21. Přehled základů logiky

Základem matematického usuzování a vyjadřování je logika. Jde o samostatný obor, který nachází uplatnění nejen v matematice, ale také v dalších přírodních vědách, ve filosofii, náboženství nebo třeba právech.

Zde stručně připomeneme základy.

21a. Výroky a spojky

Logika je obor zabývající se zkoumáním situací, ve kterých dokážeme ze znalosti, zda jsou pravdivá určitá tvrzení, odvodit spolehlivě pravdivost či nepravdivost tvrzení jiných. Tímto problémem se myslitelé zabývali několik tisíc let, vyvrcholením jejich snah byl vznik formálního systému pro zacházení s informacemi.

Základem jsou výroky (značíme je malými písmeny). Výrok je 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 (stát se to mohlo, umřel až o týden později), ale nějakou pravdivostní hodnotu to má, je to proto výrok.

Je dobré si rovnou říct (budeme na to narážet opakovaně), že konkrétní pravdivost či nepravdivost se může měnit v závislosti na kontextu. Například výrok o Zemi výše může být za několik (miliónů) let nepravdivý. Výrok o čtení skript také platí či neplatí podle toho, kdy jej řekneme. To není na závadu, obvykle pracujeme (a vyhodnocujeme tvrzení) v určitém konkrétním prostředí a od výroků požadujeme, aby tam, kde je používáme (třeba v našem světě), měly jasně dánu pravdivostní hodnotu (i když ji třeba sami neznáme).

Toto pro změnu výroky nejsou: „ahoj“, „31“, „modrá je dobrá“, „5+8“, „jsem normální“, „prší“. Kupodivu zrovna tvrzení „prší“ se často v populárnějších rozpravách o logice používá jako příklad výroku, ale výrokem se to stane až po upřesnění, kde a kdy má pršet, jinak totiž nelze určit, zda je pravdivý či ne. Věta „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 zajímají logiku. Máme jednoduché výroky (atomární), všelijak je spojujeme a modifikujeme a zajímá nás, jak pravdivost nových výroků závisí na pravdivosti těch původních. Přitom nás vůbec nebude zajímat, co vlastně jednotlivé výroky říkají, 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**.

Výroky spojujeme či modifikujeme operacemi.

21a.1 Operace

• 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. Zde zase narážíme na to, že pravdivostní hodnota výroků může záviset na kontextu (interpretaci prostředí), od negace požadujeme, aby vždy dopadla naopak než daný výrok. Například negace výroku „tady a teď prší“ je „tady a teď neprší“, protože v každé situaci platí buď jeden, nebo druhý. Rozhodně negací nebude „nejsou tu teď mraky“, protože může nastat situace, kdy jsou tvrzení „nejsou tu teď mraky“ a „tady teď prší“ obě nepravdivá.

p	$\neg p$
0	1
1	0

Fungování negace se dá elegantně vyjádřit takzvanou pravdivostní tabulkou. 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 1 pro pravdu a 0 pro nepravdu. Občas také budeme v textu používat T a F jako „true“ a „false“.

Výroky můžeme spojovat logickými spojkami. Nejpoužívanější jsou tyto čtyři operace.

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. Pro znak $\wedge$ autor doporučuje název „átítko“.

• **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. Pro znak $\vee$ autor doporučuje název „nebotítko“.

• **implikace** značená „$p \Longrightarrow q$“ popř. „$p \to q$“ 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

Rovnou poznamenejme, že spojka „nebo“ se v běžné řeči také používá ve významu vylučovacím, třeba „budeš se učit nebo nedostaneš večeři“. Autor takovéhoto výroku asi nemá v úmyslu prohlásit jej za splněný v případě, kdy jsou pravdivé obě složky najednou. Vylučování se má správně říkat „buď p, nebo q“ a je to jiná logická spojka jménem „xor“, která se v matematice běžně nepoužívá, zato ji mají rádi počítačovníci.

Operace budeme ilustrovat pomocí výroků 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, podívejme se blíže na ostatní dvě operace.

Implikace $p \Longrightarrow q$ v našem příkladě 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, že v případě neplatného předpokladu je implikace jako celek pravdivá. Na první pohled to může vypadat zvláštně, ale přesně takto to potřebujeme v aplikacích.

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.

Ekvivalence představuje pevnější vazbu mezi výroky, protože je to vlastně implikace v obou směrech. Pokud je platné p, tak musí být platné i q, a naopak.

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 je tedy pomocí ekvivalence „bonbón dostaneš právě tehdy, když budeš hodný“. Tím jsou oba základní jevy („hodný“ a „bonbón“) vzájemně propojeny a musí si pravdivostí odpovídat, aby tento slib zůstal splněn. Zajímavá je rovněž implikace „když nebudeš hodný, nedostaneš bonbón“, která rodiče vůbec nezavazuje k vydání bonbónu. Obávám se nicméně, že hodné dítě v takové situaci nedocení půvaby formální logiky.

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, r, … , pak nás zajímá, jak jeho pravdivost závisí na vstupních datech neboli na pravdivostních hodnotách těch p, q, r, … To se zase nejlépe vyjádří tabulkou.

Ukážeme 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

Všimneme si, že výsledné hodnoty jsou stejné jako v tabulce pro implikaci. To říká, že výroky $\neg p \vee q$ a $p \Longrightarrow q$ mají vždy stejnou pravdivostní hodnotu, tedy z pohledu logiky nesou stejnou informaci a jsou navzájem zaměnitelné.

To znamená, že třeba „jestliže je pátek, tak je třináctého“ má stejnou pravdivost jako „není pátek nebo je třináctého“. V praxi je většinou forma $p \Longrightarrow q$ pro člověka přístupnější a nabízí informaci v podobě, ve které se snadno aplikuje; výraz $\neg p \vee q$ se zase často hodí, když s výroky manipulujeme, protože disjunkce a negace jsou jednodušší operace.

Ve formální logice se takovéto významové shodě výroků založené čistě na jejich struktuře (nikoliv obsahu) říká „logická ekvivalence“ a značí se $\equiv$, někteří autoři také píšou $\models\!\!\models$. Platí tedy

- $[p \Longrightarrow q] \equiv [\neg p \vee q]$.

Podobně se dá ekvivalence $p \Longleftrightarrow q$ nahradit dvěma implikacemi $p \Longrightarrow q$ a $q \Longrightarrow p$, ostatně samo značení to naznačuje. Platí tedy

- $[p \Longleftrightarrow q] \equiv [(p \Longrightarrow q) \wedge (q \Longrightarrow p)]$.

Některé výroky mají stále stejnou pravdivostní hodnotu bez ohledu na vstupy, čistě kvůli své struktuře. Například výraz $p \vee \neg p$ bude vždy pravdivý pro libovolné p (je nebo není pátek). Logici takovýmto formálně vždy platným výrazům říkají tautologie, někdy se značí T jako Tautologie nebo taky True. Naopak výraz $p \wedge \neg p$ je vždy nepravdivý (je a není pátek). Tomu se v logice říká kontradikce a výrok, který je vždy nepravdivý, se značí F jako False.

21a.2 Pravidla

Pro logické operace platí řada pravidel. Nemá smysl učit se je nazpaměť, obvykle jsou zcela zjevná, pokud se trochu zamyslíme.

Začneme tím nejjednodušším.

- $p \wedge p \equiv p$, $p \vee p \equiv p$, $\neg\neg p \equiv p$;
- $p \wedge \neg p \equiv F$, $p \vee \neg p \equiv T$;
- $p \wedge T \equiv p$ $p \vee F \equiv p$;
- $p \wedge F \equiv F$, $p \vee T \equiv T$.

Logický součin a součet se chovají jako jejich algebraičtí jmenovci.

- $p \wedge q \equiv q \wedge p$, $p \vee q \equiv q \vee p$;
- $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$, $p \vee (q \vee r) \equiv (p \vee q) \vee r$;
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.

Díky asociativitě můžeme bez problémů logicky sčítat a násobit více výroků a psat to bez závorek třeba takto: $p \wedge q \wedge r \wedge s$.

V seznamu nám chybí „šipkové“ spojky. Ekvivalence je komutativní a také asociativní, takže v principu má smysl psát výrazy jako $p \iff q \iff r$. Problém je, že to není užitečné. Zrovna tento výraz je totiž splněn přesně v případě, kdy je lichý počet složek pravdivý (přesvědčete se tabulkou), jenže to neodpovídá tomu, co bychom v praxi potřebovali. My spíš potřebujeme postihnout situaci, kdy máme nějaké výroky a chceme vědět, že jsou na tom všechny stejně, tedy buď všechny pravdivé nebo všechny nepravdivé. To v matematice vystihujeme slovy, že výroky jsou „navzájem ekvivalentní“, formálně se to zapíše $[p \iff q] \wedge [q \iff r]$. Pak už automaticky platí i $p \iff r$, tedy všechny tři výroky jsou navzájem pravdivostně propojeny.

Ekvivalence tedy formálně asociativní je, ale prakticky to nepoužíváme. U implikace je to ještě jednodušší, ta ani formálně nesplňuje žádnou běžnou vlastnost, tedy není ani komutativní, ani asociativní. Obojí má zásadní dopad na praktické použití, což uvidíme záhy, zatím jen konstatujme, že nemá ani formální smysl vytvářet řetízky typu $p \implies q \implies r$. Je to podobné jako u algebraické operace dělení, kde také $16 : 4 : 2$ nemá smysl, musíme čtenáři závorkováním říct, zda má počítat $(16 : 4) : 2 = 2$ nebo $16 : (4 : 2) = 8$.

Abychom to vynahradili, zmíníme vlastnost, která pro implikaci platí a je velmi důležitá: Jestliže víme, že jsou pravdivé implikace $p \implies q$ a $q \implies r$, pak už je zaručeně pravdivá také implikace $p \implies r$. Tato vlastnost se dá zobecnit na delší navazující řetězce a potvrzuje intuitivní představu, že když se v úvahách z nějakého faktu A správnými kroky postupně posouváme přes jiné poznatky až k závěru B, tak jsme tím potvrdili, že z A plyne B. Je to jakýsi „teleskopický princip“ (sklapující se pirátský dalekohled). Pro případ dvou implikací (ať ušetříme psaní) lze tento princip vyjádřit například tak, že výrok

$$[(p \implies q) \wedge (q \implies r)] \implies [p \implies r]$$

je vždy pravdivý (tautologie). Dá se to ověřit pravdivostní tabulkou, kde ve všech osmi řádcích u tohoto výroku najdeme jedničku. Jak už jsme zmínili, totéž funguje pro ekvivalenci.

Důležitá jsou také pravidla, která nám umožňují negovat operace.

- $\neg(\neg p) \equiv p$;
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$; $\neg(p \vee q) \equiv \neg p \wedge \neg q$;
- $\neg(p \implies q) \equiv p \wedge \neg q$; $\neg(p \iff q) \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$.

Vztahy v druhém sloupci se jmenují **de Morganovy zákony**. Umožňují nám například najít negaci implikace:

$$\neg(p \implies q) \equiv \neg(\neg p \vee q) \equiv \neg\neg p \wedge \neg q \equiv p \wedge \neg q.$$

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. Formálně:

$$\neg(p \iff q) \equiv \neg[(p \implies q) \wedge (q \implies p)] \equiv \neg(p \implies q) \vee \neg(q \implies p) \equiv (p \wedge \neg q) \vee (q \wedge \neg p).$$

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. Takové situace jsou dvě, obě najdeme na konci výpočtu.

21b. Predikátová logika

Většina výroků zkoumaných v praxi má v sobě zabudovány parametry. Třeba „teď tady prší“ vlastně má 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. 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. Některé výroky platí úplně vždy, bez ohledu na naší volbu proměnné. To se vyjadřuje slovy „pro každé x platí $p(x)$“ a zapisujeme „$\forall x\colon p(x)$“. Například výrok „$x^2 \geq 0$“ je určitě pravdivý, ať už za x zvolíme jakékoliv reálné číslo. Běžný matematik by 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“. Tento zápis (kterého se v této knize budeme držet) bohužel není standardní. Někdy se místo dvojtečky používá běžná čárka, zejména logici-specialisti pak preferují zápis pomocí závorek, třeba $(\forall x \in \mathbb{R})\ x^2 \geq 0$. Je užitečné vědět (zejména v některých důkazech), že vymezení množiny se dá nahradit implikací:

$$\forall x\colon [x \in \mathbb{R} \implies x^2 \geq 0\,].$$

Specifikace množiny je nezbytná a závisí na ní pravdivost výroku, například víme, že když se namísto čísel reálných podíváme na čísla komplexní, tak už ten výrok $x^2 \geq 0$ není vždy pravdivý.

2. Někdy nám stačí ke štěstí, aby byl zkoumaný výrok pravdivý alespoň někdy. Vyjádříme to slovy „existuje x, pro které platí $p(x)$“ a zapisujeme to „$\exists x\colon p(x)$“. Příklad pravdivého existenčního 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 existuje více používaných zápisů, ale měly by být všechny srozumitelné, jsou si podobné.

Značkám $\forall$ a $\exists$ se říká **kvantifikátory**, ten první je **obecný**, ten druhý **existenční**. Když je otočíte o 180^o neboli π radiánů, dostanete písmena A a E jako „All“ a „Exists“, dobře se to pamatuje. Protože mi oficiální názvy přijdou dlouhé, říkám těmto znakům „prokaždítko“ a „existítko“, zatím se to neujalo, ale když se všichni přidáte, časem to přijde.

Při hrátkách s výroky pomáhají různá pravidla, asi nejdůležitější jsou tato:

- $\neg[\forall x \in M\colon p(x)] \equiv \exists x \in M\colon \neg p(x)$;
- $\neg[\exists x \in M\colon p(x)] \equiv \forall x \in M\colon \neg p(x)$.

Opět je to jen selský rozum. Například opak výroku „všichni jsou tu matematici“ je „je tu alespoň jeden nematematik“. Můžete si rozmyslet, že nemůže existovat skupina lidí, ve které by tyto dva výroky měly stejnou pravdivost, dokonce i v prázdné množině první platí a druhý ne.

Mohli bychom teď uvést také pravidla popisující, jak kvantifikátory interagují s logickými spojkami, ale není cílem si je pamatovat, člověk by se měl s logikou natolik spřátelit, aby mu to přišlo jasné. Abyste měli důvod se nad nimi zamyslet, necháváme je jako cvičení 21b.4.

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):

$$\big[\forall x \in M\,\forall y \in M\colon p(x,y)\big] \equiv \big[\forall y \in M\,\forall x \in M\colon p(x,y)\big] \equiv \big[\forall x, y \in M\colon p(x,y)\big];$$
$$\big[\exists x \in M\,\exists y \in M\colon p(x,y)\big] \equiv \big[\exists y \in M\,\exists x \in M\colon p(x,y)\big] \equiv \big[\exists x, y \in M\colon p(x,y)\big].$$

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 míchají 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 hledáme k němu y bez ohledu na to, jak to dopadlo při předchozím hledání. Klidně těch y pro jedno x může být víc, hlavně aby bylo alespoň jedno.

Je náš výrok vlastně platný? Ano. Když nám někdo dá libovolné 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 je bonus, bez kterého bychom se klidně obešli, ale také nevadí. Neřeší se také, zda se náhodnou některá x neshodnou na jednom y, viz třeba $x = 6$ a $x = -6$.

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. Někdy ale univerzální prvky existovat mohou. Příklad: $\exists y \in \mathbb{R}\,\forall x \in \mathbb{R}\colon (|x| + 1)^y = 1$. Stačí totiž zvolit $y = 0$ a vlastnost bude pro všechna reálná x platit.

Pro praktickou práci v matematice je 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:

• $[\exists y \in M\, \forall x \in M\colon p(x,y)] \implies [\forall x \in M\, \exists y \in M\colon p(x,y)]$.

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 21b.4. 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:

$$\exists x \in \mathbb{R}\colon \big[x+1=14 \wedge \neg[\exists y \in \mathbb{R}\setminus\{x\}\colon y+1=14\,]\big].$$

Existují i jiné možnosti, jak to jedinečnost zapsat logicky, ale ty jsou ještě delší. 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 nepřibírají.

Pro další možnosti, jak vyjádřit, že je některý objekt jedinečný, se podívejte na cvičení 21b.2, které je vůbec dobrou průpravou na matematické vyjadřování.

Poznamenejme ještě, že vymezení kvantifikátorem se bere jako jeden celek s následujícím výrokem, což šetří závorky, například výraz $x=3 \wedge \exists y \in \mathbb{R}\colon y>x$ se chápe takto: $x=3 \wedge \big[\exists y \in \mathbb{R}\colon y>x\big]$.

21b.1 Poznámka: S proměnnými se váže jedna důležitá vlastnost, a to že jsou lokální a pracovní. Vysvětlíme to na příkladě.

Podívejme se na výraz $\sum_{i=1}^{3}(i+1)^2$. Ve skutečnosti to, co vidíme, je jen popiska, skutečná věc vypadá jinak: $2^2+3^2+4^2$. Jak vidíte, i se v tom čísle vůbec nevyskytuje. Jinými slovy, význam i je schován uvnitř té sumy, zvenčí jej není vidět. Je to tedy symbol pracovní, tudíž jej můžeme (všude v sumě) zaměnit za jiné písmenko (takové, které v dané chvíli nemá jiný význam), a bude to říkat stejnou věc, například $\sum_{j=1}^{3}(j+1)^2$ nebo třeba $\sum_{\alpha=1}^{3}(\alpha+1)^2$. To je někdy velmi užitečné.

Dále, jakmile se ze sumy dostaneme ven, můžeme zase i volně použít, například v jiné sumě: $\sum_{i=1}^{3}(i+1)^2+\sum_{i=0}^{5} i$. Jde jakoby o dvě různá i, programátoři to dobře znají. To je právě ta inzerovaná lokálnost významu.

Úplně stejná věc platí pro proměnné v logických výrazech. Když napíšeme $\forall x \in \mathbb{R}\colon x^2 \geq 0$, je to naprosto totéž, jako bychom napsali $\forall h \in \mathbb{R}\colon h^2 \geq 0$. Můžeme také napsat $\big[\exists n \in \mathbb{Z}:\ n>12\big] \wedge \big[\exists n \in \mathbb{Z}:\ n<5\big]$ a je to pravdivý výrok, protože ta n v levém a pravém kvantifikátoru jsou jakoby různá n. Stačí ale změnit závorku a situace je jiná: $\exists n \in \mathbb{Z}:\ [n>12 \wedge n<5]$. Tento výrok již neplatí, jde o jedno a totéž n.

Hlavní vzkaz této poznámky je, že není dobré vázat se na konkrétní písmenka, ale spíše se soustředit na významy. Při praktické práci bývá často užitečné si písmenko změnit o své vůli. Může se třeba stát, že pracujeme zároveň se dvěma výroky, oba pracují se „svou“ proměnnou x, čímž začneme mít zmatek v tom, které x se zrovna používá. Obvykle se to dá zvládnout, ale je mnohem snazší (a pro čtenáře přehlednější), když si hned na začátku jeden z těch výroků přepíšeme tak, aby používal jinou proměnnou, rozličná písmena pak na první pohled ukazují, s čím se zrovna pracuje. Toto občas bývá velmi užitečné v důkazech, někdy je to dokonce vynuceno, beze změny písmene by to nešlo.

△

Cvičení

Cvičení 21b.1: Připomeňme, že $\mathbb{R}$ značí množinu všech reálných čísel a $\mathbb{Z}$ množinu všech celých čísel. Rozhodněte, zda jsou pravdivé následující výroky:

a) $\forall x \in \mathbb{R}\colon [x \geq 3 \vee x<5\,]$;
b) $\exists x \in \mathbb{R}\colon [x \geq 3 \wedge x<0\,]$;
c) $\forall x \in \mathbb{Z}\colon [x>3 \wedge x<7\,]$;
d) $\exists x \in \mathbb{Z}\colon [x \geq 3 \wedge x<5\,]$;
e) $\forall x \in \mathbb{R}\colon [x>3 \implies x^2>9\,]$;
f) $\forall x \in \mathbb{R}\colon [x^2>9 \implies x>3\,]$;
g) $\forall x \in \mathbb{R}\colon [x^2<0 \implies x=13\,]$;
h) $\exists x \in \mathbb{R}\colon [x \geq 5 \implies x^2=40\,]$;
i) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x+y=0$;
j) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon x+y=0$;
k) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x\cdot y=0$;
l) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon x\cdot y=0$;
m) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon \frac{x}{y}=1$;
n) $\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\colon \frac{x}{y}=1$;
o) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x<3y$;
p) $\exists y \in \mathbb{Z}\, \exists x \in \mathbb{Z}\colon x^2-y^2=3$.

Cvičení 21b.2: Uvažujme nějakou konkrétní (neprázdnou) množinu lidí L, v jejímž rámci budeme dále pracovat. Zavedeme si následující predikáty: $m(x)$ znamená, že člověk x je matematik, $n(x)$ znamená, že člověk x je normální, a $b(x,y)$ znamená, že člověk x je větší borec než člověk y.
Následující výroky zapište pomocí logického jazyka a právě zavedených množin a predikátů.
a) Matematici nejsou normální.
b) Matematici jsou větší borci než nematematici.
c) Pokud Lojza není normální, tak už nikdo.
d) Je jen jeden matematik.
e) Nikdy není jen jeden matematik.
f) Jsou dva matematici.
g) Lojza je největší borec.
h) I matematik může být normální.
i) Jedině matematici můžou být normální.
j) Lojza s Pepou jsou buď oba normální, nebo oba nenormální.

Cvičení 21b.3: Následující výrazy s proměnnou z $\mathbb{R}$ upravte pomocí distributivního zákona a pak zjednodušte:
a) $x > 3 \wedge [e^x = x^5 \vee x = 4\,]$;
b) $x < 13 \wedge [x^2 < 4 \vee x > 14\,]$;
c) $[\sin(x) < x^3 \wedge x < 3\,] \vee [\sin(x) < x^3 \wedge x > 1\,]$.

Cvičení 21b.4: Rozhodněte, zda platí obecně (tedy pro libovolné množiny M a výroky p, q) následující tvrzení o logické ekvivalenci dvou kvantifikovaných výroků. Pokud máte pocit, že některá dvojice kvantifikovaných výroků ekvivalentní není, tak najděte příklad takových výroků p, q a množiny M, aby jeden z kvantifikovaných výroků platil a druhý ne.
a) $\forall x \in M\colon [p(x) \wedge q(x)] \equiv [\forall x \in M\colon p(x)] \wedge [\forall x \in M\colon q(x)]$;
b) $\forall x \in M\colon [p(x) \vee q(x)] \equiv [\forall x \in M\colon p(x)] \vee [\forall x \in M\colon q(x)]$;
c) $\exists x \in M\colon [p(x) \wedge q(x)] \equiv [\exists x \in M\colon p(x)] \wedge [\exists x \in M\colon q(x)]$;
d) $\exists x \in M\colon [p(x) \vee q(x)] \equiv [\exists x \in M\colon p(x)] \vee [\exists x \in M\colon q(x)]$;
e) $p \wedge [\forall x \in M\colon q(x)] \equiv \forall x \in M\colon [p \wedge q(x)]$;
f) $p \vee [\forall x \in M\colon q(x)] \equiv \forall x \in M\colon [p \vee q(x)]$;
g) $p \wedge [\exists x \in M\colon q(x)] \equiv \exists x \in M\colon [p \wedge q(x)]$;
h) $p \vee [\exists x \in M\colon q(x)] \equiv \exists x \in M\colon [p \vee q(x)]$.

Cvičení 21b.5: 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.
a) $\exists x \in \mathbb{R}\colon x > 5$;
b) $\forall x \in \mathbb{Z}\colon [x > 5 \vee x^2 = 14\,]$;
c) $\exists x \in \mathbb{R}\colon [x < 3 \implies x = x - 1\,]$;
d) $[\forall x \in \mathbb{R}\colon x^2 \geq 0\,] \implies [\forall x \in \mathbb{R}\colon x < 0\,]$;
e) $[\exists x \in \mathbb{R}\colon x = \frac{x}{2}\,] \implies [\forall x \in \mathbb{R}\colon x = 13x]$;
f) $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon x < y$;
g) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon x^2 + y^2 \geq 0$;
h) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon \sin(x) = \cos(y)$.

Řešení:

21b.1: a) platí. b) neplatí (podmínky se vylučují). c) neplatí (pro některá x obě nerovnosti platí, ale to nestačí). d) platí, $x = 3$ nebo $x = 4$. e) platí. f) neplatí, protipříklad $x = -4$. g) platí (předpoklad není nikdy splněn, proto je implikace pravdivá). h) platí, $x = \sqrt{40}$ nebo třeba $x = 0$. i) platí, $y = -x$. j) neplatí. k) platí, $y = 0$. l) platí, $y = 0$. m) neplatí, pro $x \neq 0$ sice najdeme $y = x$, ale pro $x = 0$ to zařídit nejde. n) neplatí. o) platí, stačí zvolit třeba $y = |x| + 1$. p) platí, $x = 2$ a $y = 1$ (všimněte si, že kdyby tam bylo $x^2 - y^2 = 2$, tak už by to neplatilo).
21b.2: U převod přirozeného jazyka do logiky často narážíme na problém, že původní jazyk není přesný a tudíž mnohdy není jasné, co se tím vlastně míní. Nějak tím zkusíme prokličkovat.
a) Dvě možnosti, jak se omezit pouze na matematiky. Implikace: $\forall x \in L\colon [m(x) \implies \neg n(x)]$.
Vytvořením množiny: $\forall x \in \{z \in L;\ m(z)\}\colon \neg n(x)$.
b) $\forall x, y \in L\colon \big[[m(x) \wedge \neg m(y)] \implies b(x,y)\big]$.
Šlo by i pomocí vhodných množin: Nechť $M = \{z \in L;\ m(x)\}$. Pak výrok zní $\forall x \in M\, \forall y \in L \setminus M\colon b(x,y)$.
c) $\neg n(\text{Lojza}) \implies [\forall x \in L\colon \neg n(x)]$.
d) Jsou to dva výroky, že existuje a že jich není víc. To druhé se dá vyjádřit více způsoby.
$\exists x \in L\colon \big[m(x) \wedge \forall y \in L \setminus \{x\}\colon \neg m(y)\big]$.
Nebo $\exists x \in L\colon \big[m(x) \wedge \forall y \in L\colon [y \neq x \implies \neg m(y)]\big]$. Nebo $\exists x \in L\colon \big[m(x) \wedge \forall y \in L\colon [m(y) \implies x = y]\big]$.
Poznámka: Tento poslední trik je u matematiků obzvláště oblíbený.

Poznámka: Výrok $[\exists x \in L\colon m(x)] \wedge [\forall y \in L \setminus \{x\}\colon \neg m(y)]$ není správný, protože se vymezení x nevztahuje na druhý výrok, tam je x neurčeno, což by nemělo být.

e) $\neg[\exists! x \in L\colon m(x)]$. Ale $\exists!$ se snažíme vyhýbat, chce to alternativu: Vždy jsou alespoň dva, nebo taky žádný.
$\big[\exists x, y \in L\colon [x \neq y \wedge m(x) \wedge m(y)]\big] \vee [\forall x \in L\colon \neg m(x)]$.

f) Tohle je kombinace „jsou alespoň dva“ a „není víc“.
$\exists x, y \in L\colon \big[x \neq y \wedge m(x) \wedge m(y) \wedge \forall z \in L \setminus \{x, y\}\colon \neg m(z)\big]$.

g) $\forall x \in L\colon [x \neq \text{Lojza} \implies b(\text{Lojza}, x)]$. Pokud bychom napsali jen $\forall x \in L\colon b(\text{Lojza}, x)$, tak by to znamenalo, že Lojza je větší borec než on sám, což je nesmysl. Není ale nesmyslem se zeptat, co se tím „největší borec“ vlastně v přirozeném jazyce míní. Připouští to i remízu? V kapitole uvidíme, že matematická definice „největšího“ ano. Pak by být nejvyšším znamenalo, že všichni včetně Lojzy jsou „menší borci nebo stejní borci“, ale pro to druhé nemáme značení, tak to asi máme ignorovat.

h) Tady není úplně jasné, co se tím míní. Jedna možnost je brát to jako popření výroku „matematici nejsou normální“: $\neg\big[\forall x \in L\colon [m(x) \implies \neg n(x)]\big]$.

Je možné to také brát jako závěr z objevení normálního matematika: $\exists x \in L\colon [m(x) \wedge n(x)]$.

Pokud aplikujeme pravidla pro negaci a operace, zjistíme, že nakonec oba výroky říkají totéž.

i) To je opět trochu trikové. Tím se neříká, že jsou, jen že mohou. Takže nebudeme moci použít implikaci typu $m(x) \implies$. Skutečný význam této věty je tedy vymezující: Pokud někdo matematik není, pak nemůže být normální: $\forall x \in L\colon [\neg m(x) \implies \neg n(x)]$.

Jinak řečeno, když už vidíme někoho normálního, tak jedině matematika: $\forall x \in L\colon [n(x) \implies m(x)]$.

Ty implikace jsou samozřejmě totéž, jde o obměnu.

j) Doslovně: $[n(\text{Lojza}) \wedge n(\text{Pepa})] \vee [\neg n(\text{Lojza}) \wedge \neg n(\text{Pepa})]$. Ono to ale znamená, že musejí mít stejnou hodnotu normálnosti, tedy zkráceně takto: $n(\text{Lojza}) \iff n(\text{Pepa})$.

21b.3: a) $\equiv [x > 3 \wedge e^x = x^5\,] \vee [x > 3 \wedge x = 4\,] \equiv [x > 3 \wedge e^x = x^5\,] \vee x = 4$.

b) $\equiv [x < 13 \wedge x^2 < 4\,] \vee [x < 13 \wedge x > 14\,] \equiv [x^2 < 4\,] \vee F \equiv x^2 < 4$.

c) $\equiv \sin(x) < x^3 \wedge [x < 3 \vee x > 1\,] \equiv \sin(x) < x^3 \wedge T \equiv \sin(x) < x^3$.

21b.4: a) platí. Oba výrazy vyžadují platnost p i q pro všechna x.

b) neplatí, jde jen v jednom směru. Pokud platí výrok napravo, tak už platí i výrok nalevo. Pravý výrok totiž vynutí platnost p vždy, pak platí i $p \vee q$, nebo q vždy, pak platí i $p \vee q$. Ale platnost levé strany lze dosáhnout tím, že p a q se při vyrábění pravdivosti $p \vee q$ střídají pro různá x, pak ani jeden neplatí vždy. Příklad: $M = \mathbb{R}$, $p(x)$: $x \geq 13$, $q(x)$: $x < 13$.

c) 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: $M = \mathbb{R}$, $p(x)$: $x = 13$, $q(x)$: $x = 14$.

d) platí. Výrok nalevo i výrok napravo požadují, aby šlo alespoň jeden p, q alespoň jednou volbou x splnit.

e) platí. Výrok nalevo i výrok napravo požadují, aby platilo jak p, tak $q(x)$ pro všechna x.

f) 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.

g) platí. Oba výroky požadují, aby platilo jak p, tak $q(x)$ pro nějaké x.

h) 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.

21b.5: a) negace: $\forall x \in \mathbb{R}\colon x \leq 5$. Výrok platí, negace ne, třeba $x = 7$.

b) negace: $\exists x \in \mathbb{Z}\colon [x \leq 5 \wedge x^2 \neq 14\,]$. Výrok neplatí, negace ano, třeba $x = 2$.

c) negace: $\forall x \in \mathbb{R}\colon [x < 3 \wedge x \neq x - 1\,]$. Výrok platí (třeba $x = 0$, pak má implikace nesplněný předpoklad a tudíž platí), negace ne.

d) negace: $[\forall x \in \mathbb{R}\colon x^2 \geq 0\,] \wedge [\exists x \in \mathbb{R}\colon x \geq 0\,]$. Výrok neplatí, negace ano.

e) negace: $[\exists x \in \mathbb{R}\colon x = \frac{x}{2}\,] \wedge [\exists x \in \mathbb{R}\colon x \neq 13x]$. Výrok neplatí (předpoklad splněn $x = 0$, závěr ne), negace ano (první výrok splněn $x = 0$, druhý také $x = 1$).

f) negace: $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x \geq y$. Výrok neplatí (to by muselo existovat jedno číslo, které je nejmenší ze všech reálných), negace ano (pro dané x stačí zvolit $y = x - 1$).

g) negace: $\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\colon x^2 + y^2 < 0$. Výrok platí, negace ne.

h) negace: $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\colon \sin(x) \neq \cos(y)$. 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 $\sin(x)$).

21c. Implikace a usuzování

Uvažujme implikaci $p \implies q$, která může a nemusí být pravdivá. To, že pravdivá je, se někdy vyjadřuje slovy „p je postačující podmínka pro q“, popřípadě „q je nutná podmínka pro p“.

S implikací $\implies q$ je spojená její **obměna** $\neg q \implies \neg p$, která má stejnou pravdivostní hodnotu a tedy říká totéž, ale někdy nabídne užitečný alternativní pohled.

Ilustrujeme to na výrocích p: „Člověk x má alespoň 21 let“ a q: „Člověk x má alespoň 18 let“.

- $p \implies q$: „Jestli je někomu alespoň 21, tak je mu alespoň 18.“
- „Dožít se alespoň 21 je postačující k tomu, aby se zaručeně dožil 18.“
- „Je nutné dožít se alespoň 18, aby se člověk dožil 21.“
- „Pokud se někdo nedožil 18, tak se nedožil ani 21.“

Existují země, kde 18 je hranice pro řízení auta a 21 je hranice pro pití alkoholu. Implikace $p \implies q$ se pak dá vyjádřit slovy „pokud můžeš chlastat, můžeš i řídit“, což zní podezřele a raději tento příklad opustíme.

Základní otázkou filosofie a později věd je, nakolik dokážeme spolehlivě z nějakých známých faktů odvodit nějaký další čistě na základě logické souvislosti. Formálně řečeno, máme nějaké výroky p_1 až p_n, o kterých si myslíme, že jsou pravdivé. Je pak nutně pravdivý také výrok q, který s nimi nějak logicky souvisí? Pokud ano, pak řekneme, že jsme q odvodili z předpokladů p_1 až p_n.

Intuitivně správnost takového odvození souvisí s platností implikace $(p_1 \wedge \cdots \wedge p_n) \implies q$, ale není to zcela totéž. Proto se odvozováním zabývá speciální podobor logiky, který má své značení. Pokud lze z nějaké množiny faktů M spolehlivě odvodit závěr q, zapíšeme to jako $M \models q$. Moderní jazyk logiky nabízí odvozovací pravidla a také spolehlivé metody, jak rozpoznat, zda je $M \models q$ správně či ne (metoda resolvent). Ve středověku se namísto toho pracovalo s modelovými situacemi. Ukažme si dvě situace, se kterými se běžně při usuzování potkáváme.

Začneme pravidlem $\{p \implies q,\ p\} \models q$. V anglosaské literatuře se s oblibou vystihuje schématem napravo a funguje následovně. Víme, že platí implikace $p \implies q$, tedy v její pravdivostní tabulce je řádek s nulou coby výsledkem nemožný. Také víme, že platí p, takže nemožné jsou také řádky s nulou u p. Zbyl jen jediný možný řádek, ten má u q jedničku.

$$\begin{array}{l} p \implies q \\ p \\ \hline \therefore q \end{array}$$

Za středověku tomu říkali „modus ponens“ a studenti universit se to učili na vzorových příkladech. Třeba takto:

- Platí: Lidé mají duši. (Formálně: X je člověk $\implies$ X má duši)
- Platí: Bonifác je člověk.
- Závěr: Bonifác má duši.

Druhé základní pravidlo zní $\{p \implies q, \neg q\} \models \neg p$. Je to argument sporem. Pokud by p platilo, tak by podle modus ponens muselo platit i q. Ale q neplatí, proto také nemůže platit p. Za středověku tomu říkali „modus tollens“.

$$\begin{array}{l} p \implies q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

- Platí: Lidé mají duši.
- Platí: Bonifác nemá duši.
- Závěr: Bonifác není člověk. (Je to starostův kocour.)

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 doporučujeme přečíst si nějakou pěknou knížku), ale pro běžnou matematickou práci v zásadě stačí to, co vidíme výše.

21d. Důkazy

Důkaz matematického tvrzení je esej, ve které čtenáře přesvědčíme o pravdivosti dokazovaného tvrzení pomocí již známých faktů, které (s případnými předpoklady) spojujeme logicky korektními způsoby a odvozovacími kroky, dokud se nedostaneme k žádanému tvrzení. Ona korektnost při přechodu od jedněch faktů k novým zjevně souvisí s usuzováním.

Struktura důkazu záleží na struktuře tvrzení a zvoleném přístupu, takže zejména u komplikovanějších a hlubších tvrzení se dá čekat cokoliv, ale u jednodušších tvrzení se dají vysledovat určité zákonitosti, které napomohou při vytváření důkazu.

Základním pravidlem je, že argumenty (odvozovací kroky) vždy mohou vést jen od toho, co je již známo či předpokládáno, k závěru. To, co dokazujeme, ještě známo není, a proto to v důkazu nesmíme použít.

Někdy chceme tvrzení vyvrátit, což v matematice znamená ukázat, že není pravdivé.

Většina matematických tvrzení začíná kvantifikátorem, což představuje první rozcestí při rozhodování, kudy se má důkaz ubírat.

• $\exists x \in M$: $p(x)$.

Pokud tvrzení začíná existítkem, pak je (přirozeně) třeba ukázat, že existuje nějaké x žádané vlastnosti. Občas se povede takový prvek konkrétně najít či zkonstruovat pomocí známých vstupů. Tak tomu bylo v případě existenčních tvrzení v této knize (např. že rovnice má řešení).

Často to ale tak snadné není a existence se odvozuje teoreticky. To bývá velice komplikované a nejsou k tomu obecné návody, proto se zde touto situací nebudeme zabývat.

Ukázkové tvrzení: $\exists n \in \mathbb{Z}$: $n^2 = 16$.

Důkaz: Číslo $n = 4$ splňuje žádanou vlastnost.

Jak se dokazuje, že existenční výrok neplatí? Selský rozum napoví, že je potřeba vyloučit všechny možné kandidáty. Tuto představu nám potvrdí formální logika. Abychom dokázali, že neplatí výrok $\exists x \in M$: $p(x)$, je třeba dokázat, že platí jeho negace, což je podle pravidel výrok $\forall x \in M$: $\neg p(x)$. Tedy opravdu vylučujeme všechny kandidáty.

• $\forall x \in M$: $p(x)$.

Většina matematických tvrzení začíná kvantifikátorem obecným (prokaždítkem). Pak je třeba potvrdit, že výrok $p(x)$ platí pro všechny možné volby prvku x. Když je množina M malá, pak je možné prostě všechny možnosti postupně probrat. Směšně jednoduchý příklad: Jestliže $x \in \{-1, 2\}$, pak $x^4 - 5x^2 + 4 = 0$. Tvrzení dokážeme tak, že čísla $x = -1$ a $x = 2$ prostě dosadíme a uvidíme, že rovnost platí.

V typickém případě je množina M příliš velká, například nekonečná. Pak se zvolí generický zástupce (nekonkrétní) a pro něj se tvrzení ukáže čistě na základě toho, že má vlastnosti prvků množiny M.

Tvrzení: $\forall n \in \mathbb{N}$: $2n > 0$.

Důkaz: Vezměme libovolné $n \in \mathbb{N}$. Protože je to přirozené číslo, splňuje $n > 0$. Když tuto nerovnost vynásobíme dvěma, dostaneme $2n > 0$.

Postup je samozřejmě možné přizpůsobit konkrétní situaci. Zajímavá je například možnost, že si množinu M rozdělíme na podmnožiny a pro každou z nich děláme důkaz $p(x)$ zvlášť, často se tak děje proto, že některé konkrétní x jsou výjimečné a vlastnost $p(x)$ pro ně dokazujeme individuálně, pro ostatní pak hromadně.

K vyvrácení obecného výroku potřebujeme najít „protipříklad“, tedy konkrétní prvek (prvky), pro který tvrzení neplatí. Dokazujeme tak vlastně negaci původního tvrzení, která je podle pravidel rovna $\exists x \in M$: $\neg p(x)$.

Nyní ukážeme důkazy několika jednoduchých tvrzení. Obsah těchto tvrzení nás příliš nezajímá, ani konkrétní triky, kterými se k nim v důkazu dostaneme, pozornost věnujeme struktuře důkazu.

Příklad 21d.a: U následujících tvrzení si vždy nejprve ujasněte, co vlastně říkají, a rozhodněte sami o jejich pravdivosti. Můžete si i zkusit důkaz, než se podíváte na ten napsaný.

Tvrzení: $\forall x \in \mathbb{R}$: $x^2 + 1 > 0$.

Důkaz: Nechť $x \in \mathbb{R}$ je libovolné. Pak $x^2 \geq 0$. Když k této nerovnosti přičteme jedničku, dostáváme $x^2 + 1 \geq 1$. Protože také $1 > 0$, dostáváme $x^2 + 1 > 0$.

Poznámka: Šťouravý čtenář může namítnout, že v důkazu jsou mezery. Neukázali jsme, proč $x^2 \geq 0$, ani proč lze vzít dvě nerovnosti typu $a \geq b$, $b \geq c$ a spojit je do jedné $a \geq c$. Důvod je praktický. Kdybychom chtěli dokazovat úplně všechno, tak bychom se v každém důkazu museli prodrat až k samotným základům matematiky a typický důkaz by zabral jednu knihu. Proto se obvykle zvolí určitá úroveň znalostí, která se považuje za jasnou.

Tvrzení: $\forall x \in \mathbb{R}$: $x(x + 3) > 0$.

Důkaz, že není pravdivé: Číslo $x = -2$ je protipříkladem.

Tvrzení: $\exists x \in \mathbb{R}$: $x(x + 3) > 0$.

Důkaz: Číslo $x = 13$ vyhovuje žádané podmínce.

Tvrzení: $\forall n \in \mathbb{Z}$: $n \leq n^2$.

S **Rozbor:** Co se dá dělat s nerovností $n \leq n^2$. Například vykrátit to n, pokud je tedy kladné, pak vznikne $1 \leq n$, což je pravda pro spoustu celých čísel. Tento postup tedy dokáže tvrzení, ale jen pro čísla $n \geq 1$. Ještě si musíme dát pozor, až to budeme psát, že nesmíme začít s $n \leq n^2$ a skončit s $1 \leq n$, to by náš důkaz vedl špatným směrem. My musíme skončit tím, co dokazujeme, tedy tím $n \leq n^2$, a začít něčím známým, v tomto případě tím $n \geq 1$.

Protože žádanou nerovnost umíme dokázat jen pro část $\mathbb{Z}$, budeme se muset nějak vypořádat se zbývajícími čísly. To je možné, namísto hromadného zpracovávání celé dané množiny ji můžeme probírat po částech. Postatné je, že se pro každou část dojde k žádanému cíli.

Důkaz: Nechť $n \in \mathbb{Z}$ je libovolné. Rozebereme tři případy.

1) Jestliže $n \geq 1$, tak vynásobením této nerovnosti (kladným) číslem n dostáváme $n^2 \geq n$, přesně jak jsme potřebovali.

2) Jestliže $n = 0$, tak $n \leq n^2$ zní $0 \leq 0$, což je pravda.
3) Jestliže $n < 0$, tak tuto nerovnost lze spojit s nerovností $0 \leq n^2$ platnou pro všechna (celá) čísla a opět dostáváme $n \leq n^2$.
Protože naše varianty pokryly celou množinu $\mathbb{Z}$, je důkaz hotov.
△

Procesu, kdy se v důkazu probíráme všemi možnými cestami, se anglicky říká „exhaustion argument“ neboli „důkaz vyčerpáním“, myslí se tím všech možností, ale často také čtenáře a nezřídka i autora. Jsou důkazy, kde je těch možností několik set, asi nejslavnější je důkaz věty o obarvení grafu.
Podstatné je, že jednotlivé varianty musí nutně dohromady pokrýt celou množinu, o které něco dokazujeme (pokud se překrývají, není to problém, ale je to zbytečné), a všechny cesty musí dojít k tomu, co dokazujeme (nebo se některé cesty mohou ukázat jako slepé, tedy že neobsahují žádné prvky, protože takovou variantou se dokazované tvrzení nedá zneplatnit).
Výraznou úsporou může být, pokud jsou některé situace obdobné a jejich případy by se řešily stejně, jen se záměnou písmen, popřípadě jemnými (a zjevnými) modifikacemi, pak se obvykle objevují fráze jako „důkaz je obdobný předcházejícímu“.
V případě více kvantifikátorů se s nimi vypořádáváme postupně, jak přicházejí.

Příklad 21d.b: Tvrzení: $\forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}$: $x + y = 1$.
V části 21b jsme si rozmysleli, co toto vlastně znamená (ke každému x hledáme individuální y). Teď dokážeme, že to u našeho tvrzení platí.
Začneme prvním kvantifikátorem. Ten říká, že důkaz má vypadat následovně:
Důkaz: Zvolme $x \in \mathbb{R}$ libovolné. Pak ... a proto platí výrok $\exists y \in \mathbb{Z}$: $x + y = 1$.
Čímž jsme se posunuli o kousek dál k otázce, jak by se dokázal výrok $\exists y \in \mathbb{Z}$: $x + y = 1$. A na to také známe odpověď, existenční výroky se nejlépe dokazují tak, že prostě předvedeme žádaný exemplář. Čímž se dostáváme k jádru důkazu: Když máme číslo x (nevíme jaké), jsme schopni dodat číslo y vyhovující podmínce? Nabízí se kandidát $y = 1 - x$. Tím je hotova myšlenka důkazu. Jdeme na to.
Důkaz: Mějme libovolné $x \in \mathbb{R}$. Pak číslo $y = 1 - x$ splňuje podmínky, že $y \in \mathbb{Z}$ a $x + y = x + (1 - x) = 1$.

Poznámka: Častou chybou je zapomenout zmínit, že $y \in \mathbb{Z}$. Zapomíná se na to tím spíš, že je to zcela zřejmé. Číslo x je celé, tudíž samozřejmě i číslo $1 - x$ je celé, proč by měl člověk něco tak jasného okecávat. Jenže ona specifikace, že $y \in \mathbb{Z}$, je součástí dokazovaného tvrzení, bez ní by už mělo jiný význam. Nejde jen o formalitu, jsou případy, kdy zrovna kvůli nemožnosti splnit takovou podmínku je celý výrok nepravdivý. Je proto důležité to v důkazu zmínit, i když je to taková trivialitka, protože tím dáváme najevo, že jsme si vědomi důležitosti všech částí výroku, že jsme se nad tím zamysleli a že čtenář by měl také.
△

Kromě kvantifikátorů ovlivňuje strukturu důkazu to, jakou strukturu má dokazované tvrzení. Mezi matematickými větami s výrazným náskokem vedou implikace, je jich naprostá většina. Dokonce i tvrzení jiného typu nakonec často končí dokazováním nějaké implikace, například ekvivalence se obvykle dokazuje potvrzením platnosti implikace v obou směrech. Umět dokazovat implikace je tedy základ, od kterého se odvíjí vše další.
V zásadě existuje jeden univerzální typ důkazu implikace, a to je

21d.1 Přímý důkaz

Přímý důkaz implikace $p(x) \implies q(x)$ probíhá tak, že pro zvolený prvek x předpokládáme platnost $p(x)$, tedy tato informace se stává povolenou pro použití v důkazu, a pomocí ní se dojde menšími (a proto kontrolovatelnými) kroky k tomu, že platí $q(x)$.
V důkazech je třeba rozlišovat mezi danými fakty a předpoklady. Proto u předpokladů je třeba o nich čtenáře informovat.

Příklad 21d.c: Dokážeme výrok $\forall x \in \mathbb{R}$: $[x > 13 \implies x + 10 > 23]$.
Dáno $x \in \mathbb{R}$. Předpokládejme, že $x > 13$. Přičtením desítky dostáváme $x + 10 > 23$.
△

Tento důkaz by se dal znázornit schématem $p \longrightarrow \cdots \longrightarrow q$. Vezmeme p, nějak s ním (korektně) zacvičíme a vyjde nám q. Obvykle jsou ještě třeba další fakty, třeba zde jsme použili to, že je možné k oběma stranám nerovnosti přičíst konstantu, takže typický důkaz tohoto typu by se dal vyjádřit schématem

$$\begin{array}{ccccc} & & f & & \\ & & \downarrow & & \\ p & \longrightarrow & r & \longrightarrow & q. \end{array}$$

Následující důkaz správně upozorňuje na rozdíl mezi předpokládaným a známým.

Příklad 21d.d: Dokážeme výrok $\forall x \in \mathbb{R}$: $[x \geq 21 \implies x \geq 18]$.

Dáno $x \in \mathbb{R}$. Předpokládejme, že $x \geq 21$. Také platí $21 \geq 18$, z dvojice $x \geq 21 \geq 18$ vyplyne $x \geq 18$.

△

Oblíbenou chybou je napsat důkaz implikace $p \implies z$ pozpátku, od závěru k předpokladu. Takový důkaz není platný. Vzniká nepochopením užitečného triku. Někdy neumíme vymyslet řetěz kroků, který by nás od předpokladu p přivedl k závěru z. Pak může pomoci, když závěr přeformulujeme, abychom se do něj mohli lépe trefit, nebo se zamyslíme, jaký poznatek by nás k němu mohl dovést. Jinými slovy, jakoby si „jdeme naproti“.

$$p \longrightarrow \qquad\qquad x \longleftarrow y \longleftarrow z.$$

Někdy se tak dá dojít k p, ale tím vznikne cesta $z \longrightarrow p$, což je něco jiného, než zkoušíme dokázat, a je to tedy k ničemu. Pointa tohoto přístupu je, že získáním náhradního cíle se pak od p namísto do z trefujeme do x, což se často dobře podaří.

$$p \longrightarrow q \longrightarrow r \longrightarrow x \longleftarrow y \longleftarrow z.$$

Tím ale nevznikne důkaz, protože směry šipek nelze navázat. Aby to šlo zachránit, tak je potřeba, aby ty šipky v pravé polovině vedly obousměrně:

$$p \longrightarrow q \longrightarrow r \longrightarrow x \longleftrightarrow y \longleftrightarrow z.$$

Jedině pak totiž máme šanci všechny kroky správně uspořádat a znovu napsat tak, aby tvořily ucelený přechod od známého k tomu, co chceme:

$$p \longrightarrow q \longrightarrow r \longrightarrow x \longrightarrow y \longrightarrow z.$$

Další oblíbenou chybou je využít v důkazu předpoklad i závěr a dojít k nějaké banalitě typu $0 = 0$. Tím se dokáže správnost odvození $(p \wedge z) \longrightarrow T$, což opět nemá nic společného s implikací $p \implies z$.

21d.2 Nepřímý důkaz

Namísto žádané imolikace dokazujeme její obměnu, což pak děláme přímým důkazem.

Příklad 21d.e: Dokážeme, že pro každé $x \in \mathbb{R}$ platí: Jestliže $x^2 \neq 0$, pak $x \neq 0$.

Toto je evidentně pravdivé a jasná je také struktura důkazu. Vezme se libovolné $x \in \mathbb{R}$, předpokládá se $x^2 \neq 0$ a nějak se doskáče k $x \neq 0$. Má to drobný zádrhel. Máme spoustu triků, které jde provádět s rovností, ale nemáme triky pro „ne-rovnost“. Problém vyřeší, když jednotlivé části znegujeme, což nám umožní právě obměna. Důkaz:

Vezměme libovolné $x \in \mathbb{R}$. Dokážeme pro něj obměnu tvrzení, tedy implikaci $x = 0 \implies x^2 = 0$. Předpokládejme proto, že $x = 0$. Pak $x^2 = x \cdot x = 0 \cdot 0 = 0$.

△

21d.3 Důkaz sporem

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 jsme začali špatně, tedy neplatnost r nemůže nastat neboli r platí.

Formální logika to potvrdí: 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, například se tak často dokazuje neexistence nějakého objektu.

Příklad 21d.f: Dokážeme, že neexistuje číslo $z \in \mathbb{R}$ takové, že pro všechna $x \in \mathbb{R}$ platí $x + z = 0$.

Sporem: Předpokládejme platnost negace, tedy že takové číslo z existuje. Pokud použijeme jeho vlastnost s $x = 2$ a $x = 1$, dostáváme rovnosti $2 + z = 0$ a $1 + z = 0$. Když odečteme druhou rovnici od první, vyjde nám $1 = 0$, což je zjevný spor.

△

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.