá jednoznačně poznat. Můžeme například říct, že číslo x je sudé, pokud existuje celé číslo k takové, že $x = 2 \cdot k$. Když nám pak někdo dá číslo, tak se prostě podíváme, zda jej je nebo není možno zapsat příslušným způsobem, a tím se dozvíme, zda je sudé či ne.

Stojí za to poznamenat, že aby taková definice fungovala, tak ještě předtím musíme mít definice udávající, co je to rovnost a co jsou celá čísla, ty asi budou zase potřebovat další definice atd. Když se matematika dělá opravdu pořádně, dostane se člověk k úplným základům. Na to je speciální obor matematiky, většina matematiků se spokojí s tím, že určité věci už považuje za známé (rovnost, rovnice, základní algebra atd). Zkusme si tedy představit, že známe reálná čísla a víme, co je to nerovnost, a udělejme následující ukázkovou definici.

Definice.
Nechť x je reálné číslo. Řekneme, že je **kladné**, jestliže platí $x > 0$.

Zkusme si to rozebrat. První věta je uvozovací, říká nám, s jakými objekty budeme pracovat. Je to vlastně kód, myslí se tím, že x může být *libovolné* reálné číslo (někdo to občas i takto doslovně napíše, ať v tom má čtenář jasno). Správný překlad do logiky by tedy byl následující: „$\forall x \in \mathbb{R}$“.

Pro každé reálné číslo pak můžeme či nemůžeme říct, že je kladné, podle toho, jak dopadne ona definující podmínka. Tím je tento nový pojem přesně vymezen a nemůže se stát, že by dva lidé měli totéž číslo a neshodli se v názoru na to, zda je kladné.

Všimněte si jedné podstatné věci. Již z principu musí být mezi novým pojmem a podmínkou, která jej definuje, vztah ekvivalence: Pokud podmínka funguje, je použití nového pojmu oprávněné. Pokud nefunguje, není možné jej použít. Správně by tedy v definici mělo být napsáno „Řekneme, že x je kladné, právě tehdy když platí $x > 0$“. Jenže z nějakého důvodu je zvykem psát tam „jestliže“, což vlastně značí implikaci, takže tak, jak je to napsáno, to značí „$x > 0 \implies x$ kladné“. Jinými slovy, je to vlastně napsáno špatně, ale už se to tak dělá nejméně sto let a snad ve všech jazycích, tak do toho nemá smysl vrtat (občas se najde nadšenec, který si dá tu práci a píše opravdu definice jako ekvivalence, ale není jich moc).

V praxi tato nepřesnost nevadí, protože každý matematik ví, že definice se píšou takto a přitom se to bere jako ekvivalence. Je to součástí zasvěcení do matematiky, začátečníka to ale může zaskočit (pak jsou tu ovšem studenti, kteří nad tím nepřemýšlejí, ti si ničeho nevšimli a tuhle poznámku nejspíše vůbec nečtou). Vy už to tajemství znáte, vítejte v tajné lóži matematiků (na krvavý iniciační obřad si počkejte do prvního drsnějšího důkazu).

Poznámka stranou: Co když si někdo zavede jinou definici kladnosti? Pokud k tomu nemá opravdu dobrý důvod, tak jej nikdo nebude brát vážně a ta jeho definice zanikne. Pokud to bude mít dobře podloženo, pak získá následovníky a vytvoří se konkurenční typ matematiky. Naštěstí se to skoro vůbec nestává, protože lidé se při vytváření definic řídí především užitečností. Při hlubším studiu matematiky se na to dá občas narazit, pak člověk ví, že se musí při čtení knihy nejprve dobře podívat, s jakými pojmy autor pracuje. Není to ale až tak velký problém, protože na definici není podstatné jméno, ale význam dotyčného pojmu, tedy myšlenka. Matematik si tedy zjistí, jakou myšlenku dotyčným slovem autor míní, a pak už se jen dívá, co s ní v knize vyvede. Každopádně čtenář se nemusí bát, je téměř jisté, že na takovou situaci v životě nenarazí.

Narážíme tím na věc, která možná čtenáře překvapí: Definice si můžeme dělat, jak se nám zlíbí. Představme si, že by ten úplně první člověk, který pojem kladnosti zavedl, namísto toho prohlásil, že kladná čísla jsou taková, která splňují $x^2 = 13$. Co by se stalo? Z hlediska logického i matematického by na tom nebylo nic špatně, jenže problém by byl jinde: Tento pojem by nebyl příliš užitečný, nikdo by jej nepoužíval a brzy by z matematického života vymizel (darwinismus v matematice). Pojmy, které potkáváme, jsou vymyšleny tak, aby nám pomáhaly při práci, přičemž to, že se dožily současnosti, ukazuje, že se jejich autoři dobře trefili.

Definicemi vlastně vytváříme imaginární světy, záleží jen na naší představivosti, kolik a jaké vytvoříme. Úkolem matematiky pak je takové světy zkoumat.

Máme tedy pojmy a posuňme se dále. Cílem matematiky je najít o těchto užitečných pojmech co nejvíce informací. Tyto informace jsou pak sdělovány ve formě tvrzení, která se rozličně jmenují. Důležitá tvrzení se jmenují „věty“, jednoduchá zase „fakta“, používá se také přímo název „tvrzení“. Někdy z jednoho tvrzení hned s minimální prací vyplyne další, tomu pak říkáme „důsledek“. Posledním zajímavým názvem je „lemma“, to používáme pro pomocná tvrzení, často do nich schováváme nudné a pracné části důkazů vět, aby lépe vynikly hlavní myšlenky (viz Lemma 3a.5 a Věta 3c.5). Tato klasifikace je samozřejmě subjektivní a co je u jednoho autora důsledek, může mít jiný jako větu a podobně.

Ukažme si příklad.

Fakt.
Nechť $x \in \mathbb{R}$. Jestliže $x > 0$, pak $x(x + 1) > 0$.

Jako obvykle vidíme uvozovací větu a už jsme si rozmysleli, že je tam schováno slůvko „libovolné“ či „každé“. Trochu přesnější přepis by tedy byl následující:

• Pro každé $x \in \mathbb{R}$ platí: Jestliže $x > 0$, pak $x(x + 1) > 0$.

Teď už to snadno přeložíme do formálního jazyka, jak jsme jej viděli v kapitole 1a:

• $\forall x \in \mathbb{R}$: $(x > 0 \implies x(x + 1) > 0)$.

Každopádně jde o implikaci, nejoblíbenější matematickou strukturu.

Je také možné jít opačným směrem, k menší formálnosti. Můžeme třeba říct:
- Pro všechna kladná $x \in \mathbb{R}$ platí $x(x+1) > 0$.
- Pro všechna $x \in \mathbb{R}^+$ platí $x(x+1) > 0$.
- Pro každé $x > 0$ platí $x(x+1) > 0$.
- Všechna kladná x splňují $x(x+1) > 0$.

První z nich je stejně dobrá jako původní verze, jen zní méně „oficiálně“, což u méně důležitých tvrzení nemusí vadit. Druhá verze je také dobrá, dokonce je pěkně kompaktní, na druhou stranu může zkomplikovat život čtenáři, který není zvyklý na speciální značení $\mathbb{R}^+$. Její použití tedy záleží na tom, jak často autor v knize tuto značku používá a jak hodný chce na čtenáře být.

Poslední dva výroky už jsou na hranici, mnozí matematici by je považovali za nepřípustně nepřesné, protože nespecifikují, z jakého oboru vlastně x bereme (že by to byla kladná racionální čísla?). Nicméně pokud například celou kapitolu pojednáváme o reálných číslech, pak se považuje za jasné, že bereme $x \in \mathbb{R}$, a autoři občas dají přednost čitelnosti před naprostou správností.

Již jsme mluvili o tom, že spolehlivost matematiky spočívá v důkazech. I náš Fakt je tedy třeba dokázat, ukážeme si na něm nejobvyklejší metody důkazu implikace. Nejprve se ale zamyslíme nad tím, co takový důkaz vlastně je.

1b.1 Důkazy

Jak se vlastně dokáže, že nějaký výrok sestavený pomocí logických operací je (vždy) pravdivý? Většina důkazů má stejnou myšlenku: Je třeba pomocí známých faktů nějak ukázat, že ze všech řádků příslušné pravdivostní tabulky mohou reálně nastat jen ty, které mají na konci jedničku. Na to existují různé metody, podle toho, jak je výrok sestaven, ale většina z nich skončí tím, že se musí dokázat nějaká implikace. Například ekvivalence se nejčastěji dokazuje tak, že se ukážou implikace $p \implies q$ a $q \implies p$. Proto se zde na implikaci zaměříme.

Již jsme si rozmysleli, že pro pravdivost určité konkrétní implikace $p \implies q$ je naprosto kritická situace, kdy je p splněno. Co se pak stane, rozhodne o její pravdivosti, protože v situacích, kdy p splněno není, prostě nejde dotyčnou implikaci zneplatnit, ať už se stane cokoliv. Z toho vychází nejčastější způsob, jak se implikace dokazují. Představíme si, že jsme v situaci, že je p splněno, a musíme nějak ukázat, že pak za každých okolností už nutně nastane i q. Případ, kdy p splněno není, tedy při důkazu nijak neřešíme.

Ponaučení: Přímý důkaz implikace $p \implies q$ se dělá takto: Předpokládáme, že je p splněno, a pomocí argumentů ukážeme, že pak nutně nastává i q.

Všimněte si, že tím neříkáme, že je to p opravdu splněno, jen si představujeme, k čemu by vedlo, kdyby splněno bylo. Ukažme si to na příkladu implikace „Jestliže mi useknou hlavu, tak umřu“. Na začátku důkazu budeme předpokládat, že mi usekli hlavu, a pak pomocí vědy lékařské dovodíme, že jsem mrtev. Provedli jsme teď důkaz implikace „dekapitace $\implies$ kaput“, ale to neznamená, že jsem opravdu o kebuli přišel, jen jsme ukázali vzájemnou souvislost dvou určitých věcí.

Pravidlo, že při dokazování implikace zkoumáme jen situace, kdy je p splněno, má jednu zajímavou výjimku. Někdy (velice zřídka) potkáme situaci, že p splnit nikdy nejde. Pokud toto ukážeme, pak už celá implikace automaticky platí, viz pravdivostní tabulka. Takže implikace „Jestliže $13 > 23$, pak všichni studenti tohoto kursu vyletí“ je zaručeně pravdivá.

Teď se podíváme na tři hlavní postupy, kterými se v matematice dokazuje.

1b.2 Přímý důkaz:. Používá se k důkazu implikace a funguje přesně tak, jak to zní, prostě se vezme za dané, že platí její předpoklad, a dojde se nějakým zcela spolehlivým způsobem k platnosti jejího závěru. Ukážeme si to na důkazu implikace $x > 0 \implies x(x+1) > 0$.

Cestu od předpokladu k závěru si rozložíme na jednodušší kroky, které již budou jasné. Nejprve ukážeme důkaz superúplný, kde pečlivě zdokumentujeme všechny úvahy.

Celý dokazovaný výrok zní $\forall x \in \mathbb{R}$: $(x > 0 \implies x(x+1) > 0)$. Jde tedy o výrok s obecným kvantifikátorem, proto je nutno dokázat platnost oné implikace pro úplně všechna reálná čísla. Díky tomu rozhodně nebude fiungovat to, co někdy zkoušejí začátečníci: vyberou si nějaké pěkné číslo a vyzkouší to pro něj.

Kdyby byla množina reálných čísel konečná, tak by je šlo probrat jedno po druhém. Existují důkazy, které lze redukovat na konečnou množinu případů, které se pak proberou, a pokud to pokaždé dopadne dle zadání, pak je důkaz hotov (viz poznámka po důkazu Faktu 2a.3). Nicméně náš případ to není.

My musíme ukázat platnost implikace pro všechna x, což se dělá standardně tak, že si prostě vezmeme nějaké reálné číslo x, ale nespecifikujeme jaké (ani to sami nevíme), prostě máme reálné číslo x, o kterém nevíme nic konkrétního, jen tu informaci, kterou dostaneme z dokazovaného tvrzení (popřípadě věci, které jsou platné pro všechna reálná čísla).

Mějme tedy reálné číslo x a ptáme se, zda platí implikace $x > 0 \implies x(x+1) > 0$. O její pravdivosti rozhodne, zda ve všech případech, kdy je splněn předpoklad $x > 0$, je také splněn závěr. K původnímu předpokladu $x \in \mathbb{R}$ tedy přidáme předpoklad další, že $x > 0$, a zkusíme se od nich postupnými kroky dobrat k cíli.

Jestliže $x > 0$, pak také $x + 1 > 0$. Čtenáři je to asi jasné, ale zkusme se pro úplnost zamyslet, jak by to šlo odvodit ze základních vlastností čísel. Když k rovnici $x > 0$ přičteme na obou stranách jedničku, dostaneme $x + 1 > 1$, máme také $1 > 0$, díky čemuž dostáváme řetězec nerovností $x + 1 > 1 > 0$. Pak také musí platit $x + 1 > 0$ (vlastně používáme tranzitivitu relace $>$, viz kapitola 3b).

Takže teď máme předpoklad $x > 0$, také jsme odvodili, že $x + 1 > 0$, a patří mezi základní vlastnosti, že vynásobením dvou kladných čísel získáme číslo kladné, tedy $x(x + 1) > 0$.

(Je také možné argumentovat tím, že v nerovnost $x + 1 > 0$ vynásobíme obě strany kladným číslem x, čímž dostaneme tu žádanou.)

Každopádně je důkaz hotov, ukázali jsme, že jakmile je pro libovolné $x \in \mathbb{R}$ splněno $x > 0$, pak už není jiná možnost, než že $x(x + 1) > 0$.

Důkaz je správný, pokud je v něm každý krok odůvodněn, někdy se odvoláváme na předpoklady z věty (buď z preambule, nebo z předpokladu dokazované implikace), někdy na základní, již známé (a někde dokázané) vlastnosti, často také na tvrzení, která jsme dokázali dříve. Náš důkaz toto splňuje.

Takto se ale samozřejmě důkazy nepíší, ty jednodušší věci se vynechávají, protože se předpokládá, že si je čtenář domyslí. Stručnost důkazu tedy přímo závisí na tom, jak pokročilé čtenáře autor očekává. Zkusme si tu ukázat verzi důkazu vhodnou pro zcela začínajícího studenta (tedy pro tuto kapitolu):

Důkaz: Nechť x je libovolné reálné číslo. Jestliže $x > 0$, pak také $x + 1 > 0$, z těchto dvou nerovností již dostáváme $x \cdot (x + 1) > 0$.

□

Ten čtvereček je obvyklá značka udávající konec důkazu, aby čtenář věděl, že autor již nic dalšího nehodlá dodat. Čtenář by si v té chvíli měl rozmyslet, že to, co do té doby četl, je opravdu důkazem žádaného tvrzení. Používá se také celý černý čtvereček či zkratka Q.E.D. z latinského „quod erat demonstrandum“ neboli „což bylo dokázati“. Vlastenci dávají CBD.

Pro úplnost ještě ukážeme, jak by tento důkaz vypadal v knize pro pokročilejší studenty (kapitoly této knihy s vyšším číslem). Rovnou jich ukážeme několik.

Důkaz je zřejmý.

Důkaz je triviální.

Důkaz je snadný a přenecháme jej čtenáři jako cvičení.

1b.3 Nepřímý důkaz:. I ten slouží k dokazování implikace, finta spočívá v tom, že se namísto té dané dokazuje její obměna (viz 1a), což je z logického pohledu postačující.

Vrátíme se k našemu příkladu, teď musíme nejprve nahradit implikaci její obměnou:

$$\forall x \in \mathbb{R}\colon (x(x + 1) \leq 0 \implies x \leq 0).$$

Tento výrok má zase tvar implikace a tu dokážeme přímým důkazem, tedy postupně se od předpokladu k závěru nové implikace propracujeme jednoduchými kroky.

Důkaz: Mějme libovolné $x \in \mathbb{R}$ a předpokládejme, že splňuje $x(x+1) \leq 0$. Má-li být součin dvou čísel záporný či nulový, vede to na dvě možnosti.

a) Jedna možnost je, že $x \leq 0$ a $x + 1 \geq 0$. Pak máme $x \leq 0$ a důkaz je hotov.

b) Druhá možnost je, že $x \geq 0$ a $x + 1 \leq 0$. Tyto dvě nerovnosti ale nemohou pro žádné číslo x platit zároveň, tento případ proto nikdy nenastane.

Z nerovnosti $x(x + 1) \leq 0$ se tedy vždy dostáváme k případu a) a odtud k $x \leq 0$.

□

Zde jsme si ukázali další užitečnou věc. Někdy se stane, že nás důkaz dovede k rozcestí, můžeme se vydat vícero směry podle toho, s jakými objekty pracujeme. Protože u obecných důkazů nikdy přesně nevíme, s čím pracujeme, je nutné projít všechny nabízející se cestičky a u všech dojít ke správnému cíli, popřípadě ukázat, že se do té či oné cestičky vůbec nedá vejít. Ukažme si ještě jednu verzi nepřímého důkazu.

Důkaz: Mějme libovolné $x \in \mathbb{R}$ a předpokládejme, že splňuje $x(x+1) \leq 0$. Důkaz dále rozdělíme na možnosti podle znaménka $x + 1$:

a) Jestliže $x + 1 \leq 0$, pak $x \leq -1 < 0$ a tedy $x \leq 0$, přesně jak jsme potřebovali.

b) Jestliže $x+1 > 0$, pak lze nerovnost $x(x+1) \leq 0$ vydělit kladným číslem $x+1$ bez změny směru nerovnosti a dostaneme zase $x \leq 0$.

Každopádně tedy $x \leq 0$.

□

Jsou tvrzení, u kterých je nepřímý důkaz tou nejlepší volbou, ale tady to spíš neplatí, určitě bychom dali přednost přímému důkazu výše. Ukažme si příklad, kdy je nepřímý důkaz znatelně lepší.

Příklad 1b.a: Tvrzení: Jestliže je číslo $n > 2$ prvočíslo, pak je liché.

Přímý důkaz nevypadá moc nadějně, protože býti prvočíslem je docela komplikovaná vlastnost, není jasné, jak z ní něco vytěžit. Zkusme důkaz nepřímý, na to ale potřebujeme nejprve trochu logicky pracovat. Začneme tím, že si dotyčný výrok přepíšeme do správného logického tvaru. To se dá udělat více způsoby, nejpohodlnější je tento:

$\forall n \in \{x \in \mathbb{N};\ x > 2\}$: ($n$ je prvočíslo $\implies$ n je liché).

Obměna pak zní

$\forall n \in \{x \in \mathbb{N};\ x > 2\}$: ($n$ je sudé $\implies$ n není prvočíslo).

Teď toto tvrzení dokážeme přímým důkazem. Vezmeme si libovolné n z dané množiny, n je tedy přirozené číslo větší než 2. Pro něj chceme dokázat příslušnou implikaci, takže budeme navíc předpokládat, že je také sudé. To podle definice znamená, že $n = 2k$, kde k je nějaké celé číslo. Protože $n > 2$ neboli $2k > 2$, musí také platit $k > 1$. Odvodili jsme tedy, že $n = 2 \cdot k$ je možné rozložit jako součin dvou celých čísel větších než 1, což podle definice znamená, že n nemůže být prvočíslo.

Obměnu jsme dokázali, tudíž jsme dokázali i původní dané tvrzení.

△

1b.4 Důkaz sporem:. Důkaz sporem je jeden z nejmocnějších nástrojů. Mějme libovolný výrok r (ne nutně implikaci). Důkaz sporem spočívá v tom, že dokážeme implikaci $\neg r \implies F$ (například přímo či nepřímo), řečeno slovy, ukážeme, že pokud by r neplatilo, tak nastane něco, co se nikdy nemůže stát, něco, co je ve sporu s naším (matematickým) světem. Podle selského rozumu to znamená, že neplatnost r nemůže nastat neboli r platí.

Formální logika to vidí podobně: Dokázali jsme platnost implikace $\neg r \implies F$. Její závěr je ale vždy nepravdivý, a jediný případ, kdy je implikace s nepravdivým závěrem pravdivá, je tehdy, když je také předpoklad nepravdivý. Tedy $\neg r$ neplatí čili r platí.

Jednou z výhod důkazu sporem je, že jej lze aplikovat i na tvrzení, které nejsou implikace. Oblíbenou situací je, když chceme dokázat, že něco neexistuje. To se přímo dokazuje špatně (dokažte, že kolem nás nelítají neviditelní a nenahmatatelní Marťané s anténkami). Důkaz sporem znamená, že začneme naopak: Předpokládáme, že to něco existuje, což je pozitivní informace, ze které se dá s trochou štěstí něco vytěžit, pokud možno nějaký kýžený nesmysl.

Jak důkaz sporem vypadá, když takto chceme dokázat implikaci $p \implies q$? Pak bychom měli dokázat implikaci $\neg[p \implies q] \implies F$ neboli $(p \wedge \neg q) \implies F$. To nám dává praktický návod: Předpokládáme, že platí předpoklad p a neplatí závěr q, a odvodíme z toho nějaký spor.

Jako příklad znovu dokážeme (tentokráte sporem), že pro všechna reální čísla platí $x > 0 \implies x(x+1) > 0$.

Důkaz: Mějme libovolné reálné číslo x a předpokládejme, že platí $x > 0$ a také $x(x+1) \leq 0$ (negace závěru). Nerovnost můžeme vydělit kladným číslem x na obou stranách a ona pořád zůstane platná, máme tedy $x+1 \leq 0$. Spojením nerovností $x + 1 \leq 0 < x$ dostaneme $x + 1 < x$ neboli $1 < 0$, což je spor. Důkaz je hotov.

□

Pro další ukázku nepřímého důkazu a důkazu sporem viz důkaz Faktu 2a.3 a poznámky za ním. Tím jsme probrali hlavní metody důkazu.

S 1b.5 Jak vytvářet důkazy

Na vytváření důkazů žádný algoritmus či návod není, vždy je to otázka inspirace a hlavně zkušenosti a znalostí. Spíš než klasickému řešení příkladů se to podobá řešení hádanek či hlavolamů. Zmíníme zde několik zásad, které by mohly pomoci navést čtenáře na správnou cestu, když se dostane do problémů.

1. Vždy si nejprve dobře rozmyslete, s čím vlastně dokazované tvrzení pracuje. Někdy je to jasné, někdy to chce trochu přemýšlení. Jestliže máme dokazovat například prostotu zobrazení či rovnost obyčejných množin, pak je to vcelku jasné, pracujeme se zobrazeními či množinami. Co když ale máme dokázat například inkluzi $P(A) \subseteq P(B)$? Pak nemáme šanci uspět, dokud si nerozmyslíme, že $P(A)$ je množina, jejíž prvky jsou zase množiny, jmenovitě podmnožiny A. Takže když napíšeme $x \in P(A)$, tak to x vlastně splňuje $x \subseteq A$.

Mluví-li dokazované tvrzení o řešení rekurentní rovnice, co to vlastně řešení je, jaký matematický objekt? I zde je malá šance, že se důkaz povede, pokud nám není jasné, že tímto objektem je posloupnost čísel, která po dosazení do rovnice dá pravdivý výraz.

Podobně když máme dokázat nějakou vlastnost dané relace, tak si musíme rozmyslet, jak s ní budeme pracovat. Je možné pracovat s pojmem platnosti či neplatnosti xRy, je ale také možné pracovat s relací jako s množinou R dvojic a používat množinové operace, jejichž význam je pak také třeba si rozmyslet. Každý z těchto přístupů má své slabiny i výhody, je třeba se pro jeden rozhodnout.

2. Další důležitá věc je si přesně vyjasnit, co se vlastně dokazuje. Když dokazujeme indukcí, je třeba si nejprve přesně říct, jak vypadá výrok $V(n)$ a pak se toho držet. Vyplatí se si takovéto věci napsat, mozek lépe pracuje s tím, co vidí očima. Vůbec je dobré si své úvahy někde bokem črtat. Často se stane, že člověk v myšlenkách dojde do určitého bodu a neví, jak dál. Když si ten bod napíše, občas najednou zjistí, že je to dál vlastně snadné. Pracovat s pojmy v hlavě je pro méně zkušeného velice obtížné a omezuje to možnosti.

Je dobré si v průběhu dokazování čas od času občerstvit, co se vlastně chce dokázat, protože někdy člověka myšlenky svedou jinam. Vyplatí se tedy opravdu si to hlavní napsat a občas se na to podívat.

3. Většinou se vyplácí přistupovat k dokazování strukturovaně a začínat od základů, nenechat se ohromit případnou komplikovaností zadání. Máme dokázat, že $P(A) \subseteq P(B)$? Ať už jsou ty množiny sebekomplikovanější, inkluze se dělá vždy stejně, přes prvky, takže si to napišme: Chceme ukázat, že $x \in P(A) \implies x \in P(B)$. Hned máme nápovědu, na co se zaměřit.

Chceme ukázat, že nějaké T je prosté? Zase začneme od základů, napíšeme si definici prostoty a vidíme, co je třeba udělat. Podobně když máme dokázat nějakou vlastnost relace atd atd. Ztrácíme se v indukci? Začněme od základů. Krok (1) chce dokázat pro libovolné $n \geq n_0$ výrok $V(n) \implies V(n+1)$. Co to vlasně je? Dosadíme za V do dotyčné implikace a hned máme nápovědu.

4. Udělejte si pořádek v tom, jakou roli jednotlivé faktíky objevující se v problému hrají. Některé jsou dány již v zadání jako něco, co je možné použít. Některé se v průběhu důkazu takovým předpokladem stanou, buď z logiky důkazu (když třeba dokazujeme implikaci $p \implies q$, tak začneme předpokladem, že p platí, je to tedy další fakt, který je možné použít), nebo třeba proto, že jsme již to či ono úspěšně dokázali. Další faktíky jsou tu naopak od toho, abychom je dokázali.

Je opravdu důležité v tom mít jasno, opět často pomůže si to přehledně napsat. Pokud máte nutkání něco při dokazování použít, tak si ověřte, jestli je už to v kategorii „mám dáno, mohu použít“, častou chybou je totiž používat v důkazu to, co se vlastně má dokazovat. Takový důkaz je pak samozřejmě špatně. Naopak pokud se stane, že se zadrhnete, pak se vyplatí podívat na seznam věcí, které jsou k dispozici jako předpoklady. Použili už jsme všechno nebo je tam ještě něco, co jsme nevyužili? Tato jednoduchá věc často výrazně napoví. Pokud napíšete důkaz a nepoužijete v něm všechny předpoklady, tak to je většinou znamení, že je někde chyba.

5. Poté, co důkaz dopíšete, se na něj trochu z odstupu podívejte, jakou má strukturu. Plyne správným směrem? Pokud po půl stránce výpočtu vítězoslavně podtrhnete $1 = 1$, tak je to skoro určitě špatně, protože toto jste dozajista dokazovat nechtěli. Tím se ovšem dostáváme k tématu další sekce, tak s radami skončíme.

1b.6 O jedné oblíbené chybě

Představme si studenta-začátečníka, který se snaží dokázat, že pro $n \in \mathbb{N}$ platí $\frac{n+1}{n} > 1$. S vysokou pravděpodobností student začne žádanou nerovnost upravovat, dokud se nedostane k něčemu pravdivému, například takto:

$$\begin{aligned} \tfrac{n+1}{n} &> 1 \\ n+1 &> n \\ 1 &> 0. \end{aligned}$$

Načež prohlásí „což platí“ a myslí si, že má hotovo. A nemá. Toto totiž ani náhodou nedokazuje, že $\frac{n+1}{n} > 1$. Proč? Kdyby to byl opravdu důkaz, pak by fungovalo i toto:

$$\begin{aligned} 13 &= 23 \\ 13 - 18 &= 23 - 18 \\ -5 &= 5 \\ (-5)^2 &= 5^2 \\ 25 &= 25 \\ 0 &= 0. \end{aligned}$$

Je nicméně zjevné, že $13 = 23$ není pravda, tudíž tento postup nemůže být důkazem. Kde je chyba? Rozhodně ne v samotných krocích, ty jsou všechny korektní. Problém je v tom, že důkaz vede špatným směrem. Student totiž dokázal následující tvrzení:

$$\tfrac{n+1}{n} > 1 \implies 1 > 0,$$

čili jsme ukázali, že pokud platí něco, co vlastně chceme zkoumat, tak pak platí i $1 > 0$. Jenže my nechceme dokazovat, že $1 > 0$, to už víme. My naopak potřebujeme ukázat, že platí předpoklad, to ale z oné implikace nedostaneme, jak už jsme si rozmysleli v předchozí části.

Nám by pomohla opačná implikace, od známého k neznámému: $1 > 0 \implies \frac{n+1}{n} > 1$. Ten dostaneme, když předchozí postup obrátíme.

$$\begin{aligned} 1 &> 0 \\ n+1 &> n \\ \tfrac{n+1}{n} &> 1. \end{aligned}$$

Všechny provedené úpravy jsou korektní, jde tedy o správný důkaz, dostal nás od známého k žádanému.

U druhého příkladu se právě toto nepovede. Dokážeme se dostat na půl cesty,

$$\begin{aligned} 0 &= 0 \\ 25 &= 25 \\ (-5)^2 &= 5^2, \end{aligned}$$

ale odebrat mocninu z rovnosti není možné, tam se pokus o obrácený chod pokazí. Můžeme zkusit obě strany odmocnit (to je korentní úprava), dostaneme $\sqrt{(-5)^2} = \sqrt{5^2}$ neboli $|-5| = |5|$, což dává $5 = 5$ namísto toho, co bychom potřebovali.

Kupodivu se onen nesprávný postup „od konce“ často vídá. Proč tomu tak je? Pro méně zkušeného není snadné najít ten správný postup. Jak vlastně člověk přijde na to, že má začít zrovna nerovností $1 > 0$, aby se dostal k $\frac{n+1}{n} > 1$? Jak pak přijde na to, kterými úpravami se tam dostat? Onen „špatný postup“ na tyto otázky umí odpovědět, což je od něj pěkné. Jen si musíme být vědomi toho, že to důkaz není, je to prostě jen taková pomocná čmáranice, kterou jsme si udělali někde bokem. Pak ale musíme napsat „Důkaz:“ a znovu to přepsat, tentokráte v opačném pořadí, a přitom si kontrolovat, že opravdu všechny kroky lze obrátit. Pokud to vždy vyjde, dostaneme korektní důkaz.

Přesto bych doporučil se pokud možno tomuto postupu vyhýbat, a to z několika důvodů. Za prvé, je zbytečně dlouhý, často jednu stranu (ne)rovnosti vůbec neupravujeme a jen ji opisujeme (viz příklad níže). Za druhé, tento postup nás nutí omezit se jen na ekvivalentní úpravy, díky čemuž nám jsou některé užitečné triky odepřeny - to se týká zejména důkazů nerovností, které jsou při tomto postupu pro začátečníka vyloženě zrádné, viz poznámka na konci. Jak tedy vypadá doporučovaný postup?

Začne se výrazem na jedné straně (ne)rovnosti a pomocí úprav se postupně řetězcem rovností či nerovností dojde k cílovému výrazu na pravé straně.

Jako příklad si dokážeme, že pro všechna $k \in \mathbb{N}$ platí $\frac{(k-1)^2+4k}{(k+1)^2} + \frac{k-1}{k^2-k} = \frac{k+1}{k}$. Obvykle bývá lepší začít tou složitou stranou, zkusíme ji co nejvíce zjednodušit.

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

Tím je důkaz hotov, výraz nalevo se opravdu rovná výrazu úplně napravo. Tento postup je výrazně kratší, než kdybychom použili metodu postupného upravování, protože tam bychom jen opisovali pravou stranu a pak to museli ještě jednou přepsat ve správném pořadí.

Zkušenější student většinou u jednodušších rovností a nerovností dokáže odhadnout, jak s tou jednou stranou cvičit, aby z toho vznikla strana druhá. Opravdu tento postup doporučujeme. U nerovností si ještě potřebujeme pohlídat, aby všechny kroky vedly na stejnou stranu: Například z řetězce $a < b = c \leq d < e = f$ dostáváme $a < f$, ale z $a < b = c \geq d$ neplyne o vztahu mezi a a d nic.

Někdy se samozřejmě může stát, že potřebné kroky nejsou vidět, to se u složitějších nerovností stane i ostřílenému matematikovi. Pak přijde vhod onen postup „od konce“, jen si je třeba pamatovat, že to není důkaz. Ten vznikne teprve tehdy, když se to přepíše ve správném směru neboli provede zpětný chod. Někdy se čas šetří tím, že se za ten „špatný“ postup napíše věta typu „Protože všechny provedené operace jsou ekvivalentní a postup lze obrátit, žádaná (ne)rovnost je dokázána.“ Je to ale nouzovka, nedoporučujeme to.

Tyto rady mají mnohem obecnější platnost než jen u důkazů (ne)rovností. Přestavme si, že se snažíme ukázat, že z výroku p plyne výrok z. Zkoušíme přímý důkaz a pomocí úvah se přes mezikroky dostaneme k výroku u, ale nevíme, jak dál: $p \to q \to \cdots \to u$. Pak někdy stojí za pokus si vyjít vstříc z cíle a najít cestu $z \to y \to \cdots \to u$. Tím došlo k propojení, ale důkaz to není, což je pěkně vidět na obrázku:

$$p \to q \to \cdots \to u \leftarrow \cdots \leftarrow y \leftarrow z.$$

Abychom dostali platný důkaz, je třeba ověřit, že všechny kroky při postupu od konce jsou ekvivalentní, takže lze

udělat i zpětný chod. Dostáváme pak řetězec úvah

$$p \to q \to \cdots \to u \leftrightarrow \cdots \leftrightarrow y \leftrightarrow z,$$

který již dává přímý důkaz $p \to \cdots \to u \to \cdots \to z$. Pro příklad se podívejte třeba na cvičení 5a.7 (ii).

Tím v zásadě končí tato kapitola. Pokud si chce čtenář udělat jasno v korektních a ekvivalentních úpravách a problémech s důkazy zpětným chodem, přidáváme další detaily v kapitole 14.